


**Question 1**

Answer saved

Marked out of 0.50

 Flag question

Banner grabbing is an example of which hacking activity?


Select one:

- ☐ a. Application analysis
- ☐ b. Footprinting
- ☐ c. Active operating system finger printing
- ☒ d. Passive operating system finger printing

**Question 2**

Answer saved

Marked out of 0.50

 Flag question

What provides for both authentication and confidentiality in IPSec?


Select one:

- ☐ a. AH
- ☐ b. SA
- ☐ c. IKE
- ☒ d. ESP

**Question 3**

Answer saved

Marked out of 0.50

 Flag question

What is a Tabletop exercise?


Select one:

- ☐ a. A rehearsal cyber attack performed on a smaller organization before an attack is performed on a larger organization
- ☐ b. A dummy exercise with networking models on a tabletop
- ☒ c. A planned exercise to allow organisations to evaluate their response to a cyber attack
- ☐ d. An authorised attack on an identified computer system

**Question 4**

Answer saved

Marked out of 0.50

 Flag question

Who represents the greatest risk to an organization?


Select one:

- ☐ a. Black hat hacker
- ☐ b. Grey hat hacker
- ☒ c. Disgruntled employee
- ☐ d. Script kiddies

**Question 5**

Answer saved

Marked out of 0.50

 Flag question

An attacker spoofs the target's IP address and then begins sending large amounts of ICMP packets containing the MAC address FF:FF:FF:FF:FF:FF. What is this attack known as?


Select one:

- ☐ a. SYB Flood
- ☐ b. ICMP Flood
- ☒ c. Smurf
- ☐ d. Ping of Death

**Question 6**

Answer saved

Marked out of 0.50

 Flag question

Which of the following takes advantage of weaknesses in the fragment reassembly functionality of TCP/IP?


Select one:

- ☐ a. SYN Flood
- ☒ b. Teardrop
- ☐ c. Smurf attack
- ☐ d. Ping of death

**Question 7**

Answer saved

Marked out of 0.50

 Flag question

Which tool can be used to perform a DNS zone transfer on Windows?

Select one:

- ☐ a. whois
- ☒ b. NSLookup
- ☐ c. DNSLookup
- ☐ d. ifconfig

**Question 8**

Answer saved

Marked out of 0.50

 Flag question

Which are the four regional Internet registries?

Select one:

- ☐ a. APNIC, MOSTNIC, ARIN, RIPE NCC
- ☐ b. APNIC, PICNIC, NANIC, ARIN
- ☐ c. APNIC, PICNIC, NANIC, RIPE NCC
- ☒ d. APNIC, LACNIC, ARIN, RIPE NCC

**Question 9**

Answer saved

Marked out of 0.50

 Flag question

What does TCP RST command indicate?


Select one:

- ☐ a. Restores the connection to a previous state
- ☐ b. Starts a TCP connection
- ☐ c. Finishes a TCP connections
- ☒ d. Resets the TCP connection

**Question 10**

Answer saved

Marked out of 0.50

 Flag question

What attack is known as "Evil Twin"?


Select one:

- ☐ a. Session Hijacking
- ☐ b. MAC Spoofing
- ☒ c. Rogue Access Point
- ☐ d. ARP Poisoning

**Question 11**

Answer saved

Marked out of 0.50

 Flag question

If a Penetration test team member attempts to guess the ISN for a TCP session, which attack is s/he most likely carrying out?


Select one:

- ☐ a. Session Splicing
- ☒ b. Session Hijacking
- ☐ c. Cross Site Request Forgery
- ☐ d. Cross Site Scripting

**Question 12**

Answer saved

Marked out of 0.50

 Flag question

A pen test team member types the following command:

```
nc 222.15.66.78 -p 8765
```

Which of the following statements is true regarding this attack?


Select one:

- ☐ a. The attacker is attempting to kill a service on a remote machine
- ☐ b. The attacker is establishing a listening port on his machine for later use
- ☒ c. The attacker is attempting to connect to an established listening port on a remote computer
- ☐ d. The attacker is attempting a DoS against a remote computer

**Question 13**

Answer saved

Marked out of 0.50

 Flag question

Which form of encryption is used by WPA?


Select one:

- ☐ a. DES
- ☐ b. AES
- ☐ c. RSA
- ☒ d. TKIP

**Question 14**

Answer saved

Marked out of 0.50

 Flag question

Which of the following is an effective deterrent against TCP session hijacking?


Select one:

- ☐ a. Install and use an HIDS on the system
- ☐ b. Enforce good password policy
- ☒ c. Use unpredictable sequence numbers
- ☐ d. Install and use Tripwire on the system

**Question 15**

Answer saved

Marked out of 0.50

 Flag question

Why would an attacker want to perform a scan on port 137?


Select one:

- ☐ a. To check for file and print sharing on Windows systems
- ☐ b. To discover proxy servers on a network
- ☐ c.
  - To locate the FTP service on the target host
- ☒ d. To discover a target system with the NetBIOS null session vulnerability

**Question 16**

Answer saved

Marked out of 0.50

 Flag question

When is session hijacking performed?


Select one:

- ☒ a. After 3-step handshake
- ☐ b. During 3-step handshake
- ☐ c. After FIN request
- ☐ d. Before 3-step handshake

**Question 17**

Answer saved

Marked out of 0.50

 Flag question

What is the major vulnerability for an ARP request?


Select one:

- ☒ a. The address request can be spoofed with the attackers MAC address
- ☐ b. It sends out an address request to all the hosts on the LAN
- ☐ c. The address is returned with a username and password in cleartext
- ☐ d. The address request can cause a DoS

**Question 18**

Answer saved

Marked out of 0.50

 Flag question

Which character is typically used first by the penetration tester?


Select one:

- ☐ a. Double quote
- ☒ b. Single quote
- ☐ c. Semi colon
- ☐ d. Dollar sign

**Question 19**

Answer saved

Marked out of 0.50

 Flag question

A hacker is conducting the following on the target workstation:

```
nmap -sT 192.33.10.5.
```

The attacker is in which phase?


Select one:

- ☐ a. Exploit
- ☐ b. Covering Tracks
- ☒ c. Scanning & Enumeration
- ☐ d. Payload delivery

**Question 20**

Answer saved

Marked out of 0.50

 Flag question

What is (are) the forms of password cracking?

Select one:

- ☐ a. Rainbow table
- ☐ b. Brute Forcing
- ☒ c. All of the mentioned
- ☐ d. Dictionary attack