CET2032 - Computer Networks & Network Security - Practicum 03

1. Inside the P03.pcapng file, find the number of ping requests sent. (2 marks)

A: The number of ping requests sent is 6.

2. Find the IP address of the device with the MAC address 08:00:27:7c:8e:8e. (3 marks)

A: The IP address of the device is 10.0.2.22.

3. Find the version of Internet Group Management Protocol that was used in the transmission. (2 marks)

A: The version of IGMP used is version 3.

4. Find the name of the host with the IP address 10.0.2.22 and include a screenshot of it as proof. (6 marks)

A: The name of the host with the IP address 10.0.2.22 is kali.

```
▾ Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xa823310c
    Seconds elapsed: 0
  › Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.0.2.22
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_7c:8e:8e (08:00:27:7c:8e:8e)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  › Option: (53) DHCP Message Type (Request)
  ▾ Option: (12) Host Name
      Length: 4
      Host Name: kali
  › Option: (55) Parameter Request List
  › Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000000000000000000000000000
```

5. Identify the IP address of the DHCP server. (5 marks)

A: The IP address of the DHCP server is 10.0.2.3

6. Looking at frame 6822, we understand that it is a DHCP Discover packet trying to obtain an IP address from a DHCP server. What is the client that is trying to get an IP address in this particular frame? Did the client managed to obtain an IP address successfully? Explain your answer. (20 marks)

A: The client is IP 0.0.0.0, MAC address 08:00:27:4b:e3:60, host name MSEDGEWIN10.
Yes, the client managed to get an IP address successfully.

It can be seen that there are 4 packets, DHCP Discover, DHCP offer, DHCP request, DHCP ACK in frames 6822, 6823, 6824, 6825 respectively. These packets are part of the IP address allocation/lease procedure.

The DHCP Discover packet is sent out by the client and it is trying to locate all available DHCP servers on the same subnet. In that packet, if the Dynamic Host Configuration Protocol (Discover) is expanded, Option: (50) Requested IP Address shows that the requested IP address is 10.0.2.15.

The DHCP Offer packet is sent out by the DHCP server and it is trying to tell the client that the IP address requested is available, it also tells the client which DHCP server is sending this packet. In that packet, if the Dynamic Host Configuration Protocol (Offer) is expanded, under Your (client) IP address, it shows 10.0.2.15 which is the IP address requested by the client. Looking at Option: (54) DHCP Server Identifier, the IP address 10.0.2.3 of the DHCP server is shown.

The DHCP Request packet is sent out by the client. If the client receives multiple DHCP Offer requests due to multiple DHCP servers on the same subnet, it will choose one of these DHCP servers and the IP address offered. It will then send the DHCP Request to all the DHCP servers and so all the DHCP servers know if they have been chosen or not. In that packet, if the Dynamic Host Configuration Protocol (Request) is expanded, Option: (50) Requested IP Address shows that the requested IP address is 10.0.2.15. Looking at Option: (54) DHCP Server Identifier, the IP address 10.0.2.3 of the DHCP server is shown. Because there is only 1 DHCP Offer message received, only 1 DHCP Request message is sent.

The DHCP ACK packet is sent out by the DHCP server if the IP address shown in DHCP Server Identifier in the DHCP Request matches its own IP address. The DHCP ACK packet will contain all the network configuration data so that the client can configure the network interface using those data and connect to the Internet. In that packet, if the Dynamic Host Configuration Protocol (Offer) is expanded, Option: (50) Requested IP Address shows that the requested IP address is 10.0.2.15. Looking at Option: (54) DHCP Server Identifier, the IP address 10.0.2.3 of the DHCP server is shown and looking at Option (51) IP Address Lease Time is 10 minutes.

In conclusion, the client managed to obtain an IP address 10.0.2.15 successfully from DHCP server 10.0.2.3.

7. Identify the IP address of the router in the network. (5 marks)

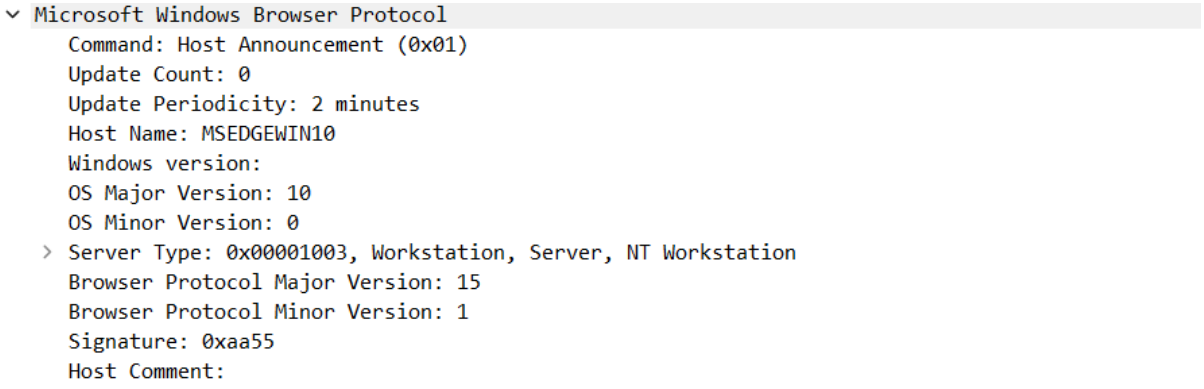
A: The IP address of the router in the network is 10.0.2.1

8. Identify all the IP addresses of the DNS servers which are available for the hosts in the network. (6 marks)

A: IP addresses of the DNS servers are 103.86.96.100 and 103.86.99.100

9. Find the name of the host with the IP address 10.0.2.15 and include a screenshot of it as proof. (6 marks)

A: The name of the host with the IP address 10.0.2.15 is MSEDGEWIN10.



10. Identify the IP address of the attacker. (10 marks)

A: 10.0.2.22

11. State the first command executed by the intruder in the system. (5 marks)

A: The first command executed by the intruder is whoami

12. Find the process ID for the Remote Desktop Protocol session. (10 marks)

A: The process ID for the RDP session is 552

13. For the account IEUser in the system, find the maximum password age. (5 marks)

A: For the account IEUser in the system, the maximum password age is 42 days.

14. Find the location which stores the file "working capital analysis.xls" and give the absolute file path. (5 marks)

A: The absolute file path is C:\Users\IEUser\Documents\working capital analysis.xls

15. Find the hidden message located in the comments and include a screenshot of it as proof. (10 marks)

A: pcap analysis is fun!