Name: Amit S Terdal
CSU ID: 2887869

Exercise 2: Lab Packet Analysis and Sniffing

Part One: Pack Analysis

File: Challenge101-0.pcapng

1.How many packets are in this trace file?

20 packets

2.What IP hosts are making a TCP connection in frames 1, 2, and 3?

Frame 1: 192.168.1.108 and 50.19.229.205
Frame 2: 50.19.229.205 and 192.168.1.108
Frame 3: 192.168.1.108 and 50.19.229.205

3.What HTTP command is sent in frame 4?

The HTTP command in frame 4 is GET.

4.What is the length of the largest frame in this trace file?

Frame 4 shows a length of 1384 bytes. Looking at the other packets, this appears to be the largest frame in the visible portion of the capture. Again, to be absolutely sure, you'd need to check the entire capture in Wireshark.

5.What protocols are seen in protocol column?

The protocols seen are: TCP and HTTP.

6.What responses are sent by the HTTP server?

The HTTP server (50.19.229.205) sends HTTP/1.1 302 Found responses in frames 6, 8, 10, 13, and 16.

File: Challenge101-1.pcapng

7. What frame number does the client request the default root web page (“/”)?

Frame 13 shows the HTTP GET request for the default root web page ("GET / HTTP/1.1").

8. What response does the server send in frame 17?

Frame 17 is an HTTP response. The server sends an HTTP/1.1 200 OK response.

9. What is the largest TCP delta (delay) value seen in this trace file?

The largest TCP delta (delay) value is indeed 15.438012000 seconds in frame 285

10. How many SYN packets arrived after at least 1 second delay?

4 SYN packets arrived after at least 1 second delay are frame 5, 2, 6 and 3.

File: Challenge101-3.pcapng

11. How many frames travel to or from 80.78.246.209?

32 frames travel to or from 80.78.246.209

12. How many DNS packets are in the trace file?

8 DNS packets are in the trace file.

13. How many frames have the TCP SYN bit set to 1?

12 frames have the TCP SYN bit set to 1.

14. How many frames contain the string "set-cookie" in upper case or lower case?

2 frames contain the string "set-cookie" in upper case or lower case.

15. How many frames contain a TCP delta time greater than 1 second?

18 frames contain a TCP delta time greater than 1 second

Part Two: Capturing Packets using ARP poisoning

• *On your **Windows** 7 system, install **WinSCP, Filezilla**, or your favorite FTP client.*
• *On you **Kali Linux** system, start a packet capture with **Wireshark** on the **eth0** interface.*
• *Turn on packet forwarding with the following command:*

echo 1 > /proc/sys/net/ipv4/ip_forward

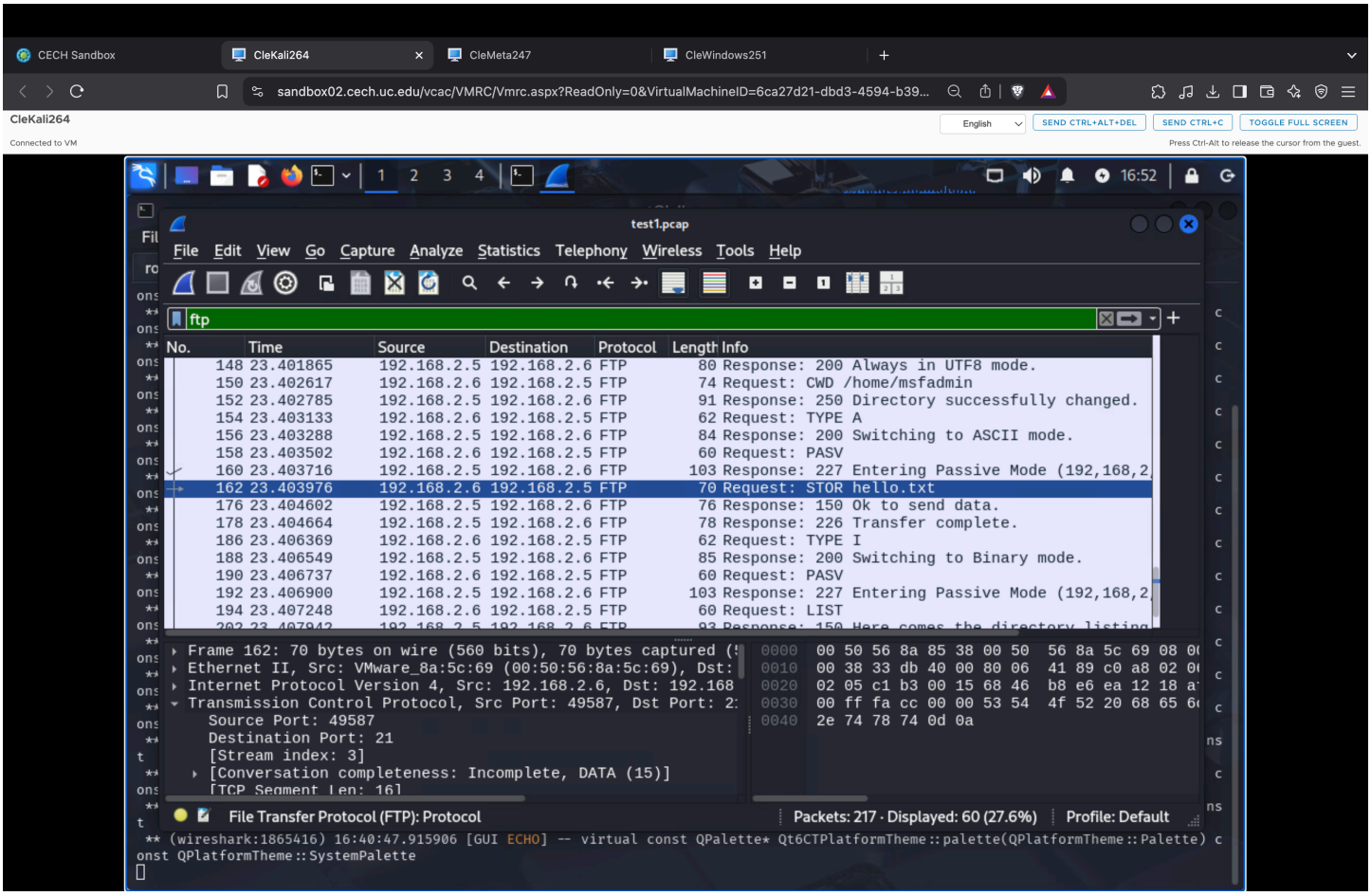
• *Start ARP poisoning your Windows 7 and metaploitable2 systems:*

arpspoof –i eth0 –t <IP of Windows 7> <IP of metasploitable2>

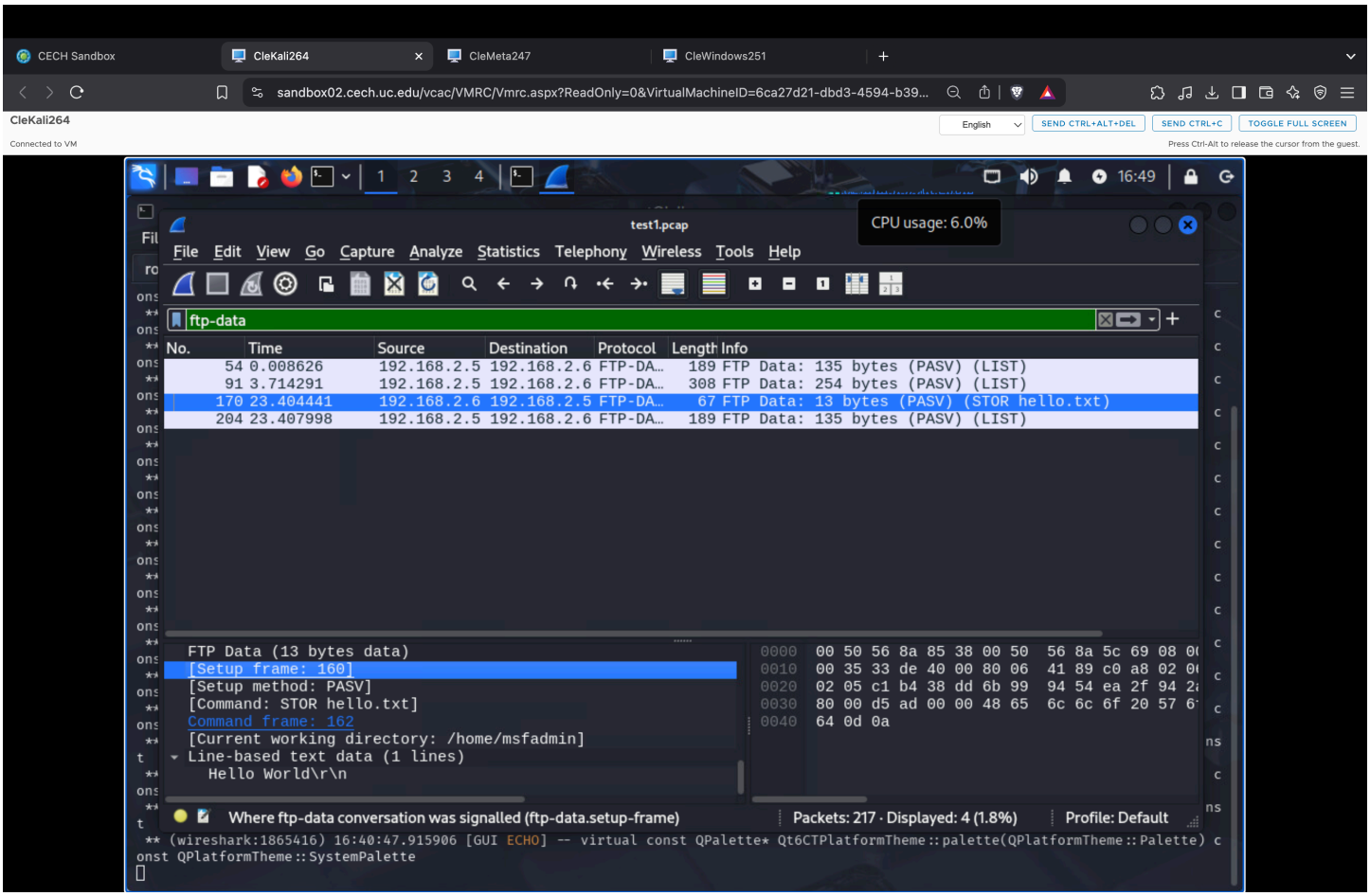
In a new terminal run the same command, but rearrange the IP addresses so you are capturing both sides of the conversation.
• *On you **Windows** 7 system, connect to **FTP** on your **metaploitable2** system using **port 21**.*
• *Login with user: **msfadmin** password: **msfadmin***
• *Create a text file on your Windows 7 system with the words "**Hello World**" in the text.*
• *Transfer this file to the metasploitable2 system using ftp.*
• *Stop the packet capture and hit **ctrl-c** in both terminal windows to stop the ARP poisoning.*
• *Analyze the packet capture and answer the following questions/paste screen shots.*
Find the packets that contain the username and password for the ftp server

16. Paste a screen shot showing each of these packets.

Find the packet that contains the text file you transferred.



17. Paste a screen shot showing the FTP Data for this



18. Are there any packets that might send up a red flag that an ARP poisoning attack is occurring?

There No packets but we can find ARP poisoning attack is occurring by ARP traffic.
Normal ARP traffic shows each machine claiming its own MAC address for its IP.
During an ARP poisoning attack, the attacker's MAC address will be associated with the IP addresses of both target machines.
You will see multiple ARP replies associating the attackers MAC address with both the targets IP addresses.
The target machines ARP tables will be constantly being updated with the attackers mac address.
This constant arp traffic, and the incorrect mac address associations are a big red flag.

19. In this example, are attack focused on two systems on the same network. If you were trying to capture traffic coming and going from two systems on different networks, what IPs would you want to poison?

Yes, the attack is focused on two systems on the same network.
If you were trying to capture traffic between two systems on different networks, you would poison the default gateway of each target network.

For example, if the two systems were on networks 192.168.1.0/24 and 10.0.0.0/24, you would poison the default gateway of 192.168.1.0/24 with the 192.168.1.x IP, and the default gateway of 10.0.0.0/24 with the 10.0.0.x IP, where x is the gateway IP.

20. What could likely occur alerting security to an attack in the last question?

ARP Table Anomalies: Network monitoring tools would detect the constant changes in the ARP tables of the targeted systems and the gateways.

Duplicate MAC Address Warnings: Some network devices and security systems can detect duplicate MAC addresses on the network, which is a key indicator of ARP poisoning.

Increased Network Traffic: The attacker's machine would be handling a lot of traffic, which could cause a noticeable increase in network load.

Intrusion Detection/Prevention Systems (IDS/IPS): These systems are designed to detect and prevent network attacks, including ARP poisoning. They would flag the unusual ARP traffic and potential man-in-the-middle activity.

Latency/Performance Issues: The targets and the gateway might experience noticeable performance degradation due to the increased traffic and the attacker's machine processing the traffic.

MAC Address Monitoring: Specialized security tools monitor MAC address changes and could detect the attackers mac address being associated with multiple IP addresses.