Version: 7.0

Question: 1

Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

A. Fast processor to help with network traffic analysis
B. They must be dual-homed
C. Similar RAM requirements
D. Fast network interface cards

Answer: B

Question: 2

Which of the following is an application that requires a host application for replication?

A. Micro
B. Worm
C. Trojan
D. Virus

Answer: D

Question: 3

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. Paros Proxy
B. BBProxy
C. BBCrack
D. Blooover

Answer: B

Question: 4

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.

B. Perform a full restore.
C. Read the first 512 bytes of the tape.
D. Read the last 512 bytes of the tape.

Answer: B

Question: 5

Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
D. Overwrites the original MBR and only executes the new virus code

Answer: B

Question: 6

Which statement is TRUE regarding network firewalls preventing Web Application attacks?

A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
C. Network firewalls can prevent attacks if they are properly configured.
D. Network firewalls cannot prevent attacks because they are too complex to configure.

Answer: B

Question: 7

Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus
B. Multipart virus
C. Macro virus
D. Stealth virus

Answer: C

Question: 8

Bluetooth uses which digital modulation technique to exchange information between paired devices?

A. PSK (phase-shift keying)
B. FSK (frequency-shift keying)
C. ASK (amplitude-shift keying)
D. QAM (quadrature amplitude modulation)

Answer: A

Question: 9

In order to show improvement of security over time, what must be developed?

A. Reports
B. Testing tools
C. Metrics
D. Taxonomy of vulnerabilities

Answer: C

Question: 10

Passive reconnaissance involves collecting information through which of the following?

A. Social engineering
B. Network traffic sniffing
C. Man in the middle attacks
D. Publicly accessible sources

Answer: D

Question: 11

How can rainbow tables be defeated?

A. Password salting
B. Use of non-dictionary words
C. All uppercase character passwords
D. Lockout accounts under brute force password cracking attempts

Answer: A

Question: 12

The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20

What is most likely taking place?

A. Ping sweep of the 192.168.1.106 network
B. Remote service brute force attempt
C. Port scan of 192.168.1.106
D. Denial of service attack on 192.168.1.106

Answer: B

Question: 13

An NMAP scan of a server shows port 25 is open. What risk could this pose?

A. Open printer sharing
B. Web portal data leak
C. Clear text authentication
D. Active mail relay

Answer: D

Question: 14

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?

Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports

PORT	STATE	SERVICE
21/tcp	open	ftp
23/tcp	open	telnet
80/tcp	open	http
139/tcp	open	netbios-ssn
515/tcp	open	
631/tcp	open	ipp
9100/tcp	open	

MAC Address: 00:00:48:0D:EE:89

A. The host is likely a Windows machine.
B. The host is likely a Linux machine.
C. The host is likely a router.
D. The host is likely a printer.

Answer: D

Question: 15

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

A. Passive
B. Reflective
C. Active
D. Distributive

Answer: C