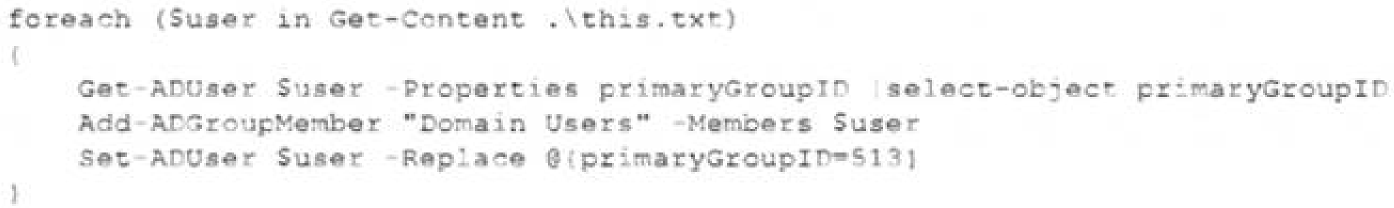
CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

NEW QUESTION 1
A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:



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

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

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

Answer: A

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

NEW QUESTION 2
A 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 3
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 4
A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

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

Answer: B

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

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

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

Answer: C

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

NEW QUESTION 7
A security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM. The analyst no longer had to jump between tools. Which of the following best describes what the security program did?

A. Data enrichment
B. Security control plane
C. Threat feed combination
D. Single pane of glass

Answer: D

Explanation:
A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems. A single pane of glass can also help reduce complexity, improve efficiency, and enhance decision making for security analysts. In this case, a security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM, which provides a single pane of glass for security operations. Official References:
https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack

NEW QUESTION 8
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 9
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 10
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/

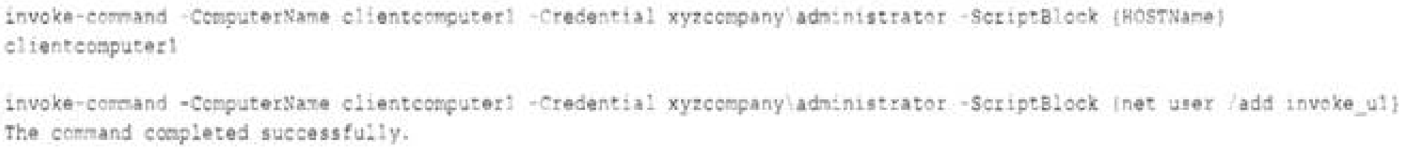
NEW QUESTION 10
Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

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

Answer: A

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

NEW QUESTION 11
The analyst reviews the following endpoint log entry:



```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {HOSTName}
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

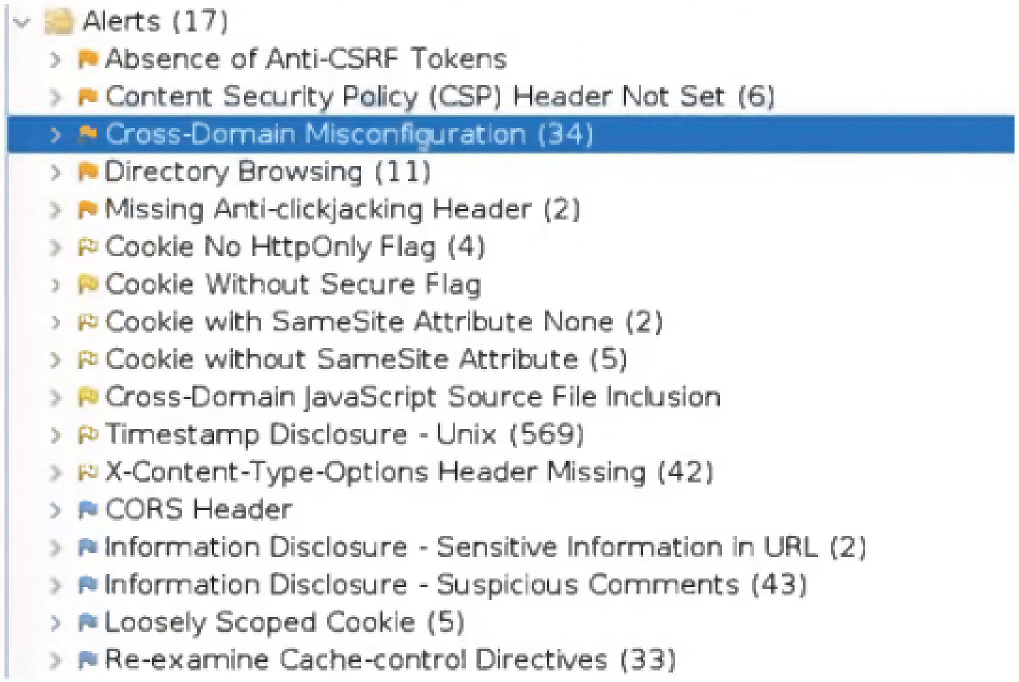
Which of the following has occurred?

A. Registry change
B. Rename computer
C. New account introduced
D. Privilege escalation

Answer: C

Explanation:
The endpoint log entry shows that a new account named “admin” has been created on a Windows system with a local group membership of “Administrators”. This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

NEW QUESTION 15
An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



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

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

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

Answer: B

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

NEW QUESTION 17
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 19
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 22

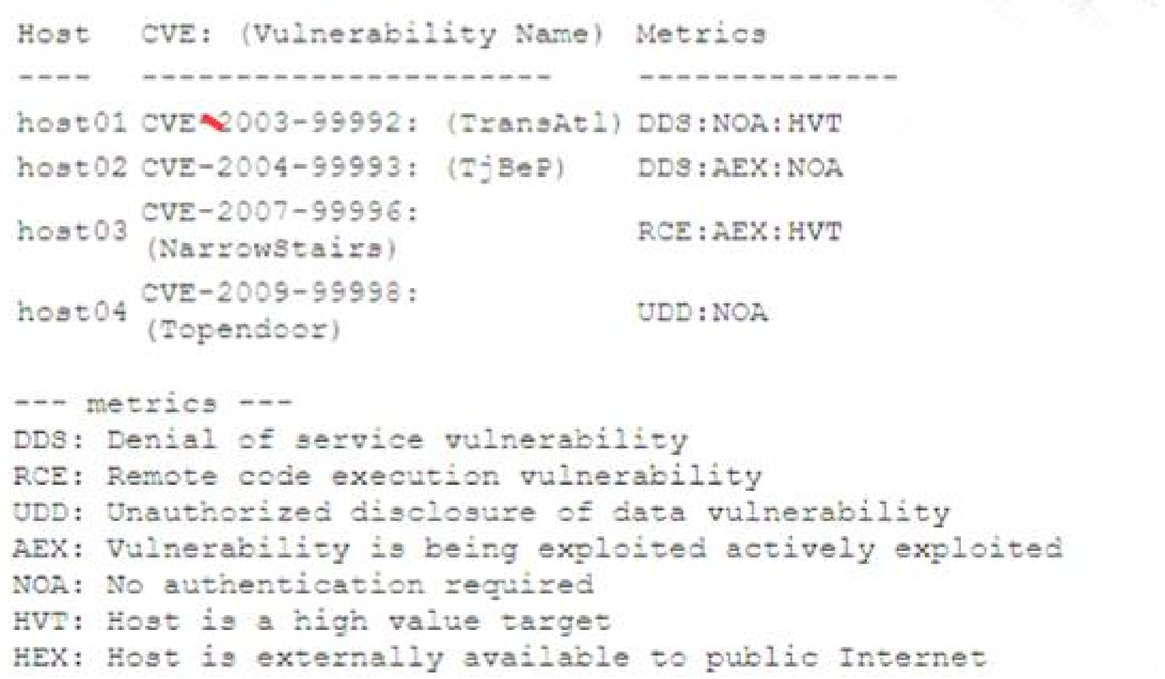
A Chief Information Security Officer (CISO) is concerned that a specific threat actor who is known to target the company's business type may be able to breach the network and remain inside of it for an extended period of time.
Which of the following techniques should be performed to meet the CISO's goals?

A. Vulnerability scanning
B. Adversary emulation
C. Passive discovery
D. Bug bounty

Answer: B

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

NEW QUESTION 23
A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:



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

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

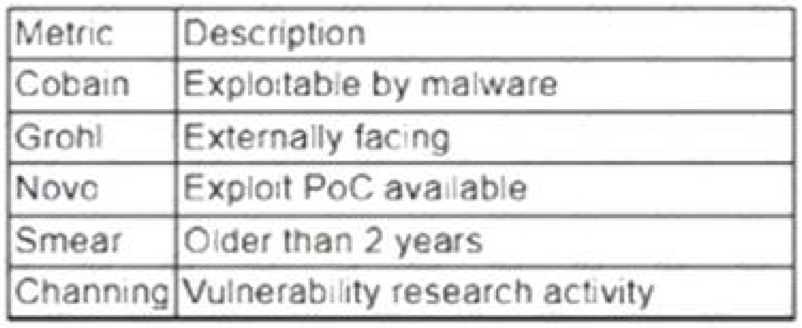
Which of the following hosts should be patched first, based on the metrics?

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

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 27
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 30
A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to https://offce365password.acme.co. The site's standard VPN logon page is
www.acme.com/logon. Which of the following is most likely true?

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

Answer: D

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

NEW QUESTION 32
Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

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

Answer: D

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

NEW QUESTION 36
Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H
Which of the following attributes correctly describes this vulnerability?

A. A user is required to exploit this vulnerability.
B. The vulnerability is network based.
C. The vulnerability does not affect confidentiality.
D. The complexity to exploit the vulnerability is high.

Answer: B

Explanation:
The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system

NEW QUESTION 37
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 40
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 43
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 47
A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

A. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
B. function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }
C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
D. function x() { info=$(traceroute -m 40 $1 | awk ‘END{print $1}’) && echo "$1 | $info" }

Answer: C

Explanation:
The function that can be used on a shell script to identify anomalies on the network routing most accurately is: function x() { info=(dig(dig -x $1 | grep PTR | tail -n 1 | awk -F “.in-addr” '{print $1} ').origin.asn.cymru.com
TXT +short) && echo “$1 | $info” }
This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

NEW QUESTION 48
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 53
Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

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

Answer: A

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

NEW QUESTION 58
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 63
An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

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

Answer: A

Explanation:
SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level

Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

NEW QUESTION 68
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 70
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 74
A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

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

Answer: A

Explanation:
Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:

- Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
- Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
- Reporting any suspicious or anomalous activity to the security team or the appropriate authority
- Following the organization’s policies and procedures on security awareness and best practices

Official References:

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

NEW QUESTION 79
A security analyst must preserve a system hard drive that was involved in a litigation request Which of the following is the best method to ensure the data on the device is not modified?

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

Answer: A

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

NEW QUESTION 80
A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

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

Answer: D

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

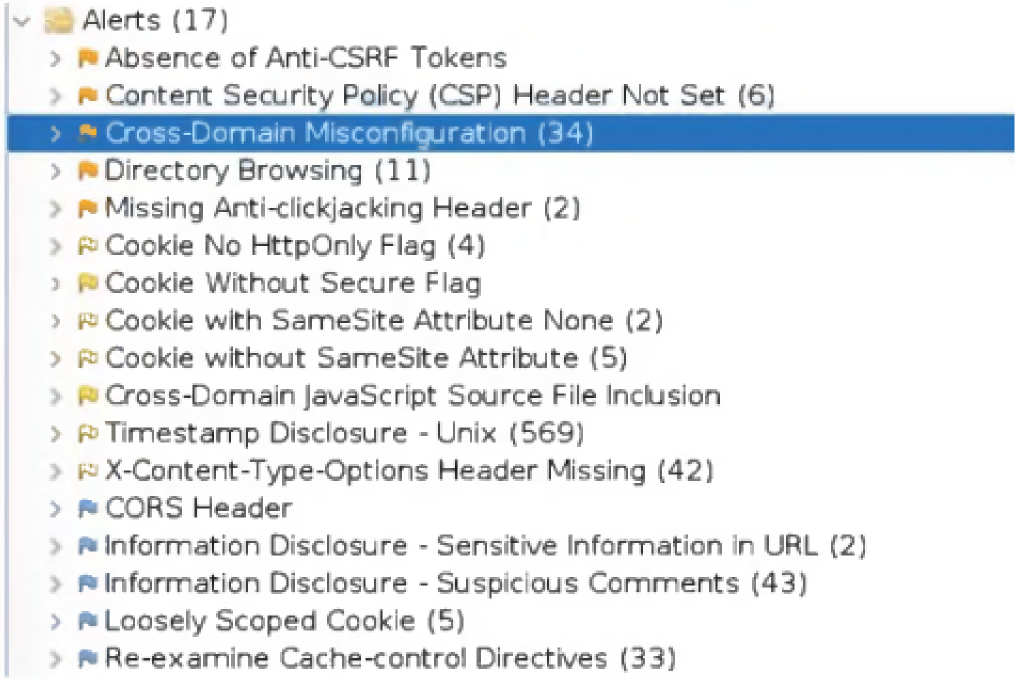
NEW QUESTION 81
New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

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

Answer: D

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

NEW QUESTION 86
An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



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

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

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

Answer: C

Explanation:
The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions.
The tuning recommendation is to configure the Access-Control-Allow-Origin header to only allow authorized domains that need to access the web application's resources. This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.

NEW QUESTION 91
Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

A. The lead should review what is documented in the incident response policy or plan
B. Management level members of the CSIRT should make that decision
C. The lead has the authority to decide who to communicate with at any t me
D. Subject matter experts on the team should communicate with others within the specified area of expertise

Answer: A

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

NEW QUESTION 92
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 97
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 102
A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

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

Answer: A

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

NEW QUESTION 106
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

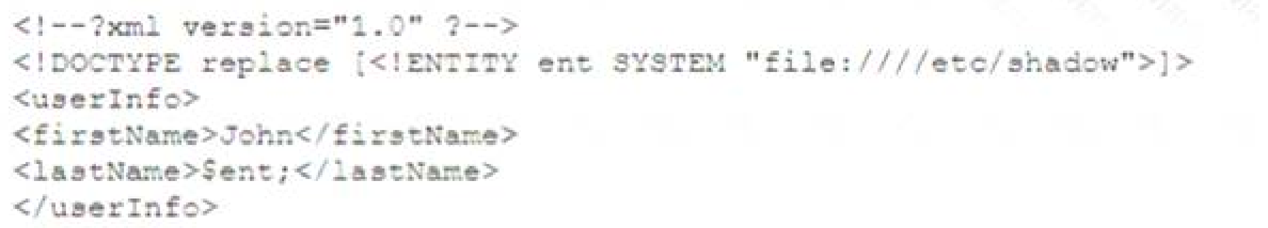
NEW QUESTION 108
A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

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

Answer: B

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

NEW QUESTION 113
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

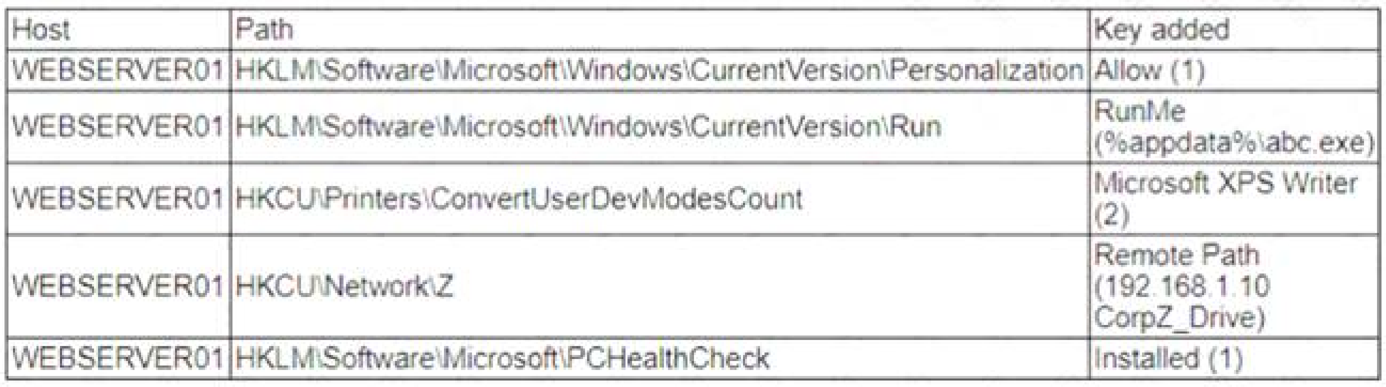
NEW QUESTION 117
Which of the following is a reason why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

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

Answer: A

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

NEW QUESTION 118
A security analyst is reviewing the following alert that was triggered by FIM on a critical system:



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

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

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

Answer: C

Explanation:
A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named “update.exe” in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official References:
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/training/books/cysa-cs0-002-study-guide

NEW QUESTION 120
An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate
as the reason for this escalation?

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

Answer: B

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

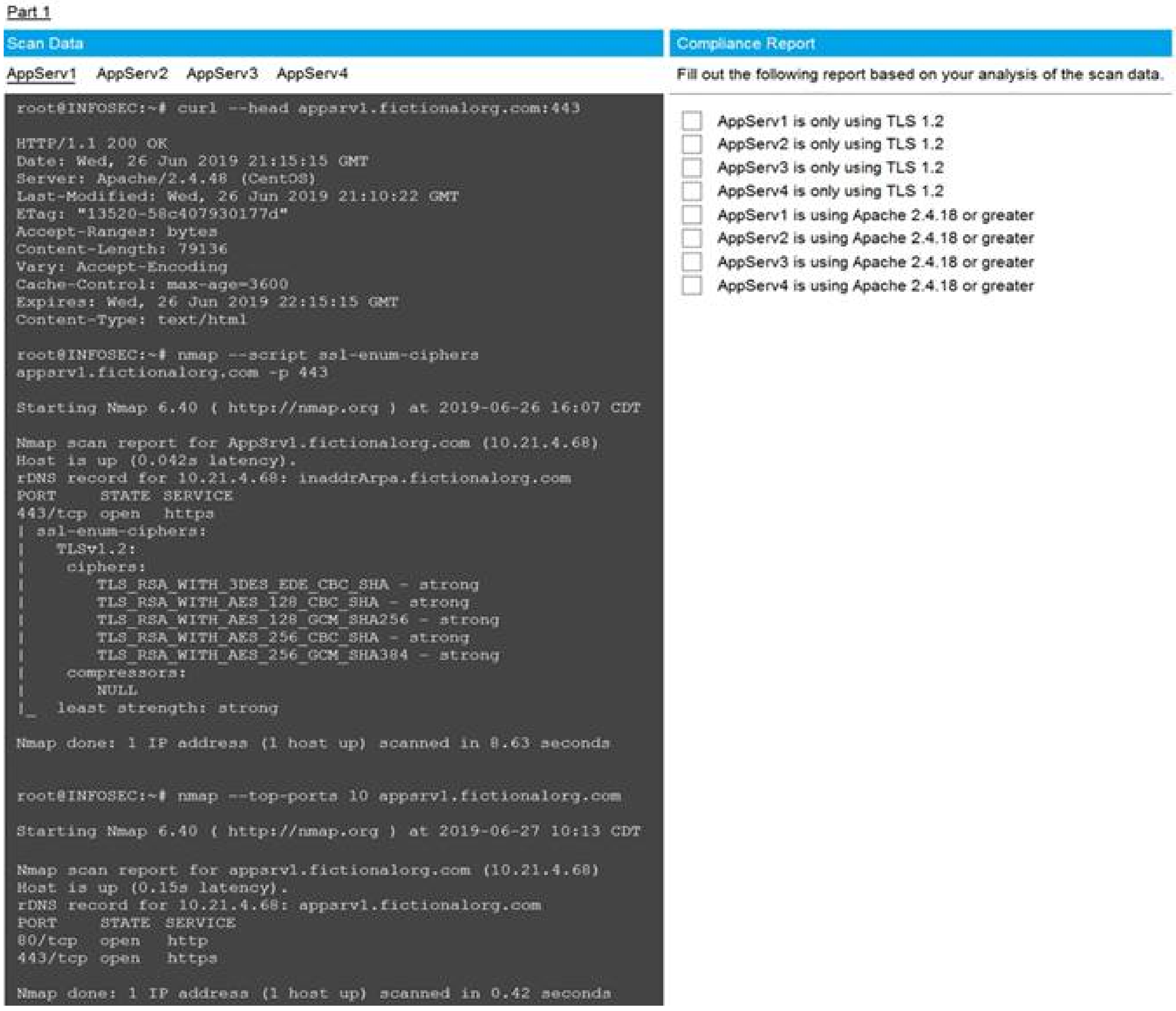
NEW QUESTION 124
A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

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

Answer: C

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

NEW QUESTION 128
You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.
The company's hardening guidelines indicate the following
• TLS 1.2 is the only version of TLS running.
• Apache 2.4.18 or greater should be used.
• Only default ports should be used.
INSTRUCTIONS
Using the supplied data, record the status of compliance with the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for Issues based ONLY on the hardening guidelines provided.
Part 1:
AppServ1:

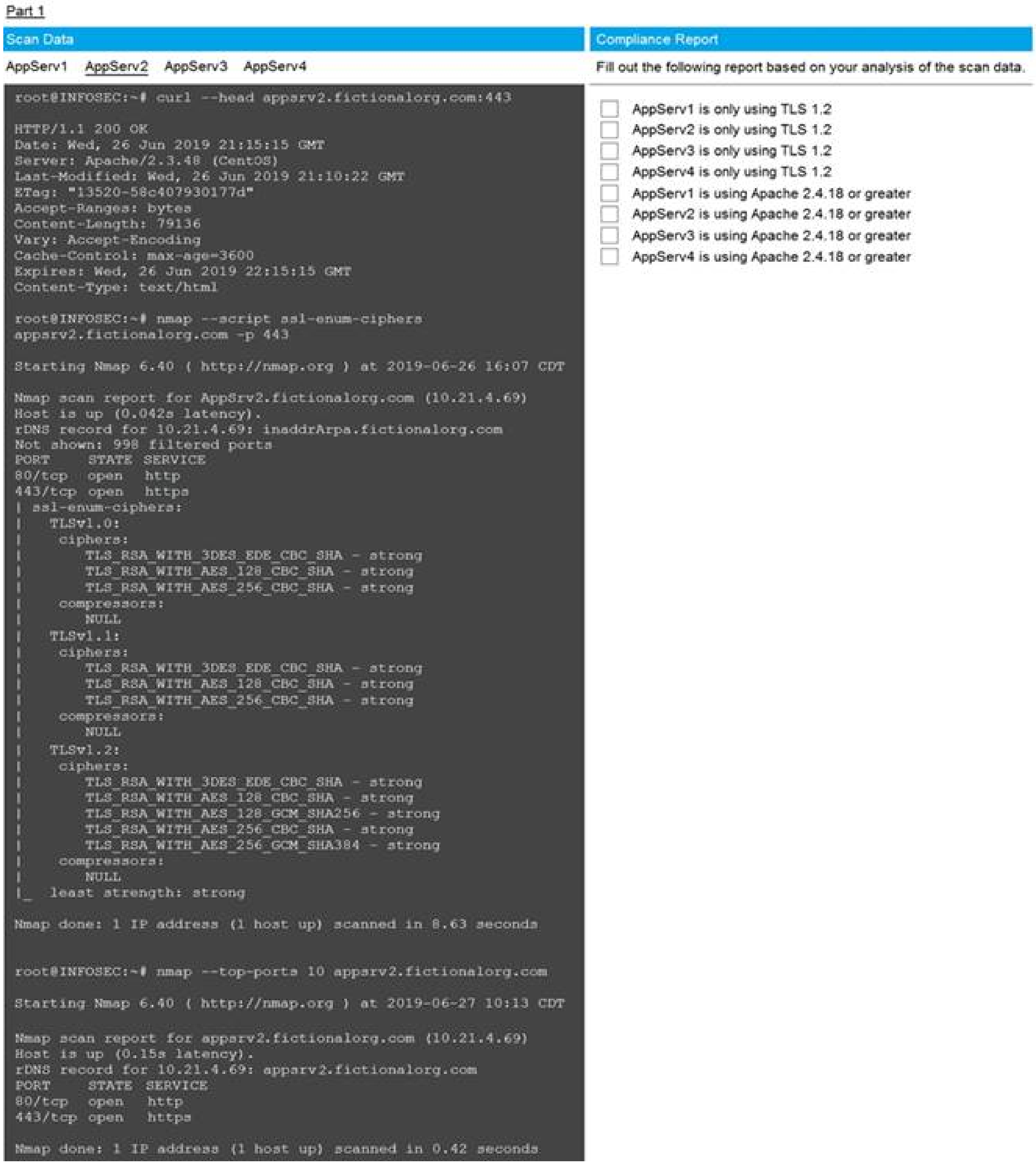


```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

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

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

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

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT     STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
|_  least strength: strong

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


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT     STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

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

□ AppServ1 is only using TLS 1.2
□ AppServ2 is only using TLS 1.2
□ AppServ3 is only using TLS 1.2
□ AppServ4 is only using TLS 1.2
□ AppServ1 is using Apache 2.4.18 or greater
□ AppServ2 is using Apache 2.4.18 or greater
□ AppServ3 is using Apache 2.4.18 or greater
□ AppServ4 is using Apache 2.4.18 or greater

AppServ2:



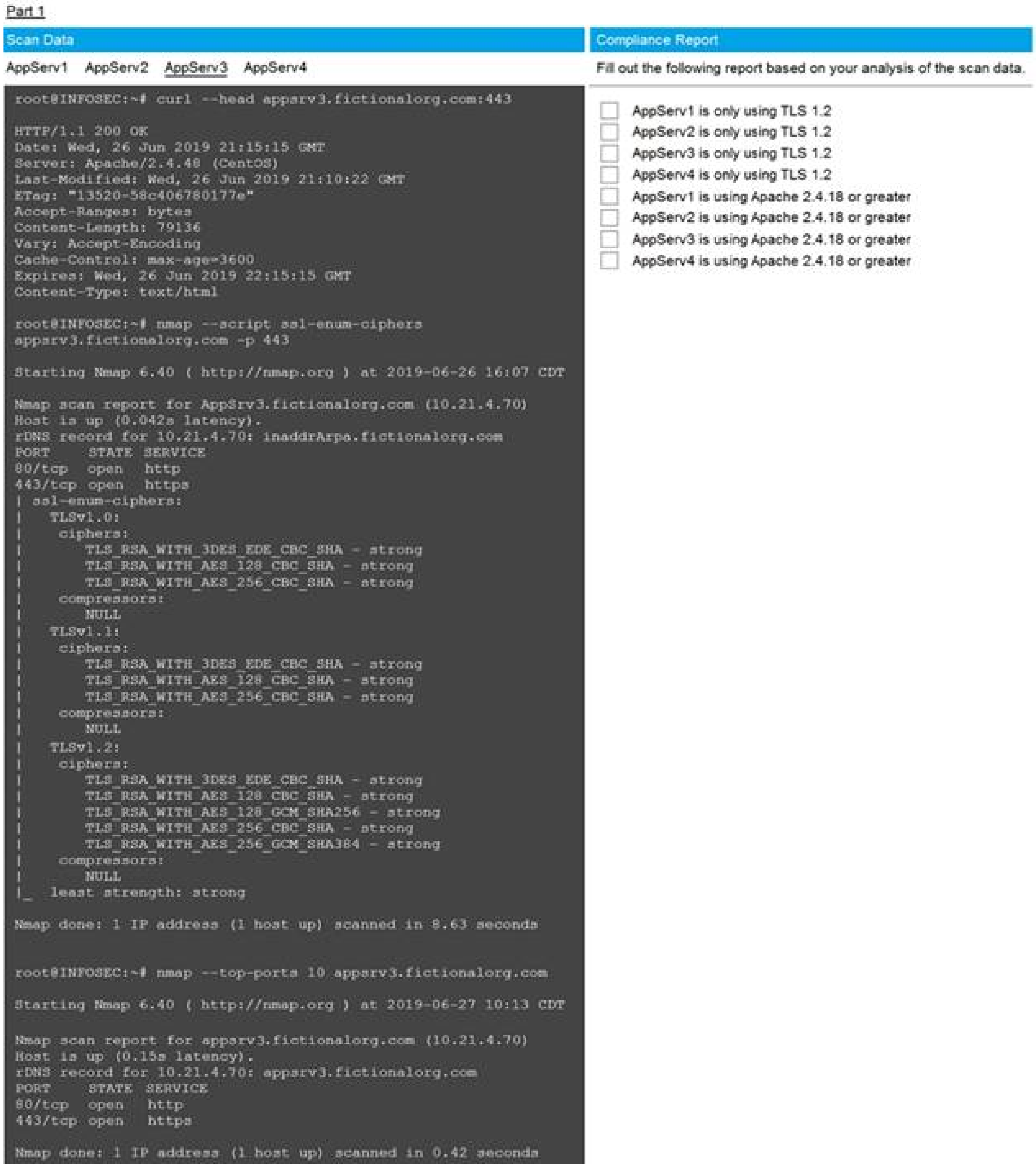
Part 1

```
root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

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

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

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

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
| ssl-enum-ciphers:
|    TLSv1.0:
|     ciphers:
|        TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|        TLS_RSA_WITH_AES_128_CBC_SHA - strong
|        TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|        NULL
|    TLSv1.1:
|     ciphers:
|        TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|        TLS_RSA_WITH_AES_128_CBC_SHA - strong
|        TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|        NULL
|    TLSv1.2:
|     ciphers:
|        TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|        TLS_RSA_WITH_AES_128_CBC_SHA - strong
|        TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|        TLS_RSA_WITH_AES_256_CBC_SHA - strong
|        TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|        NULL
|_   least strength: strong

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


root@INFOSEC:~# nmap --top-ports 10 appsrv2.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv2.fictionalorg.com (10.21.4.69)
Host is up (0.15s latency).
rDNS record for 10.21.4.69: appsrv2.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

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

- □ AppServ1 is only using TLS 1.2
- □ AppServ2 is only using TLS 1.2
- □ AppServ3 is only using TLS 1.2
- □ AppServ4 is only using TLS 1.2
- □ AppServ1 is using Apache 2.4.18 or greater
- □ AppServ2 is using Apache 2.4.18 or greater
- □ AppServ3 is using Apache 2.4.18 or greater
- □ AppServ4 is using Apache 2.4.18 or greater

AppServ3:



Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

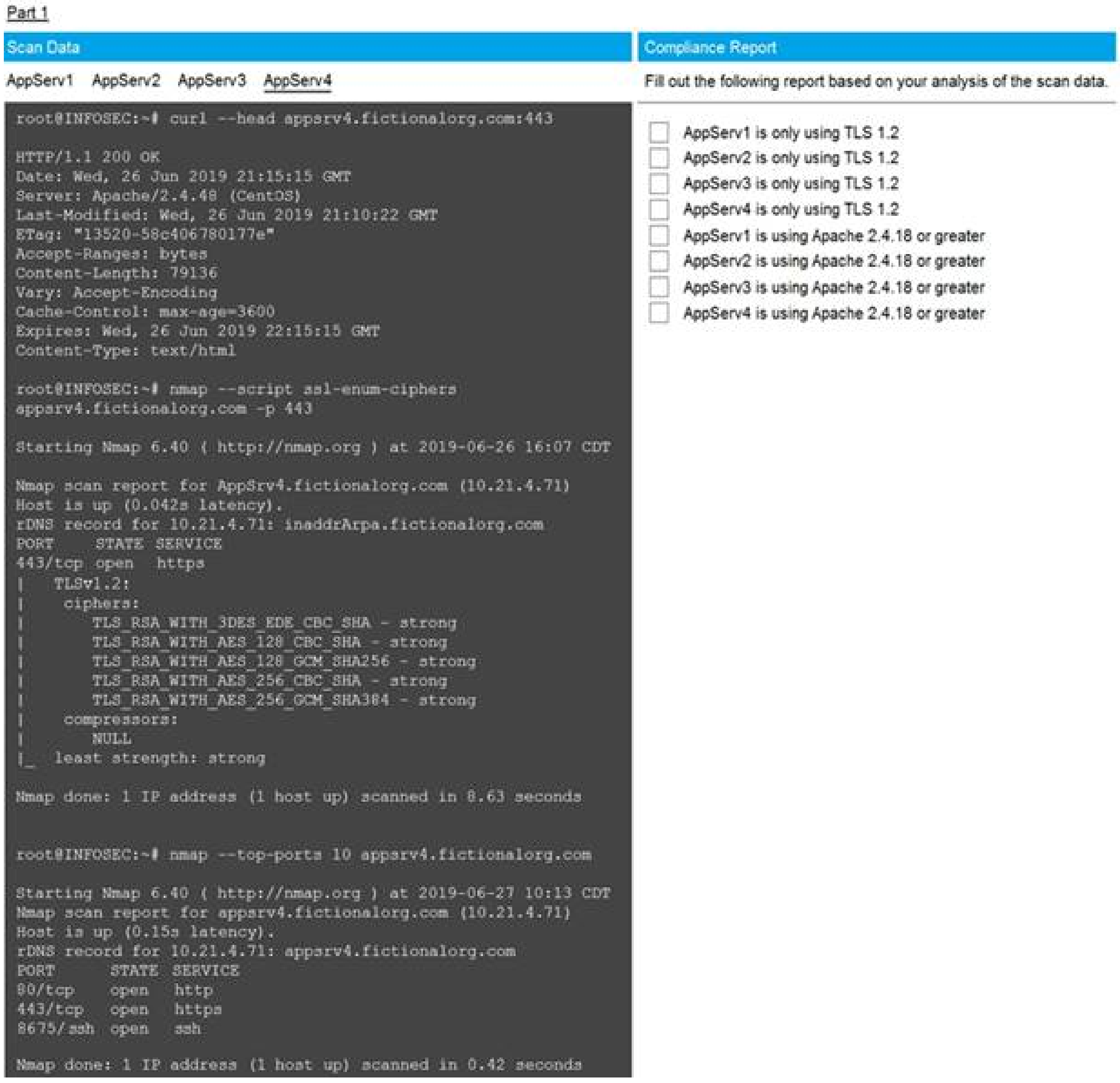
```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

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

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

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

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT     STATE SERVICE
80/tcp   open  http
443/tcp open   https
| ssl-enum-ciphers:
|   TLSv1.0:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|    compressors:
|       NULL
|   TLSv1.1:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|    compressors:
|       NULL
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
|_  least strength: strong

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


root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT     STATE SERVICE
80/tcp   open   http
443/tcp  open   https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

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

□ AppServ1 is only using TLS 1.2
□ AppServ2 is only using TLS 1.2
□ AppServ3 is only using TLS 1.2
□ AppServ4 is only using TLS 1.2
□ AppServ1 is using Apache 2.4.18 or greater
□ AppServ2 is using Apache 2.4.18 or greater
□ AppServ3 is using Apache 2.4.18 or greater
□ AppServ4 is using Apache 2.4.18 or greater

AppServ4:



Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

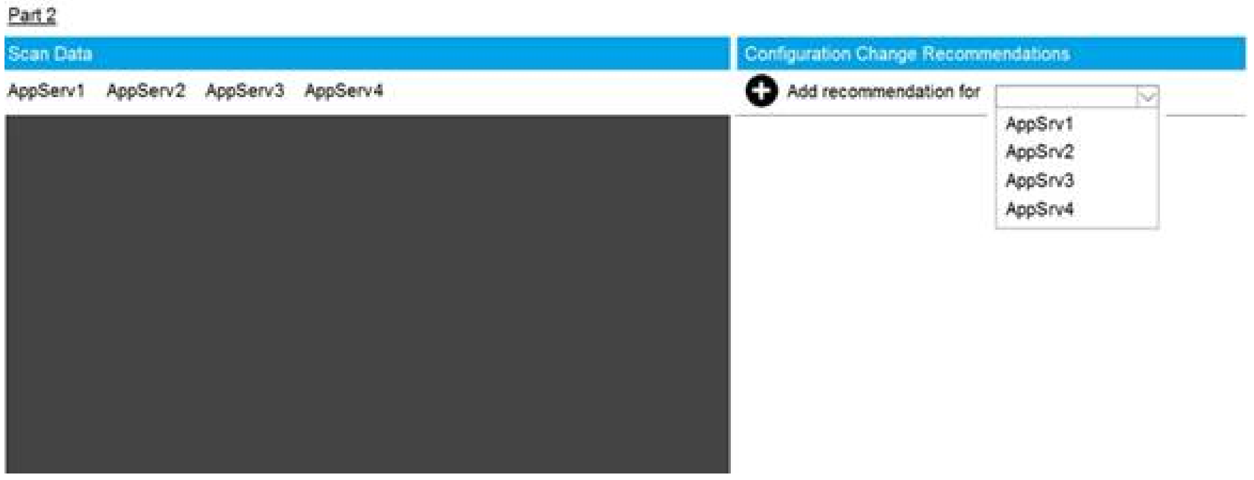
```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443

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

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

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

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
PORT     STATE SERVICE
443/tcp open   https
|   TLSv1.2:
|    ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|    compressors:
|       NULL
|_  least strength: strong

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


root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT       STATE  SERVICE
80/tcp     open   http
443/tcp    open   https
8675/ssh   open   ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

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

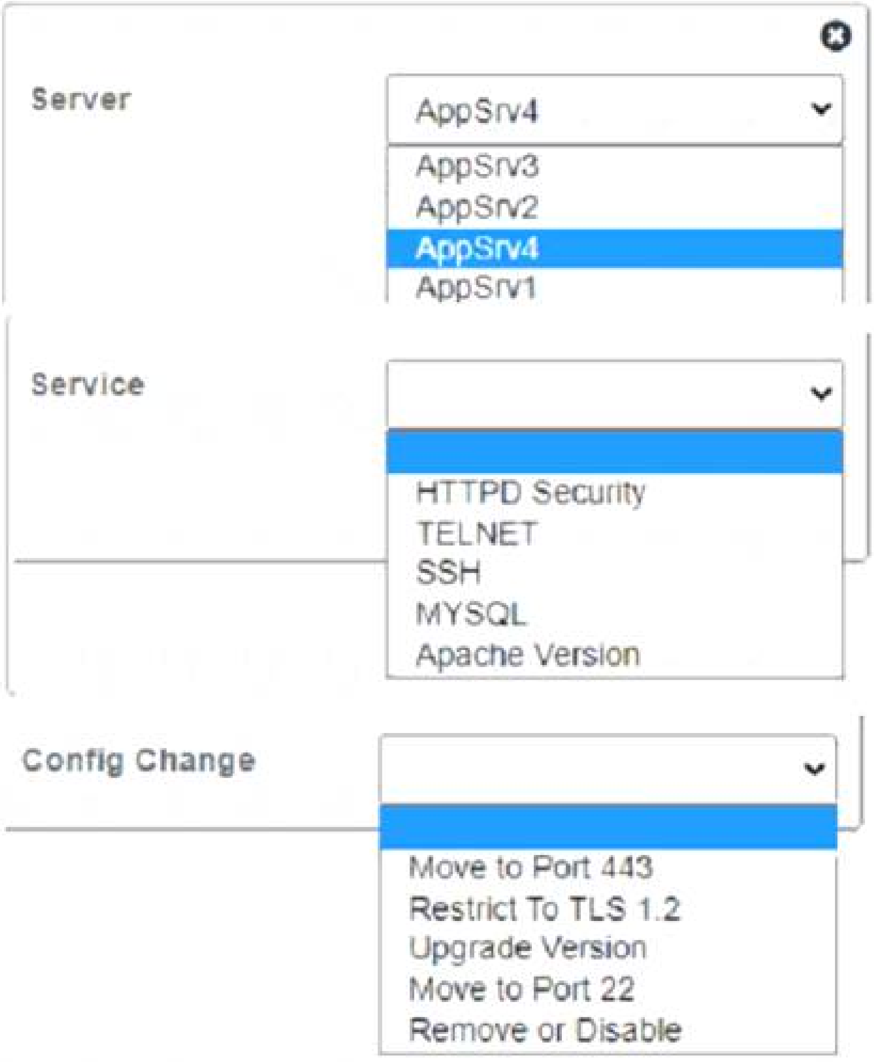
□ AppServ1 is only using TLS 1.2
□ AppServ2 is only using TLS 1.2
□ AppServ3 is only using TLS 1.2
□ AppServ4 is only using TLS 1.2
□ AppServ1 is using Apache 2.4.18 or greater
□ AppServ2 is using Apache 2.4.18 or greater
□ AppServ3 is using Apache 2.4.18 or greater
□ AppServ4 is using Apache 2.4.18 or greater

Part 2:



Part 2

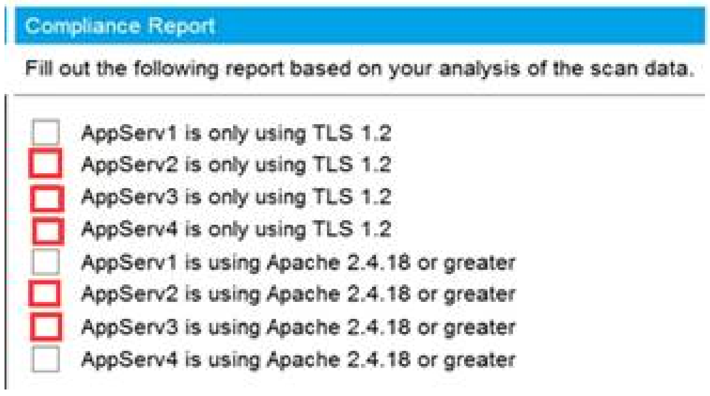
Scan Data
AppServ1 AppServ2 AppServ3 AppServ4
Configuration Change Recommendations
Add recommendation for
AppSrv1
AppSrv2
AppSrv3
AppSrv4



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1:



Compliance Report

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

□ AppServ1 is only using TLS 1.2
[✓ □] AppServ2 is only using TLS 1.2
[✓ □] AppServ3 is only using TLS 1.2
[✓ □] AppServ4 is only using TLS 1.2
□ AppServ1 is using Apache 2.4.18 or greater
[✓ □] AppServ2 is using Apache 2.4.18 or greater
[✓ □] AppServ3 is using Apache 2.4.18 or greater
□ AppServ4 is using Apache 2.4.18 or greater

Part 2:
Based on the compliance report, I recommend the following changes for each server: AppServ1: No changes are needed for this server.
AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server.
Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.
AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.
AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

NEW QUESTION 129
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 132
An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

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

Answer: A

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

NEW QUESTION 134
An organization was compromised, and the usernames and passwords of all em-ployees 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)?]

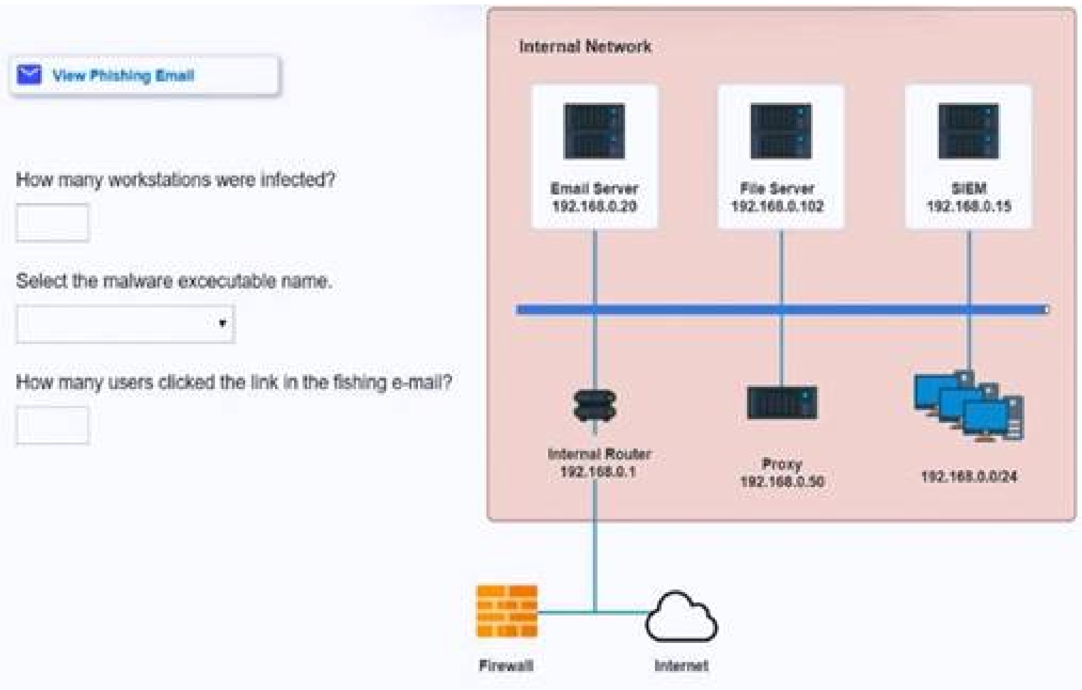
NEW QUESTION 138
A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

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.

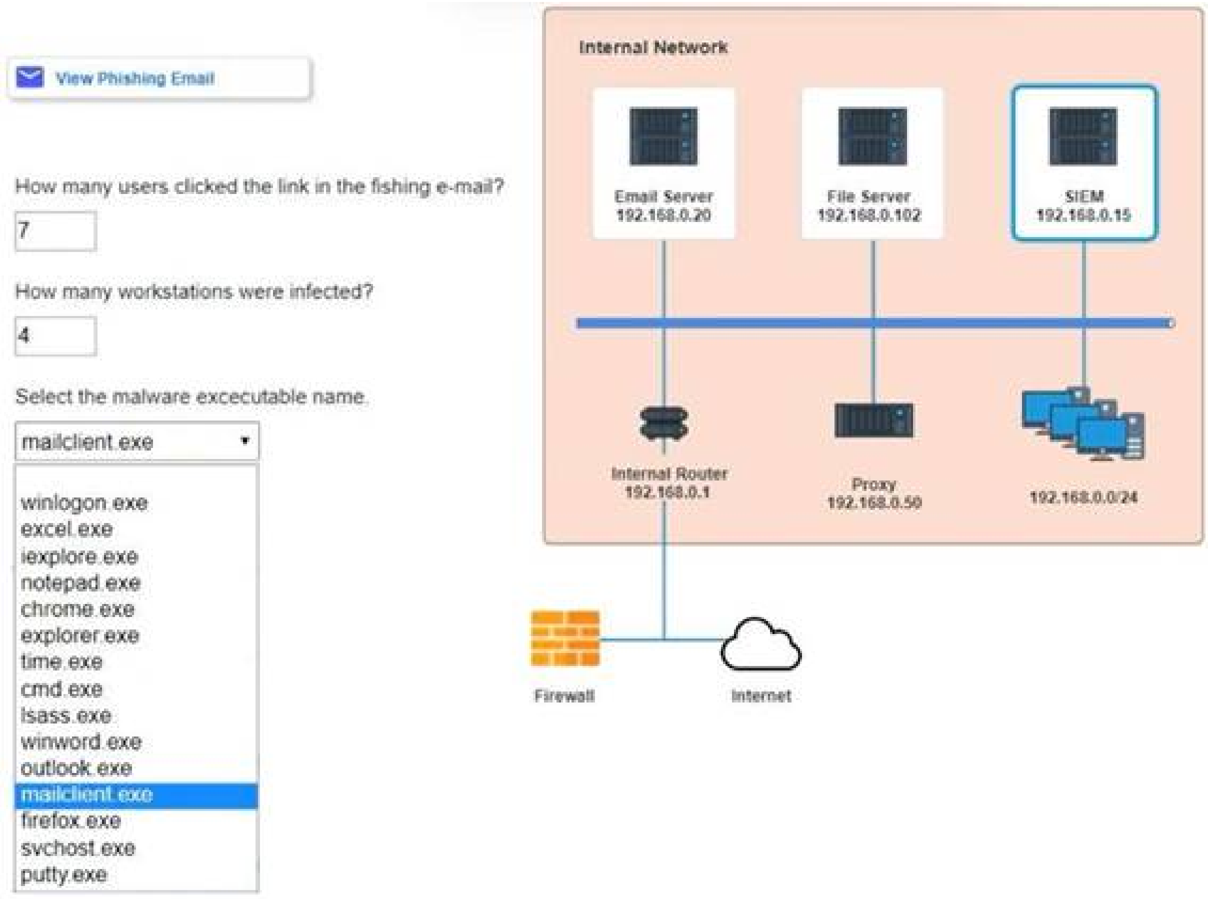
NEW QUESTION 141
Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.
Review the information provided and determine the following:
* 1. HOW many employees Clicked on the link in the Phishing email?
* 2. on how many workstations was the malware installed?
* 3. what is the executable file name of the malware?



How many workstations were infected?

Select the malware excecutable name.

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



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

7

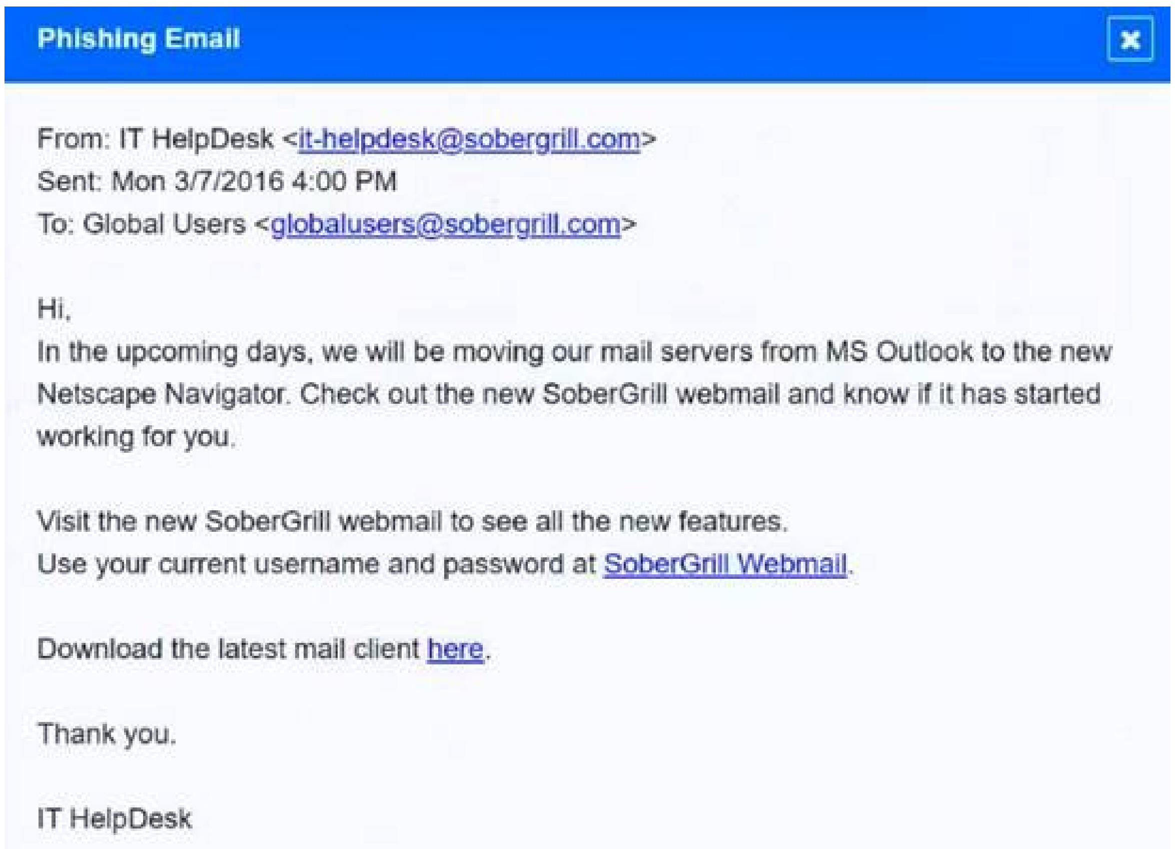
How many workstations were infected?

4

Select the malware excecutable name.

mailclient.exe ▾

- 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



Phishing Email ☒

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

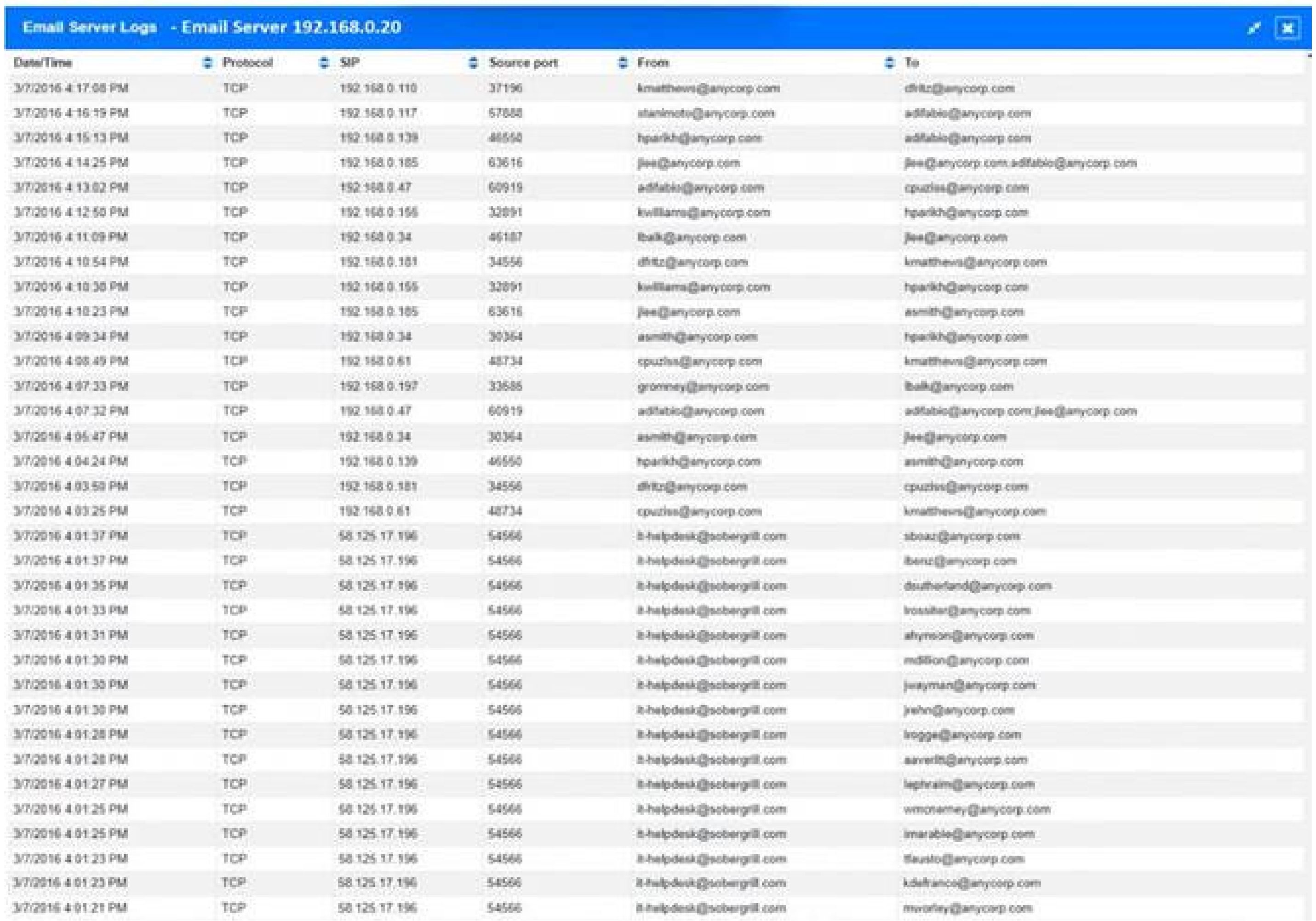
Hi,
In the upcoming days, we will be moving our mail servers from MS Outlook to the new Netscape Navigator. Check out the new SoberGrill webmail and know if it has started working for you.

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.

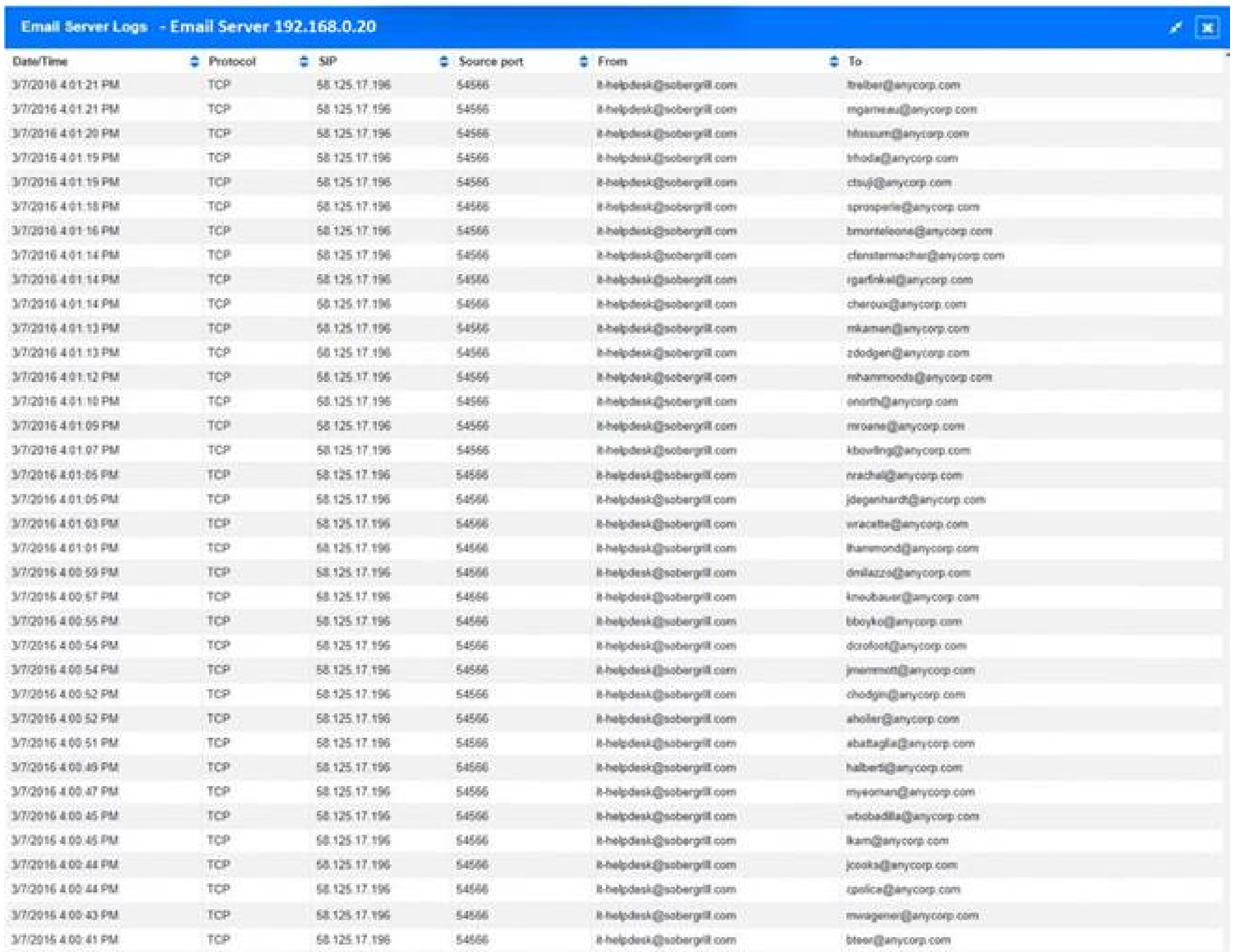
Thank you.

IT HelpDesk



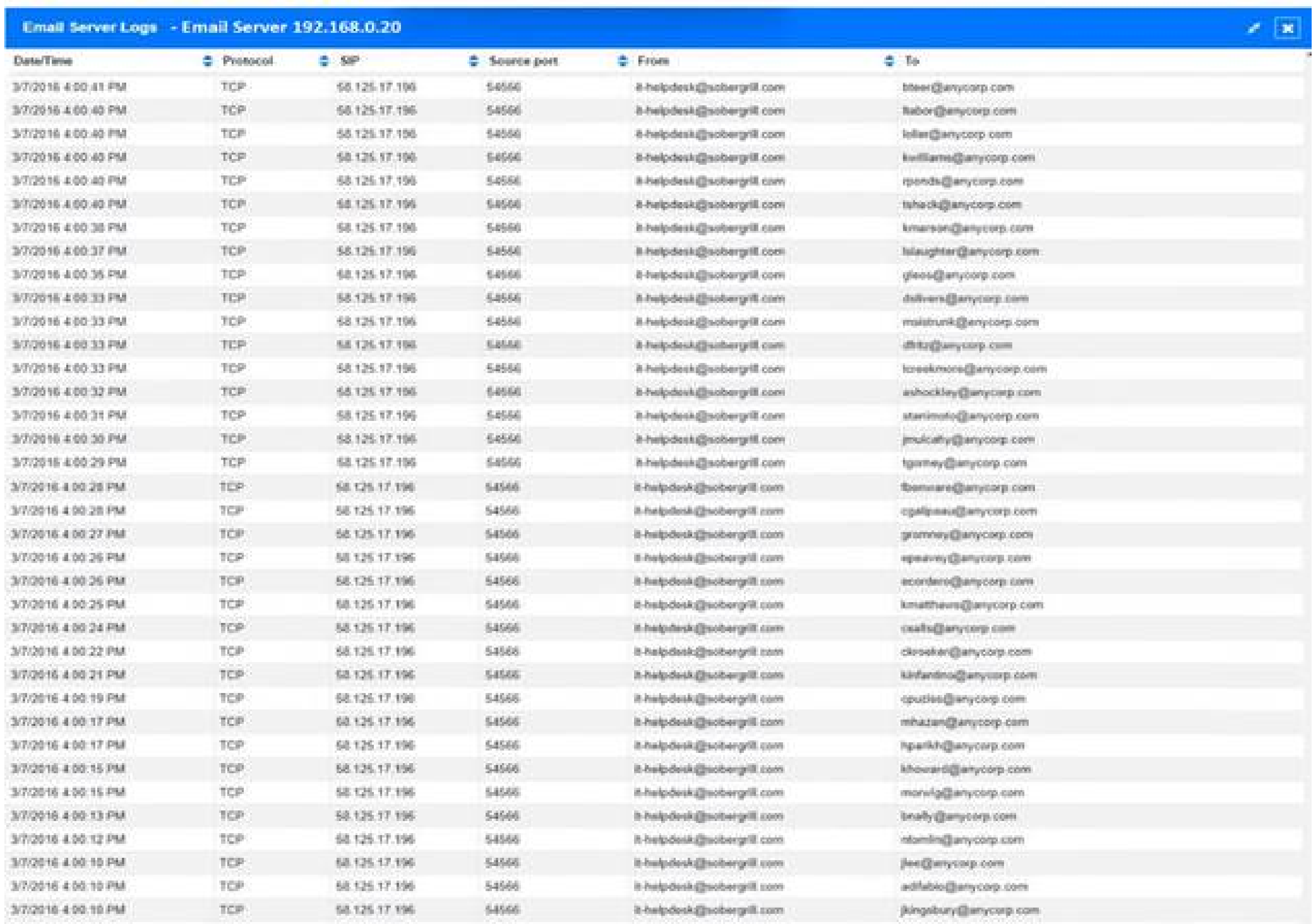
Email Server Logs - Email Server 192.168.0.20

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	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:30 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 4:03:50 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sboaz@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lbenz@anycorp.com
3/7/2016 4:01:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsutherland@anycorp.com
3/7/2016 4:01:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrossiter@anycorp.com
3/7/2016 4:01:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	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	lrogge@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aaverill@anycorp.com
3/7/2016 4:01:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lephraim@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wmcnerney@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lmarable@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



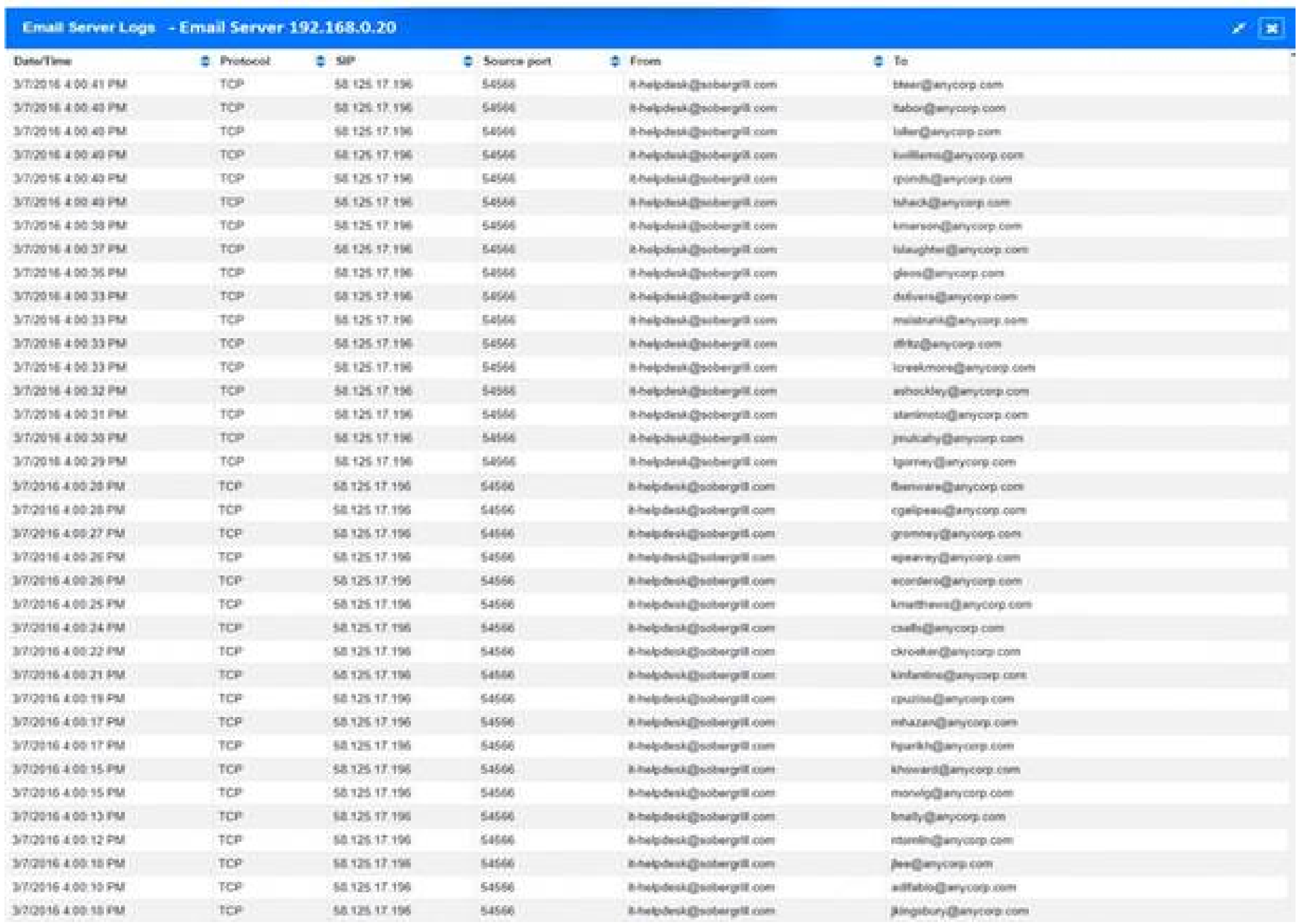
Email Server Logs - Email Server 192.168.0.20

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



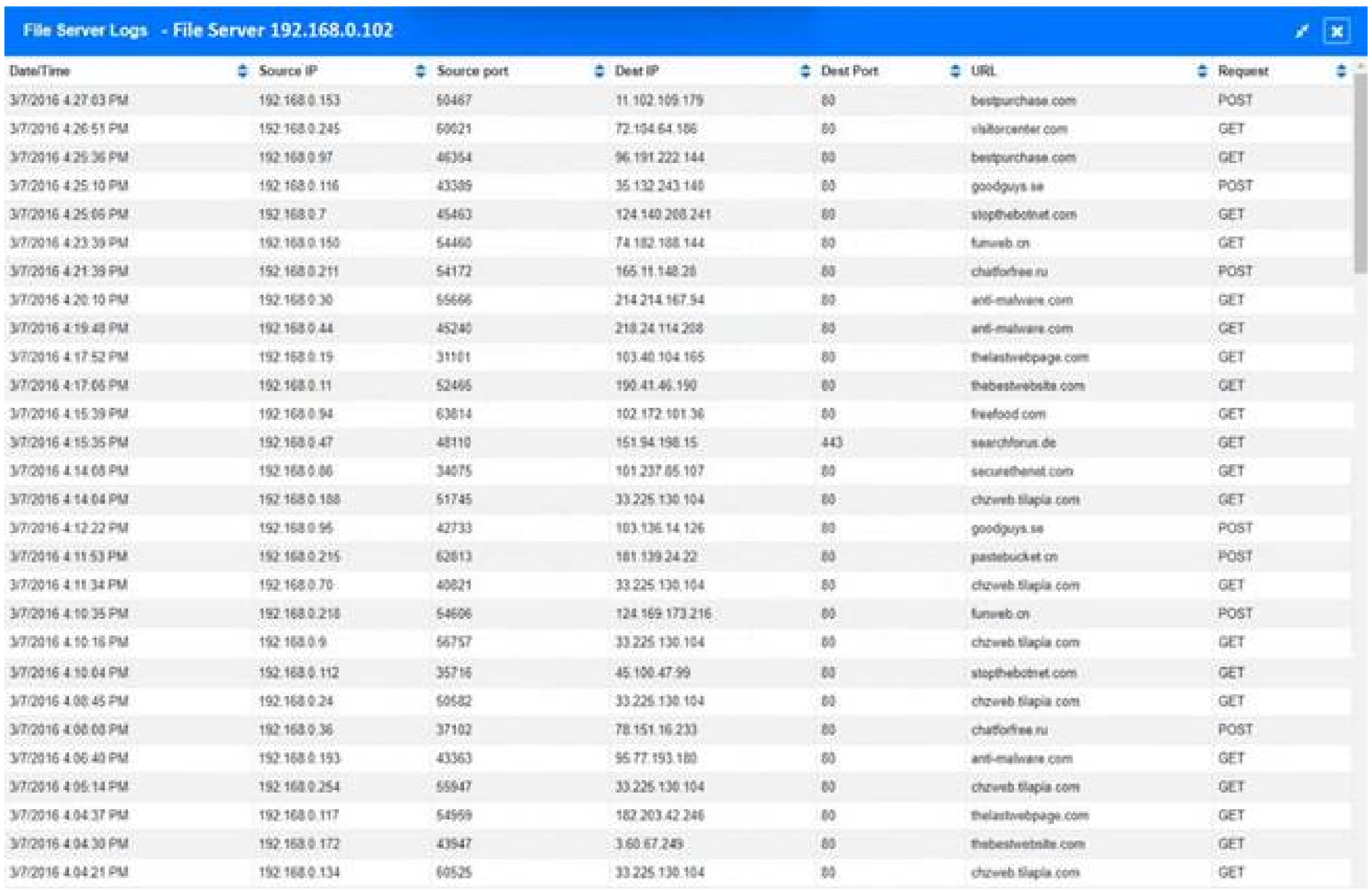
Email Server Logs - Email Server 192.168.0.20

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



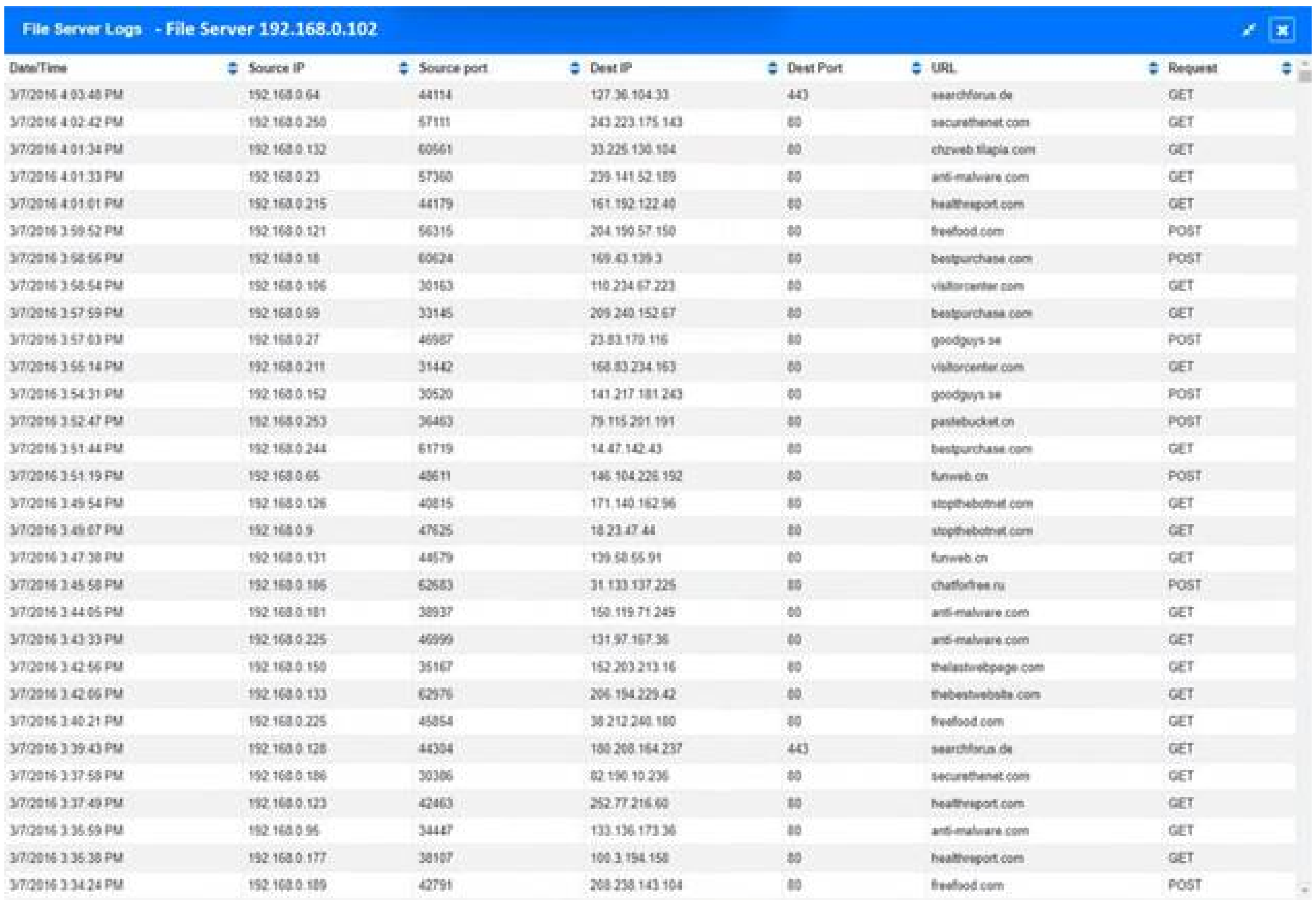
Email Server Logs - Email Server 192.168.0.20

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



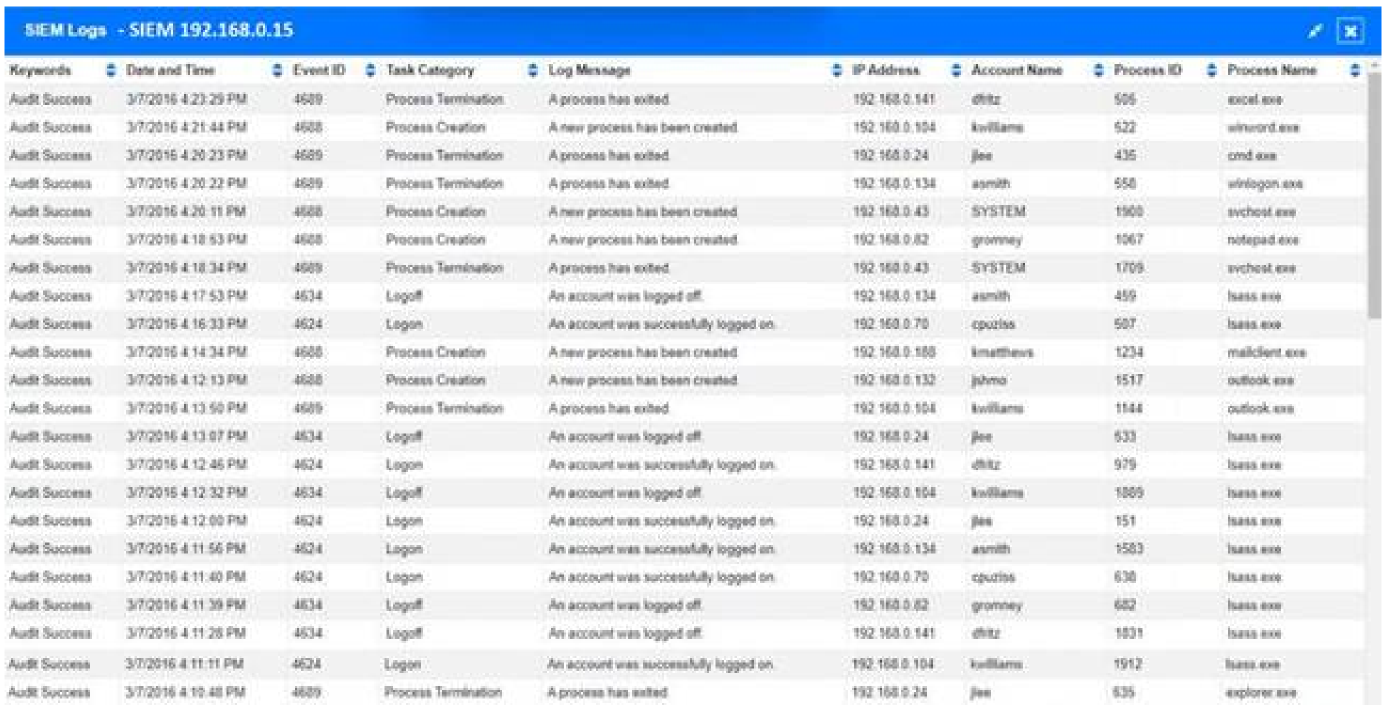
File Server Logs - File Server 192.168.0.102

Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	60467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.108.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.96	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST
3/7/2016 4:10:16 PM	192.168.0.9	56757	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:04 PM	192.168.0.112	35716	45.100.47.99	80	stopthebotnet.com	GET
3/7/2016 4:08:45 PM	192.168.0.24	50582	33.226.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:08:08 PM	192.168.0.36	37102	78.151.16.233	80	chatforfree.ru	POST
3/7/2016 4:06:40 PM	192.168.0.193	43363	95.77.193.180	80	anti-malware.com	GET
3/7/2016 4:05:14 PM	192.168.0.254	55947	33.226.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tilapia.com	GET



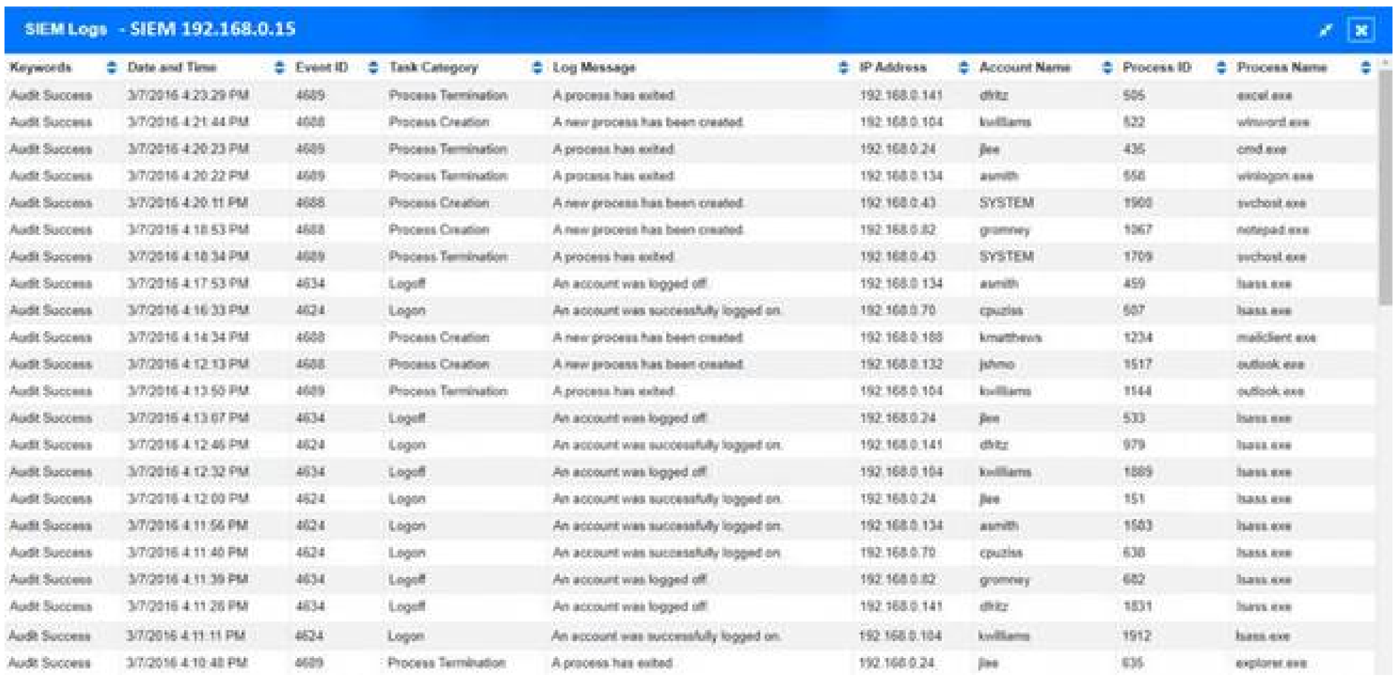
File Server Logs - File Server 192.168.0.102

Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:03:48 PM	192.168.0.64	44114	127.36.104.33	443	searchforus.de	GET
3/7/2016 4:02:42 PM	192.168.0.250	57111	243.223.175.143	80	securethenet.com	GET
3/7/2016 4:01:34 PM	192.168.0.132	60561	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:01:33 PM	192.168.0.23	57360	239.141.52.189	80	anti-malware.com	GET
3/7/2016 4:01:01 PM	192.168.0.215	44179	161.192.122.40	80	healthreport.com	GET
3/7/2016 3:59:52 PM	192.168.0.121	56315	204.150.57.150	80	freefood.com	POST
3/7/2016 3:58:56 PM	192.168.0.18	60624	169.43.139.3	80	bestpurchase.com	POST
3/7/2016 3:58:54 PM	192.168.0.106	30163	110.234.67.223	80	visitorcenter.com	GET
3/7/2016 3:57:59 PM	192.168.0.69	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 3:56:14 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	79.115.201.191	80	pastebucket.cn	POST
3/7/2016 3:51:44 PM	192.168.0.244	61719	14.47.142.43	80	bestpurchase.com	GET
3/7/2016 3:51:19 PM	192.168.0.65	48611	146.104.226.152	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	150.119.71.249	80	anti-malware.com	GET
3/7/2016 3:43:33 PM	192.168.0.225	46999	131.97.167.36	80	anti-malware.com	GET
3/7/2016 3:42:56 PM	192.168.0.150	35167	152.203.213.16	80	thelastwebpage.com	GET
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET
3/7/2016 3:39:43 PM	192.168.0.128	44304	180.208.164.237	443	searchforus.de	GET
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET
3/7/2016 3:36:59 PM	192.168.0.96	34447	133.136.173.36	80	anti-malware.com	GET
3/7/2016 3:36:38 PM	192.168.0.177	38107	100.3.194.158	80	healthreport.com	GET
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.238.143.104	80	freefood.com	POST



SIEM Logs - SIEM 192.168.0.15

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	506	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.160.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.160.0.70	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.	192.160.0.104	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.	192.160.0.70	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



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	506	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe
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 143

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 148
......

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

100% Actual & Verified — Instant Download, Please Click
Order The CS0-003 Practice Test Here