QBank Quiz May 3, 2022

Test ID: 207715745

Question #1 of 200

Question ID: 1299601

As part of implementing a vulnerability management process for your company, you are currently documenting the business processes. This includes documenting how transactions occur and which systems participate in business transactions. Which effect on the vulnerability scanning frequency are you currently documenting?

- ✗ **A)** Technical constraints
- ✗ **B)** Risk appetite
- ✗ **C)** Regulatory requirements
- ✓ **D)** Workflow

Explanation

You are currently documenting workflow as part of determining the vulnerability scanning frequency. This workflow will help provide business constraints. For example, a SQL server that is used for e-commerce transactions in a 24/7 environment might be adversely affected by vulnerability scans. However, because of the high risk for this asset, it may be necessary to increase the scan rate.

Regulatory requirements include any laws or regulations that may dictate a minimum frequency for vulnerability scans.

Technical constraints include any constraints that are in place that may limit the scanning frequency, such as performance or licensing limitations.

Risk appetite is the level of risk that an organization is willing to accept. A higher risk appetite would translate into a lower scanning frequency, while a lower risk appetite would translate into a higher scanning frequency.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #2 of 200

Question ID: 1299801

Which of the following acts as the network defense team in a training exercise?

- ✗ **A)** White team
- ✓ **B)** Blue team
- ✗ **C)** Yellow team

- ✗ **D)** Red team

Explanation

It is a convention in security training exercises that the Blue team acts as the network defense team. The Red team attempts an attack to test the Blue team's ability to respond to the attack. This serves as practice for a real attack. Their network defense tactics include accessing log data, using a SIEM, garnering threat intelligence information, and performing traffic and data flow analysis.

The White team is a group of technicians that referee the encounter between the Red team and the Blue team. Enforcing the rules of engagement might one of their roles, as well as monitoring the responses to the attack by the Blue team and making note of specific approaches employed by the Red team.

There is no Yellow team convention recognized for security training exercises.

The Red team acts as the attacking force. They typically carry out penetration tests in which they follow a well-established process of gathering information about the network, scanning the network for vulnerabilities and then attempting to take advantage of them. The actions they can take are established ahead of time in the rules of engagement. Often these individuals are third party contractors with no prior knowledge of the network. This helps to simulate attacks that are not inside jobs

Objective:
Compliance and Assessment

Sub-Objective:
Given a scenario, apply security concepts in support of organizational risk mitigation.

References:

Red Team Versus Blue Team: How to Run an Effective Simulation, http://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 20: Supporting Risk Mitigation

---

Question #3 of 200

Question ID: 1299707

Your company needs to ensure that all devices connecting to the network are prevented from introducing malware and other vulnerabilities into the network. This includes deploying patch management for systems and applications and hardening systems. What technique are you implementing?

- ✗ **A)** Sinkholes
- ✗ **B)** System isolation
- ✗ **C)** Network segmentation
- ✓ **D)** Endpoint security

Explanation

You are implementing endpoint security. Endpoint security involves protecting the endpoints (workstations, printers, and so on) in the network, including protecting them from other endpoints that spend at least some of the time outside the LAN. This is done by verifying patches and updates before the device is allowed access to the network. Endpoint security also includes the process of hardening endpoints.

You are not implementing network segmentation. Network segmentation involves dividing the network at either Layer 2 or Layer 3 to create desirable security barriers between devices in the network.

You are not implementing system isolation. Systems can be isolated from other systems through the control of communications with the device. For example, in Microsoft server isolation, you can use group policy settings to require that all communication with isolated servers must be authenticated and protected by using IPsec (and optionally encrypted as well). It also controls which devices can make the connection.

You are not implementing a sinkhole. A sinkhole is a routing mechanism that can route traffic from a device being flooded to a location where the traffic can be studied.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

What is Endpoint Security? Data Protection 101, https://digitalguardian.com/blog/what-endpoint-security-data-protection-101

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #4 of 200

Question ID: 1299761

Recently, your organization has become increasingly concerned with the security of interconnected networks. As a security analyst, you have been asked to provide vulnerabilities that can be associated with this. Which vulnerability should be of a primary concern?

- ✗ **A)** Trust relationships
- ✗ **B)** Dependency links
- ✗ **C)** Connectivity links
- ✓ **D)** Cascading failures

Explanation

Cascading failures should be of a primary concern to organizations that rely on interconnected networks. The Domain Name System (DNS) structure is an example of an interconnected network. DNS servers in the network rely on each other for communication and query information. Another example of cascading failures would be the failure of a SQL server that is used by both the warehouse and inventory application and the online sales application. If the SQL server goes down, the functionality of the warehouse and inventory application and the online sales application will also fail, resulting in a cascading failure. If networks are interconnected in a bus network, the failure of a main router could result in all networks down the line from the router being affected.

Trust relationships must exist between organizations to share authentication information, but they should not be a primary concern for interconnected networks.

Connectivity links and dependency links are not vulnerabilities. Rather, they help define the structure of interconnected networks. Connectivity links represent the ability of information to flow from one node to another. Dependency links represent the idea that a node requires support from another node, usually another network. When a network connects to and depends on another network, the pair of networks is interdependent.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Chapter 5 Vulnerability of Interdependent Networks and Networks of Networks, http://havlin.biu.ac.il/PS/Vulnerability%20of%20Interdependent%20Networks%20and%20Networks%20of%20Networks.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

---

Question #5 of 200

Question ID: 1299640

You need to control access to a server in your network to ensure that only authorized computers and devices are able to communicate with it. You need certain devices that are members of the same Microsoft domain to access the server, while ensuring that other devices do not. You need to implement the appropriate configuration to allow a few non-domain devices to authentication and connect with the server.

Which concept is this, and what configuration is needed to make it happen?

- ✗ **A)** Extranet, exception
- ✗ **B)** DMZ, acknowledgement
- ✓ **C)** System isolation, exception
- ✗ **D)** DMZ. exception

Explanation

This is an example of system isolation; in this case, it is Microsoft server isolation. The configuration required to allow the non-domain devices to be able to authenticate and connect with the server is called an exception.

Systems can be isolated from other systems through the control of communications with the device. By leveraging group policy settings, you can require that all communication with isolated servers must be authenticated and protected by using IPsec (and optionally encrypted as well). As group policy settings can ONLY be applied to computers that are domain members, devices that are not domain members must be specified as exceptions to the rules controlling access to the device if they need access.

This is not a demilitarized zone (DMZ), and an acknowledgement is used on an IDS to indicate that it has detected devices that are already known. A DMZ is a network logically separate from the intranet where resources that will be accessed from the outside world are made available without requiring authentication.

This is not an extranet. An extranet contains resources available only to certain entities from the outside world through access that is secured with authentication. Exceptions are used with server isolation, but not with extranets.

This is not a DMZ. A DMZ is a network logically separate from the intranet where resources that will be accessed from the outside world are made available. Exceptions are used with server isolation but not with DMZs.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Introduction to Server and Domain Isolation, https://technet.microsoft.com/en-us/library/cc725770(v=ws.10).aspx

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #6 of 200

Question ID: 1299703

The network team discovers that network performance is declining today. As a security analyst, you have been asked to help them view the packet payloads in an attempt to understand what types of error are occurring with several applications. Which type of tool would allow this?

- ✗ **A)** NetFlow analysis
- ✗ **B)** Traffic analysis
- ✓ **C)** Packet analysis
- ✗ **D)** Protocol analysis

Explanation

Packet analysis includes examining the entire packet, including the payload. In many cases, payload analysis is done when issues cannot be resolved by observing the header.

Protocol analysis involves examining information in the header of the packet. When protocol analyzers are used, they examine these headers for information, such as the protocol in use, and details involving the communication process, such as source and destination IP addresses and MAC addresses.

While protocol analysis looks at the information contained in the headers, and packet analysis looks at the contents of the payload, traffic analysis concerns itself with the types of traffic in the network. It does not examine the contents of the payload.

NetFlow is a technology that was developed by Cisco, and is since supported by all major vendors. NetFlow can be used to collect and subsequently export IP traffic accounting information. The traffic information is exported using UDP packets to a NetFlow analyzer, which can organize the information in useful ways. It exports records of individual one-way transmissions called flows. It is not concerned with the payloads.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

What's the difference between packet sniffers and protocol analyzers?, https://searchnetworking.techtarget.com/answer/Whats-the-difference-between-packet-sniffers-and-protocol-analyzers

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #7 of 200

Question ID: 1299782

Which two commands can be used to determine whether a device can communicate with another? (Choose two.)

- ✗ **A)** netstat
- ✗ **B)** ipconfig
- ✓ **C)** tracert
- ✓ **D)** ping
- ✗ **E)** nslookup

Explanation

The ping and tracert or traceroute commands can be used to determine if a device can communicate with another.

The ipconfig or ifconfig command can be used to display TCP/IP settings. The nslookup or dig command can be used to query DNS to obtain a host name or IP address. The netstat command is used to display protocol statistics.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

Using the ping command, https://technet.microsoft.com/en-us/library/dd469646(v=ws.10).aspx

How to Use Tracert to Identify Network Problems, https://www.howtogeek.com/134132/how-to-use-traceroute-to-identify-network-problems/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #8 of 200

Question ID: 1299590

You need to perform a vulnerability scan for all servers in the Research Department's subnet. The servers all use IP addresses in the 10.1.1.2 through 10.1.1.10 range. These servers contain highly confidential data.

You need to identify the correct scanning parameters for the servers. Match each configuration on the left with the appropriate scanning setting on the right.

{UCMS id=5765386102374400 type=Activity}

Explanation

The parameters for the vulnerability scan should be:

- Sensitivity level - Assessment scan
- Scope - 10.1.1.2 through 10.1.1.10
- Authentication - Credentialed

The sensitivity level is the type of scan (discovery scan or assessment scan). The scope is the range of computers you want to scan. The authentication method in this case should be credentialed because the servers contain confidential data.

A discovery scan simply provides an inventory of discovered hosts. An assessment scan will actually assess all the hosts based on the criteria given (such as IP address).

A credentialed scan will use login credentials of a privileged account to access data that is protected by access control lists (ACLs). A non-credentialed scan would be unable to scan certain areas on the hosts.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

Vulnerability Scanning 101, https://www.securitymetrics.com/learn/vulnerability-scanning-101

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #9 of 200

Question ID: 1299671

Your organization must comply with the regulations contained in PCI-DSS. One of your colleagues has become interested in adopting benchmarks specifically designed for this purpose that were created by a specific organization. This entity creates these benchmarks for the PCI-DSS compliance program as well as others. What organization is this?

- ✓ **A)** CIS
- ✗ **B)** NIST
- ✗ **C)** OWASP
- ✗ **D)** SANS

Explanation

Partly funded by SANS, the Center for Internet Security (CIS) is a not-for-profit entity known for supporting security in two ways:

- System design recommendations made through the publication of security controls for specific scenarios.
- Benchmarks or recommended technical settings for operating systems, middleware and software applications, and network devices. These benchmarks are directed at organizations that must comply with various compliance programs such as PCI-DSS (credit card data).

The SysAdmin, Audit, Network and Security (SANS) organization also provides guidelines for secure software development and they sponsor the Global Information Assurance Certification (GIAC). They also provide training, perform research, and publish best practices for cybersecurity, web security and application security.

The Open Web Application Security Project (OWASP) is a group that monitors attacks, specifically web attacks. OWASP maintains a list of the top ten attacks on an ongoing basis. This group also holds regular meetings at chapters throughout the world, providing resources and tools including testing procedures, code review steps, and development guidelines.

The National Institute of Standards and Technology (NIST) promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

Center for Internet Security (CIS): Who We Are, https://www.cisecurity.org/about/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

---

Question #10 of 200

Question ID: 1299653

Three companies need to allow their employees to seamlessly connect to each other's wireless corporate networks. As a security analyst for one of the companies, you suggest that the three companies keep one consistent wireless client configuration to make logging in easier.

Each company wants to maintain its own authentication infrastructure. They want to ensure that any employee who visits the other two companies will be authenticated by the home office when connecting to the other companies' wireless networks. You suggest that they implement 802.1x EAP-PEAP-MSCHAPv2 for client configuration. Which authentication mechanism should you suggest be used with single sign-on for this deployment?

✗ **A)** LDAP

✓ **B)** RADIUS

✗ **C)** Certificates

✗ **D)** Active Directory

Explanation

You should suggest that the companies implement RADIUS with single sign-on (SSO) for this deployment. 802.1x deployments require the use of a RADIUS server.

LDAP and Active Directory would not provide the required services for this deployment to work. 802.1x requires RADIUS to work.

While you could implement certificates as part of the deployment, the solution would still not work properly unless you deployed RADIUS.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

What is 802.1X?, http://www.networkworld.com/article/2216499/wireless/what-is-802-1x-.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #11 of 200

Question ID: 1299809

As a security analyst, you assess your company's current enterprise against several NIST standards for IT security. As a result of the assessment, you determine that several security controls need to be implemented. After providing your recommendations to management, you discover that three non-compliant systems must remain in their current configuration for business reasons. However, these three systems will be completely removed from the enterprise in six months. You need to ensure that these cases are documented appropriately. What should you do?

- ✗ **A)** Implement a configuration management process whereby these configurations are documented and tracked.
- ✗ **B)** Prepare a remediation plan whereby these systems are remediated within the next six months.
- ✗ **C)** Implement a change management process whereby these changes are documented and tracked.
- ✓ **D)** Implement an exception management process whereby these systems are documented and tracked.

Explanation

You should implement an exception management process whereby these systems are documented and tracked. This will ensure that any reports you must provide will include the documentation of these exceptions. It will also serve as a reminder to ensure that these systems are to be removed within six months.

You should not implement a change management process because you are not making any changes to the non-compliant systems. These systems will remain as they are until they are removed from the enterprise in six months.

You should not implement a configuration management process because these configurations are not being changed. Their configuration should already be documented.

You should not prepare a remediation plan because these systems are not being remediated in any way. They will remain as they are until they are removed from the enterprise in six months.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Exception Management Policy, https://informationsecurityprogram.com/exception-management-policy-best-practices/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

---

Question #12 of 200

Question ID: 1299587

Which of the following is the first step in a pen test?

- ✗ **A)** Gather information about attack methods against the target system or device.
- ✓ **B)** Document information about the target system or device.
- ✗ **C)** Execute attacks against the target system or device to gain user and privileged access.
- ✗ **D)** Document the results of the penetration test.

Explanation

The steps in performing a penetration test are as follows:

1. Document information about the target system or device.
2. Gather information about attack methods against the target system or device. This includes performing port scans.
3. Identify the known vulnerabilities of the target system or device.
4. Execute attacks against the target system or device to gain user and privileged access.
5. Document the results of the penetration test, and report the findings to management with suggestions for remedial action.

Document the results of the penetration test, and report the findings to management with suggestions for remedial action.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

Conducting a Penetration Test on an Organization, https://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #13 of 200

Question ID: 1299694

You are considering the purchase of a new IDS and a new antimalware system. You have compiled a list of requirements, and they include the following abilities:

- Recognize DoS and DDoS attacks as early as possible in the attack.
- Detect when a virus with no known attack signatures has infected a device.
- Recognize a port scan as soon as it starts.
- Detect unusually large volumes of data leaving the network.

What type of analysis must these devices be capable of to satisfy these requirements?

✗ **A)** Availability analysis

✗ **B)** Trend analysis

✗ **C)** Wireless analysis

✓ **D)** Behavioral analysis

Explanation

When a device is capable of behavioral analysis, it learns the patterns that exist in the network traffic flow, and therefore, can recognize behaviors that are not normal. It goes beyond anomaly detection by using models based on known intrusion procedures. It uses these tactics, techniques, and procedures (TTP) to make inferences about possible attacks, which makes it possible for it to satisfy all of the bulleted requirements.

Availability analysis is not what is required in this scenario. Availability analysis is used to calculate the relative availability of a device or network.

Wireless analysis is not what is required in this scenario. Wireless sniffers do not normally recognize certain behaviors.

Trend analysis is not what is required in this scenario. Trend analysis focuses on the long term direction in the increase or decrease in a particular type of traffic.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Intrusion Detection Systems vs. Network Behavior Analysis: Which Do You Need?, http://www.networkworld.com/article/2346145/cisco-subnet/intrusion-detection-systems-vs--network-behavior-analysis--which-do-you-need-.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #14 of 200

Question ID: 1299577

You just observed a meeting of the risk evaluation team. They were assigning the values of high, medium, and low to some threats they had identified. What part of risk evaluation are they performing?

- ✓ **A)** Technical impact review
- ✗ **B)** Technical control review
- ✗ **C)** Operational control review
- ✗ **D)** Regression analysis

Explanation

They are performing technical impact review. This is the process of assessing the potential impact of an event that is technical in nature. Once all assets have been identified and their value to the organization has been established, specific threats to each asset are identified. An attempt must be made to establish both the likelihood of the threat being realized, as well as the impact to the organization should that occur. This can be done by assigning values like high, medium, and low to the threats to describe their impact and likelihood.

This is not a part of a technical control review. After threats, likelihoods, and impacts are established, the security team should select controls that address the threat but do not cost more than the realized threat would cost. The review of these controls should be an ongoing process.

This is not part of an operational control review. Operational controls are the policies, procedures, and work practices that ether help to prevent the threat or make the threat more likely.

This is not regression analysis. Regression testing is a type of software testing performed after a change is made to ensure it still performs correctly.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, utilize threat intelligence to support organizational security.

References:

An Introduction to Information System Risk Management, https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 2: Utilizing Threat Intelligence

Question #15 of 200

Question ID: 1299796

In a presentation to the team, a vendor is describing an access control system in which users do not control access to resources. A department head classifies the sensitivity of each resource, and then access to resources is based on the sensitivity level assigned to users. What type of system is this?

- ✓ **A)** MAC
- ✗ **B)** NAC
- ✗ **C)** RBAC
- ✗ **D)** DAC

Explanation

This is mandatory access control (MAC), which prescribes that resources are classified by sensitivity and access is granted based in a sensitivity level assigned to users. It does not allow for user-controlled access.

In discretionary access control (DAC), a user is allowed to control access to a resource that he creates or owns.

In role-based access systems (RBAC), users have assigned roles, and along with those roles come a preconfigured set of rights and permissions.

Network Access Control (NAC) systems can make remote access decisions based on a combination of factors. However, they do not classify resources by sensitivity and allow access based on the sensitivity level assigned to a user.

Objective:
Compliance and Assessment

Sub-Objective:
Understand the importance of data privacy and protection.

References:

Mandatory Access Control, https://en.wikipedia.org/wiki/Mandatory_access_control

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 19: Data Privacy and Protection

Question #16 of 200

Question ID: 1299599

You have been asked to perform a vulnerability scan on all desktop computers used by the sales department, which are located throughout the network. You do not have a current inventory listing of these computers, so you decide to perform a discovery scan. Which scanning criteria have you already determined based on the type of scan being performed?

- ✗ **A)** Data type
- ✓ **B)** Sensitivity level
- ✗ **C)** Vulnerability feed
- ✗ **D)** Scope

Explanation

You have determined the scan's sensitivity level because you are performing a discovery scan, which is used to create an inventory of assets based on host or service discovery.

You have not determined the scope of the scan, which is the range of hosts or subnets included in the scan. The scenario specifically stated that the computers are located throughout the network.

You have not determined the data type, which is based on the data classification levels or on the file extension. Basing a scan on a data classification level will scan all data at that classification level across assets, such as all confidential files. Basing a scan on a data file extension will scan all files of that type across the assets, such as all .doc files.

You cannot determine the vulnerability feed. A vulnerability feed includes the updates to the vulnerability scanner that ensures that the scanner is able to recognize newly discovered vulnerabilities. Nessus refers to these feeds as plug-ins. You must periodically update your vulnerability scanner to have the most up-to-date vulnerability feed.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #17 of 200

Question ID: 1299607

You are the security analyst for a company that must comply with PCI DSS standards. You have the four vulnerability scan reports from the last year. You receive a new vulnerability scan report and compare it to the old reports. During this comparison, you notice that there are several vulnerabilities in all the reports that you know are false positives. What should you do?

- ✗ **A)** Remove the false positives from all the reports.
- ✗ **B)** Configure exceptions in the vulnerability management system for the false positives and run the vulnerability scan again.
- ✓ **C)** Add a note to the latest report that the identified vulnerabilities are false positives.
- ✗ **D)** Remove the false positives from the latest report.

Explanation

You should add a note to the latest report that the identified vulnerabilities are false positives. This is an example of reconciling results, and this solution ensures that the vulnerabilities are still in the report. PCI DSS may require that an independent assessor be brought in to verify that the vulnerabilities are indeed false positives.

You should not configure exceptions for the false positives in the vulnerability management system so that you remain compliant with PCI DSS standards. These standards do not allow the usage of exceptions in this manner.

You should not remove the false positives from ANY of the reports. Because the automated tool found the vulnerabilities, the PCI DSS standard requires that you report them. However, you can note that you have identified them as false positives.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #18 of 200

Question ID: 1299674

The software development team is adopting the best practices of the software development life cycle. They need to prevent buffer overflow attacks. Which of the following should they deploy?

- ✗ **A)** Security requirements definition
- ✓ **B)** Input validation
- ✗ **C)** Security testing
- ✗ **D)** Manual peer reviews

Explanation

Input validation ensures that all input is checked for the proper length. Validating input for length helps prevent buffer overflow attacks because buffer overflows present more input than was expected, overflowing the memory reserved for the input.

Defining security requirements is a best practice, but it will not specifically address buffer overflows. This practice involves defining security requirements for the application in development prior to starting development. Developers will also need to review application security throughout the development process. Security requirements definitions help the developers to document the areas where security controls will be needed.

Security testing is a best practice, but it also will not specifically address buffer overflows. Security testing ensures that security controls implemented in the application work as expected. In addition, it helps to identify security issues that may not have been anticipated.

Manual peer review ensures more secure code, but does not specifically address buffer overflows. Manual peer reviews are conducted so that code that is developed is reviewed prior to deployment.

The other best practices of the SDLC include:

- Security testing phases - including static code analysis, web application vulnerability scanning, and fuzz testing to identify vulnerabilities.
- User acceptance testing - designed to ensure security features do not make the application unusable from the user perspective.
- Stress test application - determines the workload that the application can with withstand.
- Security regression testing - validates that changes have not reduced the security of the application, nor opened new weaknesses that were not there prior to the change.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

SDLC - Overview, https://www.tutorialspoint.com/sdlc/sdlc_overview.htm

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

---

Question #19 of 200

Question ID: 1299735

Which of the following is the BEST method of communication to be used among stakeholders during an incident?

- ✗ **A)** Corporate email with digital signatures
- ✗ **B)** Cell phone
- ✗ **C)** VOIP
- ✓ **D)** Messaging system with end-to-end encryption

Explanation

The communication system needs to be out-of-band, meaning it is not a communication system used by the organization. It should be a separate messaging system capable of end-to-end encryption. Any digital certificates and related encryption keys used by the system should be generated separately form the organization's identity system as well.

Corporate email should not be used. The communication system should be a separate messaging system not connected to corporate email or corporate identity systems, such as single sign-on.

The communication system should not be a VOIP, as that traffic might be sniffed as it traverses the organization's network.

The communication system should not use call phones because these devices do not support easy file and data exchange.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Incident Response: Communication is Key, http://www.securitymagazine.com/articles/78810-incident-response-communication-is-key-1

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #20 of 200

Question ID: 1299628

Your organization's management has recently spent time discussing attacks against companies and their infrastructures. During the meeting, the Stuxnet attack was discussed. Against which type of system did this attack occur?

- ✗ **A)** Kerberos
- ✗ **B)** VoIP
- ✓ **C)** SCADA
- ✗ **D)** RADIUS

Explanation

A Stuxnet attack occurs against a Supervisory Control and Data Acquisition (SCADA) system. A SCADA system is also referred to as an industrial control system. SCADA is a category of software that gathers data in real time from remote locations to control equipment and conditions. It is used to monitor critical systems and control power distribution. In recent years, it has become even more vital to protect these systems. SCADA is used in the power, oil, telecommunications, gas refining, water treatment, nuclear facilities, and waste control industries. SCADA and ICS are types of building automation systems.

Kerberos is an authentication system that includes clients, servers, and a key distribution (KDC) center. The KDC gives clients tickets that the clients use to access servers and other resources.

Remote Authentication Dial-In User Server (RADIUS) is a remote access technology that allows remote users to centrally sign on to access the resources on the local network.

Voice over IP (VoIP) is technology that allows voice communication to be routed over an IP network.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Explain the threats and vulnerabilities associated with specialized technology.

References:

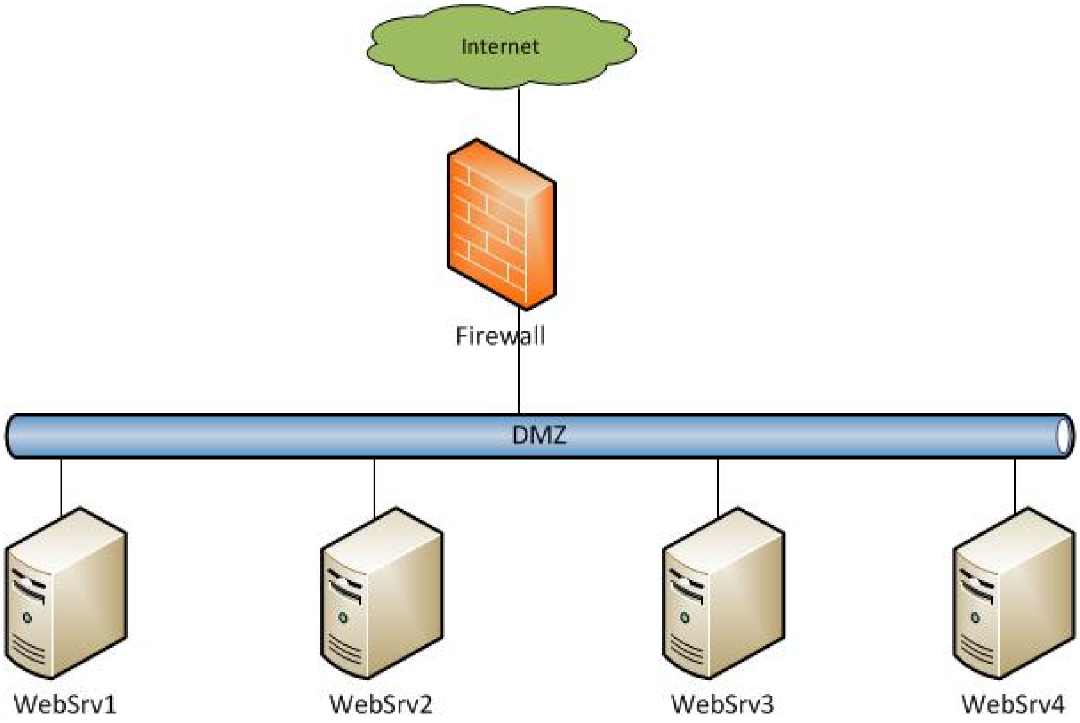
The Industrial Control System Cyber Kill Chain, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 5: Vulnerabilities Associated with Specialized Technology

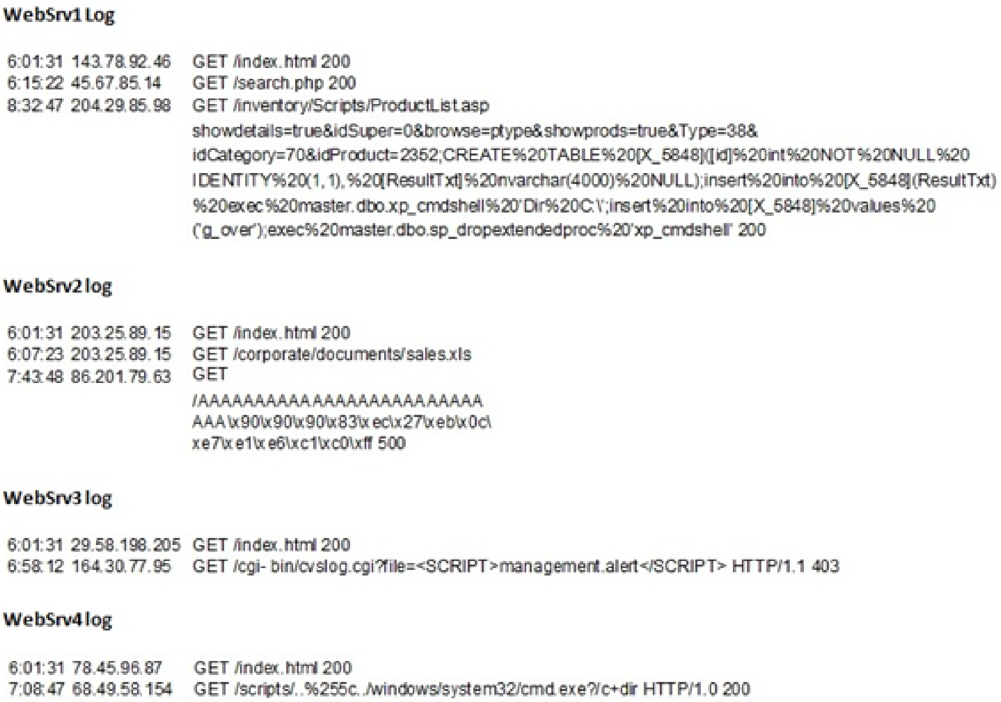
Question #21 of 200

Question ID: 1299704

As your company's security administrator, you are responsible for ensuring that all computer systems are protected against attacks.



Your company's Web site developer contacts you regarding a security issue with the Web server. He suspects that one of the Web servers is experiencing an XSS attack. You must review the Web server logs and determine which server is experiencing an XSS attack. You should click to select the line in the log that is causing this attack.



WebSrv1 Log

```
6:01:31  143.78.92.46   GET /index.html 200
6:15:22  45.67.85.14    GET /search.php 200
8:32:47  204.29.85.98   GET /inventory/Scripts/ProductList.asp
                        showdetails=true&idSuper=0&browse=ptype&showprods=true&Type=38&
                        idCategory=70&idProduct=2352;CREATE%20TABLE%20[X_5848]([id]%20int%20NOT%20NULL%20
                        IDENTITY%20(1, 1),%20[ResultTxt]%20nvarchar(4000)%20NULL);insert%20into%20[X_5848](ResultTxt)
                        %20exec%20master.dbo.xp_cmdshell%20'Dir%20C:\';insert%20into%20[X_5848]%20values%20
                        ('g_over');exec%20master.dbo.sp_dropextendedproc%20'xp_cmdshell' 200
```

WebSrv2 log

```
6:01:31  203.25.89.15   GET /index.html 200
6:07:23  203.25.89.15   GET /corporate/documents/sales.xls
7:43:48  86.201.79.63   GET
                        /AAAAAAAAAAAAAAAAAAAAAAAAAA
                        AAA\x90\x90\x90\x83\xec\x27\xeb\x0c\
                        xe7\xe1\xe6\xc1\xc0\xff 500
```

WebSrv3 log

```
6:01:31  29.58.198.205  GET /index.html 200
6:58:12  164.30.77.95   GET /cgi- bin/cvslog.cgi?file=<SCRIPT>management.alert</SCRIPT> HTTP/1.1 403
```

WebSrv4 log

```
6:01:31  78.45.96.87    GET /index.html 200
7:08:47  68.49.58.154   GET /scripts/..%255c../windows/system32/cmd.exe?/c+dir HTTP/1.0 200
```

- ✗ **A)** 0,193,577,207
- ✗ **B)** 0,40,577,55
- ✗ **C)** 0,300,577,315
- ✗ **D)** 0,28,577,43
- ✗ **E)** 0,181,577,196
- ✓ **F)** 0,313,577,328

- ✗ **G)** 0,369,577,384
- ✗ **H)** 0,204,577,259
- ✗ **I)** 0,52,577,140
- ✗ **J)** 0,381,577,396

Explanation

WebSrv3 is the Web server that is experiencing a cross-site scripting (XSS) attack. The second entry in the log is an example of an XSS attack. The attacker for the XSS attack is a host that uses the 164.30.77.95 IP address.

WebSrv1 is experiencing a SQL injection attack. The third entry in the log is the entry that should be selected. In this case, the attacker is a host that uses the 204.29.85.98 IP address.

WebSrv2 is experiencing a buffer overflow attack. The third entry in the log is an example of a buffer overflow attack. The attacker for the buffer overflow attack is a host that uses the 86.201.79.63 IP address.

WebSrv4 is experiencing a directory traversal attack. The second entry in the log is an example of a directory traversal attack. The attacker for the directory traversal attack is a host that uses the 68.49.58.154 IP address.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Detecting Attacks on Web Applications from Log Files, http://www.sans.org/reading_room/whitepapers/logging/detecting-attacks-web-applications-log-files_2074

Question #22 of 200

Question ID: 1299726

After confidential corporate information is inadvertently disclosed, you are tasked with identifying all such information that exists in the organization. Which of the following is NOT considered corporate confidential data?

- ✗ **A)** information on mergers and acquisitions
- ✓ **B)** PII
- ✗ **C)** programming code
- ✗ **D)** accounting data

Explanation

Personally identifiable information (PII) is any piece of data that can be used alone or with other information to identify a single person. Although it is certainly sensitive, it is not considered corporate confidential data.

Corporate confidential data includes data concerning:

- Mergers and acquisitions - contracts, SLAs and MPOUs that specify the details of a merger or acquisition

- Accounting data - this includes income statements, balance sheets, yearly reports and tax filings
- Trade secrets - this include recipes, plans formulas and processes
- Application programming code - source code from any proprietary software

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Confidential Data: You're Giving Away Your Corporate Secrets!, http://www.cio.com/article/2435674/infrastructure/confidential-data--you-re-giving-away-your-corporate-secrets-.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #23 of 200

Question ID: 1299770

After a recent DoS attack, you discovered that one of your internal devices that can be reached externally has command and control software installed on it that allows it to send instructions to other devices in your network,. What type of arrangement is this called?

- ✗ **A)** honeypot
- ✗ **B)** sinkhole
- ✗ **C)** rogue device
- ✓ **D)** peer-to-peer botnet

Explanation

In a peer-to-peer botnet, devices that can be reached externally are compromised and installed with server software that makes them command and control servers. The compromised devices then carry out attacks. The best course of action is to identify whether a botnet is present, and if so, to check ALL devices for malware.

If you discover a case of illegal peer-to-peer software, ensure that devices are scanned for unauthorized software on a regular basis. You should also keep all anti-malware programs up to date and ensure that users are trained in safe practices.

This is not a rogue device because it is a known device being managed. Rogue devices by definition are unknown and unmanaged.

This is not a sinkhole. A sinkhole is a target to which hostile traffic can be directed which provides an appropriate place to analyze the traffic.

This is not honeypot. A honeypot is a device made to be attractive to hackers and designed to engage them so that evidence can be gathered about them.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Peer-to-Peer Botnets for Beginners, https://www.malwaretech.com/2013/12/peer-to-peer-botnets-for-beginners.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

Question #24 of 200

Question ID: 1299664

One member of the web application security team has expressed an interest in pursuing the GIAC certification. Which organization sponsors this certification?

- ✗ **A)** ISO
- ✗ **B)** OWASP
- ✓ **C)** SANS
- ✗ **D)** CIS

Explanation

The SysAdmin, Audit, Network and Security (SANS) organization sponsors the Global Information Assurance Certification (GIAC). They also provide training, perform research, and publish best practices for cybersecurity, web security, and application security. They provide guidelines for secure software development.

The Open Web Application Security Project (OWASP) is a group that monitors attacks, specifically web attacks. OWASP maintains a list of the top ten attacks on an ongoing basis. This group also holds regular meetings at chapters throughout the world, providing resources and tools including testing procedures, code review steps, and development guidelines.

The Center for Internet Security (CIS) is a not-for-profit entity that is known for compiling CIS Security Controls (CSC). From these they publish a list of the top twenty security controls. They also provide hardened system images, training, assessment tools, and consulting services.

The International Organization for Standardization develops and publishes international standards. They are not involved in web application testing.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

Why Certify?, https://www.sans.org/why-certify

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

Question #25 of 200

Question ID: 1299647

Your organization has implemented a virtual private network (VPN) that allows branch offices to connect to the main office. Recently, you have read about a vulnerability in some VPNs whereby the key used on the VPN has been compromised. You need to ensure that your organization's key is not compromised in the future. What should you recommend?

- ✗ **A)** Enable code signing on the main office and branch offices' ends of the VPN.
- ✓ **B)** Enable PFS on the main office and branch offices' ends of the VPN.
- ✗ **C)** Enable code signing on the main office end of the VPN.
- ✗ **D)** Enable PFS on the main office end of the VPN.

Explanation

You should enable perfect forward secrecy (PFS) on the main office and branch offices' ends of the VPN. PFS increases the security for a VPN because it ensures that the same key will not be generated by forcing a new key exchange. PFS ensures that a session key created from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future. PFS depends on asymmetric or public key encryption. If you implement PFS, disclosure of the long-term secret keying information that is used to derive a single key does NOT compromise the previously generated keys.

You should not enable code signing in any way. Code signing is not used with VPN. Code signing is a method of digitally signing executable files or scripts so that users who install can be sure that the file comes from the code's author. This ensures that the original code has not been altered.

You should not only enable PFS on the main office end of the VPN. PFS must be supported on both ends of the VPN tunnel.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

PFS-VPN Tutorial, http://www.internet-computer-security.com/VPN-Guide/PFS.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #26 of 200

Question ID: 1299592

You need to deploy a security patch on several servers. Currently, you have a contract in place with a third party that states that these servers can only be updated during a regularly scheduled maintenance period. Unfortunately, the third party will not allow unscheduled maintenance because of availability needs. Which of the following is the inhibitor to this remediation?

- ✗ **A)** Functionality degradation
- ✓ **B)** SLA
- ✗ **C)** Business process interruption

- ✗ **D)** Organizational governance

Explanation

A service level agreement (SLA) is the inhibitor to this remediation. The scenario specifically stated that a contract is in place with a third party that states that these servers can only be updated during a regularly scheduled maintenance period. An SLA is a contract between two parties to provide servers and includes performance metrics that must be met.

Organizational governance includes any organizational policy or standard that can affect remediation, such as formal change control procedures.

Business process interruption includes any remediation that may result in the interruption of a business process, such as ecommerce transactions.

Functionality degradation includes any remediation that may negatively affect the performance or functionality of a device, such as a Web server.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #27 of 200

Question ID: 1299645

Your organization has decided to implement a virtual private network (VPN) so that remote employees can connect to the internal network. You decide to implement the VPN using Layer Two Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec). Which statements are TRUE of Internet Protocol Security (IPSec)? (Choose three.)

- ✓ **A)** IPSec uses encapsulation security payload (ESP) and authentication headers (AH) as security protocols for encapsulation.
- ✓ **B)** IPSec can work in either tunnel mode or transport mode.
- ✗ **C)** IPSec ensures availability of information as a part of the CIA triad.
- ✗ **D)** The IPsec framework uses L2TP as the encryption protocol.
- ✓ **E)** The IPSec framework is used in a virtual private network (VPN) implementation to secure transmissions.

Explanation

Internet Protocol Security (IPSec) can operate in tunnel mode or transport mode. In transport mode, only the payload, which is the message part of a packet, is encrypted by encapsulating security payload (ESP).

IPSec transport mode is often referred to as transport encryption. It protects a file as it travels over the FTP or HTTP protocol. In IPSec tunnel mode, the entire packet is encrypted, including the packet header and the routing information. IPSec tunnel mode provides a higher level of security than transport mode. Either of the two modes can be used to secure either gateway-to-gateway or host-to-gateway communication. If IPSec is used in gateway-to-host communication, the gateway must act as the host.

IPSec uses ESP and authentication headers (AH) as security protocols. AH provides the authentication mechanism, and ESP provides encryption, confidentiality, and message integrity.

IPSec sets up a secure channel that uses a strong encryption and authentication method between two network devices, such as routers, VPN concentrators, and firewalls.

IPSec can provide security between any two network devices running IPSec, but its chief implementation is in securing virtual private network (VPN) communications. IPSec provides security by protecting against traffic analysis and replay attacks. IPSec is primarily implemented for data communication between applications that transfer data in plaintext. IPSec secures the network device against attacks through encryption and encapsulation.

The IPSec does not use the L2TP protocol to encrypt messages. L2TP is used for communication in VPN networks and is a hybrid of L2F and PPTP. L2TP alone provides no encryption.

IPSec ensures the integrity and confidentiality of IP transmissions, but cannot ensure availability of the information. A Security Parameter Index (SPI), the identity of the security protocol

(AH or ESP), and the destination IP address are the components of an IPSec security association.

A virtual private network (VPN) is a network that is accessed using a public network but uses strong authentication and encryption to protect the devices that are accessed using the VPN. While VPNs offer better security than many other remote access options, configuring the VPN can be quite complex. The costs of implementing a VPN can be much lower than other remote access options. However, it is important that the organization works with a good service provider to ensure that its VPN is available when needed. Also, VPNs can be very flexible when you need to add new services within the VPN. You need to keep in mind that adding to the VPN's infrastructure may get more complicated and costly, depending on which components you have deployed and the vendor agreement. Finally, while a VPN will allow remote users to securely connect to internal resources, mobile devices can cause security issues, especially over wireless connections. For this reason, an added solution, such as network access control (NAC) is sometimes needed to tighten up security when logging on to the VPN with a mobile device.

There are four basic types of VPNs:

- Remote access VPN - allows access to local resources using a dial-up or Internet connection
- Site-to-site VPN - allows two or more locations to communicate using a secure tunnel over the Internet
- Extranet VPN - allows a business partner to connect to a limited set of internal resources using a secure tunnel over the Internet
- Client/Server VPN - allows client computers to connect to local resources using a secure tunnel over the Internet

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

What is IPSec?, http://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx?ppud=4

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #28 of 200

Question ID: 1299665

The software development team discovered some security vulnerabilities during vulnerability scanning. They addressed the vulnerabilities, and now they want to test the application again to see what impact these changes have had. What type of testing is this?

- ✗ **A)** Stress test application
- ✓ **B)** Security regression testing
- ✗ **C)** Manual peer review
- ✗ **D)** User acceptance testing

Explanation

Regression testing is done to verify functionality subsequent to making a change to the software. Security regression testing, a subset of that, validates that changes have not reduced the security of the application nor opened new weaknesses that were not there prior to the change.

While it is important to make web applications secure, in some cases security features make the application unusable from the user perspective. User acceptance testing is designed to ensure that does not occur.

Stress testing determines the workload that the application can with withstand. These tests should be performed in a certain way, and should always have defined objectives in place before testing begins.

Formal code review involves a careful and detailed process with multiple participants and multiple phases. In manual peer review, software developers attend meetings where each line of code is reviewed, usually using printed copies.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

A systematic classification of security regression testing approaches, https://link.springer.com/article/10.1007/s10009-015-0365-2

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

Question #29 of 200

Question ID: 1299727

After several data breaches occur, your organization performs data classification based on data sensitivity. Currently you are considering the files that contain employee information, such as social security numbers. What is the term for this type of data?

- ✓ **A)** PII
- ✗ **B)** intellectual property
- ✗ **C)** corporate confidential

- ✗ **D)** PHI

Explanation

Personally identifiable information (PII) is any piece of data that can be used alone or with other information to identify a single person. PII elements include social security numbers, employee IDs, dates of birth, and other unique values connected to an individual.

Personal Health Information (PHI) is the medical records of individuals. PHI must be protected in specific ways as prescribed by the regulations contained in the Health Insurance Portability and Accountability Act of 1996.

Intellectual property is a tangible or intangible asset to which the owner has exclusive rights. Intellectual property law is a group of laws that recognizes exclusive rights for creations of the mind.

Corporate confidential data includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Personally identifiable information, http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

Question #30 of 200

Question ID: 1299597

As a security analyst for your company, you are responsible for carrying out the vulnerability scans. Your vulnerability management process must comply with PCI DSS standards. You carried out the last vulnerability scans last month. This week, your company updated their e-commerce retail site. When should you carry out the next vulnerability scans?

- ✗ **A)** In five months
- ✓ **B)** Immediately
- ✗ **C)** In two months
- ✗ **D)** In three months

Explanation

You should carry out the next vulnerability scans immediately. PCI DSS states that scans should be carried out every three months and whenever systems are updated. Because system updates have occurred, it is necessary to carry out scans immediately.

You would carry out a vulnerability scan in two months if you were following the regular schedule. However, because of the system updates, you should immediately scan for vulnerabilities.

In three or five months are not valid answers in this case. PCI DSS requires vulnerability scans every three months, not every four months or six months, which is what the time would add up to including the scenario. Three months in the future would be the next scan as per the original schedule if no updates had occurred to the systems during that time.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #31 of 200

Question ID: 1299688

Recently, several breaches have occurred in which the malicious individual covered some of his activities by clearing the Windows audit log. You are searching the logs of some related devices to see whether this tactic was used to hide breaches on those devices as well. To what event level and ID number should you set the search filter to locate instances of the audit log being cleared?

- ✗ **A)** Informational, 4719
- ✗ **B)** Error, 4719
- ✓ **C)** Informational, 1102
- ✗ **D)** Error, 1102

Explanation

You should set the filter for Informational events and the ID number to 1102. This is the correct event level and ID number for the audit log being cleared.

You should NOT set the filter for Informational events and the ID number to 4719. This is the correct event level, but ID number 4719 is the number indicating the system audit policy has been changed. This number also indicates possible malicious activity, because a change in the policy could stop certain event types from being captured.

You should NOT set the filter for Error events and the ID number to 1102. Although the ID number is correct, this is NOT the correct event level. The level should be set to Informational.

You should NOT set the filter for Error events and the ID number to 4719. This is neither the correct event level nor ID number. 4719 is the number indicating the system audit policy has been changed. This is also an indication of possible malicious activity because a change in the policy could stop certain event types from being captured. Moreover, the level should be set to Informational, not Error.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

1102: The audit log was cleared, https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-1102

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #32 of 200

Question ID: 1299586

In which type of test is the testing team provided with limited knowledge of the network systems and devices?

- ✗ **A)** Double-blind test
- ✓ **B)** Blind test
- ✗ **C)** Regression test
- ✗ **D)** Target test

Explanation

In a blind test, the testing team is provided with limited knowledge of the network systems and devices. They are only given publicly available information. The organization's security team knows that an attack is coming. This test requires more effort by the testing team, and the testing team must simulate an actual attack.

A double-blind test resembles a blind test except that in a double blind, the organization's security team does NOT know that an attack is coming. Only a few individuals at the organization know about the attack, and they do not share this information with the security team. This test usually requires equal effort from both the testing team and the organization's security team.

In a target test, both the testing team and the organization's security team are given maximum information about the network and the type of test that will occur. This is the easiest test to complete, but will not provide a full picture of the organization's security.

A regression test is a test performed on software after a change is made to validate the functionality.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

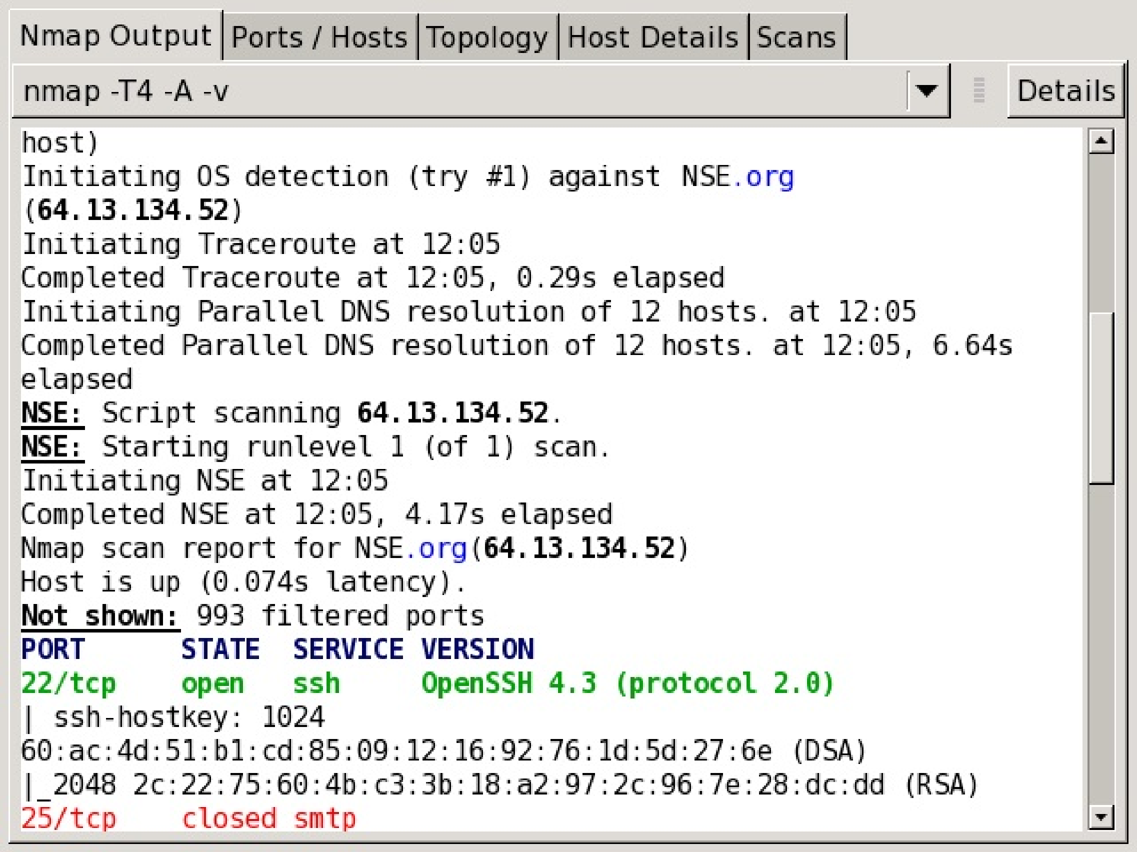
Penetration testing strategies, http://searchnetworking.techtarget.com/tutorial/Penetration-testing-strategies

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #33 of 200

Question ID: 1299689

An Nmap scan was just performed on a device in your network that may have a vulnerability, The output of this scan is shown in the following exhibit:



```
host)
Initiating OS detection (try #1) against NSE.org
(64.13.134.52)
Initiating Traceroute at 12:05
Completed Traceroute at 12:05, 0.29s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 12:05
Completed Parallel DNS resolution of 12 hosts. at 12:05, 6.64s
elapsed
NSE: Script scanning 64.13.134.52.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 12:05
Completed NSE at 12:05, 4.17s elapsed
Nmap scan report for NSE.org(64.13.134.52)
Host is up (0.074s latency).
Not shown: 993 filtered ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
|_2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
25/tcp    closed smtp
```

Considering the scan output, which of the following statements can be confirmed as TRUE?

- ✗ **A)** The device is not available for Secure Shell.
- ✗ **B)** The device is available for a protocol used to send email.
- ✗ **C)** Only one port is open.
- ✓ **D)** 993 ports are blocked at the firewall.

Explanation

There are 993 ports shown as filtered, which means they were blocked at the firewall. Therefore, we cannot tell if they are open or not on the host.

The scan output does not confirm that only one port is open. There are 993 ports shown as filtered, which means they were blocked at the firewall. Therefore, we cannot tell if they are open or not on the host.

The scan output does not confirm that the device is unavailable for Secure Shell. The device is available for Secure Shell, or SSH, because the output shows that port 22 (SSH) is open.

The scan output does not confirm that the device is available for a protocol used to send email. That protocol, SMTP, and its port (25) are shown as blocked in the scan output.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Nmap Technical Manual, http://searchsecurity.techtarget.com/tutorial/Nmap-Technical-Manual

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #34 of 200

Question ID: 1299741

When creating an incident response plan, what would be the best course of action for a small company with a single IT support person?

- ✗ **A)** Appoint the IT support person as first responder.
- ✗ **B)** Train the employees to act as responders.
- ✓ **C)** Retain an incident response provider.
- ✗ **D)** Reconsider the decision to create a plan.

Explanation

In this scenario, it may be advisable to engage the services of a third party incident response provider. In some cases an organization does not have the resources to invest in maintaining first responder capability.

It is not advisable to appoint the IT support person as first responder because this is for a small company. Most small companies cannot afford to hire an IT support person with the technical skills it takes to handled incident response properly. It is not advisable to train the employees to act as responders for the same reason. First responders need special training that most IT technicians have not had.

You should not reconsider the decision to create a plan. This is an important plan that should be created for all organizations, even if third-party assistance is required to implement the response.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

10 Questions To Help Differentiate Incident Response Service Providers, http://blogs.forrester.com/rick_holland/15-09-24-10_questions_to_help_differentiate_incident_response_service_providers

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

Question #35 of 200

Question ID: 1299683

Recently, a syslog server was deployed on the network to centralize the collection of logs from the infrastructure devices. After several days, the team decided that much of the information is normal activity, and it is filling the logs of the syslog server. You would like to limit the type of system events forwarded to the syslog server by the Cisco routers to Emergency, Alert, Critical, and Error events.

What command do you use on the routers to make this change?

- ✗ **A)** `logging trap level 4`
- ✗ **B)** `logging trap level 1`
- ✓ **C)** `logging trap level 3`
- ✗ **D)** `logging trap level 2`

Explanation

The command `logging trap level 3` will configure the router to only send Emergency, Alert, Critical, and Error events. Event types are specified by using numbers that indicate the following event types:

Emergency: 0
Alert: 1
Critical: 2
Error: 3
Warning: 4
Notice: 5
Informational: 6
Debug: 7

When you indicate a number in the command, it will send that type of event and all types with a smaller ID number. For example, specifying 3 will include event types specified by 0, 1, and 2 as well.

The `logging trap level 1` command will only send emergencies and alerts (levels 0 and 1).

The `logging trap level 2` command will only send emergencies, alerts, and critical events (levels 0, 1, and 2).

The `logging trap level 4` command will send emergencies, alerts, and critical events, but will also include warnings, which is not a requirement.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

An Overview of the syslog Protocol, http://www.ciscopress.com/articles/article.asp?p=426638

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #36 of 200

Question ID: 1299625

After performing a vulnerability scan, you receive the scanning report. A CVSS vector is provided as part of this report. For one of the vulnerabilities, you need to determine the type of access the attacker will need to the affected system for the vulnerability to occur. Which metric of the CVSS vector should you consult?

- ✗ **A)** Au
- ✗ **B)** A
- ✗ **C)** AC
- ✓ **D)** AV

Explanation

You should consult the Access Vector (AV) metric of the CVSS vector. This metric describes how the attacker would exploit the vulnerability. It has three possible values:

- L - stands for Local and means the attacker must have physical access to the affected system
- A - stands for Adjacent network and means the attacker must be on the local network
- N - stands for Network and means the attacker can cause the vulnerability from any network

The Access Complexity (AC) metric describes the difficulty of exploiting the vulnerability. It has three possible values:

- H - stands for High and means the vulnerability requires special conditions that are hard to find
- M - stands for Medium and means the vulnerability requires somewhat special conditions
- L - stands for Low and means the vulnerability does not require special conditions

The Authentication (Au) metric describes the authentication an attacker would need to get through to exploit the vulnerability. It has three possible values:

- M - stands for Multiple and means the attacker would need to get through two or more authentication mechanisms
- S - stands for Single and means the attacker would need to get through one authentication mechanism
- N - stands for None and means no authentication mechanisms are in place to stop the exploitation of the vulnerability

The Availability (A) metric describes the disruption that might occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no availability impact
- P - stands for Partial and means system performance is degraded
- C - stands for Complete and means the system is completely shut down

The Confidentiality (C) metric describes the information disclosure that may occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no confidentiality impact
- P - stands for Partial and means some access to information would occur
- C - stands for Complete and means all information on the system could be compromised

The Integrity (I) metric describes the type of data alteration that might occur and has three possible values:

- N - stands for None and means there is no integrity impact
- P - stands for Partial and means some information modification would occur
- C - stands for Complete and means all information on the system could be compromised

The CVSS vector will look something like:

CVSS2#AV:L/AC:H/Au:M/C:P/I:N/A:N

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

CVSS 2.0 Guide, https://www.first.org/cvss/v2/guide

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

---

Question #37 of 200

Question ID: 1299646

You have several virtual hosts that run VMWare. Recently, you discovered vulnerabilities in the management interface that allow remote access for administrative use. As a security analyst, you need to recommend a secure method of accessing the management interface. Which two controls should you recommend? (Choose two.)

- ✓ **A)** Secure the network connection to the management interface.
- ✗ **B)** Deploy different trust levels on each virtual host.
- ✗ **C)** Isolate the network connection to the management interface.
- ✗ **D)** Encrypt the communication with the management interface.
- ✓ **E)** Implement two-factor authentication on the management interface.

Explanation

You should recommend two controls:

- Secure the network connection to the management interface. This is usually done using an encrypted connection.
- Implement two-factor authentication on the management interface.

Both of these measures ensure that unauthorized connections do not occur.

Encrypting the communication with the management interface would protect the traffic, but it would not prevent unauthorized access.

Isolating the network connection to the management interface might make it harder to connect to the management interface. However, it would not ensure that only authorized access occurs. Network isolation is usually implemented using virtual LANs (VLANs) on switches.

Deploying different trust levels on each virtual host through segregation helps to isolate the different virtual machines on each host from each other. However, it would not ensure that only authorized access occurs over the management interface. Lower trust level VMs will typically have weaker security controls than higher trust level VMs. The weaker VMs can therefore be easier to compromise, potentially providing access to higher-risk, more sensitive VMs on the same host. For this reason, you need to provide consistency in the protection levels for VMs of different trust levels across physical and virtual environments.

In short, hosting VMs of different trust levels on the same host tends to reduce overall security for all components to that of the least protected component, meaning the weakest security implementation weakens every entity on a virtual host.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Best Practices for Mitigating Risks in Virtualized Environments, https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for%20_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #38 of 200

Question ID: 1299794

You have access to several tools as part of your IT technician job. You need to understand what the tools are used for. Match the tools on the left with the descriptions given on the right.

{UCMS id=6375046643712000 type=Activity}

Explanation

The tools and their descriptions should be matched in the following manner:

- Wireshark - Network protocol analyzer
- Nessus - Vulnerability scanner
- Snort - Network intrusion detection system
- Cain and Abel - Password recovery tool

There are many tools that can be used to manage security and network components. You should familiarize yourself with the function that the tools provide. A good place to start is with the reference provided in the References section of this question.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

Snort, https://www.snort.org/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #39 of 200

Question ID: 1299595

As part of the vulnerability management process, you have documented several factors that may affect the vulnerability scanning schedules. Which of the following factors is LEAST likely to affect them?

- ✓ **A)** SLAs
- ✗ **B)** Licensing issues
- ✗ **C)** PCI DSS requirements
- ✗ **D)** Risk appetite

Explanation

Service level agreements (SLAs) are least likely to affect vulnerability scanning schedules. On the other hand, SLAs ARE considered an inhibitor to any remediation that an organization may consider based on vulnerability reports

Factors that affect scan schedules include the organization's risk appetite, regulatory requirements (including PCI DSS requirements), technical constraints, business constraints, and licensing limitations.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #40 of 200

Question ID: 1299819

The cyber security team has collected a large amount of data from the security logs of the infrastructure devices. Now they are in the process of performing security data analytics on this information. Because of the volume of data, the team needs to filter and summarize the data in some way based on some common variable in the information. Which compensating control provides this?

- ✗ **A)** Data correlation
- ✓ **B)** Data aggregation
- ✗ **C)** Historical analysis
- ✗ **D)** Trend analysis

Explanation

Data aggregation is the process of filtering and summarizing it in some way based on some common variable in the information. Security data analytics is the process of collecting a large amount of data and using software of some sort to analyze and make sense of the data.

Data correlation is the process of locating variables in the information that seemed to be related. An example of correlation might be noting that every time there is a spike in SYN packets, we seem to have a DoS attack.

Trend analysis attempts to discover patterns in the data that indicate trends. When the data is aggregated and then graphed, it makes it much easier to discern a trend.

Historical analysis presents data in a format that allows us to look at the history of security data.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Five Steps for Better Security Analytics in 2015, https://securityintelligence.com/five-steps-for-better-security-analytics-in-2015/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

Question #41 of 200

Question ID: 1299679

Obtaining which of the following can reduce the likelihood of purchasing counterfeit equipment?

- ✗ **A)** Hash value
- ✗ **B)** Fingerprint
- ✓ **C)** OEM documentation
- ✗ **D)** SLA

Explanation

One of the ways you can reduce the likelihood of purchasing counterfeit equipment is to insist on the inclusion of verifiable original equipment manufacturer (OEM) documentation. In many cases this paperwork includes anti-counterfeiting features. Make sure you use the vendor website to verify all of the various identifying numbers in the documentation.

A service level agreement (SLA) will not reduce the likelihood of purchasing counterfeit equipment. It simply spells out the deliverable, the compensation and the services expected in support.

A fingerprint cannot be made for hardware. Fingerprints are a form of hashing that can be used to derive a value from a file that can be used to validate its integrity at a later time.

A hash value cannot be made for hardware. Hash values are derived from the contents of a file and can be used to validate its integrity at a later time

Objective:
Software and Systems Security

Sub-Objective:
Explain hardware assurance best practices.

References:

Darker shades of the IT equipment gray market, http://searchdatacenter.techtarget.com/tip/Darker-shades-of-the-IT-equipment-gray-market

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 10: Hardware Best Practices

Question #42 of 200

Question ID: 1299792

Snort is one of the tools used by your company. What functionality does this tool provide?

- ✗ **A)** Firewall
- ✓ **B)** IDS/IPS
- ✗ **C)** Vulnerability scanner
- ✗ **D)** SIEM

Explanation

Snort provides intrusion detection system (IDS) and intrusion prevention system (IPS) functionality, including logging and real-time traffic analysis.

Snort is not a firewall, security information and event management (SIEM), or vulnerability scanner. Firewalls include Cisco, Palo Alto, and Checkpoint. Firewalls can sometimes include other functionalities, such as IDS and IPS functions.

SIEM tools include ArcSight, QRadar, Splunk, AlienVault, OSSIM, and Kiwi Syslog.

Vulnerability scanners include Qualys, Nessus, OpenVAS, Nexpose, Nikto, and Microsoft Baseline Security Analyzer.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

Snort, https://www.snort.org/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

Question #43 of 200

Question ID: 1299751

After a recent incident in which several network attacks occurred at once, several systems were down longer than was necessary because the team's response was somewhat confused. The team has decided to determine the longest amount of time the company can function without an asset before causing damage to the organization. The team needs to make this determination on an asset-by-asset basis. Which of the following factors are they trying to determine?

- ✗ **A)** RTO
- ✗ **B)** MTBF
- ✓ **C)** MTD
- ✗ **D)** RPO

Explanation

Maximum tolerable downtime (MTD) is the maximum amount of time that an organization can tolerate a single resource or function being down. This is also referred to as the maximum period time of disruption (MPTD).

Mean time between failures (MTBF) is the estimated amount of time a device will operate before a failure occurs. This amount is calculated by the device vendor. System reliability is increased by a higher MTBF and a lower mean time to repair (MTTR).

Recovery point objective (RPO) is the point in time to which the disrupted resource or function must be returned.

Recovery time objective (RTO) is the shortest time period after a disaster or disruptive event within which a resource or function must be restored to avoid unacceptable consequences. RTO assumes that an acceptable period of downtime exists. The RTO value should be smaller than the MTD.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

RPO, RTO, WRT, MTDWTH?!, http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

---

Question #44 of 200

Question ID: 1299669

The software development team has deployed a new web application, and it is now live. Although much security testing was done prior to release, the team is still a bit concerned about the live environment. They would like to capture and analyze every transaction of user. Which type of web vulnerability scanning are they suggesting?

- ✓ **A)** RUM
- ✗ **B)** Fuzz testing
- ✗ **C)** Synthetic transaction monitoring
- ✗ **D)** Data flow analysis

Explanation

Real user monitoring (RUM), which is a type of passive monitoring, is a monitoring method that captures and analyzes every transaction of every application or website user. Unlike synthetic monitoring, which attempts to gain performance insights by regularly testing synthetic (pre-created) interactions, RUM cuts through the guesswork by seeing exactly how your users are interacting with the application.

Fuzz testing, or fuzzing, involves injecting invalid or unexpected input (sometimes called faults) into an application to test how the application reacts. It is usually done with a software tool that automates the process.

Synthetic transaction monitoring, uses external agents to run scripted transactions against an application, which is a type of proactive monitoring. It is often preferred for websites and applications.

Data flow analysis is a form of static code analysis and looks at run-time information while the software is in a static state.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

What is Real-User Monitoring?, https://smartbear.com/learn/performance-monitoring/what-is-real-user-monitoring/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

---

Question #45 of 200

Question ID: 1299753

It has been a hectic day for the cyber security team. Three separate attacks were detected, and attacks are still ongoing. The team is struggling to decide which incident should have the most resources devoted to it. Which of the following is NOT a factor to be considered when prioritizing the incidents?

✗ **A)** the type of data at risk

✗ **B)** the amount of downtime already experienced

✓ **C)** the order in which the incidents were reported

✗ **D)** the scope of the impact

Explanation

Incidents are NOT prioritized in the order in which they were detected and reported. When addressing incidents, the factors contributing to incident severity and prioritization include:

- The scope of impact
- The types of data at risk

The amount of downtime already experienced would be a consideration in determining the scope of impact for each incident.

The type of data at risk would be a consideration because certain types of data create more liability for the organization if compromised.

The scope of the impact would be a consideration. Impact scope includes the following factors:

- Downtime - refers to the amount of time access to resource were interrupted

- Recovery time - refers to the amount of time taken to recover from the incident
- Data integrity - refers to the amount of data corrupted or altered during the incident
- Economic - the cost of the incident to the organization
- System process criticality - refers to the criticality of the system involved

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Implementation Framework – Cyber Threat Prioritization 4.1, https://nanopdf.com/download/implementation-framework-cyber-threat-prioritization-41_pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

---

Question #46 of 200

Question ID: 1299710

You are concerned that network sniffers are going to be installed on the company's network. You need to ensure that network devices are not susceptible to the sniffers. Which of the following would be a first step to this?

- ✗ **A)** Enable promiscuous mode.
- ✗ **B)** Install an IDS.
- ✓ **C)** Disable promiscuous mode.
- ✗ **D)** Install an IPS.

Explanation

You should disable promiscuous mode on all the network devices, also referred to as network appliances, to ensure that network sniffers cannot intercept and read each network packet that arrives in its entirety.

Installing an intrusion prevention system (IPS) or intrusion detection system (IDS) will help to prevent or detect intrusions. However, they will not prevent network sniffers installed on the company's network.

Enabling promiscuous mode will allow network sniffers to read network packets.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Network Monitoring Basics: Promiscuous Mode, Hubs, and Switches, https://landetective.com/products/internet-monitor/manual/traffic-analysis.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #47 of 200

Question ID: 1299588

Which of the following is NOT an item considered during the establishment of the rules of engagement?

✓ **A)** Compensation

✗ **B)** Scope

✗ **C)** Authorization

✗ **D)** Timing

Explanation

Compensation is NOT an item considered during the establishment of the rules of engagement. That is covered in the Service level agreement (SLA).

The rules of engagement define how penetration testing should occur. These are issues that should be settled and agreed upon before any testing begins.

Items settled during establishment of the rules of engagement include:

- Timing - the time when the test will occur and a specification of any times it cannot be performed
- Scope - identifies the machines or parts of the network that can be scanned and the types of scans to be performed
- Authorization - provides both written authorization and legal authority to perform the scan
- Exploitation - lists and authorizes any exploits that may be attempted
- Communication - lists the contacts at the organization with whom the testers should communicate and the methods of communication that should be used
- Reporting - lists the types of reports to be generated and their methods of distribution

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

Penetration Testing and Rules of engagement, https://fl0x2208.wordpress.com/2016/09/03/penetration-testing-and-rules-of-engagement/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #48 of 200

Question ID: 1299775

Lately, you have become concerned that certain types of traffic that should be encrypted on the network are not in fact encrypted. An associate explains that you need to perform packet capture to assess the breadth of this problem. Which of the following tools would allow you to do this?

- ✓ **A)** Wireshark
- ✗ **B)** IPS
- ✗ **C)** IDS
- ✗ **D)** HIDS

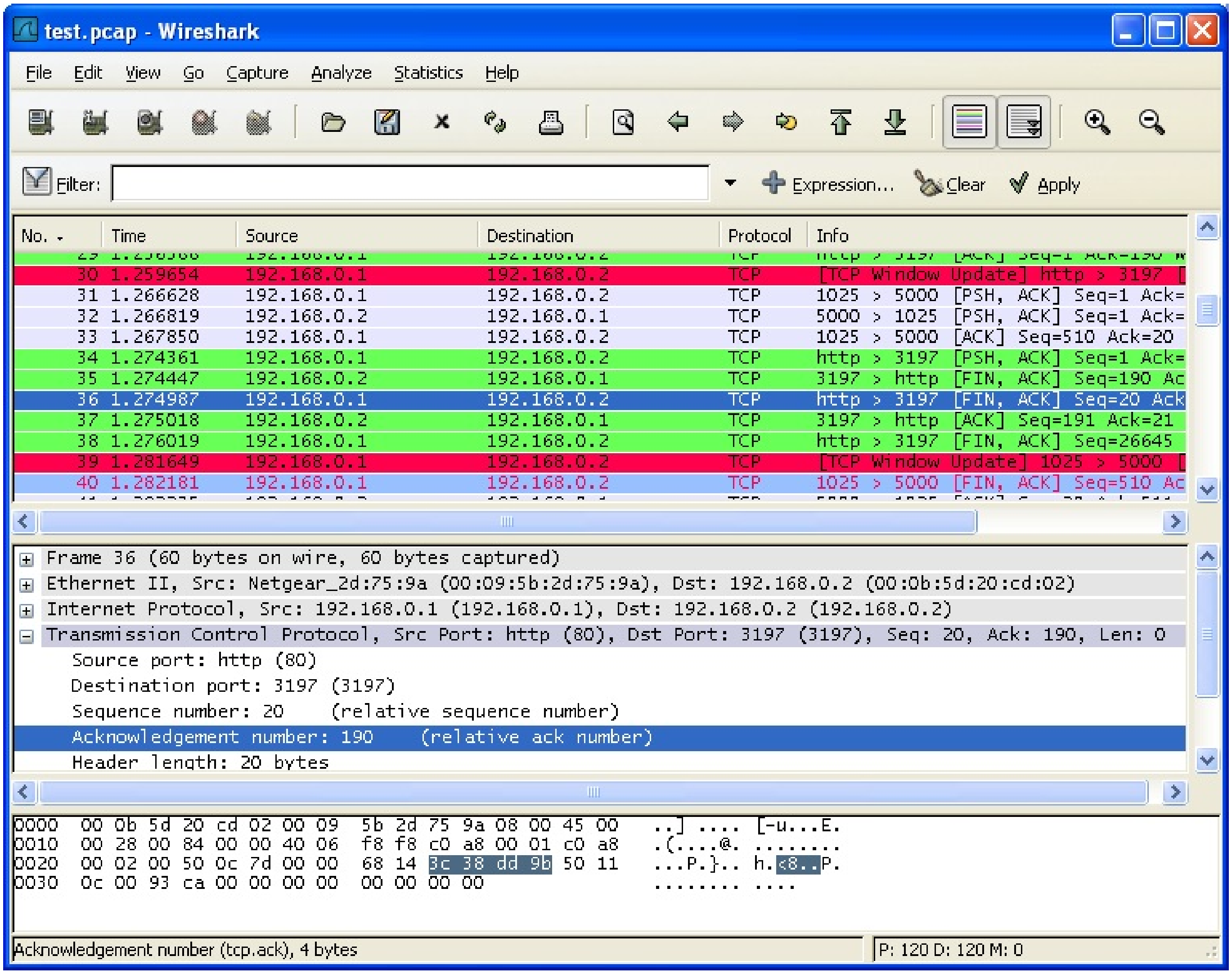
Explanation

You should use Wireshark. Wireshark is a packet capture utility that can be used to capture and inspect packets. This will allow you to determine whether the packets are encrypted.

An intrusion detection system (IDS) cannot be used to capture packets and inspect them. This tool is used to detect attacks on the network.

A host-based intrusion detection system (HIDS) cannot be used to capture packets and inspect them. This tool is used to detect attacks on a single device. A network-based IDS (NIDS) provides the same services but for an entire network instead of a single host.

An intrusion prevention system (IPS) cannot be used to capture packets and inspect them. This tool is used to detect attacks on the network and, if possible, prevent them.



```
No. -  Time        Source         Destination    Protocol  Info
  30 1.259654    192.168.0.1    192.168.0.2    TCP       [TCP Window Update] http > 3197 [
  31 1.266628    192.168.0.1    192.168.0.2    TCP       1025 > 5000 [PSH, ACK] Seq=1 Ack=
  32 1.266819    192.168.0.2    192.168.0.1    TCP       5000 > 1025 [PSH, ACK] Seq=1 Ack=
  33 1.267850    192.168.0.1    192.168.0.2    TCP       1025 > 5000 [ACK] Seq=510 Ack=20
  34 1.274361    192.168.0.1    192.168.0.2    TCP       http > 3197 [PSH, ACK] Seq=1 Ack=
  35 1.274447    192.168.0.2    192.168.0.1    TCP       3197 > http [FIN, ACK] Seq=190 Ac
  36 1.274987    192.168.0.1    192.168.0.2    TCP       http > 3197 [FIN, ACK] Seq=20 Ack
  37 1.275018    192.168.0.2    192.168.0.1    TCP       3197 > http [ACK] Seq=191 Ack=21
  38 1.276019    192.168.0.1    192.168.0.2    TCP       http > 3197 [FIN, ACK] Seq=26645
  39 1.281649    192.168.0.1    192.168.0.2    TCP       [TCP Window Update] 1025 > 5000 [
  40 1.282181    192.168.0.1    192.168.0.2    TCP       1025 > 5000 [FIN, ACK] Seq=510 Ac
```

```
⊞ Frame 36 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:2d:75:9a), Dst: 192.168.0.2 (00:0b:5d:20:cd:02)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 3197 (3197), Seq: 20, Ack: 190, Len: 0
    Source port: http (80)
    Destination port: 3197 (3197)
    Sequence number: 20    (relative sequence number)
    Acknowledgement number: 190    (relative ack number)
    Header length: 20 bytes
```

```
0000  00 0b 5d 20 cd 02 00 09  5b 2d 75 9a 08 00 45 00   ..] .... [-u...E.
0010  00 28 00 84 00 00 40 06  f8 f8 c0 a8 00 01 c0 a8   .(....@. ........
0020  00 02 00 50 0c 7d 00 00  68 14 3c 38 dd 9b 50 11   ...P.}.. h.<8..P.
0030  0c 00 93 ca 00 00 00 00  00 00 00 00               ........ ....
```

Acknowledgement number (tcp.ack), 4 bytes | P: 120 D: 120 M: 0

Objective:

Incident Response

Sub-Objective:

Given a scenario, utilize basic digital forensics techniques.

References:

Wireshark: A Guide to Color My Packets, https://www.sans.org/reading-room/whitepapers/detection/wireshark-guide-color-packets-35272

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #49 of 200

Question ID: 1299677

The security team is compiling a list of the types of patches or updates that should be performed on a regular basis. Which of the following types of patches are NOT important on routers and switches?

✓ **A)** Antivirus updates

- ✗ **B)** ROMMON updates
- ✗ **C)** Operating system updates
- ✗ **D)** Firmware updates

Explanation

Antivirus updates are not typically performed on routers. Any features designed to address this issue will be part of the operating system.

Operating system updates, such as to the Cisco IOS, can be done and usually comprise a full replacement of the current operating system image with a new version.

Firmware updates are done on routers in addition to operating system updates.

The ROMMON can be upgraded on a Cisco router. This is a mini operating system that might be considered firmware as it resides in nonvolatile RAM (NVRAM).

Objective:
Software and Systems Security

Sub-Objective:
Explain hardware assurance best practices.

References:

Time to Patch Your Cisco Routers, http://www.zdnet.com/article/time-to-patch-your-cisco-routers/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 10: Hardware Best Practices

---

Question #50 of 200

Question ID: 1299774

After a security breach occurred this morning, the cyber team is trying to identify all network-related symptoms that of the event. Which of the following is NOT a network-related symptom of an attack?

- ✓ **A)** Malicious processes
- ✗ **B)** Rogue devices on the network
- ✗ **C)** Scan sweeps
- ✗ **D)** Bandwidth consumption

Explanation

The presence of malicious processes is a host-related symptom, not a network-related symptom. Common network-related symptoms of incidents are bandwidth consumption, beaconing, irregular peer-to-peer communication, rogue devices on the network, scan sweeps, unusual traffic spikes, and common protocol over non-standard port.

Bandwidth consumption could be detected using a resource monitor on the device. If this occurs, you should suspect some sort of DoS attack. The best course of action is to identify the source of the traffic and block it at the firewall. Going forward, you should prevent all traffic from outside the network that uses a source address that is a private address, keep all anti-malware up to date, and ensure that users are trained in safe practices.

Beaconing occurs when malware attempts to remotely connect to a Command and Control host or network. It refers to traffic that leaves your network at regular intervals. This behavior could be detected by the firewall. The best course of action is to identify the destination of the traffic and block it at the firewall. Beaconing indicates some sort of malware or compromise, so the best course of action is to remove all malware. If the device still does not function properly after you remove the malware, a vulnerability scan should be run for the device. You should also keep all anti-malware up to date and ensure that users are trained in safe practices.

Irregular peer-to-peer communication could be detected by an IPS or IDS. You should suspect either illegal peer-to-peer traffic or the presence of a peer-to-peer botnet. The best course of action is to identify if a botnet is present, because if so, ALL devices must be checked for malware. If you detect illegal peer-to-peer software, ensure that devices are scanned for unauthorized software on a regular basis. You should also keep all anti-malware up to date and ensure that users are trained in safe practices.

Rogue devices on the network can be displayed by using the rogue device features found in many IDS and IPS system. The best course of action is to locate them, remove them, and identify who installed them. Going forward, you should perform regular checks for these kinds of devices.

Scan sweeps can be detected by IDS and IPS systems. They indicate an attempt to map your network. The best course of action is to identify the source of the sweeps. Going forward, you should also deploy an IPS or IDS if one is not already present in your network.

Unusual traffic spikes could be detected using anomaly-based IDS. If this occurs you should suspect some sort of DoS attack. The best course of action is to identify the source of the traffic and block it at the firewall. As a best practice, you should prevent all traffic from outside the network that uses a source address that is a private address, keep all anti-malware up to date, and ensure that users are trained in safe practices.

Malicious processes are located on devices, and thus are considered a host-related symptom. Common host-related symptoms include unusual processing consumption, memory consumption, or drive capacity consumption; unauthorized software and malicious processes; unauthorized changes and privileges; and data exfiltration. The general recommendation for all host-related attacks is to keep anti-malware up to date and ensure that all users are trained in safe practices.

Unusual processor or memory consumption could be determined by using a resource monitor on the device. If either of these symptoms occurs, you should suspect a malicious process is using the processing resources or memory. The best course of action is to scan the device for malware.

Issues with drive capacity consumption could also be determined by using a resource monitor on the device. When this symptom occurs, you should suspect that some malicious process is filling the drive as part of a DoS attack. Again, the best course of action is to scan the device for malware.

Unauthorized software could be detected with a vulnerability scan that identifies unauthorized software. When discovered, you should suspect that a malicious individual has compromised the device, even if the unauthorized software is not classified as malware. Some legitimate third-party software has known vulnerabilities that put your entire network at risk if it is installed. The best course of action is to re-image the device using the latest snapshot if available. To ensure security, you should use a policy that prevents the installation of unauthorized software, and ensure that users are trained in safe practices.

Malicious processes could be detected by using a tool like Process Explorer. You should suspect the presence of malware if you notice unusual processor, memory, or drive capacity usage on a host. The best course of action is to scan the device using anti-malware software. If you are unable to remove the malicious software, you should re-image the device using the latest snapshot if available and ensure that anti-malware programs are kept up to date.

Unauthorized changes could be discovered by performing a compliance scan in which the current device settings are compared to a baseline. When it occurs, you should suspect that the device has been compromised. You should attempt to restore the device to the correct settings and remove any unauthorized permissions that have been granted. You may need to re-image the device using the latest snapshot if available. Ensure that users are trained in safe practices and that user accounts are hardened against privilege escalation.

Unauthorized privileges could be discovered by examining the event log to determine which users are performing these privileged acts. If the user can be identified, then disciplinary action should be taken. If not, the best course of action is to scan the device for malware and for compliance to the baseline. Ensure that users are trained in safe practices and that user accounts are hardened against privilege escalation.

Data exfiltration can be discovered with DLP software, if present. If not, data exfiltration may be discovered only when it falls into the wrong hands. The best course of action is to identify the source of the disclosure if possible and then take disciplinary action, and to employ a DLP solution in the enterprise.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Three Commonly Ignored Signs of a Cyber Attack, https://observable.net/blog/three-commonly-ignored-signs-of-a-cyber-attack/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

---

Question #51 of 200

Question ID: 1299658

Last month, the network team deployed several new VLANs. After the deployment, the Sales department manager asked if there was any way traffic could be prevented between two of the devices in the Sales VLAN. You need to deploy a solution to control traffic between two devices in the same VLAN. Which of the following should you use?

✓ **A)** PVLAN
✗ **B)** STP
✗ **C)** DTP
✗ **D)** VTP

Explanation

Private VLANs (PVLANs) can be used to create smaller, private VLANs within a VLAN. Creation of PVLANs is done after the creation of the primary VLAN by setting the switch port to one of three states. The three states a port can be in when using PVLANs:

- Promiscuous - The port can communicate with all PVLAN ports. This typically is how the port that goes from the switch to the router is set.

- Isolated - The port can only communicate with promiscuous ports. These are used to isolate a device from other ports in the switch.
- Community - The port can communicate with other ports that are members of the community and to promiscuous ports but not with ports from other communities or with isolated ports.

Spanning Tree Protocol (STP) is a switching loop avoidance mechanism that operates by default on switches. It has nothing to do with VLANs.

VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that propagates VLAN information between switches. It cannot be used to control traffic between two devices in the same VLAN.

Dynamic Trunking Protocol (DTP) is a proprietary networking protocol developed by Cisco for the purpose of negotiating trunking on a link between switches. It cannot be used to control traffic between two devices in the same VLAN.

VLANs are implemented to provide network segmentation.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Configuring Isolated Private VLANs on Catalyst Switches, http://www.cisco.com/c/en/us/support/docs/lan-switching/private-vlans-pvlans-promiscuous-isolated-community/40781-194.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #52 of 200

Question ID: 1299789

You need to fine-tune some Windows security features. Which tool should you use?

- ✗ **A)** netstat
- ✗ **B)** MBSA
- ✗ **C)** ipconfig
- ✓ **D)** EMET

Explanation

You should use Microsoft's Enhanced Mitigation Experience Toolkit (EMET) to fine-tune some Windows security features.

Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to determine security state by assessing missing security updates and other security settings within Microsoft Windows. It is not used to fine-tune security settings.

Ipconfig is a Windows tool that is used to display or change the TCP/IP settings. Ifconfig is the Linux/Unix equivalent of ipconfig.

Netstat is a tool that displays network connections for TCP, routing tables, and a number of network interfaces.

Objective:

Incident Response

Sub-Objective:

Given a scenario, utilize basic digital forensics techniques.

References:

The Enhanced Mitigation Experience Toolkit, https://support.microsoft.com/en-us/help/2458544/the-enhanced-mitigation-experience-toolkit

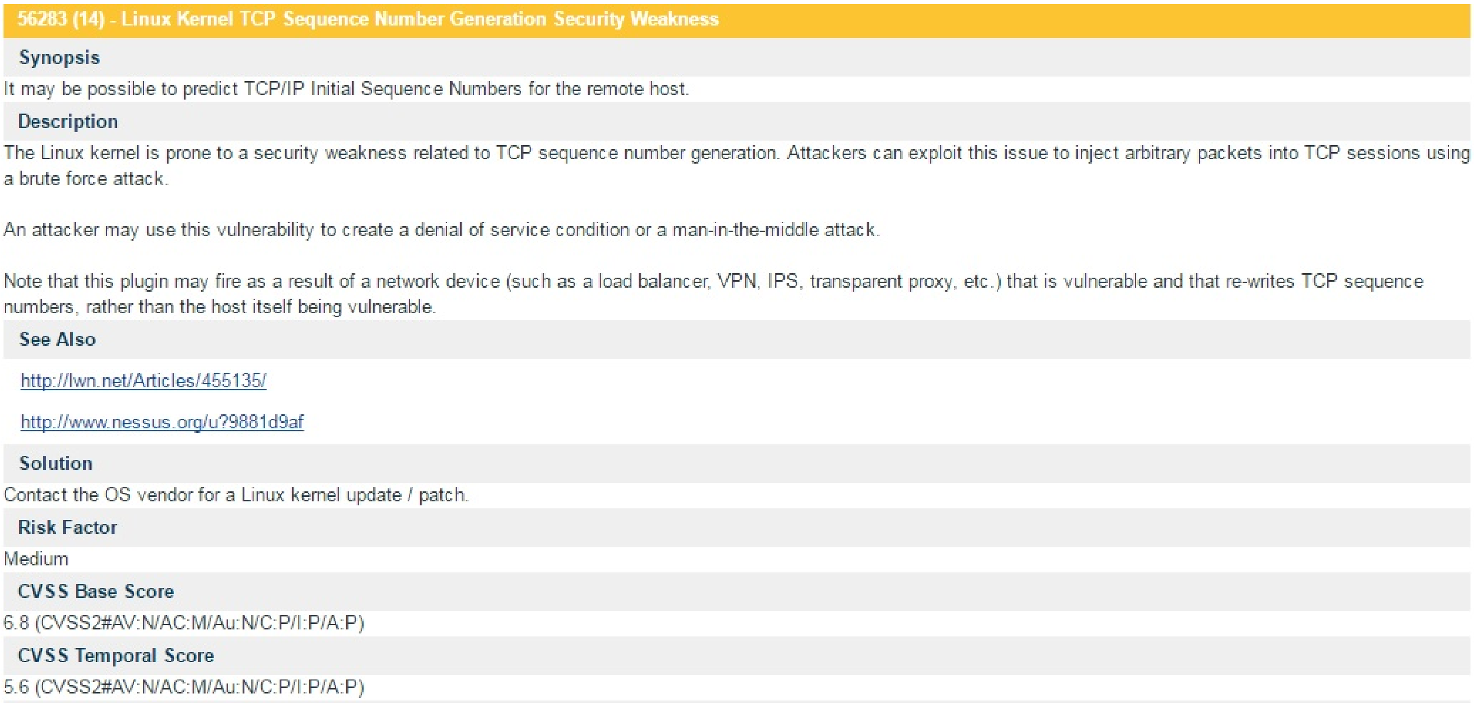
CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #53 of 200

Question ID: 1299620

After running a vulnerability scan, you receive a vulnerability report that includes the vulnerability identified below:



56283 (14) - Linux Kernel TCP Sequence Number Generation Security Weakness

Synopsis

It may be possible to predict TCP/IP Initial Sequence Numbers for the remote host.

Description

The Linux kernel is prone to a security weakness related to TCP sequence number generation. Attackers can exploit this issue to inject arbitrary packets into TCP sessions using a brute force attack.

An attacker may use this vulnerability to create a denial of service condition or a man-in-the-middle attack.

Note that this plugin may fire as a result of a network device (such as a load balancer, VPN, IPS, transparent proxy, etc.) that is vulnerable and that re-writes TCP sequence numbers, rather than the host itself being vulnerable.

See Also

http://lwn.net/Articles/455135/

http://www.nessus.org/u?9881d9af

Solution

Contact the OS vendor for a Linux kernel update / patch.

Risk Factor

Medium

CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.6 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

Based on this report, which CVSS metric should be of the most concern to you?

- ✗ **A)** A
- ✓ **B)** Au
- ✗ **C)** AC
- ✗ **D)** I

Explanation

The CVSS metric that should be of the most concern to you for this vulnerability is the Authentication (Au) metric. The Authentication (Au) metric describes the authentication an attacker would need to get through to exploit the vulnerability. It has three possible values:

- M - stands for Multiple and means the attacker would need to get through two or more authentication mechanisms

- S - stands for Single and means the attacker would need to get through one authentication mechanism
- N - stands for None and means no authentication mechanisms are in place to stop the exploitation of the vulnerability

For this metric, M is the best ranking. The Au value shown in this screenshot is N, which is the worst possible result and means there is presently no authentication mechanism that is known to stop the vulnerability.

The Availability (A) metric describes the disruption that might occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no availability impact
- P - stands for Partial and means system performance is degraded
- C - stands for Complete and means the system is completely shut down

The Access Complexity (AC) metric describes the difficulty of exploiting the vulnerability. It has three possible values:

- H - stands for High and means the vulnerability requires special conditions that are hard to find
- M - stands for Medium and means the vulnerability requires somewhat special conditions
- L - stands for Low and means the vulnerability does not require special conditions

For this metric, H is the best ranking.

The Access Vector (AV) describes how the attacker would exploit the vulnerability. It has three possible values:

- L - stands for Local and means the attacker must have physical or logical access to the affected system.
- A - stands for Adjacent network and means the attacker must be on the local network
- N - stands for Network and means the attacker can cause the vulnerability from any network

For this metric, L is the best ranking.

The Confidentiality (C) metric describes the information disclosure that may occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no confidentiality impact
- P - stands for Partial and means some access to information would occur
- C - stands for Complete and means all information on the system could be compromised

For this metric, N is the best ranking.

The Integrity (I) metric describes the type of data alteration that might occur and has three possible values:

- N - stands for None and means there is no integrity impact
- P - stands for Partial and means some information modification would occur
- C - stands for Complete and means all information on the system could be compromised

For this metric, N is the best ranking.

The CVSS vector will look something like this:

CVSS2#AV:L/AC:H/Au:M/C:P/I:N/A:N

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

CVSS 2.0 Guide, https://www.first.org/cvss/v2/guide

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

---

Question #54 of 200

Question ID: 1299583

During the investigation of a network breach, you locate evidence that someone from outside the network was sending packets with the SYN flag on in the TCP header. Which of the following operations is the malicious individual attempting?

- ✗ **A)** DoS attack
- ✗ **B)** DNS harvesting
- ✓ **C)** Service discovery
- ✗ **D)** Email harvesting

Explanation

The individual is attempting service discovery, which is the process of identifying whether a service is operational on a device and whether the device is protected by a firewall. By sending TCP SYN packets and analyzing the responses, the attacker can make inferences about these two issues.

For example, if the TCP SYN packet receives no response, the device is either filtered or located behind a firewall that is blocking that port number or IP address. If the TCP SYN packet receives a SYN/ACK packet in return, then the device is reachable, the port is open, and the service is available. If the TCP SYN packet receives a RST packet in return, then the device is reachable, but the port is closed and the service is not available.

This is not a denial of service (DoS) attack. A DoS attack attempts to make the host or its resources unavailable. Service discovery does not do that.

This is not a DNS harvesting attack. A DNS harvesting attack attempts to obtain the entire DNS records from DNS server, typically by convincing the server to perform an unauthorized zone transfer.

This is not an email harvesting attack. An email harvesting attack attempts to obtain large numbers of email addresses and uses a variety of approaches to do so, including the following:

- Through social engineering
- By buying lists from other spammers
- By accessing the emails and address books in another user's computer
- By hacking websites

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

Nmap Network Scanning Reference Guide, Chapter 15: Host Discovery, https://nmap.org/book/man-host-discovery.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #55 of 200

Question ID: 1299684

One of the employees in your organization reported that another employee is currently viewing a prohibited website. When you approach his computer, he is at the printer picking up a document. You need to display the current TCP connections on his computer. Which command should you run?

- ✗ **A)** `netstat -r`
- ✗ **B)** `netstat -m`
- ✗ **C)** `netstat -g`
- ✓ **D)** `netstat -a`

Explanation

You should use the `nestat -a` command. Netstat can be used to display various types of information, including the TCP connections that are currently in place on the device on which it is run. To display the TCP connections that are currently in place, you would use the `-a` switch.

The `netstat -g` command displays multicast group membership information, not TCP connections.

The `netstat -r` command displays the routing table, not TCP connections.

The `netstat -m` command displays memory statistics for the networking code, not TCP connections.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Netstat, https://technet.microsoft.com/en-us/library/bb490947.aspx

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #56 of 200

Question ID: 1299580

Your vulnerability analysis scan has identified several vulnerabilities and assigned them a CVSS score. Issue A has a score of 4.3, Issue B has a score of 9.1, Issue C has a score of 1.6, and Issue D has a score of 7.7. Which issue should take priority?

- ✗ **A)** Issue D

✓ **B)** Issue B

✗ **C)** Issue A

✗ **D)** Issue C

Explanation

Issue B should take priority because it has the highest CVSS value of 9.1, which is considered a critical issue.

The Common Vulnerability Scoring System (CVSS) is a system of ranking vulnerabilities that are discovered based on pre-defined metrics. This system ensures that the most critical vulnerabilities can be easily identified and addressed after a vulnerability test is met. Scores are awarded on a scale of 0 to 10, with the values having the following ranks:

- 0 - No issues
- 0.1 to 3.9 - Low
- 4.0 to 6.9 - Medium
- 7.0 to 8.9 - High
- 9.0 to 10.0 - Critical

In most cases, companies will attempt to resolve the vulnerabilities with the highest score. However, in some cases you may find that a less critically scored vulnerability can be resolved relatively quickly. In that case, you may decide to handle that vulnerability.

Keep in mind that tool updates and plug-ins for vulnerability scanners are just as important as updates are to anti-malware and anti-virus products. Tool updates and plug-ins allow the scanner to recognize the latest vulnerabilities that have been discovered. It is important to keep the vulnerability scanning tool you use up to date.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, utilize threat intelligence to support organizational security.

References:

What is CVSS?, https://searchsecurity.techtarget.com/definition/CVSS-Common-Vulnerability-Scoring-System

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 2: Utilizing Threat Intelligence

---

Question #57 of 200

Question ID: 1299815

As a security analyst, you were asked by management to perform an audit of the passwords used by the company's 50,000 users. Management is concerned that personal information, such as addresses and birthdays, is being incorporated into passwords.

The company has virtualized environments with cluster- and cloud-based resources. The company's current password policy enforces a minimum password length of 14 characters, a password reset of 90 days, and account lockout after three incorrect attempts. You need to run the password auditing software and produce a report in the shortest amount of time.

Which of the following options is BEST suited for this?

- ✗ **A)** Build a virtual machine on the administrator's desktop, transfer the password file to it, and run the password cracker on the virtual machine.
- ✗ **B)** Upload the password file to a virtualized de-duplicated storage system to reduce the password entries, and run a password cracker on that file.
- ✗ **C)** Upload the password file to cloud storage, use on-demand provisioning to build a virtual machine, and use it to run a password cracker on all the users.
- ✓ **D)** Take advantage of the company's cluster-based resources, upload the password file to the cluster, and run the password cracker on that platform.

Explanation

You should take advantage of the company's cluster-based resources, upload the password file to the cluster, and run the password cracker on that platform. This will produce the results in the shortest amount of time because all of the resources in the cluster will work together.

You should not upload the password file to a virtualized de-duplicated storage system to reduce the password entries, and run a password cracker on that file. Any solution that uses regular virtualization, instead of cluster resources, will not be as fast as using cluster resources. Virtual resources share the resources of a single host, while clusters contain multiple hosts that work together to complete the job.

You should not build a virtual machine on the administrator's desktop, transfer the password file to it, and run the password cracker on the virtual machine. Once again, this solution uses a virtual resource, which would not perform the needed actions as quickly as the cluster resources.

You should not upload the password file to cloud storage, and use on-demand provisioning to build a virtual machine to run a password cracker on all the users. Cloud storage is not guaranteed to provide you optimum access to resources, even in on-demand provisioning mode, because cloud environments usually share resources will all the cloud tenants.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Virtualization: Physical vs. Virtual Clusters, https://technet.microsoft.com/en-us/library/hh965746.aspx

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

---

Question #58 of 200

Question ID: 1299716

Over time, the remote access needs of the user base in your network have become more and more granular. For example, you need to allow the Sales group access to the VPN connection but only under the following conditions:

- If they are connecting from home using their work laptop, they can connect at any time.

- If they are connecting from anywhere else using their work laptop, they can connect from 9 a.m. to 5 p.m.
- If they are connecting from anywhere using a non-work device, they cannot connect.

What type of system could you deploy that would make these types of configurations possible?

✗ **A)** DAC

✗ **B)** MAC

✗ **C)** RBAC

✓ **D)** NAC

Explanation

Network access control (NAC) systems can make remote access decisions based on combinations of factors. They use combinations of these decision methods to make access control decisions.

- Location-based
- Time-based
- Role-based
- Rule-based

By creating policies that place requirements on the devices, such as current antivirus definitions and the latest operating systems updates, you can prevent the introduction of the devices to the network in cases where these items are missing. It is also possible to place these devices in a quarantined network until they can be updated by a remediation server.

Mandatory access control (MAC) would not provide this ability. MAC is a resource access control system, not a network access control system. It prescribes that resources are classified by sensitivity and that access is granted based on a sensitivity level assigned to users.

Discretionary access control (DAC) would not provide this ability. DAC is a resource access control system in which a user is allowed to control access to resources that he or she creates or owns.

Role-based access control (RBAC) systems are resource access control systems in which users are assigned roles. Along with those roles come a preconfigured set of rights and permissions.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, implement configuration changes to existing controls to improve security.

References:

The Critical Security Controls: What's NAC Got to Do with IT?, https://www.sans.org/reading-room/whitepapers/analyst/critical-security-controls-what-039-s-nac-it-35115

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 12: Implementing Controls to Improve Security

Question #59 of 200

Question ID: 1299619

Bob is analyzing the results of a vulnerability scan. He examines a vulnerability detected on one of his servers that has a CVSS breakdown as follows:

CVSS2#AV:N/AC:H/Au:M/C:P/I:N/A:N

Which one of the following statements is true about this vulnerability?

- ✗ **A)** Exploiting this vulnerability would result in total information disclosure.
- ✗ **B)** Exploiting this vulnerability requires either physical access to the target or a local (shell) account on the target.
- ✓ **C)** Exploiting this vulnerability would require two or more instances of authentication.
- ✗ **D)** Exploiting this vulnerability does not require specialized conditions that would be hard to find.

Explanation

Exploiting this vulnerability would require two or more instances of authentication because the Authentication (Au) metric has a value of M, which stands for Multiple. The Au metric describes the authentication an attacker would need to get through to exploit the vulnerability. It has three possible values:

- M - stands for Multiple and means the attacker would need to get through two or more authentication mechanisms
- S - stands for Single and means the attacker would need to get through one authentication mechanism
- N - stands for None and means no authentication mechanisms are in place to stop the exploitation of the vulnerability

For this metric, M is the best ranking.

Exploiting this vulnerability DOES require specialized conditions that would be hard to find because the Access Complexity (AC) metric has a value of H, which stands for High. The AC metric describes the difficulty of exploiting the vulnerability. It has three possible values:

- H - stands for High and means the vulnerability requires special conditions that are hard to find
- M - stands for Medium and means the vulnerability requires somewhat special conditions
- L - stands for Low and means the vulnerability does not require special conditions

For this metric, H is the best ranking.

Exploiting this vulnerability does NOT require either physical access to the target or a local (shell) account on the target because the Access Vector (AV) metric has a value of N, which stands for Network. The AV describes how the attacker would exploit the vulnerability. It has three possible values:

- L - stands for Local and means the attacker must have physical or logical access to the affected system.
- A - stands for Adjacent network and means the attacker must be on the local network
- N - stands for Network and means the attacker can cause the vulnerability from any network

For this metric, L is the best ranking.

Exploiting this vulnerability would NOT result in total information disclosure because the Confidentiality (C) metric has a value of P, which stands for Partial. The C metric describes the information disclosure that may occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no confidentiality impact
- P - stands for Partial and means some access to information would occur
- C - stands for Complete and means all information on the system could be compromised

For this metric, N is the best ranking.

The Availability (A) metric describes the disruption that might occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no availability impact
- P - stands for Partial and means system performance is degraded
- C - stands for Complete and means the system is completely shut down

For this metric, N is the best ranking.

The Integrity (I) metric describes the type of data alteration that might occur and has three possible values:

- N - stands for None and means there is no integrity impact
- P - stands for Partial and means some information modification would occur
- C - stands for Complete and means all information on the system could be compromised

For this metric, N is the best ranking.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

CVSS 2.0 Guide, https://www.first.org/cvss/v2/guide

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

---

Question #60 of 200

Question ID: 1299630

You and the other members of your team are discussing the benefits and risks of a cloud environment versus an on-premises environment. The discussion turns to security. Which statement is NOT true regarding cloud security?

✓ **A)** It is easier to control administrative access.

✗ **B)** Malicious behavior by insiders may compromise data.

✗ **C)** There is ambiguous responsibility.

✗ **D)** Co-locations create a larger attack surface.

Explanation

Controlling administrative access is MORE difficult in a cloud environment because access is provided through the Internet, eliminating the physical security and perimeter security provided in the on-premises environment.

It is true that insiders with the provider may cause issues due to the rights they have working in your support.

It is true that with the responsibility split between the provider and the tenant, gaps in securing the solution may appear.

It is true that co-locations create a larger attack surface. In this scenario, you are sharing the virtual environment and there is more danger from other tenants, which is an issue that does not exist in on-premises environments.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Explain the threats and vulnerabilities associated with operating in the cloud.

References:

Security for Cloud Computing Ten Steps to Ensure Success Version 2.0, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

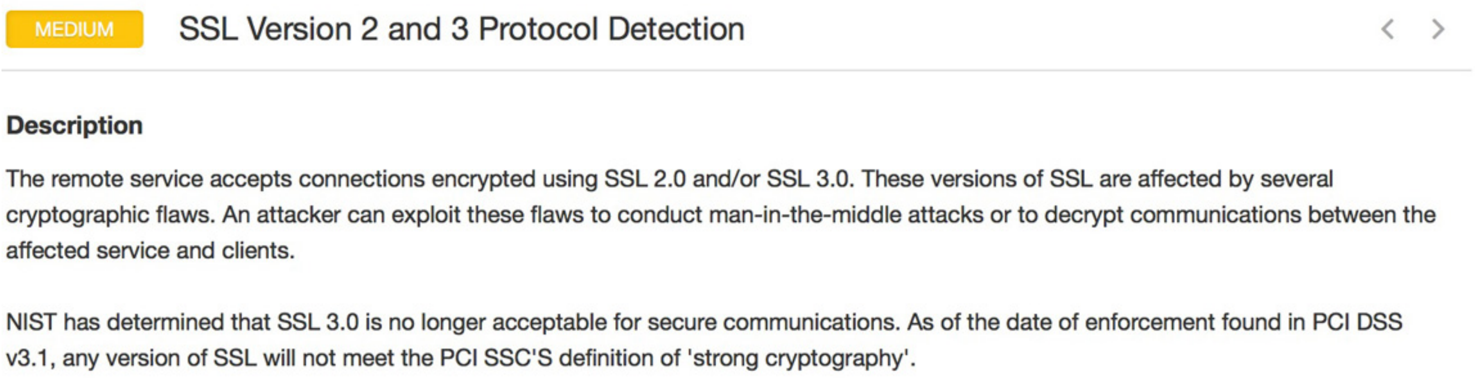
CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 6: Cloud Vulnerabilities

---

Question #61 of 200

Question ID: 1299634

During a recent vulnerability scan, you were scanning the network infrastructure. When the scan finished, you received the following vulnerability message:



MEDIUM SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC'S definition of 'strong cryptography'.

How should you address this vulnerability?

- ✓ **A)** Change to TLS 1.1 or higher.
- ✗ **B)** Remove SSL 3.0.
- ✗ **C)** Remove SSL 2.0.
- ✗ **D)** Implement IPsec.

Explanation

You should change to TLS 1.1 or higher. All versions of SSL are unacceptable because of security issues. SSL should be replaced with TLS.

Internet Protocol Security (IPSec) is not considered a replacement for SSL. IPSec is used to connect to networks, while SSL is used to connect users to services and applications inside those networks. In this scenario, SSL is used, and TLS is an appropriate replacement.

Network infrastructure vulnerabilities can result in successful attacks. Security analysts must assess the network infrastructure, including the network devices and network medium, for vulnerabilities that exist. Vulnerabilities can include insecure/exposed ports, indiscriminate enabling of services, improper system configuration, poor anti-virus or firewall implementation, poor intrusion detection system (IDS) setups, weak password implementation, downloads from untrusted sites, unsecure applications/programs, application and device backdoors, poor physical security, and insufficient training and awareness.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

References:

Vulnerabilities in Network Infrastructures and Prevention/Containment Measures, http://proceedings.informingscience.org/InSITE2012/InSITE12p053-067Awodele0012.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 7: Implementing Controls

---

Question #62 of 200

Question ID: 1299734

Which of the following data types, if disclosed, is most likely to be covered by a legal requirement to communicate the breach to the data owner?

- ✗ **A)** Corporate confidential
- ✓ **B)** PII
- ✗ **C)** Trade secrets
- ✗ **D)** Public

Explanation

Personally identifiable information (PII), if disclosed, is more likely to be covered by a legal requirement to communicate the breach to the data owner. Forty-seven states have laws requiring that data breaches involving PII must be communicated to the data owner (in this case, the person identified by the information).

The exposure of corporate confidential data is unlikely to require disclosure by law unless it involves the release of PII in the process.

The release of public information is not really considered a breach, as it is already publicly available by definition.

The disclosure of trade secrets will be damaging to an organization, but it is unlikely to require disclosure by law.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Security breach notification laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #63 of 200

Question ID: 1299654

You are the security analyst for DreamSuites, Inc. After DreamSuites purchases InterConn, DreamSuites will import all of InterConn's users into its authentication system. DreamSuites uses 802.1x authentication with a RADIUS server, and InterConn uses a captive SSL portal with an LDAP backend.

You need to suggest the best way to integrate these two networks while providing the most secure authentication. Which of the following should you recommend?

- ✗ **A)** Enable LDAP/TLS authentication on DreamSuites' devices.
- ✓ **B)** Enable 802.1x on InterConn's devices.
- ✗ **C)** Enable LDAP authentication on DreamSuites' devices.
- ✗ **D)** Enable RADIUS on InterConn's devices.

Explanation

You should recommend that the company enable 802.1x on InterConn's devices. 802.1x authentication is more secure than LDAP authentication.

You should not enable RADIUS on InterConn's devices. InterConn's devices will use 802.1x to authenticate with the RADIUS servers in DreamSuites' network. InterConn's devices will not even be aware of the RADIUS process that occurs behind the scenes because RADIUS communication occurs between the DreamSuites network access device and the RADIUS server, not between the InterConn device and the RADIUS server.

You should not enable LDAP or LDAP/TLS authentication on DreamSuites' devices because LDAP is not as secure at 802.1x authentication.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

What is 802.1X?, http://www.networkworld.com/article/2216499/wireless/what-is-802-1x-.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #64 of 200

Question ID: 1299760

Which of the following is used to drive improvement in the security posture of the organization?

- ✗ **A)** change control process
- ✗ **B)** incident response plan
- ✓ **C)** lessons learned document
- ✗ **D)** incident summary report

Explanation

: The lessons learned documents will briefly list and discuss what we now know either about the attack or about our environment of which we were formerly unware.

The incident summary report covers the major points of the incident. Some of the highlights that should be included are:

- When was the problem first detected and by whom?
- What was the scope of the incident?
- How it was contained and eradicated?
- What work was performed during recovery?
- In which areas were the CIRT teams effective?
- In which areas did the CIRT teams need improvement?

The incident response plan contains the steps to be followed during an incident. The lessons learned exercise may also uncover flaws in your IR plan. If this is the case, it should be appropriately updated to reflect the needed changes in your procedures.

The change control process is used to manage change and ensure consistency. The lessons learned report may generate a number of changes that should be made to the network infrastructure. All of these changes regardless of how necessary should go through the standard change control process.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Incident Handler's Handbook, https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

---

Question #65 of 200

Question ID: 1299696

During a meeting with upper management, your boss provided some statistics in which he refers several times to a "number of nines" when describing several servers. What type of analysis was performed that generated this information?

- ✗ **A)** Trend analysis
- ✓ **B)** Availability analysis
- ✗ **C)** Anomaly analysis
- ✗ **D)** Wireless analysis

Explanation

These figures are generated by using availability analysis, which is used to describe the amount of uptime divided by the total amount of time. The number of nines to which your boss is referring is the number of nines in the percentage of uptime for a server. So 99.9% (three nines) would be good and 99.99% (four nines) would be better.

This information was not generated using wireless analysis. This is done using a wireless sniffer and does not generate uptime information.

This information was not generated using anomaly analysis. Anomaly analysis focuses on identifying something that is unusual or abnormal. This type of analysis is typically done by an IDS or IPS system.

This information was not generated using trend analysis. Trend analysis focuses on the long term direction in the increase or decrease in a particular type of traffic.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

How to calculate network availability?, https://netbeez.net/2014/09/30/how-to-calculate-network-availability/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #66 of 200

Question ID: 1299788

While performing vulnerability scanning, you discover a Linux computer that has NAXSI installed. What is the purpose of this tool?

- ✗ **A)** IDS
- ✗ **B)** IPS
- ✓ **C)** Web application firewall
- ✗ **D)** Packet capture

Explanation

The purpose of NAXSI is to be a Web application firewall (WAF).

NAXSI does not provide packet capture, IDS, or IPS. Packet capture tools include Wireshark, tcpdump, Network General, and Aircrack-ng.

IDS and IPS tools include Sourcefire, Snort, and Bro.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

How to Install and Configure NAXSI, https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-naxsi-on-ubuntu-14-04

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #67 of 200

Question ID: 1299648

Which of the following vulnerabilities is likely to only affect virtual machines?

- ✓ **A)** VM Escape
- ✗ **B)** CSRF
- ✗ **C)** CSS
- ✗ **D)** SQL injection

Explanation

VM Escape is likely to only affect virtual machines and virtual infrastructure. In an escape attack, the attacker has access to a single virtual host, and then leverages that access to intrude upon the resources assigned to a different virtual machine.

Cross-site scripting (XSS) attacks occur when malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

Cross-site request forgery (CSRF) attacks occur when a malicious web site, email, or application causes a web browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

A SQL injection attack occurs when SQL statement code is injected into an entry field of a web application.

For the CySA+ exam, you need to understand the vulnerabilities associated with virtual infrastructure, including virtual hosts, virtual networks, and the management interface. All virtual hosts need to deploy the same security controls that physical hosts would normally need because VMs will have the same vulnerabilities. The same goes for virtual networks. If you deploy a virtual switch, you need to make sure that you have the same security controls present that you would install on a physical switch. Finally, you need to watch for vulnerabilities with the management interface. For example, if you allow remote administration, you should use SSH instead of Telnet.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Virtual Machine Escape, http://whatis.techtarget.com/definition/virtual-machine-escape

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #68 of 200

Question ID: 1299730

Which department is responsible for providing the manpower, skills, and knowledge to act as a first responder and to remediate all issues found for a large enterprise?

- ✗ **A)** Management
- ✗ **B)** HR
- ✓ **C)** IT
- ✗ **D)** Legal

Explanation

The role of the IT and security teams will be to recognize, identify, and react to incidents, and to provide support in analyzing those incidents when the time comes for a large enterprise. For a small company, this will not be the case as they will need to hire an outside consultant for incident response. In a large enterprise, though, the IT and security teams will provide the manpower, skills, and knowledge to act as first responder and to remediate all issues found. For this reason, advanced training is recommended for those operating in IR-related positons.

The main role of management is to fully back and support all efforts of the IR team and ensure that this support extends throughout the organization.

The HR department has two roles in incident response:

- Develop job descriptions for those persons who will be hired for positions involved in incident response.
- Create policies and procedures that support the removal of employees found to be engaging in improper or illegal activity.

The legal department has three roles in incident response:

- Review the non-disclosure agreement (NDA) to ensure legal support for incident response efforts.
- Develop wording of documents used to contact sites and organizations possibly affected by an incident that originated with your company's software, hardware, or services.
- Assess site liability for illegal computer activity.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Incident Response: Communication is Key, http://www.securitymagazine.com/articles/78810-incident-response-communication-is-key-1

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #69 of 200

Question ID: 1299700

While assisting a senior cyber security technician, you observe him using a tool that allows him to identify specific conversations in the network. He explains that each "conversation" is unique based on various characteristics including the following:

- Source MAC address
- Destination MAC Address
- IP source address
- IP destination address
- Source port
- Destination port

What type of analysis is the technician performing?

✗ **A)** Heuristic analysis

✗ **B)** Trend analysis

✓ **C)** NetFlow analysis

✗ **D)** Anomaly analysis

Explanation

The technician is performing NetFlow analysis. NetFlow is a technology developed by Cisco, and since supported by all major vendors, that can be used to collect and subsequently export IP traffic accounting information. The traffic information is exported using UDP packets to a NetFlow analyzer, which can organize the information in useful ways. It exports records of individual one-way transmissions called flows.

The NetFlow results display the date, start time, duration, transport protocol, source and destination IP address/port number pairs, number of packets, bytes, and number of flows. While many graphical tools are available, a basic dump of a flow would resemble the following output:

```
Date  Start  D  TP  source  IP /port  dest IP/port  PKts  B  Flow
2016-09-01 00:00:00.459  0.000 UDP  192.168.0.1:24920  ->  192.168.0.1:22126  1  46  1
2016-09-01 00:00:00.363  0.000 UDP  192.168.0.1:22126 ->  127.0.0.1:24920  1  80  1
```

The technician is not performing anomaly analysis. Anomaly analysis focuses on identifying traffic or communication that is unusual or abnormal. This type of analysis is typically done by an IDS or IPS system.

The technician is not performing heuristics analysis. Heuristic analysis determines the susceptibility of a system towards a particular threat or risk using decision rules or weighing methods. It is often utilized by antivirus software to identify threats that cannot be discovered with signature analysis because the threat is either too new to have been analyzed (called a zero-day threat) or it is a multi-pronged attack, which is constructed in a way that existing signatures do not identify the threat.

The technician is not performing trend analysis. Trend analysis focuses on the long term direction in the increase or decrease in a particular type of traffic.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Introduction to Cisco IOS NetFlow - A Technical Overview, http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #70 of 200

Question ID: 1299812

Your organization has decided to implement a security continuous monitoring program based on NIST SP 800-137. As your company's security analyst, you have been asked to head this initiative. Which step should you complete first?

- ✗ **A)** Establish a continuous monitoring program to determine metrics, status monitoring frequencies, control assessment frequencies, and a technical architecture.
- ✓ **B)** Define your company's continuous monitoring strategy for assets, vulnerability information, threat information, and business impacts, based on its risk tolerance.
- ✗ **C)** Analyze the data collected, and report findings, determining the appropriate response.
- ✗ **D)** Implement a continuous monitoring program and collect the security-related information required for metrics, assessments, and reporting.

Explanation

You should first define your company's continuous monitoring strategy for assets, vulnerability information, threat information, and business impacts, based on your company's risk tolerance.

The steps for implementing a security continuous monitoring programs are as follows:

1. Define your company's continuous monitoring strategy that includes assets, vulnerability information, threat information, and business impacts and accounts for its risk tolerance.
2. Establish a continuous monitoring program that determines metrics, status monitoring frequencies, control assessment frequencies, and a technical architecture.

3. Implement a continuous monitoring program and collect the security-related information required for metrics, assessments, and reporting.
4. Analyze the data collected, and report findings, determining the appropriate response.
5. Respond to findings with technical, management, and operational mitigating activities or with acceptance, transference/sharing, or avoidance/rejection.
6. Review and update the monitoring program, adjusting the continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

---

Question #71 of 200

Question ID: 1299670

The software development team has started developing a new application. They are assigning a privacy impact rating to the data that will be handled and /or generated by the application. Which best practice prescribed by the SDLC model does this support?

- ✗ **A)** manual peer reviews
- ✓ **B)** security requirements definition
- ✗ **C)** security testing phases
- ✗ **D)** user acceptance testing

Explanation

This process described in the scenario supports the security requirements definition. The security requirements of the solution must be identified. Assigning a privacy impact rating to the data helps to guide measures intended to protect the data from exposure.

Security testing phases are undertaken after security requirements have been defined, because only when the requirements have been defined can one know if they have been met.

In manual peer review, software developers attend meetings where each line of code is reviewed, usually using printed copies.

While it is important to make web applications secure, in some cases security features make the application unusable from the user perspective. User acceptance testing is designed to ensure that does not occur.

Objective:
Software and Systems Security

Sub-Objective:

Explain software assurance best practices.

References:

Security in the software development life cycle, http://searchsecurity.techtarget.com/tip/Security-in-the-software-development-life-cycle

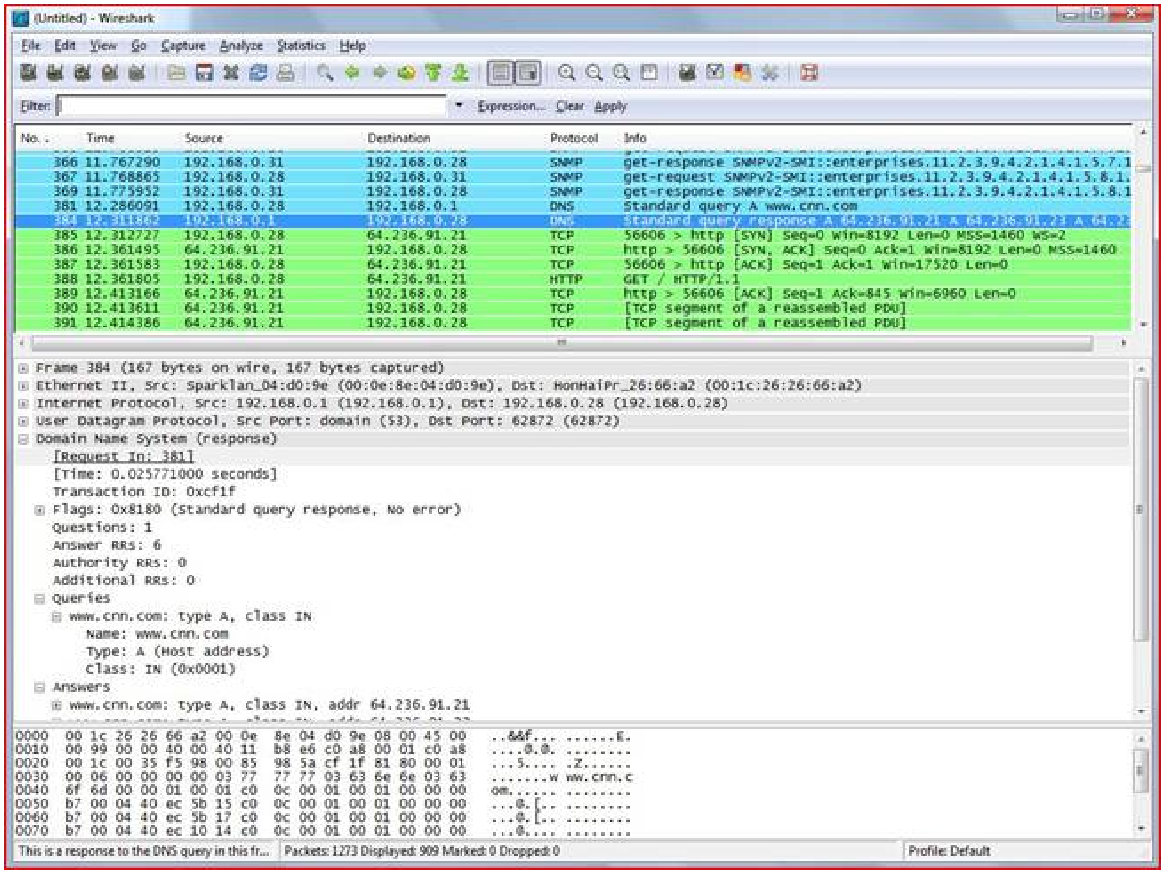
CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

---

Question #72 of 200

Question ID: 1299612

You have just been hired as a junior cyber security analyst. The orientation process involves shadowing a senior analyst. To gauge your current knowledge level, the senior analyst is testing your ability to recognize various tools of the trade. He gives you a quick look at a tool's GUI.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time       Source          Destination     Protocol  Info
  366 11.767290  192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
  367 11.768865  192.168.0.28    192.168.0.31    SNMP      get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1.
  369 11.775952  192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
  381 12.286091  192.168.0.28    192.168.0.1     DNS       Standard query A www.cnn.com
  384 12.311862  192.168.0.1     192.168.0.28    DNS       Standard query response A 64.236.91.21 A 64.236.91.23 A 64.2
  385 12.312727  192.168.0.28    64.236.91.21    TCP       56606 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  386 12.361495  64.236.91.21    192.168.0.28    TCP       http > 56606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
  387 12.361583  192.168.0.28    64.236.91.21    TCP       56606 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
  388 12.361805  192.168.0.28    64.236.91.21    HTTP      GET / HTTP/1.1
  389 12.413166  64.236.91.21    192.168.0.28    TCP       http > 56606 [ACK] Seq=1 Ack=845 Win=6960 Len=0
  390 12.413611  64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
  391 12.414386  64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
```

```
⊞ Frame 384 (167 bytes on wire, 167 bytes captured)
⊞ Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)
⊟ Domain Name System (response)
    [Request In: 381]
    [Time: 0.025771000 seconds]
    Transaction ID: 0xcf1f
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.cnn.com: type A, class IN
        Name: www.cnn.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.cnn.com: type A, class IN, addr 64.236.91.21
```

```
0000  00 1c 26 26 66 a2 00 0e  8e 04 d0 9e 08 00 45 00   ..&&f... ......E.
0010  00 99 00 00 40 00 40 11  b8 e6 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 1c 00 35 f5 98 00 85  98 5a cf 1f 81 80 00 01   ...5.... .Z......
0030  00 06 00 00 00 00 03 77  77 77 03 63 6e 6e 03 63   .......w ww.cnn.c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om...... ........
0050  b7 00 04 40 ec 5b 15 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0060  b7 00 04 40 ec 5b 17 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0070  b7 00 04 40 ec 10 14 c0  0c 00 01 00 01 00 00 00   ...@.... ........
```

This is a response to the DNS query in this fr... | Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0 | Profile: Default

What type of tool is displayed?

- ✗ **A)** Resource monitoring tool
- ✗ **B)** Firewall log
- ✗ **C)** NetFlow analyzer
- ✓ **D)** Packet analyzer

Explanation

The tool shown is Wireshark, which is a packet analyzer. Packet analyzers are also called sniffers and sometimes protocol analyzers. This type of tool captures traffic on the network.

The tool is not a resource monitoring tool. These tools focus on the use of CPU, disk, memory, and network resources on a system. They do not capture traffic on the network. Windows Resource Monitor is an example of this type of tool.

The tool is not a NetFlow analyzer. NetFlow is a technology developed by Cisco, and since supported by all major vendors, that can be used to collect and subsequently export IP traffic accounting information. The traffic information is exported using UDP packets to a NetFlow analyzer, which can organize the information in useful ways. It exports records of individual one-way transmissions called flows. While they identify these flows as they go through the monitored device such as a router, they do not capture traffic on the network. While many graphical tools are available, a basic dump of a flow is shown below. It displays the date, start time, duration, transport protocol, source and destination IP address/port number pairs, number of packets, bytes, and number of flows:

```
Date  Start  D  TP  source  IP /port  dest IP/port  PKts  B  Flow
2016-09-01  00:00:00.459  0.000 UDP  192.168.0.1:24920 -> 192.168.0.1:22126  1  46  1
2016-09-01  00:00:00.363 0.000 UDP  192.168.0.1:22126 -> 127.0.0.1:24920  1  80  1
```

The tool is not a firewall log. These types of tool display traffic that has been allowed and denied passage through the firewall, not captured packets.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

How to Use Wireshark to Capture, Filter and Inspect Packets, http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

Question #73 of 200

Question ID: 1299800

Which of the following helps to prioritize the application of resources to the most critical vulnerabilities?

- ✓ **A)** Risk assessment matrix
- ✗ **B)** PERT chart
- ✗ **C)** Access control matrix
- ✗ **D)** Gantt chart

Explanation

Typically, a risk assessment matrix is created where subject experts grade all risk on their likelihood and their impact. This help to prioritize the application of resources to the most critical vulnerabilities.

An access control matrix is a table that lists subjects (users) in rows and objects (resources) in columns. It characterizes the rights of each subject with respect to every object in the system.

PERT charts and Gantt charts are used in project management to schedule tasks, organize resources and gain a greater understanding of their projects.

Objective:
Compliance and Assessment

Sub-Objective:
Given a scenario, apply security concepts in support of organizational risk mitigation.

References:

A Critical Tool for Assessing Project Risk, http://www.brighthubpm.com/risk-management/88566-tool-for-assessing-project-risk/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 20: Supporting Risk Mitigation

---

Question #74 of 200

Question ID: 1299702

The security team notices that several peer-to-peer programs are being used in the network to share music and movies, possibly in violation of intellectual property laws. You would like to identify the users of these programs. What type of analysis needs to be performed?

- ✗ **A)** Heuristic analysis
- ✗ **B)** Trend analysis
- ✓ **C)** Protocol analysis
- ✗ **D)** Anomaly analysis

Explanation

Protocol analysis needs to be performed. Because you want to identify users of the programs, you need to capture packets that are using this program or protocol and identify the source and destination IP addresses. Protocol analysis involves examining information in the header of the packet. When protocol analyzers are used, they examine these headers for information like the protocol in use or details involving the communication process, such as source and destination IP address and MAC address.

Anomaly analysis focuses on identifying traffic or communication that is unusual or abnormal. This type of analysis is typically done by an IDS or IPS system. In this case, you are specifically interested in identifying packets using the program and the source and destination IP addresses.

Heuristic analysis determines the susceptibility of a system towards a particular threat or risk using decision rules or weighing methods. It is often utilized by antivirus software to identify threats that cannot be discovered with signature analysis because the threat is either too new to have been analyzed (called a zero-day threat) or it is a multi-pronged attack, which is constructed in a way that existing signatures do not identify the threat. In this scenario, we are specifically interested in identifying packets using the program and the source and destination IP addresses.

Trend analysis focuses on the long-term direction in the increase or decrease in a particular type of traffic. In this case, we are specifically interested in identifying packets using the program and the source and destination IP addresses.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

What's the difference between packet sniffers and protocol analyzers?, https://searchnetworking.techtarget.com/answer/Whats-the-difference-between-packet-sniffers-and-protocol-analyzers

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #75 of 200

Question ID: 1299771

While performing a regular analysis of the firewall log, you discover that there is traffic leaving your network at regular intervals from the same device to the same destination. What is this type of traffic called?

- ✗ **A)** ping sweep
- ✗ **B)** peer-to-peer
- ✗ **C)** probe request
- ✓ **D)** beaconing

Explanation

Beaconing refers to traffic that leaves your network at regular intervals. This type of traffic could be generated by compromised hosts that are attempting to communicate with (or call home to) the malicious party that compromised the host. The compromised hosts do this in response to the command and control software that is running on the hacker's device. The best course of action is to identify the destination of the traffic and block it at the firewall. Beaconing indicates some sort of malware or compromise is present, so the best course of action is to remove all malware, and if the device still does not function properly after the malware removal, re-image the device. You should also keep all anti-malware up to date and ensure that users are trained in safe practices.

This is not a ping sweep. A ping sweep would touch the device only once. Ping sweeps use the ICMP protocol to identify all live hosts by pinging all IP addresses in the known network. All devices that answer the ping are known to be up and running. The symptoms of this attack are unusual spikes in network traffic. These sweeps can be detected by IDS and IPS systems. They indicate an attempt to map your network. The best course of action is to identify the source of the sweeps. Going forward, you should also deploy an IPS or IDS if not already present

This is not a probe request. The device would not send these at regular intervals. That is a wireless transmission sent by a wireless station to associate with a WLAN that is not advertising its SSID.

This is not peer-to-peer traffic. Peer-to-peer traffic occurs between peers within your network or with hosts outside the network. This traffic would not be at regular intervals.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Testing Your Defenses - Beaconing, http://blog.opensecurityresearch.com/2012/12/testing-your-defenses-beaconing.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

---

Question #76 of 200

Question ID: 1299776

You are assisting a senior forensics investigator with a crime scene. While you are watching, he runs the following command:

```
user@kaplan:~# md5sum /dev/pw3
```

He receives the following output:

```
9b98b637a132974e41e3c6ae1fc9fc96 /dev/pw3
```

What is the long string of values in the output called?

- ✓ **A)** Hash value
- ✗ **B)** Initialization vector
- ✗ **C)** Salt value
- ✗ **D)** Encryption key

Explanation

That value is the hash value, and it was derived by running the file against the MD5 hashing algorithm. This algorithm generates this value based on the contents of the file or volume against which it was run. Its value is in providing a way to determine at a later time if the file or volume has changed. To validate an image, a hash is generated for both the original and the copy. If the hashes match, the images are identical. Both hashes should be recorded as part of the forensic log for the investigation. Hashing can be used to check to see if there have been any changes to binaries.

It is not an encryption key. Encryption keys are used to encipher a message. MD5 does not perform encryption. It generates a value that can be used to determine the integrity of the file or volume.

It is not an initialization vector (IV). These are values used within certain encryption algorithms to add randomness to the calculations to prevent patterns in the output that can be used to reverse-engineer the encryption key.

A salt value is random data that is used as an additional input to a one-way function that "hashes" a password or passphrase. It is used to make cracking the hash more difficult.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

What is MD5 Hash and How to Use it, https://www.gohacking.com/what-is-md5-hash/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

Question #77 of 200

Question ID: 1299711

You have discovered that several workstation computers on your company's network have been infected with a Trojan that is used to target a single server. Which vulnerability has infected the workstation computers?

- ✗ **A)** Spyware
- ✓ **B)** DDoS
- ✗ **C)** Ransomware
- ✗ **D)** APT

Explanation

A Distributed Denial of Service (DDoS) is the vulnerability that has infected the workstation computers. The workstations will now act as zombies to carry out the attack on a single server.

Spyware enables an attacker to obtain information about another's computer activities by transmitting data covertly from their hard drive.

Ransomware is malicious software that blocks access to a computer system until a sum of money is paid.

An advanced persistent threat (APT) is an attack in which an unauthorized user accesses a network and stays there undetected for a long period of time with the intention of stealing data.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

What is a DDoS attack?, http://www.digitalattackmap.com/understanding-ddos/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #78 of 200

Question ID: 1299708

Which of the following is a system that has been isolated from the other systems and is used for analyzing suspect files and messages for malware?

- ✗ **A)** Virtual machine
- ✗ **B)** Sandbox
- ✗ **C)** Honeypot
- ✓ **D)** Sheep dip computer

Explanation

One option for studying malware is to set up a sheep dip computer. This is a system that has been isolated from the other systems and is used for analyzing suspect files and messages for malware.

A virtual machine can be isolated from other systems and could in fact be a sheep dip computer, but that is not its main function.

A sandbox is a technique that can used to run a possibly malicious program in a safe environment, so that it does not infect the local system. The term refers to the technique and not the computer itself.

A honeypot is a system designed to attract hackers and engage them so that information can be gathered about the attacker.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

What is a sheep-dip?, http://sheepdip.sourceforge.net/Definition.php

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #79 of 200

Question ID: 1299744

Which of the following is NOT considered to be a stakeholder to the incident response process?

- ✗ **A)** HR
- ✗ **B)** Marketing
- ✓ **C)** Sales
- ✗ **D)** Management

Explanation

While all departments may be involved in a specific investigation, the stakeholders are those who receive updates though the process and may provide input. The most common stakeholders are:

- HR

- Legal
- Marketing
- Management

The HR department has two roles in incident response:

- Develop job descriptions for those persons who will be hired for positions involved in incident response.
- Create policies and procedures that support the removal of employees found to be engaging in improper or illegal activity.

The legal department has three roles in incident response:

- Review the non-disclosure agreement (NDA) to ensure legal support for incident response efforts.
- Develop wording of documents used to contact sites and organizations possibly affected by an incident that originated with your company's software, hardware, or services.
- Assess site liability for illegal computer activity.

Marketing can be involved in the following activities in support of the incident response plan:

- Create newsletters and other educational materials to be used in employee response training.
- Coordinate with the legal team to prepare media responses and internal communications regarding incidents before they occur.

The MOST important factor that will ensure the success of an incident response plan is the support of upper management, both verbally and financially (through the budget process). Moreover, all other levels of management should fall in line to support all incident response efforts. Specifically, management's role in incident response can be defined as:

- Communicate the importance of the incident response plan to all parts of the organization.
- Create agreements detailing the authority of the IR team to take over business systems if necessary.
- Create decision systems for determining when key systems must be removed from the network.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Incident Response: How to Fight Back, https://www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #80 of 200

Question ID: 1299720

Which of the following is a technique that can be used to run a possibly malicious program in a safe environment so it does not infect the local system?

✗ **A)** Network segmentation

✗ **B)** System isolation

✓ **C)** Sandboxing

✗ **D)** Decomposition

Explanation

A sandbox is a technique that can used to run a possibly malicious program in a safe environment, so it does not infect the local system.

Network segmentation creates security zones that are separated from one another by devices such as firewalls and routers that can be used to control the flow of traffic between the zones. This is used to isolate a group of devices.

Decomposition is the process of breaking something down to discover how it works. When applied to software, it is the process of discovering how the software works, perhaps who created it and in some cases, how to prevent the software from performing malicious activity.

System isolation is used to isolate a system from other systems through the control of communications with the device. This would isolate a single device but would not isolate the malicious program in its own processing area.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, implement configuration changes to existing controls to improve security.

References:

3 Essential Steps for Your Vulnerability Remediation Process, https://resources.whitesourcesoftware.com/blog-whitesource/3-essential-steps-for-your-vulnerability-remediation-process

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 12: Implementing Controls to Improve Security

---

Question #81 of 200

Question ID: 1299709

When you study malware to discover how it functions, what operation are you performing?

✓ **A)** Reverse engineering

✗ **B)** Rules of engagement

✗ **C)** Penetration testing

✗ **D)** Vulnerability testing

Explanation

Reverse engineering means to take something apart to discover how it works and perhaps to replicate it. In cybersecurity, reverse engineering is used to analyze both hardware and software and for various reasons. Among these reasons are:

- To discover how malware functions
- To determine whether malware is present in software
- To locate software bugs

- To locate security problems in hardware

You are not performing penetration testing. A penetration test (often called a pentest) is designed to simulate an attack on a system, a network, or an application. Its value lies in its potential to discover security holes that may have gone unnoticed.

You are not establishing rules of engagement. The rules of engagement define how penetration testing should occur. These are issues that should be settled and agreed upon before any testing begins.

You are not performing vulnerability testing. A vulnerability test attempts to identify vulnerabilities and address them.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

The AlienVault Blogs> Reverse Engineering Malware, https://www.alienvault.com/blogs/labs-research/reverse-engineering-malware

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #82 of 200

Question ID: 1299629

Which of the following attacks is more likely to only affect mobile devices and not desktop computers?

- ✗ **A)** Malware
- ✓ **B)** QR code-based attacks
- ✗ **C)** Phishing attacks
- ✗ **D)** DDoS attacks

Explanation

Quick response (QR) code attacks are more likely to only affect mobile devices and not desktop computers because they require the reading of a QR code, which most desktop computers do not support.

All of the other attacks can affect mobile devices and desktop computers.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Explain the threats and vulnerabilities associated with specialized technology.

References:

Security Attacks via Malicious QR Codes, https://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/#gref

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 5: Vulnerabilities Associated with Specialized Technology

Question #83 of 200

Question ID: 1299639

You would like to provide isolation between two systems to ensure that communication between them is not intercepted by other parties or devices. You would like to make it Layer 2 isolation. Which of the following techniques would be appropriate?

- ✗ **A)** Subnets
- ✗ **B)** Jump box
- ✓ **C)** VLANs
- ✗ **D)** DMZ

Explanation

A virtual local area network (VLAN) would be appropriate. VLANs separate devices logically at Layer 2 and Layer 3. Enterprise-level switches are capable of creating VLANs. These logical subdivisions of a switch segregate ports from one another as if they were in different LANs. Even if two devices in different VLANs had IP addresses in the same subnet, they would not be capable of communicating because of the separation at Layer 2.

The solution would not be subnets. Subnets create a separation only at Layer 3.

The solution would not be a jump box. A jump server or jump box is a server that is used to access devices that have been placed in a secure network zone, such as a DMZ. The server would span the two networks to provide access from an administrative desktop to the managed device. This would be done at Layer 3.

The solution would not be a DMZ. A demilitarized zone (DMZ) is a network logically separate at Layer 3 from the intranet where resources that will be accessed from the outside world are made available. Exceptions are used with server isolation but not with DMZs.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Understanding and Configuring VLANs, http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/18ew/configuration/guide/config/vlans.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #84 of 200

Question ID: 1299632

Recently, your network suffered an attack that was unsuccessful. As a result, you are reviewing the access control list (ACL) on the routers. Which of the following is NOT a recommendation for ACLs?

- ✗ **A)** Allow responses to requests that were initiated from inside the network
- ✗ **B)** Block incoming IP addresses that have a private IP address as the source
- ✓ **C)** Never include a permit statement in an ACL
- ✗ **D)** Block incoming traffic that uses the ICMP protocol

Explanation

Never including a permit statement in an ACL is NOT a recommendation. If you do not include at least one permit statement in the ACL, you might as well shut down the interface, because no traffic will be allowed. There is an implied deny all rule at the end of every ACL, and therefore, you must specifically allow any traffic that needs to be allowed.

It is recommended to block incoming IP addresses that have a private IP address as the source. These are always spoofed packets, as private IP addresses are not routable on the Internet.

It is recommended to block incoming traffic that uses the ICMP protocol. This should only be allowed inside the network (if at all). It can be used to perform some stages of topology discovery.

It is recommended to allow responses to requests that were initiated from inside the network. Since this traffic is a response to a connection initiated from inside the network, it should be safe.

Performing router and firewall ACL review will help you to determine why certain traffic is being allowed or denied. Remember that the order of the rules in the ACL will affect the communication as well.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

References:

Securing Your Network With an Internet Access Router (or Getting Your Money's Worth From Your Cisco Gear), https://www.sans.org/reading-room/whitepapers/networkdevs/securing-network-internet-access-router-or-moneys-worth-c-242

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 7: Implementing Controls

---

Question #85 of 200

Question ID: 1299635

You are examining a server that has undergone a SQL injection attack. Which server is most likely the victim of this attack?

- ✗ **A)** File server
- ✓ **B)** Database server
- ✗ **C)** Web server
- ✗ **D)** Email server

Explanation

A database server is most likely the victim in a SQL injection attack. A SQL injection attack inserts a SQL query as the input from the client to the application. The purpose of this attack is to read sensitive data from the database, modify the data, execute administrative operations on the database, recover the content of a given file, and even issue commands to the operating system.

The web server is usually the means whereby the SQL injection attack is delivered, but it is not really the victim of the attack. A web server is most likely the victim of cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks.

A file server is not the victim of this attack. A file server is more likely to become a victim of a directory traversal or some other access attack.

An email server is not the victim of this attack. An email server is more likely to become a victim of a Denial of Service (DoS) attack.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

References:

What is a SQL injection attack?, https://www.malwarebytes.com/sql-injection/

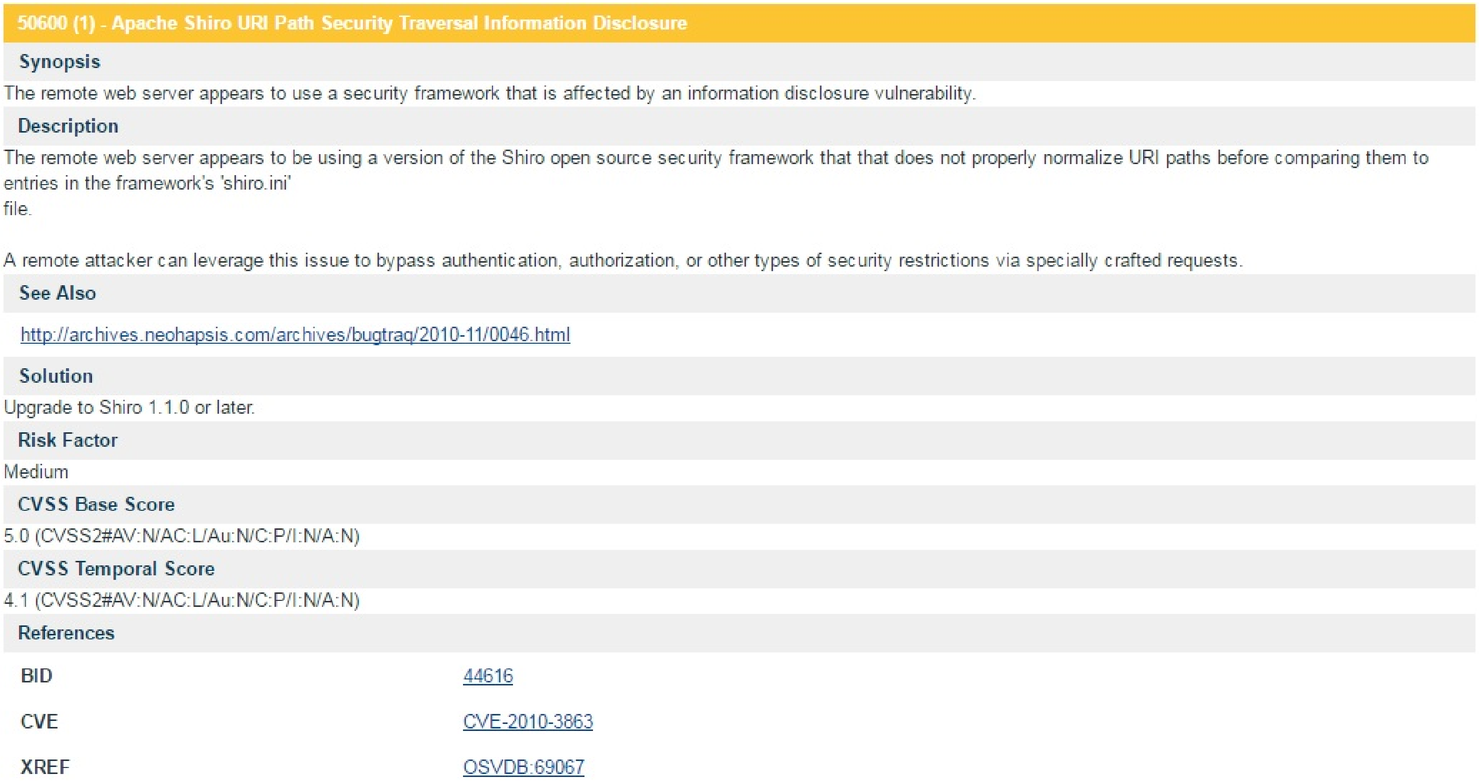
CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 7: Implementing Controls

---

Question #86 of 200

Question ID: 1299614

While analyzing the results of the most recent vulnerability scan, Sara reads the following information about a vulnerability detected on an Apache web server:



50600 (1) - Apache Shiro URI Path Security Traversal Information Disclosure

Synopsis

The remote web server appears to use a security framework that is affected by an information disclosure vulnerability.

Description

The remote web server appears to be using a version of the Shiro open source security framework that that does not properly normalize URI paths before comparing them to entries in the framework's 'shiro.ini'
file.

A remote attacker can leverage this issue to bypass authentication, authorization, or other types of security restrictions via specially crafted requests.

See Also

http://archives.neohapsis.com/archives/bugtraq/2010-11/0046.html

Solution

Upgrade to Shiro 1.1.0 or later.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

BID	44616
CVE	CVE-2010-3863
XREF	OSVDB:69067

What condition is needed to exploit this vulnerability?

- ✗ **A)** Minimally specialized conditions are required.
- ✗ **B)** Highly specialized conditions are required.
- ✗ **C)** Somewhat specialized conditions are required.
- ✓ **D)** No special conditions are required.

Explanation

No special conditions are required to exploit this vulnerability because the Access Complexity (AC) metric is L, which stands for Low. The AC metric describes the difficulty of exploiting the vulnerability. It has three possible values:

- H - stands for High and means the vulnerability requires special conditions that are hard to find
- M - stands for Medium and means the vulnerability requires somewhat special conditions
- L - stands for Low and means the vulnerability does not require special conditions

For this metric, H is the best ranking.

Objective:

Threat and Vulnerability Management

Sub-Objective:

Given a scenario, analyze the output from common vulnerability assessment tools.

References:

CVSS 2.0 Guide, https://www.first.org/cvss/v2/guide

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

Question #87 of 200

Question ID: 1299747

You perform a vulnerability scan and receive the vulnerability report. After you mitigate the vulnerabilities, you must prepare a report for management. One of management's favorite reports is a trending report that graphs the types of vulnerabilities over time. When you complete the report, you notice there has been a steady rise of malware infections on desktop computers over the past six months, despite the fact that anti-malware software is installed. You need to provide a solution to this issue. Which of the following should you suggest?

- ✗ **A)** Restart the anti-malware software on all desktops.
- ✓ **B)** Require that all users attend mandatory security awareness training.
- ✗ **C)** Reinstall the anti-malware software on all desktops.
- ✗ **D)** Update the anti-malware software on all desktops.

Explanation

You should suggest that all users attend mandatory security awareness training. Anti-malware software may not catch all instances of anti-malware. Unsafe user practices are the likely cause of the malware infections that are occurring in this environment.

You should not update the anti-malware software on all desktops. While this action may help to prevent some future infections, no anti-malware software is 100% effective. Because malware infection can be caused by unsafe user practices, you need to ensure that users are trained on how to recognize and avoid malware.

You should not restart the anti-malware software on all desktops. While this action may help to prevent future infections, no anti-malware software is completely foolproof.

You should not reinstall the anti-malware software on all desktops. While this action may help to prevent future infections, no anti-malware software is completely foolproof.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

How Security Awareness Training Can Save You From The Horror Of Malware, https://resources.infosecinstitute.com/category/enterprise/securityawareness/employee-security-threats/security-awareness-and-malware/#gref

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

Question #88 of 200

Question ID: 1299817

You have been hired as the cybersecurity analyst for Verigon, Inc. Management has informed you that the company recently adopted a new initiative to implement NIST's Framework for Improving Critical Infrastructure Cybersecurity. You must work first to perform the Identify Framework Core Function.

Which of the following activities is NOT part of this function?

- ✗ **A)** asset management
- ✗ **B)** risk assessment
- ✓ **C)** information protection procedures
- ✗ **D)** governance

Explanation

Information protection procedures are NOT part of the Identify Framework Core Function. It is part of the Protect Function.

NIST's Cybersecurity Framework has the following five Core Functions:

1. Identify - includes risk assessment, asset management, governance, business environment, and risk management strategy
2. Protect - includes information processes and procedures, access control, awareness and training, data security, maintenance, and protective technology.
3. Detect - includes anomalies and events, security continuous monitoring, and detection processes.
4. Respond - includes response planning, communications, analysis, mitigation, and improvements.
5. Recover - includes recovery planning, improvements, and communications.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

Question #89 of 200

Question ID: 1299680

Which of the following is a good example of exercising care in ensuring the source authenticity and integrity of the components of hardware purchased from a vendor?

- ✓ **A)** Trusted Foundry program
- ✗ **B)** Hashing
- ✗ **C)** Decomposition
- ✗ **D)** Fingerprinting

Explanation

The Trusted Foundry program is a good example of exercising care in ensuring the source authenticity and integrity of the components of hardware purchased from a vendor. This DoD program identifies "trusted "vendors, and ensures what is called a trusted supply chain. A trusted supply chain begins with trusted design and continues with trusted mask, foundry, packaging/assembly, and test services. This is also an example of ensuring the source authenticity of hardware.

Fingerprinting or hashing is the process of taking a large document or file and using a hashing algorithm to reduce the file to a character string that can be used to verify the integrity of the file. A fingerprint or hash will show if the file has changed in any way from when it was first hashed.

Hashing is another term for fingerprinting when applied to document integrity.

Decomposition is the process of breaking something down to discover how it works. When applied to software, it is the process of discovering how the software works, perhaps who created it and in some cases, how to prevent the software from performing malicious activity.

Objective:
Software and Systems Security

Sub-Objective:
Explain hardware assurance best practices.

References:

DMEA Trusted IC Program, https://www.dmea.osd.mil/TrustedIC.aspx

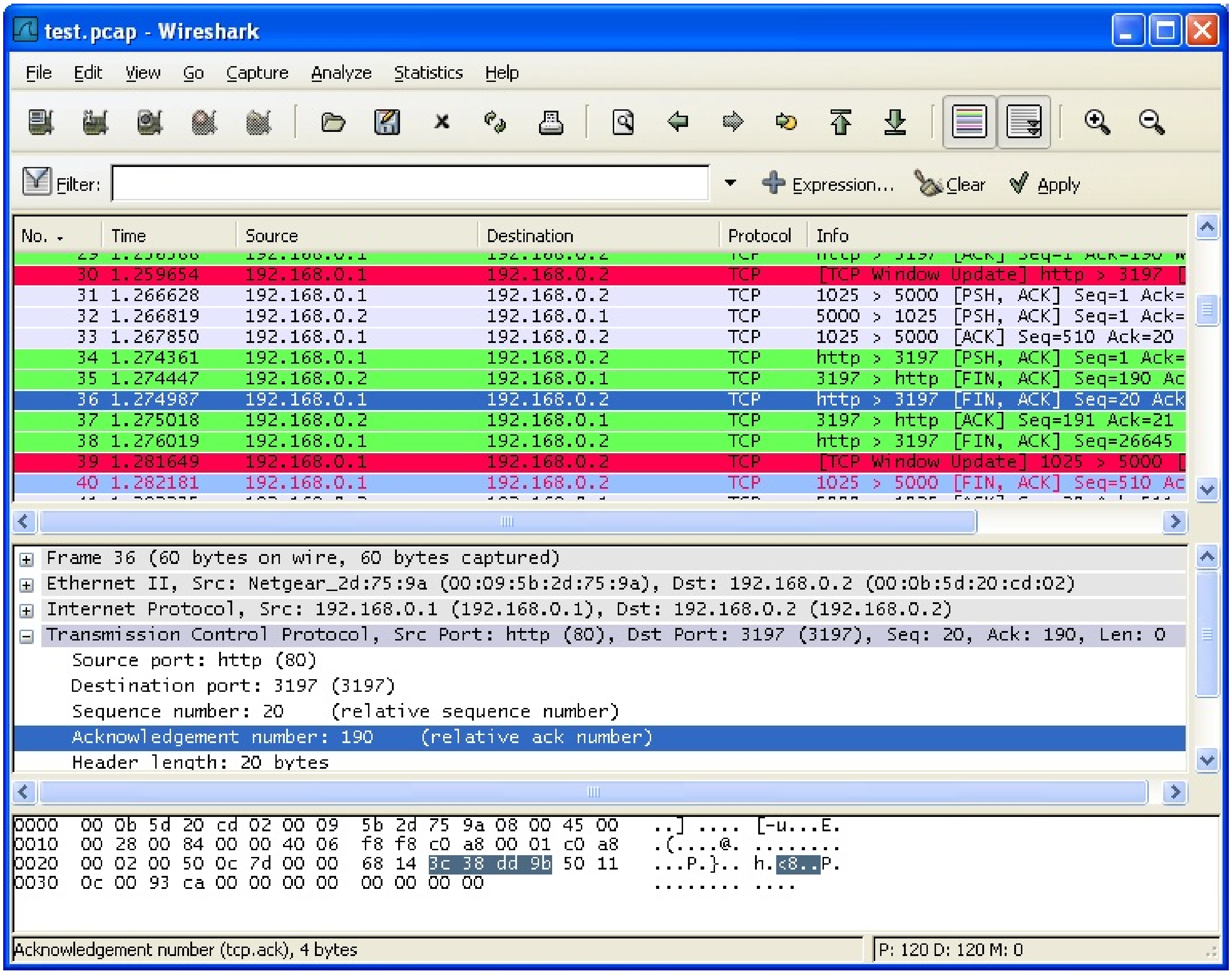
CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 10: Hardware Best Practices

---

Question #90 of 200

Question ID: 1299691

You have been capturing packets to troubleshoot a network issue. The exhibit shows an excerpt of some of the packets captured.



```
No. -  Time      Source        Destination   Protocol Info
   30 1.259654  192.168.0.1   192.168.0.2   TCP      [TCP Window Update] http > 3197 [
   31 1.266628  192.168.0.1   192.168.0.2   TCP      1025 > 5000 [PSH, ACK] Seq=1 Ack=
   32 1.266819  192.168.0.2   192.168.0.1   TCP      5000 > 1025 [PSH, ACK] Seq=1 Ack=
   33 1.267850  192.168.0.1   192.168.0.2   TCP      1025 > 5000 [ACK] Seq=510 Ack=20
   34 1.274361  192.168.0.1   192.168.0.2   TCP      http > 3197 [PSH, ACK] Seq=1 Ack=
   35 1.274447  192.168.0.2   192.168.0.1   TCP      3197 > http [FIN, ACK] Seq=190 Ac
   36 1.274987  192.168.0.1   192.168.0.2   TCP      http > 3197 [FIN, ACK] Seq=20 Ack
   37 1.275018  192.168.0.2   192.168.0.1   TCP      3197 > http [ACK] Seq=191 Ack=21
   38 1.276019  192.168.0.1   192.168.0.2   TCP      http > 3197 [FIN, ACK] Seq=26645
   39 1.281649  192.168.0.1   192.168.0.2   TCP      [TCP Window Update] 1025 > 5000 [
   40 1.282181  192.168.0.1   192.168.0.2   TCP      1025 > 5000 [FIN, ACK] Seq=510 Ac
```

```
⊞ Frame 36 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:2d:75:9a), Dst: 192.168.0.2 (00:0b:5d:20:cd:02)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 3197 (3197), Seq: 20, Ack: 190, Len: 0
    Source port: http (80)
    Destination port: 3197 (3197)
    Sequence number: 20    (relative sequence number)
    Acknowledgement number: 190    (relative ack number)
    Header length: 20 bytes
```

```
0000  00 0b 5d 20 cd 02 00 09  5b 2d 75 9a 08 00 45 00   ..] .... [-u...E.
0010  00 28 00 84 00 00 40 06  f8 f8 c0 a8 00 01 c0 a8   .(....@. ........
0020  00 02 00 50 0c 7d 00 00  68 14 3c 38 dd 9b 50 11   ...P.}.. h.<8..P.
0030  0c 00 93 ca 00 00 00 00  00 00 00 00               ........ ....
```

Acknowledgement number (tcp.ack), 4 bytes   P: 120 D: 120 M: 0

Which of the following statements is TRUE about packet number 36 (highlighted in blue)?

- ✗ **A)** The packet came from 192.168.0.2.
- ✗ **B)** The source port is 3197.
- ✓ **C)** The packet is a response from a web server.
- ✗ **D)** Only the ACK flag is set.

Explanation

The output indicates that packet number 36 came from a web server because the source port is 80, which is used by HTTP. This information is listed in the TCP section of the byte view, which is the lower of the two panels.

Both the FIN and ACK flags are set. This information can be seen in the info section in the upper pane on right side where the flags are listed in brackets like this: `[FIN, ACK]`.

The packet came from 192.168.0.1, not 192.168.0.2. This information can be seen in both panes. In the bottom pane, it is listed in the IP section of the packet.

The source port is not 3197. That is the destination port on the web client. The source port is 80. This information is listed in the TCP section of the byte view, which is the lower of the two panels.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

How to Use Wireshark to Capture, Filter, and Inspect Packets, http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #91 of 200

Question ID: 1299785

Which of the following tools should you use to create and view certificates?

- ✗ **A)** Nexpose
- ✗ **B)** EnCase
- ✗ **C)** MD5sum
- ✓ **D)** OpenSSL

Explanation

OpenSSL can be installed to create and view certificates.

EnCase is a forensic suite. Other forensic suites include FTK, Helix, Sysinternals, and Cellebrite.

Nexpose and Metasploit are exploit frameworks. MD5sum and SHA are hashing tools.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

OpenSSL, https://whatis.techtarget.com/definition/OpenSSL

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

Question #92 of 200

Question ID: 1299626

You have run a Nessus vulnerability scan on several Linux servers. When you receive the scan report, you suspect that there are several false positives on the report. What should you do FIRST?

- ✗ **A)** Configure exceptions in Nessus for the false positives to ensure they are no longer reported.
- ✓ **B)** Verify the false positives to ensure that you can eliminate them from the report.
- ✗ **C)** Install the Nessus plug-ins to resolve the false positives.
- ✗ **D)** Resolve the false positives in order based on their CVSS value.

Explanation

You should first verify or validate the false positives to ensure that you can eliminate them from the report. While validation of false positives can be very time consuming, it is a necessary step to ensure that they are not true positives. Once they are verified, you can then configure exceptions for them.

You should not resolve the false positives in order based on their Common Vulnerability Scoring System (CVSS) value. False positives do not need to be resolved because these issues actually do not exist. When a true vulnerability is found, the CVSS should act as a prioritization guide. However, the CVSS should not be the only guide you use. Other factors in resolving vulnerabilities include the difficulty of implementing a solution and the asset's value.

You should not install the Nessus plug-ins for the false plug-ins. Nessus plug-ins are created by Tenable's research staff when new vulnerabilities are discovered. These should be installed to help you discover new vulnerabilities. Based on the scenario, you know that the plug-ins for the vulnerabilities were already installed because the false positives were reported.

You should not configure exceptions in Nessus for the false positives to ensure they are no longer reported. This should only be done after you have verified that the false positives are indeed false positives.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

CVSS 2.0 Guide, https://www.first.org/cvss/v2/guide

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

Question #93 of 200

Question ID: 1299738

Which of the following is NOT a role of the legal department in the creation of an incident response plan?

- ✗ **A)** Develop wording of documents used to contact possibly affected sites and organizations
- ✓ **B)** Create policies and procedures that support the removal of employees found to be engaging in improper or illegal activity.
- ✗ **C)** Review non-disclosure agreement to ensure their support for incident response efforts.
- ✗ **D)** Assess site liability for illegal computer activity.

Explanation

It is not a role of the legal department to create policies and procedures that support the removal of employees found to be engaging in improper or illegal activity. That is a role of the HR department. The HR department has two roles in incident response:

- Develop job descriptions for those persons who will be hired for positions involved in incident response.
- Create policies and procedures that support the removal of employees found to be engaging in improper or illegal activity.

The legal department has three roles in incident response:

- Review the non-disclosure agreement (NDA) to ensure legal support for incident response efforts.
- Develop wording of documents used to contact sites and organizations possibly affected by an incident that originated with your company's software, hardware, or services.
- Assess site liability for illegal computer activity.

If an incident occurs, the organization is responsible for coordinating incident response activities with relevant entities, including:

- Legal
- Human resources
- Public relations
- Internal and external
- Law enforcement
- Senior leadership
- Regulatory bodies

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Incident Response: Communication is Key, http://www.securitymagazine.com/articles/78810-incident-response-communication-is-key-1

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #94 of 200

Question ID: 1299656

Your company currently implements context-based authentication for all users. All users log in using their own user account. As part of this context-based authentication solution, supervisors are allowed to log in from any facility in your company.

Recently, while performing a security review, you noticed that a supervisor logged in from multiple facilities on the same day. You realize that it was not physically possible for that supervisor to be in both facilities on the same day. After researching this issue, you think that one of the logins was not actually made by the supervisor. You immediately work with the supervisor to change his password. Now you need to take measures to prevent something like this from happening again. What should you do?

✓ **A)** Change the supervisors from location-based authentication to rule-based authentication.

- ✗ **B)** Change the supervisors from time-based authentication to rule-based authentication.
- ✗ **C)** Change the supervisors from location-based authentication to frequency-based authentication.
- ✗ **D)** Change the supervisors from time-based authentication to frequency-based authentication.

Explanation

You should change the supervisors from location-based authentication to rule-based authentication. With rule-based authentication, you can use multiple factors for the authentication context. In this case, you would still want to use location-based authentication, but you also want to ensure that supervisors cannot log in from geographically dispersed locations at or near the same time. Rule-based authentication will allow you to configure multiple context-based factors.

You should not change the supervisors from time-based authentication to rule-based authentication. Time-based authentication is used to control the times that users are allowed to log in. According to the scenario, the supervisors are using location-based authentication, not time-based authentication.

You should not change the supervisors from location-based authentication to frequency-based authentication. Frequency-based authentication allows the configured number of logins within a certain time period. You do not want to limit the supervisor accounts to frequency-based authentication. If their equipment or connection fails, they may have to log in frequently to reconnect to their session. You still want the supervisors to have location-based authentication, but you want to include other factors, such as location and frequency together, which would require changing to rule-based authentication.

You should not change the supervisors from time-based authentication to frequency-based authentication. The supervisors are not currently using time-based authentication.

For the CySA+ exam, you need to understand the security issues associated with the following context-based authentication types:

- Time - With this authentication, users are only allowed to log in during set times. This may cause problems if a user needs to work outside their normal shift time.
- Location - With this authentication, users are only allowed to log in from certain locations, usually based on geo-location statistics or IP address. This may cause problems if a user needs to work from a different location.
- Frequency - With this authentication, users are limited with the number of logins that can occur during a certain time period, such as a maximum of two logins within an hour. This may cause problems if a user is having trouble maintaining a connection, thereby requiring that they login multiple times within the same time period.
- Behavioral - With this authentication, user behavior is based on behavior patterns, such as keystroke dynamics, mouse movements, gesture and touch, and motion patterns. This may cause problems if user behaviors change or cannot be replicated, such as the user breaking their hand and changing to a one-handed typing style.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Moving Beyond 2-Factor Authentication With 'Context', http://www.darkreading.com/endpoint/authentication/moving-beyond-2-factor-authentication-with-context/a/d-id/1317911

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #95 of 200

Question ID: 1299777

You responded to a security incident and engaged in a digital forensic investigation. You need to take steps to ensure that the hard drive contents can be presented in court and deemed to be unchanged from the moment you obtained it as evidence. What type of tool do you need to provide this assurance?

- ✗ **A)** Imaging utility
- ✗ **B)** Cryptography tool
- ✓ **C)** Hashing utility
- ✗ **D)** Analysis utility

Explanation

Hashing utilities use hashing algorithms to create a value that can be used later to verify the information is unchanged. The two most common algorithms used are Message Digest 5 (MD5) and Secure Hashing Algorithm (SHA).

One of the tasks that you will be performing is to make copies of storage devices. To do this you need a disk imaging tool, but this tool cannot ensure integrity of the drive.

Analysis utilities are used to analyze the drive, which should not be done on the original copy. These tools are not used to ensure that the hard drive contents can be presented in court and deemed to be unchanged.

Cryptography tools are used when the investigator encounters encrypted evidence, which is becoming more common. Some of these tools can not only attempt to decrypt the most common types of encryption such as BitLocker, BitLocker to go, PGP and TrueCrypt but they may also be able to locate decryption keys from RAM dumps and hibernation files.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

10 Tools to Verify File Integrity Using MD5 and SHA1 Hashes, https://www.raymond.cc/blog/7-tools-verify-file-integrity-using-md5-sha1-hashes/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

Question #96 of 200

Question ID: 1299642

Which of the following is NOT a measure typically taken on a sheep dip system?

- ✗ **A)** The installation of one or more antivirus programs
- ✗ **B)** The installation of port monitors

✓ **C)** The installation of a vulnerability scanner

✗ **D)** The installation of network monitors

Explanation

Sheep dip computers are NOT used to perform vulnerability scanning. A sheep dip computer is a system that has been isolated from the other systems and is used for analyzing suspect files and messages for malware

Among the measures taken on a sheep dip system are:

- The installation of port monitors to discover ports used by the malware
- The installation of file monitors to discover what changes may be made to files
- The installation of network monitors to identify what communications the malware may attempt
- The installation of one or more antivirus programs to perform malware analysis

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

What is a sheep-dip?, http://sheepdip.sourceforge.net/Definition.php

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #97 of 200

Question ID: 1299714

You are performing a manual review of the logs that have been collected by the syslog server. You find the following entry:

```
*May 1 23:02:27.143: %SEC-6-IPACCESSLOGP: list ACL-IPv4-E0/0-IN permitted tcp 192.168.1.3(1026) ->
192.168.2.1(80), 1 packet
```

What is the source IP address and port number shown in the entry?

✗ **A)** 192.168.2.1 and 80

✓ **B)** 192.168.1.3 and 1026

✗ **C)** 192.168.1.3 and 80

✗ **D)** 192.18.2.1 and 1026

Explanation

The source IP address is 192.168.1.3, and the source port number is 1026. Below are the meanings of each part of the entry:

Time /day `*May 1 23:02:27.143`
Facility `%SEC` (security)
Severity `6`

Informational: Informational messages

Source `IPACCESSLOGP:  list ACL-IPv4-E0/0-IN` (name of access list)

Action `permitted`

From `192.168.1.3  port 1026`

To `192.168.2.1  port 80`

Amount `1 packet`

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

The Ins and Outs of System Logging Using Syslog,

https://www.sans.org/reading-room/whitepapers/logging/ins-outs-system-logging-syslog-1168

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #98 of 200

Question ID: 1299739

Which of the following incident response plan stakeholders create newsletters and other educational materials to be used in employee response training?

- ✗ **A)** Law enforcement
- ✗ **B)** Technical
- ✓ **C)** Marketing
- ✗ **D)** Management

Explanation

Marketing can be involved in the following activities in support of the incident response plan:

- Create newsletters and other educational materials to be used in employee response training.
- Coordinate with the legal team to prepare media responses and internal communications regarding incidents before they occur.

The technical role, which consists of the IT and security teams, will be to recognize, identify, and react to incidents, and to provide support in analyzing those incidents once they occur. They will provide the manpower, skills, and knowledge to act as first responders and to remediate all issues found. In smaller organizations the role of first responder may be outsourced to a third party provider, in which case the IT and security teams would coordinate with the first responder to implement the incident response plan.

The role of law enforcement is to assist the investigation, and in some cases to take over the investigation when a crime has been committed.

Management's role in incident response can be defined as:

- Communicate the importance of the incident response plan to all parts of the organization.
- Create agreements detailing the authority of the IR team to take over business systems if necessary.
- Create decision systems for determining when key systems must be removed from the network.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Incident Response: Communication is Key, http://www.securitymagazine.com/articles/78810-incident-response-communication-is-key-1

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #99 of 200

Question ID: 1299621

You run a vulnerability scan and receive the scanning report. You want to address the four vulnerabilities with the CVSS Base Score as shown below:

- Vulnerability A - 1.7
- Vulnerability B - 9.4
- Vulnerability C - 8.2
- Vulnerability D - 5.3

When you analyze the vulnerabilities, you discover that Vulnerabilities A and C are easily addressed with minimal effort. Vulnerability B requires extensive effort, and Vulnerability D requires a medium amount of effort.

Which vulnerability should you address first?

✗ **A)** D

✓ **B)** C

✗ **C)** A

✗ **D)** B

Explanation

You should first address Vulnerability C because, of the two options that will take minimal effort, Vulnerability C has the highest CVSS Base Score.

You should not address Vulnerability A first because it has a low CVSS Base Score. You should not address Vulnerability B first because it will require extensive effort. You should not address Vulnerability D first because it does not have the highest CVSS Base Score and it will require medium effort.

When assessing which vulnerabilities to address, you should attempt to address the vulnerabilities with the highest Common Vulnerability Scoring System (CVSS). However, you should also consider the amount of effort it takes to mitigate the vulnerability.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

CVSS 2.0 Guide, https://www.first.org/cvss/v2/guide

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

---

Question #100 of 200

Question ID: 1299766

A user is complaining about the performance of his device. You investigate and discover that an application that the user downloaded and installed is using more and more memory as you monitor its use of memory. There appears to be no network activity while this is occurring. Which of the following is most likely the source of this issue?

- ✓ **A)** memory overflow
- ✗ **B)** SYN flood
- ✗ **C)** buffer overflow
- ✗ **D)** DoS attack

Explanation

This is most likely a memory overflow caused by the application that is being monitored. Memory overflows occur when an application uses more memory than the operating system has assigned to it. In some cases, it simply causes the system to run slowly as the application uses more and more memory. The best course of action is to remove the application or obtain an update to the application that prevents the application from overflowing the memory. If it is malware, then the best course of action is to scan the device for malware. Going forward, you should keep all anti-malware up to date and ensure that users are trained in safe practices.

This would not be a SYN flood. SYN flood attacks would have a symptom of network usage, but the scenario states that network usage is zero. A SYN flood attack sends thousands of packets to the target with the SYN flag on. The target answers with SYN/ACK packets and reserves memory for the response, but the responses never come, and eventually the target runs out of memory. You should implement a stateful firewall at the perimeter. This measure can help to prevent SYN flood attacks.

This would not be a buffer overflow. A buffer overflow occurs when the system receives input that is larger than the memory reserved for that input. A buffer overflow would indicate some type of network usage and that usage is zero. A buffer overflow attack is prevented by ensuring that all web applications perform proper input validation.

This is not a DoS attack. All DoS attacks generate network usage, but that usage is zero in the scenario. If these attacks occur, you should locate the source of the attack and block the source at the firewall.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

What is Memory Leak? How Can We Avoid?, https://www.geeksforgeeks.org/what-is-memory-leak-how-can-we-avoid/

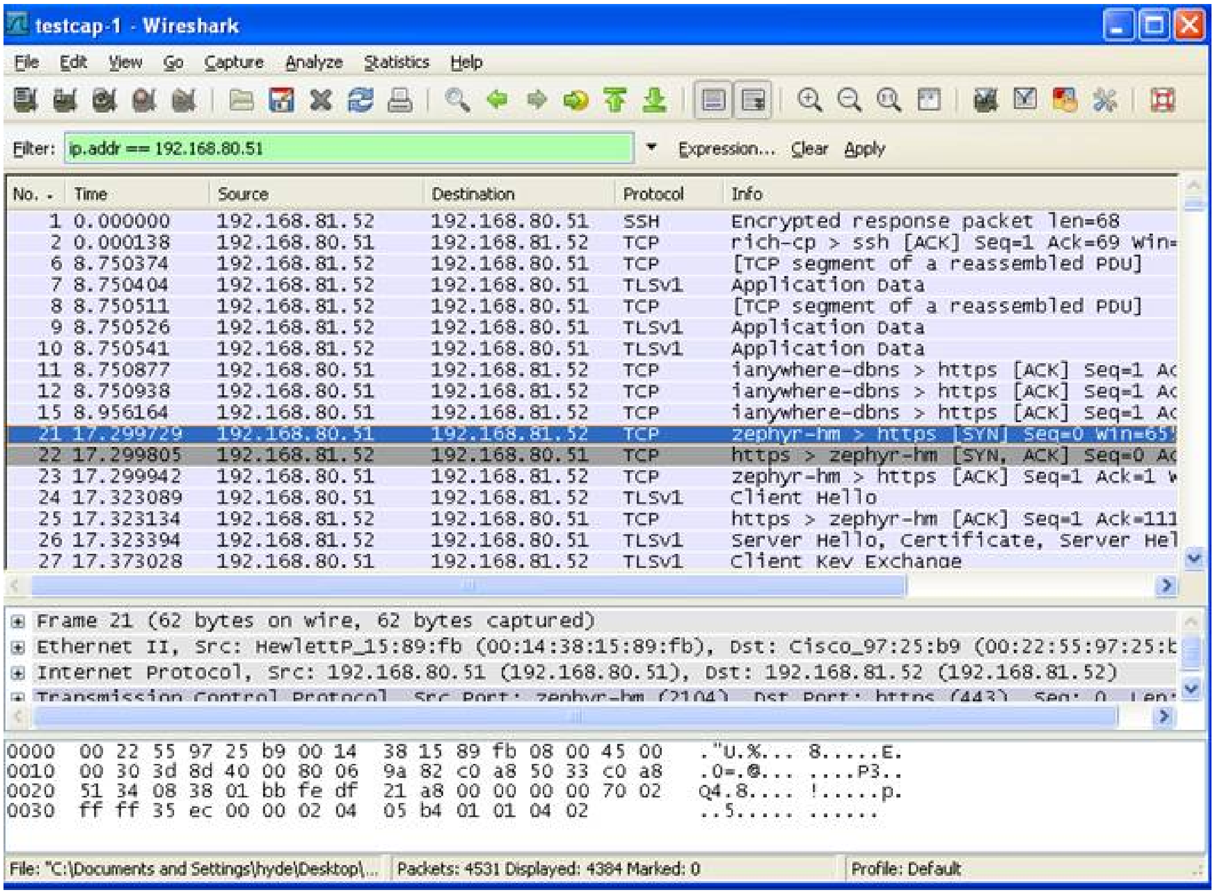
CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

---

Question #101 of 200

Question ID: 1299690

You are trying to troubleshoot an issue by using a packet capture tool. Your assistant is observing and asks you to show him a TCP handshake in the exhibit.



Filter: ip.addr == 192.168.80.51

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.81.52	192.168.80.51	SSH	Encrypted response packet len=68
2	0.000138	192.168.80.51	192.168.81.52	TCP	rich-cp > ssh [ACK] Seq=1 Ack=69 Win=
6	8.750374	192.168.81.52	192.168.80.51	TCP	[TCP segment of a reassembled PDU]
7	8.750404	192.168.81.52	192.168.80.51	TLSv1	Application Data
8	8.750511	192.168.81.52	192.168.80.51	TCP	[TCP segment of a reassembled PDU]
9	8.750526	192.168.81.52	192.168.80.51	TLSv1	Application Data
10	8.750541	192.168.81.52	192.168.80.51	TLSv1	Application Data
11	8.750877	192.168.80.51	192.168.81.52	TCP	ianywhere-dbns > https [ACK] Seq=1 Ac
12	8.750938	192.168.80.51	192.168.81.52	TCP	ianywhere-dbns > https [ACK] Seq=1 Ac
15	8.956164	192.168.80.51	192.168.81.52	TCP	ianywhere-dbns > https [ACK] Seq=1 Ac
21	17.299729	192.168.80.51	192.168.81.52	TCP	zephyr-hm > https [SYN] Seq=0 Win=65
22	17.299805	192.168.81.52	192.168.80.51	TCP	https > zephyr-hm [SYN, ACK] Seq=0 Ac
23	17.299942	192.168.80.51	192.168.81.52	TCP	zephyr-hm > https [ACK] Seq=1 Ack=1 W
24	17.323089	192.168.80.51	192.168.81.52	TLSv1	Client Hello
25	17.323134	192.168.81.52	192.168.80.51	TCP	https > zephyr-hm [ACK] Seq=1 Ack=111
26	17.323394	192.168.81.52	192.168.80.51	TLSv1	Server Hello, Certificate, Server Hel
27	17.373028	192.168.80.51	192.168.81.52	TLSv1	Client Key Exchange

```
⊞ Frame 21 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: HewlettP_15:89:fb (00:14:38:15:89:fb), Dst: Cisco_97:25:b9 (00:22:55:97:25:b
⊞ Internet Protocol, Src: 192.168.80.51 (192.168.80.51), Dst: 192.168.81.52 (192.168.81.52)
⊞ Transmission Control Protocol, Src Port: zephyr-hm (2104), Dst Port: https (443), Seq: 0, Len:
```

```
0000  00 22 55 97 25 b9 00 14  38 15 89 fb 08 00 45 00   ."U.%... 8.....E.
0010  00 30 3d 8d 40 00 80 06  9a 82 c0 a8 50 33 c0 a8   .0=.@... ....P3..
0020  51 34 08 38 01 bb fe df  21 a8 00 00 00 00 70 02   Q4.8.... !.....p.
0030  ff ff 35 ec 00 00 02 04  05 b4 01 01 04 02         ..5..... ......
```

File: "C:\Documents and Settings\hyde\Desktop\... | Packets: 4531 Displayed: 4384 Marked: 0 | Profile: Default

Which packets in the capture display the entire sequence?

- ✓ **A)** Packets 21, 22, and 23
- ✗ **B)** Packets 11, 12, and 15
- ✗ **C)** Packets 26 and 27
- ✗ **D)** Packets 21, 22, and 25

Explanation

Packets 21, 22, and 23 show the TCP handshake. Looking in the `Info` column of the first section, you can see which flags are set in each packet that uses TCP. A complete sequence is done between the same two IP addresses and is completed before any other data transfer takes place.

The first packet, 21, is a SYN packet from 192.168.80.51 to 192.168.81.52 with the SYN flag set.

The second packet, 22, is a SYN/ACK packet from 192.168.81.52 to 192.168.80.51 with the SYN and ACK flags set.

The third packet, 23, is an ACK packet from 192.168.80.51 to 192.168.81.52 with the ACK flag set.

Packets 11, 12, and 15 are not a TCP handshake. These are acknowledgement packets sent from 192.198.80.51 to 192.168.81.52 for data sent in earlier packets.

Packets 21, 22, and 25 do not show a complete handshake. Although the third packet, 25, has the ACK flag set, the packet is an acknowledgment of the TLS hello packet (packet 24).

Packets 26 and 27 do not show a complete handshake. They are part of certificate key exchange.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

How to Use Wireshark to Capture, Filter, and Inspect Packets, http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #102 of 200

Question ID: 1299787

Recently, it has become increasingly hard to manage all the event and audit logs generated by devices and servers on your company's network. You need to deploy a solution that allows you to consolidate the logs for easier analysis. Which tool should you use?

- ✗ **A)** Sysinternals
- ✓ **B)** Splunk
- ✗ **C)** Nexpose
- ✗ **D)** MRTG

Explanation

You should use Splunk to consolidate the logs for easier analysis. Splunk is a security information and event management (SIEM) tool. Other SIEM products include ArcSight, QRadar, AlienVault, OSSIM, and Kiwi Syslog.

Nexpose is a vulnerability scanning tool. Other vulnerability scanning tools include Qualys, Nessus, OpenVAS, Nikto, and Microsoft Baseline Security Analyzer (MBSA).

Sysinternals is a tool technical that includes resources and utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.

MRTG is an analytical monitoring tool to monitor the traffic load on network links. Other monitoring tools include Nagios, SolarWinds, Cacti, and NetFlow Analyzer.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

What is Splunk and How Does It Work?, https://helgeklein.com/blog/2014/09/splunk-work/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #103 of 200

Question ID: 1299721

You have come up with a remediation for a vulnerability that was discovered on the most recent vulnerability scan of your company's file servers. You are unsure of the effects of the remediation. What should you do first?

- ✓ **A)** Deploy the remediation in a sandbox environment.
- ✗ **B)** Submit a change request to the change control board.
- ✗ **C)** Determine which file server is most critical, and deploy the remediation on that server.
- ✗ **D)** Determine which file server is least critical, and deploy the remediation on that server.

Explanation

You should deploy the remediation in a sandbox environment. This will allow you to test the remediation to see if it has any adverse effects on the file servers prior to deploying the remediation in the live environment.

You should not determine which file server is least or most critical and deploy the remediation on that server. Remediation should not be deployed until it has been tested and then submitted to the change control board.

You should not submit a change request to the change control board until the remediation (change) has been tested. Then you will be able to submit the test results with the change request.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, implement configuration changes to existing controls to improve security.

References:

3 Essential Steps for Your Vulnerability Remediation Process, https://resources.whitesourcesoftware.com/blog-whitesource/3-essential-steps-for-your-vulnerability-remediation-process

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 12: Implementing Controls to Improve Security

---

Question #104 of 200

Question ID: 1299797

Your assistant applied the following access list to a router interface:

```
ip access-list standard workstations
permit 172.16.2.88
deny 172.16.3.13
```

Which of the following statement is TRUE of the access list?

- ✗ **A)** The only device denied will be at 172.16.3.13.
- ✗ **B)** No devices will be allowed.
- ✗ **C)** The only device allowed will be at 172.16.2.88, and the only device denied will be at 172.16.3.13.
- ✓ **D)** The only device allowed will be at 172.16.2.88.

Explanation

The only device allowed will be at 172.16.2.88. Because all access lists end with an implied (hidden) "deny all" statement, only devices explicitly permitted by a `permit` statement are allowed. 172.16.2.88 is the only device allowed by such a `permit` statement.

Although 172.16.3.13 is denied explicitly, it is not the only device that will be denied. All devices except the one at 172.16.2.88 will be denied.

It is not true that the only device allowed will be 172.16.2.88 and the only device denied will be 172.16.3.13. The only device allowed will be 172.16.2.88, and all others will be denied.

It is not true that no devices will be allowed. The only device allowed will be 172.16.2.88, and all others will be denied.

Objective:
Compliance and Assessment

Sub-Objective:
Understand the importance of data privacy and protection.

References:

Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S, http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/sec-create-ip-apply.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 19: Data Privacy and Protection

Question #105 of 200

Question ID: 1299598

As part of your company's comprehensive vulnerability scanning policy, you decide to perform a passive vulnerability scan on one of your company's subnetworks. Which statement is true of this scan?

- ✗ **A)** It is limited to a particular operating system.
- ✗ **B)** It includes the appropriate permissions for the different data types.
- ✗ **C)** It allows a more in-depth analysis than other scan types.
- ✓ **D)** It impacts the hosts and network less than other scan types.

Explanation

A passive scan impacts the hosts and network less than other scan types.

To perform a more in-depth analysis than other scan types, you would perform an active scan.

To include the appropriate permissions for the different data types, you should perform a credentialed scan. A non-credentialed scan does operate within the context of a user account. The appropriate permissions may be needed to be able to access all the data and applications on devices. Permissions and access to the entire hosts are provided with a credentialed scan.

Although not always possible, limiting a scan to a particular operating system can be done with an agent-based scan. With an agent-based scan, agents are installed on devices. These agents then send scan reports back to a central agent. In a server-based scan, the scanner runs from a server that then scans all the devices. Agent-based scanning is considered better than server-based scanning because it has less impact on the network. But an agent-based scan usually has more of an impact on the device on which the agent is installed.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #106 of 200

Question ID: 1299724

During a data classification meeting, someone mentions a type of data covered by PCI-DSS. What type of data is this?

- ✗ **A)** PHI
- ✗ **B)** intellectual property
- ✗ **C)** corporate confidential
- ✓ **D)** credit card data

Explanation

The Payment Card Industry Data Security Standard (PCI DSS) affects any organizations that handle cardholder information for the major credit card companies. The latest version of the standard is 3.0. To prove compliance with the standard, an organization must be reviewed annually.

Personal Health Information (PHI) is the medical records of individuals and must be protected in specific ways as prescribed by the regulations contained in the Health Insurance Portability and Accountability Act of 1996

Intellectual property is a tangible or intangible asset to which the owner has exclusive rights. Intellectual property law is a group of laws that recognizes exclusive rights for creations of the mind. This includes books and music.

Corporate confidential data includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

PCI Security, https://www.pcisecuritystandards.org/pci_security/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #107 of 200

Question ID: 1299573

A security service to which you subscribe just announced that a new threat exists for which no mitigation has been found. However, the application targeted by the threat is known. What would be the best description of this threat?

- ✗ **A)** unknown
- ✗ **B)** known
- ✓ **C)** known unknown
- ✗ **D)** unknown known

Explanation

When the existence of a threat is known, but no mitigation has been developed, it is called a *known unknown* threat. The best approaches to these types of threat are to use tools that identify attacks by finding suspicious network behavior, rather than identifying the signatures of known attacks.

A known threat is one that is understood and for which mitigations exist.

An unknown threat is one that has not been publicized or identified, and for which no mitigations exist.

In cyber threat classification, there is no term such as "unknown known".

Objective:
Threat and Vulnerability Management

Sub-Objective:
Explain the importance of threat data and intelligence.

References:

IT security admins, get to know your known unknowns, https://www.csoonline.com/article/2630150/it-security-admins--get-to-know-your-known-unknowns.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 1: Threat Data and Intelligence

---

Question #108 of 200

Question ID: 1299618

Bob is analyzing the results of a vulnerability scan. He examines a vulnerability detected on one of his servers that has a CVSS breakdown as follows:

CVSS2#AV:A/AC:H/Au:M/C:N/I:C/A:N

Which one of the following statements is TRUE about this vulnerability?

✗ **A)** Exploiting this vulnerability requires one instance of authentication.

✓ **B)** Exploiting this vulnerability would result in total compromise of system integrity.

✗ **C)** Exploiting this vulnerability would result in total information disclosure.

✗ **D)** Exploiting this vulnerability would result in total shutdown of the affected resource.

Explanation

Exploiting this vulnerability would result in total compromise of system integrity because the Integrity (I) metric has a value of C, which stands for Complete. The I metric describes the type of data alteration that might occur and has three possible values:

- N - stands for None and means there is no integrity impact
- P - stands for Partial and means some information modification would occur
- C - stands for Complete and means all information on the system could be compromised

For this metric, N is the best ranking.

Exploiting this vulnerability would NOT result in total shutdown of the affected resource because the Availability (A) metric has a value of N, which stands for None. The Availability (A) metric describes the disruption that might occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no availability impact
- P - stands for Partial and means system performance is degraded
- C - stands for Complete and means the system is completely shut down

For this metric, N is the best ranking.

Exploiting this vulnerability would NOT result in total information disclosure because the Confidentiality (C) metric has a value of N, which stands for None. The C metric describes the information disclosure that may occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no confidentiality impact
- P - stands for Partial and means some access to information would occur
- C - stands for Complete and means all information on the system could be compromised

For this metric, N is the best ranking.

Exploiting this vulnerability does NOT require one instance of authentication because the Authentication (Au) metric has a value of M, which stands for Multiple. The Au metric describes the authentication an attacker would need to get through to exploit the vulnerability. It has three possible values:

- M - stands for Multiple and means the attacker would need to get through two or more authentication mechanisms
- S - stands for Single and means the attacker would need to get through one authentication mechanism
- N - stands for None and means no authentication mechanisms are in place to stop the exploitation of the vulnerability

For this metric, M is the best ranking.

The Access Complexity (AC) metric describes the difficulty of exploiting the vulnerability. It has three possible values:

- H - stands for High and means the vulnerability requires special conditions that are hard to find
- M - stands for Medium and means the vulnerability requires somewhat special conditions
- L - stands for Low and means the vulnerability does not require special conditions

For this metric, H is the best ranking.

The Access Vector (AV) metric describes how the attacker would exploit the vulnerability. It has three possible values:

- L - stands for Local and means the attacker must have physical or logical access to the affected system.
- A - stands for Adjacent network and means the attacker must be on the local network
- N - stands for Network and means the attacker can cause the vulnerability from any network

For this metric, L is the best ranking.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

CVSS 2.0 Guide, https://www.first.org/cvss/v2/guide

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

---

Question #109 of 200

Question ID: 1299793

Which of the following can be used as an IDS on a Unix computer?

✗ **A)** ModSecurity

- ✓ **B)** Bro
- ✗ **C)** Nessus
- ✗ **D)** Qualys

Explanation

Bro can be used as an intrusion detection system (IDS) on a Unix computer. It can also be used as an intrusion prevention system (IPS), or implemented as a host IDS (HIDS) or host IPS (HIPS).

ModSecurity is a Web application firewall (WAF). Qualys and Nessus are vulnerability scanning tools.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

The Bro Network Security Monitor, https://www.bro.org/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #110 of 200

Question ID: 1299808

You are your company's security analyst. In the past year, your organization has endured more frequent phishing attacks. Management decided to deploy the following controls to help prevent these attacks:

- Spam filters that detect viruses, blank senders, and other malicious email
- Anti-virus applications on all computers with automatic updates
- Web filters that block malicious websites

After performing vulnerability scan and penetration testing, you discover that employees are still falling victim to phishing attacks. Which of the following should you deploy as compensating controls for this problem? (Choose all that apply.)

- ✗ **A)** Deploy an IPS between the internal network and the Internet.
- ✓ **B)** Deploy security awareness training for all users.
- ✗ **C)** Deploy an IDS between the internal network and the Internet.
- ✗ **D)** Implement a new password policy forcing users to change their passwords every 60 days.
- ✓ **E)** Implement a new security policy regarding clicking links in email messages.
- ✗ **F)** Implement a new account lockout policy that will lockout accounts after three invalid attempts.

Explanation

You should deploy the following as compensating controls to protect against phishing attacks:

- Implement a new security policy regarding clicking links in email messages.

- Deploy security awareness training for all users.

Both of these measures should help compensate for phishing attacks by providing users on guidance when they receive links in email messages.

Deploying an intrusion prevention system (IPS) between the internal network and the Internet will only protect against certain attacks. Phishing attacks are sent via email and are not detected by IPSs. A phishing attack occurs when an email is sent with a link that redirects a user from a seemingly legitimate website to a malicious website.

Deploying an intrusion detection system (IDS) between the internal network and the Internet will only detect certain attacks. It cannot detect phishing attacks because phishing attacks are sent via email and are not detected by IDSs.

Implementing a new password policy forcing users to change their passwords every 60 days or changing the account lockout policy to lock accounts after three invalid attempts both help prevent password attacks, not phishing attacks.

Compensating controls substitute for a primary access control, and mainly act as mitigations to risks. In this case, the spam filters, anti-virus applications, and Web files are the primary preventive controls for phishing attacks. However, they do not prevent all of these attacks, so you must deploy compensating controls, such as policies and training.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Phishing Attack Prevention: How to Identify & Avoid Phishing Scams, https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

---

Question #111 of 200

Question ID: 1299802

As a security analyst for your company, you are responsible for helping to analyze risks. After completing this process, you need to document the amount of risk your organization is willing to tolerate in their computing environment. Which term is used to describe this risk amount?

- ✗ **A)** Risk analysis
- ✗ **B)** Quantitative risk
- ✗ **C)** Qualitative risk
- ✓ **D)** Risk appetite

Explanation

Risk appetite is the term used for the amount of risk an organization is willing to tolerate in their computing environment.

Risk analysis is the process of determining the risks that your company has. Quantitative and qualitative risk analyses are two risk analysis types that can be used.

Objective:
Compliance and Assessment

Sub-Objective:
Given a scenario, apply security concepts in support of organizational risk mitigation.

References:

Understanding Risk Appetite, https://erm.ncsu.edu/library/article/understanding-risk-appetite

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 20: Supporting Risk Mitigation

---

Question #112 of 200

Question ID: 1299593

After completing a vulnerability scan, you determine that you need to remediate all your company's database servers. What should you do first?

- ✗ **A)** Deploy the remediation on the most critical database server.
- ✗ **B)** Deploy the remediation during the scheduled maintenance window on all the database servers.
- ✗ **C)** Deploy the remediation on the least critical database server.
- ✓ **D)** Deploy the remediation in a sandbox environment.

Explanation

First you should deploy the remediation in a sandbox environment. This will allow you to test the effects of the remediation to ensure that the servers will be able to function properly after deployment. If the deployment causes issues in the sandbox, you will not deploy the remediation to the database servers.

You should not deploy the remediation on the least or more critical database server until after the remediation has been tested in a sandbox.

You should not deploy the remediation during the scheduled maintenance window on all the database servers. While you should deploy remediation during the scheduled maintenance window, you should not do so until after it has been tested. In addition, most companies will deploy the remediation on a single device at a time.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #113 of 200

Question ID: 1299698

Last week, one of the tools you use created a number of false positives when you stayed late to download patch files from a vendor site. What type of analysis caused these false positives?

- ✗ **A)** NetFlow analysis
- ✗ **B)** Wireless analysis
- ✓ **C)** Anomaly analysis
- ✗ **D)** Trend analysis

Explanation

Anomaly analysis focuses on identifying something that is unusual or abnormal. This type of analysis is typically done by IDS or IPS system. These types of systems can generate false positives when activity occurs that is out of the ordinary such as working late and generating traffic at unusual times.

It was not NetFlow analysis that caused the false positives. NetFlow is a technology developed by Cisco, and since supported by all major vendors, that can be used to collect and subsequently export IP traffic accounting information. The traffic information is exported using UDP packets to a NetFlow analyzer, which can organize the information in useful ways. It exports records of individual one-way transmissions called flows.

It was not wireless analysis that caused the false positives. False positives are generated by IDS or IPS systems or antimalware products, not by wireless sniffers.

It was not trend analysis that caused the false positives. Trend analysis focuses on the long term direction in the increase or decrease in a particular type of traffic. Trend analysis does not have false positives because it is analyzing trends.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Network Anomaly Detection: The Essential Antimalware Tool, http://searchsecurity.techtarget.com/tip/Network-anomaly-detection-The-essential-antimalware-tool

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #114 of 200

Question ID: 1299758

After several issues were created by using a production workstation to process a forensic investigation, the company decided to build a dedicated forensic workstation. Which of the following does SANS NOT recommend as a requirement for that workstation?

✗ **A)** The system must be able to identify deleted files.

✓ **B)** The system must support wireless connectivity.

✗ **C)** The system must have the ability to validate image and file integrity.

✗ **D)** The system must support IDE.

Explanation

While it is a requirement that the system have network connectivity, it does not have to be wireless connectivity.

The SAN institute lists the following requirements of a forensic workstation in the document "Building a Low Cost Forensics Workstation". They include:

- The system must support IDE.
- The system must support SCSI.
- The system must have network connectivity.
- The system must support hardware-based drive duplication.
- The system must support remote- and network-based drive duplication.
- The system must support duplication and analysis of these common file system types:
    - NTFS
    - FAT16/32
    - Solaris UFS
    - BSD UFS
    - EXT2 (Linux)
    - EXT3 (Linux)
    - HFS & HFS+ (Macintosh)
    - Swap
    - Solaris
    - BSD
    - Linux
- The system must have the ability to validate image and file integrity.
- The system must be able to identify dates and times that files have been modified, accessed and created.
- The system must have the ability to create file system activity timelines.
- The system must be able to identify deleted files.
- The system must be able to analyze allocated drive space.
- The system must be able to isolate and analyze unallocated drive space.
- The system must allow the investigator to directly associate disk images and evidence to a case.
- The system must allow the investigator to associate notes to cases and specific evidence.
- The system must support removable media for storage and transportation of evidence and disk images.
- Evidence collected by the system must be admissible in a court of law.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Building a Low Cost Forensics Workstation,https://www.sans.org/reading-room/whitepapers/incident/building-cost-forensics-workstation-895

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

Question #115 of 200

Question ID: 1299749

Today you received an email from a department head, who informs you that data located on the Sales server has been altered and is not in the state it was last week. Upon investigation, you find that an attack on the server occurred last week and the team knew of the attack. Which part of determining the scope of the attack was NOT done?

- ✗ **A)** economic impact assessment
- ✓ **B)** verifying data integrity
- ✗ **C)** determining downtime
- ✗ **D)** estimating recovery time

Explanation

Assessing data integrity is part of determining the scope of an attack. Data integrity refers to the correctness, completeness, and soundness of the data. One of the goals of integrity services is to protect the integrity of data, or at least to provide a means of discovering when data has been corrupted or changed without authorization. Because data does not move from its storage location in a data integrity attack, one security challenge is that the effects of the attack may not be detected for years, until there is a reason to question the data.

Determining the scope of an attack is an important step required to prioritize responses to attacks. Scope includes the following factors:

- Downtime - refers to the amount of time access to resource were interrupted
- Recovery time - refers to the amount of time taken to recover from the incident
- Data integrity - refers to the amount of data corrupted or altered during the incident
- Economic - the cost of the incident to the organization
- System process criticality - refers to the criticality of the system involved

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Defining the Scope, http://catalogue.pearsoned.co.uk/samplechapter/0130462233.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

Question #116 of 200

Question ID: 1299725

Your organization's reputation is staked on a book it publishes yearly. When you performing data classification, how should you classify this book and its contents?

- ✗ **A)** PHI
- ✓ **B)** intellectual property
- ✗ **C)** corporate confidential
- ✗ **D)** personally identifiable information

Explanation

Intellectual property is a tangible or intangible asset to which the owner has exclusive rights. Intellectual property law is a group of laws that recognizes exclusive rights for creations of the mind. This includes books and music.

Personally identifiable information (PII) is any piece of data that can be used alone or with other information to identify a single person.

Personal Health Information (PHI) is the medical records of individuals and must be protected in specific ways as prescribed by the regulations contained in the Health Insurance Portability and Accountability Act of 1996.

Corporate confidential data includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred. The book contains corporate data, but it cannot be considered confidential if it is released into the public realm every year.

You need to ensure that you understand the factors contributing to data criticality. Most often data criticality is determined by the type of data, including:

- Personally identifiable information (PII)
- Personal health information (PHI)
- Special protected information (SPI)
- High value assets
- Financial information
- Intellectual property
- Corporate information

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

What is Intellectual Property?, http://www.wipo.int/about-ip/en/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

Question #117 of 200

Question ID: 1299661

You have discovered an application vulnerability on a computer. The application is secure if the user exercises certain procedures in a certain way. It is not possible to replace the application at this time or remove the vulnerability. The use of the application is mission critical. Which of the following would be a compensating control?

- ✓ **A)** Provide special training to the users
- ✗ **B)** Ensure that backups are performed regularly
- ✗ **C)** Scan for malware weekly
- ✗ **D)** Configure the computer to perform automatic updates

Explanation

Training the users to exercise certain procedures in a certain way will not eliminate the vulnerability, but it will make it less likely, which is the definition of a compensating (or compensatory) control.

While all of the other options are certainly good security measures to take, they do nothing to reduce the vulnerability described. For that reason, they are not compensating controls for this vulnerability.

Ensuring that backups are performed regularly would be a compensating control for the possibility of the hard drive dying.

Configuring the computer to perform automatic updates would be a compensating control for the possibility of new operating system attacks.

Scanning for malware weekly would be a compensating control for the possibility of malware attacks.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

Compensating Control (Alternative Control), http://whatis.techtarget.com/definition/compensating-control

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

Question #118 of 200

Question ID: 1299722

After running a vulnerability scan on your network, you analyze the vulnerabilities that were identified. You notice that a server in the accounting department has several vulnerabilities listed. You need to obtain information on the applications and services installed on the server. Which of the following is most likely to contain the information you need?

- ✗ **A)** SIEM
- ✗ **B)** SCAP
- ✓ **C)** Configuration management system

✗ **D)** Change management system

Explanation

The configuration management system is most likely to contain the information you need. A configuration management system identifies the components of a network and their properties, including applications installed, services running, and so on. Organizations can determine the depth of information stored in the configuration management system.

A change management system is responsible for managing changes to components of a network. The change management system ensures that changes are analyzed, approved, and deployed in a controlled process.

Security information and event management (SIEM) provides a centralized method of management information and events regarding the devices on your network, including logs and other security-related documentation.

Security Content Automation Protocol (SCAP) allows an organization to use automated vulnerability management and security policy compliance metrics.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, implement configuration changes to existing controls to improve security.

References:

What is Configuration Management and Why is it Important?, https://www.upguard.com/blog/5-configuration-management-boss

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 12: Implementing Controls to Improve Security

---

Question #119 of 200

Question ID: 1299675

Match the web site application code attack types on the left with the mitigations given on the right. Choose the mitigation that BEST applies to the attack.

{UCMS id=5742755248603136 type=Activity}

Explanation

The attacks and their mitigations should be matched in the following manner:

- Cross-site request forgery (CSRF) - Validate both the client and server side.
- Cross-site scripting (XSS) - Implement input validation.
- Session hijacking - Encrypt communications between the two parties.
- Malicious add-ons - Implement application white-listing.

It is important that you understand application attacks and how to prevent them.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

Cross-site Request Forgery (CSRF) Prevention Cheat Sheet, https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

How To: Prevent Cross-Site Scripting in ASP.NET, http://msdn.microsoft.com/en-us/library/ff649310.aspx

Session hijacking, http://searchsoftwarequality.techtarget.com/definition/session-hijacking

Application whitelisting: Is it the best way to beat malware?, http://www.techrepublic.com/blog/it-security/application-whitelisting-is-it-the-way-to-beat-malware/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

Question #120 of 200

Question ID: 1299655

As your company's security analyst, you help provide guidance on authentication. Currently your company implements two-factor, context-based authentication. Users provide their user names and passwords to the authentication system. Then the system also authenticates based on the device from which they log in.

Administrators are complaining because some users need to ability to log in from multiple devices that are not currently part of their profile. You need to recommend a solution while still ensuring maximum authentication security. Which of the following should you recommend?

- ✗ **A)** Configure an exception for the users needing this ability.
- ✗ **B)** Implement rule-based authentication for the users needing this ability.
- ✗ **C)** Disable context-based authentication for the users needing this ability.
- ✓ **D)** Implement a mechanism that issues a one-time password code from a security token for the users needing this ability.

Explanation

You should implement a mechanism that issues a one-time password code from a security token for those users needing this ability. When the one-time password code is authenticated, this will add the device from which the user is authenticating to the approved devices for that user.

You should not disable context-based authentication for the users needing this ability. This would not provide maximum authentication security.

You should not implement rule-based authentication for the users needing this ability. The current mechanism already provides location-based authentication. You just need to configure a method whereby users can easily add devices to the approved device list.

You should not configure an exception for the users needing this ability. Exceptions would prevent context-based policies from being applied to certain users. This would be the same as disabling context-based authentication for the users, which would not provide maximum authentication security.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Moving Beyond 2-Factor Authentication With 'Context', http://www.darkreading.com/endpoint/authentication/moving-beyond-2-factor-authentication-with-context/a/d-id/1317911

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #121 of 200

Question ID: 1299636

You are your organization's security analyst. Recently, you discovered that an attacker injected malicious code into a Web application on your organization's Web site. You discovered this attack by reviewing the log data on the Web servers. Which type of attack did your organization experience?

- ✗ **A)** path traversal
- ✓ **B)** cross-site scripting
- ✗ **C)** SQL injection
- ✗ **D)** buffer overflow

Explanation

Your organization experienced a cross-site scripting (XSS) attack. An XSS attack occurs when an attacker locates a vulnerability on a Web site that allows the attacker to inject malicious code into a Web application. A persistent XSS attack occurs when data provided to the Web application is first stored persistently on the server and later displayed to users without being encoded using HTML on the Web client. A non-persistent XSS attack occurs when data provided by a Web client is used immediately by server-side scripts to generate results for that user. XSS flaws occur every time an application takes user-supplied data and sends it to a Web browser without first confirming or encoding the data.

To locate XSS attacks, you should look for lines in the Web server log that contain JavaScript or other scripting languages that forward a user's session cookie to an external location or Web page.

A buffer overflow occurs when an invalid amount of input is written to the buffer area.

A SQL injection occurs when an attacker inputs actual database commands into the database input fields instead of the valid input. You should include input validation to prevent SQL injection attacks.

Path traversal occurs when the ../ characters are entered into the URL to traverse directories that are not supposed to be available from the Web.

Some possible countermeasures to input validation attacks include the following:

- Filter out all known malicious requests.

- Validate all information coming from the client, both at the client level and at the server level.
- Implement a security policy that includes parameter checking in all Web applications.

Another application issue that you need to understand is click-jacking. Click-jacking is a technique that is used to trick users into revealing confidential information or taking over the user's computer when clicking links.

Often you will need to determine the attack vector used. Reverse engineering is the best way to do this.

When designing a Web application, security should be one of the facets that you should always keep in mind. An application should be secure by design, by default, and by deployment. Secure by design means that the application is designed with security in mind. Secure by default means that the application defaults to being secure without changing application settings. Secure by deployment means that the environment into which the application is deployed is taken into consideration from a security standpoint.

For the CySA+ exam, you also need to understand exploits that will cause security issues with identity and access management:

- Impersonation - Attackers may try to impersonate a legitimate user to obtain access credentials. Identity proofing is mitigation for this type of attack.
- Man-in-the-middle (MITM) - This attack occurs when an attacker intercepts messages between two devices and eavesdrop on the communication. The attacker attempts to impersonate each party. Using one-time-passwords and mutual authentication are mitigations for this attack.
- Session hijack - This attack occurs when an attacker attempts to take over a session that is already occurring. Encryption is a mitigation for this attack.
- Rootkit - A rootkit is a set of software tools that allow an attacker to gain control of a device. The best mitigation is to remove all rootkits.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

References:

Cross-site Scripting, https://www.acunetix.com/websitesecurity/cross-site-scripting/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 7: Implementing Controls

---

Question #122 of 200

Question ID: 1299596

You are your company's security analyst. As part of your job duties, you must configure the company's vulnerability management solution to perform credentialed scans of certain servers. Which permissions should you assign the account used for the vulnerability scans?

- ✓ **A)** Read only
- ✗ **B)** Write only
- ✗ **C)** Modify
- ✗ **D)** Full control

Explanation

The account used for vulnerability scans should be assigned Read only permissions. Credentialed scans only require read-only access to target servers. You should follow the principle of least privilege and limit the access available to the scanner.

All of the other permissions grant access rights that are not necessary to perform the scans, and may result in security issues.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #123 of 200

Question ID: 1299579

You need to provide your company with a report regarding potential security-related software flaws. You need to use standardized names so that a security analyst contractor can understand the report. Which SCAP component should you use?

- ✗ **A)** CVSS
- ✓ **B)** CVE
- ✗ **C)** CCE
- ✗ **D)** CPE

Explanation

You should use the Common Vulnerabilities and Exposures (CVE), which provides standardized names for security-related software flaws.

Common Platform Enumeration (CPE) provides standard names for product names and versions. Common Configuration Enumeration (CCE) provides standard names for system configuration issues. Common Vulnerability Scoring System (CVSS) provides a standardized metric that measures and describes the severity of security-related software flaws.

Keep in mind that you may need to provide reports on identified vulnerabilities to different audiences. While technical staff may be able to read and comprehend the automatic reports generated by a vulnerability scanner, you may need to create an executive report for other non-technical staff that contains information that is more easily understood.

While having the vulnerability scanner deliver reports automatically delivery may be preferred, it is not the best solution. Understanding automated versus manual distribution issues will ensure that you, as the security analyst, can provide your audience with information they need and understand. Automatic distribution distributes the reports automatically through internal mechanisms, often via email. Manual distribution would require more effort on the security analyst to ensure that the appropriate individuals receive the correct report.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, utilize threat intelligence to support organizational security.

References:

SCAP Content Components, https://docs.bmc.com/docs/ServerAutomation/86/using/analyzing-system-compliance/scap-compliance-analysis/security-content-automation-protocol-overview/scap-content-components

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 2: Utilizing Threat Intelligence

Question #124 of 200

Question ID: 1299765

An organization recently suffered a data breach. When the issue was investigated, it was found that a disgruntled employee concealed product release dates within an image file he sent to someone else. What is this process called?

- ✗ **A)** double tagging
- ✓ **B)** steganography
- ✗ **C)** data exfiltration
- ✗ **D)** masquerading

Explanation

Steganography is the process of removing some the bits of information about a graphic and inserting data you want to hide in place of the missing graphic information. This swapping does not typically have a noticeable effect on the graphic, but allows the sender to hide data that can be extracted later by means of the same application used to insert it into the graphic. The best defense against steganography is to periodically scan PCs for questionable software. The presence of steganography software on any system should be prohibited unless it is specifically required for business purposes.

Although the end result of this incident is data exfiltration (sensitive data exiting the network), the encoding process itself is called steganography. Data exfiltration behavior can be discovered with data loss prevention (DLP) software if present. If it is not, data exfiltration may only be reported when it falls into the wrong hands. When it occurs, the best course of action is to identify the source of the disclosure if possible and then take disciplinary action. Going forward, a DLP solution should be deployed in your enterprise.

This is not double tagging. Double tagging is an attack that allows a malicious individual to access a VLAN for which they are not a member. Double-tagging attacks can be prevented by keeping the native VLAN of the trunk ports different from the user VLANs.

This is not masquerading. Masquerading is when a single public IP address is used by all interior devices when accessing the Internet. This is done by deploying Network Address Translation (NAT). It is called NAT because none of the devices will reveal their private IP address to the outside world.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Steganography: Hiding Data Within Data, http://www.garykessler.net/library/steganography.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

---

Question #125 of 200

Question ID: 1299813

After a recent audit, the third-party auditor recommended that your company increase its implementation of physical security controls. As the security analyst, management has asked you to recommend some physical controls. Which of the following should you suggest?

- ✓ **A)** guards, biometrics, CCTV, and perimeter fencing
- ✗ **B)** passwords, IDS, investigation procedures, and CCTV
- ✗ **C)** routers, auditing, biometrics, and perimeter fencing
- ✗ **D)** separation of duties, job rotation, encryption, and biometrics

Explanation

You should suggest guards, biometrics, CCTV, and perimeter fencing because all of these are physical controls. Physical controls protect facilities and personnel from physical access. Physical controls also include locks, badges, and mantraps.

Biometrics can also be considered a logical control. Passwords, encryption, routers, auditing, and IDSs are logical or technical controls. Logical or technical controls are software or hardware components that restrict access. Logical controls include smart cards, encryption, and data backups.

Investigation procedures, separation of duties, and job rotation are administrative controls. Administrative or managerial controls direct the organization's assets and personnel. Administrative controls include policies, procedures, separation of duties, job rotation, disaster plans, and security awareness training.

Security analysts must ensure that they provide the appropriate control selection based on criteria defined. In this scenario, the auditor specifically defined physical controls were needed. Controls based on the defined needs should be implemented to ensure that all aspects of access control are provided: administrative, logical, and physical.

Some organizations will have organizationally defined parameters that also need to be understood by security analysts. Analysts should obtain the organization's policies to ensure that all the parameters are documented prior to selecting the controls to implement.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Types of Controls, http://ishandbook.bsewall.com/risk/Assess/Risk/control_types.html

Question #126 of 200

Question ID: 1299574

Recently your network was attacked, and the attack had the following characteristics:

- It appeared to be directed at your organization specifically.
- It was carried out over a long period of time.
- It appeared to originate from multiple sources.
- The attack targeted specific assets.

The team is performing threat classification. Which of the following is the best description of this attack?

✗ **A)** passive

✗ **B)** known

✗ **C)** zero-day

✓ **D)** APT

Explanation

The attack described has all the elements of an advanced persistent threat (APT). An APT is a hacking process that targets a specific entity and is carried out over a long period of time. In most cases, the victim of an APT is a large corporation or government entity. The attacker is usually a group of organized individuals or a hostile government.

In an APT, the attackers have a pre-defined objective, such as a specific asset belonging to your organization (including smartcard credentials, control of social media logins, a database of PII, and so on). Once the objective is met, the attacks stop. APTs can often be detected by monitoring logs and network performance metrics.

A passive attack is one in which the attacker only captures information, but does not take any actions or send any data on the network. APT attacks are active attacks in which actions are taken by the attacker. However, APTs typically begin with passive reconnaissance.

A zero-day attack is one discovered in live environments for which no current fix or patch exists. An APT attack can incorporate a zero-day attack, but that would not be the best description in this case, as APTs involve ongoing attacks in multiple channels over a period of time.

A known threat is one for which mitigations are known. In this case, we do not know if the attack is known or unknown.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Explain the importance of threat data and intelligence.

References:

Advanced persistent threat (APT), http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 1: Threat Data and Intelligence

---

Question #127 of 200

Question ID: 1299678

The team has been assigned to perform host hardening of the servers in the sales domain. Which of the following activities would NOT be a part of this goal?

- ✓ **A)** Using encryption for all transmissions
- ✗ **B)** Updating security patches
- ✗ **C)** Closing all but required ports
- ✗ **D)** Removing unneeded applications

Explanation

While it is certainly recommended in scenarios where the transmission will be sensitive, using encryption for all transmissions is NOT considered part of host hardening. The tasks in host hardening include the following:

- Block unused ports/services
- Patch
- Set software and hardware components used to restrict access
- Control physical access
- Disable unused interfaces
- Remove unnecessary protocols
- Apply access control to resources
- Practice least privilege when assigning access
- Use strong passwords
- Disable unused accounts
- Install a host firewall and antimalware software

Objective:
Software and Systems Security

Sub-Objective:
Explain hardware assurance best practices.

References:

NIST SP 800-123: Guide to General Server Security, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 10: Hardware Best Practices

---

Question #128 of 200

Question ID: 1299624

After performing a vulnerability scan, you receive the scanning report. A CVSS vector is provided as part of this report. For one of the vulnerabilities, you need to determine which metric measured may be a concern. The CVSS vector for this vulnerability is:

CVSS2#AV:L/AC:H/Au:N/C:N/I:N/A:N

Which metric has a value that is undesirable?

- ✓ **A)** Au
- ✗ **B)** AC
- ✗ **C)** I
- ✗ **D)** AV

Explanation

The Authentication (Au) metric has a value that is undesirable. The Authentication (Au) metric describes the authentication an attacker would need to get through to exploit the vulnerability. It has three possible values:

- M - stands for Multiple and means the attacker would need to get through two or more authentication mechanisms
- S - stands for Single and means the attacker would need to get through one authentication mechanism
- N - stands for None and means no authentication mechanisms are in place to stop the exploitation of the vulnerability

For this metric, M is the best ranking.

The Access Complexity (AC) metric describes the difficulty of exploiting the vulnerability. It has three possible values:

- H - stands for High and means the vulnerability requires special conditions that are hard to find
- M - stands for Medium and means the vulnerability requires somewhat special conditions
- L - stands for Low and means the vulnerability does not require special conditions

For this metric, H is the best ranking.

The Access Vector (AV) describes how the attacker would exploit the vulnerability. It has three possible values:

- L - stands for Local and means the attacker must have physical or logical access to the affected system.
- A - stands for Adjacent network and means the attacker must be on the local network
- N - stands for Network and means the attacker can cause the vulnerability from any network

For this metric, L is the best ranking.

The Integrity (I) metric describes the type of data alteration that might occur. It has three possible values:

- N - stands for None and means there is no integrity impact
- P - stands for Partial and means some information modification would occur
- C - stands for Complete and means all information on the system could be compromised

For this metric, N is the best ranking.

The Confidentiality (C) metric describes the information disclosure that may occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no confidentiality impact
- P - stands for Partial and means some access to information would occur
- C - stands for Complete and means all information on the system could be compromised

For this metric, N is the best ranking.

The Availability (A) metric describes the disruption that might occur if the vulnerability is exploited. It has three possible values:

- N - stands for None and means there is no availability impact
- P - stands for Partial and means system performance is degraded
- C - stands for Complete and means the system is completely shut down

For this metric, N is the best ranking.

The CVSS vector will look something like:

CVSS2#AV:L/AC:H/Au:M/C:P/I:N/A:N

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

CVSS 2.0 Guide, https://www.first.org/cvss/v2/guide

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

Question #129 of 200

Question ID: 1299715

Recently an employee was fired after it was discovered that he was stealing from the company. He was able to keep the theft secret for quite some time because he was both the person responsible for accounts payable and accounts receivable. Which of the following is NOT a concept that could be put into practice to prevent this in the future?

✓ **A)** Succession planning

✗ **B)** Mandatory vacations

✗ **C)** Separation of duties

✗ **D)** Job rotation

Explanation

Succession planning could not prevent this type of incident from occurring. Succession planning should take place to ensure that individuals are groomed to take over key position before those positions need filing due to planned or unplanned vacancy. It will not stop or prevent fraud.

The concept of separation of duties prescribes that sensitive operations should be divided among multiple users so that no one user has the rights and access to carry out the operation alone. Having the same person responsible for accounts payable and receivable is the opposite of separation of duties.

Job rotation or cross training ensures that more than one person fulfills the job tasks of a single position within an organization. This strategy ensures that more than one person is capable of performing those tasks, providing redundancy. It is also an important tool in helping an organization to recognize when fraudulent activities have occurred.

Mandatory vacations, in which all users are required to take time off, allow another user to fill their position while gone. It enhances the opportunity to discover unusual activity while the primary employee is off premises.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Three Easy Fixes to Help Reduce Fraud, http://www.mlrpc.com/articles/three-easy-fixes-to-help-reduce-fraud/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #130 of 200

Question ID: 1299699

While observing a presentation of sniffers and network analysis, the presenter demonstrates a tool that displays the following counts for frame types captured:

```
Beacons  5483
Probe requests  320
Data  8952
<output omitted>
```

Given this information, what type of analysis is being performed?

- ✓ **A)** Wireless analysis
- ✗ **B)** Trend analysis
- ✗ **C)** Heuristic analysis
- ✗ **D)** NetFlow analysis

Explanation

Because beacon and probe request frames were captured, the output must display the results of wireless analysis. Beacon and probe request frames are only found in an 802.11 network.

The results are not NetFlow analysis. NetFlow is a technology developed by Cisco, and since supported by all major vendors, that can be used to collect and subsequently export IP traffic accounting information. The traffic information is exported using UDP packets to a NetFlow analyzer, which can organize the information in useful ways. It exports records of individual one-way transmissions called flows. The NetFlow results display the date, start time, duration, transport protocol, source and destination IP address/port number pairs, number of packets, bytes, and number of flows. While many graphical tools are available, a basic dump of a flow would resemble the following output:

```
Date  Start  D  TP  source  IP /port  dest IP/port  PKts  B  Flow
2016-09-01 00:00:00.459  0.000 UDP  192.168.0.1:24920  ->  192.168.0.1:22126  1  46  1
```

```
2016-09-01 00:00:00.363  0.000 UDP  192.168.0.1:22126 ->  127.0.0.1:24920  1  80  1
```

The results are not heuristic analysis. Heuristic analysis determines the susceptibility of a system towards a particular threat or risk using decision rules or weighing methods. It is often utilized by antivirus software to identify threats that cannot be discovered with signature analysis because the threat is either too new to have been analyzed (called a zero-day threat) or it is a multi-pronged attack, which is constructed in a way that existing signatures do not identify the threat.

The results are not trend analysis. Trend analysis focuses on the long term direction in the increase or decrease in a particular type of traffic. While this information might be used to perform trend analysis, it is not the best answer.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

802.11 frames: A starter guide to learn wireless sniffer traces, https://supportforums.cisco.com/document/52391/80211-frames-starter-guide-learn-wireless-sniffer-traces

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #131 of 200

Question ID: 1299803

To address recent issues in the parking lot, the company has installed a CCTV camera to monitor the lot. What type control is this?

- ✗ **A)** Corrective
- ✓ **B)** Detective
- ✗ **C)** Preventative
- ✗ **D)** Directive

Explanation

A camera is a detective control because it allows you to detect when an issue occurs.

It is not a preventative control. A preventative control is when one that stops something from occurring. Examples of preventive controls include locks, badges, biometric systems, encryption, intrusion prevention systems (IPSs), antivirus software, personnel security, security guards, passwords, and security awareness training.

It is not a directive control. Directive controls specify acceptable practice within an organization. The most popular directive control is an acceptable use policy (AUP) that lists proper (and often examples of improper) procedures and behaviors that personnel must follow.

It is not a corrective control. Corrective controls are in place to reduce the effect of an attack or other undesirable event. Using corrective controls fixes or restores the entity that is attacked. Examples of corrective controls include installing fire extinguishers, isolating or terminating a connection, implementing new firewall rules, and using server images to restore to a previous state.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Security Controls, https://www.sans.edu/cyber-research/security-laboratory/article/security-controls

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

---

Question #132 of 200

Question ID: 1299641

The organization has a web server that needs to be available to all traffic on the Internet. It needs to be placed where access to external traffic can occur without authentication, but external access to the internal LAN cannot. In which of the following should it be placed?

- ✗ **A)** LAN
- ✗ **B)** Extranet
- ✓ **C)** DMZ
- ✗ **D)** WAN

Explanation

The web server should be placed in a DMZ. A demilitarized zone (DMZ) is a network that is logically separate from the intranet, and where resources that will be accessed from the outside world are made available. The difference between an extranet and a DMZ is an extranet usually contains resources available only to certain entities from the outside world and access is secured with authentication, while the DMZ usually contains resources available to all from the outside world and makes it available without authentication.

A local area network (LAN) does not contain resources available to all from the outside world without authentication. The LAN is the private network that firewalls are designed to protect.

An extranet does not contain resources available to all from the outside world without authentication. An extranet contains resources available only to certain entities from the outside world, and that access is secured with authentication.

A wide area network (WAN) does not contain resources available to all from the outside world without authentication. A WAN represents a connection between two LANs and does not contain resources.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

DMZ Setup and Configuration Network security DMZ (demilitarized zone), https://searchsecurity.techtarget.com/definition/DMZ

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #133 of 200

Question ID: 1299673

A new version of a web application has been developed. The software development team is injecting invalid or unexpected input into the application to test how the application reacts. Which type of testing are they performing?

✓ **A)** Fuzzing

✗ **B)** Web app vulnerability scanning

✗ **C)** Using an interception proxy to crawl the application

✗ **D)** Static code analysis

Explanation

Fuzz testing, or fuzzing, involves injecting invalid or unexpected input (sometimes called faults) into an application to test how the application reacts. It is usually done with a software tool that automates the process.

Static code analysis is form of code review and testing that must occur throughout the entire application development life cycle. It is done without the code executing.

Web vulnerability scanners can operate in two ways, using synthetic transaction monitoring and real user monitoring. In synthetic transaction monitoring, preformed (synthetic) transactions are executed against the application in an automated fashion, and the behavior of the application is recorded. In real user monitoring the application, real user transactions are monitored while the web application is live.

An interception proxy is an application that stands between the web server and the client and passes all requests and response back and forth. While it does so, it analyzes the information to test the security of the web application. A web application proxy can also "crawl" the site and its application to discover the links and content contained.

All of the given options are security testing phases.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

How fuzz testing and tools can optimize testing processes, , http://www.computerweekly.com/feature/How-fuzz-testing-and-tools-can-optimise-testing-processes

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

Question #134 of 200

Question ID: 1299810

As a security analyst, you performed vulnerability assessment from inside and outside your organization's network. After the assessments were complete, you provided a report to management and made recommendations on the security controls that the company should implement. After you implemented the controls, management wants to verify that the controls were implemented properly. What should you do?

- ✗ **A)** Perform an audit to determine whether all the recommended controls have been implemented.
- ✗ **B)** Assess the current environment against security frameworks to identify missing controls.
- ✗ **C)** Perform another vulnerability assessment to assess the effectiveness of the current controls.
- ✓ **D)** Verify that the security controls' installation and configuration align with security frameworks.

Explanation

You should verify that the security controls' installation and configuration align with security frameworks. The purpose of security frameworks is to ensure that security controls are implemented properly. Both risk-based and prescriptive frameworks should be used and should be selected on the type of organization.

Assessing the current environment against security frameworks to identify missing controls would not assess whether the current controls were correctly implemented. It would only provide you with new controls that should be implemented.

Performing another vulnerability assessment would provide any vulnerabilities that still exist or new ones that have cropped up. It does not assess the current control implementation.

Performing an audit to determine that all the recommended controls have been implemented does not test the implementation and functionality of the controls. It just verifies that they exist.

Security analysts must ensure that control testing procedures are in place to verify the implementation and functionality of current security controls. If the security controls do not function as expected, you will not be protecting yourself against the vulnerabilities for which they are designed.

As part of control testing procedures, organizations should implement audits, evaluations, assessments, maturity models, and certification.

- Audits should be performed internally and by third parties to determine compliance with laws and regulations.
- Evaluations usually verify compliance by comparing the current state to checklists or frameworks.
- Assessments are usually more systematic that evaluations and measure against benchmarks.
- Certification is a formal process whereby a client's operations are assessed to determine if they align with requirements set by a standards organization. Certification usually occurs through third-party audits.
- Maturity models provide an assessment of the current security state against a backdrop of maturity and capability, with levels usually being reactive, compliant, proactive, and optimized. Reactive is the lowest maturity, and optimized is the highest maturity.

Objective:

Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Technical Guide to Information Security Testing and Assessment, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

Question #135 of 200

Question ID: 1299584

Which of the following rules of engagement includes a list of all devices that are included in the test as well as a description of all testing methodologies to be used?

- ✓ **A)** Scope
- ✗ **B)** Timing
- ✗ **C)** Authorization
- ✗ **D)** Exploitation

Explanation

The scope of the test incudes the timeline, but also includes a list of all devices that are included in the test as well as a description of all testing methodologies to be used.

The authorization part of the rules of engagement gives written approval by upper management to the tester to perform the test. Without this authorization, the tester could be liable for attempting to compromise the network.

The timing part of the rules of engagement establishes the dates and times of day the testing will occur.

The exploitation part of the rules of engagement establishes beforehand whether exploits will be attempted if vulnerable systems are found. This is intentionally included in some cases so the incident response plan can be tested.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

Pre-engagement, http://www.pentest-standard.org/index.php/Pre-engagement

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #136 of 200

Question ID: 1299572

You have several SQL servers that were recently brought down by a DDoS attack. The attack was never detected by your signature-based IPS. When you received support from your vendor, you were told that the attack used an approach that was never seen before. What type of attack did you suffer?

- ✗ **A)** passive
- ✓ **B)** zero-day
- ✗ **C)** APT
- ✗ **D)** known

Explanation

A zero-day attack is one discovered in live environments for which no current fix or patch exists, as in this case.

It is not a passive attack. A passive attack is one in which the attacker only captures information but does not take any actions or send any data on the network. A DDoS attack is not considered a passive attack.

It is not a known attack. A known attack is one that is understood and for which mitigations exist.

It is not an advanced persistent threat (APT). An APT is a hacking process that targets a specific entity and is carried out over a long period of time. In most cases, the victim of an APT is a large corporation or government entity. The attacker is usually a group of organized individuals or even a hostile government. The attackers have a pre-defined objective. Attacks of this type usually steal information rather than perform DDoS.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Explain the importance of threat data and intelligence.

References:

What is a Zero-Day Vulnerability?, http://www.pctools.com/security-news/zero-day-vulnerability/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 1: Threat Data and Intelligence

---

Question #137 of 200

Question ID: 1299799

The accounting team has asked for your advice concerning the handling of some sensitive data. They want to protect the information with cryptography when it is stored on a server. Which encryption algorithm would you suggest to be used for this?

- ✗ **A)** ECC
- ✗ **B)** RSA
- ✗ **C)** DSA
- ✓ **D)** AES

Explanation

Data at rest as in this case should be encrypted with a symmetric key algorithm. Of the options given, Advanced Encryption Standard (AES) is the ONLY symmetric key algorithm offered as an option. These algorithms use the same key to encrypt as to decrypt, are very fast, and are used on data stored on hard drives, thumb drives, or in any scenario where the key can easily be shared.

Other examples of symmetric algorithms include:

- Digital Encryption Standard (DES)
- Triple DES (3DES)
- Blowfish

Asymmetric algorithms use both a public key and a private or secret key. The public key is known by all parties, and the private key is known only by its owner. One of these keys encrypts the message, and the other decrypts the message. These are used for data in transit. Examples include:

- Rivest Shamir Adleman (RSA)
- Diffie-Helman
- Elliptic Curve Cryptography (ECC)
- ElGamal
- Digital Signature Algorithm (DSA)

Objective:
Compliance and Assessment

Sub-Objective:
Understand the importance of data privacy and protection.

References:

How symmetric and asymmetric encryption algorithms differ, http://searchsecurity.techtarget.com/answer/What-are-the-differences-between-symmetric-and-asymmetric-encryption-algorithms

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 19: Data Privacy and Protection

---

Question #138 of 200

Question ID: 1299795

Your assistant is trying to learn about access control lists (ACLs). He is compiling some notes about ACLs. Which of the following statements is NOT true of ACLS?

✗ **A)** The packet is compared with lines of the access list only until a match is made.

✓ **B)** The packet is compared to every line on the list, the "best" match is selected, and the specified action is taken.

✗ **C)** The packet is always compared with each line of the access list in sequential order.

✗ **D)** If a packet does not match the condition on any of the lines in the access list, the packet will be discarded.

Explanation

An ACL does NOT read all rules before making a decision. The packet is compared with lines of the access list only until a match is made. Once it matches the condition on a line of the access list, the packet is acted upon and no further comparisons take place.

Access lists operate as a series of if-then statements. If a given condition is met, then a given action is taken. If the condition is not met, nothing happens and the next statement is evaluated. Once the lists are built, they can be applied to either inbound or outbound traffic on any interface. Applying an access list causes the router to analyze every packet crossing that interface in the specified direction and take the appropriate action

There are three important rules that a packet follows when it is being compared with an access list:

- The packet is always compared with each line of the access list in sequential order. It will always start with the first line of the access list, move on to line 2, then line 3, and so on.
- The packet is compared with lines of the access list only until a match is made. Once it matches the condition on a line of the access list, the packet is acted upon and no further comparisons take place.
- There is an implicit "deny" at the end of each access list. This means that if a packet does not match the condition on any of the lines in the access list, the packet will be discarded.

Objective:
Compliance and Assessment

Sub-Objective:
Understand the importance of data privacy and protection.

References:

Chapter: Creating an IP Access List and Applying It to an Interface, http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/sec-create-ip-apply.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 19: Data Privacy and Protection

---

Question #139 of 200

Question ID: 1299643

Which of the following is another term for system isolation?

- ✗ **A)** DMZ
- ✗ **B)** Sheep dip
- ✗ **C)** VLAN
- ✓ **D)** Air gap

Explanation

When a system is physically isolated, we say that there is an air gap between it and the other systems. Air gaps are not totally secure, however. As was proved by the Stuxnet attack, corrupted USB drives can be used to "jump" the air gap.

A sheep dip computer is a system that has been isolated from the other systems and is used for analyzing suspect files and messages for malware. It may be isolated using an air gap, but is not the air gap itself.

A virtual LAN is a logical Layer 2 segmentation technique used on switches. It does not create an air gap, because systems are still physically connected.

A demilitarized zone (DMZ) is a section of the network separated from the internal network logically where resources are place that can be accessed from the Internet. A DMZ does not create an air gap since systems are still physically connected.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Disconnect from the Internet - Whale's e-Gap In-Depth, https://www.sans.org/reading-room/whitepapers/firewalls/disconnect-internet-whales-e-gap-in-depth-802

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #140 of 200

Question ID: 1299697

Yesterday, a discussion occurred during a meeting between the network and security teams. The network team is concerned that the use of the SQL server is increasing at such a rate that additional resources need to be dedicated to this system. The security team feels that although use is increasing, there is still plenty of time until the situation requires this action. What type of analysis could be used to settle the discussion?

- ✓ **A)** Trend analysis
- ✗ **B)** Anomaly detection
- ✗ **C)** NetFlow analysis
- ✗ **D)** Wireless analysis

Explanation

Trend analysis could be used to settle the discussion. The information needed in this scenario is the rate of increase in the use of the SQL server. By determining this, a point in time in the future in which action must be taken can be determined. Trend analysis focuses on the long term direction in the increase or decrease in a particular type of traffic.

NetFlow analysis would not be best for this. NetFlow is a technology developed by Cisco, and since supported by all major vendors, that can be used to collect and subsequently export IP traffic accounting information. The traffic information is exported using UDP packets to a NetFlow analyzer, which can organize the information in useful ways. It exports records of individual one-way transmissions called flows.

Wireless analysis would not be best for this because it alone will not provide the information you need. Wireless analysis might be used in the process of performing trend analysis.

Anomaly detection would not be appropriate. Anomaly analysis focuses on identifying something that is unusual or abnormal. This type of analysis is typically done by an IDS or IPS system.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Analyzing Your Network: Statistical Monitoring vs. Real-Time Performance, http://searchnetworking.techtarget.com/tip/Analyzing-your-network-Statistical-monitoring-vs-real-time-performance

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #141 of 200

Question ID: 1299763

You suspect that a device has been compromised and is communicating with a remote C&C server. Which of the following symptoms would be indicative of this?

- ✗ **A)** The device is suddenly unavailable
- ✗ **B)** An usually high number of ping requests to multiple hosts on your network within a short time frame
- ✗ **C)** An unusual spike in network traffic
- ✓ **D)** Traffic leaving your network at regular intervals from the same device to the same destination.

Explanation

The activity described is called beaconing. Beaconing refers to traffic leaving your network at regular intervals from the same device to the same destination. This type of traffic could be generated by compromised hosts that are attempting to communicate with (or call home to) the malicious party that compromised the host. Hosts attempt to communicate with what is called a command and control (C&C) server. The best course of action is to first identify the destination of the traffic and block it at the firewall. It indicates some sort of malware or compromise so you should also remove all malware. If the device still does not function properly after the malware removal, re-image the device. You should also keep all anti-malware up to date and ensure that users are trained in safe practices.

An usually high number of ping requests to multiple hosts on your network within a short time frame is an indication of a ping sweep. Ping sweeps use the ICMP protocol to identify all live hosts by pinging all IP addresses in the known network. All devices that answer are up and running. These sweeps can be detected by IDS and IPS systems. They indicate an attempt to map your network. The best course of action is to identify the source of the sweeps. Going forward, you should also deploy an IPS or IDS if not already present.

An unusual spike in network traffic is an indication of a DoS attack. If these attacks occur, you should locate the source of the attack and block the source at the firewall.

Another indication of a DoS attack is when the device is suddenly unavailable. If these attacks occur, you should locate the source of the attack and block the source at the firewall.

While data exfiltration (sensitive data exiting the network) could be occurring along with the beaconing, that is not the typical purpose of the beaconing, which is to check for instructions from the C&C server.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Testing Your Defenses - Beaconing, http://blog.opensecurityresearch.com/2012/12/testing-your-defenses-beaconing.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

Question #142 of 200

Question ID: 1299742

Which of the following roles in the incident response must fully back and support all efforts of the IR team and ensure that this support extends throughout the organization?

✗ **A)** Law enforcement

✗ **B)** Marketing

✗ **C)** Technical

✓ **D)** Management

Explanation

Management must fully back and support all efforts of the incident response team and ensure that this support extends throughout the organization. The MOST important factor that will ensure the success of an incident response plan is the support of upper management, both verbally and financially (through the budget process). Moreover, all other levels of management should fall in line to support all incident response efforts. Specifically, management's role in incident response can be defined as:

- Communicate the importance of the incident response plan to all parts of the organization.
- Create agreements detailing the authority of the IR team to take over business systems if necessary.
- Create decision systems for determining when key systems must be removed from the network.

The role of the technical role (IT and security teams) will be to recognize, identify, and react to incidents, and to provide support in analyzing those incidents when an incident has occurred.

The role of law enforcement is to assist the investigation and in some cases take over the investigation when a crime has been committed.

Marketing can be involved with the following activities in support of the incident response plan:

- Create newsletters and other educational materials to be used in employee response training.
- Coordinate with the legal team to prepare media responses and internal communications regarding incidents before they occur..

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Incident Response: Communication is Key, http://www.securitymagazine.com/articles/78810-incident-response-communication-is-key-1

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #143 of 200

Question ID: 1299718

Recently, there was an attack on a device that was targeted via Telnet. Telnet connections are never used in your network. Technicians must use SSH for remote sessions at the command line. You would like to stop this type of attack from happening again. What would be the quickest way to stop this?

- ✗ **A)** Set a complex password for Telnet on all systems
- ✗ **B)** Teach the users how to disable Telnet
- ✓ **C)** Block port 23 at the perimeter firewall
- ✗ **D)** Manually disable Telnet on all systems

Explanation

The quickest option is to block Telnet, which uses port 23 at the perimeter firewall. This would prevent any Telnet sessions from being established from outside the network.

Manually disabling Telnet on all systems might be a good action to take in the long run to prevent session inside the network, but the quickest option is to block Telnet at the perimeter firewall.

Setting a complex password for Telnet on all systems would be a good idea if the intent was to use Telnet, but using Telnet is not a good idea because it transmits in clear text. That is why SSH is used today as a replacement.

Teaching the users how to disable Telnet is not a good idea for several reasons. For one, you cannot be completely sure they will complete the task in the prescribed manner. Secondly, in the process you are also teaching them how to enable Telnet, which is not a good idea.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, implement configuration changes to existing controls to improve security.

References:

Port 23 Details, http://www.speedguide.net/port.php?port=23

Question #144 of 200

Question ID: 1299767

One of your users is complaining about poor performance on his device. When you examine his device, you find that although he has no programs running, processor utilization is very high. At the same time, there is zero network utilization. Which issue may you be facing?

- ✗ **A)** ping sweep
- ✓ **B)** malware
- ✗ **C)** port scan
- ✗ **D)** vulnerability scan

Explanation

Of the options listed, this is most likely an issue with malware. When the processor is very busy with very little or nothing running to generate the activity, it could be a sign that the processor is working on behalf of malicious software. This is one of the key reasons why any compromise is typically accompanied by a drop in performance. If this symptom occurs, you should suspect a malicious process is using processing resources. The best course of action is to scan the device for malware. The best prevention is to keep all anti-malware up to date and ensure that users are trained in safe practices.

This is probably not a port scan. A port scan sends a TCP SYN packet to each port on a single device. Answering these packets would not likely cause the high processor utilization, though it may cause temporary network card utilization. These scans can be detected by IDS and IPS systems. They indicate an attempt to map your network. The best course of action is to identify the source of the sweeps. The best response is to deploy an IPS or IDS if one is not already present.

This is not a vulnerability scan. These scans will generate network traffic to the device, but the scenario states that network utilization is zero. Vulnerability scans can be detected by IDS and IPS systems. Like ping sweeps, they indicate an attempt to map your network. The best course of action is to identify the source of the scans. The best prevention is to deploy an IPS or IDS if one is not already present.

This probably not a ping sweep. Ping sweeps use the ICMP protocol to identify all live hosts by pinging all IP addresses in the known network. All devices that answer are up and running. These sweeps can be detected by IDS and IPS systems. They indicate an attempt to map your network. The best course of action is to identify the source of the sweeps. The best prevention is to deploy an IPS or IDS if one is not already present.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

13+ Warning Signs that Your Computer is Malware-Infected [Updated], https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

Question #145 of 200

Question ID: 1299712

Recently, your company's users have reported they have been receiving emails purporting to be from reputable companies. These emails attempt to induce users to reveal personal information, such as passwords and credit card numbers. Which endpoint vulnerability has occurred?

- ✓ **A)** Phishing
- ✗ **B)** Spear phishing
- ✗ **C)** Ransomware
- ✗ **D)** Whaling

Explanation

Phishing has occurred. In this attack, users receive emails purporting to be from reputable companies. The emails attempt to induce users to reveal personal information like passwords and credit card numbers in order to steal from or impersonate the users.

Whaling occurs when scam emails masquerade as critical business emails. They appear to originate from a legitimate business authority and are sent to high profile end users, such as executives.

Spear phishing is similar to phishing, except spear phishing targets a specific victim.

Ransomware is malicious software that blocks access to a computer system until a sum of money is paid.

Endpoints include client computer, laptops, tablets, mobile devices, and printers that are installed on a network. Endpoints are often easy to attack because they do not have a high level of security. Security analysts should ensure that the appropriate controls, applications, and policies are in place to protect endpoints.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

How to recognize phishing email messages, links, or phone calls, http://www.ancsite.com/recognize-phishing-email-messages-links-phone-calls

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #146 of 200

Question ID: 1299652

As a security analyst, you must ensure that your company implements secure identity and access management solutions. Management is concerned with identity provisioning for both employees and online customers. Employees are issued identities via manual provisioning, and online customers are issued identities via automatic provisioning. Which of the following should you recommend?

- ✗ **A)** Online customer provisioning should include identity proofing, and employee provisioning should include CAPTCHA.
- ✓ **B)** Online customer provisioning should include CAPTCHA, and employee provisioning should include identity proofing.
- ✗ **C)** Both online customer and employee provisioning should include CAPTCHA.
- ✗ **D)** Both online customer and employee provisioning should include identity proofing.

Explanation

Online customer provisioning should include CAPTCHA, and employee provisioning should include identity proofing. Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) should only be used with automatic provisioning systems. CAPTCHA ensures that humans are creating the accounts, not bots or machines. Identity proofing ensures that users are who they say, usually by requiring some form of identification.

Both online customer and employee provisioning should NOT include CAPTCHA because CAPTCHA should only be used in automatic provisioning. CAPTCHA does not ensure proof of identity.

Both online customer and employee provisioning should NOT include identity proofing. Identity proofing should only be used when you can fully verify that a person is who they say. This is next to impossible with online customers.

Online customer provisioning should NOT include identity proofing, and employee provisioning should NOT include CAPTCHA. This is the opposite of what you need in this scenario.

For the CySA+ exam, you need to understand manual vs. automatic provisioning/deprovisioning. Manual provisioning creates accounts via an administrator creating the account. Identity proofing should be used to ensure that only valid accounts are created. Accounts should be deprovisioned when they are no longer being used. Automatic provisioning creates accounts via an application without human intervention. Automatic provisioning is faster but often does not provide the security controls needed.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

What is CAPTCHA?, https://www.pandasecurity.com/mediacenter/panda-security/what-is-captcha/

Identity Proofing, https://www.idology.com/blog/identity-proofing/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #147 of 200

Question ID: 1299780

A recent digital forensics investigation went well with the exception of one part. Although it did not cause an issue prosecuting this incident, there was very shoddy documentation work performed. When questioned during a lesson learned meeting, one of the responders said that they could have done a better job in that area if the proper forms were readily available. Which of the following forms does not have to be in the forensics kit?

- ✗ **A)** incident form
- ✗ **B)** incident response plan
- ✓ **C)** forensic equipment list
- ✗ **D)** chain of custody form

Explanation

While it might be helpful to have this list to verify all equipment is in the kit, it is not critical and certainly would not hamper documentation efforts. Tools that should be included in the kit consist of:

- Digital forensics workstation - A dedicated workstation for processing an investigation that includes special tools and utilities that make the process easier and more productive
- Write blockers - A tool that permits read-only access to data storage devices without compromising the integrity of the data.
- Cables - You should carry a variety of cables for connecting to storage devices.
- Drive adapters - Adapters can enable connections to drives for which you have no cable.
- Wiped removable media - Your kit should have removable media of various types that has been wiped clean. These may include USB flash drives, external hard drives, Multimedia Cards (MMC), Secure Digital s (SD), Compact Flash card (CF), Memory Sticks, xD Picture cards, CDs, CD-RW, DVDs, and Blu-ray discs.
- Cameras - Digital cameras with 12 MP (megapixels) or greater image sensors and manual exposure settings (in addition to any automatic or programmed exposure modes) are usually suitable for crime scene and evidence photography.
- Crime tape - Flagging or adhesive pre-preprinted tape intended to block the area and prevent any unauthorized individuals from entering.
- Tamper-proof seals - Used to ensure that the chain of custody is maintained.
- Documentation/forms - Specific forms are used to document the crime, the crime scene, and the evidence. There may also be interviews with witnesses. Most of these form templates are developed by the company based on standards.

The forms that should be present in the kit are:

- Chain of custody form - This form will indicate who has handled the evidence, when they handled it, and the order in which the handler was in possession of the evidence.
- Incident response plan - This plan should be formally designed, well communicated, and followed. It should specifically address cyber-attacks against an organization's IT systems.
- Incident form - This form is used to describe the incident in detail. It should include sections to record CMOS, hard drive information, image archive details, analysis platform information and other details.
- Call list/escalation list - This list should indicate under what circumstance individuals should be contacted, and should include current contact information.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

Day 4 - Preparation: What Goes Into a Response Kit, https://isc.sans.edu/forums/diary/Day+4+Preparation+What+Goes+Into+a+Response+Kit/5125/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

Question #148 of 200

Question ID: 1299613

You are working with a new security analyst on a recent non-credentialed Nessus vulnerability scan. You need to document the number of devices that are impacted by a particular vulnerability. The new security analyst does not know how to obtain this information. Which of the following should you instruct the analyst to obtain?

- ✓ **A)** Vulnerabilities Grouped by Plugin
- ✗ **B)** Suggested Remediations
- ✗ **C)** Vulnerabilities Grouped by Host
- ✗ **D)** Credentialed scan

Explanation

You should instruct the new security analyst to obtain the Vulnerabilities Grouped by Plugin subset of the current scan. This is available from the main report in Nessus. A plugin is a simple program that checks for a given flaw.

You should not instruct the analyst to obtain Vulnerabilities Grouped by Host subset of the current scan. This will list the vulnerabilities for a given host.

You should not instruct the analyst to obtain the Suggested Remediations subset of the current scan. It summarizes the actions to take that address the largest quantity of vulnerabilities on the network.

You should not instruct the analyst to obtain a Credentialed scan. You can obtain the information you need from the current non-credentialed scan.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

Group Vulnerabilities, https://docs.tenable.com/nessus/Content/GroupVulnerabilities.htm

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

Question #149 of 200

Question ID: 1299701

Due to performance issues with the network, the networking team has asked your cyber security team to assist them in identifying the following:

- Network utilization
- Download/upload speeds
- Type and size of packets

What type of analysis should you suggest they perform?

☒ **A)** Protocol analysis

✓ **B)** Traffic analysis

☒ **C)** Heuristic analysis

☒ **D)** Packet analysis

Explanation

When you are interested in traffic statistics rather than the individual communications themselves, you should perform traffic analysis. While protocol analysis looks at the information contained in the headers, and packet analysis looks at the contents of the payload, traffic analysis concerns itself with the types of traffic in the network.

Protocol analysis looks at information contained in the headers. Packet analysis looks at the contents of the payload. Neither will assist with identifying the network utilization statistics or download and upload speeds.

Heuristic analysis determines the susceptibility of a system towards a particular threat or risk using decision rules or weighing methods. It is often utilized by antivirus software to identify threats that cannot be discovered with signature analysis because the threat is either too new to have been analyzed (called a zero-day threat) or it is a multi-pronged attack, which is constructed in a way that existing signatures do not identify the threat.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

5 Major Benefits You Could Get Out of Traffic Analysis, https://blogs.manageengine.com/network/netflowanalyzer/2011/10/11/5-major-benefits-you-could-get-out-of-traffic-analysis.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #150 of 200

Question ID: 1299772

You are investigating the symptoms displayed by a device in your network. The system is experiencing very high consumption of bandwidth during a time when there should not be a heavy workload on the device. Which issue is the most likely concern?

☒ **A)** buffer overflow

- ✓ **B)** DoS attack
- ✗ **C)** rogue devices
- ✗ **D)** ping sweep

Explanation

While all of these issues should be a concern, when heavy bandwidth consumption is detected in the network, your first concern should be a DoS attack. High bandwidth usage is the key symptom of a DoS attack. The best course of action is to identify the source of the traffic and block it at the firewall. Going forward, you should prevent all traffic from outside the network that uses a source address that is a private address, keep all anti-malware up to date, and ensure that users are trained in safe practices.

Any time new devices appear on the network, there should be cause for suspicion. However, the presence of a rogue device would not usually cause high bandwidth consumption. Rogue devices on the network often indicate that an attacker is trying to capture communication that occurs on your network. The best course of action for rogue devices is to perform periodic scans, locate the rogue device, and remove it from the network or disable it.

A ping sweep would only touch this device once as it answers the sweep; therefore, it should not be a cause of high bandwidth usage. The symptom of a ping sweep attack is unusual spikes in network traffic that indicate an attempt to map your network. These sweeps can be detected by IDS and IPS systems. The best course of action is to identify the source of the sweeps. Going forward, you should also deploy an IPS or IDS if one is not already present.

A buffer overflow would not typically cause a surge in bandwidth usage. When these attacks occur, in many cases the device crashes. A symptom is when a device suddenly becomes unavailable. All web applications in the device should be checked for proper input validation.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Security Tip (ST04-015): Understanding Denial-of-Service Attacks, https://www.us-cert.gov/ncas/tips/ST04-015

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

Question #151 of 200

Question ID: 1299814

You are the security analyst for your company. Management contacts you regarding a subpoena they have received. The subpoena requests a series of emails from five years ago as evidence production. You need to determine if the company can provide the email in question. Which of the following should you consult?

- ✓ **A)** Data retention policy
- ✗ **B)** Acceptable use policy
- ✗ **C)** Account management policy

- ✗ **D)** Data ownership policy
- ✗ **E)** Data classification policy

Explanation

You should consult the data retention policy. A data retention policy details the archiving procedures for old data. Each data type should have a defined data retention period and data retention medium.

You should not consult the account management policy. This policy details how accounts are created, managed, and deleted. In addition, it should include information on monitoring accounts to ensure that unused accounts are removed in a timely manner.

You should not consult the data ownership policy. This policy defines who owns the data assets in the company. This is used to ensure that data custodians know whom to consult when users request access to data.

You should not consult an acceptable use policy. This policy defines how users are allowed to utilize company resources.

You should not consult the data classification policy. This policy defines how to classify data based on its value to the company.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

What is data retention policy?, https://searchdatabackup.techtarget.com/definition/data-retention-policy

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

Question #152 of 200

Question ID: 1299713

As your company's security analyst, you often perform vulnerability scans, penetration tests, and log reviews. During a recent assessment, you discovered that several phishing attacks have been attempted on your network. Based on this data, you need to recommend solutions that are appropriate for these attacks. Which of the following entities is targeted by these attacks?

- ✓ **A)** Personnel
- ✗ **B)** Endpoints
- ✗ **C)** Roles
- ✗ **D)** Servers

Explanation

The entities that are targeted with phishing attacks are personnel. To prevent security issues associated with personnel and end users, you should implement security awareness training and multi-factor authentication. In addition, you should limit the use of privileged accounts. Shared accounts should not be allowed.

None of the other identities is targeted with phishing attacks, although the ultimate result of a successful phishing attack is access to the network and resources on the network.

Endpoints are the mobile devices, computers, and printers that are in use on the network. Rogue endpoints are a concern on networks as they can introduce security issues. To prevent security issues associated with endpoints, you should implement NAC security policies to verify a minimal security configuration. Endpoints that are not properly configured are quarantined until the configuration issues are resolved. Organizations should also scan for rogue endpoints on the network.

Servers hold valuable digital resources for an organization. Servers are often the victim of denial of service (DoS) attacks. To prevent security issues on servers, you should implement all hardening techniques. Servers may be the victim of DoS attacks. Implementing a firewall can often prevent these attacks.

Roles are associated with users and groups to allow them access to resources based on the rights held by the roles. However, role-based access control may cause security issues because you may not be able to track individual transactions based to a single person. To prevent security issues with roles, roles should be given the minimum permissions needed to perform their duties. In addition, users should be removed from roles they no longer should have. Unfortunately, with role-based access control, you may not be able to track transactions back to a single user.

For the CySA+ exam, you also need to understand the security issues associated with the following services and applications.

To prevent security issues with services, you should disable unneeded services. In addition, you may want to configure the services to use non-default ports. Also, limit the scope of a service by having it log on as a user and control the actions it can take, rather than letting it log on as the system account (default).

To prevent security issues with applications, application accounts should be properly secured. In addition, default accounts should be renamed or deleted.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Targeted Phishing, https://www.mimecast.com/content/targeted-phishing/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #153 of 200

Question ID: 1299667

After returning from a software development workshop, the software development team is implementing a system where two authors develop code together at the same workstation. Which type of software testing does this support?

- ✗ **A)** User acceptance testing
- ✗ **B)** Security regression testing
- ✓ **C)** Manual peer review

- ✗ **D)** Stress test application

Explanation

Pair programming, in which two authors develop code together at the same workstation, provides a form of manual peer review that occurs at an early stage of the process.

While it is important to make web applications secure, in some cases security features make the application unusable from the user perspective. User acceptance testing is designed to ensure that does not occur.

Stress testing determines the workload that the application can with withstand. These tests should be performed in a certain way, and there should always be defined objectives before the testing begins.

Regression testing is done to verify functionality subsequent to making a change to the software. Security regression testing, a subset of that, validates that changes have not reduced the security of the application nor opened new weaknesses that were not there prior to the change.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

Peer Review, https://www.tutorialspoint.com/software_testing_dictionary/peer_review.htm

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

---

Question #154 of 200

Question ID: 1299606

You have been hired by your company as a security analyst. You discover that a vulnerability management process was never established. You need to implement an information security vulnerability management process. What is the first step you should complete?

- ✗ **A)** Establish the scanning frequency.
- ✗ **B)** Configure the tools to perform the vulnerability scan.
- ✓ **C)** Identify requirements.
- ✗ **D)** Execute the vulnerability scan.

Explanation

The first step of implementing an information security vulnerability management process is to identify the requirements.

The steps of implementing an information security vulnerability management process are as follows:

1. Identify requirements.
2. Establish scanning frequency.
3. Configure the tools to perform the vulnerability scan.

4. Execute the vulnerability scan.
5. Generate reports.
6. Implement remediation.
7. Ongoing scanning and continuous monitoring.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #155 of 200

Question ID: 1299759

Which of the following is used to sanitize a SSD?

✓ **A)** special commands

✗ **B)** shredding

✗ **C)** degaussing

✗ **D)** zeroing

Explanation

Most solid-state drive vendors provide sanitization commands that can be used to erase the data on the drive. Security professionals should research these commands to ensure that they are effective.

Degaussing is not effective on a solid state drive. It only works on magnetic hard disk drives.

Zeroing is not effective on a solid state drive. An SSD will write new data to a new location.

Shredding will render the device unusable. Sanitizing it with commands will not render it unusable.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Guidelines for Media Sanitization, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

Question #156 of 200

Question ID: 1299804

A new addition was made recently to the secure part of the company website. Now, when new users are creating an account, they are prompted to identify the letters in a grainy graphic. What is this process called?

- ✗ **A)** NAC
- ✓ **B)** CAPTCHA
- ✗ **C)** SSO
- ✗ **D)** Jump box

Explanation

A Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) system uses a graphic, which is difficult for a bot to read but not a human, to ensure that bots (automated process used by hackers to create accounts) are not allowed to create accounts.

This is not NAC. Network access control (NAC) systems make remote access decision's based on combinations of factors. They use combinations of these decision methods to make access control decisions, including:

- Location-based
- Time-based
- Role-based
- Rule-based

This is not a jump box. A jump server or jump box is a server that is used to access devices that have been placed in a secure network zone, such as a DMZ. The server would span the two networks to provide access from an administrative desktop to the managed device. This would be done at Layer 3.

This is not single sign-on (SSO). SSO is a process that allows users to log on once to the network and thereafter not to be required to issue another password to access resources.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart), http://searchsecurity.techtarget.com/definition/CAPTCHA

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

Question #157 of 200

Question ID: 1299784

As a security analyst, you need to assess the passwords used by your users. Which tool should you use?

- ✓ **A)** John the Ripper
- ✗ **B)** DD
- ✗ **C)** MD5sum
- ✗ **D)** SHAsum

Explanation

You should use John the Ripper to assess the passwords used by your users. You could also use Cain and Abel.

DD is an imaging tool. MD5sum and SHAsum are hashing tools.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

John the Ripper Password Cracker, http://www.openwall.com/john/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #158 of 200

Question ID: 1299663

You have a new application that will be used as part of a workflow process within the organization. The application is finished, and now the team would like to do the following:

- Perform the testing in an environment that mirrors the live environment.
- Identify real-world use cases for execution.

What type of testing are they most likely planning?

- ✗ **A)** Stress test application
- ✗ **B)** Manual peer review
- ✗ **C)** Security regression testing
- ✓ **D)** User acceptance testing

Explanation

While it is important to make web applications secure, in some cases security features make the application unusable from the user perspective. User acceptance testing is designed to ensure that does not occur. This type of testing usually performs testing in an environment that mirrors the live environment. It identifies real-world cases for execution.

Stress testing determines the workload that the application can with withstand. These tests should be performed in a certain way, and should always have defined objectives in place before testing begins.

Regression testing is done to verify functionality subsequent to making a change to the software. Security regression testing, a subset of that, validates that changes have not reduced the security of the application nor opened new weaknesses that were not there prior to the change.

Formal code review involves a careful and detailed process with multiple participants and multiple phases. In manual peer review, software developers attend meetings where each line of code is reviewed, usually using printed copies.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

5 types of user acceptance tests the perfect UAT framework, http://usersnap.com/blog/types-user-acceptance-tests-frameworks/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

Question #159 of 200

Question ID: 1299604

A team is working to design the information security vulnerability management process for a large company. They have identified all the requirements for this process. What is the next step that they should complete?

- ✗ **A)** Generate reports.
- ✗ **B)** Execute the vulnerability scan.
- ✗ **C)** Configure the tools to perform the vulnerability scan.
- ✓ **D)** Establish scanning frequency.

Explanation

The next step that the team should complete is to establish the scanning frequency.

The steps of implementing an information security vulnerability management process are as follows:

1. Identify requirements.
2. Establish scanning frequency.
3. Configure the tools to perform the vulnerability scan.
4. Execute the vulnerability scan.
5. Generate reports.
6. Implement remediation.
7. Ongoing scanning and continuous monitoring.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #160 of 200

Question ID: 1299748

After performing a vulnerability scan, you receive a vulnerability report. While working to remove the vulnerabilities from your network, you notice that one of the vulnerabilities could result in a DoS attack. One of your company's servers was recently the victim of a DoS attack. You want to determine if that attack was the result of the vulnerability reported. What should you do?

- ✗ **A)** Perform another vulnerability scan of the server.
- ✓ **B)** Review the logs on the server from the time when the attack occurred.
- ✗ **C)** Capture the network traffic for the server.
- ✗ **D)** Review the current logs on the server.

Explanation

You should review the logs on the server from the time when the attack occurred. Logs are often used to research issues because they contain transaction records.

You should not review the current logs on the server because they probably will not contain the information about the DoS attack.

You should not perform another vulnerability scan of the server. All this will do it provide you with a list of the vulnerabilities on that server. It will provide no information about the DoS attack that occurred.

You should not capture the network traffic for the server. The current traffic will not give you any information about the DoS attack that occurred in the past.

After vulnerability scans, security analysts should work to validate the results and correlate other data points. This includes comparing the results to best practices or compliance, reconciling the results, reviewing related logs and/or other data sources, and determining trends.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Understanding Denial of Service Attacks, https://www.us-cert.gov/ncas/tips/ST04-015

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

---

Question #161 of 200

Question ID: 1299764

There have been reports from several users that they cannot access the Internet using the WLAN. You question them and find that they have connected to the same SSID they always do. Further investigation indicates that the source MAC address of the wireless frames being received by the users with the issue is NOT the MAC address of the wireless router. What type of issues should you suspect?

- ✗ **A)** WLAN sniffing
- ✗ **B)** malware
- ✓ **C)** rogue AP
- ✗ **D)** war driving

Explanation

This is most likely a rogue AP. A rogue access point (AP) is an AP placed in the network that is not managed by you. When it is set up to have the same SSID as your WLAN, it is called an evil twin. Because stations select access points by SSID, they may associate with the rogue AP. When they do, they will be in the same network with the attacker, and he can then start a peer-to-peer attack. The best course of action for rogue devices is to perform periodic scans, locate the rogue device, and remove it from the network or disable it.

This is not an indication of malware. Malware does not typically cause users to connect to a rogue AP. If a malware infection occurs, the best course of action is to scan the device for malware. Going forward, you should keep all anti-malware up to date and ensure that users are trained in safe practices.

This is not an indication of WLAN sniffing. This occurs when a hacker uses a wireless sniffer to capture 802.11 packets. That would not cause users to associate with a rogue AP. This sniffing would be undetectable by you even if it were occurring. As there is neither a way to prevent nor to detect WLAN sniffing, you should ensure that all sensitive traffic is encrypted.

This is not war driving. War driving is simply the act of driving around and looking for open WLANs. The only step you can take to prevent this is to hide your SSID, but if the hacker is determined, he can discern the SSID with a wireless sniffer.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Understanding Rogue Access Points, https://www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/topics/concept/wireless-rogue-ap.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

Question #162 of 200

Question ID: 1299791

While analyzing network traffic as a security consultant, you discover an appliance that is installed at the company's network perimeter. This appliance is used to avert attacks and alert administrators. Which product did you most likely encounter?

- ✗ **A)** Imperva
- ✓ **B)** Sourcefire
- ✗ **C)** Nmap
- ✗ **D)** AlienVault

Explanation

You most likely encountered Sourcefire, because the product described in the scenario is an intrusion prevention system (IPS). None of the other listed tools has IPS functionality.

Imperva is a Web application firewall (WAF). AlienVault is a security information and event management (SIEM) tool. Nmap is a network scanning and mapping tool

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

Sourcefire 101 Overview, http://www.thesecurityblogger.com/sourcefire-101-overview/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #163 of 200

Question ID: 1299638

You have several servers to which you would like access to be possible only from a designated administrative workstation. Which of the following should you deploy?

- ✓ **A)** Jump box
- ✗ **B)** VLAN
- ✗ **C)** Subnet
- ✗ **D)** Honeypot

Explanation

You should deploy a jump box. A jump server or jump box is a server that is used to access devices that have been placed in a secure network zone, such as a DMZ. The server would span the two networks to provide access from an administrative desktop to the managed device.

You should not deploy a virtual local area network (VLAN). VLANs separate devices logically at Layer 2 and Layer 3. Enterprise-level switches are capable of creating VLANs. These are logical subdivisions of a switch that segregate ports from one another as if they were in different LANs. This would not allow for access only from a designated administrative workstation.

You should not deploy subnets. IP subnets are used to separate devices at Layer 3. They would not allow for access only from a designated administrative workstation.

You should not deploy a honeypot. Honeypots are systems that are configured to be attractive to hackers and lure them into spending time attacking them while information is gathered about the attack.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Jump Boxes Improve Security, If You Set Them Up Right, http://www.infoworld.com/article/2612700/security/-jump-boxes--improve-security--if-you-set-them-up-right.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #164 of 200

Question ID: 1299693

Your organization has a new firewall and is endeavoring to configure it according to industry best practices. The following entry is found in the firewall log:

```
2016-09-20 10:38:21 DROP TCP 192.168.72.196 10.20.72.12 5333 23 48 SA 4175551841 892874455 17520 - - -
RECEIVE
```

Which of the following best practices is supported by the rule that caused this entry?

- ✗ **A)** Block outgoing traffic from private IP addresses
- ✗ **B)** Block incoming UDP traffic
- ✗ **C)** Block incoming IP addresses using protocols that should only be used internally
- ✓ **D)** Block incoming requests from private IP addresses

Explanation

The rule that caused this event is designed to block incoming requests from private IP addresses. It is a best practice to block incoming requests from private IP addresses because they are frequently spoofed.

The log indicates that an incoming request was dropped from 192.168.72.196 to 10.20.72.12 using the TCP transport protocol. It also indicates that the SYN and the ACK flags are set in the packet, as indicated by the `SA`. Finally, it indicates that the source port was 5333 and the destination 23. These two values come after the source and destination IP addresses, `192.168.72.196 10.20.72.12`.

The entry does not support the best practice of blocking incoming IP addresses using protocols that should only be used internally. The packet is sourced from port 5333 and directed to port 23, which is Telnet. This is not a protocol that should only be used internally. Examples of protocols that should only be used internally are DHCP and routing protocol traffic.

The entry does not support blocking outgoing traffic from private IP addresses. That is not a best practice, although it may be required in some cases. It is a best practice to block incoming requests from private IP addresses as they are spoofed.

The entry does not support blocking incoming UDP traffic. Blocking incoming UDP traffic is not a best practice. Also, nothing in the output indicates the packet is using UDP.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Step 5: Viewing the Firewall Log, https://technet.microsoft.com/en-us/library/cc753781(v=ws.10).aspx

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #165 of 200

Question ID: 1299719

Which of the following is a common standard used for network access control?

- ✗ **A)** 802.11i
- ✓ **B)** 802.1x
- ✗ **C)** 802.10
- ✗ **D)** 802.11

Explanation

The 802.1x standard describes a method of port based network access control in which a device's port to the network is not made functional until the device has been authenticated by a central authentication server.

The 802.11 standard describes a method for creating wireless local area networks (WLAN).

The 802.11i standard is an amendment to the original IEEE 802.11, implemented as Wi-Fi Protected Access II (WPA2). It operates using the same basic architecture as 802.1x, but describes mechanisms for wireless networks.

The 802.10 standard a former standard for security functions that could be used in both local area networks and metropolitan area networks based on IEEE 802 protocols. This standard was withdrawn in 2004.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, implement configuration changes to existing controls to improve security.

References:

Wired 802.1x Security, https://www.sans.org/reading-room/whitepapers/firewalls/wired-8021x-security-1654

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 12: Implementing Controls to Improve Security

Question #166 of 200

Question ID: 1299806

You have used Nessus to produce comprehensive vulnerability scan reports on all systems. Management specifically wants you to review the reports against Center for Internet Security (CIS) benchmarks. Which type of report should you review?

- ✗ **A)** Patch audit
- ✗ **B)** Non-credentialed network scan
- ✗ **C)** Credentialed network scan
- ✓ **D)** Compliance audit

Explanation

You should review the compliance audit produced by Nessus. A compliance audit supplies vulnerabilities as measured against CIS benchmarks.

A patch audit analyzes systems and devices against patch management system of vendors to determine if the organization has not deployed the available patches.

A credentialed network scan scans the network for vulnerabilities using credentials to ensure that all areas of the devices can be examined.

A non-credential network scan scans the network without credentials so areas that require credentials for access will not be scanned.

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Compliance, https://docs.tenable.com/nessus/Content/Compliance.htm

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

Question #167 of 200

Question ID: 1299762

You just received an alert from the IDS that there has been a big spike in traffic during the last five minutes. Which of the following possible explanations is NOT a valid concern?

- ✗ **A)** SYN flood
- ✗ **B)** Smurf attack
- ✗ **C)** Fraggle attack
- ✓ **D)** Rogue AP

Explanation

While you may have a rogue AP, it is not the source of the spike in traffic. Rogue access points (APs) are those that you do not manage and may not be aware of. They can cause users to connect to them instead of to legitimate APs, which makes them vulnerable to a peer-to-peer attack from the owner of the rogue AP. However, there is nothing about their operation that creates a spike in traffic. The best course of action for rogue devices is to perform periodic scans, locate the rogue device, and remove it from the network or disable it.

Any of the other three options could be performed as a distributed denial of service (DDoS) attack. In these attacks, multiple machines are recruited to attack the target, greatly amplifying the attack and its effects. This will cause a big spike in traffic.

A SYN flood attack is performed by sending many packets to the target with the SYN flag turned on. The target will respond with a SYN/ACK packet and will reserve memory for the expected response (an ACK packet) of the TCP three way handshake. When the ACK packets are never received and the SYN packets keep coming, the target will eventually run out of memory and cease to function. The best course of action is to deploy a stateful firewall at the perimeter.

A smurf attack occurs when a hacker sends an ICMP echo packet to the network broadcast address with the source IP address set to the target. When every computer in the network responds to the ping, it overwhelms the resources of the target. The best course of action to disable the use of IP-directed broadcasts on the network.You can also configure your firewall to drop ICMP messages.

A fraggle attack is like a smurf attack, except the attacker sends UDP packets to the broadcast address rather than ICMP packets. The effect is the same.The best course of action to disable the use of IP- directed broadcasts on the network.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Security Tip (ST04-015): Understanding Denial-of-Service Attacks, https://www.us-cert.gov/ncas/tips/ST04-015

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

---

Question #168 of 200

Question ID: 1299603

You have been hired as a security consultant to help a large corporation to establish their information security vulnerability management process. Currently, you are working with a team to document the company's risk appetite, regulatory requirements, technical constraints, and workflow. Which step of the information security vulnerability management process are you completing?

- ✗ **A)** Identify requirements.
- ✗ **B)** Generate reports.
- ✗ **C)** Execute the vulnerability scan.
- ✓ **D)** Establish scanning frequency.

Explanation

You are establishing scanning frequency when you document the company's risk appetite, regulatory requirements, technical constraints, and workflow.

The steps of implementing an information security vulnerability management process are as follows:

1. Identify requirements.
2. Establish scanning frequency.
3. Configure the tools to perform the vulnerability scan.
4. Execute the vulnerability scan.
5. Generate reports.
6. Implement remediation.
7. Ongoing scanning and continuous monitoring.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #169 of 200

Question ID: 1299746

After performing a vulnerability scan on your company's SQL server, you identify several issues that need to be handled. All of the identified issues will require changes to the current configuration of the SQL server. Your company has an establish change control process in place. What should you submit to start this process?

- ✓ **A)** RFC
- ✗ **B)** MOU
- ✗ **C)** SLA
- ✗ **D)** CCB

Explanation

You should submit a request for change (RFC) to start the formal change control process for the issues identified by the SQL server vulnerability scan. The RFC is evaluated and submitted to the change control board (CCB) for approval. If the RFC is approved, the appropriate steps will be taken to complete the change. If it is denied, no actions are taken.

All changes should be logged in a change log to ensure that records are maintained for both approved and denied RFCs. During the change control process, communication is key because the change status needs to be conveyed to the appropriate individuals. In addition, communication must occur to ensure that the change is completed once it is approved.

A service level agreement (SLA) is an agreement with a third party to provide services. It includes all of the parameters of the service that the third party will provide.

A memorandum of understanding (MOU) is an agreement between two parties that is similar to an SLA, but is considered a preliminary document that is generated before a formal agreement is signed.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Change Management, https://itsm.ucsf.edu/change-management

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

---

Question #170 of 200

Question ID: 1299589

Which of following attempts to exploit vulnerabilities?

- ✗ **A)** Port scan
- ✓ **B)** Penetration test
- ✗ **C)** Vulnerability test
- ✗ **D)** Risk assessment

Explanation

A penetration test (often called a pentest) attempts to exploit vulnerabilities. It is designed to simulate an attack on a system, a network, or an application. Its value lies in its potential to discover security holes that may have gone unnoticed. It differs from a vulnerability test in that it attempts to exploit vulnerabilities rather than to simply identify them.

A vulnerability test does not attempt to exploit vulnerabilities. It simply identifies them.

A risk assessment does not attempt to exploit vulnerabilities. Risk assessments attempt to identify vulnerabilities and adopt controls that address the vulnerabilities, or at least reduce the risk to an acceptable level.

A port scan does not attempt to exploit vulnerabilities. While it can be a step in a presentation test, by itself it locates open ports. It does not attempt to exploit them.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

Penetration Testing: Assessing Your Overall Security Before Attackers Do, https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

---

Question #171 of 200

Question ID: 1299631

Your assistant created an access list on a Cisco router, and the list is not working correctly. The first thing you ask him is whether he understands how these lists work. In what order are the lines of an access list read when an access list is applied to a router interface? (Choose two.)

- ✗ **A)** Bottom to top, if it is an extended access list
- ✓ **B)** Top to bottom, if it is an extended access list
- ✓ **C)** Top to bottom, if it is a standard access list
- ✗ **D)** Bottom to top, if it is a standard access list

Explanation

Both extended access lists and standard access lists are read from top to bottom. Therefore, when creating access lists, you want to create the more specific statements and the more frequently occurring conditions towards the top of the list and the more general statements towards the end of the list.

When a deny statement is encountered in an access list, all statements that follow the deny and apply to the same type of traffic on that interface will be ignored.

Access lists express the set of rules that give added control for packets that enter inbound interfaces, packets that are relayed through the router, or packets that exit outbound interfaces of the router. Access lists do not act on packets that originate from the router itself. Instead, access lists are statements that specify conditions on how the router will handle the traffic flowing through specified interfaces.

There are two types of access lists: standard and extended. Extended access lists can be either named or numbered. Named access lists include the following characteristics:

- Individual statements within the list can be deleted, rather than deleting the entire list as is required with numbered lists.
- Named lists must specify whether they are standard or extended. With numbered lists, this is indicated by the use of specific list number ranges.

Standard access lists are applied as close to the destination as possible (outbound), and can only base their filtering criteria on the source IP address. The number used while creating an access list specifies the type of access list created. The range used for standard access lists is 1 to 99 and 1300 to 1999.

Extended access lists are applied as close to the source as possible (inbound), and can base their filtering criteria on the source or destination IP address, or on the specific protocol being used. The range used for extended access lists is 100 to 199 and 2000 to 2699.

The other options are incorrect because access lists are always read from top to bottom.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

References:

Configuring IP Access Lists, https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 7: Implementing Controls

---

Question #172 of 200

Question ID: 1299692

You and a colleague are reviewing the firewall log. You are trying to locate an entry that indicates that someone is attempting to externally attack the port used by SMB. Which of the following entries indicates the presence of this attack?

- ✗ **A)** `2016-09-20 9:38:41 DROP TCP 19.168.72.196 10.20.72.12 5333 143 48 S 4175551841 892874455 17520 - - - RECEIVE`
- ✗ **B)** `2016-09-20 10:45:31 DROP UDP 19.168.72.196 10.20.72.12 5333 443 S 4175551841 892874455 17520 - - - RECEIVE`
- ✗ **C)** `2016-09-20 11:38:25 DROP TCP 19.168.72.196 10.20.72.12 5333 21 48 S 4175551841 892874455 17520 - - - RECEIVE`
- ✓ **D)** `2016-09-20 10:38:21 DROP TCP 19.168.72.196 10.20.72.12 5333 445 48 S 4175551841 892874455 17520 - - - RECEIVE`

Explanation

Port 445 is the port used for Server Message Block (SMB) protocol, and it is a common attack point. Although most attacks are done internally by malware, SMB traffic should be blocked at the perimeter.

The entry in the output below indicates the attack source is 19.168.72.196 and the target is 10.20.72.12. The source port is 5333 and the destination is 445. It is also using TCP as its transport protocol.

```
2016-09-20 10:38:21 DROP TCP 19.168.72.196 10.20.72.12 5333 445 48 S 4175551841 892874455 17520 - - - RECEIVE
```

The entry below indicates the destination port is 21, which is used by FTP, rather than 445, which is used by SMB.

```
2016-09-20 11:38:25 DROP TCP 19.168.72.196 10.20.72.12 5333 21 48 S 4175551841 892874455 17520 - - - RECEIVE
```

The entry below indicates the destination port is 443, which is used by HTTPS, rather than 445. Also, the transport protocol is UDP, which is not used for SMB.

```
2016-09-20 10:45:31 DROP UDP 19.168.72.196 10.20.72.12 5333 443 S 4175551841 892874455 17520 - - - RECEIVE
```

The entry below indicates the destination port is 143, which is used by IMAP, rather than 445.

```
2016-09-20 9:38:41 DROP TCP 19.168.72.196 10.20.72.12 5333 143 48 S 4175551841 892874455 17520 - - - RECEIVE
```

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Step 5: Viewing the Firewall Log, https://technet.microsoft.com/en-us/library/cc753781(v=ws.10).aspx

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #173 of 200

Question ID: 1299681

Several weeks ago, the network suffered a DoS attack, and the database server was down for two hours. Analysts were slowed during the investigation by the need to access the local logs of the database server, routers, and switches in the network. You would like to suggest a solution that would centralize these logs in one place.

Which two options are available? (Choose two.)

- ✗ **A)** WSUS server
- ✓ **B)** Syslog server
- ✓ **C)** SIEM system
- ✗ **D)** Packet analyzer
- ✗ **E)** MBSA

Explanation

You could use either a security incident and event management (SIEM) system or a syslog server. A syslog server can be configured to collect all logs and store them in one place. A SIEM system collects security logs from all devices and uses the combined data to identity vulnerabilities and attacks. They provide real-time analysis of security alerts generated by network hardware and applications. Log review is always part of any environmental reconnaissance.

The Microsoft Baseline Security Analyzer (MBSA) cannot help with this issue. MBSA is a vulnerability scanner that can identify missing OS updates, missing security patches, and other vulnerabilities present in the hosts on the network.

A packet analyzer cannot help with this issue. These tools are used to capture and inspect raw packets from the network.

A Windows Server Update Services (WSUS) server cannot help with this issue. This is used to download updates from Microsoft and store them for local distribution to hosts after testing.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

Successful SIEM and Log Management Strategies for Audit and Compliance, https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #174 of 200

Question ID: 1299651

Recently, while reviewing log data, you discover that a hacker has used a design flaw in an application to obtain unauthorized access to the application. Which type of attack has occurred?

- ✗ **A)** maintenance hook
- ✓ **B)** privilege escalation
- ✗ **C)** buffer overflow
- ✗ **D)** backdoor

Explanation

An escalation of privileges attack occurs when an attacker has used a design flaw in an application to obtain unauthorized access to the application. Privilege escalation includes incidents where a user logs in with valid credentials and then takes over the privileges of another user, or where a user logs in with a standard account and uses a system flaw to obtain administrative privileges.

There are two types of privilege escalation: vertical and horizontal. With vertical privilege escalation, the attacker obtains higher privileges by performing operations that allow the attacker to run unauthorized code. With horizontal privilege escalation, the attacker obtains the same level of permissions as he already has, but uses a different user account to do so.

A backdoor is a term for lines of code that are inserted into an application to allow developers to enter the application and bypass the security mechanisms. Backdoors are also referred to as maintenance hooks.

A buffer overflow occurs when an application erroneously allows an invalid amount of input in the buffer. It can be used to perform a denial of service (DoS) attack or a distributed denial of service (DDoS) attack.

For the CySA+ exam, you also need to understand the following application issues:

- Time of use (TOU). To eliminate race conditions, application developers should create code that processes exclusive-lock resources in a certain sequence and unlocks them in reverse order.
- Insecure direct object references - occurs when a developer exposes a reference to an internal object, such as a file, directory, database record, or key, as a URL or form parameter without implementing the appropriate security control. An attacker can manipulate direct object references to access other objects without authorization. Implementing an access control check helps to protect against these attacks
- Cross-site request forgery (CSRF) - occurs when a malicious site executes unauthorized commands from a user on a Web site that trusts the user. It is also referred to as one-click attack or session riding. Implementing anti-forgery tokens protect against this attack.

- Improper error and exception handling - occurs when developers do not design appropriate error or exception messages in an application. The most common problem because of this issue is the fail-open security check, which occurs when access is granted (instead of denied) by default. Other issues include system crashes and resource consumption. Error handling mechanisms should be properly designed, implemented, and logged for future reference and troubleshooting.
- Improper storage of sensitive data - occurs when sensitive data is not properly secured when it is stored. Sensitive data should be encrypted and protected with the appropriate access control list. Also, when sensitive data is in memory, it should be locked.
- Secure cookie storage and transmission - Cookies store a user's Web site data, often including confidential data, such as usernames, passwords, and financial information. A secure cookie has the secure attribute enabled and is only used via HTTPS, ensuring that the cookie is always encrypted during transmission.
- Memory leaks - occur when an application does not release memory after it is finished working with it. Reviewing coding and designing best practices helps to prevent memory leaks.
- Integer overflows - occurs when an operation attempts to input an integer that is too large for the register or variable. The best solution is to use a safe integer class that has been built to avoid these problems.
- Geo-tagging - occurs when media, such as photos or videos, are tagged with geographical information. Turning off the geo-tagging feature on your device protects against releasing this type of information. It is also possible to remove geo-tagging information from media before using it in an application or Web site.
- Data remnants - occurs when applications are removed but data remnants, including registry entries, are left behind. Specialty tools and apps are available to ensure that applications have been completely removed from a device.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

What Is Privilege Escalation and Why Is It Important?, https://www.netsparker.com/blog/web-security/privilege-escalation/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

Question #175 of 200

Question ID: 1299786

A security analyst runs MBSA on a Windows computer. Which function is provided by this tool?

- ✗ **A)** Fuzzer
- ✓ **B)** Vulnerability scan
- ✗ **C)** Interception proxy
- ✗ **D)** Packet capture

Explanation

Microsoft Baseline Security Analyzer (MBSA) is a vulnerability scan tool. Other vulnerability scanning tools include Qualys, Nessus, OpenVAS, Nexpose, and Nikto.

Fuzzers include Untidy, Peach Fuzzer, and Microsoft SDL File/Regex Fuzzer. Interception proxies include Burp Suite, Zap, and Vega. Packet capture tools include Wireshark, tcpdump, Network General, and Aircrack-ng.

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

How to Use the Microsoft Baseline Security Analyzer, https://msdn.microsoft.com/en-us/library/ff647642.aspx

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

---

Question #176 of 200

Question ID: 1299752

Today there are two active attacks that have been detected by the IDS. One appears to be a malware attack affecting most of the network, and the other is a DDoS attack on your DNS server. Your boss has instructed the team to determine the scope of each attack before the attacks are prioritized for response. Which of the following is NOT considered a part of scope consideration?

- ✗ **A)** the length of time that the DNS server has been down
- ✗ **B)** the number of devices infected with the malware
- ✓ **C)** the type of data that could be at risk
- ✗ **D)** the estimated amount of time to recover the DNS server

Explanation

The type of data at risk is certainly a consideration when prioritizing the response to multiple attacks, but it is not a consideration that applies to scope. The type of data at risk is a separate priority consideration, and is especially critical with the following data types:

- Personally Identifiable Information (PII) - any information that can be used to identify an individual
- Personal Health Information (PHI) - the medical records of an individual
- Payment card information - credit card numbers, passwords, pins and other card related data
- Intellectual property - unique creations of the mind protected by copyright or patent
- Corporate confidential - information that must be kept secret because it imparts a business advantage to the organization

The scope of an attack is gauged by the following factors:

- Downtime - refers to the amount of time access to resource were interrupted
- Recovery time - refers to the amount of time taken to recover from the incident
- Data integrity - refers to the amount of data corrupted or altered during the incident
- Economic - the cost of the incident to the organization
- System process criticality - refers to the criticality of the system involved

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Defining the Scope, http://catalogue.pearsoned.co.uk/samplechapter/0130462233.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

Question #177 of 200

Question ID: 1299633

Recently there was a DoS attack on one of the servers that succeeded in taking it down for three hours. You would like to deploy a solution that would allow you to detect a huge rush of traffic to a specific device and route it somewhere away from the device. What technique could you use?

- ✗ **A)** Endpoint security
- ✓ **B)** Sinkholes
- ✗ **C)** Network segmentation
- ✗ **D)** System isolation

Explanation

You could use a sinkhole. A sinkhole is a routing mechanism that can route traffic from a device being flooded to a location where the traffic can be studied.

You could not use network segmentation. Network segmentation involves dividing the network at either Layer 2 or Layer 3 to create desirable security barriers between devices in the network. It cannot route traffic from a device being flooded to a location where the traffic can be studied.

You could not use endpoint security, which is the practice of protecting the endpoints (workstations, printers, etc.) in the network. Endpoint protection includes protecting them from other endpoints that spend at least some of the time outside the LAN. This is done by verifying patches and updates before the device is allowed access to the network. Endpoint security also includes the hardening process of endpoints. It cannot route traffic from a device being flooded to a location where the traffic can be studied.

You could not use system isolation. Systems can be isolated from other systems through the control of communications with the device. For example, in Microsoft server isolation, using group policy settings can require that all communication with isolated servers must be authenticated and protected by using IPsec (and optionally encrypted as well). It also controls which devices can make the connection. It cannot route traffic from a device being flooded to a location where the traffic can be studied.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

References:

Am I Sending Traffic to a "Sinkhole?", https://isc.sans.edu/forums/diary/Am+I+Sending+Traffic+to+a+Sinkhole/17048/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 7: Implementing Controls

Question #178 of 200

Question ID: 1299736

Which statement is FALSE with respect to involving law enforcement in an incident?

- ✗ **A)** Before involving law enforcement, try to rule out other potential causes of the event such as accidents and hardware or software failure.
- ✓ **B)** Law enforcement may be more motivated to stop the attacks and its damage than you are.
- ✗ **C)** More abstract crimes and events may be better served by involving law enforcement at the federal level, where greater skill sets are available.
- ✗ **D)** In cases where obvious laws have been broken (child pornography for example), immediately involve law enforcement.

Explanation

Law enforcement will view the incident differently that the company security team. While your team may be more motivated to stop the attacks and its damage, law enforcement may be inclined to let the attack proceed so that more evidence can be gathered.

The technical expertise of law enforcement varies. While local law enforcement may be indicated for such incidents as the physical theft of computers, more abstract crimes and events may be better served by involving law enforcement at the federal level, where greater skill sets are available.

Before involving law enforcement, you should try to rule out other potential causes of the event, such as accidents and hardware or software failure.

In cases where obvious laws have been broken, such as the presence of child pornography on your organization's network or hardware, you should immediately involve law enforcement. This includes any incidents that may be felonies, regardless of how small the loss to the company may have been.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Chapter 2: Introduction to the Incident Response Process, http://media.techtarget.com/searchNetworking/Downloads/IncidentResponseChapter2.pdf

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

Question #179 of 200

Question ID: 1299807

Your company has recently been contracted to work on a project with the U.S. Department of Defense. As a result, your company must ensure that the enterprise follows the guidelines set forth in NIST Special Publication 800-53 Revision 4.

As a security analyst, you are tasked with analyzing the enterprise and making suggestions on the appropriate access controls to implement. When your analysis is complete, you recommend the following controls be added to the enterprise:

- Security awareness training for all levels of personnel
- Job rotation in all departments
- Biometric authentication for the data center
- Centralized data backups for all systems
- Mantraps for the data center
- CCTV at building entry and areas where sensitive data is accessed

You need to provide a report to management regarding these suggested controls that details the type of control provided by them. What type of control is provided by each of these control measures?

You need to identify the type of control each provides. Match each control on the left with the appropriate control type on the right. (Each control should only be matched with one control type.)

{UCMS id=4772525089226752 type=Activity}

Explanation

The control types should be matched up with the suggested controls in the following manner:

- Detective administrative control - Job rotation
- Detective physical control - CCTV
- Recovery logical control - Centralized data backups
- Preventive administrative control - Security awareness training
- Preventive logical control - Biometric authentication
- Preventive physical control - Mantraps

Physical controls protect facilities and personnel from physical access. Physical controls include fencing, locks, guards, badges, mantraps, and CCTV.

Logical or technical controls are software or hardware components that restrict access. Logical controls include passwords, biometrics, smart cards, encryption, data loss prevention (DLP), data masking, data deidentification, tokenization, digital rights management (DRM), watermarking, geographic access requirements, access controls, and data backups.

Administrative or managerial controls direct the organization's assets and personnel. Administrative controls include policies, procedures, separation of duties, job rotation, disaster plans, and security awareness training.

Detective controls identify when security issues arise. Detective controls include monitoring, job rotation, investigations, intrusion detection systems (IDSs), auditing, guards, and CCTV.

Recovery controls return systems to normal operation. Recovery controls include disaster recovery plans, data backups, and alternate sites.

Preventive controls avert security issues from occurring. Preventive controls include security awareness training, separation of duties, biometrics, encryption, mantraps, badges, and guards.

Non-technical controls include: classification, ownership, retention, data types, retention standards, confidentiality, legal requirements, data sovereignty, data minimization, purpose limitation, and non-disclosure agreement (NDA).

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

Security and Privacy Controls for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Types of Controls, http://ishandbook.bsewall.com/risk/Assess/Risk/control_types.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

---

Question #180 of 200

Question ID: 1299805

You are a security analyst employed by an organization that provides vulnerability scanning services to other organizations. You are participating in vulnerability scanning projects for several third parties. You need to ensure that organizations that are affected by FISMA are compliant with the regulation. Which entity is affected by this law?

- ✗ **A)** Retail businesses
- ✓ **B)** Government agencies
- ✗ **C)** Banks
- ✗ **D)** Healthcare organizations

Explanation

Government agencies are affected by the Federal Information Security Management Act (FISMA). This law defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats. It requires that government agencies conduct vulnerability scans.

None of the other organizations is affected by FISMA. Although they have many laws and regulations they must follow, banks do not have any requirements on vulnerability scanning from FISMA. Bank and retail businesses may have vulnerability scanning requirements if they must comply with the Payment Card Industry Data Security Standard (PCI DSS).

Objective:
Compliance and Assessment

Sub-Objective:
Explain the importance of frameworks, policies, procedures, and controls.

References:

What is FISMA Compliance?, https://digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

---

Question #181 of 200

Question ID: 1299706

There have been a number of occasions lately where users have been tempted to click links in spam emails that lead them to malicious sites. While they have been warned about doing so, it continues to occur, and last week it caused a malware epidemic on the network. You would like to set up a system that can prevent users from connecting to known malicious websites. Which type of system should you set up?

- ✗ **A)** Botnet
- ✗ **B)** NAC
- ✗ **C)** Honeypot
- ✓ **D)** DNS sinkhole

Explanation

You should set up a DNS sinkhole. A properly configured DNS sinkhole could greatly reduce the problem in the scenario. It is a local DNS server that answers queries for known malicious websites with an IP address that goes nowhere or goes to a page telling the user to stop clicking dangerous links. In that regard, it is masquerading as the authoritative DNS server for the domain name.

Network access control (NAC) systems do not have this ability to prevent users from connecting to known malicious websites. They make inbound remote access decisions based on a combination of factors.

A honeypot cannot prevent users from connecting to known malicious websites. It is a system set up to be attractive to hackers. It is used to distract them from more critical resources and engage them so additional information can be gathered.

A botnet does not have the ability to prevent users from connecting to known malicious websites. A botnet is a large group of systems, recruited by a hacker using malware, which attacks a target system at the same time, amplifying the attack.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

DNS Sinkhole, https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

---

Question #182 of 200

Question ID: 1299600

As a security analyst for a US government body, you must implement a vulnerability scanning rate that fits within the confines of the Federal Information Security Management Act (FISMA). Of which scanning factor is this a part?

- ✗ **A)** Risk appetite
- ✗ **B)** Technical constraints
- ✓ **C)** Regulatory requirements
- ✗ **D)** Workflow

Explanation

The Federal Information Security Management Act (FISMA) is a part of the regulatory requirements that affect the vulnerability scanning rate. All laws and regulations that affect the organization must be fully analyzed to determine their effect on the scanning rate.

Risk appetite is the level of risk that an organization is willing to accept. A higher risk appetite would translate into a lower scanning frequency, while a lower risk appetite would translate into a higher scanning frequency.

Technical constraints include any constraints that are in place that may limit the scanning frequency, such as performance or licensing limitations.

Workflow is the flow of transactions and processes that affect the scanning rate.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

FISMA & NIST Standards, https://www.compliancepoint.com/regulations/nist/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #183 of 200

Question ID: 1299668

Now that security requirements have been defined, the software development team is ready to start the security testing phase. They want to analyze the code without the code executing and plan to repeat this testing throughout the entire application development life cycle. What type of testing are they planning?

- ✗ **A)** Fuzzing
- ✗ **B)** Use interception proxy to crawl application
- ✓ **C)** Static code analysis
- ✗ **D)** Web application vulnerability scanning

Explanation

Static code analysis is performed without the code executing. Code review and testing must occur throughout the entire application development life cycle. Code review and testing must identify bad programming patterns, security misconfigurations, functional bugs, and logic flaws.

Web vulnerability scanners can operate in two ways, using synthetic transaction monitoring and real user monitoring. In synthetic transaction monitoring, preformed (synthetic) transactions are executed against the application in an automated fashion and the behavior of the application is recorded. In real user monitoring the application, real user transactions are monitored while the web application is live.

Fuzz testing, or fuzzing, involves injecting invalid or unexpected input (sometimes called faults) into an application to test how the application reacts. It is usually done with a software tool that automates the process.

An interception proxy is an application that stands between the web server and the client and passes all requests and response back and forth. While it does so, it analyzes the information to test the security of the web application. A web application proxy can also "crawl" the site and its application to discover the links and content contained.

Objective:
Software and Systems Security

Sub-Objective:
Explain software assurance best practices.

References:

What Is Static Analysis? And What Is Static Code Analysis?, https://www.perforce.com/blog/sca/what-static-analysis

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 9: Software Best Practices

Question #184 of 200

Question ID: 1299750

The cyber team just returned from a security conference where they learned about the value of determining the MTD for each asset. They have made these determinations. Now they are creating realistic goals for recovering these assets in the event they go down. What determination are they now making?

- ✗ **A)** RPO
- ✗ **B)** WRT
- ✗ **C)** MTBF
- ✓ **D)** RTO

Explanation

Recovery time objective (RTO) is the shortest time period after a disaster or disruptive event within which a resource or function must be restored to avoid unacceptable consequences. RTO assumes that an acceptable period of downtime exists. The RTO should be smaller than the maximum tolerable downtime (MTD).

Mean time between failures (MTBF) is the estimated amount of time a device will operate before a failure occurs. This amount is calculated by the device vendor. System reliability is increased by a higher MTBF and a lower mean time to repair (MTTR).

Work recovery time (WRT) is the difference between RTO and MTD. WRT is the remaining time that is left over after the RTO before reaching the maximum tolerable downtime.

Recovery point objective (RPO) is the point in time to which the disrupted resource or function must be returned.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

RPO, RTO, WRT, MTDWTH?!, http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

---

Question #185 of 200

Question ID: 1299728

Last week there were two active attacks detected by the IDS. One appeared to be a malware attack, and the other was a DDoS attack on your DNS server. After consulting documents prepared earlier to assist in incident prioritization, it was decided to respond to the DNS server attack first. Which of the following scope considerations was MOST LIKELY the one that lead to this decision?

- ✗ **A)** Recovery time
- ✓ **B)** System process criticality
- ✗ **C)** Data integrity
- ✗ **D)** Economic

Explanation

Some assets are systems that provide access to information rather than the information itself. When these system or groups of systems provide access to data required to continue to do business, they are called critical systems. Because a loss of domain name system (DNS) services would cause an impact to the entire network, including access to data, it is a critical process.

The time to recover an asset or recovery time is a scope consideration but probably not the one that lead to this decision. This decision was made because DNS is a critical process.

The economic impact of the attack is a scope consideration but probably not the one that lead to this decision. This decision was made because DNS is a critical process.

The data integrity of an attacked system is a scope consideration but probably not the one that lead to this decision. This decision was made because DNS is a critical process. DHCP, SQL, and web services are likely to be deemed critical, but organizations must make these determinations based on their business needs.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Preparing For A Disaster: Determining the Essential Functions That Should Be Up First, https://www.sans.org/reading-room/whitepapers/recovery/preparing-disaster-determining-essential-functions-first-1658

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #186 of 200

Question ID: 1299769

You just received a call from an associate who said he discovered a rogue switch on the network. What is the best course of action to take in response?

- ✗ **A)** Disable unauthorized zone transfers on the DNS server.
- ✗ **B)** Implement DAI on the switch.
- ✗ **C)** Deploy a stateful firewall at the perimeter.
- ✓ **D)** Disable DTP on all switch ports.

Explanation

The best course of action is to disable DTP on all switch ports. Rogue switches can attempt to create a trunk link with a legitimate switch, thus providing access to all VLANs. This can occur if Dynamic Trunking Protocol (DTP) is enabled on the legitimate switch. For this reason, this protocol should be disabled in all switch ports.

You should not implement Dynamic Arp Inspection (DAI). This measure is used to prevent an ARP spoofing attack. This is an attack whereby the attacker pollutes the ARP cache of a neighbor so that the malicious individual receives traffic intended for the neighbor.

You should not deploy a stateful firewall at the perimeter. This measure can help to prevent SYN flood attacks. This attack sends thousands of packets to the target with the SYN flag on. The target answers with SYN/ACK packets and reserves memory for the response, but the responses never come, causing the target to eventually run out of memory.

While you should disable open relay on the DNS servers, that solution will not address a rogue switch. This solution helps prevent a DNS harvesting attack. In a DNS harvesting attack, the attacker obtains access to the DNS records, usually through an unauthorized zone transfer.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

How to secure your Cisco Catalyst switch, https://www.fir3net.com/Switches/Cisco/security-on-cisco-catalyst-switches.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

Question #187 of 200

Question ID: 1299571

Which of the following is the final step in a pen test?

- ✗ **A)** Gather information about attack methods against the target system or device.
- ✓ **B)** Document the results of the penetration test, and report the findings to management with suggestions for remedial action.
- ✗ **C)** Document information about the target system or device.
- ✗ **D)** Execute attacks against the target system or device to gain user and privileged access.

Explanation

The steps in performing a penetration test are as follows:

1. Document information about the target system or device.
2. Gather information about attack methods against the target system or device. This includes performing port scans.
3. Identify the known vulnerabilities of the target system or device.
4. Execute attacks against the target system or device to gain user and privileged access.
5. Document the results of the penetration test, and report the findings to management with suggestions for remedial action.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Explain the importance of threat data and intelligence.

References:

Conducting a Penetration Test on an Organization, https://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 1: Threat Data and Intelligence

Question #188 of 200

Question ID: 1299737

Which of the following statements is FALSE with respect to the communication process among incident response plan stakeholders?

- ✗ **A)** Communication should only take place with those who have been designated beforehand to receive such communications.
- ✗ **B)** The content of these communications should be limited to what is necessary for each stakeholder to perform their role.

- ✓ **C)** All responders should act to encourage the disclosure of any information to parties that are not specified in the communication plan.
- ✗ **D)** All communications that take place between the stakeholders should use a secure communication process.

Explanation

All responders should act to ***prevent*** the disclosure of any information to parties that are not specified in the communication plan. Moreover, all information released to the public and the press should be handled by public relations staff or by persons trained for this type of communication. The timing of all communications should also be specified in the plan.

During an incident, communications should only take place with those who have been designated beforehand to receive such communications. Moreover, the content of these communications should be limited to what is necessary for each stakeholder to perform their role.

All communications that take place between the stakeholders should use a secure communication process to ensure that information is not sniffed. Make use of strong cryptographic mechanisms for these communications.

In addition, you should limit communication to trusted parties. When an incident occurs, you should disclose the incident based on regulatory/legislative requirements. It is important that you prevent the inadvertent release of information.

The communication plan should contain a section on the reporting requirements for all the types of incidents that can occur.

Objective:
Incident Response

Sub-Objective:
Explain the importance of the incident response process.

References:

Incident Response: Communication is Key, http://www.securitymagazine.com/articles/78810-incident-response-communication-is-key-1

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 15: The Incident Response Process

---

Question #189 of 200

Question ID: 1299754

After some issues with damaged evidence during a forensic investigation, the team is reviewing the collection and storage of evidence to improve the process. You are reviewing the features of various tamper-evident bags to be used to hold evidence, such as hard drives and other storage devices. Which of the following is the most important feature?

- ✗ **A)** Made of non-translucent material
- ✗ **B)** Includes form on bag cover
- ✗ **C)** Made of fireproof material
- ✓ **D)** Provides anti-static shielding

Explanation

The most important factor is that it be made of anti-static materials to prevent static buildup from damaging or corrupting any of the contents of the storage device.

While some bags are marketed as fire resistant, there is none that is truly fireproof. Moreover, the heat will probably damage the hard drive anyway.

Most evidence bags do include the form on bag cover, but that is not the most important feature. The most important factor is that it be made of anti-static materials.

It is not important that the bag be made of non-translucent material. The only reason for that would be to prevent seeing what is in the bag and that is relatively unimportant for evidence that is located on the drive and cannot be seen.

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

Packaging, Transportation, and Storage of Digital Evidence, https://www.coursehero.com/file/pkrbjv/Packaging-Transportation-and-Storage-of-Digital-Evidence-2010-September-1/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

---

Question #190 of 200

Question ID: 1299610

You are reviewing the report submitted by a penetration tester. In the report she states that when she used Nmap to scan for the state of ports on the device at 192.168.5.5, she received a state of Filtered for port 80. What does that state mean?

- ✗ **A)** The state of the port cannot be determined.
- ✗ **B)** The application operating on that port is not available to accept connections.
- ✗ **C)** The host at that address is accepting connections to that port.
- ✓ **D)** The port is being blocked by a firewall.

Explanation

When a port is reported by Nmap to be in a Filtered state, it means that the request for the port was blocked by firewall before the request reached the host.

When the host at that address is accepting connections to that port, the state will be reported as Open.

When the application operating on that port is not available to accept connections, the state will be reported as Closed.

When the state of the port cannot be determined, it will be reported as Unfiltered.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

Nmap Network Scanning Reference Guide, Chapter 15: Port Scanning Basics, https://nmap.org/book/man-port-scanning-basics.html

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

---

Question #191 of 200

Question ID: 1299773

You are in the process of completing final documentation of an incident investigation. You are classifying all of the symptoms exhibited during the incident. One of these symptoms of the target machine was unusually high memory consumption. Which of the following incident types could cause this condition?

- ✗ **A)** dictionary attack
- ✓ **B)** malware
- ✗ **C)** data exfiltration
- ✗ **D)** privilege escalation

Explanation

High memory consumption is considered a host-related symptom. It typically indicates the presence of malware. Host-related symptoms are those related to use of resources on the host that will be recorded in the local logs of a device. Unusual processor or memory consumption could be determined by using a resource monitor on the device. If either of these symptoms occurs, you should suspect a malicious process is using the processing resources or memory. The best course of action is to scan the device for malware.

Common host-related symptoms include unusual processing consumption, memory consumption, or drive capacity consumption; unauthorized software and malicious processes; unauthorized changes and privileges; data exfiltration; abnormal operating system (OS) process behavior; file system change or anomaly; registry change or anomaly; and unauthorized scheduled task.

Data exfiltration does not cause high memory usage. This is the theft of data from a device or network. Data exfiltration can be discovered with DLP software, if present. If not, data exfiltration may be discovered only when it falls into the wrong hands. The best course of action is to identify the source of the disclosure if possible and then take disciplinary action, and to employ a DLP solution in the enterprise.

Privilege escalation does not cause high memory usage. Privilege escalation occurs when an attacker escalates privileges in the guest operating system. Unauthorized privileges could be discovered by examining the event log to determine which users are performing these privileged acts. If the user can be identified, then disciplinary action should be taken. If not, the best course of action is to scan the device for malware and for compliance to the baseline. Ensure that users are trained in safe practices and that user accounts are hardened against privilege escalation.

Issues with drive capacity consumption could also be determined by using a resource monitor on the device. When this symptom occurs, you should suspect that some malicious process is filling the drive as part of a DoS attack. Again, the best course of action is to scan the device for malware.

Unauthorized software could be detected with a vulnerability scan that identifies unauthorized software. When discovered, you should suspect that a malicious individual has compromised the device, even if the unauthorized software is not classified as malware. Some legitimate third-party software has known vulnerabilities that put your entire network at risk if it is installed. The best course of action is to re-image the device using the latest snapshot if available. To ensure security, you should use a policy that prevents the installation of unauthorized software, and ensure that users are trained in safe practices.

Malicious processes could be detected by using a tool like Process Explorer. You should suspect the presence of malware if you notice unusual processor, memory, or drive capacity usage on a host. The best course of action is to scan the device using anti-malware software. If you are unable to remove the malicious software, you should re-image the device using the latest snapshot if available and ensure that anti-malware programs are kept up to date.

Unauthorized changes could be discovered by performing a compliance scan in which the current device settings are compared to a baseline. When it occurs, you should suspect that the device has been compromised. You should attempt to restore the device to the correct settings and remove any unauthorized permissions that have been granted. You may need to re-image the device using the latest snapshot if available. Ensure that users are trained in safe practices and that user accounts are hardened against privilege escalation.

The general recommendation for all host-related attacks is to keep anti-malware up to date and ensure that all users are trained in safe practices.

A dictionary attack will not cause high memory usage. This is an attack that uses a text file of words from a dictionary and attempts each as a password to crack into the system or a user account.

You also need to understand the application-related activities that could occur and might signify a security issue, including: anomalous activity, introduction of new accounts, unexpected output, unexpected outbound communication, service interruption, and application log.

Objective:
Incident Response

Sub-Objective:
Given an incident, analyze potential indicators of compromise.

References:

Three Commonly Ignored Signs of a Cyber Attack, https://observable.net/blog/three-commonly-ignored-signs-of-a-cyber-attack/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 17: Analyzing Indicators of Compromise

---

Question #192 of 200

Question ID: 1299756

After arriving at the scene of a security incident, you secure the area and begin collecting evidence. As you begin this process, you record who has handled the evidence, when they handled it, and the order in which the handlers were in possession of the evidence on a form included in the digital forensic toolkit. What is this form called?

✓ **A)** Chain of custody form

- ☒ **B)** Incident response plan
- ☒ **C)** Call list/escalation list
- ☒ **D)** Incident form

Explanation

The chain of custody form will indicate who has handled the evidence, when they handled it, and the order in which the handler were in possession of the evidence.

The incident response plan will not include space for this information, but should be formally designed, well communicated, and followed; therefore it should be included in the kit. The incident response plan should help the investigator by providing the procedures the investigator should follow.

The incident form will be used to describe the incident in detail, but not the handling of the evidence. It should include sections to record CMOS and hard drive information, image archive details, analysis platform information, and other details.

The call/escalation list will indicate under what circumstance individuals should be contacted so as to avoid unnecessary alerts and to keep the process moving in an organized manner. It will not record the handling of the evidence

Objective:
Incident Response

Sub-Objective:
Given a scenario, apply the appropriate incident response procedure.

References:

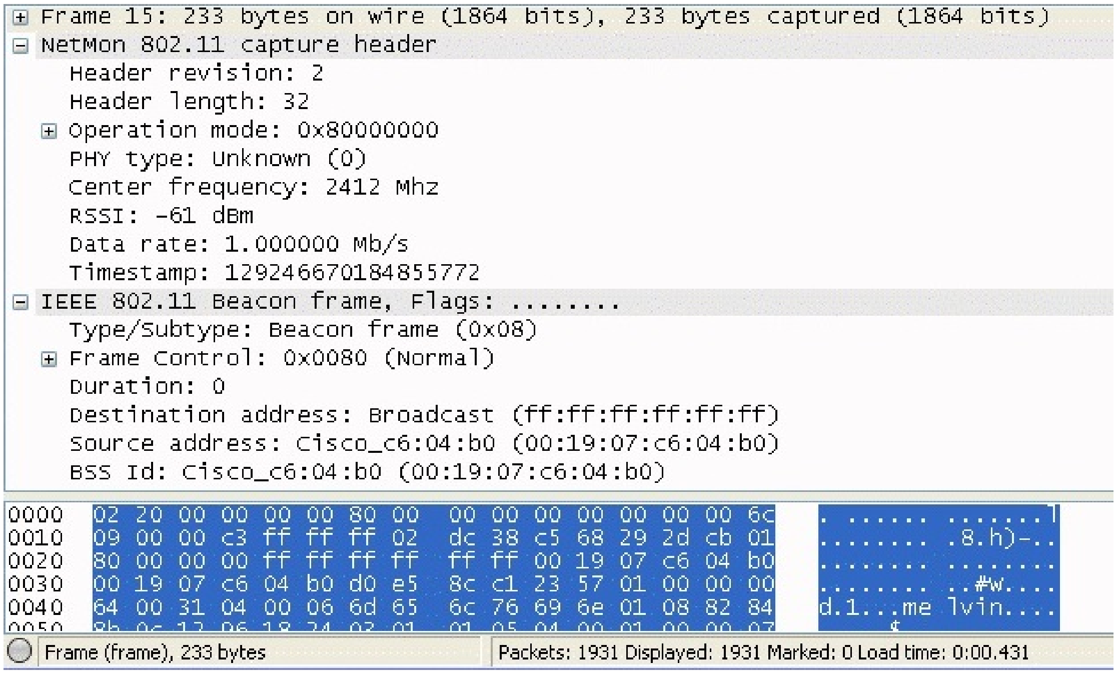
Day 4 - Preparation: What Goes Into a Response Kit,
https://isc.sans.edu/forums/diary/Day+4+Preparation+What+Goes+Into+a+Response+Kit/5125/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 16: Applying the Appropriate Incident Response Procedure

Question #193 of 200

Question ID: 1299609

You were just assigned to shadow a senior cybersecurity analyst as part of your training. Your first encounter with her catches her right in the middle of using a sniffer. She is focused on the packet shown in the figure below:



```
⊞ Frame 15: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits)
⊟ NetMon 802.11 capture header
    Header revision: 2
    Header length: 32
  ⊞ Operation mode: 0x80000000
    PHY type: Unknown (0)
    Center frequency: 2412 Mhz
    RSSI: -61 dBm
    Data rate: 1.000000 Mb/s
    Timestamp: 129246670184855772
⊟ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x08)
  ⊞ Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Cisco_c6:04:b0 (00:19:07:c6:04:b0)
    BSS Id: Cisco_c6:04:b0 (00:19:07:c6:04:b0)

0000  02 20 00 00 00 00 80 00  00 00 00 00 00 00 00 6c   . ...... .......l
0010  09 00 00 c3 ff ff ff 02  dc 38 c5 68 29 2d cb 01   ........ .8.h)-..
0020  80 00 00 00 ff ff ff ff  ff ff 00 19 07 c6 04 b0   ........ ........
0030  00 19 07 c6 04 b0 d0 e5  8c c1 23 57 01 00 00 00   ........ ..#W....
0040  64 00 31 04 00 06 6d 65  6c 76 69 6e 01 08 82 84   d.1...me lvin....
0050  8b 0c 12 96 18 24 03 01  01 05 04 00 01 00 00 07         $

Frame (frame), 233 bytes    Packets: 1931 Displayed: 1931 Marked: 0 Load time: 0:00.431
```

Based on the figure, which of the following statements is TRUE?

- ☓ **A)** The frame is encrypted.
- ☓ **B)** This frame came from a firewall.
- ✓ **C)** She is sniffing a wireless network.
- ☓ **D)** This frame type is very rare.

Explanation

The analyst is sniffing a wireless network. There are several clues that indicate this. Among them are:

- The frame is listed as an 802.11 frame.
- It contains an RSSI value, which indicates signal strength.
- It is described a beacon frame, which are unique to 802.1 networks.

The frame did not come from a firewall. Beacon frames ONLY come from wireless APs and wireless routers.

The frame type is NOT rare. Beacon frames are sent by the AP thousands of times a day.

The frame is not encrypted. If this were the case, you would not be able to read the name Melvin in the data portion in the lower right hand corner of the output.

There are several variables that you must consider when performing a vulnerability scan:

- Wireless versus wired - If you need to scan both, ensure that your scanning tool can scan wirelessly.
- Virtual versus physical - Scanning by IP address is the same for both assets, but you have to get the scanner on the same virtual network as the virtual machines (VMs). It may be necessary to connect the virtual switch to the host NIC or to a physical switch if that is not already the case.
- Internal versus external - External scans will give you an idea of what an attacker might see from the outside. Internal scans may uncover issues with employees.
- On-premises versus cloud - When scanning a cloud, you will probably need the cooperation of the cloud vendor.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, analyze the output from common vulnerability assessment tools.

References:

802.11 Frames: A starter guide to learn wireless sniffer traces, https://supportforums.cisco.com/document/52391/80211-frames-starter-guide-learn-wireless-sniffer-traces

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 4: Analyzing Assessment Output

---

Question #194 of 200

Question ID: 1299627

Your company has a centralized patch deployment system. Which of the following systems is MOST likely to still have patch vulnerabilities?

- ✗ **A)** Mobile devices
- ✗ **B)** Virtual hosts
- ✓ **C)** IoT
- ✗ **D)** VPN

Explanation

Internet of Things (IoT) devices are most likely to still have patch vulnerabilities, even though your company has a centralized patch deployment system. IoT devices are often deployed before their security issues are fully analyzed by the manufacturer or the purchaser. Most of these devices have complicated update processes that are not easily deployed in a centralized patch deployment system.

All of the other devices can usually interoperate with a centralized patch deployment systems. For all systems and applications deployed on a company network, security personnel should ensure that the devices and applications are updated promptly with patches from the vendors.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Explain the threats and vulnerabilities associated with specialized technology.

References:

The Internet of Things Is Wildly Insecure And Often Unpatchable, https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 5: Vulnerabilities Associated with Specialized Technology

---

Question #195 of 200

Question ID: 1299591

After completing the vulnerability scan, you deploy the remediation to all devices in the proper manner. What is the next step you should perform?

- ✗ **A)** Generate reports
- ✓ **B)** Ongoing scanning and continuous monitoring
- ✗ **C)** Establish scanning frequency
- ✗ **D)** Identify requirements

Explanation

After completing remediation, you should perform ongoing scanning and continuous monitoring. The vulnerability scanning cycle is never really over.

The steps of implementing an information security vulnerability management process are as follows:

1. Identify requirements.
2. Establish scanning frequency.
3. Configure the tools to perform the vulnerability scan.
4. Execute the vulnerability scan.
5. Generate reports.
6. Implement remediation.
7. Ongoing scanning and continuous monitoring.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, perform vulnerability management activities.

References:

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 3: Vulnerability Management Activities

Question #196 of 200

Question ID: 1299644

You need to perform a vulnerability scan on all systems on your company's network. You need to ensure that you identify all systems. Which corporate entity should you consult for this information?

- ✗ **A)** Corporate policy
- ✓ **B)** Asset inventory
- ✗ **C)** Regulatory environment
- ✗ **D)** Data classification

Explanation

You should consult the company's asset inventory to identify all systems that need to have a vulnerability scan.

The corporate policy contains the goals and responsibilities for corporate security. The regulatory environment includes any laws and regulations that affect the vulnerability scanning policy. Data classification includes the data types and allows security professionals to determine the controls needed to protect data.

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Asset Inventory: A Necessary First Step in Robust Cyber Security, https://www.qualys.com/offer/asset-inventory-necessary-first-step-robust-cyber-security

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management

---

Question #197 of 200

Question ID: 1299790

Which of the following type of tool is NOT considered a preventive tool used by security analysts?

- ✓ **A)** SIEM
- ✗ **B)** Firewall
- ✗ **C)** IPS
- ✗ **D)** Anti-virus

Explanation

Of the tools listed, security information and event management (SIEM) tools are not considered preventive. They are collective tools that are used to manage event and other logs.

All of the other tools are considered preventive tools. Preventive tools include intrusion prevention systems (IPSs), host IPSs (HIPSs), firewalls, anti-virus, anti-malware, Enhanced Mitigation Experience Toolkit (EMET), Web proxies, and Web application firewalls (WAF).

Objective:
Incident Response

Sub-Objective:
Given a scenario, utilize basic digital forensics techniques.

References:

Security information and event management, http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 18: Digital Forensics Techniques

Question #198 of 200

Question ID: 1299578

The security team is doing some planning for a risk evaluation. Recently some security events went unrecorded because the log was full. Today the team was discussing the proper mitigation for that issue. What part of risk evaluation are they performing?

- ✓ **A)** Technical control review
- ✗ **B)** Incident likelihood analysis
- ✗ **C)** Technical impact review
- ✗ **D)** Operational control review

Explanation

Correcting the log retention setting is a technical control; therefore, this is a part of technical control review. After threats, likelihoods, and impacts are established, the security team should select controls that address the threat but do not cost more than the realized threat would cost. The review of these controls should be an ongoing process.

Since this is a technical control issue and not operational, this is not part of an operational control review. Operational controls are the policies, procedures, and work practices that ether help to prevent the threat or make the threat more likely.

This is not a part of technical impact review. This is the process of assessing the potential impact of an event from a technical standpoint. Once all assets have been identified and their value to the organization has been established, specific threats to each asset are identified. An attempt must be made to establish both the likelihood of the threat being realized as well as the impact to the organization should that occur. This can be done by assigning values like high, medium, and low to the threats to describe their impact and likelihood.

This is not incident likelihood analysis. This is used to establish the likelihood of a threat's realization.

Objective:
Threat and Vulnerability Management

Sub-Objective:
Given a scenario, utilize threat intelligence to support organizational security.

References:

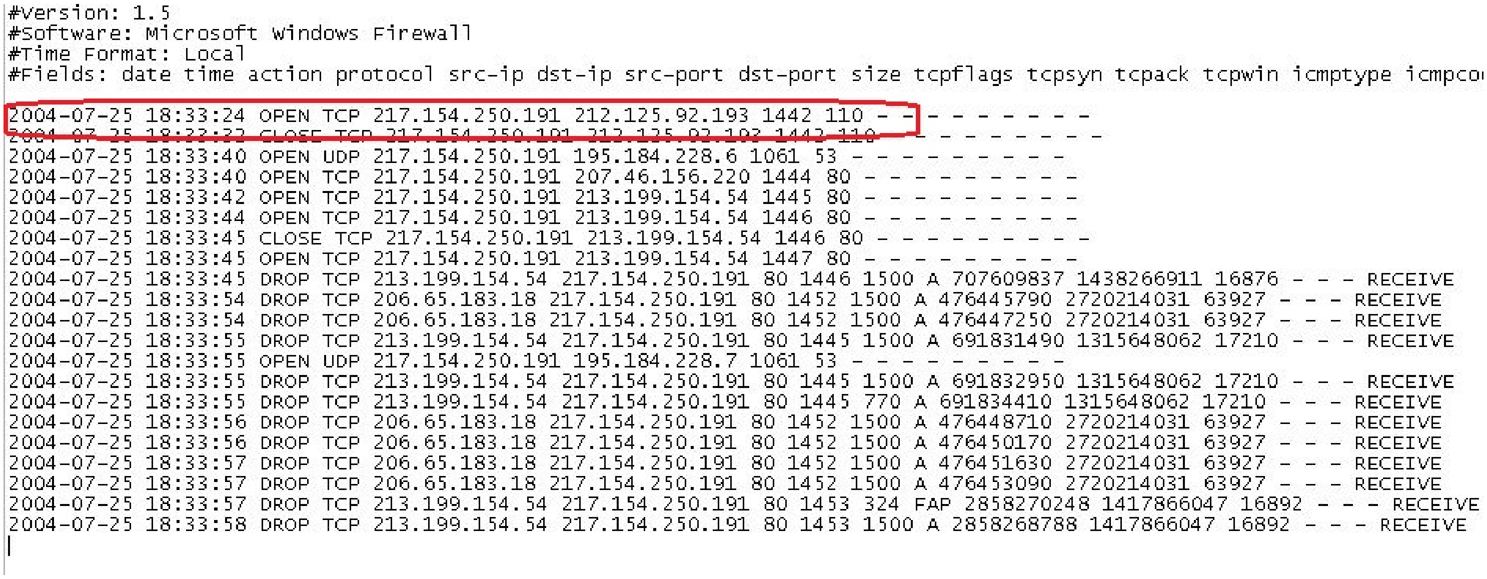
Measuring effectiveness in Information Security Controls, https://www.sans.org/reading-room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 2: Utilizing Threat Intelligence

Question #199 of 200

Question ID: 1299682

One of your more advanced users is trying to learn about the Windows firewall log. He has a portion of the log displayed on this device.



```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpco

2004-07-25 18:33:24 OPEN TCP 217.154.250.191 212.125.92.193 1442 110 - - - - - - - - - -
2004-07-25 18:33:32 CLOSE TCP 217.154.250.191 212.125.92.193 1442 110 - - - - - - - - - -
2004-07-25 18:33:40 OPEN UDP 217.154.250.191 195.184.228.6 1061 53 - - - - - - - - - -
2004-07-25 18:33:40 OPEN TCP 217.154.250.191 207.46.156.220 1444 80 - - - - - - - - - -
2004-07-25 18:33:42 OPEN TCP 217.154.250.191 213.199.154.54 1445 80 - - - - - - - - - -
2004-07-25 18:33:44 OPEN TCP 217.154.250.191 213.199.154.54 1446 80 - - - - - - - - - -
2004-07-25 18:33:45 CLOSE TCP 217.154.250.191 213.199.154.54 1446 80 - - - - - - - - - -
2004-07-25 18:33:45 OPEN TCP 217.154.250.191 213.199.154.54 1447 80 - - - - - - - - - -
2004-07-25 18:33:45 DROP TCP 213.199.154.54 217.154.250.191 80 1446 1500 A 707609837 1438266911 16876 - - - RECEIVE
2004-07-25 18:33:54 DROP TCP 206.65.183.18 217.154.250.191 80 1452 1500 A 476445790 2720214031 63927 - - - RECEIVE
2004-07-25 18:33:54 DROP TCP 206.65.183.18 217.154.250.191 80 1452 1500 A 476447250 2720214031 63927 - - - RECEIVE
2004-07-25 18:33:55 DROP TCP 213.199.154.54 217.154.250.191 80 1445 1500 A 691831490 1315648062 17210 - - - RECEIVE
2004-07-25 18:33:55 OPEN UDP 217.154.250.191 195.184.228.7 1061 53 - - - - - - - - - -
2004-07-25 18:33:55 DROP TCP 213.199.154.54 217.154.250.191 80 1445 1500 A 691832950 1315648062 17210 - - - RECEIVE
2004-07-25 18:33:55 DROP TCP 213.199.154.54 217.154.250.191 80 1445 770 A 691834410 1315648062 17210 - - - RECEIVE
2004-07-25 18:33:56 DROP TCP 206.65.183.18 217.154.250.191 80 1452 1500 A 476448710 2720214031 63927 - - - RECEIVE
2004-07-25 18:33:56 DROP TCP 206.65.183.18 217.154.250.191 80 1452 1500 A 476450170 2720214031 63927 - - - RECEIVE
2004-07-25 18:33:57 DROP TCP 206.65.183.18 217.154.250.191 80 1452 1500 A 476451630 2720214031 63927 - - - RECEIVE
2004-07-25 18:33:57 DROP TCP 206.65.183.18 217.154.250.191 80 1452 1500 A 476453090 2720214031 63927 - - - RECEIVE
2004-07-25 18:33:57 DROP TCP 213.199.154.54 217.154.250.191 80 1453 324 FAP 2858270248 1417866047 16892 - - - RECEIVE
2004-07-25 18:33:58 DROP TCP 213.199.154.54 217.154.250.191 80 1453 1500 A 2858268788 1417866047 16892 - - - RECEIVE
```

Based on this output, which statement is TRUE about the entry that is circled in red?

- ✗ **A)** The transport protocol is providing best effort delivery.
- ✗ **B)** The destination port number is the default number for Telnet.
- ✗ **C)** The frame came from 212.125.92.193.
- ✓ **D)** The source port number is 1442.

Explanation

The source port number is 1442. The last two numbers on the right for the circled line are the source and destination port numbers, respectively, in this case source 1442 and destination 110. These entries were recorded because the firewall is a rule-based firewall, which has access control lists (ACL) configured to control traffic.

The frame did not come from 212.125.92.193. The two values to the left of the port numbers are the source and destination IP addresses. The source IP address is 217.154.250.191, and the destination is 212.125.92.193.

The destination port number is the NOT default number for Telnet. The destination is port 110, which is the default port for POP3.

The transport protocol is NOT providing best effort delivery. The transport protocol is listed to the left of the IP addresses and is TCP, which is guaranteed delivery, not best effort.

Objective:
Security Operations and Monitoring

Sub-Objective:
Given a scenario, analyze data as part of security monitoring activities.

References:

How to Track Firewall Activity With the Windows Firewall Log, http://www.howtogeek.com/220204/how-to-track-firewall-activity-with-the-windows-firewall-log/

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 11: Analyzing Data as Part of Security Monitoring Activities

Question #200 of 200

Question ID: 1299660

Despite the fact the organization performs vulnerability testing on a regular basis with scanning tools, your team still executes manual reviews of relevant logs. While doing so, you notice that a packet with a private IP address was blocked attempting to enter the network. In which of the following logs would you most likely find this entry?

- ✓ **A)** Firewall log
- ✗ **B)** System log
- ✗ **C)** Authentication log
- ✗ **D)** Application log

Explanation

This entry would be in the firewall log as the firewall is typically used to enforced controls at Layer 3. Moreover, it is advisable and quite common to find perimeter firewalls blocking the entry of private IP addresses.

This would not be in any authentication log. These logs identify and authorize entities wishing to access a system or resource and they not typically make this decision at Layer 3.

This would not be in a system log. System logs record operating system events, not security events.

This would not be in an application log. These logs record events about applications and add-on components to the operating system.

Typically, manual review of logs covers the following types:

- Firewall log
- Syslogs
- Authentication logs
- Event logs (which include system and application logs)

Objective:
Software and Systems Security

Sub-Objective:
Given a scenario, apply security solutions for infrastructure management.

References:

Getting the Most out of your Firewall Logs, https://www.sans.org/reading-room/whitepapers/firewalls/firewall-logs-811

CompTIA Cybersecurity Analyst (CySA+) Cert Guide (Certification Guide) 2nd Edition, Chapter 8: Secure Infrastructure Management