Free Questions for GCED by vceexamstest

Shared by Day on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is a major problem that attackers often encounter when attempting to develop or use a kernel mode rootkit?

Options:

A- Their effectiveness depends on the specific applications used on the target system.

B- They tend to corrupt the kernel of the target system, causing it to crash.

C- They are unstable and are easy to identify after installation

D- They are highly dependent on the target OS.

Answer:

B

Question 2

Question Type: MultipleChoice

What is the BEST sequence of steps to remove a bot from a system?

Options:

A- Terminate the process, remove autoloading traces, delete any malicious files

B- Delete any malicious files, remove autoloading traces, terminate the process

C- Remove autoloading traces, delete any malicious files, terminate the process

D- Delete any malicious files, terminate the process, remove autoloading traces

Answer:

A

Question 3

Question Type: MultipleChoice

What attack was indicated when the IDS system picked up the following text coming from the Internet to the web server?

select user, password from user where user= "jdoe" and password= 'myp@55!' union select "text",2 into outfile "/tmp/file1.txt" - - '

Options:

A- Remote File Inclusion

B- URL Directory Traversal

C- SQL Injection

D- Binary Code in HTTP Headers

Answer:

C

Explanation:

An example of manipulating SQL statements to perform SQL injection includes using the semi-colon to perform multiple queries. The following example would delete the users table:

Username: ' or 1=1; drop table users; - -

Password: [Anything]

Question 4

Question Type: MultipleChoice

When running a Nmap UDP scan, what would the following output indicate?

```
161/udp  open|filtered snmp
```

Options:

A- The port may be open on the system or blocked by a firewall

B- The router in front of the host accepted the request and sent a reply

C- An ICMP unreachable message was received indicating an open port

D- An ACK was received in response to the initial probe packet

Answer:

A

Explanation:

When Nmap shows an "open filtered" response for the scan results, this indicates a couple of different reasons. The port could be open but a firewall could be blocking the use ACK flags; only TCP packets do.

Question 5

Question Type: MultipleChoice

How does an Nmap connect scan work?

Options:

A- It sends a SYN, waits for a SYN/ACK, then sends a RST.

B- It sends a SYN, waits for a ACK, then sends a RST.

C- It sends a SYN, waits for a ACK, then sends a SYN/ACK.

D- It sends a SYN, waits for a SYN/ACK, then sends a ACK

Answer:

A

Explanation:

An Nmap connect scan sends a SYN, waits for a SYN/ACK, then sends a ACK to complete the three-way handshake. A Nmap half-open scan sends a SYN, waits for a SYN/ACK, then sends a RST.

Question 6

Question Type: MultipleChoice

Enabling port security prevents which of the following?

Options:

A- Using vendors other than Cisco for switching equipment as they don't offer port security

B- Spoofed MAC addresses from being used to cause a Denial of Service condition

C- Legitimate MAC addresses from being used to cause a Denial of Service condition

D- Network Access Control systems from functioning properly

Answer:

C

Question 7

Question Type: MultipleChoice

The creation of a filesystem timeline is associated with which objective?

Options:

A- Forensic analysis

B- First response

C- Access control

D- Incident eradication

Answer:

A

Question 8

Question Type: MultipleChoice

Which of the following is the best way to establish and verify the integrity of a file before copying it during an investigation?

Options:

A- Write down the file size of the file before and after copying and ensure they match

B- Ensure that the MAC times are identical before and after copying the file

C- Establish the chain of custody with the system description to prove it is the same image

D- Create hash of the file before and after copying the image verifying they are identical

Answer:

D

Question 9

Question Type: MultipleChoice

Which of the following is an outcome of the initial triage during incident response?

Options:

A- Removal of unnecessary accounts from compromised systems

B- Segmentation of the network to protect critical assets

C- Resetting registry keys that vary from the baseline configuration

D- Determining whether encryption is in use on in scope systems

Answer:

B