-ATHARVA KATKAR

TABLE OF CONTENTS

Denial of Service (DoS)

A Denial of Service (DoS) attack is a type of cyberattack where an attacker tries to make a system, server, or network unavailable to legitimate users by overloading it with traffic or requests.

Denial of Service (DoS) is an attack that prevents legitimate users from accessing a system or network by overwhelming it with excessive traffic or resource requests

---

How DoS Works (Simple Explanation)

- A server has limited resources (CPU, memory, bandwidth).
- The attacker sends too many requests at once.
- The server becomes slow or crashes.
- Genuine users cannot access the service.

Types of Denial of Service Attacks

1. DoS (Single-source attack)

- Attack comes from one system.
- Easier to detect and block.

2. Distributed DoS (DDoS)

- Attack comes from many systems (botnet).
- Harder to stop because traffic looks legitimate.

Common DoS Attack Techniques

Attack Type	Explanation
SYN Flood	Exploits TCP handshake to exhaust server connections
UDP Flood	Sends large UDP packets to random ports
ICMP Flood (Ping Flood)	Overloads network using ping requests
HTTP Flood	Sends excessive HTTP requests to a web server
Slowloris	Keeps connections open for long time

Impact of DoS Attacks

- Website or service goes offline
- Financial loss
- Reputation damage
- Interrupts business operations

Prevention & Mitigation

- Firewalls & IDS/IPS
- Rate limiting
- Load balancers
- DDoS protection services (Cloudflare, AWS Shield)
- Network traffic monitoring

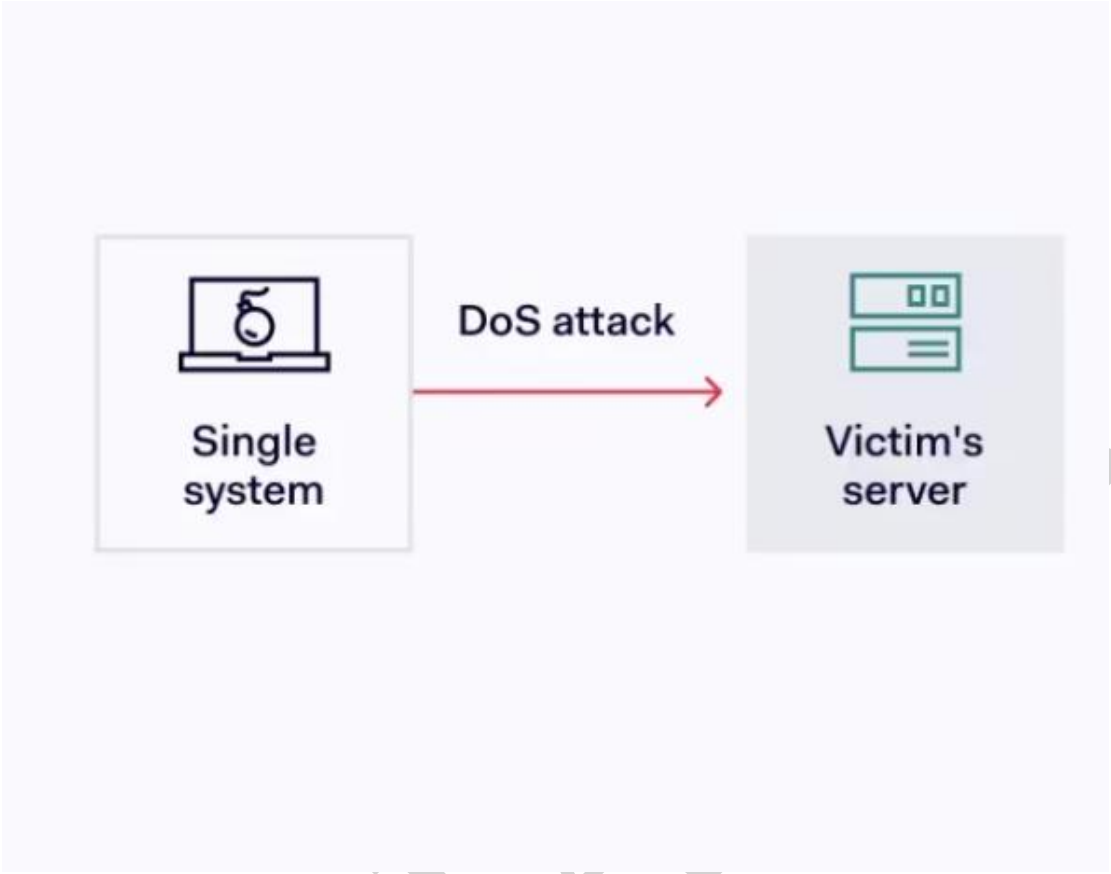
DoS vs DDoS

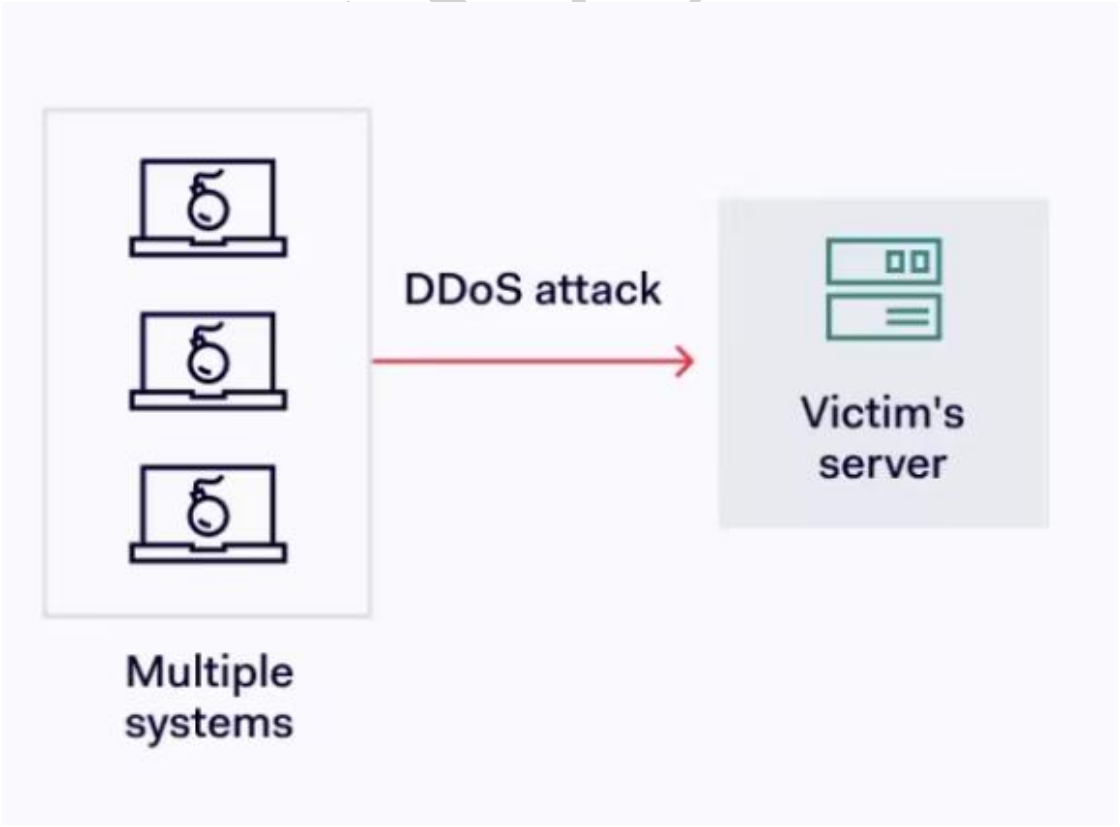
Feature	DoS	DDoS
Number of sources	Single	Multiple
Detection	Easy	Difficult
Impact	Lower	High

Objectives of DoS and DDoS Attacks :

1. To disrupt the availability of services for legitimate users.
2. To overload system resources like CPU, memory, or bandwidth.
3. To crash or freeze the target system using malicious input or traffic.
4. To exhaust network capacity and slow down performance.
5. To distract security teams while launching more serious attacks.
6. To extort money by threatening continuous service outages.
7. To protest against organizations or governments for ideological reasons.
8. To test or probe the strength of an organization’s cyber defenses.
9. To sabotage competitors by taking their services offline.
10. To take revenge on a target for personal or political motives.

Difference between DoS & DDoS





Categories of DoS/DDoS Attacks:

1. Volume-Based Attacks (Volumetric Attacks)

Goal:

Consume the entire bandwidth of the target network or system, making services unavailable to legitimate users.

Examples:

- **UDP Flood** – Sends massive volumes of UDP packets to random ports, overwhelming network bandwidth.
- **ICMP Flood (Ping Flood)** – Overloads the target by sending a large number of ICMP Echo Request (ping) packets.
- **DNS Amplification** – Spoofs the victim's IP address in DNS queries, causing DNS servers to send large response traffic to the victim.

Metrics:

- Measured in **Gigabits Per Second (Gbps)** or **Packets Per Second (pps)**

---

2. Protocol Attacks (Network Layer Attacks)

Goal:

Exploit weaknesses in network protocols to exhaust server, router, or firewall resources.

Examples:

- **SYN Flood** – Sends a high volume of SYN packets to consume server memory and connection state.
- **Ping of Death** – Sends malformed or oversized packets that cause the target system to crash.
- **Smurf Attack** – Spoofs ICMP echo requests to a broadcast address, amplifying traffic toward the victim.
- **ACK Flood** – Sends大量 ACK packets to overload firewalls and stateful network devices.

Metrics:

- Measured in **Packets Per Second (pps)**

---

3. Application Layer Attacks (Layer 7 Attacks)

Goal:
Crash or significantly slow down web applications by exhausting server-side application resources.

Examples:

- **HTTP GET/POST Flood** – Sends excessive HTTP requests to overwhelm the web server.
- **Slowloris** – Sends partial HTTP requests very slowly to keep connections open for long periods.
- **RUDY (R U Dead Yet?)** – Slowly sends POST requests to tie up server resources.
- **DNS Query Flood** – Floods DNS servers with large volumes of seemingly legitimate queries.

Metrics:

- Measured in **Requests Per Second (rps)**

---

4. Resource Exhaustion Attacks

Goal:
Drain system resources such as CPU, memory, or process limits rather than consuming network bandwidth.

Examples:

- **Fork Bomb** – Recursively creates processes to exhaust CPU and system process limits.
- **Memory Leak Exploits** – Force applications to consume excessive RAM until the system becomes unstable.

---

5. Multi-Vector Attacks

Goal:
Combine multiple attack techniques simultaneously to bypass security defenses and increase attack impact.

Examples:

- A **DDoS attack** using both **SYN Flood (Protocol Layer)** and **HTTP Flood (Application Layer)**.
- Combining **DNS Amplification** with **Slowloris** attacks in a coordinated manner.

Perform DOS/DDOS Using Metasploit

Metasploit Framework is a penetration-testing platform used by security professionals to test, validate, and demonstrate vulnerabilities in systems. It contains DoS-related auxiliary modules that can simulate denial-of-service conditions in a controlled and authorized environment.

How to use it -:

- Open kali linux terminal and type msfconsole

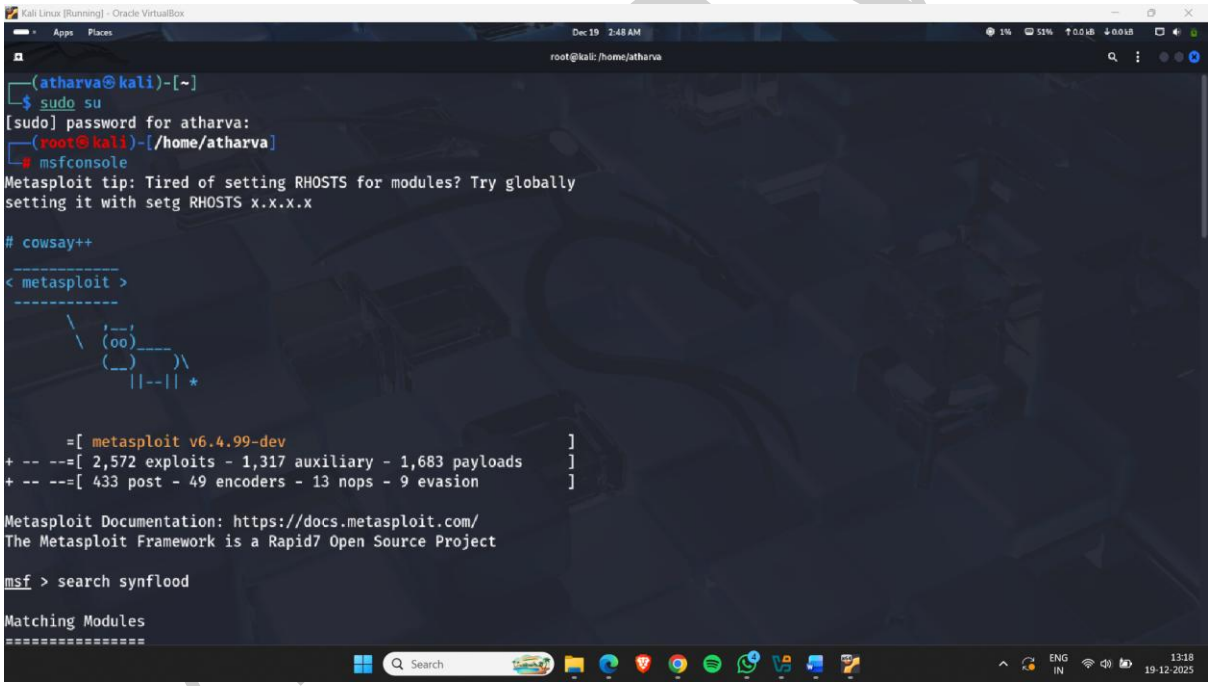


Figure 1

- Now search synflood & use the auxillary which is showing…

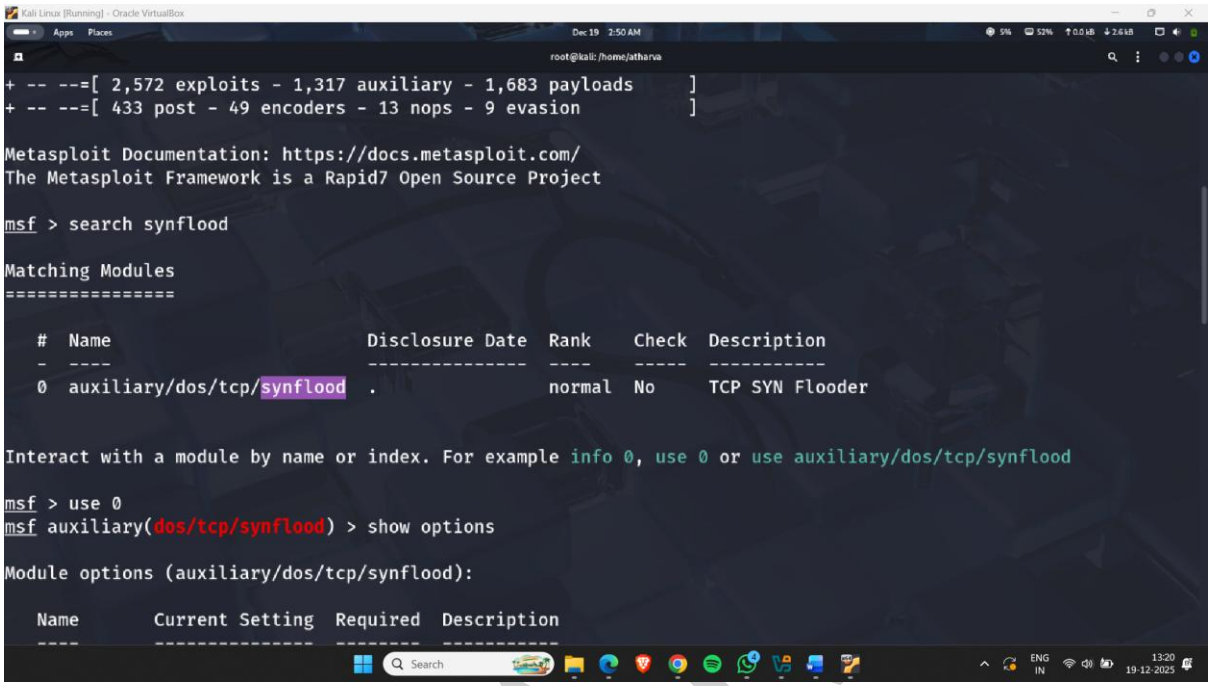


Figure 2

- The command show options displays all configurable parameters required to simulate the attack.

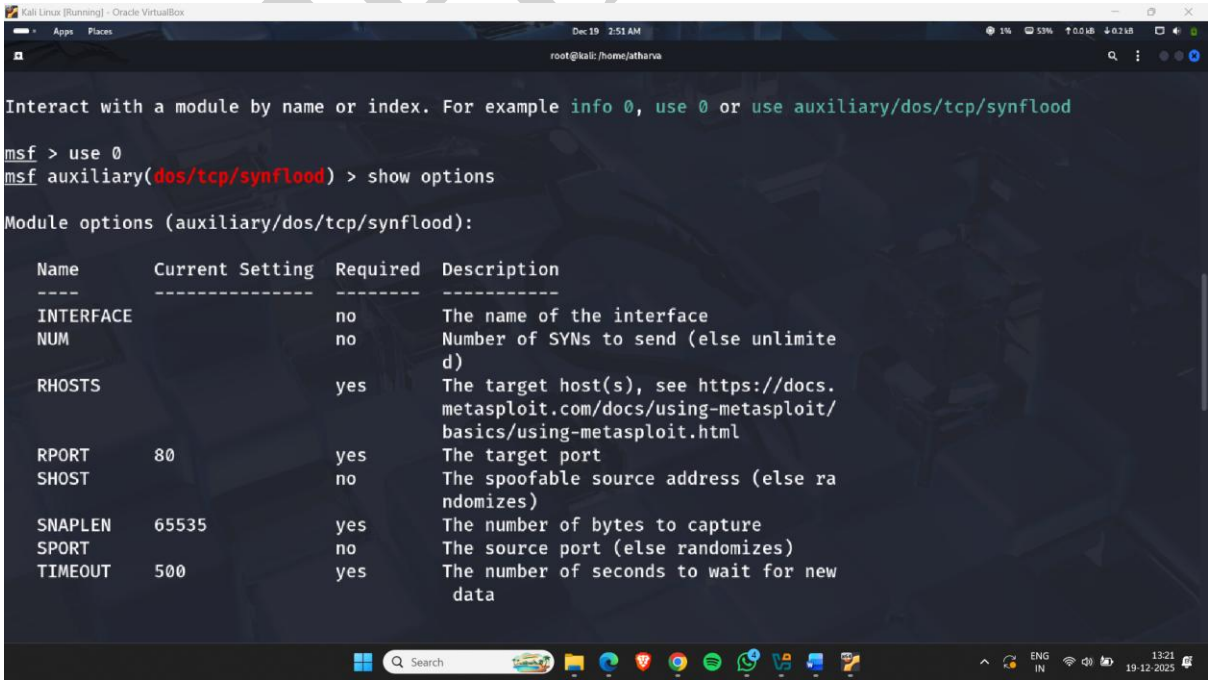


Figure 3

- Now set RHOST and Network Interface.

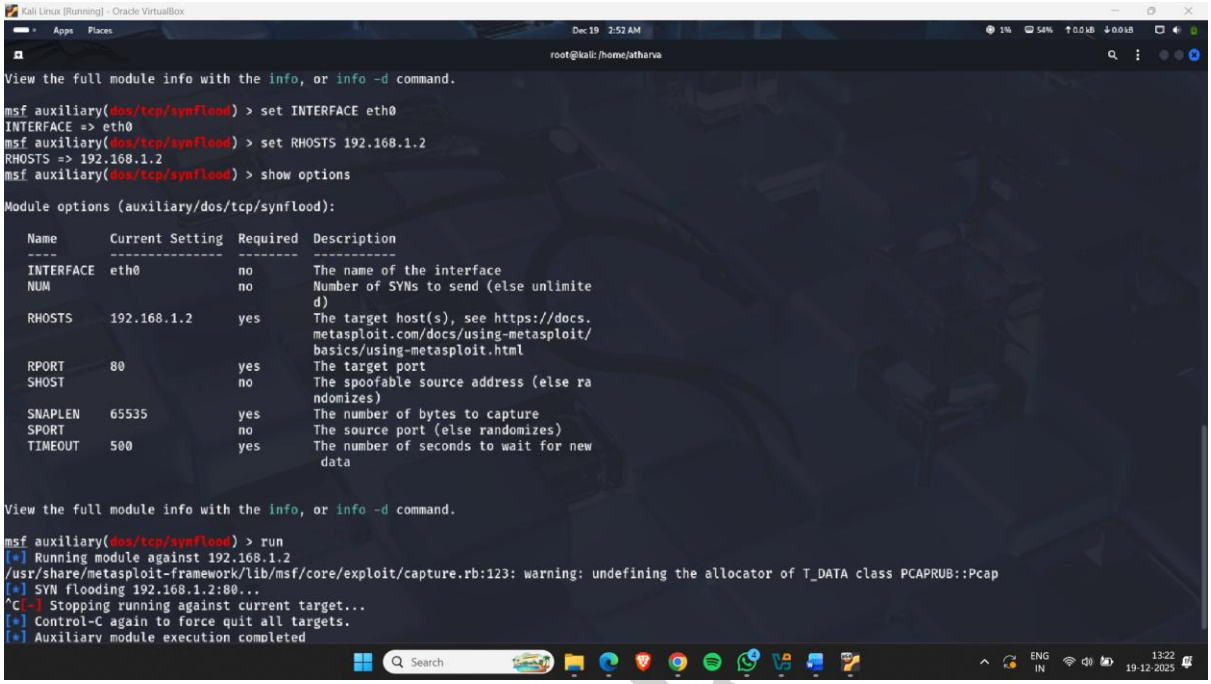


Figure 4

- Open wireshark to monitor
- It Shows network traffic captured during a TCP SYN Flood DoS attack.

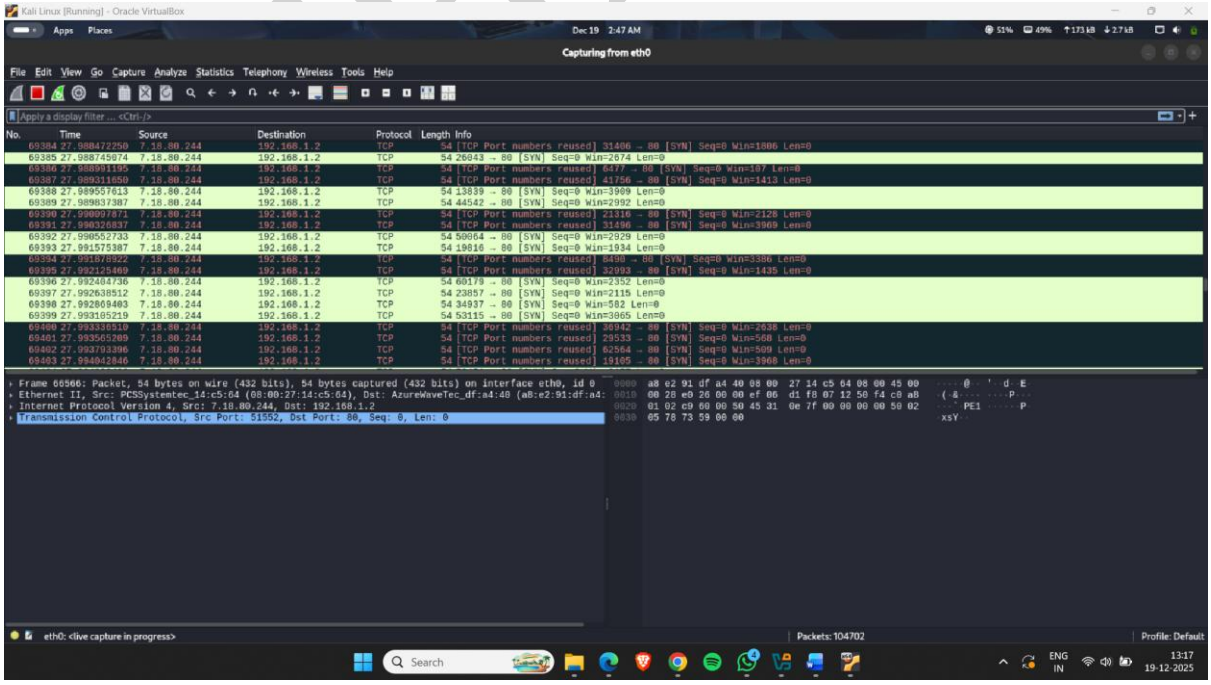


Figure 5

Perform DOS/DDOS Using Hping3

hping3 is a command-line network tool used for packet crafting, scanning, firewall testing, and DoS simulation. It is especially useful in penetration testing and network troubleshooting.

How to use it -:

- Open kali linux terminal and type hping3 command.

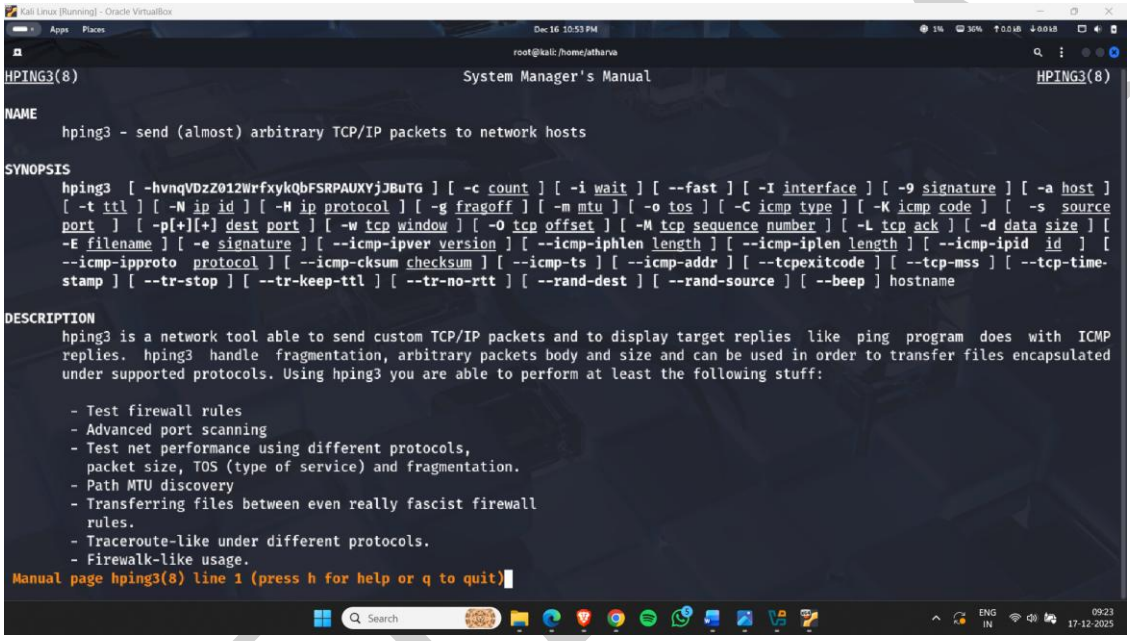


Figure 6

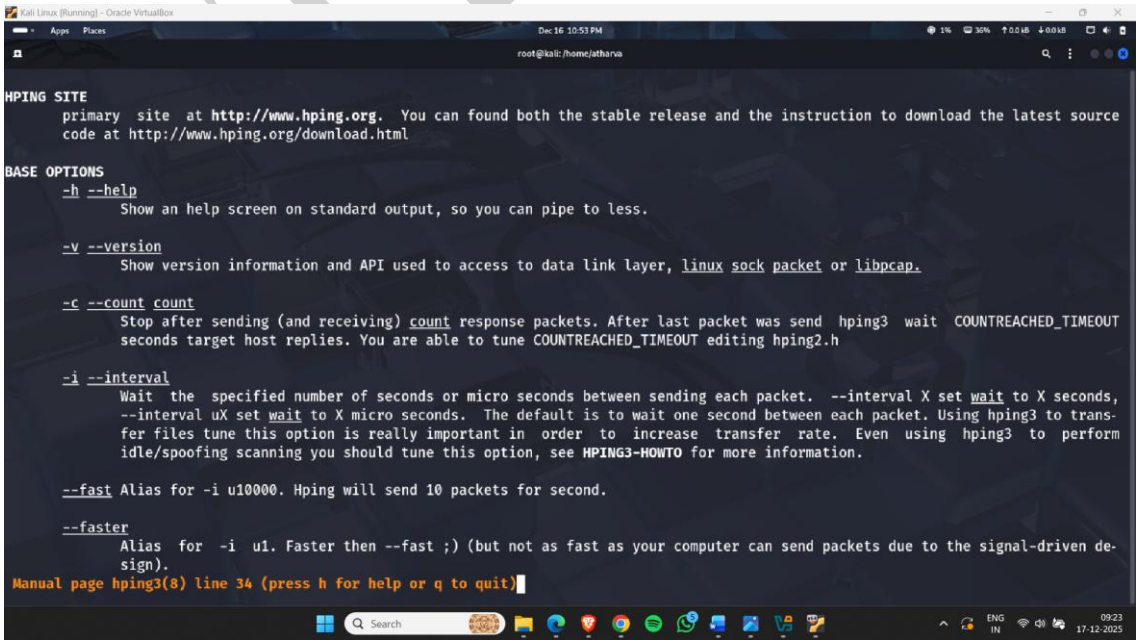


Figure 7

1)--fast

- Sends 10 packets per second.
- Use Case: Good for basic network discovery or testing firewall rules without overwhelming the target or your own CPU. It is slightly more aggressive than the default mode but still very "polite."

Command --: hping3 -1 192.168.1.40 --rand-source -p 80 --fast

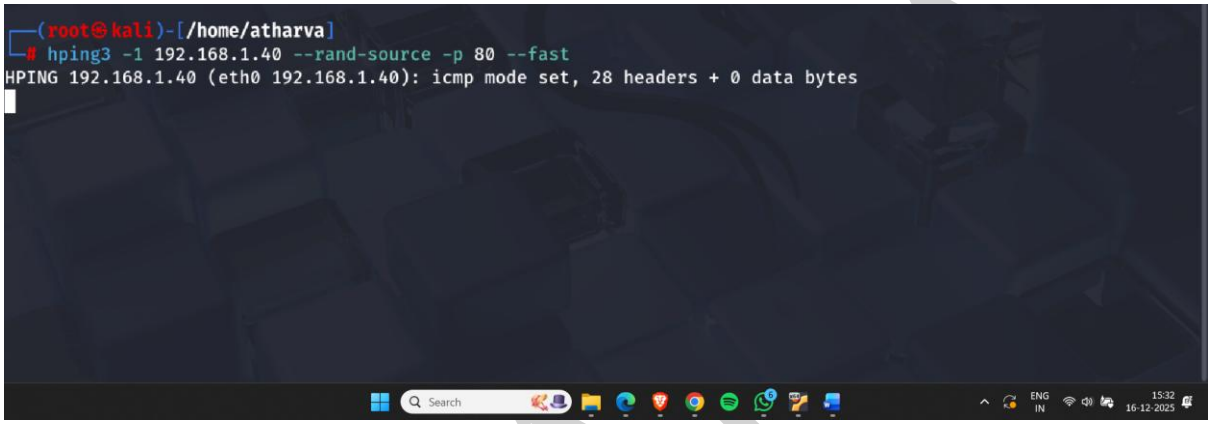


Figure 8

- Open Wireshark to analyse the packets….

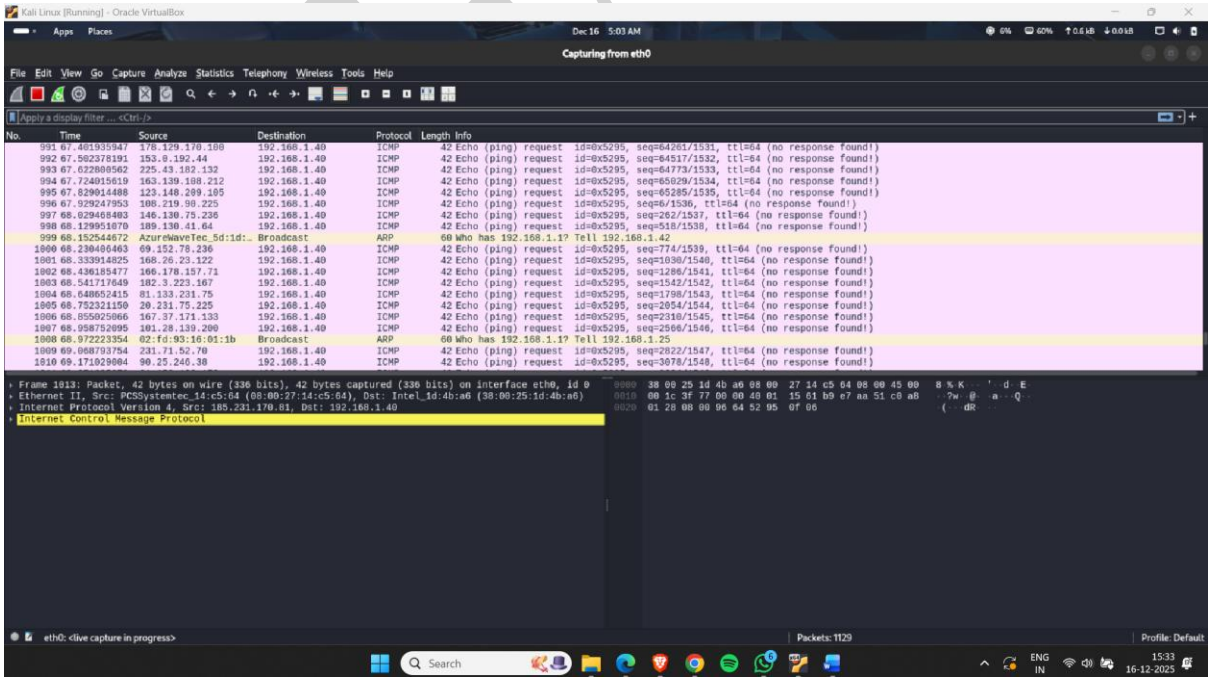


Figure 9

- Packets sent to the Target

2)--faster

- Sends 100 packets per second.
- Use Case: Useful for testing if a network device (like an entry-level router) can handle a moderate stream of traffic. It begins to consume more significant bandwidth and processing power.

Command -- hping3 -1 192.168.1.40 --rand-source -p 80 --faster

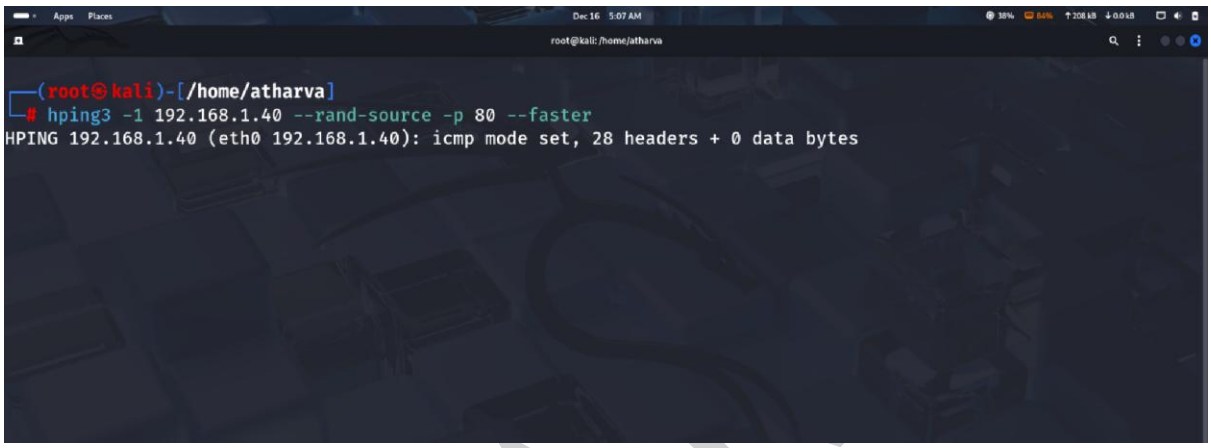


Figure 10

- Open Wireshark to analyse the packets….

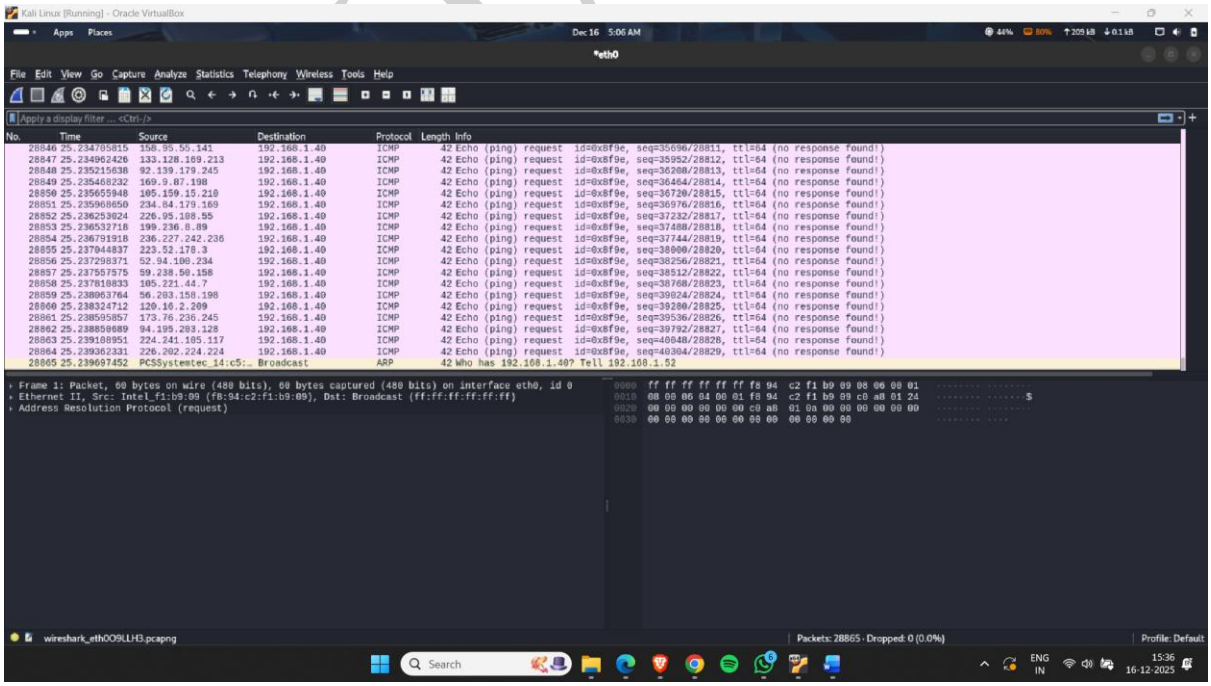


Figure 11

- Packets sent to the Target

3)—flood

- Sends packets as fast as possible (as fast as your CPU and network interface can push them out).
- Mechanism: It does not wait for any incoming replies; it simply blasts the target.This can easily crash a service, saturate a network link, or even cause your own machine to become unresponsive.

Command -: hping3 -1 192.168.1.40 --rand-source -p 80 --flood

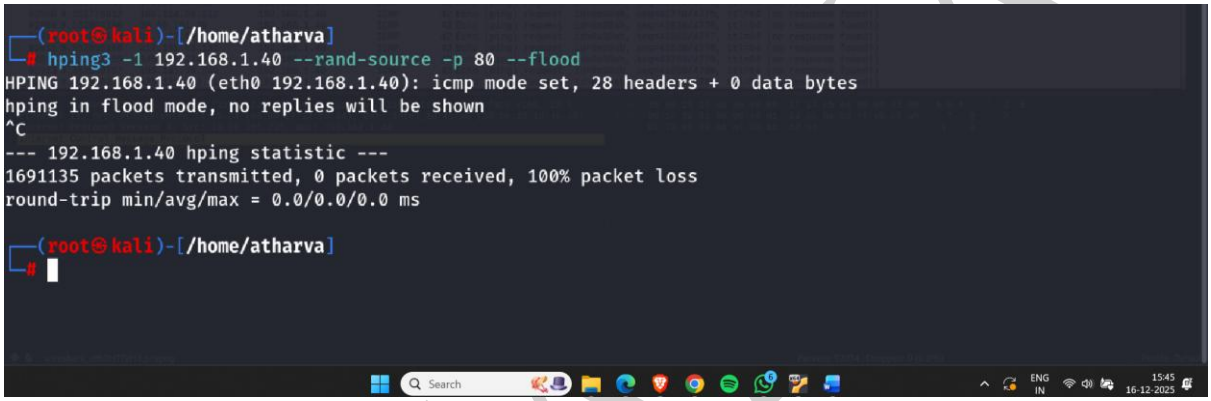


Figure 12

- Open Wireshark to analyse the packets….

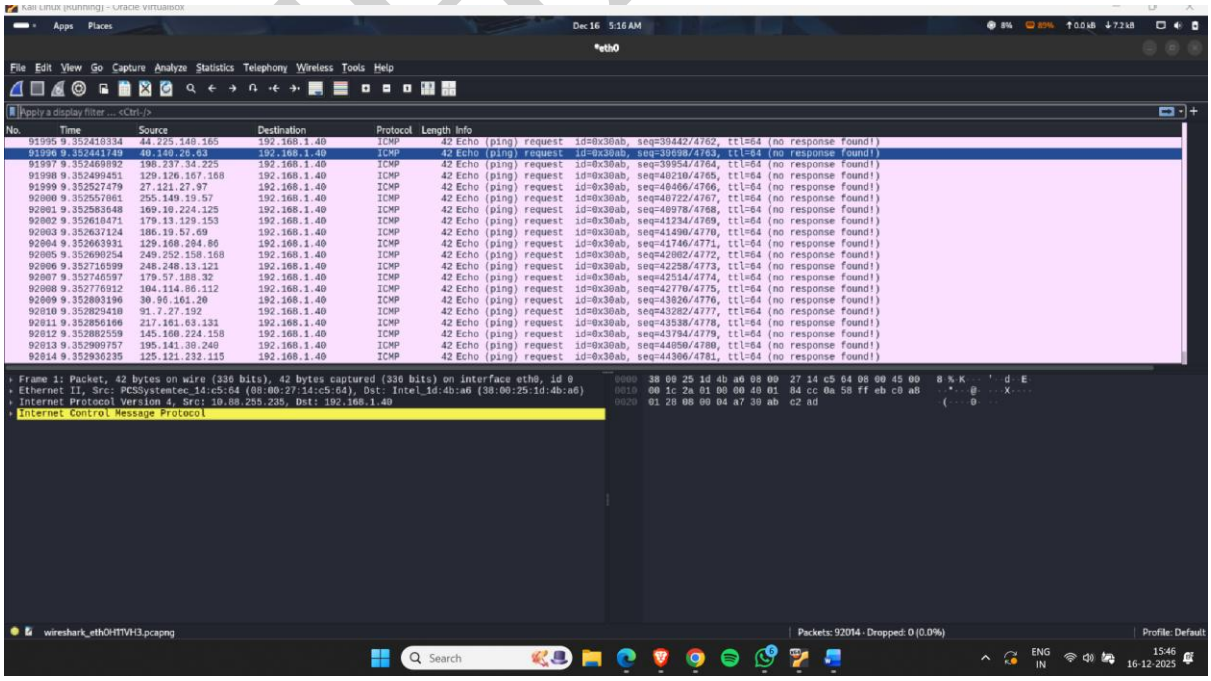


Figure 13

- Packets sent to the Target

Perform DOS/DDOS Using Raven Storm

Raven-Storm is an open-source DoS/DDoS attack tool designed for educational and stress-testing purposes. It's written in Python and allows users to simulate denial-of-service attacks on local networks or lab environments.

How to use it -:

• First download tool from git hub

https://github.com/Tmpertor/Raven-Storm

• After Downloading completed Open kali linux terminal and go to the Raven-Storm Directory

• Use python3 main.py to run raven-storm.

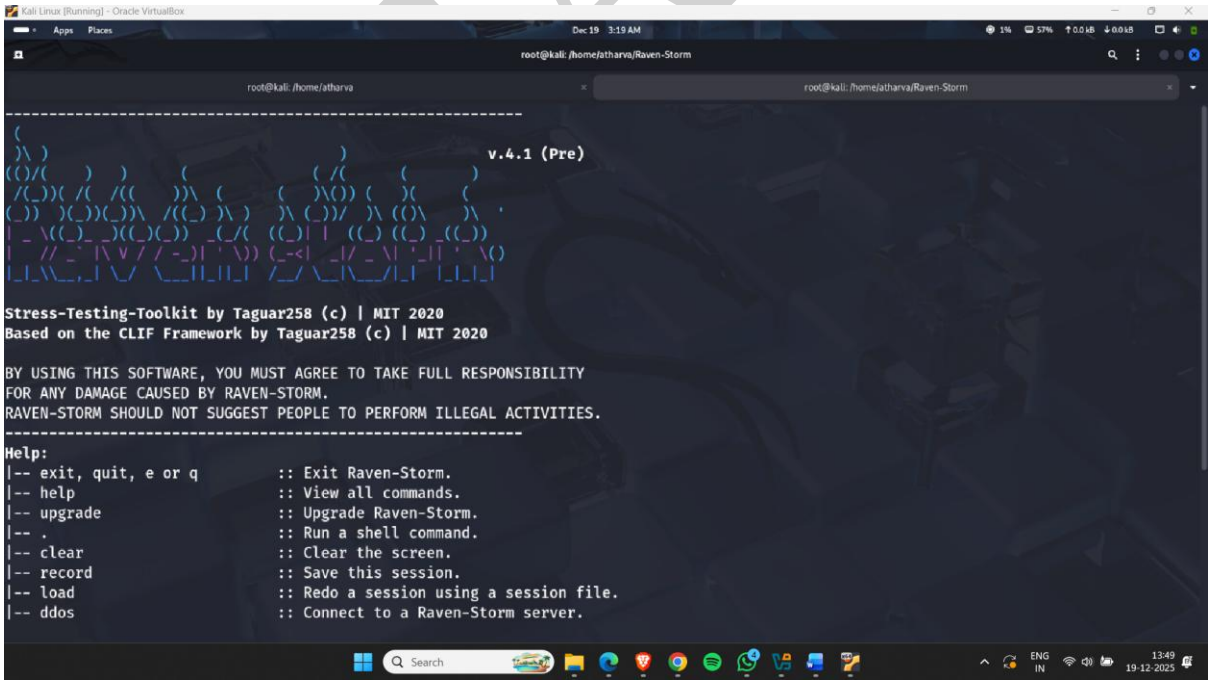


Figure 8

- Use L4 – for layer four attack (transport layer attack)

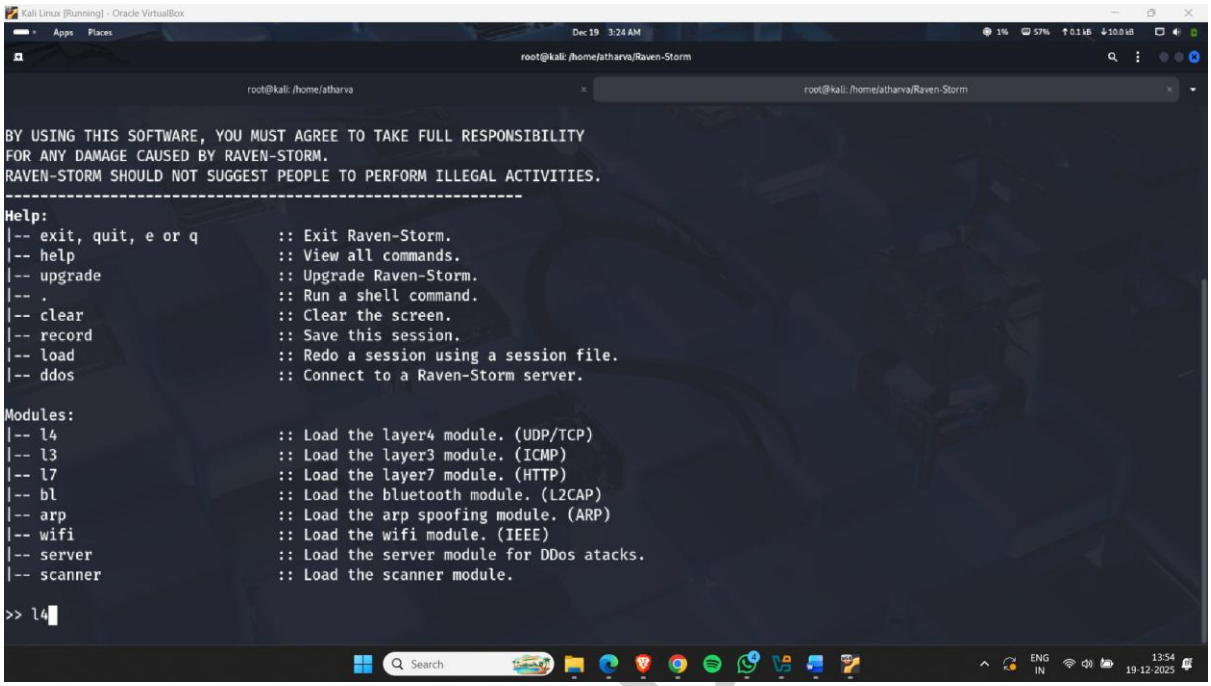


Figure 9

- Set target ip address & Set port number

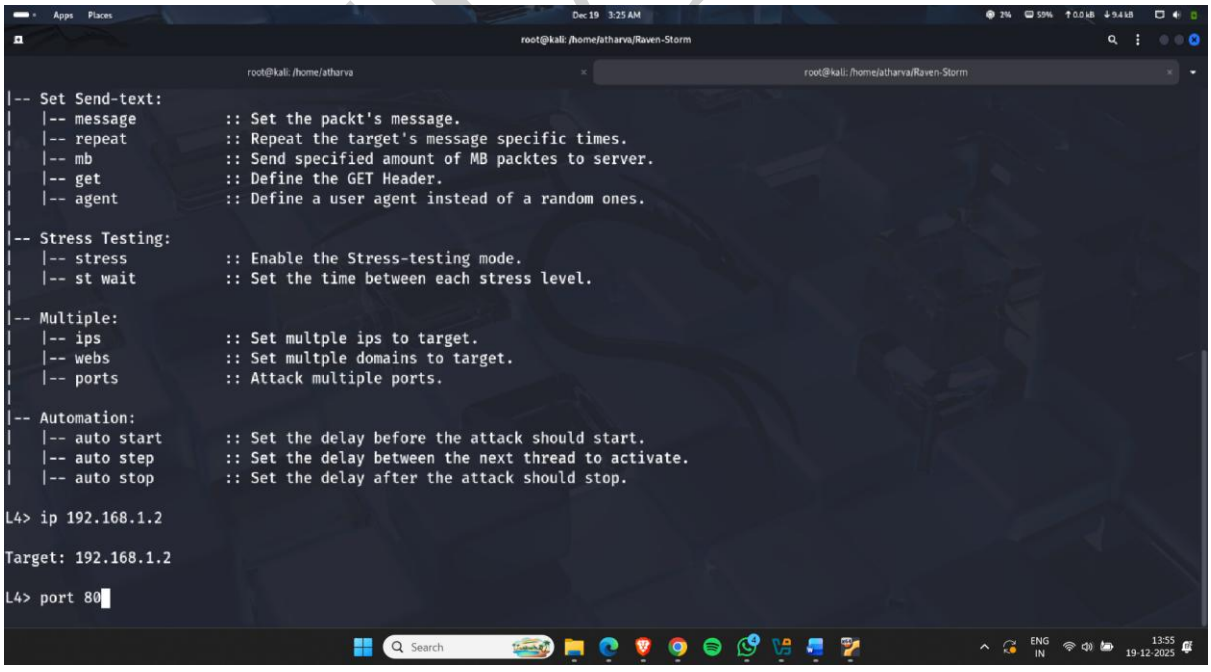


Figure 10

- Set threads & then Run the attack…

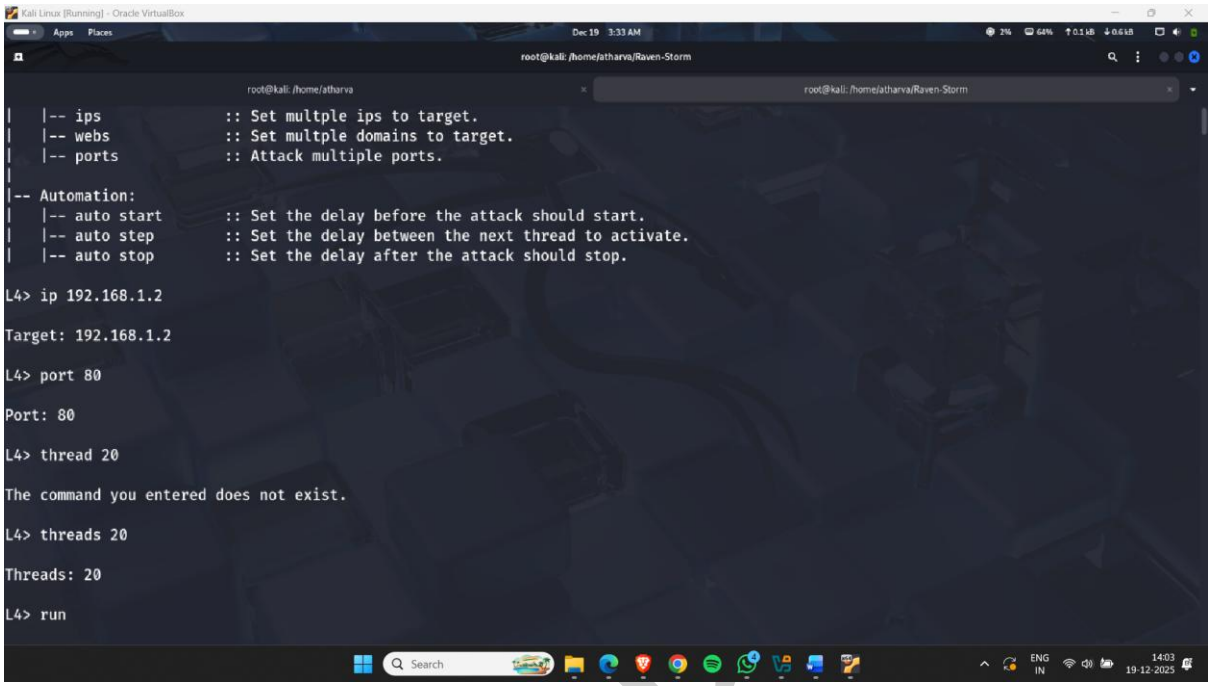


Figure 11

- Open wireshark
- The Wireshark capture shows a high volume of UDP packets targeting DNS port 53, indicating a DNS/UDP Flood attack.

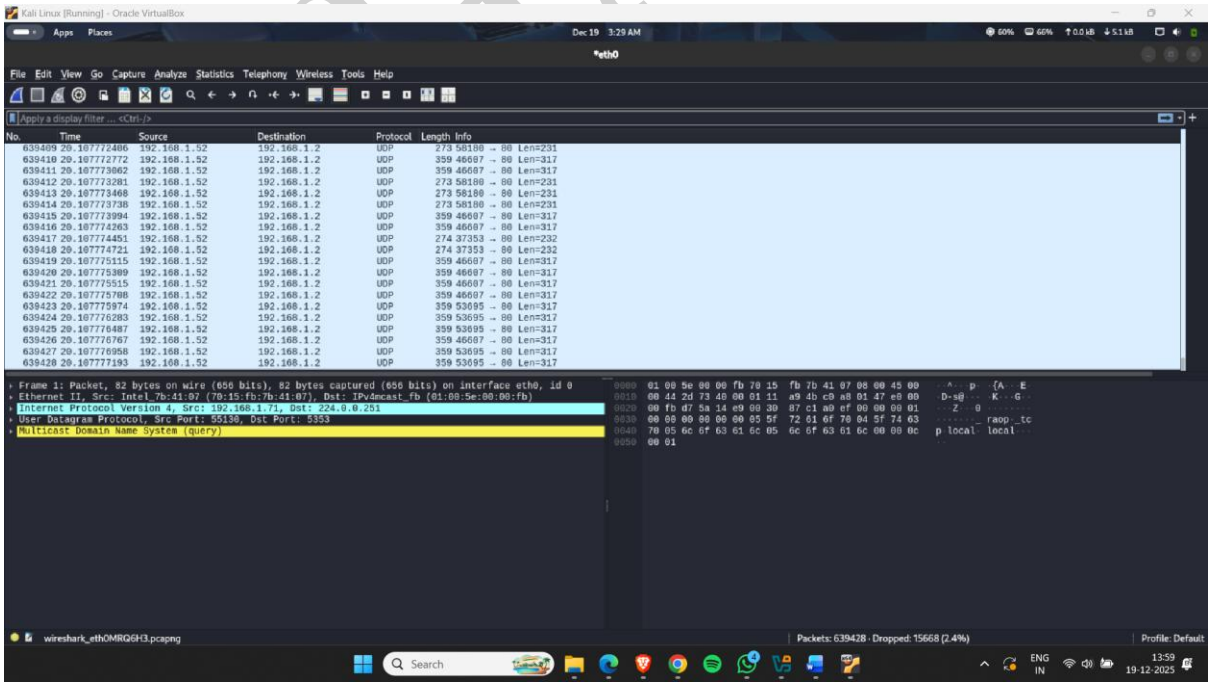


Figure 12

Perform DOS/DDOS Using Slowloris

Slowlorisis a Denial-of-Service (DoS) attack tool that targets web servers by exploiting how they handle connections. It allows one single machine to take down a web server by keeping many connections open and slowly sending partial HTTP requests, never completing them.

How to use it -: Open kali linux terminal and type slowloris

Slowloris<target ip>

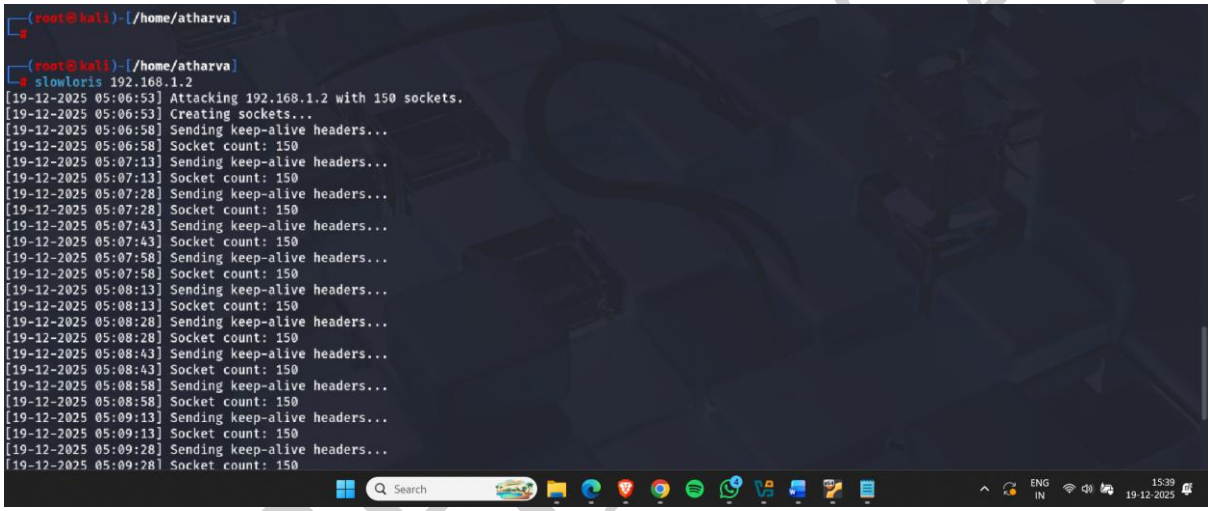


Figure 13

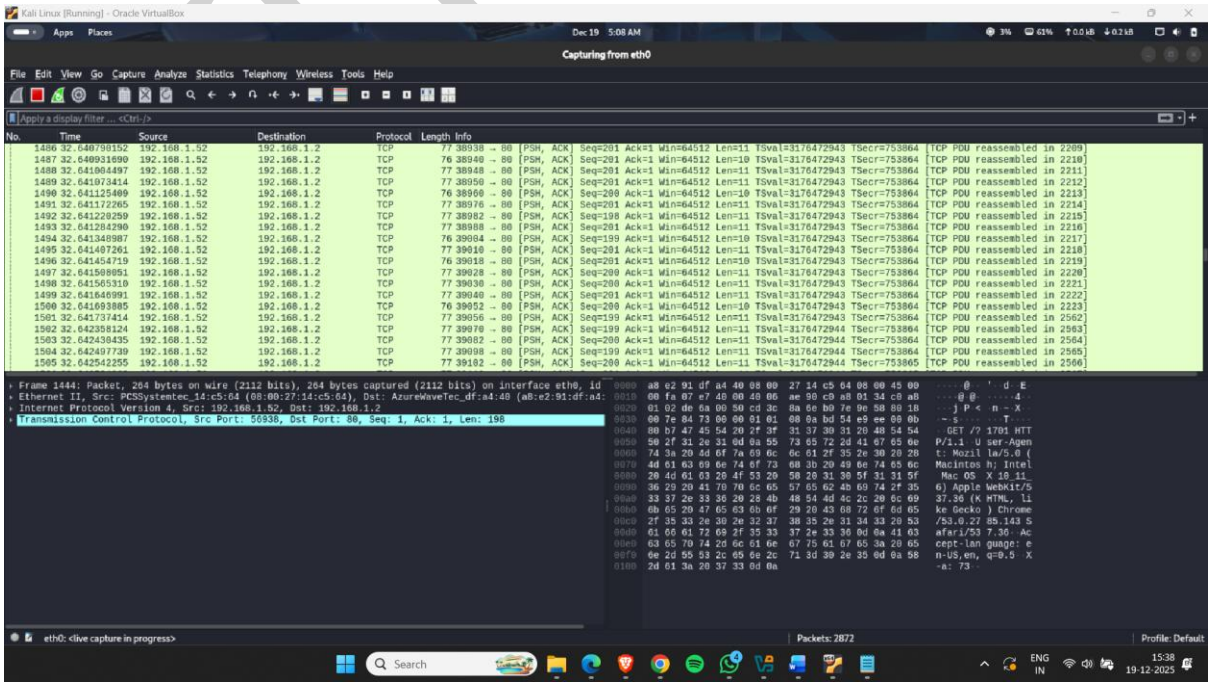


Figure 14

Perform DOS/DDOS Using LOIC

LOIC stands for Low Orbit Ion Cannon — it is an open-source DoS (Denial of Service) attack tool that is used to flood a target with massive amounts of TCP, UDP, or HTTP requests, causing the target server to slow down or crash.

Originally developed for network stress testing, it became widely known when it was used by hacktivist groups like Anonymous in large-scale DDoS attacks.

Download link: https://sourceforge.net/projects/loic/

How to use it –:

- After installation open the app

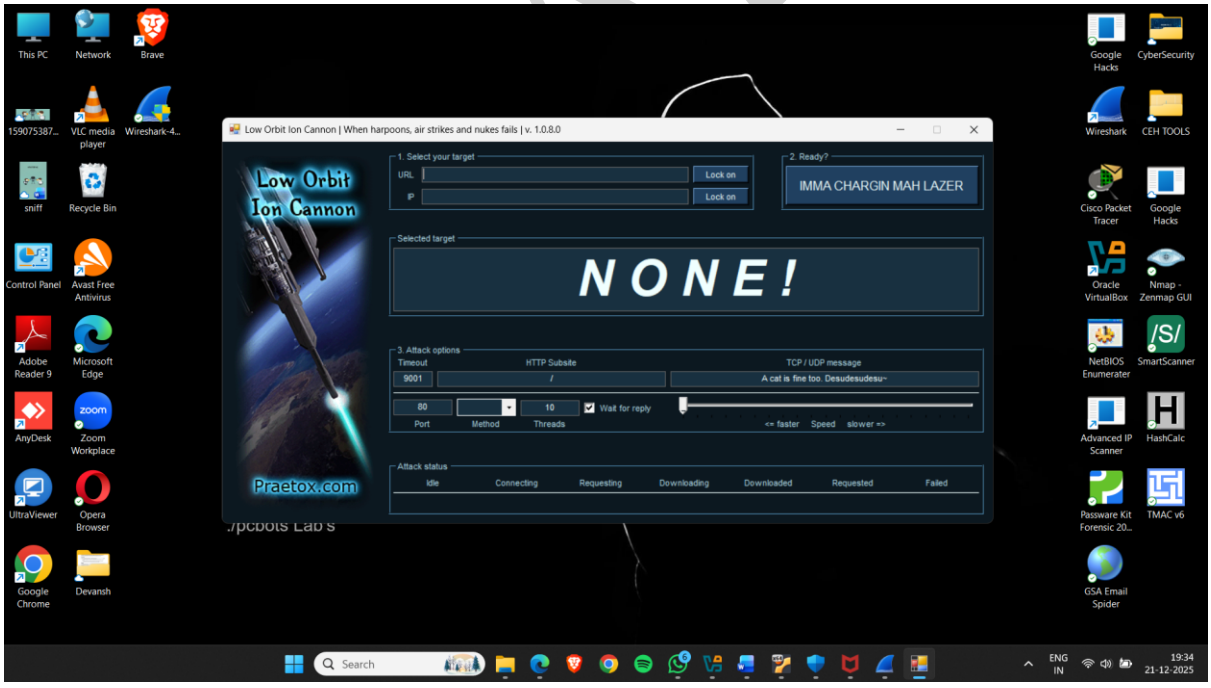


Figure 15

- Now open LOIC and enter url to start dos attack.
- Enter url or ip address and tap on lockon.

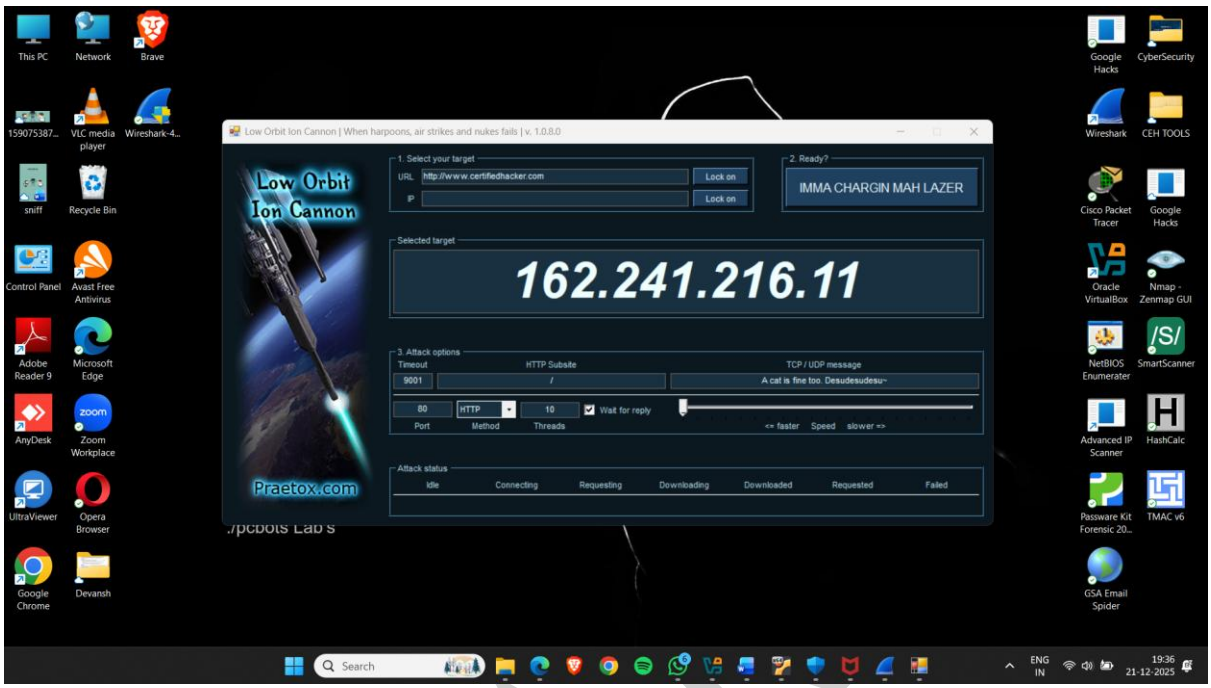


Figure 16

- Set method you want to select.
- Set threads and then click of **IMMA CHARGIN MAH LAZER.**

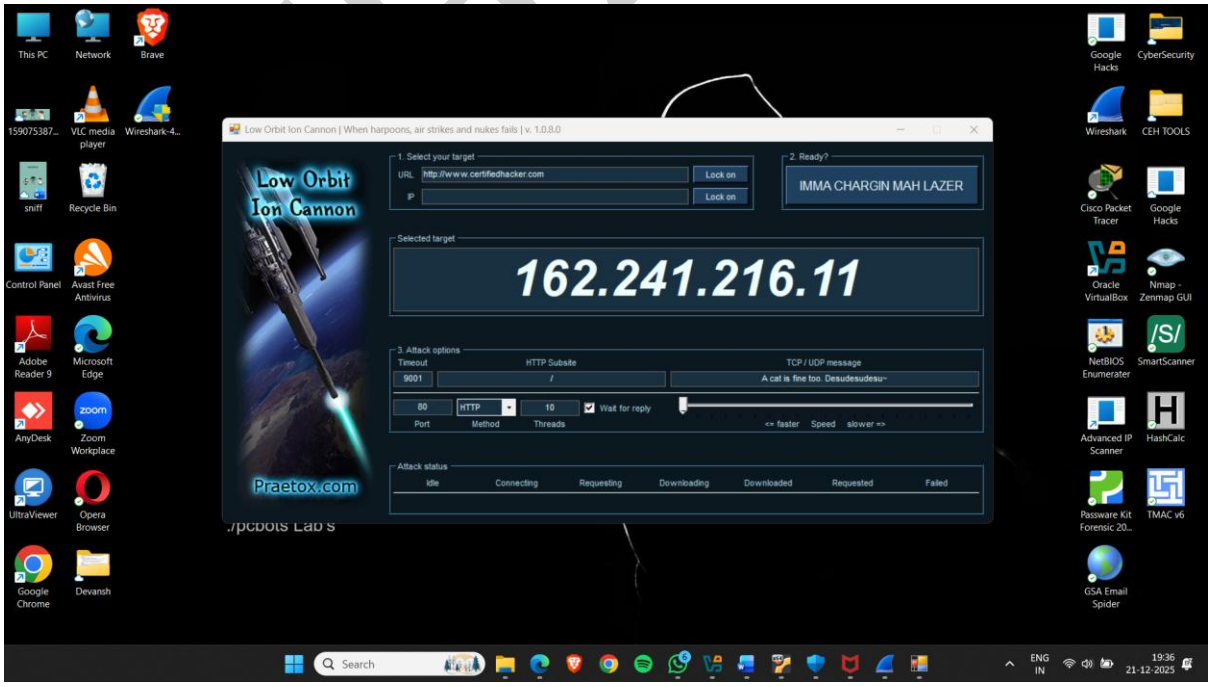


Figure 17

- Now open wireshark for monitoring packets

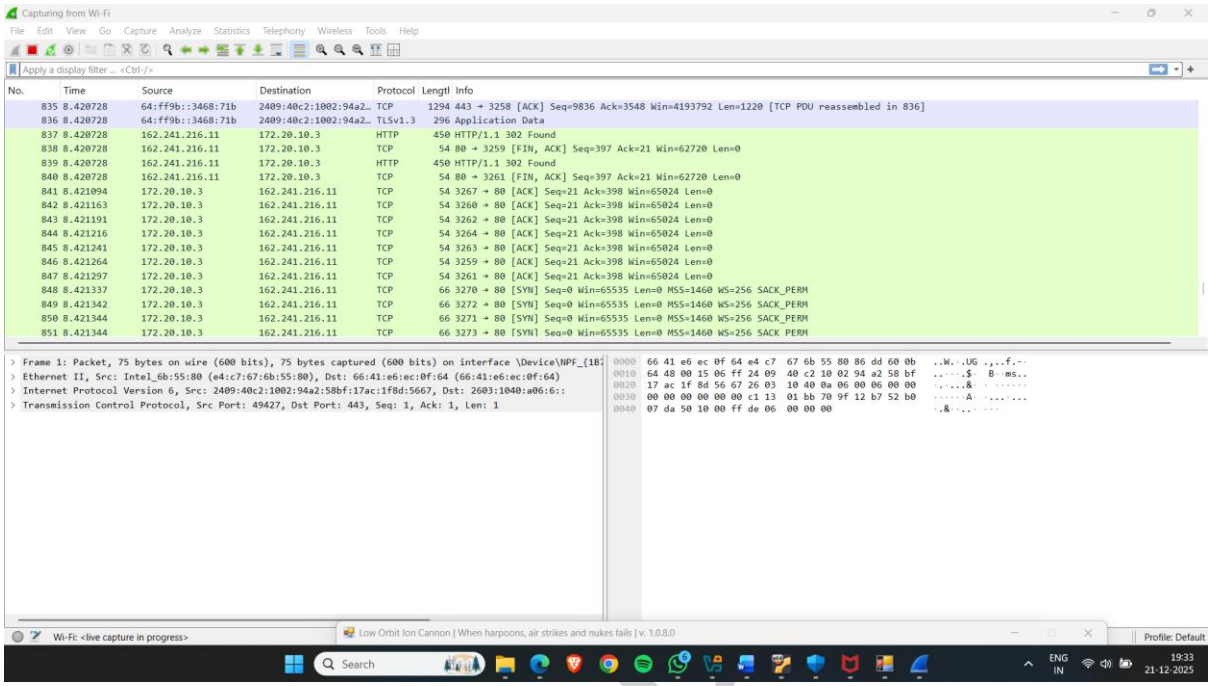


Figure 18

- **<u>Important note-:</u>**

✓ LOIC **does NOT hide the attacker's IP**
✓ Using it on real targets **without permission is illegal**
✓ Should be used **only for educational or authorized testing**
✓ Makes website slow or unavailable
✓ Can be used in **single-user mode** or **coordinated attacks.**
✓ **Floods TCP / UDP / HTTP packets** to a target IP or website.
✓ Perform **DoS attack** by sending a huge number of requests

Perform DOS/DDOS Using HOIC

HOIC (High Orbit Ion Cannon) is a powerful DoS (Denial of Service) tool designed to launch HTTP flood attacks against web servers. It is an advanced version of the LOIC (Low Orbit Ion Cannon) tool but with a more powerful and distributed attack mechanism. It is primarily used for flooding web servers with HTTP requests to overload and crash the target system.
HOIC is popular in the hacktivist community and has been used in large-scale DDoS (Distributed Denial of Service) attacks.

Download : https://sourceforge.net/projects/high-orbit-ion-cannon/

How to use it - : After installation open the app

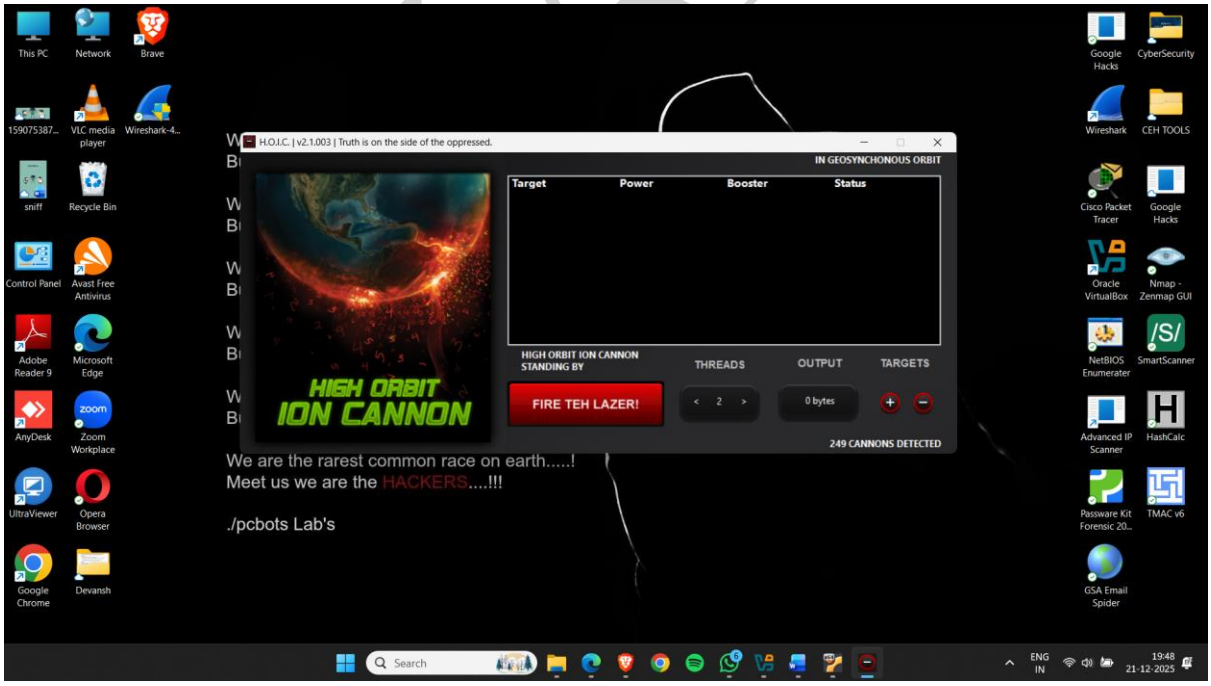


Figure 19

- Click on plus button and add target url.
- Click on add button then add url and set power &click on add.

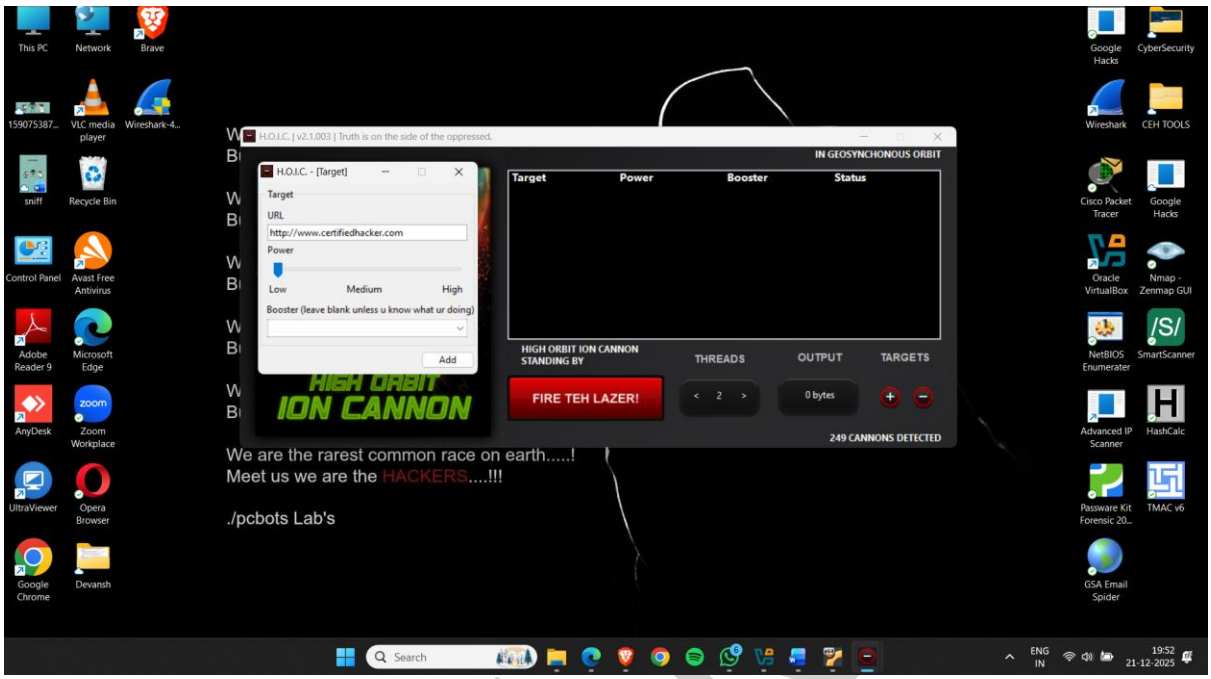


Figure 20

- Now adjust threads & click on **FIRE THE LAZER!**

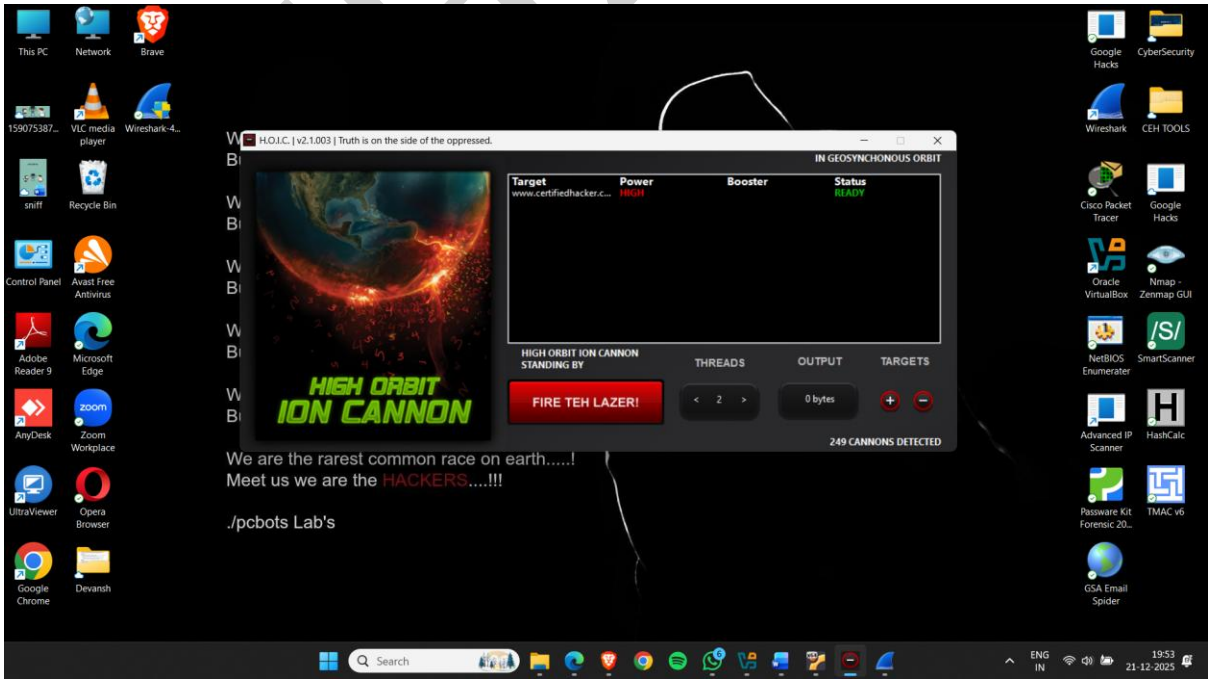


Figure 21

- Attack started…

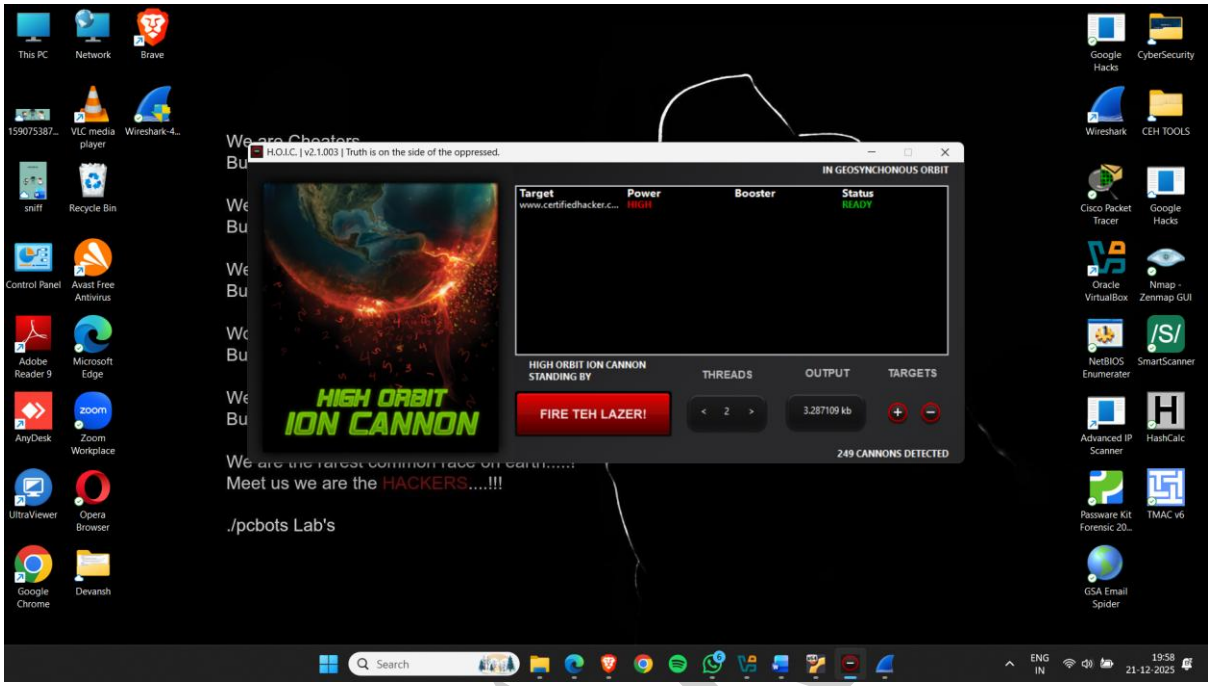


Figure 22

- Now open wireshark for monitoring attack.

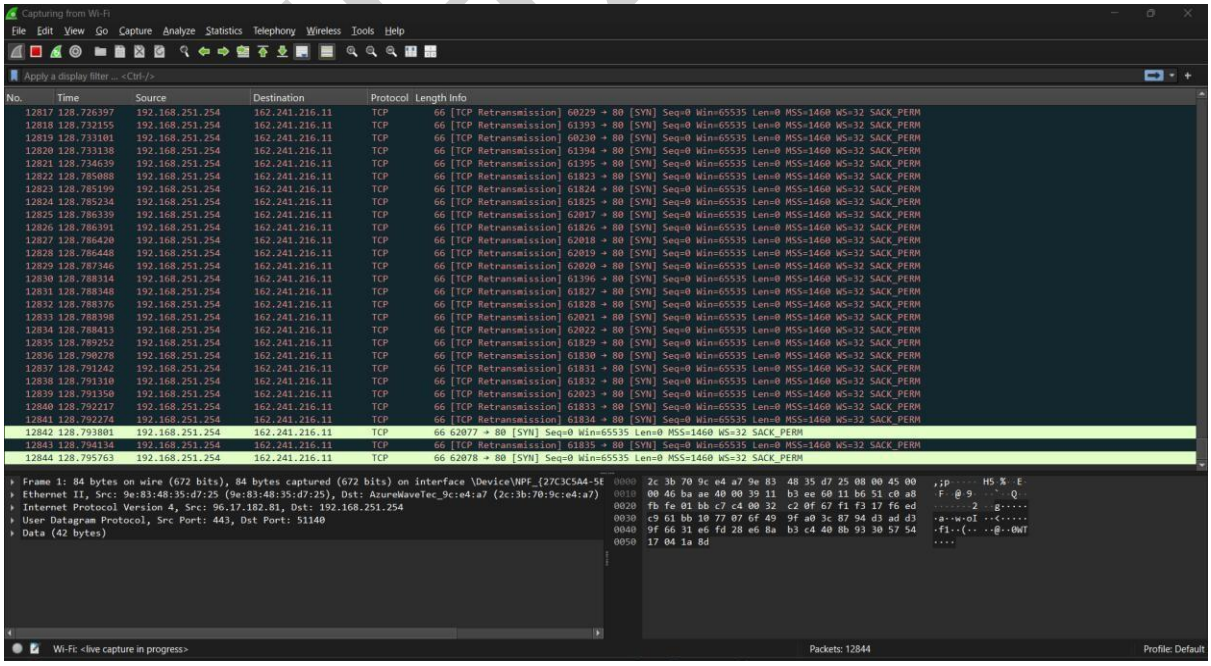


Figure 23

Perform DOS/DDOS Using Macof

Macof is a MAC flooding tool from the dsniff suite used in cybersecurity labs to perform Layer 2 attacks on switches.
It generates thousands of fake MAC addresses to overflow the switch CAM table, forcing the switch to act like a hub.

How to use it - :

- Open kali linux
- Type sudo apt install macof
- Now start attack using macof
  Command -: macof -I eth -d<target ip>
  Target: certifiedhacker.com

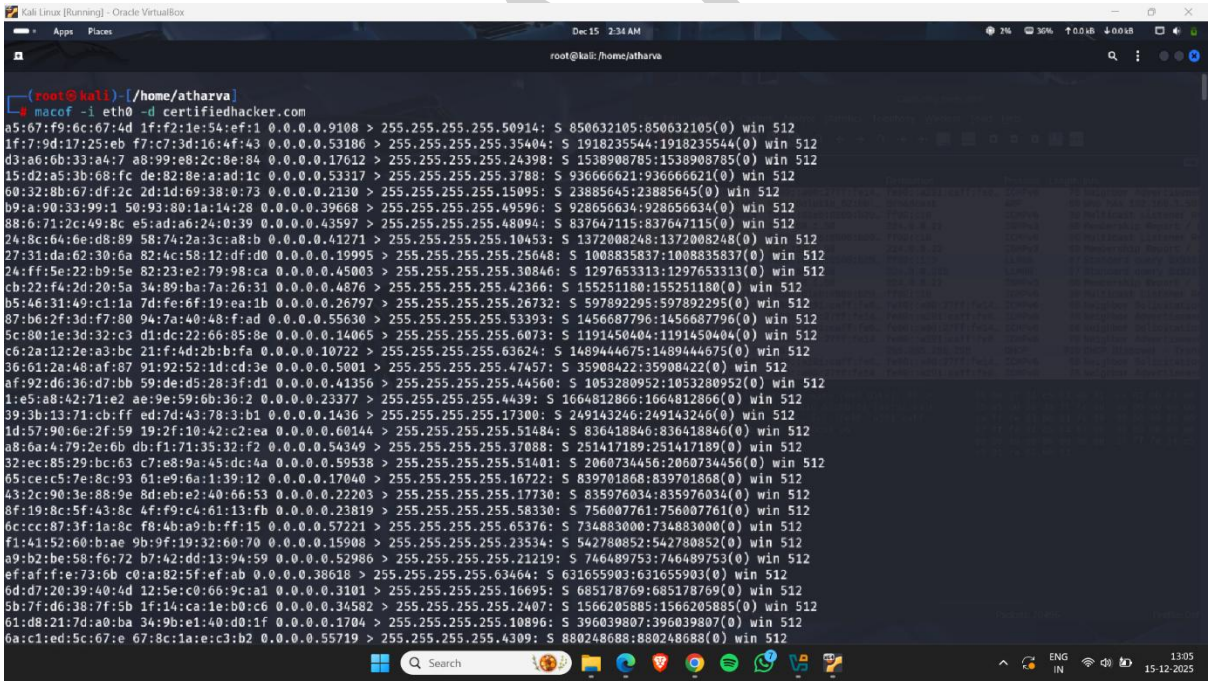


Figure 24

- Open Wireshark and monitor the Attack

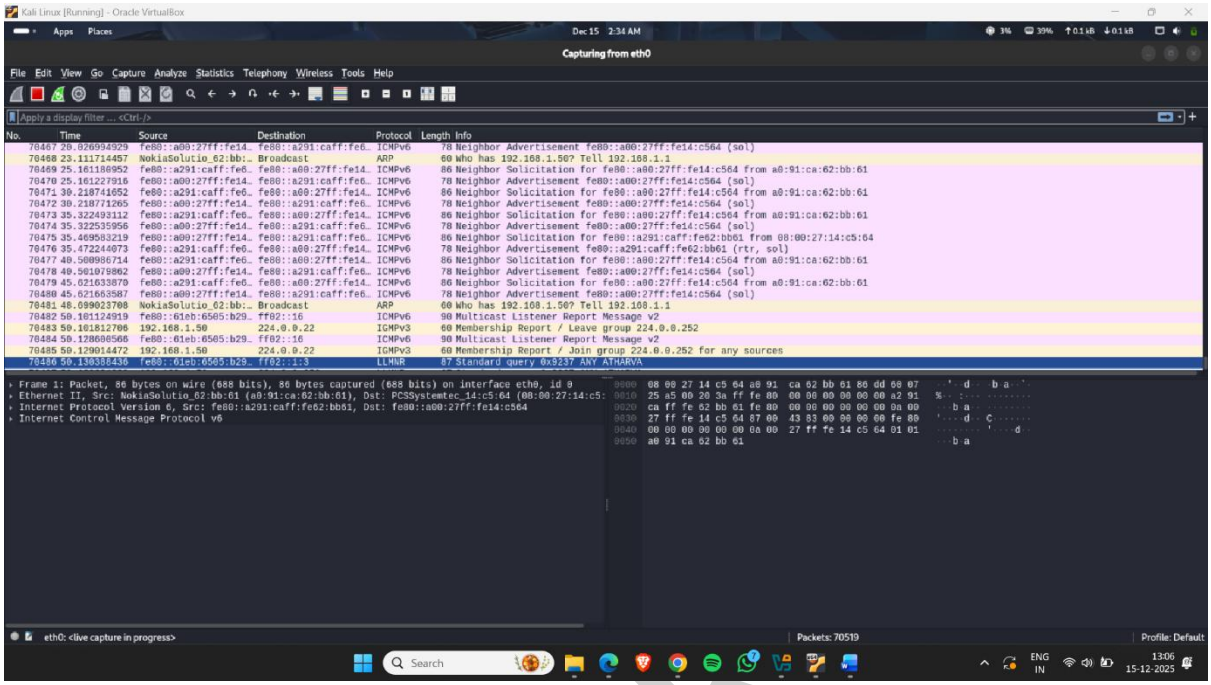


Figure 25

HOW TO PREVENT FROM DOS AND DDOS ATTACK

Preventing DoS and DDoS attacks requires a combination of network hardening, traffic filtering, resource scaling, and incident response planning. Here's a breakdown of effective prevention and mitigation strategies:

1. Network-Level Protection

- **Firewall Rules**: Block unused ports and restrict access to critical services.
- **Rate Limiting**: Limit the number of requests from a single IP address.
- **Geo-blocking**: Block or limit traffic from high-risk regions if not needed.
- **Intrusion Prevention Systems (IPS)**: Detect and stop suspicious traffic.

2. Use Anti-DDoS Services

- **CDN & Cloud Protection**: Use services like:
  - **Cloudflare** o **AWS Shield** o **Google Cloud Armor**
  - **Azure DDoS Protection**
- These services absorb large-scale traffic before it reaches your server.

3. Application-Level Defenses

- **Web Application Firewall (WAF)**:
  - Blocks malicious HTTP traffic (e.g., HTTP floods).
  - Helps filter bad bots and SQL injection attempts.
- **Captcha/Challenge Pages**:
  - Stops automated traffic during attacks (e.g., Cloudflare "I'm Under Attack" mode).

4. Monitoring & Detection

- **Log Monitoring**:
  - Use tools like **Splunk**, **ELK Stack**, or **Graylog** to analyze traffic.
- **Traffic Anomaly Detection**:
  - Alerts if traffic spikes suddenly or unusual patterns are found.
- **Tools**:
  - Wireshark, NetFlow, SNORT, or Suricata can help detect unusual traffic.

5. Infrastructure Design

- **Redundancy & Load Balancing**:
  - Distribute traffic across multiple servers or data centers.
- **Auto-scaling**:
  - Cloud services can automatically scale up during spikes.
- **Separate Public & Private Services**:
  - Keep critical services (like admin panels or internal APIs) on separate networks.

6. Use Reverse Proxies

- Acts as a buffer between users and servers.
- Helps hide the real IP of your web server.

7. Have an Incident Response Plan

- Define steps to follow during an attack.
- Have contact points for your ISP and DDoS mitigation providers.
- Set up alerting systems and regular backups.

Tools for Testing (Ethical Use Only)

- **LOIC**, **HOIC**, **Slowloris**, **Hping3**, **D0sinator** – for lab simulations.
- Test only in **controlled environments** (CTFs, home labs, VMs).