GIAC
GCIH
GIAC Certified Incident Handler (GCIH)

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.**

Latest Version: 6.0

Question: 1

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. On the We-are-secure login page, he enters ='or''=' as a username and successfully logs in to the user page of the Web site.
The we-are-secure login page is vulnerable to a _____.

A. Dictionary attack
B. SQL injection attack
C. Replay attack
D. Land attack

Answer: B

Question: 2

Which of the following types of attack can guess a hashed password?

A. Brute force attack
B. Evasion attack
C. Denial of Service attack
D. Teardrop attack

Answer: A

Question: 3

Ryan, a malicious hacker submits Cross-Site Scripting (XSS) exploit code to the Website of Internet forum for online discussion. When a user visits the infected Web page, code gets automatically executed and Ryan can easily perform acts like account hijacking, history theft etc.
Which of the following types of Cross-Site Scripting attack Ryan intends to do?

A. Non persistent
B. Document Object Model (DOM)
C. SAX
D. Persistent

Answer: D

Question: 4

Buffer overflows are one of the major errors used for exploitation on the Internet today. A buffer overflow occurs when a particular operation/function writes more data into a variable than the variable was designed to hold.
Which of the following are the two popular types of buffer overflows?
Each correct answer represents a complete solution. Choose two.

A. Dynamic buffer overflows
B. Stack based buffer overflow
C. Heap based buffer overflow
D. Static buffer overflows

Answer: B,C

Question: 5

Which of the following applications is an example of a data-sending Trojan?

A. SubSeven
B. Senna Spy Generator
C. Firekiller 2000
D. eBlaster

Answer: D

Question: 6

Adam works as a Security Analyst for Umbrella Inc. Company has a Windows-based network. All computers run on Windows XP. Manager of the Sales department complains Adam about the unusual behavior of his computer. He told Adam that some pornographic contents are suddenly appeared on his computer overnight.
Adam suspects that some malicious software or Trojans have been installed on the computer. He runs some diagnostics programs and Port scanners and found that the Port 12345, 12346, and 20034 are open. Adam also noticed some tampering with the Windows registry, which causes one application to run every time when Windows start.
Which of the following is the most likely reason behind this issue?

A. Cheops-ng is installed on the computer.
B. Elsave is installed on the computer.
C. NetBus is installed on the computer.
D. NetStumbler is installed on the computer.

Answer: C

Question: 7

Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?

A. Gathering private and public IP addresses
B. Collecting employees information
C. Banner grabbing
D. Performing Neotracerouting

Answer: B

Question: 8

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks.
As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

A. IIS buffer overflow
B. NetBIOS NULL session
C. SNMP enumeration
D. DNS zone transfer

Answer: A

Question: 9

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

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

Answer: C

Question: 10

Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following actions:
- Remove the network cable wires.
- Isolate the system on a separate VLAN
- Use a firewall or access lists to prevent communication into or out of the system.
- Change DNS entries to direct traffic away from compromised system

Which of the following steps of the incident handling process includes the above actions?

A. Identification
B. Containment
C. Eradication
D. Recovery

Answer: B

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/