CET2032 - Computer Networks & Network Security - Practicum 03

Topics Covered: Application-layer Protocols

Learning Objectives:

- Understanding of the DHCP protocol
- Identifying threat actor in a network
- Familiarize with packet flow and Wireshark

Deliverables:

- Submit a single PDF file containing your name and answers to the tasks below with the format `CET2032_P03_<Trainee_name>.pdf`. Eg: `CET2032_P03_John_Doe.pdf`.

Network Traffic Analysis

You are given a ".pcapng" file, **P03.pcapng**, with network traffic captured on a network that was breached by intruder. Using the pcapng file, answer the following questions.

Use the **resources.pdf** file to help you in this practicum.

Tasks

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

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

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

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)

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

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)

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

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

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)

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

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

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

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

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

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

Rubrics

For the maximum allocation of marks, refer to the marks assigned for each task.