# **Network Forensic by Wireshark**

## **Assignment Objectives:**

The objective of this assignment is to conduct network forensic analysis using Wireshark. Participants will simulate a DDoS attack and capture the network traffic using Wireshark. Subsequently, they will analyze the captured packets to understand the network activities during the attack. Additionally, participants will take on the role of a Network Defense Analyst in three different scenarios, where they will thoroughly analyze captured network traffic to identify malicious activities, understand network behavior, and extract relevant information such as service and protocol usage, IP and MAC addresses of devices, and the exfiltrated file.

## **Grading**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Task** | **Item Graded** | **Points** | **Task** | **Item Graded** | **Points** |
| Task 5 | Screenshot | 5 | Task 13 | Short Answer | 5 |
| Task 8 | Short Answer | 5 | Task 14 | Short Answer | 5 |
| Task 9 | Short Answer | 5 | Task 15 | Short Answer | 5 |
| Task 10 | Short Answer | 5 | Task 16 | Short Answer | 5 |
| Task 11 | Short Answer | 5 | Task 17 | Short Answer | 5 |
| Task 12 | Short Answer | 5 | Task 18 | Short Answer | 5 |
| **Total** | | | **60** | | |

## **Preparation:**

1. You need two virtual machines to run this assignment:
   * VM1: Kali Linux
   * VM2: one of the following – Ubuntu, Windows 7, Windows XP, or Windows Server 2008
2. Ensure both VMs are connected to the same network.

## **Tools Required:**

* Wireshark
* hping3

## **Run Wireshark:**

Task 1: On the internal Kali VM start the Wireshark application in capture mode: Kali -> Applications -> Sniffing & Spoofing -> wireshark.

Task 2: Select the interface you wish to monitor (i.e., eth0)

## **Simulate a DDoS Attack:**

Task 3: Open a terminal in the Kali VM and launch a simulated DDoS attack with the following command.

* hping3 --rand-source --flood -f -S 192.168.10.xxx -p 80

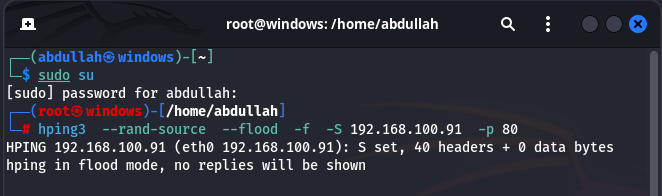
We will use hping3 to create a SYN flood attack with fake IPs.

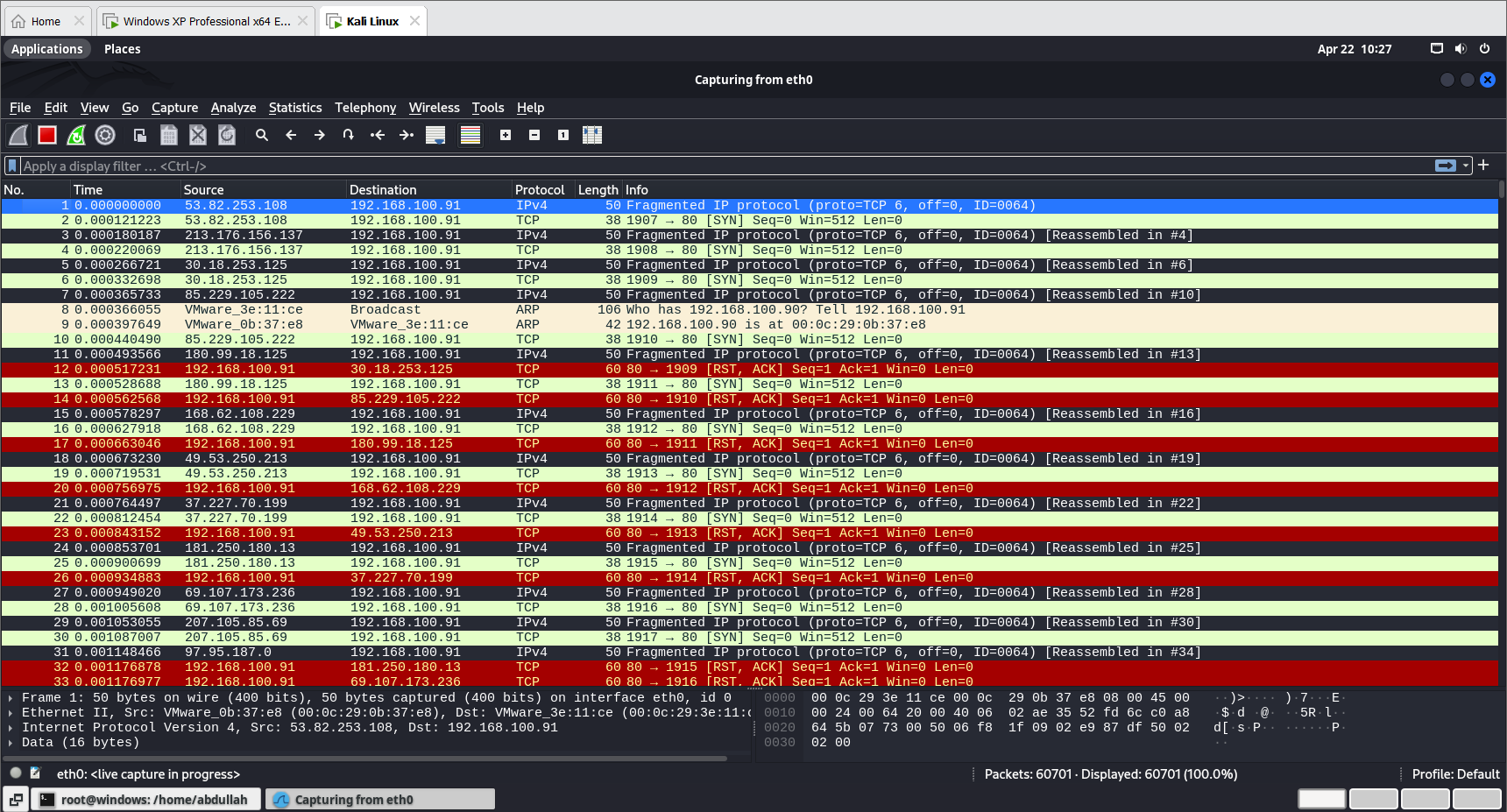
* --rand-source will send random fake source IP to the target.
* --flood will send out flood attacks
* -f is fragments to make the traffic look real
* -S is SYN packets
* 192.168.10.xxx is the IP of the other VM, your attack target.

NOTE: If you use your own environment, make sure your network setting is set to “local only” on VMs. Your VMs should not have Internet access. Otherwise, IT security from your network will detect the malicious DDoS traffic. Please run this hping3 command for only a second and then stop it immediately. Otherwise, it will create too many malicious traffic.

Task 4: Start live capture with Wireshark in Kali VM or the other VM (Wireshark is just installed in the Kali and Ubuntu VMs).

Task 5: Provide a screenshot from the captured packets in the Wireshark while you are running DDoS attack.





Task 6: Click the stop capturing button and save the captured packets on your Desktop with the default extension.

## **Packet analysis:**

Task 7: Open your captured file in the Wireshark.

Task 8: Briefly describe the network activities that happened during the capture session.

Answer: This capture session appears to show network traffic involving multiple TCP SYN packets being sent from various source IP addresses to the destination IP address 192.168.100.91 on port 80, indicating attempted connections to a web server.

Here's a summary of the activities:

1. Multiple fragmented IPv4 packets containing TCP SYN segments are being reassembled.
2. Each reassembled packet consists of a TCP SYN segment from a different source IP address (e.g., 53.82.253.108, 213.176.156.137, 30.18.253.125, etc.).
3. Each TCP SYN segment is attempting to establish a connection with the destination IP address (192.168.100.91) on port 80.
4. Additionally, there are ARP (Address Resolution Protocol) requests and responses occurring within the local network, involving IP addresses 192.168.100.90 and 192.168.100.91.

It seems like there are multiple external hosts attempting to establish connections with a web server located at 192.168.100.91 on port 80. Additionally, there are local ARP requests and responses happening concurrently.

## **Network Forensic by Wireshark**

Scenario 1:

In this scenario you will be taking the role of the Network Defense Analyst. You will perform a thorough analysis of the captured network forensic artifact. The network packet capture is saved in a file titled NetworkTraffic1.pcapng.

Task 9: Describe the main fields in a typical output of a Wireshark capture.

Answer: The network traffic captures reveal repetitive ARP requests for various IP addresses, indicating a potential ARP cache poisoning attack or misconfigured network device. Additionally, there are multicast DNS (MDNS) queries and browser election requests, suggesting local network service discovery and election processes. An attempted TCP connection to port 80 is observed, followed by a reset (RST) response, indicative of a failed connection attempt.

Top of Form

Task 10: Briefly describe the network activities that transpired during the capture session.

Answer:

Based on the provided network forensic artifact, we can make several observations and analyses, the artifact indicates normal network activity such as ARP resolution, service discovery, and Windows networking protocols. However, the continuous ARP requests and unsuccessful TCP SYN attempt may warrant further investigation to ensure network stability and security.

Scenario 2:

In this scenario you will be taking the role of the Network Defense Analyst. You will perform a thorough analysis of the captured network forensic artifact. The network packet capture is saved in a file titled NetworkTraffic2.pcapng.

Task 11: Briefly describe the network activities that transpired during the capture session.

Answer:

This artifact appears to be a packet capture from a network. It includes ARP (Address Resolution Protocol) requests and TCP traffic. This capture indicates that the device at 192.168.11.107 is attempting to communicate with various services or devices on the network but is encountering issues or being actively blocked, as evidenced by the TCP RST packets. Further investigation would be needed to determine the cause of these connection failures and whether they are indicative of malicious activity or misconfiguration.

Task 12: What is the client computer trying to achieve? Explain.

Answer:

From the provided network forensic artifact, it appears to be a packet capture log, likely captured by a network monitoring tool or device. Let's break down the information:

1. The log starts with a series of Address Resolution Protocol (ARP) requests. ARP is used to map IP addresses to MAC addresses on a local network. In this case, the device with the MAC address "Dell\_02:a6:31" is trying to resolve the MAC addresses of various IP addresses (e.g., 10.1.1.151, 10.1.1.171, etc.) by sending ARP requests.
2. Following the ARP requests, there are TCP packets exchanged between IP addresses 192.168.11.107 and 192.168.11.88. These packets include TCP handshake packets (SYN, SYN-ACK, ACK) and reset packets (RST). It seems that port scanning or connection attempts are happening from 192.168.11.107 to various ports on 192.168.11.88.
3. There are numerous TCP connections attempted from 192.168.11.107 to various ports on 192.168.11.88, followed by immediate reset (RST) packets from 192.168.11.88. This behavior suggests that the connections were actively rejected by the destination host (192.168.11.88).
4. The log continues with more TCP connections from 192.168.11.107 to different ports on 192.168.11.88, all resulting in RST packets from the destination host.
5. Towards the end of the log, there are additional TCP connections attempted from 192.168.11.107 to other ports on 192.168.11.88, each followed by a RST packet from the destination host.

Based on this analysis, it appears that 192.168.11.107 is attempting to establish connections with various ports on 192.168.11.88, but all these attempts are being actively rejected by the destination host, which is sending reset (RST) packets. This activity could indicate a port scanning or intrusion attempt from 192.168.11.107 towards 192.168.11.88. Further investigation would be necessary to determine the intent and origin of these connection attempts, as well as to assess any potential security implications.

Scenario 3:

A security analyst working for a state government agency has a suspicion that some state employee is trying to exfiltrate important documents from a file archiving system at the District Attorney’s office. Thus, the analyst requested a packet capture on the network traffic occurring on the suspected employee’s computer. Several packet capture events were conducted during the evening hours of May 2 and 3. The most incriminating evidence produced by the network packet capture activities was saved in a file titled NetworkTraffic3.pcap.

In this scenario you will be taking the role of the Network Defense Analyst. You will perform a thorough analysis of the captured network forensic artifact.

Task 13: What is (are) the service(s) and/or protocol(s) used during the session?

Answer: The service/protocol used during the session is TFTP (Trivial File Transfer Protocol)

Task 14: What are the IP address and MAC address of each of the devices?

Answer :

Based on the provided packet capture, here are the IP addresses and MAC addresses of each device involved:

Device 1 (Client):

* IP Address: 192.168.0.253
* MAC Address: (Not Found)

Device 2 (Server):

* IP Address: 192.168.0.10
* MAC Address: (Not Found)

Task 15: What is the name of the file that is being exfiltrated? Will you be able to extract and examine the entire content of the file? How?

Answer: The name of the file being exfiltrated is "rfc1350.txt". As for whether I can extract and examine the entire content of the file from the provided packet capture, unfortunately, the content of the file itself is not directly visible in the packet capture. TFTP operates at the transport layer (Layer 4) of the OSI model, and it transfers files in blocks of data. Each block contains a portion of the file being transferred, but the actual content of the file is not visible in the packet capture in plaintext.

However, if you want to reconstruct the file from the captured TFTP traffic, you could extract and concatenate all the data packets (Data Packet) exchanged between the client and server. Each data packet carries a block of data from the file being transferred. By combining all these blocks in the order they were transmitted, you could reconstruct the original file.

Once you have reconstructed the file, you could examine its content using a text editor or any appropriate software for the file type (in this case, a text file)

Scenario 4:

Telnet is a network protocol used for remote terminal access to other computers over a network, typically the internet. It allows users to log in to a remote system and execute commands as if they were directly connected to that system’s console. Telnet operates on TCP/IP and provides a text-based interface for communication. Due to security vulnerabilities, such as transmitting data in plaintext, Telnet is now largely replaced by more secure protocols like SSH (Secure Shell). However, network administrators still occasionally use Telnet for specific purposes or in legacy systems where SSH is not available or feasible.

In this scenario you will perform a thorough analysis of the captured network forensic artifact. The network packet capture is saved in a file titled NetworkTraffic4.pcapng.

Task 16: Will you be able to identify the victim IP and extract the login user and password?

Answer:

The victim IP is 192.168.1.140, initiating the Telnet connection. However, the provided network traffic does not contain the plaintext login user and password

## **Reflection**

Answer the questions below regarding this assignment.

* Describe any challenges you experienced with this lab. Explain how you overcame the challenge. If you did experience any challenges, describe what you learned from this lab.

Task 17: Your answer below.

Answer:

The Biggest challenge for me to analyze the packets capture by the wireshark

* Share your thoughts about this lab. What did you like or dislike about this lab? How can this lab be improved? What was the best part of this lab?

Task 18: Your answer below.

Answer:

This Lab Experiencing a good Knowledge for me and best thing I like that is analyzing the wireshark capture’s packets. This lab can be improved by attacking using telnet Port to gain remote access. Analyzing the wireshark capture’s packets is the best part of this lab

## **When Completed**

1. Save this document with your answers.
2. Submit this completed document in the assignment.