Lab 03

CIS4367.01 – Computer Security

Jaleel Rogers

Contents

Abstract

Lab 03 focuses on Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, which can disrupt the availability of critical systems. The lab encompasses two primary tasks involving Windows Server and Parrot Linux, offering hands-on experience with DoS and DDoS attack techniques, as well as an optional extra credit section using Raven-Storm. This lab is helpful in providing an example of how to damage a network along with understanding more about hacking.

Tasks

Task 1: SYN Flooding Windows Web Service

Steps

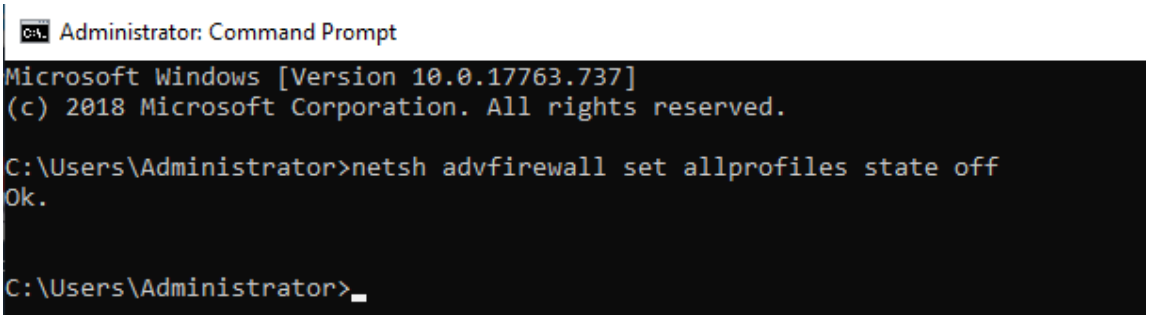

Figure 1 - Turning Off Firewall

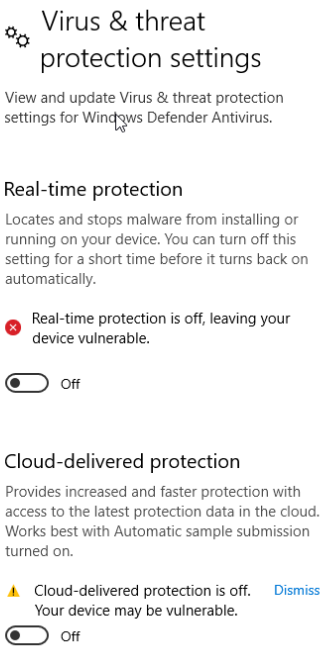

Figure 2 - Turning Off Real-time protection

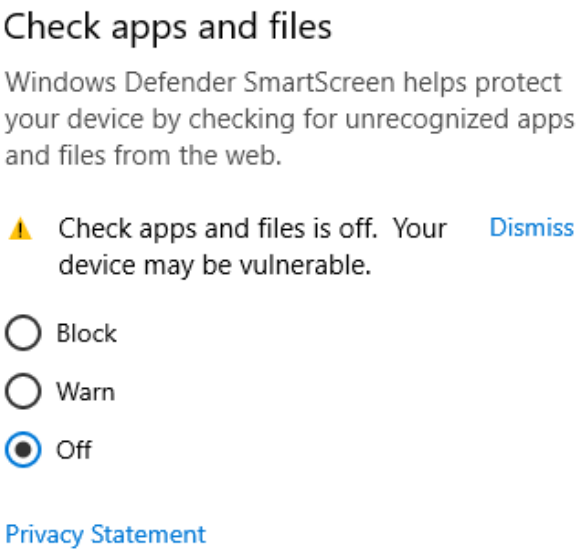

Figure 3 - Turning Off Check apps and files

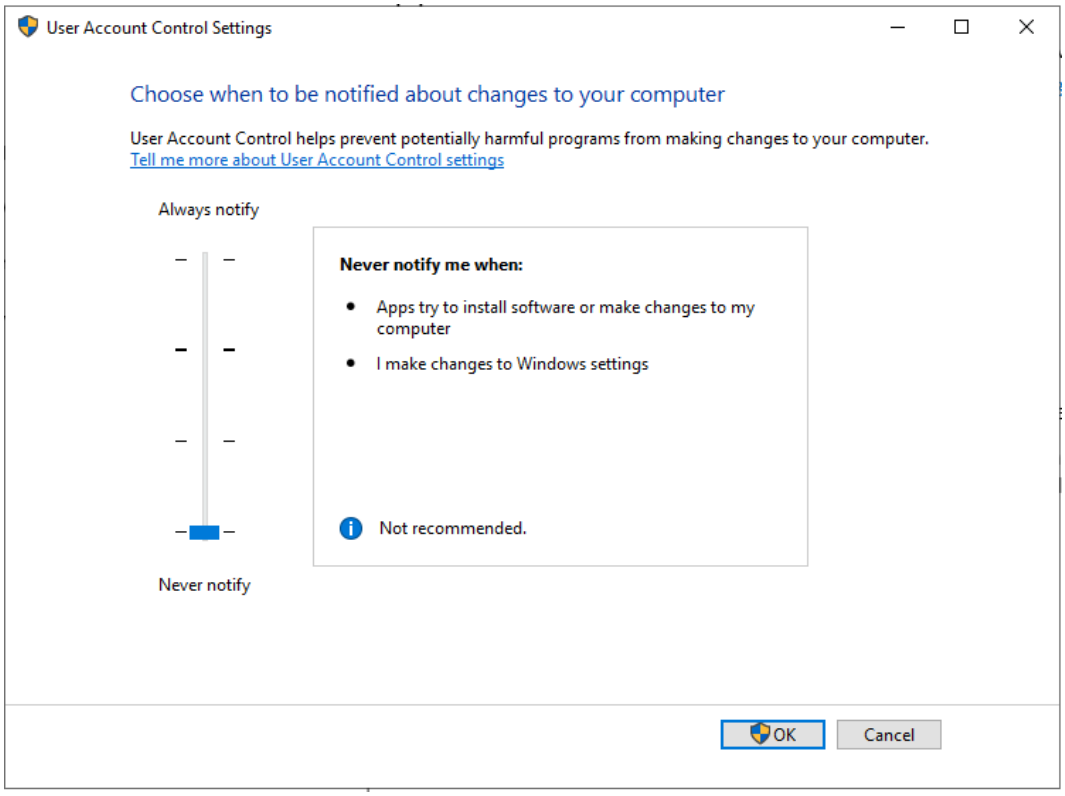

Figure 4 - Setting UAC to Never notify

When making Windows Server 2019 unsecured, I turned off my firewall using the command prompt, as shown in Figure 1. For turning off virus protection, I was excessively disabling as many features as possible. Besides turning off the main barrier to my DoS attack, "Real-time protection," as shown in Figure 2, I was worried about a few additional things. I turned off "Check apps and files" (Figure 3) and modified User Account Control (UAC) to "Never notify" (Figure 4) as I knew I was going to install 'suspicious' applications.

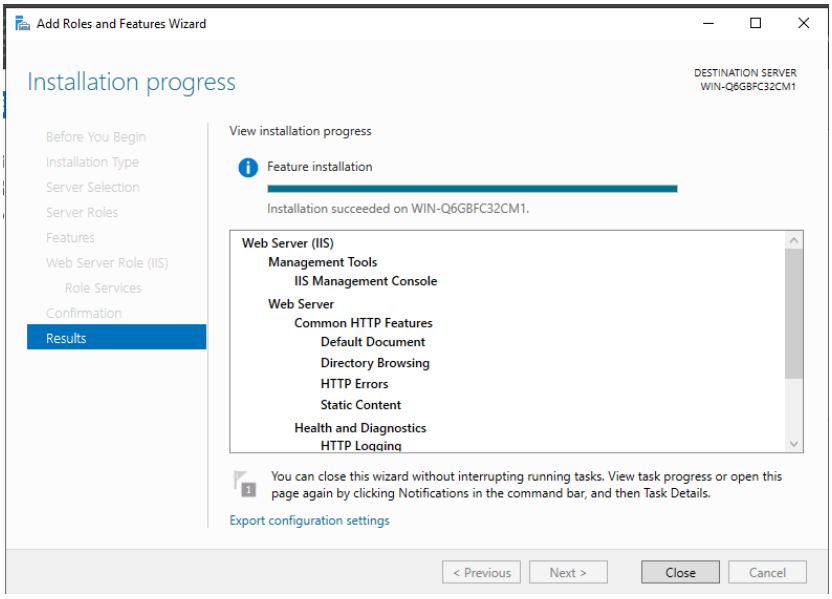

Figure 5 - Installing IIS on Windows Server 2019

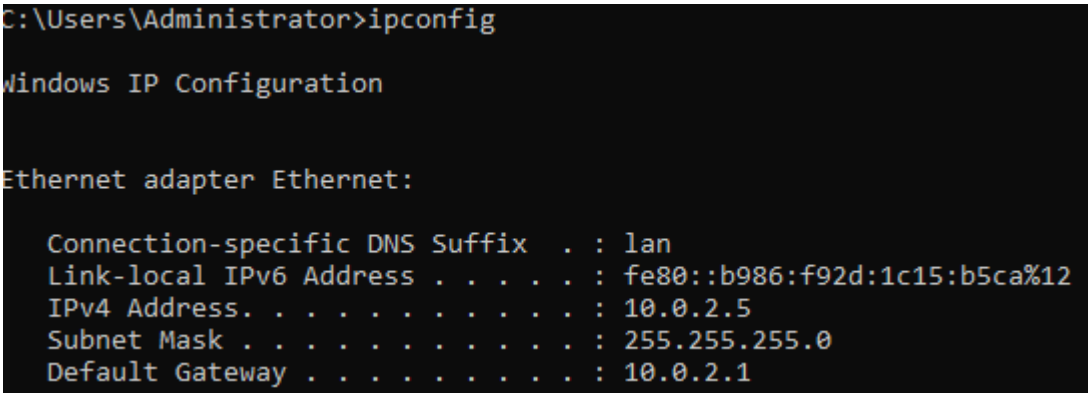

Figure 6 - Finding Windows Server 2019's IP Address

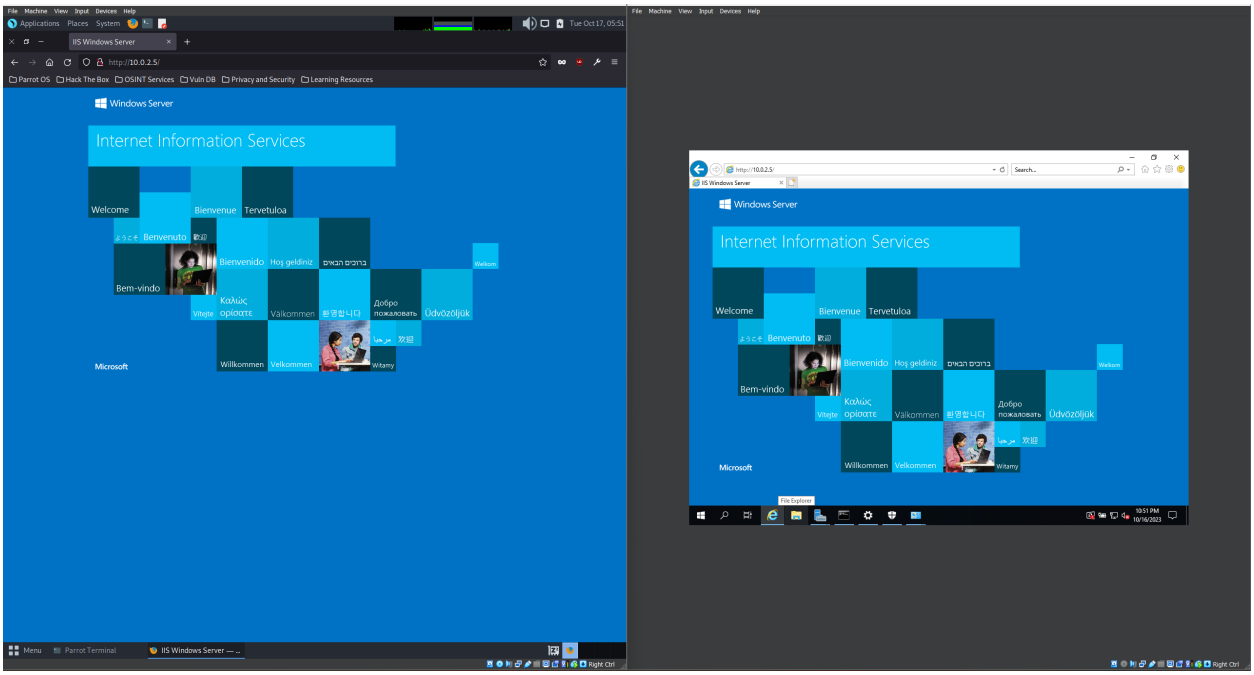

Figure 7 - Parrot and Windows Accessing Windows' Default Website

I discovered that IIS is Microsoft Software and was available on the Server Manager, so installing it was easy, as seen in Figure 5. For me to access Windows Server 2019 on the internet, I needed the IP address of it. After performing an 'ipconfig' command in Figure 6, I used Internet Explorer on Windows search using the IP address (right side of Figure 7) and vice versa on Parrot using FireFox (left side of Figure 7).

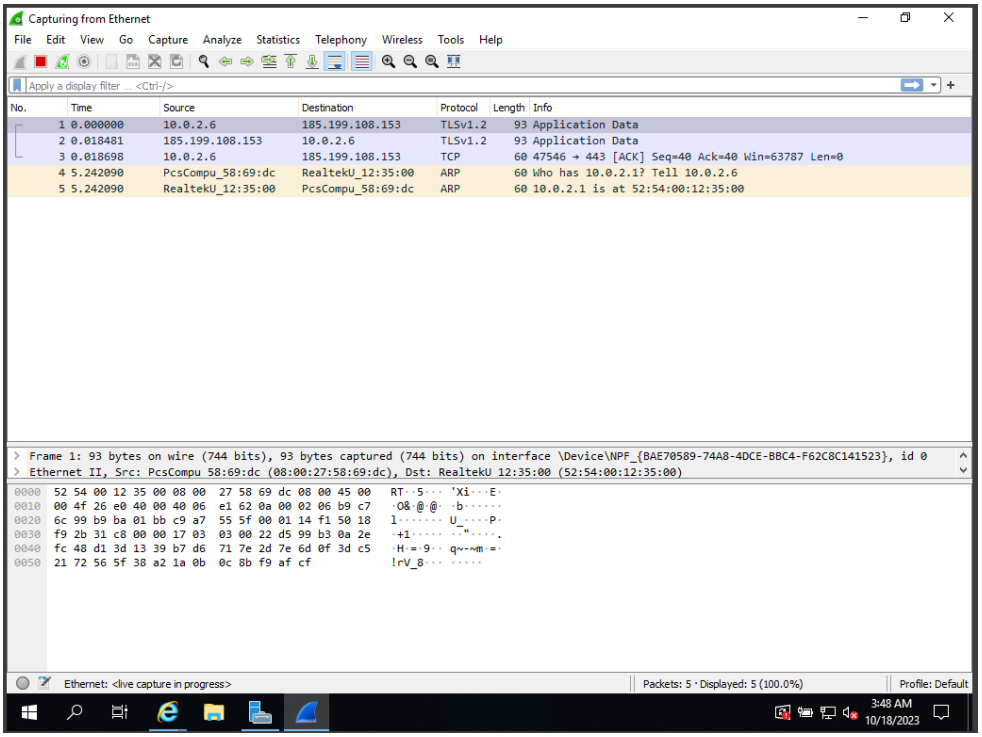

Figure 8 - Wireshark Capturing Packets on Windows Server 2019 Pre-SYN Flood

Installing and running Wireshark was simple, and I could start capturing packets and using the Ethernet interface without any issues, as shown in Figure 8.

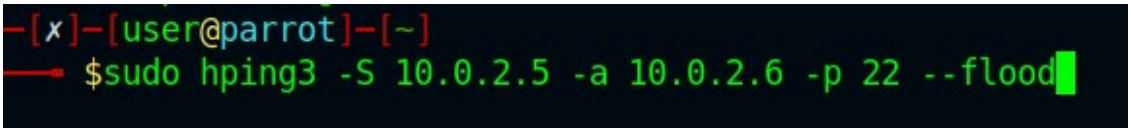

Figure 9 - Launching SYN Flood from Parrot OS to Windows Server 2019

In Parrot OS, I used the command provided to launch the SYN Flood (Figure 9). I learned that hping3 primarily sends response packets to a system like ICMP. It seems outdated as there are already substitutes like Nmap or Netcat.

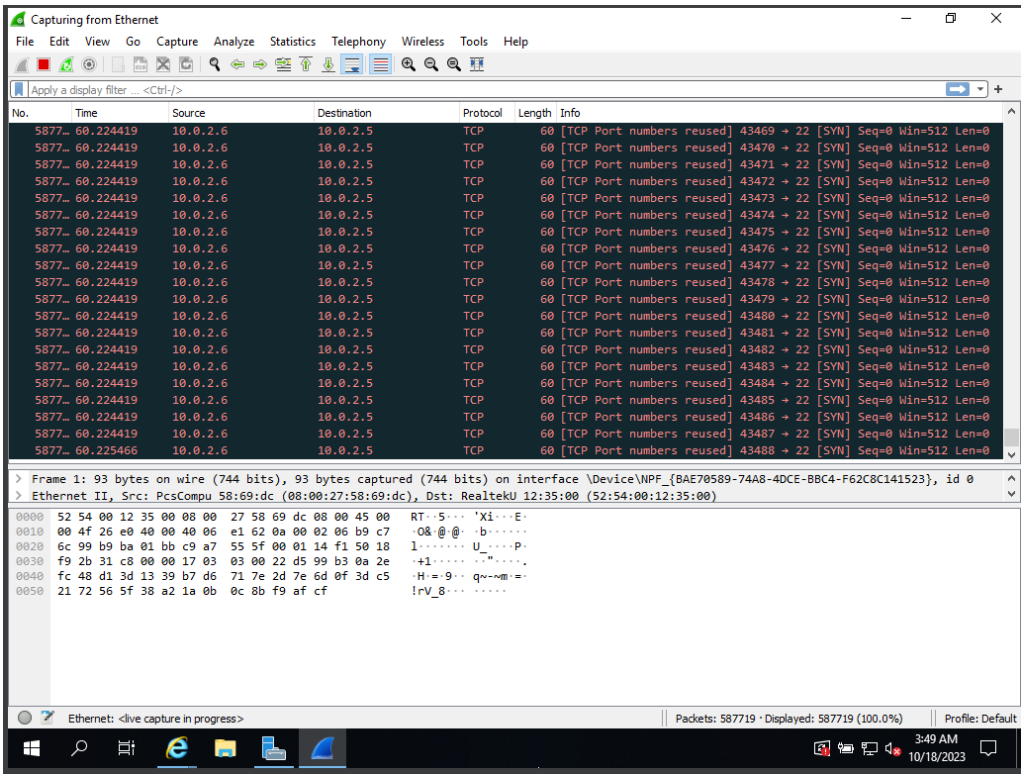

Figure 10 - Wireshark Capturing Packets on Windows Server 2019 Post-SYN Flood

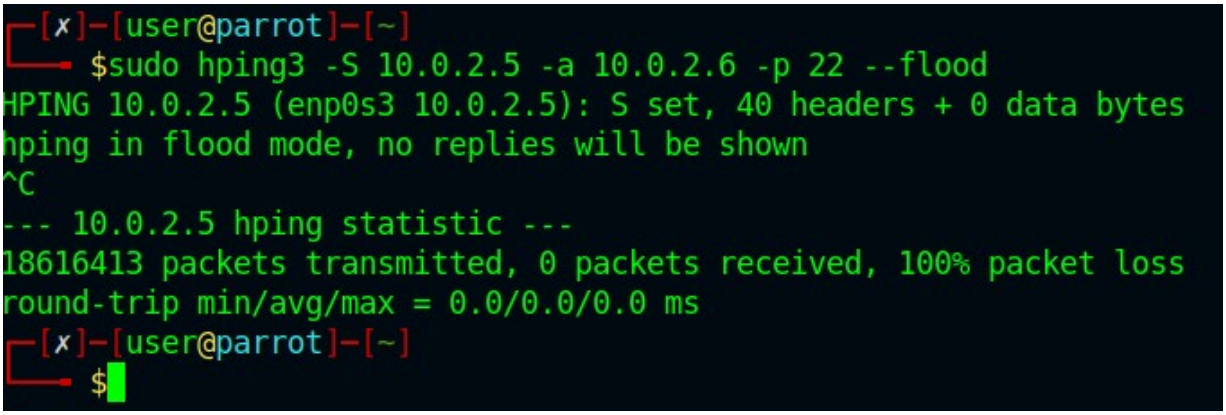

Figure 11 - Stopping the SYN Flood on Parrot OS

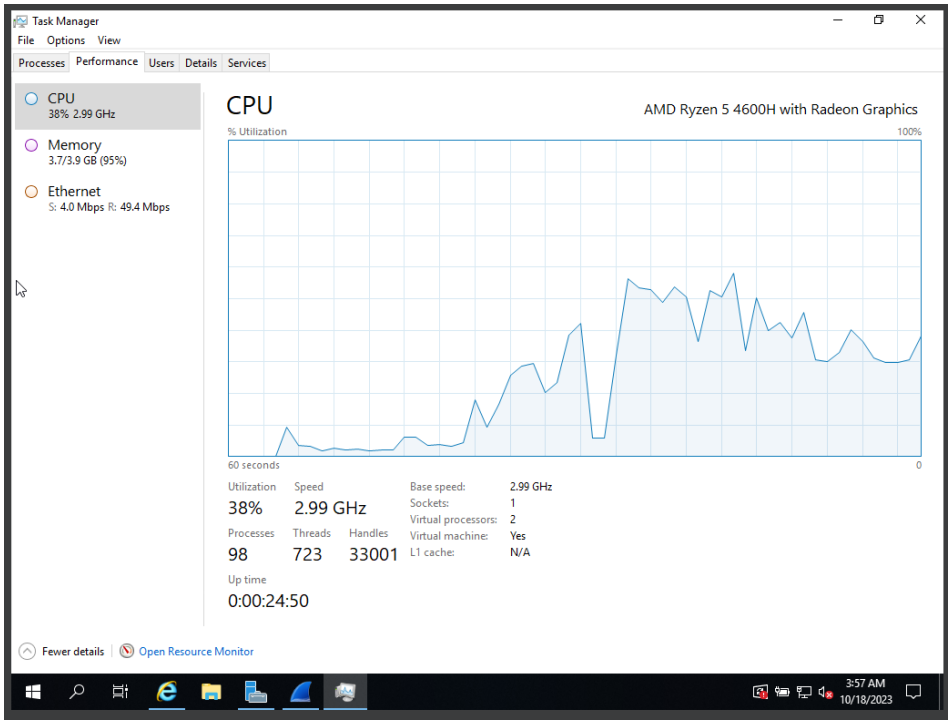

Figure 12 - Windows Server 2019 CPU Usage During SYN Flood

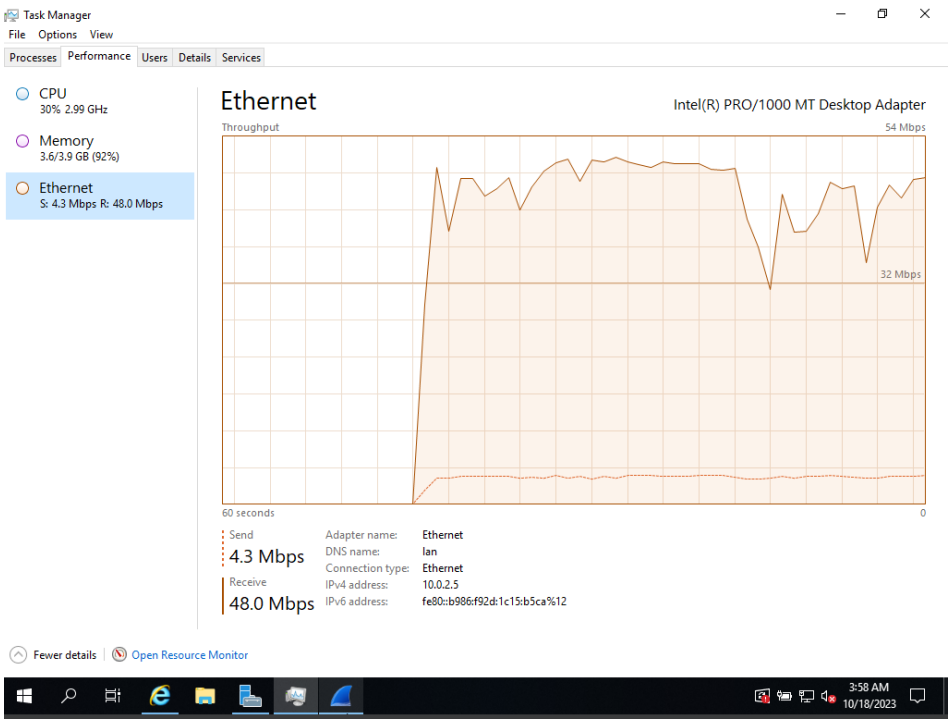

Figure 13 - Windows Server 2019 Ethernet Usage During SYN Flood

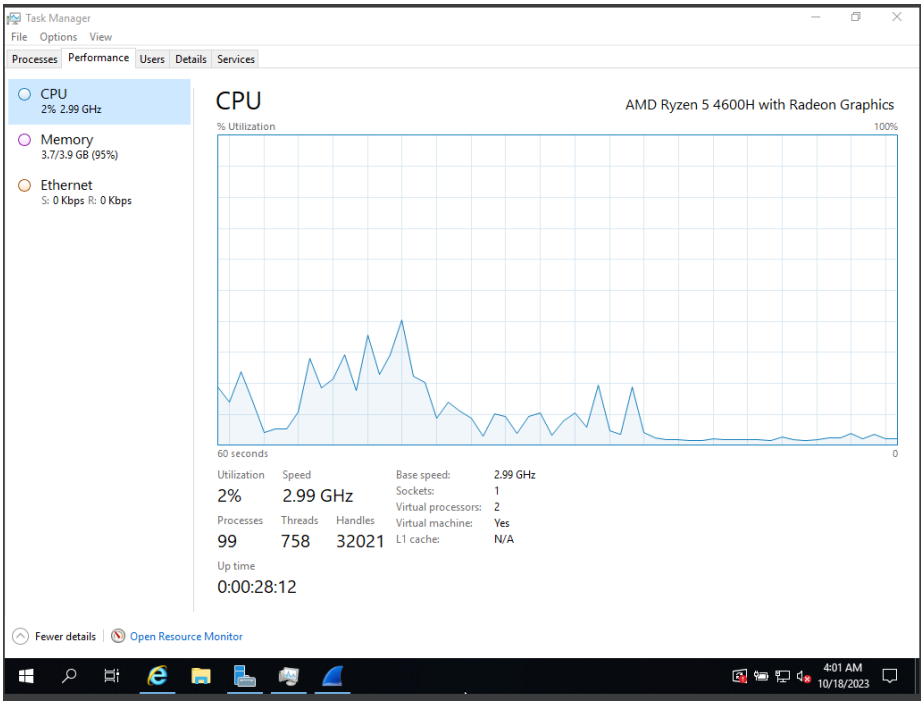

Figure 14 - Windows Server 2019 CPU Usage Post-SYN Flood

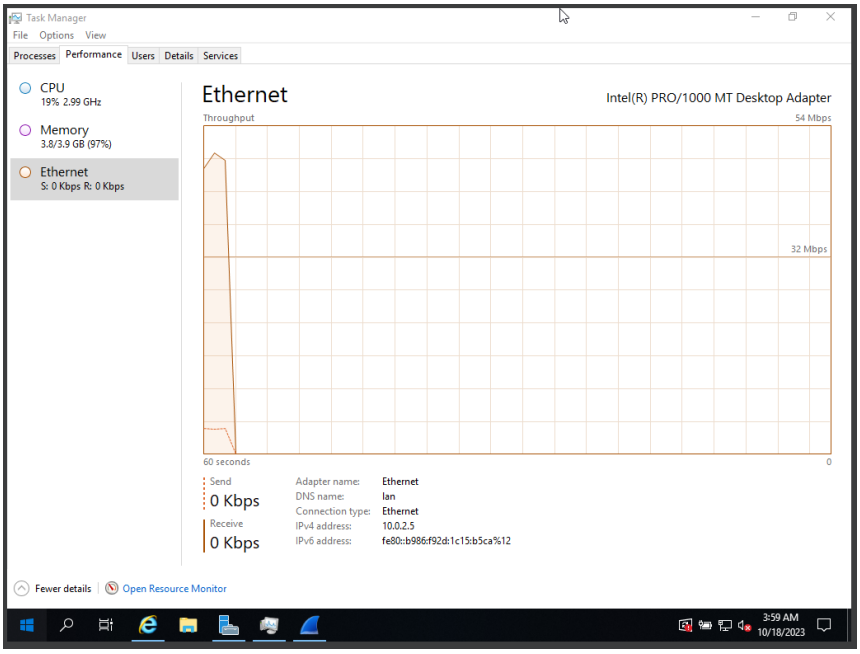

Figure 15 - Windows Server 2019 Ethernet Usage Post-SYN Flood

Almost immediately, I was flooded with packets coming from 10.0.2.6 (Parrot), as seen in Figure 10. All the packets are marked in black, representing a bad packet. When I checked on the performance of the CPU, it spiked from around 15% to 39% (Figure 11), while my Ethernet went from 0 Kbps to 4.3 Mbps (Figure 12). After stopping the command in Parrot (Figure 13), my CPU (Figure 14) and Ethernet (Figure 15) went back to normal levels. This attack would be dangerous if I had other hosts on my network, but it was manageable because there was only one host besides Windows.

Task 2: DDoS Attack parrot Web Service Using HOIC

Steps

Figure 16 - Launching HTTP Server

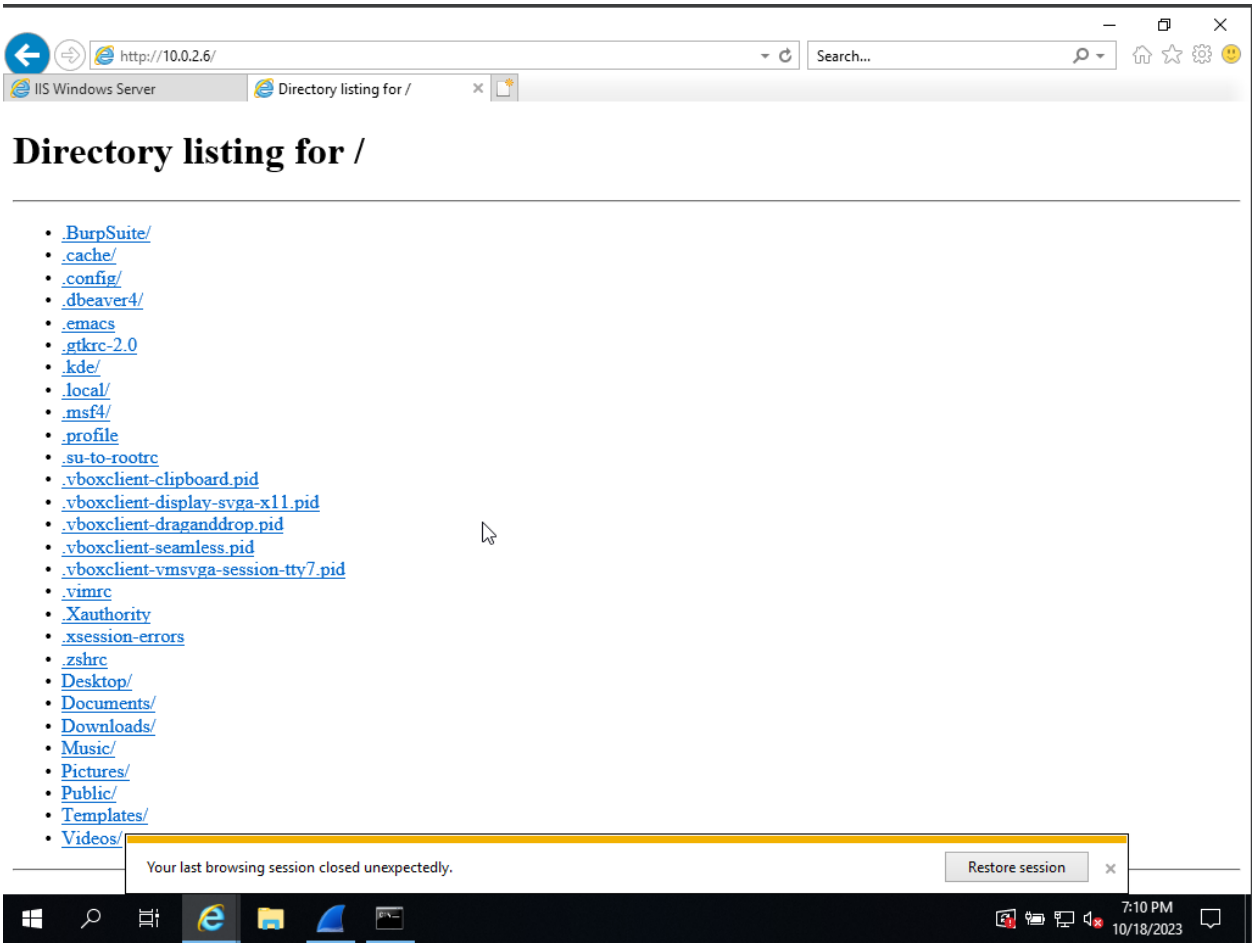

Figure 17 - Parrot's Default Website

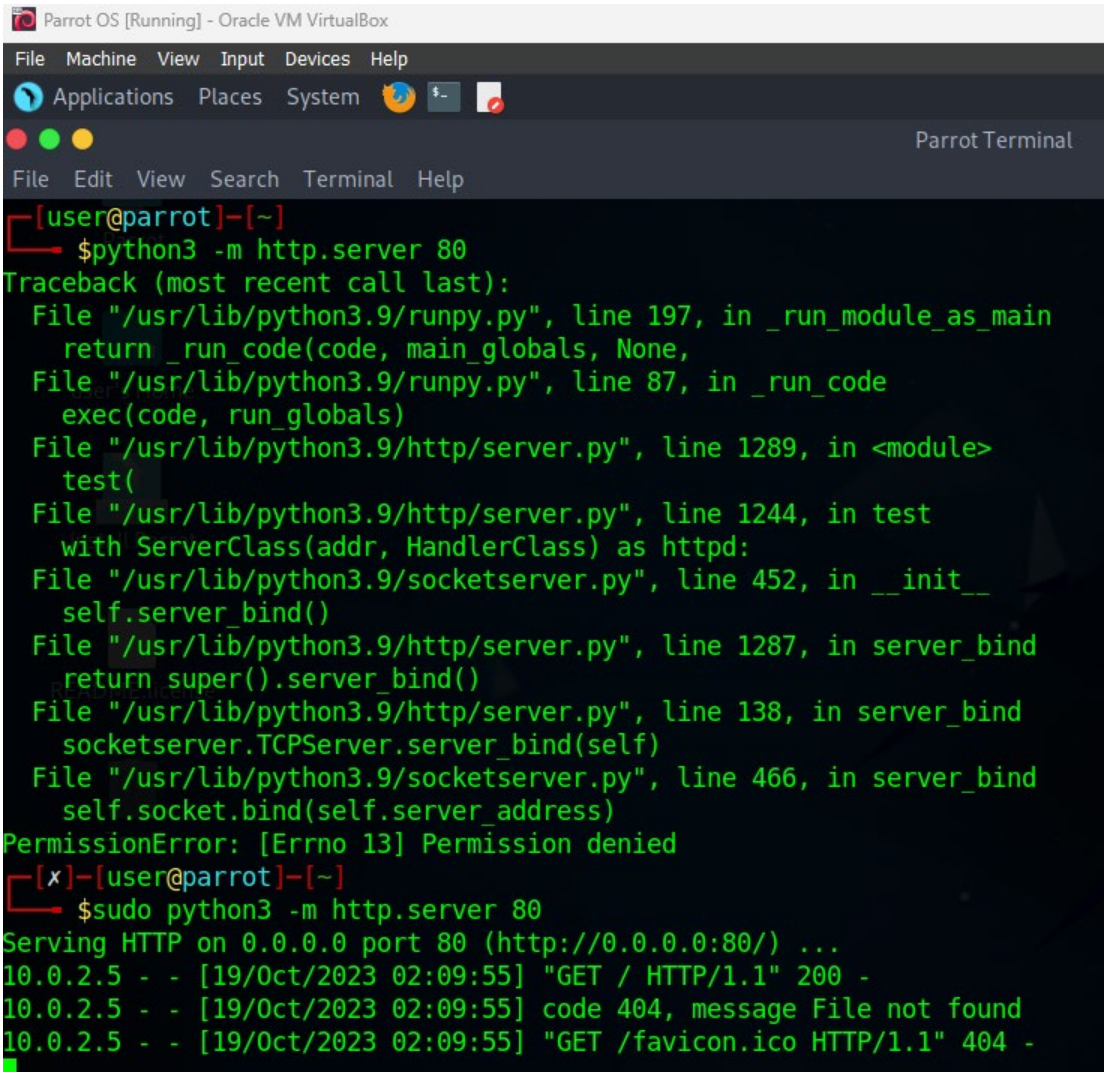

Figure 18 - HTTP Server Pre-DDoS

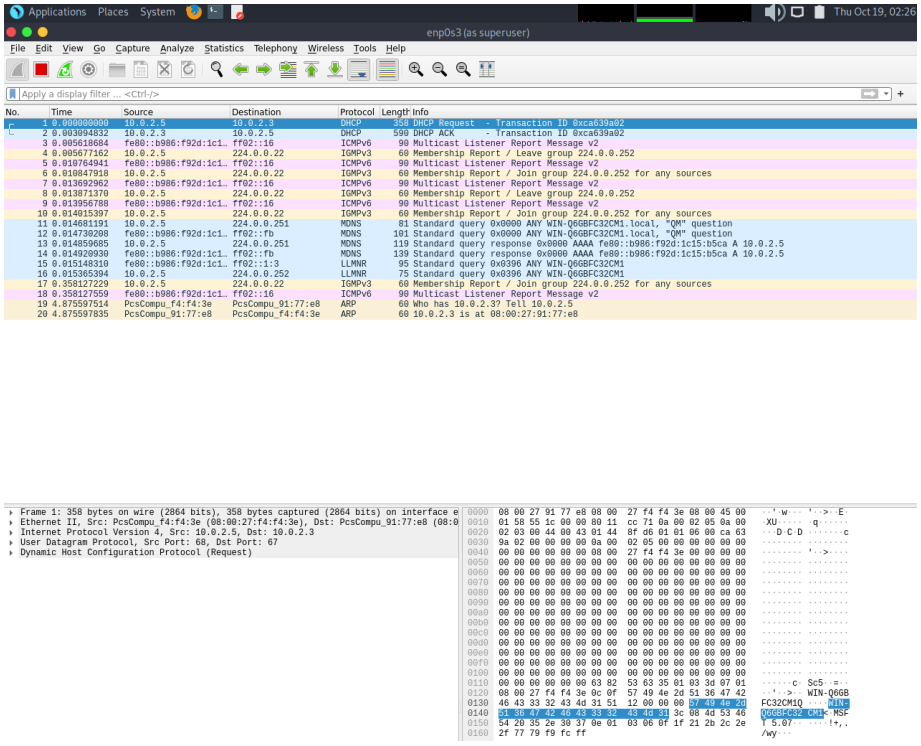

Figure 19 - Wireshark Capturing Packets on Parrot Pre-DDos

Figure 16: I set up the HTTP server in Parrot and checked the default website for Parrot in Figure 17 in Windows Server 2019 to verify the connection. I looked back at the terminal in Parrot to verify the connection on Parrot's end, as displayed in Figure 18. I ran Wireshark and started to capture packets in Parrot (Figure 19).

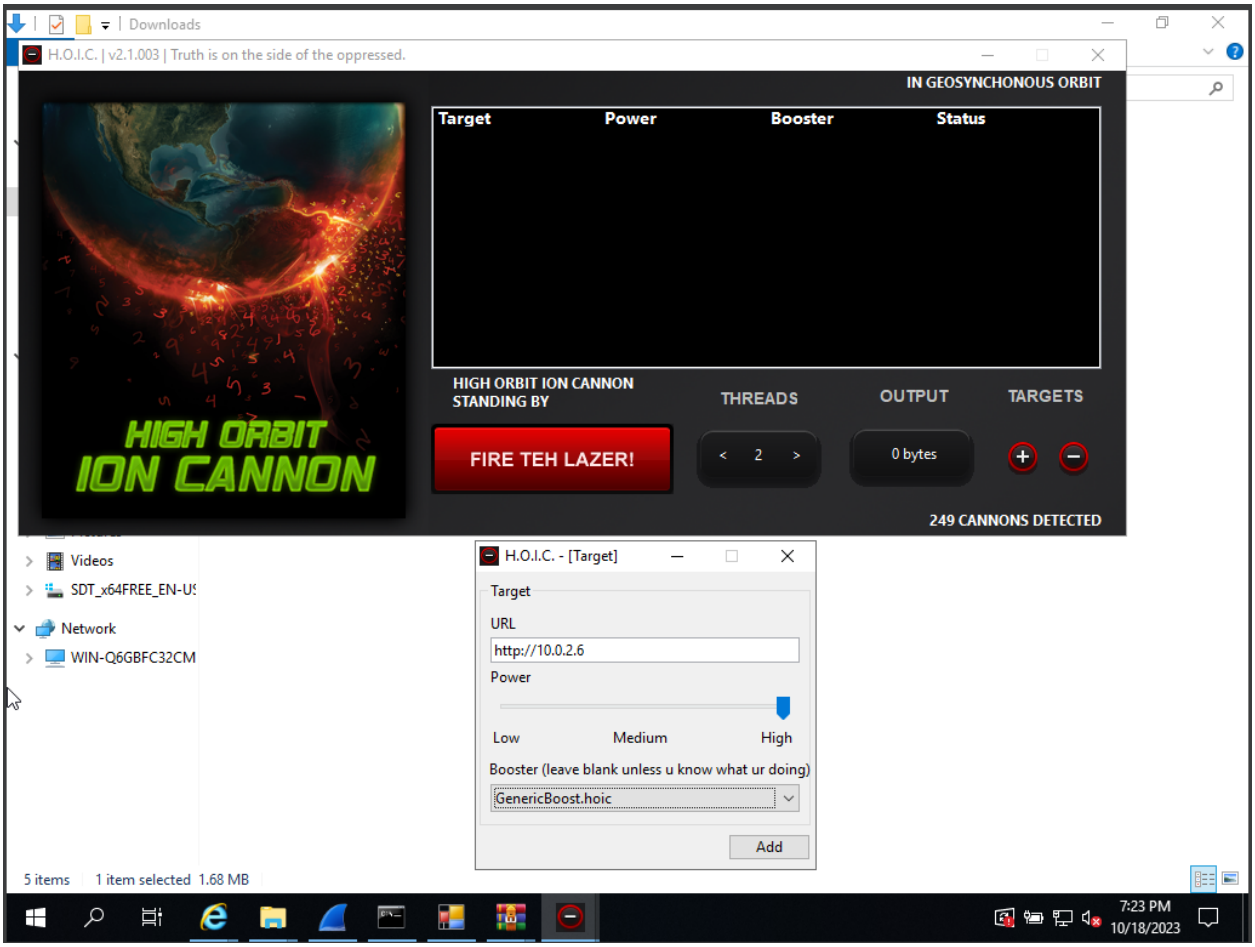

Figure 20 - Setting Up HOIC Target

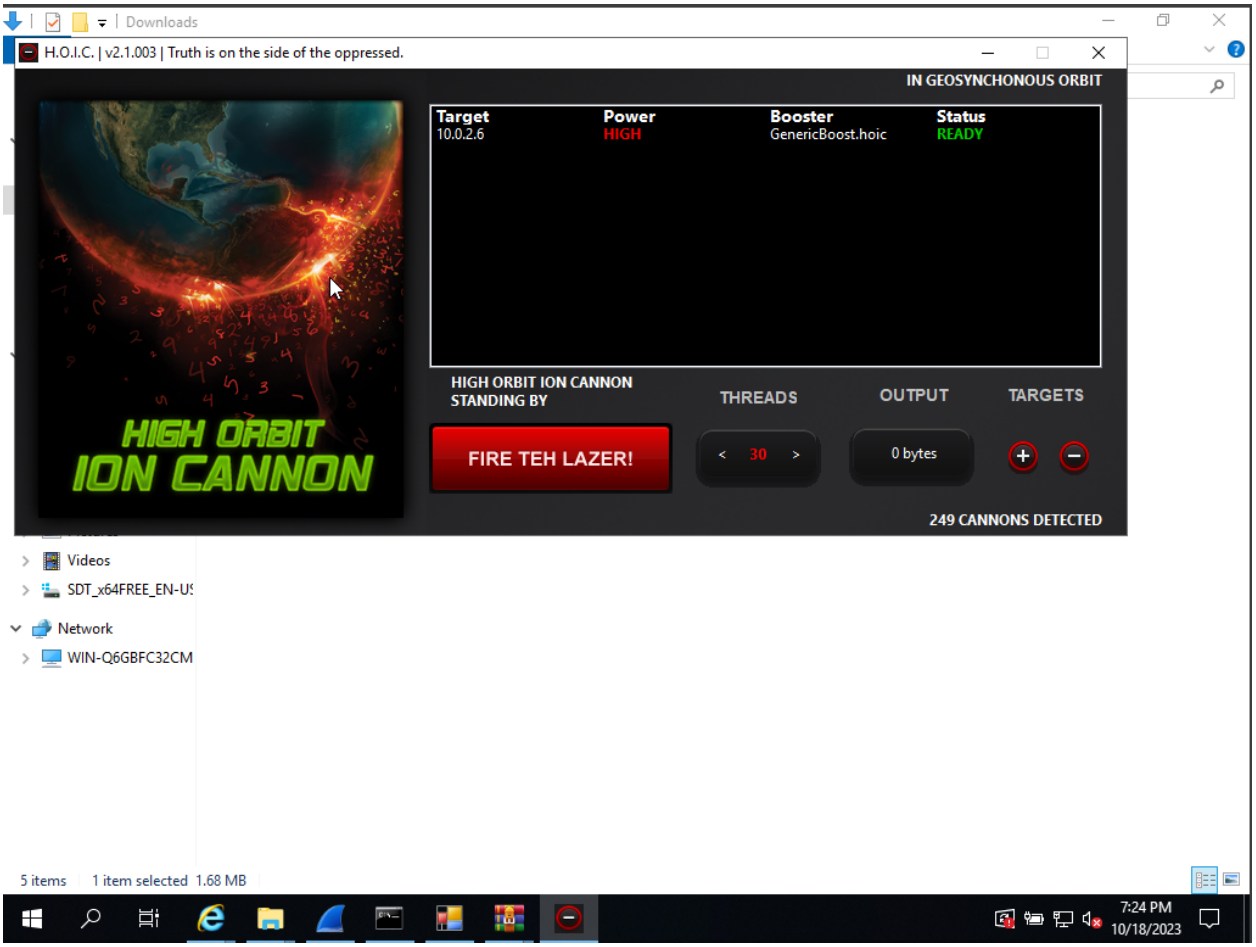

Figure 21 - Setting Threads, Preparing to FIRE TEH LAAZER!

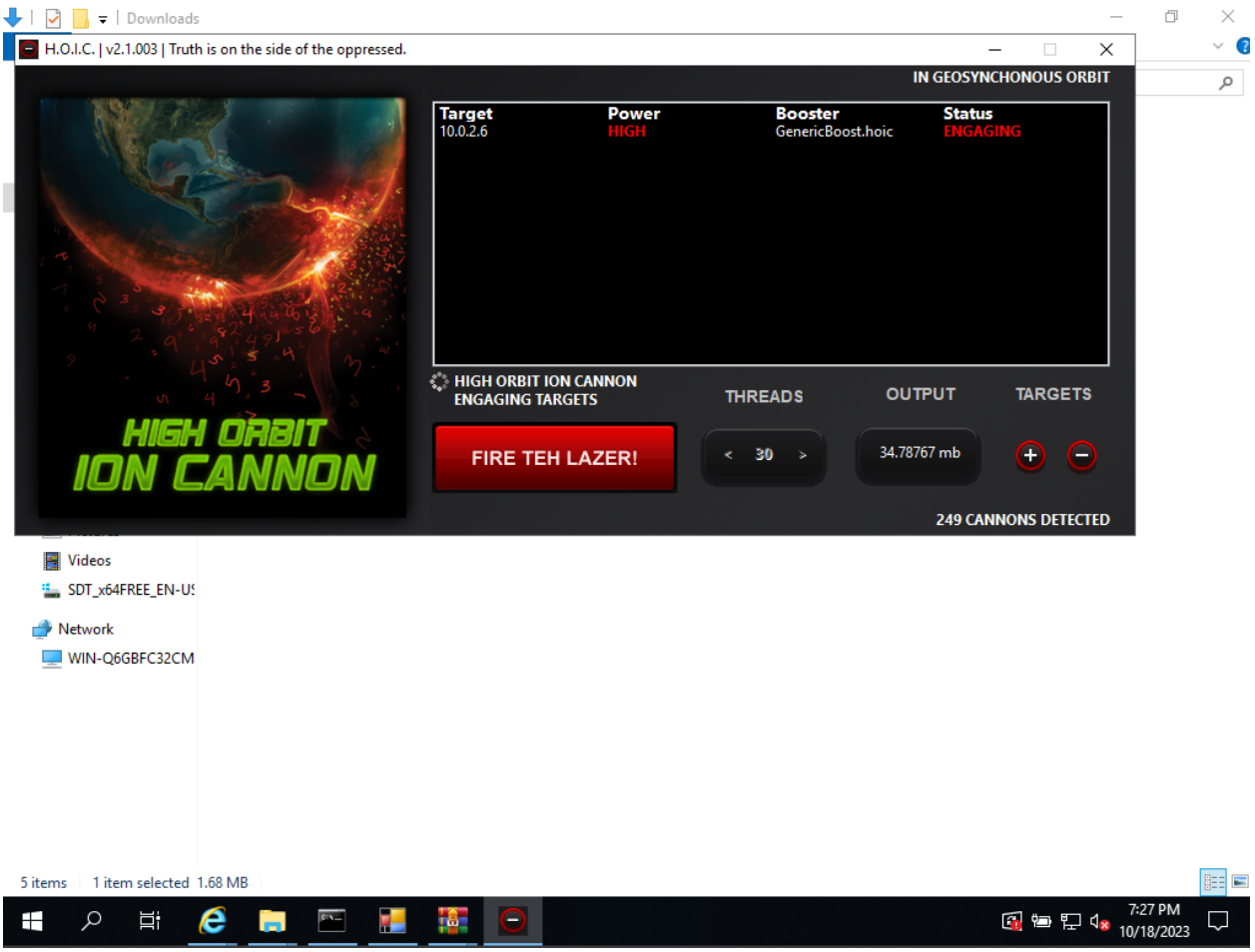

Figure 22 - HOIC Firing in Progress

HOIC was very simple to configure and implement. In Figure 20, I set up the target. Figure 21: I was setting up the threads in Figure 22, and I executed the file. I am familiar with LOIC and HOIC as it has been used by script kiddies to disrupt LANs from my local knowledge.

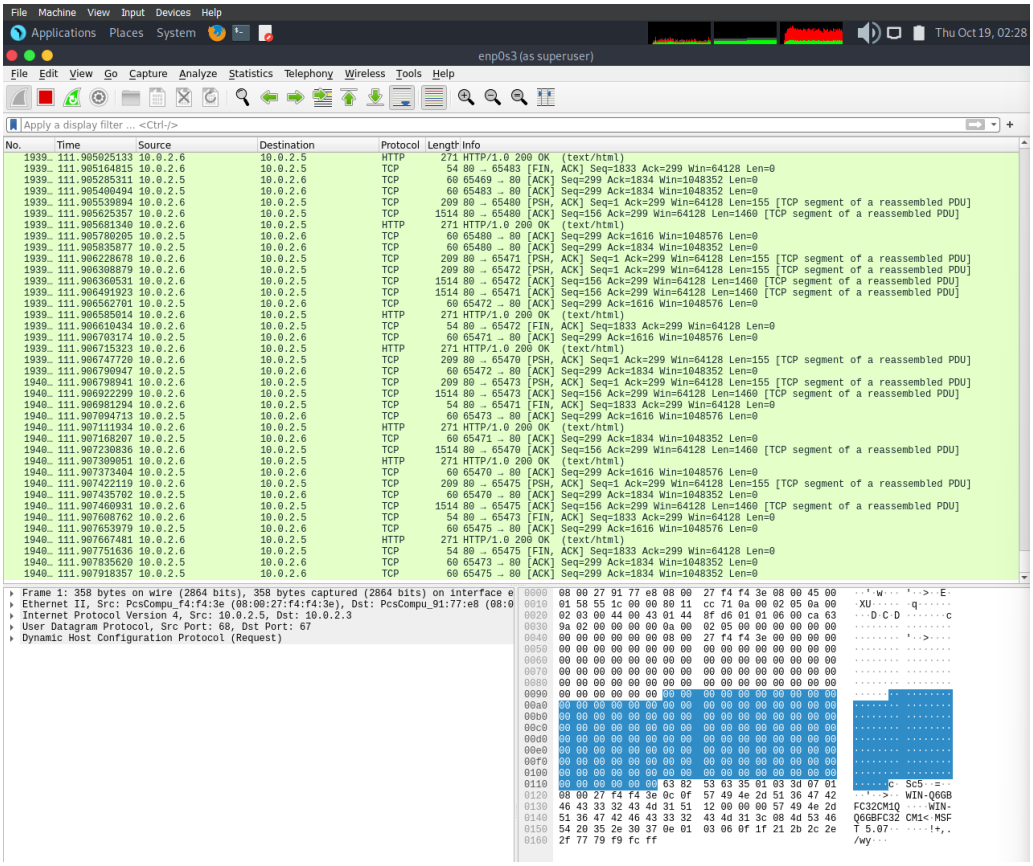

Figure 23 - Wireshark Capturing Packets on Parrot OS Post-DDos

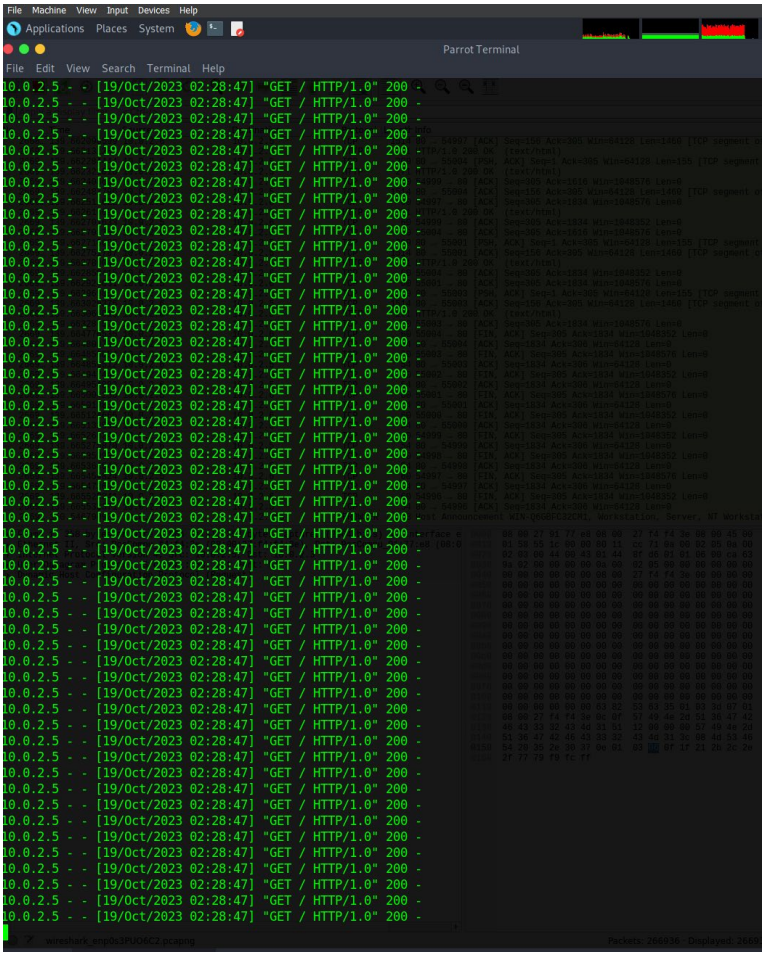

Figure 24 - HTTP Server Post DDos

When using Wireshark, Task 1 contained bad packets from Parrot to Windows. On the other hand, in Task 2, when packets are coming to Parrot from Windows, the packets look normal (Figure 23). But just like Task 1, many packets are still coming to the HTTP Server. This can

further be shown in Figure 24, where we can see the source of all these packets coming from 10.0.2.5 (Windows), all requesting the server.

Extra Credit

Raven-Storm Attacks

Steps

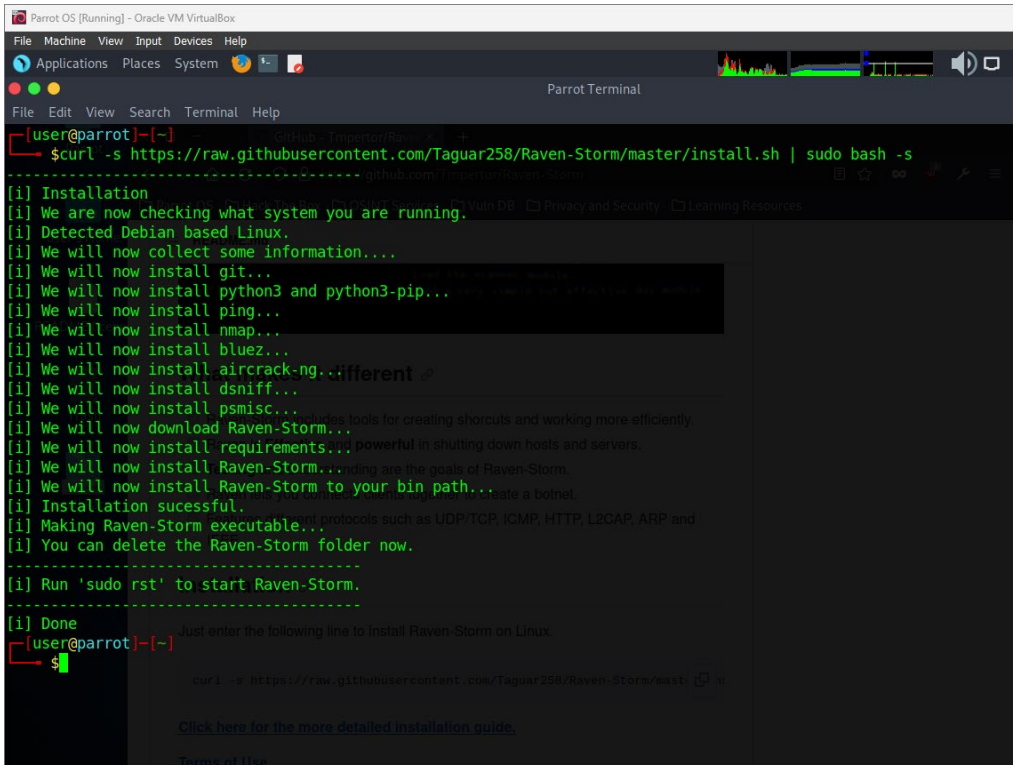

Figure 25 - Successful Install of Raven-Storm

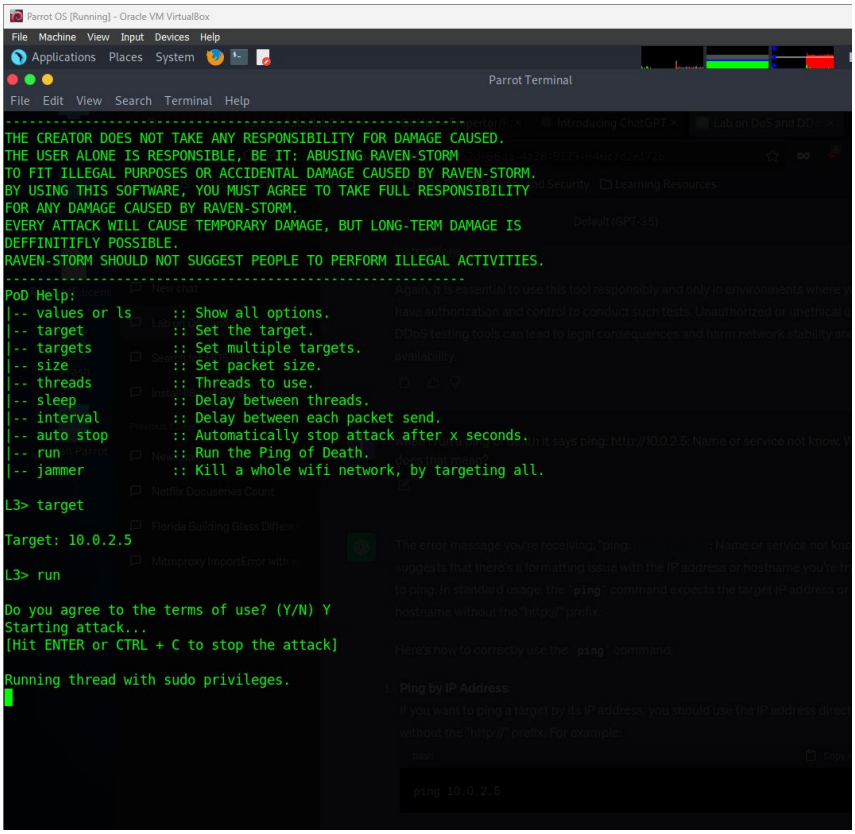

Figure 26 - Running l3 Ping Attack

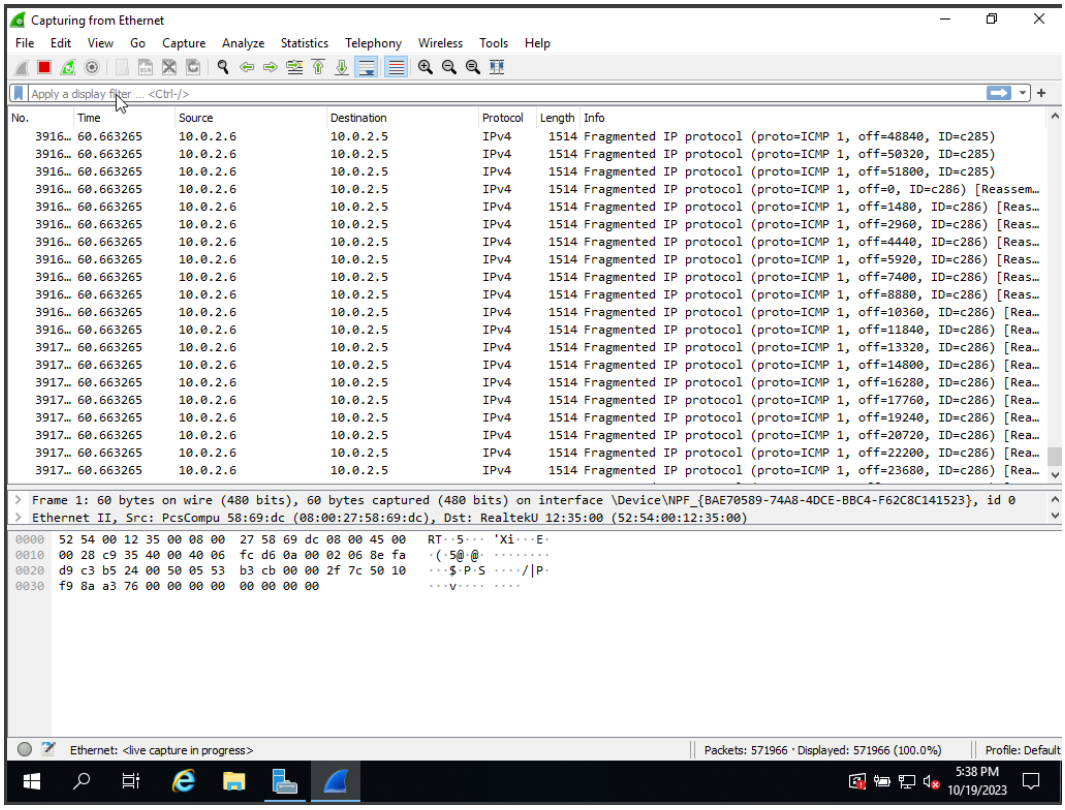

Figure 27 - l3 Ping Attack on Wireshark

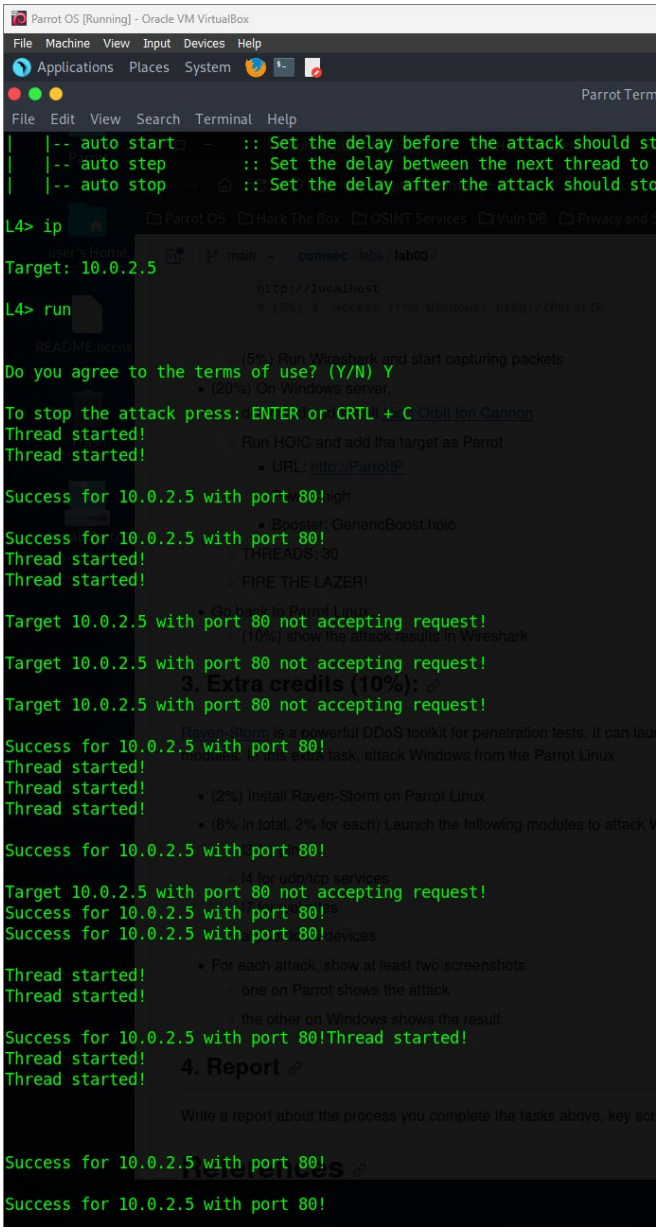

Figure 28 – Running I4 TCP/UDP Attack

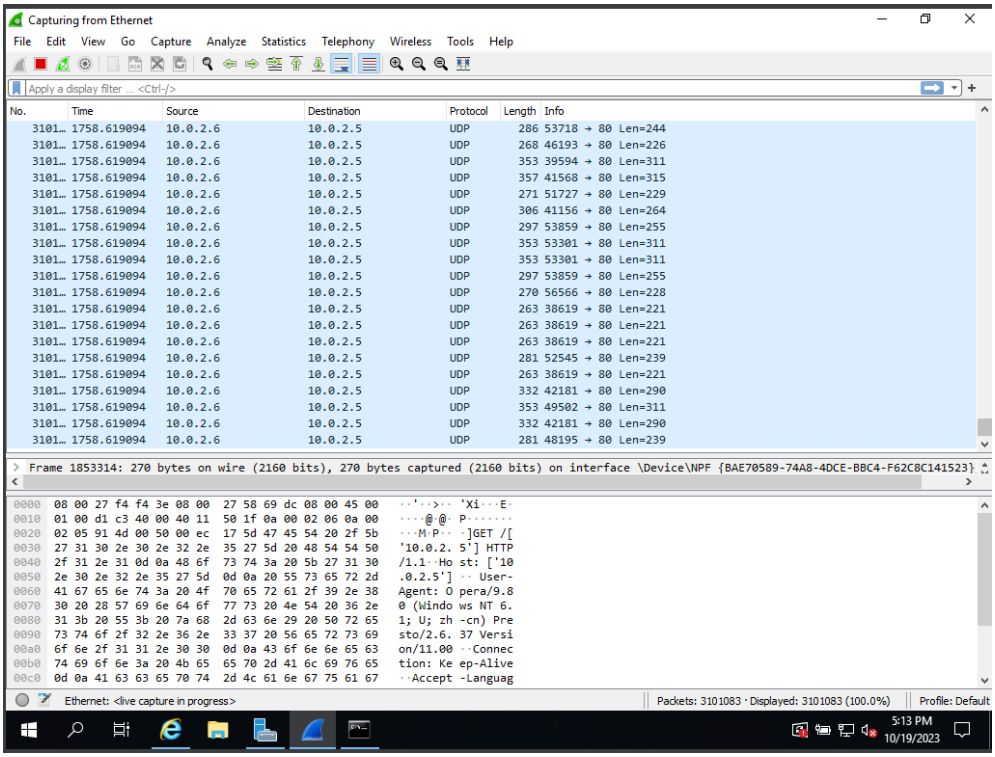

Figure 29 - l4 TCP/UDP Attack on Wireshark

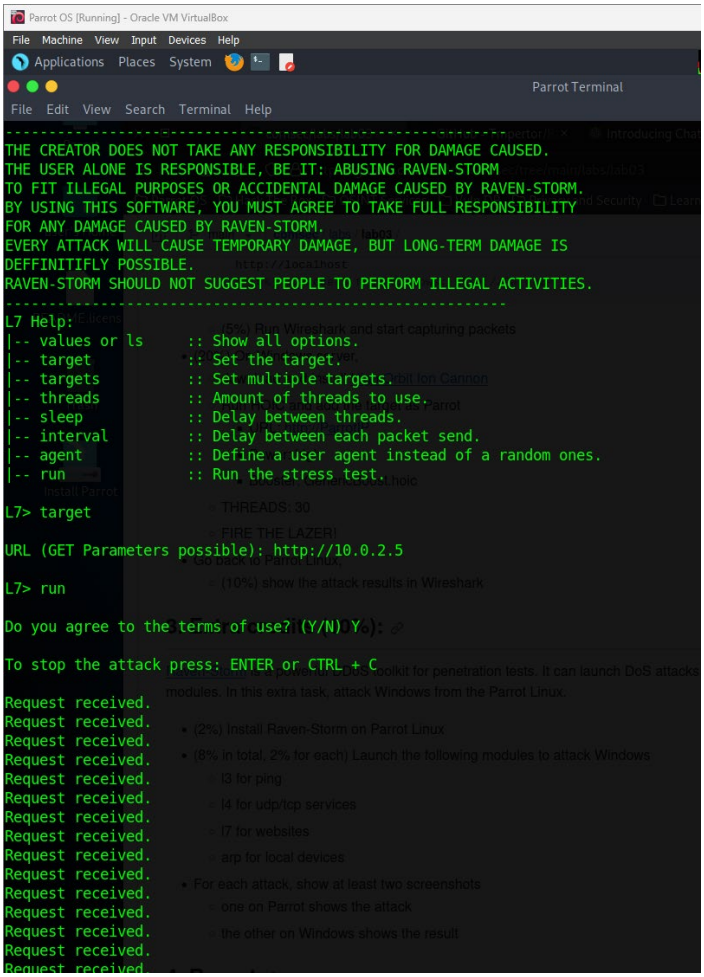

Figure 30 - Running l7 Website Attack

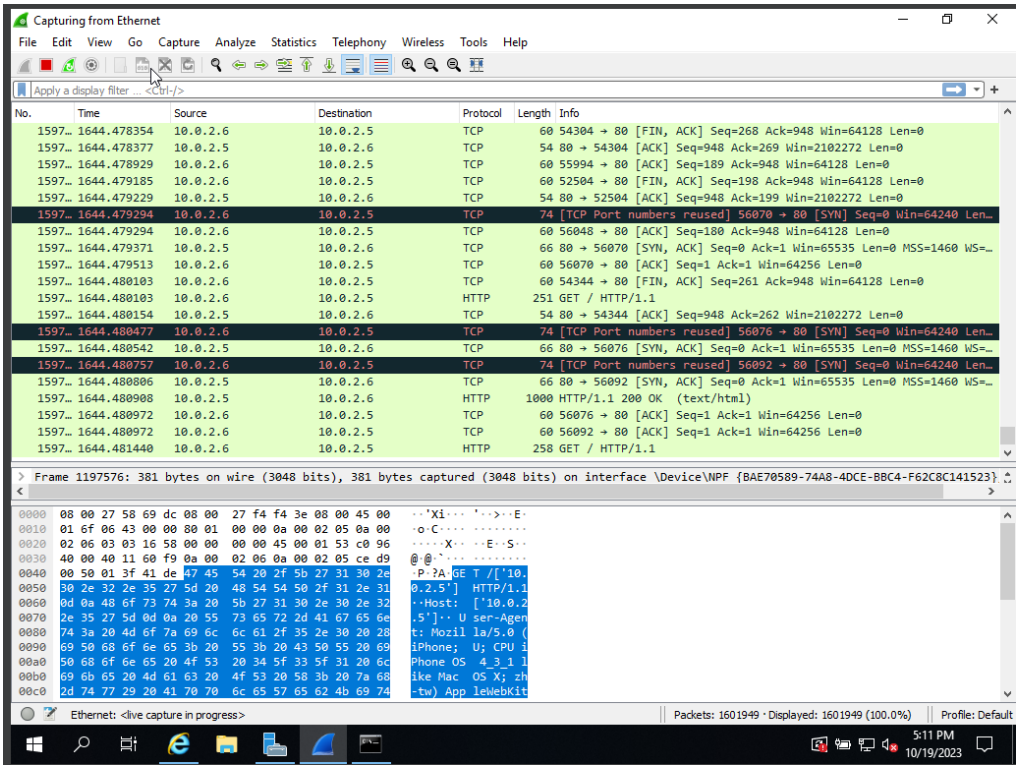

Figure 31 - l7 Website Attack on Wireshark

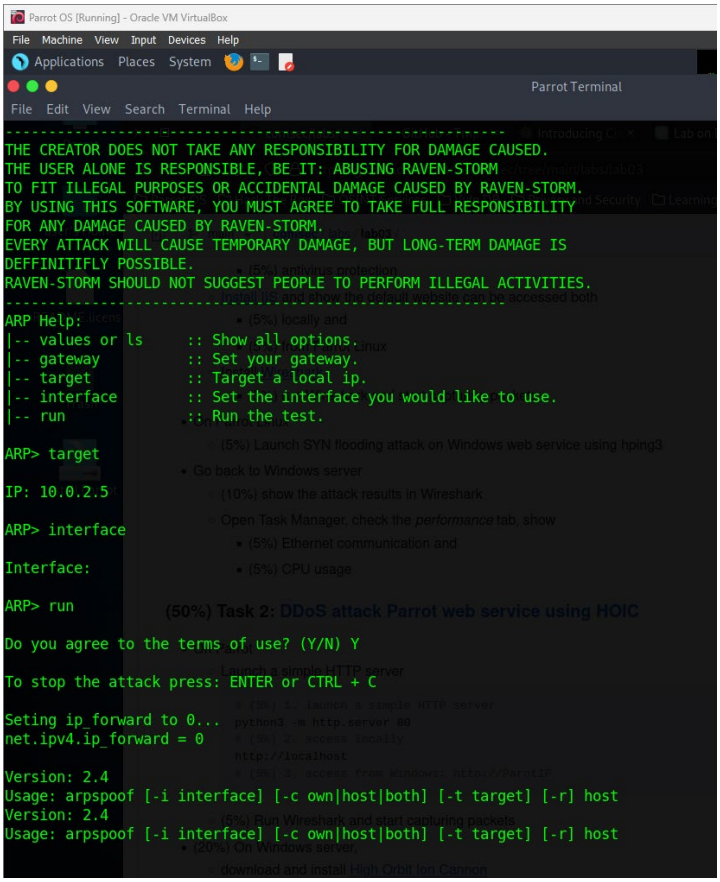

Figure 32 - Running arp Local Devices Attack

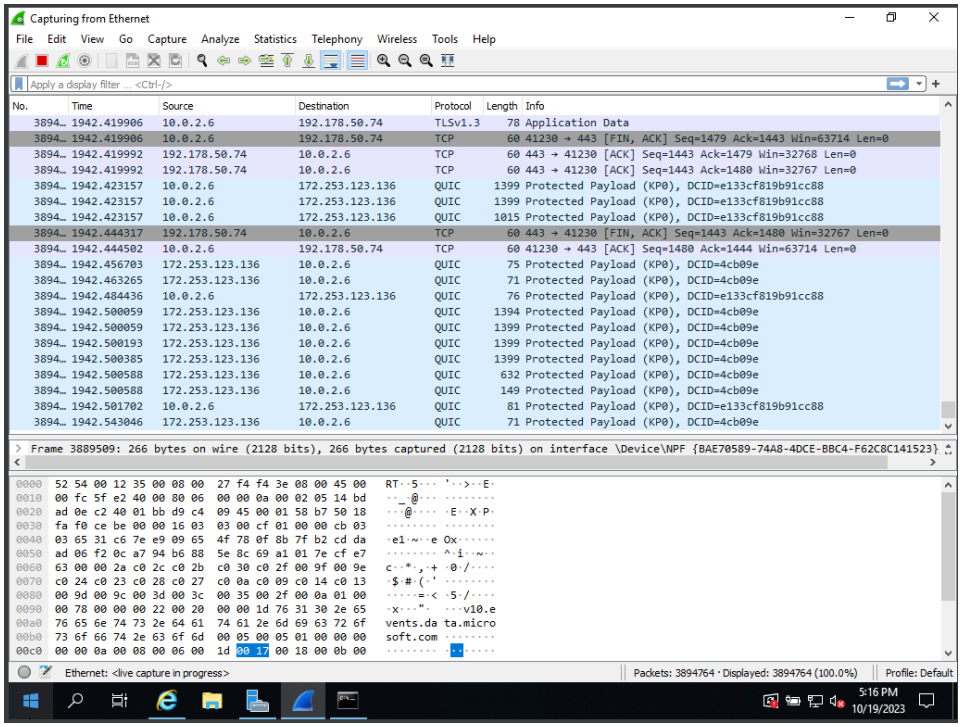

Figure 33 - arp Local Devices Attack on Wireshark

Raven-storm was easy to install and use (Figure 25). My first attack was the ping of death on l3, where I sent numerous pings to a target (Figure 26). What is unique about this attack compared to the other 3I used to be the protocol used was IPv4. When launching an attack on the UDP service using l4, the protocol was UDP (Figure 29). L7 focused on attacking the target's website on port 80, which uses the TCP protocol (Figure 31). The last attack arp uses QUIC protocol (Figure 33).

Issues Or Problems

For Task 1, I was initially confused about where to download IIS because you referred to Windows as “locally,” but I realized that I could only install IIS through Windows Server 2019. Task 2: the primary issue was installing HOIC. I didn’t know where to download HOIC, so I used the first link. Originally, HOIC came as a .rar file, so I had to install WinRAR to extract the .exe file from the .rar file to execute the program. I installed and used LOIC throughout the process because it was easier to install as it was established as a .zip instead of a .rar. I would say the main issue for the Bonus Task was performing execution commands for l4 (UDP/TCP services). Before executing the attack, I assumed that a port number was needed. Since Windows Server 2019 used HTTP, I thought port 80 and set the protocol to TCP since HTTP uses the TCP protocol. After executing the attack, there was a connection failure; however, Windows Server 2019 was still aware of the connection attempt due to ICMP showing up in the packets. However, I was able to get a successful connection after re-rerunning Raven-Storm again.

Conclusion

The lab provided practical hands-on experience with various DoS and DDoS attack techniques, demonstrating their impact on network resources and system performance. It allowed for exploring familiar tools like hping3 and less standard tools like Raven-Storm, allowing students to understand the challenges and implications of network attacks. The lab emphasized the importance of using such tools responsibly and ethically, as unauthorized use can have legal and ethical consequences. Overall, it offered valuable insights into network security and the techniques for assessing and mitigating vulnerabilities.

References

DDoS attack using HOIC. GitHub. (n.d.-a). https://github.com/Samsar4/Ethical-Hacking-Labs/blob/master/9-Denial-of-Service/2-DDoS-using-HOIC.md

GmbH, win. rar. (n.d.). *WinRAR*. WinRAR download free and support. https://www.win-rar.com/start.html?&L=0

High orbit ion cannon. SourceForge. (2020, September 19). https://sourceforge.net/projects/highorbitioncannon/

Syn flooding. GitHub. (n.d.-b). https://github.com/Samsar4/Ethical-Hacking-Labs/blob/master/9-Denial-of-Service/1-SYN-Flooding.md

Tmpertor. (n.d.). *TMPERTOR/Raven-Storm: Raven-Storm is a powerful ddos toolkit for penetration tests, including attacks for several protocols written in python. takedown many connections using several exotic and classic protocols.* GitHub. https://github.com/Tmpertor/Raven-Storm

Wang, X. (n.d.). *DOS attack, Detection and Defense*. GitHub.

https://github.com/ufidon/comsec/tree/main/labs/lab03

Wireshark · go deep. Wireshark. (n.d.). https://www.wireshark.org/