# Denial-of-Service

## Module 10

# Denial of Service

*Denial-of-Service is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.*

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## Lab 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.

## Lab Objectives

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

**Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service**

## Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

## Lab Duration

Time: 45 Minutes

## 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:

| Lab No. | Lab Exercise Name | Core* | Self-study** | iLabs *** |
|---|---|---|---|---|
| 1 | Perform DoS and DDoS Attacks using Various Techniques | √ | √ | √ |
| | 1.1 Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit | | √ | √ |

| | | | | |
|---|---|---|---|---|
| | 1.2 Perform a DoS Attack on a Target Host using hping3 | √ | | √ |
| | 1.3 Perform a DDoS Attack using HOIC | √ | | √ |
| | 1.4 Perform a DDoS Attack using LOIC | | √ | √ |
| **2** | Detect and Protect Against DoS and DDoS Attacks | √ | | √ |
| | 2.1 Detect and Protect against DDoS Attack using Anti DDoS Guardian | √ | | √ |

**Remark**

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

## Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion of your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

# Perform DoS and DDoS Attacks using Various Techniques

*As an expert hacker and pen tester, you must implement various techniques to launch DoS or DDoS attacks on target computers or networks.*

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

## 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 DDoS attack using HOIC
- Perform a DDoS attack using LOIC

## Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- HOIC located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\High Orbit Ion Cannon (HOIC)**
- LOIC located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)**
- You can also download the latest version of the above-mentioned tools from their official website. If you decide to download the latest version, the screenshots shown in this lab might differ from what you see on your screen.

## Lab Duration

Time: 35 Minutes

## 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

# Lab Tasks

## TASK 1 — Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit

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

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.

**Note**: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine to perform SYN flooding on the **Windows 10** (**10.10.10.10**) virtual machine through **port 21**.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. 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.

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.


Figure 1.1.1: Parrot Security login page

**Note**:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

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

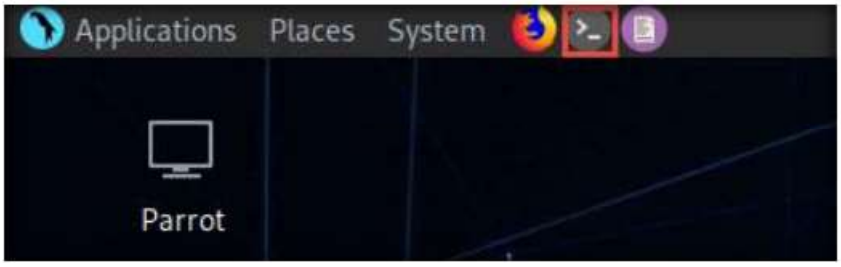


Figure 1.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. First, determine whether port 21 is open or not. This involves using Nmap to determine the state of the port.

**TASK 1.1**

**Check for Open Port**

8. 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**.

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

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

**Note**: If the port in your lab environment turns out to be closed, look for an open port using Nmap.

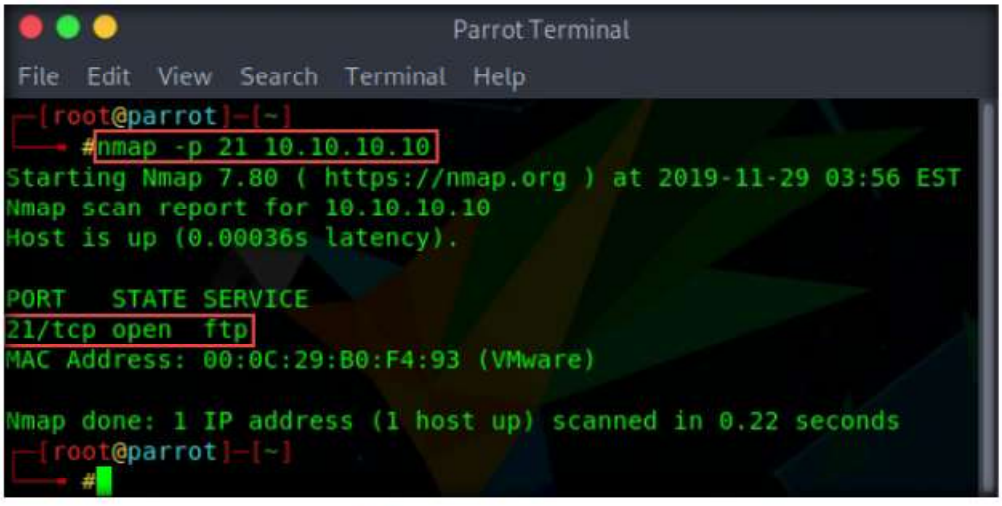


Figure 1.1.3: Performing the Nmap port scan

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

**TASK 1.2**

**Perform DoS Attack**

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.

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

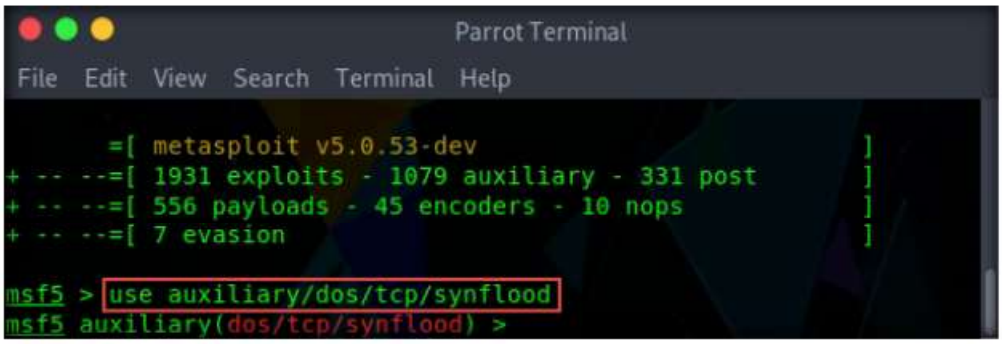


Figure 1.1.4: Using the Auxiliary Module for DoS attack

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.

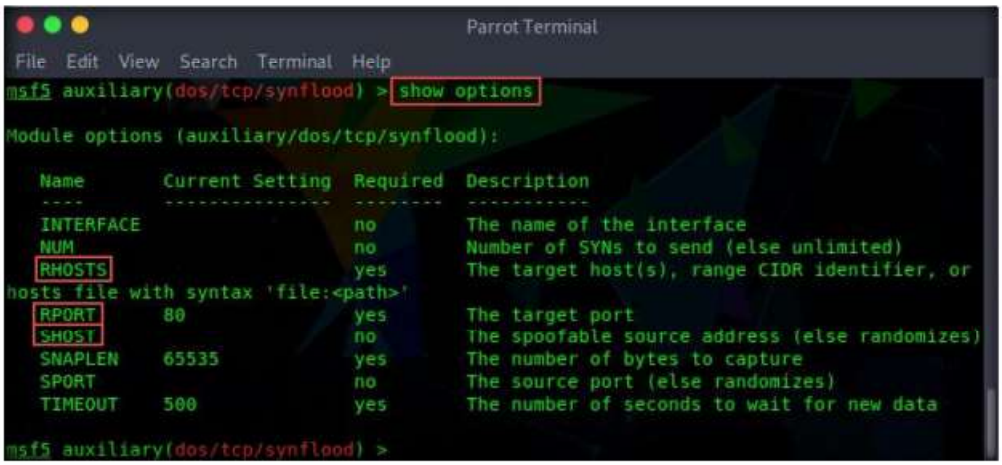


Figure 1.1.5: Viewing options

16. 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.
17. Issue the following commands:
    - **set RHOST <Target IP Address>** (here, **10.10.10.10**)
    - **set RPORT 21**
    - **set SHOST <Spoofable IP Address>** (here, **10.10.10.19**)

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


Figure 1.1.6: Configuring options

18. Once the auxiliary module is configured with the required options, start the DoS attack on the **Windows 10** virtual machine.
19. To do so, type **exploit** and press **Enter**. This begins SYN flooding the **Windows 10** virtual machine.

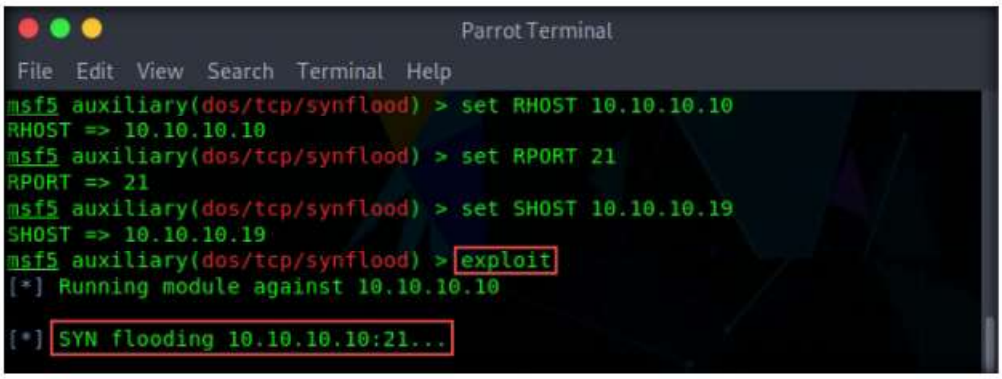


Figure 1.1.7: Initiating DoS attack

**TASK 1.3**

**Examine the DoS Attack**

20. To confirm, switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
21. Click the **Type here to search** field present at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.
22. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.

**Note**: The network interface might differ in your lab environment.

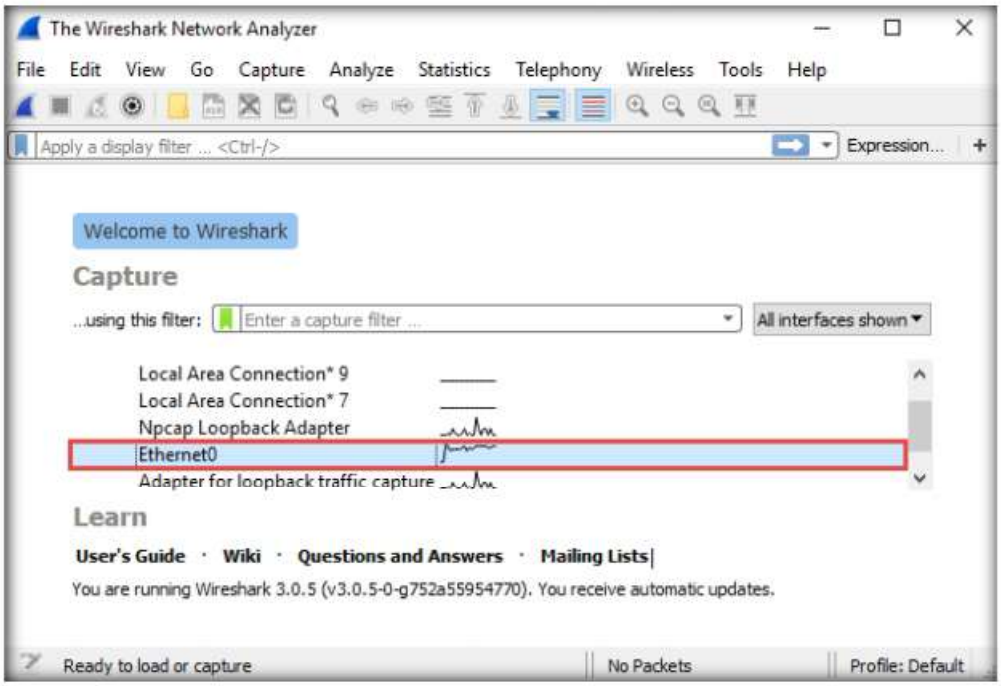


Figure 1.1.8: Capturing traffic through Wireshark

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** (**10.10.10.19**) virtual machine. This implies that the IP address of the **Parrot Security** machine has been spoofed.

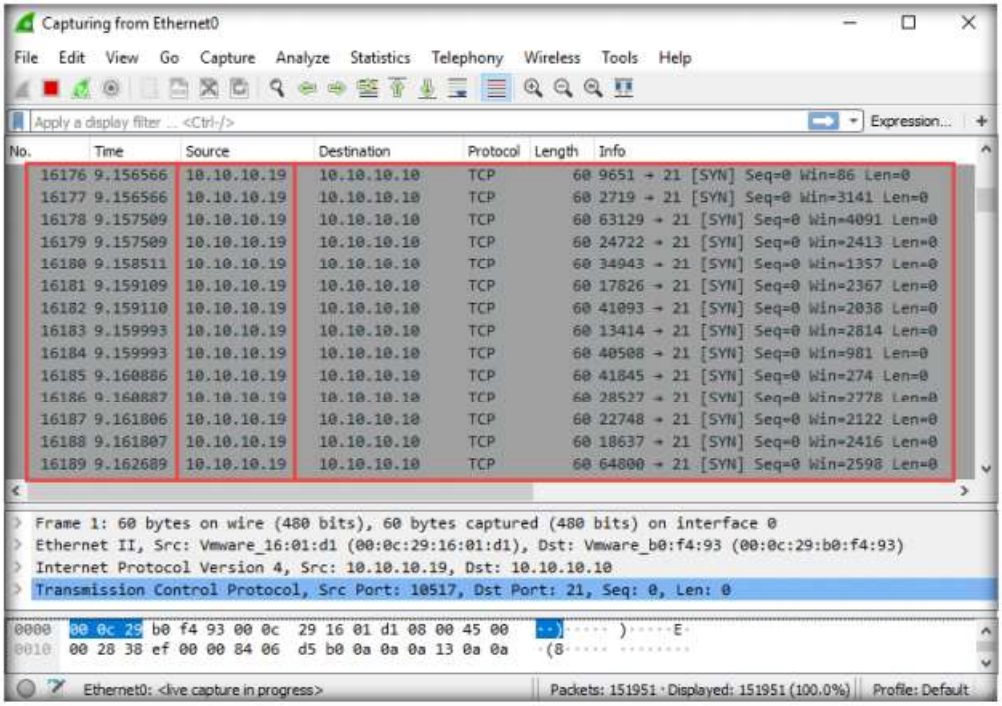


Figure 1.1.9: Analyzing the traffic

24. Observe that the target machine (**Windows 10**) 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, switch to the **Parrot Security** virtual machine and press **Ctrl+C** to terminate the attack.

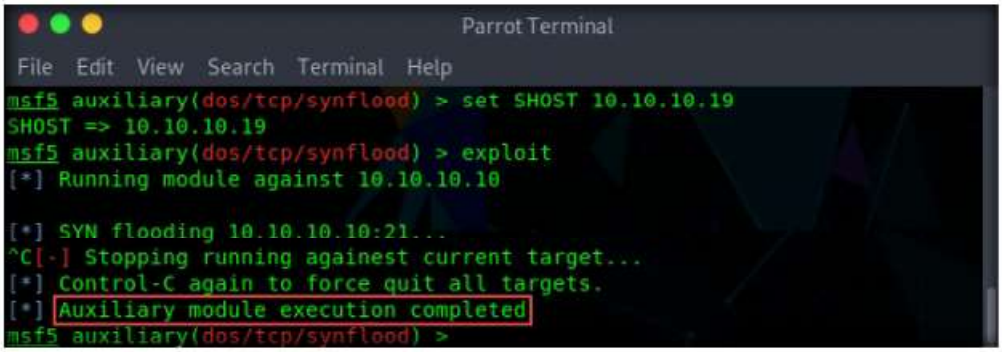


Figure 1.1.10: Terminating the attack

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

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.

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.

1. Turn on the **Windows Server 2019** virtual machine.

**Note**: Ensure that the **Windows 10** and **Parrot Security** virtual machines are running.

2. On the **Windows 10** virtual machine, click the **Type here to search** field at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.
3. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.
4. **Wireshark** starts capturing the packets; leave it running.

### TASK 2.1 — Perform SYN Flooding using hping3

5. Switch to the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

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

hping3 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.

9. In the terminal window; type **hping3 -S <Target IP Address> -a <Spoofable IP Address> -p 22 --flood** and press **Enter**.

**Note**: Here, the target IP address is **10.10.10.10** [**Windows 10**], and the spoofable IP address is **10.10.10.19** [**Windows Server 2019**])

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

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

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

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

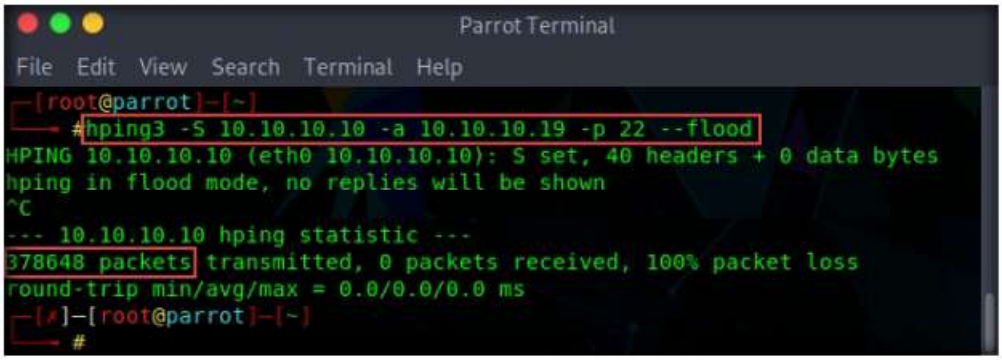


Figure 1.2.1: Attack successfully launched from Parrot Security

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

13. Switch to the **Windows 10** virtual machine and observe the TCP-SYN packets captured by **Wireshark**.

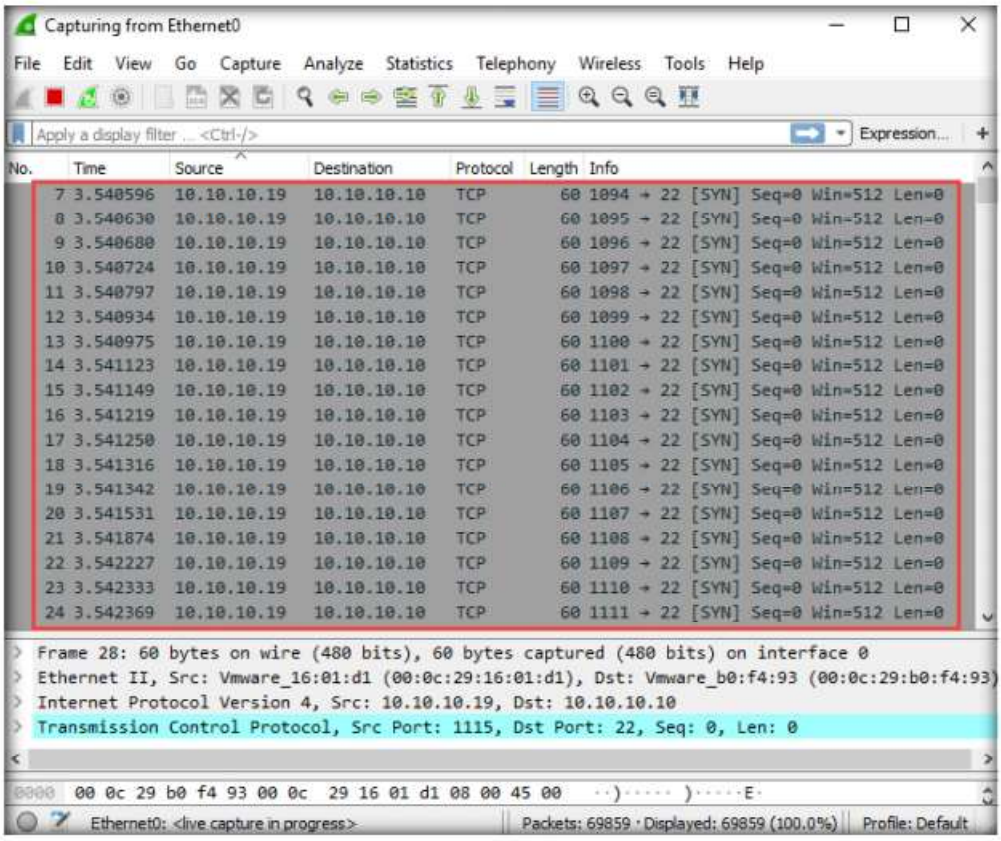


Figure 1.2.2: Wireshark with packets traffic

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.

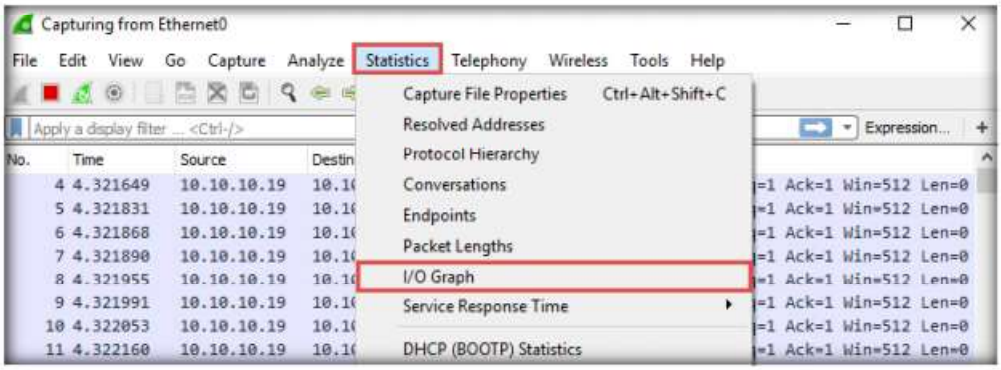


Figure 1.2.3: Wireshark: I/O Graph option

15. The **Wireshark . IO Graphs . Ethernet0** 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.

16. After analyzing the **I/O Graph**, click **Close** to close the **Wireshark . IO Graphs . Ethernet0** window.

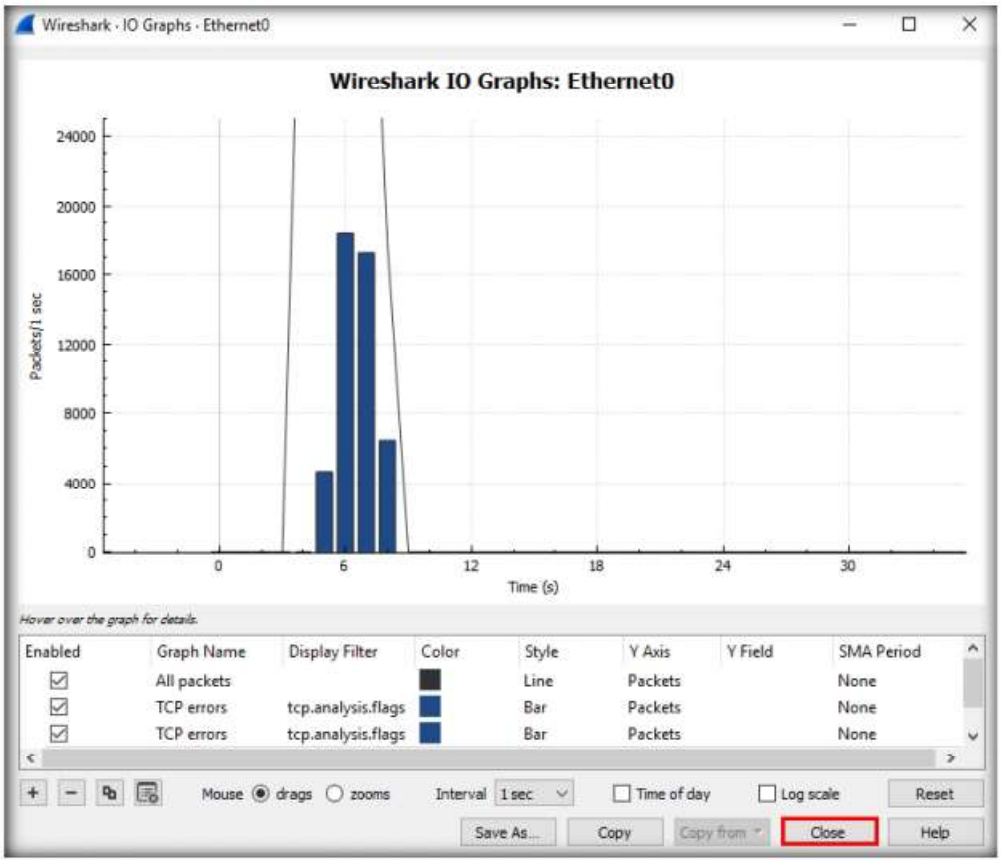


Figure 1.2.4: Wireshark - IO Graphs

**TASK 2.2**

**Perform Ping of Death (PoD) Attack Using hping3**

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. Switch to the **Parrot Security** virtual 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**.

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

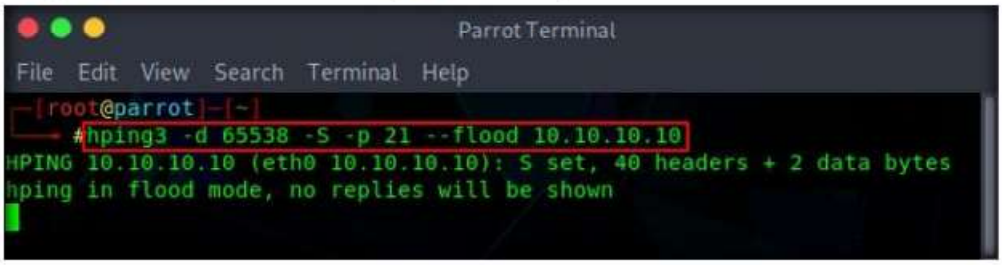


Figure 1.2.5: Attack successfully launched from Parrot Security

20. This command initiates the PoD attack on the **Windows 10** virtual machine.

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

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.

**TASK 2.3**

**Analyze Target System's Performance**

22. Switch to the **Windows 10** virtual machine, click the **Type here to search** field present at the bottom of **Desktop**, and type **task**. Click **Task Manager** from the results.
23. The **Task Manager** window appears; by default, the **Processes** tab appears, as shown in the screenshot.

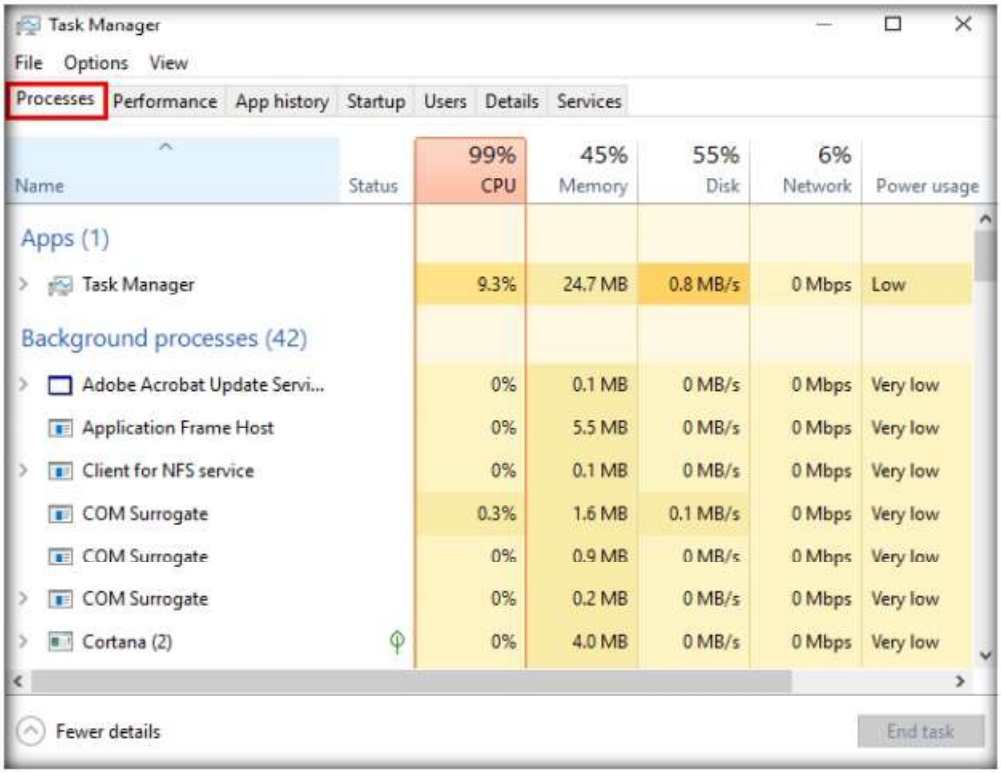


Figure 1.2.6: Task Manager window

24. Click the **Performance** tab to view the performance of various system components (**CPU**, **Memory**, **Disk**, **Ethernet**).
25. 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.
26. Observe the degradation in the performance of the system, which might result in the system crashing.

**Note**: The results might differ in your lab environment.

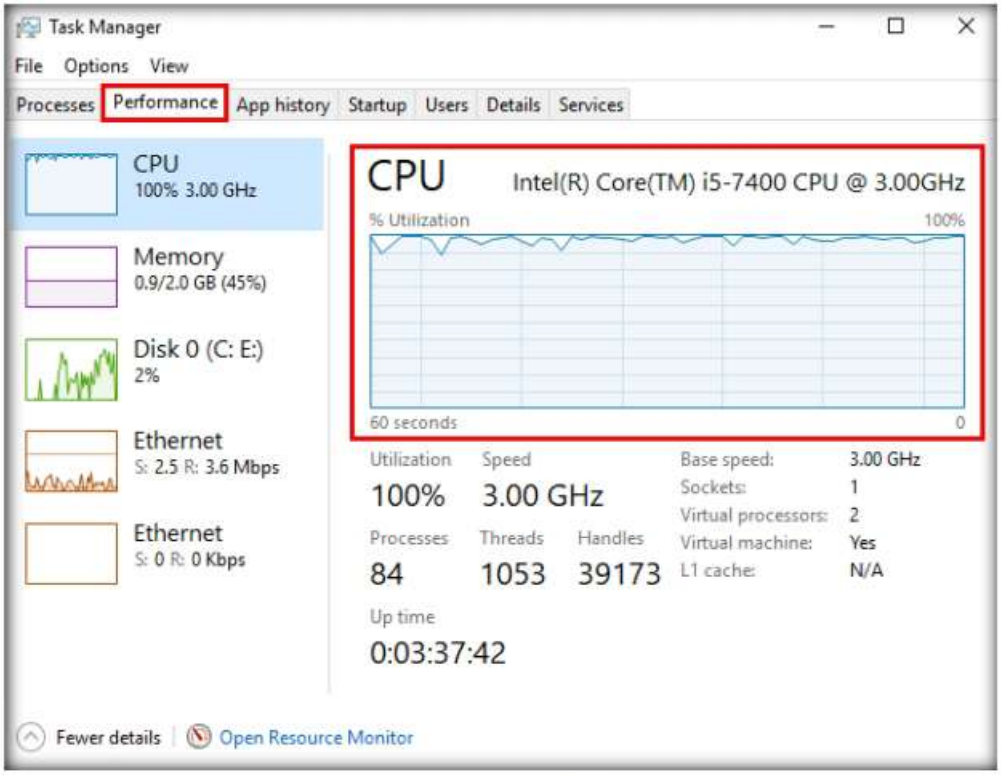


Figure 1.2.7: Performance Tab: CPU Utilization

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

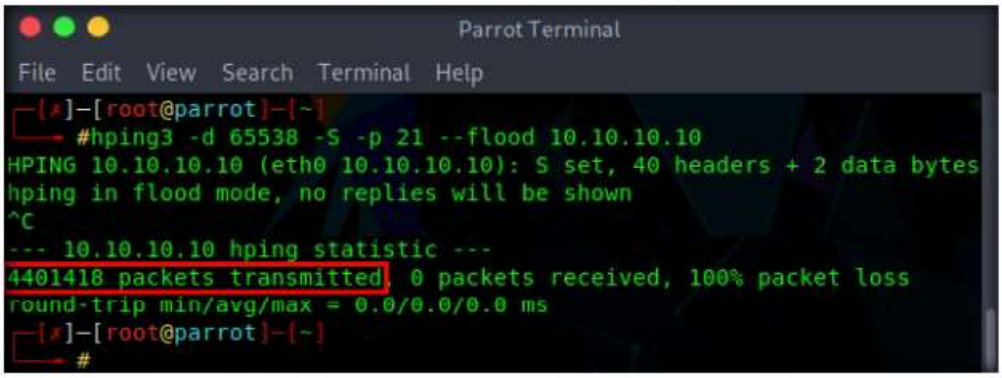


Figure 1.2.8: Terminate PoD attack

**TASK 2.4**

**Check for Open NetBIOS Port**

28. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** virtual 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 **10.10.10.19** [**Windows Server 2019**]) and press **Enter**.

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

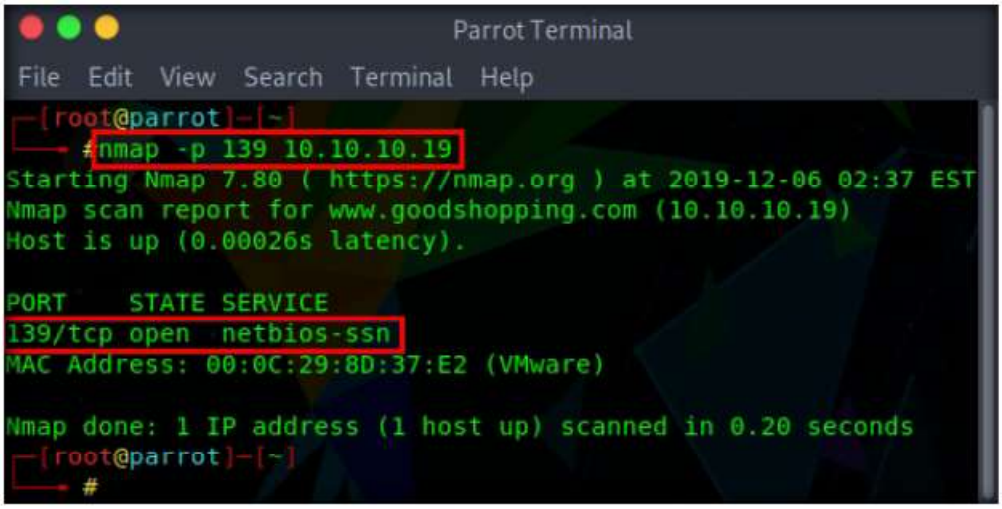


Figure 1.2.9: Check for open port

**TASK 2.5**

**Perform UDP Application Layer Flood Attack using hping3**

30. 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**.

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

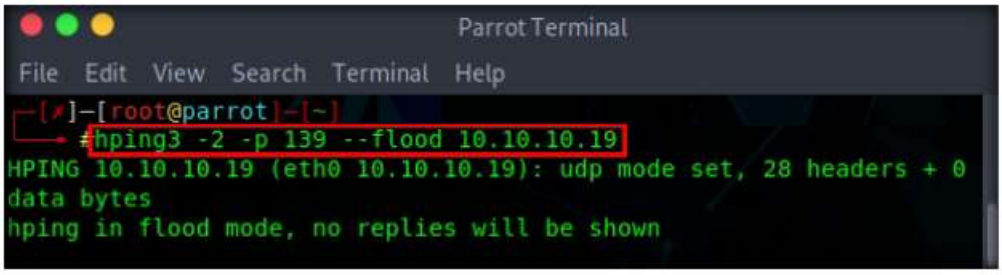


Figure 1.2.10: Performing a UDP Application Layer Flood Attack

31. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
32. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.

**TASK 2.6**

**Analyze the Network Traffic**

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

33. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.

**Note**: The network interface might differ in your lab environment.

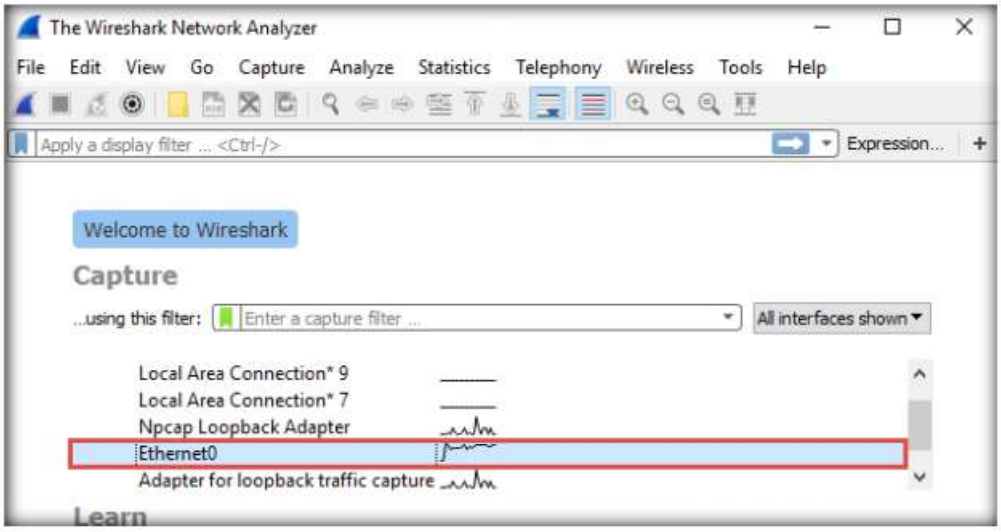


Figure 1.2.11: Capturing traffic through Wireshark

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

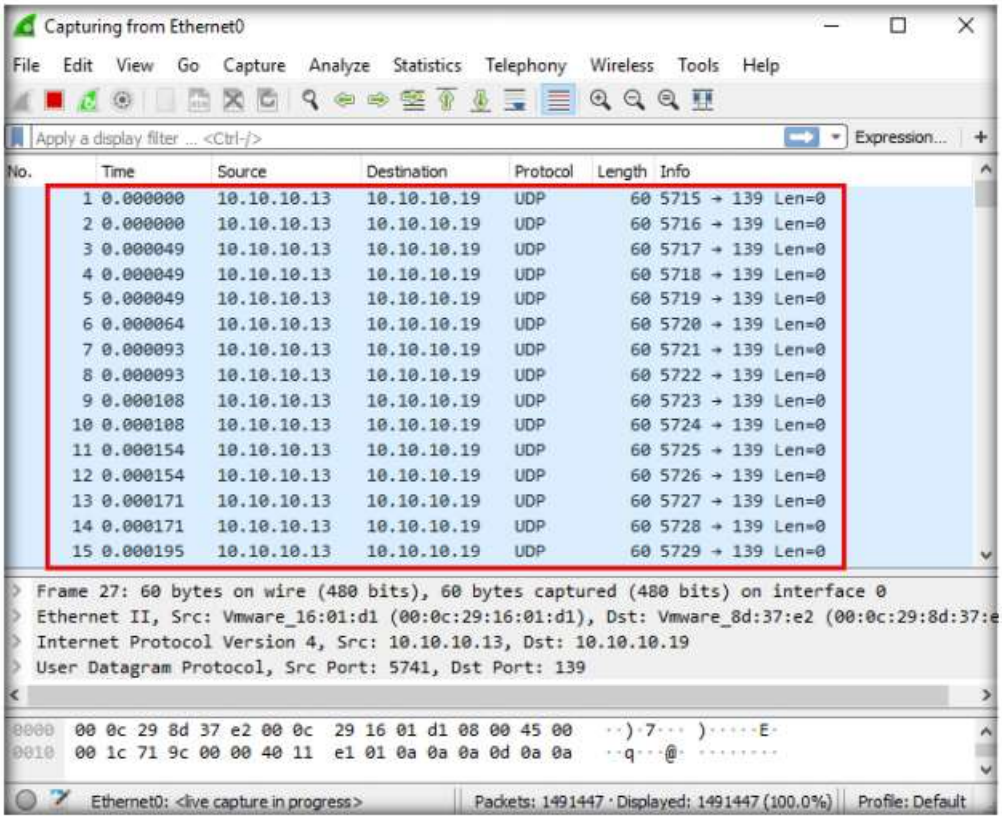


Figure 1.2.12: Analyzing the traffic

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

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

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

- **CharGEN** (Port 19)
- **SNMPv2** (Port 161)
- **QOTD** (Port 17)
- **RPC** (Port 135)
- **SSDP** (Port 1900)
- **CLDAP** (Port 389)
- **TFTP** (Port 69)
- **NetBIOS** (Port 137,138,139)
- **NTP** (Port 123)
- **Quake Network Protocol** (Port 26000)
- **VoIP** (Port 5060)

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.
38. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

## TASK 3 Perform a DDoS Attack using HOIC

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

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.

**Note**: In this task, we will use the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines to launch a DDoS attack on the **Parrot Security** virtual machine.

1. Turn on the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.
2. On the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**. Navigate to **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.

**Note**: To perform the DDoS attack, run this tool from various virtual machines at once. If you run the tool directly from the shared drive in the virtual 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.

3. Similarly, follow the previous step (**Step #2**) on the **Windows Server 2019** and **Windows Server 2016** virtual machines.

**Note**: On the **Windows Server 2019** and **Windows Server 2016** virtual machines, the **High Orbit Ion Cannon (HOIC)** folder is located at **Z:\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools**.

TASK 3.1

**Configure HOIC**

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

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

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

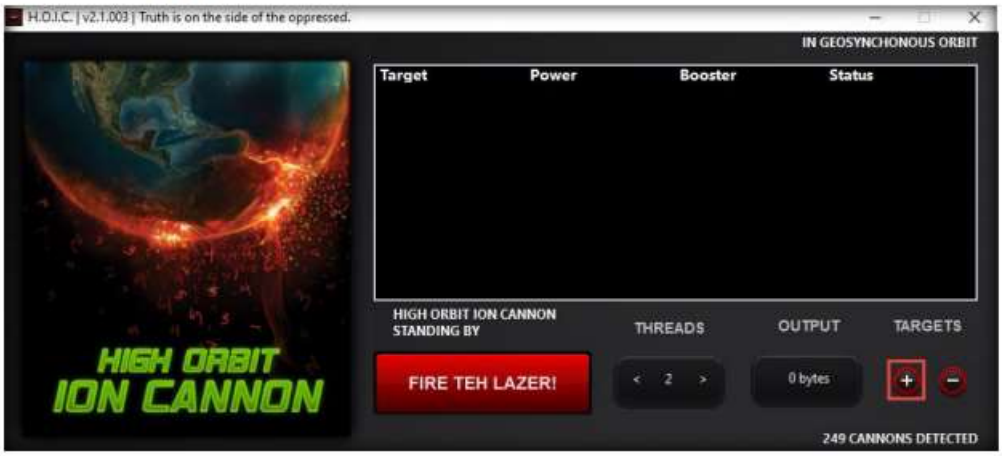


Figure 1.3.1: HOIC GUI

HOIC (High Orbit Ion Cannon) 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.

6. 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**.

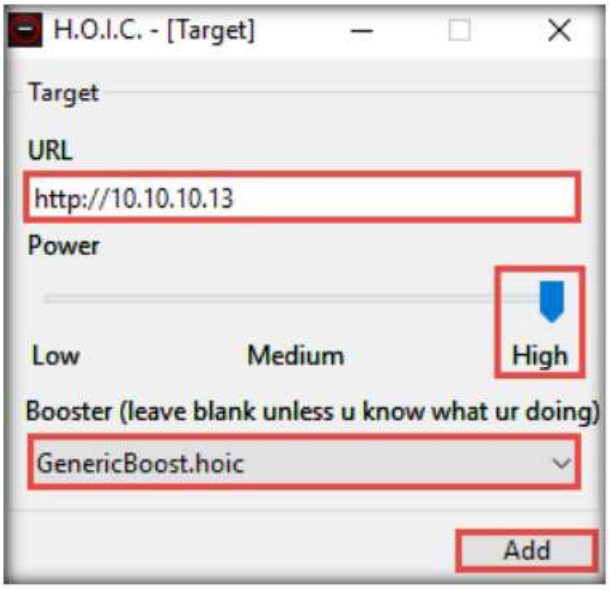


Figure 1.3.2: HOIC - [Target] Pop-up

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


Figure 1.3.3: Setting the THREADS Value

8. Now, switch to the **Windows Server 2019** and **Windows Server 2016** virtual machines and follow **Steps 4 - 7** to configure HOIC.

**Note**: In the **Windows Server 2019** and **Windows Server 2016** virtual machines, log in with credentials **Administration**/**Pa$$w0rd**.

**TASK 3.2**

**Perform DDoS Attack**

9. Once **HOIC** is configured on all machines, switch to each machine (**Windows 10**, **Windows Server 2019**, and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target the **Parrot Security** machine.

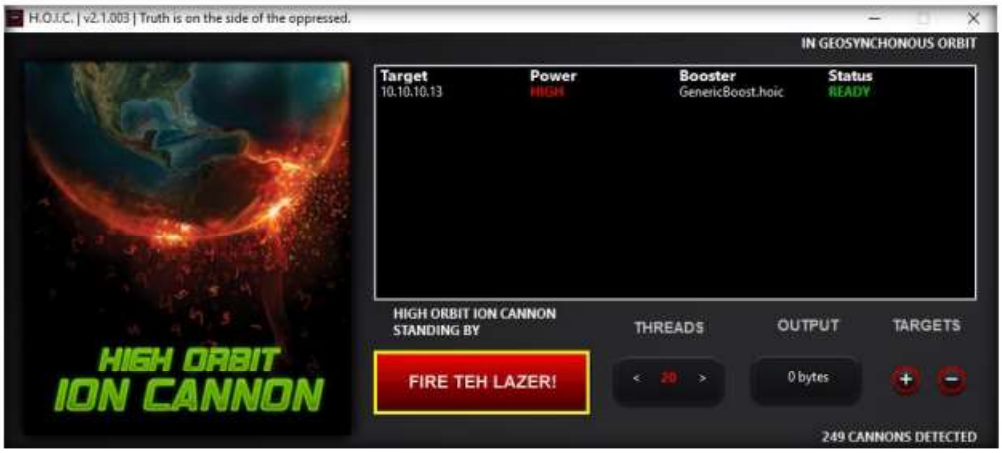


Figure 1.3.4: Clicking FIRE THE LAZER!

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


Figure 1.3.5: Performing a DDoS attack

11. Switch to the **Parrot Security** virtual machine.
12. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
13. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
14. The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.

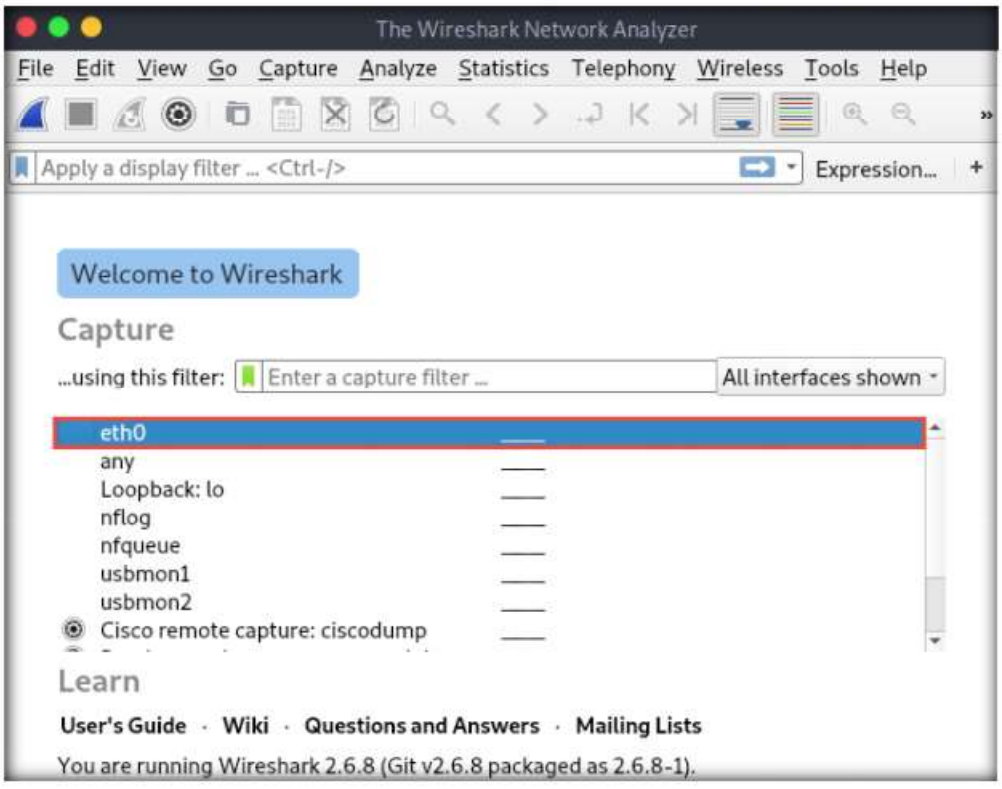


Figure 1.3.6: Wireshark window

**TASK 3.3**

**Analyze the Captured Packets**

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

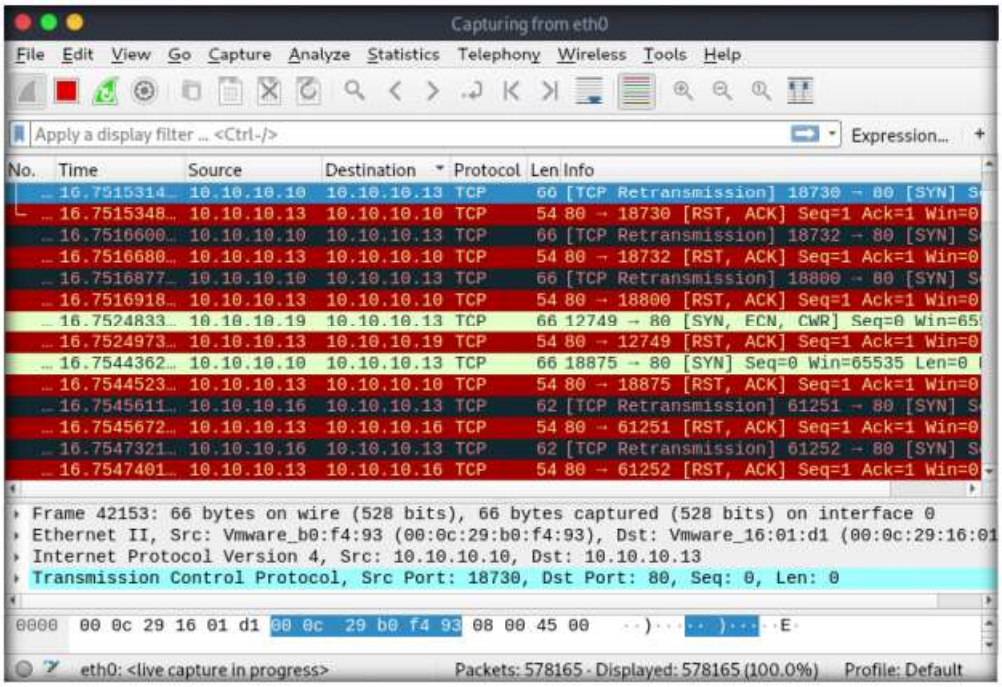


Figure 1.3.7: Wireshark capturing the packets

16. Leave the machine intact for 5–10 minutes, and then open it again. Observe that the performance of the machine is slightly affected and that its response is slowing down.
17. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, **Parrot Security**) resources are completely consumed, and the machine is overwhelmed.

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

18. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all the attacker virtual machines. Also, close the Wireshark window on the Parrot Security virtual machine.
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 4

# Perform a DDoS Attack using LOIC

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

**Note**: In this task, we will use the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines to launch a DDoS attack on the **Parrot Security** virtual machine.

TASK 4.1

**Configure 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.

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

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

2. The **Low Orbit Ion Cannon** main window appears.
3. Perform the following settings:
   - Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.10.13**), 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.

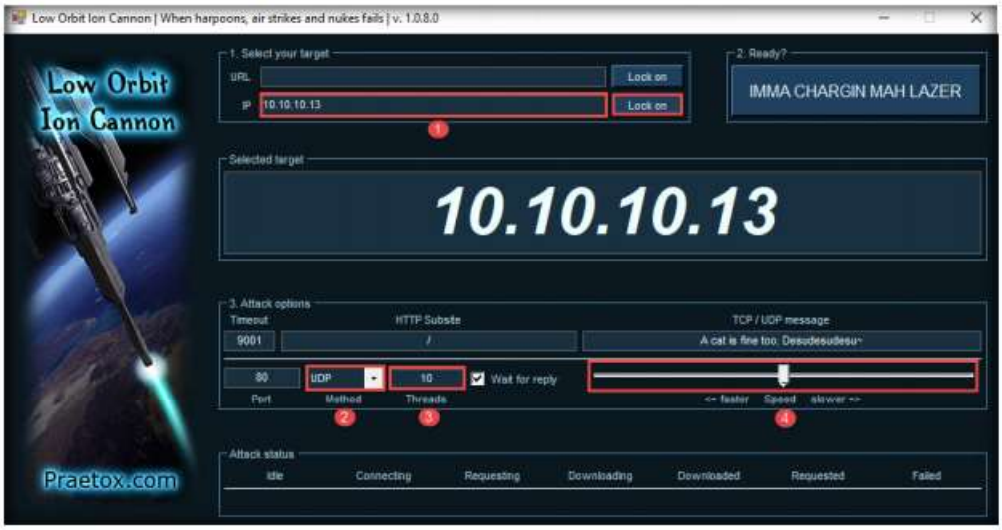


Figure 1.4.1: LOIC main window

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

**Note**: On the **Windows Server 2019** and **Windows Server 2016** virtual machines, LOIC is located at **Z:\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)**.

**TASK 4.2**

**Perform DDoS Attack**

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.

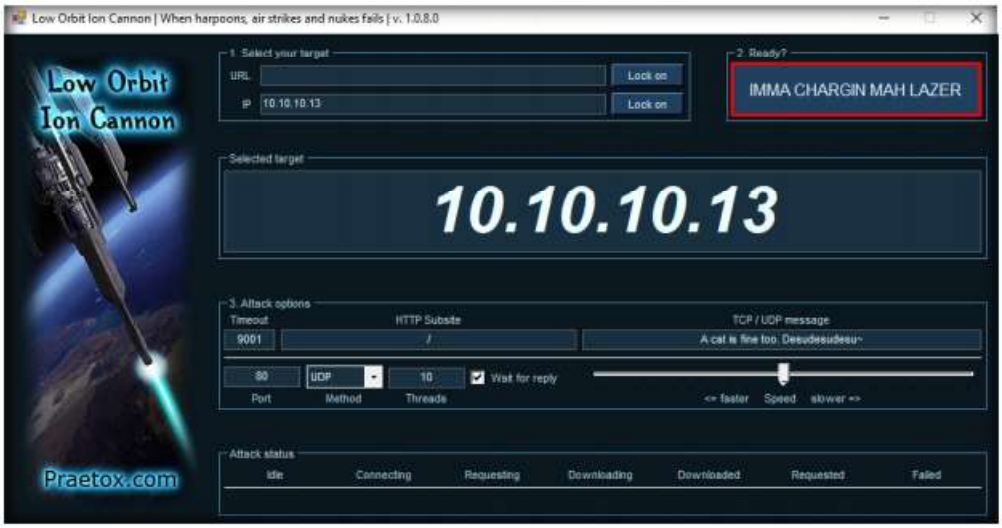


Figure 1.4.2: Performing a DDoS attack

6. Switch to the **Parrot Security** virtual 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.

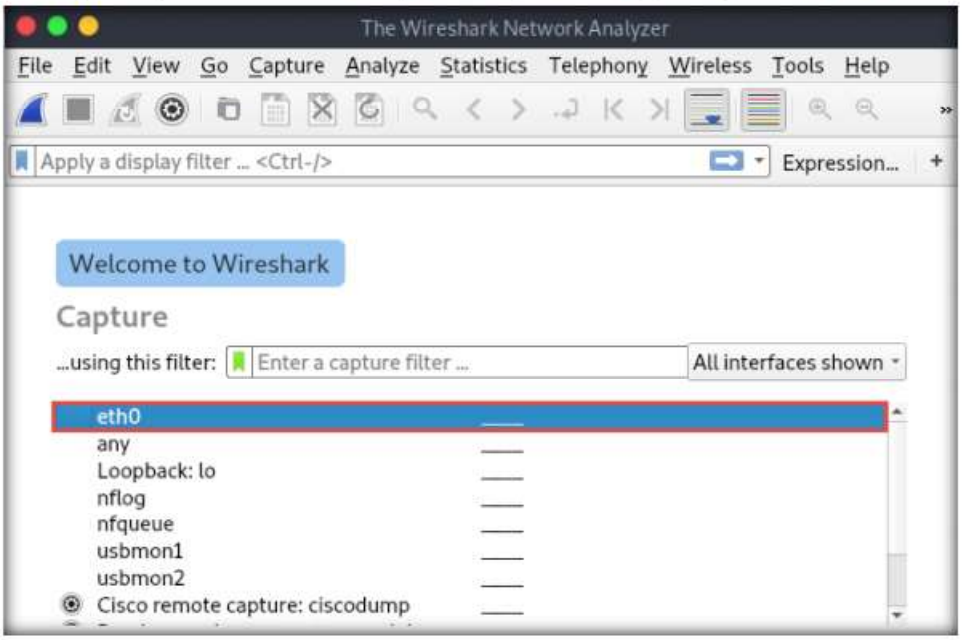


Figure 1.4.3: Wireshark window

**TASK 4.3**

**Analyze the Captured Packets**

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

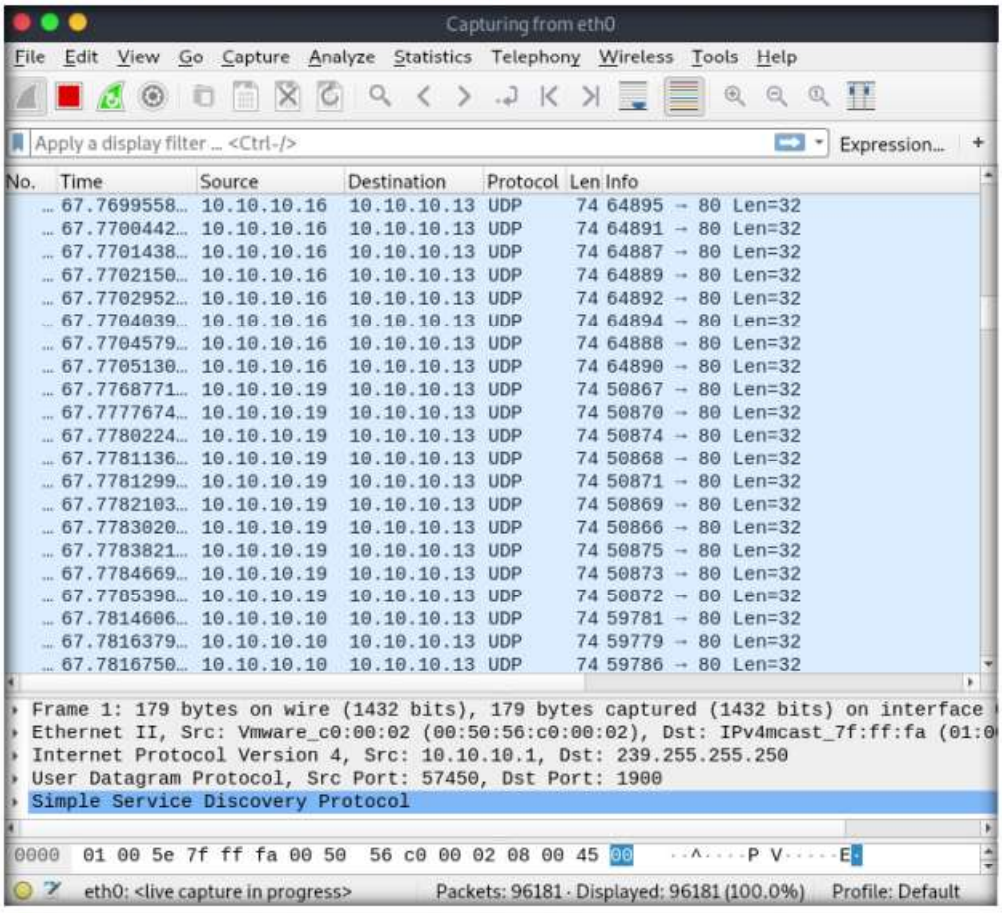


Figure 1.4.4: Wireshark capturing the packets

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 **IMMA CHARGIN MAH LAZER** again, and then close the LOIC window on all the attacker virtual machines.
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.
15. Turn off the **Windows 10**, **Windows Server 2019**, **Windows Server 2016**, and **Parrot Security** virtual machines.

You can also use other DoS and DDoS attack tools such as **XOIC** (http://anonhacktivism.blogspot.com), **HULK** (https://siberianlaika.ru), **Tor's Hammer** (https://sourceforge.net), and **Slowloris** (https://github.com) to perform DoS and DDoS attacks.

## Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |

Lab 2

# Detect and Protect Against DoS and DDoS Attacks

*DoS and DDoS attack detection techniques are based on identifying and discriminating between illegitimate traffic increases and flash events from legitimate packet traffic.*

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

## 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

## Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- A browser with an Internet connection
- Administrator privileges to run the tools
- Anti DDoS Guardian located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in this lab might differ from what you see on your screen.

## Lab Duration

Time: 10 Minutes

## 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 Attack using Anti DDoS Guardian

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

**Note**: In this task, we will use the **Windows Server 2019** and **Windows Server 2016** virtual machines to perform a DDoS attack on the target system, **Windows 10**.

TASK 1.1

**Install and Launch Anti DDoS Guardian**

1. Turn on the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. Login to the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double click **Anti_DDoS_Guardian_setup.exe**.

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

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.

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


Figure 2.1.1: Setup - Anti DDoS Guardian

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.

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

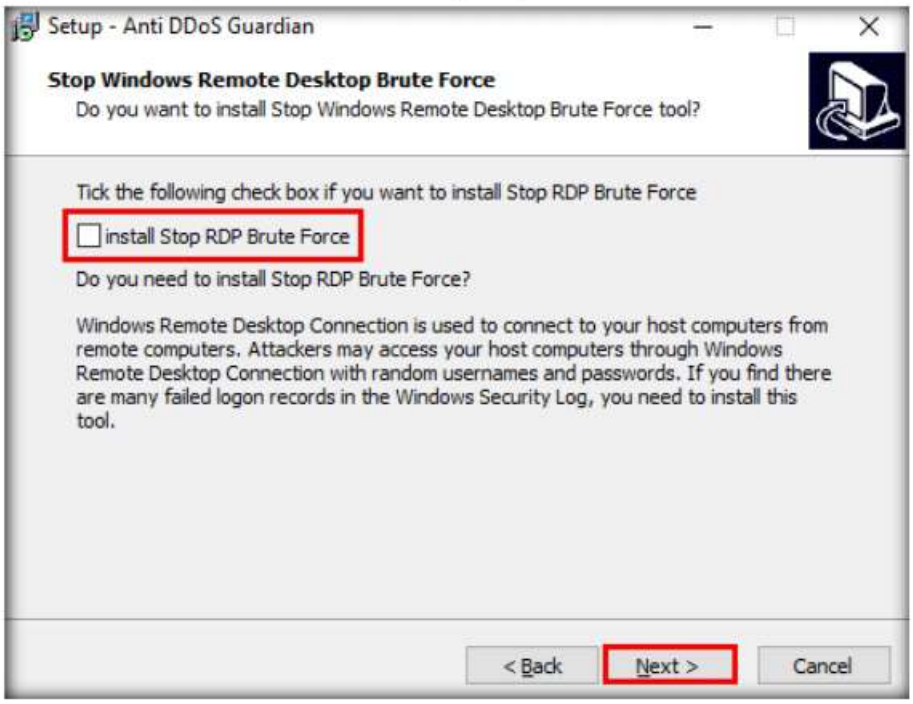


Figure 2.1.2: Stop Windows Remote Desktop Brute Force wizard

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

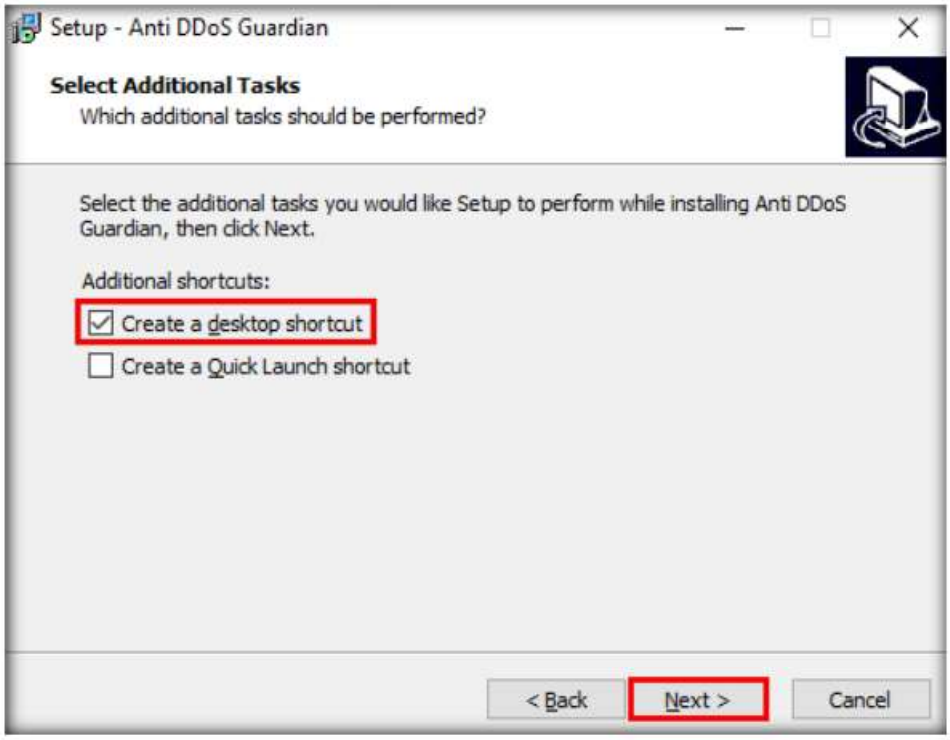


Figure 2.1.3: Select Additional Tasks wizard

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

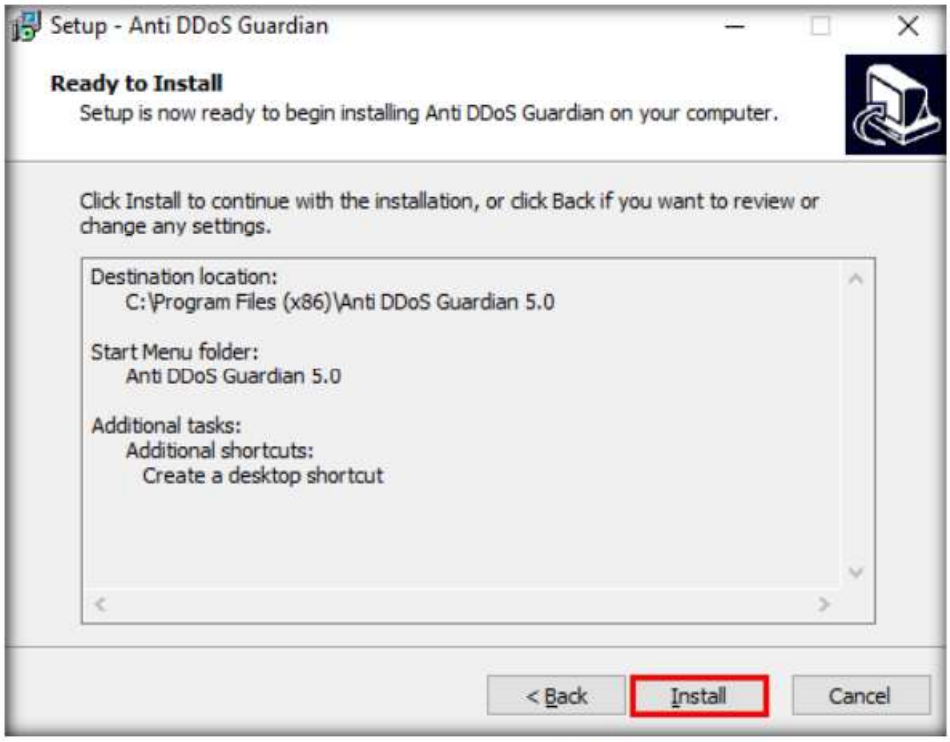


Figure 2.1.4: Ready to Install wizard

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

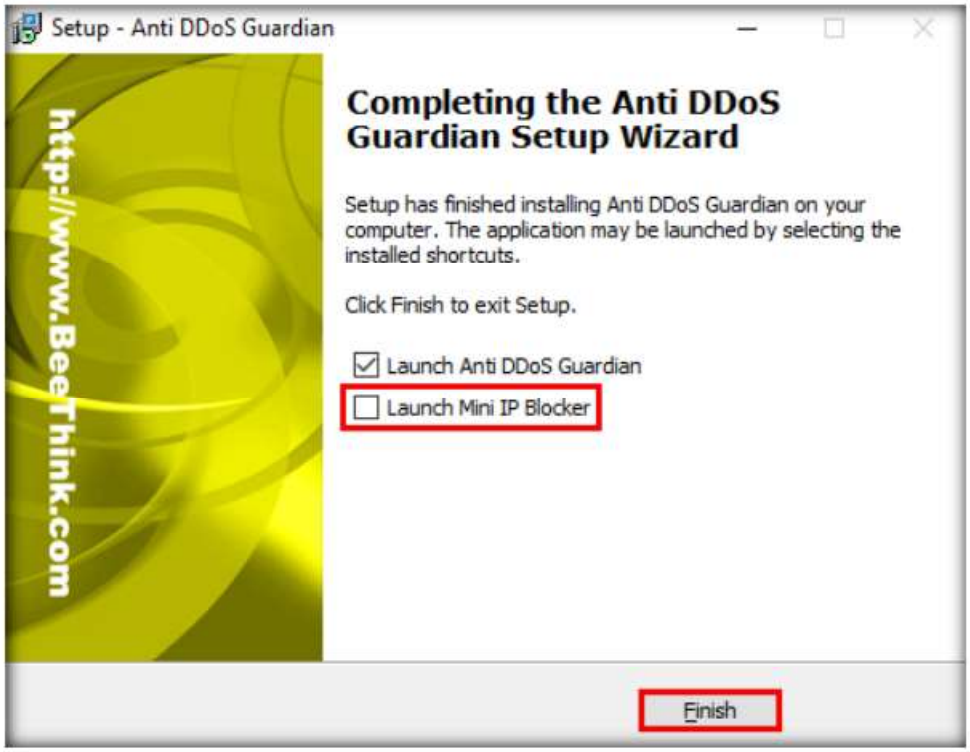


Figure 2.1.5: Completing the Anti DDoS Guardian Setup Wizard window

8. The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.
9. Click **Show hidden icons** ( ) from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon ( ).

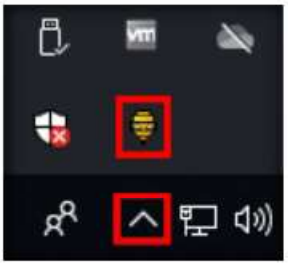

Figure 2.1.6: Launch Anti DDoS Guardian

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

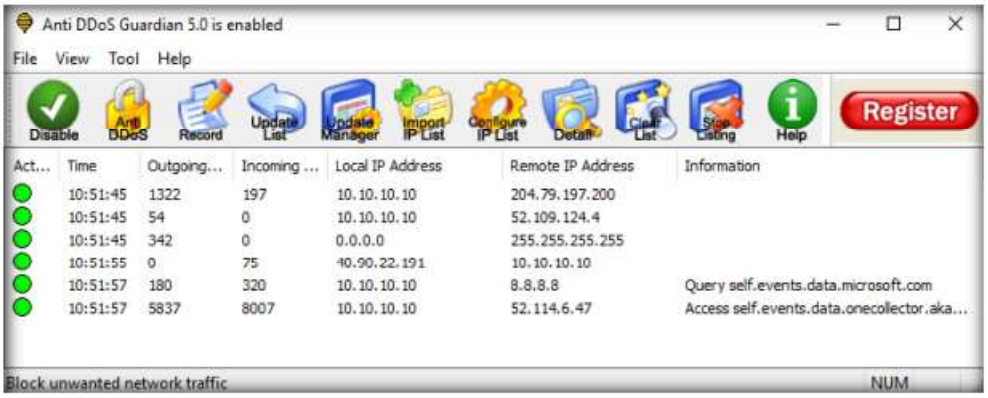


Figure 2.1.7: Anti DDoS Guardian window

**TASK 1.2**

**Configure HOIC**

11. Now, switch to the **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.
12. Navigate to **Desktop**, open the **High Orbit Ion Cannon (HOIC)** folder, and double-click **hoic2.1.exe**.

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

13. The **HOIC** GUI main window appears. Click the "**+**" button below the **TARGETS** section.


Figure 2.1.8: HOIC GUI

14. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.10.10** [**Windows 10**]) 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**.

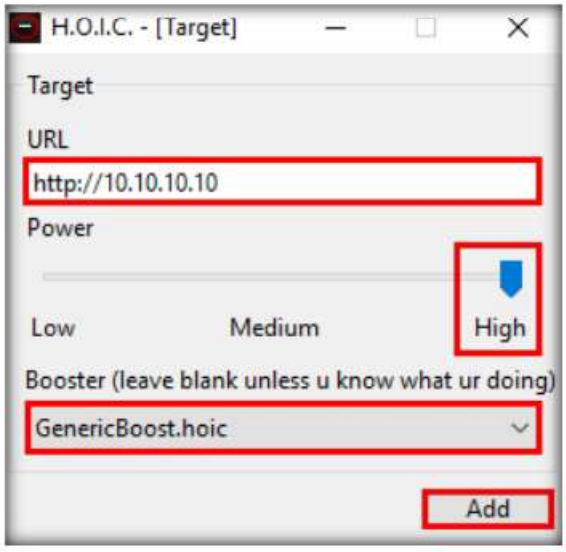


Figure 2.1.9: HOIC - [Target] Pop-up

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

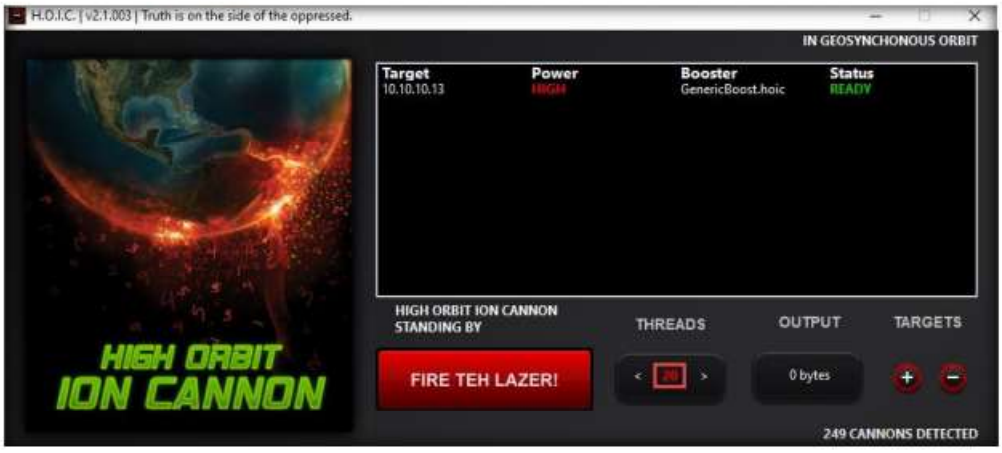


Figure 2.1.10: Setting the THREADS Value

16. Now, switch to **Windows Server 2016** and log in with the credentials **Administrator** and **Pa$$w0rd**. Follow **Steps 12 - 15** to launch and configure HOIC.

17. Once **HOIC** is configured on both machines, switch to each machine (**Windows Server 2019** and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target **Windows 10** machine.

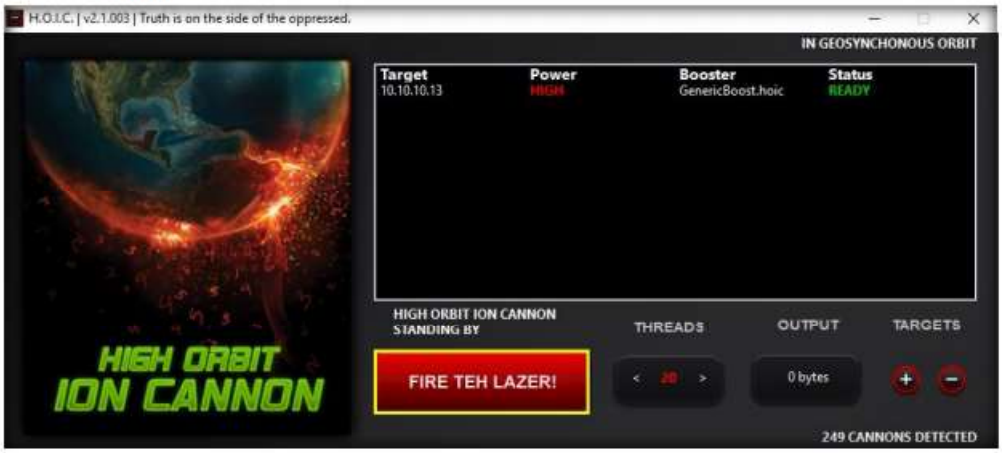


Figure 2.1.11: Clicking FIRE THE LAZER!

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


Figure 2.1.12: Performing a DDoS attack

**TASK 1.3**

**Analyze Captured Sessions**

19. Switch back to the **Windows 10** virtual machine and observe the packets captured by **Anti DDoS Guardian**.
20. Observe the huge number of packets coming from the host machines (**10.10.10.19** [**Windows Server 2019**] and **10.10.10.16** [**Windows Server 2016**]).

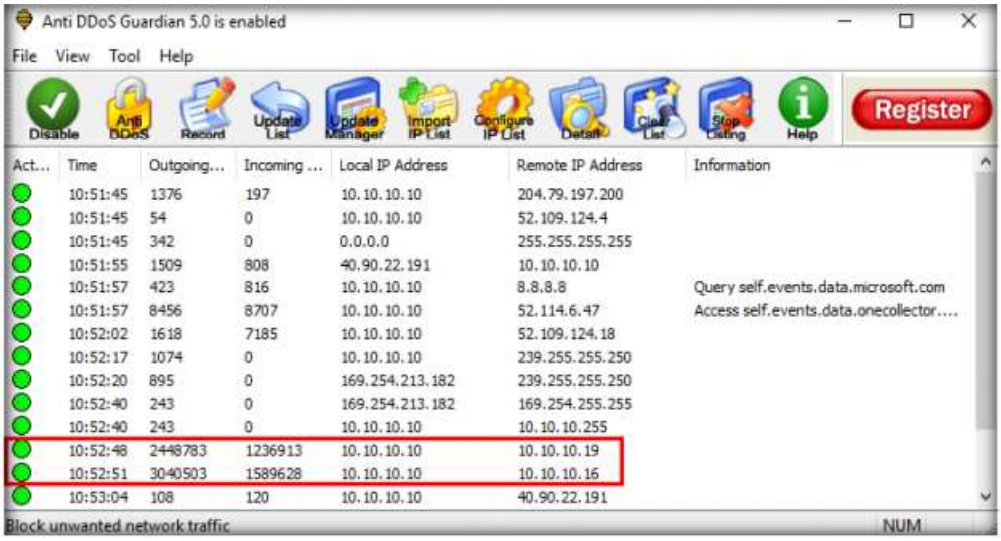


Figure 2.1.13: Anti DDoS Guardian window captured sessions

21. Double-click any of the sessions **10.10.10.19** or **10.10.10.16**.

**Note**: Here, we have selected 10.10.10.16. You can select either of them.

22. 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 10.10.10.16**, as shown in the screenshot.
23. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the **Block IP** option blocks the IP address sending the huge number of packets.

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

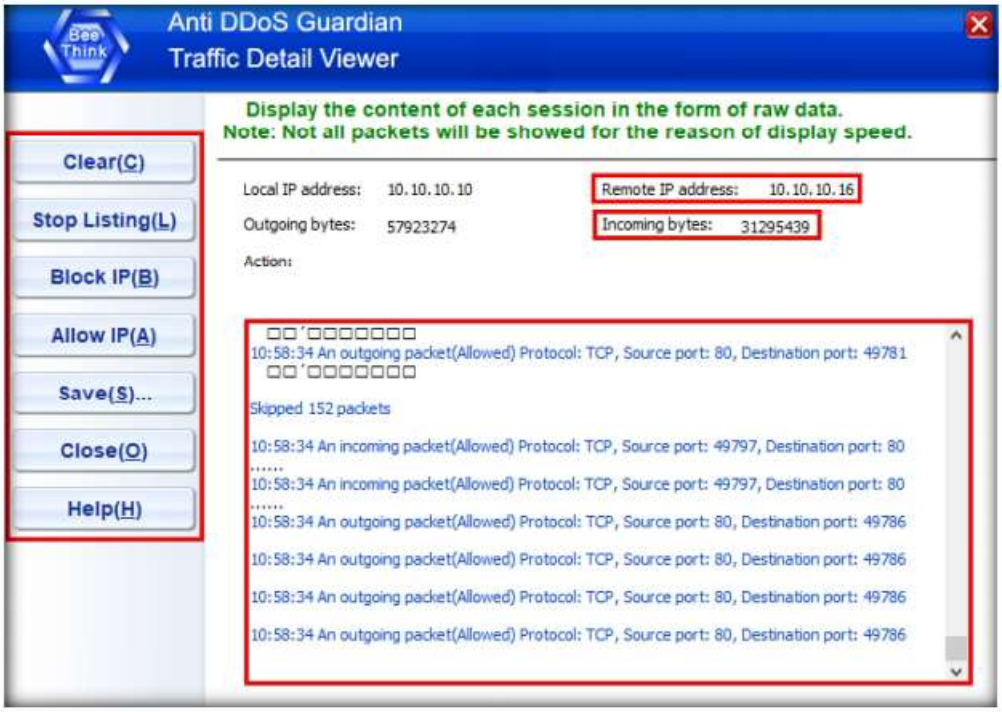


Figure 2.1.14: Traffic Details Viewer window

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

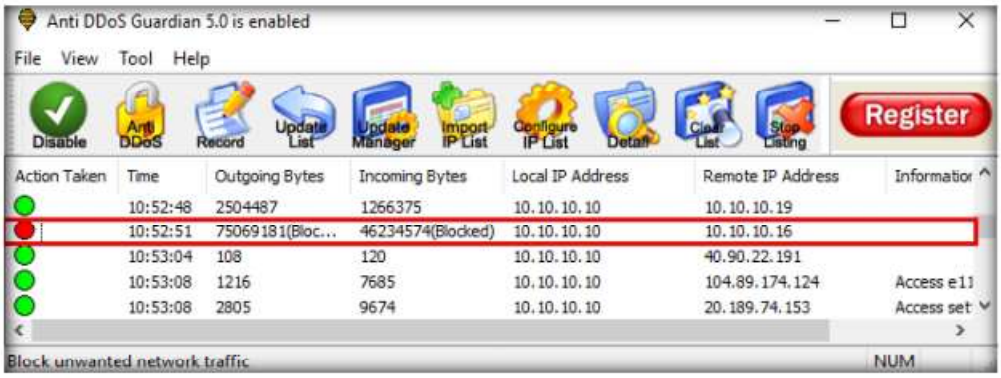


Figure 2.1.15: Blocked IP address session

26. Similarly, you can **Block IP** the address of the **10.10.10.19** session.
27. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all attacker virtual machines (**Windows Server 2019** and **Windows Server 2016**).
28. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
29. Close all open windows and document all the acquired information.

You can also use other DoS and DDoS protection tools such as **Imperva Incapsula DDoS Protection** (https://www.incapsula.com), **DOSarrest's DDoS protection service** (https://www.dosarrest.com), **DDoS-GUARD** (https://ddos-guard.net), and **Cloudflare** (https://www.cloudflare.com) to protect organization's systems and networks from DoS and DDoS attacks.

30. Navigate to **Control Panel** → **Programs** → **Programs and Features** and uninstall **Anti DDoS Guardian**.
31. Turn off the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.

## Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |