DUMPSARENA

CompTIA CyberSecurity Analyst CySA+ Certification Exam

CompTIA CS0-003

Version Demo

Total Demo Questions: 56

Total Premium Questions: 612

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Operations	271
Topic 2, Vulnerability Management	190
Topic 3, Incident Response and Management	119
Topic 4, Reporting and Communication	32
Total	612

QUESTION NO: 1

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 goals of adding a digital signature to executive email messages in this scenario. A digital signature is created using the sender's private key and is validated by recipients using the corresponding public key, allowing recipients to verify that the signed email content has not been altered after signing. This directly supports Integrity because any modification to the message or signed content would cause signature validation to fail. Digital signatures also support Non-repudiation because the signature is bound to the signer's private key and identity, helping demonstrate that the message originated from the executive who signed it. In contract negotiations and other legally sensitive communications, this is especially important because the organization needs confidence that the signed communication can be attributed to the sender and that the content received is the same content that was sent. NIST describes digital signatures as a cryptographic mechanism used to verify origin and detect unauthorized modification, and it defines non-repudiation as assurance that someone cannot deny a previous action. See NIST: Digital Signature and NIST: Non-repudiation.

QUESTION NO: 2

Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

A. The lead should review what is documented in the incident response policy or plan

B. Management level members of the CSIRT should make that decision

C. The lead has the authority to decide who to communicate with at any time

D. Subject matter experts on the team should communicate with others within the specified area of expertise

ANSWER: A

Explanation:

The lead should review what is documented in the incident response policy or plan is correct because incident communications should be governed by predefined procedures rather than improvised during the pressure of an active event. A well-built incident response plan defines communication roles, escalation paths, notification thresholds, internal and external points of contact, timing requirements, and approval processes for releasing information. This helps the CSIRT lead coordinate with stakeholders such as IT operations, legal, management, human resources, public relations, customers, regulators, or law enforcement when appropriate. It also helps ensure that communications are accurate, consistent, timely, and aligned with business, contractual, and legal obligations. CompTIA CySA+ objectives emphasize following incident response processes, including communication and stakeholder coordination, as part of effective incident handling. NIST similarly identifies communication and coordination as core elements of incident response planning, including contact lists, reporting procedures, and escalation criteria. See NIST's guidance in Computer Security Incident Handling Guide SP 800-61 Rev. 2 and CISA's incident response resources at Incident Response Plan Basics.

QUESTION NO: 3

Which of the following in the digital forensics process is considered a critical activity that often includes a graphical representation of process and operating system events?

A. Registry editing

B. Network mapping

C. Timeline analysis

D. Write blocking

ANSWER: C

Explanation:

Timeline analysis is the correct answer because it is the forensic activity focused on reconstructing events in chronological order so an analyst can understand what happened, when it happened, and how different artifacts relate to one another. In incident response and digital forensics, timelines commonly combine timestamps from file systems, event logs, process execution artifacts, registry artifacts, browser history, and other operating system evidence. Presenting those events visually or graphically helps analysts identify suspicious sequences, correlate attacker activity with system behavior, and distinguish normal activity from malicious actions. This is especially important when investigating malware execution, lateral movement, privilege escalation, or data access because the order and proximity of events often reveal the attack path. Tools such as Plaso/log2timeline are widely used to generate and analyze forensic timelines from many artifact sources. For additional context, see the Plaso documentation and NIST guidance on forensic analysis practices in NIST SP 800-86.

QUESTION NO: 4 - (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.

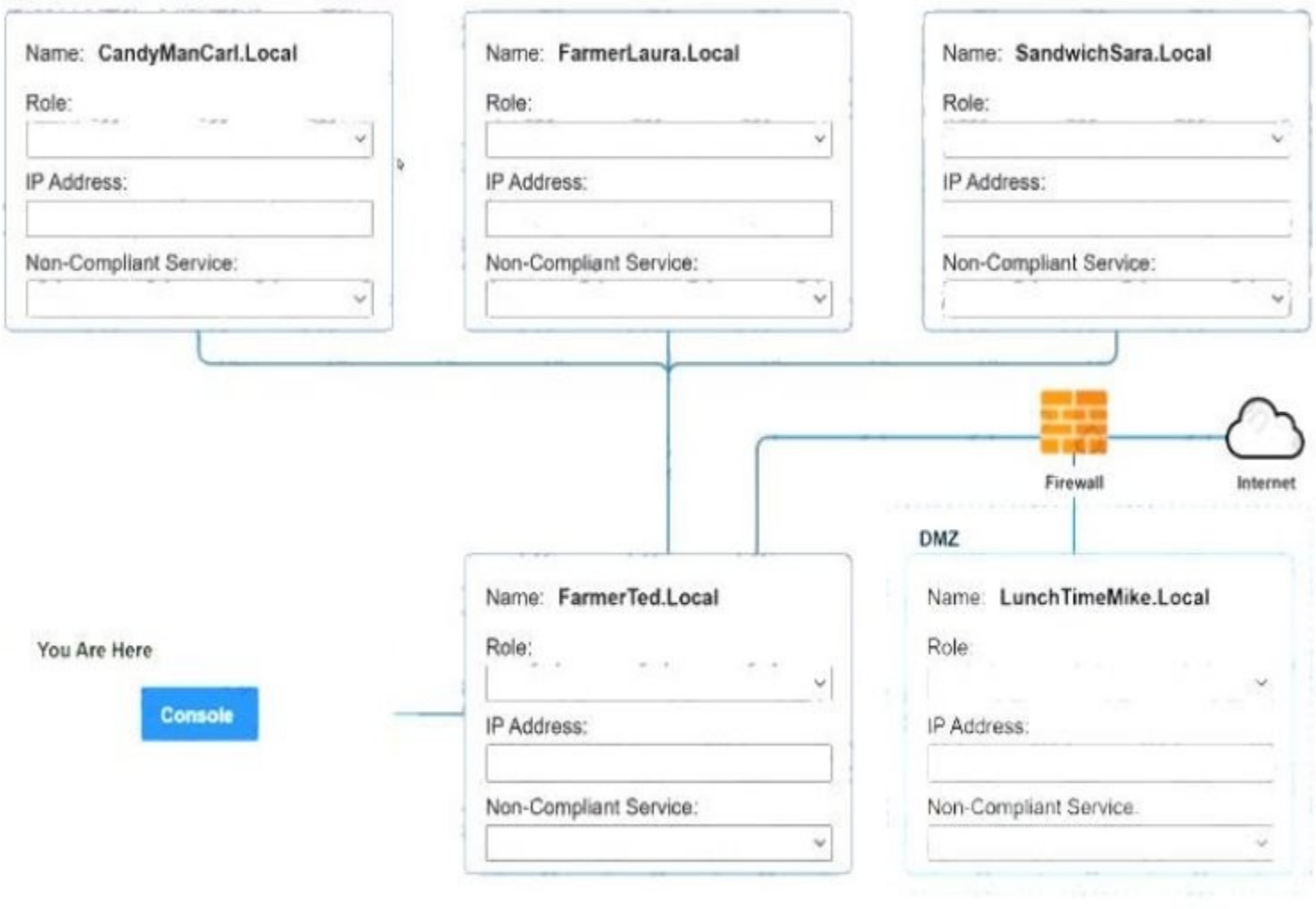
The corporate internet presence should be placed in a protected subnet Instructions :

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

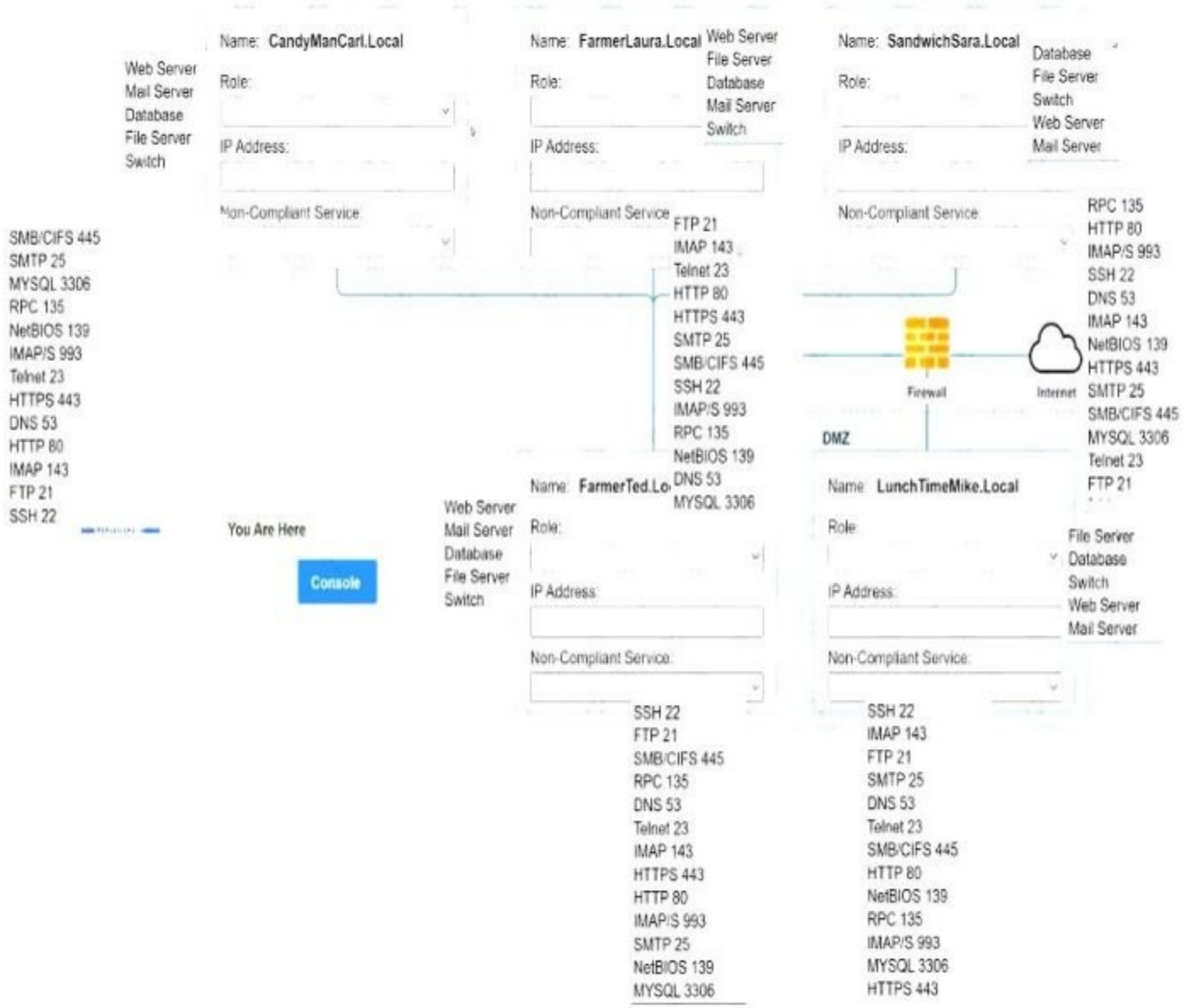
You must determine

ip address of each device

The primary server or service each device



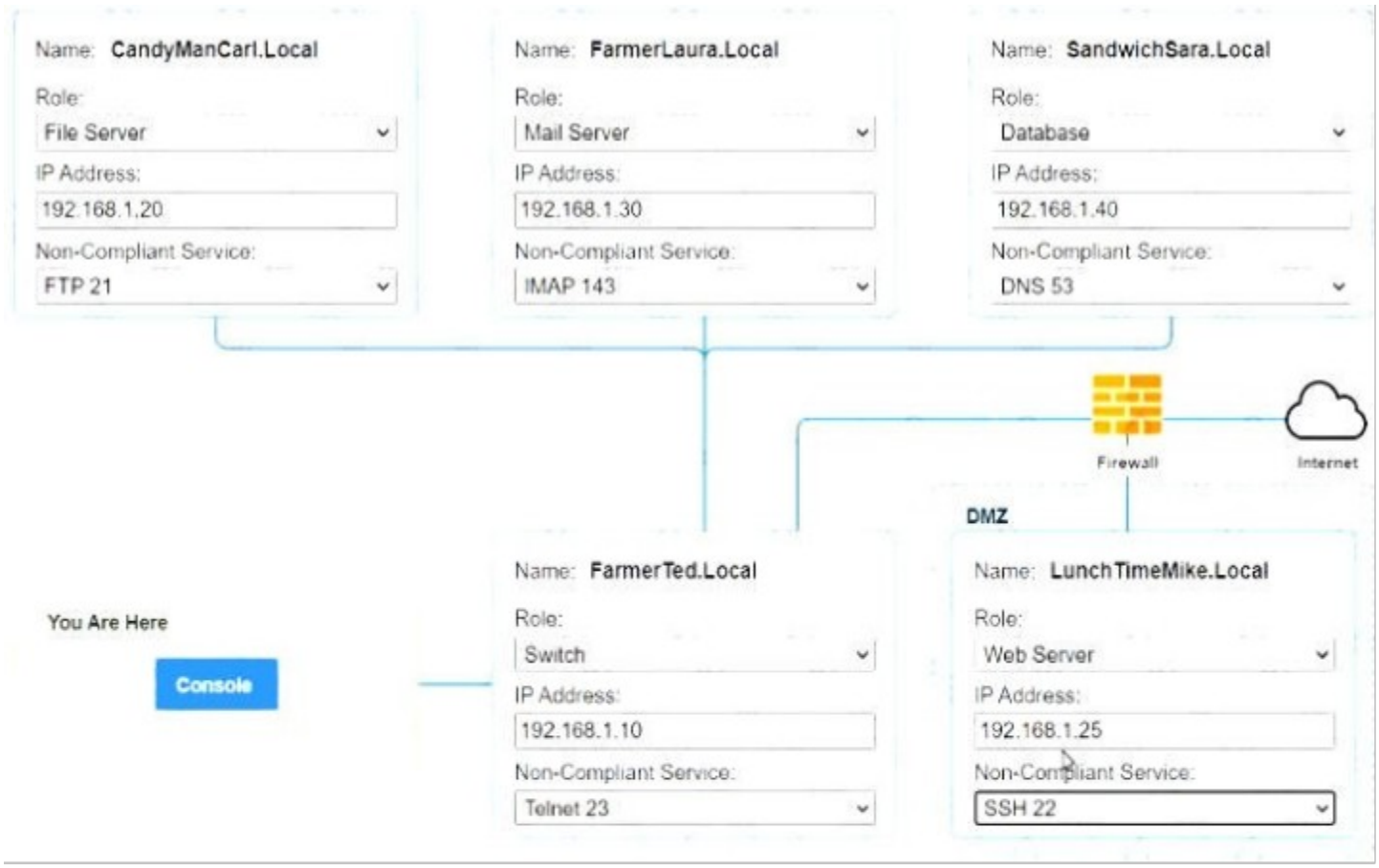
The protocols that should be disabled based on the hardening guidelines

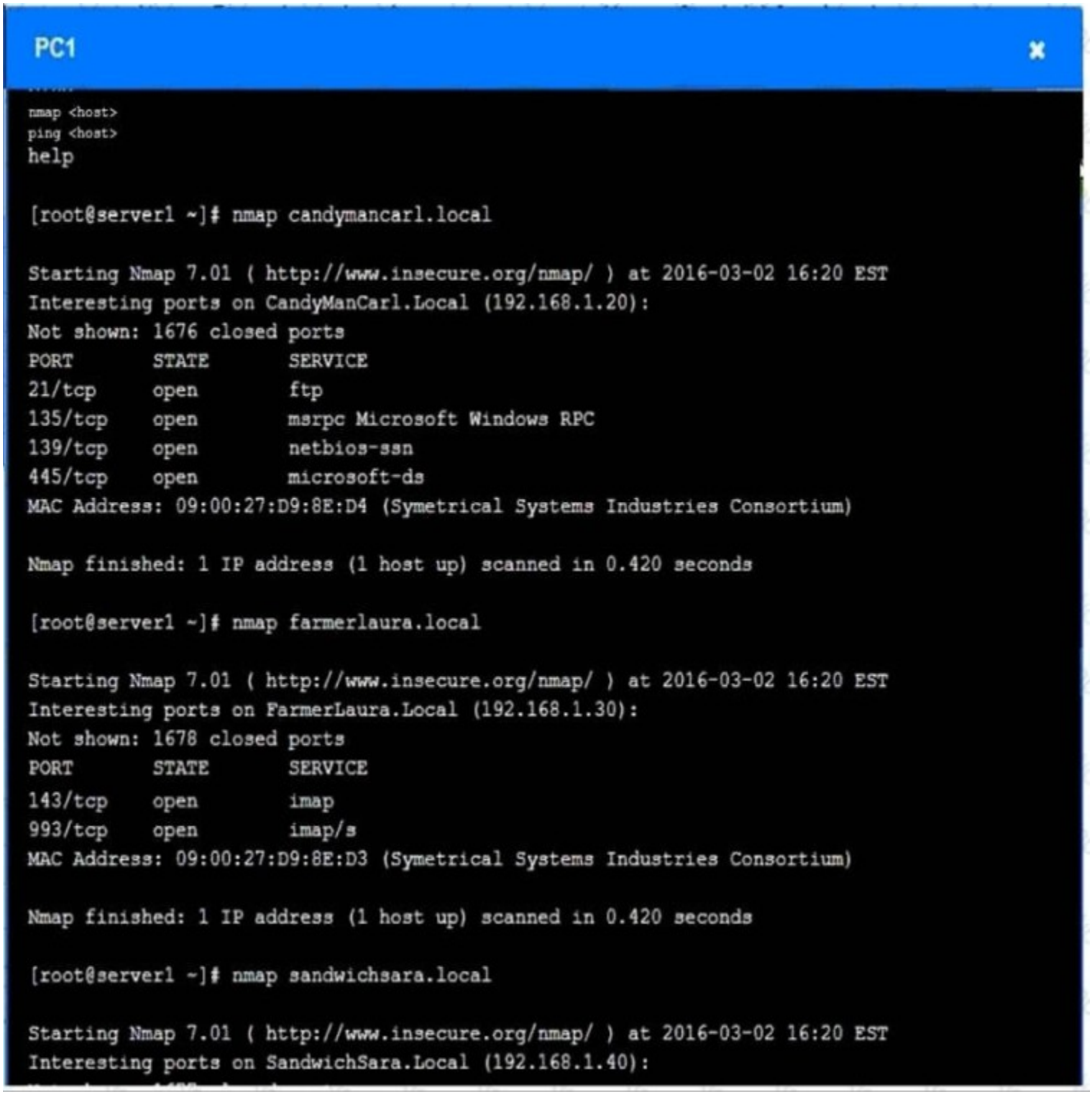


see the answer below in explanation:

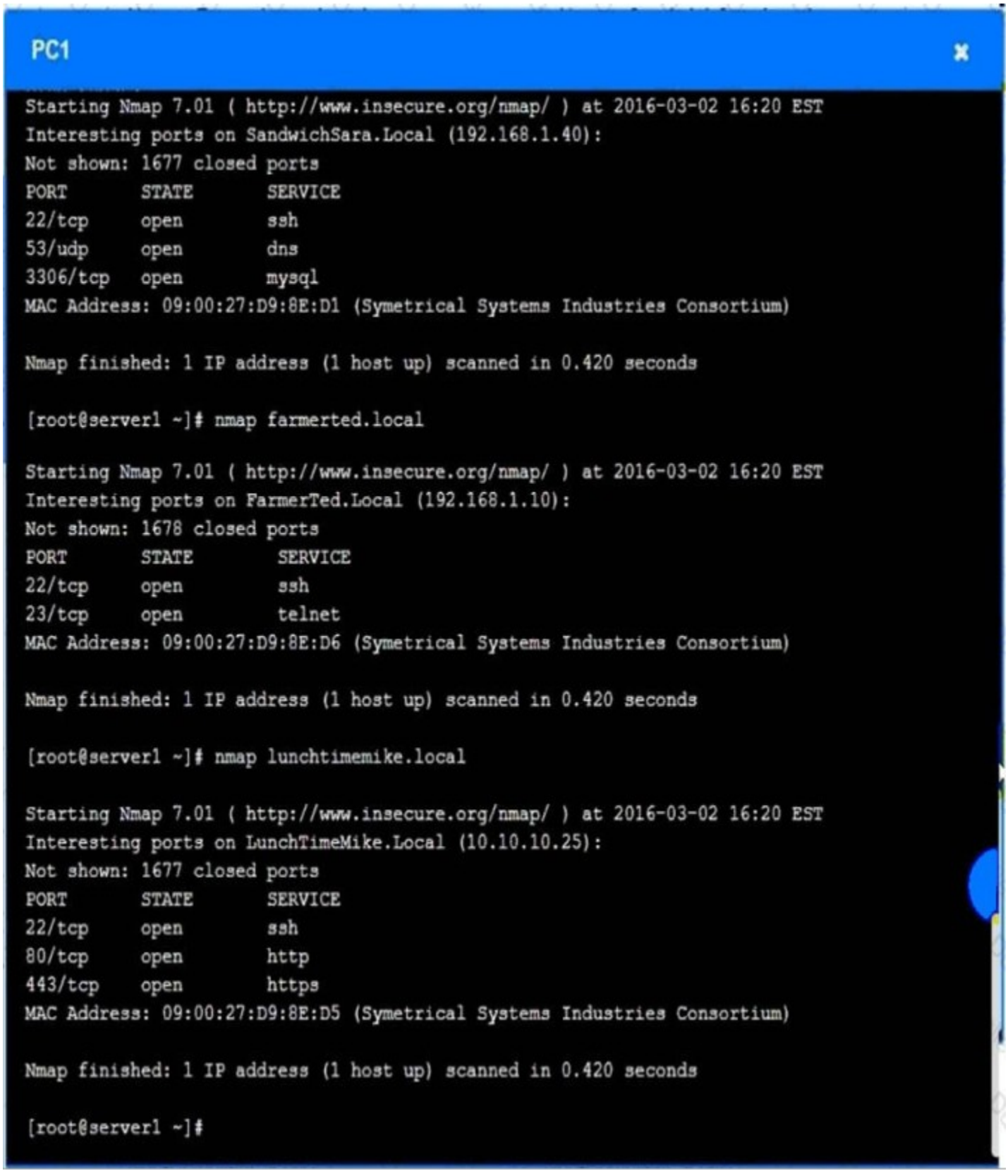
Explanation:

Answer below images





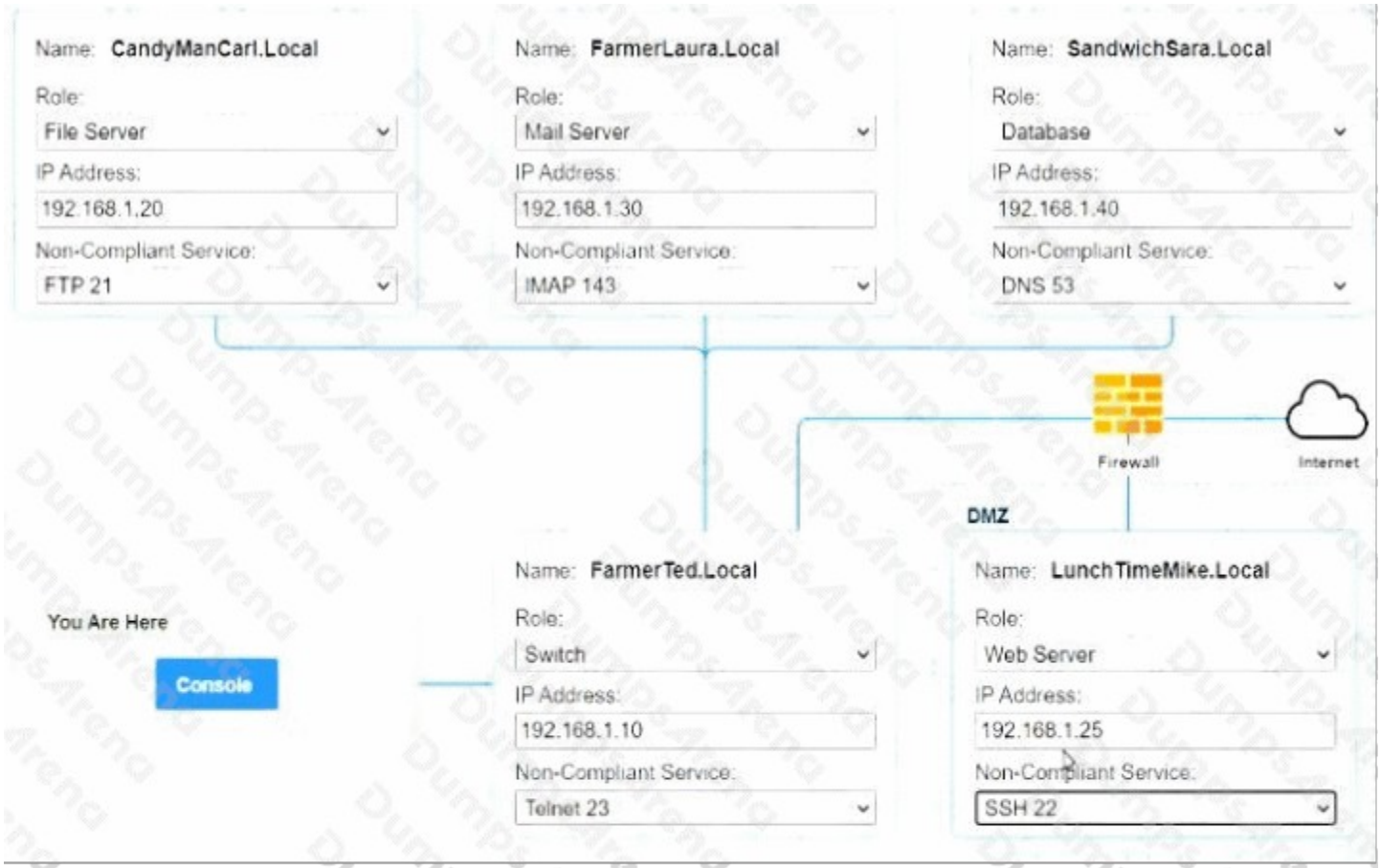
A computer screen with white text Description automatically generated

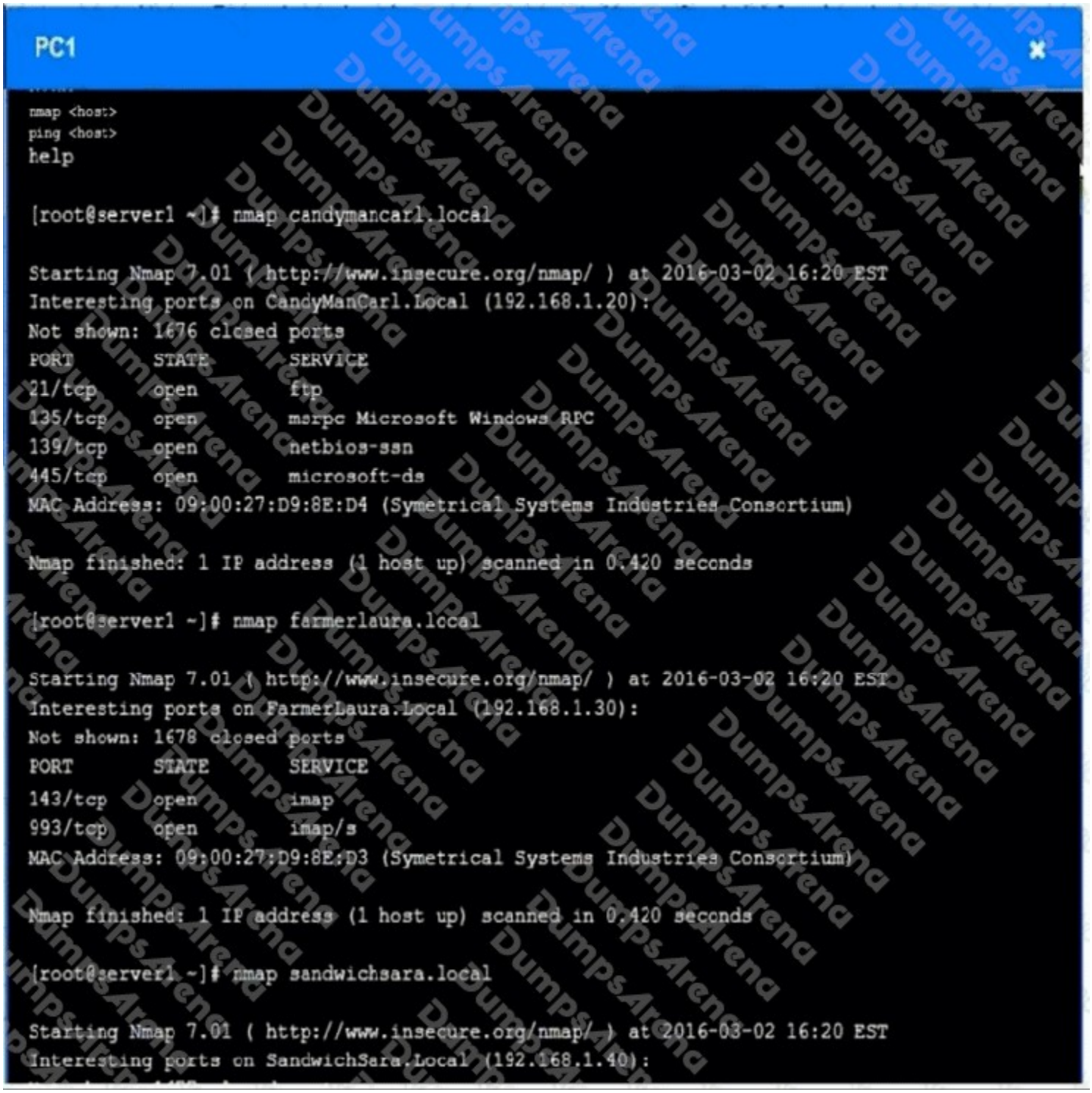


ANSWER: See the explanation for the answer

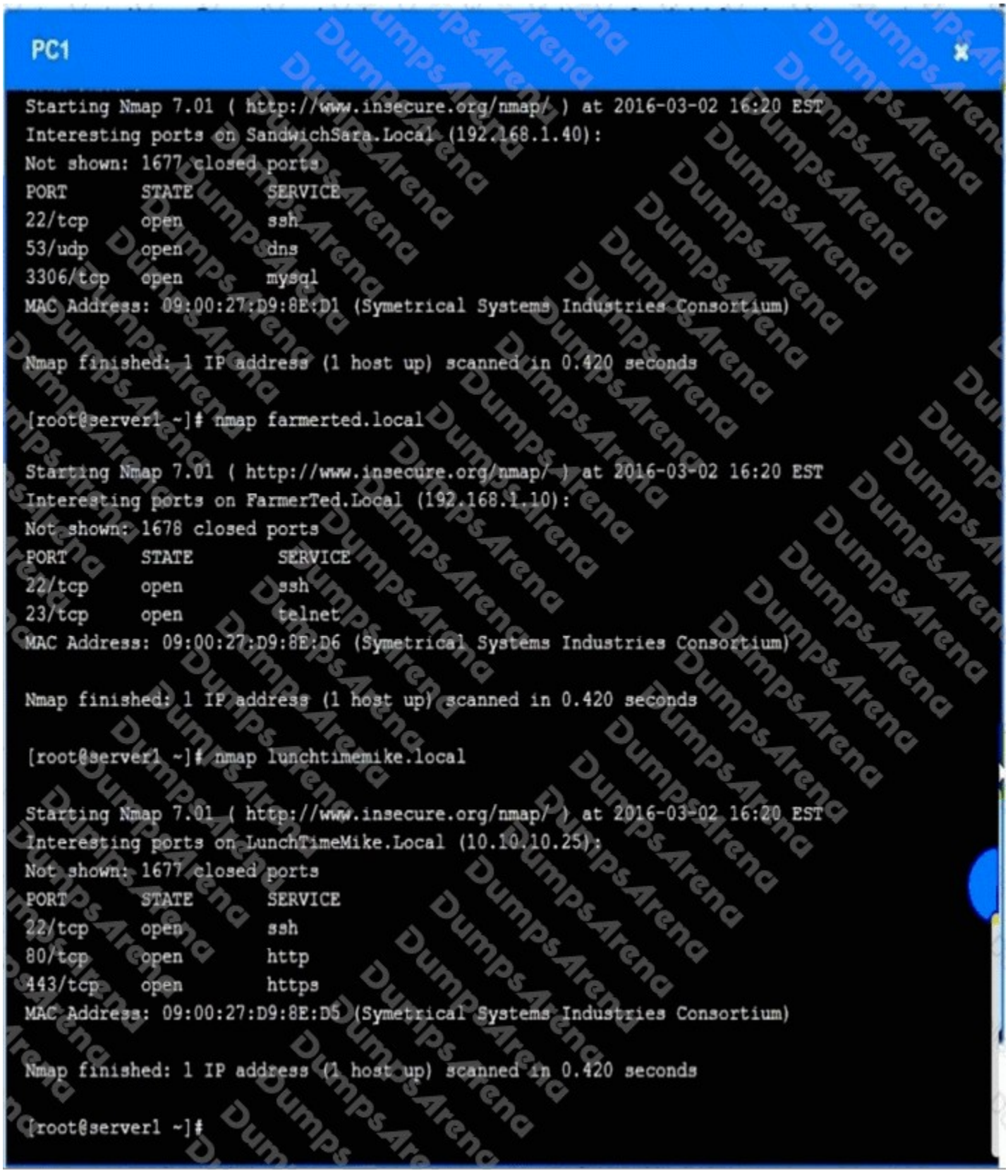
Explanation:

Answer below images





A computer screen with white text Description automatically generated



QUESTION NO: 5

Which Of the following techniques would be best to provide the necessary assurance for embedded software that drives centrifugal pumps at a power Plant?

A. Containerization

B. Manual code reviews

C. Static and dynamic analysis

D. Formal methods

ANSWER: D

Explanation:

Formal methods is the best choice because the software described is embedded control software in a power plant, which makes it part of a safety-critical industrial control environment. When software failure can cause physical damage, operational disruption, or safety hazards, the assurance technique should provide the strongest evidence that the system behaves exactly as intended under defined conditions. Formal methods use mathematically precise specifications, models, proofs, and verification techniques to demonstrate correctness properties such as safety, liveness, boundary behavior, and absence of certain classes of defects. This level of rigor is especially valuable for embedded systems that control physical processes, because testing alone may not cover every possible state, timing condition, or edge case. NIST recognizes formal methods as part of high-assurance engineering and verification practices for trustworthy systems, particularly where stronger confidence is required in system behavior. See NIST SP 800-160 Volume 1 Revision 1 and NIST SP 800-53 Revision 5 for related secure engineering and verification guidance.

QUESTION NO: 6

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 correct because a formal change management process should include a planned recovery, rollback, or backout approach before a change is implemented. If the deployment causes instability or a critical service failure, the team needs predefined steps to restore service quickly, reduce downtime, and limit business impact. This aligns with common change control expectations that changes should be tested, approved, scheduled, and paired with recovery plans before production implementation.

Identify assets with dependencies that could be impacted by the change is also correct because dependency and impact analysis is central to effective change management. Understanding which systems, applications, databases, network paths, identities, or third-party services rely on the changed component helps teams anticipate cascading effects and plan the deployment safely. This supports better scheduling, communication, testing scope, risk assessment, and contingency preparation. CompTIA's CySA+ objectives include change management concepts such as impact analysis and operational risk considerations; see the CompTIA CySA+ certification page. NIST also emphasizes configuration change control and security impact analysis in NIST SP 800-128.

QUESTION NO: 7 - (HOTSPOT)

HOTSPOT

An organization has noticed large amounts of data are being sent out of its network. An

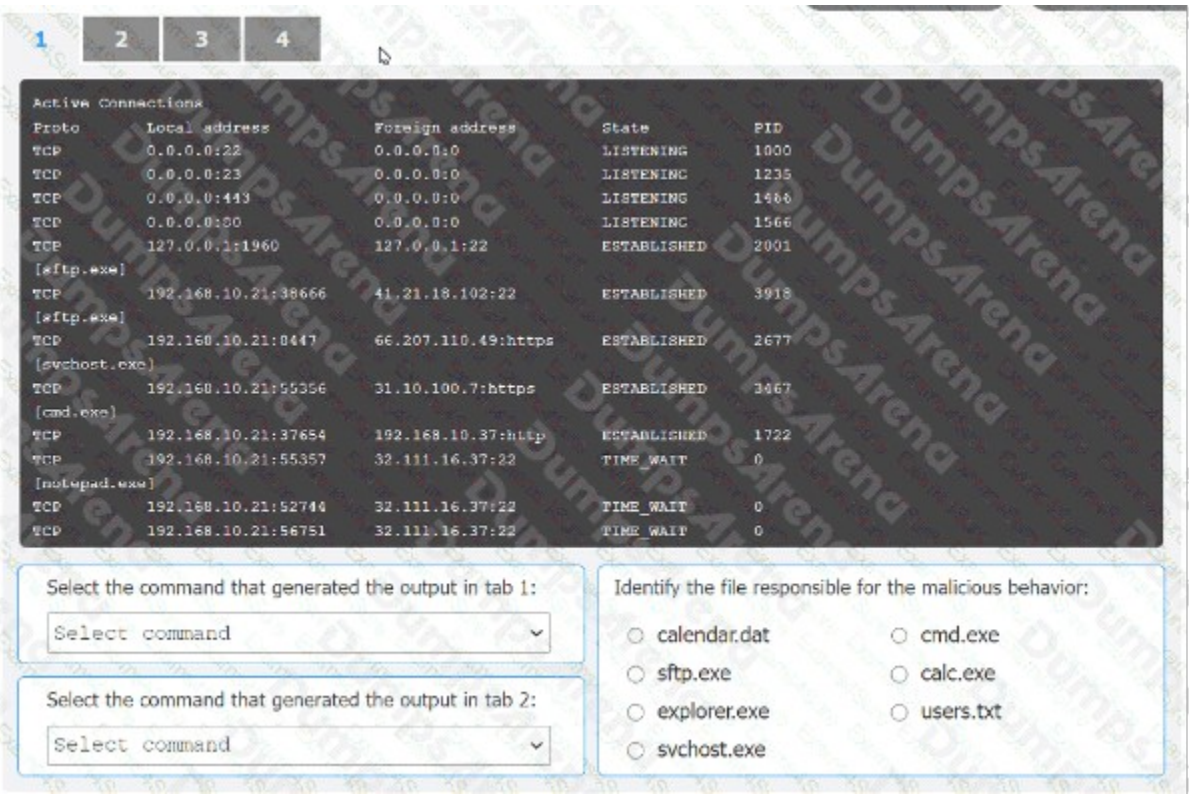
analyst is identifying the cause of the data exfiltration.

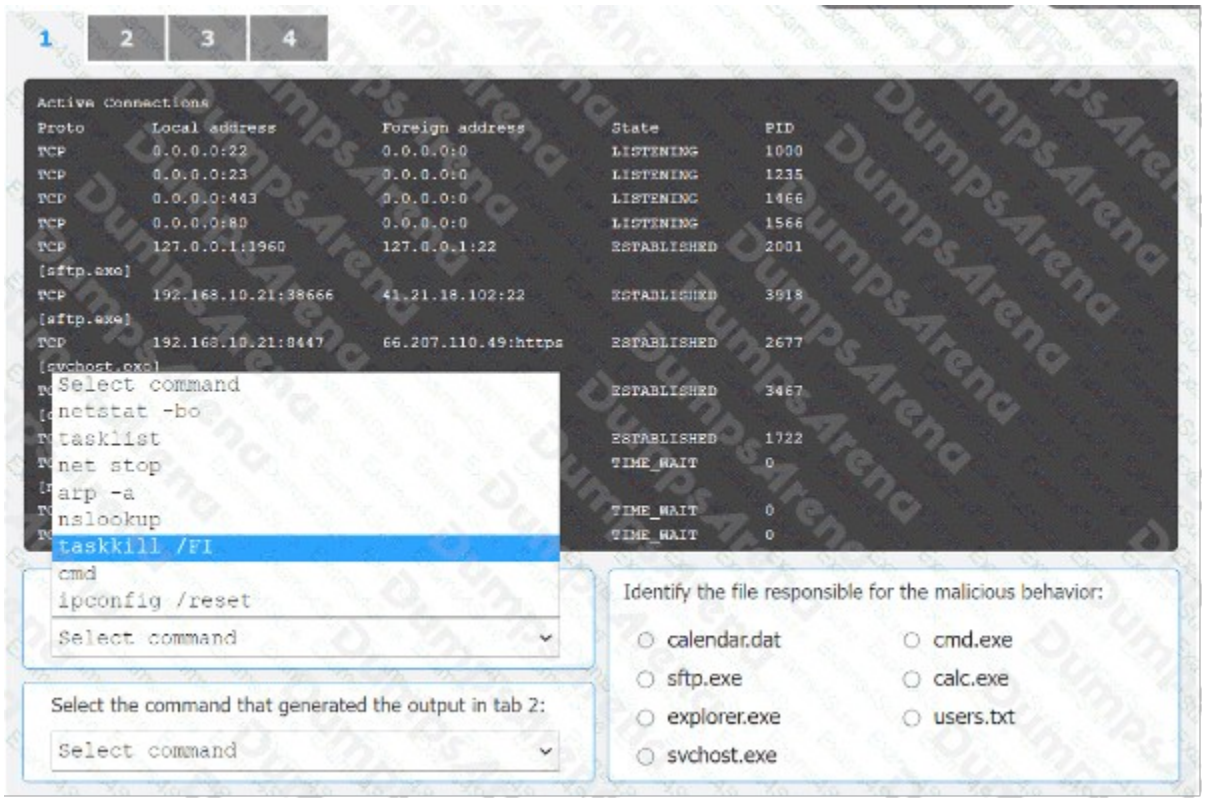
INSTRUCTIONS

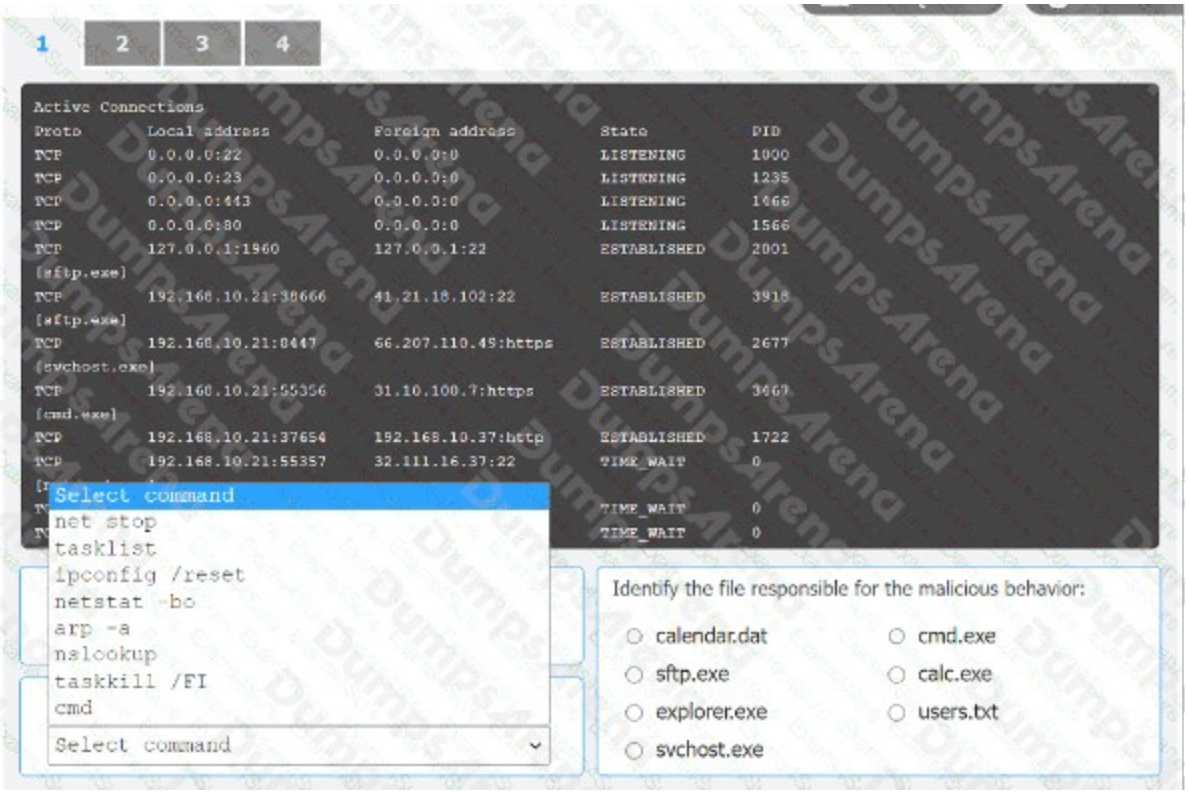
Select the command that generated the output in tabs 1 and 2.

Review the output text in all tabs and identify the file responsible for the malicious behavior.

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







1 2 3 4

```
Image Name                     PID              Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
Cmd.exe                      3467 Console                    0     18,020 K
sftp.exe                     2001 Console                    0         17 K
sftp.exe                     3918 Console                    0      1,788 K
svchost.exe                  2677 Console                    0        188 K
calc.exe                     1677 Console                    0         11 K
notepad.exe                       Console                    0          0 K
```

Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe

1 2 3 4

```
> Get-ChildItem | Get-FileHash -Algorithm MD5

Algorithm       Hash                                                                   File
---------       ----                                                                   ----
MD5             372ab227fd5ca779c211a1451881d1e1                                       cmd.exe
MD5             173ab22a5d5ea87bb212c14588aad4c2                                       calc.exe
MD5             412aba2efd5ea[illegible]9c2112b451881affe7                             explorer.exe
MD5             df6ab147fd5ecb79c331a146f8dad199                                       users.txt
MD5             212ac257fd5ea7f9c337ba22bab1d1f5                                       calendar.dat
MD5             10ad132ffed0217c6c3854a22bab215c6                                      sftp.exe
MD5             33c141f5ad107bcdd39952d2ba111401                                       svchost.exe
```

Select the command that generated the output in tab 1:

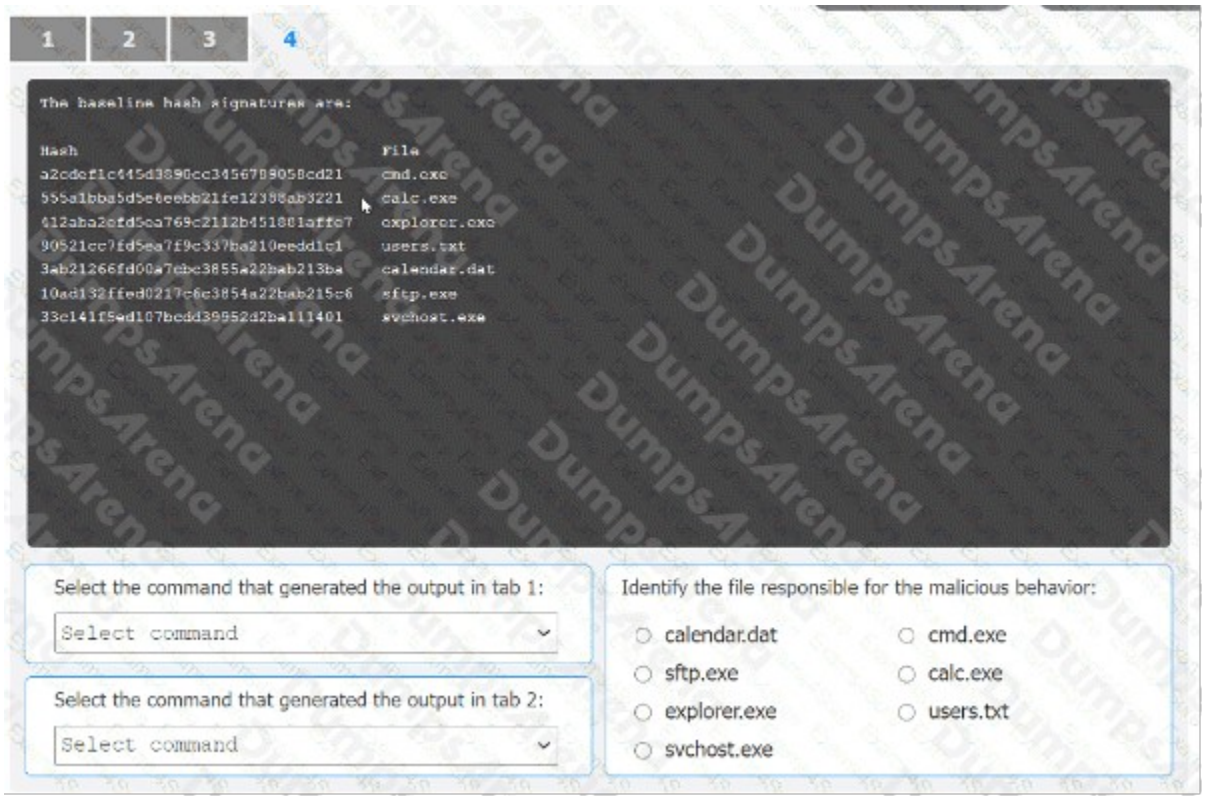
Select command

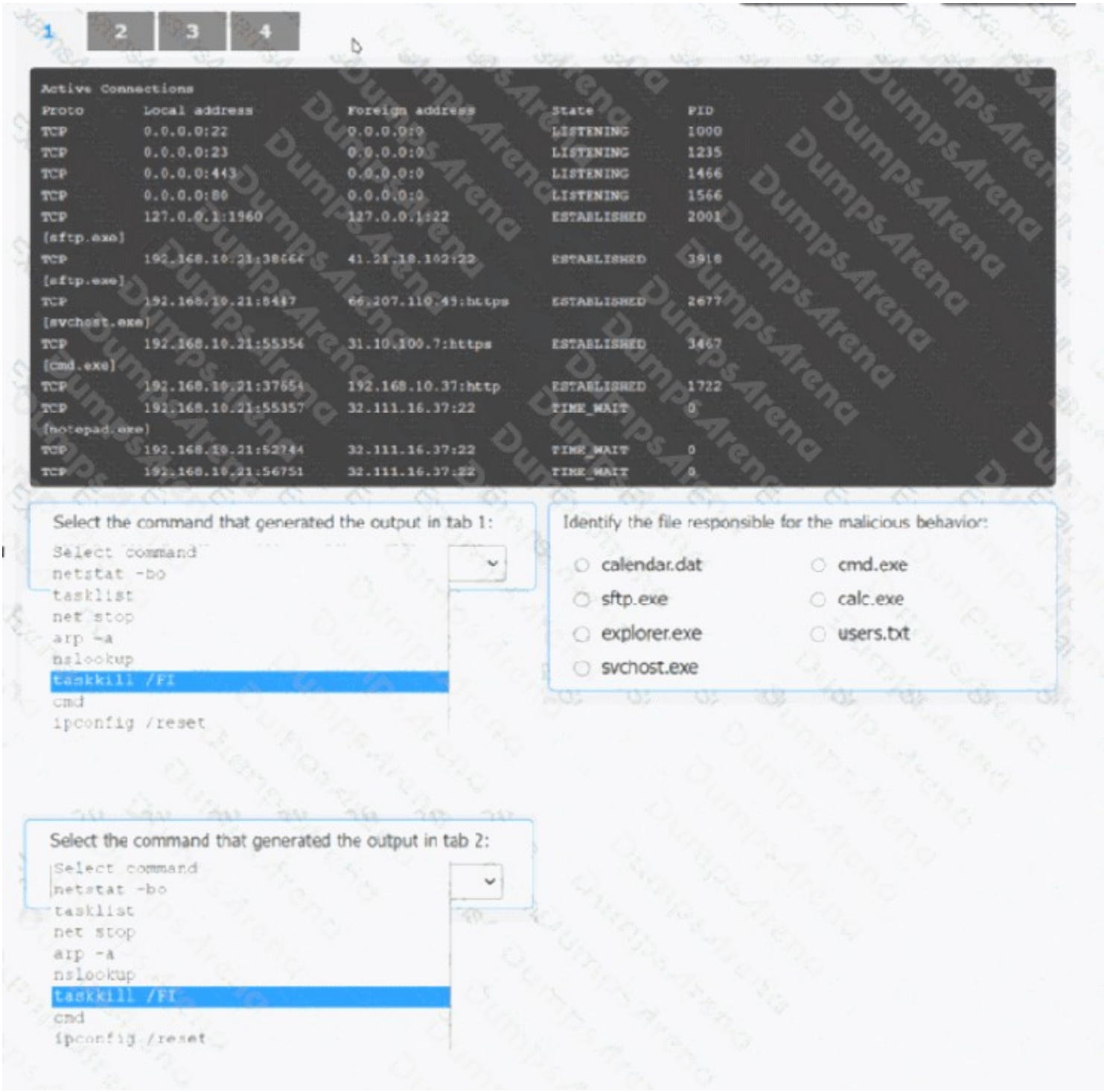
Select the command that generated the output in tab 2:

Select command

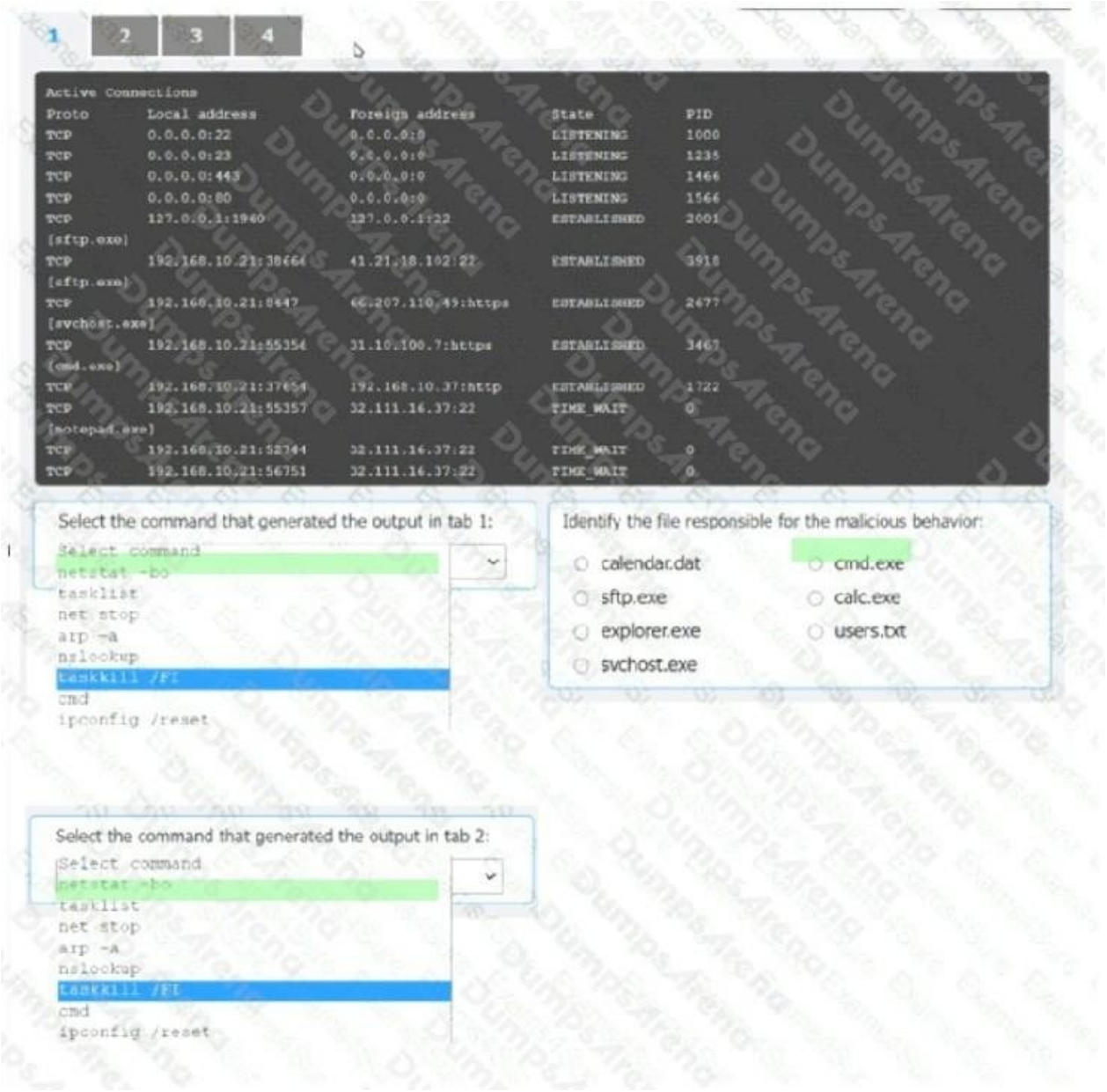
Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe


1
2
3
4
The baseline hash signatures are:
Hash File
a2cdcf1c445d3890cc3456789058cd21 cmd.exe
555a1bba5d5e6eebb21fe12398ab3221 calc.exe
412aba2cfd5ca769c2112b451881affe7 explorer.exe
90521cc7fd5ea7f9c337ba210eeddlc1 users.txt
3ab21266fd00a7ebc3855a22bab213ba calendar.dat
10ad132ffed0217c6c3854a22bab215c6 sftp.exe
33c141f5ed107bcdd39952d2ba111401 svchost.exe
Select the command that generated the output in tab 1:
Select command
Select the command that generated the output in tab 2:
Select command
Identify the file responsible for the malicious behavior:
calendar.dat
cmd.exe
sftp.exe
calc.exe
explorer.exe
users.txt
svchost.exe


1
2
3
4
Active Connections
Proto Local address Foreign address State PID
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING 1000
TCP 0.0.0.0:23 0.0.0.0:0 LISTENING 1235
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 1466
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 1566
TCP 127.0.0.1:1960 127.0.0.1:22 ESTABLISHED 2001
[sftp.exe]
TCP 192.168.10.21:38664 41.21.18.162:22 ESTABLISHED 3918
[sftp.exe]
TCP 192.168.10.21:8487 66.207.110.49:https ESTABLISHED 2677
[svchost.exe]
TCP 192.168.10.21:55356 31.10.100.7:https ESTABLISHED 3467
[cmd.exe]
TCP 192.168.10.21:37654 192.168.10.37:http ESTABLISHED 1722
TCP 192.168.10.21:55357 32.111.16.37:22 TIME_WAIT 0
[notepad.exe]
TCP 192.168.10.21:52744 32.111.16.37:22 TIME_WAIT 0
TCP 192.168.10.21:56751 32.111.16.37:22 TIME_WAIT 0
Select the command that generated the output in tab 1:
Select command
netstat -bo
tasklist
net stop
arp -a
nslookup
taskkill /FI
cmd
ipconfig /reset
Identify the file responsible for the malicious behavior:
calendar.dat
cmd.exe
sftp.exe
calc.exe
explorer.exe
users.txt
svchost.exe
Select the command that generated the output in tab 2:
Select command
netstat -bo
tasklist
net stop
arp -a
nslookup
taskkill /FI
cmd
ipconfig /reset

ANSWER:



Explanation:

The correct selections are **netstat -bo** for the first tab, **tasklist** for the second tab, and **cmd.exe** as the file responsible for the malicious behavior. The first tab shows active TCP connections, listening ports, remote endpoints, connection states, process IDs, and the executable names associated with those connections. On Windows, the `netstat` command with the `-b` option displays the executable involved in each connection, and the `-o` option displays the owning process ID, which matches the format shown in the first tab. Microsoft documents these netstat options in its command reference: Microsoft netstat command reference.

The second tab shows a process inventory with columns such as Image Name, PID, Session Name, Session#, and Mem Usage. That is the normal output format of the Windows `tasklist` command, which is used to display currently running processes and their process IDs. Microsoft's reference for this command is available here: Microsoft tasklist command reference.

The malicious file is **cmd.exe** because the network connection data shows `cmd.exe` associated with an established outbound HTTPS connection to an external address, and the process list confirms that the same process ID is running. The file hash comparison then shows that the current hash for `cmd.exe` does not match the known baseline hash. In incident analysis, a mismatch between a known-good baseline hash and the current executable hash is strong evidence that the binary has been modified, replaced, or tampered with. Combined with the suspicious outbound connection, `cmd.exe` is the file tied to the data exfiltration behavior.

QUESTION NO: 8

After an upgrade to a new EDR, a security analyst received reports that several endpoints were not communicating with the SaaS provider to receive critical threat signatures. To comply with the incident response playbook, the security analyst was required to validate connectivity to ensure communications. The security analyst ran a command that provided the following output:

ComputerName: comptia007

RemotePort: 443

InterfaceAlias: Ethernet 3

TcpTestSucceeded: False

Which of the following did the analyst use to ensure connectivity?

A. nmap
nmap: While nmap can scan ports, it does not provide direct feedback on connection success or failure in the manner shown.

B. tnc
tnc (Test-NetConnection in PowerShell): This command in PowerShell is specifically designed to test connectivity to a specified port and IP address. The output (TcpTestSucceeded: False) is characteristic of the tnc command.

C. ping
ping: The ping command only tests ICMP echo replies and does not indicate success or failure on specific ports.

D. tracert
tracert: tracert traces the path packets take to reach a host but does not provide a direct indication of port availability or success. [References:, Microsoft PowerShell Documentation: Test-NetConnection cmdlet, which details TCP port testing., NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, covering connectivity testing methods., ,]

ANSWER: B

Explanation:

tnc is correct because the displayed fields match the output format of the Windows PowerShell Test-NetConnection cmdlet, for which tnc is a common alias. Test-NetConnection is used to troubleshoot network connectivity and can test whether a TCP connection to a specific remote host and port succeeds. In this scenario, the analyst needed to validate that endpoints could communicate with a SaaS EDR provider over HTTPS, which commonly uses TCP port 443. The output values, including ComputerName, RemotePort, InterfaceAlias, and especially TcpTestSucceeded: False, are characteristic of Test-NetConnection when run with a port test. The False result indicates that the TCP connection attempt to the specified service port did not succeed, which directly supports the analyst's incident response task of validating connectivity to receive critical threat signatures. Microsoft documents Test-NetConnection as a diagnostic cmdlet that displays diagnostic information for a connection and supports TCP port testing using the Port parameter. See Microsoft Learn: Test-NetConnection and Microsoft Learn: about Aliases.

QUESTION NO: 9

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 best choices for centralizing the internal security team's workload after a new EDR deployment increases the alert volume. SIEM provides a central platform for collecting, normalizing, correlating, and prioritizing security events from EDR and other sources, giving analysts a single place to investigate activity instead of working from separate tool consoles. SOAR complements that by centralizing response workflows, case management, playbooks, enrichment, and automation. When alert counts rise sharply, SOAR can help reduce repetitive analyst effort by automating triage steps, routing incidents, opening tickets, gathering context, and triggering approved response actions. Used together, SIEM and SOAR allow the organization to consolidate visibility and streamline remediation work for the internal team. This pairing aligns with common security operations architecture, where SIEM is used for monitoring and correlation, while SOAR is used for orchestration and response automation. Microsoft describes Microsoft Sentinel as a cloud-native platform that combines SIEM and SOAR capabilities for enterprise security operations: Microsoft Sentinel overview. NIST also defines SIEM as a capability for collecting and analyzing security event information: NIST CSRC SIEM glossary.

QUESTION NO: 10

A security analyst received an alert regarding multiple successful MFA log-ins for a particular user When reviewing the authentication logs the analyst sees the following:

Which of the following are most likely occurring, based on the MFA logs? (Select two).

A. Dictionary attack

B. Push phishing

C. Impossible geo-velocity

D. Subscriber identity module swapping

E. Rogue access point

F. Password spray

ANSWER: B C

Explanation:

Push phishing and impossible geo-velocity are the most likely conclusions when MFA logs show multiple successful approvals for the same user in a suspicious pattern, especially when those approvals are associated with geographically distant locations in a short period of time. Push phishing, also commonly called MFA fatigue or MFA bombing, occurs when an attacker already has the user's primary credentials and repeatedly triggers MFA prompts until the user approves one by mistake, out of confusion, or due to social engineering. Microsoft specifically recommends number matching and additional context to help defend against this kind of MFA fatigue attack: Microsoft Entra MFA number matching. Impossible geo-velocity is also indicated when successful authentications for one identity appear from locations that cannot realistically be traveled between in the observed time window. In identity security tools, this is often treated as an "atypical travel" or location-based risk signal because it suggests the same account may be in use by an attacker from a different region while the legitimate user is elsewhere. Microsoft Entra ID Protection documents this type of identity risk detection here: Microsoft Entra ID Protection risk detections.

QUESTION NO: 11

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.
Implement an IPS in front of the web server

B. Enable MFA on the website.
Enable MFA on the website

C. Take the website offline until it is patched.
Take the website offline until it is patched
While this might temporarily mitigate the risk, it is not a practical solution for ongoing operations, especially when effective preventative controls (e.g., WAF rules or code updates) can be implemented without disabling the service.

D. Implement a compensating control in the source code.
Implement a compensating control in the source code

E. Configure TLS v1.3 on the website.
Configure TLS v1.3 on the website

F. Fix the vulnerability using a virtual patch at the WAF.
Fix the vulnerability using a virtual patch at the WAF
References:
OWASP XSS Prevention Cheat Sheet: Detailed guidance on encoding, sanitizing, and safe coding practices to prevent XSS.
NIST SP 800-44: Guidelines on Web Security, discussing WAFs and application-layer protections.
CWE-79: Common Weakness Enumeration on Cross-Site Scripting, which outlines ways to address and prevent XSS attacks.

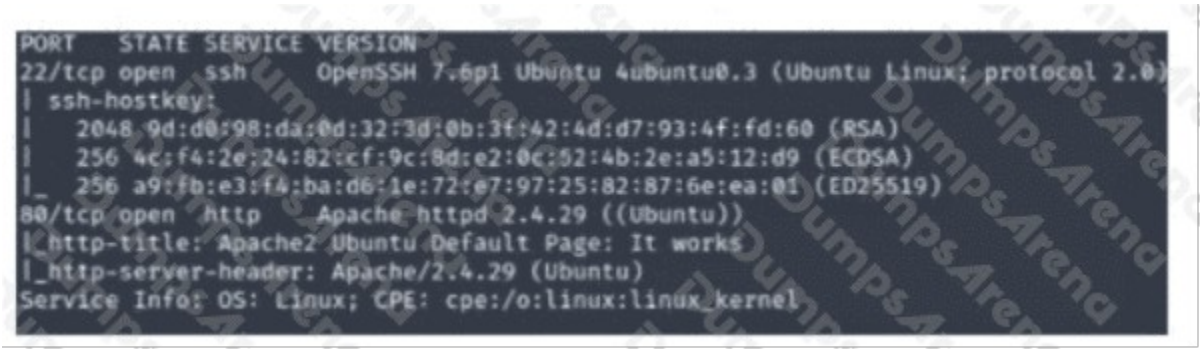
ANSWER: D F

Explanation:

Implement a compensating control in the source code and Fix the vulnerability using a virtual patch at the WAF are the best recommendations because they directly address exploitation of cross-site scripting. XSS occurs when an application allows untrusted input to be rendered by a browser as executable script. The strongest long-term prevention is application-layer remediation, such as output encoding, safe handling of user-controlled data, input validation where appropriate, and use of secure frameworks or libraries. A compensating control in the source code can prevent malicious script from being accepted, stored, reflected, or executed in the user's browser. OWASP's guidance emphasizes contextual output encoding and safe coding patterns as core XSS defenses: OWASP Cross-Site Scripting Prevention Cheat Sheet. A virtual patch at the WAF is also appropriate, especially when code changes require development and release time. A WAF rule can block known malicious payloads or suspicious request patterns before they reach the vulnerable application, reducing immediate risk while permanent code remediation is planned. OWASP also recognizes virtual patching as a practical mitigation for web application vulnerabilities: OWASP Virtual Patching Best Practices.

QUESTION NO: 12

A security analyst scans a host and generates the following output:



Which of the following best describes the output?

A. The host is unresponsive to the ICMP request.

B. The host Is running a vulnerable mall server.

C. The host Is allowlng unsecured FTP connectlons.

D. The host is vulnerable to web-based exploits.

ANSWER: D

Explanation:

The host is vulnerable to web-based exploits is the best description because the scan output indicates an exposed HTTP/web service, which is the relevant attack surface shown by the results. In a security assessment, a discovered web service on a host—especially when the scan identifies the service and version—should be treated as a potential web-exploitation target until validated through vulnerability research, configuration review, or additional testing. Tools such as Nmap commonly report open ports, service names, and version details, and analysts use that information to map exposed services to known vulnerabilities, misconfigurations, and exploit paths. For example, an open HTTP service may be affected by vulnerable server software, unsafe web application code, weak authentication, directory traversal, injection flaws, or other web-layer issues. This aligns with CySA+ analysis expectations: interpret scan results, identify exposed services, and determine the most likely security implication from the evidence shown. See the Nmap version detection documentation for how service/version output supports vulnerability analysis, and the OWASP Top 10 for common categories of web-based exploitation risk.

QUESTION NO: 13

A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
|_http-server-header: openresty
| ssl-enum-ciphers:
| TLSv1.1:
| ciphers:
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
```

Which of the following best describes the output?

A. The host is not up or responding.

B. The host is running excessive cipher suites.

C. The host is allowing insecure cipher suites.

D. The Secure Shell port on this host is closed

ANSWER: C

Explanation:

The host is allowing insecure cipher suites is the correct description because the displayed network mapping output is consistent with an Nmap SSL/TLS cipher enumeration, such as the ssl-enum-ciphers NSE script. That type of scan lists the SSL/TLS protocol versions and cipher suites accepted by a service, typically HTTPS on TCP port 443, and grades the

cryptographic strength of what the server permits. In a PCI audit context, findings such as support for deprecated protocols like SSLv3 or weak algorithms such as RC4 indicate that the system is still accepting cryptographic configurations that are no longer considered secure. PCI DSS requires strong cryptography to protect transmission of cardholder data across open, public networks, so allowing obsolete TLS/SSL versions or weak cipher suites would be a compliance and security concern. Nmap's documentation specifically describes ssl-enum-ciphers as a script that enumerates supported SSL/TLS ciphers and reports the strength of the offered configurations. See the Nmap ssl-enum-ciphers documentation and PCI SSC guidance on PCI security standards for the relevance of strong cryptography in payment environments.

QUESTION NO: 14

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 the best tools for capturing anomalous traffic from a compromised host because both are packet capture and packet analysis utilities. tcpdump is a lightweight command-line tool commonly used on Linux and Unix-like systems to capture packets directly from a network interface, filter them with Berkeley Packet Filter syntax, and save them to a packet capture file for later analysis. This makes it especially useful during incident response when an analyst needs quick evidence collection from a host or network segment. Wireshark provides deep packet inspection through a graphical interface and can open live captures or saved capture files, allowing analysts to inspect protocols, conversations, payload details, timing, and indicators of suspicious behavior. Together, these tools support both collection and detailed review of network traffic associated with a compromised system. For reference, Wireshark documents its packet capture and protocol analysis capabilities in the official Wireshark documentation, and tcpdump usage and capture-filter behavior are documented in the official tcpdump manual page.

QUESTION NO: 15

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:

Review and approve new contracts acquired as a result of an event is correct because incident response often requires urgent engagement with outside parties such as forensic investigators, breach counsel, managed security providers, cloud vendors, public relations firms, or recovery specialists. The legal team helps ensure those agreements protect the organization, preserve confidentiality and privilege where appropriate, define responsibilities, and address liability, evidence handling, and data-protection requirements. Advise the Incident response team on matters related to regulatory reporting is also correct because many security incidents create legal notification duties involving regulators, affected individuals, business partners, insurers, or law enforcement. Legal counsel helps determine whether an incident meets breach-notification thresholds, which jurisdictions apply, what timelines must be met, and what language should be used in notifications. NIST's incident response guidance specifically notes that legal advisors may be needed for issues such as liability, evidence, and reporting requirements during incident handling; see NIST SP 800-61 Rev. 2. CompTIA's CySA+ exam objectives also emphasize incident response coordination, communication, compliance, and stakeholder responsibilities; see the CompTIA exam objectives resource page.

QUESTION NO: 16

Which of the following can be used to learn more about TTPs used by cybercriminals?

A. ZenMAP

B. MITRE ATT&CK

C. National Institute of Standards and Technology

D. theHarvester

ANSWER: B

Explanation:

MITRE ATT&CK is correct because it is a curated, publicly available knowledge base that organizes adversary tactics, techniques, and procedures based on real-world observations. In cybersecurity, TTPs describe how threat actors operate: their goals, the methods they use to achieve those goals, and the operational patterns defenders can look for. MITRE ATT&CK maps this behavior into a structured framework, making it useful for threat intelligence, detection engineering, incident response, adversary emulation, control validation, and security gap analysis. For example, analysts can use it to understand common techniques such as credential dumping, phishing, lateral movement, persistence, and command-and-control activity, then align those techniques to detections and mitigations. This makes it one of the most widely used resources for learning how cybercriminals and other adversaries behave across enterprise, cloud, mobile, and industrial control system environments. More information is available from the official MITRE ATT&CK site and MITRE's Getting Started with ATT&CK guidance.

QUESTION NO: 17

An incident response analyst is investigating the root cause of a recent malware outbreak. Initial binary analysis indicates that this malware disables host security services and performs cleanup routines on it infected hosts, including deletion of initial dropper and removal of event log entries and prefetch files from the host. Which of the following data sources would most likely reveal evidence of the root cause?

(Select two).

A. Creation time of dropper

B. Registry artifacts

C. EDR data

D. Prefetch files

E. File system metadata

F. Sysmon event log

ANSWER: B C

Explanation:

Registry artifacts and EDR data are the best sources for determining the root cause in this scenario because they can preserve evidence even when the malware attempts local cleanup. Registry artifacts can show important host changes and historical execution evidence, such as modified service configurations, disabled security controls, persistence mechanisms, autorun entries, and application execution traces. Since the malware disables host security services, the registry is a likely place to find configuration changes that help reconstruct what happened and how the malware maintained or expanded access.

EDR data is also highly valuable because endpoint detection and response platforms typically collect process execution, command-line activity, parent-child process relationships, file operations, network connections, and behavioral telemetry. This telemetry is often forwarded or stored centrally, making it more resilient when malware deletes local event logs, prefetch data, or the original dropper. Together, Registry artifacts and EDR data can help identify the initial execution chain, the affected processes, and the actions that led to the outbreak. For more context, see Microsoft's guidance on advanced hunting with endpoint telemetry and Microsoft's documentation on the Windows registry.

QUESTION NO: 18

A regulated organization experienced a security breach that exposed a list of customer names with corresponding PH data. Which of the following is the best reason for developing the organization's communication plans?

A. For the organization's public relations department to have a standard notification

B. To ensure incidents are immediately reported to a regulatory agency

C. To automate the notification to customers who were impacted by the breach

D. To have approval from executive leadership on when communication should occur

ANSWER: B

Explanation:

To ensure incidents are immediately reported to a regulatory agency is the best answer because regulated data breaches often trigger legally defined notification obligations. When protected health information is exposed, the organization must be prepared to notify the appropriate oversight bodies, affected parties, and other required stakeholders within mandated timeframes and using approved content. A communication plan helps define who is responsible for notification, what information must be gathered before reporting, how messages are approved, and which regulatory contacts or reporting channels must be used. This reduces delays and helps the organization preserve evidence, maintain consistency, and meet compliance obligations during a high-pressure incident response. For example, the HIPAA Breach Notification Rule requires covered entities and business associates to provide breach notifications to the U.S. Department of Health and Human Services and, in many cases, affected individuals and the media. See the HHS Breach Notification Rule. NIST also emphasizes that incident response planning should include external communications and reporting requirements as part of coordinated response activities; see NIST SP 800-61 Rev. 2.

QUESTION NO: 19

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:

The services on ports 21 and 23 should be investigated further because they are classic examples of unsecured network services. Port 21 is used by FTP control traffic, and traditional FTP does not protect authentication or session data with encryption. Usernames, passwords, commands, and file-transfer metadata can be exposed to anyone able to capture traffic on the network. The FTP specification includes commands such as USER and PASS, which highlights why unencrypted FTP is risky when used without a secure wrapper or replacement such as SFTP or FTPS; see RFC 959.

Port 23 is used by Telnet, another legacy protocol that provides remote terminal access without native encryption. Telnet sessions can expose credentials and administrative commands in cleartext, making them inappropriate for modern secure administration. The Telnet protocol is defined in RFC 854, and current security best practice is to replace Telnet with encrypted administration protocols such as SSH. During a security audit, finding 21 and 23 open is a strong indicator that the team should verify business need, restrict access, and migrate to encrypted alternatives wherever possible.

QUESTION NO: 20

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:

The services listening on 21 and 23 should be investigated further because they commonly indicate FTP and Telnet, two legacy protocols that are considered unsecured for modern environments. FTP on 21 typically transmits authentication credentials and file contents without encryption, which can expose usernames, passwords, and sensitive data to packet capture or interception on the network. Telnet on 23 is also plaintext-based and is especially risky because it is often used for remote administration, meaning credentials and commands can be observed or manipulated by anyone with access to the traffic path. In a security audit focused on unsecured network services, these ports are high-priority findings because safer alternatives are widely available, such as SFTP/FTPS for file transfer and SSH for remote administration. The security team should validate business need, identify the host owners, review exposure scope, and either disable the services or replace them with encrypted alternatives. FTP security concerns are discussed in RFC 2577, and Telnet plaintext risks are described in the Red Hat Enterprise Linux Security Guide.

QUESTION NO: 21

Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

A. Log retention

B. Log rotation

C. Maximum log size

D. Threshold value

ANSWER: D

Explanation:

Threshold value is correct because alerting processes need a defined trigger point that separates normal or low-priority activity from events that require review. In security monitoring, compliance tracking, and violation analysis, thresholds are commonly used to reduce alert noise by generating notifications only when an event count, severity, duration, or metric exceeds an established baseline or policy limit. For example, a security team might alert only after a certain number of failed authentication attempts within a defined time window, repeated policy violations by the same account, or traffic volume above an expected range. This helps analysts focus on events that are more likely to indicate meaningful risk, rather than being overwhelmed by every individual log entry or minor deviation. Threshold-based alerting is also a common part of SIEM and monitoring design because it supports tuning, reduces false positives, and makes escalation workflows more manageable. CompTIA CySA+ objectives emphasize analyzing logs, events, and alerts while using appropriate tuning methods to support effective detection and response. For additional context, see Splunk's overview of alert thresholds and Microsoft's guidance on Azure Monitor alerts.

QUESTION NO: 22

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country.

Which of the following best describes what is happening? (Choose two.)

A. Beaconinq

B. Domain Name System hijacking

C. Social engineering attack

D. On-path attack

E. Obfuscated links

F. Address Resolution Protocol poisoning

ANSWER: C E

Explanation:

Social engineering attack and Obfuscated links are the correct descriptions. The scenario describes emails crafted to target a specific privileged group: company administrators. That is consistent with a social engineering attack because the attacker is attempting to manipulate recipients into taking an unsafe action, such as clicking a link, rather than relying only on a direct technical exploit. Targeting administrators also increases the potential impact because those users often have elevated privileges and access to sensitive systems. The concealed URL is accurately described as Obfuscated links because the true destination is hidden or disguised from the recipient. Attackers commonly use URL shorteners, misleading anchor text, encoded characters, redirects, or lookalike domains to make a malicious or suspicious destination appear legitimate. In phishing and spear-phishing campaigns, obfuscated links are frequently used to lure selected users to credential-harvesting pages, malware download sites, or attacker-controlled infrastructure. CISA describes phishing as a common social engineering technique that uses deceptive messages and links to trick users, while OWASP documents URL redirection and related techniques that can disguise destinations and support phishing activity. References: CISA: Avoiding Social Engineering and Phishing Attacks and OWASP: URL Redirection Attack.

QUESTION NO: 23

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 include **Affected hosts** because the report must clearly identify which systems are exposed to each discovered weakness. This typically includes hostnames, IP addresses, operating systems, open services, ports, and sometimes asset ownership or business function. Without the affected asset details, security teams cannot validate findings, assign remediation work, or determine whether the vulnerability applies to a critical production system or a lower-priority asset.

Risk score is also a core part of vulnerability reporting because it helps prioritize remediation based on severity and potential impact. Vulnerability scanners commonly use scoring models such as CVSS to communicate exploitability, impact, and urgency in a standardized way. A risk score allows analysts and system owners to focus first on vulnerabilities that present the greatest threat to confidentiality, integrity, or availability. This aligns with vulnerability management best practices, where scan output is triaged and ranked before remediation activities are assigned. For more context, see the official FIRST CVSS documentation and NIST guidance on vulnerability management in NIST SP 800-40 Rev. 4.

QUESTION NO: 24

Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

A. Install a firewall.

B. Implement vulnerability management.

C. Deploy sandboxing.

D. Update the application blocklist.

ANSWER: C

Explanation:

Deploy sandboxing is correct because sandboxing provides an isolated, controlled execution environment for suspicious files, scripts, documents, or processes. When antivirus does not recognize or block a new ransomware variant, sandboxing can still reduce impact by containing execution and observing behavior before the code is allowed to interact broadly with production systems, shared drives, user data, or other endpoints. This is especially valuable against new or modified ransomware that may evade signature-based detection, because the focus is on isolating and analyzing behavior rather than relying only on a known malware signature. In a CySA+ context, sandboxing is commonly used as a malware analysis and containment control: suspicious attachments, downloads, or executables can be detonated in a safe environment to identify encryption behavior, command-and-control activity, privilege escalation attempts, or file system changes. That containment helps limit the ransomware's ability to encrypt business data or propagate while analysts investigate and respond. For additional context, CISA recommends layered ransomware defenses and malware handling practices in its StopRansomware guidance, and NIST discusses malware containment and analysis approaches in NIST SP 800-83 Rev. 1.

QUESTION NO: 25

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 most likely recipients of a vulnerability scan report because vulnerability reporting must support both governance-level risk decisions and hands-on remediation. Executive management typically needs the summarized business-risk view: overall exposure, severity trends, remediation progress, exceptions, and resource or budget needs. This allows leadership to prioritize risk reduction, approve remediation efforts, and track whether the organization's vulnerability management program is meeting its objectives. Systems admininstration needs the detailed technical findings because administrators are usually responsible for applying patches, changing insecure configurations, validating affected assets, coordinating maintenance windows, and confirming remediation through rescans. In a mature vulnerability management process, reports are tailored for the audience, with executives receiving summarized risk metrics and technical teams receiving actionable vulnerability details. This aligns with NIST guidance that vulnerability management includes identifying vulnerabilities, assessing risk, prioritizing remediation, and tracking corrective actions across responsible organizational roles. See NIST SP 800-40 Rev. 4 and CISA Known Exploited Vulnerabilities Catalog for related vulnerability management and prioritization guidance.

QUESTION NO: 26

During an incident, a security analyst discovers a large amount of PII has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's

personal email. Which of the following should the analyst recommend be done first?

A. Place a legal hold on the employee's mailbox.

B. Enable filtering on the web proxy.

C. Disable the public email access with CASB.

D. Configure a deny rule on the firewall.

ANSWER: A

Explanation:

Place a legal hold on the employee's mailbox is correct because the first priority in this insider data-exfiltration scenario is to preserve potentially relevant evidence in a defensible manner. The employee has already sent a large amount of personally identifiable information to a personal email address, which may lead to legal, regulatory, HR, or law-enforcement actions. A legal hold ensures mailbox content, including sent messages and items that might later be deleted or altered, is retained for investigation and eDiscovery. This supports evidence preservation, helps maintain the integrity of the investigation, and reduces the risk that key artifacts are lost before the organization can complete its incident response process. In Microsoft 365 environments, litigation hold and eDiscovery hold capabilities are specifically designed to preserve mailbox data for legal or investigation purposes, including deleted content when configured appropriately. See Microsoft's guidance on creating a litigation hold and the broader Microsoft Purview eDiscovery documentation for details on preserving content during investigations.

QUESTION NO: 27

A security analyst is conducting a vulnerability assessment of a company's online store. The analyst discovers a critical vulnerability in the payment processing system that could be exploited, allowing attackers to steal customer payment information. Which of the following should the analyst do next?

A. Leave the vulnerability unpatched until the next scheduled maintenance window to avoid potential disruption to business.

B. Perform a risk assessment to evaluate the potential impact of the vulnerability and determine whether additional security measures are needed.

C. Ignore the vulnerability since the company recently passed a payment system compliance audit.

D. Isolate the payment processing system from production and schedule for reimaging.

ANSWER: B

Explanation:

Perform a risk assessment to evaluate the potential impact of the vulnerability and determine whether additional security measures are needed is the correct next action. In a vulnerability assessment, finding a critical issue is not the end of the process; the analyst must evaluate the real business risk by considering exploitability, asset criticality, exposure, likelihood of exploitation, and potential impact. Because the affected system processes customer payment information, the assessment should quickly establish how urgent the response must be, what compensating controls may be required, and how remediation should be prioritized against operational impact. This aligns with standard vulnerability management practices, where identified vulnerabilities are analyzed and prioritized based on risk before remediation actions are selected and tracked. NIST describes vulnerability response as a process that includes identifying, analyzing, prioritizing, and remediating vulnerabilities in a risk-informed manner; see NIST SP 800-40 Revision 4. CISA also emphasizes prioritizing vulnerability remediation using risk factors such as exploitation evidence and asset importance; see CISA SSVC guidance.

QUESTION NO: 28

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 correct because endpoint detection and response tooling provides visibility, alerting, and response actions on the compromised hosts while allowing required services to remain online. In a law-enforcement-supported active investigation, containment often needs to limit attacker actions without immediately destroying evidence or interrupting monitored access. EDR can help detect malicious processes, credential dumping, persistence mechanisms, suspicious database access, and lateral movement, and it can support response actions such as process termination, host isolation policies, and forensic collection. See CISA Incident Response Playbook.

use micro segmentation to restrict connectivity to/from the web and database servers is also correct because it narrows the permitted communication paths to only what the business and investigation require: internet access through the reverse proxy and controlled connectivity between the web server and database server. Microsegmentation applies granular network controls around workloads, reducing the adversary’s ability to pivot, scan internal systems, or exfiltrate data through

unauthorized routes while preserving the required application flow. This aligns with containment best practices and zero trust principles described by NIST SP 800-207 Zero Trust Architecture.

QUESTION NO: 29

A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

A. Create a timeline of events detailinq the date stamps, user account hostname and IP information associated with the activities

B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation

C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identity the case as an HR-related investigation

D. Notify the SOC manager for awareness after confirmation that the activity was intentional

ANSWER: B

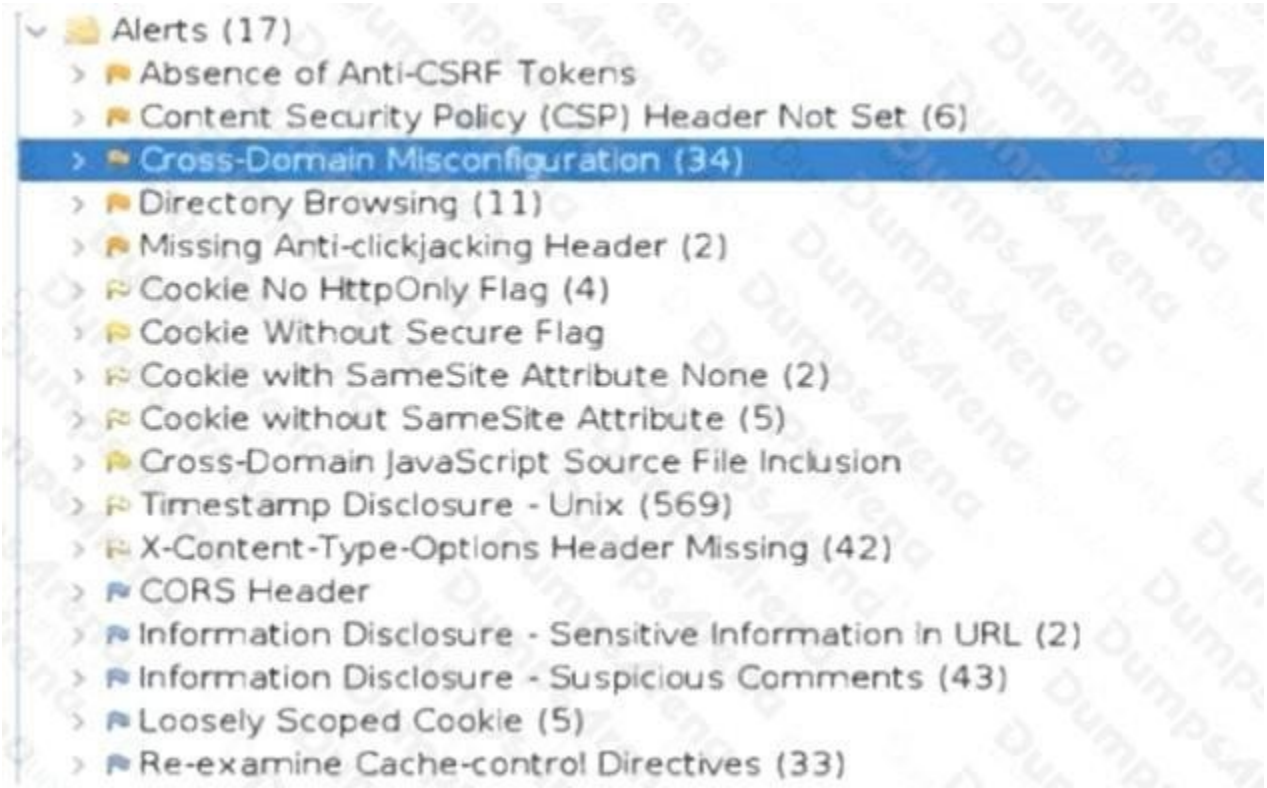
Explanation:

Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation is correct because HR-sensitive security investigations should apply privacy-by-design principles: collect and retain only what is necessary, minimize exposure of personally identifiable information, and limit access to people with a legitimate need to know. In this scenario, the evidence may support a terminable offense, so mishandling the user's identity or browsing details could create unnecessary privacy, employment, or legal risk. Masking or removing user-identifiable details from general case notes helps reduce inappropriate disclosure while still preserving the underlying evidence for authorized reviewers. Password protecting the evidence and restricting access also supports confidentiality, integrity, and chain-of-custody expectations during an investigation.

This aligns with common incident response and privacy practices. NIST incident handling guidance emphasizes proper evidence handling, documentation, and controlled access during security investigations; see NIST SP 800-61 Rev. 2. NIST's privacy guidance also promotes limiting data processing and access to reduce privacy risk; see the NIST Privacy Framework.

QUESTION NO: 30

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Which of the following tuning recommendations should the security analyst share?

A. Set an HttpOnlvflaq to force communication by HTTPS

B. Block requests without an X-Frame-Options header

C. Configure an Access-Control-Allow-Origin header to authorized domains

D. Disable the cross-origin resource sharing header

ANSWER: C

Explanation:

Configure an Access-Control-Allow-Origin header to authorized domains is the correct tuning recommendation when a vulnerability assessment identifies an overly permissive cross-origin resource sharing configuration. CORS controls which external origins are allowed by a browser to read responses from the web application. If the application allows arbitrary origins, such as reflecting any supplied Origin value or using a wildcard inappropriately, a malicious site may be able to make browser-based requests and read sensitive application responses in a user's authenticated session. The safer configuration is to explicitly allow only trusted, business-approved domains that genuinely need cross-origin access, and to avoid broad or dynamic trust decisions. This recommendation aligns with OWASP guidance to validate origins against an allowlist and with browser behavior for the Access-Control-Allow-Origin response header described by MDN. See the OWASP CORS Cheat Sheet and MDN Access-Control-Allow-Origin documentation for implementation guidance.

QUESTION NO: 31

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:

Reduce repetitive tasks and Generate reports and metrics are the correct process improvements associated with implementing a SOAR solution. Security Orchestration, Automation, and Response platforms are designed to connect security tools, automate repeatable response actions, and run standardized playbooks. This helps analysts avoid manually performing the same enrichment, triage, notification, containment, and ticket-updating steps for every alert. By reducing repetitive tasks, a SOAR solution improves consistency, speeds up response, and allows analysts to focus on higher-value investigation and decision-making.

SOAR platforms also commonly generate reports and metrics from the workflows they execute. Because playbooks, cases, approvals, escalations, and response actions are tracked in the platform, teams can measure useful operational data such as incident volume, response times, closure rates, analyst workload, and automation effectiveness. These reports support continuous improvement in the security operations center by showing where processes are working well and where workflows need tuning. Microsoft describes SOAR automation in Sentinel as a way to automate response and orchestrate workflows, and IBM similarly describes SOAR as supporting case management, automation, and measurable response processes. References: Microsoft Learn: SOAR automation in Microsoft Sentinel and IBM: What is SOAR?.

QUESTION NO: 32

A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

A. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }

B. function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }

C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn. cymru.com TXT +short) && echo "$1 | $info" }

D. function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

ANSWER: C

Explanation:

The function using `dig` with `origin.asn.cymru.com` is correct because it is designed to identify the autonomous system number associated with an IP address. Routing anomalies are often investigated by looking at BGP-related information, especially whether traffic or destination prefixes are associated with an unexpected ASN. Team Cymru provides a DNS-based IP-to-ASN mapping service that allows analysts to query an IP address and receive ASN, prefix, country, registry, and allocation information. In this script, the reverse DNS-style representation of the IP address is extracted and then queried against Team Cymru's `origin.asn.cymru.com` zone, returning routing ownership information that can be compared against expected network paths or known legitimate ASNs.

This approach is more directly tied to routing analysis than simply measuring reachability or location. For anomaly detection, ASN data can help reveal suspicious route changes, unexpected hosting providers, or possible BGP hijacking indicators. The underlying technique aligns with Team Cymru's documented IP-to-ASN DNS lookup method and with common use of DNS query tools such as `dig`. References: Team Cymru IP to ASN Mapping and BIND dig DNS lookup utility.

QUESTION NO: 33

An incident responder was able to recover a binary file through the network traffic. The binary file was also found in some machines with anomalous behavior. Which of the following processes most likely can be performed to understand the purpose of the binary file?

A. File debugging

B. Traffic analysis

C. Reverse engineering

D. Machine isolation

ANSWER: C

Explanation:

Reverse engineering is correct because the responder has recovered an unknown binary and needs to determine what it does, how it behaves, and whether it is responsible for the anomalous activity on affected machines. In malware and incident response workflows, reverse engineering commonly involves static analysis, such as reviewing file metadata, hashes, embedded strings, imports, packers, and disassembled code, as well as dynamic analysis, such as running the binary in a controlled sandbox or lab to observe file, process, registry, persistence, command-and-control, and network behaviors. These techniques help analysts understand the binary's purpose, capabilities, indicators of compromise, and potential impact so they can support containment, eradication, and detection engineering. This aligns with established malware-handling guidance, where analysis of suspicious code is used to characterize malware behavior and develop response actions. See NIST SP 800-83 Rev. 1 for malware incident prevention and handling guidance, and MITRE ATT&CK malware analysis resources for common analysis practices and context.

QUESTION NO: 34

An organization wants to establish a disaster recovery plan for critical applications that are hosted on premises. Which of the following is the first step to prepare for supporting this new requirement?

A. Choose a vendor to utilize for the disaster recovery location.

B. Establish prioritization of continuity from data and business owners.

C. Negotiate vendor agreements to support disaster recovery capabilities.

D. Advise the leadership team that a geographical area for recovery must be defined.

ANSWER: B

Explanation:

Establish prioritization of continuity from data and business owners is correct because a disaster recovery plan must begin with understanding which business functions, applications, and data are most critical and how quickly they must be restored. This is normally accomplished through a business impact analysis, where application owners, data owners, and business stakeholders define operational impact, dependencies, maximum tolerable downtime, recovery time objectives, and recovery point objectives. Those inputs drive the recovery strategy, including what infrastructure is required, what order systems should be restored in, and what level of redundancy or alternate-site capability is justified.

For on-premises critical applications, technical teams should not start by selecting recovery locations or vendors before business priorities are known. The recovery design must be based on business requirements rather than assumptions. NIST describes business impact analysis as a key planning step for identifying and prioritizing critical information systems and components for contingency planning. Similarly, Ready.gov notes that business impact analysis helps identify time-sensitive or critical business functions and processes. These practices align with CompTIA disaster recovery and business continuity concepts: determine criticality and continuity priorities first, then build the recovery approach around those requirements. See NIST SP 800-34 Rev. 1 and Ready.gov Business Impact Analysis.

QUESTION NO: 35

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:

getconnection (database01, "alpha " , "AXTV. 127GdCx94GTd") ;

Which of the following is the most likely vulnerability in this system?

A. Lack of input validation

B. SQL injection

C. Hard-coded credential

D. Buffer overflow attacks

ANSWER: C

Explanation:

Hard-coded credential is correct because the debugger output appears to show a database connection function being called with a database host, a username-like value, and a password-like value directly embedded in the application logic or runtime command. A value such as `"AXTV. 127GdCx94GTd"` being passed alongside `database01` and `"alpha "` strongly indicates that authentication material is stored in code or configuration in a way that can be exposed during debugging, reverse engineering, source code review, memory inspection, or log collection. This aligns with the common weakness described as using hard-coded credentials, where software contains fixed usernames, passwords, keys, or similar secrets rather than retrieving them securely from a protected secrets-management mechanism. The security impact is significant because anyone who discovers the embedded credential may be able to authenticate to the database or related service, and changing the credential can require code changes, rebuilds, or redeployment. Secure practice is to externalize secrets into protected vaults or environment-specific secure stores and rotate them regularly. See CWE-798: Use of Hard-coded Credentials and OWASP: Use of hard-coded password.

QUESTION NO: 36

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:

The greatest concerns for potential data exfiltration are the entries showing outbound connections from internal hosts to external destinations using protocols that can transfer or conceal data. The entry with source 172.16.1.30 connecting to 5.29.1.5 over TCP 443 using HTTPS Browser.exe is concerning because encrypted web traffic can be used to hide unauthorized uploads to an external server. HTTPS is normal in many environments, but when the destination is an unfamiliar external IP address rather than a known business service, it warrants investigation as a possible covert exfiltration channel.

The entry with source 172.16.1.25 connecting to bank.backup.com over TCP 21 using FTP FileZilla is also a strong exfiltration concern. FTP is specifically designed for file transfers, and an outbound FTP session to an external backup-related domain indicates data may be leaving the organization. FTP also lacks native encryption, increasing the risk that sensitive data or credentials could be exposed in transit. Security monitoring guidance commonly treats unusual outbound transfers, especially to external destinations and over file-transfer protocols, as indicators requiring triage. See CISA's guidance on detecting malicious activity at CISA and OWASP's discussion of data exfiltration risks at OWASP.

QUESTION NO: 37

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, or Security Orchestration, Automation, and Response, is designed to improve security operations processes by connecting tools, automating workflows, and standardizing response activities. Reduce repetitive tasks is correct because SOAR platforms use playbooks and automation to handle routine analyst actions such as enriching alerts, opening tickets, collecting indicators, quarantining assets, or notifying stakeholders. This reduces manual effort, speeds response, and helps analysts focus on higher-value investigation and decision-making. Generate reports and metrics is also correct because SOAR platforms commonly track workflow execution, incident status, response times, analyst actions, and case outcomes. These reporting and metrics capabilities help security teams measure operational effectiveness, identify bottlenecks, demonstrate compliance, and continuously improve incident response processes. Microsoft describes security automation as a way to streamline common SOC workflows through playbooks and automated response actions in Microsoft Sentinel automation. Palo Alto Networks also describes SOAR as combining orchestration, automation, and incident response to standardize processes and improve SOC efficiency in its SOAR overview.

QUESTION NO: 38 - (HOTSPOT)

HOTSPOT

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

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

INSTRUCTIONS

Part 1

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

Part 2

Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each

control may only be used once, and not all controls will be used.

Firewall log:

File integrity Monitoring Report:

File integrity monitoring report

Shows files, folders, shares, and permissions that were created, deleted, or modified.

Action	Object type	What	Who	When
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Removed Where: Workstation: Date created:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx "11/30/19 12:05:34"	Domainusers\user1	11/30/19 12:25:13
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Renamed Where: Workstation: Name changed from:	File Host1 172.30.0.152	resume1.docx to resume2.docx	Domainusers\user1	12/1/19 14:25:30

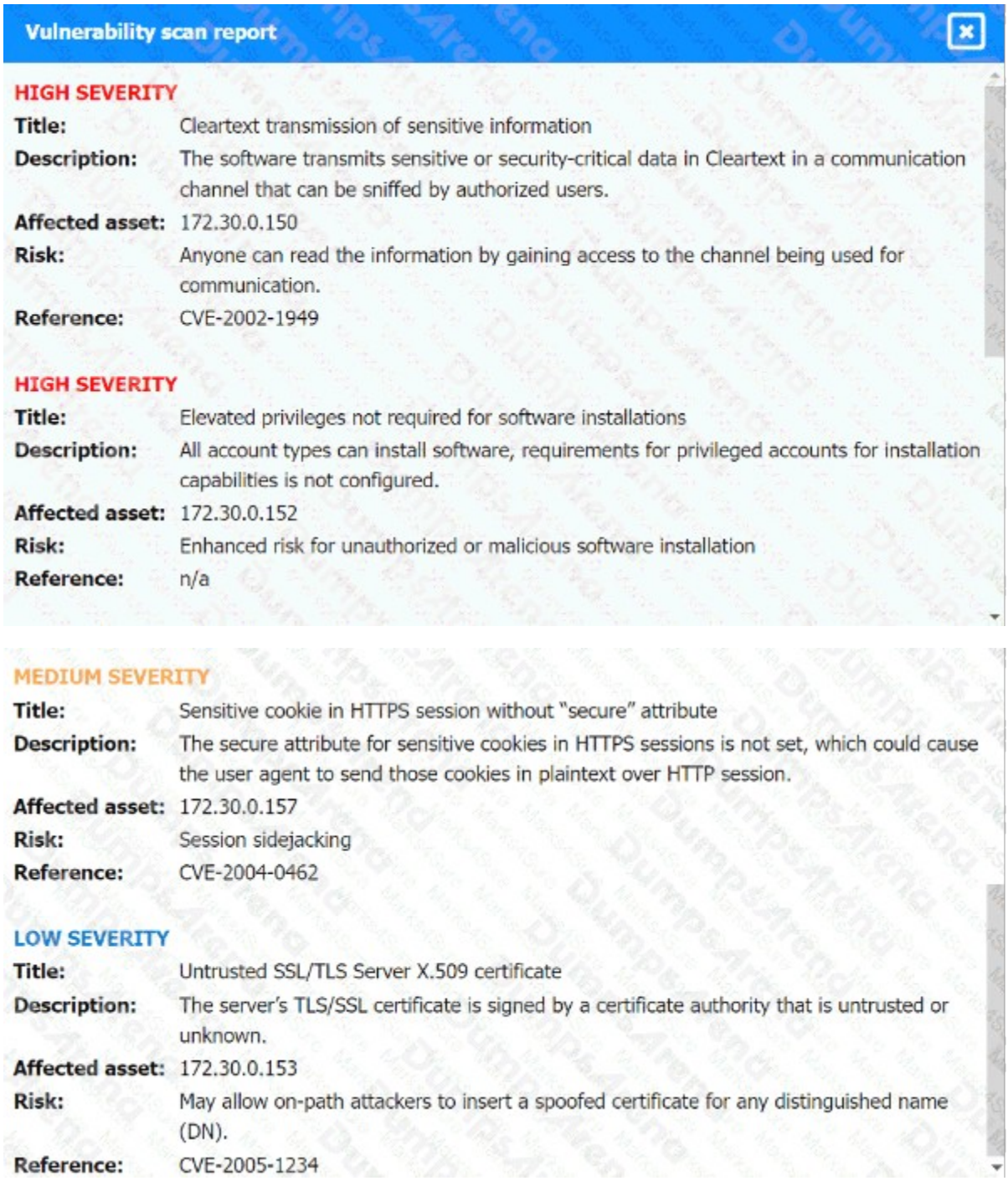
Malware domain list:

Malware domain list

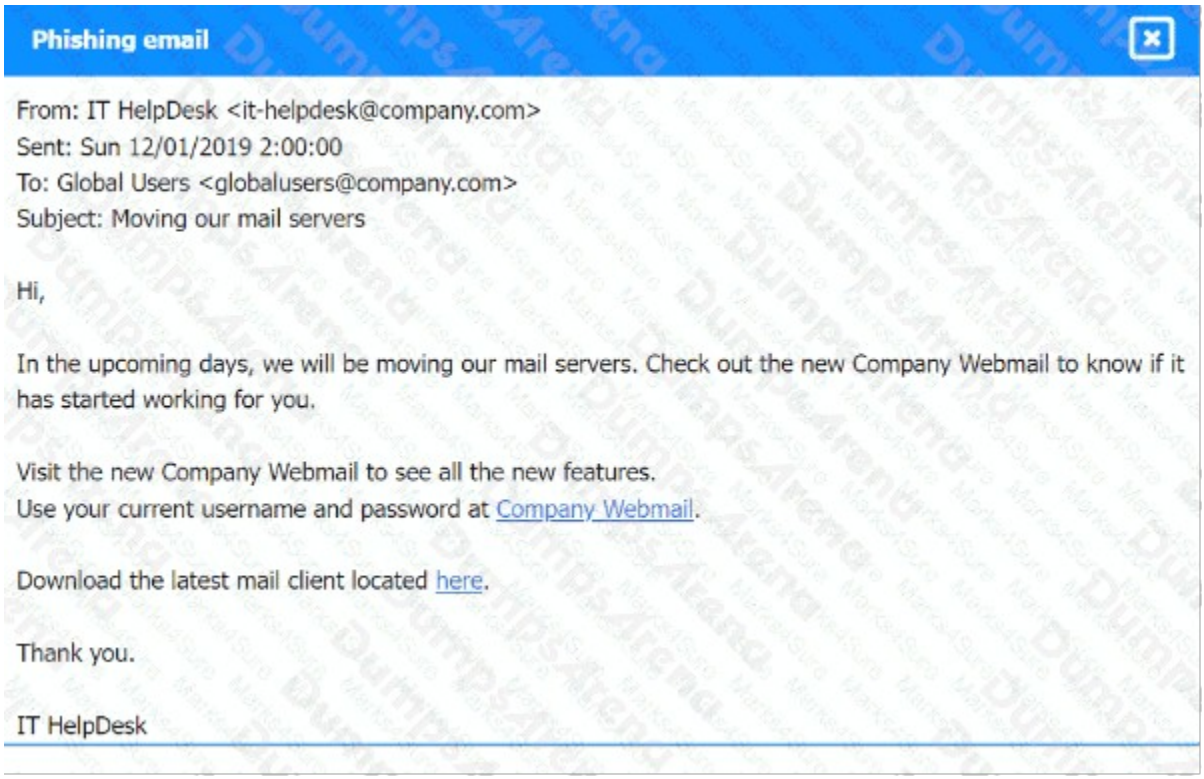
```
# MalwareDomainList.com Host List #
# http://www.maowaredomainlist.com/hostlist/hosts.txt #
# Last updated: 3 Dec 2019, 21:00:00 #
# IP #

171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115
```

Vulnerability Scan Report:



Phishing Email:


Phishing email
From: IT HelpDesk <it-helpdesk@company.com>
Sent: Sun 12/01/2019 2:00:00
To: Global Users <globalusers@company.com>
Subject: Moving our mail servers
Hi,
In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.
Visit the new Company Webmail to see all the new features.
Use your current username and password at Company Webmail.
Download the latest mail client located here.
Thank you.
IT HelpDesk


Kill chain item
Phishing email
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups
Malware install
Active links
Malware execution
Malicious website access
File encryption
Malware downbac
Identify the following:
Malicious executable
Select option
invoice.exe
resume1.docx
resume2.docx
payroll.xlsx
Malicious IP address
81.161.63.103
81.161.63.253
171.25.193.20
185.220.101.194
192.168.2.1
171.25.193.25
10.1.1.238
Date/time malware entered organization
1 Dec 2019 11:24:16
1 Dec 2019 14:03:19
1 Dec 2019 14:03:55
30 Nov 2019 12:05:39
1 Dec 2019 14:25:30
1 Dec 2019 12:56:25
30 Nov 2019 12:25:13

ANSWER:

Explanation:

The artifacts point to a single malware event tied to the phishing email. The firewall alert identifies **invoice.exe** as suspicious traffic coming from **81.161.63.253**, and that same address appears in the malware domain list, confirming it is the malicious source. The file integrity monitoring report then shows **invoice.exe** being added to the user's Downloads folder on Host1 at **1 Dec 2019 14:03:55**, which is the best timestamp for when the executable landed on the internal workstation.

The controls align naturally to the attack flow. **Email filtering** helps stop phishing messages before users see them. **Plain text email format** reduces the risk from embedded clickable links because links are less likely to be hidden behind deceptive display text. **IP blocklist** is appropriate for access to a known malicious website or host, especially when the malicious address is present in threat intelligence. **Firewall file type filter** helps prevent executable content from being downloaded through allowed web traffic. **Restricted local user permissions** addresses the scan finding that users could install software without elevated privileges, which directly enabled malware installation. **Updated antivirus** is suited to stopping or detecting malware execution on the endpoint. Finally, **Backups** are the key resilience control for file encryption incidents because they allow restoration of affected data after ransomware-like activity. These layered defenses match guidance from resources such as CISA phishing guidance, MITRE ATT&CK user execution guidance, and the CISA StopRansomware Guide.

QUESTION NO: 39

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

A. A mean time to remediate of 30 days

B. A mean time to detect of 45 days

C. A mean time to respond of 15 days

D. Third-party application testing

ANSWER: A

Explanation:

A mean time to remediate of 30 days is correct because the key risk described is the gap between public patch availability and active exploitation. If attackers are commonly weaponizing vulnerabilities about 45 days after a patch is released, the organization needs a vulnerability and patch remediation objective that consistently closes exposure before that exploitation window. A 30-day mean time to remediate establishes a measurable operational target for applying fixes, validating remediation, and reducing the period during which vulnerable systems remain exploitable. In vulnerability management, remediation time is a central performance metric because it directly reflects how quickly known weaknesses are eliminated after they are identified or after vendor fixes become available. NIST guidance on enterprise patch management emphasizes timely deployment of patches as part of reducing organizational exposure to known vulnerabilities; see NIST SP 800-40 Rev. 4. CISA's focus on rapidly remediating known exploited vulnerabilities also reinforces the importance of fixing vulnerabilities before they are broadly exploited; see the CISA Known Exploited Vulnerabilities Catalog. By setting remediation to 30 days, the organization creates a defensible buffer ahead of the 45-day exploitation trend.

QUESTION NO: 40

An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?

A. The firewall service account was locked out.

B. The firewall was using a paid feed.

C. The firewall certificate expired.

D. The firewall failed open.

ANSWER: C

Explanation:

The firewall certificate expired is the best answer because a certificate-dependent integration can fail suddenly when the certificate reaches its validity end date. Firewall log feeds, API integrations, and enrichment connectors commonly rely on TLS certificates for encrypted transport and, in some environments, mutual authentication between the firewall, SIEM, SOAR, or threat intelligence platform. Once the certificate is no longer valid, the receiving system may reject the connection or the firewall may be unable to establish a trusted session, causing that specific enrichment source to stop while unrelated open intelligence feeds continue operating normally. This matches the scenario: the issue is isolated to the firewall feed rather than a broad enrichment platform outage. Certificate lifecycle management is therefore a key operational dependency for security monitoring integrations. Microsoft notes that expired certificates can disrupt secure communications and require renewal or replacement to restore trust; see Microsoft Azure Well-Architected Framework: Certificate management. For general TLS behavior and certificate validation concepts, see Cloudflare: What happens when an SSL certificate expires?.

QUESTION NO: 41

An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?

A. Beaconing

B. Cross-site scripting

C. Buffer overflow

D. PHP traversal

ANSWER: A

Explanation:

Beaconing is correct because the observed behavior matches a compromised internal host attempting to communicate with an external command-and-control endpoint. Malware commonly uses periodic or structured outbound connections over allowed protocols such as HTTPS to check in, receive instructions, or exfiltrate small amounts of encoded data. The mention of HTTPS traffic to a known-malicious foreign IP strongly indicates outbound command-and-control activity, and the additional characters in the header can represent encoded identifiers, session information, campaign tags, or other data inserted by malware to identify the infected host to the attacker-controlled infrastructure. This type of traffic is often designed to blend in with normal web traffic, which is why analysts look for suspicious destinations, unusual headers, repeated callbacks, and anomalous encrypted sessions during detection and response. MITRE ATT&CK describes this behavior under application-layer command-and-control using web protocols such as HTTP and HTTPS: MITRE ATT&CK: Web Protocols. CISA also discusses detecting malicious command-and-control communications as part of network defense and incident response practices: CISA Resources and Tools.

QUESTION NO: 42

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

• Five of the systems only required a reboot to finalize the patch application.

• Two of the servers are running outdated operating systems and cannot be patched

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

A. Compensating controls

B. Due diligence

C. Maintenance windows

D. Passive discovery

ANSWER: A

Explanation:

Compensating controls is correct because the servers have a known security weakness that cannot be remediated through normal patching. When a primary control, such as applying vendor security updates, is not possible, an organization should implement alternative safeguards that reduce the likelihood or impact of exploitation. In this scenario, isolating the outdated servers is a compensating control because it limits network exposure, restricts attacker reachability, and can be combined with firewall rules, access control lists, segmentation, monitoring, or intrusion prevention to reduce the chance of compromise. This aligns with common vulnerability management practice: when a vulnerability cannot be fixed directly, the organization should document and apply mitigating or compensating measures until the vulnerable asset can be upgraded, replaced, or retired. NIST describes compensating controls as controls employed in place of recommended controls that provide equivalent or comparable protection, while CISA vulnerability guidance emphasizes mitigation actions when patching is unavailable or impractical. See NIST CSRC: Compensating Security Controls and CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 43

Which of the following best explains the importance of the implementation of a secure software development life cycle in a company with an internal development team?

A. Increases the product price by using the implementation as a piece of marketing

B. Decreases the risks of the software usage and complies with regulatory requirements

C. Improves the agile process and decreases the amount of tests before the final deployment

D. Transfers the responsibility for security flaws to the vulnerability management team

ANSWER: B

Explanation:

Decreases the risks of the software usage and complies with regulatory requirements is correct because a secure software development life cycle embeds security activities throughout planning, design, coding, testing, deployment, and maintenance. For an internal development team, this means security is treated as a built-in quality requirement rather than something checked only at the end. Practices such as threat modeling, secure coding standards, code review, dependency analysis, security testing, and remediation tracking reduce the likelihood that exploitable vulnerabilities will be introduced or released into production. This directly lowers business risk associated with data exposure, service disruption, fraud, and incident response costs.

A secure SDLC also supports regulatory and contractual compliance because many frameworks require organizations to demonstrate secure development practices, vulnerability management, access control, logging, and protection of sensitive data. For example, NIST describes secure software development practices in the Secure Software Development Framework, and OWASP provides widely used guidance through the Software Assurance Maturity Model. Implementing these practices gives the company repeatable evidence that security controls are consistently applied during development.

QUESTION NO: 44

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

A. Beaconinq

B. Domain Name System hijacking

C. Social engineering attack

D. On-path attack

E. Obfuscated links

F. Address Resolution Protocol poisoning

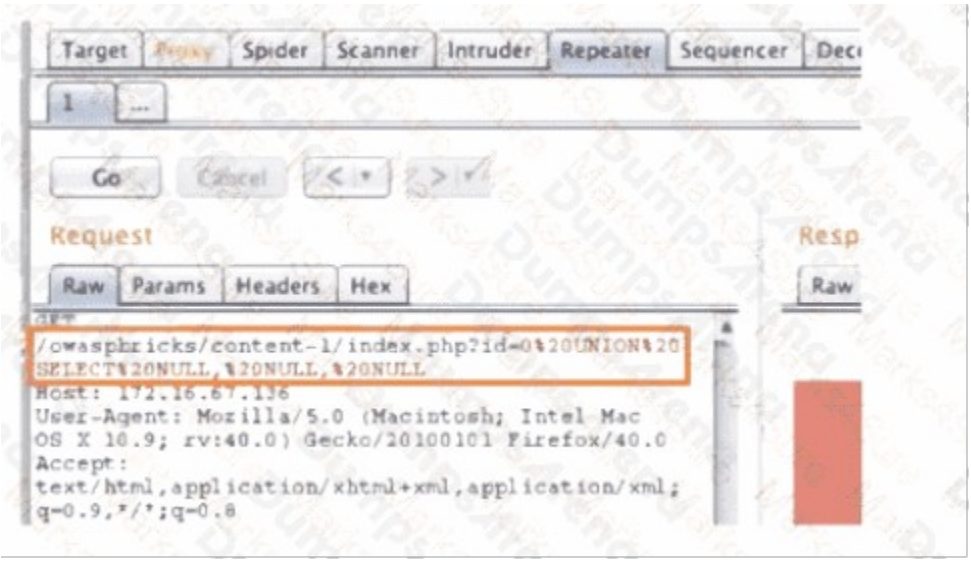
ANSWER: C E

Explanation:

Social engineering attack and Obfuscated links are the correct descriptions. The scenario describes emails crafted to influence a specific group of people, the company administrators, into taking an action such as clicking a link. That is a classic social engineering pattern because the attacker is relying on deception and user interaction rather than directly exploiting a network protocol flaw. Since the emails are aimed only at administrators, the activity also resembles targeted phishing or spear phishing, where privileged users are selected because their accounts or systems may provide greater access if compromised. The concealed URL is also important: hiding, disguising, or otherwise masking the destination of a link is a common tactic used to make malicious links appear safer or less suspicious. MITRE documents phishing via links as a common initial access technique in which users are persuaded to follow attacker-controlled URLs, often leading to credential theft or malware delivery: MITRE ATT&CK Spearphishing Link. CISA also highlights deceptive emails and malicious links as common phishing and social engineering methods: CISA Avoid Phishing.

QUESTION NO: 45

A penetration tester is conducting a test on an organization ' s software development website. The penetration tester sends the following request to the web interface:



Which of the following exploits is most likely being attempted?

A. SQL injection

B. Local file inclusion

C. Cross-site scripting

D. Directory traversal

ANSWER: A

Explanation:

SQL injection is correct because the request shown includes a database query manipulation pattern, specifically a “UNION SELECT” style payload. In a SQL injection attack, the tester places SQL syntax into an application parameter or form field to determine whether the application improperly concatenates user input into backend database queries. The UNION operator is commonly used during exploitation to append attacker-controlled SELECT statements to the application’s original query, allowing the tester to enumerate database structure or retrieve data from additional tables when the number and type of returned columns can be matched. This is a classic indicator of SQL injection testing against a web application interface. CompTIA CySA+ expects analysts to recognize common web application attack signatures in requests and logs, and SQL keywords such as SELECT, UNION, WHERE, OR, and comment markers are strong evidence of attempted query injection. For more detail, see the OWASP overview of SQL Injection and PortSwigger’s explanation of SQL injection UNION attacks.

QUESTION NO: 46

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 correct remediation steps. Padding oracle attacks target weaknesses in how certain block cipher modes, especially CBC, handle padding validation during decryption. If an attacker can force or negotiate a TLS configuration that uses CBC-based cipher suites, the server may become exposed to attacks such as Lucky Thirteen-style padding oracle exploitation. Removing cipher suites that use CBC directly eliminates the vulnerable mode of operation from negotiation, forcing clients to use safer authenticated encryption modes such as AES-GCM or ChaCha20-Poly1305.

Preferring TLS 1.3 is also appropriate because TLS 1.3 removed support for legacy and weak cryptographic options, including CBC-mode cipher suites. TLS 1.3 only supports AEAD cipher suites, which combine encryption and authentication and are designed to avoid this class of padding-related weakness. In practice, a hardened web server should prioritize TLS 1.3 while still carefully controlling any TLS 1.2 fallback configuration so that CBC suites are unavailable. See the TLS 1.3 RFC and Mozilla's Server Side TLS guidance for supported modern TLS configuration recommendations.

QUESTION NO: 47

Several vulnerability scan reports have indicated runtime errors as the code is executing. The dashboard that lists the errors has a command-line interface for developers to check for vulnerabilities. Which of the following will enable a developer to correct this issue? (Select two).

A. Performing dynamic application security testing

B. Reviewing the code

C. Fuzzing the application

D. Debugging the code

E. Implementing a coding standard

F. Implementing IDS

ANSWER: B D

Explanation:

Reviewing the code and Debugging the code are the best choices because the issue has already been identified as runtime errors occurring while the application executes, and the developer needs to move from detection to correction. Reviewing the code allows the developer to inspect the affected functions, input handling, control flow, exception handling, and security-sensitive logic that may be producing the reported vulnerability conditions. Secure code review is a standard way to validate whether the implementation contains flaws that can lead to exploitable behavior, as described in the OWASP Code Review Guide. Debugging the code is also essential because runtime errors often require reproducing the failure, stepping through execution, inspecting variables, checking stack traces, and confirming the exact point where the application behaves incorrectly. Debugging tools help developers isolate the defect and verify that the code fix resolves the problem without introducing new issues; Microsoft provides a good overview of this process in its debugging documentation. Together, code review and debugging provide the practical remediation workflow needed to correct vulnerabilities reflected by runtime error reports.

QUESTION NO: 48

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 both bring in outside expertise to find security weaknesses without requiring the company to add more internal staff or divert existing teams. Contracting a penetration test gives the organization a structured, time-bound assessment in which skilled testers simulate real-world attack techniques against the internet-facing application. This is especially useful after repeated compromises because it can validate whether previously identified design flaws are still exploitable and uncover additional weaknesses in authentication, authorization, session handling, input validation, and business logic. The OWASP Web Security Testing Guide describes this kind of systematic testing approach for web applications. Creating a bug bounty program complements that effort by allowing external researchers to continuously report vulnerabilities under defined rules of engagement. This can broaden coverage across different testing styles and perspectives while scaling vulnerability discovery beyond the company's internal capacity. OWASP's Vulnerability Disclosure Cheat Sheet also supports structured external reporting processes for receiving and handling security findings.

QUESTION NO: 49

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 is the correct remediation priority because it represents the best combination of high technical severity and immediate exploitability. In vulnerability management, analysts should not rely on the CVSS base score alone; they should prioritize findings by considering whether the weakness is exploitable in the current environment, whether exploitation is known or practical, and what impact a successful attack would have. A vulnerability with a CVSS score of 7.1 is already in the high-severity range, and the added fact that it is exploitable makes it more urgent from an operational risk perspective. This aligns with common prioritization guidance: CVSS helps measure severity, while exploitability and environmental

context help determine what should be fixed first. The FIRST CVSS framework describes CVSS as a way to communicate vulnerability severity, and the NIST National Vulnerability Database CVSS guidance emphasizes the role of CVSS metrics in vulnerability assessment. Given the analyst's goal of making the best use of time, concentrating remediation efforts on SVR02 addresses a vulnerability that is both significant in severity and actionable by an attacker.

QUESTION NO: 50

A security analyst needs to identify the devices in a critical infrastructure network that handles an oil and gas pipeline. The network has devices connected over IPv4 using either HTTP or Modbus protocols running on the standard ports. Which of the following approaches should the analyst use to achieve the objective?

A. Employ the IT vulnerability scanner to target ports 80 and 502.

B. Use banner grabbing with Netcat on TCP ports 80 and 502.

C. Perform an Nmap -sS -A -p 80,502 scan.

D. Scan the ICS network using Masscan --open-only -p80,502.

ANSWER: B

Explanation:

Use banner grabbing with Netcat on TCP ports 80 and 502 is correct because it is the most targeted and least intrusive way to identify devices and services in a sensitive industrial control system environment. In an oil and gas pipeline network, availability and operational safety are major concerns, so the analyst should avoid broad, aggressive, or high-speed scanning that could affect fragile OT/ICS devices. Since the question states that the environment uses IPv4 with HTTP and Modbus on their standard ports, the analyst already knows the specific ports to check: TCP 80 for HTTP and TCP 502 for Modbus. Banner grabbing with Netcat allows a controlled connection attempt to those ports to collect service responses, protocol information, or other identifying details without running extensive probes or vulnerability checks. This aligns with common ICS security guidance that emphasizes cautious assessment methods, change control, and minimizing disruption to critical infrastructure. CISA's ICS guidance highlights the importance of protecting operational environments and using practices appropriate for industrial systems: CISA ICS Recommended Practices. Modbus is also a well-known industrial protocol commonly associated with TCP port 502, as documented by the Modbus organization: Modbus FAQ.

QUESTION NO: 51

A security analyst provides the management team with an after-action report for a security incident. Which of the following is the management team most likely to review in order to correct validated issues with the incident response processes?

A. Tabletop exercise

B. Lessons learned

C. Root cause analysis

D. Forensic analysis

ANSWER: B

Explanation:

Lessons learned is correct because it is the post-incident activity specifically intended to turn findings from an after-action report into improvements to the incident response program. After an incident has been contained, eradicated, and recovered from, the organization should review what happened, what actions were effective, where delays or gaps occurred, and which procedures, communications, tools, or controls need to be updated. Management typically uses the lessons learned review to validate issues discovered during the response and approve corrective actions such as updating playbooks, improving escalation paths, refining roles and responsibilities, adjusting training, or changing policy.

This aligns with standard incident response guidance. NIST describes post-incident activity as a way to improve security measures and the incident handling process based on information collected during the incident. CompTIA CySA+ objectives also include post-incident activities, where lessons learned and after-action review concepts are used to improve future response capability. See NIST SP 800-61 Rev. 2 and CompTIA exam objectives resources.

QUESTION NO: 52

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 are the correct entities to involve when an incident manager is preparing communications for the general public. Legal helps ensure that public statements follow applicable breach notification laws, regulatory requirements, contractual obligations, evidence-preservation needs, and liability considerations. This is especially important because incident details released too early, inaccurately, or without proper review can create compliance exposure or interfere with subsequent investigation activities. Public relations is equally important because it manages the organization's external messaging strategy, tone, timing, and consistency across channels. During a cybersecurity incident, public communication must be accurate, coordinated, and understandable while also protecting sensitive investigative details. NIST guidance for incident response emphasizes the importance of predefined communication and coordination processes, including interaction with public affairs and legal counsel. See NIST SP 800-61 Rev. 2. CISA also highlights the need for incident response planning that includes communication roles and responsibilities before an incident occurs; see CISA Incident Response Plan Basics.

QUESTION NO: 53

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

A. config. ini

B. ntds.dit

C. Master boot record

D. Registry

ANSWER: D

Explanation:

Registry is correct because Windows stores a large portion of operating system, hardware, software, service, security, and user configuration data in the Windows Registry. The Registry is a hierarchical configuration database made up of hives, keys, subkeys, and values, which matches the wording in the question about "system configuration keys and values." Administrators and analysts commonly review or restrict access to Registry locations when controlling how users or applications can modify system behavior. In a Windows environment, these configuration items can be viewed and managed using tools such as Registry Editor and command-line utilities, and permissions can be applied to Registry keys to limit

access in a way similar to file-system access control. Microsoft describes the Registry as the central hierarchical database used by Windows to store information necessary to configure the system for users, applications, and hardware devices. For more detail, see Microsoft's documentation on the Windows Registry and the reg command.

QUESTION NO: 54

The DevSecOps team is remediating a Server-Side Request Forgery (SSRF) issue on the company's public- facing website. Which of the following is the best mitigation technique to address this issue?

A. Place a Web Application Firewall (WAF) in front of the web server.

B. Install a Cloud Access Security Broker (CASB) in front of the web server.

C. Put a forward proxy in front of the web server.

D. Implement MFA in front of the web server.

ANSWER: C

Explanation:

Put a forward proxy in front of the web server is the best mitigation listed because SSRF abuses the server's ability to make outbound requests on behalf of an attacker. A properly configured forward proxy can act as an egress control point for those server-initiated requests, enforcing destination allowlists, blocking access to private IP ranges, link-local addresses, cloud metadata services, and other internal-only resources, and creating centralized logs for detection and response. This directly addresses the core SSRF risk: an attacker causing the application server to reach systems or URLs that should never be reachable through user-controlled input. OWASP's SSRF guidance emphasizes strict allowlisting, network-layer controls, and preventing requests to internal or sensitive destinations, which aligns well with using a controlled outbound proxy. PortSwigger also describes SSRF as a vulnerability where the server is induced to make unintended backend requests, making outbound request control especially relevant. See OWASP SSRF Prevention Cheat Sheet and PortSwigger SSRF overview.

QUESTION NO: 55

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:

The machines to address first are server3 and Server5 because vulnerability remediation should be prioritized using risk, not just a simple patch queue. Server5 has a critical finding and resides in the database network, which typically represents high business impact because databases often store sensitive or mission-critical information. A patch is also available, so the analyst can reduce a high-impact risk quickly. server3 has a high-severity finding in the perimeter network, which increases the likelihood of exploitation because perimeter systems are more exposed to external attack paths. Even if a patch is not available, the system still needs to be addressed immediately through compensating controls such as disabling the vulnerable service, restricting access with firewall rules, applying a virtual patch, adding monitoring, or isolating the host until a permanent fix exists. This aligns with vulnerability management guidance to prioritize remediation based on severity, exposure, exploitability, and asset criticality. NIST's enterprise patch management guidance emphasizes risk-based remediation and mitigation when patches are unavailable, and CISA's vulnerability management guidance similarly encourages prioritizing vulnerabilities that present the greatest operational risk. References: NIST SP 800-40 Rev. 4 and CISA Known Exploited Vulnerabilities Catalog.

QUESTION NO: 56

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 is correct because the attack is repeatedly trying to authenticate with one valid domain account. A lockout threshold limits how many password guesses can be made before the account is temporarily locked, greatly reducing the chance that repeated guessing will eventually succeed. Microsoft specifically recommends account lockout policy settings as a way to help prevent attackers from guessing user passwords; see Microsoft account lockout policy.

Block inbound to TCP port 3389 from untrusted remote IP addresses at the perimeter firewall is also correct because RDP uses TCP port 3389 by default, and restricting inbound RDP exposure at the network edge reduces the ability of untrusted systems to reach the service at all. This is especially effective for internet-facing RDP because it reduces the attack surface before authentication attempts reach the server. Microsoft's RDP documentation identifies TCP 3389 as the default listener port, and secure administration best practices commonly recommend limiting management access to trusted sources; see Microsoft Remote Desktop listener documentation.