Domain 6 - Security Assessment and Testing

Test ID: 178283618

Question #1 of 29

Question ID: 1111759

You are in the process of defining and implementing an information security continuous monitoring (ISCM) program for your organization according to NIST SP 800-137. What is an expected input to defining this program?

✗ **A)** reports on security status

✓ **B)** organizational risk assessment

✗ **C)** automation specification

✗ **D)** reporting requirements

Explanation

The organizational risk assessment is an input to the Define the ISCM strategy step. It is also an input to the Establish the ISCM program step. NIST SP 800-137 guides the development of information security continuous monitoring (ISCM) for federal information systems and organizations. It defines the following steps to establish, implement, and maintain ISCM:

- Define an ISCM strategy.
- Establish an ISCM program.
- Implement an ISCM program.
- Analyze data, and report findings.
- Respond to findings.
- Review and update the ISCM strategy and program.

Reporting requirements is an input to the Establish an ISCM program step. The automation specifications are an input to the Implement an ISCM program step. The reports on security status are an input to the Respond to finding step.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, NIST SP 800-137

NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

Question #2 of 29

Question ID: 1192958

Your company has hired a security firm to test your network's security. What would need to be used outside your network?

- ✓ **A)** penetration tester
- ✗ **B)** port scanner
- ✗ **C)** protocol analyzer
- ✗ **D)** vulnerability scanner

Explanation

A penetration tester would need to be used outside your network. This tests your network's security to see if it can be penetrated. You can only penetrate a network from outside of it.

None of the other tests needs to be used outside your network. A vulnerability scanner checks your network for known vulnerabilities and provides methods for protection against the vulnerabilities. A port scanner identifies ports and services that are available on your network. A protocol analyzer captures packets on your network.

A penetration test originates from outside the network. A vulnerability scan usually originates from within the network.

A penetration test should include the following steps:

The formal steps in the penetration test are as follows:

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

The IP addresses of the computers are usually discovered during a penetration test. As components of the network are discovered, the methods used will be determined.

Objective:
Security Assessment and Testing

Sub-Objective:
Analyze test output and generate report

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Penetration Testing

Penetration Testing Reconnaissance,
http://searchsecuritychannel.techtarget.com/tip/0,289483,sid97_gci1235335,00.html

---

Question #3 of 29

Question ID: 1113994

You must provide SOC 2 and SOC 3 reports on the security, availability, confidentiality, processing integrity, and privacy of operational controls. As part of these reports, you must provide information regarding the disclosure of data to third parties. To which tenet of SOC 2 and SOC 3 does this information apply?

- ✗ **A)** security
- ✓ **B)** privacy
- ✗ **C)** confidentiality
- ✗ **D)** availability

Explanation

Disclosure of data to third parties applies to the privacy tenet of SOC 2 and SOC 3. Privacy includes management, privacy notice, data collections, data use and retention, data access, data quality, and monitoring and enforcement.

Security includes the IT security policy, security awareness, risk assessment, logical and physical access, security monitoring, user authentication, incident management, asset classification, personnel security, and other topics.

Confidentiality includes the confidentiality policy, input confidentiality, data processing confidentiality, output confidentiality, information disclosure, and systems development confidentiality.

Availability includes backup and restoration of data, environmental controls, disaster recovery, business continuity, and availability process.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct or facilitate security audits

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Conduct Audits

---

Question #4 of 29

Question ID: 1105376

During a recent security conference, you attended training that explained the difference between active and passive security monitoring. What is a passive measure that can be used to detect hacker attacks?

- ✗ **A)** connection termination
- ✗ **B)** process termination
- ✗ **C)** firewall reconfiguration
- ✓ **D)** event logging

Explanation

Event logging is a passive measure that can be used to detect hacker attacks. Event logging is considered a passive measure because it does not create obstacles to attacks. Administrators can, however, review log files after an attack to determine the source and the means of the attack. The information obtained from log files can be used to implement active prevention measures. Log files can also be used as legal evidence when prosecuting attackers, so log files should be protected and measures should be taken to ensure their integrity.

Connection termination, firewall reconfiguration, and process termination are active measures for the prevention of hacker attacks; these methods establish obstacles intended to foreclose, or at least limit, the possibility of attack.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Network Vulnerability Scan

---

Question #5 of 29

Question ID: 1105368

You are investigating possible unauthorized access to a Windows Server 2003 computer. The first step in your company's investigation policy states that the current network connections must be documented. Which command should you use?

- ✗ **A)** tracert
- ✗ **B)** ipconfig
- ✗ **C)** ping

✓ **D)** netstat

Explanation

You should use the netstat command. This tool displays incoming and outgoing connections, routing tables, and network interface statistics.

The ping tool is used to test the availability of a computer over a network. You can ping computers based on their DNS host name or IP address.

The ipconfig tool displays a computer's IP address, subnet mask, and default gateway. It can also be used to release and renew a Dynamic Configuration Host Protocol (DHCP) IP address lease. The UNIX equivalent tool is ifconfig.

The tracert tool is used to determine the route a packet takes across a Windows IP network. UNIX computers have a similar tool called traceroute.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

Netstat, http://www.netstat.net/

Question #6 of 29

Question ID: 1105366

Your company must comply with a cybersecurity certification body's requirements. Management has requested that you perform a test prior to applying for this certification. Which type of test should you perform?

✗ **A)** Perform an external assessment or audit using personnel from within the company.

✗ **B)** Perform an internal assessment or audit using personnel from the certification body.

✓ **C)** Perform an internal assessment or audit using personnel from within the company.

✗ **D)** Perform an external assessment or audit using personnel from the certification body.

Explanation

You should perform an internal assessment or audit using personnel from within the company. Internal assessments or audits should be performed first so that personnel can then work on fixing any identified vulnerabilities, risks, or issues.

You should not perform an external assessment or audit of any kind until after you have performed an internal assessment or audit and resolved as many of the issues identified there as possible.

You should not perform an internal or external assessment or audit using personnel from the certification body until after organizational personnel has performed these assessments and worked to fix any identified issues.

Internal assessments or audits are completed from within the enterprise and can be completed by personnel from within the company or a third party. External assessments are completed from outside the enterprise and can be completed by personnel from within the company or a third party. While some certifying bodies will provide personnel to perform the assessment or audit as part of the certification process, some may require that organizations work with a third-party organization to perform the assessment or audit.

Objective:
Security Assessment and Testing

Sub-Objective:
Design and validate assessment, test, and audit strategies

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Design and Validate Assessment and Testing Strategies

---

Question #7 of 29

Question ID: 1192957

You install a network analyzer to capture your network's traffic as part of your company's security policy. Later, you examine the captured packets and discover that only Subnet 1 traffic was captured. You need to capture packets from all four subnets on your network.

What could you do?

a. Install a port scanner.

b. Install the network analyzer on all four subnets.

c. Install a distributed network analyzer.

d. Install the network analyzer on a router.

e. Install the network analyzer on the firewall.

- ✓ **A)** options b and c only
- ✗ **B)** option a
- ✗ **C)** option c and e only
- ✗ **D)** option b
- ✗ **E)** option e
- ✗ **F)** options c and d only
- ✗ **G)** option c
- ✗ **H)** options a and b only
- ✗ **I)** option d

Explanation

You could either install the network analyzer on all four subnets or install a distributed network analyzer. Standard network analyzers only capture packets on the local subnet. To capture packets on a multi-subnet network, you could install the network analyzer on all four subnets. Alternatively, you could purchase a network analyzer that can capture all packets across the subnets. A distributed network analyzer typically consists of a dedicated workstation network analyzer installed on one subnet, and software probes installed on the other subnets.

You should not install a port scanner. A port scanner reports which ports and services are being used on your network.

You should not install the network analyzer on a router. This will only allow you to capture packets on the two subnets connected to the router.

You should not install the network analyzer on the firewall. This will only allow you to capture packets on the subnets connected to the firewall.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

What is a Packet Sniffer?, HYPERLINK "https://www.lifewire.com/what-is-a-packet-sniffer-2487312" \t "sean" http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

---

Question #8 of 29

Question ID: 1105386

Which of the following is NOT part of a penetration test?

✗ **A)** Enumeration

✗ **B)** Exploitation

✓ **C)** Implementation of controls

✗ **D)** Discovery

Explanation

A penetration test does NOT include implementation of controls. Controls are implemented based on the recommendations in the final penetration test report. However, these controls are not implemented as part of the penetration test. It is a separate process or operation.

A penetration test should include the following steps:

The formal steps in the penetration test are as follows:

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

Objective:
Security Assessment and Testing

Sub-Objective:
Collect security process data (e.g., technical and administrative)

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Penetration Testing

---

Question #9 of 29

Question ID: 1105381

Your company's security policy states that passwords should never be transmitted in plain text. You need to determine if this policy is being followed. Which tool should you use?

✗ **A)** password cracker

✓ **B)** protocol analyzer

✗ **C)** vulnerability scanner

✗ **D)** network mapper

Explanation

You should use a protocol analyzer to determine if passwords are being transmitted in plain text. Protocol analyzers capture packets as they are transmitted on the network. If a password is transmitted in plain text, you will be able to see the password in the packet. Protocol analyzers are also called network analyzers or packet sniffers.

A password cracker is used to test the strength of your passwords. It attempts to obtain a password using dictionary or brute force attacks.

A vulnerability scanner tests your network for known vulnerabilities and suggests ways to prevent the vulnerabilities.

A network mapper obtains a visual map of the topology of your network, including all devices on the network.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 5 Identity and Access Management Sniffer Attack

---

Question #10 of 29

Question ID: 1192956

What is the correct definition of penetration testing?

✗ **A)** intrusion by hackers

✗ **B)** security response procedures undertaken for system and application hardening

✗ **C)** security response procedures undertaken to detect brute force attacks

✓ **D)** test procedure performed by security professionals with management approval

Explanation

Penetration testing, which is also called ethical hacking, is performed by security professionals after receiving management approval. When security tools are used by security experts to exploit system vulnerabilities for ethical purposes, it is termed penetration testing or ethical hacking. Ethical hackers find but do not exploit the vulnerabilities they find in an organization's network infrastructure. The primary objective of penetration testing or ethical hacking is to assess the capability of the system to resist attacks and prove that system and network vulnerabilities exist.

Penetration testing involves the use of tools to simulate attacks on the network and on the computer systems after seeking prior approval and authorization from the senior management. Initially, you should define management objectives and conduct configuration reviews, vulnerability assessments, and social engineering. Penetration testing is performed to verify the security flaws that were discovered during the vulnerability assessment, and is limited to testing the impact of the vulnerability on the infrastructure's security. This process enables an organization to take corrective action, such as patching up the systems against vulnerabilities or bugs. A penetration test team reports the findings to the senior management after completing the documentation process. ISS, Ballista, and SATAN are some examples of penetration testing or ethical hacking tools used to identify network and system vulnerabilities.

Intrusion performed by hackers with a malicious intention is termed as hacking or cracking instead of ethical hacking and penetration testing.

Penetration testing is not used to detect attacks, such as brute force attacks. Penetration testing is designed to identify vulnerabilities in the system by using security tools. To detect hacking attacks, you can use either an IDS or a firewall.

Security response procedures undertaken for system and application hardening are undertaken after the security flaws have been identified by using ethical hacking. Security response procedures can be detective or corrective in nature. Examples of security response procedures include analysis of logs and provision of incident responses.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Penetration Testing

---

Question #11 of 29

Question ID: 1192959

You are using a network analyzer to monitor traffic on your network. Users report that sessions are hanging intermittently throughout the day. You suspect that your network is under attack. You decide to use the network analyzer to determine the problem.

Which information should you examine?

- ✓ **A)** packet capture
- ✗ **B)** port statistics
- ✗ **C)** station statistics
- ✗ **D)** protocol statistics

Explanation

You should use packet capture information to examine the sessions that are hanging intermittently throughout the day. You will need to examine the packets being sent and determine which devices failed to respond. A packet capture provides detailed information on each packet on your network.

All of the other options should only be used if you know which protocol, station (device), or port is the cause of the problem.

You should not use protocol statistics for this problem because you are not sure which protocol, if any, is causing the problem.

Objective:
Security Assessment and Testing

Sub-Objective:
Analyze test output and generate report

References:

What is a Packet Sniffer?, HYPERLINK "https://www.lifewire.com/what-is-a-packet-sniffer-2487312" \t "sean" http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

---

Question #12 of 29

Question ID: 1302572

What is a vulnerability scanner?

- ✗ **A)** an application that protects a system against viruses
- ✗ **B)** an application that detects when network intrusions occur and identifies the appropriate personnel
- ✗ **C)** an application that identifies ports and services that are at risk on a network
- ✓ **D)** an application that identifies security issues on a network and gives suggestions on how to prevent the issues

Explanation

A vulnerability scanner is an application that identifies security issues on a network and gives suggestions on how to prevent the issues. Often a vulnerability scanner goes beyond what a port scanner can do.

A port scanner is an application that identifies ports and services that are at risk on a network.

An intrusion detection system (IDS) is an application that detects when network intrusions occur and identifies the appropriate personnel.

A virus scanner is an application that protects a system against viruses.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Vulnerability Assessment

---

Question #13 of 29

Question ID: 1111763

You have been asked to carry out a penetration test on your organization's network. You obtain a footprint of the network. What should you do next?

- ✓ **A)** Perform port scans and resource identification.
- ✗ **B)** Attempt to gain unauthorized access by exploiting the vulnerabilities.
- ✗ **C)** Report to management.
- ✗ **D)** Identify vulnerabilities in systems and resources.

Explanation

You should perform port scans and resource identification.

A penetration test should include the following steps:

- Discovery - Obtain the footprint and information about the target and attack methods that can be used.
- Enumeration - Perform ports scans and resource identification.
- Vulnerability mapping - Identify vulnerabilities in systems and resources.
- Exploitation - Attempt to gain unauthorized access by exploiting the vulnerabilities.
- Report - Report the results to management with suggested countermeasures.

The formal steps in the penetration test are as follows:

- Document information about the target system or device. (This is discovery.)
- Gather information about attack methods against the target system or device. This includes performing port scans. (This is enumeration.)

- Identify the known vulnerabilities of the target system or device. (This is vulnerability mapping.)
- Execute attacks against the target system or device to gain user and privileged access. (This is exploitation.)
- Document the results of the penetration test and report the findings to management, with suggestions for remedial action. (This is reporting.)

Objective:
Security Assessment and Testing

Sub-Objective:
Collect security process data (e.g., technical and administrative)

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Penetration Testing

---

Question #14 of 29

Question ID: 1105394

Your company has implemented a Security Assessment and Testing, strategy that includes an information security continuous monitoring (SCM) program. As part of this program, you must provide a detailed report for users, auditors, and other stakeholders that focuses on security, availability, confidentiality, processing integrity, and privacy. Which report should you provide?

✓ **A)** SOC 2
✗ **B)** SOC 3
✗ **C)** SAS 70
✗ **D)** SOC 1

Explanation

You should provide users, auditors, and other stakeholders with an SOC 2 report. This report focuses on security, availability, confidentiality, processing integrity, and privacy.

SAS 70 focused specifically on risks related to financial reporting. It was retired in 2011.

SOC 1 focuses on financial reporting risks and controls. It is a detailed report for users and auditors.

SOC 3 is a short report for public dissemination that focuses on security, availability, confidentiality, processing integrity, and privacy.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct or facilitate security audits

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Conduct Audits

---

Question #15 of 29

Question ID: 1111762

Which methodology is used to analyze operating system vulnerabilities in a penetration testing project?

✗ **A)** Open Web Application Security Project methodology
✗ **B)** vulnerability assessment and recovery methodology
✗ **C)** operating system fingerprint methodology
✓ **D)** flaw hypothesis methodology

Explanation

The flaw hypothesis methodology is used to analyze operating system vulnerabilities in a penetration testing project. The flaw hypothesis methodology refers to a system analysis and penetration technique in which the specifications and documentation for an operating system are analyzed to compile a list of possible flaws. The flaws are prioritized according to the following considerations:

- existence of a flaw
- ease with which a flaw can be exploited
- extent of control or compromise the flaw can lead to

The prioritized list is used to perform penetration testing of operating systems.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

Analysis of Remote Active Operating System Fingerprinting Tools, http://www.packetwatch.net/documents/papers/osdetection.pdf

Guide to Penetration Testing, Part 5: Testing Methodology and Standards, http://searchnetworking.techtarget.com/general/0,295582,sid7_gci1083724,00.html

Question #16 of 29

Question ID: 1111758

During which step of the NIST SP 800-137 are the decisions on risk responses made?

✗ **A)** Review and update the monitoring program and strategy.

✗ **B)** Establish the ISCM program.

✗ **C)** Define the ISCM strategy.

✓ **D)** Respond to findings.

Explanation

The decisions on risk responses are made during the Respond to findings step of the NIST SP 800-137. They are considered an output of this step.

NIST SP 800-137 guides the development of information security continuous monitoring (ISCM) for federal information systems and organizations. It defines the following steps to establish, implement, and maintain ISCM:

- Define an ISCM strategy.
- Establish an ISCM program.
- Implement an ISCM program.
- Analyze data, and report findings.
- Respond to findings.
- Review and update the ISCM strategy and program.

The decisions on risk responses are not part of any of the other listed steps of the NIST SP 800-137.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, NIST SP 800-137

NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

Question #17 of 29

Question ID: 1105388

You are designing the reporting solution for your company's information security continuous monitoring (SCM) program. You need to create a mechanism whereby end users are able to create the reports that they need. You set up the business intelligence (BI) solution, connect it to the data sources, establish security settings, and determine which objects users can access. Which type of reporting are you implementing?

✗ **A)** data feed

✗ **B)** recurring reporting

✗ **C)** automated reporting

✓ **D)** ad-hoc reporting

Explanation

Ad-hoc reporting is being used when you set up the business intelligence (BI) solution, connect it to the data sources, establish security settings, and determine which objects users can access.

Automated reporting delivers information by setting up in advance the reports that need to be run and then automatically generating and delivering these reports. With automated reporting, users do not create the reports they need.

Recurring reporting is very similar to automated reporting. It allows reports to be generated on a regular basis for information that is always needed. With recurring reporting, users do not create the reports they need.

A data feed allows users to receive updated data from data sources. A web feed or RSS feed are popular forms of data feeds. With data feeds, users receive information, not reports.

Objective:
Security Assessment and Testing

Sub-Objective:
Analyze test output and generate report

References:

Ad-hoc reporting, https://www.logianalytics.com/resources/bi-encyclopedia/ad-hoc-reporting/

Question #18 of 29

Question ID: 1114767

Which programs are tools used to obtain user passwords?

a. L0phtCrack

b. John the Ripper

c. Tripwire

d. Crack

- ✗ **A)** option c
- ✗ **B)** option d
- ✗ **C)** options a, b, and c only
- ✗ **D)** options a and b only
- ✗ **E)** option b
- ✓ **F)** options a, b and d only
- ✗ **G)** option a

Explanation

L0phtCrack, John the Ripper, and Crack are tools used to obtain user passwords.

Tripwire is NOT used to obtain user passwords.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Penetration Testing

---

Question #19 of 29

Question ID: 1114769

Which statement is true of event logging?

- ✓ **A)** Only system administration, internal audit, and security staff should have access to the log files.
- ✗ **B)** System and application logs should be delivered over the network in plain text.
- ✗ **C)** System and application logs should permit modification of the existing entries.
- ✗ **D)** Logging should be performed once a day.

Explanation

To ensure confidentiality and integrity of log records, only system administration staff, internal audit staff, and security staff should have access to log files for the purposes of analysis and review. Logging enables the network administration staff to detect vulnerable points in a network, identify performance issues, log suspicious activity from a specific user or a system, and identify a security breach. It is important that the logs be reviewed periodically and archived. The period of a log archive depends on the sensitivity of data and the organization's retention policy.

Logging should not be performed once a day. Logging should be permanently enabled on all computer systems and infrastructure equipment, such as routers and firewalls, to constantly monitor the operations. The events can be logged for both Windows and UNIX systems. In a UNIX system, the events logged include the use of Setuid and Setgid. In Windows systems, the events logged include successful and unsuccessful login attempts. For both systems, file permission changes should also be logged.

System and application logs should not permit modification of the existing entries. Logging provides detailed information about the system resource usage and the system activities. In the event of an intrusion, logging provides the system logs and the audit trails, helping to detect the source of an attack.

System and application logs should not be delivered over the network in plain text. If log data is transferred over a WAN link, it is recommended that such information be encrypted while it travels over the network. Log encryption ensures the confidentiality and integrity of the information. Other recommendations while transferring log data over a WAN link are as follows:

Logs should be centralized to enable easy collection and analysis.

All computer systems and infrastructure equipment must have their clock synchronized to a central timeserver, and the log entries should contain time and date stamps.

Log files should be stored on a secure system by using stringent access control to prevent modification, destruction, or deletion.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 5 Identity and Access Management Accountability

---

Question #20 of 29

Question ID: 1111764

What is the final step in a penetration test?

✗ **A)** Execute attacks against the target system.

✗ **B)** Implement the appropriate controls to prevent the identified issues in the report.

✓ **C)** Document the results, and report the findings to management.

✗ **D)** Identify the known vulnerabilities of the target system.

Explanation

The final step in a penetration test is to document the results and report the findings to management.

A penetration test does not include implementing the appropriate controls to prevent the identified issues in the report. As part of a penetration test, you should only provide recommendations. Implementing any of the suggested recommendations is separate from the penetration test and has its own process.

A penetration test should include the following steps:

- Discovery - Obtain the footprint and information about the target and attack methods that can be used.
- Enumeration - Perform ports scans and resource identification.
- Vulnerability mapping - Identify vulnerabilities in systems and resources.
- Exploitation - Attempt to gain unauthorized access by exploiting the vulnerabilities.
- Report - Report the results to management with suggested countermeasures.
- Discovery - Obtain the footprint and information about the target and attack methods that can be used.
- Enumeration - Perform ports scans and resource identification.
- Vulnerability mapping - Identify vulnerabilities in systems and resources.
- Exploitation - Attempt to gain unauthorized access by exploiting the vulnerabilities.
- Report - Report the results to management with suggested countermeasures.
- Discovery - Obtain the footprint and information about the target and attack methods that can be used.
- Enumeration - Perform ports scans and resource identification.
- Vulnerability mapping - Identify vulnerabilities in systems and resources.
- Exploitation - Attempt to gain unauthorized access by exploiting the vulnerabilities.
- Report - Report the results to management with suggested countermeasures.

The formal steps in the penetration test are as follows:

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

Objective:
Security Assessment and Testing

Sub-Objective:
Collect security process data (e.g., technical and administrative)

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Penetration Testing

---

Question #21 of 29

Question ID: 1192960

You are using a network analyzer to monitor traffic on your network. A user reports trouble communicating with the file server. You suspect that the file server is the victim of a denial of service attack. You decide to use the network analyzer to determine the problem.

Which information should you examine?

- ✗ **A)** packet capture
- ✗ **B)** port statistics
- ✓ **C)** station statistics
- ✗ **D)** protocol statistics

Explanation

You should use station (device) statistics to examine the communication between the user's computer and the file server. Both computers' traffic should be examined to determine exactly where the communication fails.

You should not use protocol statistics because you do not know which protocol, if any, is causing the problem.

You should not use packet capture information because this will provide information on all packets. You know which computers are part of the problem. Therefore, examining station statistics would provide information that is more relevant.

You should not use port statistics because you do not know which port, if any, is causing the problem.

Objective:
Security Assessment and Testing

Sub-Objective:
Analyze test output and generate report

References:

What is a Packet Sniffer?, HYPERLINK "https://www.lifewire.com/what-is-a-packet-sniffer-2487312" \t "sean" http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

---

Question #22 of 29

Question ID: 1105380

Which type of vulnerability assessment is more likely to demonstrate the success or failure of a possible attack?

- ✓ **A)** double-blind test
- ✗ **B)** blind test
- ✗ **C)** targeted test
- ✗ **D)** penetration test

Explanation

A double-blind test is more likely to demonstrate the success or failure of a possible attack. In this test, the security team of the network being tested does NOT know about the test. This test evaluates how the team reacts to the attack.

In a blind test, the security team of the network being tested knows about the test. Assessors have only publicly available information on the network.

In a targeted test, tests are carried out on specific areas or systems.

In a penetration test, the security of a computer or network is tested to discover vulnerabilities and weaknesses. Blind tests, double-blind tests, and targeted tests are specific types of penetration tests.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Penetration Testing

---

Question #23 of 29

Question ID: 1105375

Which tool is used to perform a vulnerability test?

- ✗ **A)** penetration test

✗ **B)** black box test

✗ **C)** white box test

✓ **D)** scanning tool

Explanation

A scanning tool is used to perform a vulnerability test. A vulnerability test identifies the vulnerabilities in a network. After the vulnerabilities are identified, a penetration test exploits the identified vulnerabilities to prove that the vulnerability actually exists.

A penetration test has several ways of exploiting system vulnerabilities. A white box test is a penetration test where the ethical hacker is given network and system details to better target the attack. A black box test is performed "in the dark," meaning the ethical hacker has no previous knowledge of the network or system.

A vulnerability test and a penetration test are NOT the same thing. A vulnerability test leads to the penetration test. You must first identify the vulnerabilities in the vulnerability test and then attempt to exploit the vulnerabilities using a penetration test.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Network Vulnerability Scan

---

Question #24 of 29

Question ID: 1111760

You are defining and implementing an information security continuous monitoring (ISCM) program for your organization according to NIST SP 800-137. You are currently collecting the security-related information required for metrics, assessments, and reporting. Which step of NIST SP 800-137 are you completing?

✗ **A)** Establish an ISCM program.

✓ **B)** Implement an ISCM program.

✗ **C)** Define an ISCM strategy.

✗ **D)** Analyze the data collected, and report findings.

Explanation

You are completing the Implement an ISCM program step of NIST SP 800-137. NIST SP 800-137 guides the development of and provides information about information security continuous monitoring (ISCM) for federal information systems and organizations. It defines the following steps to establish, implement, and maintain ISCM:

- Define an ISCM strategy.
- Establish an ISCM program.
- Implement an ISCM program.
- Analyze data, and report findings.
- Respond to findings.
- Review and update the ISCM strategy and program.

Defining an ISCM strategy involves determining your organization's official ISCM strategy. Establishing an ISCM program determines the metrics, monitoring, and assessment frequencies in addition to the ISCM architecture. Analyzing the data collected and reporting findings determines any issues and implements the appropriate response. Responding to the findings involves implementing new controls that address any findings you have. Reviewing and updating the monitoring program involves ensuring that the program is still relevant and allows you to make any necessary changes to the program.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, NIST SP 800-137

NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

---

Question #25 of 29

Question ID: 1111757

Match the tools on the left with the descriptions given on the right.

{UCMS id=5721518380154880 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:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Conduct Security Control Testing

---

Question #26 of 29

Question ID: 1105378

Which tool is NOT a back door application?

✗ **A)** Back Orifice
✓ **B)** Nessus
✗ **C)** Masters Paradise
✗ **D)** NetBus

Explanation

Nessus is NOT a back door application. It is a network vulnerability scanner.

Back Orifice, NetBus, and Masters Paradise are all back door applications. These applications work by installing a client application on the attacked computer and then using a remote application to gain access to the attacked computer.

Back doors can also be mechanisms created by hackers to gain network access at a later time. Back doors are very hard to trace, as an intruder will often create several avenues into a network to be exploited later. The only real way to be sure these avenues are closed after an attack is to restore the operating system from the original media, apply the patches, and restore all data and applications

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Vulnerability Assessment

Nessus, http://www.nessus.org/nessus/

Information on Back Orifice and NetBus, http://www.symantec.com/avcenter/warn/backorifice.html

---

Question #27 of 29

Question ID: 1113992

You have been hired as a security engineer for a new federal government agency. You have been asked to implement an information security continuous monitoring (ISCM) program for the agency. Which standard should you consult?

✗ **A)** NIST SP 800-92
✗ **B)** NIST SP 800-121
✓ **C)** NIST SP 800-137
✗ **D)** NIST SP 800-53

Explanation

You should consult NIST SP 800-137 for information about security continuous monitoring (ISCM) for federal information systems and organizations. This standard defines the following steps to establish, implement, and maintain ISCM:

- Define an ISCM strategy.
- Establish an ISCM program.
- Implement an ISCM program.
- Analyze data, and report findings.
- Respond to findings.
- Review and update the ISCM strategy and program.

NIST SP 800-53 covers the security and privacy controls for federal information systems and organizations. NIST SP 800-92 covers the guidelines for computer security log management. NIST SP 800-121 covers the guidelines for Bluetooth security.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct security control testing

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, NIST SP 800-137

NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

---

Question #28 of 29

Question ID: 1105393

You must provide SOC 2 and SOC 3 reports on the security, availability, confidentiality, processing integrity, and privacy of operational controls. As part of these reports, you must provide information regarding the backup and restoration of data. To which tenet of SOC 2 and SOC 3 does this information apply?

✗ **A)** privacy
✗ **B)** confidentiality
✓ **C)** availability
✗ **D)** security

Explanation

Backup and restoration of data applies to the availability tenet of the SOC 2 and SOC 3 reports. Availability also includes environmental controls, disaster recovery, business continuity, and availability process.

Privacy includes management, privacy notice, data collections, data use and retention, data access, data disclosure to third parties, data quality, and monitoring and enforcement.

Security includes the IT security policy, security awareness, risk assessment, logical and physical access, security monitoring, user authentication, incident management, asset classification, personnel security, and other topics.

Confidentiality includes the confidentiality policy, input confidentiality, data processing confidentiality, output confidentiality, information disclosure, and systems development confidentiality.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct or facilitate security audits

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Conduct Audits

Question #29 of 29

Question ID: 1105391

You have been asked to manage your company's information security continuous monitoring (ISCM) program. Which of the following statements regarding automated versus manual reporting is FALSE?

✗ **A)** Automated tools recognize patterns and relationships that may escape the notice of human analysts or manual monitoring.

✓ **B)** Manual tools are more thorough in their reporting than automated methods.

✗ **C)** Automated tools improve the reliability of monitoring security-related information.

✗ **D)** Automated tools lower the costs of monitoring security-related information.

Explanation

Manual tools are NOT more thorough in their reporting than automated methods.

All of the other statements are true. Automated tools recognize patterns and relationships that may escape the notice of human analysts or manual monitoring. Automated tools lower the costs and improve the reliability of monitoring security-related information.

Objective:
Security Assessment and Testing

Sub-Objective:
Conduct or facilitate security audits

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, NIST SP 800-137