GIAC

GCIH
GIAC Incident Handler

For More Information – Visit link below:
https://www.examsempire.com/
Product Version
1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

https://examsempire.com/

Latest Version: 6.0

Question: 1

Which of the following virus is a script that attaches itself to a file or template?
Response:

A. Boot sector
B. Trojan horse
C. Macro virus
D. E-mail virus

Answer: C

Question: 2

In which of the following attacks does the attacker gather information to perform an access attack?
Response:

A. Land attack
B. Reconnaissance attack
C. Vulnerability attack
D. DoS attack

Answer: B

Question: 3

Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?
Response:

A. Signature-based IDS
B. Network-based IDS
C. Passive IDS
D. Active IDS

Answer: D

Question: 4

What advantage does running netstat with the flags "-nao" have over running netstat with the "-na" flags in Windows?
Response:

A. The "o" flag shows the socket state
B. The "o" flag shows the process ID (PID)
C. The "o" flag shows UDP connections only
D. The "o" flag shows the user ID (UID) of the owner of the socket

Answer: B

Question: 5

What is the purpose of configuring a password protected screen saver on a computer?
Response:

A. For preventing unauthorized access to a system.
B. For preventing a system from a Denial of Service (DoS) attack.
C. For preventing a system from a social engineering attack.
D. For preventing a system from a back door attack.

Answer: A

Question: 6

Which of the following statements about Ping of Death attack is true?
Response:

A. In this type of attack, a hacker sends more traffic to a network address than the buffer can handle.
B. This type of attack uses common words in either upper or lower case to find a password.
C. In this type of attack, a hacker maliciously cuts a network cable.
D. In this type of attack, a hacker sends ICMP packets greater than 65,536 bytes to crash a system.

Answer: D

Question: 7

An organization has enabled local account token filtering in the registry for workstations. What additional step do they need to take in order to defend against pass-the-hash attacks?
Response:

A. Remove active command prompts
B. Disable the local administrator account
C. Disable null sessions on the domain
D. Block outbound access to TCP port 139

Answer: D

Question: 8

When would a web-based reconnaissance tool be preferred over a direct/local reconnaissance tool?
Response:

A. When more comprehensive TCP port scanning is required than what is offered by local tools
B. In the event that the target is running third-party web applications
C. When the target's employees are using a VPN to connect to the central office
D. To keep traffic from the attacker's system from hitting the target network

Answer: C

Question: 9

In which of the following attacks does an attacker use packet sniffing to read network traffic between two parties to steal the session cookie?
Response:

A. Session fixation
B. Cross-site scripting
C. Session sidejacking
D. ARP spoofing

Answer: C

Question: 10

You have configured a virtualized Internet browser on your Windows XP professional computer. Using the virtualized Internet browser, you can protect your operating system from which of the following?
Response:

A. Brute force attack
B. Mail bombing
C. Distributed denial of service (DDOS) attack
D. Malware installation from unknown Web sites

Answer: D

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/