Vendor:EC-COUNCIL

Exam Code:312-50V7

Exam Name: Ethical Hacking and Countermeasures (CEHv7)

Version: Demo

QUESTION 1

Information gathered from social networking websites such as Facebook, Twitter and LinkedIn can be used to launch which of the following types of attacks? (Choose two.)

A. Smurf attack

B. Social engineering attack

C. SQL injection attack

D. Phishing attack

E. Fraggle attack

F. Distributed denial of service attack

Correct Answer: BD

QUESTION 2

Which of the following represent weak password? (Select 2 answers)

A. Passwords that contain letters, special characters, and numbers ExamplE. ap1$%##f@52

B. Passwords that contain only numbers ExamplE. 23698217

C. Passwords that contain only special characters ExamplE. and*#@!(%)

D. Passwords that contain letters and numbers ExamplE. meerdfget123

E. Passwords that contain only letters ExamplE. QWERTYKLRTY

F. Passwords that contain only special characters and numbers ExamplE. 123@$45

G. Passwords that contain only letters and special characters ExamplE. bob@andba

H. Passwords that contain Uppercase/Lowercase from a dictionary list ExamplE. OrAnGe

Correct Answer: EH

QUESTION 3

SSL has been seen as the solution to a lot of common security problems. Administrator will often time make use of SSL to encrypt communications from points A to point B. Why do you think this could be a bad idea if there is an Intrusion Detection System deployed to monitor the traffic between point A and B?

A. SSL is redundant if you already have IDS\\'s in place

B. SSL will trigger rules at regular interval and force the administrator to turn them off

C. SSL will slow down the IDS while it is breaking the encryption to see the packet content

D. SSL will blind the content of the packet and Intrusion Detection Systems will not be able to detect them

Correct Answer: D

QUESTION 4

What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

A. Scripting languages are hard to learn.

B. Scripting languages are not object-oriented.

C. Scripting languages cannot be used to create graphical user interfaces.

D. Scripting languages are slower because they require an interpreter to run the code.

Correct Answer: D

QUESTION 5

Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP

B. Nikto

C. Ike-scan

D. Arp-scan

Correct Answer: C

QUESTION 6

Fred is scanning his network to ensure it is as secure as possible. Fred sends a TCP probe packet to a host with a FIN flag and he receives a RST/ACK response. What does this mean?

A. This response means the port he is scanning is open.

B. The RST/ACK response means the port Fred is scanning is disabled.

C. This means the port he is scanning is half open.

D. This means that the port he is scanning on the host is closed.

Correct Answer: D

QUESTION 7

You want to capture Facebook website traffic in Wireshark. What display filter should you use that shows all TCP packets that contain the word \\'facebook\\'?

A. display==facebook

B. traffic.content==facebook

C. tcp contains facebook

D. list.display.facebook

Correct Answer: C

QUESTION 8

Steven the hacker realizes the network administrator of Acme Corporation is using syskey in Windows 2008 Server to protect his resources in the organization. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to use brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2008 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch the attack. How many bits does Syskey use for encryption?

A. 40-bit encryption

B. 128-bit encryption

C. 256-bit encryption

D. 64-bit encryption

Correct Answer: B

QUESTION 9

In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

A. Design

B. Elimination

C. Incorporation

D. Replication

E. Launch

F. Detection

Correct Answer: E

QUESTION 10

John runs a Web server, IDS and firewall on his network. Recently his Web server has been under constant hacking attacks. He looks up the IDS log files and sees no intrusion attempts but the Web server constantly locks up and needs rebooting due to various brute force and buffer overflow attacks but still the IDS alerts no intrusion whatsoever. John becomes suspicious and views the Firewall logs and he notices huge SSL connections constantly hitting his Web server. Hackers have been using the encrypted HTTPS protocol to send exploits to the Web server and that was the reason the IDS did not detect the intrusions. How would John protect his network from these types of attacks?

A. Install a proxy server and terminate SSL at the proxy

B. Enable the IDS to filter encrypted HTTPS traffic

C. Install a hardware SSL "accelerator" and terminate SSL at this layer

D. Enable the Firewall to filter encrypted HTTPS traffic

Correct Answer: AC

QUESTION 11

A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 - Application

B. Layer 4 TCP

C. Layer 3 Internet protocol

D. Layer 2 Data link

Correct Answer: B

QUESTION 12

How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80 HEAD / HTTP/1.0

B. telnet webserverAddress 80 PUT / HTTP/1.0

C. telnet webserverAddress 80 HEAD / HTTP/2.0

D. telnet webserverAddress 80 PUT / HTTP/2.0

Correct Answer: A