

## Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

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



### NEW QUESTION 1

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

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

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

- A. PowerShell
- B. Ruby
- C. Python
- D. Shell script

**Answer: A**

#### Explanation:

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

### NEW QUESTION 2

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

- created the initial evidence log.
- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

- A. Update the system firmware and reimage the hardware.
- B. Install an additional malware scanner that will send email alerts to the analyst.
- C. Configure the system to use a proxy server for Internet access.
- D. Delete the user profile and restore data from backup.

**Answer: A**

#### Explanation:

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

### NEW QUESTION 3

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

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

**Answer: D**

#### Explanation:

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

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

### NEW QUESTION 4

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 5**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 6**

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

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

**Answer:** D

**Explanation:**

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls<sup>1</sup>  
The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

**NEW QUESTION 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 pipeline.
- 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

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 9

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 10

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 10

A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to <https://office365password.acme.co>. The site's standard VPN logon page is [www.acme.com/logon](http://www.acme.com/logon). Which of the following is most likely true?

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

**Answer: D**

#### Explanation:



for the outbound traffic to a host IP that resolves to <https://office365password.acme.co>, while the site's standard VPN logon page is [www.acme.com/logon](http://www.acme.com/logon). A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (office365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. Official References:

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

#### NEW QUESTION 12

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

- A. 

```
function w() { a=$(ping -c 1 $1 | awk-F "/" 'END{print $1}') && echo "$1 | $a" }
```
- B. 

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

```
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." 'in-addr' '{print $1}').origin.asn.cymru.com TXT +short }
```
- D. 

```
function z() { c=$(geoiplookup$1) && echo "$1 | $c" }
```

**Answer: C**

#### Explanation:

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

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

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

#### NEW QUESTION 16

The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

- A. Reduce the administrator and privileged access accounts
- B. Employ a network-based IDS
- C. Conduct thorough incident response
- D. Enable SSO to enterprise applications

**Answer: A**

#### Explanation:

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts. Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

#### NEW QUESTION 19

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 overflows<sup>1</sup>. 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 runs<sup>2</sup>.

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 heap<sup>3</sup>. 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 24

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

- A. A mean time to remediate of 30 days

- B. A mean time to detect of 45 days
- C. A mean time to respond of 15 days
- D. Third-party application testing

**Answer:** A

**Explanation:**

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

**NEW QUESTION 25**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 29**

Which of the following items should be included in a vulnerability scan report? (Choose two.)

- A. Lessons learned
- B. Service-level agreement
- C. Playbook
- D. Affected hosts
- E. Risk score
- F. Education plan

**Answer:** DE

**Explanation:**

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

**NEW QUESTION 33**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 38**

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.

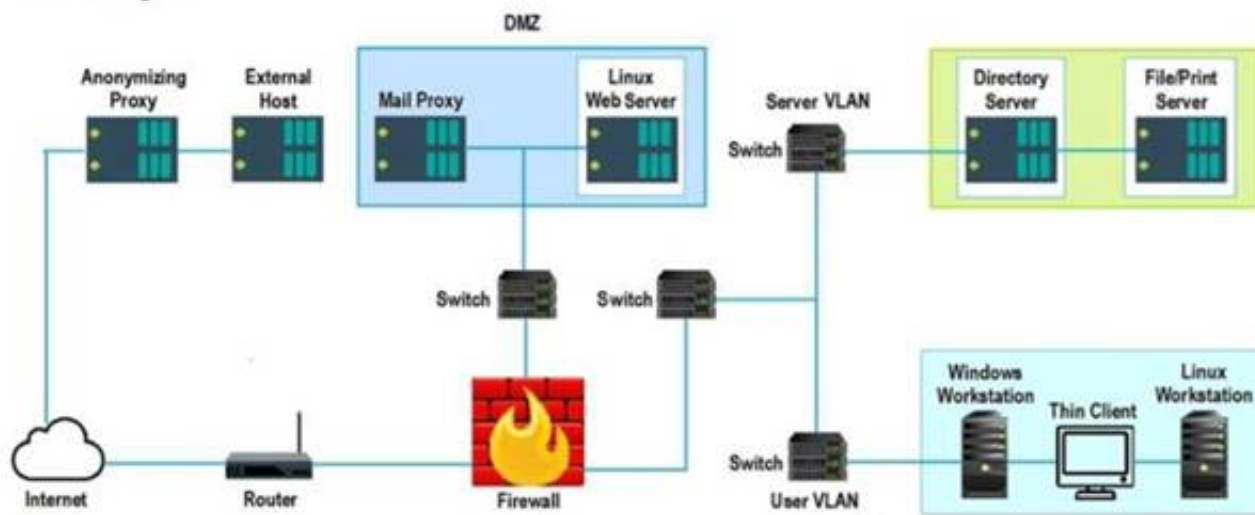
Instructions:

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.

Network Diagram



## Hot Area:

False Positive	Findings Listing	Results Generated
<input type="radio"/>	<b>Findings Listing 1</b> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x:3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	Credentialed Non-Credentialed Compliance
<input type="radio"/>	<b>Findings Listing 2</b> Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035) Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	Credentialed Non-Credentialed Compliance
<input type="radio"/>	<b>Findings Listing 3</b> WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves	Credentialed Non-Credentialed Compliance

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

## Hot Area:

False Positive	Findings Listing	Results Generated
<input checked="" type="radio"/>	<b>Findings Listing 1</b> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x:3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	Credentialed Non-Credentialed Compliance
<input checked="" type="radio"/>	<b>Findings Listing 2</b> Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035) Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	Credentialed Non-Credentialed Compliance
<input checked="" type="radio"/>	<b>Findings Listing 3</b> WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves	Credentialed Non-Credentialed Compliance

## NEW QUESTION 40

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/S{@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, and could lead to further compromise of the system. The other log entries do not show any signs of command injection, as they do not contain any special characters or commands that could alter the intended behavior of the application. Official References:

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

**NEW QUESTION 44**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 48**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 52**

A company is in the process of implementing a vulnerability management program. Which 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:**

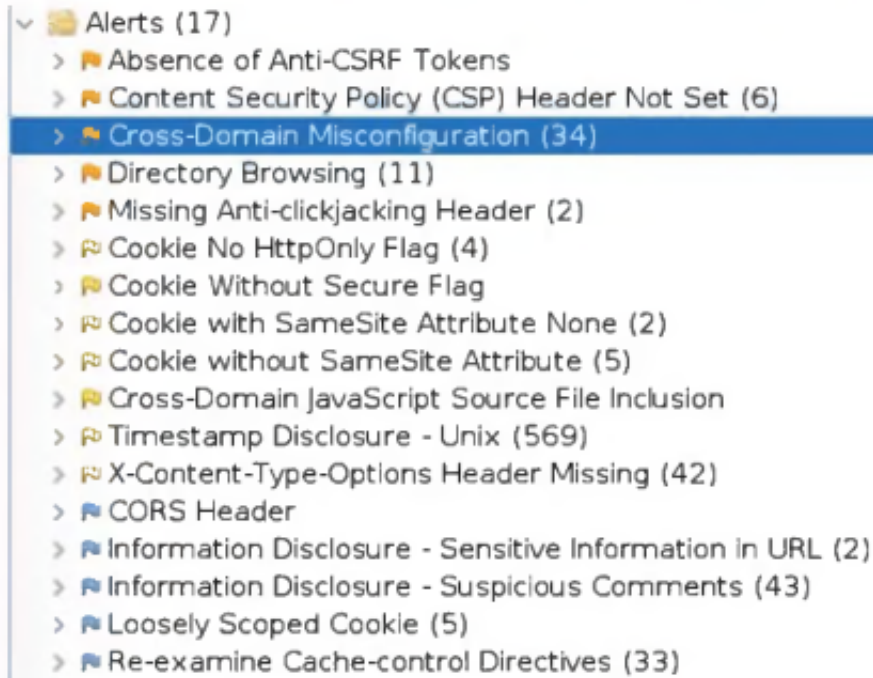
Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification 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 56

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



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

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

**Answer: C**

#### Explanation:

The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions.

The tuning recommendation is to configure the Access-Control-Allow-Origin header to only allow authorized domains that need to access the web application's resources. This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.

#### NEW QUESTION 57

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

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

**Answer: B**

#### Explanation:

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References:

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

#### NEW QUESTION 58

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 63

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 65**

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 69**

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

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

**Answer:** C

**Explanation:**

The correct answer is C. Legal department.

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

**NEW QUESTION 70**

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 75

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

- A. Hard disk
- B. Primary boot partition
- C. Malicious tiles
- D. Routing table
- E. Static IP address

**Answer:** A

#### Explanation:

The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

#### NEW QUESTION 80

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 analysis<sup>12</sup>

#### NEW QUESTION 81

An organization was compromised, and the usernames and passwords of all employees were leaked online. Which of the following best describes the remediation that could reduce the impact of this situation?

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

**Answer:** A

#### Explanation:

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

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

#### NEW QUESTION 85

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

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



Answer: C

**Explanation:**

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

**NEW QUESTION 86**

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 90**

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 .

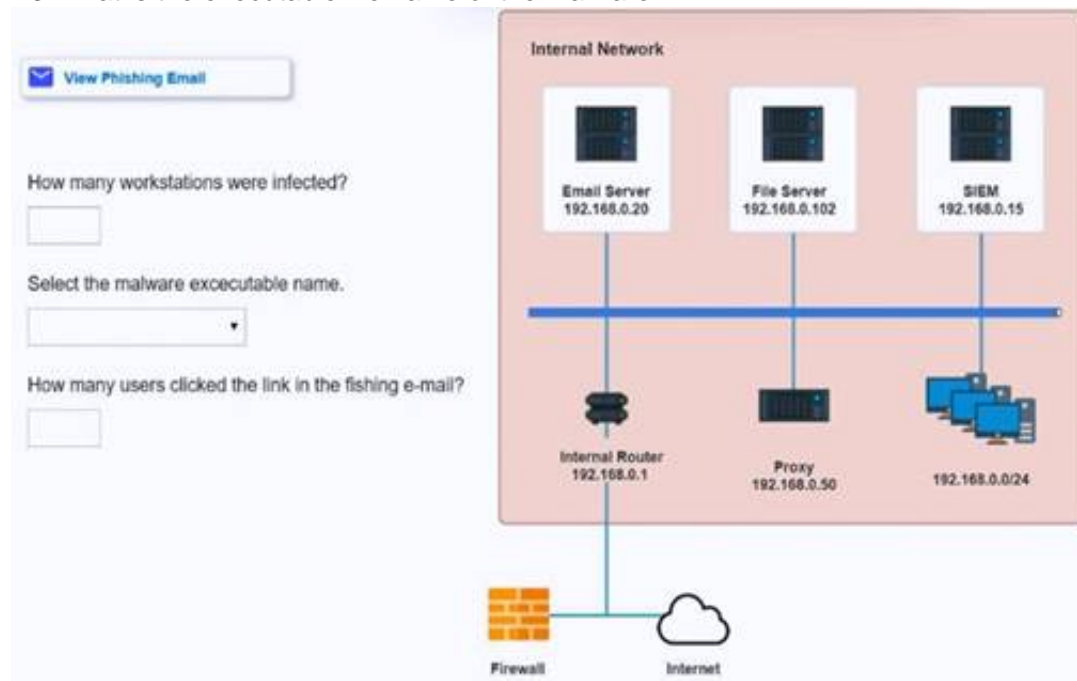
The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not 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 95**

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?



View Phishing Email

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

How many workstations were infected?

Select the malware executable name.

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

Internal Network

Phishing Email

From: IT HelpDesk <[it-helpdesk@sobergrill.com](mailto:it-helpdesk@sobergrill.com)>  
Sent: Mon 3/7/2016 4:00 PM  
To: Global Users <[globalusers@sobergrill.com](mailto: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	dfiltz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57868	stanimoto@anycorp.com	adfabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adfabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adfabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adfabio@anycorp.com	cpuzles@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.156	32891	kvillams@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	dfiltz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:30 PM	TCP	192.168.0.155	32891	kvillams@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	cpuzles@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gronney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adfabio@anycorp.com	adfabio@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	dfiltz@anycorp.com	cpuzles@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuzles@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	lrossiter@anycorp.com
3/7/2016 4:01:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	atynson@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mdillon@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	logge@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aaveritt@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	wmcnamey@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	imabile@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfautio@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@sobergill.com	it-elber@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	mgarnneau@anycorp.com
3/7/2016 4:01:20 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lmsusum@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lhodie@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ctsu@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	sprosperie@anycorp.com
3/7/2016 4:01:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lrmonteione@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	clensternachar@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	rgarfinkel@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	charoux@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	mkaman@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	zodogden@anycorp.com
3/7/2016 4:01:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	mhmonda@anycorp.com
3/7/2016 4:01:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	onorth@anycorp.com
3/7/2016 4:01:09 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	mroana@anycorp.com
3/7/2016 4:01:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kbouling@anycorp.com
3/7/2016 4:01:06 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	nrachal@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	jdegenhardt@anycorp.com
3/7/2016 4:01:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	wracette@anycorp.com
3/7/2016 4:01:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lhammond@anycorp.com
3/7/2016 4:00:59 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	dmilazzo@anycorp.com
3/7/2016 4:00:57 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	knoubauer@anycorp.com
3/7/2016 4:00:55 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	bboyko@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	dcrofoot@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	jmenemott@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	chodging@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	aholler@anycorp.com
3/7/2016 4:00:51 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	abataglia@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	halbert@anycorp.com
3/7/2016 4:00:47 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	myeoman@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	wtobadilla@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lkam@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	jcooka@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	cpolice@anycorp.com
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	mwagener@anycorp.com
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	btear@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@sobergill.com	btear@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	labon@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	loller@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kuillams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	rponds@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	tshek@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kmerson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lslaughter@anycorp.com
3/7/2016 4:00:36 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	glyos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	delivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	malstunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	dfitz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	loekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	starimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	jmdicathy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lgomey@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lbenware@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	cgalfredu@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	epearney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kmatheus@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	oxalts@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ckrocker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kifandno@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	cpuzles@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	monvig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lnady@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ntamling@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	adlabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	jkingbury@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@sobergirl.com	bsen@anycorp.com
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	itabor@anycorp.com
3/7/2016 4:00:48 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	laker@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	kuillemo@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	rpounds@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	tsheck@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	kmerson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	tslaughter@anycorp.com
3/7/2016 4:00:36 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	glenn@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	delivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	malstunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	drftz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	lozekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	starimeto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	jrukahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	lgmney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	flennare@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	cgelpesu@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	apeervey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	knutthews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	csaffi@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	ckrocker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	klrlantins@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	cpulioe@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	hgarkh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	moniq@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	bnatty@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	rtorin@anycorp.com
3/7/2016 4:00:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	jee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	adffabio@anycorp.com
3/7/2016 4:00:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergirl.com	kingibury@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	72.154.64.106	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	124.140.200.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:49 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	31181	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	183.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62613	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.tlapia.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.tlapia.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 4:00:45 PM	192.168.0.24	50582	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:00:00 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 4:06:14 PM	192.168.0.254	55947	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tlapia.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.tlapia.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	bestpurchasa.com	GET
3/7/2016 3:57:03 PM	192.168.0.27	46987	23.93.170.116	80	goodguys.se	POST
3/7/2016 3:56:14 PM	192.168.0.211	31442	168.83.234.163	80	visitorcenter.com	GET
3/7/2016 3:54:31 PM	192.168.0.152	30520	141.217.181.243	80	goodguys.se	POST
3/7/2016 3:52:47 PM	192.168.0.253	36463	79.115.291.191	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	152.263.213.16	80	thelastwebpage.com	GET
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET
3/7/2016 3:39:43 PM	192.168.0.128	44304	180.208.164.237	443	searchforus.de	GET
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET
3/7/2016 3:36:59 PM	192.168.0.95	34447	133.136.173.36	80	anti-malware.com	GET
3/7/2016 3:36:38 PM	192.168.0.177	38187	100.3.194.158	80	healthreport.com	GET
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.258.143.104	80	freefood.com	POST

SIEM Logs - SIEM 192.168.0.15								
Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited	192.168.0.134	asmith	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	Login	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	kmathews	1234	malclient.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	Login	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	1089	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Login	An account was successfully logged on	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Login	An account was successfully logged on	192.168.0.134	asmith	1503	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Login	An account was successfully logged on	192.168.0.70	cpuziss	636	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 4:11:26 PM	4634	Logoff	An account was logged off	192.168.0.141	dfritz	1031	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Login	An account was successfully logged on	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited	192.168.0.24	jlee	635	explorer.exe

SIEM Logs - SIEM 192.168.0.15								
Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited	192.168.0.134	asmith	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	Login	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	kmathews	1234	malclient.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	Login	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	1089	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Login	An account was successfully logged on	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Login	An account was successfully logged on	192.168.0.134	asmith	1503	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Login	An account was successfully logged on	192.168.0.70	cpuziss	636	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 4:11:26 PM	4634	Logoff	An account was logged off	192.168.0.141	dfritz	1031	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Login	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 99

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

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

Answer: A

#### Explanation:

The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server's data and state at a specific point in time. Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

#### NEW QUESTION 101

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

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

## Money Back Guarantee

### 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