

# CompTIA

## Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam



**NEW QUESTION 1**

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

- A. Human resources
- B. Public relations
- C. Marketing
- D. Internal network operations center

**Answer: B**

**NEW QUESTION 2**

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

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

**Answer: D**

**NEW QUESTION 3**

An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC. Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

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

**Answer: B**

**NEW QUESTION 4**

After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:

Port	State	Service	Version
80/tcp	open	http	Apache httpd 2.2.14
111/udp	open	rpcbind	
443/tcp	filtered	https	Apache httpd 2.2.14
2222/tcp	open	ssh	OpenSSH 5.3p1 Debian
3306/tcp	open	mysql	5.5.40-0ubuntu0.14.1

Which of the following suggests the system that produced output was compromised?

- A. Secure shell is operating of compromise on this system.
- B. There are no indicators of compromise on this system.
- C. MySQL services is identified on a standard PostgreSQL port.
- D. Standard HTP is open on the system and should be closed.

**Answer: B**

**NEW QUESTION 5**

A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentiality protection. Which of the following is the BEST technical security control to mitigate this risk?

- A. Switch to RADIUS technology
- B. Switch to TACACS+ technology.
- C. Switch to 802.1X technology
- D. Switch to the WPA2 protocol.

**Answer: B**

**NEW QUESTION 6**

Which of the following should be found within an organization's acceptable use policy?

- A. Passwords must be eight characters in length and contain at least one special character.
- B. Customer data must be handled properly, stored on company servers, and encrypted when possible
- C. Administrator accounts must be audited monthly, and inactive accounts should be removed.
- D. Consequences of violating the policy could include discipline up to and including termination.

**Answer: D**

**NEW QUESTION 7**

A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

- A. alert udp any any → root any → 21
- B. alert tcp any any → any 21 (content:"root")
- C. alert tcp any any → any root 21
- D. alert tcp any any → any root (content:"ftp")

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

#### NEW QUESTION 8

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

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

**Answer: B**

#### NEW QUESTION 9

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

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

**Answer: AD**

#### NEW QUESTION 10

A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future. Which of the following would be the BEST solution to recommend to the director?

- A. Install a data loss prevention system, and train human resources employees on its use
- B. Provide PII training to all employees at the company
- C. Encrypt PII information.
- D. Enforce encryption on all emails sent within the company
- E. Create a PII program and policy on how to handle data
- F. Train all human resources employees.
- G. Train all employees
- H. Encrypt data sent on the company network
- I. Bring in privacy personnel to present a plan on how PII should be handled.
- J. Install specific equipment to create a human resources policy that protects PII data
- K. Train company employees on how to handle PII data
- L. Outsource all PII to another company
- M. Send the human resources director to training for PII handling.

**Answer: A**

#### NEW QUESTION 10

An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server. Which of the following is MOST likely to be a false positive?

- A. OpenSSH/OpenSSL Package Random Number Generator Weakness
- B. Apache HTTP Server Byte Range DoS
- C. GDI+ Remote Code Execution Vulnerability (MS08-052)
- D. HTTP TRACE / TRACK Methods Allowed (002-1208)
- E. SSL Certificate Expiry

**Answer: E**

#### NEW QUESTION 11

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

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

**Answer: D**

#### NEW QUESTION 15

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

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

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

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

**Answer: B**

#### NEW QUESTION 18

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

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

**Answer: A**

#### NEW QUESTION 21

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

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

**Answer: B**

#### NEW QUESTION 26

Which of the following MOST accurately describes an HSM?

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

**Answer: A**

#### NEW QUESTION 27

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

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

**Answer: B**

#### NEW QUESTION 32

It is important to parameterize queries to prevent:

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

Answer: A

NEW QUESTION 37

A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking `http://<malwaresource>/a.php` in a phishing email. To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the.

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

Answer: C

NEW QUESTION 39

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

The company's hardening guidelines indicate the following:

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

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

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

Part 1

Scan Data	Compliance Report
<div>AppServ1AppServ2AppServ3AppServ4</div> <pre>root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443  HTTP/1.1 200 OK Date: Wed, 26 Jun 2019 21:15:15 GMT Server: Apache/2.4.48 (CentOS) Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT ETag: "13520-58c407930177d" Accept-Ranges: bytes Content-Length: 79136 Vary: Accept-Encoding Cache-Control: max-age=3600 Expires: Wed, 26 Jun 2019 22:15:15 GMT Content-Type: text/html  root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT  Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68) Host is up (0.042s latency). rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com PORT      STATE SERVICE 443/tcp   open  https   ssl-enum-ciphers:     TLSv1.2:       ciphers:         TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong         TLS_RSA_WITH_AES_128_CBC_SHA - strong         TLS_RSA_WITH_AES_128_GCM_SHA256 - strong         TLS_RSA_WITH_AES_256_CBC_SHA - strong         TLS_RSA_WITH_AES_256_GCM_SHA384 - strong       compressors:         NULL  _  least strength: strong  Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds  root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT  Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68) Host is up (0.15s latency). rDNS record for 10.21.4.68: appsrv1.fictionalorg.com PORT      STATE SERVICE 80/tcp    open  http 443/tcp    open  https  Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds</pre>	<p>Fill out the following report based on your analysis of the scan data.</p> <ul style="list-style-type: none"><li><input type="checkbox"/> AppServ1 is only using TLS 1.2</li><li><input type="checkbox"/> AppServ2 is only using TLS 1.2</li><li><input type="checkbox"/> AppServ3 is only using TLS 1.2</li><li><input type="checkbox"/> AppServ4 is only using TLS 1.2</li><li><input type="checkbox"/> AppServ1 is using Apache 2.4.18 or greater</li><li><input type="checkbox"/> AppServ2 is using Apache 2.4.18 or greater</li><li><input type="checkbox"/> AppServ3 is using Apache 2.4.18 or greater</li><li><input type="checkbox"/> AppServ4 is using Apache 2.4.18 or greater</li></ul>



Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

Compliance Report

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

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

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

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

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

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

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

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

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

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

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

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

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

Compliance Report

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

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

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

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

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

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

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

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

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

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

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

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



Part 1

Scan Data	Compliance Report
<p>AppServ1 AppServ2 AppServ3 AppServ4</p> <pre>root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443  HTTP/1.1 200 OK Date: Wed, 26 Jun 2019 21:15:15 GMT Server: Apache/2.4.48 (CentOS) Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT ETag: "13520-58c406780177e" Accept-Ranges: bytes Content-Length: 79136 Vary: Accept-Encoding Cache-Control: max-age=3600 Expires: Wed, 26 Jun 2019 22:15:15 GMT Content-Type: text/html  root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT  Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71) Host is up (0.042s latency). rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com PORT      STATE SERVICE 443/tcp   open  https   TLSv1.2:     ciphers:       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong       TLS_RSA_WITH_AES_128_CBC_SHA - strong       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong       TLS_RSA_WITH_AES_256_CBC_SHA - strong       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong     compressors:       NULL  _  least strength: strong  Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds  root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71) Host is up (0.15s latency). rDNS record for 10.21.4.71: appsrv4.fictionalorg.com PORT      STATE SERVICE 80/tcp    open  http 443/tcp    open  https 8675/tcp  open  ssh  Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds</pre>	<p>Fill out the following report based on your analysis of the scan data.</p> <ul style="list-style-type: none"><li><input type="checkbox"/> AppServ1 is only using TLS 1.2</li><li><input type="checkbox"/> AppServ2 is only using TLS 1.2</li><li><input type="checkbox"/> AppServ3 is only using TLS 1.2</li><li><input type="checkbox"/> AppServ4 is only using TLS 1.2</li><li><input type="checkbox"/> AppServ1 is using Apache 2.4.18 or greater</li><li><input type="checkbox"/> AppServ2 is using Apache 2.4.18 or greater</li><li><input type="checkbox"/> AppServ3 is using Apache 2.4.18 or greater</li><li><input type="checkbox"/> AppServ4 is using Apache 2.4.18 or greater</li></ul>

Part 2

Scan Data	Configuration Change Recommendations
<p>AppServ1 AppServ2 AppServ3 AppServ4</p> <div></div>	<p>+ Add recommendation for</p> <div><div>AppSrv1</div><div>AppSrv2</div><div>AppSrv3</div><div>AppSrv4</div></div>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Part 1 Answer

Check on the following:

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



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

### Scan Data

AppServ1
AppServ2
AppServ3
AppServ4

```

root@INF0SEC:~# curl --head appsrv2.fictionalorg.com:443

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

root@INF0SEC:~# nmap --script ssl-enum-ciphers appsrv2.fictionalorg.com -p 443

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

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
| ssl-enum-ciphers:
|_ TLSv1.0:

```

### Configuration Change Recommendations

+ Add Recommendation for AppSrv2

Server
AppSrv2

Service
Apache Version

Config Change
Upgrade Version

Server
AppSrv3
+

Service
HTTPD Security

Config Change
Restrict To TLS 1.2

Server
AppSrv4
+

Service
SSH

Config Change
Remove or Disable

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

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

NEW QUESTION 46

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

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

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

**NEW QUESTION 51**

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

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

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

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

**Answer: D**

#### NEW QUESTION 55

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

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

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

**Answer: AC**

#### NEW QUESTION 58

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

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

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

**Answer: A**

#### NEW QUESTION 59

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

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

**Answer: B**

#### NEW QUESTION 63

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities.

Which of the following would be BEST to implement to alleviate the CISO's concern?

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

**Answer: D**

#### NEW QUESTION 67

Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

- A. Self-encrypting drive

- B. Bus encryption
- C. TPM
- D. HSM

**Answer:** A

#### NEW QUESTION 72

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

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

**Answer:** A

#### NEW QUESTION 75

An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.

Which of the following would BEST identify potential indicators of compromise?

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

**Answer:** C

#### NEW QUESTION 77

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

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

**Answer:** A

#### NEW QUESTION 82

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

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

**Answer:** C

#### NEW QUESTION 83

An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework. At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?

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

**Answer:** A

#### NEW QUESTION 87

A security analyst is reviewing the following web server log:

```
GET %2F..%2F..%2F..%2F..%2F..%2F..%2F../etc/passwd
```

Which of the following BEST describes the issue?

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

**Answer:** A

#### NEW QUESTION 92

A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in 1marketingpartners.com Below is the existing SPF record:

```
v=spf1 a mx -all
```

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

A)

```
v=spf1 a mx redirect:mail.marketingpartners.com ?all
```

B)

```
v=spf1 a mx include:mail.marketingpartners.com -all
```

C)

```
v=spf1 a mx +all
```

D)

```
v=spf1 a mx include:mail.marketingpartners.com ~all
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer:** B

#### NEW QUESTION 94

Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

- A. Reverse engineering
- B. Fuzzing
- C. Penetration testing
- D. Network mapping

**Answer:** C

#### NEW QUESTION 97

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic. Which of the following would BEST accomplish this goal?

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

**Answer:** B

#### NEW QUESTION 98

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

Which of the following will remediate this software vulnerability?

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

**Answer:** D

#### NEW QUESTION 99

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

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

**Answer:** D

#### NEW QUESTION 103

An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company. Which of the following technical controls would BEST accomplish this goal?

- A. DLP



- B. Encryption
- C. Data masking
- D. SPF

**Answer:** A

#### NEW QUESTION 108

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

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

**Answer:** A

#### NEW QUESTION 109

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

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

**Answer:** C

#### NEW QUESTION 112

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

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

**Answer:** E

#### NEW QUESTION 115

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

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

**Answer:** D

#### NEW QUESTION 116

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

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

**Answer:** D

#### NEW QUESTION 119

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

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

**Answer:** A

#### NEW QUESTION 122

A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached.

Which of the following is the NEXT step the analyst should take to address the issue?

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

**Answer: B**

#### NEW QUESTION 126

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

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

**Answer: D**

#### NEW QUESTION 127

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

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

**Answer: D**

#### NEW QUESTION 131

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

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

**Answer: E**

#### NEW QUESTION 134

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

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

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

**Answer: A**

#### NEW QUESTION 138

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

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

**Answer: B**

#### NEW QUESTION 143

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

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

**Answer:** A

#### NEW QUESTION 146

A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review.

Which of the following commands would MOST likely indicate if the email is malicious?

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

**Answer:** A

#### NEW QUESTION 151

A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

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

**Answer:** B

#### NEW QUESTION 155

A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

- A. Review the firewall logs.
- B. Review syslogs from critical servers.
- C. Perform fuzzing.
- D. Install a WAF in front of the application server.

**Answer:** C

#### NEW QUESTION 159

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

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

**Answer:** D

#### NEW QUESTION 164

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

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

**Answer:** D

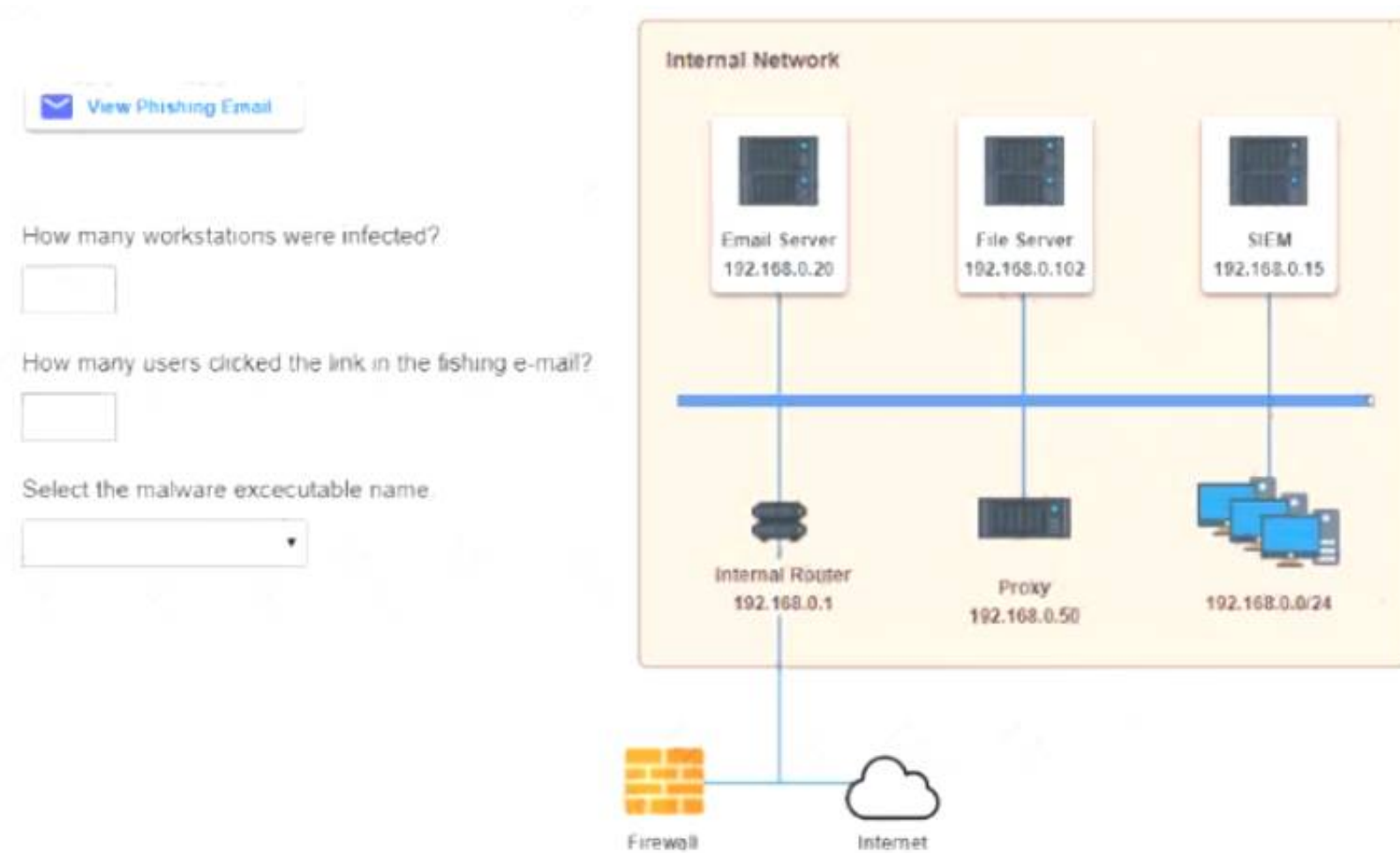
#### NEW QUESTION 168

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

##### INSTRUCTIONS

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 or the malware?



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Select the following answer as per diagram below:

**NEW QUESTION 169**

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

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

**Answer:** A

**NEW QUESTION 174**

A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch. Which of the following is the MOST appropriate threat classification for these incidents?

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

**Answer:** B

**NEW QUESTION 177**

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

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

**Answer:** D

**NEW QUESTION 180**

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

Antivirus is installed on the remote host:

Installation path: C:\Program Files\AVProduct\Win32\ Product Engine: 14.12.101

Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.

The engine version is out of date. The oldest supported version from the vendor is 4.2.11. The analyst uses the vendor's website to confirm the oldest supported



version is correct. Which of the following BEST describes the situation?

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

**Answer: C**

#### NEW QUESTION 184

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

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

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

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

**Answer: B**

#### NEW QUESTION 188

A network attack that is exploiting a vulnerability in the SNMP is detected. Which of the following should the cybersecurity analyst do FIRST?

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

**Answer: A**

#### NEW QUESTION 193

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

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

**Answer: A**

#### NEW QUESTION 198

Which of the following technologies can be used to house the entropy keys for task encryption on desktops and laptops?

- A. Self-encrypting drive
- B. Bus encryption
- C. TPM
- D. HSM

**Answer: A**

#### NEW QUESTION 200

During an investigation, an incident responder intends to recover multiple pieces of digital media. Before removing the media, the responder should initiate:

- A. malware scans.
- B. secure communications.
- C. chain of custody forms.
- D. decryption tools.

**Answer: C**

#### NEW QUESTION 205

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

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

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

**Answer: D**

**NEW QUESTION 210**

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

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

**Answer: C**

**NEW QUESTION 214**

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

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

**Answer: A**

**NEW QUESTION 216**

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

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

**Answer: AC**

**NEW QUESTION 219**

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

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

**Answer: D**

**NEW QUESTION 222**

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

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

**Answer: D**

**NEW QUESTION 223**

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

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

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

- A. Run `crontab -r; rm -rf /tmp/.t` to remove and disable the malware on the system.
- B. Examine the server logs for further indicators of compromise of a web application.
- C. Run `kill -9 1325` to bring the load average down so the server is usable again.

D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

**Answer: B**

#### NEW QUESTION 224

Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

- A. Enumeration and OS fingerprinting
- B. Email harvesting and host scanning
- C. Social media profiling and phishing
- D. Network and host scanning

**Answer: C**

#### NEW QUESTION 229

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

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

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

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

**Answer: D**

#### NEW QUESTION 230

A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

```
-----
Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,
Windows 8.1 and Windows Server 2012 allows remote attackers to execute
arbitrary code via crafted HTTP requests, aka "HTTP.sys remote code execution
vulnerability"

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation='enabled';
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config
-----
```

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

- A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
- B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be completed.
- C. Ignore i
- D. This is false positive, and the organization needs to focus its efforts on other findings.
- E. Ensure HTTP validation is enabled by rebooting the server.

**Answer: A**



**NEW QUESTION 231**

A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach. Which of the following is the BEST mitigation to prevent unauthorized access?

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

**Answer: E**

**NEW QUESTION 234**

An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

- The source of the breach is linked to an IP located in a foreign country.
- The breach is isolated to the research and development servers.
- The hash values of the data before and after the breach are unchanged.
- The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

- A. The confidentiality of the data is unaffected.
- B. The threat is an APT.
- C. The source IP of the threat has been spoofed.
- D. The integrity of the data is unaffected.
- E. The threat is an insider.

**Answer: BD**

**NEW QUESTION 237**

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

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

**Answer: A**

**NEW QUESTION 241**

A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

- A. Client-side whitelisting
- B. Server-side whitelisting
- C. Server-side blacklisting
- D. Client-side blacklisting

**Answer: B**

**NEW QUESTION 246**

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

Tool A reported the following:

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

Tool B reported the following:

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

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

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

**Answer: CE**

**NEW QUESTION 251**



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

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

**Answer: B**

**NEW QUESTION 253**

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

To BEST mitigate this risk, the analyst should use.

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

**Answer: C**

**NEW QUESTION 256**

.....

## 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

### CS0-002 Practice Exam Features:

- \* CS0-002 Questions and Answers Updated Frequently
- \* CS0-002 Practice Questions Verified by Expert Senior Certified Staff
- \* CS0-002 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* CS0-002 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CS0-002 Practice Test Here](#)**