Free Questions for CS0-003 by certscare

Shared by Ortiz on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A vulnerability analyst is writing a report documenting the newest, most critical vulnerabilities identified in the past month. Which of the following public MITRE repositories would be best to review?

Options:

A- Cyber Threat Intelligence

B- Common Vulnerabilities and Exposures

C- Cyber Analytics Repository

ATT&CK

Answer:

B

Explanation:

The Common Vulnerabilities and Exposures (CVE) is a public repository of standardized identifiers and descriptions for common cybersecurity vulnerabilities. It helps security analysts to identify, prioritize, and report on the most critical vulnerabilities in their systems

and applications.The other options are not relevant for this purpose: Cyber Threat Intelligence (CTI) is a collection of information and analysis on current and emerging cyber threats; Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the ATT&CK adversary model; ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

Reference: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of various cybersecurity frameworks and standards, such as CVE, CTI, CAR, and ATT&CK, in chapter 1.Specifically, it explains the meaning and function of each framework and standard, such as CVE, which provides a common language for describing and sharing information about vulnerabilities1, page 28. Therefore, this is a reliable source to verify the answer to the question.

Question 2

Question Type: MultipleChoice

A security analyst has prepared a vulnerability scan that contains all of the company's functional subnets. During the initial scan, users reported that network printers began to print pages that contained unreadable text and icons.

Which of the following should the analyst do to ensure this behavior does not oocur during subsequent vulnerability scans?

Options:

A- Perform non-credentialed scans.

B- Ignore embedded web server ports.

C- Create a tailored scan for the printer subnet.

D- Increase the threshold length of the scan timeout.

Answer:

C

Explanation:

The best way to prevent network printers from printing pages during a vulnerability scan is to create a tailored scan for the printer subnet that excludes the ports and services that trigger the printing behavior. The other options are not effective for this purpose: performing non-credentialed scans may not reduce the impact on the printers; ignoring embedded web server ports may not cover all the possible ports that cause printing; increasing the threshold length of the scan timeout may not prevent the printing from occurring.

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of vulnerability scanning tools, such as Nessus, Nmap, and Qualys, in chapter 4. Specifically, it explains the meaning and function of each component in vulnerability scanning, such as credentialed vs. non-credentialed scans, port scanning, and scan scheduling1, pages 149-160. It also discusses the common issues and challenges of vulnerability scanning, such as network disruptions, false positives, and scan scope1, pages 161-162. Therefore, this is a reliable source to verify the answer to the question.

Question 3

Question Type: MultipleChoice

The Chief Information Security Officer (CISO) of a large management firm has selected a cybersecurity framework that will help the organization demonstrate its investment in tools and systems to protect its dat

a. Which of the following did the CISO most likely select?

Options:

A- PCI DSS

B- COBIT

C- ISO 27001

D- ITIL

Answer:

C

Explanation:

ISO 27001 is an international standard that establishes a framework for implementing, maintaining, and improving an information security management system (ISMS). It helps organizations demonstrate their commitment to protecting their data and complying with various regulations and best practices. The other options are not relevant for this purpose: PCI DSS is a standard that focuses on protecting payment card data; COBIT is a framework that provides guidance on governance and management of enterprise IT; ITIL is a framework that provides guidance on service management and delivery.

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of various cybersecurity frameworks and standards, such as ISO 27001, PCI DSS, COBIT, and ITIL, in chapter 1. Specifically, it explains the meaning and function of each framework and standard, such as ISO 27001, which provides a comprehensive approach to information security management1, page 29. Therefore, this is a reliable source to verify the answer to the question.

Question 4

Question Type: **MultipleChoice**

While reviewing the web server logs, a security analyst notices the following snippet:

.. \ .. / .. \ .. /boot.ini

Which of the following Is belng attempted?

Options:

A- Directory traversal

B- Remote file inclusion

C- Cross-site scripting

D- Remote code execution

E- Enumeration of /etc/passwd

Answer:

A

Explanation:

The snippet shows an attempt to access the boot.ini file, which is a configuration file for Windows operating systems. The "... \ ... /" pattern is used to navigate up the directory structure and reach the root directory, where the boot.ini file is located. This is a common technique for exploiting directory traversal vulnerabilities, which allow an attacker to access files and directories outside the intended web server path. The other options are not relevant for this purpose: remote file inclusion involves injecting a malicious file into a web application; cross-site scripting involves injecting malicious scripts into a web page; remote code execution involves executing arbitrary commands on a remote system; enumeration of /etc/passwd involves accessing the file that stores user information on Linux systems.

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of web

server logs, which record the requests and responses of web applications, in chapter 6. Specifically, it explains the meaning and function of each component in web server logs, such as the HTTP method, the URL, the status code, and the user agent1, page 244. It also discusses the common types and indicators of web-based attacks, such as directory traversal, which use special characters to manipulate the web server path1, page 251. Therefore, this is a reliable source to verify the answer to the question.

Question 5

Question Type: MultipleChoice

A security analyst has received an incident case regarding malware spreading out of control on a customer's network. The analyst is unsure how to respond. The configured EDR has automatically obtained a sample of the malware and its signature. Which of the following should the analyst perform next to determine the type of malware, based on its telemetry?

Options:

A- Cross-reference the signature with open-source threat intelligence.

B- Configure the EDR to perform a full scan.

C- Transfer the malware to a sandbox environment.

D- Log in to the affected systems and run necstat.

Answer:

A

Explanation:

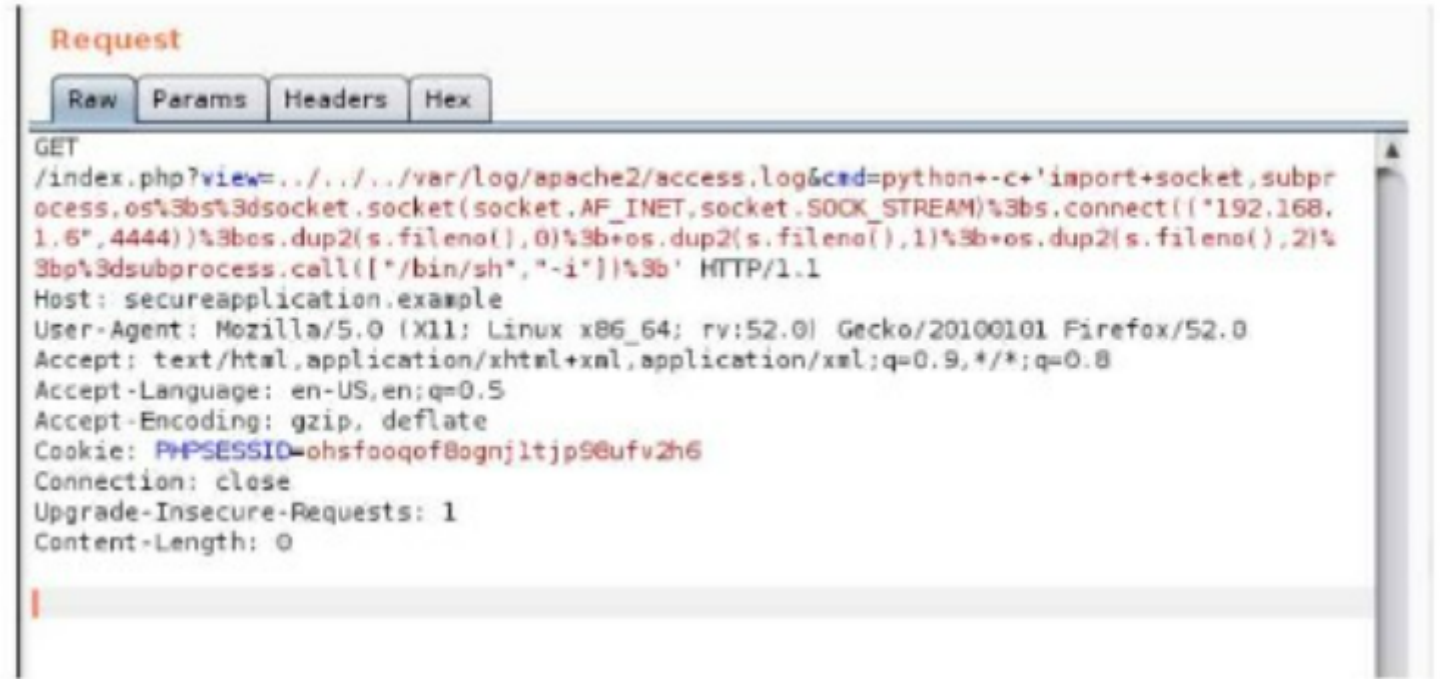
The signature of the malware is a unique identifier that can be used to compare it with known malware samples and their behaviors. Open-source threat intelligence sources provide information on various types of malware, their indicators of compromise, and their mitigation strategies. By cross-referencing the signature with these sources, the analyst can determine the type of malware and its telemetry. The other options are not relevant for this purpose: configuring the EDR to perform a full scan may not provide additional information on the malware type; transferring the malware to a sandbox environment may expose the analyst to further risks; logging in to the affected systems and running netstat may not reveal the malware activity.

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of EDR, a tool used for endpoint security, in chapter 5. Specifically, it explains the meaning and function of malware signatures and how they can be used to identify malware types1, page 203. It also discusses the benefits and challenges of using open-source threat intelligence sources to enhance security analysis1, page 211. Therefore, this is a reliable source to verify the answer to the question.

Question 6

Question Type: MultipleChoice

A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:



Which of the following vulnerabilitles Is the securlty analyst trylng to valldate?

Options:

A- SQL injection

B- LFI

C- XSS

D- CSRF

Answer:

B

Explanation:

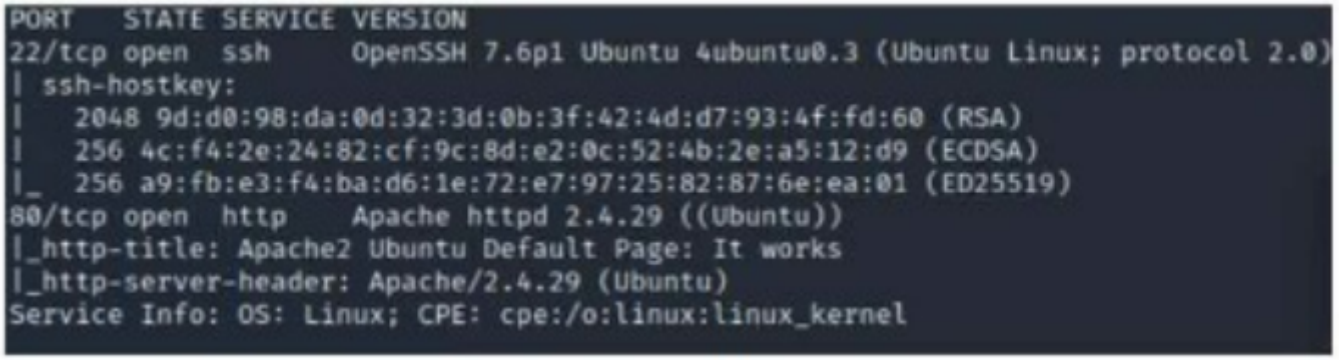
The security analyst is validating a Local File Inclusion (LFI) vulnerability, as indicated by the "/.../.../.../" in the GET request which is a common indicator of directory traversal attempts associated with LFI. The other options are not relevant for this purpose: SQL injection involves injecting malicious SQL statements into a database query; XSS involves injecting malicious scripts into a web page; CSRF involves tricking a user into performing an unwanted action on a web application.

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of Burp Suite, a tool used for testing web application security, in chapter 6. Specifically, it explains the meaning and function of each component in Burp Suite, such as Repeater, which allows the security analyst to modify and resend individual requests1, page 239. Therefore, this is a reliable source to verify the answer to the question.

Question 7

Question Type: MultipleChoice

A security analyst scans a host and generates the following output:



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9d:d0:98:da:0d:32:3d:0b:3f:42:4d:d7:93:4f:fd:60 (RSA)
|   256 4c:f4:2e:24:82:cf:9c:8d:e2:0c:52:4b:2e:a5:12:d9 (ECDSA)
|_  256 a9:fb:e3:f4:ba:d6:1e:72:e7:97:25:82:87:6e:ea:01 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Which of the following best describes the output?

Options:

A- The host is unresponsive to the ICMP request.

B- The host Is running a vulnerable mall server.

C- The host Is allowlng unsecured FTP connectlons.

D- The host is vulnerable to web-based exploits.

Answer:

D

Explanation:

The output shows that port 80 is open and running an HTTP service, indicating that the host could potentially be vulnerable to web-based attacks.The other options are not relevant for this purpose: the host is responsive to the ICMP request, as shown by the "Host is up" message; the host is not running a mail server, as there is no SMTP or POP3 service detected; the host is not allowing unsecured FTP connections, as there is no FTP service detected. Reference:According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition123, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of nmap, a popular network scanning tool, in chapter 5.Specifically, it explains the meaning and function of each option in nmap, such as "-sV" for version detection2, page 195. Therefore, this is a reliable source to verify the answer to the question.