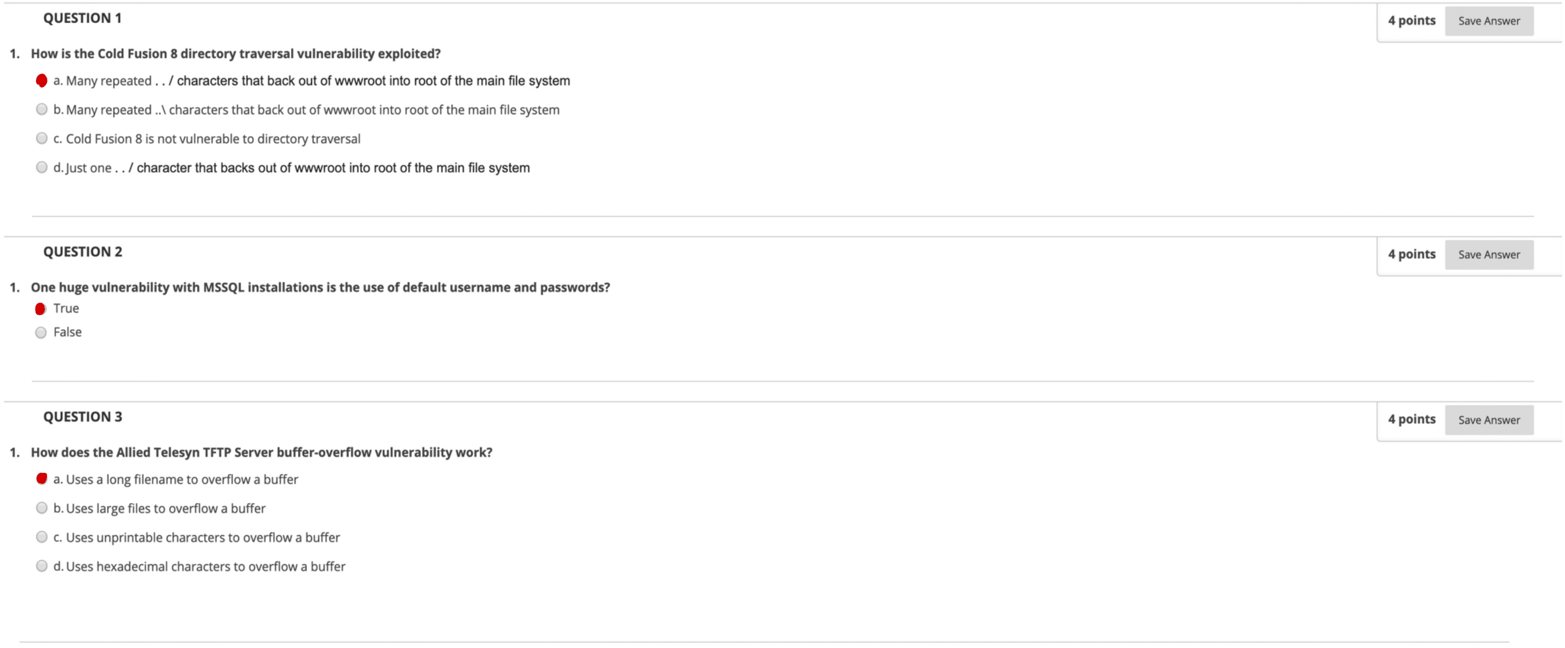


QUESTION 1

1. **How is the Cold Fusion 8 directory traversal vulnerability exploited?**

● a. Many repeated . . / characters that back out of wwwroot into root of the main file system

○ b. Many repeated ..\ characters that back out of wwwroot into root of the main file system

○ c. Cold Fusion 8 is not vulnerable to directory traversal

○ d. Just one . . / character that backs out of wwwroot into root of the main file system

QUESTION 2

1. **One huge vulnerability with MSSQL installations is the use of default username and passwords?**

● True

○ False

QUESTION 3

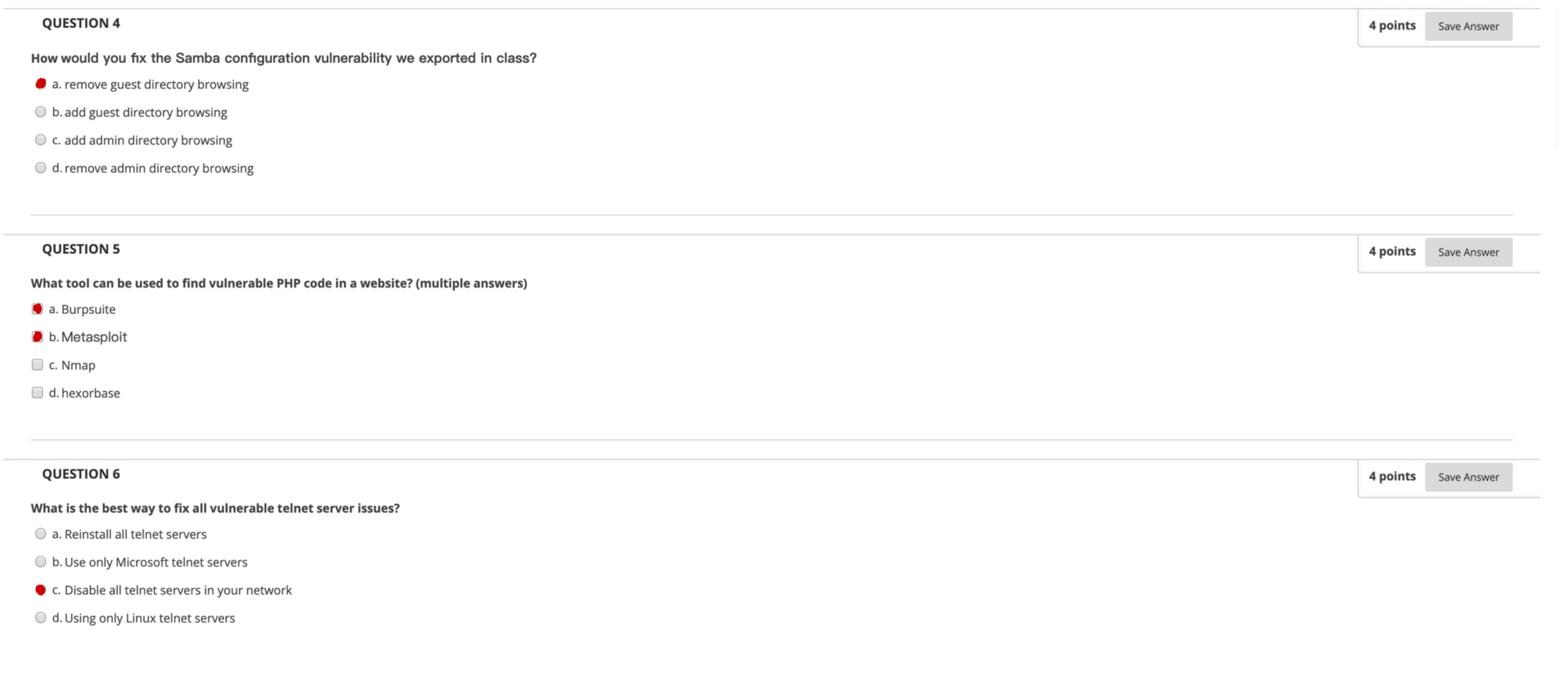
1. **How does the Allied Telesyn TFTP Server buffer-overflow vulnerability work?**

● a. Uses a long filename to overflow a buffer

○ b. Uses large files to overflow a buffer

○ c. Uses unprintable characters to overflow a buffer

○ d. Uses hexadecimal characters to overflow a buffer



QUESTION 4

How would you fix the Samba configuration vulnerability we exported in class?

● a. remove guest directory browsing

○ b. add guest directory browsing

○ c. add admin directory browsing

○ d. remove admin directory browsing

QUESTION 5

What tool can be used to find vulnerable PHP code in a website? (multiple answers)

☑ a. Burpsuite

☑ b. Metasploit

☐ c. Nmap

☐ d. hexorbase

QUESTION 6

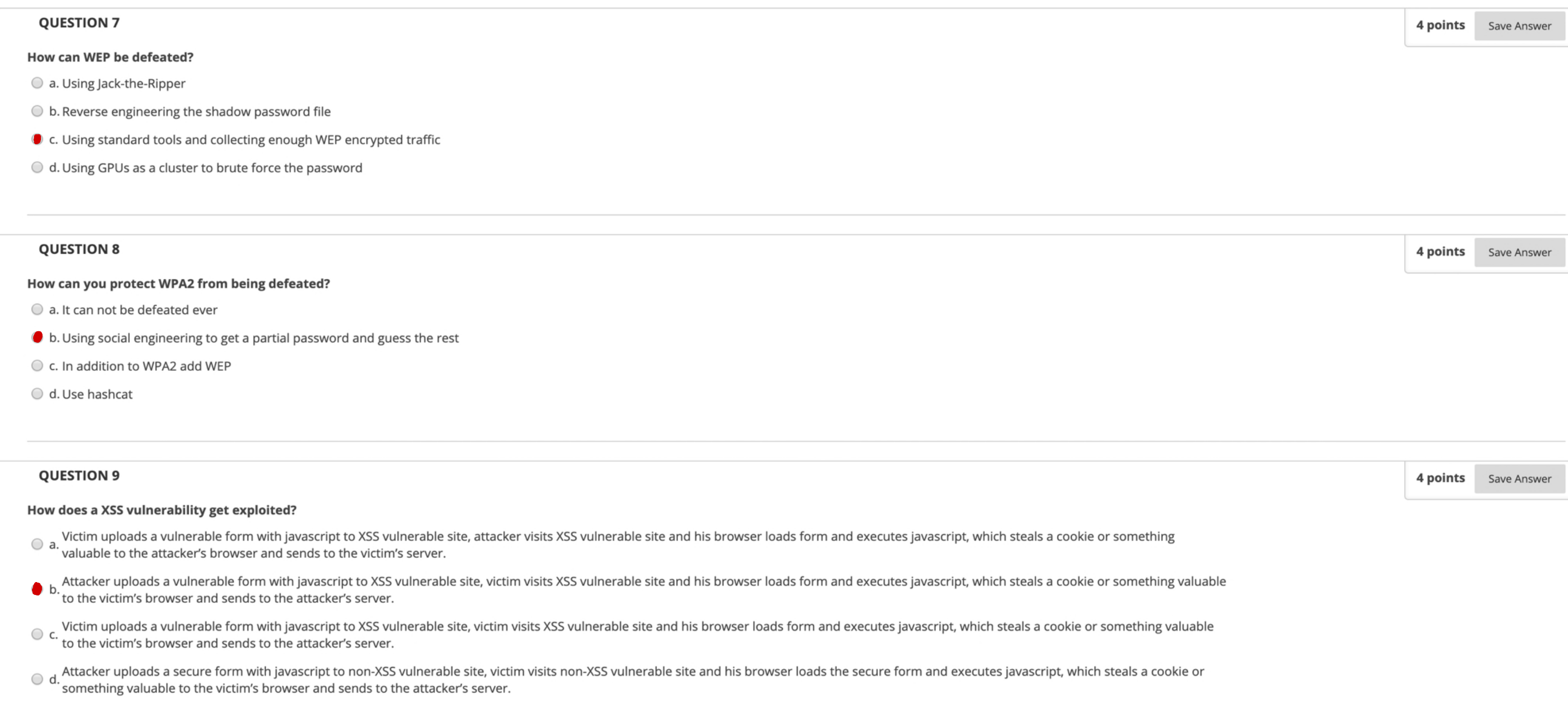
What is the best way to fix all vulnerable telnet server issues?

○ a. Reinstall all telnet servers

○ b. Use only Microsoft telnet servers

● c. Disable all telnet servers in your network

○ d. Using only Linux telnet servers



QUESTION 7

How can WEP be defeated?

○ a. Using Jack-the-Ripper

○ b. Reverse engineering the shadow password file

● c. Using standard tools and collecting enough WEP encrypted traffic

○ d. Using GPUs as a cluster to brute force the password

QUESTION 8

How can you protect WPA2 from being defeated?

○ a. It can not be defeated ever

● b. Using social engineering to get a partial password and guess the rest

○ c. In addition to WPA2 add WEP

○ d. Use hashcat

QUESTION 9

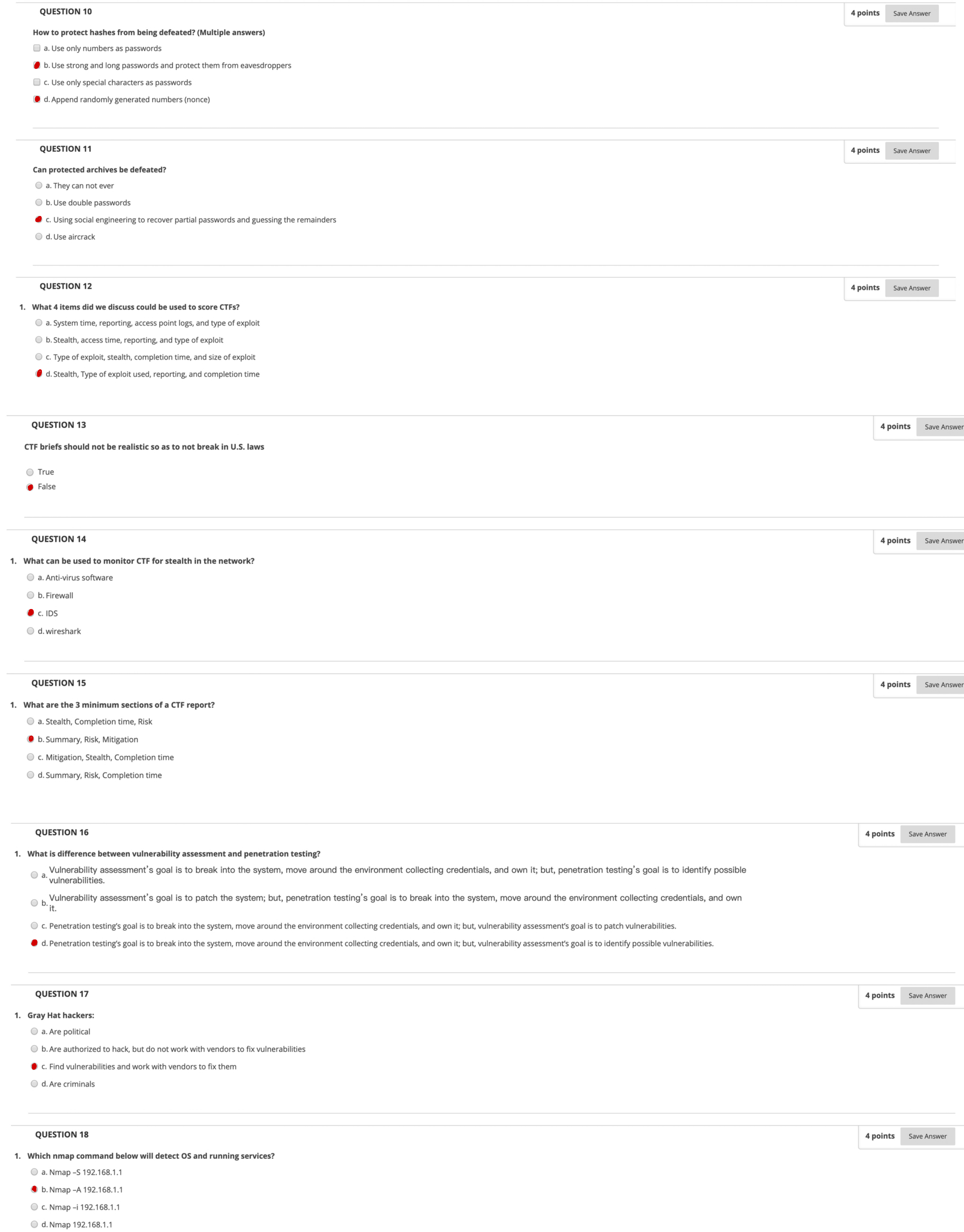
How does a XSS vulnerability get exploited?

○ a. Victim uploads a vulnerable form with javascript to XSS vulnerable site, attacker visits XSS vulnerable site and his browser loads form and executes javascript, which steals a cookie or something valuable to the attacker's browser and sends to the victim's server.

● b. Attacker uploads a vulnerable form with javascript to XSS vulnerable site, victim visits XSS vulnerable site and his browser loads form and executes javascript, which steals a cookie or something valuable to the victim's browser and sends to the attacker's server.

○ c. Victim uploads a vulnerable form with javascript to XSS vulnerable site, victim visits XSS vulnerable site and his browser loads form and executes javascript, which steals a cookie or something valuable to the victim's browser and sends to the attacker's server.

○ d. Attacker uploads a secure form with javascript to non-XSS vulnerable site, victim visits non-XSS vulnerable site and his browser loads the secure form and executes javascript, which steals a cookie or something valuable to the victim's browser and sends to the attacker's server.



QUESTION 10

4 points Save Answer

How to protect hashes from being defeated? (Multiple answers)

☐ a. Use only numbers as passwords

☑ b. Use strong and long passwords and protect them from eavesdroppers

☐ c. Use only special characters as passwords

☑ d. Append randomly generated numbers (nonce)

QUESTION 11

4 points Save Answer

Can protected archives be defeated?

○ a. They can not ever

○ b. Use double passwords

● c. Using social engineering to recover partial passwords and guessing the remainders

○ d. Use aircrack

QUESTION 12

4 points Save Answer

1. **What 4 items did we discuss could be used to score CTFs?**

○ a. System time, reporting, access point logs, and type of exploit

○ b. Stealth, access time, reporting, and type of exploit

○ c. Type of exploit, stealth, completion time, and size of exploit

● d. Stealth, Type of exploit used, reporting, and completion time

QUESTION 13

4 points Save Answer

CTF briefs should not be realistic so as to not break in U.S. laws

○ True

● False

QUESTION 14

4 points Save Answer

1. **What can be used to monitor CTF for stealth in the network?**

○ a. Anti-virus software

○ b. Firewall

● c. IDS

○ d. wireshark

QUESTION 15

4 points Save Answer

1. **What are the 3 minimum sections of a CTF report?**

○ a. Stealth, Completion time, Risk

● b. Summary, Risk, Mitigation

○ c. Mitigation, Stealth, Completion time

○ d. Summary, Risk, Completion time

QUESTION 16

4 points Save Answer

1. **What is difference between vulnerability assessment and penetration testing?**

○ a. Vulnerability assessment's goal is to break into the system, move around the environment collecting credentials, and own it; but, penetration testing's goal is to identify possible vulnerabilities.

○ b. Vulnerability assessment's goal is to patch the system; but, penetration testing's goal is to break into the system, move around the environment collecting credentials, and own it.

○ c. Penetration testing's goal is to break into the system, move around the environment collecting credentials, and own it; but, vulnerability assessment's goal is to patch vulnerabilities.

● d. Penetration testing's goal is to break into the system, move around the environment collecting credentials, and own it; but, vulnerability assessment's goal is to identify possible vulnerabilities.

QUESTION 17

4 points Save Answer

1. **Gray Hat hackers:**

○ a. Are political

○ b. Are authorized to hack, but do not work with vendors to fix vulnerabilities

● c. Find vulnerabilities and work with vendors to fix them

○ d. Are criminals

QUESTION 18

4 points Save Answer

1. **Which nmap command below will detect OS and running services?**

○ a. Nmap –S 192.168.1.1

● b. Nmap –A 192.168.1.1

○ c. Nmap –i 192.168.1.1

○ d. Nmap 192.168.1.1

QUESTION 19

4 points Save Answer

1. **Flags should:**

○ a. have unrealistic filenames

○ b. be in esoteric directories not mentioned in the brief

● c. not be put off of root

○ d. have esoteric filenames not mentioned in the brief

QUESTION 20

4 points Save Answer

1. **Which is NOT an example of a post-exploitation or pivoting challenge?**

○ a. Privilege escalation

○ b. Data extraction

○ c. Moving around network

● d. Buffer-overflow

QUESTION 21

4 points Save Answer

1. **The Hexorbase tool can NOT be used for:**

○ a. Administration of MySQL DB

○ b. Brute forcing SQLServer logins

○ c. Administration of Orace DB

● d. Brute forcing ColdFusion logins

QUESTION 22

4 points

1. **Which command is NOT a Meterpreter command?**

○ a. Exit

○ b. Background

● c. Show options

○ d. Keyscan_start

QUESTION 23

4 points

1. **Burpsuite is a:**

● a. Web application scanner

○ b. Network traffic sniffer

○ c. Wireless network scanner

○ d. Wireless access point password cracker

QUESTION 24

4 points

Which command can be used to probe multiple nearby wireless networks?

○ a. airodump-ng <interface> -w <filename> --bssid <MAC Address> --ivs

● b. iwlist <interface> scanning

○ c. aircrack-ng –a <# of seconds> -b <MAC address> <filename>

○ d. aireplay-ng <interface> -deauth <# of packets> -a <MAC Add#1> -c <MAC Add#2>

QUESTION 25

4 points Save Ans

Which command can be used to break wireless access point encryption?

○ a. airodump-ng <interface> -w <filename> --bssid <MAC Address> --ivs

○ b. iwlist <interface> scanning

● c. aircrack-ng –a <# of seconds> -b <MAC address> <filename>

○ d. aireplay-ng <interface> -deauth <# of packets> -a <MAC Add#1> -c <MAC Add#2>

Click Save and Submit to save and submit. Click Save All Answers to save all answers.

Save All Answers Save and Su