DUMPSBOSS.

CompTIA CyberSecurity Analyst CySA+ Certification Exam

CompTIA CS0-003

Version Demo

Total Demo Questions: 62

Total Premium Questions: 624

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Operations	259
Topic 2, Vulnerability Management	192
Topic 3, Cyber Incident Response	122
Topic 4, Reporting and Communication	51
Total	624

QUESTION NO: 1

Which of the following is the first step that should be performed when establishing a disaster recovery plan?

A. Agree on the goals and objectives of the plan

B. Determine the site to be used during a disaster

C. Identify applications to be run during a disaster

ANSWER: A

Explanation:

Agree on the goals and objectives of the plan is the appropriate first step because it establishes the business purpose, scope, and intended recovery outcomes that the disaster recovery effort must support. Clear objectives define what the organization considers an acceptable recovery result, such as restoring essential services within approved recovery time objectives, preserving the integrity and availability of critical data, meeting contractual or regulatory obligations, and protecting personnel. These objectives must be agreed on by relevant business stakeholders and management so that recovery priorities reflect organizational risk tolerance and operational needs. Once those goals are established, the organization can make defensible decisions about which services are most critical, the resources required for recovery, recovery locations, and the testing criteria that will demonstrate the plan can meet its intended outcomes. This approach aligns with NIST contingency-planning guidance, which emphasizes organizational policy, business impact analysis, and recovery strategies driven by business requirements. It also supports the resilience and recovery planning concepts addressed in the CompTIA CySA+ exam objectives. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and CompTIA CySA+ certification overview.

QUESTION NO: 2

An organization is deploying a new SIEM and wants to ensure that investigators can reliably correlate events from endpoints, firewalls, and identity systems. Which of the following should be implemented? (Select two).

A. Synchronize system clocks with a common time source.

B. Normalize log fields before correlation.

C. Disable logging on systems with low event volume.

D. Store each log source in a separate isolated console.

E. Configure all assets to use the same IP address range.

F. Remove user identifiers from all security events.

ANSWER: A B

Explanation:

Synchronizing system clocks with a common time source is essential because accurate and consistent timestamps allow investigators to sequence events across multiple data sources. Without time synchronization, a login event, endpoint process execution, and firewall connection may appear in the wrong order, impairing timeline analysis and correlation. Network Time Protocol is commonly used to maintain consistent time across infrastructure.

Normalizing log fields is also appropriate because different products represent equivalent information in different formats. For example, one source may use `src_ip`, another may use `sourceAddress`, and an identity platform may record a user in a different field format. Mapping these values to common fields enables SIEM correlation rules and queries to operate consistently. NIST discusses the value of centralized logging and time synchronization in NIST SP 800-92.

QUESTION NO: 3

An XSS vulnerability was reported on one of the 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: D F

Explanation:

Implementing a compensating control in the source code is the most durable recommendation because it addresses the application behavior that permits cross-site scripting. Appropriate code-level controls include context-aware output encoding, server-side validation of untrusted input, and use of well-maintained sanitization mechanisms where user-supplied HTML must be supported. These measures ensure that untrusted data is handled as data rather than interpreted by a browser as executable script. OWASP identifies output encoding as a primary defense for XSS and emphasizes that the encoding must match the output context, such as HTML body, attribute, JavaScript, CSS, or URL contexts. See the OWASP Cross Site Scripting Prevention Cheat Sheet.

Fixing the vulnerability using a virtual patch at the WAF is also an effective immediate protection. A web application firewall can apply a narrowly targeted rule to identify and block known exploit patterns before requests reach the vulnerable application. This compensating safeguard reduces exposure while the application owner develops, tests, and deploys the permanent source-code correction. Virtual patching is particularly valuable for public-facing applications because it can be deployed rapidly and centrally, helping prevent active exploitation during the remediation window. CISA describes web application firewalls as a protective control that can help filter malicious HTTP requests; see CISA guidance on using WAFs to protect web applications.

QUESTION NO: 4

An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).

A. Drop the tables on the database server to prevent data exfiltration.

B. Deploy EDR on the web server and the database server to reduce the adversaries capabilities.

C. Stop the httpd service on the web server so that the adversary can not use web exploits

D. use micro segmentation to restrict connectivity to/from the web and database servers.

E. Comment out the HTTP account in the / etc/passwd file of the web server

F. Move the database from the database server to the web server.

ANSWER: B D

Explanation:

Deploy EDR on the web server and the database server to reduce the adversaries capabilities is an appropriate compensating control because it adds continuous endpoint visibility and detection while preserving the web application and database services needed for the investigation. EDR telemetry can identify malicious processes, persistence, suspicious command execution, credential-access activity, and attempted lateral movement. It also enables measured response actions

and collection of endpoint evidence that may be valuable to incident responders and law enforcement without automatically taking the required services offline.

use micro segmentation to restrict connectivity to/from the web and database servers is also appropriate because it constrains communication to the minimum required application flows. Policy can permit inbound internet traffic only through the reverse proxy, allow the web server to reach the database on the required port, and block unnecessary access to internal systems and unauthorized outbound destinations. This limits the compromised host's opportunity to pivot, scan, establish command-and-control channels, or exfiltrate data while allowing the service to remain operational. These controls support containment through increased monitoring and restricted access paths, consistent with the containment concepts in the CISA Incident Response Playbook and workload-level access control principles in NIST SP 800-207.

QUESTION NO: 5 - (SIMULATION)

You are a cybersecurity analyst tasked with interpreting scan data from Company As 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.

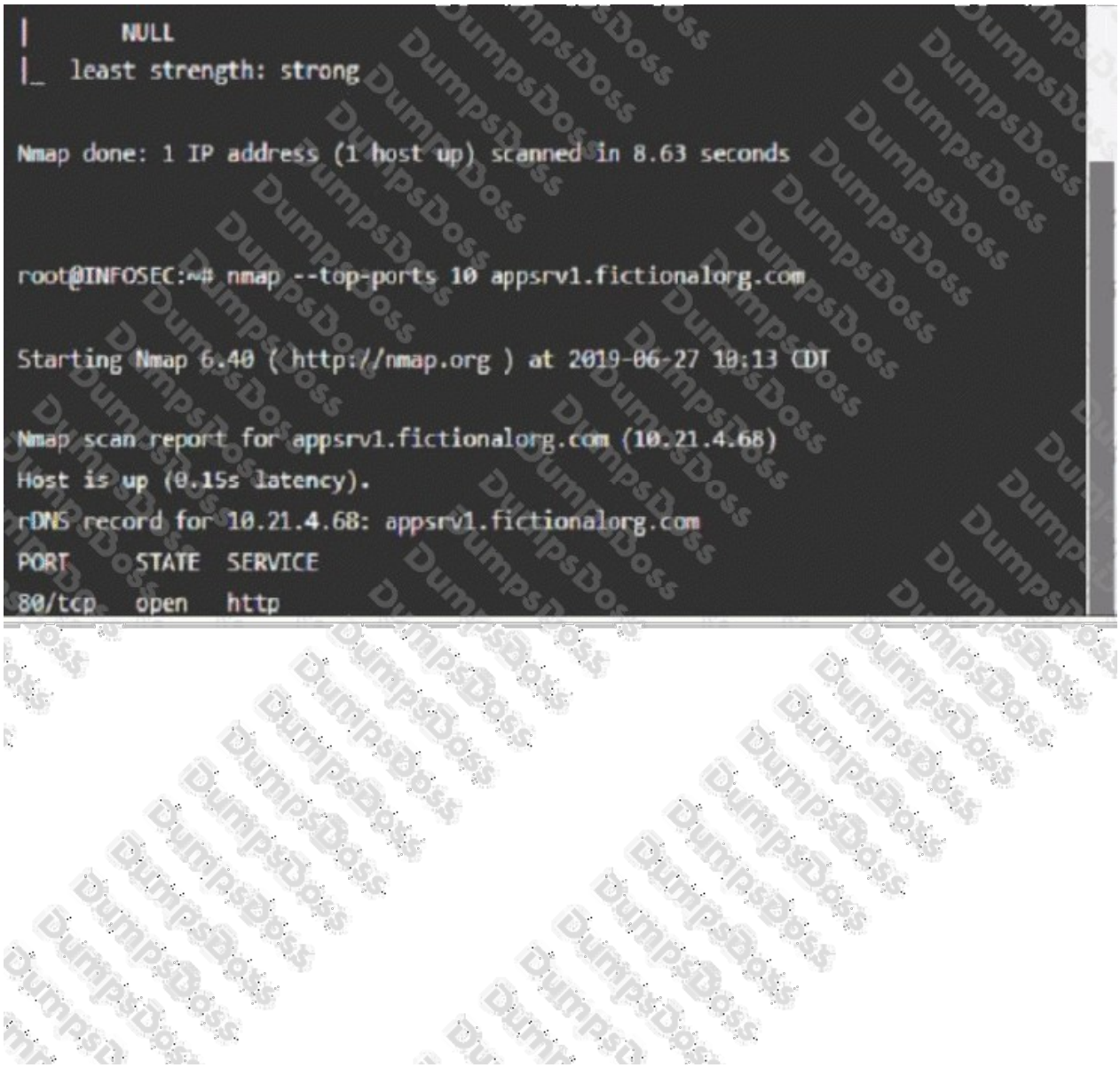
Part 1: AppServ1:

AppServ1 AppServ2 AppServ3 AppServ4

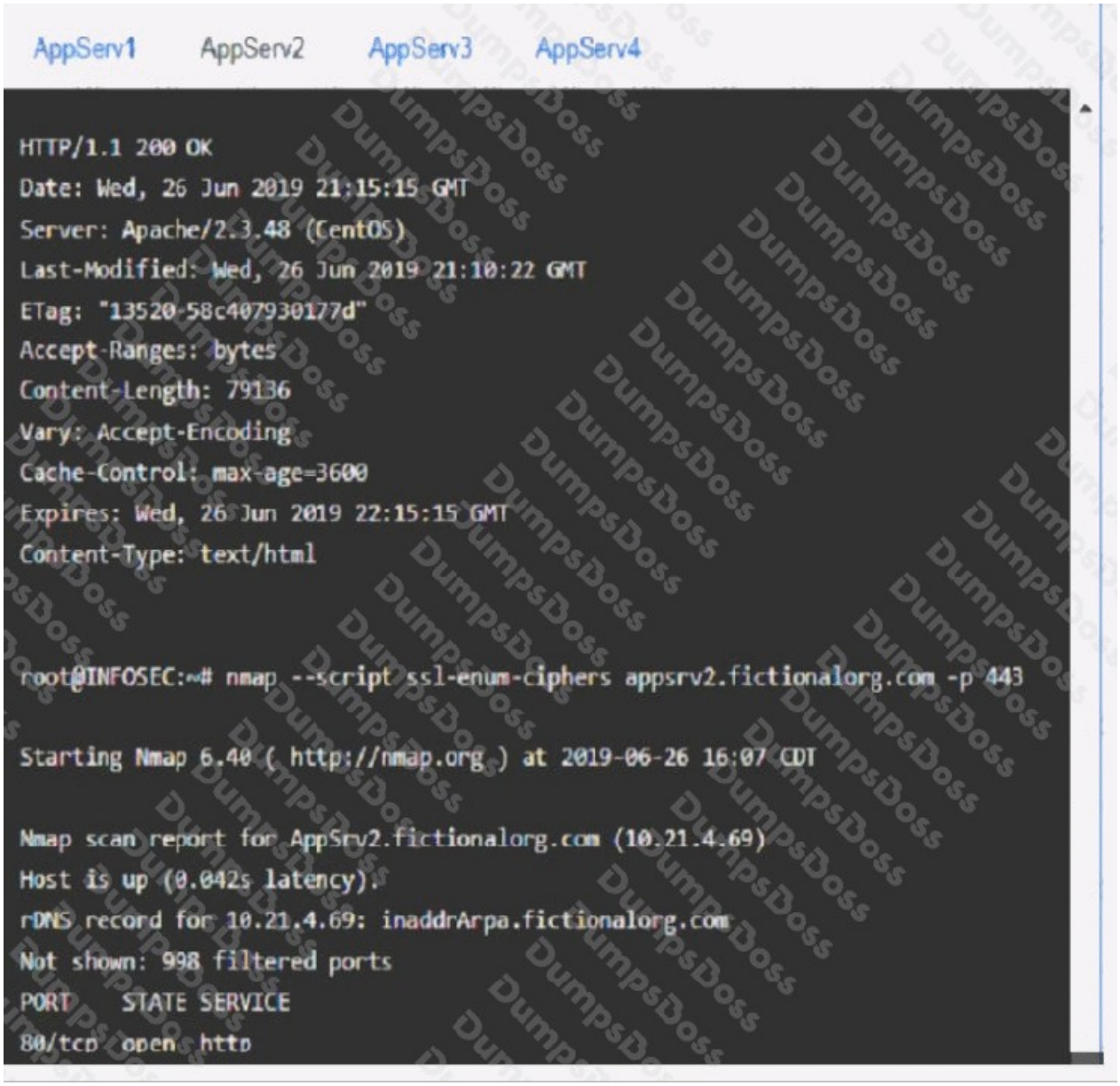
```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

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
```

```
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)
```

```
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

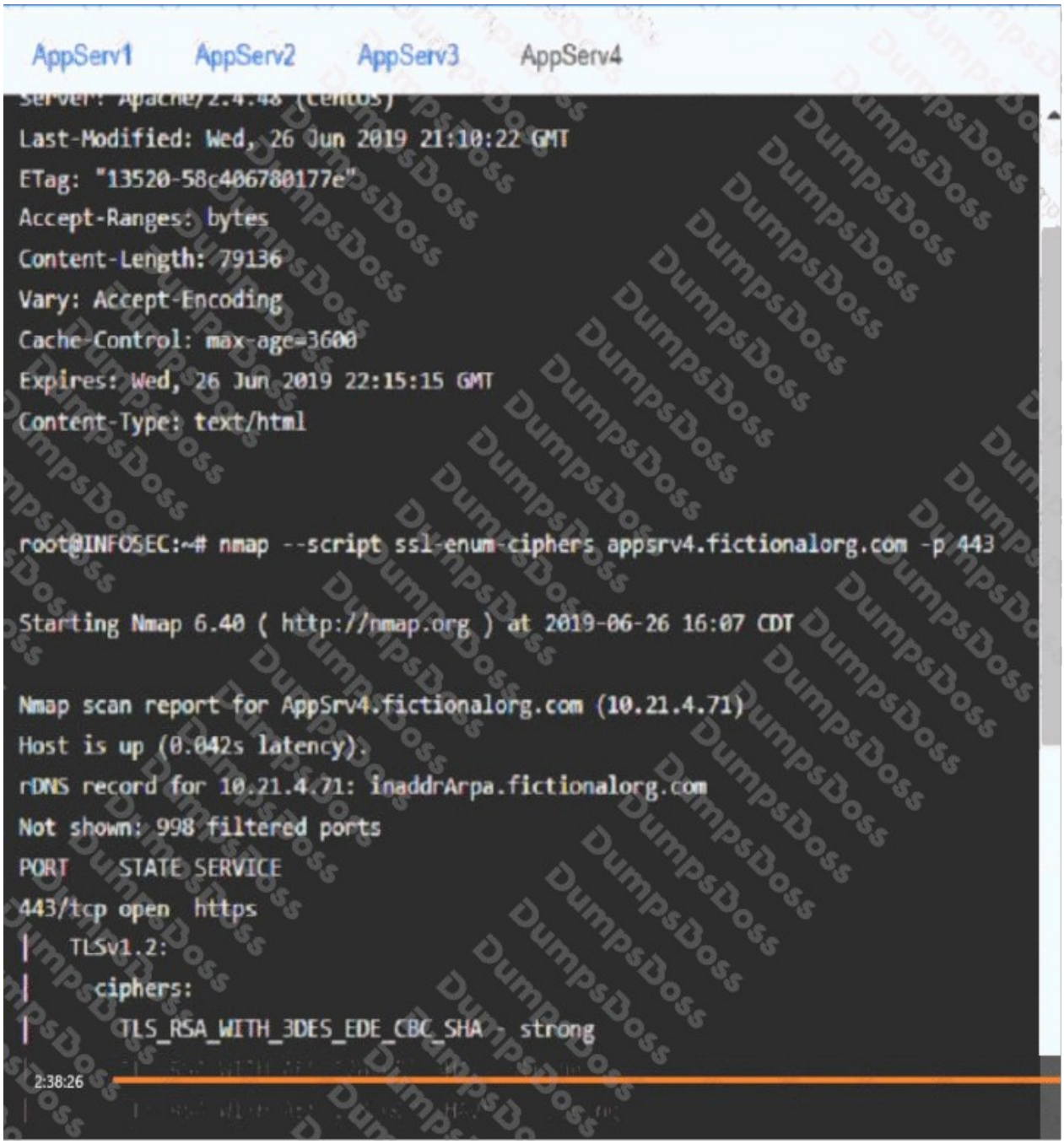
AppServ2:

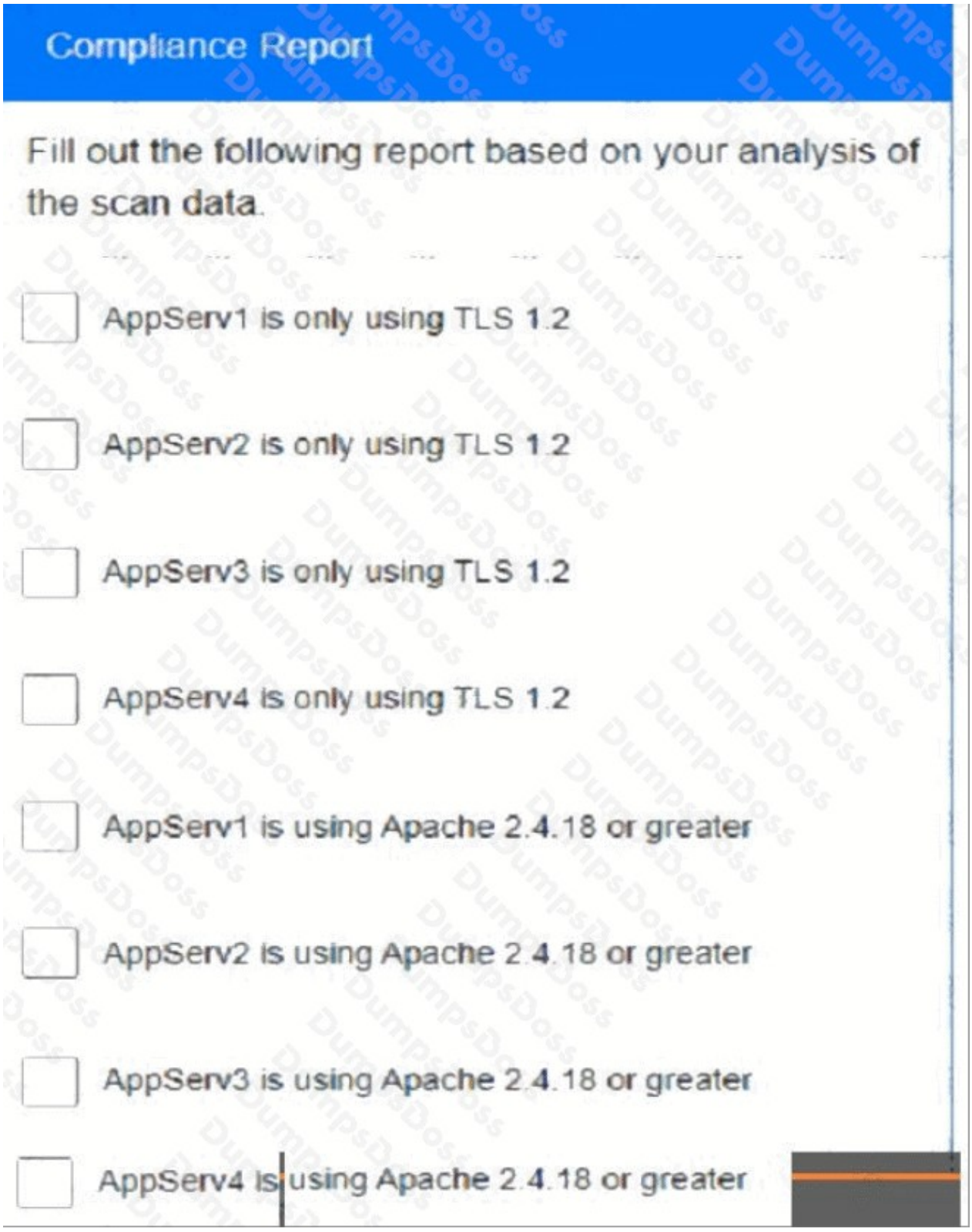

AppServ1
AppServ2
AppServ3
AppServ4
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 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:

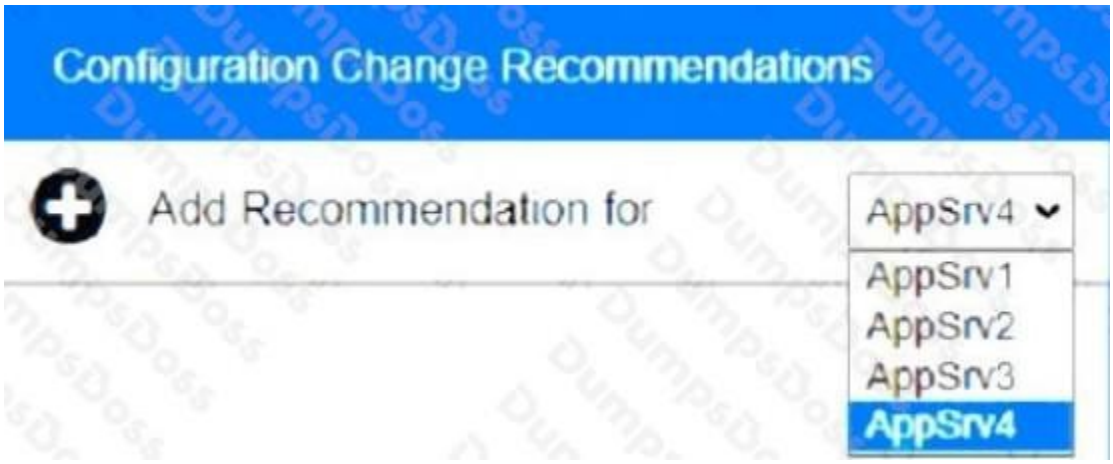
AppServ1
AppServ2
AppServ3
AppServ4
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 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

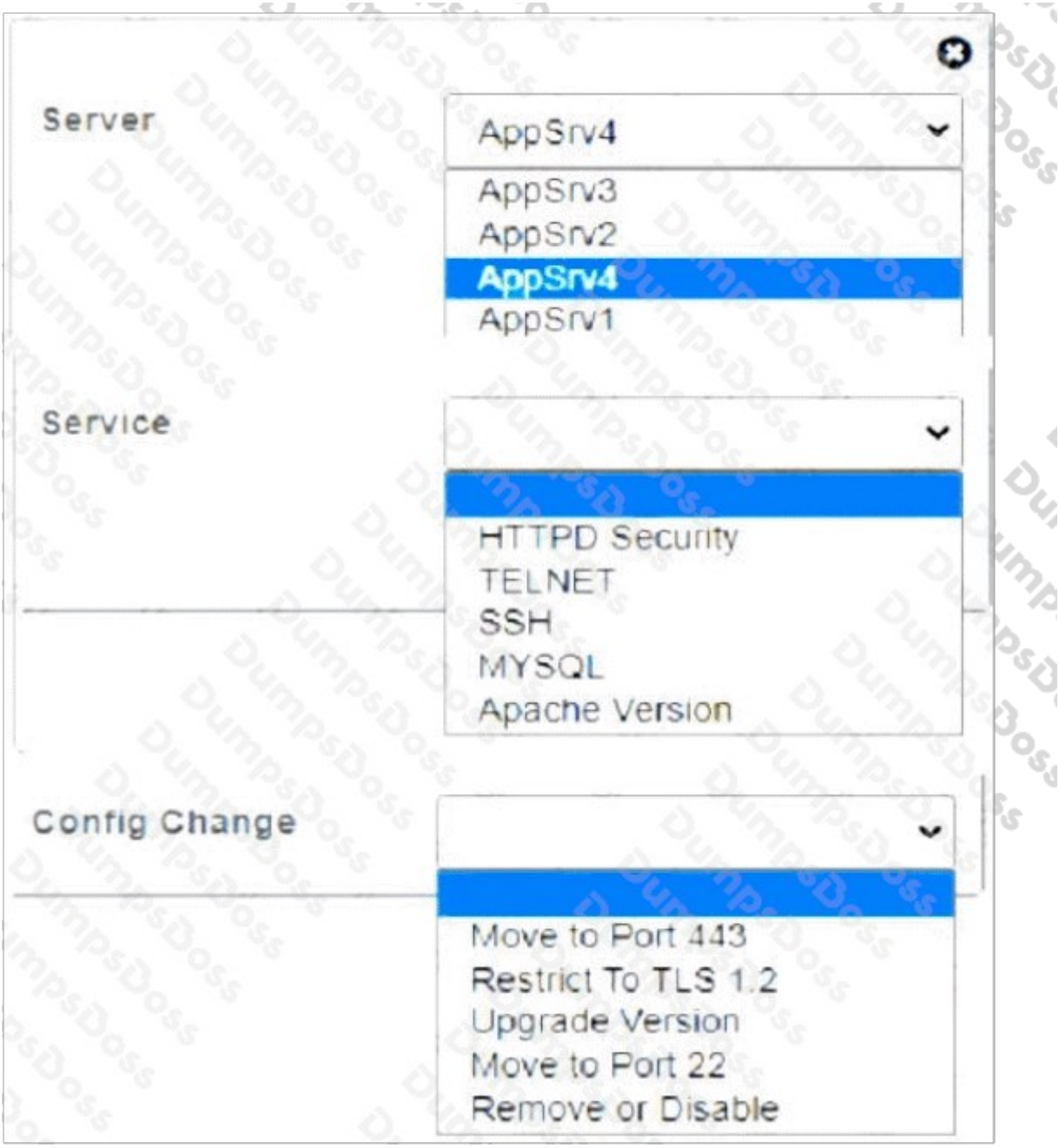
AppServ4:


AppServ1
AppServ2
AppServ3
AppServ4
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


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:

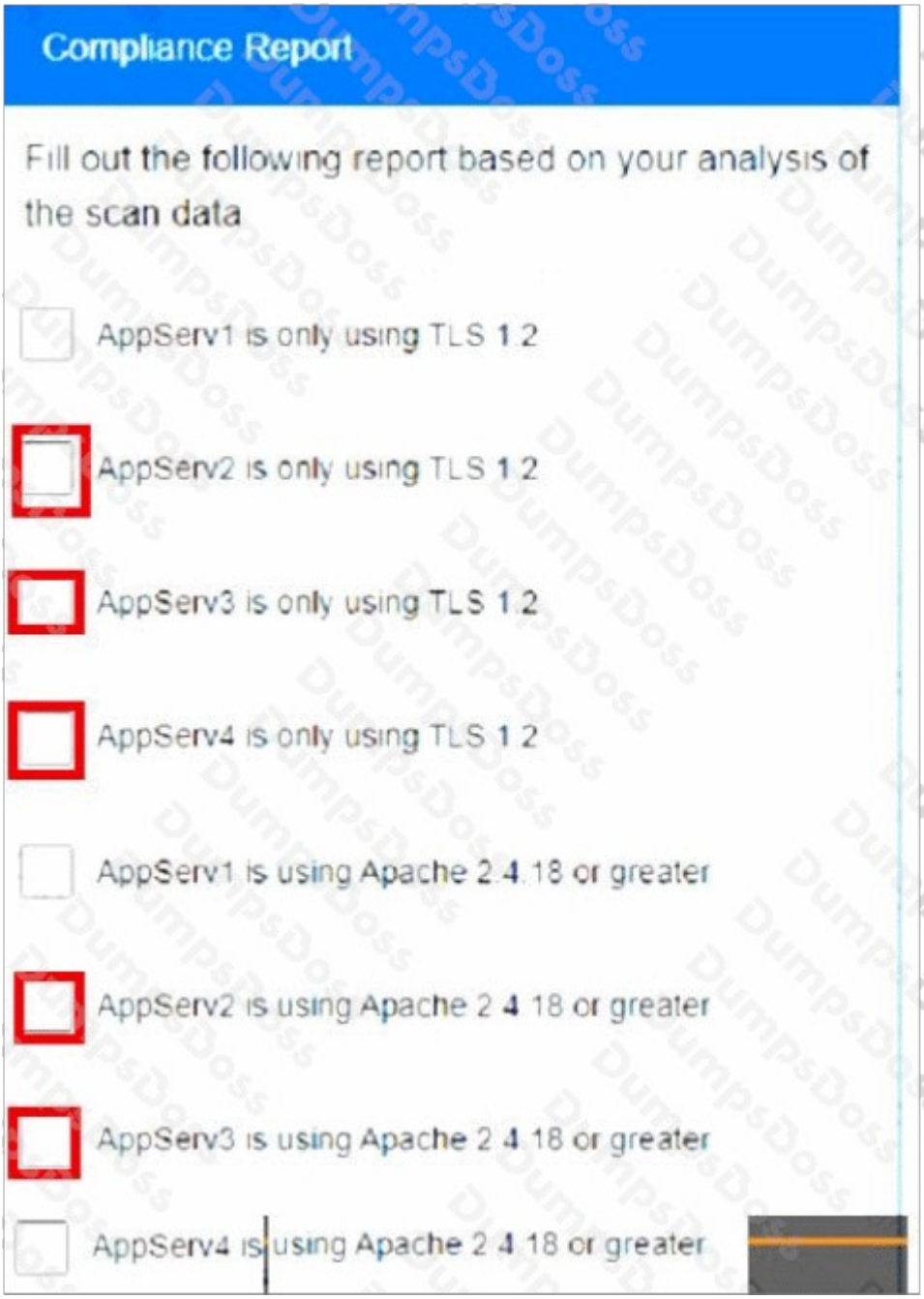




check the explanation part below for the solution:

Explanation:

Part 1:



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.

ANSWER: See the explanation for the answer

Explanation:

Part 1 — Compliance status

Select/check the compliant report items:

Part 2 — Configuration-change recommendations

Do **not** recommend downgrading AppServ3. Version 2.4.19 already satisfies the stated requirement of Apache 2.4.18 or greater.

QUESTION NO: 6

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: D E

Explanation:

A vulnerability scan report should identify the **Affected hosts** for each finding. Asset identification, such as a hostname, IP address, device role, operating system, and discovered service, enables the organization to determine exactly where a vulnerability exists. These details allow findings to be validated, assigned to the responsible asset owner, and tracked through remediation and rescanning. Accurate asset context is fundamental to a useful vulnerability-management process because the same technical issue can have very different business consequences depending on the affected system.

A **Risk score** should also be included so remediation teams can prioritize findings consistently. Scanners commonly report severity using CVSS-based information and may supplement it with environmental or business context. A standardized score communicates the potential impact and exploitability of a vulnerability, helping analysts focus remediation resources on the findings that present the greatest organizational risk. NIST vulnerability-management guidance emphasizes assessing and prioritizing vulnerabilities as part of remediation planning, while CVSS provides an industry-standard framework for describing vulnerability severity. See NIST SP 800-40 Rev. 4 and the FIRST CVSS documentation.

QUESTION NO: 7

The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled. Which of the following should the organization utilize to best centralize the workload for the internal security team? (Select two).

A. SOAR

B. SIEM

C. MSP

D. NGFW

E. XDR

F. DLP

ANSWER: A B

Explanation:

SOAR and SIEM are the appropriate technologies for centralizing the security team's increased alert-handling workload. A SIEM consolidates security telemetry and events from the EDR platform, endpoints, network devices, identity systems, applications, and other sources. It normalizes and correlates this data so analysts can monitor, investigate, prioritize, and search relevant activity from a centralized security-operations interface rather than moving among individual product consoles. This centralized visibility is particularly valuable when an EDR deployment substantially increases the number of findings requiring review.

SOAR centralizes and streamlines the response side of operations. It provides case management, workflow orchestration, integrations, enrichment, alert routing, and repeatable response playbooks. Security teams can automate approved, routine tasks such as collecting indicators, checking reputation data, creating tickets, notifying stakeholders, and initiating predefined containment actions. This reduces the manual effort associated with high-volume alerts while ensuring analysts follow consistent remediation processes. Together, SIEM supplies consolidated collection, analysis, and correlation, while SOAR coordinates investigation and response activities across the team. NIST's definition of SIEM is available through the NIST CSRC SIEM glossary. For an example of combined security operations capabilities, see the Microsoft Sentinel overview.

QUESTION NO: 8

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

A. Human resources must email a copy of a user agreement to all new employees

B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement

C. All new employees must take a test about the company security policy during the onboarding process

D. All new employees must sign a user agreement to acknowledge the company security policy

ANSWER: D

Explanation:

All new employees must sign a user agreement to acknowledge the company security policy is the most appropriate recommendation because it establishes documented individual accountability. The immediate issue is that personnel were not made aware of the restriction on personal devices during onboarding. A signed agreement confirms that each employee was provided the applicable policy, had an opportunity to review it, and formally accepted responsibility for complying with it. This record is important for governance, enforcement, and any subsequent corrective action, because the organization can demonstrate that policy expectations were clearly communicated and acknowledged.

In security programs, such agreements are commonly called rules of behavior or acceptable-use agreements. They define the user's responsibilities for organizational systems and resources, including device restrictions, and require acknowledgement before access is granted or continued. NIST SP 800-53 control PL-4, Rules of Behavior, calls for organizations to establish rules describing user responsibilities and obtain signed acknowledgements from individuals who access organizational systems. Incorporating this requirement into the new-hire process directly addresses the awareness gap while creating auditable evidence of each employee's acceptance. The agreement should be paired with onboarding awareness training and periodic renewal as policies change. See NIST SP 800-53 Rev. 5, PL-4: Rules of Behavior and NIST SP 800-50: Building an Information Technology Security Awareness and Training Program.

QUESTION NO: 9

A security analyst performs a vulnerability scan. Given the following findings:

Machine	IP	Environment	Criticality	Patch available (Yes/No)
Server1	10.5.14.120	Internal network	Medium	No
Server2	10.250.10.8	Perimeter network	Low	Yes
Server3	154.6.80.34	Perimeter network	High	No
Server4	10.5.10.154	Internal network	High	Yes
Server5	10.0.3.45	Database network	Critical	Yes
Server6	10.0.3.38	Database network	Medium	No

Which of the following machines should the analyst address first? (Select two).

A. Server1

B. Server2

C. server3

D. Server4

E. Server5

F. Server 6

ANSWER: C E

Explanation:

server3 and **Server5** should be addressed first because vulnerability remediation must be prioritized according to overall risk: the vulnerability's severity, the affected asset's business value, exposure to attack, and the availability of practical remediation or compensating controls. server3 has a high-severity finding on the perimeter network. Perimeter-facing systems are exposed to external attack paths, so a serious weakness there has a substantially elevated likelihood of exploitation. The analyst should promptly mitigate that risk, including with access restrictions, service disablement, network segmentation, monitoring, or a virtual patch when a vendor patch is unavailable.

Server5 has a critical-severity vulnerability in the database network. Database systems commonly support sensitive, high-value, or mission-critical data and services; therefore, compromise can produce substantial confidentiality, integrity, and availability impact. Because a patch is available, remediating Server5 is an immediate and effective means of reducing a critical risk. NIST recommends enterprise patch and vulnerability management decisions based on risk and supports using mitigations when a patch cannot immediately be deployed. CISA likewise emphasizes prioritizing vulnerabilities that pose the greatest risk to an organization. See NIST SP 800-40 Rev. 4 and CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 10

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

A. Testing

B. Implementation

C. Validation

D. Rollback

ANSWER: C

Explanation:

Validation is the appropriate next step because remediation is not complete merely when a patch has been applied. The technician needs to verify both that the patch deployed successfully and that it resolved the identified vulnerability without disrupting the server's required operation. This commonly involves confirming the installed version or patch level, checking relevant system and application logs, rescanning the affected host with the vulnerability-management tool, and confirming that the original finding is no longer present. Validation may also confirm that any required reboot occurred and that dependent services remain available and perform normally. These checks provide evidence that the organization's risk was actually reduced and support an accurate decision to close or document the remediation ticket. NIST patch-management guidance describes the need to monitor, verify, and assess patch deployment as part of an ongoing enterprise patch-management process. The CIS Controls likewise identify remediation and verification as essential elements of continuous vulnerability management. See NIST SP 800-40 Rev. 4 and CIS Control 7: Continuous Vulnerability Management.

QUESTION NO: 11

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 because the suspected condition is a TCP SYN flood, in which an attacker sends many TCP connection requests but does not complete the three-way handshake. The target retains state for these incomplete, or half-open, connections until they time out, potentially exhausting memory and connection-table resources. Packet capture provides direct evidence of the network behavior responsible for that state. On the affected Linux host, an administrator can use TCPDump to capture traffic on the relevant interface and apply a TCP-flags filter to observe inbound SYN packets and determine whether corresponding final ACK packets are absent. The capture can also establish the packet rate, targeted service port, source-address patterns, and timing of the attempted connections. This information directly supports or disproves the hypothesis that incomplete TCP handshakes are causing resource consumption. TCPDump supports detailed packet filtering and inspection, including filtering based on TCP header flags; see the TCPDump manual page. For background on how SYN floods create many half-open connections and consume target resources, see Cloudflare's SYN flood overview.

QUESTION NO: 12 - (HOTSPOT)

HOTSPOT

A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of risk categorization and prioritization.

INSTRUCTIONS

-

Click on the audit report and risk matrix to review their contents.

Assign a categorization to each risk and determine the order in which the findings must be prioritized for remediation according to the risk rating score.

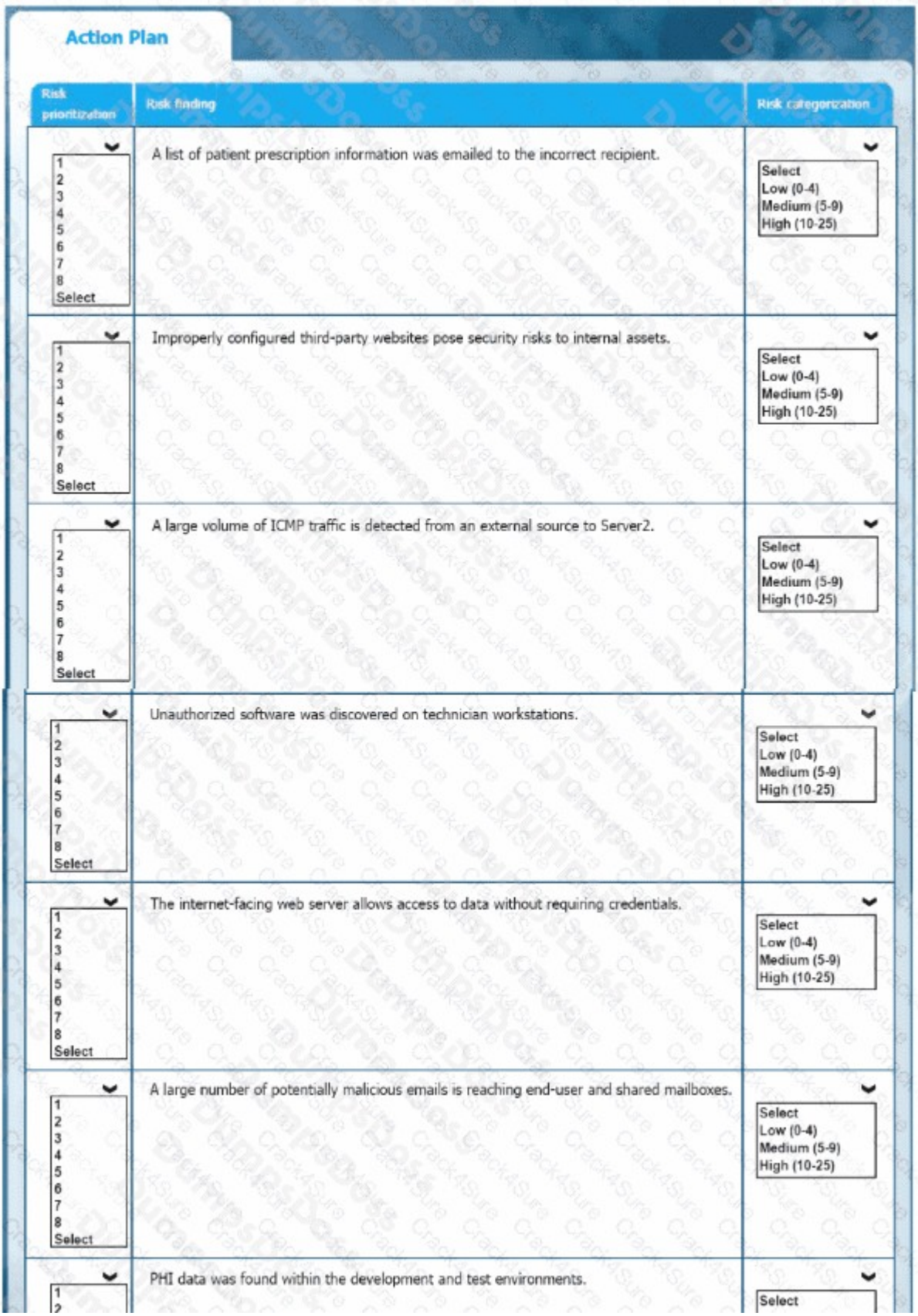
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

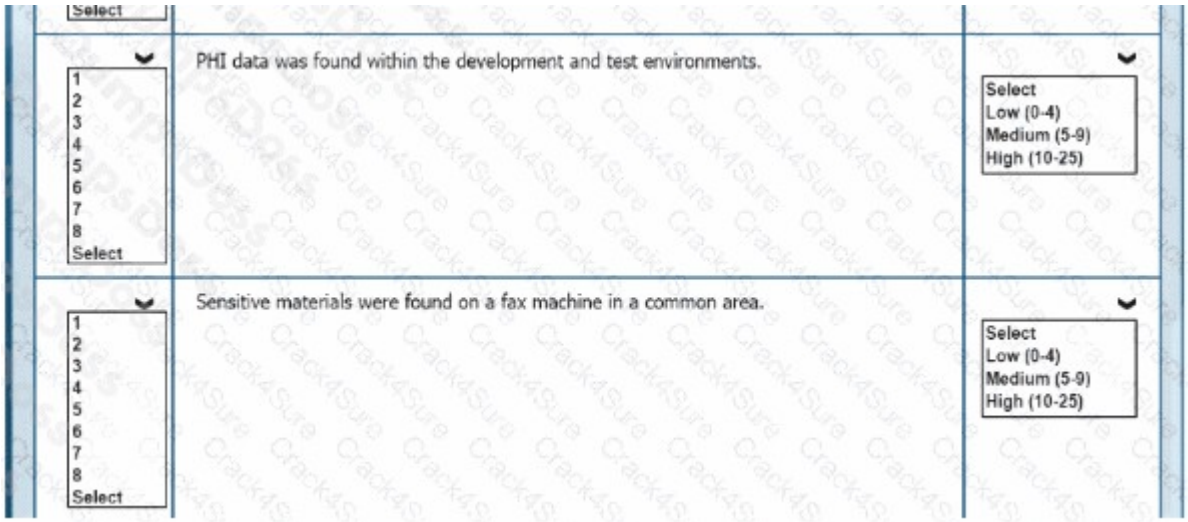
Risk matrix

Severity of impact		Likelihood of occurrence				
		Very unlikely 1	Unlikely 2	Possible 3	Likely 4	Very likely 5
Critical	5	5	10	15	20	25
Severe	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

Risk audit report

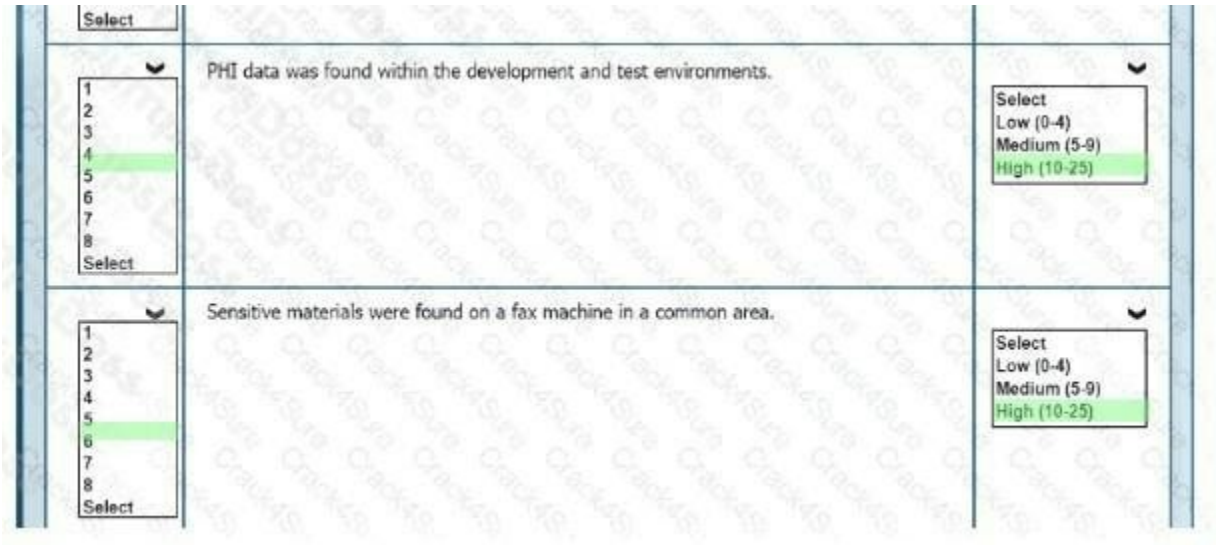
Risk	Description	Risk Rating Score
Improperly configured third-party websites pose security risks to internal assets.	During sampling, ten successful connections to websites with expired or invalid security certificates were found. Sites found during assessment include: www.cnn.com www.localbank.com www.shopping.com	Likelihood of occurrence: 2 Severity of impact: 1
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	A heavy volume of phishing and/or spam messages are reaching end user and shared mailboxes increasing the risk of malicious attachments being opened or links being clicked.	Likelihood of occurrence: 5 Severity of impact: 5
Unauthorized software was discovered on technician workstations.	Unauthorized software was found on a station used by technicians in patient-facing roles. Software found: Weather Toolbar Shopping Helper Newsfeed Live	Likelihood of occurrence: 2 Severity of impact: 2
PHI data was found within the development and test environments.	Controls are not in place to prevent sensitive production data from being used in the test/dev environment, leading to the potential of unauthorized access to and exfiltration of sensitive data.	Likelihood of occurrence: 3 Severity of impact: 3
The internet-facing web server allows access to data without requiring credentials.	Data on the server was found to be accessible via the internet without requiring login credentials. The marketing material stored on this server is required to be publically available.	Likelihood of occurrence: 3 Severity of impact: 1
Sensitive materials were found on a fax machine in a common area.	Documents containing patient information were found unattended on a printer/fax machine located in a common area and was potentially accessible by patients and other non-staff.	Likelihood of occurrence: 3 Severity of impact: 2
A list of patient prescription information was emailed to the incorrect recipient.	A list containing the PHI of 15 patients, including prescription information, was emailed to the incorrect recipient outside of the organization. There was a BPA with the recipient and notification to the patients was deemed unnecessary.	Likelihood of occurrence: 3 Severity of impact: 5
A large volume of ICMP traffic is detected from an external source to Server2.	Review of logs show that a large volume of ICMP traffic has been consistently directed at Server2 for an extended period.	Likelihood of occurrence: 5 Severity of impact: 4


Action Plan
Risk prioritization
Risk finding
Risk categorization
1
2
3
4
5
6
7
8
Select
A list of patient prescription information was emailed to the incorrect recipient.
Select
Low (0-4)
Medium (5-9)
High (10-25)
Improperly configured third-party websites pose security risks to internal assets.
Select
Low (0-4)
Medium (5-9)
High (10-25)
A large volume of ICMP traffic is detected from an external source to Server2.
Select
Low (0-4)
Medium (5-9)
High (10-25)
Unauthorized software was discovered on technician workstations.
Select
Low (0-4)
Medium (5-9)
High (10-25)
The internet-facing web server allows access to data without requiring credentials.
Select
Low (0-4)
Medium (5-9)
High (10-25)
A large number of potentially malicious emails is reaching end-user and shared mailboxes.
Select
Low (0-4)
Medium (5-9)
High (10-25)
PHI data was found within the development and test environments.
Select


Select
1
2
3
4
5
6
7
8
Select
PHI data was found within the development and test environments.
Select
Low (0-4)
Medium (5-9)
High (10-25)
1
2
3
4
5
6
7
8
Select
Sensitive materials were found on a fax machine in a common area.
Select
Low (0-4)
Medium (5-9)
High (10-25)

ANSWER:

Action Plan
Risk prioritization
Risk finding
Risk categorization
A list of patient prescription information was emailed to the incorrect recipient.
Select
Low (0-4)
Medium (5-9)
High (10-25)
Improperly configured third-party websites pose security risks to internal assets.
A large volume of ICMP traffic is detected from an external source to Server2.
Unauthorized software was discovered on technician workstations.
The internet-facing web server allows access to data without requiring credentials.
A large number of potentially malicious emails is reaching end-user and shared mailboxes.
PHI data was found within the development and test environments.



Explanation:

The action plan should use the risk matrix's numerical method: multiply likelihood by impact, map the resulting value to its stated category, and then order remediation from the largest score to the smallest. This ensures that remediation effort is directed first to findings with the greatest combined probability and operational, privacy, or security consequence. This is consistent with risk assessment practices described in NIST SP 800-30 Rev. 1 and the risk-management guidance in NIST's Risk Management Framework.

The malicious-email finding has the maximum calculated score of 25, making it High and the first remediation priority. The large external ICMP traffic finding has a score of 20, so it is High and second. Prescription information sent to an incorrect recipient has a score of 15, making it High and third. PHI located in development and test environments has a score of 9, which falls in the Medium range and makes it fourth. Sensitive material left on a common-area fax machine scores 6, also Medium, and is fifth.

Unauthorized software on technician workstations has a score of 4, placing it in the Low range and sixth in remediation order. The internet-facing server that allows unauthenticated access scores 3, also Low, and is seventh. Improperly configured third-party websites score 2, which is Low and the final remediation priority. The full prioritization is therefore based strictly on descending calculated risk score, while each category reflects the matrix threshold associated with that score.

QUESTION NO: 13

An analyst is trying to capture anomalous traffic from a compromised host. Which of the following are the best tools for achieving this objective? (Select two).

A. tcpdump

B. SIEM

C. Vulnerability scanner

D. Wireshark

E. Nmap

F. SOAR

ANSWER: A D

Explanation:

tcpdump and **Wireshark** are appropriate tools for capturing anomalous traffic associated with a compromised host. tcpdump is a command-line packet-capture utility that collects packets directly from a network interface. An analyst can apply capture filters to focus collection on relevant hosts, ports, protocols, or traffic directions, reducing noise while preserving

evidence in a PCAP file. Its lightweight nature makes it particularly useful for rapid incident-response collection on servers and other systems where a graphical interface may not be available.

Wireshark supports both live packet capture and detailed inspection of saved PCAP files. It enables an analyst to examine protocol fields, sessions, timing, endpoints, DNS requests, HTTP activity, and packet payloads to identify suspicious communications or possible command-and-control behavior. Wireshark can also apply display filters after collection, allowing investigators to pivot through captured evidence without changing the original packet data. In practice, tcpdump may be used to quickly capture traffic on the affected system, while Wireshark is used for deeper interactive analysis of that capture. See the tcpdump manual page and the Wireshark documentation.

QUESTION NO: 14

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.

E. The developer did not properly validate, sanitize, or encode user-supplied input.

ANSWER: E

Explanation:

The developer did not properly validate, sanitize, or encode user-supplied input. The Arachni finding identifies a possible cross-site scripting issue in the `txtSearch` form input and reports that the response is tainted. This indicates that scanner-controlled input submitted to the search function was included in the server response. When an application reflects untrusted request data into a page without handling it safely for its specific output context, a browser may interpret injected content as markup or script rather than as plain text.

Search pages commonly redisplay the submitted search term, such as in a results heading or input value. Secure implementation requires treating that value as untrusted and applying context-aware output encoding wherever it is rendered. For example, data placed into HTML element content must be HTML encoded, while data used in an attribute or JavaScript context needs encoding appropriate to that context. Strict allowlist input validation can further limit unexpected characters, and sanitization is needed when an application intentionally accepts limited HTML. These controls prevent attacker-supplied content from becoming executable in a victim's browser. OWASP describes output encoding as a primary XSS defense in its Cross Site Scripting Prevention Cheat Sheet. See also PortSwigger's reflected XSS guidance.

QUESTION NO: 15

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

[-] 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.

E. The developer did not properly encode or sanitize untrusted input before including it in the application response.

ANSWER: E

Explanation:

The developer did not properly encode or sanitize untrusted input before including it in the application's response is the most likely cause. Arachni's report identifies the `txtSearch` form input as the injection point and states that the response is tainted. In this context, taint means data supplied through the request appears in the returned page in a way that may preserve its executable meaning. When an application places request data into HTML, an HTML attribute, JavaScript, a URL, or CSS without context-appropriate output encoding, an attacker can supply markup or script that the browser interprets rather than displays as text. This is the fundamental condition that produces reflected XSS in a search form or comparable user-controlled field.

Secure development requires treating all request values as untrusted, applying allow-list validation where the business function permits it, and, critically, using output encoding appropriate to the exact rendering context. Modern templating frameworks can often provide automatic HTML encoding, but developers must retain it and use safe APIs for dynamic client-side rendering. OWASP's XSS Prevention Cheat Sheet describes context-specific output encoding as the primary control: OWASP Cross Site Scripting Prevention Cheat Sheet. The OWASP Web Security Testing Guide also describes testing reflected input for XSS: OWASP Web Security Testing Guide.

QUESTION NO: 16

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: D F

Explanation:

Implementing a compensating control in the source code is an appropriate long-term recommendation because cross-site scripting is fundamentally an application-layer issue: untrusted data must be handled safely in the context where it is

rendered. Effective code-level controls include context-aware output encoding, allowlist-based input validation where appropriate, and sanitization for user-supplied HTML that must be accepted. These controls prevent attacker-controlled content from being interpreted by a browser as executable script, which directly reduces the opportunity for exploitation. The OWASP guidance on this approach is available in the Cross Site Scripting Prevention Cheat Sheet.

Fixing the vulnerability using a virtual patch at the WAF is also a strong recommendation, particularly while the application owner schedules, tests, and deploys the permanent source-code correction. A WAF rule can inspect HTTP requests and, where applicable, responses to identify and block known malicious XSS payload patterns before they reach the vulnerable functionality or are delivered to users. This provides a compensating layer of protection without requiring an immediate application release. For a public, non-mission-critical site, virtual patching is a practical risk-reduction measure that can be implemented quickly while preserving service availability. OWASP describes WAFs and other defensive controls in its Web Application Firewall guidance.

QUESTION NO: 17

An organization's email account was compromised by a bad actor. Given the following Information:

Which of the following is the length of time the team took to detect the threat?

A. 25 minutes

B. 40 minutes

C. 45 minutes

D. 2 hours

ANSWER: B

Explanation:

40 minutes is the time to detect because detection time measures the elapsed interval between the initial malicious activity or compromise and the point at which the organization identifies the incident. In this email-account-compromise scenario, the relevant starting point is when the bad actor gained control of the account. The endpoint is when the security team, help desk, monitoring tooling, or user reports brought the malicious activity to the organization’s attention. The stated interval between those events is 40 minutes.

This measure is commonly tracked as mean time to detect (MTTD), although a single event is more precisely described as time to detect. It is an important security-operations metric because it reflects the effectiveness of telemetry, alerting, monitoring, triage, and reporting workflows. Prompt detection reduces the period in which an attacker can use a compromised account to send phishing messages, access email content, establish persistence, or pivot to other resources. NIST incident-handling guidance treats detection and analysis as a core incident-response function, requiring teams to identify and validate indicators and events before containment and recovery activities begin. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and the CISA incident response resources.

QUESTION NO: 18

A security audit for unsecured network services was conducted, and the following output was generated:

Which of the following services should the security team investigate further? (Select two).

A. 21

B. 22

C. 23

D. 636

E. 1723

F. 3389

ANSWER: A C

Explanation:

21 and **23** should be investigated because these well-known ports commonly correspond to FTP and Telnet, respectively, and both protocols lack built-in protection for sensitive communications. Traditional FTP uses a separate control channel and transmits user names, passwords, commands, and file contents without cryptographic confidentiality. An attacker able to monitor the relevant network path can therefore capture credentials or data. RFC 2577 specifically documents FTP security considerations, including risks associated with cleartext passwords and data transfer: RFC 2577.

Telnet is likewise a cleartext remote-terminal protocol. Its authentication exchanges and administrative session traffic can be exposed to packet capture, creating significant risk when it is enabled on a server, network appliance, or other managed asset. During an audit, the team should identify the systems listening on these ports, confirm whether the services are externally reachable, determine whether there is a valid business dependency, and remediate unnecessary exposure. Where file-transfer capability is needed, an encrypted managed alternative should be used; where remote administration is required, SSH provides protected remote-access communications. NIST's guidance on secure remote access and administration reinforces the importance of protecting management traffic with strong cryptographic controls: NIST SP 800-46 Rev. 2.

QUESTION NO: 19

An organization has established a formal change management process after experiencing several critical system failures over the past year. Which of the following are key factors that the change management process will include in order to reduce the impact of system failures? (Select two).

A. Ensure users the document system recovery plan prior to deployment.

B. Perform a full system-level backup following the change.

C. Leverage an audit tool to identify changes that are being made.

D. Identify assets with dependence that could be impacted by the change.

E. Require diagrams to be completed for all critical systems.

F. Ensure that all assets are properly listed in the inventory management system.

ANSWER: D F

Explanation:

"Identify assets with dependence that could be impacted by the change" is essential because a change rarely affects only the system directly modified. Identifying upstream and downstream dependencies allows the change owner to perform a meaningful impact analysis, schedule appropriate testing, involve affected service owners, and prepare safeguards before implementation. This limits the likelihood that a change to one component will unexpectedly disrupt a dependent application, service, or business process.

"Ensure that all assets are properly listed in the inventory management system" provides the reliable asset baseline needed for that analysis. An accurate inventory identifies the hardware, software, systems, and owners that may be within a change's scope. It supports complete planning, authorization, testing, monitoring, and recovery decisions, while reducing the risk that unmanaged or undocumented assets will be missed. Together, dependency identification and complete asset inventory data enable change management to assess operational risk before deployment and contain the blast radius if an issue occurs. NIST configuration-management guidance emphasizes documenting system components and relationships to support impact analysis and controlled changes, while its asset-inventory control requires accurate, complete, and current system component inventories. See NIST SP 800-128 and NIST SP 800-53 CM-8.

QUESTION NO: 20

Which of the following stakeholders are most likely to receive a vulnerability scan report? (Select two).

A. Executive management

B. Law enforcement

C. Marketing

D. Legal

E. Product owner

F. Systems admininstration

ANSWER: A F

Explanation:

Executive management and Systems admininstration are the appropriate recipients because vulnerability-scan reporting must support both organizational risk decisions and technical remediation. Executive management needs an audience-appropriate summary that communicates the organization's risk posture, significant exposures, vulnerability trends, remediation status, and any resource or risk-acceptance decisions requiring leadership involvement. This information enables leaders to prioritize investments and oversee whether the vulnerability-management program is reducing material cyber risk.

Systems admininstration requires the detailed, actionable report because these personnel commonly own the systems and configurations identified during scanning. Technical findings, including affected assets, vulnerability severity, remediation guidance, and validation results, enable administrators to schedule patches, correct insecure configurations, coordinate maintenance, and verify that remediation was effective through rescanning. Effective vulnerability management assigns remediation work to responsible asset and system owners while providing management with metrics and summaries aligned to governance responsibilities. NIST describes enterprise patch and vulnerability management as an organizational process involving identification, prioritization, remediation, and verification. See NIST SP 800-40 Rev. 4 and the CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 21

Which of the following are process improvements that can be realized by implementing a SOAR solution? (Select two).

A. Minimize security attacks

B. Itemize tasks for approval

C. Reduce repetitive tasks

D. Minimize setup complexity

E. Define a security strategy

F. Generate reports and metrics

ANSWER: C F

Explanation:

SOAR platforms improve security-operations processes by orchestrating disparate security tools and automating repeatable steps through defined playbooks. "Reduce repetitive tasks" is correct because SOAR can automatically enrich alerts, correlate contextual data, open and update tickets, notify stakeholders, and initiate approved containment actions. Removing this manual, repetitive work helps analysts handle alerts more consistently and devote more time to investigations, threat hunting, and decisions that require human judgment. It also supports a more repeatable incident-response process, reducing the chance that essential procedural steps are skipped during high alert volumes.

"Generate reports and metrics" is also correct because SOAR platforms centrally track cases, alerts, workflow executions, task completion, escalation events, and response actions. That data can be used to report operational measures such as alert and incident volumes, mean time to acknowledge or respond, case-resolution trends, playbook performance, and automation usage. Security teams can use these metrics to identify bottlenecks, tune playbooks, demonstrate SOC effectiveness, and drive continuous process improvement. These capabilities align with SOAR's core emphasis on

automation, orchestration, case management, and measurable incident-response workflows. See IBM Think: What is SOAR? and Microsoft Learn: Automate threat response with automation rules and playbooks.

QUESTION NO: 22

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: C E

Explanation:

Legal and **Public relations** should be engaged for incident communications directed at the general public. Legal counsel ensures proposed disclosures align with applicable laws and regulations, breach-notification duties, contractual commitments, privacy requirements, and litigation-related considerations. Legal review also helps the incident response team preserve privilege where applicable and avoid releasing information that could create unnecessary liability or compromise investigative or evidentiary needs. Public relations coordinates the organization's external message, including the approved spokesperson, communication channels, timing, tone, and consistency of statements to customers, media, partners, and the broader public. Its involvement helps ensure that information is clear, factual, and appropriately scoped while maintaining stakeholder confidence during a disruptive event. Together, these functions support a predefined, coordinated communications process: technical responders provide validated facts; legal validates disclosure obligations and risk; and public relations delivers the approved message effectively. NIST incident-response guidance identifies coordination with legal counsel and public affairs as an important part of incident-response communications and stakeholder management. CISA likewise recommends establishing communication roles, responsibilities, and procedures in an incident response plan before an event occurs. See NIST SP 800-61 Rev. 2 and CISA Incident Response Plan Basics.

QUESTION NO: 23

An email hosting provider added a new data center with new public IP addresses. Which of the following most likely needs to be updated to ensure emails from the new data center do not get blocked by spam filters?

A. DKIM

B. SPF

C. SMTP

D. DMARC

ANSWER: B

Explanation:

SPF is correct because the Sender Policy Framework publishes, in DNS, the IP addresses and mail systems that are authorized to send messages for a domain. When the hosting provider begins transmitting mail from the new data center, its new public IP addresses must be included in the domain's SPF TXT record, either directly with appropriate IP mechanisms or indirectly through an authorized include mechanism maintained by the provider. Recipient mail systems evaluate SPF using the sending server's connecting IP address. A message sent from an address not authorized by the SPF policy can produce an SPF failure, which is an important authentication signal used by anti-spam systems and by DMARC evaluation.

Updating the SPF policy therefore establishes that mail originating from the new infrastructure is legitimate for the domain and helps preserve delivery to recipients' inboxes. The SPF specification defines how receivers check the client IP against the domain's published SPF record: RFC 7208: Sender Policy Framework. Microsoft's implementation guidance also describes SPF as a DNS-based method for identifying authorized outbound email servers: Configure SPF in Microsoft Defender for Office 365.

QUESTION NO: 24

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:

Unintentional insider threat is correct because the described control is aimed at reducing the risk created when authorized users inadvertently introduce malware or expose organizational resources. Employees, contractors, and other legitimate users can be manipulated through phishing or social-engineering messages that contain malicious attachments. Even though the user has authorized access, opening an unsafe attachment can result in malware execution, credential theft, ransomware, or unauthorized access to internal systems. Encouraging users to open attachments only when the sender and context are known is a security-awareness measure that addresses this accidental, human-driven risk. In the CySA+ threat landscape, insider threats include both deliberate actions and unintentional actions by trusted individuals; the defining point here is that the user does not intend to harm the organization. CISA specifically advises users to be cautious with unexpected email attachments and to verify messages before opening files, because malicious attachments are a frequent phishing delivery mechanism. See CISA: Recognize and Report Phishing and CISA: Insider Threat Mitigation.

QUESTION NO: 25

A cloud security analyst suspects an attacker used compromised credentials to modify security groups and access an IaaS virtual machine. Which of the following data sources should the analyst review to investigate the suspected activity? (Select two).

A. Cloud audit logs

B. VPC Flow Logs

C. Browser history from the analyst workstation

D. Printer spooler logs

E. Physical access badge records

F. Domain controller replication logs

ANSWER: A B

Explanation:

Cloud audit logs and VPC Flow Logs are the appropriate data sources. Cloud audit logs, such as AWS CloudTrail logs, record control-plane API activity. The analyst can use these records to identify the identity that modified a security group, the source IP address, the time of the change, and the specific API request that was used. This information is essential for determining whether unauthorized cloud-management actions occurred.

VPC Flow Logs provide network-flow metadata for traffic to and from cloud network interfaces. They can help the analyst determine whether the affected virtual machine communicated with suspicious external addresses, received unexpected inbound traffic after a security-group change, or initiated possible command-and-control or data-exfiltration activity. Together, the audit trail establishes what cloud resources were changed, while flow logs provide evidence of associated network behavior. AWS documents these services in the AWS CloudTrail User Guide and the Amazon VPC Flow Logs documentation.

QUESTION NO: 26

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 is correct because a service level agreement is the contract or formally documented agreement that establishes measurable service commitments between a provider and a customer. When an external vendor maintains systems in a secure environment, the SLA identifies the maintenance and support services to be delivered and defines the required levels of performance. Typical provisions include service availability targets, maintenance windows, support hours, incident-response and resolution time objectives, escalation paths, performance reporting, responsibilities, and remedies or credits when a provider does not meet agreed commitments. These measurable requirements enable the organization to hold a vendor accountable for maintaining services that support business operations and security objectives. They also give security and operations teams a documented basis for monitoring vendor performance, managing service disruptions, and assessing third-party risk. NIST describes a service level agreement as an agreement between service providers and consumers that defines services, priorities, responsibilities, guarantees, and warranties. See the NIST Computer Security Resource Center SLA glossary entry. For vendor and supply-chain cybersecurity risk-management context, see NIST SP 800-161 Rev. 1.

QUESTION NO: 27

An organization has implemented code into a production environment. During a routine test, a penetration tester found that some of the code had a backdoor implemented, causing a developer to make changes outside of the change management windows. Which of the following is the best way to prevent this issue?

A. SDLC training

B. Dynamic analysis

C. Debugging

D. Source code review

ANSWER: D

Explanation:

Source code review is the best preventive control because it examines application changes before they are accepted into the production codebase or deployed. A backdoor is typically intentional, concealed logic that enables unauthorized access or behavior; identifying it requires visibility into the source, commit history, pull requests, and associated approvals. Requiring peer review of every change, combined with protected branches and documented approval workflows, creates separation of duties and makes it much harder for an individual developer to introduce unapproved code outside established change-

management windows. Reviewers can validate that a change has a legitimate business purpose, is linked to an authorized ticket, follows secure coding requirements, and contains no hidden authentication bypasses, hardcoded secrets, or suspicious conditional behavior. Automated static security checks can complement the human review, but the review process itself provides essential accountability and traceability for unauthorized modifications. The NIST Secure Software Development Framework recommends reviewing code and verifying the integrity of software releases as part of secure development practices: NIST SP 800-218. OWASP also identifies code review as a key practice for finding security issues in source before release: OWASP Code Review Guide.

QUESTION NO: 28

An incident response team is investigating a suspected data breach involving a database containing customer records. Which of the following evidence sources would best help determine whether large volumes of records were accessed or exported? (Select two).

A. Database audit logs

B. NetFlow data

C. Employee security awareness completion records

D. The organization's password complexity policy

E. Printer queue logs

F. Physical visitor badges from the prior year

ANSWER: A B

Explanation:

Database audit logs are an appropriate source because they can record authentication events, queries, privileged actions, schema changes, bulk export operations, and access to sensitive tables. Reviewing these events can help the team identify which account accessed customer records, the queries executed, and whether activity occurred outside normal patterns.

NetFlow data is also valuable because it provides network metadata such as source and destination addresses, ports, connection timing, and byte counts. While NetFlow does not reveal database query contents, unusually large outbound transfers from the database server or an associated application server can help establish the timing and scope of possible exfiltration. Correlating network volume with database audit events strengthens the investigation. NIST describes the importance of log management and incident evidence collection in NIST SP 800-92 and NIST SP 800-86.

QUESTION NO: 29

An analyst has discovered the following suspicious command:

```
<?php if(isset($_REQUEST['xyz'])){echo "<pre>"; $xyz = ($_REQUEST['xyz']); system($xyz); echo "</pre>"; die; }?>
```

Which of the following would best describe the outcome of the command?

A. Cross-site scripting

B. Reverse shell

C. Backdoor attempt

D. Logic bomb

ANSWER: C

Explanation:

Backdoor attempt is the best description because the command shown is consistent with creating or invoking a web-accessible mechanism for executing commands on the underlying host. This behavior is commonly associated with a web shell: malicious server-side code, often implemented in a web programming language, that accepts attacker-supplied input and passes it to an operating-system command interpreter. Once placed on a compromised web server, a web shell gives an attacker a concealed remote administration channel that can be used to execute commands, enumerate the environment, retrieve files, install additional tooling, and maintain access. The resulting capability is a backdoor because it bypasses intended administrative access paths and enables unauthorized command execution with the permissions available to the web-service process. MITRE ATT&CK classifies web shells as a server software component technique used to establish persistence and execute attacker actions through a compromised server. OWASP likewise describes web shells as scripts that enable attackers to execute commands remotely on a web server. See MITRE ATT&CK: Web Shell and OWASP: Web Shell.

QUESTION NO: 30

A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

A. nessie.explosion

B. vote.4p

C. sweet.bike

D. great.skills

ANSWER: A

Explanation:

nessie.explosion should be prioritized because the CVSS v3.1 exploitability information shown for it represents the most readily exploitable condition in the workstation environment after administrator rights were removed. CVSS exploitability is determined from Attack Vector, Attack Complexity, Privileges Required, and User Interaction. Of particular importance here, Privileges Required measures the level of authorization an attacker must already possess before exploitation can occur. A vulnerability that can be exploited without elevated privileges remains a practical risk for standard end-user accounts, whereas the removal of local administrator rights reduces the likelihood that vulnerabilities dependent on elevated authorization can be exploited directly by those users or by malware running in their security context.

Prioritizing the vulnerability with the strongest exploitability characteristics helps the organization remediate the issue most likely to be successfully exploited on its endpoints. This is consistent with the purpose of the CVSS exploitability sub-score: to describe the technical ease and preconditions for an attacker to exploit a vulnerability. The analyst should still consider asset criticality, exposure, and threat intelligence during final remediation planning, but based on the supplied CVSS v3.1 exploitability metrics and the stated privilege-control change, **nessie.explosion** is the appropriate first remediation target. See the FIRST CVSS v3.1 Specification and the FIRST CVSS v3.1 User Guide.

QUESTION NO: 31

Executives at an organization email sensitive financial information to external business partners when negotiating valuable contracts. To ensure the legal validity of these messages, the cybersecurity team recommends a digital signature be added to emails sent by the executives. Which of the following are the primary goals of this recommendation? (Select two).

A. Confidentiality

B. Integrity

C. Privacy

D. Anonymity

E. Non-repudiation

F. Authorization

ANSWER: B E

Explanation:

Integrity and Non-repudiation are the primary security goals provided by a digital signature on an executive's email. A digital signature is generated over the message data using the sender's private key. Recipients validate it with the associated public key, which enables them to detect whether the signed message changed after it was signed. This provides integrity: the receiving business partner can establish that the financial details and contractual statements being relied on are the same as those originally signed by the executive. Any post-signature alteration causes validation to fail.

Digital signatures also provide non-repudiation by creating cryptographic evidence linking the signed message to the holder of the corresponding private key. When identities and private keys are properly managed, this evidence supports accountability and helps demonstrate that the executive authorized the communication. That assurance is particularly important in high-value negotiations, where the organization and its partners may later need to establish the origin and authenticity of an email's commitments. NIST defines a digital signature as a cryptographic mechanism that verifies origin and detects unauthorized modification, and identifies non-repudiation as assurance that a party cannot deny a prior action. See NIST's Digital Signature glossary entry and NIST's Non-repudiation glossary entry.

QUESTION NO: 32

Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?

A. CASB

B. DMARC

C. SIEM

D. PAM

ANSWER: A

Explanation:

CASB is correct because a cloud access security broker is a security policy enforcement point positioned between cloud-service consumers and cloud-service providers. Its purpose is to give an organization visibility into cloud use and apply its security requirements when users access SaaS, PaaS, or IaaS resources. A CASB can enforce controls such as access policies, multifactor-authentication requirements, conditional access, data loss prevention rules, encryption or tokenization policies, malware detection, and compliance monitoring. This directly matches the question's description of enforcing security policy between cloud customers and cloud services. Depending on the product and deployment model, a CASB may operate through API connections to cloud applications, an inline forward or reverse proxy, or analysis of cloud-service logs. These approaches enable organizations to monitor sanctioned and unsanctioned cloud use while consistently applying enterprise policy to data and user activity outside the traditional network perimeter. Microsoft describes Defender for Cloud Apps as a CASB that provides visibility, control over data travel, and analytics to identify and address cloud-app risks. The Cloud Security Alliance also identifies policy enforcement and visibility as fundamental CASB capabilities. See Microsoft Defender for Cloud Apps documentation and Cloud Security Alliance CASBs 101.

QUESTION NO: 33

ID

Source

Destination

Protocol

Service

1

172.16.1.1

172.16.1.10

ARP

AddrResolve

2

172.16.1.10

172.16.1.20

TCP 135

RPC Kerberos

3

172.16.1.10

172.16.1.30

TCP 445

SMB WindowsExplorer

4

172.16.1.30

5.29.1.5

TCP 443

HTTPS Browser.exe

5

11.4.11.28

172.16.1.1

TCP 53

DNS Unknown

6

20.109.209.108

172.16.1.1

TCP 443

HTTPS WUS

7

172.16.1.25

bank.backup.com

TCP 21

FTP FileZilla

Which of the following represents the greatest concerns with regard to potential data exfiltration? (Select two.)

A. 1

B. 2

C. 3

D. 4

E. 5

F. 6

G. 7

ANSWER: D G

Explanation:

“4” and “7” are the strongest potential data-exfiltration indicators because both show outbound connections from RFC 1918 internal addresses to destinations outside the private network, using protocols that can carry files or arbitrary application data. Entry “4” shows 172.16.1.30 initiating encrypted HTTPS traffic to the public IP address 5.29.1.5. HTTPS is common business traffic, but encryption prevents network monitoring tools from inspecting transferred content unless TLS inspection or endpoint telemetry is available. An outbound connection to an unrecognized public IP, particularly when its expected business purpose is not established, should be triaged for potentially unauthorized uploads or command-and-control activity.

Entry “7” is an especially direct concern because FileZilla is a file-transfer client and TCP 21 is FTP control traffic. A session from 172.16.1.25 to an external destination named bank.backup.com could transfer organizational files outside the environment. Analysts should validate whether this host, destination, account, transfer volume, and timing are authorized, then review associated FTP data-channel activity and endpoint logs. CompTIA’s CySA+ objectives include analyzing network traffic and identifying indicators of malicious activity, including data exfiltration. CISA also recommends investigating anomalous outbound connections and transfers as possible malicious activity. See the CompTIA exam objectives and CISA’s cybersecurity advisory guidance.

QUESTION NO: 34

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

A. Determine the sophistication of the audience that the report is meant for

B. Include references and sources of information on the first page

C. Include a table of contents outlining the entire report

D. Decide on the color scheme that will effectively communicate the metrics

ANSWER: A

Explanation:

Determine the sophistication of the audience that the report is meant for is the best first step because a “What We Learned” report is a post-incident lessons-learned communication whose content, terminology, format, and level of detail must be appropriate for its readers. Identifying the intended audience first lets the author decide how to frame the incident’s impact, findings, root cause, corrective actions, and remaining risks. Executive leadership generally needs a concise account of business impact, organizational risk, decisions needed, and remediation priorities. Technical responders and system owners need sufficiently detailed timelines, technical findings, affected assets, indicators, and actions to improve detection and response. Legal, compliance, and privacy stakeholders may require emphasis on notification obligations, evidence handling, and control implications. Establishing audience sophistication also helps ensure that the report is actionable rather than either overly technical or too vague to support informed decisions. NIST identifies lessons learned as a key activity after incident recovery, including using the results to improve incident-response processes and capabilities. Effective dissemination of those findings depends on presenting information in a usable form for the stakeholders responsible for decisions and improvements. See NIST SP 800-61 Rev. 2 and CISA Cybersecurity Incident and Vulnerability Response Playbooks.

QUESTION NO: 35

A security analyst identifies a scheduled task on a Windows workstation that launches PowerShell with an encoded command every time a user logs on. Which of the following techniques is most likely being used?

A. Scheduled task persistence

B. ARP poisoning

C. Pass-the-hash

D. SQL injection

ANSWER: A

Explanation:

Scheduled task persistence is the correct answer because the task is configured to execute automatically at user logon. Attackers commonly create or modify scheduled tasks to maintain execution after reboot or user sign-in. The encoded PowerShell command may be used to conceal the command content and make detection more difficult, but the scheduled task is the persistence mechanism described in the scenario.

Analysts should collect the task name, creator, trigger, action, command line, associated account, and creation time, then determine whether similar tasks exist on other systems. MITRE ATT&CK documents scheduled task and job activity as a technique that adversaries may use for execution, persistence, or privilege escalation. See MITRE ATT&CK: Scheduled Task/Job: Scheduled Task.

QUESTION NO: 36

Which of the following documents sets requirements and metrics for a third-party response during an event?

A. BIA
BIA (Business Impact Analysis)

B. DRP
DRP (Disaster Recovery Plan)

C. SLA
SLA (Service Level Agreement)

D. MOU
MOU (Memorandum of Understanding)

ANSWER: C

Explanation:

SLA (Service Level Agreement) is correct because it formally establishes measurable service expectations between an organization and a third-party provider. For an event such as a security incident, outage, or other service disruption, an SLA can define required response and notification time frames, support coverage hours, escalation procedures, restoration or resolution targets, communication requirements, and methods for measuring provider performance. These documented commitments let the customer assess whether the provider met its contractual operational and incident-response obligations. This is particularly important where a provider operates, supports, monitors, or can affect systems and data on the organization's behalf. The agreement gives both parties a shared, objective basis for coordinating response activities and holding the provider accountable for agreed service levels. CompTIA's CySA+ objectives include assessing vendor risk and using appropriate agreements as part of third-party management. NIST also identifies service-level agreements as a mechanism for defining the security and operational requirements applicable to externally provided services. See the CompTIA exam objectives resource and NIST SP 800-53, control SA-9, External System Services.

QUESTION NO: 37

An organization is preparing to decommission a server that processed regulated customer information. Which of the following actions should be performed to reduce the risk of data exposure during decommissioning? (Select two).

A. Sanitize the storage media using an approved method.

B. Remove the server from asset inventory and monitoring systems after decommissioning.

C. Retain the local administrator password for future access.

D. Disable encryption before disposing of the drives.

E. Leave the server connected until the next vulnerability scan completes.

F. Publish the server configuration to all employees.

ANSWER: A B

Explanation:

Sanitize the storage media using an approved method is necessary because the server may contain customer records, temporary files, logs, encryption keys, database files, or other remnants of regulated information. Approved sanitization methods make data recovery infeasible before the media is reused, transferred, or disposed of. The method selected should be appropriate for the media type and the organization's data-handling requirements.

Remove the server from asset inventory and monitoring systems after decommissioning is also appropriate because asset-management records, vulnerability scanning, EDR, SIEM ingestion, and support ownership should reflect the server's retired status. This prevents stale records, unnecessary alerts, and uncertainty about responsibility for an asset that is no longer operating. NIST provides media sanitization guidance in NIST SP 800-88 Rev. 1.

QUESTION NO: 38

Which of the following best describes the key goal of the containment stage of an incident response process?

A. To limit further damage from occurring

B. To get services back up and running

C. To communicate goals and objectives of theincidentresponse plan

D. To prevent data follow-on actions by adversary exfiltration

ANSWER: A

Explanation:

To limit further damage from occurring is the key goal of containment. Once an incident has been identified and initially analyzed, responders must take measured actions to stop the threat from continuing to affect systems, users, data, and business operations. Containment reduces the incident's scope and impact while preserving enough operational capability to support investigation, eradication, and recovery. Depending on the incident, this can include isolating a compromised endpoint, disabling or resetting an affected account, blocking malicious indicators at network controls, restricting access to a vulnerable service, or segmenting a network area. Effective containment decisions balance urgency, business impact, evidence preservation, and the risk that an adversary could spread laterally or cause additional harm. Containment may involve immediate short-term controls followed by longer-term measures that remain in place while responders remove the root cause and validate that the environment is safe. NIST's incident-handling guidance specifically describes containment as limiting the damage caused by an incident and preventing further damage. See NIST SP 800-61 Rev. 2 and the CISA incident response resources.

QUESTION NO: 39

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: B

Explanation:

`tcpdump -n -r packets.pcap host [IP address]` is the appropriate command because it reads the gateway packet-capture file and applies a packet-aware Berkeley Packet Filter (BPF) to identify traffic associated with the suspicious address. The `-r packets.pcap` argument instructs tcpdump to process packets from the specified capture file rather than attempting a live capture. The `host [IP address]` filter matches packets where that address is either the source or destination, which directly supports identifying inbound and outbound connections involving the indicator. The `-n` switch prevents name and service resolution, so tcpdump displays numeric addresses and ports. This improves analysis speed and avoids generating additional DNS traffic that could alter the investigation context or obscure the original IP-based indicator. Tcpdump's documentation describes `-r` as reading packets from a saved capture file and documents the `host` primitive as matching either source or destination host addresses. This approach is a practical CySA+ workflow for scoping network evidence to a known suspicious indicator before performing deeper review of sessions, ports, timestamps, and payloads. See the tcpdump manual page and CompTIA's exam objectives resource.

QUESTION NO: 40

An organization has established a formal change management process after experiencing several critical system failures over the past year. Which of the following are key factors that the change management process will include in order to reduce the impact of system failures? (Select two).

A. Ensure users document a system recovery plan prior to deployment.

B. Perform a full system-level backup following the change.

C. Leverage an audit tool to identify changes that are being made.

D. Identify assets with dependencies that could be impacted by the change.

E. Require diagrams to be completed for all critical systems.

F. Ensure that all assets are properly listed in the inventory management system.

ANSWER: A D

Explanation:

Ensure users document a system recovery plan prior to deployment is a key change-management control because every production change should have a documented contingency method before implementation begins. A recovery, backout, or rollback plan defines how the organization will restore the prior known-good state if the change produces an outage, degraded service, data issue, or unexpected security consequence. Preparing and approving this plan in advance enables a faster, coordinated response and reduces the duration and business impact of a failure.

Identify assets with dependencies that could be impacted by the change is equally essential because changes rarely affect only one isolated system. Dependency and impact analysis identifies connected applications, services, data stores, network components, identity services, integrations, and business processes that may be affected. This analysis supports appropriate risk assessment, test coverage, implementation scheduling, stakeholder notification, and contingency planning. Together, a recovery plan and dependency analysis make changes more predictable and resilient by ensuring the organization understands both how broadly a failure could propagate and how it will restore operations. NIST configuration-management guidance addresses documenting, assessing, approving, implementing, and monitoring changes, including security impact considerations: NIST SP 800-128. CompTIA's CySA+ certification coverage also includes vulnerability and risk-management practices relevant to operational change control: CompTIA CySA+.

QUESTION NO: 41

A public web application hosted in AWS is vulnerable to server-side request forgery. The application must continue to retrieve content from an approved external API. Which of the following controls will best reduce the risk of exploitation? (Select two).

A. Implement egress filtering to allow only approved destinations.

B. Require IMDSv2 on the affected instances.

C. Enable HTTP on TCP port 80 for all inbound sources.

D. Disable TLS certificate validation in the application.

E. Allow the application to resolve any external domain.

F. Add additional local administrator accounts to the web server.

ANSWER: A B

Explanation:

Implementing egress filtering to allow only approved destinations reduces SSRF risk by preventing the web application from making arbitrary outbound requests. The organization can permit only the required external API endpoints and deny connections to internal address ranges, cloud management endpoints, and other unapproved destinations. This limits an attacker's ability to use the application as a proxy to access sensitive internal services.

Requiring IMDSv2 is also appropriate for AWS workloads because IMDSv2 requires a session-oriented token before an application can retrieve instance metadata. This adds protection against common SSRF attempts targeting the instance metadata service to obtain temporary IAM credentials. These controls should complement permanent application remediation, including strict URL allowlisting and validation. AWS documents IMDSv2 protections in the EC2 instance metadata service documentation. OWASP describes SSRF defenses in the Server-Side Request Forgery Prevention Cheat Sheet.

QUESTION NO: 42

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: A

Explanation:

Reschedule the upgrade and deploy the patch is the appropriate remediation because the organization has an explicit service-level requirement to patch critical vulnerabilities within 24 hours. Critical findings require expedited treatment because they can create substantial business impact if exploited. When planned routine maintenance conflicts with an urgent security remediation deadline, the normal change-management process should be adjusted to accommodate the higher-priority, risk-reducing patch. The asset owner and change-management stakeholders should coordinate an emergency or expedited change, assess patch dependencies and rollback procedures, and deploy the vendor-approved fix as safely as practical within the required window. This action directly removes or reduces the known vulnerability exposure while maintaining compliance with the defined SLA. NIST describes enterprise patch management as identifying, prioritizing, acquiring, testing, deploying, and verifying patches in a manner appropriate to organizational risk; critical vulnerabilities with short remediation timelines warrant prioritized action. CISA similarly emphasizes the importance of prompt remediation for vulnerabilities that pose significant risk. See NIST SP 800-40 Revision 4 and CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 43 - (SIMULATION)

You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following.

There must be one primary server or service per device. Only default port should be used

Non- secure protocols should be disabled.

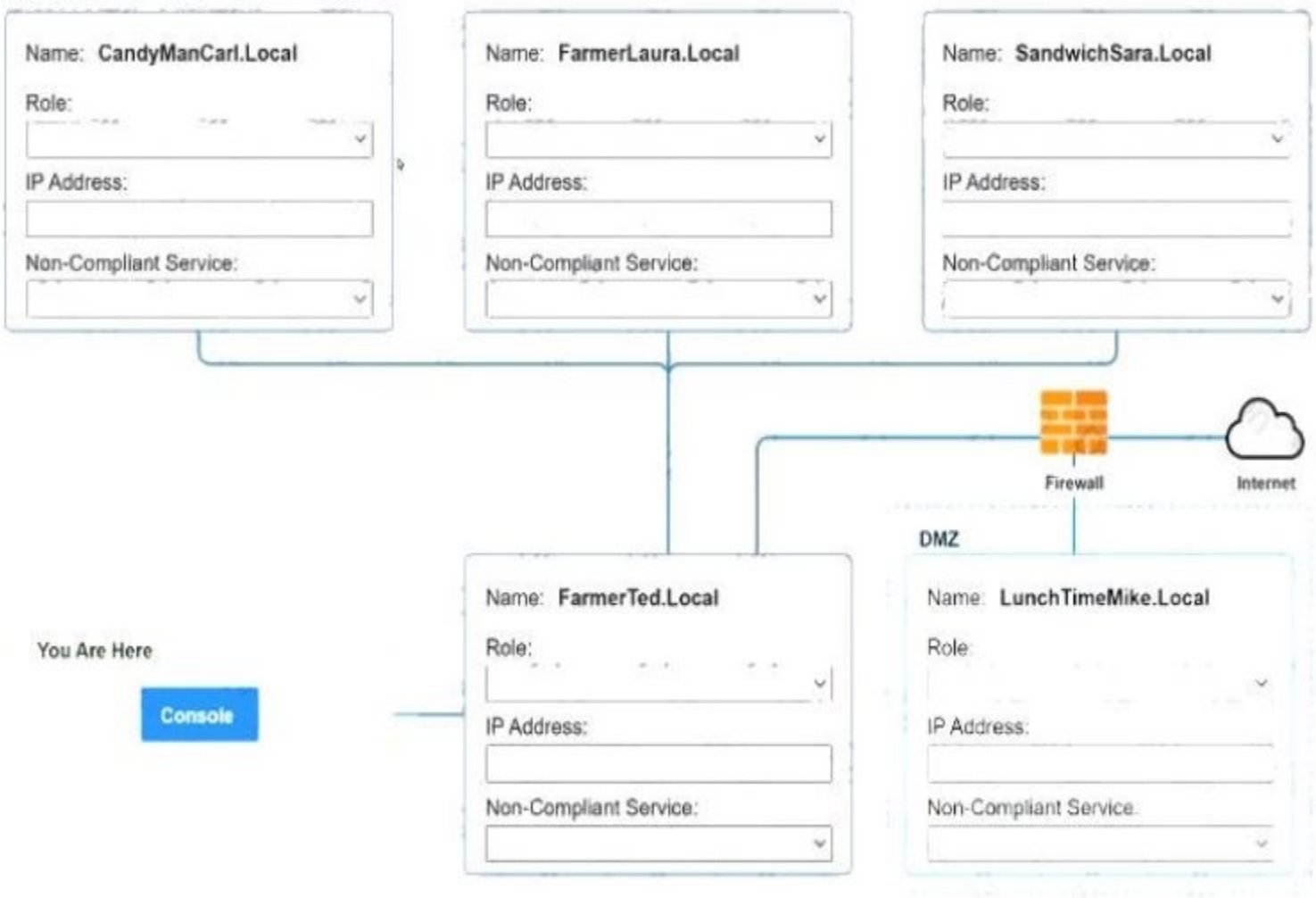
The corporate internet presence should be placed in a protected subnet Instructions :

Using the available tools, discover devices on the corporate network and the services running on these devices.

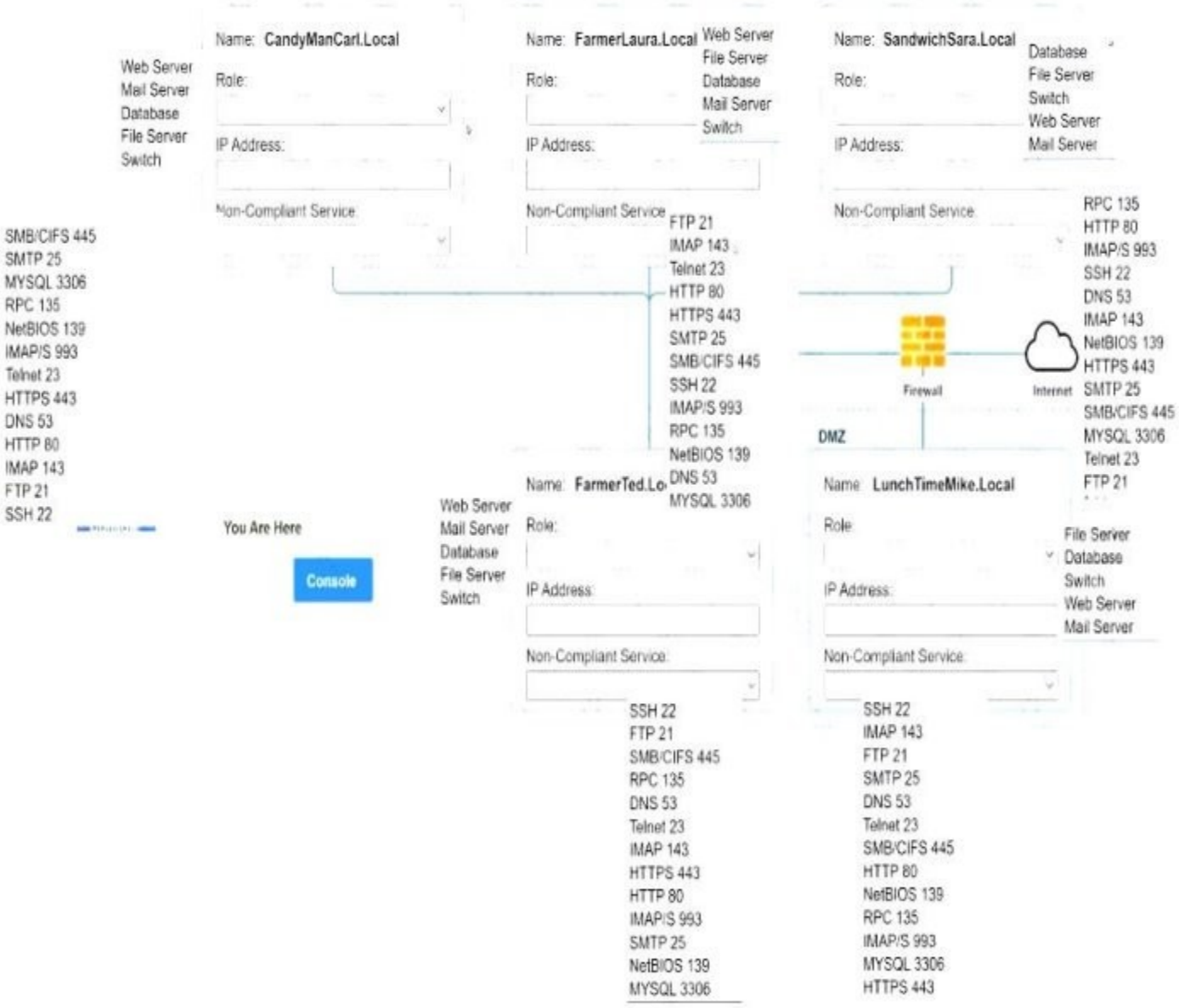
You must determine

ip address of each device

The primary server or service each device



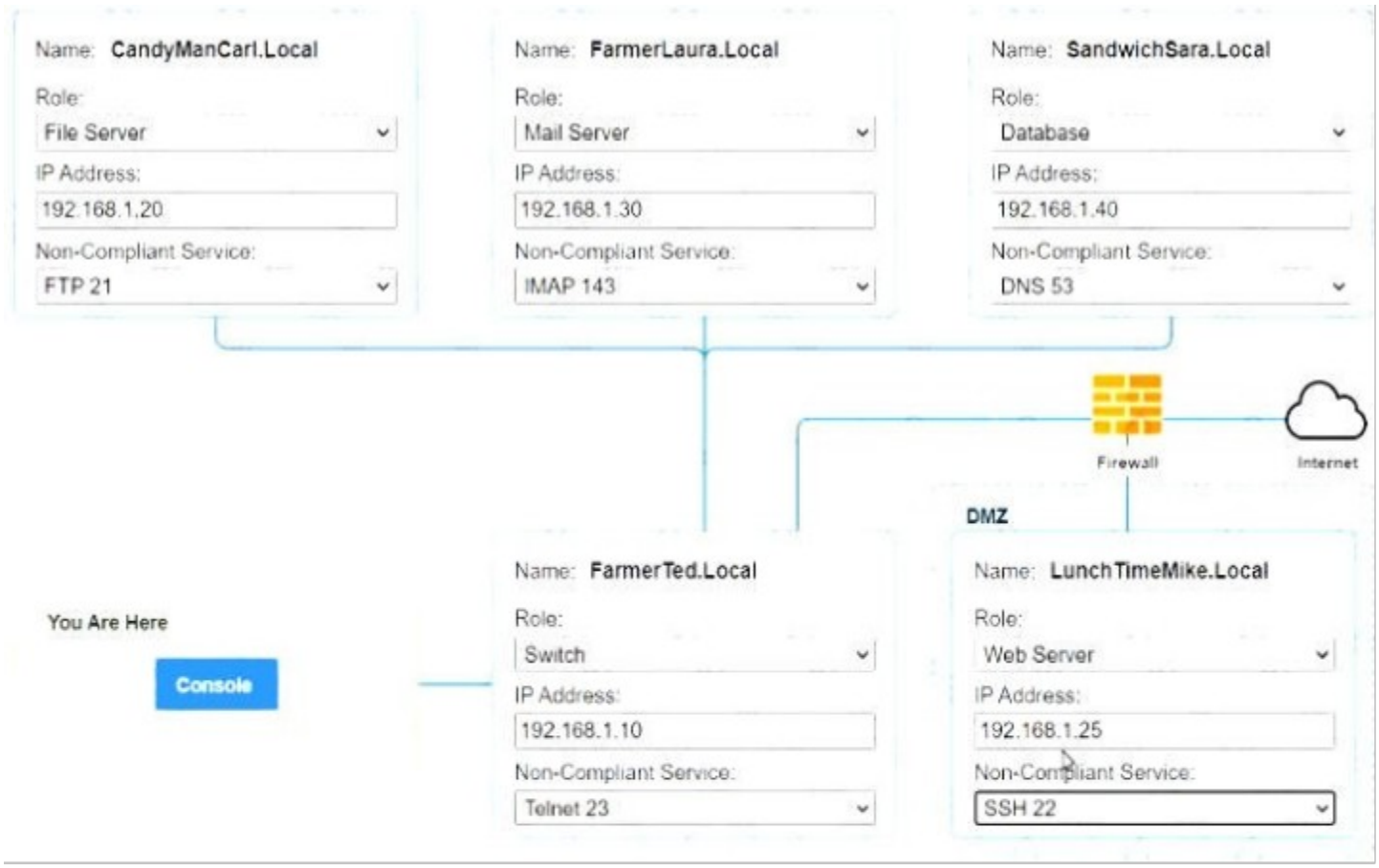
The protocols that should be disabled based on the hardening guidelines

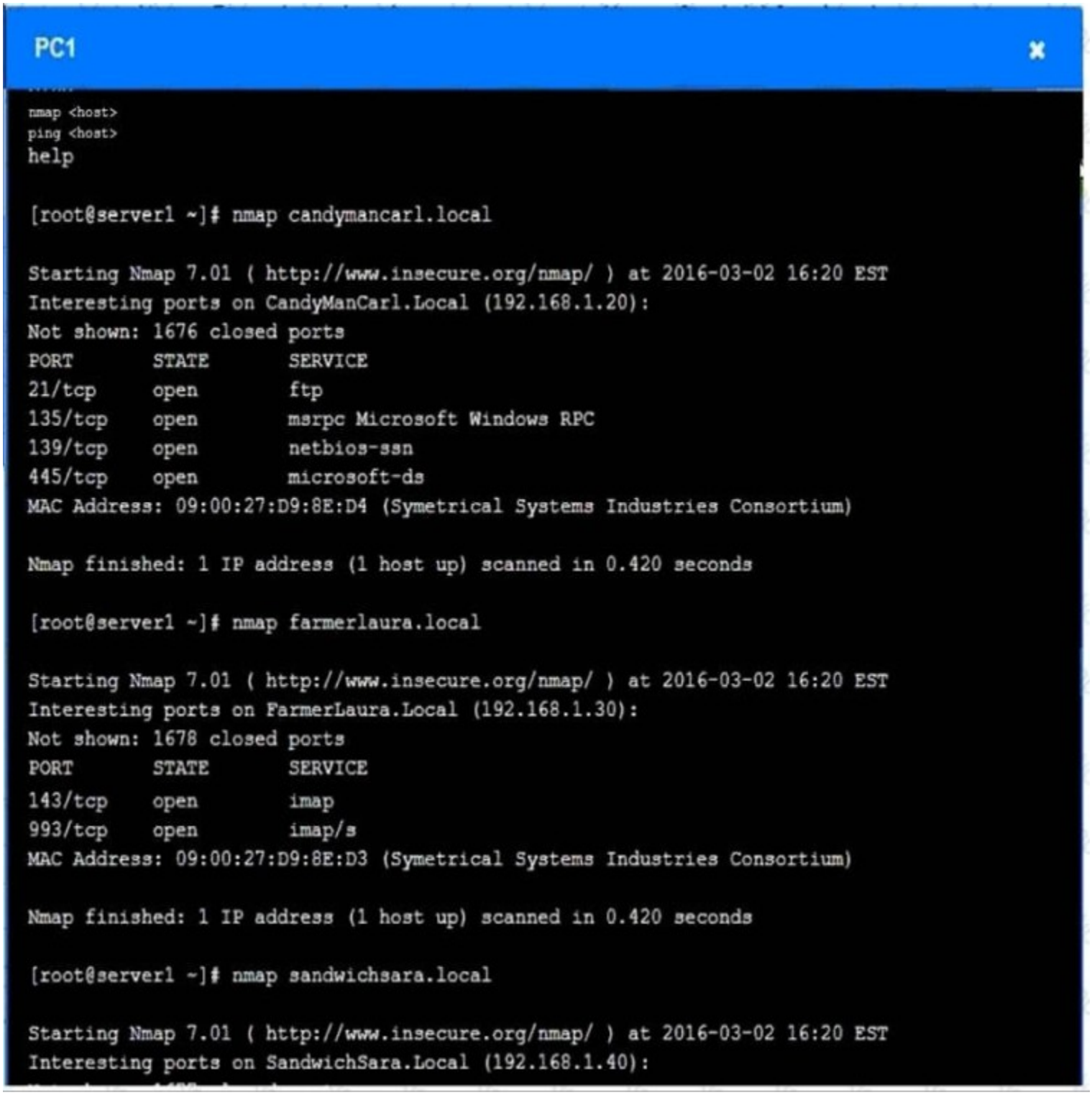


see the answer below in explanation:

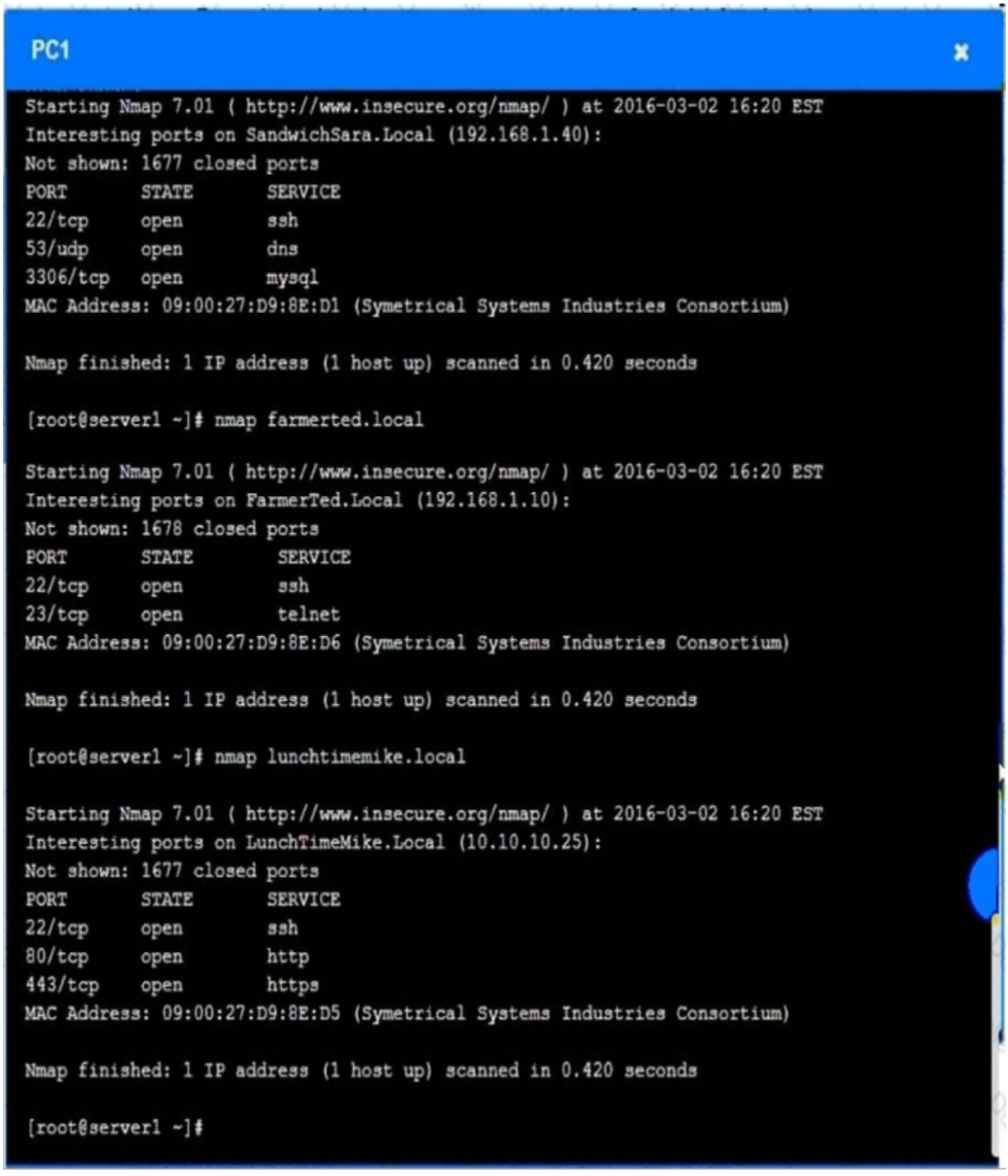
Explanation:

Answer below images


Name: CandyManCarl.Local
Role:
File Server
IP Address:
192.168.1.20
Non-Compliant Service:
FTP 21
Name: FarmerLaura.Local
Role:
Mail Server
IP Address:
192.168.1.30
Non-Compliant Service:
IMAP 143
Name: SandwichSara.Local
Role:
Database
IP Address:
192.168.1.40
Non-Compliant Service:
DNS 53
Firewall
Internet
DMZ
You Are Here
Console
Name: FarmerTed.Local
Role:
Switch
IP Address:
192.168.1.10
Non-Compliant Service:
Telnet 23
Name: LunchTimeMike.Local
Role:
Web Server
IP Address:
192.168.1.25
Non-Compliant Service:
SSH 22



A computer screen with white text Description automatically generated



ANSWER: See the explanation for the answer

Explanation:

Use Nmap service/version detection to identify every live host, its IP address, and its primary service:

`nmap -sS -sV -O -Pn -p- <corporate-network-CIDR>`

For a faster initial inventory scan, use:

```
nmap -sn <corporate-network-CIDR>
nmap -sV -Pn -p- <each-live-IP>
```

Record the `Host is up` addresses and use the detected service on the standard/default port as the device's primary service. Examples of acceptable primary-service mappings are:

`22/tcp` → SSH server
`53/tcp` or `53/udp` → DNS server
`25/tcp` → SMTP/mail server
`80/tcp` or `443/tcp` → web server
`445/tcp` → file server/SMB server
`3306/tcp` → MySQL database server

Hardening action: retain only one required primary server/service per device and ensure it uses its IANA default port. A service found on an alternate/high port is a hardening violation; move it to its default port or remove it if it is not required.

Protocols to disable:

`Telnet` (`23/tcp`) — replace with SSH.
`FTP` (`21/tcp`) and `TFTP` (`69/udp`) — replace with SFTP/SCP or another encrypted file-transfer method.
`HTTP` (`80/tcp`) when it is serving unencrypted traffic — replace/redirect to HTTPS (`443/tcp`).
`rlogin`, `rsh`, and `rexec` — disable and use SSH.
Unencrypted `POP3`/`IMAP` and non-TLS management services — disable or require TLS.
`SNMPv1`/`SNMPv2c` if present — disable or migrate to SNMPv3.
`SMBv1` if present — disable it; retain only a supported SMB version if file sharing is required.

Network placement: any externally reachable corporate web, mail relay, or public DNS service must be placed in the protected subnet/DMZ. It must not be directly hosted on the internal corporate LAN.

Do not disable secure, required services merely because they are open on their normal ports. For example, `SSH/22` and `HTTPS/443` are normally retained when required; the insecure alternatives above are the services that should be disabled.

QUESTION NO: 44

The Chief Information Security Officer wants the same level of security to be present whether a remote worker logs in at home or at a coffee shop. Which of the following should be recommended as a starting point?

A. Non-persistent virtual desktop infrastructures

B. Passwordless authentication

C. Standard-issue laptops

D. Serverless workloads

ANSWER: A

Explanation:

Non-persistent virtual desktop infrastructures provide a centrally controlled workspace that is delivered to the remote user regardless of the network or physical location from which the user connects. The organization manages the virtual desktop image, its operating-system and application patches, endpoint security configuration, access controls, and logging centrally. Each user session can begin from an approved, known-good image and be discarded or reset at logoff, which limits persistence of user changes, malware, and sensitive enterprise data on the desktop environment. This creates a more consistent security baseline for work performed from a home network or an untrusted public Wi-Fi location. Sensitive processing and data can remain within managed infrastructure rather than residing on the user's local device. A secure VDI deployment should still use strong identity controls, encrypted remote-access connections, and appropriate monitoring, but non-persistent VDI is the best starting point among the available choices for standardizing the remote work environment. NIST's telework guidance emphasizes centrally managed remote-access architectures and protecting information used outside organizational facilities: NIST SP 800-46 Rev. 2. Microsoft also describes security considerations for centrally managed virtual desktop deployments: Azure Virtual Desktop security guide.

QUESTION NO: 45 - (HOTSPOT)

HOTSPOT

The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.

If the venerability is not valid, the analyst must take the proper steps to get the scan clean.

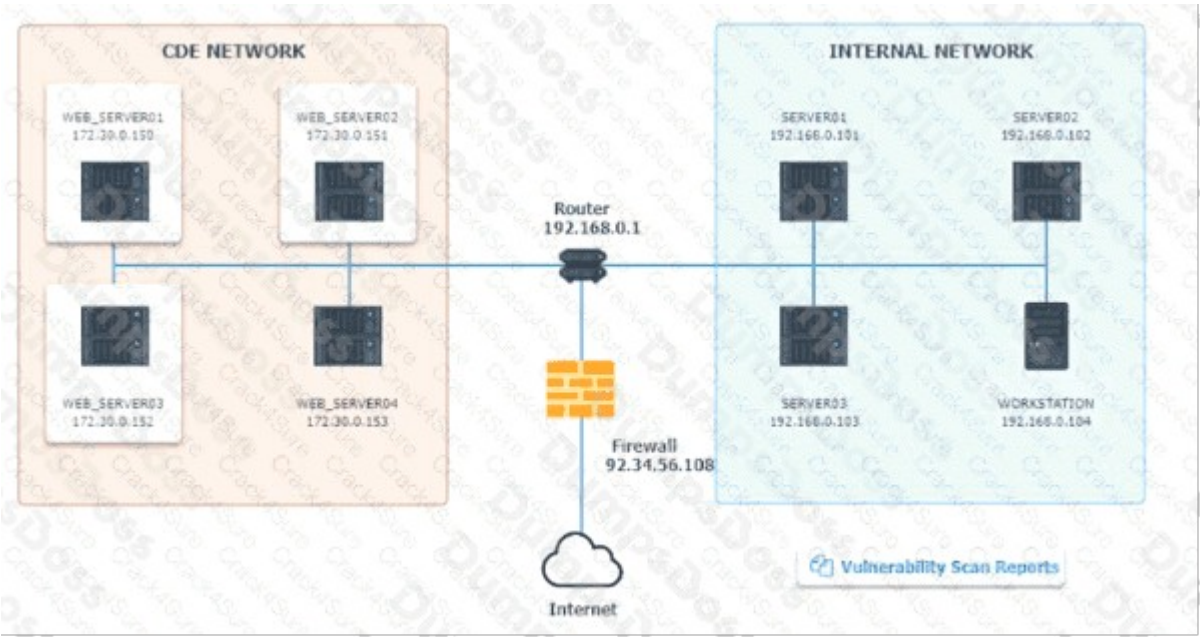
If the venerability is valid, the analyst must remediate the finding.

After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

INTRUCTIONS:

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.

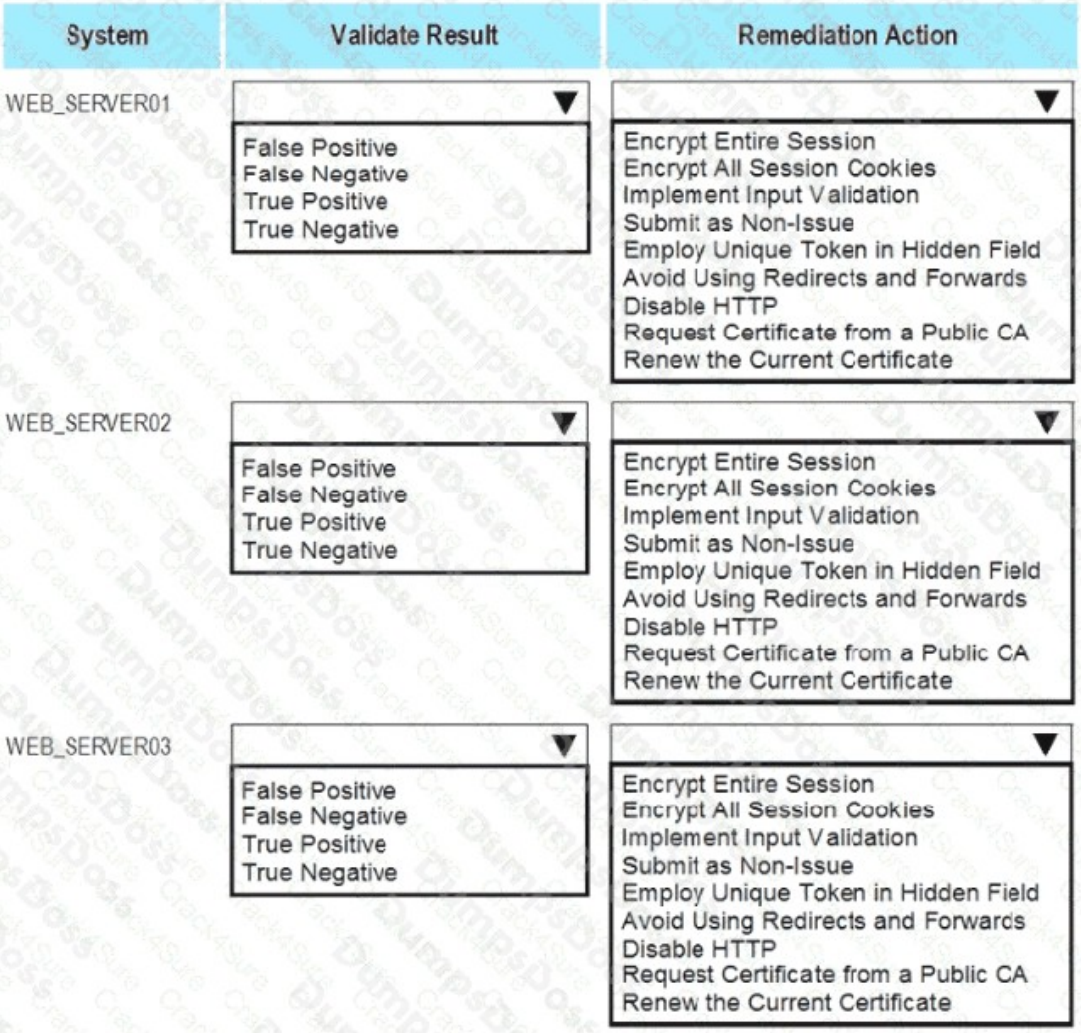


STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

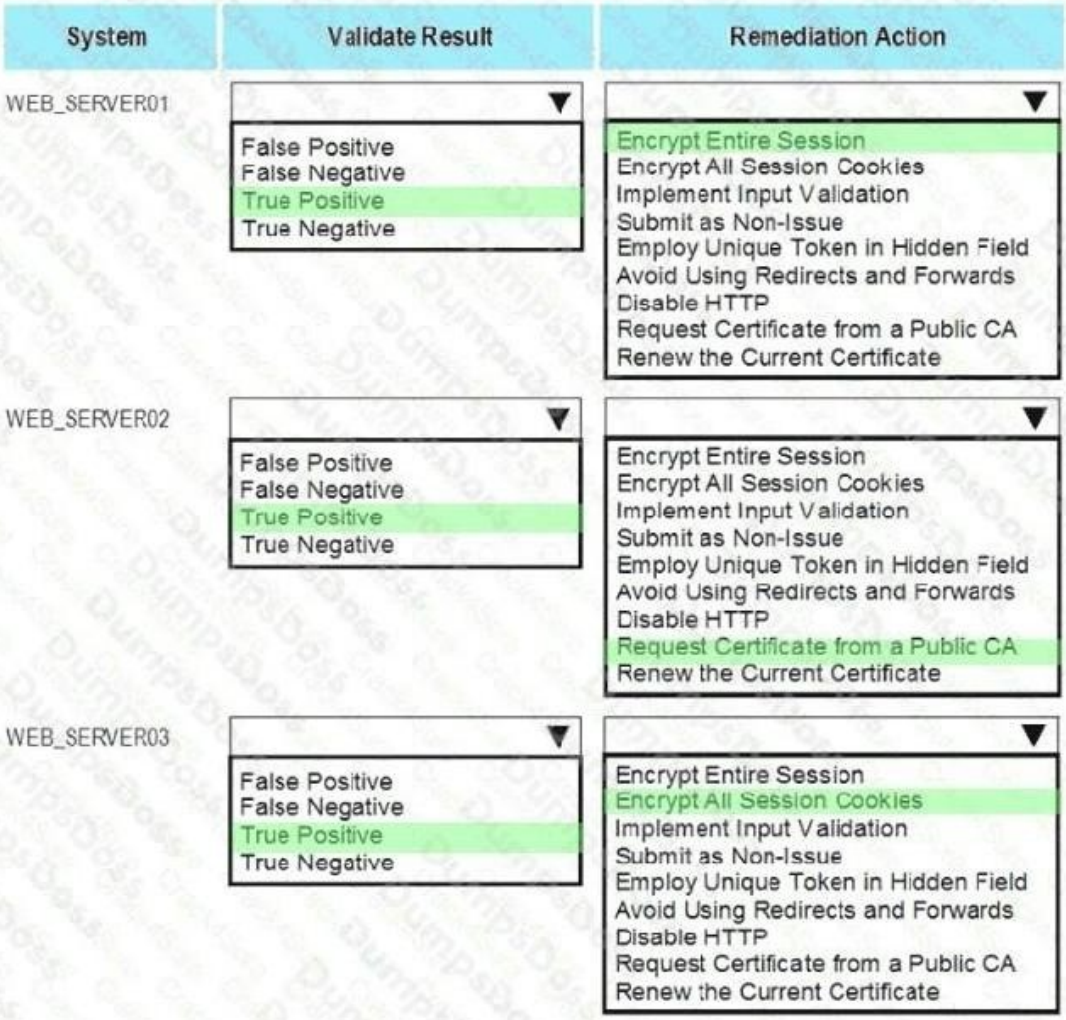


ANSWER:

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.



Explanation:

Each listed scan result is validated as a true positive because it identifies a condition that creates a real security exposure on a web server handling sensitive traffic. For WEB_SERVER01, the appropriate remediation is to encrypt the entire session. Full-session encryption protects data in transit, including authentication data, session identifiers, and any cardholder-related information, by ensuring the connection uses strong TLS rather than permitting cleartext transmission. PCI DSS requires strong cryptography for cardholder data sent across open or public networks; see the PCI Security Standards Council standards overview.

For WEB_SERVER02, requesting a certificate from a public certificate authority restores the trust relationship required for a public-facing TLS service. A certificate issued by a publicly trusted CA enables browsers and other clients to validate the server identity through a recognized certificate chain. This is essential to establishing an authenticated TLS connection and preventing users from receiving certificate-trust warnings. NIST guidance on TLS configuration and authentication is available in NIST SP 800-52 Rev. 2.

For WEB_SERVER03, encrypting all session cookies protects session state during HTTPS use. Sensitive cookies need secure transport protections so browsers send them only through encrypted connections, reducing the likelihood that session tokens are exposed in transit. The OWASP guidance on the Secure Cookie Attribute explains the importance of restricting cookies to HTTPS. Therefore, the completed selections correctly validate every finding and pair each server with the remediation that directly addresses its confirmed vulnerability.

QUESTION NO: 46

A security team has identified a critical vulnerability in an internet-facing application. The vendor patch will not be available for several days, but the application must remain online. Which of the following are the best compensating controls? (Select two).

A. Deploy a virtual patch at the WAF.

B. Restrict access to approved source networks.

C. Disable all application logging.

D. Publish the vulnerability details on the application home page.

E. Increase the session timeout for all users.

F. Remove endpoint protection from the web server.

ANSWER: A B

Explanation:

Deploying a virtual patch at the WAF is an effective compensating control because a targeted rule can detect and block requests that match the known exploit pattern before they reach the vulnerable application. This reduces exposure during the period before the vendor provides a permanent remediation. The rule should be tested and monitored to ensure it blocks malicious requests without disrupting legitimate application traffic.

Restricting access to approved source networks is also appropriate when the application does not require unrestricted public access. Network restrictions can reduce the number of potential attackers able to reach the vulnerable service by allowing only required partner, corporate, VPN, or trusted administrative source ranges. This reduces attack surface while maintaining necessary availability. NIST describes compensating controls as alternative safeguards that can provide equivalent protection when primary controls cannot be implemented. OWASP describes virtual patching practices in its Virtual Patching Best Practices.

QUESTION NO: 47

A security analyst is working on a server patch management policy that will allow the infrastructure team to be informed more quickly about new patches. Which of the following would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly? (Select two).

A. Hostname

B. Missing KPI

C. CVE details

D. POC availability

E. loCs

F. npm identifier

ANSWER: C D

Explanation:

CVE details are required because a CVE provides the standardized identifier that connects a reported vulnerability to vendor advisories, affected product versions, technical descriptions, available fixes, and severity information. Using the CVE identifier, infrastructure personnel can rapidly determine whether their server software is affected, obtain the applicable vendor patch or mitigation, and document remediation against a consistent vulnerability record. The CVE Program describes CVE Records as standardized identifiers and associated information for publicly known cybersecurity vulnerabilities: CVE Program overview.

POC availability is also important remediation-prioritization information. A proof of concept demonstrates that a vulnerability can be exploited under defined conditions. When exploit code or a reliable proof of concept is available, teams can elevate the urgency of patch deployment, validate exposure in their environment, and apply compensating controls while a patch is being tested or rolled out. This supports risk-based patch management by helping the team focus first on vulnerabilities with credible, actionable exploitation potential. NIST recommends prioritizing patch and vulnerability response based on risk and establishing processes to identify, assess, and remediate vulnerabilities promptly: NIST SP 800-40 Rev. 4.

QUESTION NO: 48

An analyst is reviewing proxy logs after receiving a threat intelligence report containing a malicious file hash. Which of the following actions will best determine whether the organization downloaded the identified file?

A. Search the proxy logs for the file hash.

B. Search DNS logs for the user account.

C. Review domain password policy settings.

D. Compare firewall rules to the threat report.

ANSWER: A

Explanation:

Search the proxy logs for the file hash is the best action because secure web gateways and proxy services can record file-download metadata, including hashes, URLs, source users, requesting hosts, timestamps, and disposition results. A direct hash search can identify whether the known malicious artifact traversed the proxy and provide the endpoint and user context needed for scoping and containment.

Searching DNS logs could show whether a system resolved a related domain, but it cannot establish that the specific file was downloaded. Reviewing authentication logs or firewall rules may provide useful context during the investigation, but neither directly confirms delivery of the malicious file. NIST identifies file hashes as useful technical indicators for detecting and analyzing malicious activity. See NIST SP 800-61 Rev. 2 and CISA Information Sharing.

QUESTION NO: 49

While a security analyst for an organization was reviewing logs from web servers. the analyst found several successful attempts to downgrade HTTPS sessions to use cipher modes of operation susceptible to padding oracle attacks. Which of the following combinations of configuration changes should the organization make to remediate this issue? (Select two).

A. Configure the server to prefer TLS 1.3.

B. Remove cipher suites that use CBC.

C. Configure the server to prefer ephemeral modes for key exchange.

D. Require client browsers to present a user certificate for mutual authentication.

E. Configure the server to require HSTS.

F. Remove cipher suites that use GCM.

ANSWER: A B

Explanation:

"Configure the server to prefer TLS 1.3." and "Remove cipher suites that use CBC." are the appropriate remediation measures. Padding-oracle risks arise when an endpoint processes malformed padding in Cipher Block Chaining encryption in a distinguishable way. An attacker able to negotiate or downgrade a connection to a CBC-based TLS cipher suite may use those observable differences to recover protected plaintext over many requests.

Removing cipher suites that use CBC prevents the affected mode from being selected during TLS negotiation. The remaining permitted suites should use modern authenticated-encryption designs, such as AES-GCM or ChaCha20-Poly1305, which provide encryption and integrity protection without CBC padding processing. The organization should apply this restriction to every still-enabled legacy TLS version, particularly any retained TLS 1.2 configuration.

Configuring the server to prefer TLS 1.3 further reduces downgrade exposure because TLS 1.3 defines only authenticated-encryption cipher suites and does not support CBC-mode suites. TLS 1.3 also includes downgrade-sentinel behavior in its server random value for certain version-negotiation scenarios. Together, prioritizing TLS 1.3 and eliminating CBC suites ensure that a successful negotiation cannot select the padding-oracle-susceptible cipher mode. See RFC 8446, The Transport Layer Security Protocol Version 1.3 and NIST SP 800-52r2.

QUESTION NO: 50

A security analyst is reviewing a recent vulnerability scan report for a new server infrastructure. The analyst would like to make the best use of time by resolving the most critical vulnerability first. The following information is provided:

Hostname	Asset priority	CVSS score	Exploitable?
SVR01	Medium	8.9	No
SVR02	Medium	7.1	Yes
SVR03	Low	3.5	Yes
SVR04	High	6.7	No

Which of the following should the analyst concentrate remediation efforts on first?

A. SVR01

B. SVR02

C. SVR03

D. SVR04

ANSWER: B

Explanation:

SVR02 should receive remediation attention first because the scan information identifies it as a high-severity vulnerability with confirmed exploitability. A CVSS score of 7.1 falls within the High severity range, indicating potentially significant impact if the weakness is successfully exploited. More importantly for operational prioritization, confirmed exploitability means an attacker has a practical path to use the vulnerability rather than the issue being only a theoretical condition. This increases the likelihood component of risk and creates a more immediate exposure for the new server infrastructure.

Effective vulnerability management is risk-based: severity scores are an important starting point, but remediation decisions should also account for exploit availability or evidence of exploitation, exposure, asset importance, and compensating controls. Addressing a high-severity, exploitable weakness first reduces the organization's near-term attack surface and is the best use of limited remediation time. FIRST explains that CVSS measures technical severity rather than an organization's complete risk, so analysts should apply contextual threat intelligence when setting remediation priorities. CISA similarly emphasizes prioritizing vulnerabilities known to be exploited because they present heightened real-world risk. See FIRST CVSS and the CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 51

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 SHA-256 hash.

ANSWER: D

Explanation:

Make a forensic image of the device and create a SHA-256 hash is the best evidence-preservation action because it produces a bit-for-bit acquisition of the laptop's storage while leaving the original device available for secure preservation. A properly acquired forensic image can include active files, filesystem metadata, logs, unallocated space, deleted-file remnants, and other artifacts that may be material to an HR or legal investigation. Analysis should be conducted on verified working copies rather than directly on the original laptop, minimizing the risk that investigative activity changes evidence.

Calculating and recording a SHA-256 cryptographic hash at acquisition establishes a baseline integrity value for the image. Investigators can recalculate the hash when the image is copied, transferred, or presented for review to demonstrate that its contents have not changed. This practice supports a defensible chain of custody, reproducibility, and the reliability of findings. The original device should also be secured and access documented while the image is handled under established forensic procedures. NIST guidance discusses preserving digital evidence and using forensic acquisition techniques in NIST SP 800-86; NIST's forensic-science materials also address digital-evidence integrity and handling in its Digital Evidence resources.

QUESTION NO: 52

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

Security Policy 1006: Vulnerability Management

1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.

2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.

3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch?

A)

Name: THOR.HAMMER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Internal System

B)

Name: CAP.SHIELD
CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
External System

C)

Name: LOKI.DAGGER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
External System

D)

Name: THANOS.GAUNTLET
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Internal System

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: B

Explanation:

Option B is the highest remediation priority because the policy establishes a specific decision sequence based on CVSS v3.1 base metrics and organizational business priorities. The analyst must first assess exploitability and impact using the CVSS Base Score Metric Group, which captures the vulnerability's inherent technical characteristics without incorporating temporary or environmental factors. When candidates present a tradeoff involving impact to confidentiality and availability, the policy explicitly directs the organization to give confidentiality the greater weight. This reflects the company's stated need to protect data from unauthorized disclosure. The policy also directs the analyst to prioritize publicly available systems and services over internally available systems when prioritization choices are necessary. Therefore, the vulnerability represented by Option B best satisfies the policy's combined requirements: CVSS-based evaluation, emphasis on confidentiality impact, and the elevated urgency assigned to an externally accessible asset or service. This is a policy-driven prioritization decision rather than a decision based solely on an overall numerical severity label. The CVSS v3.1 specification defines the Exploitability and Impact metric groups used for this analysis: FIRST CVSS v3.1 Specification. CompTIA's CySA+ objectives also include vulnerability management and using vulnerability-scoring information to support remediation prioritization: CompTIA Exam Objectives.

QUESTION NO: 53

Which of the following responsibilities does the legal team have during an incident management event? (Select two).

A. Coordinate additional or temporary staffing for recovery efforts.

B. Review and approve new contracts acquired as a result of an event.

C. Advise the Incident response team on matters related to regulatory reporting.

D. Ensure all system security devices and procedures are in place.

E. Conduct computer and network damage assessments for insurance.

F. Verify that all security personnel have the appropriate clearances.

ANSWER: B C

Explanation:

The legal team is responsible for reviewing and approving new contracts acquired as a result of an event because incident response can require rapid engagement of external organizations, including digital-forensics firms, breach-response counsel, public-relations providers, recovery specialists, and managed security service providers. Legal review helps ensure the organization has appropriate contractual terms for confidentiality, scope of work, liability, evidence handling, privacy obligations, and preservation of attorney-client privilege or work-product protections where applicable. The legal team also advises the Incident response team on matters related to regulatory reporting. Counsel evaluates whether the incident triggers notification obligations under applicable breach-notification laws, sector-specific rules, contractual commitments, or privacy regulations. This guidance includes identifying relevant jurisdictions, required recipients, reporting deadlines, required notification content, and the need to coordinate communications with regulators, law enforcement, cyber-insurance carriers, and affected parties. These responsibilities allow incident responders to contain and remediate the event while ensuring response decisions and external communications meet the organization's legal and compliance duties. NIST identifies legal advisers as key incident-response stakeholders for matters involving reporting requirements, liability, privacy,

and evidence handling; see NIST SP 800-61 Rev. 2. CompTIA's current exam objectives resources are available through the CompTIA Exam Objectives page.

QUESTION NO: 54

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 is the appropriate authentication method because the analyst is building a non-interactive script that must authenticate to cloud APIs and collect asset configuration throughout the tenancy. Public-key cryptography supports this automation without requiring a person to complete an interactive sign-in each time the script runs. The cloud provider or identity service associates the public key with an authorized principal, while the script securely retains the private key and uses it to sign or prove authorization for requests. This enables repeatable collection during incident response and allows access to be controlled through narrowly scoped IAM policies, logging, key rotation, and secure storage of the private key. The word "tenancy" is especially associated with Oracle Cloud Infrastructure, where API requests use signing keys: a user or workload registers an API signing public key and uses the corresponding private key to sign API requests. OCI's CLI and SDK tools similarly use key-based API credentials for programmatic administration and inventory retrieval. See Oracle's API signing key documentation and CLI configuration documentation.

QUESTION NO: 55

In the last hour, a high volume of failed RDP authentication attempts has been logged on a critical server. All of the authentication attempts originated from the same remote IP address and made use of a single valid domain user account. Which of the following mitigating controls would be most effective to reduce the rate of success of this brute-force attack? (Select two).

A. Increase the granularity of log-on event auditing on all devices.

B. Enable host firewall rules to block all outbound traffic to TCP port 3389.

C. Configure user account lockout after a limited number of failed attempts.

D. Implement a firewall block for the IP address of the remote system.

E. Install a third-party remote access tool and disable RDP on all devices.

F. Block inbound to TCP port 3389 from untrusted remote IP addresses at the perimeter firewall.

ANSWER: C F

Explanation:

Configure user account lockout after a limited number of failed attempts directly limits the number of password guesses that can be made against the targeted valid domain account. Once the configured failed-attempt threshold is reached, the account is locked for the organization's defined duration or until an administrator unlocks it. This materially reduces the likelihood that repeated password guessing will eventually identify the correct password, while also generating a clear condition for investigation and response. The threshold, duration, and reset-counter values should be selected carefully to balance brute-force resistance with the risk of operational disruption. Microsoft documents these settings in its Account lockout policy guidance.

Block inbound to TCP port 3389 from untrusted remote IP addresses at the perimeter firewall reduces the exposed attack surface before authentication traffic reaches the critical server. RDP normally listens on TCP 3389, so applying source-based restrictions—ideally permitting only approved administrative networks, a VPN gateway, or a hardened jump host—prevents untrusted internet hosts from initiating RDP authentication attempts. Combining network-access restrictions with account lockout provides both preventative protection at the perimeter and a safeguard if an authorized access path is abused. Microsoft identifies the default RDP listening port in its Remote Desktop listener documentation.

QUESTION NO: 56

The analyst reviews the following endpoint log entry:

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {HOSTName}
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

Which of the following has occurred?

A. Registry change

B. Rename computer

C. New account introduced

D. Privilege escalation

ANSWER: C

Explanation:

New account introduced is correct because the endpoint log records the creation of a user identity on the Windows endpoint. Windows logs account-creation activity under the User Account Management audit category; in particular, Security Event ID 4720 is generated when a user account is created. The relevant event data identifies the newly created account and the security principal that performed the creation, allowing an analyst to establish both what identity was introduced and the context in which it was added.

This is significant during triage and threat hunting because unauthorized account creation can establish durable access. An attacker or unauthorized administrator may create a local or domain account for later authentication, use it to evade reliance on an existing compromised account, or assign it roles in subsequent actions. The directly evidenced occurrence in the log is the account's introduction, so the analyst should validate whether the account was approved, whether its naming and creation time are expected, who initiated the event, and whether later logs show authentication or group-membership changes involving that identity. Microsoft's audit-event reference defines Event ID 4720 as "A user account was created"; see Microsoft: Event 4720. For account-management monitoring context, see Microsoft: Audit User Account Management.

QUESTION NO: 57

Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

A. Mean time to detect

B. Number of exploits by tactic

C. Alert volume

D. Quantity of intrusion attempts

ANSWER: A

Explanation:

Mean time to detect is the most appropriate metric because the combined purpose of SIEM, SOAR, and ticketing investments is to improve the speed and consistency with which security-relevant activity is identified and handled as an actionable alert. A SIEM aggregates logs and telemetry from across the environment, correlates events, and generates detections that help analysts recognize potential incidents earlier. SOAR platforms enrich alerts, automate repetitive triage activities, and apply playbooks, reducing the time between an alert being generated and its recognition as a security event. A ticketing system records alert creation, ownership, escalation, and status changes with timestamps, providing the operational data needed to calculate and trend detection performance consistently over time.

Tracking mean time to detect lets the organization assess whether these investments are reducing the period during which malicious activity can remain unidentified. This supports the Detect function of the NIST Cybersecurity Framework, which emphasizes timely discovery and analysis of cybersecurity events. It is also a meaningful operational metric because it can be measured repeatedly and used to identify workflow, telemetry, or automation improvements. See the NIST Cybersecurity Framework and IBM's overview of security orchestration, automation, and response.

QUESTION NO: 58

An analyst is investigating suspected Kerberoasting activity in an Active Directory environment. Which of the following findings would most strongly support the analyst's conclusion? (Select two).

A. A high volume of service-ticket requests for service accounts from a single workstation.

B. Service-ticket requests using RC4 encryption for service accounts.

C. Repeated DNS queries for external TXT records.

D. Multiple failed VPN logons against a disabled account.

E. A web server certificate approaching its expiration date.

F. An increase in outbound SMTP messages from a marketing system.

ANSWER: A B

Explanation:

A high volume of service-ticket requests for service accounts from a single workstation is a strong indicator of possible Kerberoasting. In this technique, an attacker requests Kerberos ticket-granting service tickets for accounts with service principal names and then attempts to crack the ticket data offline to recover service-account passwords. A workstation that normally does not request numerous tickets for many service accounts should be investigated.

Service-ticket requests using RC4 encryption for service accounts are also suspicious, particularly in environments where stronger encryption types are expected. Attackers may request tickets using RC4 because the resulting ticket data can be more favorable for offline password-cracking attempts. The analyst should correlate the Kerberos activity with account behavior, endpoint process execution, PowerShell logs, and authentication events before confirming the incident. MITRE ATT&CK documents Kerberoasting at MITRE ATT&CK: Kerberoasting. Microsoft documents Kerberos service-ticket auditing through event ID 4769 in Microsoft event 4769 documentation.

QUESTION NO: 59

A company's internet-facing web application has been compromised several times due to identified design flaws. The company would like to minimize the risk of these incidents from reoccurring and has provided the developers with better security training. However, the company cannot allocate any more internal resources to the issue. Which of the following are the best options to help identify flaws within the system? (Select two).

A. Deploying a WAF

B. Performing a forensic analysis

C. Contracting a penetration test

D. Holding a tabletop exercise

E. Creating a bug bounty program

F. Implementing threat modeling

ANSWER: C E

Explanation:

Contracting a penetration test and Creating a bug bounty program are the best choices because they use external security expertise to identify application flaws without requiring the company to assign additional internal personnel. A contracted penetration test provides a defined, focused assessment by experienced testers who evaluate the internet-facing application using realistic adversarial techniques. It can validate whether the design weaknesses associated with prior compromises remain exploitable and identify further issues in areas such as authorization, authentication, session management, input handling, and business logic. The OWASP Web Security Testing Guide describes a systematic approach to assessing web-application security controls and vulnerabilities.

Creating a bug bounty program extends vulnerability discovery beyond a one-time engagement by enabling independent external researchers to submit findings under established rules, scope, and disclosure procedures. This provides diverse testing perspectives and can identify issues that a single assessment may not encounter. A well-managed program includes clear reporting channels, triage, remediation coordination, and safe-harbor expectations. OWASP guidance for receiving and managing reports is available in its Vulnerability Disclosure Cheat Sheet. Together, these approaches directly support the objective of finding technical and design flaws while accommodating the stated internal-resource constraint.

QUESTION NO: 60

A development team is adding security testing to a CI/CD pipeline. The organization wants to identify insecure coding patterns and vulnerable third-party libraries before an application is deployed. Which of the following should be implemented? (Select two).

A. Static application security testing

B. Software composition analysis

C. Network port scanning

D. Full disk encryption

E. Endpoint detection and response

F. Packet capture analysis

ANSWER: A B

Explanation:

Static application security testing and software composition analysis are the correct choices. Static application security testing examines source code, bytecode, or binaries without executing the application. It can identify insecure coding patterns, such as injection weaknesses, unsafe functions, hardcoded secrets, and improper error handling, early in the development lifecycle.

Software composition analysis identifies open-source and third-party components used by an application and compares their versions against known vulnerability information. This allows developers to identify vulnerable dependencies and prioritize upgrades, replacements, or other remediation before release. OWASP describes secure software-development practices and application-security verification in the OWASP Application Security Verification Standard. CISA also provides guidance for managing open-source software and software supply-chain risk at CISA Open Source Software Security.

QUESTION NO: 61

A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

A. CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

B. CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

C. CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

ANSWER: C

Explanation:

`CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H` is the correct remediation priority because its Attack Vector is Network (AV:N). In CVSS v3.0, Network means the vulnerable component can be exploited remotely over one or more networks, without the attacker needing local system access, adjacent-network proximity, or physical access. This gives the weakness the broadest exposure and highest Attack Vector exploitability weight among the available vector categories. When findings have similar CVSS base scores, reviewing the individual base metrics helps the analyst identify the vulnerability with the most immediate practical reachability. Here, the network-reachable condition is combined with low attack complexity, low privileges required, no user interaction, and high impacts to confidentiality, integrity, and availability. That combination indicates an attacker can potentially exploit the issue with relatively few prerequisites while causing substantial harm to the affected organization. CVSS is a prioritization input rather than a complete risk decision, so the analyst should also consider asset criticality, exposure, and active exploitation. However, based specifically on the listed CVSS base metrics, Network is the attack vector to address first. The CVSS v3.0 metric definitions and weights are documented by FIRST; see also the NIST National Vulnerability Database CVSS guidance.

QUESTION NO: 62

An XSS vulnerability was reported on one of the 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: D F

Explanation:

Implement a compensating control in the source code is an appropriate long-term recommendation because cross-site scripting occurs when an application includes untrusted data in a browser response without handling it safely for its output context. The application owner can remediate this in code through context-aware output encoding, safe DOM APIs and templating mechanisms, and, where required, properly designed input validation or HTML sanitization. These controls prevent attacker-supplied content from being interpreted as executable browser script. OWASP identifies output encoding and safe sinks as primary defenses against XSS in its Cross Site Scripting Prevention Cheat Sheet.

Fix the vulnerability using a virtual patch at the WAF is also an appropriate recommendation to reduce exposure promptly. A web application firewall can apply a targeted rule that detects and blocks known XSS payload patterns before they reach the vulnerable endpoint. This is particularly valuable while the application owner develops, tests, and deploys the permanent source-code change. Virtual patching provides a protective layer for the known vulnerable request path and reduces the likelihood of exploitation during the remediation window. OWASP describes this approach and its operational use in its

Virtual Patching Best Practices. Together, source-code remediation and a WAF virtual patch provide durable prevention plus immediate compensating protection.