Vendor: GIAC

Exam Code: GCIH

Exam Name: GIAC Certified Incident Handler

Version: DEMO

QUESTION 1
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 2
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 3
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: ABD

QUESTION 4
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 5
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: BC

QUESTION 6
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: ABC

QUESTION 7
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.

Answer: canary

QUESTION 8
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

QUESTION 9
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: ABC

QUESTION 10
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: ACD

QUESTION 11
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

QUESTION 12
Which of the following commands is used to access Windows resources from Linux workstation?

A. mutt
B. scp
C. rsync
D. smbclient

Answer: D

QUESTION 13
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

QUESTION 14
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

QUESTION 15
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: ACD

QUESTION 16
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

QUESTION 17
Which of the following types of attacks is mounted with the objective of causing a negative impact on the performance of a computer or network?

A. Vulnerability attack
B. Man-in-the-middle attack
C. Denial-of-Service (DoS) attack
D. Impersonation attack

Answer: C

QUESTION 18
You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. An attacker uses software that keeps trying password combinations until the correct password is found. Which type of attack is this?

A. Denial-of-Service
B. Man-in-the-middle
C. Brute Force
D. Vulnerability

Answer: C

QUESTION 19
You want to scan your network quickly to detect live hosts by using ICMP ECHO Requests. What type of scanning will you perform to accomplish the task?

A. Idle scan
B. TCP SYN scan
C. XMAS scan
D. Ping sweep scan

Answer: D

QUESTION 20
Which of the following is a network worm that exploits the RPC sub-system vulnerability present in the Microsoft Windows operating system?

A. Win32/Agent
B. WMA/TrojanDownloader.GetCodec
C. Win32/Conflicker
D. Win32/PSW.OnLineGames

Answer: C

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **BDNT2014**