Free Questions for CS0-003

Shared by Slater on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An analyst is investigating a phishing incident and has retrieved the following as part of the investigation:

cmd.exe /c c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -NoLogo -NoProfile -EncodedCommand

Which of the following should the analyst use to gather more information about the purpose of this command?

Options:

A- Echo the command payload content into 'base64 -d'.

B- Execute the command from a Windows VM.

C- Use a command console with administrator privileges to execute the code.

D- Run the command as an unprivileged user from the analyst workstation.

Answer:

A

Explanation:

The command in question involves an encoded PowerShell command, which is typically used by attackers to obfuscate malicious scripts. To decode and understand the payload, one would need to decode the base64 encoded string. This is why option A is the correct answer, as 'base64 -d' is a command used to decode data encoded with base64. This process will reveal the plaintext of the encoded command, which can then be analyzed to understand the actions that the attacker was attempting to perform. Option B is risky and not advised without a controlled and isolated environment. Option C is not safe because executing unknown or suspicious code with administrator privileges could cause harm to the system or network. Option D also poses a risk of executing potentially harmful code on an analyst's workstation.

Question 2

Question Type: MultipleChoice

A high volume of failed RDP authentication attempts was logged on a critical server within a one-hour period. All of the attempts originated from the same remote IP address and made use of a single valid domain user account. Which of the following would be the most effective mitigating control to reduce the rate of success of this brute-force attack?

Options:

A- Enabling a user account lockout after a limited number of failed attempts

B- Installing a third-party remote access tool and disabling RDP on all devices

C- Implementing a firewall block for the remote system's IP address

D- Increasing the verbosity of log-on event auditing on all devices

Answer:

A

Explanation:

Enabling a user account lockout policy is a security measure that can effectively mitigate brute-force attacks. After a predetermined number of consecutive failed login attempts, the account will be locked, preventing the attacker from continuing to try different password combinations. This control directly addresses the issue of multiple failed attempts from the same IP address using a single user account, making it the most effective among the options provided. Option B suggests replacing RDP with another remote access tool, which does not address the brute-force attempt but rather avoids the RDP protocol. Option C, implementing a firewall block, could be effective but does not prevent attacks from other IP addresses and may not be as immediate. Option D, increasing log verbosity, enhances monitoring but does not prevent the attack itself.

Question 3

Question Type: MultipleChoice

An email hosting provider added a new data center with new public IP addresses. Which of the following most likely needs to be updated to ensure emails from the new data center do not get blocked by spam filters?

Options:

A- DKIM

B- SPF

C- SMTP

D- DMARC

Answer:

B

Explanation:

SPF (Sender Policy Framework) is a DNS TXT record that lists authorized sending IP addresses for a given domain. If an email hosting provider added a new data center with new public IP addresses, the SPF record needs to be updated to include those new IP addresses, otherwise the emails from the new data center may fail SPF checks and get blocked by spam filters123 Reference: 1: Use DMARC to validate email, setup steps 2: How to set up SPF, DKIM and DMARC: other mail & hosting providers providers 3: Set up SPF, DKIM, or DMARC records for my hosting email

Question 4

Question Type: MultipleChoice

Following an attack, an analyst needs to provide a summary of the event to the Chief Information Security Officer. The summary needs to include the who-what-when information and evaluate the effectiveness of the plans in place. Which of the following incident management life cycle processes

does this describe?

Options:

A- Business continuity plan

B- Lessons learned

C- Forensic analysis

D- Incident response plan

Answer:

B

Explanation:

The lessons learned process is the final stage of the incident management life cycle, where the incident team reviews the incident and evaluates the effectiveness of the response and the plans in place. The lessons learned report should include the who-what-when information and any recommendations for improvement123 Reference: 1: What is incident management? Steps, tips, and best practices 2: 5 Steps of the Incident Management Lifecycle | RSI Security 3: Navigating the Incident Response Life Cycle: A Comprehensive Guide

Question 5

Question Type: MultipleChoice

A network analyst notices a long spike in traffic on port 1433 between two IP addresses on opposite sides of a WAN connection. Which of the following is the most likely cause?

Options:

A- A local red team member is enumerating the local RFC1918 segment to enumerate hosts.

B- A threat actor has a foothold on the network and is sending out control beacons.

C- An administrator executed a new database replication process without notifying the SOC.

D- An insider threat actor is running Responder on the local segment, creating traffic replication.

Answer:

C

Explanation:

Port 1433 is commonly used by Microsoft SQL Server, which is a database management system. A spike in traffic on this port between two IP addresses on opposite sides of a WAN connection could indicate a database replication process, which is a way of copying and distributing data from one database server to another. This could be a legitimate activity performed by an administrator, but it should be communicated to the security operations center (SOC) to avoid confusion and false alarms.

Question 6

Question Type: MultipleChoice

A security analyst would like to integrate two different SaaS-based security tools so that one tool can notify the other in the event a threat is detected. Which of the following should the analyst utilize to best accomplish this goal?

Options:

A- SMB share

B- API endpoint

C- SMTP notification

D- SNMP trap

Answer:

B

Explanation:

An API endpoint is a point of entry for a communication between two different SaaS-based security tools. It allows one tool to send requests and receive responses from the other tool using a common interface. An API endpoint can be used to notify the other tool in the event a threat is detected and trigger an appropriate action. SMB share, SMTP notification, and SNMP trap are not suitable for SaaS integration security, as they are either network protocols or email services that do not provide a direct and secure communication between two different SaaS tools. Reference: Top 10 Best SaaS Security Tools - 2023, What is SaaS Security? A Guide to Everything SaaS Security, 6 Key Considerations for SaaS Integration Security | Prismatic, Introducing Security for Interconnected SaaS - Palo Alto Networks

Question 7

Question Type: MultipleChoice

A web application team notifies a SOC analyst that there are thousands of HTTP/404 events on the public-facing web server. Which of the following is the next step for the analyst to take?

Options:

A- Instruct the firewall engineer that a rule needs to be added to block this external server.

B- Escalate the event to an incident and notify the SOC manager of the activity.

C- Notify the incident response team that a DDoS attack is occurring.

D- Identify the IP/hostname for the requests and look at the related activity.

Answer:

D

Explanation:

A HTTP/404 error code means that the requested page or resource was not found on the web server. This could be caused by various reasons, such as incorrect URLs, moved or deleted pages, missing assets, or server misconfigurations123. The analyst should first identify the source of the requests and examine the related activity to determine if they are legitimate or malicious, and what actions

need to be taken to resolve the issue. The other options are either premature or irrelevant without further investigation. Reference: 1: 404 Page Not Found Error: What It Is and How to Fix It 2: 404 Error Code: What Causes Them and How To Fix It 3: About 404 errors and how to Troubleshoot it?

Question 8

Question Type: MultipleChoice

A security administrator needs to import PII data records from the production environment to the test environment for testing purposes. Which of the following would best protect data confidentiality?

Options:

A- Data masking

B- Hashing

C- Watermarking

D- Encoding

Answer:

A

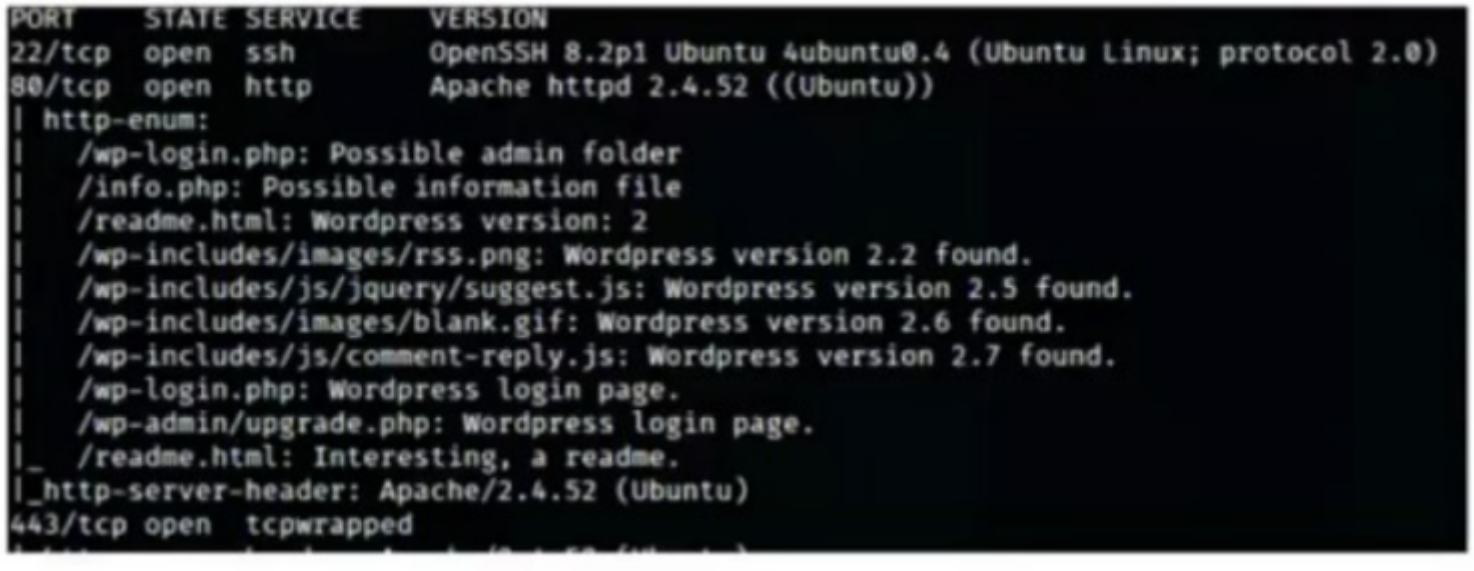
Explanation:

Data masking is a technique that replaces sensitive data with fictitious or anonymized data, while preserving the original format and structure of the data. This way, the data can be used for testing purposes without revealing the actual Pll information. Data masking is one of the best practices for data analysis of confidential data1. Reference: CompTIA CySA+ CS0-003 Certification Study Guide, page 343; Best Practices for Data Analysis of Confidential Data

Question 9

Question Type: MultipleChoice

A security analyst reviews the following extract of a vulnerability scan that was performed against the web server:



Which of the following recommendations should the security analyst provide to harden the web server?

Options:

A- Remove the version information on http-server-header.

B- Disable tcp_wrappers.

C- Delete the /wp-login.php folder.

D- Close port 22.

Answer:

A

Explanation:

The vulnerability scan shows that the version information is visible in the http-server-header, which can be exploited by attackers to identify vulnerabilities specific to that version. Removing or obfuscating this information can enhance security.

Question 10

Question Type: MultipleChoice

Which of the following stakeholders are most likely to receive a vulnerability scan report? (Select two).

Options:

A- Executive management

B- Law enforcement

C- Marketing

D- Legal

E- Product owner

F- Systems admininstration

Answer:

A, F

Explanation:

Executive management and systems administration are the most likely stakeholders to receive a vulnerability scan report because they are responsible for overseeing the security posture and remediation efforts of the organization. Law enforcement, marketing, legal, and product owner are less likely to be involved in the vulnerability management process or need access to the scan results. Reference: Cybersecurity Analyst+ - CompTIA, How To Write a Vulnerability Assessment Report | EC-Council, Driving Stakeholder Alignment in Vulnerability Management - LogicGate

Question 11

Question Type: MultipleChoice

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

Options:

A- Uncredentialed scan

B- Discqyery scan

C- Vulnerability scan

D- Credentialed scan

Answer:

B

Explanation:

A discovery scan is a type of web application scanning that involves identifying active, internet-facing web applications and their URIs, without performing any intrusive or in-depth tests. This type of scan can help to understand the scope and structure of a web application before conducting more comprehensive vulnerability scans12. Reference: 1: OWASP Vulnerability Scanning Tools 2: CISA Web Application Scanning

Question 12

Question Type: MultipleChoice

An incident responder was able to recover a binary file through the network traffic. The binary file was also found in some machines with anomalous behavior. Which of the following processes most likely can be performed to understand the purpose of the binary file?

Options:

A- File debugging

B- Traffic analysis

C- Reverse engineering

D- Machine isolation

Answer:

C

Explanation:

Reverse engineering is the process of analyzing a binary file to understand its structure, functionality, and behavior. It can help to identify the purpose of the binary file, such as whether it is a malicious program, a legitimate application, or a library.Reverse engineering can

involve various techniques, such as disassembling, decompiling, debugging, or extracting strings or resources from the binary file123.Reverse engineering can also help to find vulnerabilities, backdoors, or hidden features in the binary file