CS0-003 Dumps

CompTIA CySA+ Certification Beta Exam

https://www.certleader.com/CS0-003-dumps.html

NEW QUESTION 1
Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?

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

Answer: B

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

NEW QUESTION 2
The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

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

Answer: A

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

NEW QUESTION 3
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:
A social engineering attack is underway is the most likely 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 4
A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

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

Answer: A

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

NEW QUESTION 5
A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following
does this most likely describe?

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

Answer: A

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

NEW QUESTION 6
An organization has tracked several incidents that are listed in the following table:

Start time	Detection time	Time elapsed in minutes
7:20 a.m.	10:30 a.m.	180
12:00 a.m.	2:30 a.m.	150
9:25 a.m.	12:15 p.m.	170
3:25 p.m.	5:45 p.m.	140

Which of the following is the organization's MTTD?

A. 140
B. 150
C. 160
D. 180

Answer: C

Explanation:
The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data: (180+150+170+140)/4 = 160 minutes. This is the correct answer according to the CompTIA CySA+ CS0-003 Certification Study Guide1, Chapter 4, page 161. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4, page 153; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4, page 161.

NEW QUESTION 7
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 8
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 9
A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve
this issue?

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

Answer: A

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

NEW QUESTION 10
Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

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

Answer: C

Explanation:
The correct answer is C. Impact.
The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact

metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service1.

The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

NEW QUESTION 10

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

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

Answer: D

Explanation:

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

NEW QUESTION 15

A security analyst has found a moderate-risk item in an organization's point-of-sale application. The organization is currently in a change freeze window and has decided that the risk is not high enough to correct at this time. Which of the following inhibitors to remediation does this scenario illustrate?

A. Service-level agreement
B. Business process interruption
C. Degrading functionality
D. Proprietary system

Answer: B

Explanation:

Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation. Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment12. Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it3. References: Inhibitors to Remediation — SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation…

NEW QUESTION 20

HOTSPOT

A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.

INSTRUCTIONS

Part 1

Review the artifacts associated with the security incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.

Part 2

Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each control may only be used once, and not all controls will be used.

Firewall log   File integrity monitoring report   Malware domain list   Vulnerability scan report   Phishing email

Firewall log:

Firewall log ⊠

Traffic denied:

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

Alert messages:

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

Critical messages:

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

File integrity Monitoring Report:

File integrity monitoring report ⊠

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

Action	Object type	What	Who	When
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Removed Where: Workstation: Date created:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx "11/30/19 12:05:34"	Domainusers\user1	11/30/19 12:25:13
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Added	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Where: Workstation:	Host1 172.30.0.152			
Renamed Where: Workstation: Name changed from:	File Host1 172.30.0.152 resume1.docx to resume2.docx		Domainusers\user1	12/1/19 14:25:30

Malware domain list:

Malware domain list ☒

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

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

Vulnerability Scan Report:

Vulnerability scan report ☒

HIGH SEVERITY

Title:	Cleartext transmission of sensitive information
Description:	The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected asset:	172.30.0.150
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

HIGH SEVERITY

Title:	Elevated privileges not required for software installations
Description:	All account types can install software, requirements for privileged accounts for installation capabilities is not configured.
Affected asset:	172.30.0.152
Risk:	Enhanced risk for unauthorized or malicious software installation
Reference:	n/a

MEDIUM SEVERITY

Title:	Sensitive cookie in HTTPS session without "secure" attribute
Description:	The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset:	172.30.0.157
Risk:	Session sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 certificate
Description:	The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.
Affected asset:	172.30.0.153
Risk:	May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference:	CVE-2005-1234

Phishing Email:

Phishing email ✖

From: IT HelpDesk <it-helpdesk@company.com>
Sent: Sun 12/01/2019 2:00:00
To: Global Users <globalusers@company.com>
Subject: Moving our mail servers

Hi,

In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

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

Download the latest mail client located here.

Thank you.

IT HelpDesk
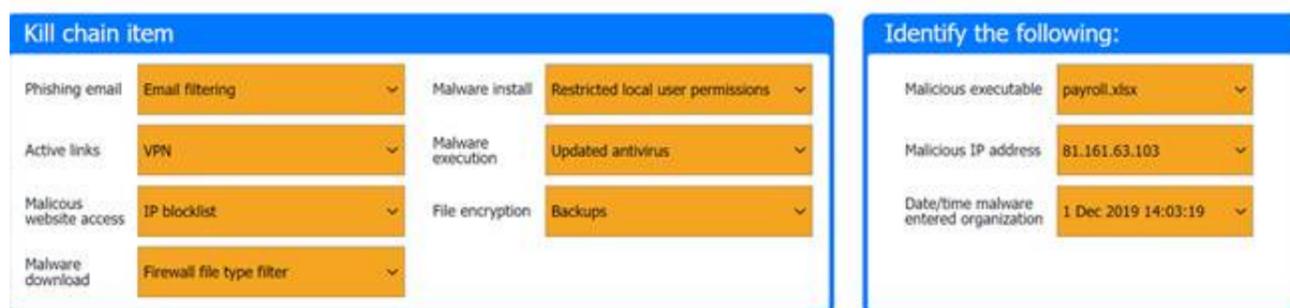
Kill chain item

Phishing email — Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Active links — Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Malicous website access — Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Malware download — Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Malware install — Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Malware execution — Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

File encryption — Select control
- Firewall file type filter
- Honeypot
- MFA
- MAC filtering
- Restricted local user permissions
- Email filtering
- Disk-level encryption
- Updated antivirus
- Network segmentation
- Plain text email format
- VPN
- IP blocklist
- Backups

Identify the following:

Malicious executable — Select option
- invoice.exe
- resume1.docx
- resume2.docx
- payroll.xlsx

Malicious IP address — Select option
- 81.161.63.103
- 81.161.63.253
- 171.25.193.20
- 185.220.101.194
- 192.168.2.1
- 171.25.193.25
- 10.1.1.238

Date/time malware entered organization — Select option
- 1 Dec 2019 11:24:16
- 1 Dec 2019 14:03:19
- 1 Dec 2019 14:03:55
- 30 Nov 2019 12:05:34
- 1 Dec 2019 14:25:30
- 1 Dec 2019 13:59:25
- 30 Nov 2019 12:25:13

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Kill chain item			
Phishing email	Email filtering	Malware install	Restricted local user permissions
Active links	VPN	Malware execution	Updated antivirus
Malicous website access	IP blocklist	File encryption	Backups
Malware download	Firewall file type filter		

Identify the following:	
Malicious executable	payroll.xlsx
Malicious IP address	81.161.63.103
Date/time malware entered organization	1 Dec 2019 14:03:19

NEW QUESTION 22
During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

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

Answer: C

Explanation:
Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official References:
? https://www.cisa.gov/stopransomware/ransomware-guide
? https://www.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
? https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

NEW QUESTION 26
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 28
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 31
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 vulnerabilit 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 34
An attacker recently gained unauthorized access to a financial institution's database, which contains confidential information. The attacker exfiltrated a large amount of data before being detected and blocked. A security analyst needs to complete a root cause analysis to determine how the attacker was able to gain access. Which of the following should the analyst perform first?

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

Answer: C

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

NEW QUESTION 38
Which of the following security operations tasks are ideal for automation?

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

Answer: D

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

NEW QUESTION 41
Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

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

Answer: C

NEW QUESTION 46

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

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

Answer: A

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

NEW QUESTION 51
A security manager is looking at a third-party vulnerability metric (SMITTEN) to improve upon the company's current method that relies on CVSSv3. Given the following:

Vulnerability 1

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - Base Score: 7.5 High
SMITTEN: Malware exploitable: No; Exploit Activity: Low; Exposed Externally: No

Vulnerability 2

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N - Base Score: 5.4 Medium
SMITTEN: Malware exploitable: Yes; Exploit Activity: HIGH; Exposed Externally: Yes

Vulnerability 3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - Base Score: 9.8 Critical
SMITTEN: Malware exploitable: No; Exploit Activity: None; Exposed Externally: Yes

Vulnerability 4

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H - Base Score: 9.9 Critical
SMITTEN: Malware exploitable: Yes; Exploit Activity: Medium; Exposed Externally: No

Which of the following vulnerabilities should be prioritized?

A. Vulnerability 1
B. Vulnerability 2
C. Vulnerability 3
D. Vulnerability 4

Answer: B

Explanation:
 Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric. References:
Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Program, Section: Vulnerability Severity.

NEW QUESTION 52
Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

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

Answer: A

Explanation:
 An important aspect that should be included in the lessons-learned step after an incident is to identify any improvements or changes in the incident response plan or procedures. The lessons-learned step is a process that involves reviewing and evaluating the incident response activities and outcomes, as well as identifying

and documenting any strengths, weaknesses, gaps, or best practices. Identifying any improvements or changes in the incident response plan or procedures can help enhance the security posture, readiness, or capability of the organization for future incidents

NEW QUESTION 55
Exploit code for a recently disclosed critical software vulnerability was publicly available (or download for several days before being removed. Which of the following CVSS v.3.1 temporal metrics was most impacted by this exposure?

A. Remediation level
B. Exploit code maturity
C. Report confidence
D. Availability

Answer: B

Explanation:
Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.
The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

NEW QUESTION 58
A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

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

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

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

Answer: D

Explanation:
The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

NEW QUESTION 59
Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

A. MFA
B. User and password
C. PAM
D. Key pair

Answer: D

Explanation:
Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.
References: Authentication Methods - Configuring Tenant-Wide Settings in Azure …, Cloud Foundation - Oracle Help Center

NEW QUESTION 60
Which of the following statements best describes the MITRE ATT&CK framework?

A. It provides a comprehensive method to test the security of applications.
B. It provides threat intelligence sharing and development of action and mitigation strategies.
C. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.
D. It tracks and understands threats and is an open-source project that evolves.

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

Answer: D

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

NEW QUESTION 65
A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network.
Which of the following would best aid in decreasing the workload without increasing staff?

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

Answer: C

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

NEW QUESTION 70
An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

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

Answer: D

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

NEW QUESTION 72
Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

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

Answer: D

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

NEW QUESTION 77
While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?

A. If appropriate logging levels are set
B. NTP configuration on each system
C. Behavioral correlation settings
D. Data normalization rules

Answer: B

Explanation:
The NTP configuration on each system should be checked first, as it is essential for ensuring accurate and consistent time stamps across different systems. NTP

is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP configuration is not consistent or correct on each system, the time stamps of the logs and events may differ, making it difficult to correlate incidents across different systems. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23.
References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, What is SIEM? | Microsoft Security

NEW QUESTION 78
An organization was compromised, and the usernames and passwords of all em-ployees were leaked online. Which of the following best describes the remedia-tion that could reduce the impact of this situation?

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

Answer: A

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

NEW QUESTION 82
A security analyst receives an alert for suspicious activity on a company laptop An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

Which of the following has most likely occurred?

A. An Office document with a malicious macro was opened.
B. A credential-stealing website was visited.
C. A phishing link in an email was clicked
D. A web browser vulnerability was exploited.

Answer: A

Explanation:
An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis. The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute code from a URL.

NEW QUESTION 83
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 88
A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

A. Block the attacks using firewall rules.
B. Deploy an IPS in the perimeter network.
C. Roll out a CDN.
D. Implement a load balancer.

Answer: C

Explanation:
Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website12. References: How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

NEW QUESTION 89
A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

A. Nmap
B. TCPDump
C. SIEM
D. EDR

Answer: B

Explanation:
TCPDump is the best tool to prove whether the server was experiencing a DoS attack related to half-open TCP sessions consuming memory. TCPDump is a command-line tool that can capture and analyze network traffic, such as TCP, UDP, and ICMP packets. TCPDump can help the administrator to identify the source and destination of the traffic, the TCP flags and sequence numbers, the packet size and frequency, and other information that can indicate a DoS attack. A DoS attack related to half-open TCP sessions is also known as a SYN flood attack, which is a type of volumetric attack that aims to exhaust the network bandwidth or resources of the target server by sending a large amount of TCP SYN requests and ignoring the TCP SYN-ACK responses. This creates a backlog of half-open connections on the server, which consume memory and CPU resources, and prevent legitimate connections from being established12. TCPDump can help the administrator to detect a SYN flood attack by looking for a high number of TCP SYN packets with different source IP addresses, a low number of TCP SYN-ACK packets, and a very low number of TCP ACK packets34. References: SYN flood DDoS attack | Cloudflare, What is a SYN flood attack and how to prevent it? | NETSCOUT, TCPDump - A Powerful Tool for Network Analysis and Security, How to Detect a SYN Flood Attack with TCPDump

NEW QUESTION 92
After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

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

Answer: A

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

NEW QUESTION 93

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 94
A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

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

Answer: A

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

NEW QUESTION 99
An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:
/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator
Which of the following controls would work best to mitigate the attack represented by this snippet?

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

Answer: A

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

NEW QUESTION 102
A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server
logs for evidence of exploitation of that particular vulnerability?

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

Answer: A

Explanation:
/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited

to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official References:
? https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
? https://www.comptia.org/certifications/cybersecurity-analyst
? https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your- questions-answered

NEW QUESTION 107
A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A. grep [IP address] packets.pcapB cat packets.pcap | grep [IP Address]
B. tcpdump -n -r packets.pcap host [IP address]
C. strings packets.pcap | grep [IP Address]

Answer: C

Explanation:
tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official References:
? https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
? https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test- questions-with-answers
? https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_studied/

NEW QUESTION 110
While reviewing web server logs, a security analyst found the following line:
<IMG SRC='vbscript:msgbox("test")'>
Which of the following malicious activities was attempted?

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

Answer: D

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

NEW QUESTION 112
Which of the following best describes the goal of a tabletop exercise?

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

Answer: A

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

NEW QUESTION 117
A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

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

Answer: C

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

NEW QUESTION 121
AXSS vulnerability was reported on one of the non-sensitive/non-mission-critical public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

A. Implement an IPS in front of the web server.
B. Enable MFA on the website.
C. Take the website offline until it is patched.
D. Implement a compensating control in the source code.
E. Configure TLS v1.3 on the website.
F. Fix the vulnerability using a virtual patch at the WAF.

Answer: DF

Explanation:
The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code. These recommendations are effective, efficient, and less disruptive than the other options. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

NEW QUESTION 125
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 129
An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

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

Answer: A

Explanation:
 Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS).

Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts.
OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

NEW QUESTION 133

A security analyst detects an email server that had been compromised in the internal network. Users have been reporting strange messages in their email inboxes and unusual network traffic. Which of the following incident response steps should be performed next?

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

Answer: C

Explanation:
After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise. ReferencesC: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

NEW QUESTION 136

A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

A. The NTP server is not configured on the host.
B. The cybersecurity analyst is looking at the wrong information.
C. The firewall is using UTC time.
D. The host with the logs is offline.

Answer: A

Explanation:
The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23. References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and …

NEW QUESTION 139

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

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

Answer: B

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

NEW QUESTION 143

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

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

Answer: C

Explanation:

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

NEW QUESTION 144
A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

Time stamp	Message
20:06:05	LDAP: A read operation was performed on an object: Domain Admins
20:06:05	LDAP: A read operation was performed on an object: Domain Servers
20:06:09	EDR: A local group was enumerated: Administrators
20:06:23	EDR: SMB connection attempts to multiple hosts from single host: PC021

Which of the following is most likely occurring, based on the events in the log?

A. An adversary is attempting to find the shortest path of compromise.
B. An adversary is performing a vulnerability scan.
C. An adversary is escalating privileges.
D. An adversary is performing a password stuffing attack..

Answer: B

Explanation:
Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161; Monitor logs from vulnerability scanners, Section: Reports on Nessus vulnerability data.

NEW QUESTION 146
A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

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

Answer: B

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

NEW QUESTION 148
Which of the following would an organization use to develop a business continuity plan?

A. A diagram of all systems and interdependent applications
B. A repository for all the software used by the organization
C. A prioritized list of critical systems defined by executive leadership
D. A configuration management database in print at an off-site location

Answer: C

Explanation:
A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption2. The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization3. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity4. References: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

NEW QUESTION 151
A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

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

B. Create a compensating control item until the system can be fully patched.
C. Accept the risk and decommission current assets as end of life.
D. Request an exception and manually patch each system.

Answer: A

Explanation:
 Integrating an IT service delivery ticketing system to track remediation and closure is the best approach to ensure all vulnerabilities are patched in accordance with the SLA. A ticketing system is a software tool that helps manage, organize, and track the tasks and workflows related to IT service delivery, such as incident management, problem management, change management, and vulnerability management. A ticketing system can help the security team to prioritize, assign, monitor, and document the remediation of the vulnerabilities, and to ensure that they are completed within the specified time frame and quality standards. A ticketing system can also help the security team to communicate and collaborate with other teams, such as the IT operations team, the development team, and the business stakeholders, and to report on the status and progress of the remediation efforts12. Creating a compensating control item, accepting the risk, and requesting an exception are not the best approaches to ensure all vulnerabilities are patched in accordance with the SLA, as they do not address the root cause of the problem, which is the large number of critical and high findings that require patching. These approaches may also introduce more risks or challenges for the security team, such as compliance issues, resource constraints, or business impacts3 . References: What is a Ticketing System? | Freshservice ITSM Glossary, Vulnerability Management Best Practices, Compensating Controls: An Impermanent Solution to an IT … - Tripwire, [Risk Acceptance in Information Security - Infosec Resources], [Exception Management - ISACA]

NEW QUESTION 152
Which of the following tools would work best to prevent the exposure of PII outside of an organization?

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

Answer: D

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

NEW QUESTION 157
A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been
compromised. Which of the following steps should the administrator take next?

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

Answer: B

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

NEW QUESTION 159
A company has a primary control in place to restrict access to a sensitive database. However, the company discovered an authentication vulnerability that could bypass this control. Which of the following is the best compensating control?

A. Running regular penetration tests to identify and address new vulnerabilities
B. Conducting regular security awareness training of employees to prevent socialengineering attacks
C. Deploying an additional layer of access controls to verify authorized individuals
D. Implementing intrusion detection software to alert security teams of unauthorized access attempts

Answer: C

Explanation:
Deploying an additional layer of access controls to verify authorized individuals is the best compensating control for the authentication vulnerability that could bypass the primary control. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a threat when the primary control is not sufficient or feasible. A compensating control should provide a similar or greater level of protection as the primary control, and should be closely related to the vulnerability or the threat it is addressing1. In this case, the primary control is to restrict access to a sensitive database, and the vulnerability is an authentication bypass. Therefore, the best compensating control is to deploy an additional layer of access controls, such as multifactor authentication, role-based access control, or encryption, to verify the identity and the authorization of the individuals who are accessing the database. This way, the compensating control can prevent unauthorized access to the database, even if the primary control is bypassed23. Running regular penetration tests, conducting regular security awareness training, and implementing intrusion detection software are all good security practices, but they are not compensating controls for the authentication vulnerability,

as they do not provide a similar or greater level of protection as the primary control, and they are not closely related to the vulnerability or the threat they are addressing. References: Compensating Controls: An Impermanent Solution to an IT … - Tripwire, What is Multifactor Authentication (MFA)? | Duo Security, Role-Based Access Control (RBAC) and Role-Based Security, [What is a Penetration Test and How Does It Work?]

NEW QUESTION 163
Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

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

Answer: A

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

NEW QUESTION 164
Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

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

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

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

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

Answer: B

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

NEW QUESTION 166
The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

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

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

A. Vulnerability A

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

Answer: B

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

NEW QUESTION 169
Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

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

Answer: B

Explanation:
The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.
A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business1. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks2345.
By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture2345.
Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access © may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real- time threat detection and response. Therefore, B is the best option among the choices given.

NEW QUESTION 171
After updating the email client to the latest patch, only about 15% of the workforce is able to use email. Windows 10 users do not experience issues, but Windows 11 users have constant issues. Which of the
following did the change management team fail to do?

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

Answer: B

Explanation:
Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users. Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.
References: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

NEW QUESTION 174
An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

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

Answer: B

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

NEW QUESTION 176
A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

A. Deploy agents on all systems to perform the scans.

B. Deploy a central scanner and perform non-credentialed scans.
C. Deploy a cloud-based scanner and perform a network scan.
D. Deploy a scanner sensor on every segment and perform credentialed scans.

Answer: A

Explanation:
USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario. References:
? CompTIA CySA+ CS0-003 Certification Study Guide, page 247
? What are Attack Vectors: Definition & Vulnerabilities, section "How to secure attack vectors"
? Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user "schroeder"

NEW QUESTION 179
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 181
A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

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

Answer: A

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

NEW QUESTION 184
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 186
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 189
Which of the following most accurately describes the Cyber Kill Chain methodology?

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

Answer: C

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

NEW QUESTION 194
A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being
used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

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

Answer: B

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

NEW QUESTION 198
SIMULATION
Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.

File Server Logs

Date/Time	Source IP	Source port	Dest IP	Dest Port		URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80		bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80		visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80		goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80		stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80		funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80		chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	56666	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 4:16:39 PM	192.168.0.94	63814	102.172.101.36	80		freefood.com	GET
3/7/2016 4:15:36 PM	192.168.0.47	48110	151.94.198.15	443		searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80		securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80		chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80		goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80		pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80		chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	174.169.173.216	80		funweb.cn	POST

SIEM Logs

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuzlss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1809	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuzlss	638	lsass.exe
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe

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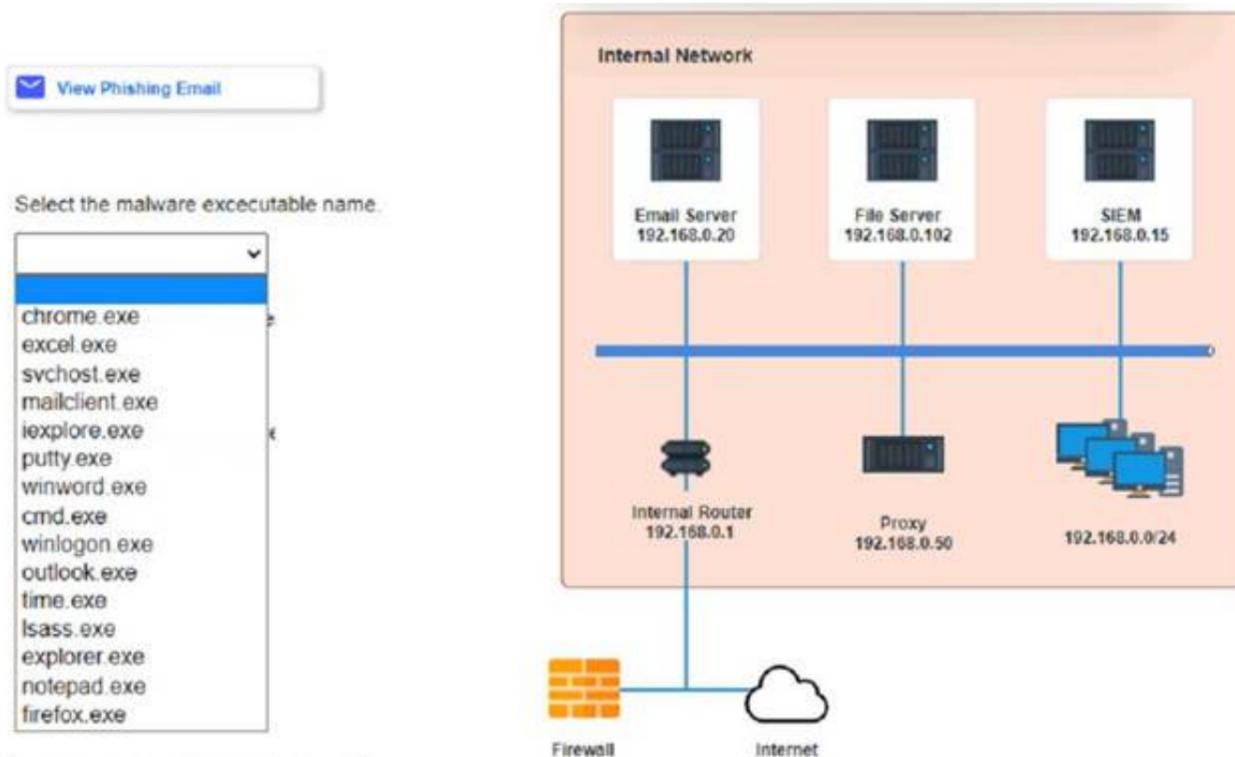
View Phishing Email

Select the malware excecutable name.

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

Internal Network

Email Server 192.168.0.20
File Server 192.168.0.102
SIEM 192.168.0.15

Internal Router 192.168.0.1
Proxy 192.168.0.50
192.168.0.0/24

Firewall
Internet

How many workstations were infected?

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

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. Answers
? 1. 25
? 2. 15
? 3. svchost.EXE

NEW QUESTION 202
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 204
......

Thank You for Trying Our Product

* 100% Pass or Money Back

> All our products come with a 90-day Money Back Guarantee.

* One year free update

> You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

> We currently serve more than 30,000,000 customers.

* Shop Securely

> All transactions are protected by VeriSign!

100% Pass Your CS0-003 Exam with Our Prep Materials Via below:

https://www.certleader.com/CS0-003-dumps.html