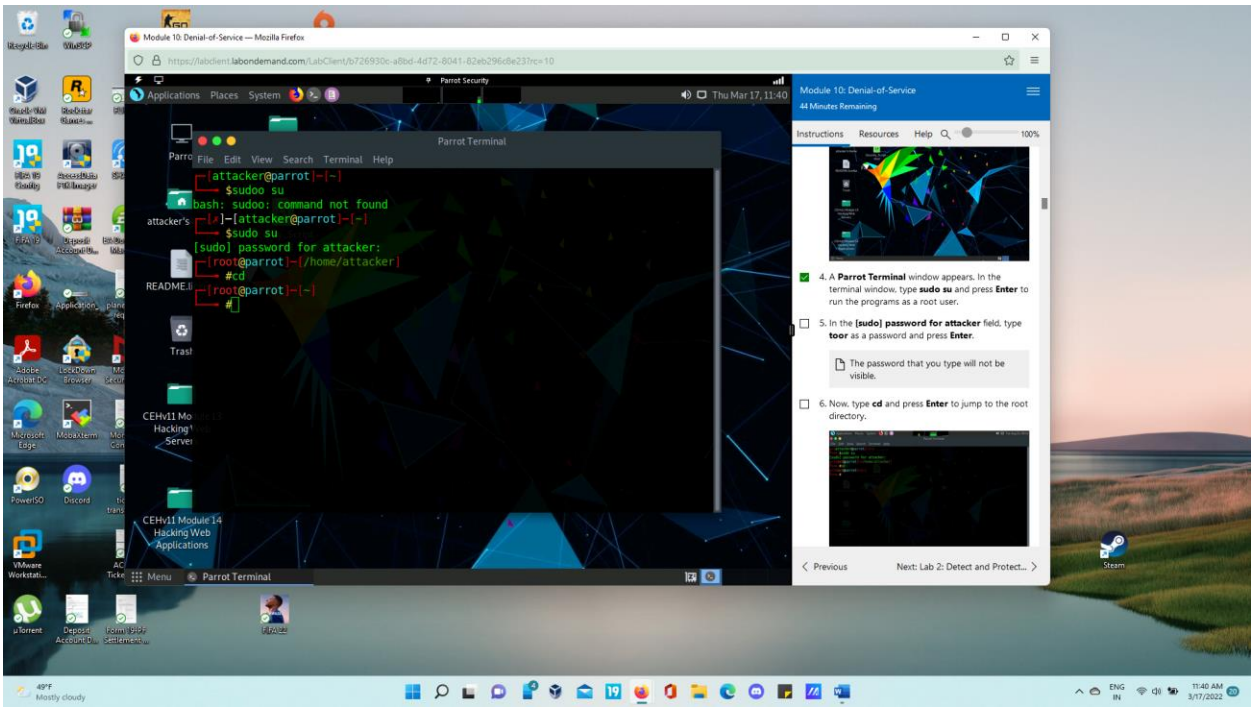
Contents

Module 10: Denial-of-Service

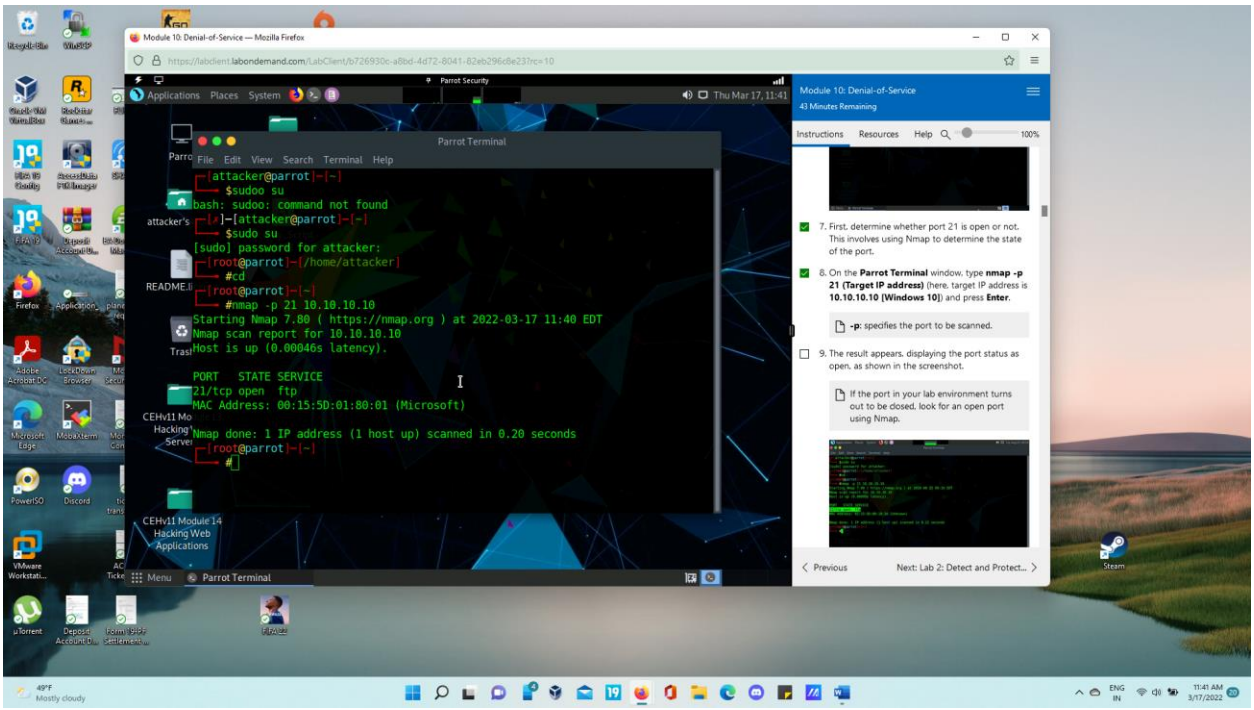
Lab 1: Perform DoS and DDoS Attacks using Various Techniques

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

Click Parrot Security to switch to the Parrot Security machine.

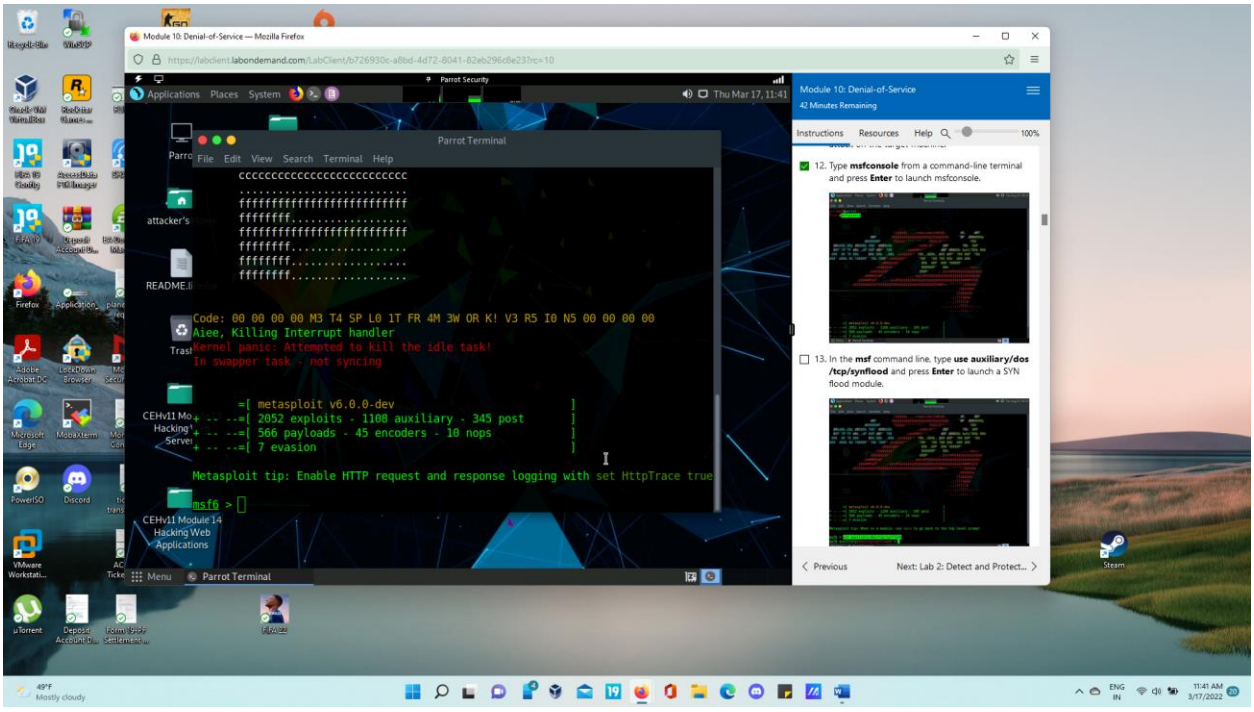


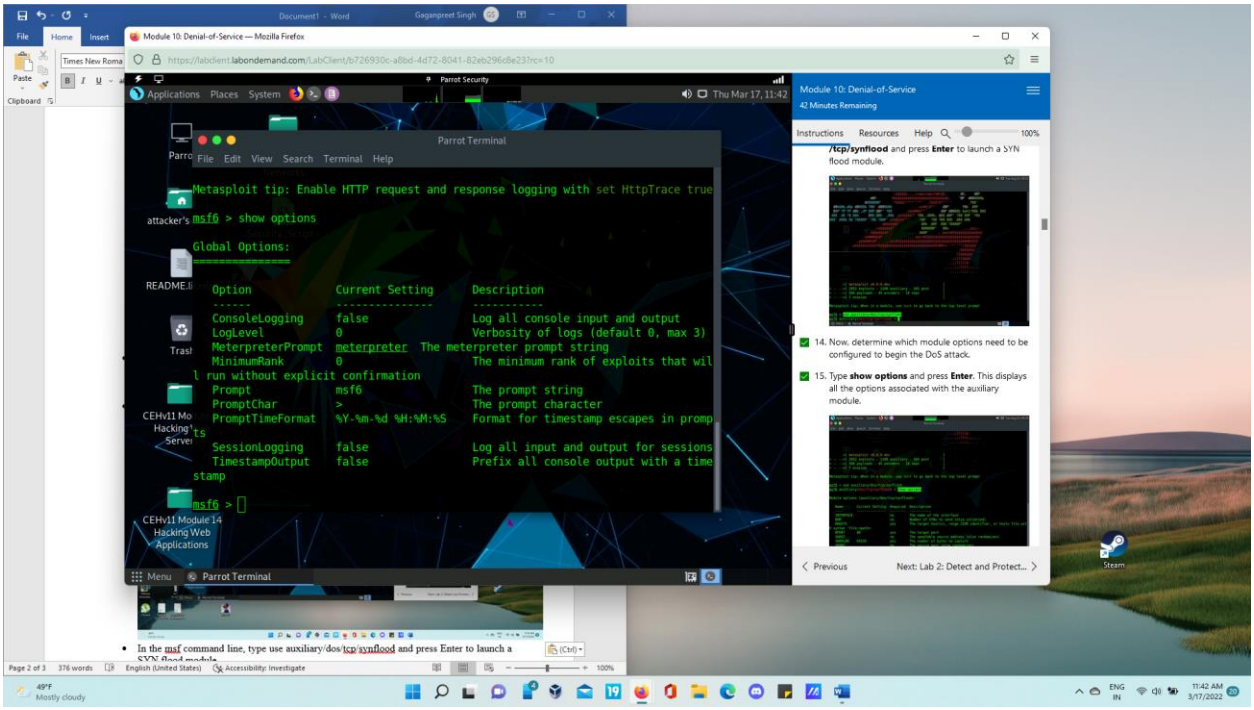
First, determine whether port 21 is open or not. This involves using Nmap to determine the state of the port. On the Parrot Terminal window, type nmap -p 21 (Target IP address) (here, target IP address is 10.10.10.10 [Windows 10]) and press Enter.



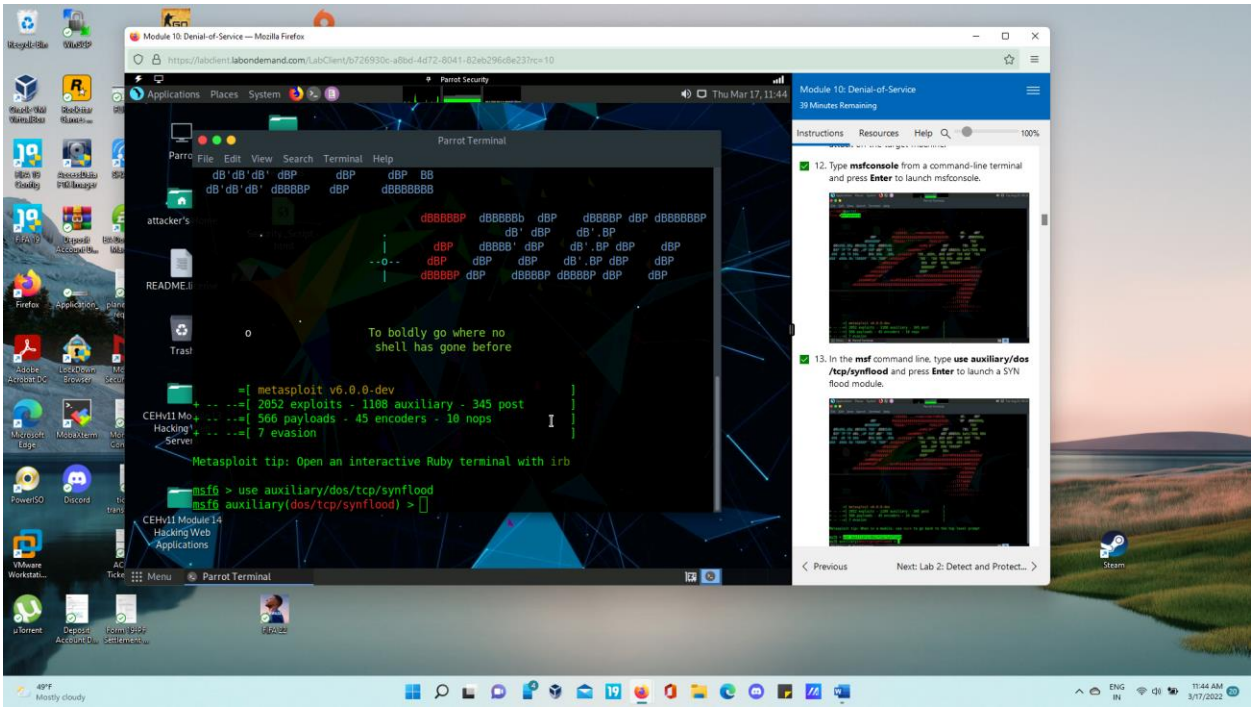
The result appears, displaying the port status as open, as shown in the screenshot. Now, we will perform SYN flooding on the target machine (Windows 10) using port 21. In this task, we will use an auxiliary module of Metasploit called synflood to perform a DoS attack on the target machine.

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

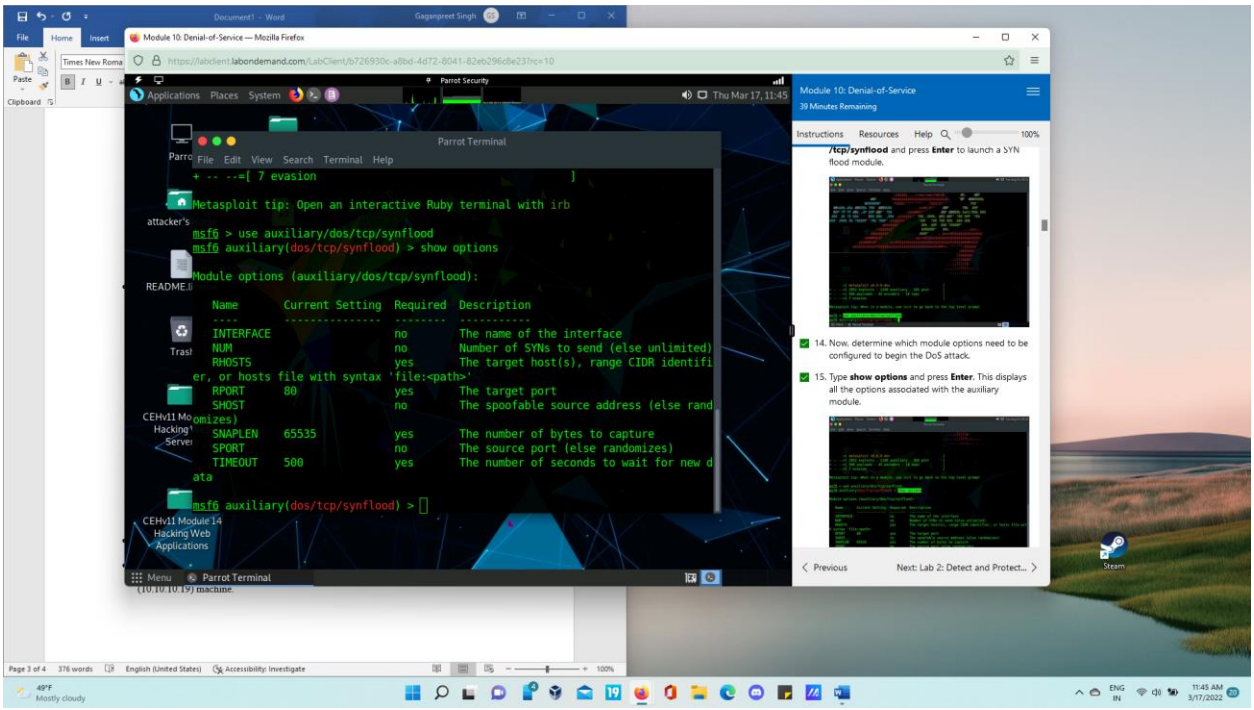




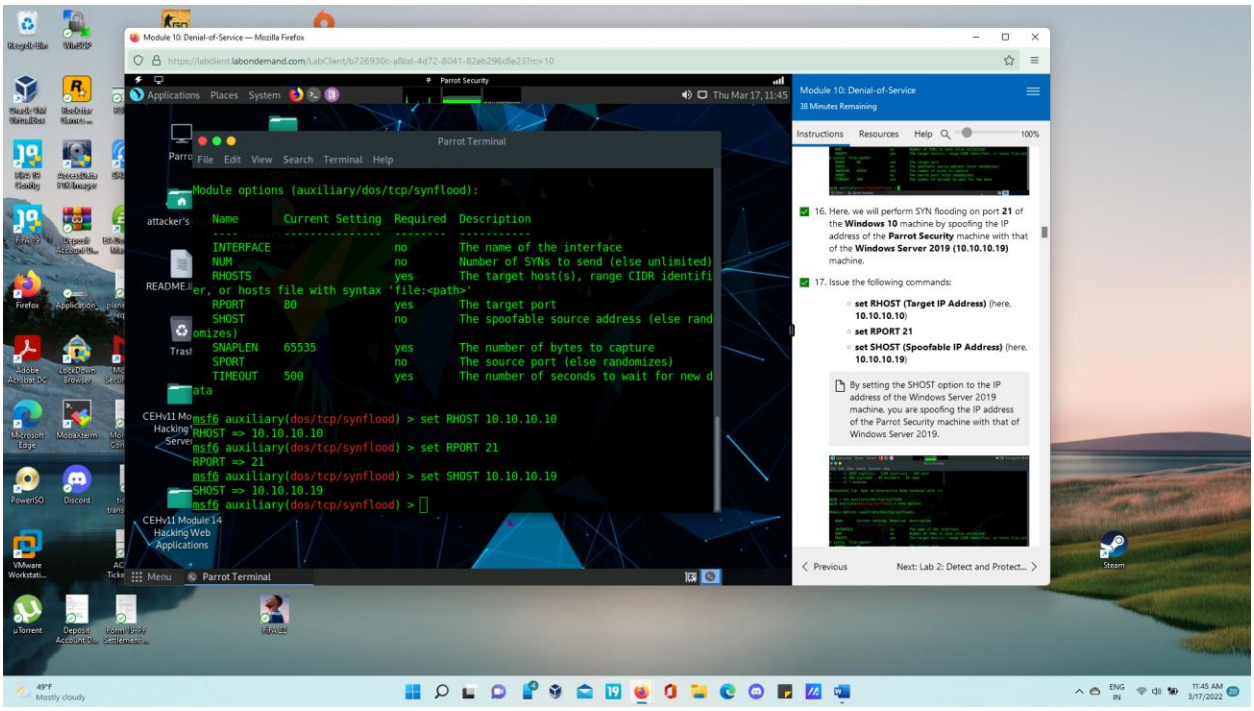
In the msf command line, type use auxiliary/dos/tcp/synflood and press Enter to launch a SYN flood module.



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

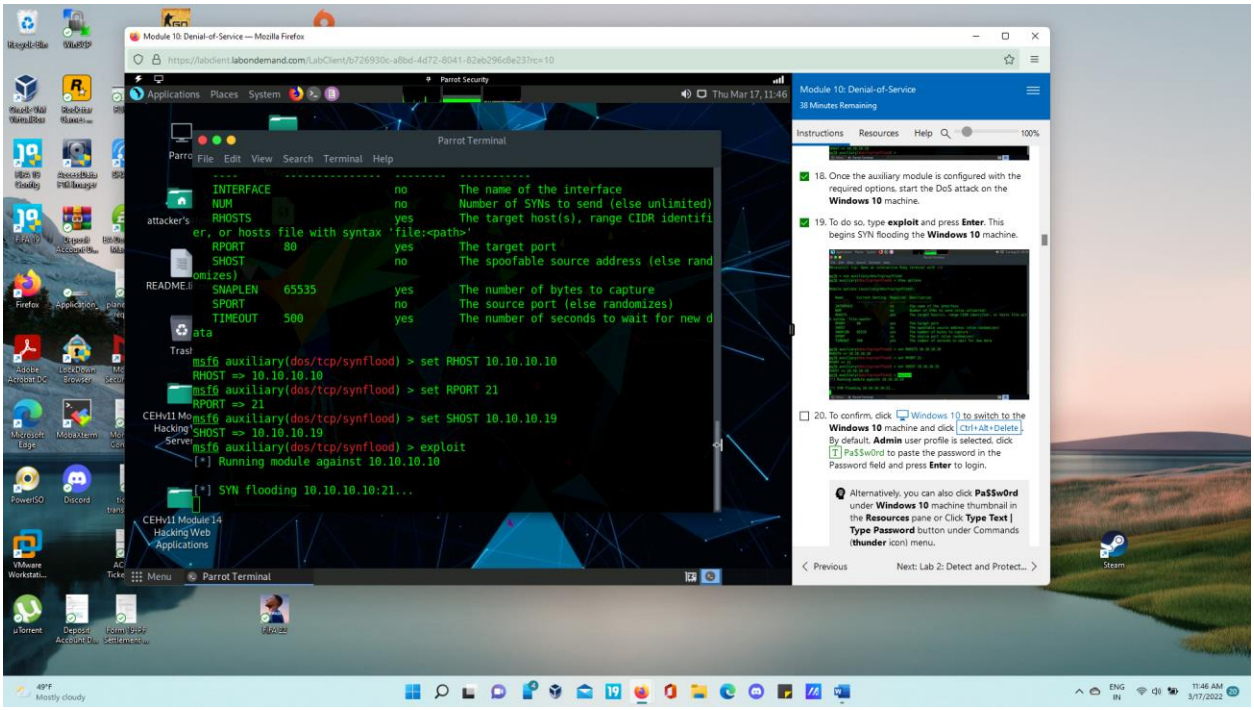


Here, we will perform SYN flooding on port 21 of the Windows 10 machine by spoofing the IP address of the Parrot Security machine with that of the Windows Server 2019 (10.10.10.19) machine.



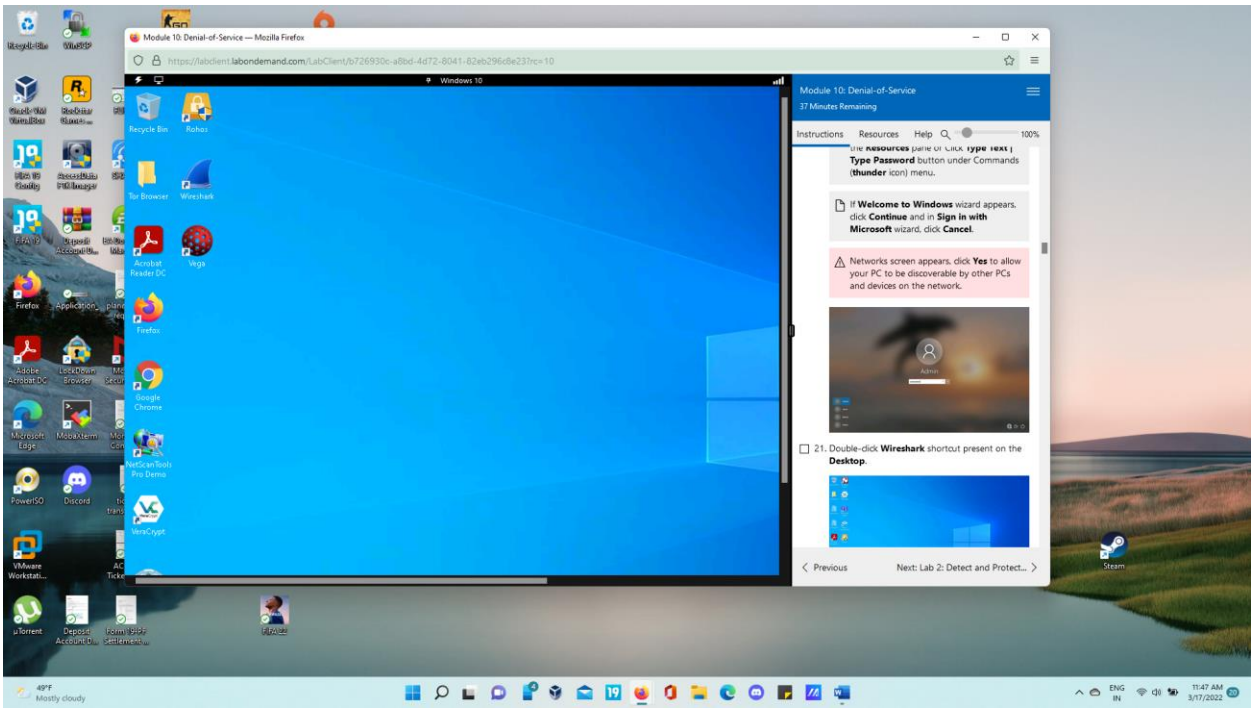
Once the auxiliary module is configured with the required options, start the DoS attack on the Windows 10 machine.

To do so, type exploit and press Enter. This begins SYN flooding the Windows 10 machine.

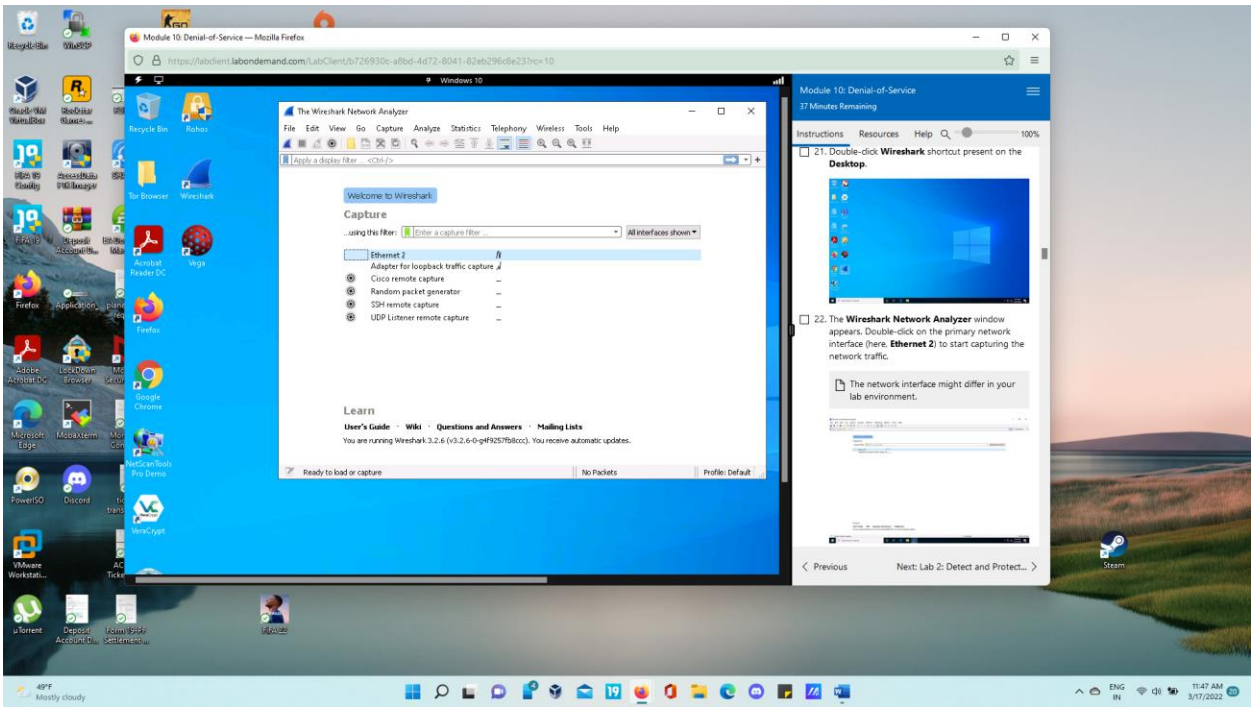


To confirm, click Windows 10 to switch to the Windows 10 machine and click Ctrl+Alt+Delete. By default, Admin user profile is selected, click Pa$$w0rd to paste the password in the Password field and press Enter to login.

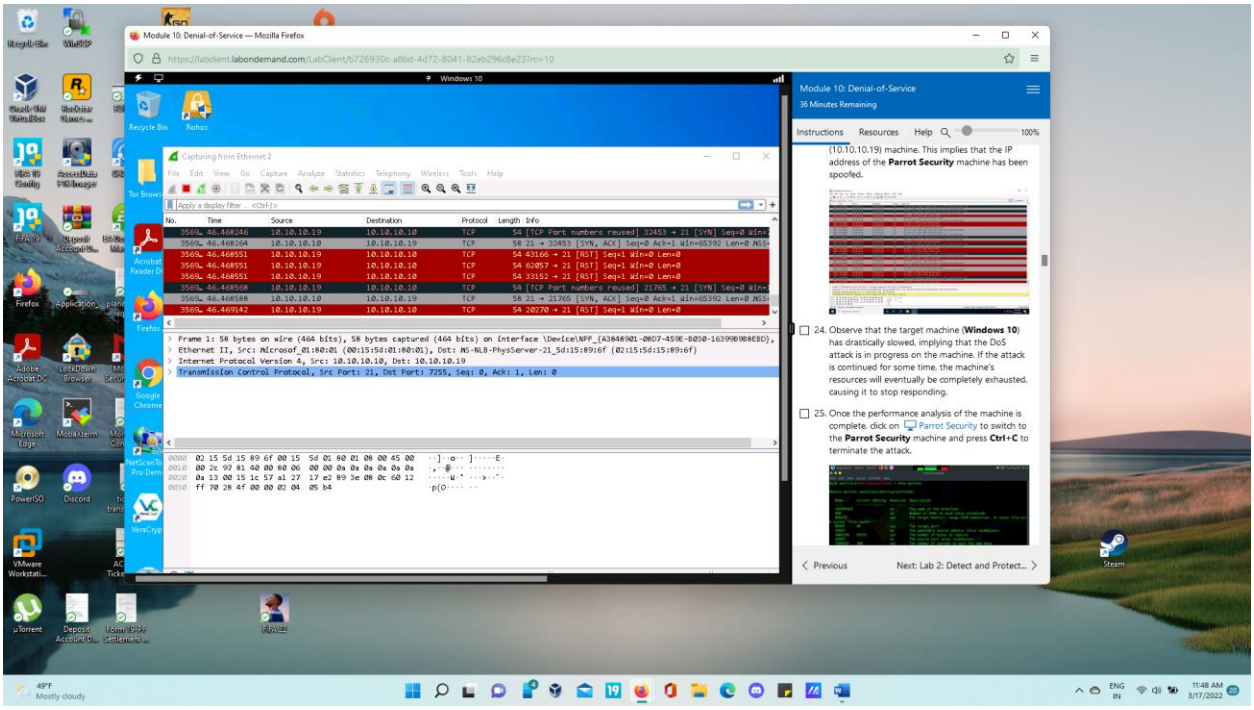
Double-click Wireshark shortcut present on the Desktop.



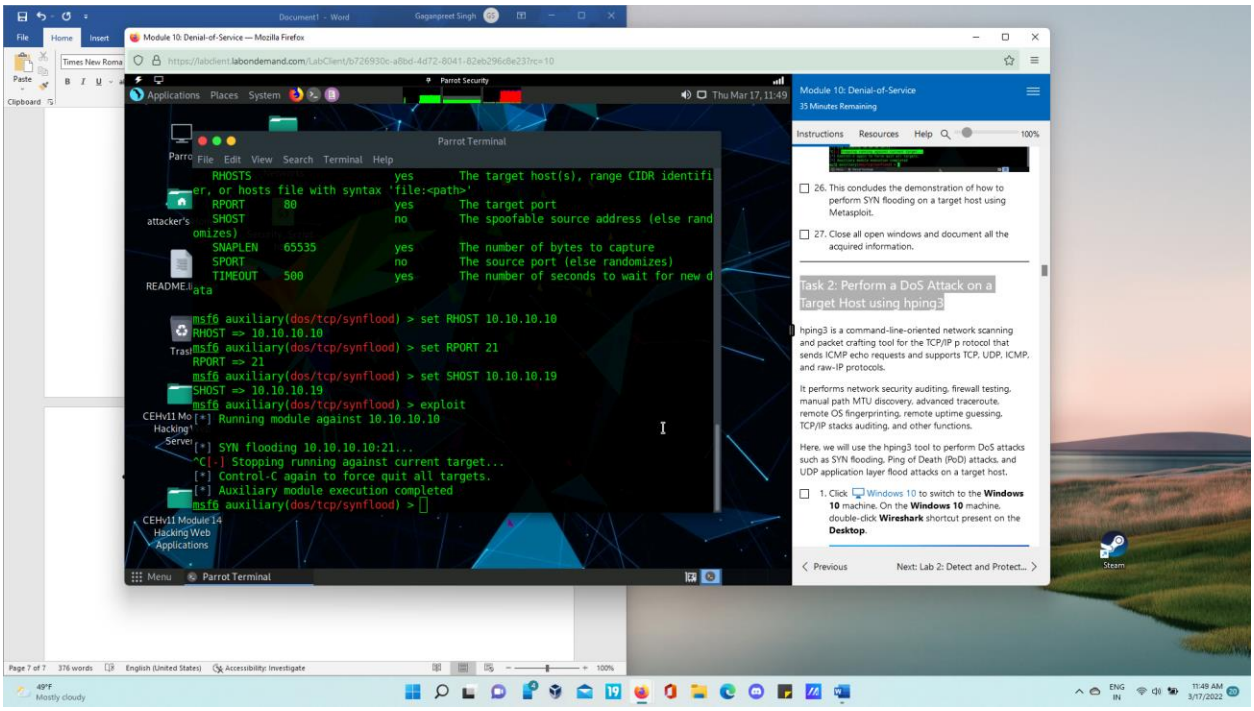
The Wireshark Network Analyzer window appears. Double-click on the primary network interface (here, Ethernet 2) to start capturing the network traffic.



Wireshark displays the traffic coming from the machine. Here, you can observe that the Source IP address is that of the Windows Server 2019 (10.10.10.19) machine. This implies that the IP address of the Parrot Security machine has been spoofed.

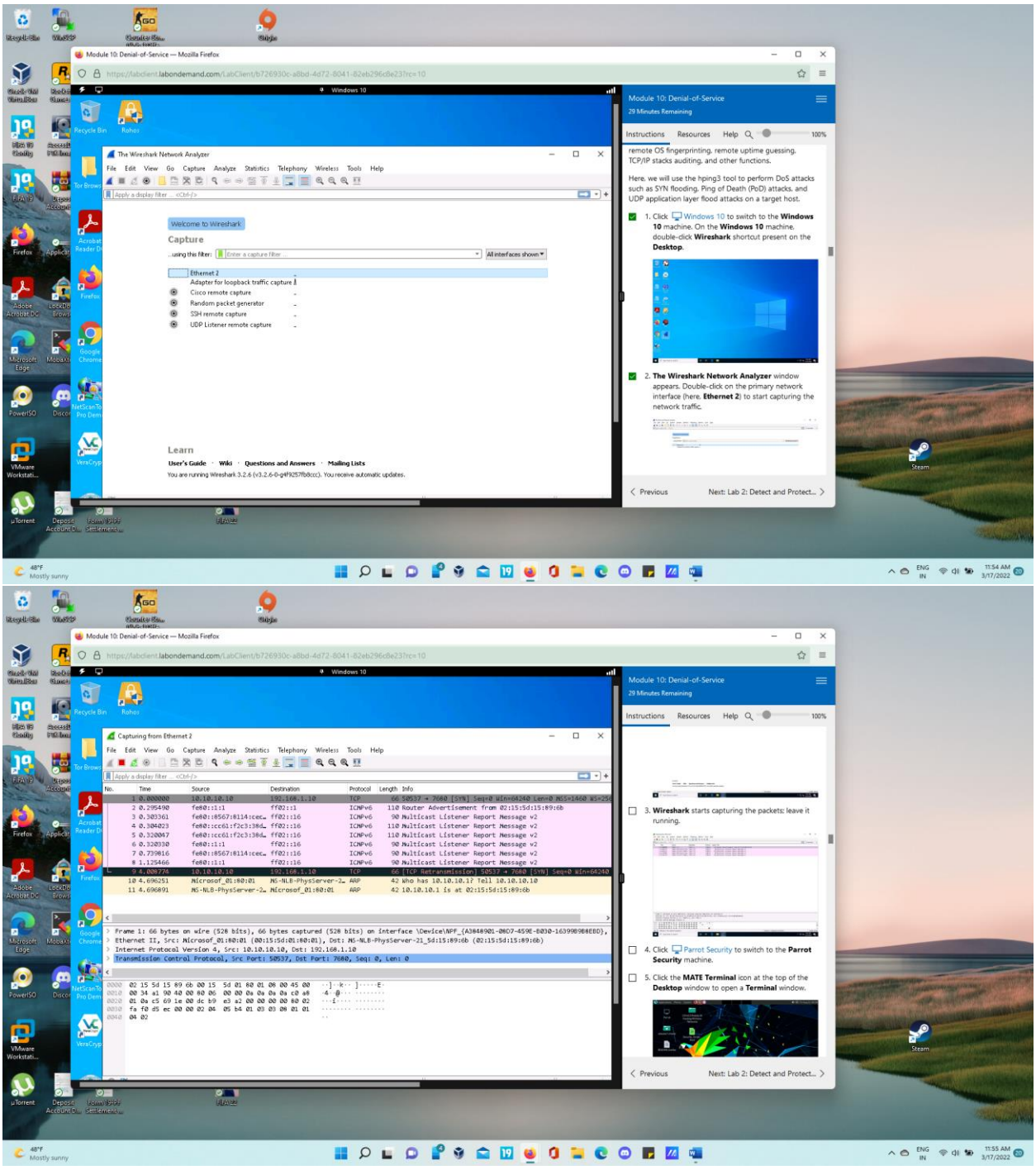


Once the performance analysis of the machine is complete, click on Parrot Security to switch to the Parrot Security machine and press Ctrl+C to terminate the attack.

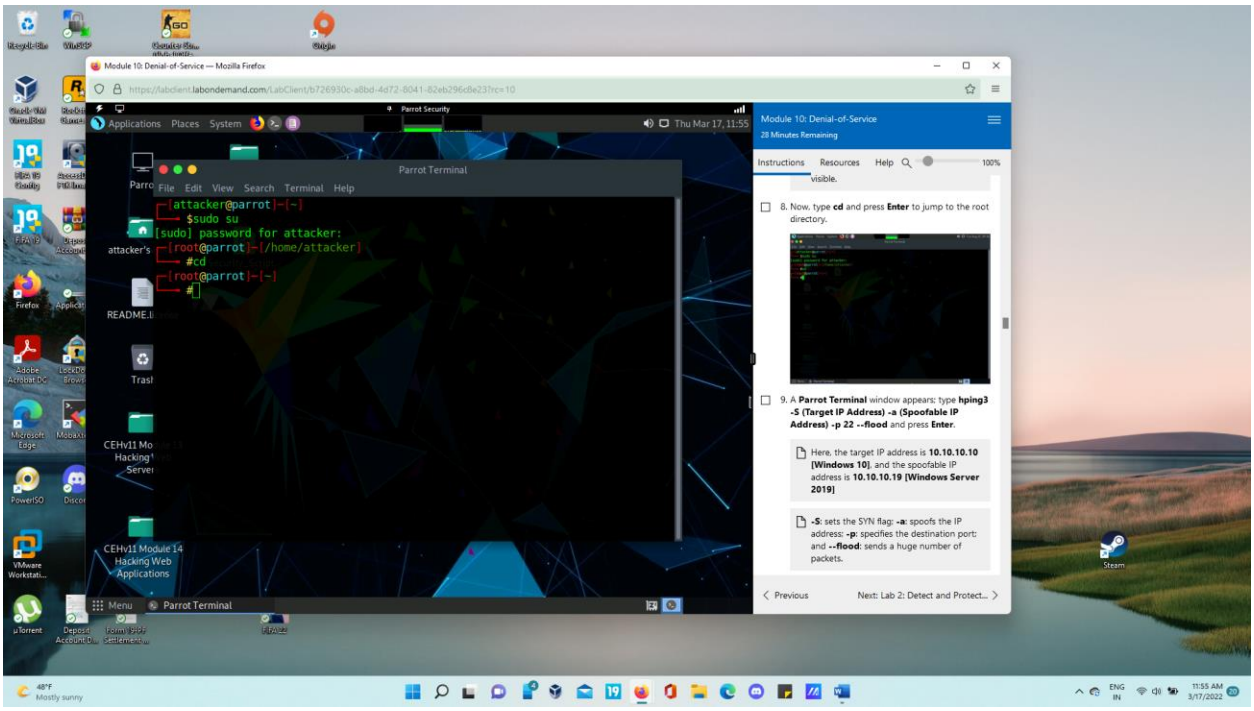


Task 2: Perform a DoS Attack on a Target Host using hping3

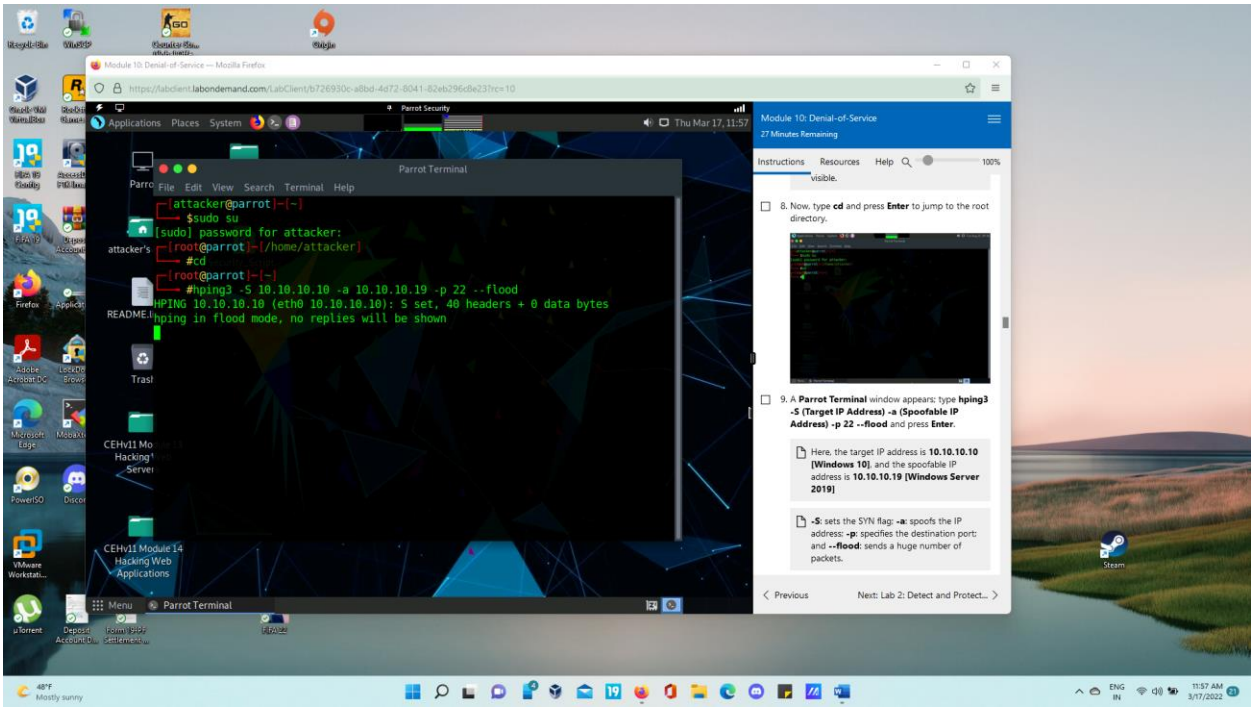
- Click Windows 10 to switch to the Windows 10 machine. On the Windows 10 machine, double-click Wireshark shortcut present on the Desktop.
- The Wireshark Network Analyzer window appears. Double-click on the primary network interface (here, Ethernet 2) to start capturing the network traffic.



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

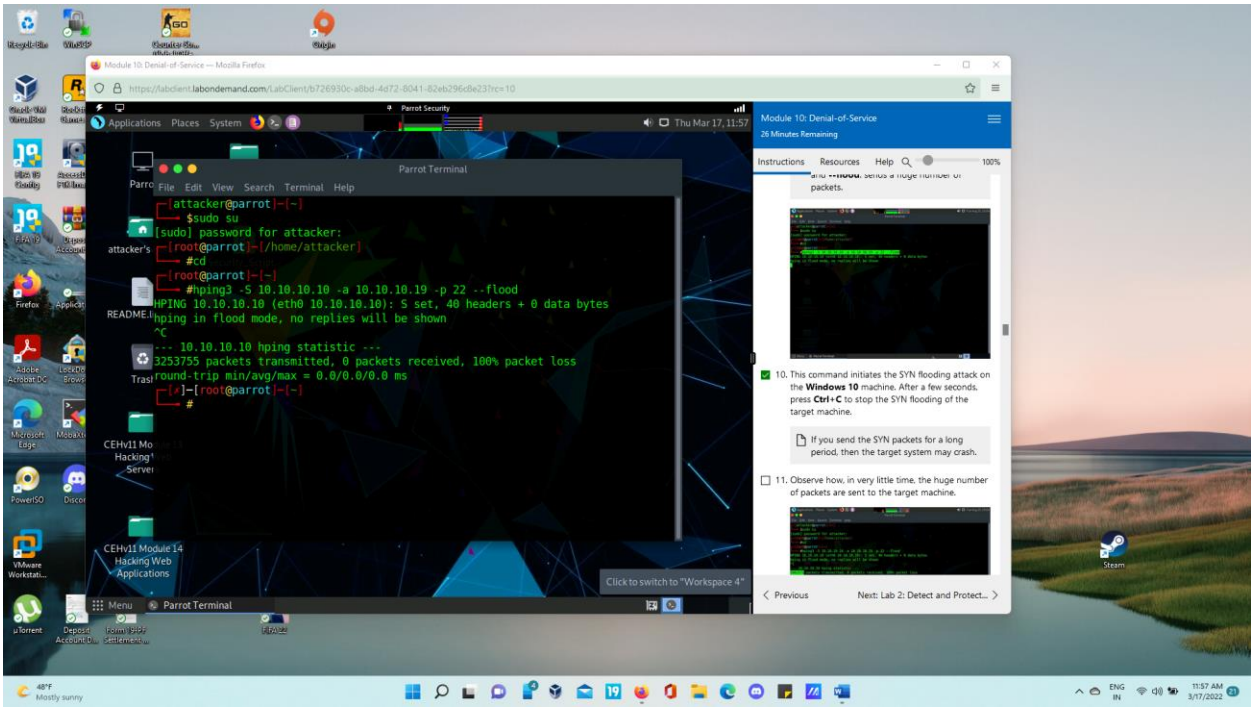


- A Parrot Terminal window appears; type hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood and press Enter.

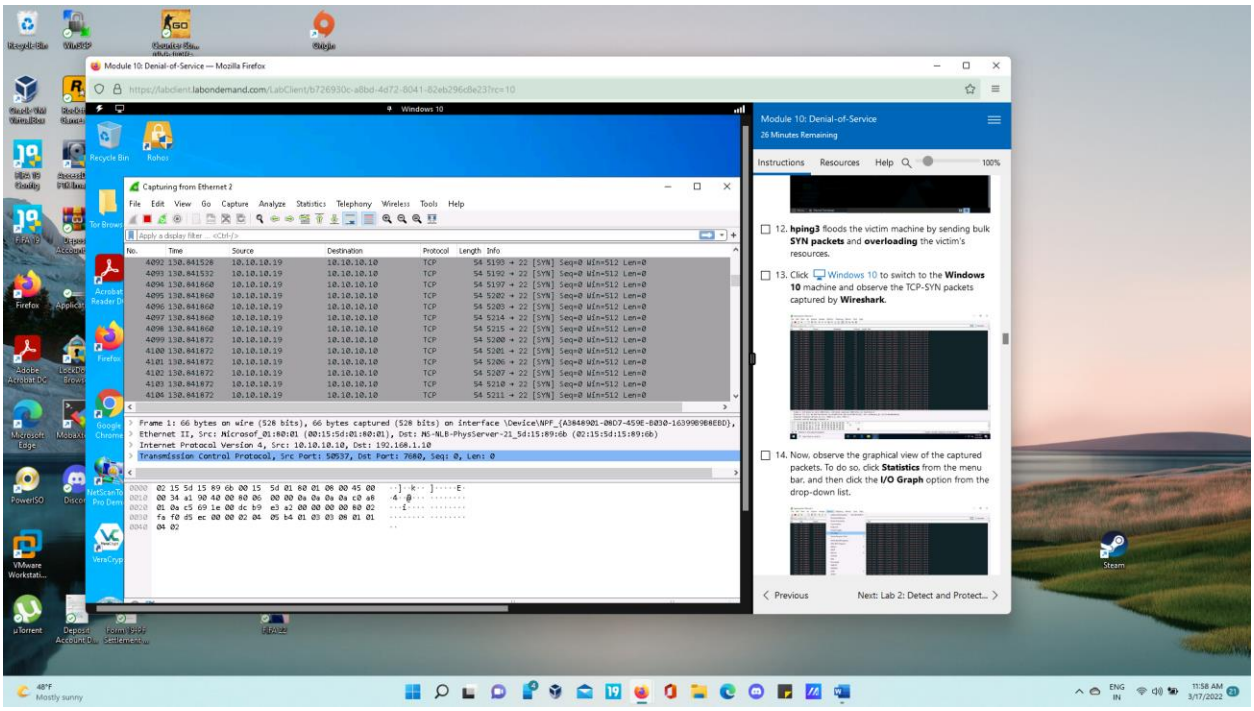


- This command initiates the SYN flooding attack on the Windows 10 machine. After a few seconds, press Ctrl+C to stop the SYN flooding of the target machine.

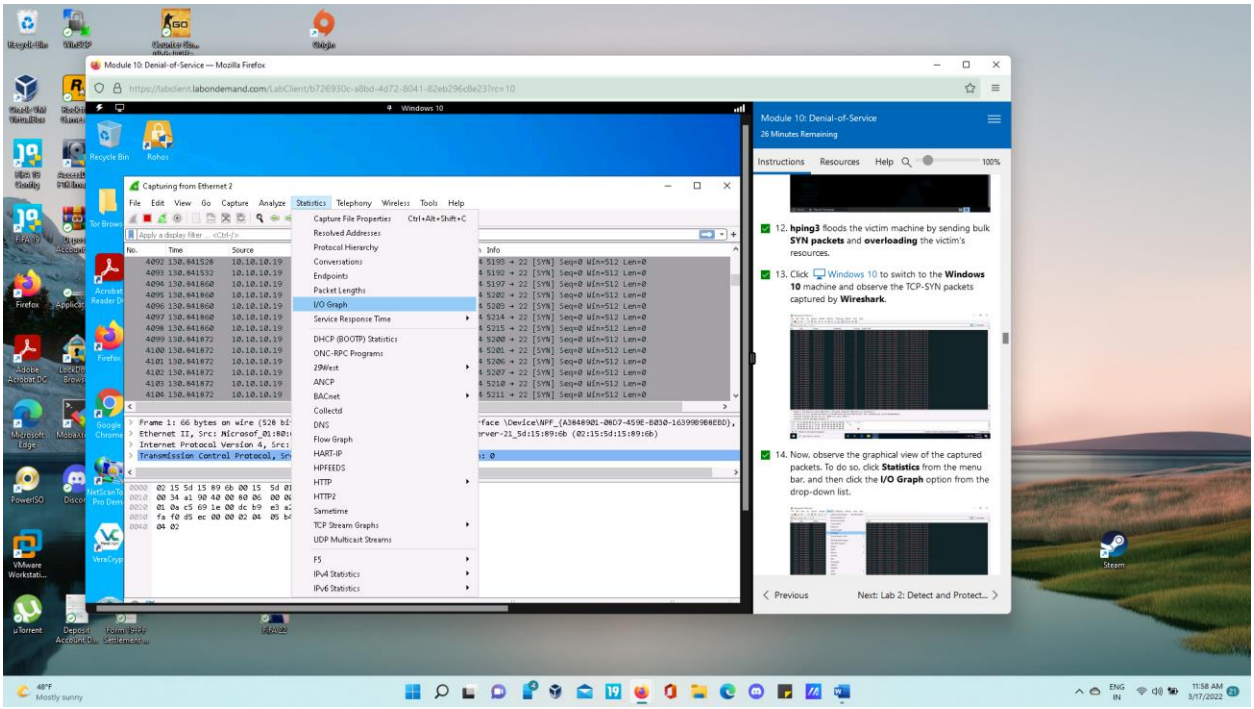
- Observe how, in very little time, the huge number of packets are sent to the target machine.



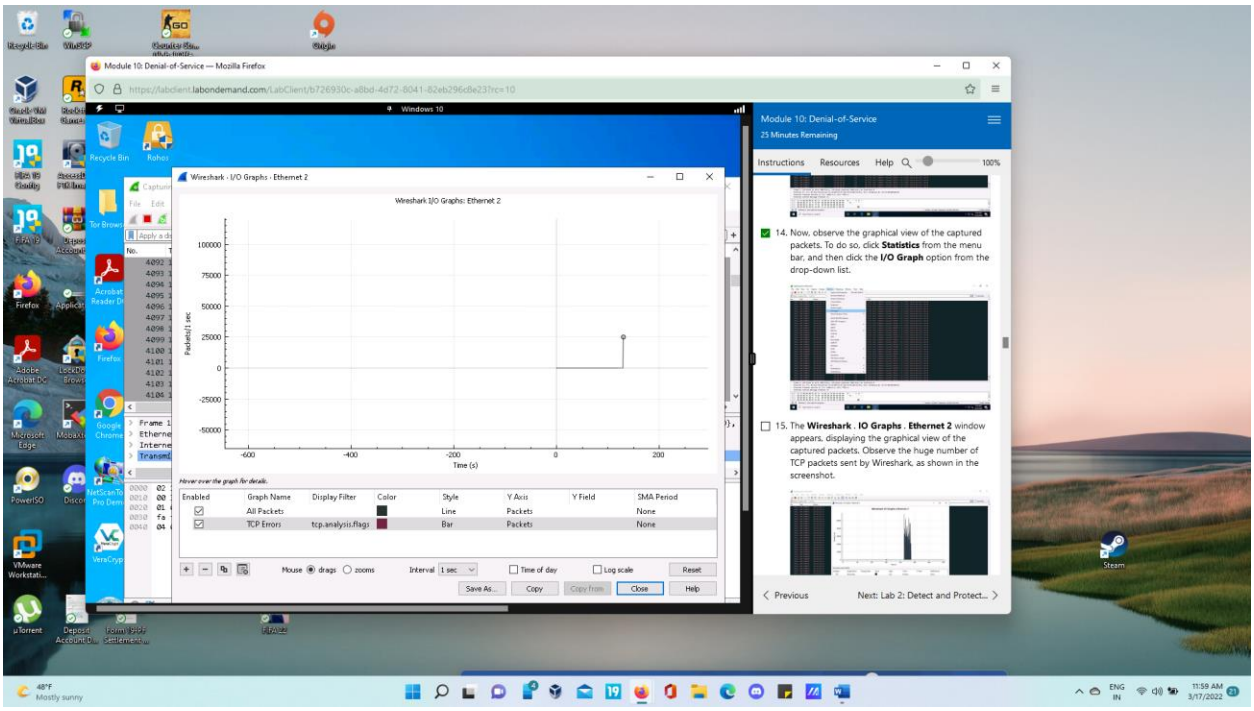
- Click Windows 10 to switch to the Windows 10 machine and observe the TCP-SYN packets captured by Wireshark.

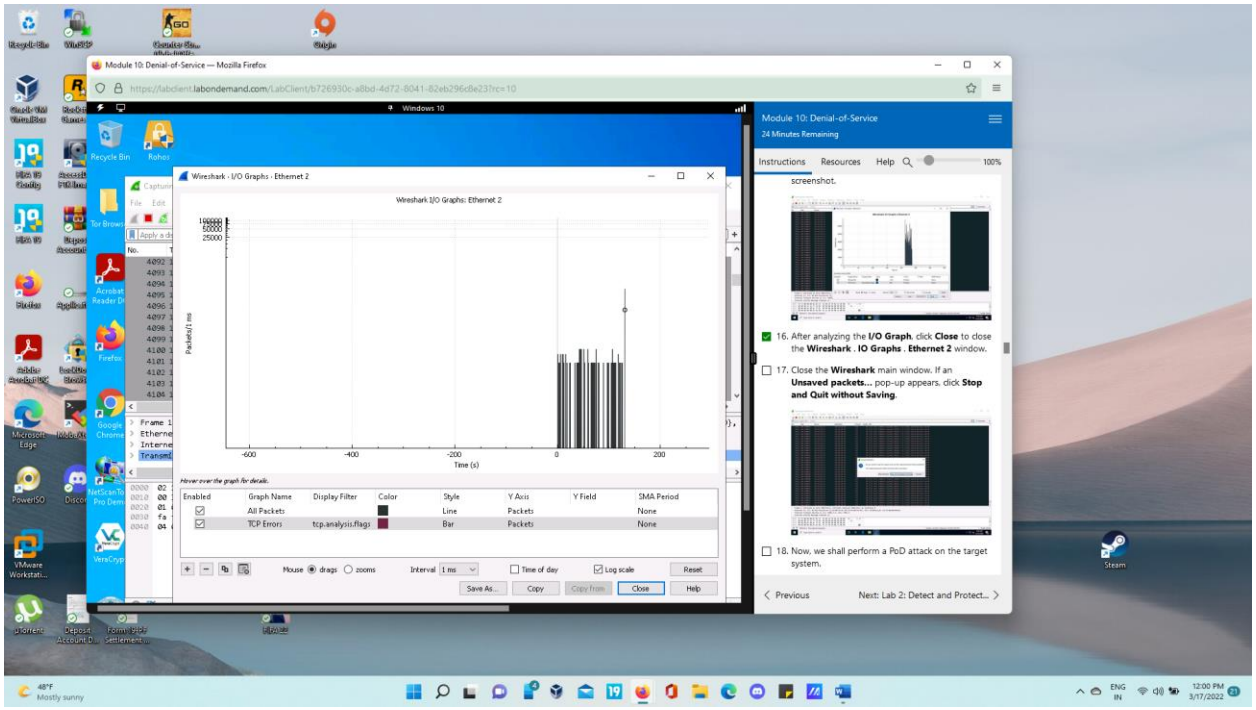


- Now, observe the graphical view of the captured packets. To do so, click Statistics from the menu bar, and then click the I/O Graph option from the drop-down list.

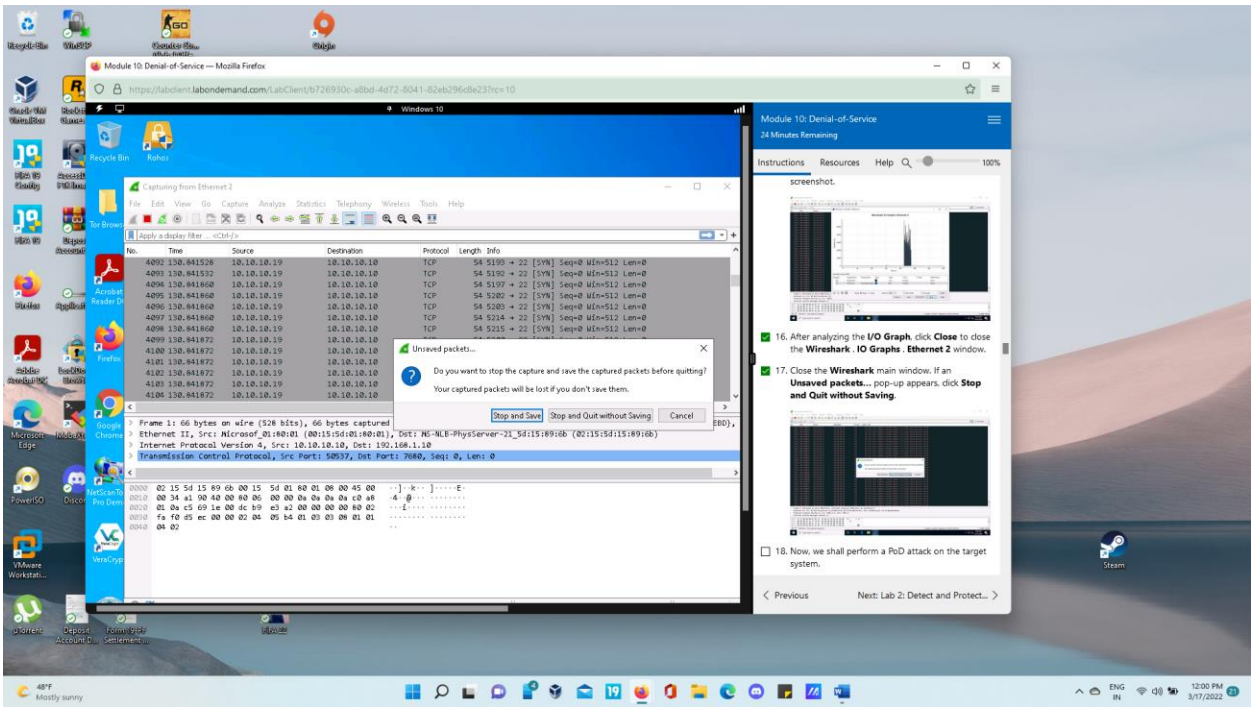


- The Wireshark . IO Graphs . Ethernet 2 window appears, displaying the graphical view of the captured packets. Observe the huge number of TCP packets sent by Wireshark, as shown in the screenshot.

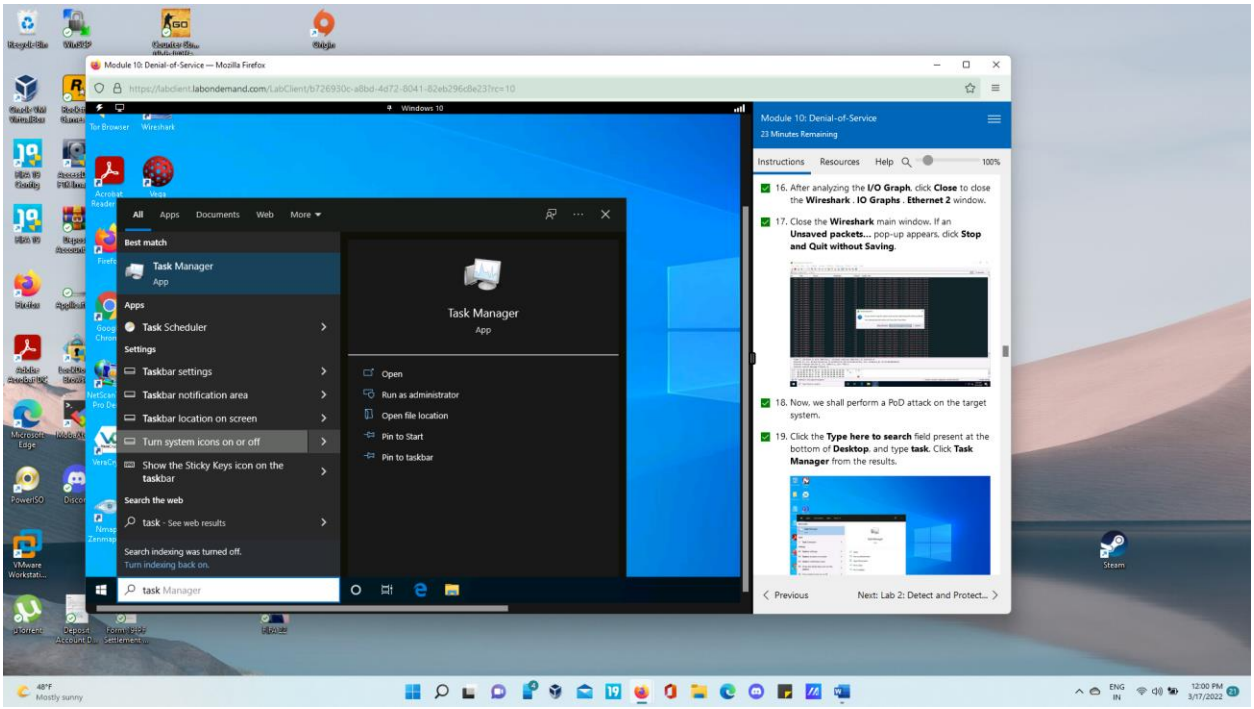




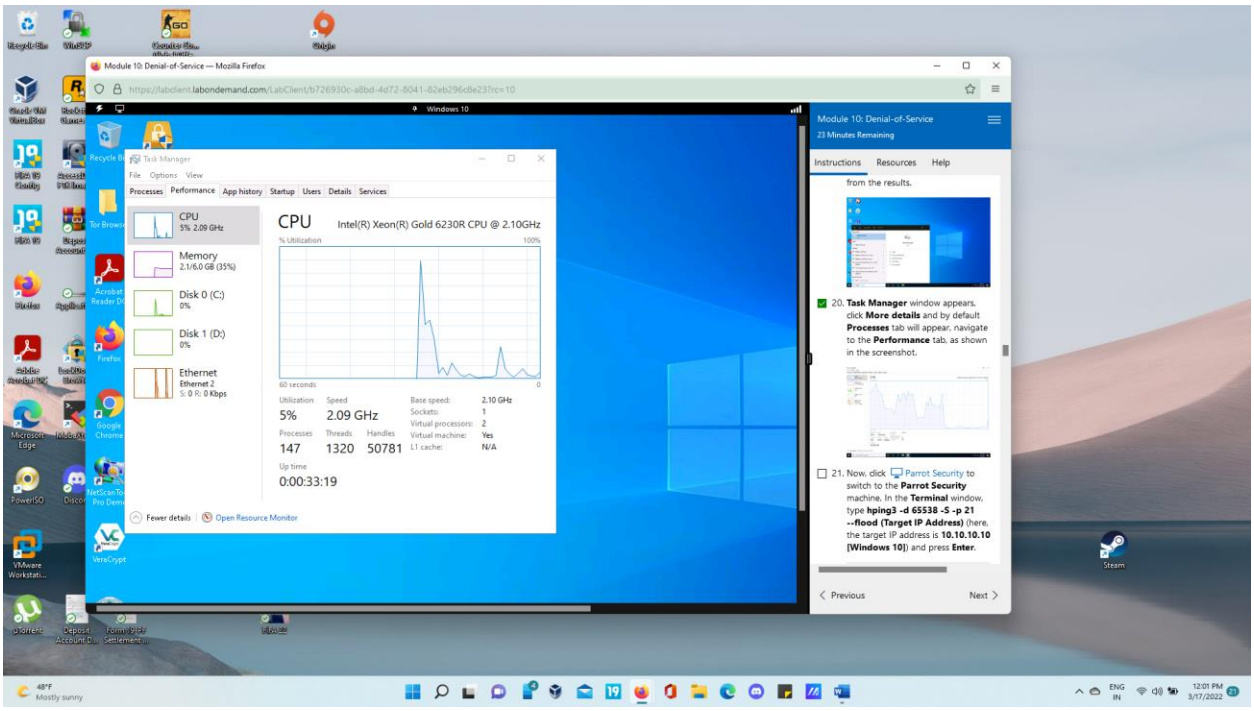
- After analyzing the I/O Graph, click Close to close the Wireshark . IO Graphs . Ethernet 2 window. Close the Wireshark main window. If an Unsaved packets… pop-up appears, click Stop and Quit without Saving.



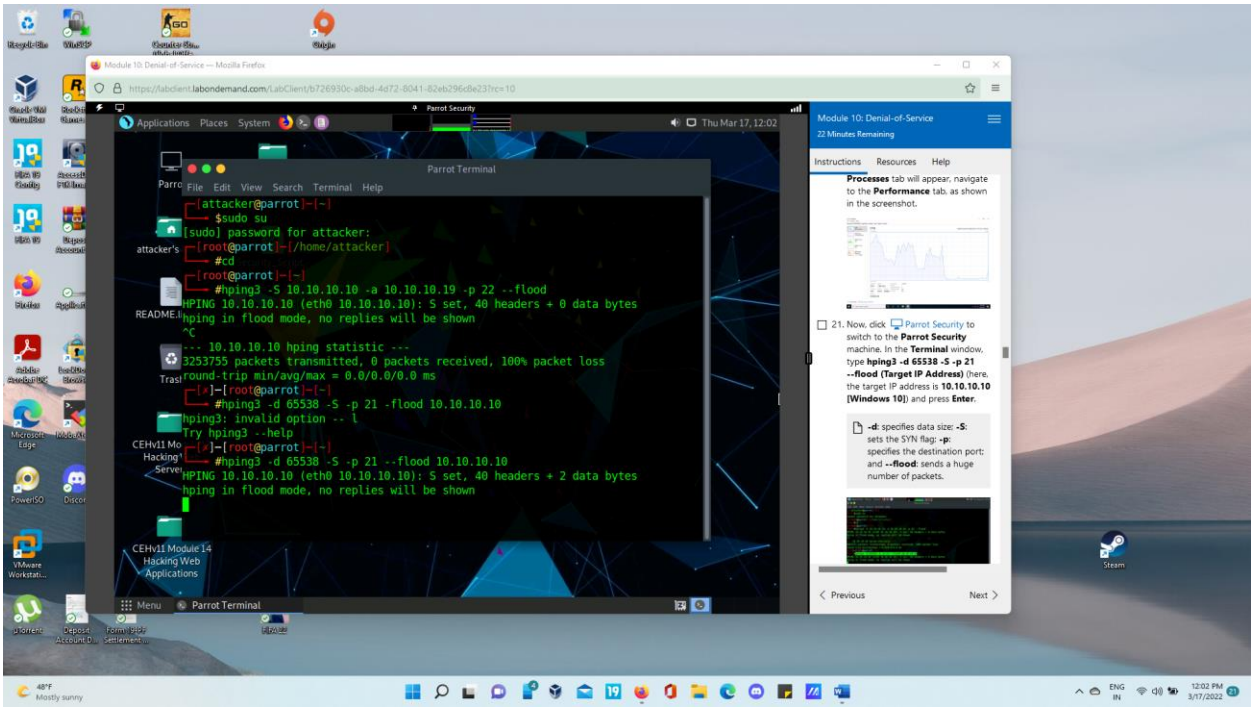
- Click the Type here to search field present at the bottom of Desktop, and type task. Click Task Manager from the results.



- Task Manager window appears, click More details and by default Processes tab will appear, navigate to the Performance tab, as shown in the screenshot.



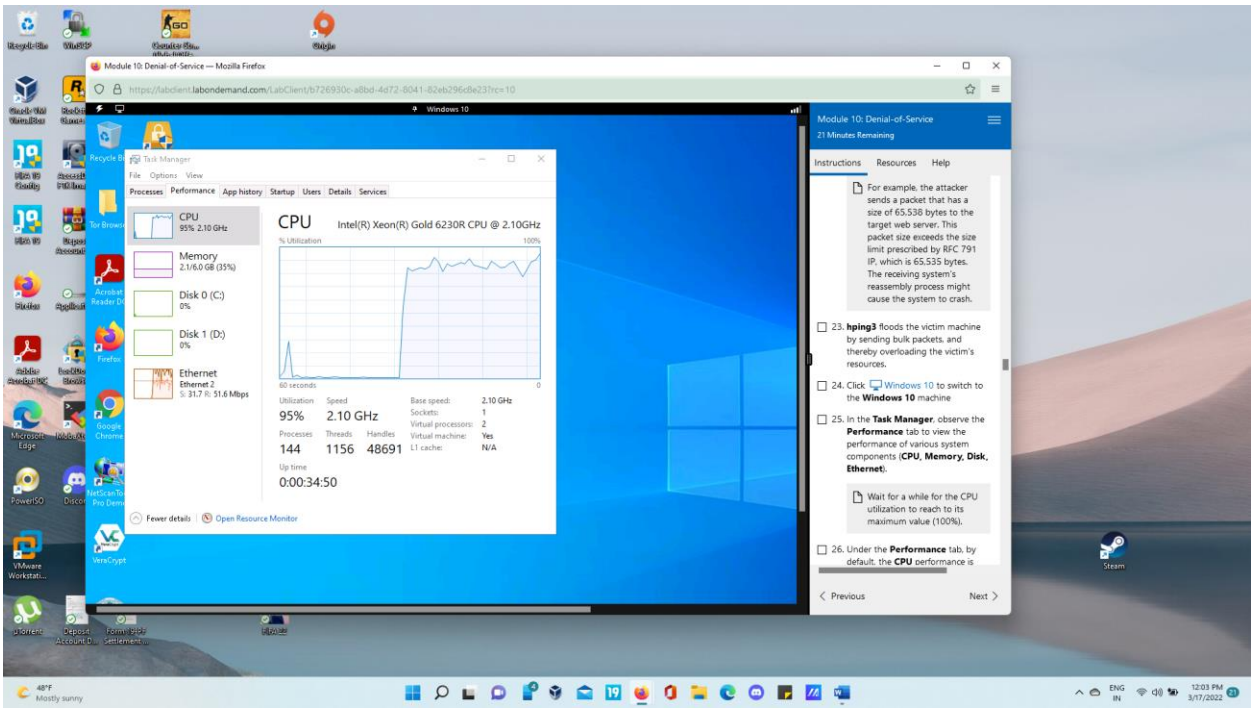
- Now, click Parrot Security to switch to the Parrot Security machine. In the Terminal window, type hping3 -d 65538 -S -p 21 --flood (Target IP Address) (here, the target IP address is 10.10.10.10 [Windows 10]) and press Enter.



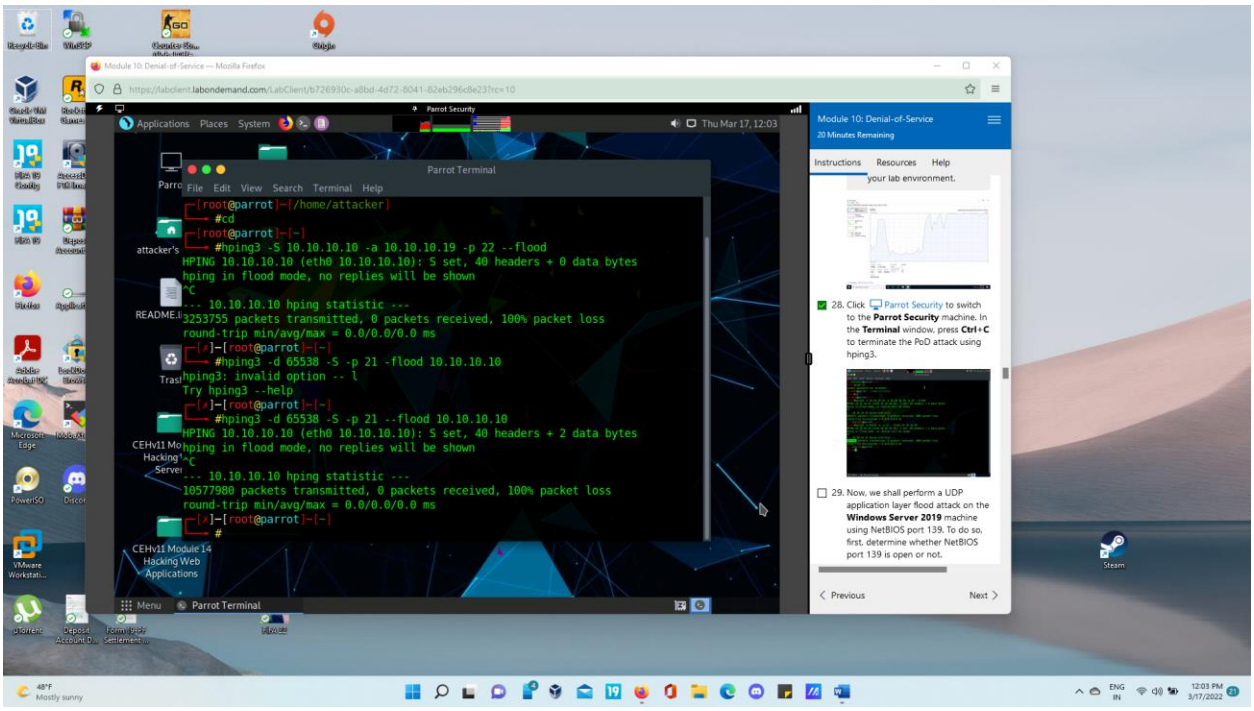
- hping3 floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.

- Click Windows 10 to switch to the Windows 10 machine.

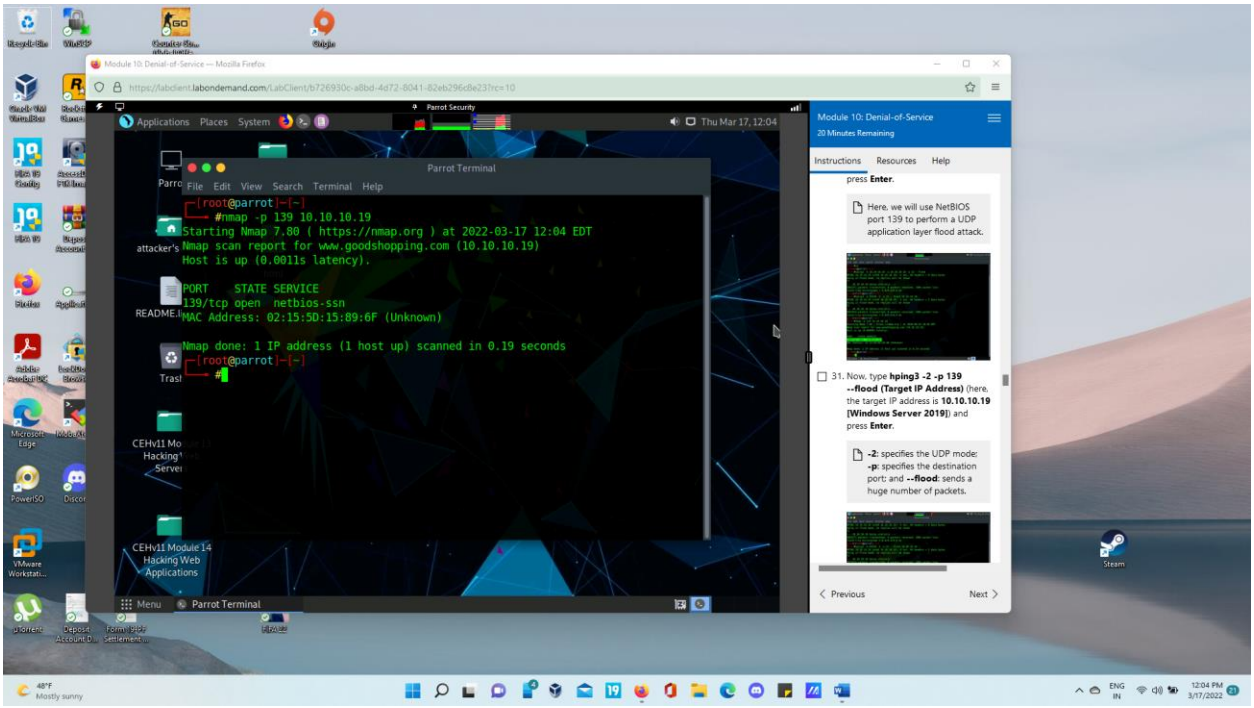
- In the Task Manager, observe the Performance tab to view the performance of various system components (CPU, Memory, Disk, Ethernet). Under the Performance tab, by default, the CPU performance is displayed in the right-hand pane. Observe that the CPU Utilization percentage is 100%, indicating a DoS attack on the system. Observe the degradation in the performance of the system, which might result in the system crashing.



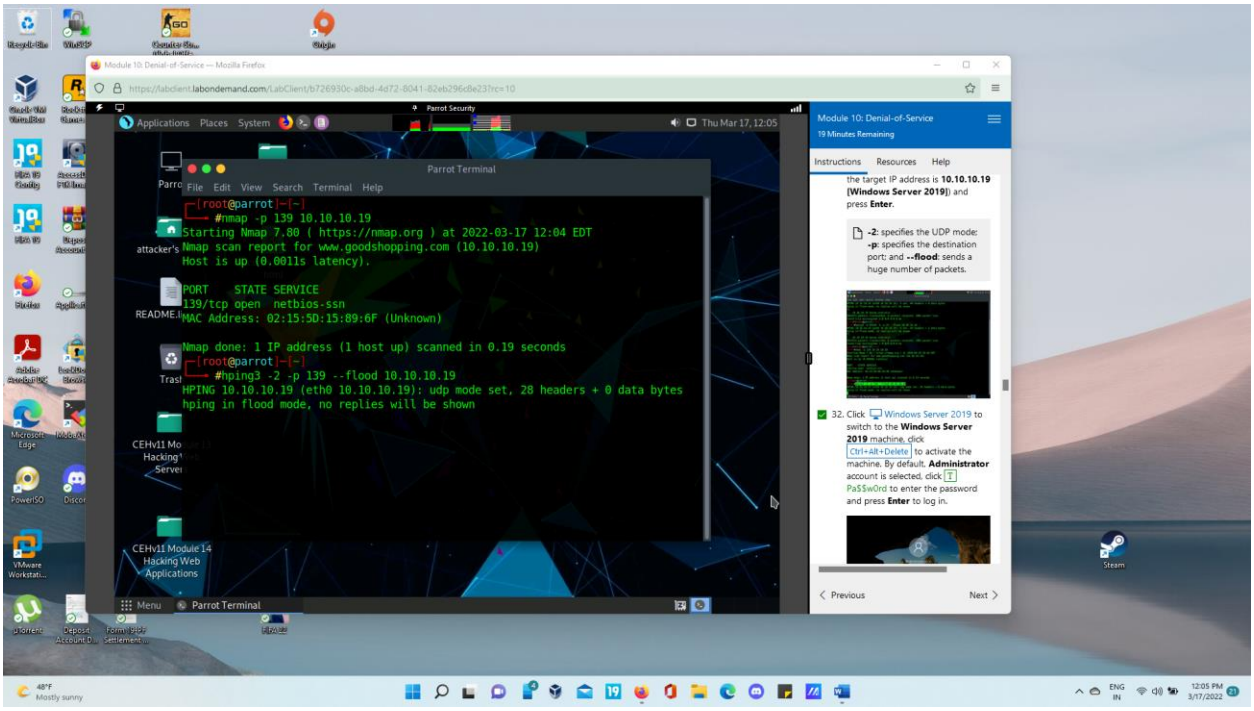
- Click Parrot Security to switch to the Parrot Security machine. In the Terminal window, press Ctrl+C to terminate the PoD attack using hping3.



- 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.
- In the terminal window, type nmap -p 139 (Target IP Address) (here, the target IP address is 10.10.10.19 [Windows Server 2019]) and press Enter.

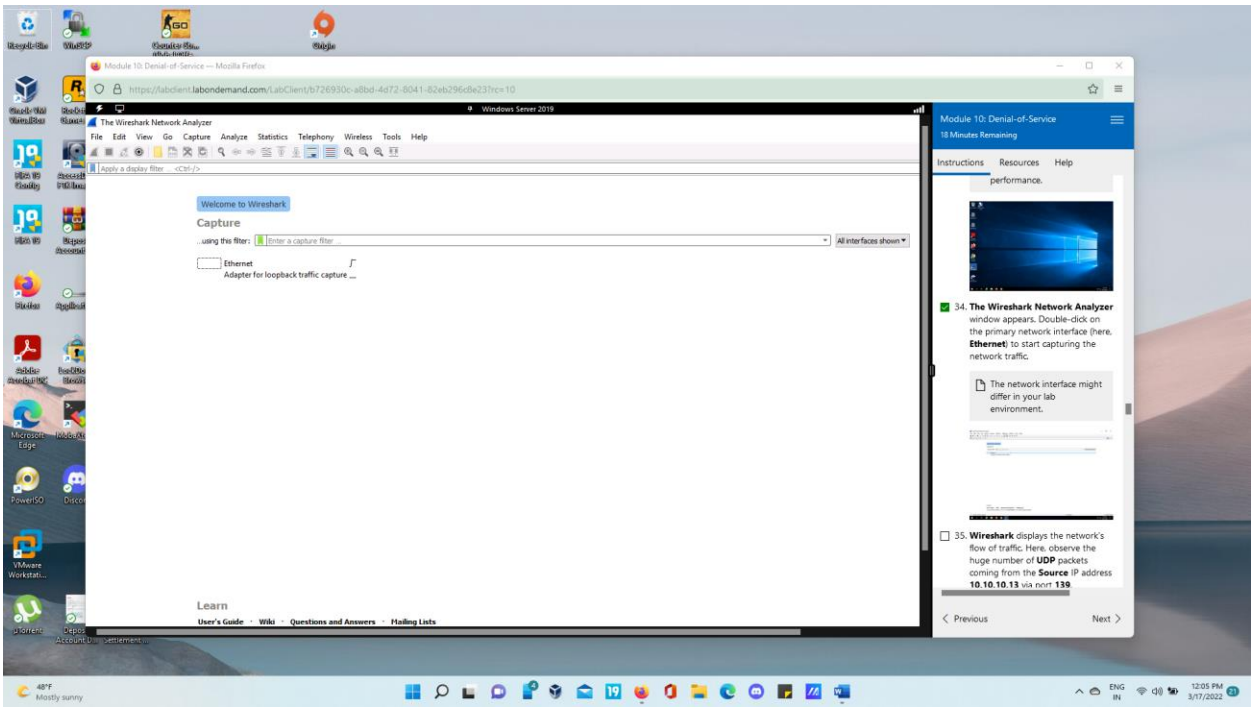


- Now, type hping3 -2 -p 139 --flood (Target IP Address) (here, the target IP address is 10.10.10.19 [Windows Server 2019]) and press Enter.

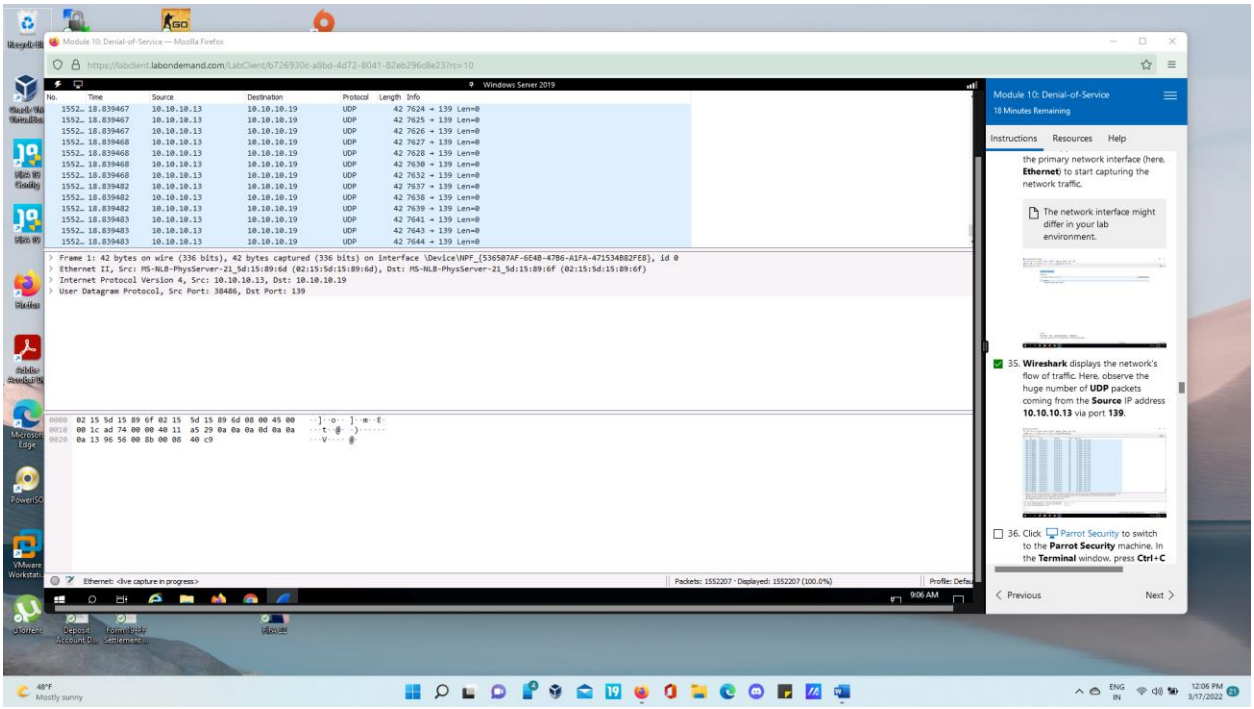


- Click Windows Server 2019 to switch to the Windows Server 2019 machine.

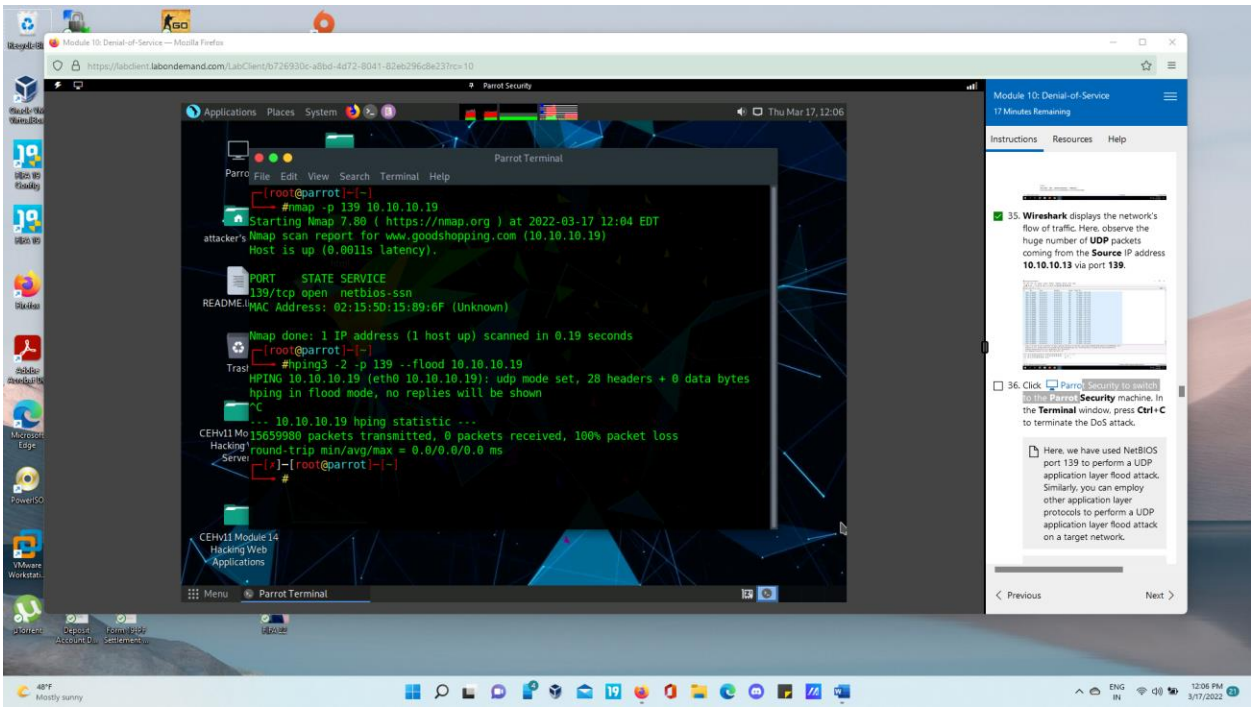
- Double-click Wireshark shortcut present on the Desktop.
- The Wireshark Network Analyzer window appears. Double-click on the primary network interface (here, Ethernet) to start capturing the network traffic.



- Wireshark displays the network's flow of traffic. Here, observe the huge number of UDP packets coming from the Source IP address 10.10.10.13 via port 139.



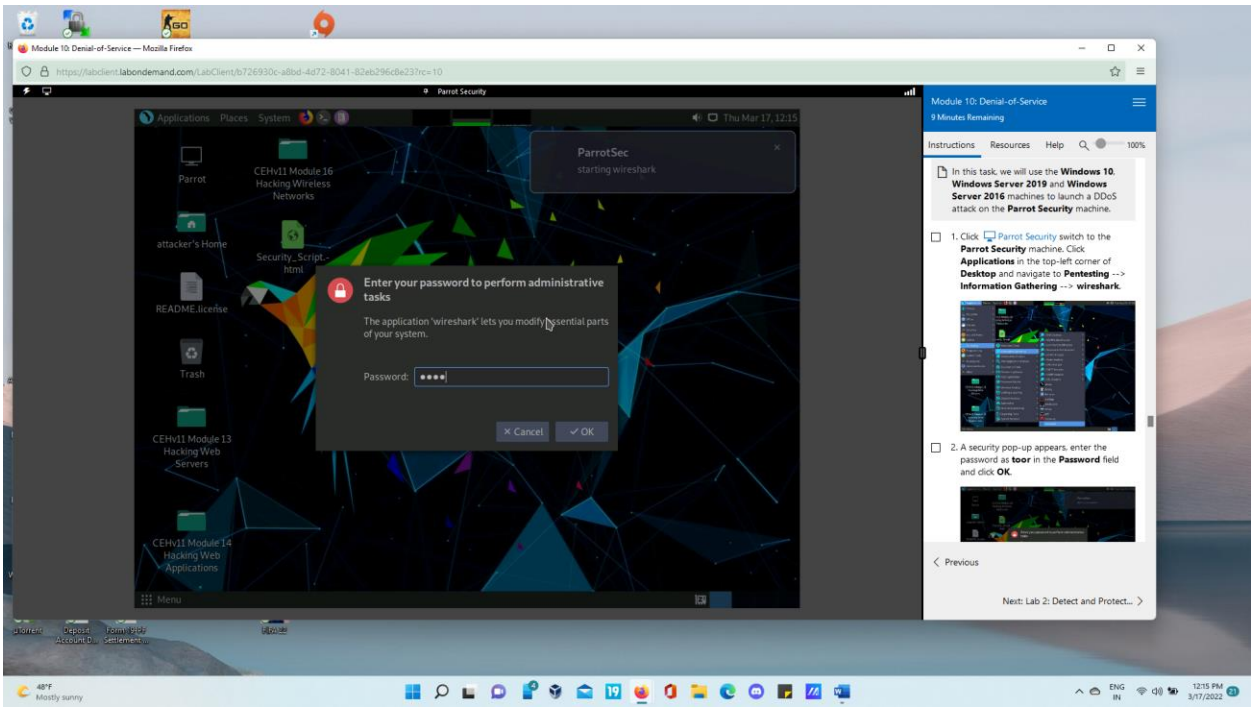
- Click Parrot Security to switch to the Parrot Security machine. In the Terminal window, press Ctrl+C to terminate the DoS attack.



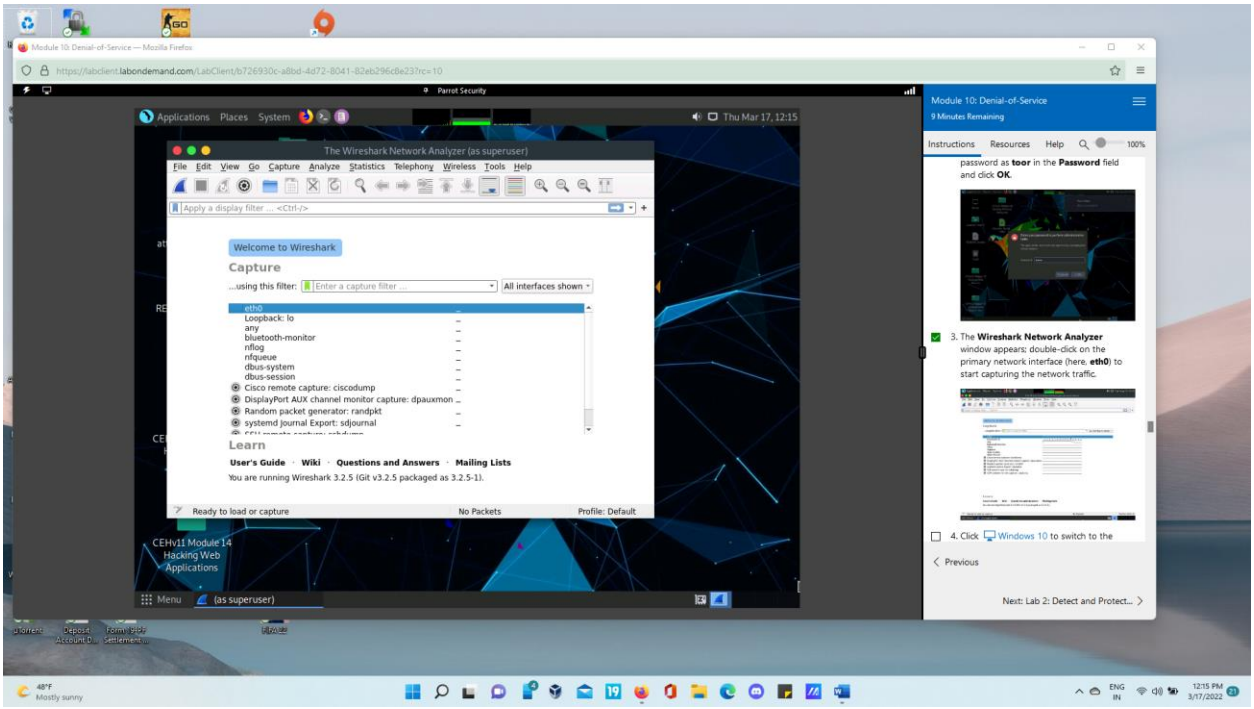
- This concludes the demonstration of how to perform DoS attacks (SYN flooding, PoD attacks, and UDP Application Layer Flood Attacks) on a target host using hping3.

Task 3: Perform a DDoS Attack using HOIC

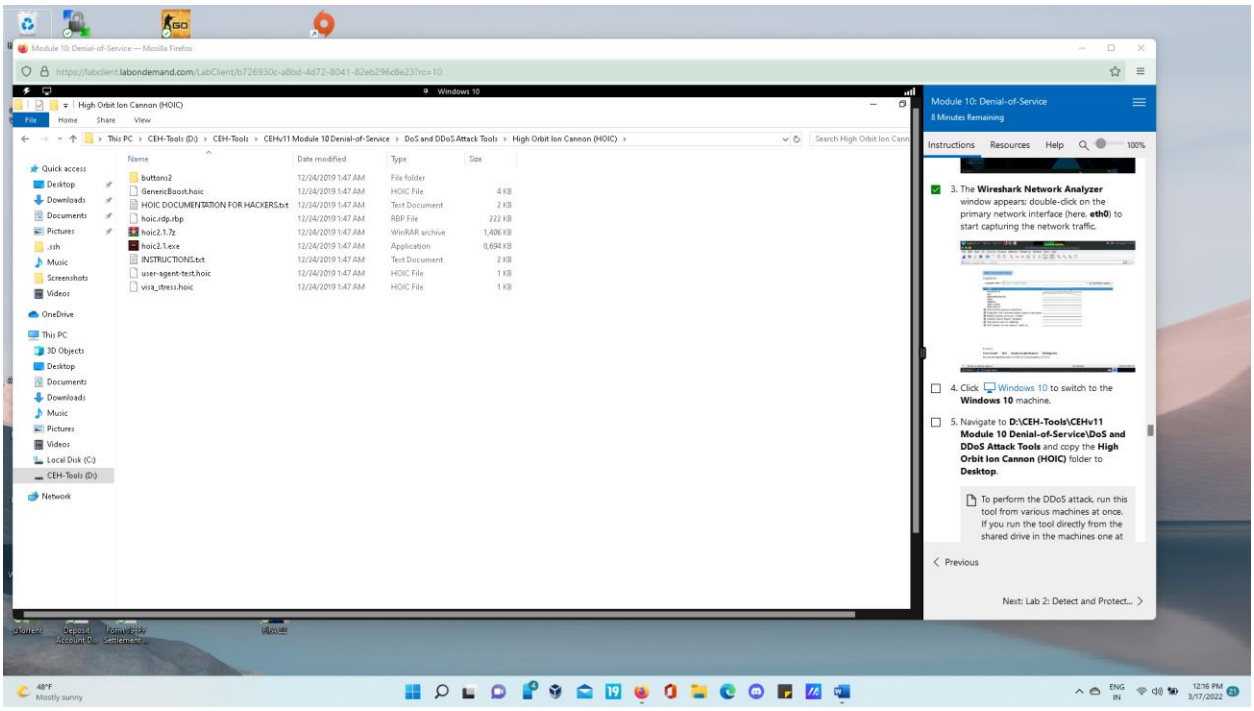
- Click Parrot Security switch to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



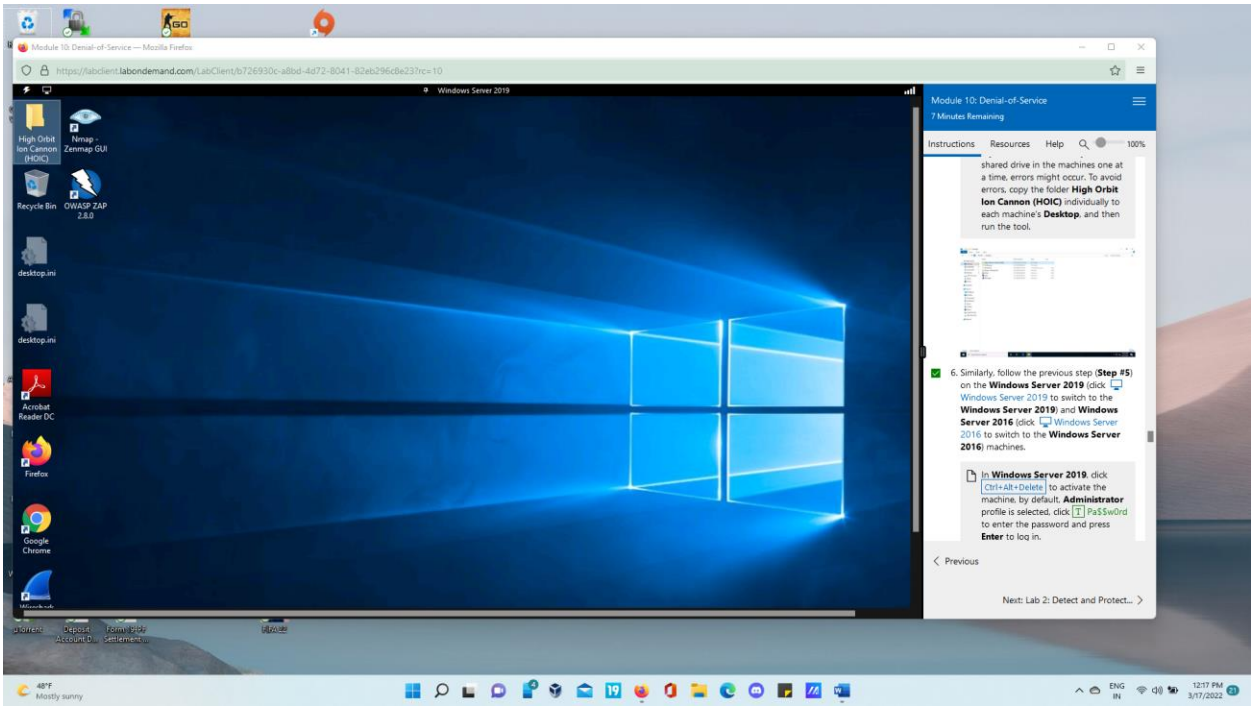
- The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.



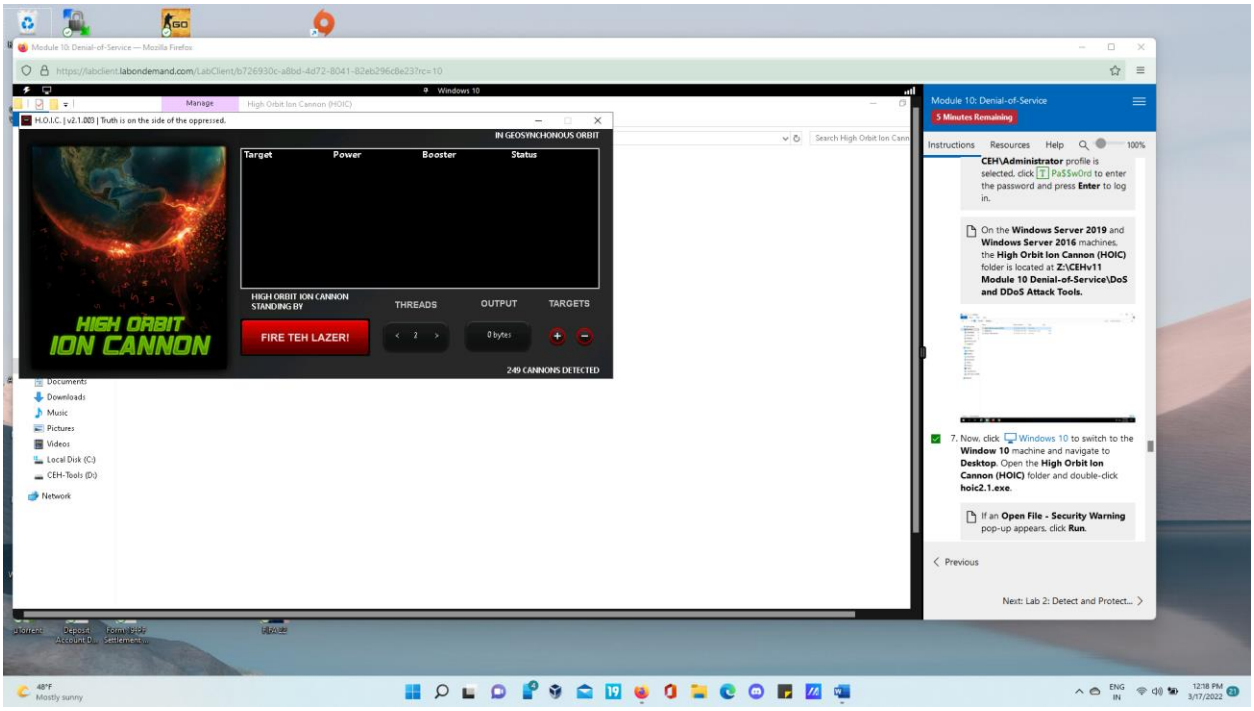
- Click Windows 10 to switch to the **Windows 10** machine. Navigate to **D:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.



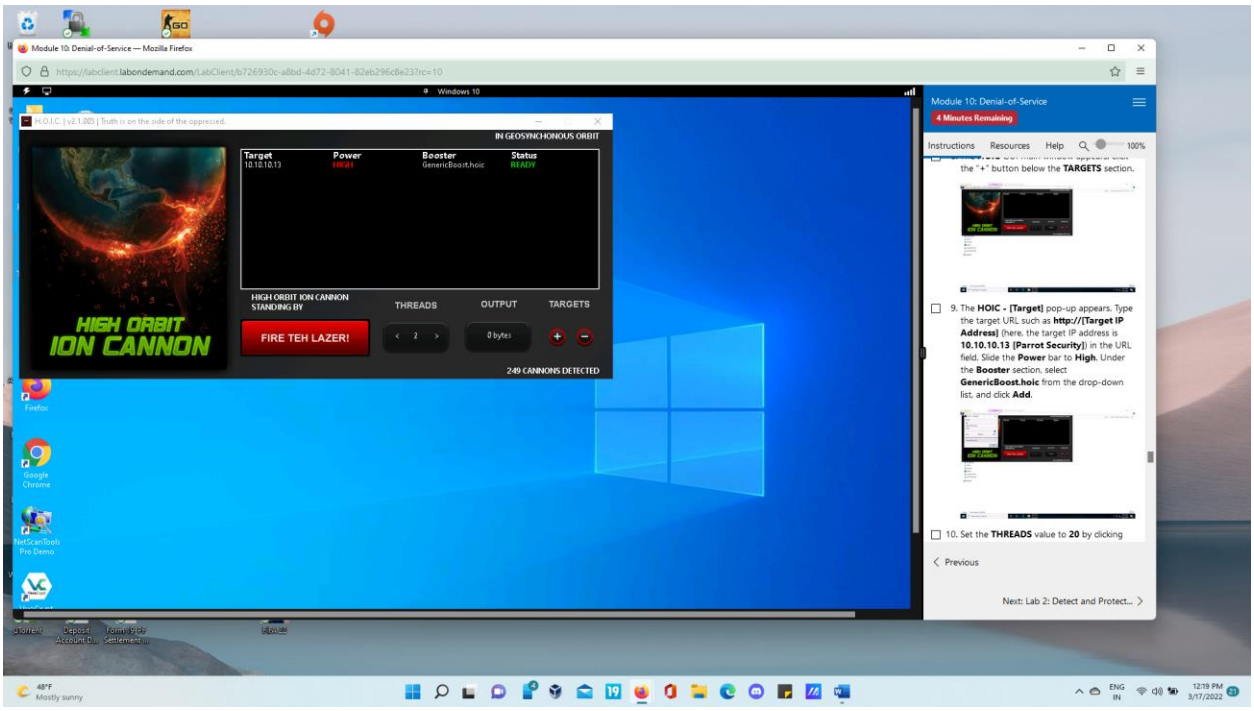
- Similarly, follow the previous step (**Step #5**) on the **Windows Server 2019** (click Windows Server 2019 to switch to the **Windows Server 2019**) and **Windows Server 2016** (click Windows Server 2016 to switch to the **Windows Server 2016**) machines.



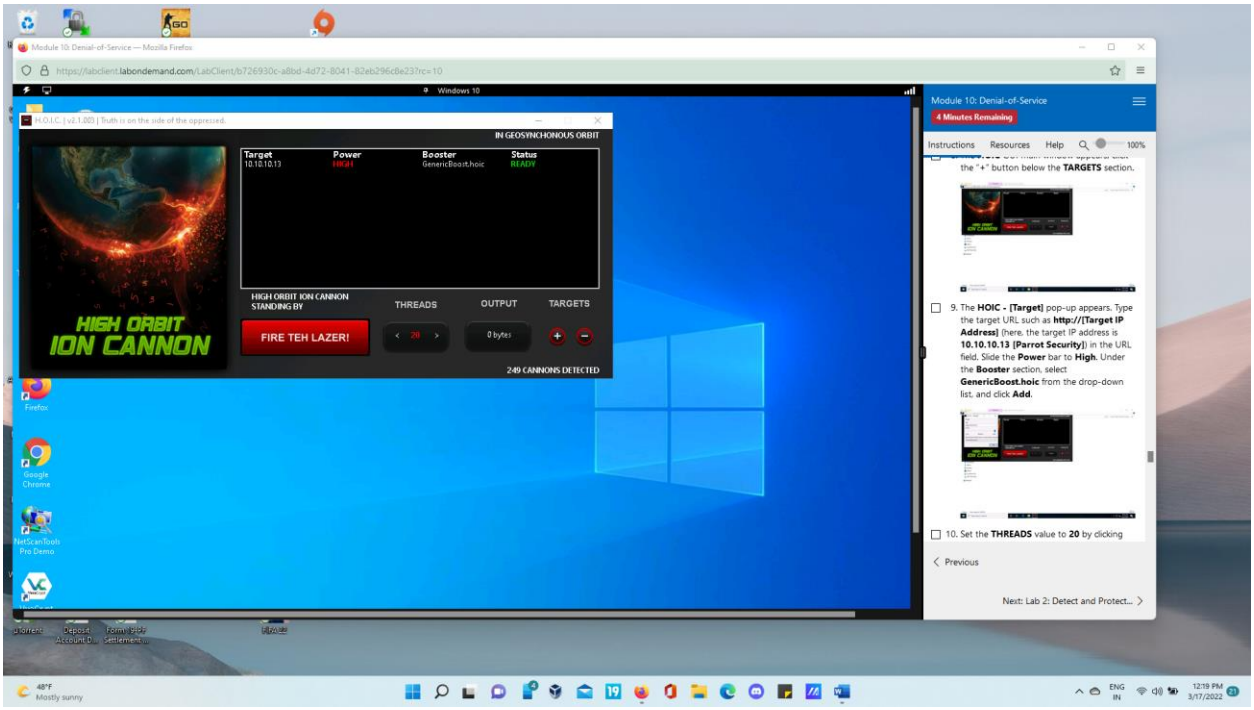
- Now, click Windows 10 to switch to the **Window 10** machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**.



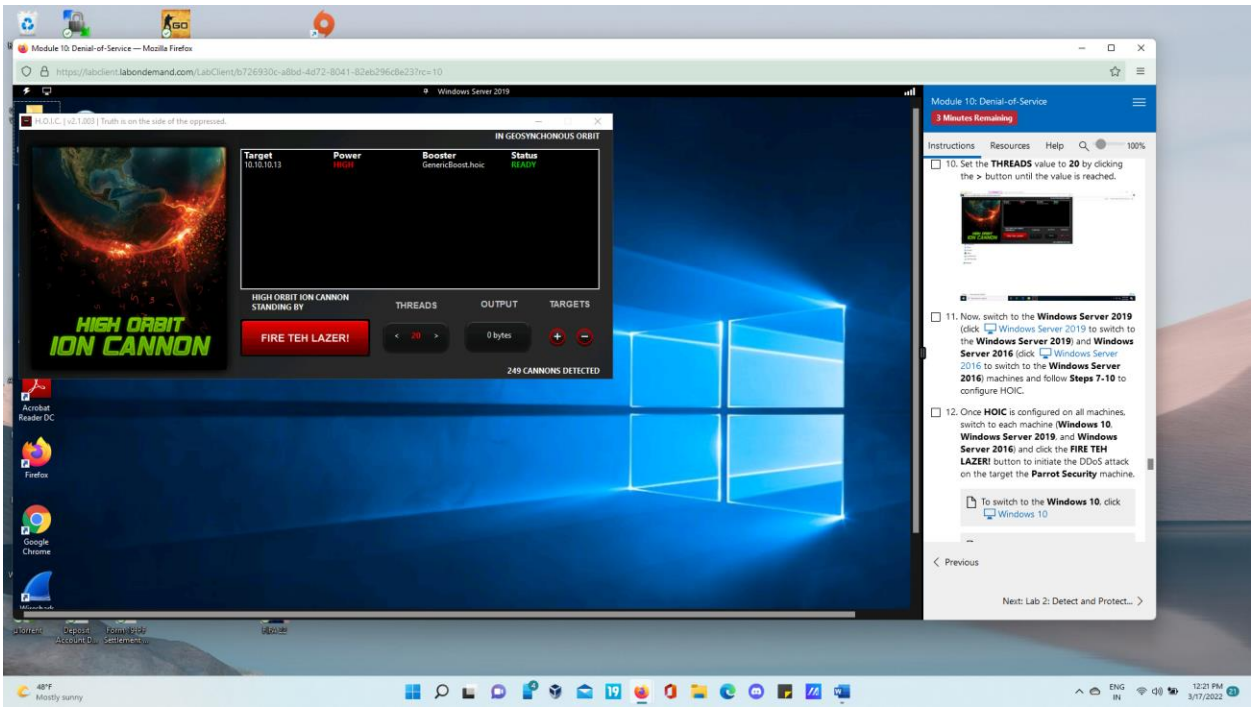
- The **HOIC** GUI main window appears; click the "**+**" button below the **TARGETS** section.
- The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.10.13 [Parrot Security]**) in the URL field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list, and click **Add**.

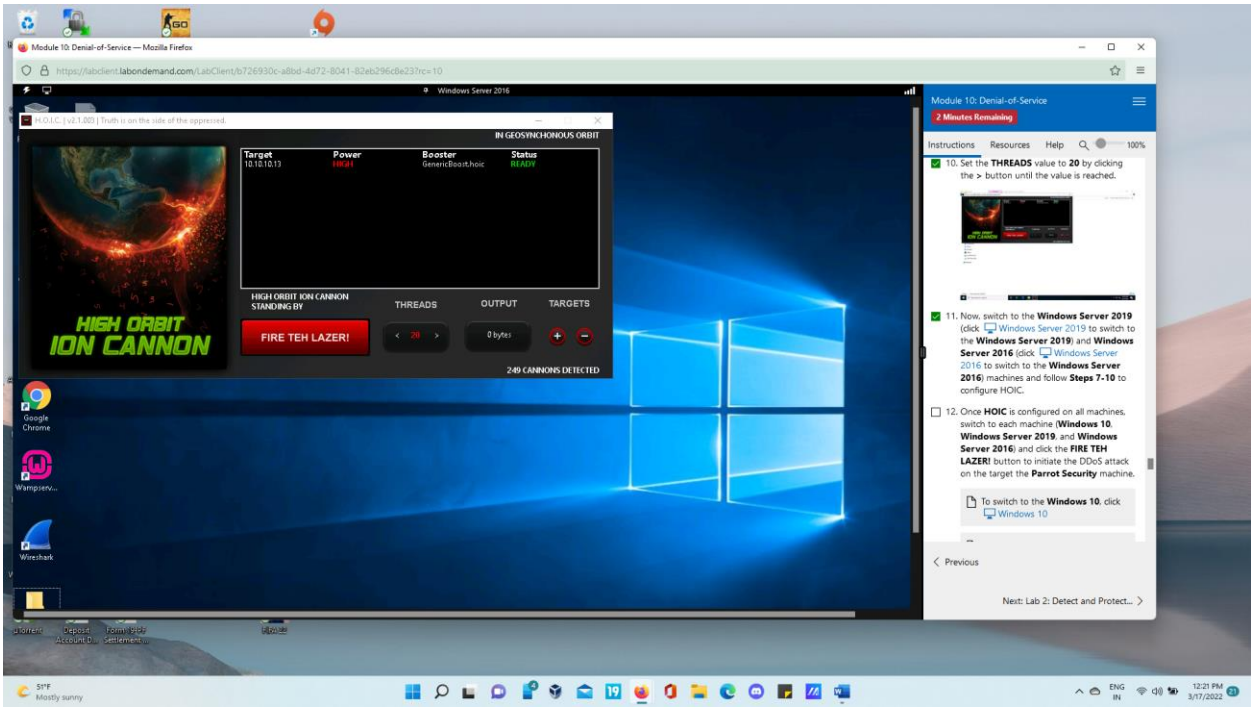


- Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

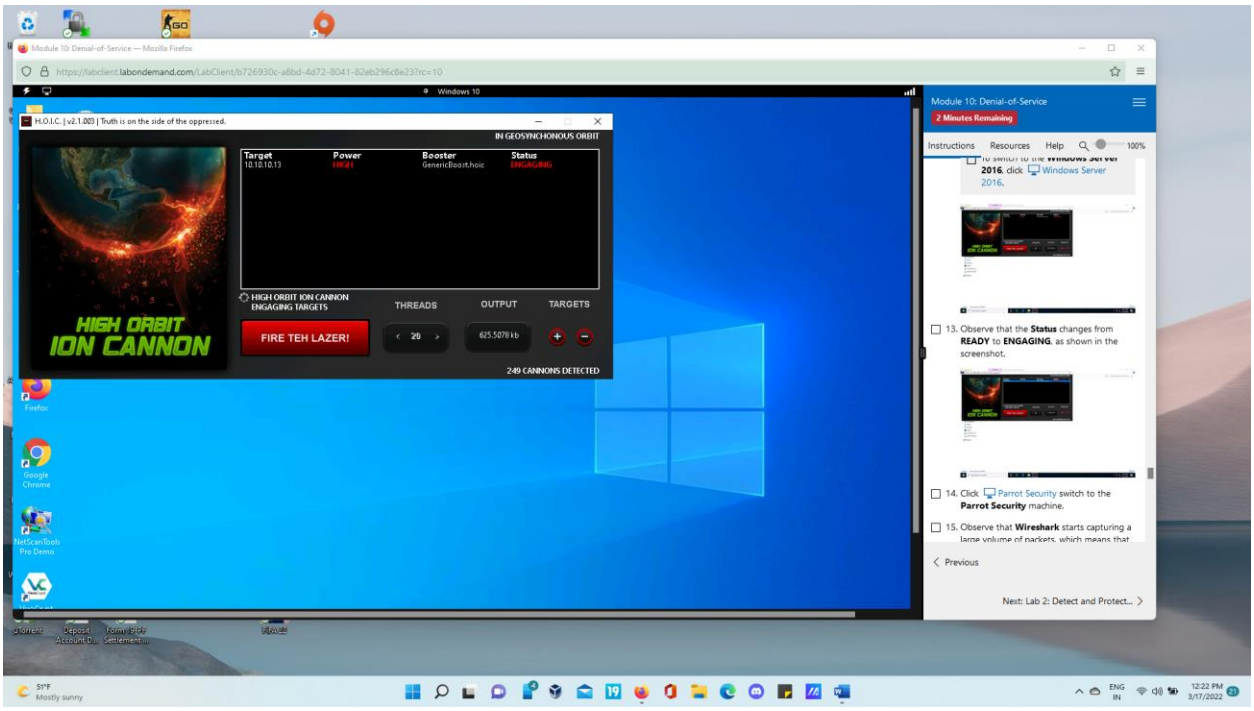


- Now, switch to the **Windows Server 2019** (click Windows Server 2019 to switch to the **Windows Server 2019**) and **Windows Server 2016** (click Windows Server 2016 to switch to the **Windows Server 2016**) machines and follow **Steps 7-10** to configure HOIC.

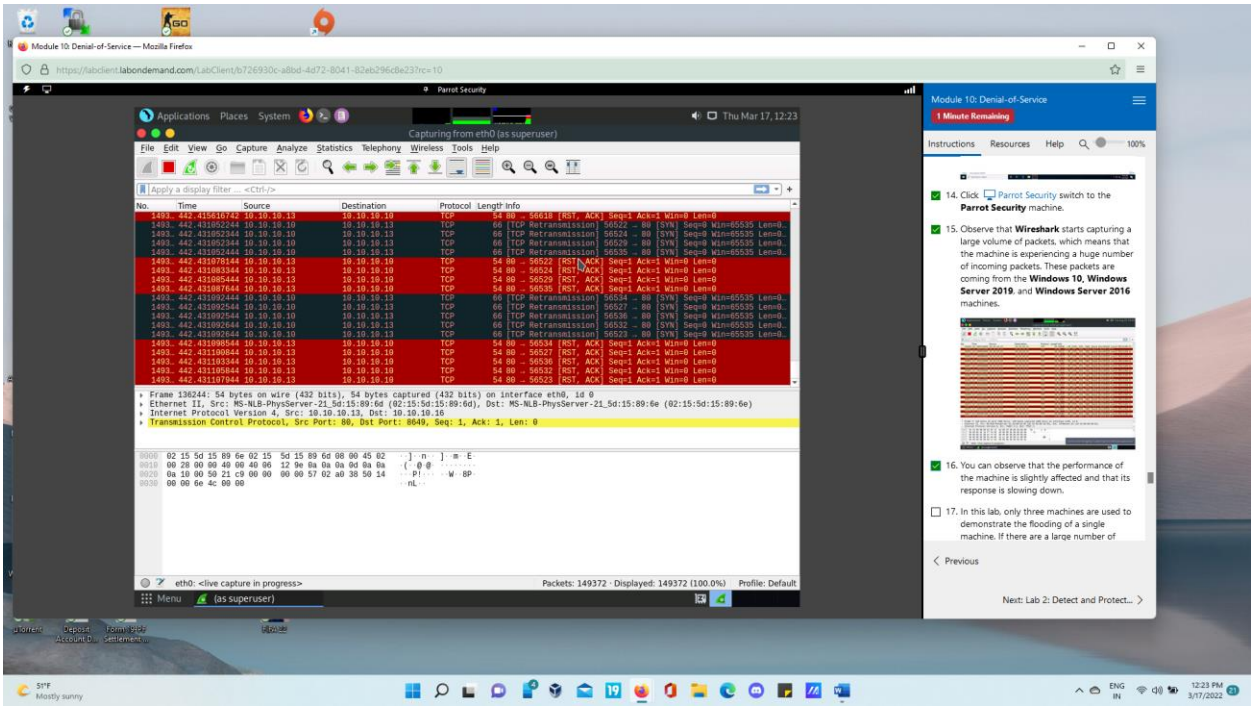




- Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.

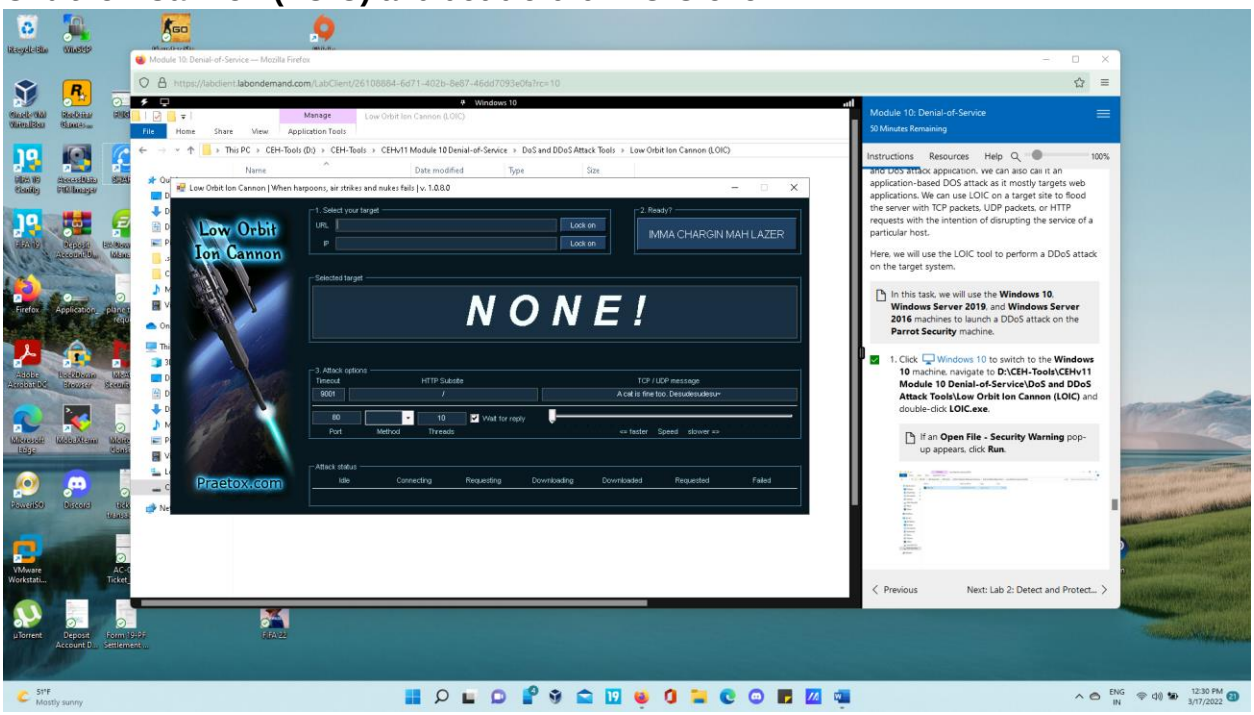


- Click Parrot Security switch to the **Parrot Security** machine.
- Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 10, Windows Server 2019**, and **Windows Server 2016** machines.

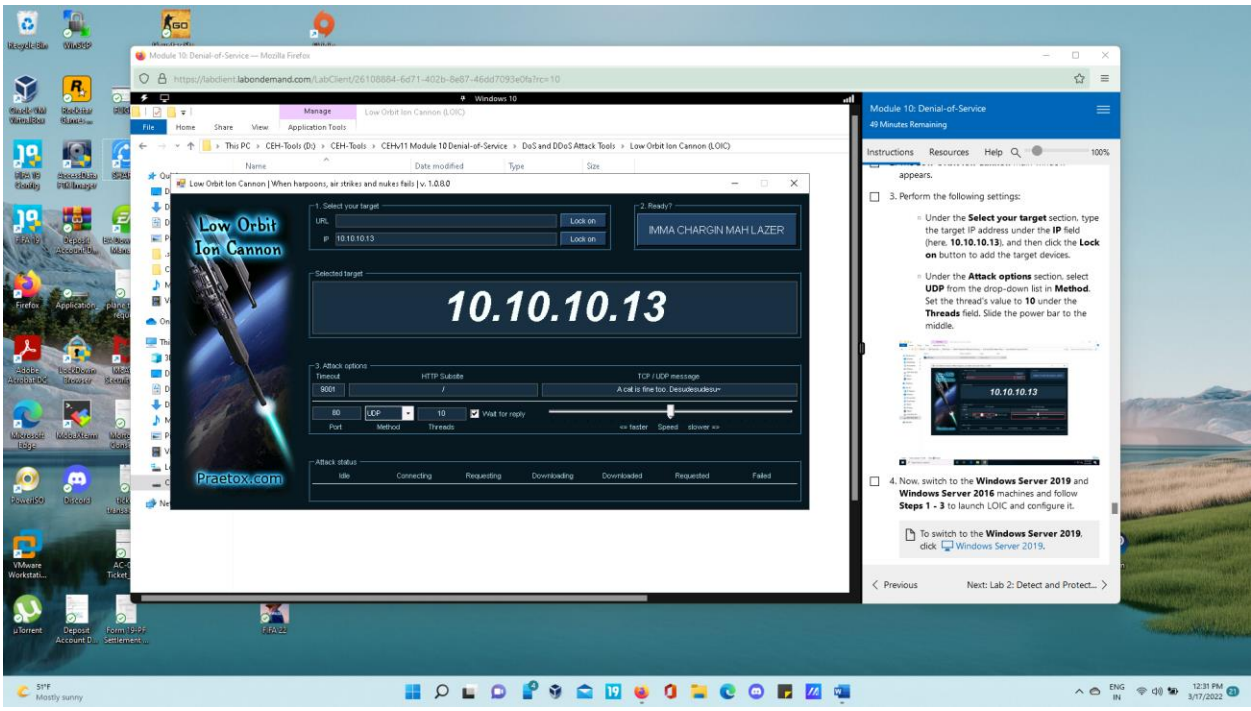


Task 4: Perform a DDoS Attack using LOIC

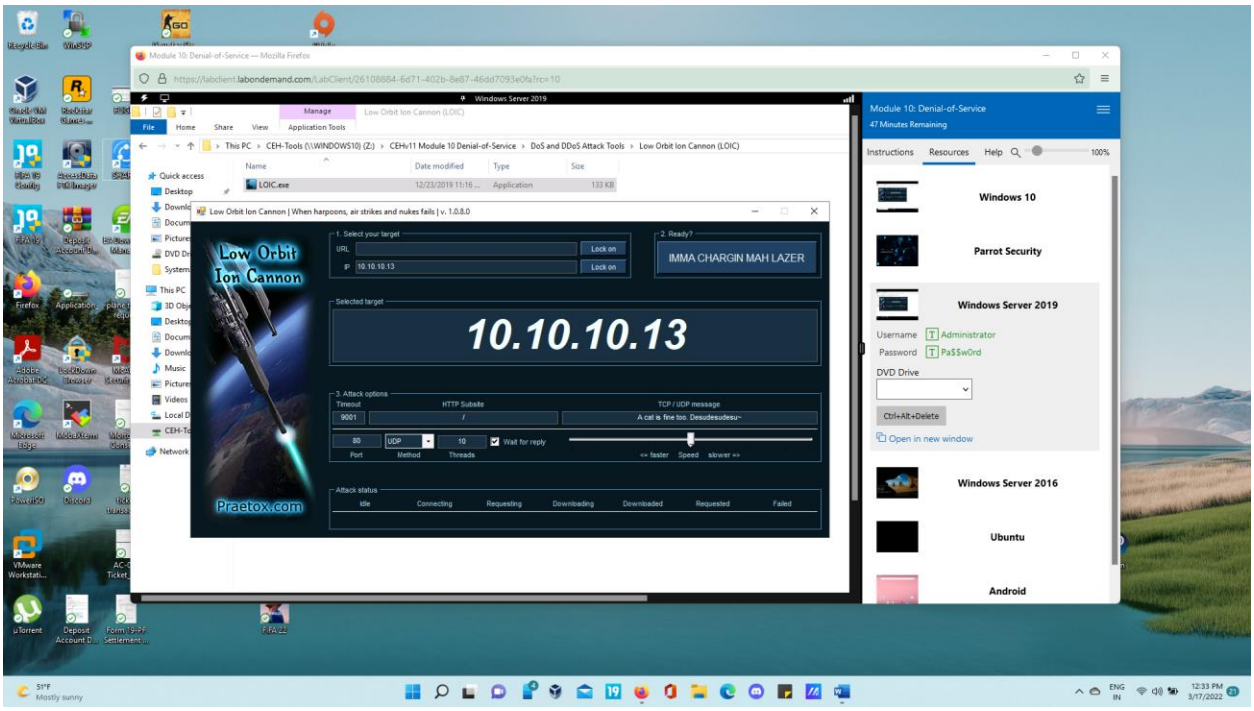
- Click Windows 10 to switch to the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

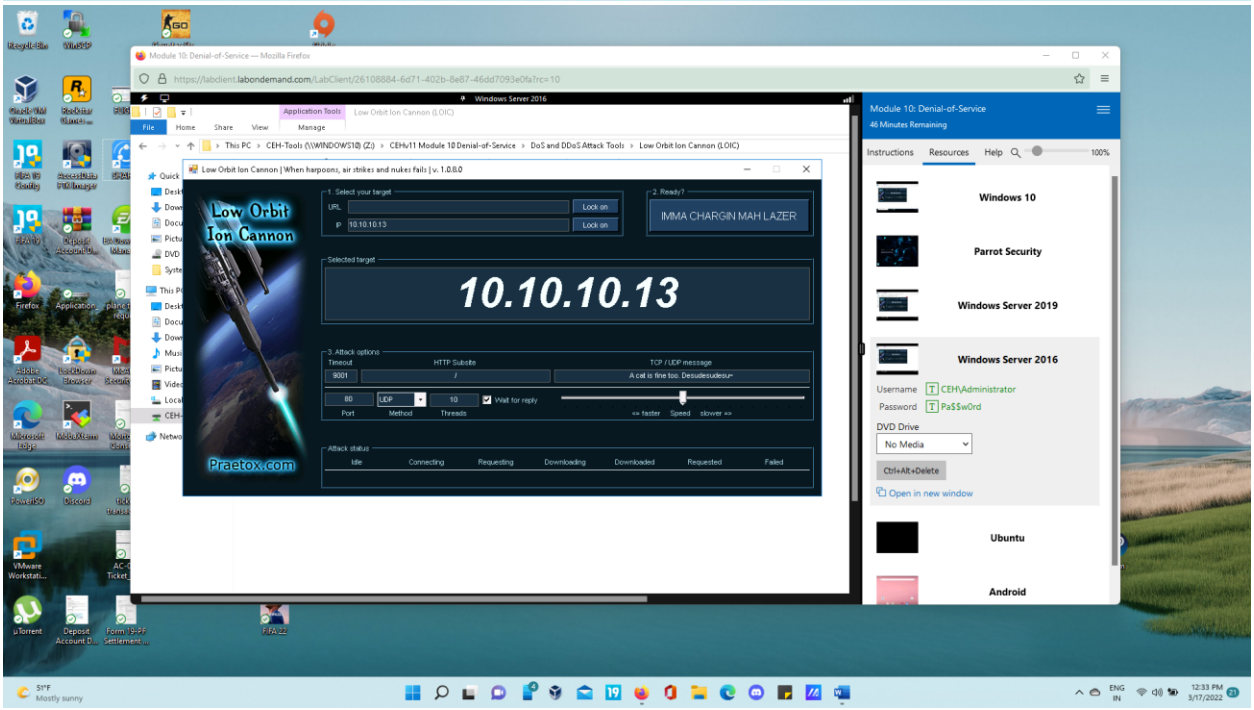


- Perform the following settings:
  - Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.10.13**), and then click the **Lock on** button to add the target devices.
  - Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **10** under the **Threads** field. Slide the power bar to the middle.

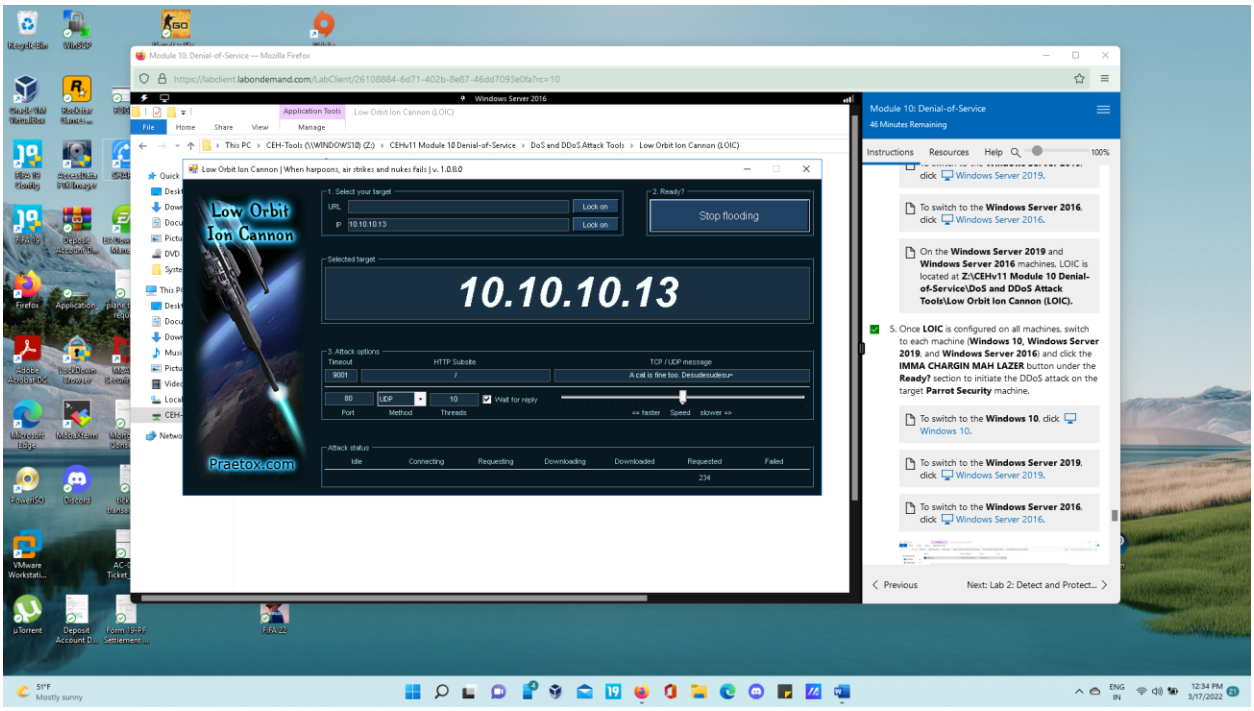


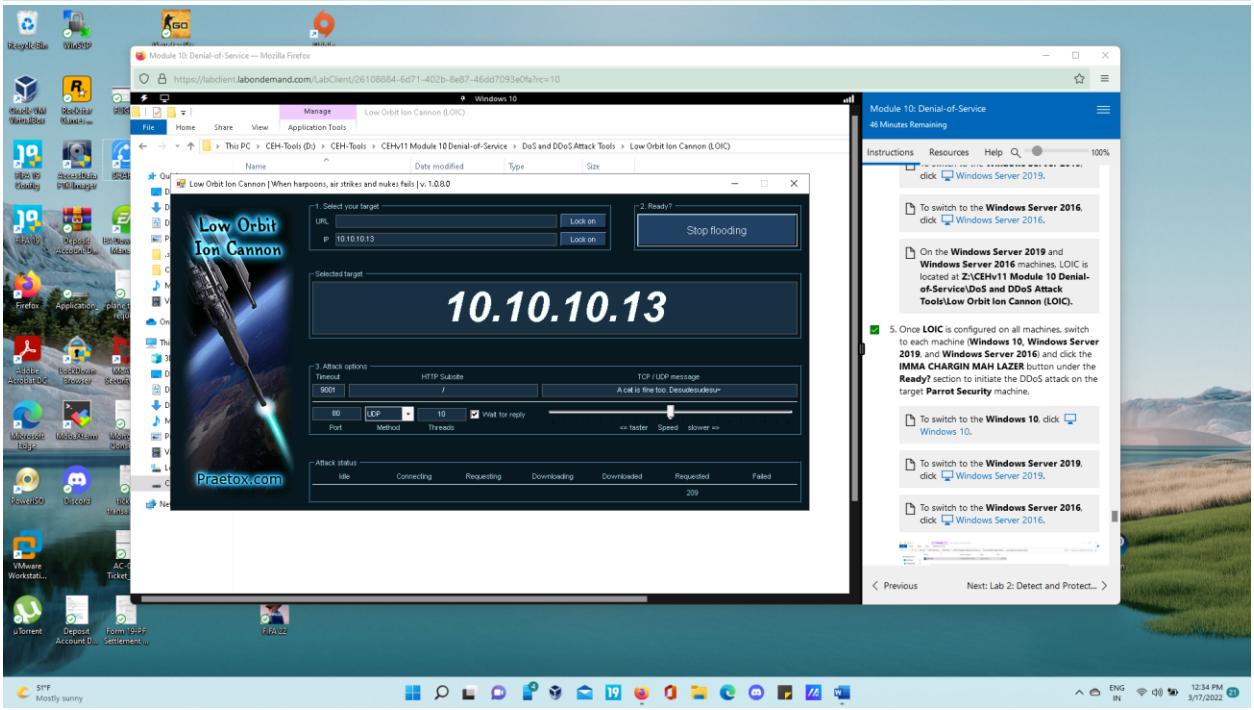
- Now, switch to the **Windows Server 2019** and **Windows Server 2016** machines and follow **Steps 1 - 3** to launch LOIC and configure it.

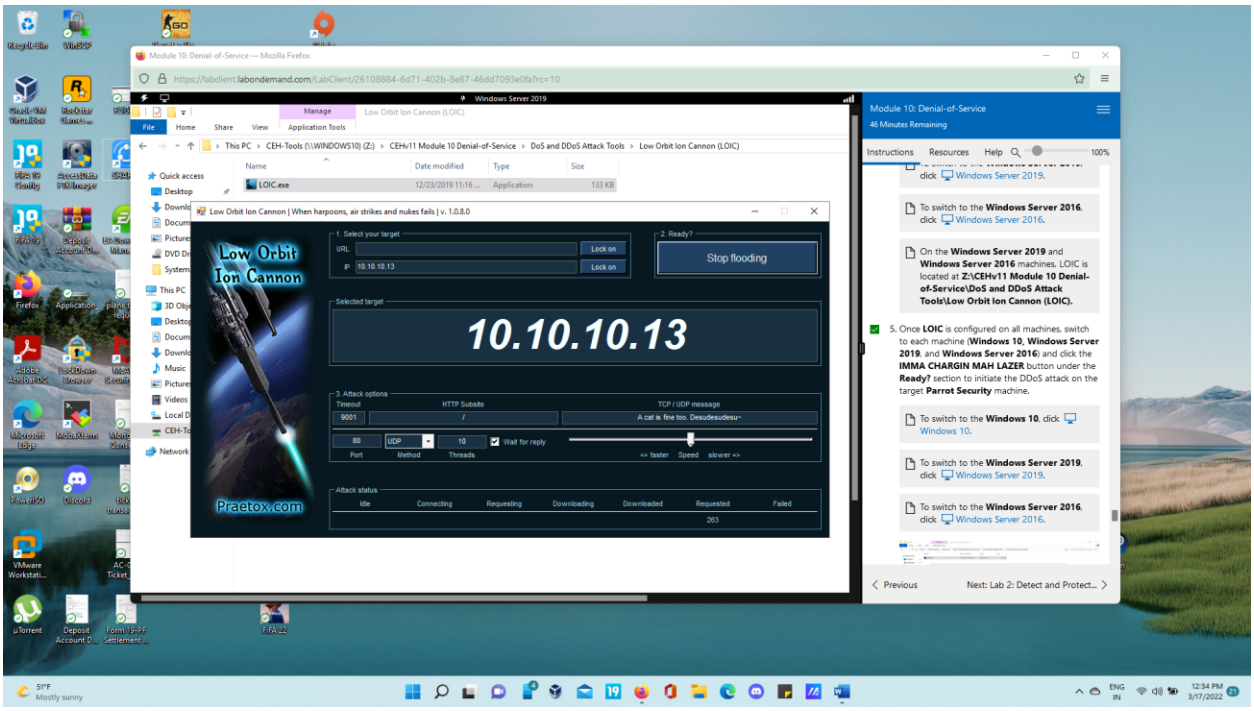




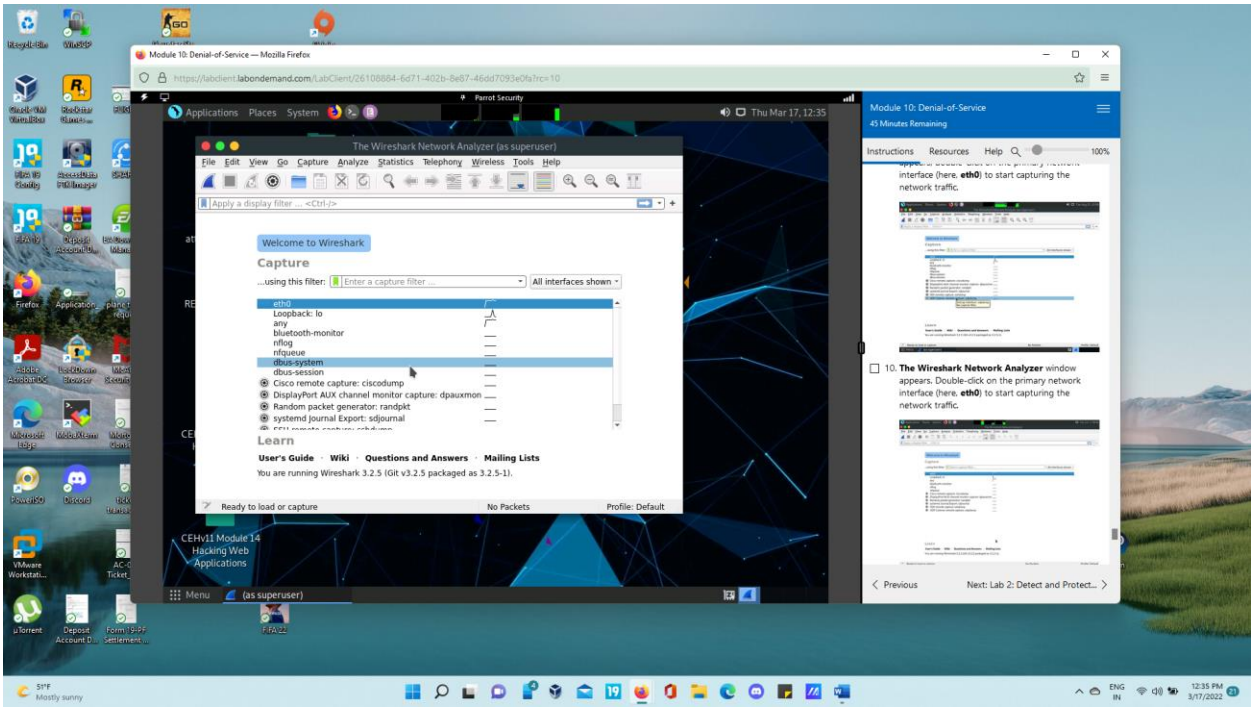
- Once **LOIC** is configured on all machines, switch to each machine (**Windows 10, Windows Server 2019**, and **Windows Server 2016**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Parrot Security** machine.


Module 10: Denial-of-Service — Mozilla Firefox
Windows Server 2016
Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0
Low Orbit Ion Cannon
Praetox.com
1. Select your target
URL
IP
10.10.10.13
Lock on
2. Ready?
Stop flooding
Selected target
10.10.10.13
3. Attack options
Timeout
HTTP Subsite
TCP / UDP message
9001
/
A cat is fine too. Desudesudesu~
80
Port
UDP
Method
10
Threads
Wait for reply
<= faster
Speed
slower =>
Attack status
Idle
Connecting
Requesting
Downloading
Downloaded
Requested
Failed
234
Module 10: Denial-of-Service
46 Minutes Remaining
Instructions
Resources
Help
100%
To switch to the Windows Server 2019, click Windows Server 2019.
To switch to the Windows Server 2016, click Windows Server 2016.
On the Windows Server 2019 and Windows Server 2016 machines, LOIC is located at Z:\CEHv11 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 10, Windows Server 2019, and Windows Server 2016) 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 10, click Windows 10.
To switch to the Windows Server 2019, click Windows Server 2019.
To switch to the Windows Server 2016, click Windows Server 2016.
Previous
Next: Lab 2: Detect and Protect...


Module 10: Denial-of-Service — Mozilla Firefox
Windows 10
Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0
Low Orbit Ion Cannon
Praetox.com
1. Select your target
URL
IP
10.10.10.13
Lock on
2. Ready?
Stop flooding
Selected target
10.10.10.13
3. Attack options
Timeout
HTTP Subsite
TCP / UDP message
9001
/
A cat is fine too. Desudesudesu~
80
Port
UDP
Method
10
Threads
Wait for reply
<= faster
Speed
slower =>
Attack status
Idle
Connecting
Requesting
Downloading
Downloaded
Requested
Failed
209
Module 10: Denial-of-Service
46 Minutes Remaining
Instructions
Resources
Help
100%
To switch to the Windows Server 2016, click Windows Server 2016.
On the Windows Server 2019 and Windows Server 2016 machines, LOIC is located at Z:\CEHv11 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 10, Windows Server 2019, and Windows Server 2016) 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 10, click Windows 10.
To switch to the Windows Server 2019, click Windows Server 2019.
To switch to the Windows Server 2016, click Windows Server 2016.
Previous
Next: Lab 2: Detect and Protect...

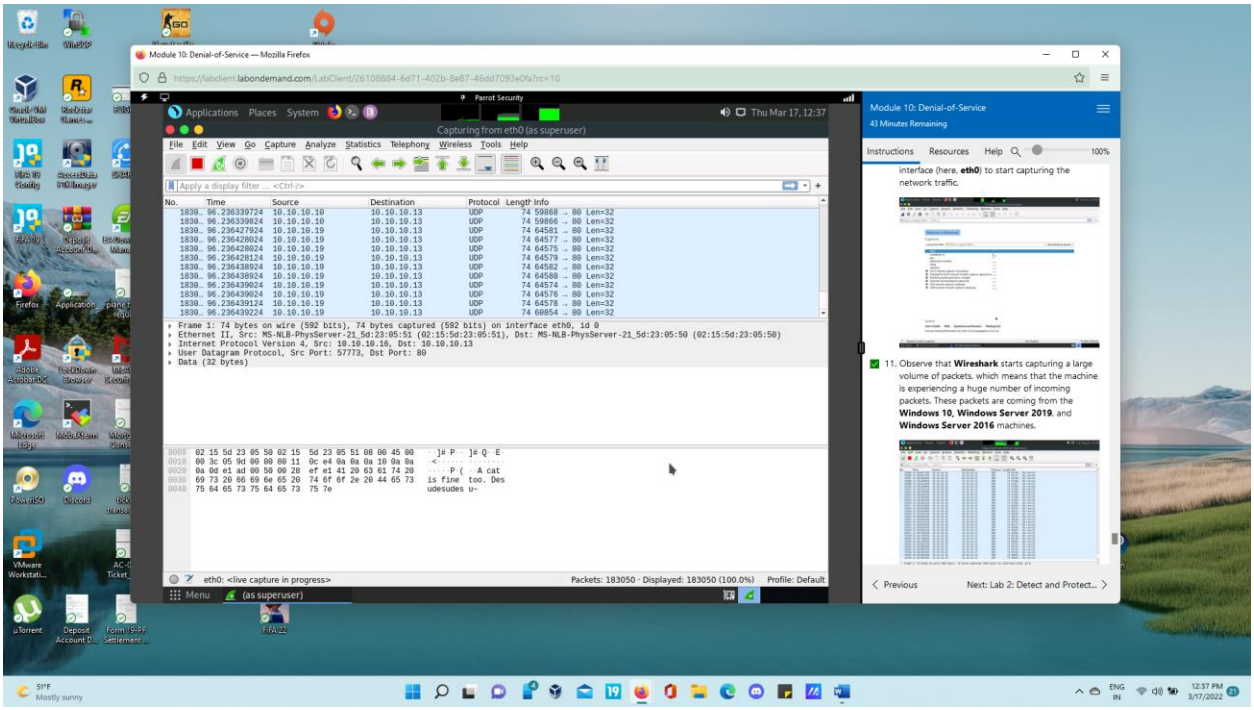


- Click Parrot Security to switch to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.
- A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

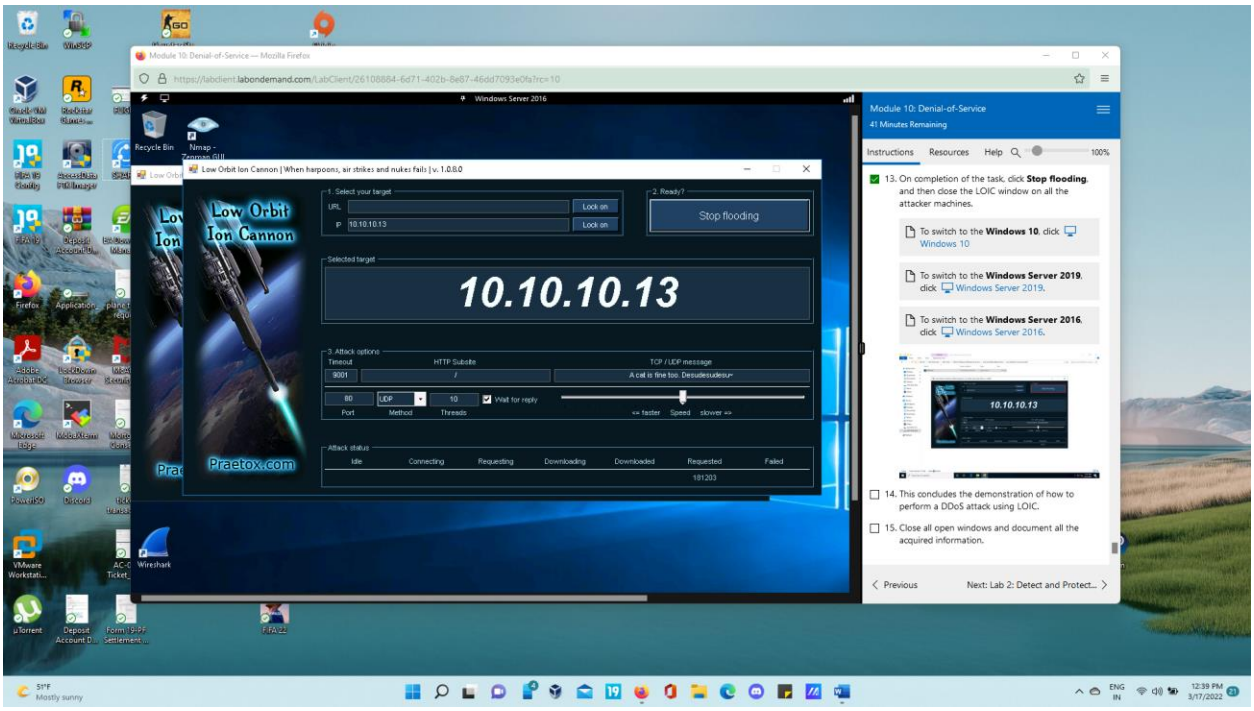


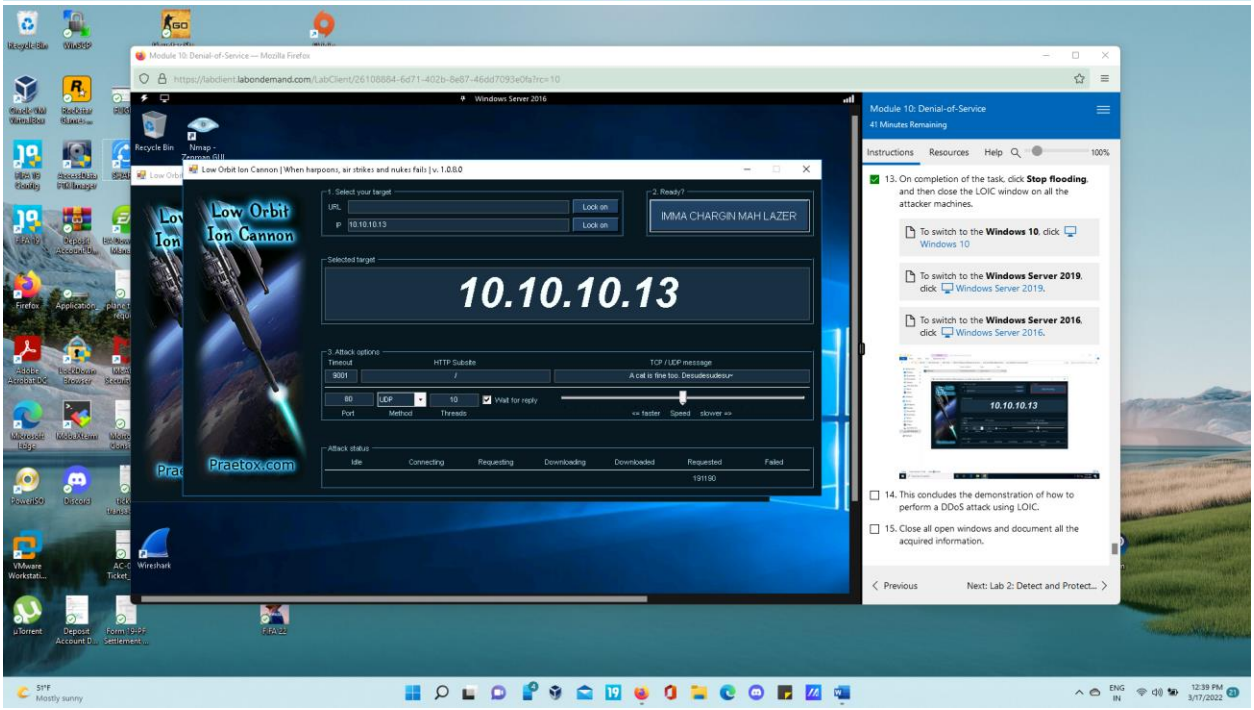
- The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.

- 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 10, Windows Server 2019**, and **Windows Server 2016** machines.



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





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