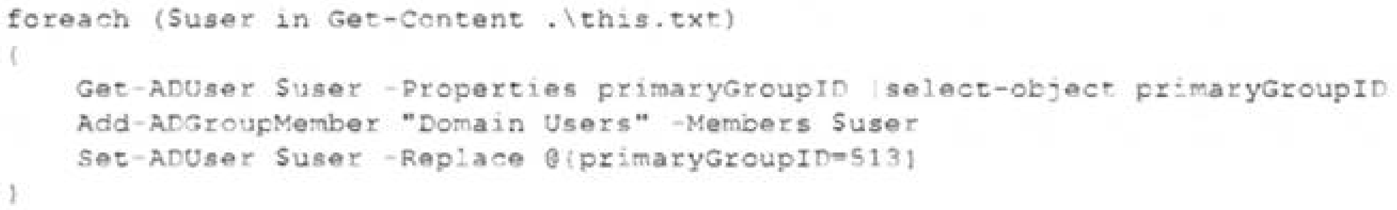
Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

https://www.2passeasy.com/dumps/CS0-003/

NEW QUESTION 1
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}
}
```

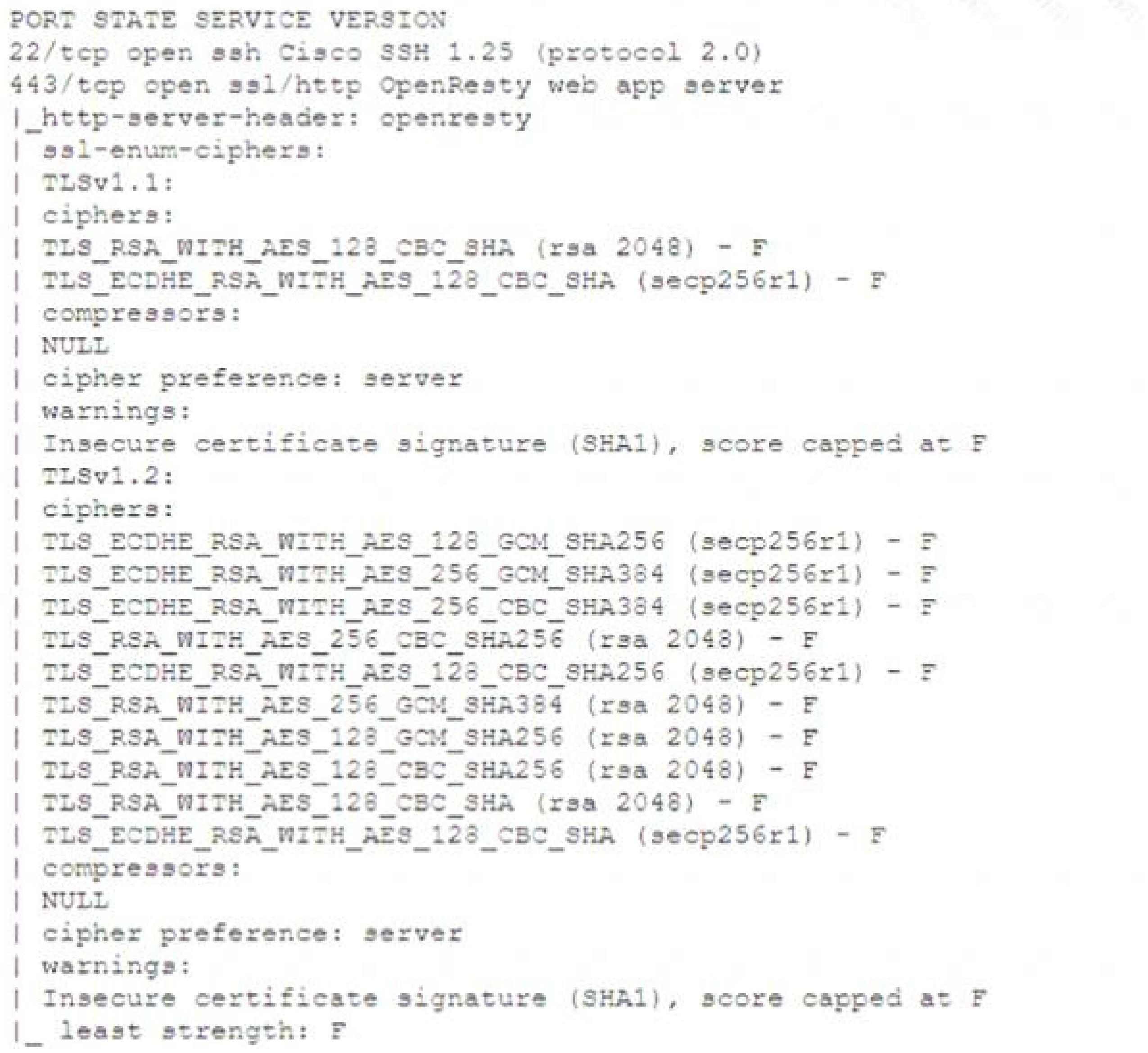
Which of the following scripting languages was used in the script?

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

Answer: A

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.

NEW QUESTION 2
A technician is analyzing output from a popular network mapping tool for a PCI audit:



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

Which of the following best describes the output?

A. The host is not up or responding.
B. The host is running excessive cipher suites.
C. The host is allowing insecure cipher suites.
D. The Secure Shell port on this host is closed

Answer: C

Explanation:
The 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.

NEW QUESTION 3
A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system. Which of the following best meets this
requirement?

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

Answer: D

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

- https://www.comptia.org/certifications/cybersecurity-analyst
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
- https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/

NEW QUESTION 4
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

Answer: D

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 References:
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

NEW QUESTION 5
An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

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

Answer: A

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

NEW QUESTION 6
A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server
logs for evidence of exploitation of that particular vulnerability?

A. /etc/ shadow
B. curl localhost
C. ; printenv
D. cat /proc/self/

Answer: A

Explanation:

/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official References:

- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION 7
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

Answer: D

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.

NEW QUESTION 8
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

Answer: B

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.

NEW QUESTION 9
Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

A. Join an information sharing and analysis center specific to the company's industry.
B. Upload threat intelligence to the IPS in STIX/TAXII format.
C. Add data enrichment for IPS in the ingestion pipleline.
D. Review threat feeds after viewing the SIEM alert.

Answer: C

Explanation:
The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline.
Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS’s capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.
The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company’s industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

NEW QUESTION 10
An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).

A. Drop the tables on the database server to prevent data exfiltration.
B. Deploy EDR on the web server and the database server to reduce the adversaries capabilities.
C. Stop the httpd service on the web server so that the adversary can not use web exploits
D. use micro segmentation to restrict connectivity to/from the web and database servers.
E. Comment out the HTTP account in the / etc/passwd file of the web server
F. Move the database from the database server to the web server.

Answer: BD

Explanation:
Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. Official References:

- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION 10
A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:
• DNS traffic while a tunneling session is active.
• The mean time between queries is less than one second.
• The average query length exceeds 100 characters. Which of the following attacks most likely occurred?

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

Answer: A

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

- DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.
- The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred.
- The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the DNS packets.

Official References:

- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://resources.infosecinstitute.com/topic/bypassing-security-products-via-dns-data-exfiltration/
- https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns_exfiltration_

NEW QUESTION 12
After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

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

Answer: C

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

NEW QUESTION 16
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

Answer: C

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.

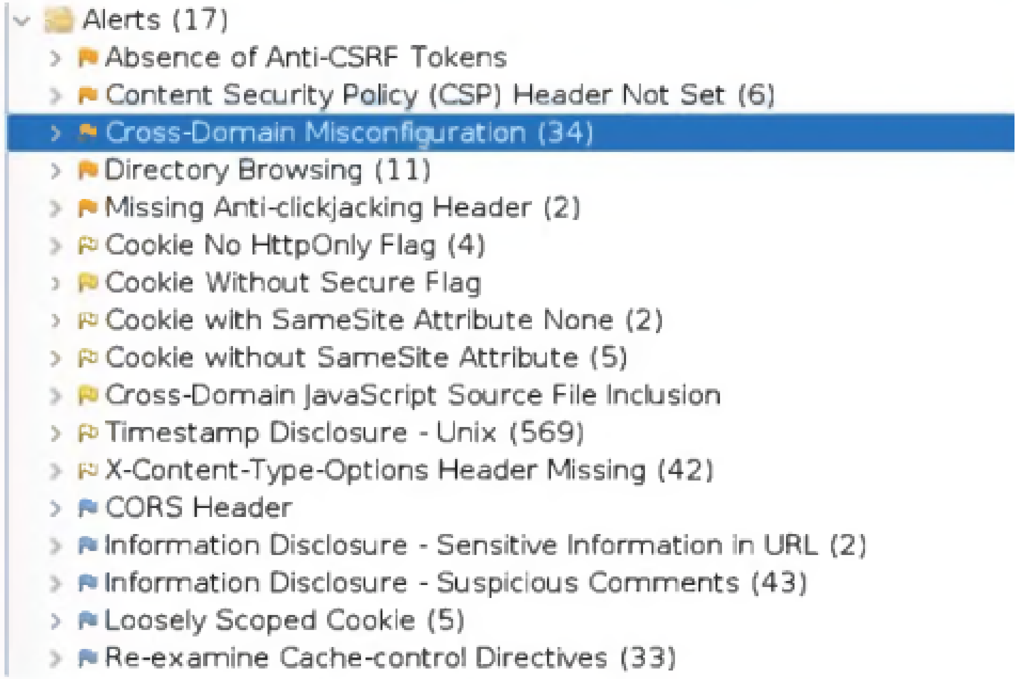
NEW QUESTION 17
An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

A. Beaconinq
B. Domain Name System hijacking
C. Social engineering attack
D. On-path attack
E. Obfuscated links
F. Address Resolution Protocol poisoning

Answer: CE

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.

NEW QUESTION 22
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)
```

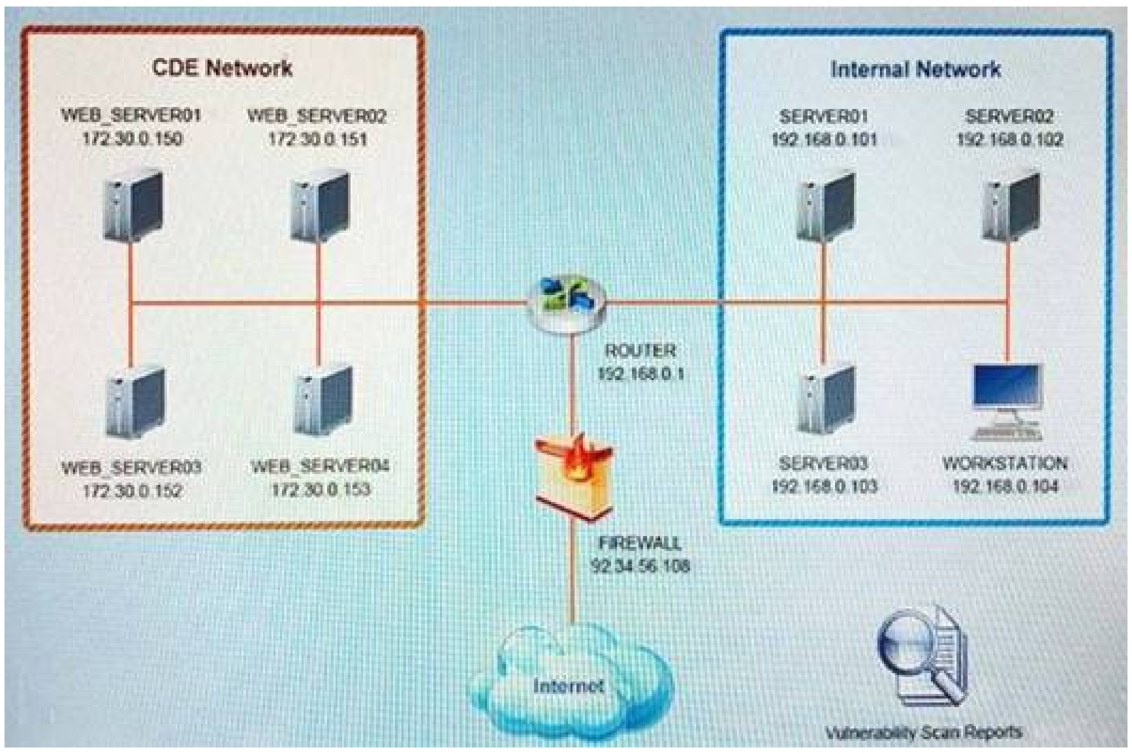
Which of the following tuning recommendations should the security analyst share?

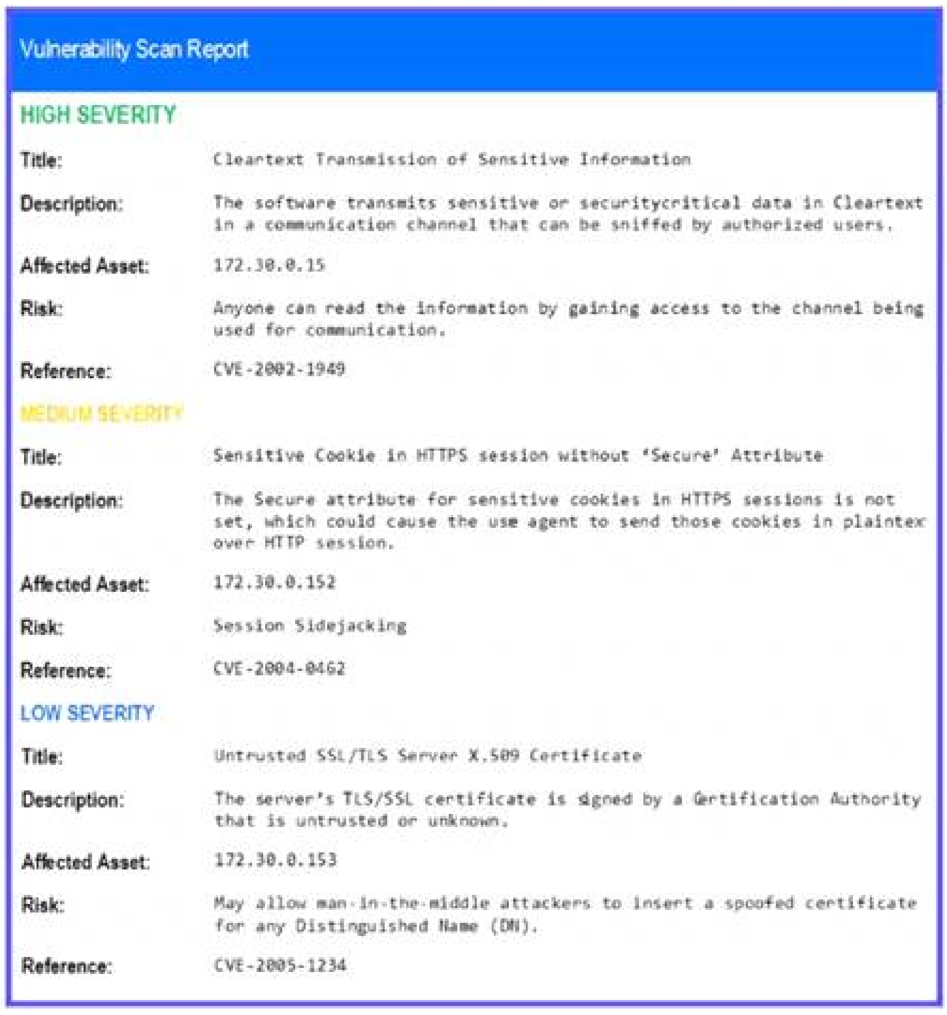
A. Set an HttpOnlvflaq to force communication by HTTPS
B. Block requests without an X-Frame-Options header
C. Configure an Access-Control-Allow-Origin header to authorized domains
D. Disable the cross-origin resource sharing header

Answer: B

Explanation:
The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

NEW QUESTION 26
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.


CDE Network
WEB_SERVER01 172.30.0.150
WEB_SERVER02 172.30.0.151
WEB_SERVER03 172.30.0.152
WEB_SERVER04 172.30.0.153
ROUTER 192.168.0.1
FIREWALL 92.34.56.108
Internet
Internal Network
SERVER01 192.168.0.101
SERVER02 192.168.0.102
SERVER03 192.168.0.103
WORKSTATION 192.168.0.104
Vulnerability Scan Reports



Vulnerability Scan Report

HIGH SEVERITY

Title:	Cleartext Transmission of Sensitive Information
Description:	The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected Asset:	172.30.0.15
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

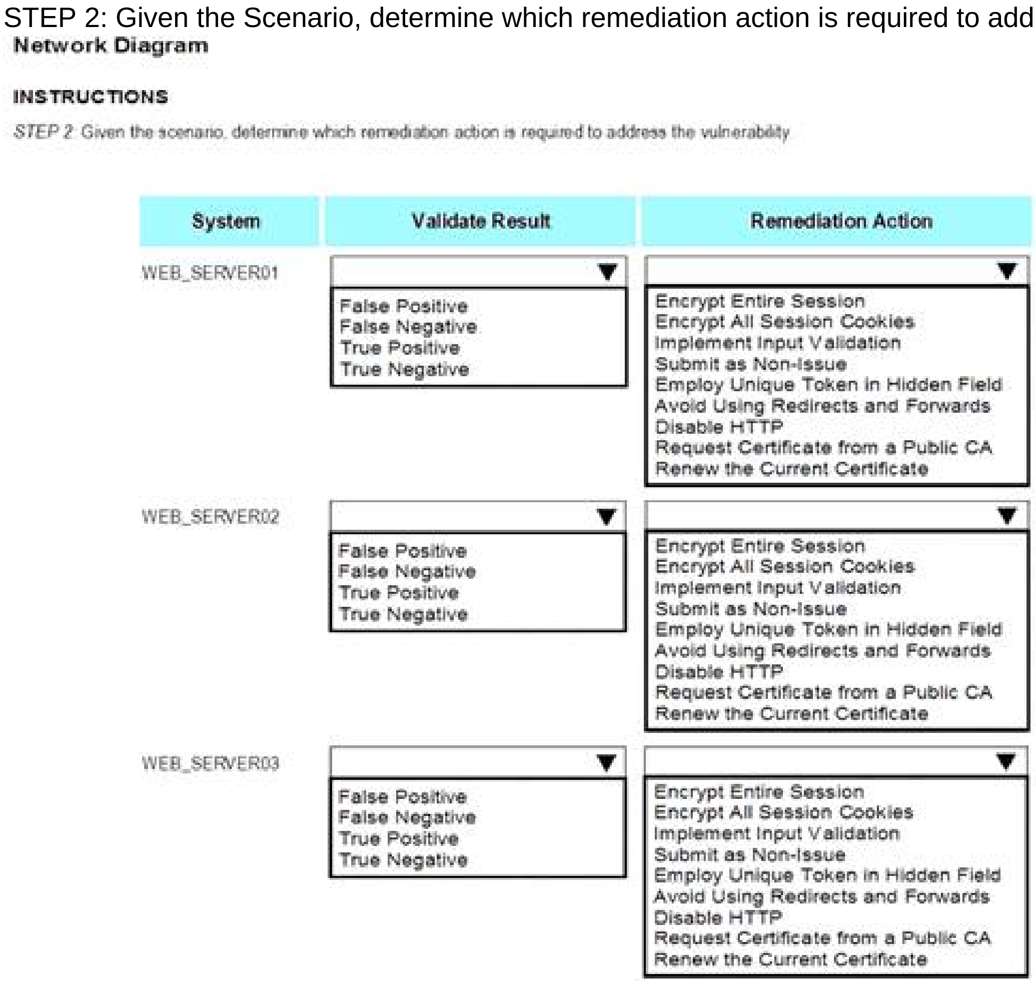
MEDIUM SEVERITY

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 use agent to send those cookies in plaintex over HTTP session.
Affected Asset:	172.30.0.152
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 Certification Authority that is untrusted or unknown.
Affected Asset:	172.30.0.153
Risk:	May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).
Reference:	CVE-2005-1234

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



Network Diagram

INSTRUCTIONS

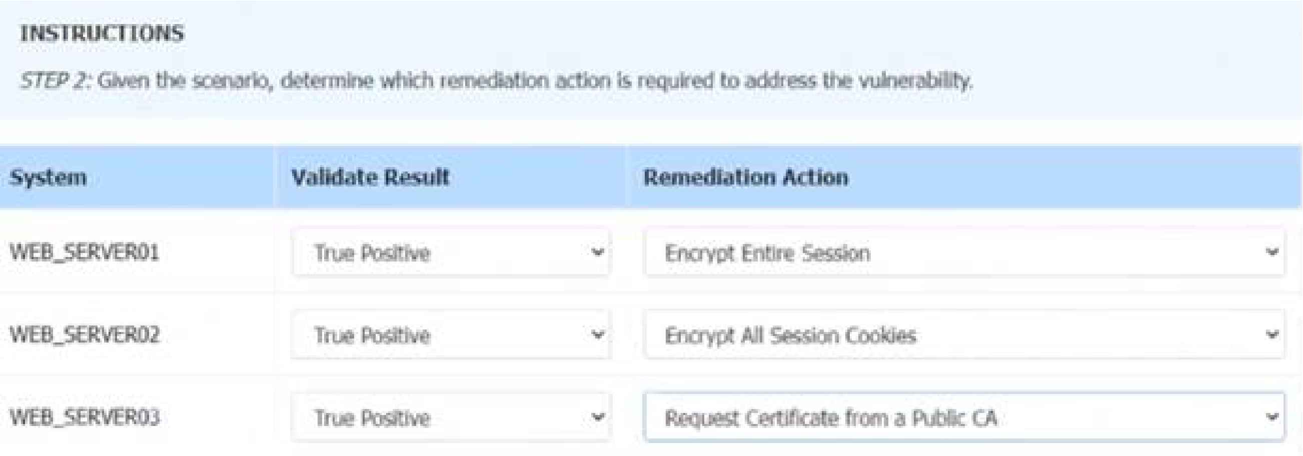
STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



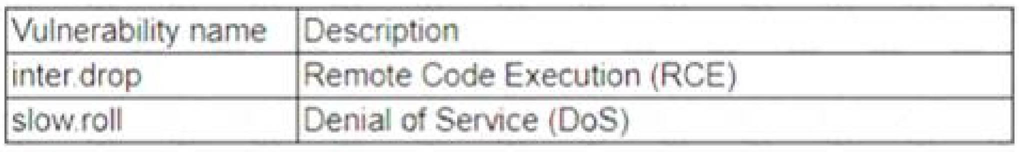
INSTRUCTIONS

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

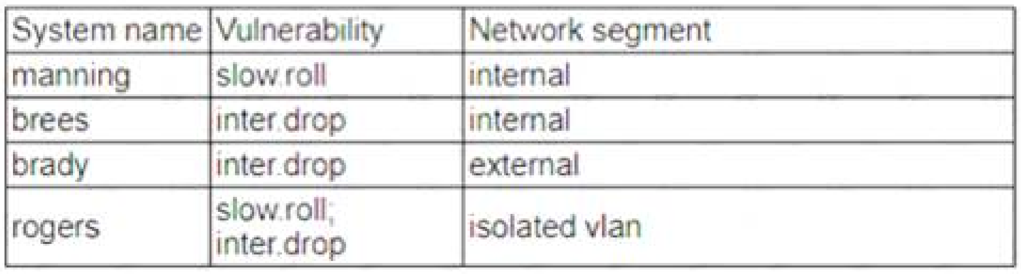
System	Validate Result	Remediation Action
WEB_SERVER01	True Positive	Encrypt Entire Session
WEB_SERVER02	True Positive	Encrypt All Session Cookies
WEB_SERVER03	True Positive	Request Certificate from a Public CA

NEW QUESTION 28

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

Answer: B

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.

NEW QUESTION 30

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

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

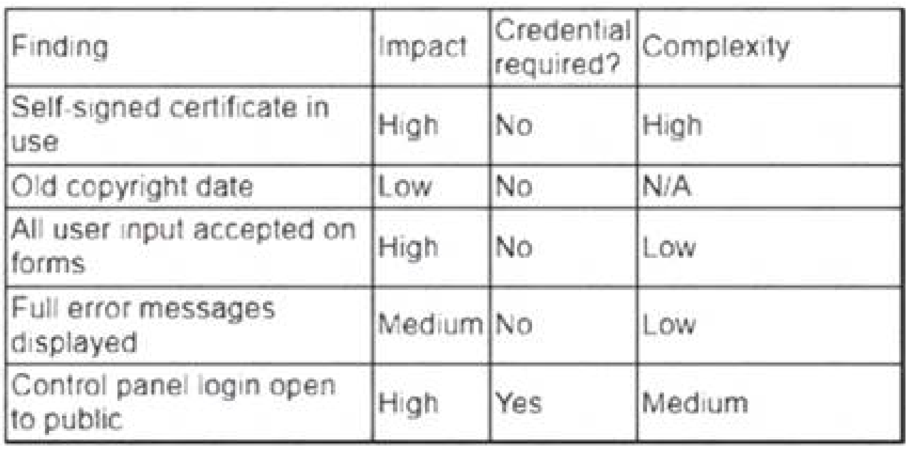
Answer: C

Explanation:

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

NEW QUESTION 35

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

Answer: D

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.

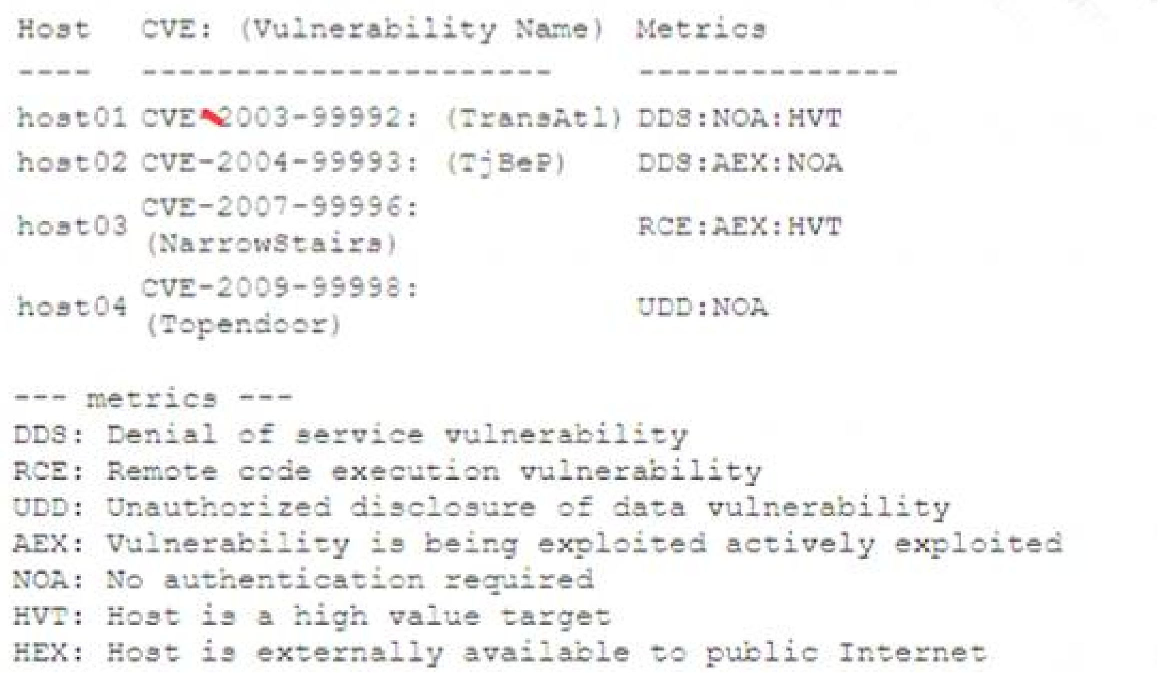
NEW QUESTION 38
Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

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

Answer: A

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.

NEW QUESTION 39
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                            RCE:AEX:HVT
       (NarrowStairs)
       CVE-2009-99998:
host04                            UDD:NOA
       (Topendoor)

--- 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
```

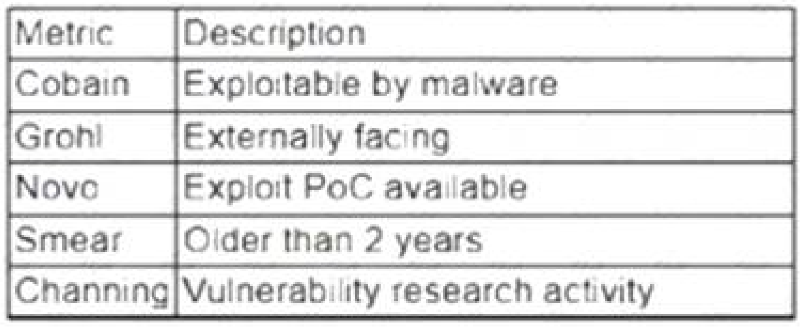
Which of the following hosts should be patched first, based on the metrics?

A. host01
B. host02
C. host03
D. host04

Answer: C

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.

NEW QUESTION 40
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

Answer: B

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.

NEW QUESTION 43
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

Answer: A

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.

NEW QUESTION 46
A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to https://offce365password.acme.co. The site's standard VPN logon page is
www.acme.com/logon. Which of the following is most likely true?

A. This is a normal password change URL.
B. The security operations center is performing a routine password audit.
C. A new VPN gateway has been deployed
D. A social engineering attack is underway

Answer: D

Explanation:
for the outbound traffic to a host IP that resolves to https://offce365password.acme.co, while the site's standard VPN logon page is www.acme.com/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (offce365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. Official References:
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION 47
Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

A. Isolate Joe's PC from the network
B. Reimage the PC based on standard operating procedures
C. Initiate a remote wipe of Joe's PC using mobile device management
D. Perform no action until HR or legal counsel advises on next steps

Answer: D

Explanation:
The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee’s system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee’s system or network.

NEW QUESTION 52
Which of the following security operations tasks are ideal for automation?

A. Suspicious file analysis:Look for suspicious-looking graphics in a folder.Create subfolders in the original folder based on category of graphics found.Move the suspicious graphics to the appropriate subfolder
B. Firewall IoC block actions:Examine the firewall logs for IoCs from the most recently published zero-day exploit Take mitigating actions in the firewall to block the behavior found in the logsFollow up on any false positives that were caused by the block rules
C. Security application user errors:Search the error logs for signs of users having trouble with the security application Look up the user's phone numberCall the user to help with any questions about using the application
D. Email header analysis:Check the email header for a phishing confidence metric greater than or equal to five Add the domain of sender to the block listMove the email to quarantine

Answer: D

Explanation:
Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

NEW QUESTION 57
During an extended holiday break, a company suffered a security incident. This information was properly relayed to appropriate personnel in a timely manner and the server was up to date and configured with appropriate auditing and logging. The Chief Information Security Officer wants to find out precisely what happened. Which of the following actions should the analyst take first?

A. Clone the virtual server for forensic analysis
B. Log in to the affected server and begin analysis of the logs
C. Restore from the last known-good backup to confirm there was no loss of connectivity
D. Shut down the affected server immediately

Answer: A

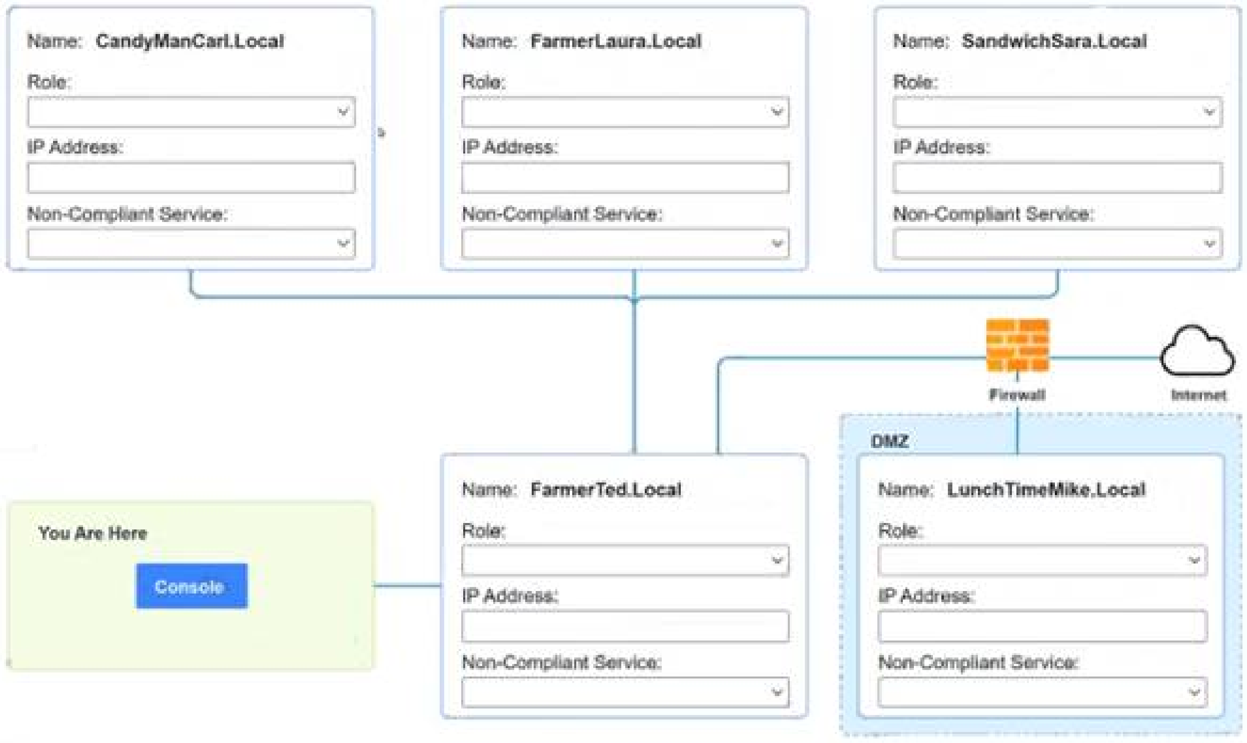
Explanation:
The first action that the analyst should take in this case is to clone the virtual server for forensic analysis. Cloning the virtual server involves creating an exact copy or image of the server’s data and state at a specific point in time. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence. Cloning the virtual server can also allow the analyst to safely analyze and investigate the incident without affecting the original server or its operations.

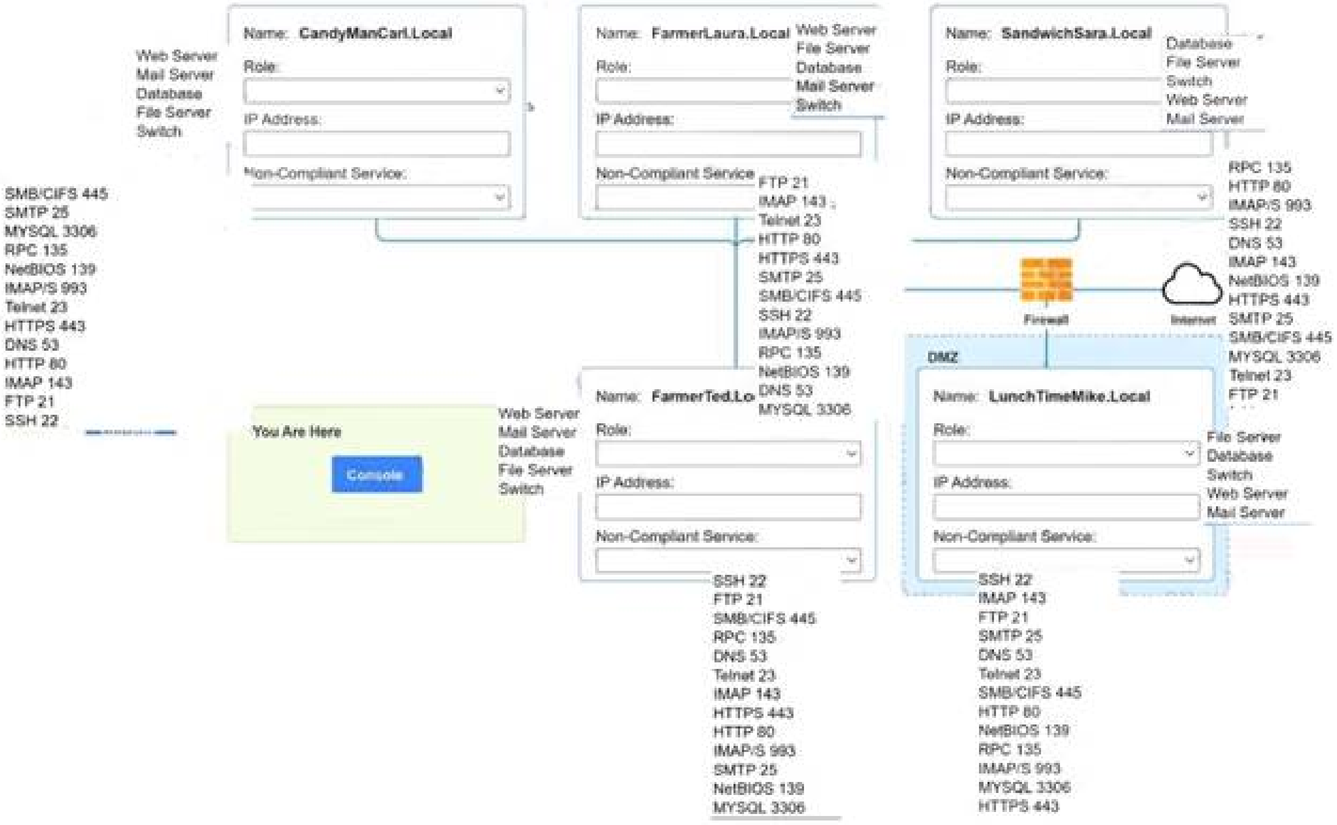
NEW QUESTION 59
You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following.

- 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

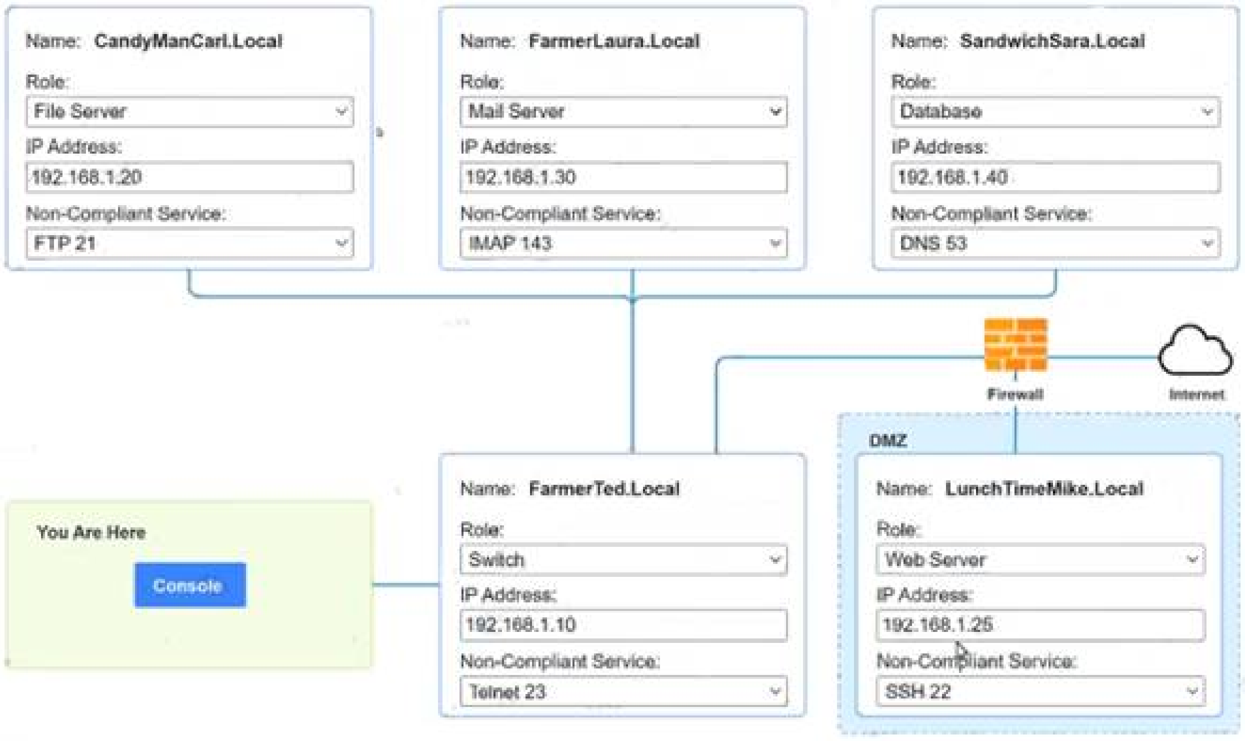




A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer below images



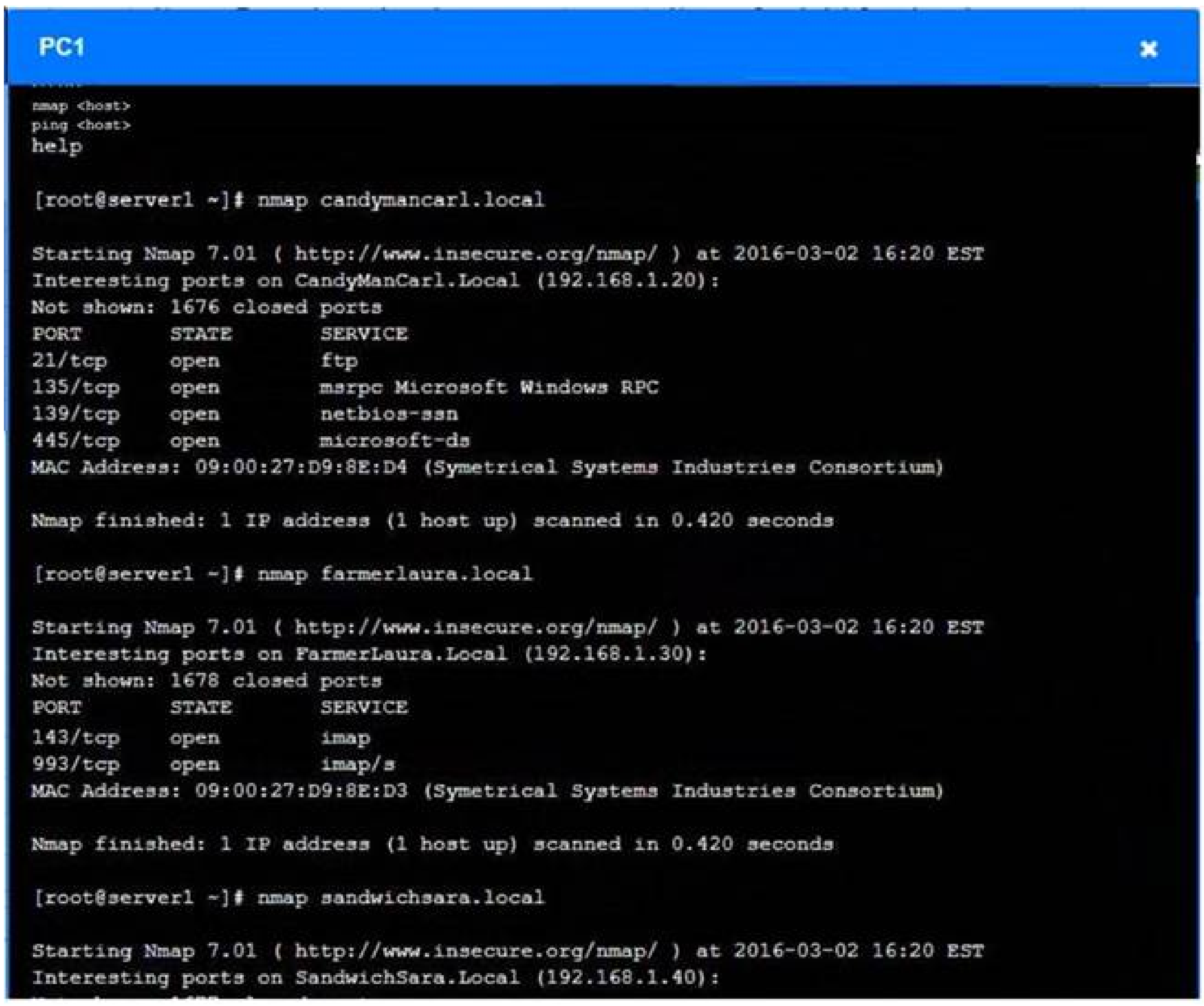
Name: CandyManCarl.Local
Role: File Server
IP Address: 192.168.1.20
Non-Compliant Service: FTP 21

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

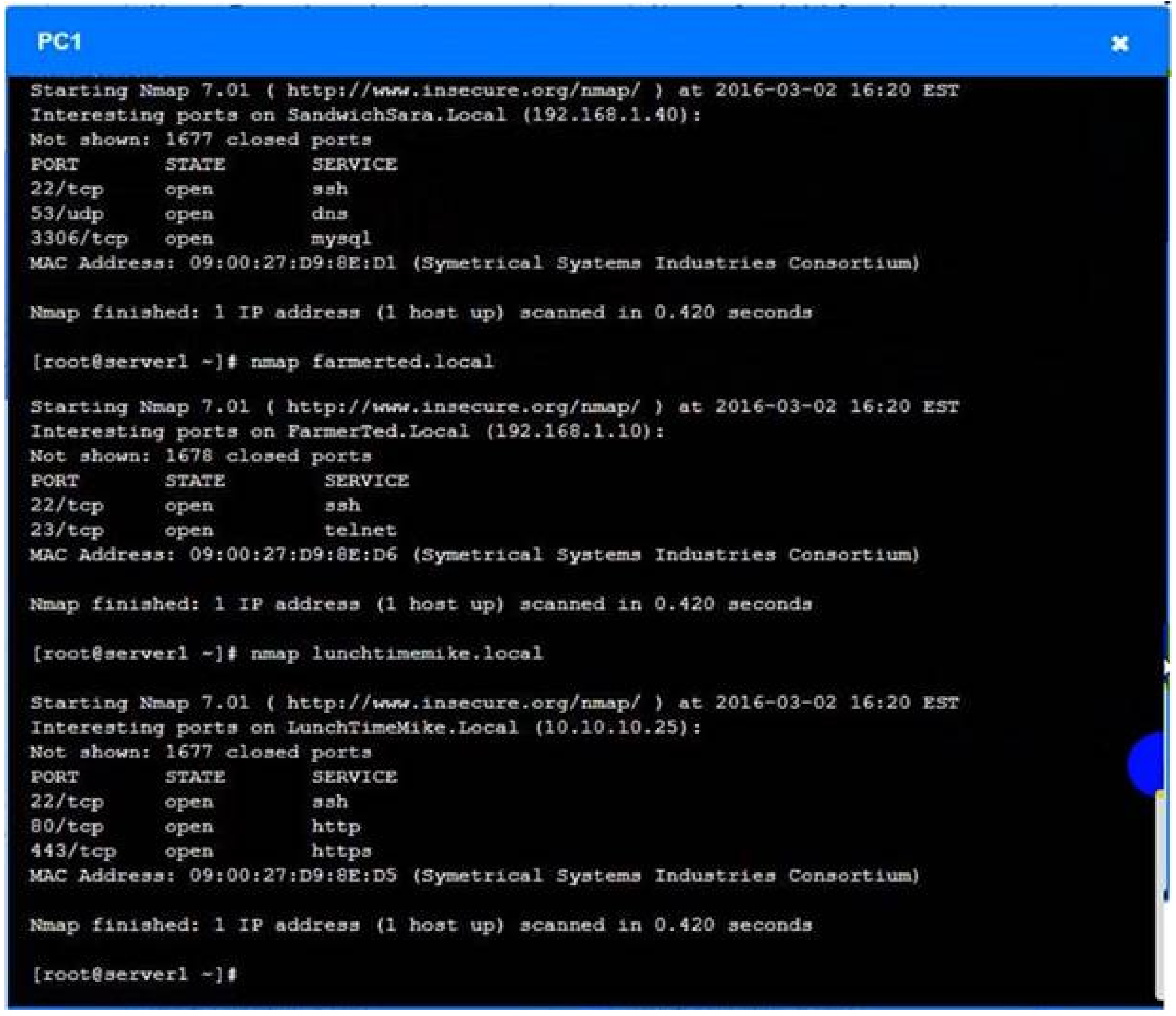
Name: FarmerTed.Local
Role: Switch
IP Address: 192.168.1.10
Non-Compliant Service: Telnet 23

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):
```

A computer screen with white text Description automatically generated



```
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 ~]#
```

NEW QUESTION 62
Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

A. SLA
B. MOU
C. Best-effort patching
D. Organizational governance

Answer: A

Explanation:
An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of

the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer12
An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.
Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.
Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

NEW QUESTION 67
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

Answer: C

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.

NEW QUESTION 68
Which of the following best describes the key elements of a successful information security program?

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

Answer: B

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

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

NEW QUESTION 72
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

Answer: A

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

NEW QUESTION 75
An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP

address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

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

Answer: A

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

NEW QUESTION 78
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.

Answer: D

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.

NEW QUESTION 80
Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

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

Answer: A

Explanation:
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.

NEW QUESTION 85
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

Answer: D

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.

NEW QUESTION 89
When starting an investigation, which of the following must be done first?

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

Answer: B

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

NEW QUESTION 91
A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

A. Increasing training and awareness for all staff
B. Ensuring that malicious websites cannot be visited
C. Blocking all scripts downloaded from the internet
D. Disabling all staff members' ability to run downloaded applications

Answer: A

Explanation:
Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:
- Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
- Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
- Reporting any suspicious or anomalous activity to the security team or the appropriate authority
- Following the organization’s policies and procedures on security awareness and best practices

Official References:
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION 95
A security analyst must preserve a system hard drive that was involved in a litigation request Which of the following is the best method to ensure the data on the device is not modified?

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

Answer: A

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

NEW QUESTION 100
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

Answer: C

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.

NEW QUESTION 103

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.

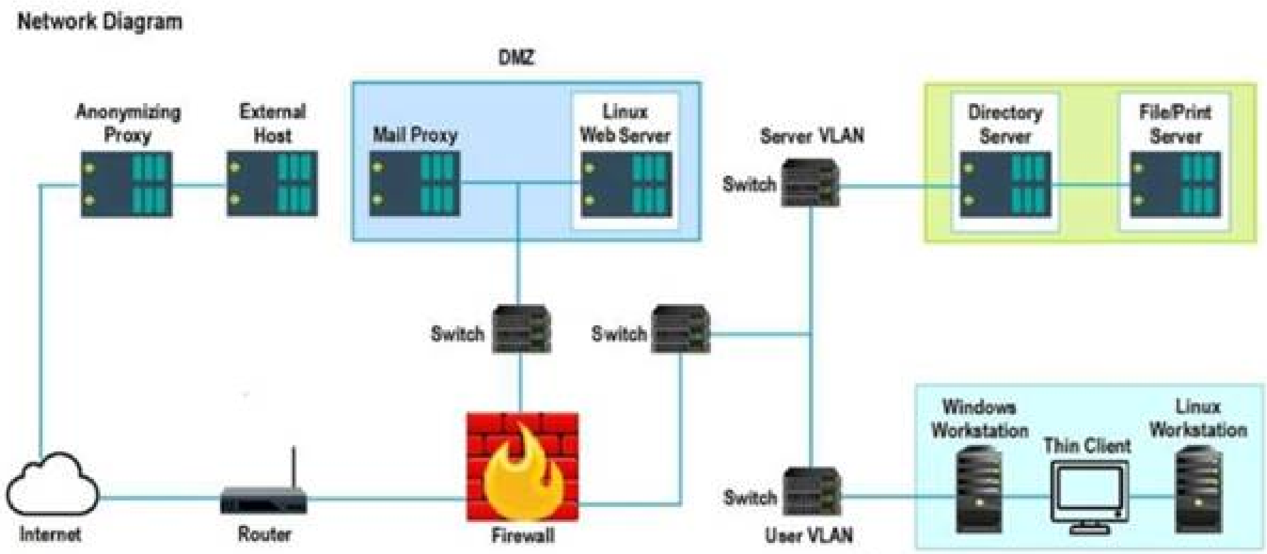
Instructions:

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.

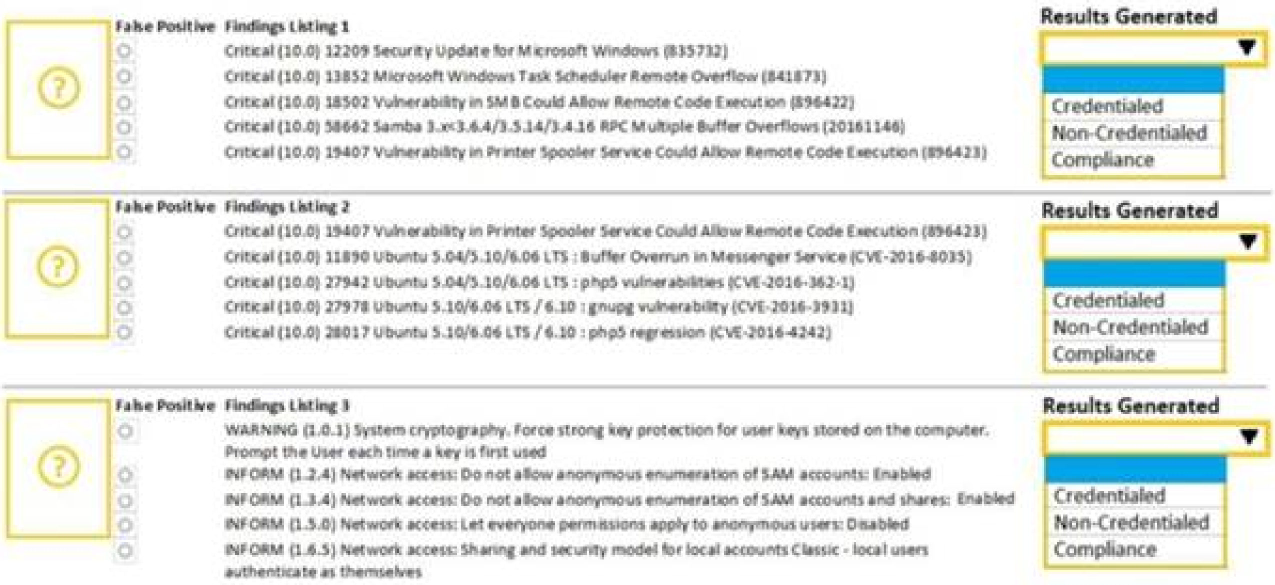
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

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.



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

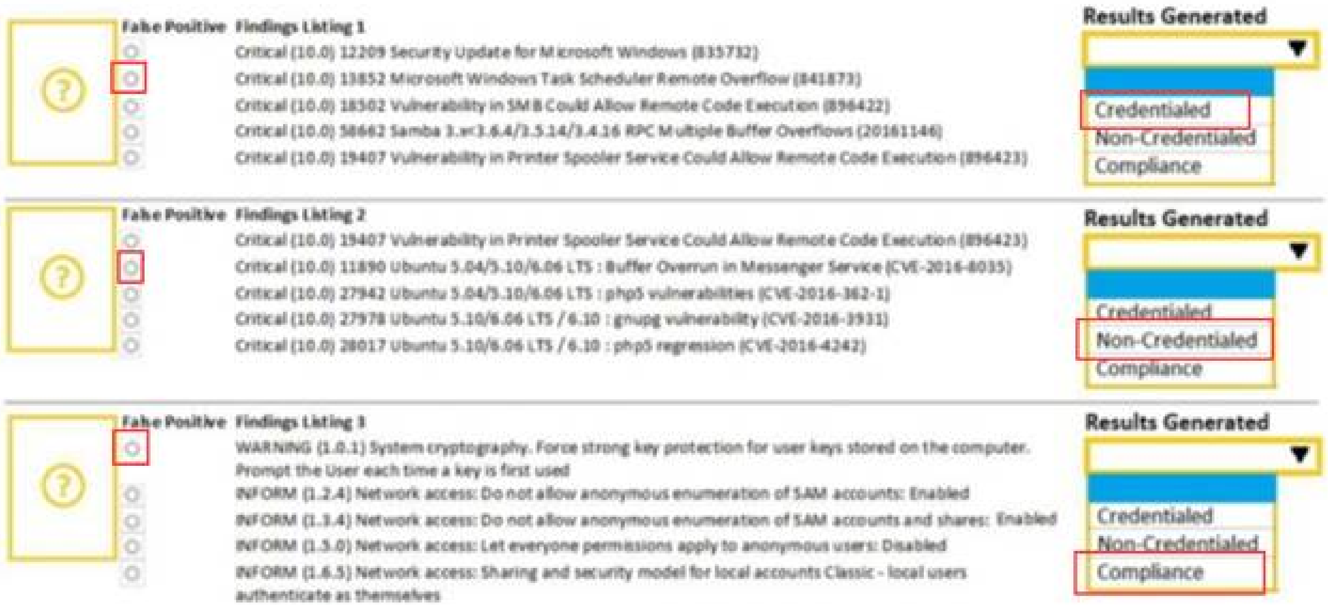
Results Generated: Credentialed / Non-Credentialed / Compliance

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

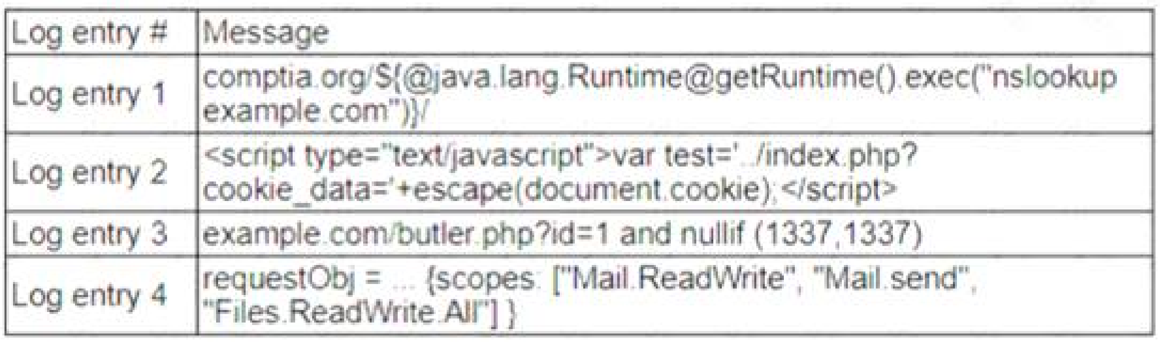
False Positive | Findings Listing 3

[✓ ○] 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]

NEW QUESTION 105

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:



Log entry #	Message
Log entry 1	comptia.org/${@java.lang.Runtime@getRuntime().exec("nslookup example.com")}/
Log entry 2	<script type="text/javascript">var test='../index.php?cookie_data='+escape(document.cookie);</script>
Log entry 3	example.com/butler.php?id=1 and nullif (1337,1337)
Log entry 4	requestObj = ... {scopes: ["Mail.ReadWrite", "Mail.send", "Files.ReadWrite.All"] }

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

Answer: D

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/passwd file, which contains user account information, an 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 References:

- https://www.imperva.com/learn/application-security/command-injection/
- https://www.zerodayinitiative.com/advisories/published/

NEW QUESTION 108
A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

A. Create a timeline of events detailinq the date stamps, user account hostname and IP information associated with the activities
B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identity the case as an HR-related investigation
D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Answer: B

Explanation:
The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

NEW QUESTION 110
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

Answer: B

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.

NEW QUESTION 112
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

Answer: C

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 References: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

NEW QUESTION 113
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

Answer: D

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.

NEW QUESTION 115
An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

A. Passive network foot printing
B. OS fingerprinting
C. Service port identification
D. Application versioning

Answer: A

Explanation:
Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts. OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

NEW QUESTION 119
A company is in the process of implementing a vulnerability management program. no-lich of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

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

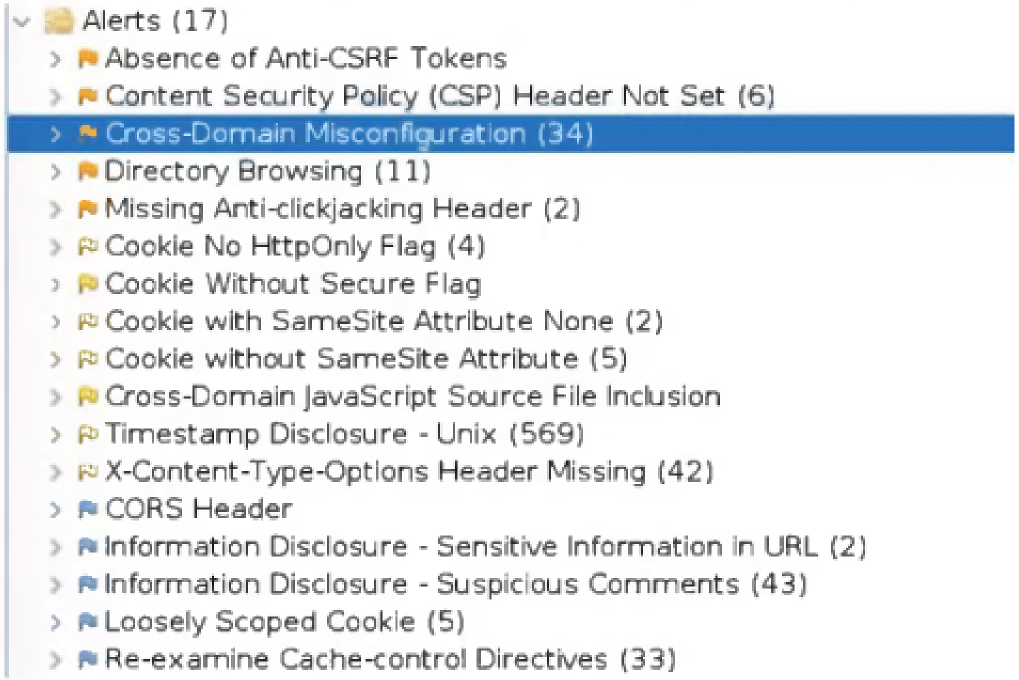
Answer: B

Explanation:
Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

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

NEW QUESTION 121

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.

Answer: C

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-Allow-Origin 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.

NEW QUESTION 125

Which of the following describes the best reason for conducting a root cause analysis?

A. The root cause analysis ensures that proper timelines were documented.
B. The root cause analysis allows the incident to be properly documented for reporting.
C. The root cause analysis develops recommendations to improve the process.
D. The root cause analysis identifies the contributing items that facilitated the event

Answer: D

Explanation:

The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting and reporting incidents can help to communicate and share information about problems and solutions, but it does not necessarily identify or address the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

NEW QUESTION 128

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

A. Develop a call tree to inform impacted users
B. Schedule a review with all teams to discuss what occurred
C. Create an executive summary to update company leadership
D. Review regulatory compliance with public relations for official notification

Answer: B

Explanation:

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The

purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References:
https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

NEW QUESTION 129
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

Answer: C

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 modeling 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.

NEW QUESTION 130
An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

A. Access rights
B. Network segmentation
C. Time synchronization
D. Invalid playbook

Answer: C

Explanation:
Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page 23

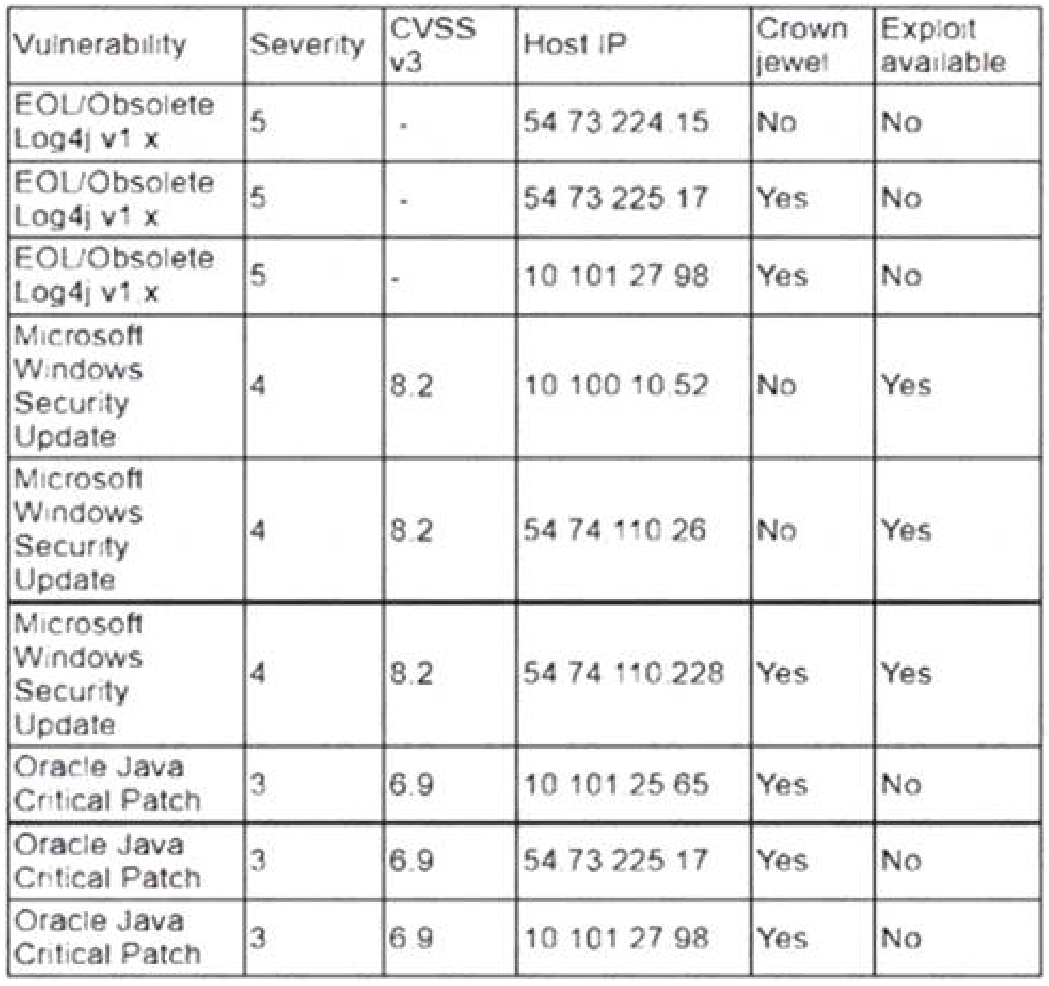
NEW QUESTION 131
A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to
reduce risks associated with the application development?

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

Answer: D

Explanation:
Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application. Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities. OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.
References: OWASP Logging Cheat Sheet, OWASP Logging Guide, C9: Implement Security Logging and Monitoring - OWASP Foundation

NEW QUESTION 133
An analyst is reviewing a vulnerability report for a server environment with the following entries:



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

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

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

Answer: D

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

NEW QUESTION 137
An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

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

Answer: A

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

NEW QUESTION 142
Which of the following best describes the goal of a tabletop exercise?

A. To test possible incident scenarios and how to react properly
B. To perform attack exercises to check response effectiveness
C. To understand existing threat actors and how to replicate their techniques
D. To check the effectiveness of the business continuity plan

Answer: A

Explanation:
A tabletop exercise is a type of simulation exercise that involves testing possible incident scenarios and how to react properly, without actually performing any actions or using any resources. A tabletop exercise is usually conducted by a facilitator who presents a realistic scenario to a group of participants, such as a cyberattack, a natural disaster, or a data breach. The participants then discuss and evaluate their roles, responsibilities, plans, procedures, and policies for responding to the incident, as well as the potential impacts and outcomes. A tabletop exercise can help identify strengths and weaknesses in the incident response plan, improve communication and coordination among the stakeholders, raise awareness and preparedness for potential incidents, and provide feedback and recommendations for improvement.

NEW QUESTION 144
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

Answer: A

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.

NEW QUESTION 146
A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

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

Answer: D

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

> https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
> https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
> https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers

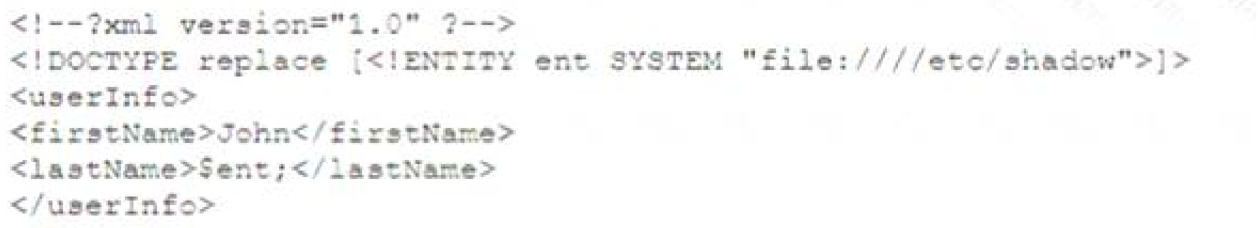
NEW QUESTION 150
A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is
taking place?

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

Answer: D

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

NEW QUESTION 155
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

Answer: B

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 References:

- https://portswigger.net/web-security/xxe
- https://portswigger.net/web-security/ssrf
- https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.ht

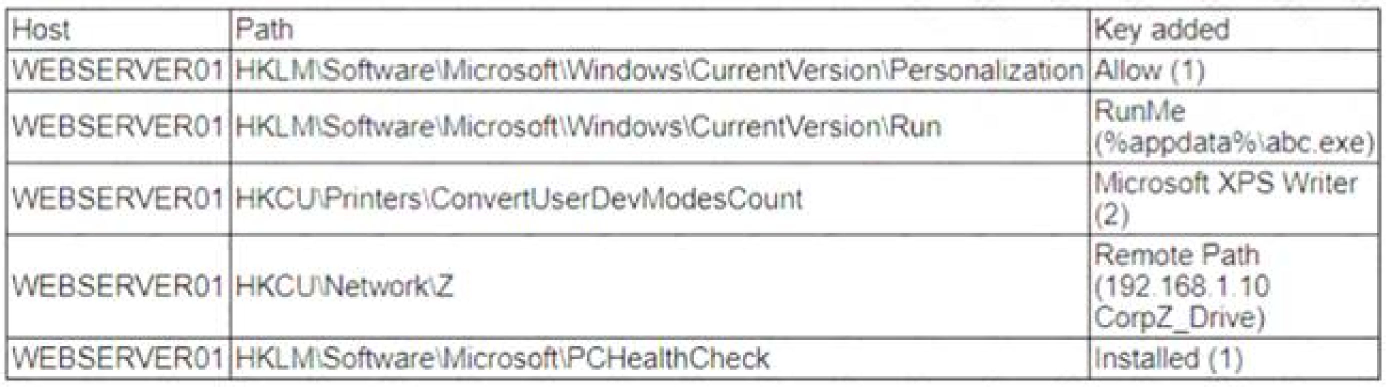
NEW QUESTION 158
Which of the following is a reason why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

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

Answer: A

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 lessons-learned 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.

NEW QUESTION 160
A security analyst is reviewing the following alert that was triggered by FIM on a critical system:



Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?

A. A fake antivirus program was installed by the user.
B. A network drive was added to allow exfiltration of data
C. A new program has been set to execute on system start
D. The host firewall on 192.168.1.10 was disabled.

Answer: C

Explanation:
A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official References:

- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/training/books/cysa-cs0-002-study-guide

NEW QUESTION 164
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

Answer: B

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.

NEW QUESTION 166
A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

A. Testing
B. Implementation
C. Validation
D. Rollback

Answer: C

Explanation:
The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

NEW QUESTION 168
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

Answer: A

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.

NEW QUESTION 171
An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

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

Answer: A

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

NEW QUESTION 175
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

Answer: A

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.
References: CompTIA CySA+ Certification Exam Objectives, [What Is Multifactor Authentication (MFA)?]

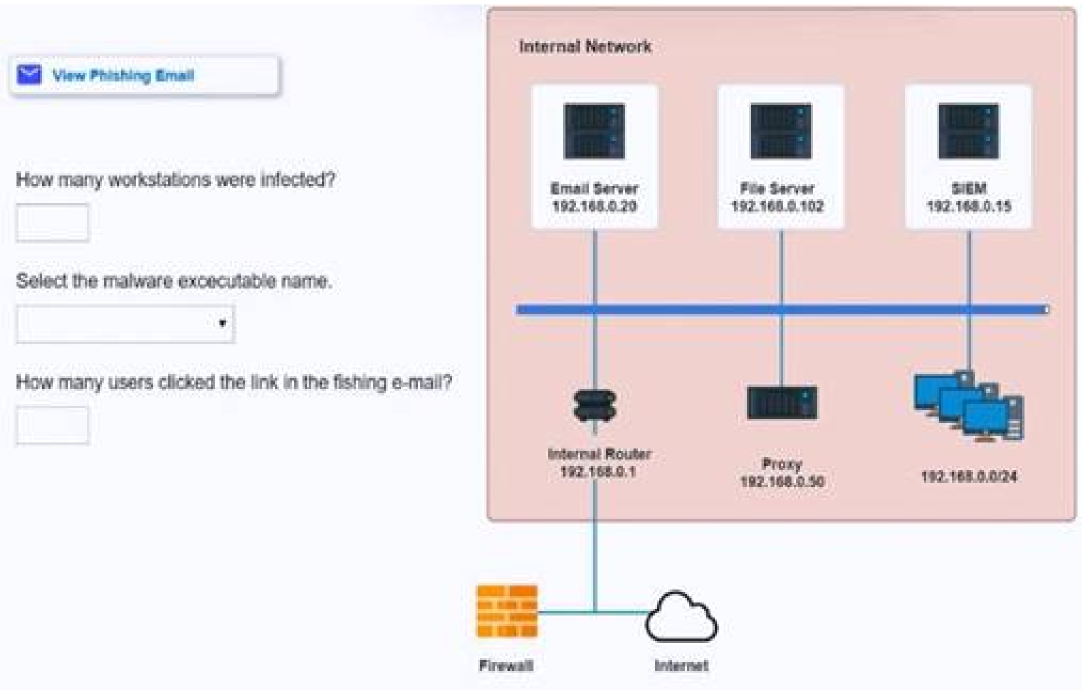
NEW QUESTION 179
A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

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

Answer: A

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.

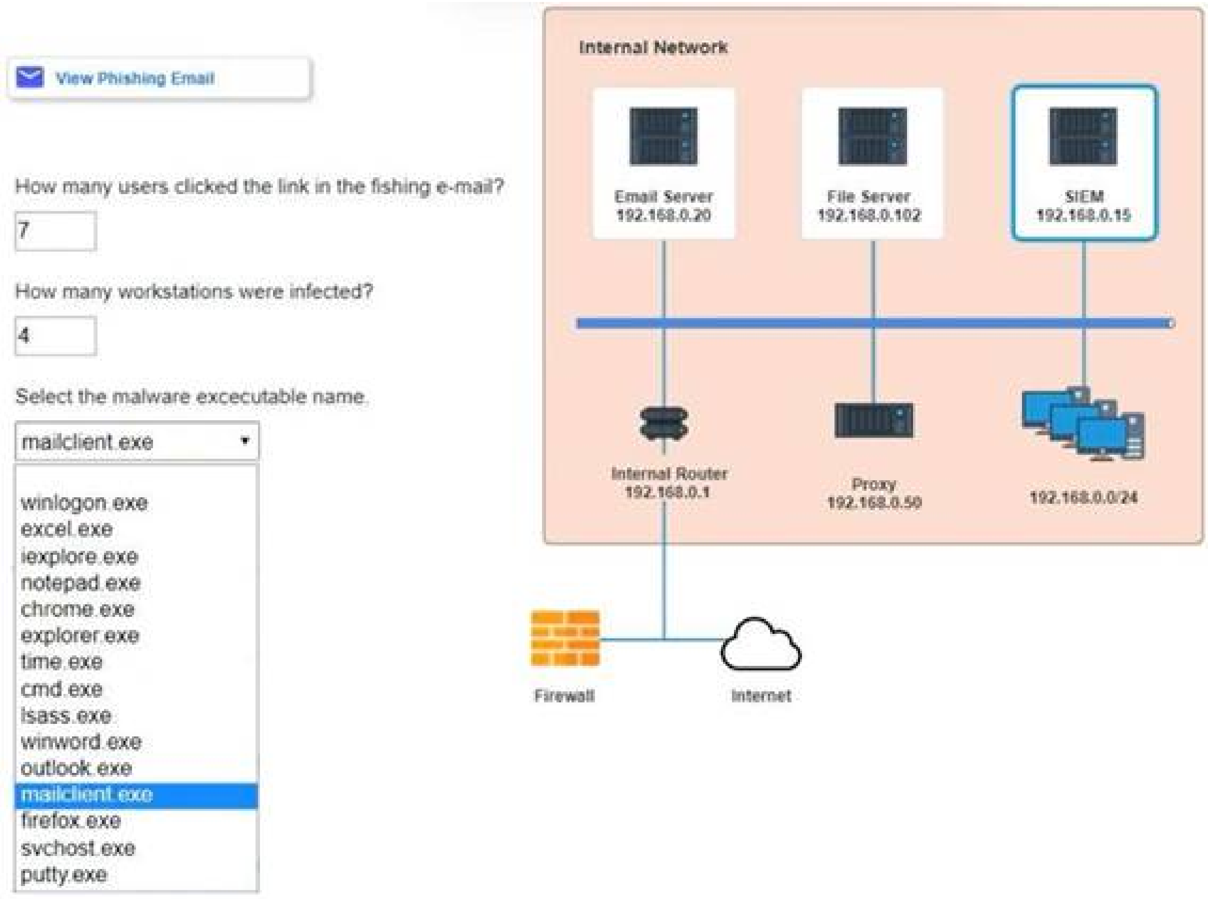
NEW QUESTION 183
Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.
Review the information provided and determine the following:
* 1. HOW many employees Clicked on the link in the Phishing email?
* 2. on how many workstations was the malware installed?
* 3. what is the executable file name of the malware?



How many workstations were infected?

Select the malware excecutable name.

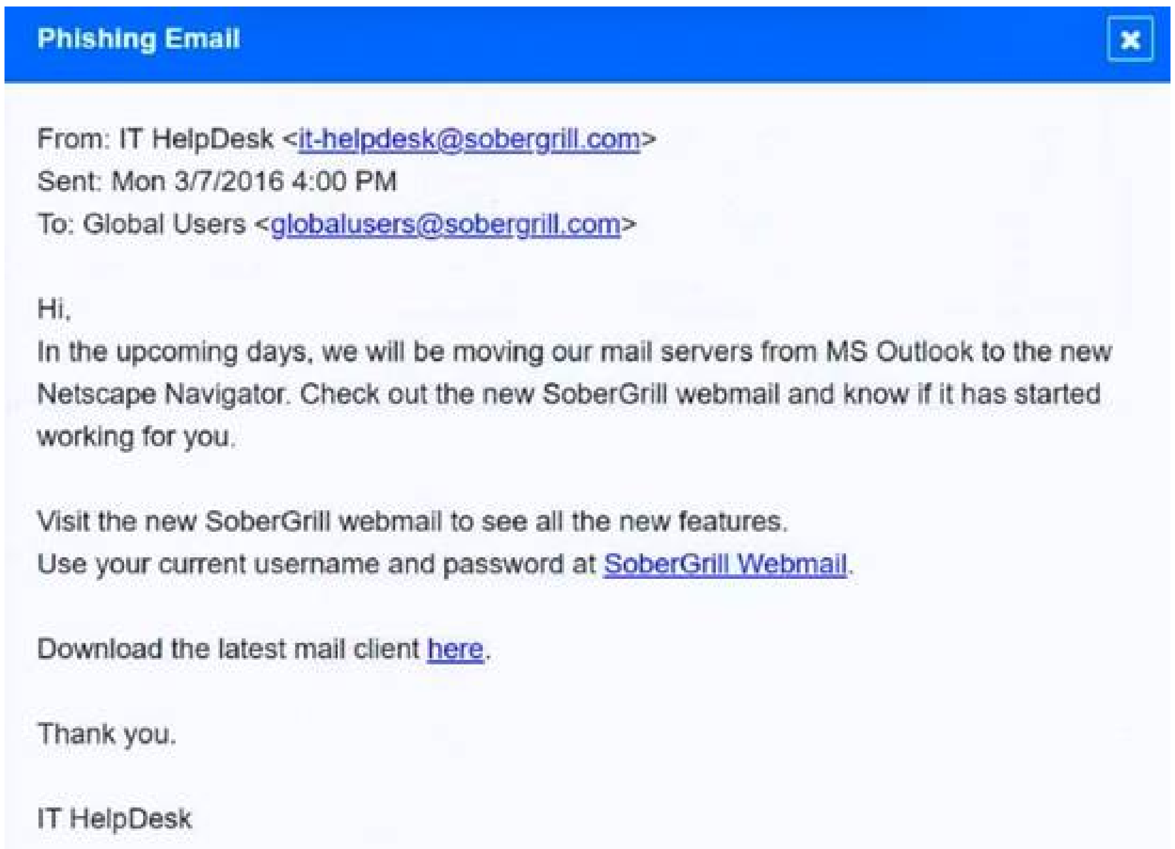
How many users clicked the link in the fishing e-mail?



How many users clicked the link in the fishing e-mail?
7

How many workstations were infected?
4

Select the malware excecutable name.
mailclient.exe



From: IT HelpDesk <it-helpdesk@sobergrill.com>
Sent: Mon 3/7/2016 4:00 PM
To: Global Users <globalusers@sobergrill.com>

Hi,

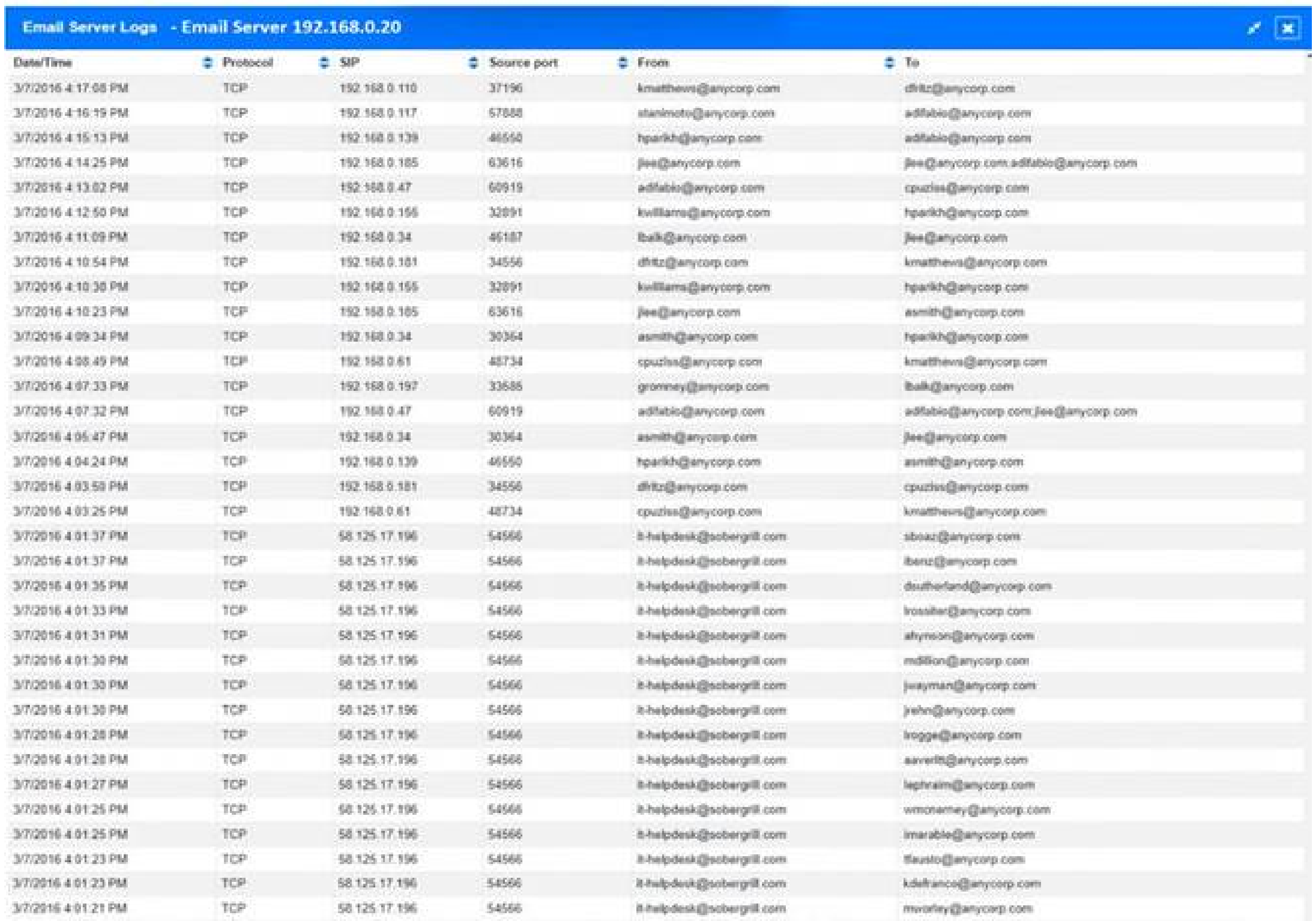
In the upcoming days, we will be moving our mail servers from MS Outlook to the new Netscape Navigator. Check out the new SoberGrill webmail and know if it has started working for you.

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

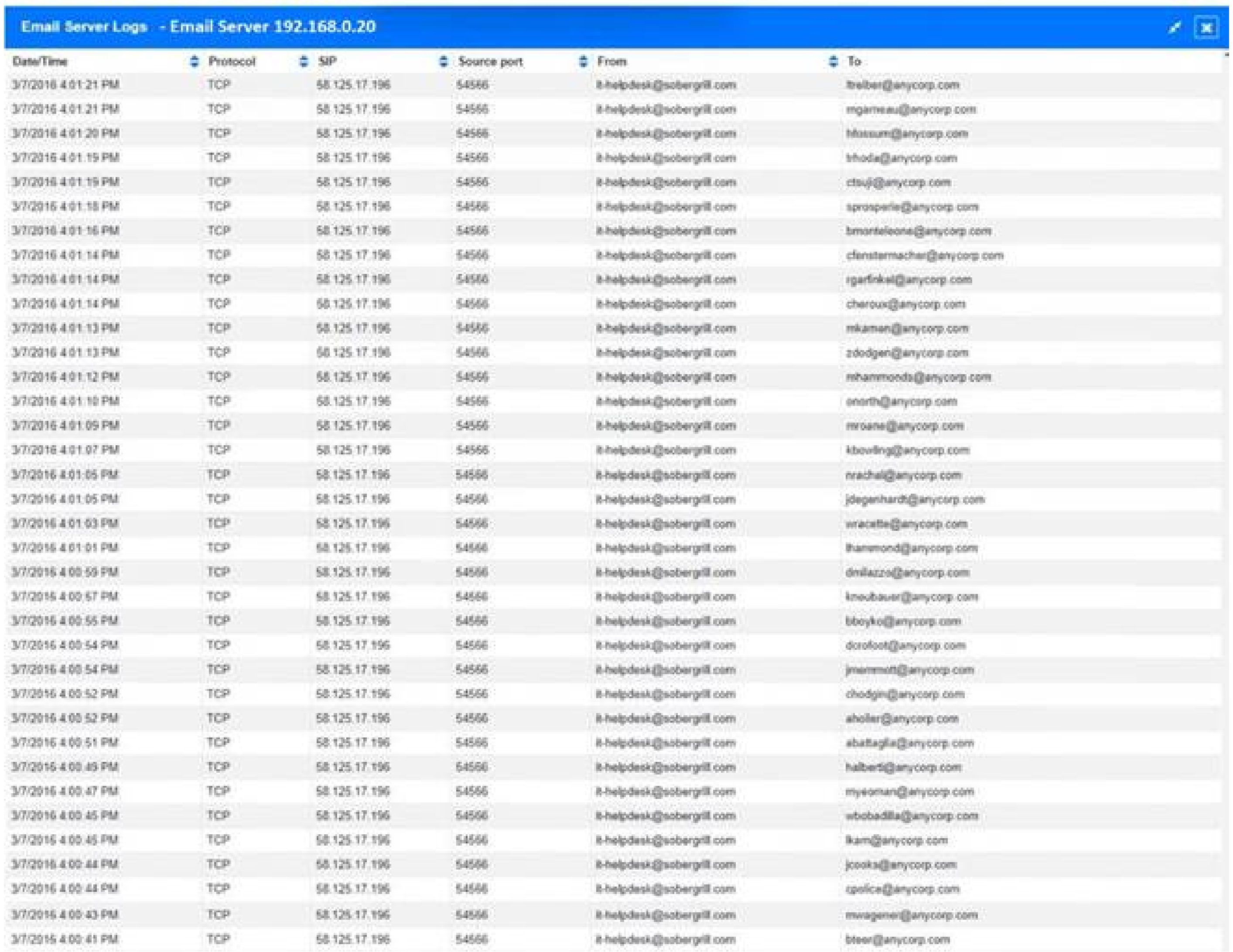
Download the latest mail client here.

Thank you.

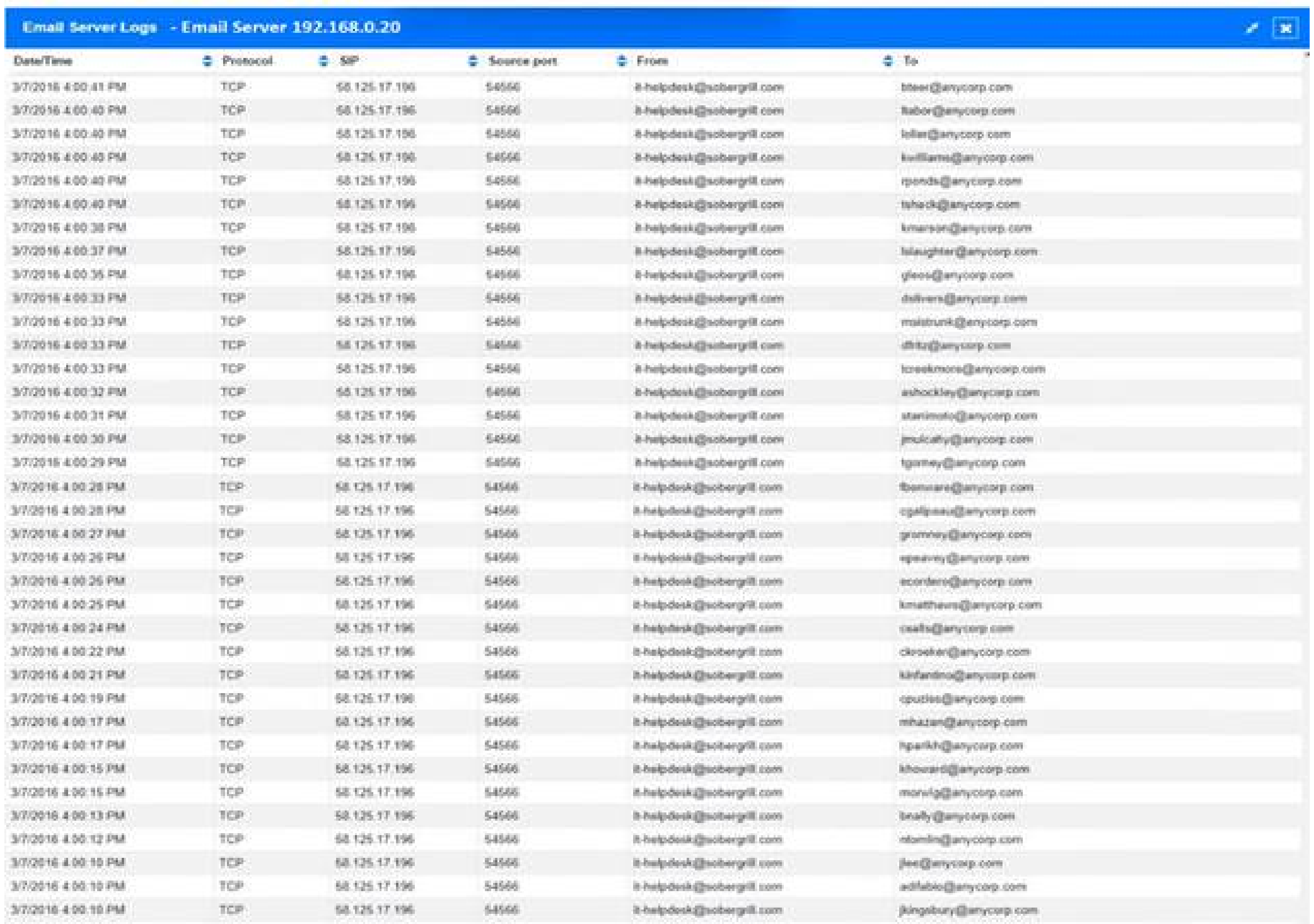
IT HelpDesk



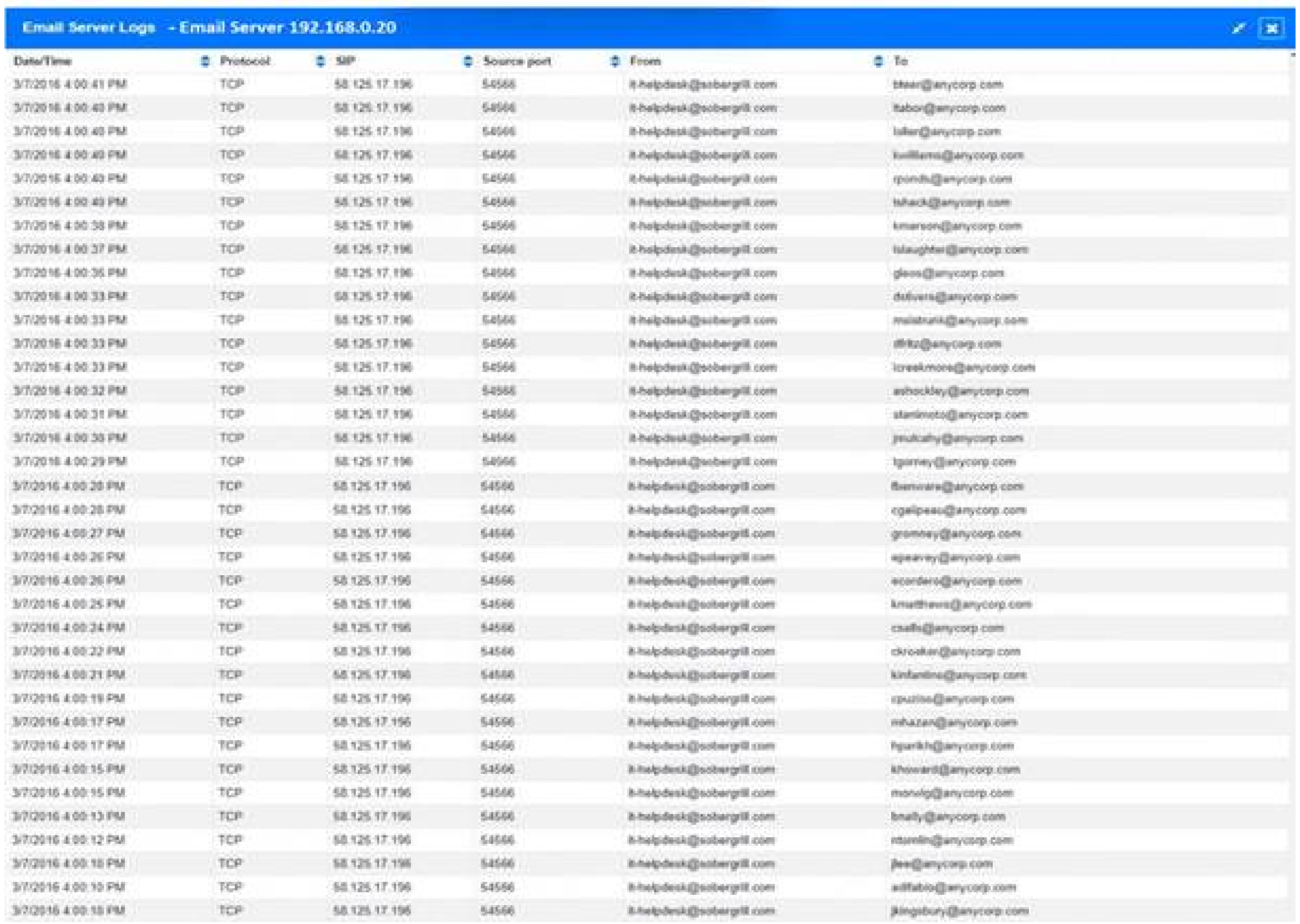
Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	67888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 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	192.168.0.156	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	33686	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 4:06:47 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
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lbenz@anycorp.com
3/7/2016 4:01:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsutherland@anycorp.com
3/7/2016 4:01:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrossiter@anycorp.com
3/7/2016 4:01:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ahymson@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mdillion@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jwayman@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jrehn@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrogge@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aaverill@anycorp.com
3/7/2016 4:01:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lephraim@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wmcnerney@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	imarable@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfausto@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kdefranco@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mvorley@anycorp.com



Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltreiber@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mgarneau@anycorp.com
3/7/2016 4:01:20 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hfossum@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	trhoda@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ctsuji@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com
3/7/2016 4:01:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bmonteleone@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cfenstermacher@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgarfinkel@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cheroux@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mkaman@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	zdodgen@anycorp.com
3/7/2016 4:01:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhammonds@anycorp.com
3/7/2016 4:01:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	onorth@anycorp.com
3/7/2016 4:01:09 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mroane@anycorp.com
3/7/2016 4:01:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kbowling@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nrachal@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jdegenhardt@anycorp.com
3/7/2016 4:01:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wracette@anycorp.com
3/7/2016 4:01:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lhammond@anycorp.com
3/7/2016 4:00:59 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dmilazzo@anycorp.com
3/7/2016 4:00:57 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kneubauer@anycorp.com
3/7/2016 4:00:55 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bboyko@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dcrofoot@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmemmott@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	chodgin@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aholler@anycorp.com
3/7/2016 4:00:51 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	abattaglia@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	halberti@anycorp.com
3/7/2016 4:00:47 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	myeoman@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wbobadilla@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lkam@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jcooks@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpolice@anycorp.com
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mwagener@anycorp.com
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com

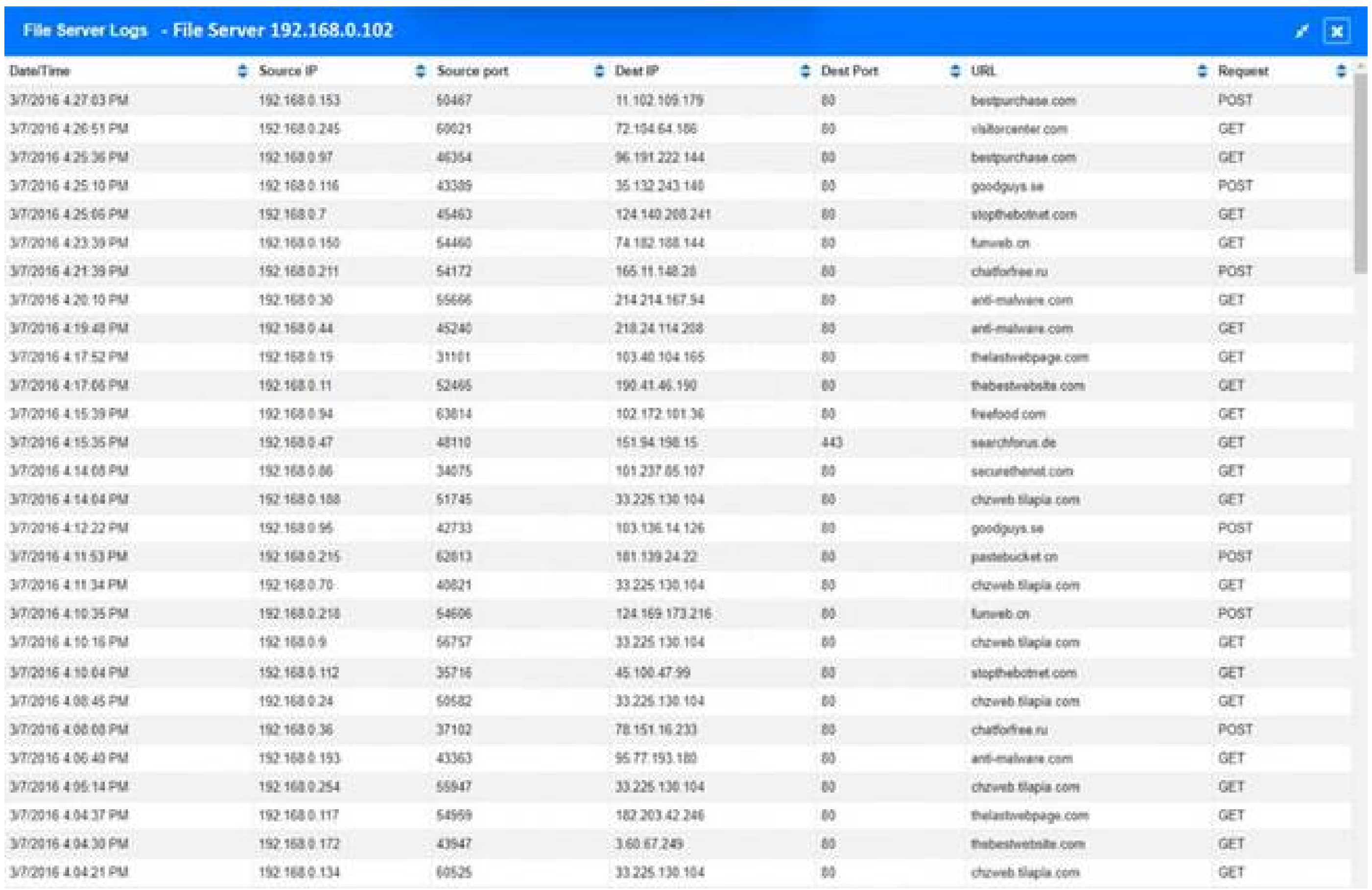


Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltabor@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	loller@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kwilliams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rponds@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tshack@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmarson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dolivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mslstrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgorney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbenvare@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgalipeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmatthews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckroeker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuzios@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	morvig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingsbury@anycorp.com



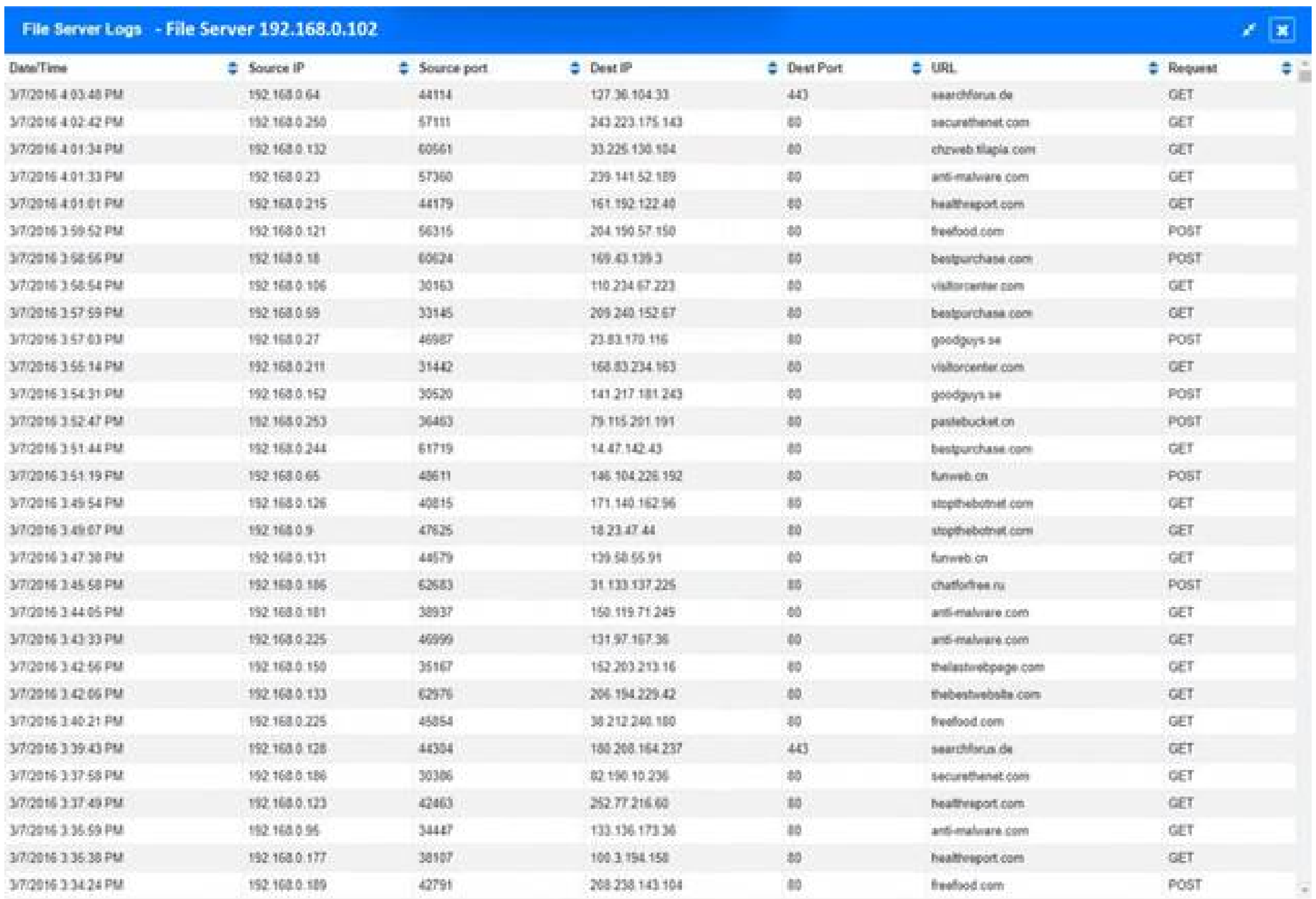
Email Server Logs - Email Server 192.168.0.20

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bleer@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltabor@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lolier@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kwilliams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rponds@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lshack@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmerson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com
3/7/2016 4:00:36 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsilvers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	msistrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgorney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbenware@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgalipeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmatthews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckrooker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuzios@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	morwig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mtomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingsbury@anycorp.com



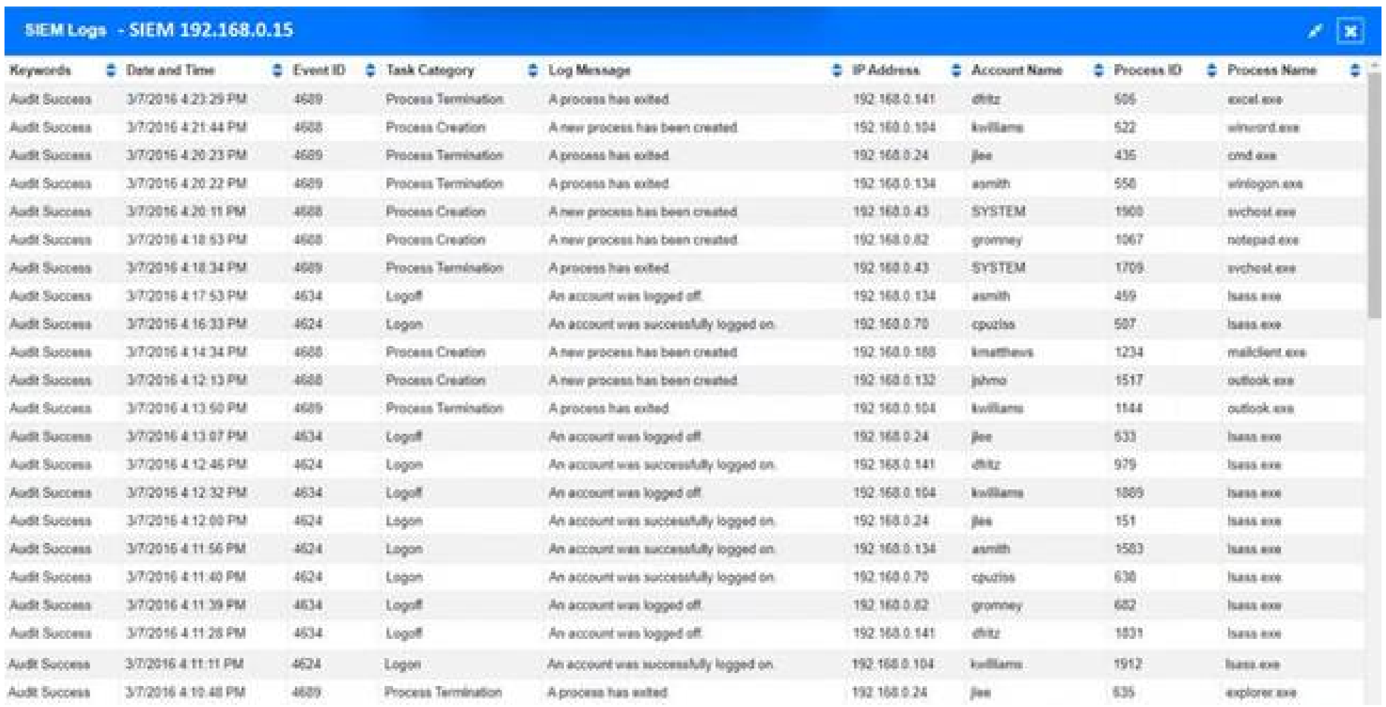
File Server Logs - File Server 192.168.0.102

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	74.182.108.144	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	192.168.0.96	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
3/7/2016 4:10:16 PM	192.168.0.9	56757	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:04 PM	192.168.0.112	35716	45.100.47.99	80	stopthebotnet.com	GET
3/7/2016 4:08:45 PM	192.168.0.24	50582	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:08:08 PM	192.168.0.36	37102	78.151.16.233	80	chatforfree.ru	POST
3/7/2016 4:06:40 PM	192.168.0.193	43363	95.77.193.180	80	anti-malware.com	GET
3/7/2016 4:05:14 PM	192.168.0.254	55947	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tilapia.com	GET



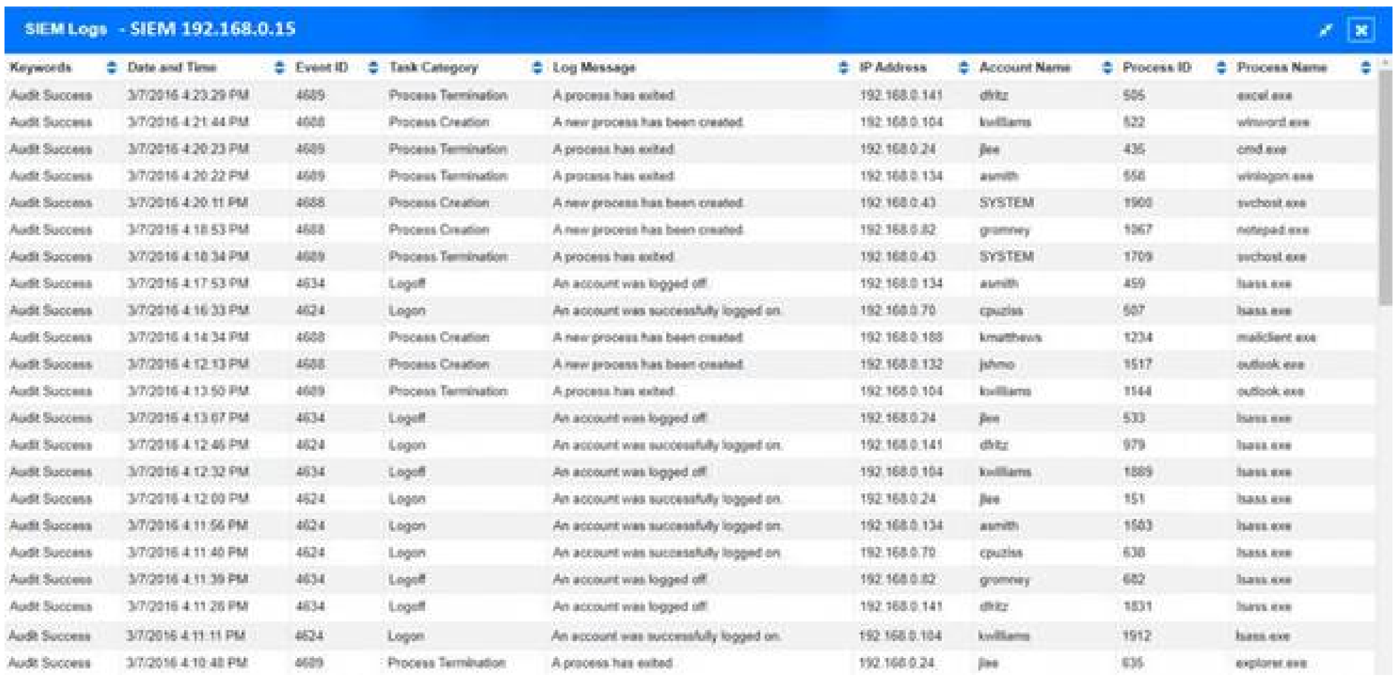
File Server Logs - File Server 192.168.0.102

Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:03:48 PM	192.168.0.64	44114	127.36.104.33	443	searchforus.de	GET
3/7/2016 4:02:42 PM	192.168.0.250	57111	243.223.175.143	80	securethenet.com	GET
3/7/2016 4:01:34 PM	192.168.0.132	60561	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:01:33 PM	192.168.0.23	57360	239.141.52.189	80	anti-malware.com	GET
3/7/2016 4:01:01 PM	192.168.0.215	44179	161.192.122.40	80	healthreport.com	GET
3/7/2016 3:59:52 PM	192.168.0.121	56315	204.150.57.150	80	freefood.com	POST
3/7/2016 3:58:56 PM	192.168.0.18	60624	169.43.139.3	80	bestpurchase.com	POST
3/7/2016 3:58:54 PM	192.168.0.106	30163	110.234.67.223	80	visitorcenter.com	GET
3/7/2016 3:57:59 PM	192.168.0.59	33145	209.240.152.67	80	bestpurchase.com	GET
3/7/2016 3:57:03 PM	192.168.0.27	46987	23.83.170.116	80	goodguys.se	POST
3/7/2016 3:55:14 PM	192.168.0.211	31442	168.83.234.163	80	visitorcenter.com	GET
3/7/2016 3:54:31 PM	192.168.0.152	30520	141.217.181.243	80	goodguys.se	POST
3/7/2016 3:52:47 PM	192.168.0.253	36463	79.115.201.191	80	pastebucket.cn	POST
3/7/2016 3:51:44 PM	192.168.0.244	61719	14.47.142.43	80	bestpurchase.com	GET
3/7/2016 3:51:19 PM	192.168.0.65	48611	146.104.226.192	80	funweb.cn	POST
3/7/2016 3:49:54 PM	192.168.0.126	40815	171.140.162.96	80	stopthebotnet.com	GET
3/7/2016 3:49:07 PM	192.168.0.9	47625	18.23.47.44	80	stopthebotnet.com	GET
3/7/2016 3:47:38 PM	192.168.0.131	44579	139.58.55.91	80	funweb.cn	GET
3/7/2016 3:45:58 PM	192.168.0.186	62683	31.133.137.225	80	chatforfree.ru	POST
3/7/2016 3:44:05 PM	192.168.0.181	38937	150.119.71.245	80	anti-malware.com	GET
3/7/2016 3:43:33 PM	192.168.0.225	46999	131.97.167.36	80	anti-malware.com	GET
3/7/2016 3:42:56 PM	192.168.0.150	35167	152.203.213.16	80	thelastwebpage.com	GET
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET
3/7/2016 3:39:43 PM	192.168.0.128	44304	180.208.164.237	443	searchforus.de	GET
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET
3/7/2016 3:36:59 PM	192.168.0.95	34447	133.136.173.36	80	anti-malware.com	GET
3/7/2016 3:36:38 PM	192.168.0.177	38107	100.3.194.158	80	healthreport.com	GET
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.238.143.104	80	freefood.com	POST



SIEM Logs - SIEM 192.168.0.15

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	cpuzlss	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	cpuzlss	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
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe



SIEM Logs - SIEM 192.168.0.15

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	cpuzlss	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	cpuzlss	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
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 187
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

Answer: C

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.

NEW QUESTION 189
......