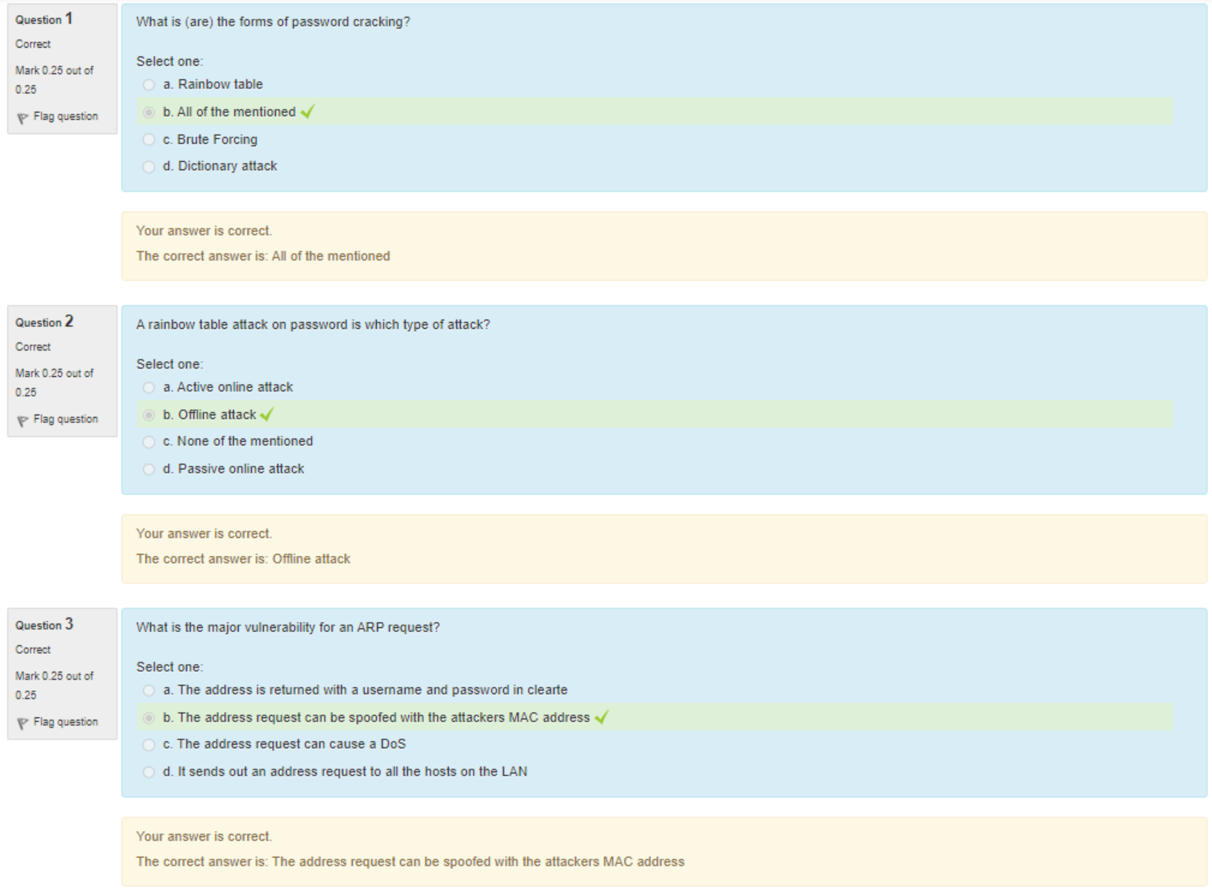
Ethical Hacking QUIZ 3



Question 1
Correct
Mark 0.25 out of 0.25
Flag question

What is (are) the forms of password cracking?

Select one:

○ a. Rainbow table

● b. All of the mentioned ✓

○ c. Brute Forcing

○ d. Dictionary attack

Your answer is correct.

The correct answer is: All of the mentioned

Question 2
Correct
Mark 0.25 out of 0.25
Flag question

A rainbow table attack on password is which type of attack?

Select one:

○ a. Active online attack

● b. Offline attack ✓

○ c. None of the mentioned

○ d. Passive online attack

Your answer is correct.

The correct answer is: Offline attack

Question 3
Correct
Mark 0.25 out of 0.25
Flag question

What is the major vulnerability for an ARP request?

Select one:

○ a. The address is returned with a username and password in clearte

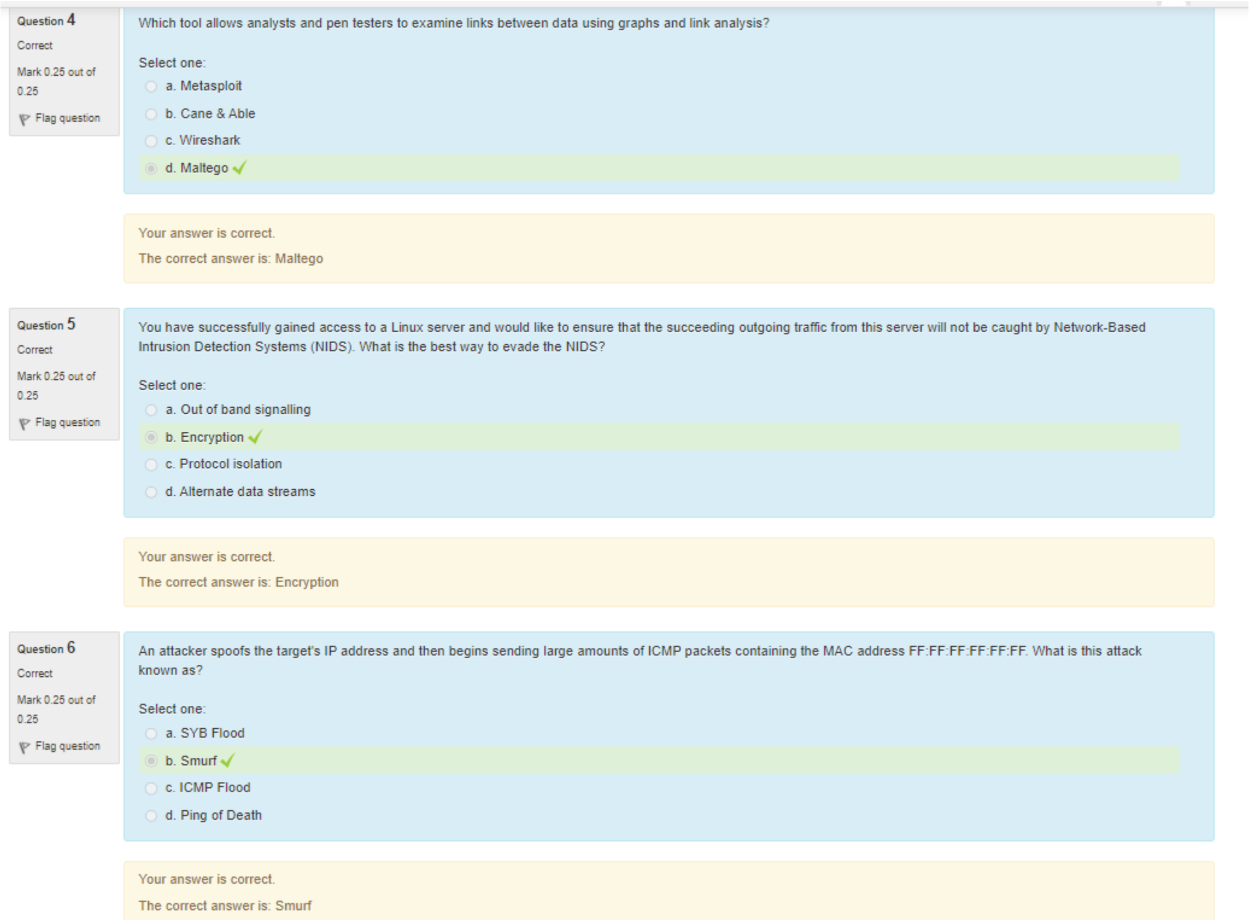
● b. The address request can be spoofed with the attackers MAC address ✓

○ c. The address request can cause a DoS

○ d. It sends out an address request to all the hosts on the LAN

Your answer is correct.

The correct answer is: The address request can be spoofed with the attackers MAC address



Question 4

Correct

Mark 0.25 out of 0.25

Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

Select one:

○ a. Metasploit

○ b. Cane & Able

○ c. Wireshark

● d. Maltego ✓

Your answer is correct.

The correct answer is: Maltego

Question 5

Correct

Mark 0.25 out of 0.25

You have successfully gained access to a Linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by Network-Based Intrusion Detection Systems (NIDS). What is the best way to evade the NIDS?

Select one:

○ a. Out of band signalling

● b. Encryption ✓

○ c. Protocol isolation

○ d. Alternate data streams

Your answer is correct.

The correct answer is: Encryption

Question 6

Correct

Mark 0.25 out of 0.25

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

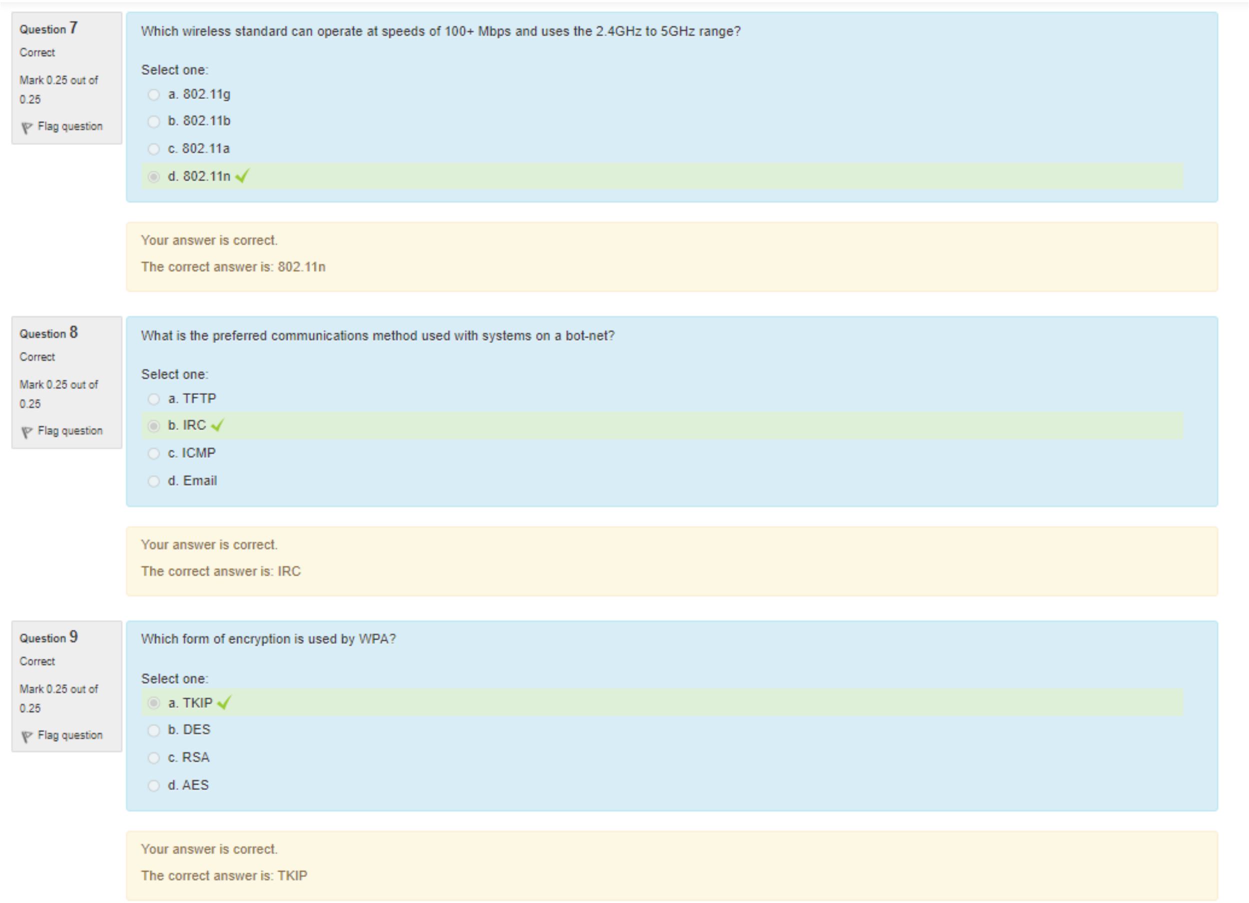
● b. Smurf ✓

○ c. ICMP Flood

○ d. Ping of Death

Your answer is correct.

The correct answer is: Smurf



Question 7

Correct

Mark 0.25 out of 0.25

Flag question

Which wireless standard can operate at speeds of 100+ Mbps and uses the 2.4GHz to 5GHz range?

Select one:

○ a. 802.11g

○ b. 802.11b

○ c. 802.11a

● d. 802.11n ✓

Your answer is correct.

The correct answer is: 802.11n

Question 8

Correct

Mark 0.25 out of 0.25

Flag question

What is the preferred communications method used with systems on a bot-net?

Select one:

○ a. TFTP

● b. IRC ✓

○ c. ICMP

○ d. Email

Your answer is correct.

The correct answer is: IRC

Question 9

Correct

Mark 0.25 out of 0.25

Flag question

Which form of encryption is used by WPA?

Select one:

● a. TKIP ✓

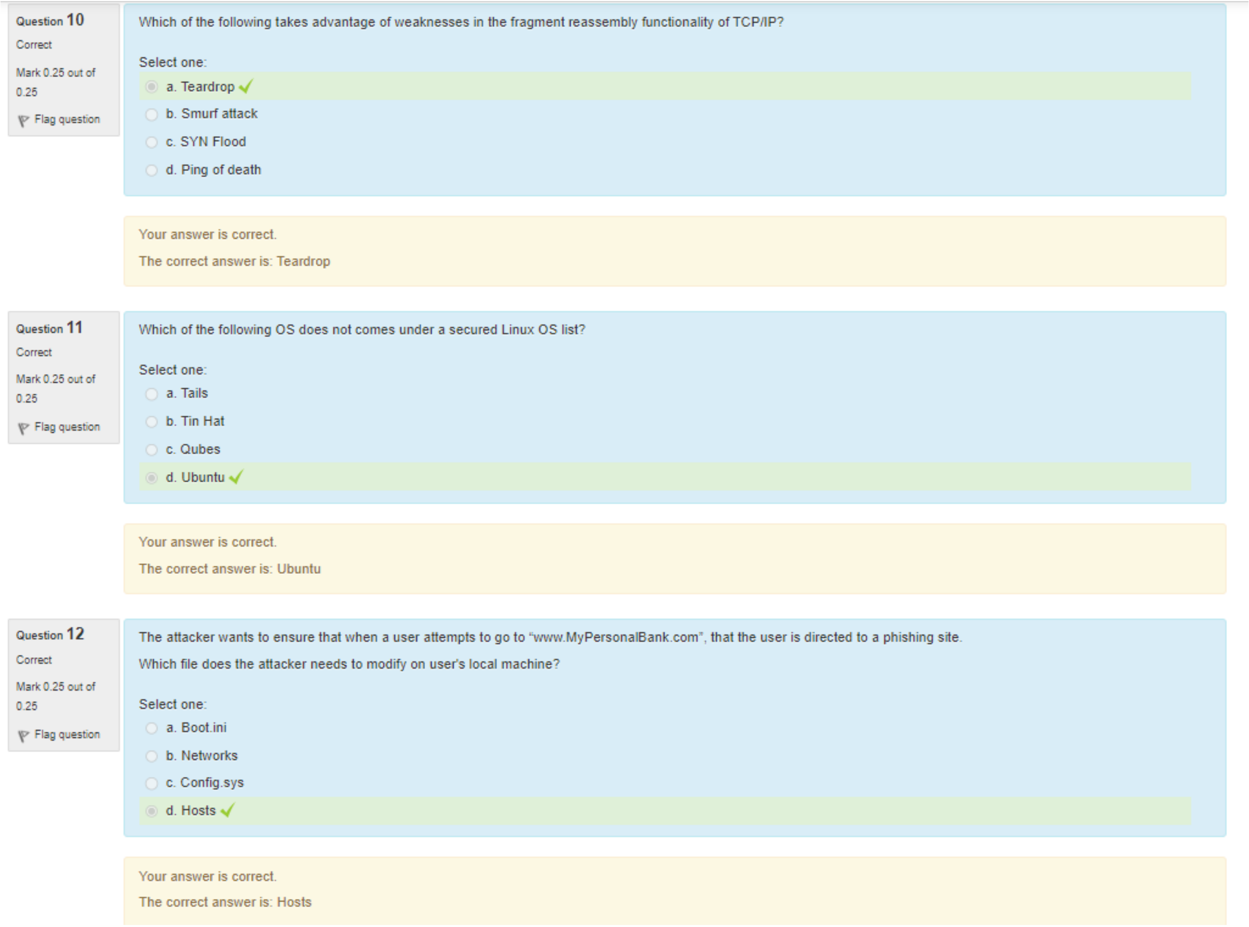
○ b. DES

○ c. RSA

○ d. AES

Your answer is correct.

The correct answer is: TKIP



Question 10

Correct

Mark 0.25 out of 0.25

Flag question

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

Select one:

● a. Teardrop ✓

○ b. Smurf attack

○ c. SYN Flood

○ d. Ping of death

Your answer is correct.

The correct answer is: Teardrop

Question 11

Correct

Mark 0.25 out of 0.25

Flag question

Which of the following OS does not comes under a secured Linux OS list?

Select one:

○ a. Tails

○ b. Tin Hat

○ c. Qubes

● d. Ubuntu ✓

Your answer is correct.

The correct answer is: Ubuntu

Question 12

Correct

Mark 0.25 out of 0.25

Flag question

The attacker wants to ensure that when a user attempts to go to “www.MyPersonalBank.com”, that the user is directed to a phishing site.

Which file does the attacker needs to modify on user's local machine?

Select one:

○ a. Boot.ini

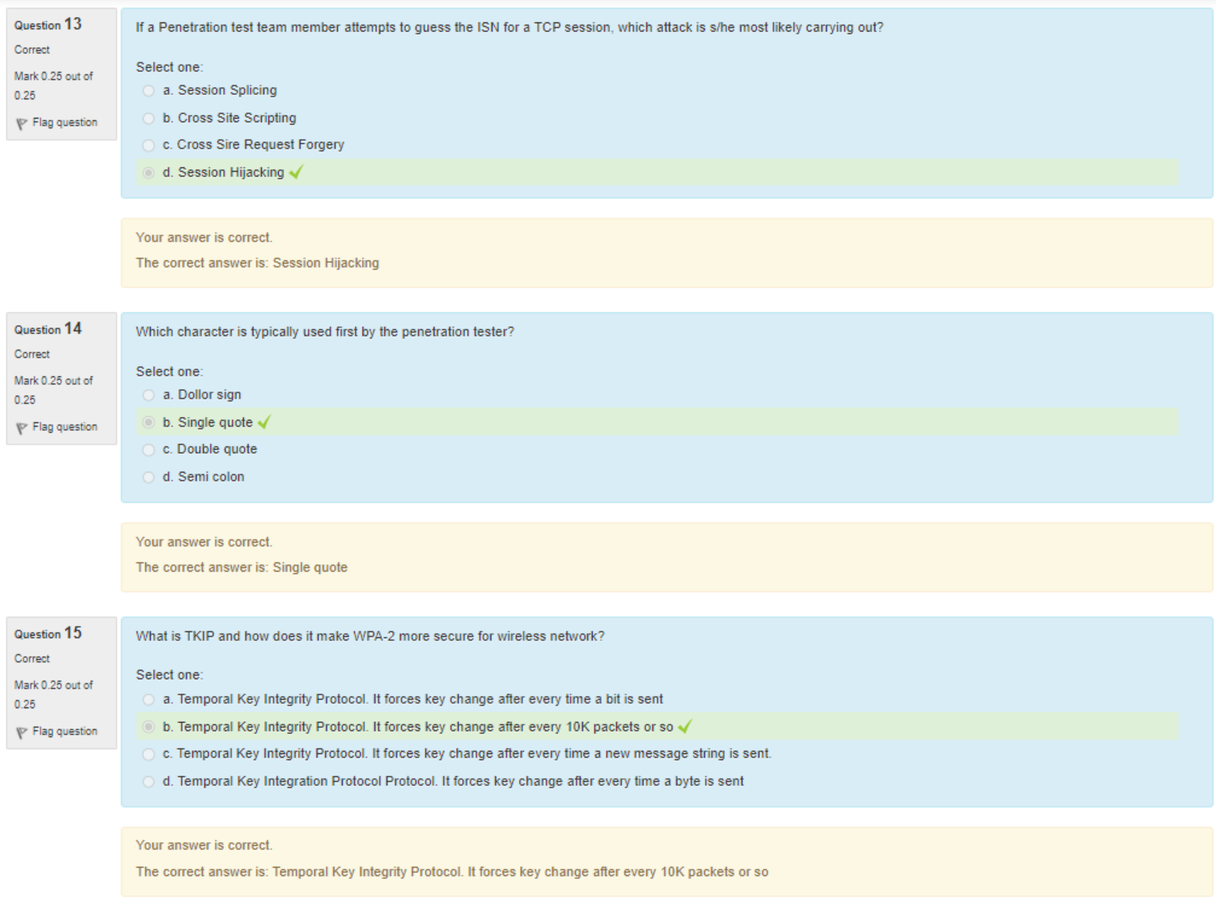
○ b. Networks

○ c. Config.sys

● d. Hosts ✓

Your answer is correct.

The correct answer is: Hosts



Question 13

Correct

Mark 0.25 out of 0.25

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. Cross Site Scripting

○ c. Cross Sire Request Forgery

● d. Session Hijacking ✓

Your answer is correct.

The correct answer is: Session Hijacking

Question 14

Correct

Mark 0.25 out of 0.25

Flag question

Which character is typically used first by the penetration tester?

Select one:

○ a. Dollor sign

● b. Single quote ✓

○ c. Double quote

○ d. Semi colon

Your answer is correct.

The correct answer is: Single quote

Question 15

Correct

Mark 0.25 out of 0.25

Flag question

What is TKIP and how does it make WPA-2 more secure for wireless network?

Select one:

○ a. Temporal Key Integrity Protocol. It forces key change after every time a bit is sent

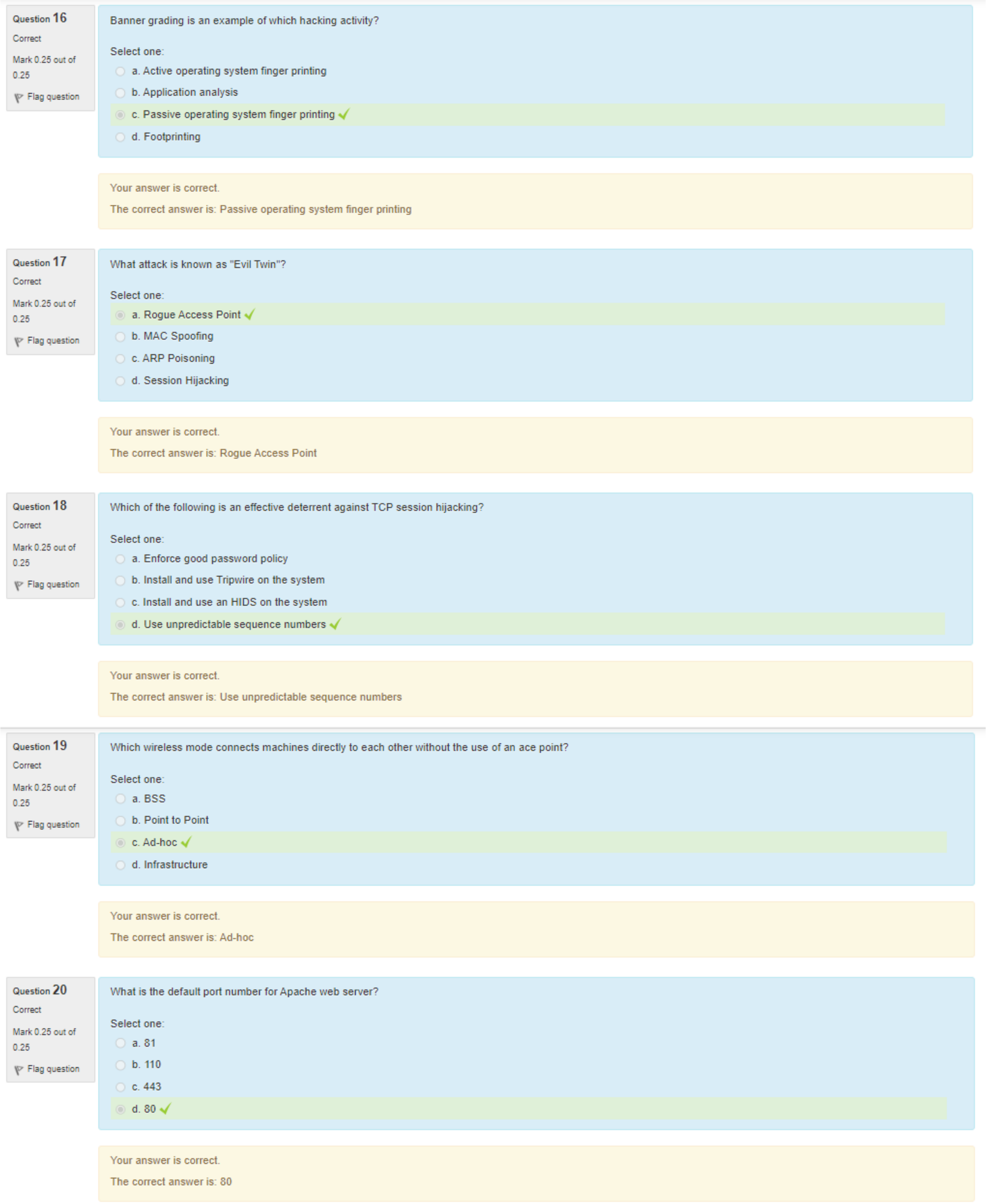
● b. Temporal Key Integrity Protocol. It forces key change after every 10K packets or so ✓

○ c. Temporal Key Integrity Protocol. It forces key change after every time a new message string is sent.

○ d. Temporal Key Integration Protocol Protocol. It forces key change after every time a byte is sent

Your answer is correct.

The correct answer is: Temporal Key Integrity Protocol. It forces key change after every 10K packets or so



Question 16
Correct
Mark 0.25 out of 0.25
Flag question

Banner grading is an example of which hacking activity?

Select one:

○ a. Active operating system finger printing
○ b. Application analysis
● c. Passive operating system finger printing ✓
○ d. Footprinting

Your answer is correct.

The correct answer is: Passive operating system finger printing

Question 17
Correct
Mark 0.25 out of 0.25
Flag question

What attack is known as "Evil Twin"?

Select one:

● a. Rogue Access Point ✓
○ b. MAC Spoofing
○ c. ARP Poisoning
○ d. Session Hijacking

Your answer is correct.

The correct answer is: Rogue Access Point

Question 18
Correct
Mark 0.25 out of 0.25
Flag question

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

Select one:

○ a. Enforce good password policy
○ b. Install and use Tripwire on the system
○ c. Install and use an HIDS on the system
● d. Use unpredictable sequence numbers ✓

Your answer is correct.

The correct answer is: Use unpredictable sequence numbers

Question 19
Correct
Mark 0.25 out of 0.25
Flag question

Which wireless mode connects machines directly to each other without the use of an ace point?

Select one:

○ a. BSS
○ b. Point to Point
● c. Ad-hoc ✓
○ d. Infrastructure

Your answer is correct.

The correct answer is: Ad-hoc

Question 20
Correct
Mark 0.25 out of 0.25
Flag question

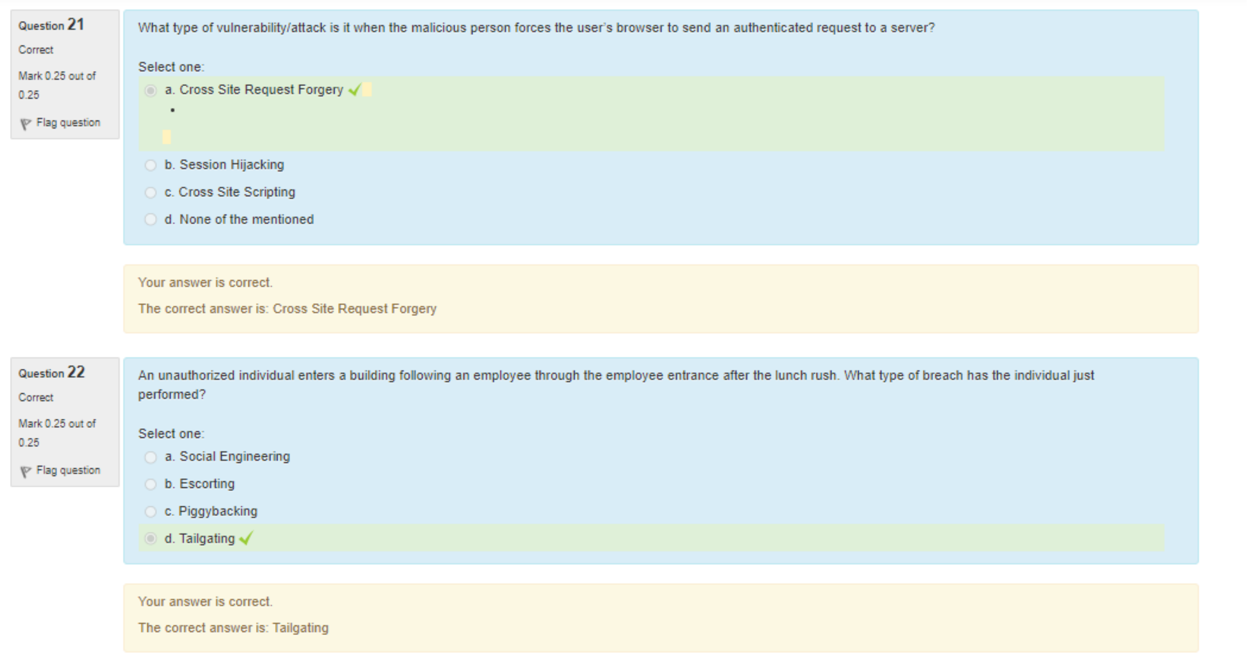
What is the default port number for Apache web server?

Select one:

○ a. 81
○ b. 110
○ c. 443
● d. 80 ✓

Your answer is correct.

The correct answer is: 80



Question 21

Correct

Mark 0.25 out of 0.25

Flag question

What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

Select one:

● a. Cross Site Request Forgery ✓

-

○ b. Session Hijacking

○ c. Cross Site Scripting

○ d. None of the mentioned

Your answer is correct.

The correct answer is: Cross Site Request Forgery

Question 22

Correct

Mark 0.25 out of 0.25

Flag question

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

Select one:

○ a. Social Engineering

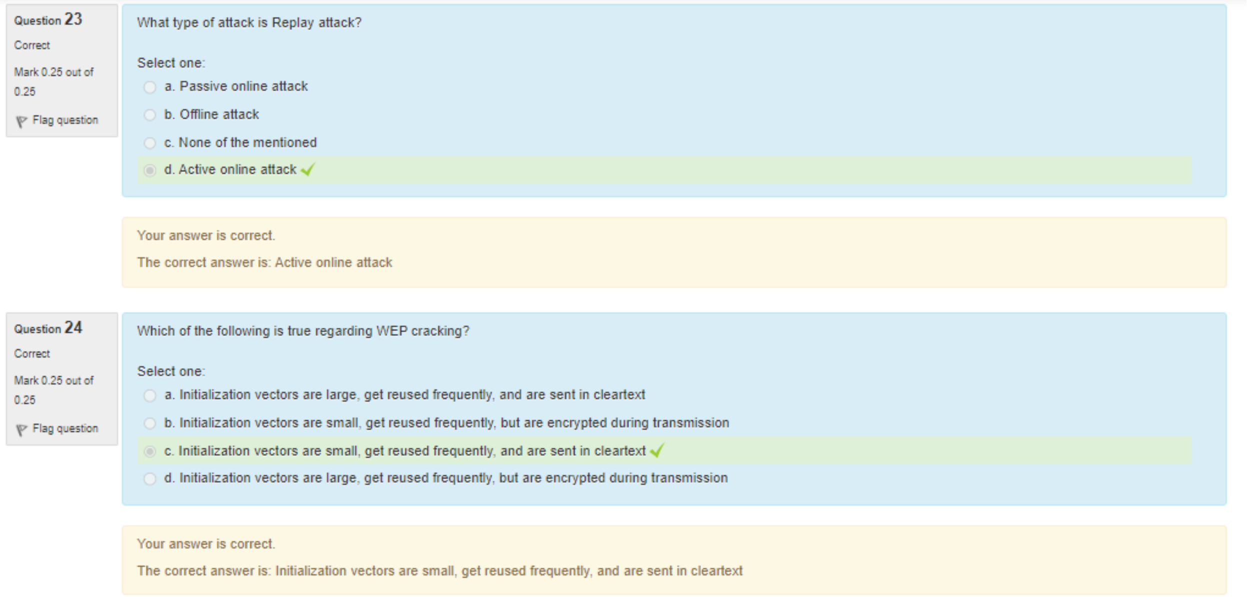
○ b. Escorting

○ c. Piggybacking

● d. Tailgating ✓

Your answer is correct.

The correct answer is: Tailgating



Question 23

Correct

Mark 0.25 out of 0.25

Flag question

What type of attack is Replay attack?

Select one:

○ a. Passive online attack

○ b. Offline attack

○ c. None of the mentioned

● d. Active online attack ✓

Your answer is correct.

The correct answer is: Active online attack

Question 24

Correct

Mark 0.25 out of 0.25

Flag question

Which of the following is true regarding WEP cracking?

Select one:

○ a. Initialization vectors are large, get reused frequently, and are sent in cleartext

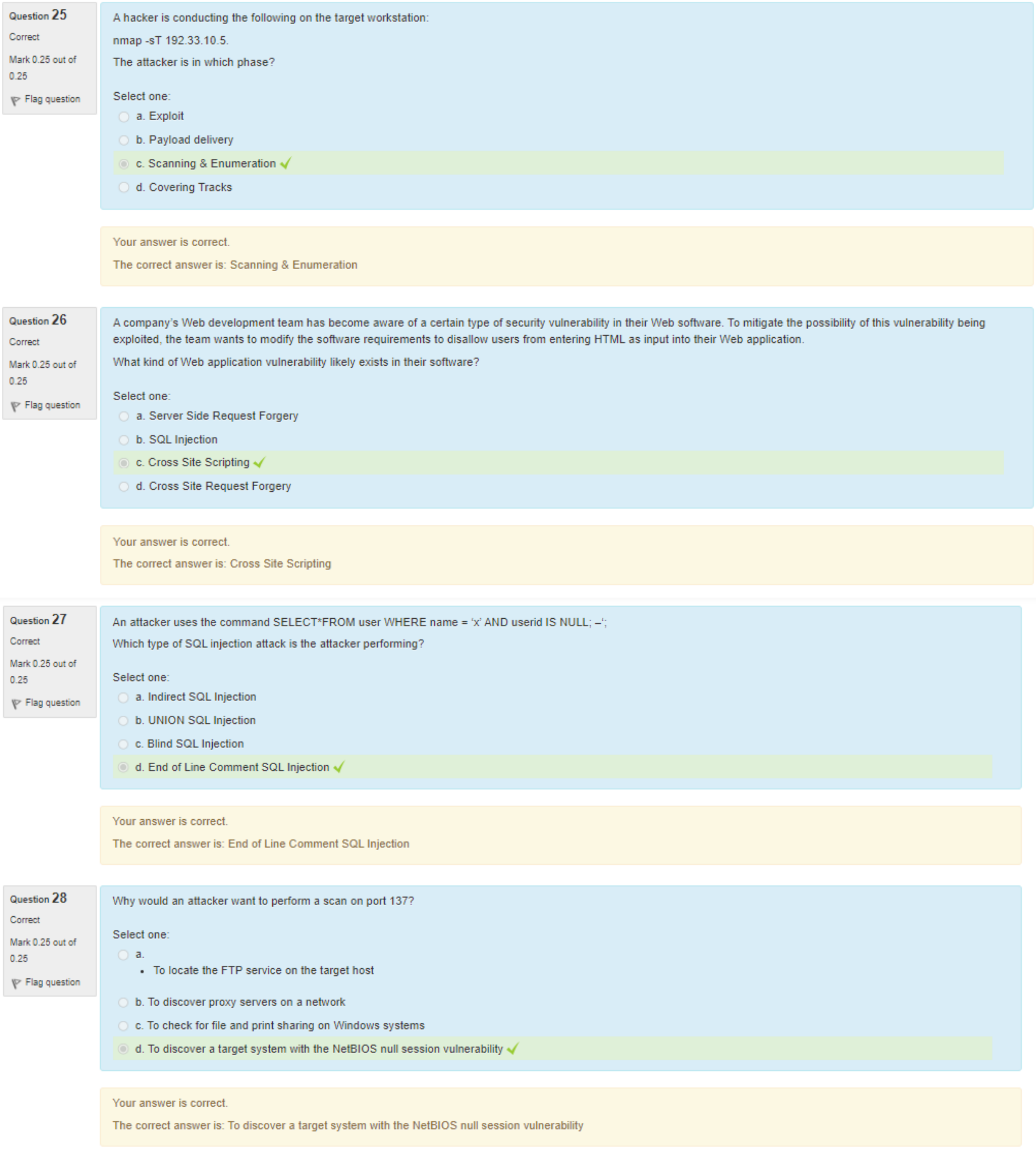
○ b. Initialization vectors are small, get reused frequently, but are encrypted during transmission

● c. Initialization vectors are small, get reused frequently, and are sent in cleartext ✓

○ d. Initialization vectors are large, get reused frequently, but are encrypted during transmission

Your answer is correct.

The correct answer is: Initialization vectors are small, get reused frequently, and are sent in cleartext



Question **25**

Correct

Mark 0.25 out of 0.25

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. Payload delivery

● c. Scanning & Enumeration ✓

○ d. Covering Tracks

Your answer is correct.

The correct answer is: Scanning & Enumeration

Question **26**

Correct

Mark 0.25 out of 0.25

Flag question

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

Select one:

○ a. Server Side Request Forgery

○ b. SQL Injection

● c. Cross Site Scripting ✓

○ d. Cross Site Request Forgery

Your answer is correct.

The correct answer is: Cross Site Scripting

Question **27**

Correct

Mark 0.25 out of 0.25

Flag question

An attacker uses the command SELECT*FROM user WHERE name = ‘x’ AND userid IS NULL; –‘;

Which type of SQL injection attack is the attacker performing?

Select one:

○ a. Indirect SQL Injection

○ b. UNION SQL Injection

○ c. Blind SQL Injection

● d. End of Line Comment SQL Injection ✓

Your answer is correct.

The correct answer is: End of Line Comment SQL Injection

Question **28**

Correct

Mark 0.25 out of 0.25

Flag question

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

Select one:

○ a.
- To locate the FTP service on the target host

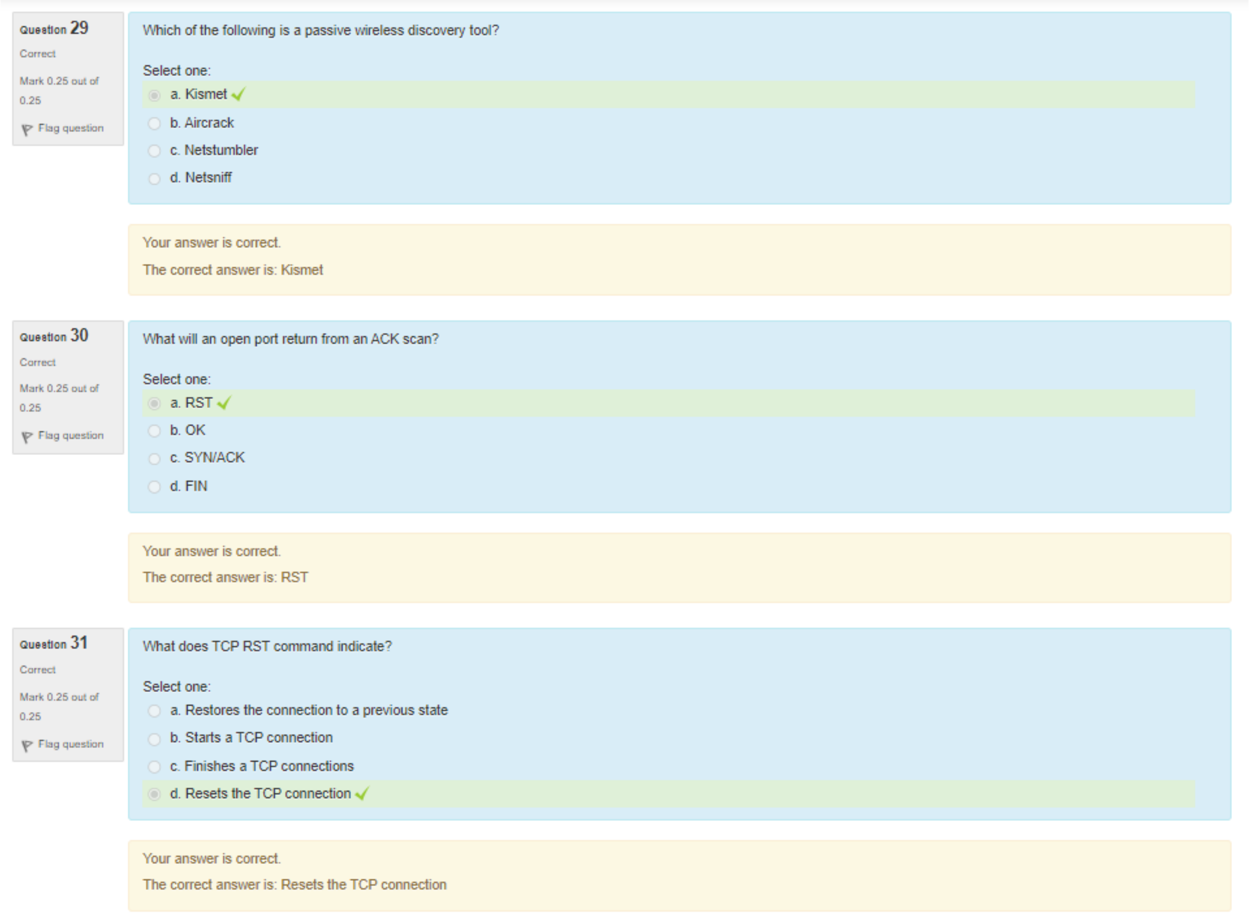
○ b. To discover proxy servers on a network

○ c. To check for file and print sharing on Windows systems

● d. To discover a target system with the NetBIOS null session vulnerability ✓

Your answer is correct.

The correct answer is: To discover a target system with the NetBIOS null session vulnerability



Question 29

Correct

Mark 0.25 out of 0.25

Flag question

Which of the following is a passive wireless discovery tool?

Select one:

● a. Kismet ✓

○ b. Aircrack

○ c. Netstumbler

○ d. Netsniff

Your answer is correct.

The correct answer is: Kismet

Question 30

Correct

Mark 0.25 out of 0.25

Flag question

What will an open port return from an ACK scan?

Select one:

● a. RST ✓

○ b. OK

○ c. SYN/ACK

○ d. FIN

Your answer is correct.

The correct answer is: RST

Question 31

Correct

Mark 0.25 out of 0.25

Flag question

What does TCP RST command indicate?

Select one:

○ a. Restores the connection to a previous state

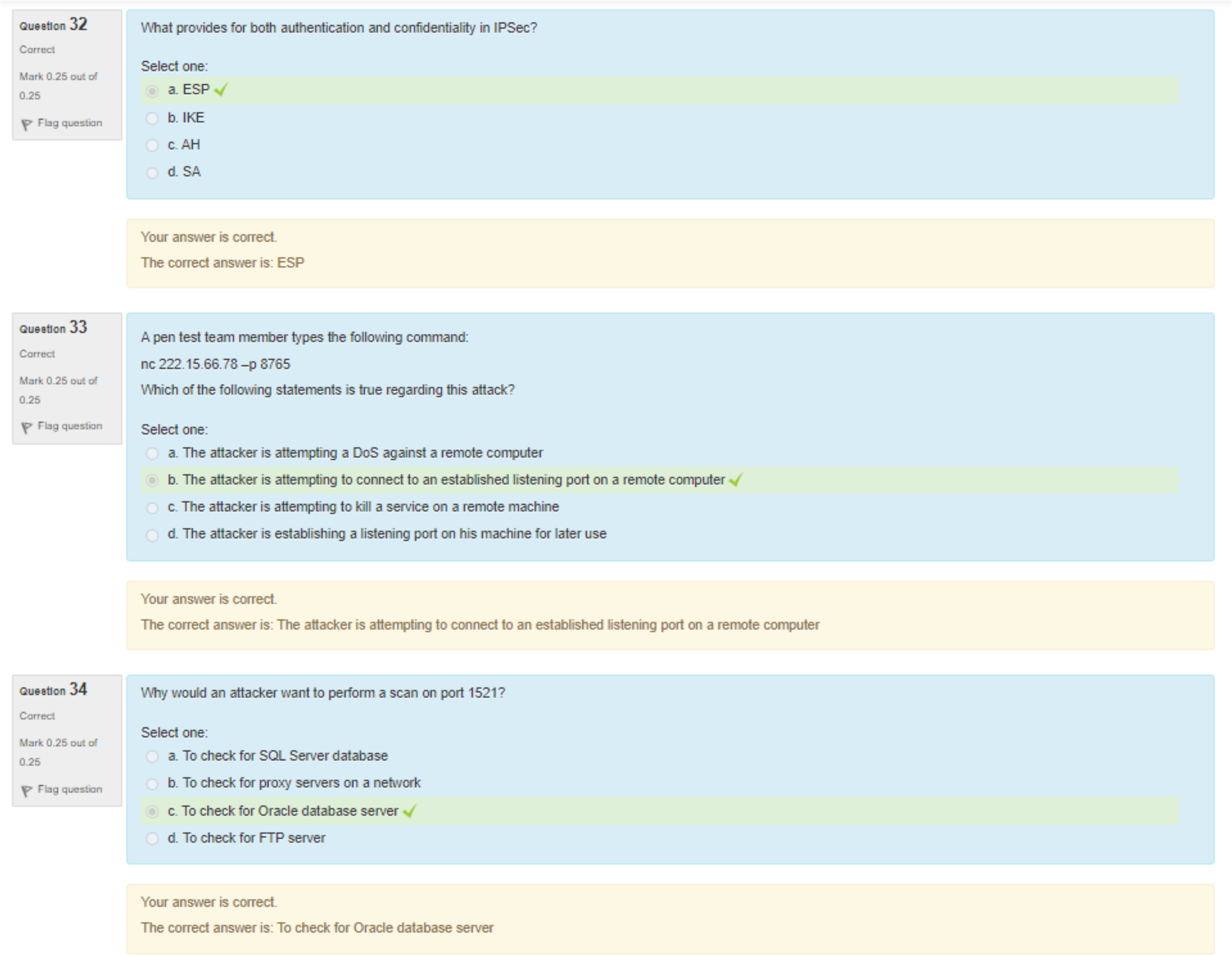
○ b. Starts a TCP connection

○ c. Finishes a TCP connections

● d. Resets the TCP connection ✓

Your answer is correct.

The correct answer is: Resets the TCP connection



Question 32

Correct

Mark 0.25 out of 0.25

What provides for both authentication and confidentiality in IPSec?

Select one:

● a. ESP ✓

○ b. IKE

○ c. AH

○ d. SA

Your answer is correct.

The correct answer is: ESP

Question 33

Correct

Mark 0.25 out of 0.25

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 a DoS against a remote computer

● b. The attacker is attempting to connect to an established listening port on a remote computer ✓

○ c. The attacker is attempting to kill a service on a remote machine

○ d. The attacker is establishing a listening port on his machine for later use

Your answer is correct.

The correct answer is: The attacker is attempting to connect to an established listening port on a remote computer

Question 34

Correct

Mark 0.25 out of 0.25

Why would an attacker want to perform a scan on port 1521?

Select one:

○ a. To check for SQL Server database

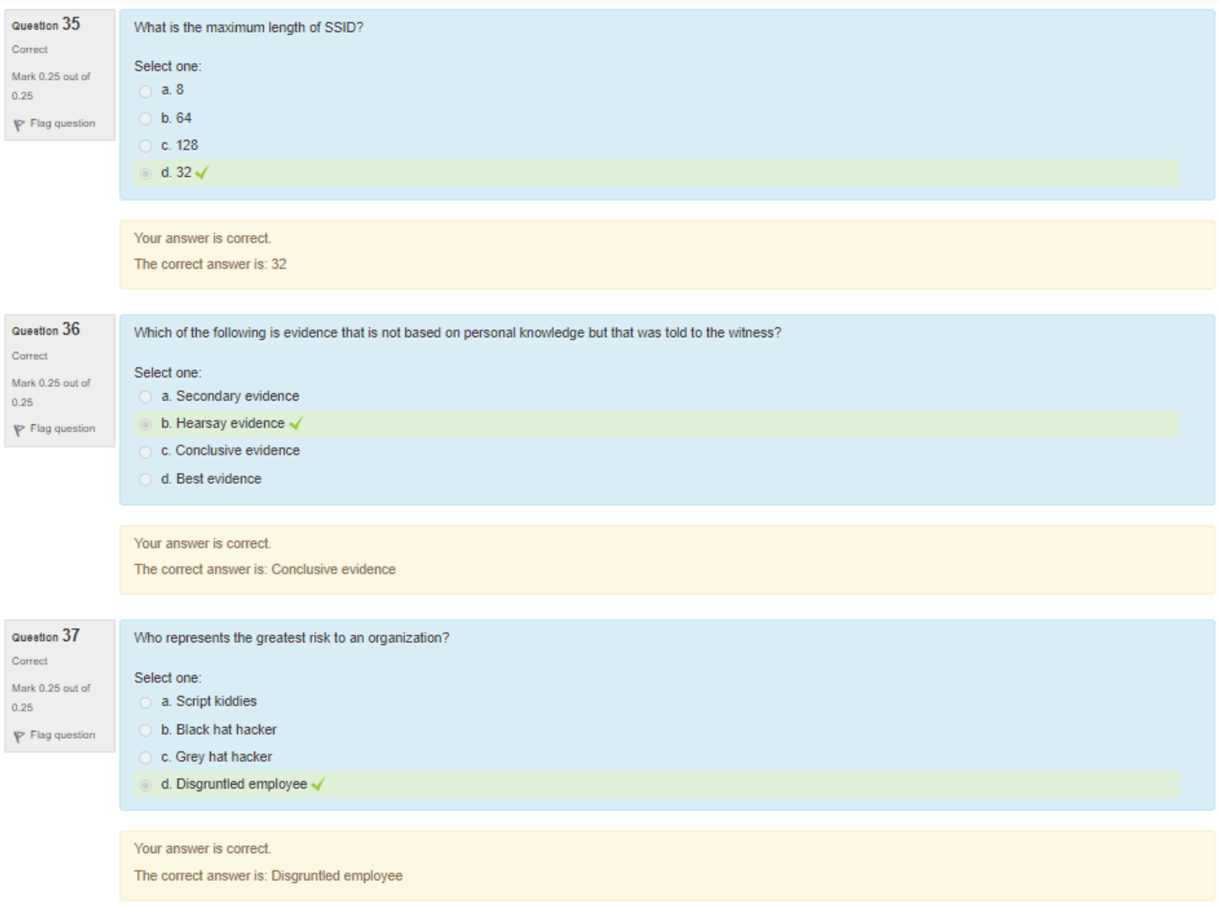
○ b. To check for proxy servers on a network

● c. To check for Oracle database server ✓

○ d. To check for FTP server

Your answer is correct.

The correct answer is: To check for Oracle database server



Question 35

Correct

Mark 0.25 out of 0.25

Flag question

What is the maximum length of SSID?

Select one:

○ a. 8

○ b. 64

○ c. 128

● d. 32 ✓

Your answer is correct.

The correct answer is: 32

Question 36

Correct

Mark 0.25 out of 0.25

Flag question

Which of the following is evidence that is not based on personal knowledge but that was told to the witness?

Select one:

○ a. Secondary evidence

● b. Hearsay evidence ✓

○ c. Conclusive evidence

○ d. Best evidence

Your answer is correct.

The correct answer is: Conclusive evidence

Question 37

Correct

Mark 0.25 out of 0.25

Flag question

Who represents the greatest risk to an organization?

Select one:

○ a. Script kiddies

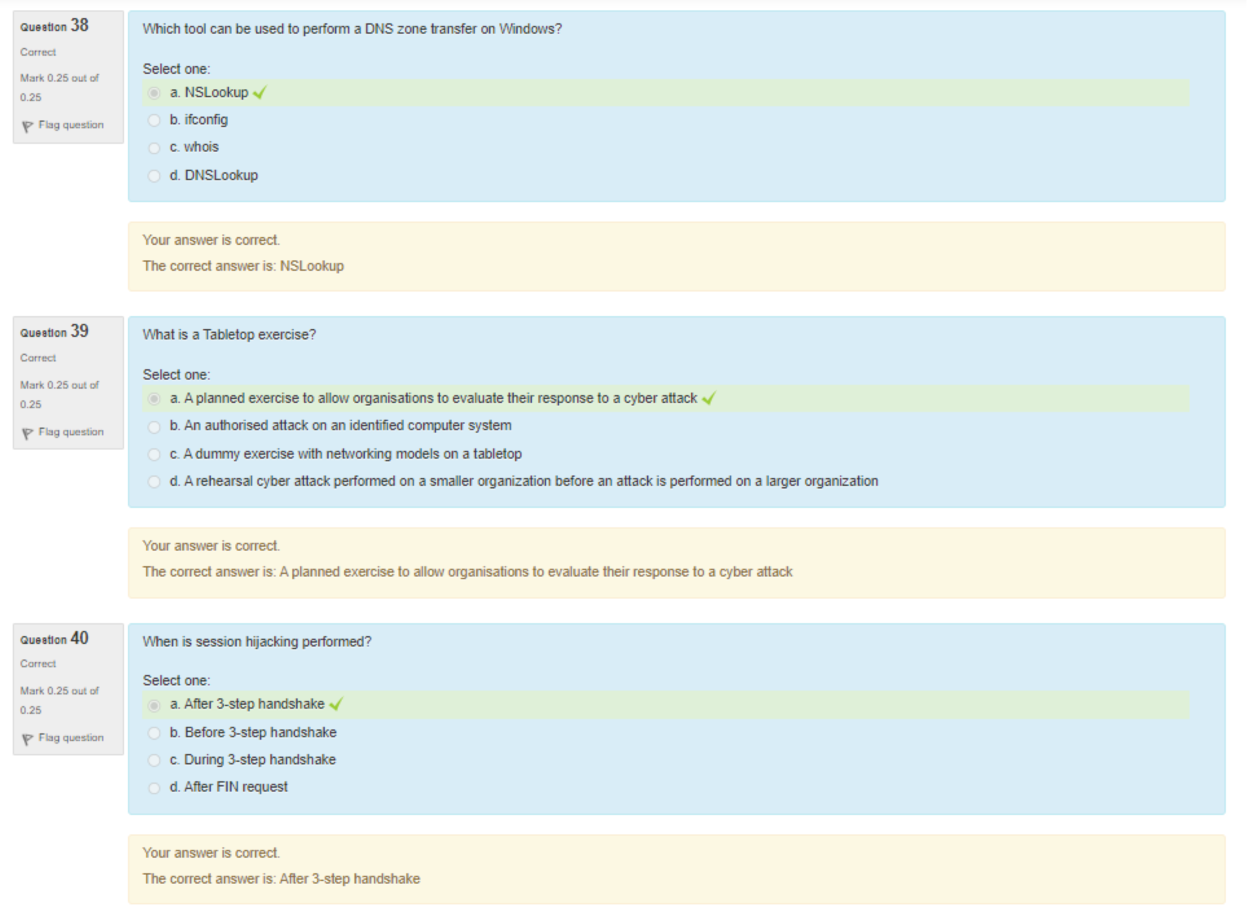
○ b. Black hat hacker

○ c. Grey hat hacker

● d. Disgruntled employee ✓

Your answer is correct.

The correct answer is: Disgruntled employee



Question 38

Correct

Mark 0.25 out of 0.25

Flag question

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

Select one:

● a. NSLookup ✓

○ b. ifconfig

○ c. whois

○ d. DNSLookup

Your answer is correct.

The correct answer is: NSLookup

Question 39

Correct

Mark 0.25 out of 0.25

Flag question

What is a Tabletop exercise?

Select one:

● a. A planned exercise to allow organisations to evaluate their response to a cyber attack ✓

○ b. An authorised attack on an identified computer system

○ c. A dummy exercise with networking models on a tabletop

○ d. A rehearsal cyber attack performed on a smaller organization before an attack is performed on a larger organization

Your answer is correct.

The correct answer is: A planned exercise to allow organisations to evaluate their response to a cyber attack

Question 40

Correct

Mark 0.25 out of 0.25

Flag question

When is session hijacking performed?

Select one:

● a. After 3-step handshake ✓

○ b. Before 3-step handshake

○ c. During 3-step handshake

○ d. After FIN request

Your answer is correct.

The correct answer is: After 3-step handshake