# CompTIA

## Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

**NEW QUESTION 1**
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 2**
An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of- life date. Which of the following best describes a security analyst's concern?

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

**Answer:** A

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

**NEW QUESTION 3**
During the log analysis phase, the following suspicious command is detected

```
<?php preg_replace('/.*/e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

Which of the following is being attempted?

A. Buffer overflow
B. RCE
C. ICMP tunneling
D. Smurf attack

**Answer:** B

**Explanation:**
RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types & Vulnerabilities - Fortinet1, What Is a Smurf Attack? Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of …3

**NEW QUESTION 4**
A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network.
Which of the following metrics should the team lead include in the briefs?

A. Mean time between failures
B. Mean time to detect
C. Mean time to remediate
D. Mean time to contain

**Answer:** D

**Explanation:**
Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

**NEW QUESTION 5**
Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

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

**Answer:** A

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

**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**
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 8**
The security analyst received the monthly vulnerability report. The following findings were included in the report
• Five of the systems only required a reboot to finalize the patch application.
• Two of the servers are running outdated operating systems and cannot be patched
The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls
B. Due diligence
C. Maintenance windows
D. Passive discovery

**Answer:** A

**Explanation:**
Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

**NEW QUESTION 9**
Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?

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

**Answer:** A

**Explanation:**
A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and best practices. A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats12
The other options are not correct. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle unauthenticated messages34 SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks56 PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges. PAM can help prevent credential theft, data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to critical resources78

**NEW QUESTION 10**
Which of the following tools would work best to prevent the exposure of PII outside of an organization?

A. PAM
B. IDS
C. PKI
D. DLP

**Answer:** D

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

**NEW QUESTION 10**
Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

A. SLA
B. LOI
C. MOU
D. KPI

**Answer:** A

**Explanation:**
SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

**NEW QUESTION 15**
A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following
would be missing from a scan performed with this configuration?

A. Operating system version

B. Registry key values
C. Open ports
D. IP address

**Answer:** B

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

**NEW QUESTION 19**
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 20**
A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

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

**Answer:** C

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

**NEW QUESTION 25**
During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

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

**Answer:** D

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

**NEW QUESTION 28**
A security audit for unsecured network services was conducted, and the following output was generated:

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

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

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

A. 21
B. 22
C. 23
D. 636
E. 1723
F. 3389

**Answer:** CD

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

**NEW QUESTION 33**
Which of the following risk management principles is accomplished by purchasing cyber insurance?

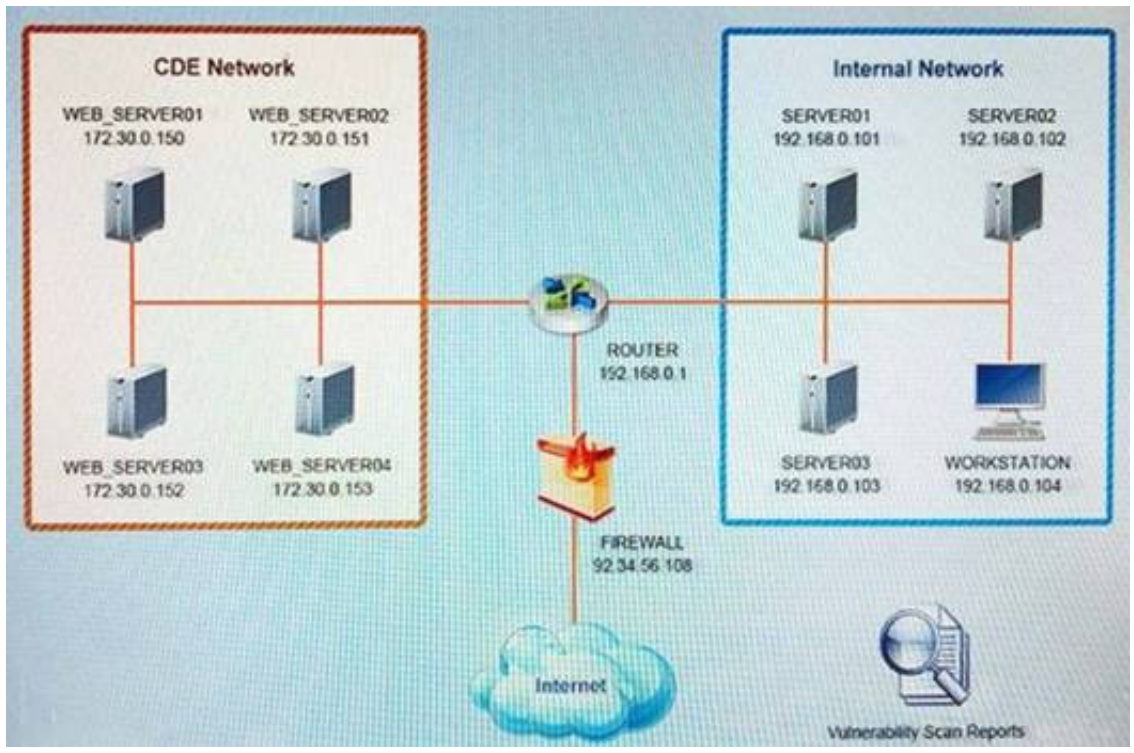
A. Accept
B. Avoid
C. Mitigate
D. Transfer

**Answer:** D

**Explanation:**
Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions. Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. 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 34**
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.




**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**

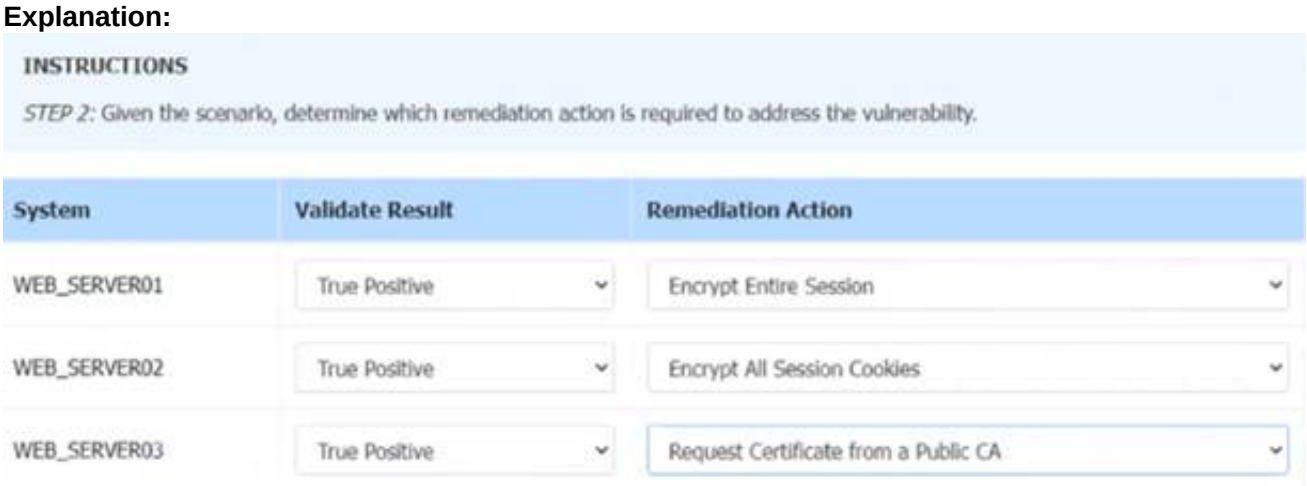
*STEP 2* Given the scenario, determine which remediation action is required to address the vulnerability

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

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 37**
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 41**
Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

A. Mean time to detect
B. Number of exploits by tactic
C. Alert volume
D. Quantity of intrusion attempts

**Answer:** A

**Explanation:**
Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs. MTTD can be improved by using tools and processes that can collect, correlate, analyze, and alert on security data from various sources. SIEM, SOAR, and ticketing systems are examples of such tools and processes that can help reduce MTTD and enhance security operations. Official References:
https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack

**NEW QUESTION 45**
A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

A. The current scanners should be migrated to the cloud
B. Cloud-specific misconfigurations may not be detected by the current scanners
C. Existing vulnerability scanners cannot scan IaaS systems
D. Vulnerability scans on cloud environments should be performed from the cloud

**Answer:** B

**Explanation:**
Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases,

virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs.
Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

**NEW QUESTION 47**
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 49**
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 50**
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
host03 CVE-2007-99996:
       (NarrowStairs)             RCE:AEX:HVT
host04 CVE-2009-99998:
       (Topendoor)                UDD:NOA

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

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

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

**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 52**
An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

A. PCI Security Standards Council
B. Local law enforcement
C. Federal law enforcement
D. Card issuer

**Answer:** D

**Explanation:**
Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach. The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official References: https://www.pcisecuritystandards.org/

**NEW QUESTION 55**
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 59**
Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

A. MITRE ATTACK
B. Cyber Kill Cham
C. OWASP
D. STIXTAXII

**Answer:** A

**Explanation:**
MITRE ATT&CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT&CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT&CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

**NEW QUESTION 62**
After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

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

**Answer:** A

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

**NEW QUESTION 64**
An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?

A. Beaconing
B. Cross-site scripting
C. Buffer overflow
D. PHP traversal

**Answer:** A

**NEW QUESTION 66**
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 68**
While reviewing web server logs, an analyst notices several entries with the same time stamps, but all contain odd characters in the request line. Which of the following steps should be taken next?

A. Shut the network down immediately and call the next person in the chain of command.
B. Determine what attack the odd characters are indicative of
C. Utilize the correct attack framework and determine what the incident response will consist of.
D. Notify the local law enforcement for incident response

**Answer:** B

**Explanation:**
Determining what attack the odd characters are indicative of is the next step that should be taken after reviewing web server logs and noticing several entries with the same time stamps, but all contain odd characters in the request line. This step can help the analyst identify the type and severity of the attack, as well as the possible source and motive of the attacker. The odd characters in the request line may indicate that the attacker is trying to exploit a vulnerability or inject malicious code into the web server or application, such as SQL injection, cross-site scripting, buffer overflow, or command injection. The analyst can use tools and techniques such as log analysis, pattern matching, signature detection, or threat intelligence to determine what attack the odd characters are indicative of, and then proceed to the next steps of incident response, such as containment, eradication, recovery, and lessons learned. 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 71**
An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

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

**Answer:** D

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

**NEW QUESTION 74**
Which of the following is the first step that should be performed when establishing a disaster recovery plan?

A. Agree on the goals and objectives of the plan
B. Determine the site to be used during a disasterC Demonstrate adherence to a standard disaster recovery process

C. Identity applications to be run during a disaster

**Answer:** A

**Explanation:**
The first step that should be performed when establishing a disaster recovery plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve, such as minimizing downtime, restoring critical functions, ensuring data integrity, or meeting compliance requirements. The goals and objectives of the plan should also be aligned with the business needs and priorities of the organization and be measurable and achievable.

**NEW QUESTION 77**
While performing a dynamic analysis of a malicious file, a security analyst notices the memory address changes every time the process runs. Which of the following controls is most likely preventing the analyst from finding the proper memory address of the piece of malicious code?

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

**Answer:** A

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

**NEW QUESTION 79**
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?

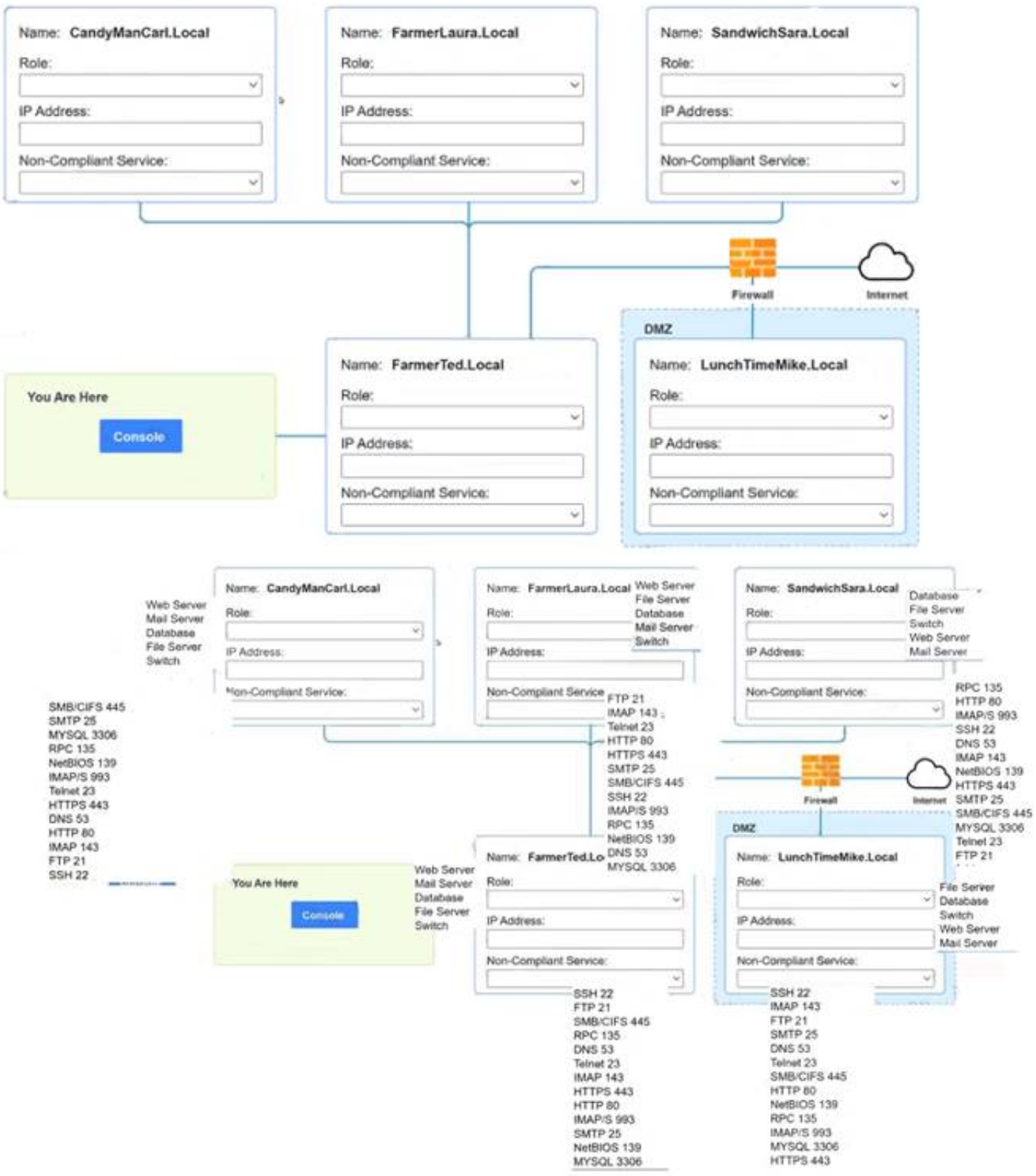
A. Clone the virtual server for forensic analysis
B. Log in to the affected server and begin analysis of the logs
C. Restore from the last known-good backup to confirm there was no loss of connectivity
D. Shut down the affected server immediately

**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 83**
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.

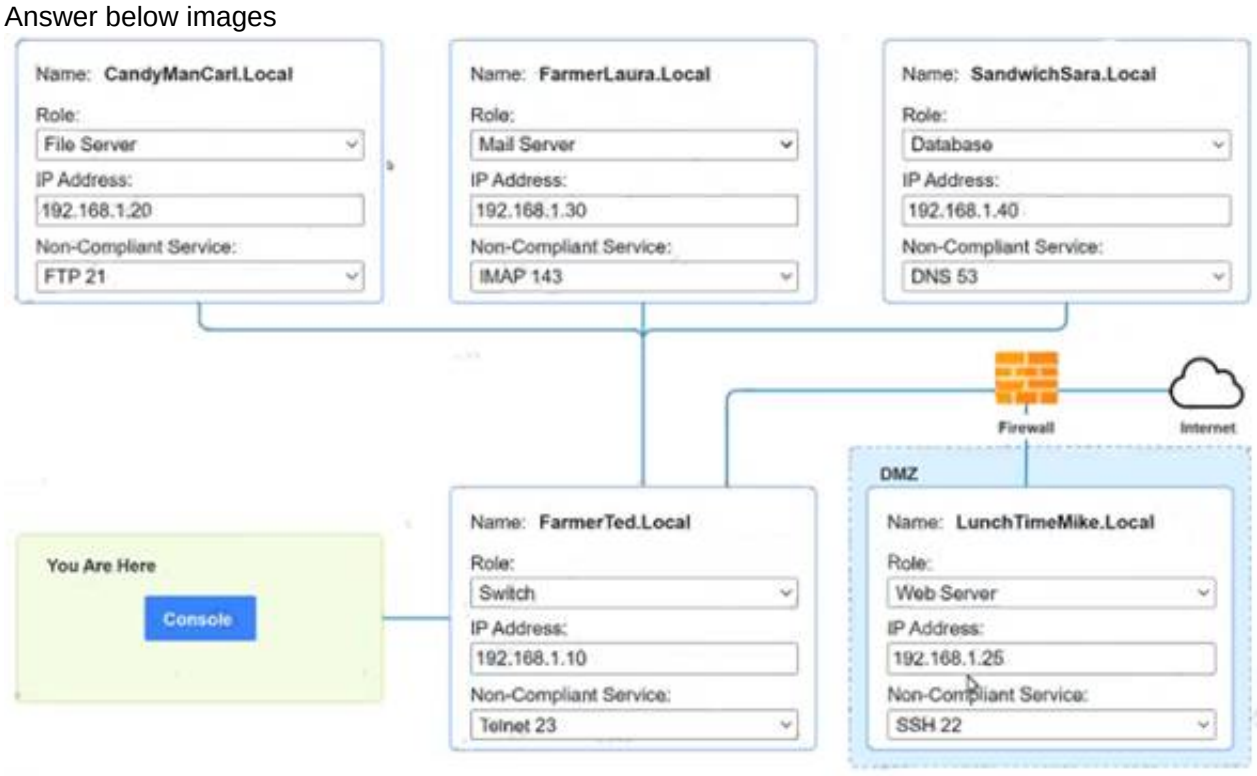
You must determine
- ip address of each device
- The primary server or service each device
- The protocols that should be disabled based on the hardening guidelines

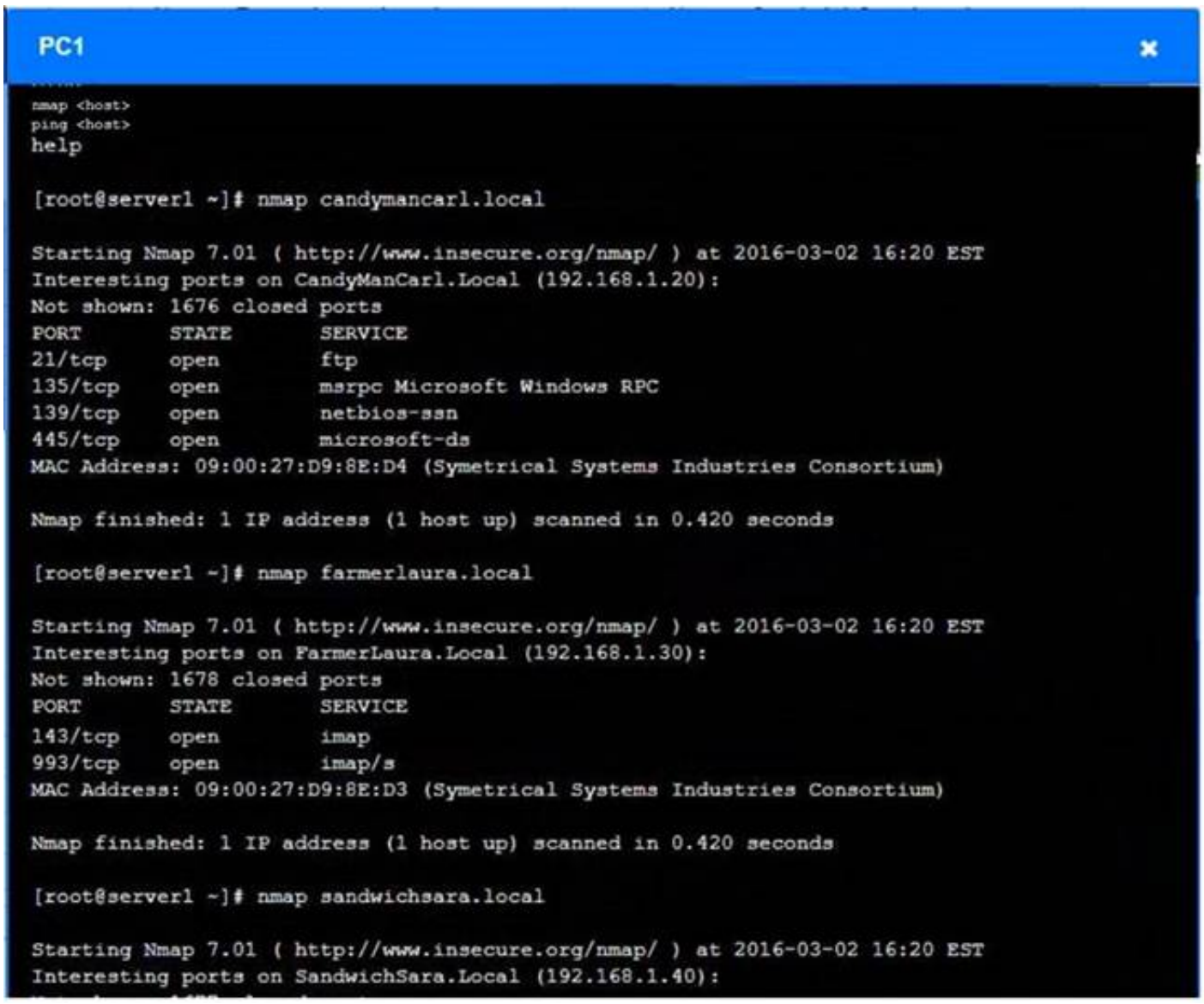



A. Mastered
B. Not Mastered

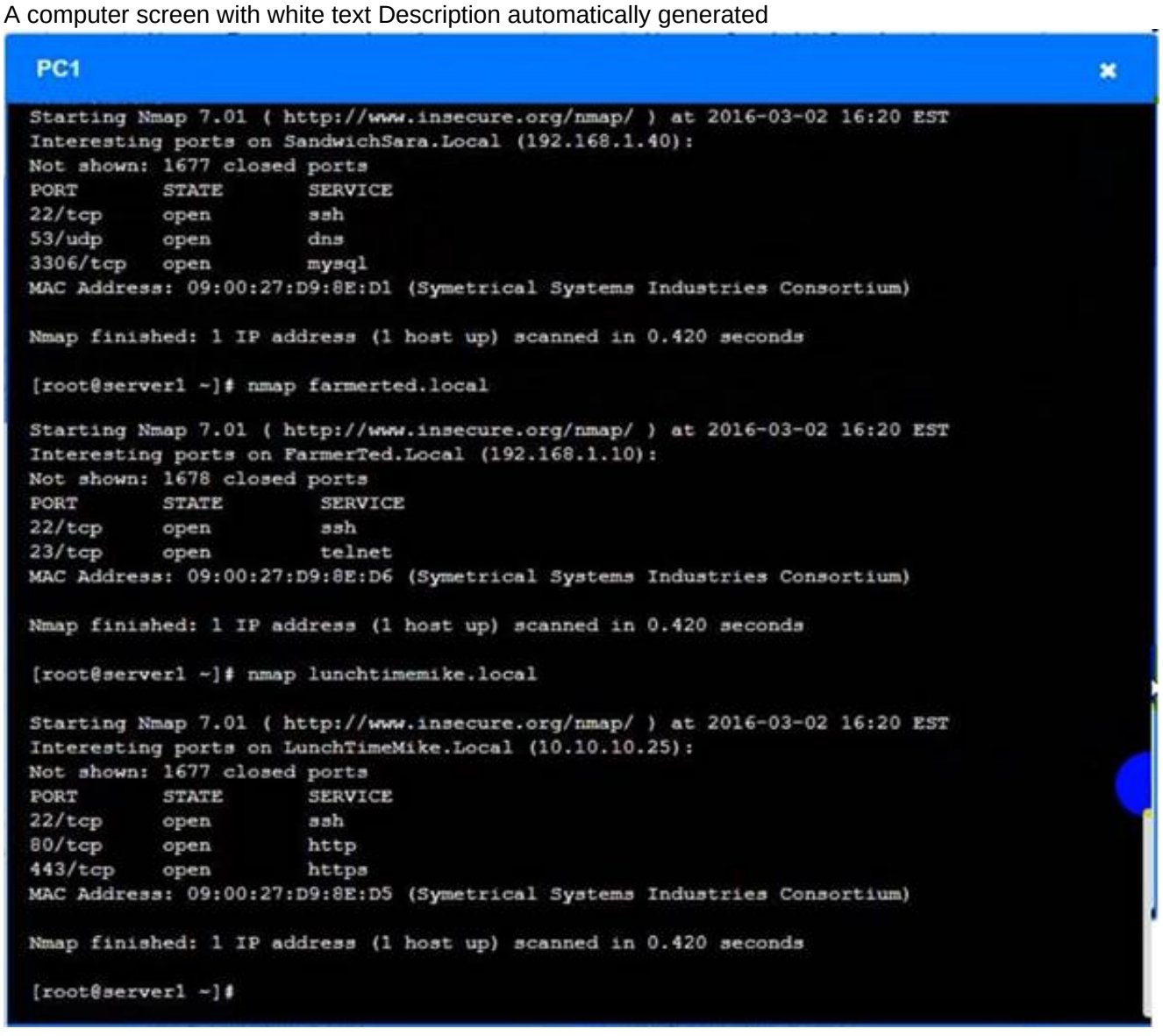
**Answer:** A

**Explanation:**
Answer below images






A computer screen with white text Description automatically generated




**NEW QUESTION 88**
A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

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

**Answer:** C

**Explanation:**
CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H is the attack vector that the analyst should remediate first, as it has the highest CVSSv3 score of 8.1. CVSSv3

(Common Vulnerability Scoring System version 3) is a standard framework for rating the severity of vulnerabilities, based on various metrics that reflect the characteristics and impact of the vulnerability. The CVSSv3 score is calculated from three groups of metrics: Base, Temporal, and Environmental. The Base metrics are mandatory and reflect the intrinsic qualities of the vulnerability, such as how it can be exploited, what privileges are required, and what impact it has on confidentiality, integrity, and availability. The Temporal metrics are optional and reflect the current state of the vulnerability, such as whether there is a known exploit, a patch, or a workaround. The Environmental metrics are also optional and reflect the context of the vulnerability in a specific environment, such as how it affects the asset value, security requirements, or mitigating controls. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.
The attack vector in question has the following Base metrics:
- Attack Vector (AV): Network (N). This means that the vulnerability can be exploited remotely over a network connection.
- Attack Complexity (AC): Low (L). This means that the attack does not require any special conditions or changes to the configuration of the target system.
- Privileges Required (PR): Low (L). This means that the attacker needs some privileges on the target system to exploit the vulnerability, such as user-level access.
- User Interaction (UI): None (N). This means that the attack does not require any user action or involvement to succeed.
- Scope (S): Unchanged (U). This means that the impact of the vulnerability is confined to the same security authority as the vulnerable component, such as an application or an operating system.
- Confidentiality Impact ©: High (H). This means that the vulnerability results in a total loss of confidentiality, such as unauthorized disclosure of all data on the system.
- Integrity Impact (I): High (H). This means that the vulnerability results in a total loss of integrity, such as unauthorized modification or deletion of all data on the system.
- Availability Impact (A): High (H). This means that the vulnerability results in a total loss of availability,

such as denial of service or system crash.
Using these metrics, we can calculate the Base score using this formula: Base Score = Roundup(Minimum[(Impact + Exploitability), 10]) Where:
Impact = 6.42 x [1 - ((1 - Confidentiality) x (1 - Integrity) x (1 - Availability))]
Exploitability = 8.22 x Attack Vector x Attack Complexity x Privileges Required x User Interaction Using this formula, we get:
Impact = 6.42 x [1 - ((1 - 0.56) x (1 - 0.56) x (1 - 0.56))] = 5.9
Exploitability = 8.22 x 0.85 x 0.77 x 0.62 x 0.85 = 2.8
Base Score = Roundup(Minimum[(5.9 + 2.8), 10]) = Roundup(8.7) = 8.8
Therefore, this attack vector has a Base score of 8.8, which is higher than any other option.
The other attack vectors have lower Base scores, as they have different values for some of the Base metrics:
- CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.2, as it has a lower value for

Attack Vector (Physical), which means that the vulnerability can only be exploited by having physical access to the target system.
- CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 7.4, as it has a lower value for Attack Vector (Adjacent Network), which means that the vulnerability can only be exploited by being on the same physical or logical network as the target system.
- CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.8, as it has a lower value for Attack Vector (Local), which means that the vulnerability can only be exploited by having local access to the target system, such as through a terminal or a command shell.

**NEW QUESTION 93**
A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve
this issue?

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

**Answer:** A

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

**NEW QUESTION 98**
Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

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

**Answer:** C

**Explanation:**
The correct answer is C. Impact.
The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service1.
The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The

timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

**NEW QUESTION 103**
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 105**
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 107**
The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

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

**Answer:** A

**Explanation:**
A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

**NEW QUESTION 108**
A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

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

**Answer:** A

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

**NEW QUESTION 109**
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 113**
Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

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

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

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

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

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

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

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

**Answer:** E

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

**NEW QUESTION 117**
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.

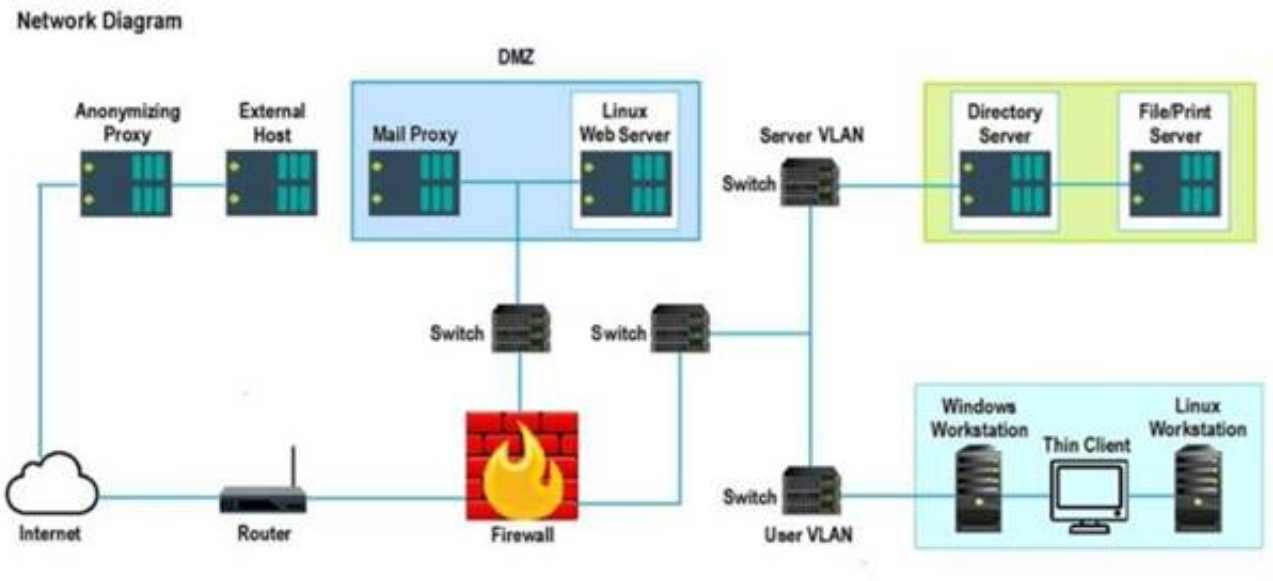
**NEW QUESTION 118**
During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

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 122**
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.



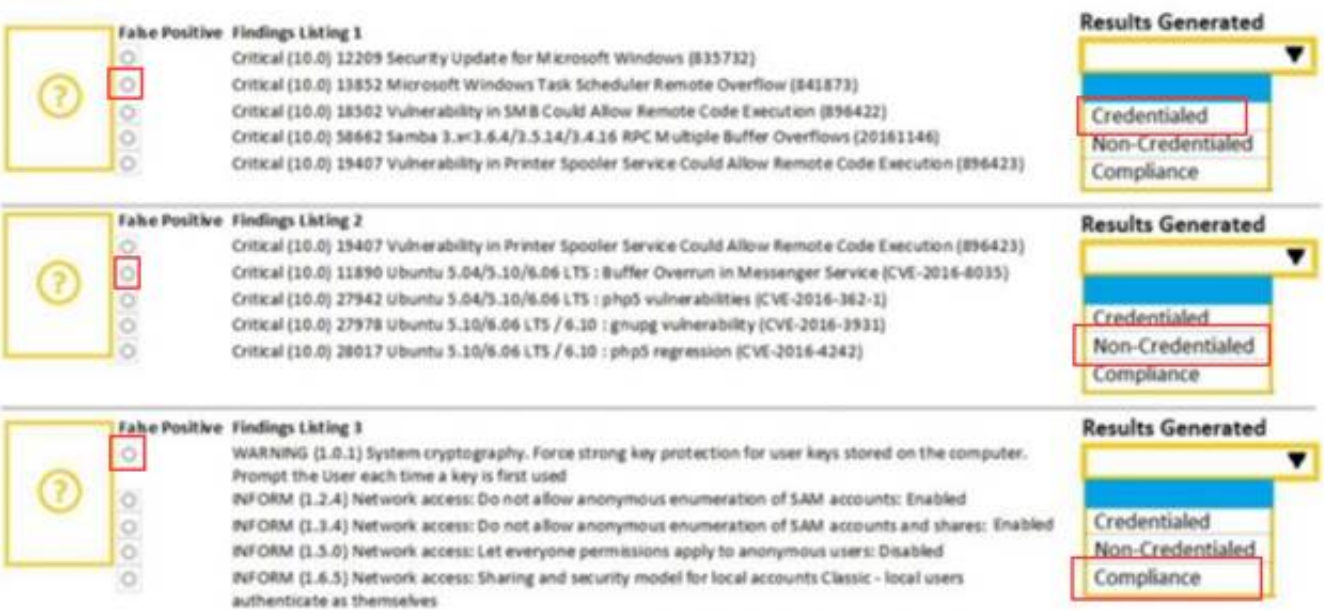

**Hot Area:**


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**Hot Area:**




**NEW QUESTION 127**
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 131**
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 135**
Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

A. MOU
B. NDA
C. BIA
D. SLA

**Answer:** D

**Explanation:**
SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements. 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 137**
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 138**
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 141**
A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

A. Inform the internal incident response team.
B. Follow the company's incident response plan.
C. Review the lessons learned for the best approach.
D. Determine when the access started.

**Answer:** B

**Explanation:**
An incident response plan is a set of predefined procedures and guidelines that an organization follows when faced with a security breach or attack. An incident response plan helps to ensure that the organization can quickly and effectively contain, analyze, eradicate, and recover from the incident, as well as prevent or minimize the damage and impact to the business operations, reputation, and customers. An incident response plan also defines the roles and responsibilities of the incident response team, the communication channels and protocols, the escalation and reporting procedures, and the tools and resources available for the incident response.
By following the company’s incident response plan, the administrator can ensure that they are following the best practices and standards for handling a security incident, and that they are coordinating and collaborating with the relevant stakeholders and authorities. Following the company’s incident response plan can also help to avoid or reduce any legal, regulatory, or contractual liabilities or penalties that may arise from the incident.
The other options are not as effective or appropriate as following the company’s incident response plan. Informing the internal incident response team (A) is a good step, but it should be done according to the company’s incident response plan, which may specify who, when, how, and what to report. Reviewing the lessons learned for the best approach © is a good step, but it should be done after the incident has been resolved and closed, not during the active response phase. Determining when the access started (D) is a good step, but it should be done as part of the analysis phase of the incident response plan, not before following the plan.

**NEW QUESTION 144**
A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

A. confi
B. ini
C. ntds.dit
D. Master boot record
E. Registry

**Answer:** D

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

**NEW QUESTION 146**
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 151**
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 154**
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 157**
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 161**
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 162**
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 166**

The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

| Vulnerability title | Attack vector | Attack complexity | Authentication required | User interaction required |
|---|---|---|---|---|
| Vulnerability A | Network | Low | No | Yes |
| Vulnerability B | Local | Low | Yes | Yes |
| Vulnerability C | Network | High | Yes | Yes |
| Vulnerability D | Local | Low | No | No |

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

A. Vulnerability A
B. Vulnerability B
C. Vulnerability C
D. Vulnerability D

**Answer:** B

**Explanation:**
Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that end users frequently click on malicious links sent via email. Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connects to the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook. Therefore, the analyst should prioritize patching this vulnerability as soon as possible to prevent potential compromise of the workstations.

**NEW QUESTION 171**
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 175**
A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following
would best aid in decreasing the workload without increasing staff?

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

**Answer:** C

**Explanation:**
SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

**NEW QUESTION 180**
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 181**
After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASB to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

A. SIEM ingestion logs are reduced by 20%.
B. Phishing alerts drop by 20%.
C. False positive rates drop to 20%.
D. The MTTR decreases by 20%.

**Answer:** D

**Explanation:**
The MTTR (Mean Time to Resolution) decreases by 20% is the best possible outcome that this effort hopes to achieve, as it reflects the improvement in the efficiency and effectiveness of the incident response process by reducing analyst alert fatigue. Analyst alert fatigue is a term that refers to the phenomenon of security analysts becoming overwhelmed, desensitized, or exhausted by the large number of alerts they receive from various security tools or systems, such as DLP (Data Loss Prevention) or CASB (Cloud Access Security Broker). DLP is a security solution that helps to prevent unauthorized access, use, or transfer of sensitive data, such as personal information, intellectual property, or financial records. CASB is a security solution that helps to monitor and control the use of cloud-based applications and services, such as SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service). Both DLP and CASB can generate alerts when they detect potential data breaches, policy violations, or malicious activities, but they can also produce false positives, irrelevant information, or duplicate notifications that can overwhelm or distract the security analysts. Analyst alert fatigue can have negative consequences for the security posture and performance of an organization, such as missing or ignoring critical alerts, delaying or skipping investigations or remediations, making errors or mistakes, or losing motivation or morale. Therefore, it is important to reduce analyst alert fatigue and optimize the alert management process by using various strategies, such as tuning the alert thresholds and rules, prioritizing and triaging the alerts based on severity and context, enriching and correlating the alerts with additional data sources, automating or orchestrating repetitive or low-level tasks or actions, or integrating and consolidating different security tools or systems into a unified platform. By reducing analyst alert fatigue and optimizing the alert management process, the effort hopes to achieve a decrease in the MTTR, which is a metric that measures the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. A lower MTTR indicates a faster and more effective incident response process, which can help to minimize the impact and damage of security incidents, improve customer satisfaction and trust, and enhance security operations and outcomes. The other options are not as relevant or realistic as the MTTR decreases by 20%, as they do not reflect the best possible outcome that this effort hopes to achieve. SIEM ingestion logs are reduced by 20% is not a relevant outcome, as it does not indicate any improvement in the incident response process or any reduction in analyst alert fatigue. SIEM (Security Information and Event Management) is a security 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 ingestion logs are records of the data that is ingested by the SIEM system from different sources. Reducing SIEM ingestion logs may imply less data volume or less data sources for the SIEM system, which may not necessarily improve its performance or accuracy. Phishing alerts drop by 20% is not a realistic outcome, as it does not depend on the integration of DLP and CASB or any reduction in analyst alert fatigue. Phishing alerts are notifications that indicate potential phishing attempts or attacks, such as fraudulent emails, websites, or messages that try to trick users into revealing sensitive information or installing malware. Phishing alerts can be generated by various security tools or systems, such as email security solutions, web security solutions, endpoint security solutions, or user awareness training programs. Reducing phishing alerts may imply less phishing attempts or attacks on the organization, which may not necessarily be influenced by the integration of DLP and CASB or any reduction in analyst alert fatigue. False positive rates drop to 20% is not a realistic outcome

**NEW QUESTION 184**
Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

A. Log retention
B. Log rotation
C. Maximum log size
D. Threshold value

**Answer:** D

**Explanation:**
A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a

threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis12

**NEW QUESTION 187**
A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being
used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

A. Leave the proxy as is.
B. Decomission the proxy.
C. Migrate the proxy to the cloud.
D. Patch the proxy

**Answer:** B

**Explanation:**
The best practice that the company should follow with this proxy is to decommission the proxy. Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning the proxy can help eliminate the vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

**NEW QUESTION 189**
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 192**
Which of the following is the most important factor to ensure accurate incident response reporting?

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

**Answer:** A

**Explanation:**
A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official References:
- https://www.ibm.com/topics/incident-response
- https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

**NEW QUESTION 195**
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.

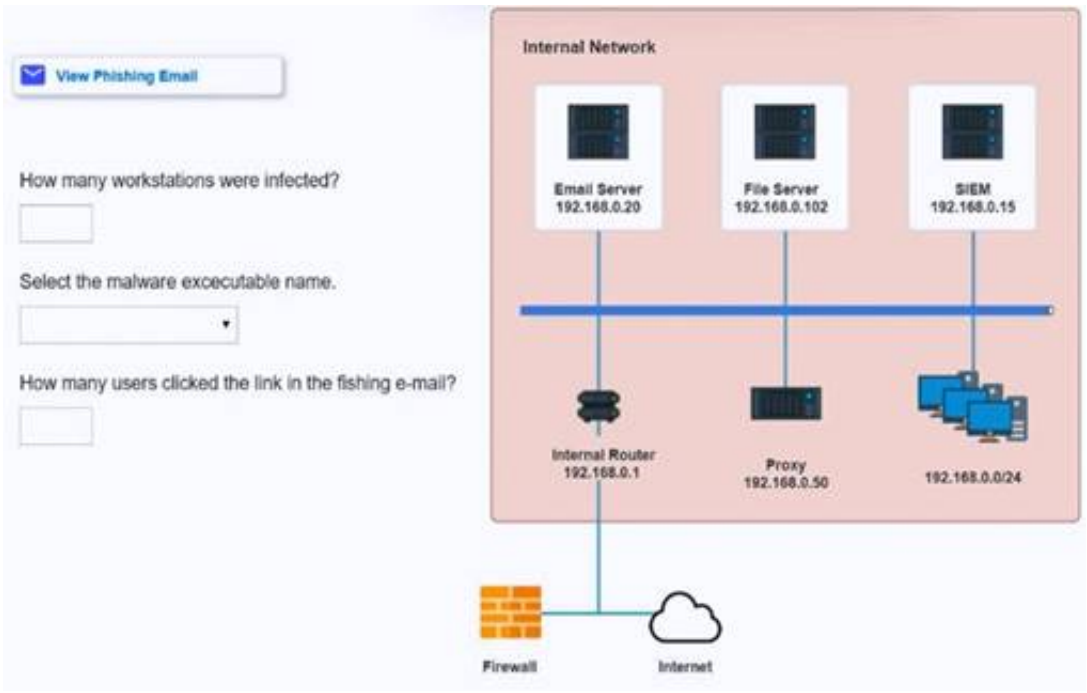
**NEW QUESTION 199**
A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

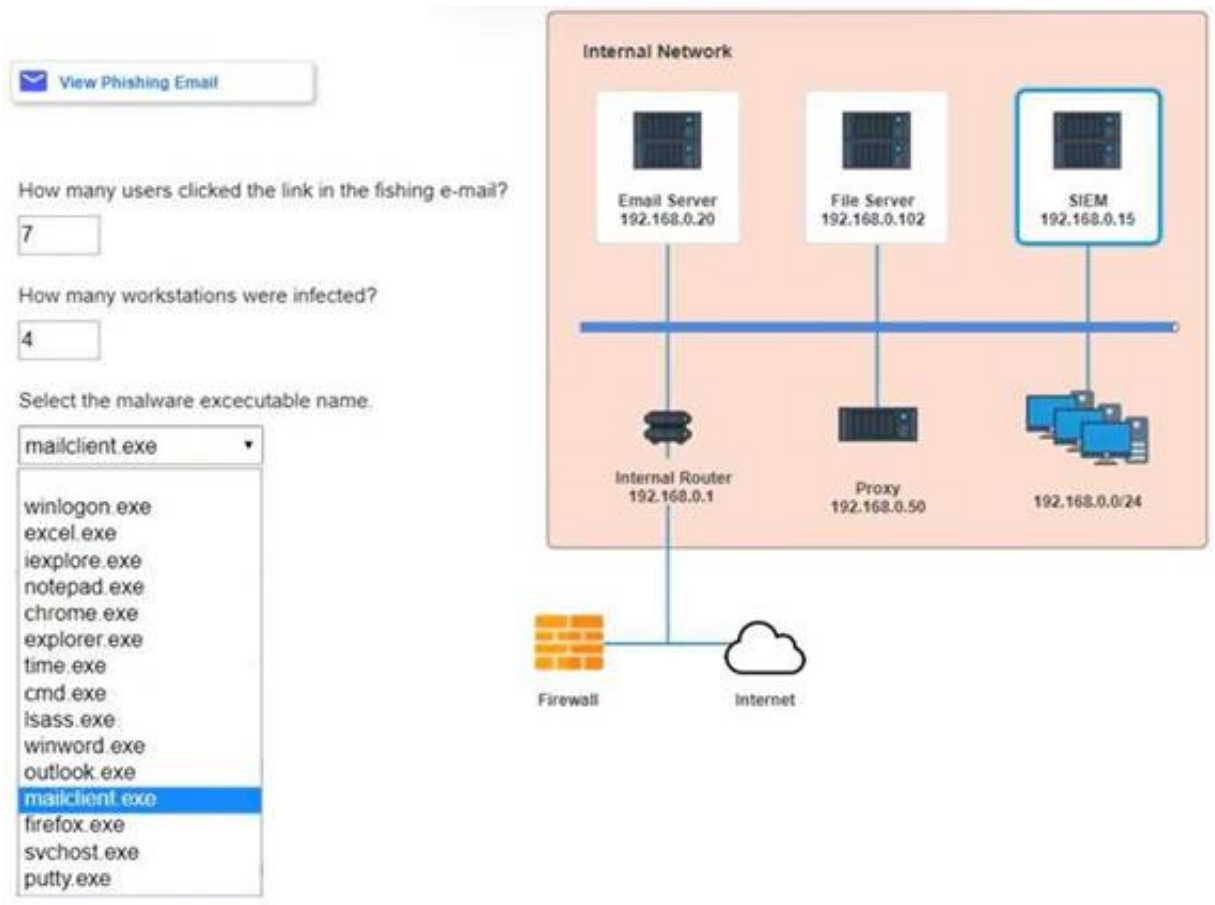
A. OSSTMM
B. Diamond Model Of Intrusion Analysis
C. OWASP
D. MITRE ATT&CK

**Answer:** D

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

**NEW QUESTION 203**
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?



**Phishing Email**

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

**Email Server Logs - Email Server 192.168.0.20**

| 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 | 57688 | stanimoto@anycorp.com | adifabio@anycorp.com |
| 3/7/2016 4:15:13 PM | TCP | 192.168.0.139 | 46550 | hparikh@anycorp.com | adifabio@anycorp.com |
| 3/7/2016 4:14:25 PM | TCP | 192.168.0.185 | 63616 | jlee@anycorp.com | jlee@anycorp.com;adifabio@anycorp.com |
| 3/7/2016 4:13:02 PM | TCP | 192.168.0.47 | 60919 | adifabio@anycorp.com | cpuziss@anycorp.com |
| 3/7/2016 4:12:50 PM | TCP | 192.168.0.155 | 32891 | kwilliams@anycorp.com | hparikh@anycorp.com |
| 3/7/2016 4:11:09 PM | TCP | 192.168.0.34 | 46187 | lbalk@anycorp.com | jlee@anycorp.com |
| 3/7/2016 4:10:54 PM | TCP | 192.168.0.181 | 34556 | dfritz@anycorp.com | kmatthews@anycorp.com |
| 3/7/2016 4:10:38 PM | TCP | 192.168.0.155 | 32891 | kwilliams@anycorp.com | hparikh@anycorp.com |
| 3/7/2016 4:10:23 PM | TCP | 192.168.0.185 | 63616 | jlee@anycorp.com | asmith@anycorp.com |
| 3/7/2016 4:09:34 PM | TCP | 192.168.0.34 | 30364 | asmith@anycorp.com | hparikh@anycorp.com |
| 3/7/2016 4:08:49 PM | TCP | 192.168.0.61 | 48734 | cpuziss@anycorp.com | kmatthews@anycorp.com |
| 3/7/2016 4:07:33 PM | TCP | 192.168.0.197 | 33685 | gromney@anycorp.com | lbalk@anycorp.com |
| 3/7/2016 4:07:32 PM | TCP | 192.168.0.47 | 60919 | adifabio@anycorp.com | adifabio@anycorp.com;jlee@anycorp.com |
| 3/7/2016 4:05:47 PM | TCP | 192.168.0.34 | 30364 | asmith@anycorp.com | jlee@anycorp.com |
| 3/7/2016 4:04:24 PM | TCP | 192.168.0.139 | 46550 | hparikh@anycorp.com | asmith@anycorp.com |
| 3/7/2016 4:03:58 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 | ibenz@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 | krossiter@anycorp.com |
| 3/7/2016 4:01:31 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | ahynson@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 | brogge@anycorp.com |
| 3/7/2016 4:01:28 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | aaverlitt@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 | wmcnarney@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 |

**Email Server Logs - Email Server 192.168.0.20**

| 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 | lbreiber@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 | bhoda@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 | mkamen@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 | jdeganhardt@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 | jmammott@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 | halbert@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 |

**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 | bteer@anycorp.com |
| 3/7/2016 4:00:40 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | tfabor@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 | tslaughter@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 | dsilvers@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 | starimoto@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 | fbemvare@anycorp.com |
| 3/7/2016 4:00:28 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | cgallpeau@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 | cputliss@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**

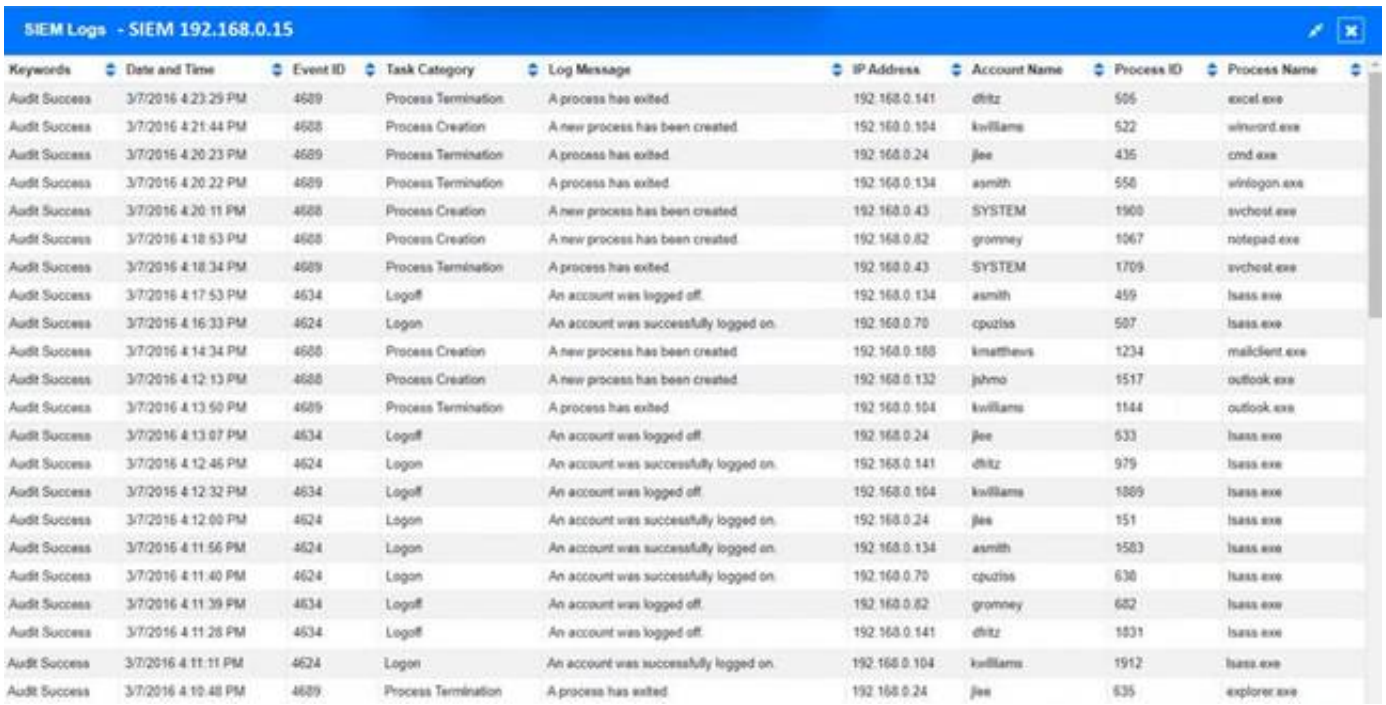
| Date/Time | Protocol | SIP | Source port | From | To |
|---|---|---|---|---|---|
| 3/7/2016 4:00:41 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | bteer@anycorp.com |
| 3/7/2016 4:00:40 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | tfabor@anycorp.com |
| 3/7/2016 4:00:40 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | lsller@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 | rpondu@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 4:00:39 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 | dsilvers@anycorp.com |
| 3/7/2016 4:00:33 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | rsolstrunk@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 | jsulcahy@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 | fbenivare@anycorp.com |
| 3/7/2016 4:00:28 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | cgallpeau@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 | cpuzino@anycorp.com |
| 3/7/2016 4:00:17 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | mhazen@anycorp.com |
| 3/7/2016 4:00:17 PM | TCP | 58.125.17.196 | 54566 | it-helpdesk@sobergrill.com | hpatrikh@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 | monulg@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 |

**File Server Logs - File Server 192.168.0.102**

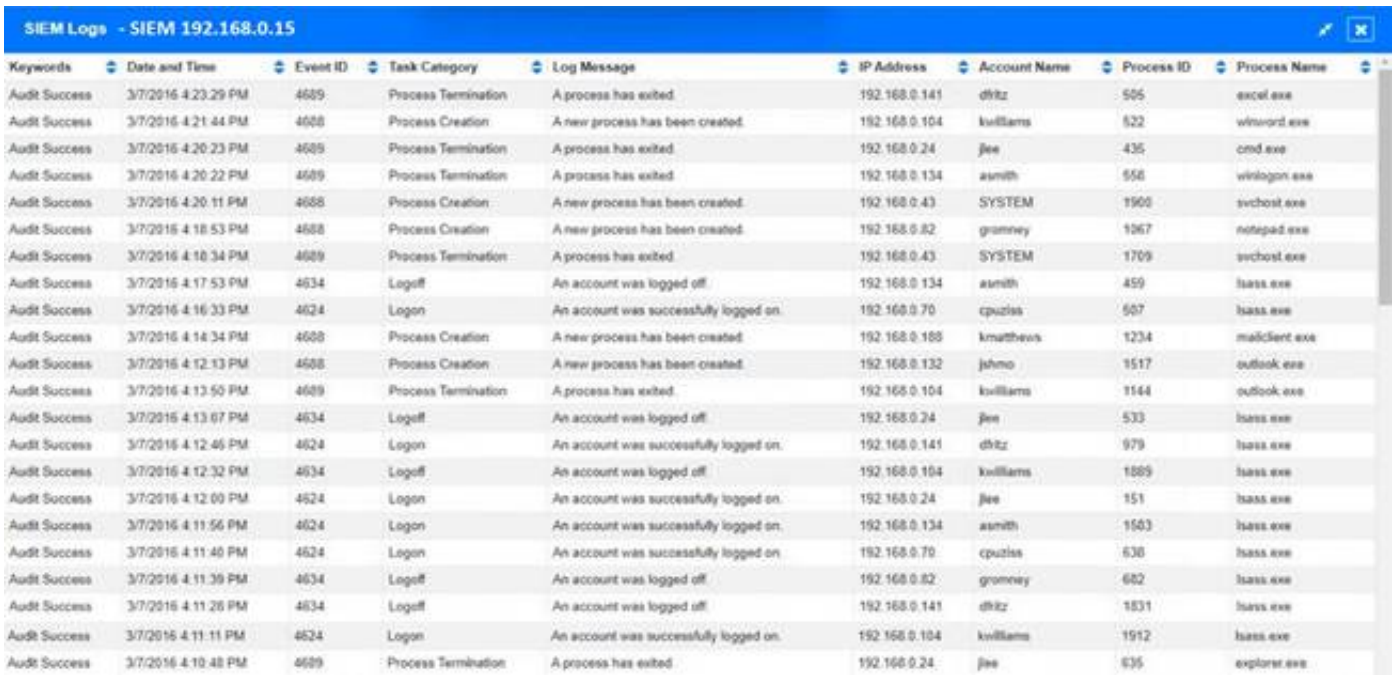
| Date/Time | Source IP | Source port | Dest IP | Dest Port | URL | Request |
|---|---|---|---|---|---|---|
| 3/7/2016 4:27:03 PM | 192.168.0.153 | 50467 | 11.102.109.179 | 80 | bestpurchase.com | POST |
| 3/7/2016 4:26:51 PM | 192.168.0.245 | 60021 | 72.104.64.186 | 80 | visitorcenter.com | GET |
| 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 | 124.140.268.241 | 80 | stopthebotnet.com | GET |
| 3/7/2016 4:23:39 PM | 192.168.0.150 | 54460 | 74.182.188.144 | 80 | funweb.cn | GET |
| 3/7/2016 4:21:39 PM | 192.168.0.211 | 54172 | 165.11.148.28 | 80 | chatforfree.ru | POST |
| 3/7/2016 4:20:10 PM | 192.168.0.30 | 55666 | 214.214.167.54 | 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 | 101.237.65.107 | 80 | securethenet.com | GET |
| 3/7/2016 4:14:04 PM | 192.168.0.188 | 51745 | 33.225.130.104 | 80 | chzweb.tilapia.com | GET |
| 3/7/2016 4:12:22 PM | 192.168.0.95 | 42733 | 103.136.14.126 | 80 | goodguys.se | POST |
| 3/7/2016 4:11:53 PM | 192.168.0.215 | 62813 | 181.139.24.22 | 80 | pastebucket.cn | POST |
| 3/7/2016 4:11:34 PM | 192.168.0.70 | 40821 | 33.225.130.104 | 80 | chzweb.tilapia.com | GET |
| 3/7/2016 4:10:35 PM | 192.168.0.218 | 54606 | 124.169.173.216 | 80 | funweb.cn | POST |
| 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 | 55547 | 33.225.130.104 | 80 | chzweb.tilapia.com | GET |
| 3/7/2016 4:04:37 PM | 192.168.0.117 | 54559 | 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 | 204.190.57.150 | 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 | 39520 | 141.217.181.243 | 80 | goodguys.se | POST |
| 3/7/2016 3:52:47 PM | 192.168.0.253 | 36463 | 79.115.291.191 | 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 3:35:59 PM | 192.168.0.95 | 34447 | 133.136.173.36 | 80 | anti-malware.com | GET |
| 3/7/2016 3:35:38 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 |




| 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 | 556 | winlogon.exe |
| Audit Success | 3/7/2016 4:20:11 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.43 | SYSTEM | 1900 | svchost.exe |
| Audit Success | 3/7/2016 4:18:53 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.82 | gromney | 1067 | notepad.exe |
| Audit Success | 3/7/2016 4:18:34 PM | 4689 | Process Termination | A process has exited. | 192.168.0.43 | SYSTEM | 1709 | svchost.exe |
| Audit Success | 3/7/2016 4:17:53 PM | 4634 | Logoff | An account was logged off. | 192.168.0.134 | asmith | 459 | lsass.exe |
| Audit Success | 3/7/2016 4:16:33 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.70 | cpuziss | 507 | lsass.exe |
| Audit Success | 3/7/2016 4:14:34 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.188 | kmatthews | 1234 | mailclient.exe |
| Audit Success | 3/7/2016 4:12:13 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.132 | jshmo | 1517 | outlook.exe |
| Audit Success | 3/7/2016 4:13:50 PM | 4689 | Process Termination | A process has exited. | 192.168.0.104 | kwilliams | 1144 | outlook.exe |
| Audit Success | 3/7/2016 4:13:07 PM | 4634 | Logoff | An account was logged off. | 192.168.0.24 | jlee | 533 | lsass.exe |
| Audit Success | 3/7/2016 4:12:46 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.141 | dfritz | 979 | lsass.exe |
| Audit Success | 3/7/2016 4:12:32 PM | 4634 | Logoff | An account was logged off. | 192.168.0.104 | kwilliams | 1889 | lsass.exe |
| Audit Success | 3/7/2016 4:12:00 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.24 | jlee | 151 | lsass.exe |
| Audit Success | 3/7/2016 4:11:56 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.134 | asmith | 1583 | lsass.exe |
| Audit Success | 3/7/2016 4:11:40 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.70 | cpuziss | 638 | lsass.exe |
| Audit Success | 3/7/2016 4:11:39 PM | 4634 | Logoff | An account was logged off. | 192.168.0.82 | gromney | 682 | lsass.exe |
| 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 |




| 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 | 556 | winlogon.exe |
| Audit Success | 3/7/2016 4:20:11 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.43 | SYSTEM | 1900 | svchost.exe |
| Audit Success | 3/7/2016 4:18:53 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.82 | gromney | 1067 | notepad.exe |
| Audit Success | 3/7/2016 4:18:34 PM | 4689 | Process Termination | A process has exited. | 192.168.0.43 | SYSTEM | 1709 | svchost.exe |
| Audit Success | 3/7/2016 4:17:53 PM | 4634 | Logoff | An account was logged off. | 192.168.0.134 | asmith | 459 | lsass.exe |
| Audit Success | 3/7/2016 4:16:33 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.70 | cpuziss | 507 | lsass.exe |
| Audit Success | 3/7/2016 4:14:34 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.188 | kmatthews | 1234 | mailclient.exe |
| Audit Success | 3/7/2016 4:12:13 PM | 4688 | Process Creation | A new process has been created. | 192.168.0.132 | jshmo | 1517 | outlook.exe |
| Audit Success | 3/7/2016 4:13:50 PM | 4689 | Process Termination | A process has exited. | 192.168.0.104 | kwilliams | 1144 | outlook.exe |
| Audit Success | 3/7/2016 4:13:07 PM | 4634 | Logoff | An account was logged off. | 192.168.0.24 | jlee | 533 | lsass.exe |
| Audit Success | 3/7/2016 4:12:46 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.141 | dfritz | 979 | lsass.exe |
| Audit Success | 3/7/2016 4:12:32 PM | 4634 | Logoff | An account was logged off. | 192.168.0.104 | kwilliams | 1889 | lsass.exe |
| Audit Success | 3/7/2016 4:12:00 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.24 | jlee | 151 | lsass.exe |
| Audit Success | 3/7/2016 4:11:56 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.134 | asmith | 1583 | lsass.exe |
| Audit Success | 3/7/2016 4:11:40 PM | 4624 | Logon | An account was successfully logged on. | 192.168.0.70 | cpuziss | 638 | lsass.exe |
| Audit Success | 3/7/2016 4:11:39 PM | 4634 | Logoff | An account was logged off. | 192.168.0.82 | gromney | 682 | lsass.exe |
| 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 208**
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 209**
.....

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## CS0-003 Practice Exam Features:

* CS0-003 Questions and Answers Updated Frequently

* CS0-003 Practice Questions Verified by Expert Senior Certified Staff

* CS0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year