examunion

Certified IT Exam Material Authority

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.examunion.com

Exam : **GCIH**

Title : GIAC Certified Incident Handler

Version : Demo

1.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

2.Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd.

Which of the following is the mostly likely the cause of the problem.?

A. Computer is infected with the stealth kernel level rootkit.
B. Computer is infected with stealth virus.
C. Computer is infected with the Stealth Trojan Virus.
D. Computer is infected with the Self-Replication Worm.

Answer: A

3.Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack
B. Replay attack
C. Teardrop attack
D. Land attack

Answer: A

4.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

5.In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?
A. Ping of death
B. Jolt
C. Fraggle
D. Teardrop
Answer: A

6.Adam has installed and configured his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop.
Which of the following attacks has been occurred on the wireless network of Adam?
A. NAT spoofing
B. DNS cache poisoning
C. MAC spoofing
D. ARP spoofing
Answer: C

7.Which of the following is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines?
A. Demon dialing
B. Warkitting
C. War driving
D. Wardialing
Answer: D

8.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: D

9.Which of the following statements are true about tcp wrappers?
Each correct answer represents a complete solution. Choose all that apply.
A. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
C. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as

tokens to filter for access control purposes.
D. tcp wrapper protects a Linux server from IP address spoofing.
Answer: A, B, C

10.Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?
A. Evasion attack
B. Denial-of-Service (DoS) attack
C. Ping of death attack
D. Buffer overflow attack
Answer: D

11.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

12.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

13.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

14.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

15.Which of the following statements are true about worms?
Each correct answer represents a complete solution. Choose all that apply.
A. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
B. Worms can exist inside files such as Word or Excel documents.
C. One feature of worms is keystroke logging.
D. Worms replicate themselves from one system to another without using a host file.
Answer: A, B, D

16.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

17.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

18.Which of the following are the primary goals of the incident handling team?
Each correct answer represents a complete solution. Choose all that apply.
A. Freeze the scene.
B. Repair any damage caused by an incident.
C. Prevent any further damage.

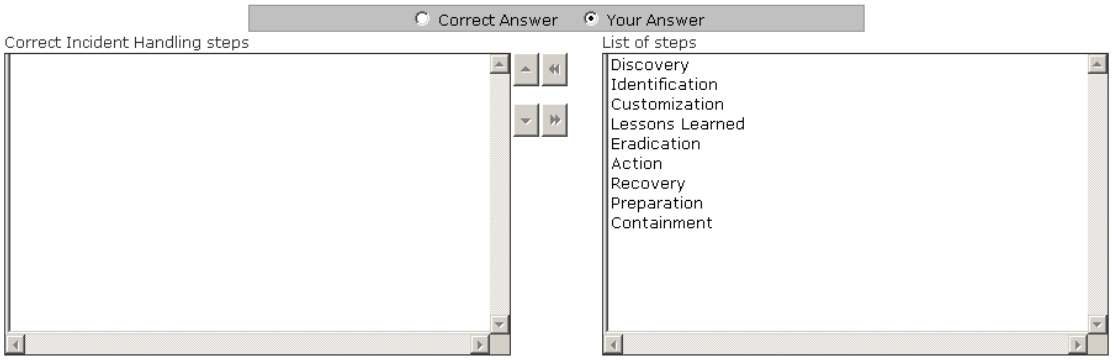
D. Inform higher authorities.
Answer: A, B, C

19.Fill in the blank with the appropriate word.
StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use _____ defense against buffer overflow attacks.
A. canary
Answer: A

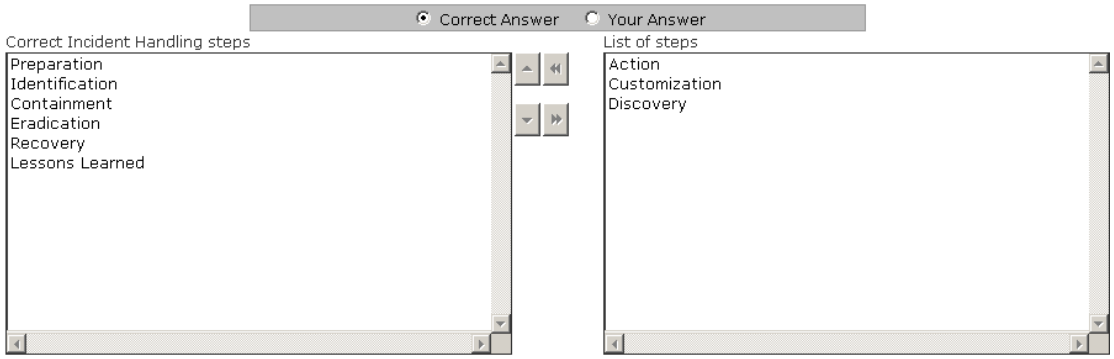
20.Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?
A. Whishker
B. Nessus
C. SARA
D. Nmap
Answer: B

21.Which of the following statements are true about a keylogger?
Each correct answer represents a complete solution. Choose all that apply.
A. It records all keystrokes on the victim's computer in a predefined log file.
B. It can be remotely installed on a computer system.
C. It is a software tool used to trace all or specific activities of a user on a computer.
D. It uses hidden code to destroy or scramble data on the hard disk.
Answer: A, B, C

22.Choose and reorder the steps of an incident handling process in their correct order.



A.



Answer: A

23.John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows:
C:\whisker.pl -h target_IP_address
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =
= Host: target_IP_address
= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1
mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
+ 200 OK: HEAD /cgi-bin/printenv
John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server.
Which of the following statements about 'Printenv' vulnerability are true?
Each correct answer represents a complete solution. Choose all that apply.
A. This vulnerability helps in a cross site scripting attack.
B. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.
C. The countermeasure to 'printenv' vulnerability is to remove the CGI script.
D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.
Answer: A, C, D

24.Which of the following statements about *buffer overflow* is true?
A. It manages security credentials and public keys for message encryption.
B. It is a collection of files used by Microsoft for software updates released between major service pack releases.
C. It is a condition in which an application receives more data than it is configured to accept.
D. It is a false warning about a virus.
Answer: C

25.Which of the following commands is used to access Windows resources from Linux workstation?
A. mutt
B. scp
C. rsync
D. smbclient
Answer: D

26.Adam, a malicious hacker, wants to perform a reliable scan against a remote target. He is not concerned about being stealth at this point.
Which of the following type of scans would be most accurate and reliable?
A. UDP sacn
B. TCP Connect scan
C. ACK scan
D. Fin scan

Answer: B

27.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?
A. Brute force attack
B. Mail bombing
C. Distributed denial of service (DDOS) attack
D. Malware installation from unknown Web sites
Answer: D

28.Which of the following statements about *Denial-of-Service (DoS)* attack are true?
Each correct answer represents a complete solution. Choose three.
A. It disrupts services to a specific computer.
B. It changes the configuration of the TCP/IP protocol.
C. It saturates network resources.
D. It disrupts connections between two computers, preventing communications between services.
Answer: A, C, D

29.You see the career section of a company's Web site and analyze the job profile requirements. You conclude that the company wants professionals who have a sharp knowledge of Windows server 2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?
A. Scanning
B. Covering tracks
C. Reconnaissance
D. Gaining access
Answer: C

30.John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure Website login page, he enters ='or''=' as a username and successfully logs on to the user page of the Web site. Now, John asks the we-aresecure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are-secure Website login page from the SQL injection attack?
A. Use the escapeshellarg() function
B. Use the session_regenerate_id() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellcmd() function
Answer: C