

Ethical Hacking QUIZ 2

Question 1

Correct

Mark 0.25 out of 0.25

🚩 Flag question

What is DNS Zone transfer?

Select one:

- ☐ a. Allows secondary DNS server to share its zone database with primary DNS server
- ☐ b. None of the mentioned
- ☒ c. Allows secondary DNS server to update its zone database from primary DNS server ✓
- ☐ d. Allows secondary DNS server to functional independently of primary DNS server

Your answer is correct.

The correct answer is: Allows secondary DNS server to update its zone database from primary DNS server

Question 2

Correct

Mark 0.25 out of 0.25

🚩 Flag question

ReamWeaver is tool for?

Select one:

- ☐ a. Internet scrapping
- ☐ b. Wardriving
- ☐ c. Intelligence gathering
- ☒ d. Website cloning ✓

Your answer is correct.

The correct answer is: Website cloning

Question 3

Correct

Mark 0.25 out of 0.25

🚩 Flag question

Which of these is not a valid enumeration type?

Select one:

- ☐ a. NTP
- ☒ b. FTP ✓
- ☐ c. SMB
- ☐ d. NetBIOS

Your answer is correct.

The correct answer is: FTP

Question 4

Correct

Mark 0.25 out of 0.25

🚩 Flag question

Which command can be used to find and plot the path to an IP address?

Select one:

- ☐ a. Nmap
- ☒ b. Traceroute ✓
- ☐ c. Nslookup
- ☐ d. Whoami

Your answer is correct.

The correct answer is: Traceroute

Question 5

Correct

Mark 0.25 out of 0.25

Flag question

Which of the following is a passive wireless discovery tool?

Select one:

- ☐ a. Net Sniff
- ☐ b. Net Stumbler
- ☐ c. AirCrack
- ☒ d. Kismet ✓

Your answer is correct.

The correct answer is: Kismet

Question 6

Correct

Mark 0.25 out of 0.25

Flag question

Which is a foot printing tool?

Select one:

- ☐ a. Whois
- ☐ b. Google Groups
- ☒ c. All of the mentioned ✓
- ☐ d. Sam Spade

Your answer is correct.

The correct answer is: All of the mentioned

Question 7

Correct

Mark 0.25 out of 0.25

Flag question

What type of information can be collected by scanning port 137?

Select one:

- ☐ a. Locate the FTP service on target host
- ☒ b. Discover a target system with the NetBIOS null session vulnerability ✓
- ☐ c. Discover Proxy servers on a network
- ☐ d. File and Print sharing details on Windows

Your answer is correct.

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

Question 8

Correct

Mark 0.25 out of 0.25

Flag question

What information is normally gathered during foot printing?

Select one:

- ☐ a. Location details
- ☐ b. Domain name details
- ☒ c. All of the mentioned ✓
- ☐ d. Contact details

Your answer is correct.

The correct answer is: All of the mentioned

Question 9

Correct

Mark 0.25 out of 0.25

🚩 Flag question

What is the maximum length of SSID name?

Select one:

- ☐ a. 16 chars
- ☐ b. 48 chars
- ☒ c. 32 chars ✓
- ☐ d. 64 chars

Your answer is correct.

The correct answer is: 32 chars

Question 10

Correct

Mark 0.25 out of 0.25

🚩 Flag question

Banner grabbing is an example of?

Select one:

- ☒ a. Passive OS fingerprinting ✓
- ☐ b. Active OS fingerprinting
- ☐ c. Footprinting
- ☐ d. Application fingerprinting

Your answer is correct.

The correct answer is: Passive OS fingerprinting

Question 11

Correct

Mark 0.25 out of 0.25

🚩 Flag question

Which one is not a scanning tool?

Select one:

- ☐ a. Zenmap
- ☐ b. Nmap
- ☒ c. Ghidra ✓
- ☐ d. Wireshark

Your answer is correct.

The correct answer is: Ghidra

Question 12

Correct

Mark 0.25 out of 0.25

🚩 Flag question

Core function of Internet are managed by?

Select one:

- ☐ a. DARPA
- ☐ b. GNSO
- ☐ c. CCNSO
- ☒ d. ICANN ✓

Your answer is correct.

The correct answer is: ICANN

Question 13

Correct

Mark 0.25 out of 0.25

🚩 Flag question

Which wireless standard can operate speed above 100 MB/per second and usage both 2.4 and 5 GHz bands?

Select one:

- ☐ a. 802.11a
- ☐ b. 802.11g
- ☐ c. 802.11b
- ☒ d. 802.11n ✓

Your answer is correct.

The correct answer is: 802.11n

Question 14

Correct

Mark 0.25 out of 0.25

🚩 Flag question

What type of scanning is a packet with all flags set?

Select one:

- ☐ a. TCP Connect
- ☐ b. Full scanning
- ☐ c. SYN Scan
- ☒ d. XMAS ✓

Your answer is correct.

The correct answer is: XMAS

Question 15

Correct

Mark 0.25 out of 0.25

🚩 Flag question

Which tool is used to enumerate 'hidden' files in a website?

Select one:

- ☐ a. Wget
- ☐ b. RevealAll
- ☒ c. DirBuster ✓
- ☐ d. All of the mentioned

Your answer is correct.

The correct answer is: DirBuster

Question 16

Correct

Mark 0.25 out of 0.25

🚩 Flag question

What is 'Evil Twin' attack?

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 17

Correct

Mark 0.25 out of 0.25

Flag question

Which record type reveals the IP of a domain's mail server in Nslookup command?

Select one:

- ☐ a. NX
- ☒ b. MX ✓
- ☐ c. HINFO
- ☐ d. CNAME

Your answer is correct.

The correct answer is: MX

Question 18

Correct

Mark 0.25 out of 0.25

Flag question

Which wireless mode connects machines directly to one another without an Access Point?

Select one:

- ☐ a. Point to Point
- ☐ b. WEP
- ☒ c. Ad-hoc ✓
- ☐ d. BSS

Your answer is correct.

The correct answer is: Ad-hoc

Question 19

Correct

Mark 0.25 out of 0.25

Flag question

Which tool(s) is/are used for LDAP scanning?

Select one:

- ☐ a. LEX
- ☒ b. All of the mentioned ✓
- ☐ c. Explorer
- ☐ d. LDAP Admin

Your answer is correct.

The correct answer is: All of the mentioned

Question 20

Correct

Mark 0.25 out of 0.25

Flag question

ARIN is an organisation responsible for?

Select one:

- ☐ a. RIR for Europe
- ☐ b. None of the mentioned
- ☒ c. RIR - mainly for US and Canada ✓
- ☐ d. RIR for Americas (North and South America)

Your answer is correct.

The correct answer is: RIR - mainly for US and Canada