Bryant Watkins

3/29/26

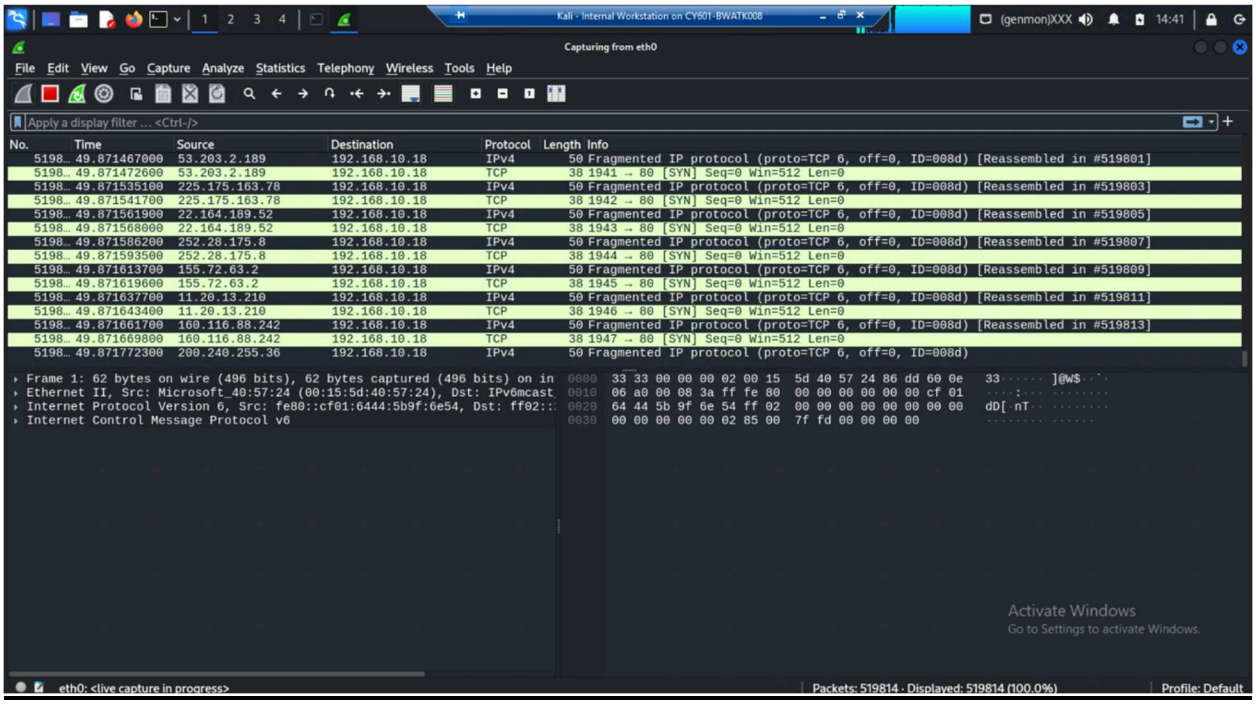
NETWORK FORENSIC BY WIRESHARK LAB REPORT

CYSE 601

Relevant Systems

- pfSense firewall VM (IP: 192.168.10.2)
- Internal Kali Linux machine (IP: 192.168.10.13)
- Ubuntu VM (IP: 192.168.10.18)

Simulate a DDoS Attack: Task 5



Packet Analysis: Task 8

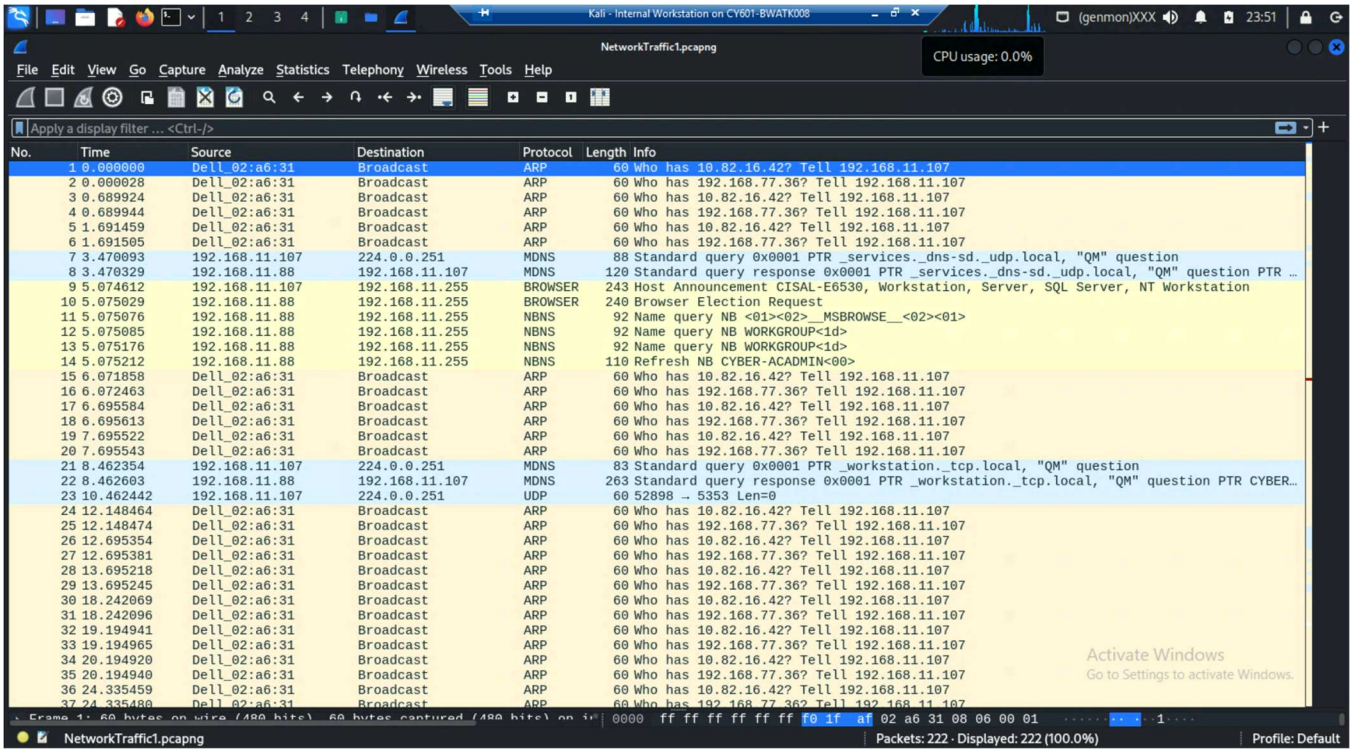
Brief Description of The Above Image – The image above illustrates what constitutes a Distributed Denial of Service (DDoS) attack. A single Destination address is repeatedly and aggressively sent packets from many different Source addresses. The Source addresses appear to be randomly generated and different each time. There is a distinctive pattern to all the packets as well, which is abnormal, as packets typically vary in protocol and size. It is also noteworthy that none of these SYN packets are accompanied by ACK packets, as ACK packets are part of the typical three-way handshake. The packets captured above also all possess the exact same length, as well as the exact same protocols. When combining all the factors – heavy influx of traffic,

identical packet size and protocol, and SYN packets unaccompanied by ACK packets; it appears that the above image illustrates what is known as a TCP SYN Flood DDoS attack.

Scenarios

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.

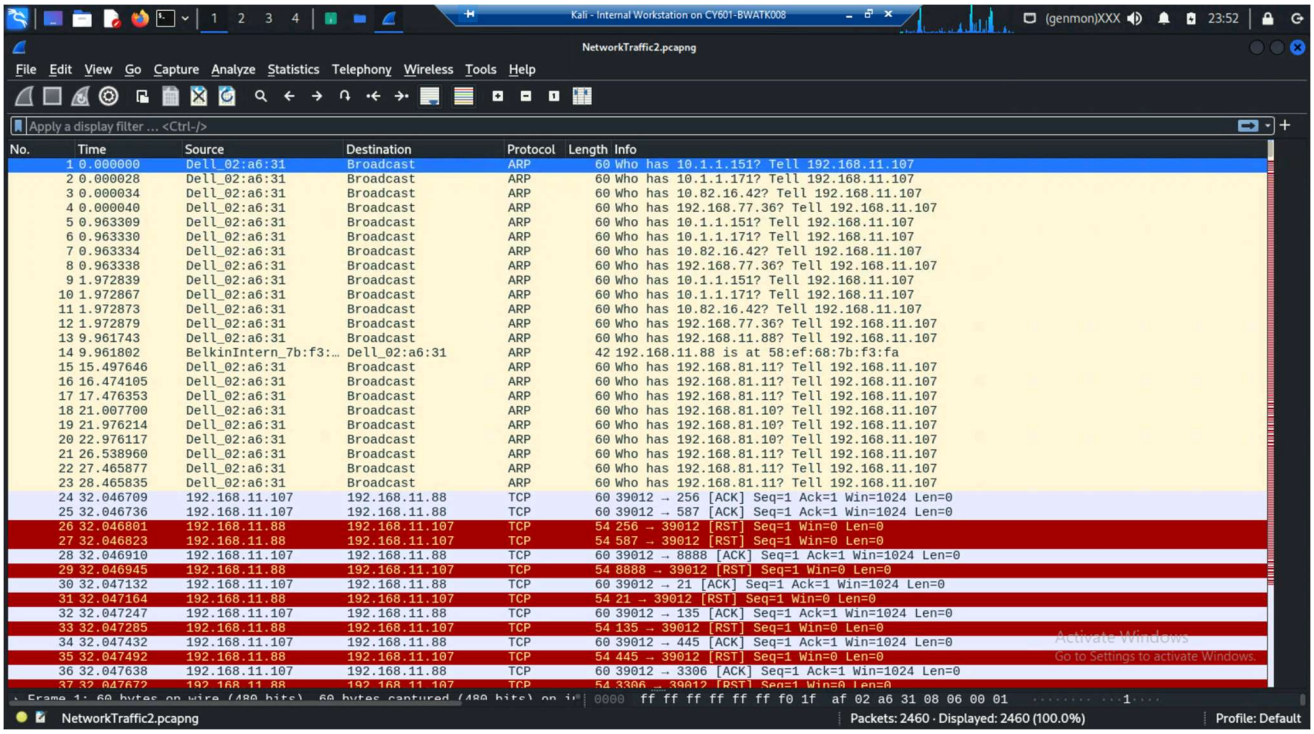
The main fields of a typical Wireshark capture include – *No.* (number), *Time*, *Source*, *Destination*, *Protocol*, *Length*, and *Info*. *Number* simply refers to the chronological sequence in which the packets have been received. *Source* and *Destination* refer to the address the packet originated from and the address the packet is sent to respectively. *Protocol* represents the applicable protocol identified from the packet. *Length* displays the size of the packet. Finally, *Info* contains numerous pieces of data. Some of the data provided by *Info* includes – error messages, flags, port numbers, etc.

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

The packets are overwhelmingly attempting Address Resolution Protocol requests, It appears as though the Source address is attempting to map a known IP address to a MAC address. These findings are evident by the displayed ARP protocol and "Who has" text found within both the *Protocol* and *Info* columns.

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.

There is a plethora of TCP packets flagged in red. TCP packets flagged in red are typically indicated due to errors. These packets observed are specifically TCP RST packets. TCP RST packets are packets resulting from connection errors, such as unopen ports or unexpected connection termination. The packet details pane provides further information and confirmation of initial findings. Under *Transmission Control Protocol*, one will find "Incomplete" as the status identified next to *Conversation Completeness*. These details all indicate unsuccessful attempts at a network connection.

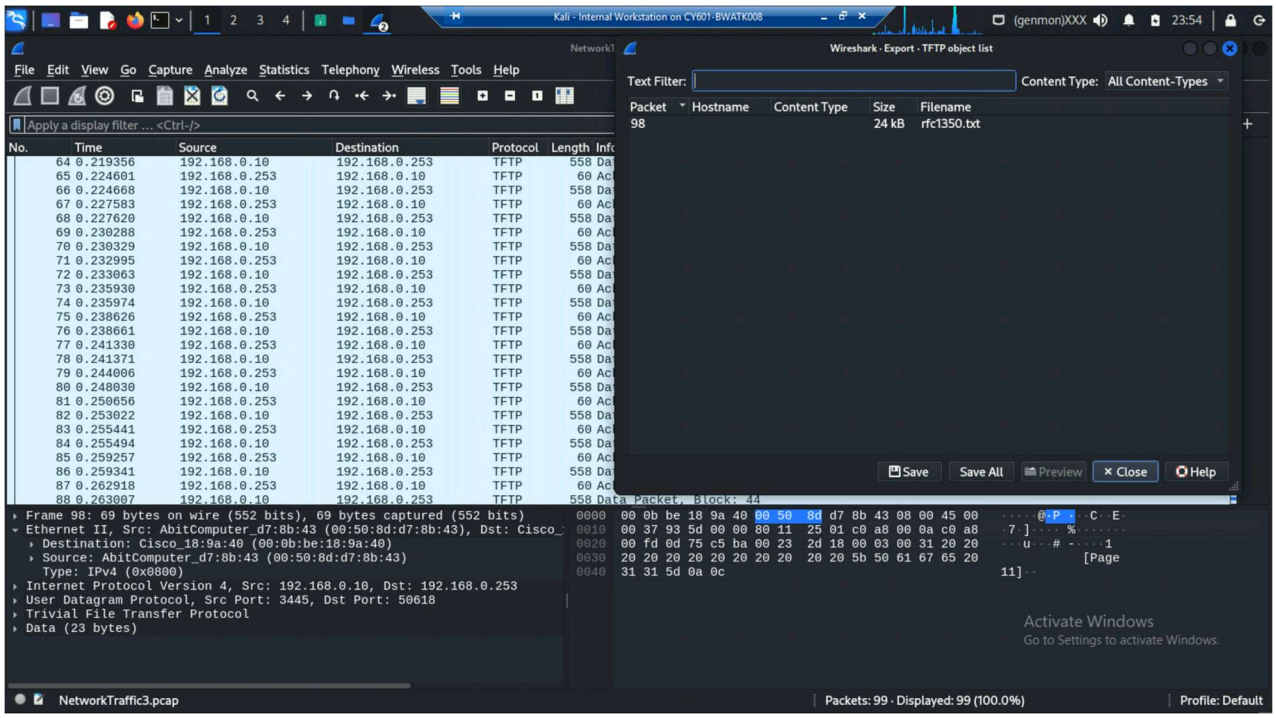
Task 12: What is the client computer trying to achieve? Explain.

The client computer appears to be attempting to establish a network connection to a newly discovered MAC address they believe to be mapped to a known IP address. The connection is ultimately unsuccessful and indicated by the RST (Reset) TCP flags.

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.pcapng."

"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?

The service(s) and/or protocol(s) used during the session are UDP (User Datagram Protocol) and TFTP (Trivial File Transfer Protocol).

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

192.168.0.10, 192.168.0.253, 00:50:8d:d7:8b:43, 00:0b:be:18:9a:40

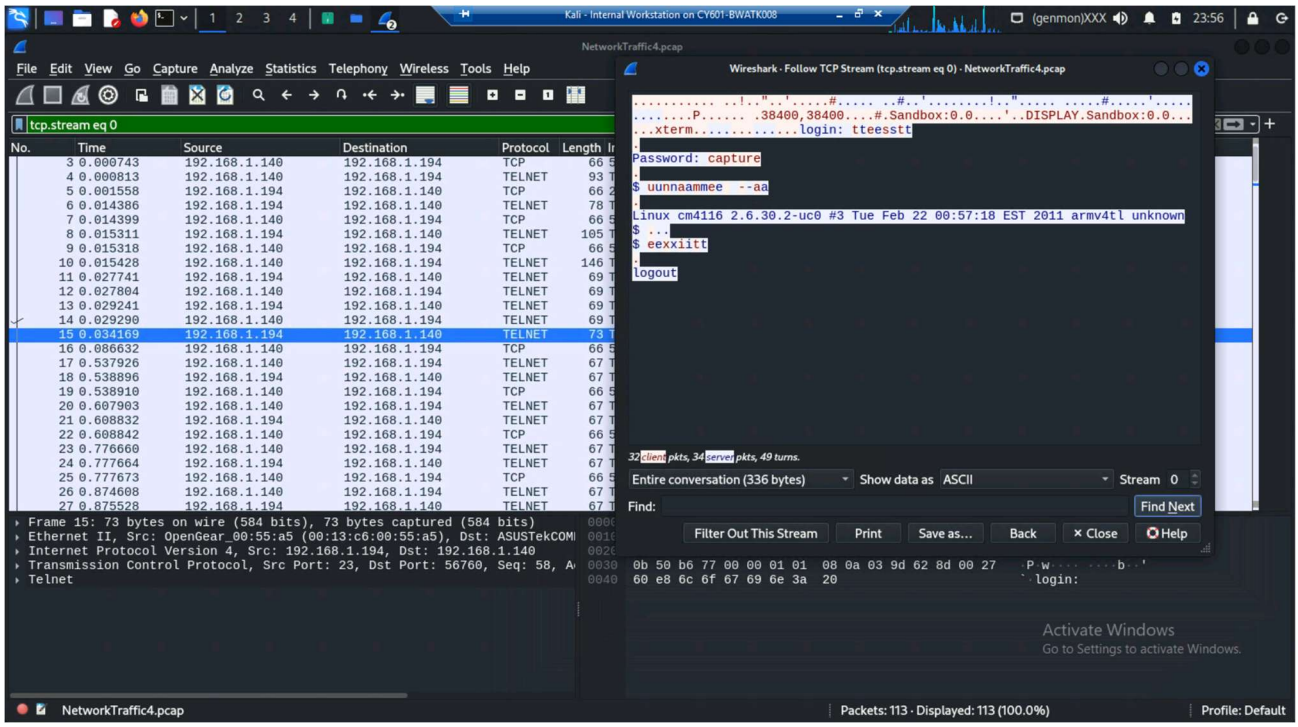
Task 15: What is the name of the file that is being exfiltrated? Will you be able to extract and examine the entire content of the file? How?

Rfc1350.txt, yes one can extract and examine the content of the file. One may do so by navigating to the *File* tab, hovering over *export objects*, selecting *TFTP*, and selecting the applicable file of the listed available. The selected file can then be saved to the desired location and opened for viewing of its full contents. If simply seeking to view the contents, one can also right-click a packet, hover over *follow*, and then select *UDP Stream*.

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?

Yes, the packet details pane provides the victim IP address, as well as login user and password upon following the TC stream.

Task 17: Describe any challenges you experienced with this lab. Explain how you overcame the challenge. If you did not experience any challenges, describe what you learned from this lab.

I was fortunate to not face any significant challenges of note in completing this lab. I did, however, learn a great deal from this lab assignment. My biggest takeaway from the completion of this lab assignment is a strengthened ability to analyze traffic patterns and packet data. Critical thinking, problem solving, and analysis skills are all very much critical to the success of a cybersecurity professional. Completing this assignment provides me with further extensive experience in analyzing packet data, identifying patterns, and the overall navigation of one of the most widely used forensic analysis and cybersecurity tools worldwide.

Task 18: 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?

I thoroughly enjoyed this lab assignment, as I enjoy partaking in critical thinking and analysis cybersecurity activities. My only suggestion for improvement would be to allow students to conduct the searches necessary for the packet captures already present, as this added experience would be helpful. The first capture was manually completed; however, the remaining were provided. While that is incredibly convenient, students manually creating those captures would provide for more experience. The best part of the lab was getting to analyze a plethora of different scenarios. Experiencing different scenarios allows students to experience different tasks and points of view necessary to being a well-rounded cybersecurity professional.