Name : kunal Jawale

Module 10 : Denial of Service

Dos (denial of service) :-

A **DoS (Denial of Service) attack** is a type of cyberattack where the attacker seeks to make a computer, network, or service unavailable to its intended users by overwhelming it with a flood of traffic or exploiting vulnerabilities.

Types of DoS Attacks:

1. **Volume-Based Attacks**
   - Floods the target with massive amounts of data.
   - Example: UDP flood, ICMP flood, etc.
2. **Protocol Attacks**
   - Exploit weaknesses in layer 3 and layer 4 protocols.
   - Example: SYN flood, Ping of Death.
3. **Application Layer Attacks**
   - Target the layer where web pages are generated.
   - Example: HTTP flood.

A denial-of-service (DoS) attack is a cyberattack where an attacker disrupts the normal functioning of a computer or network by overloading it with traffic, rendering it inaccessible to legitimate users. These attacks aim to make a resource, like a website or server, unavailable for its intended purpose.

How it Works:

- **Overloading:**

  Attackers flood the target with excessive requests or traffic, exceeding its capacity to handle legitimate requests.

- **Resource Exhaustion:**

  DoS attacks can exhaust the target's resources, such as memory, processing power, or network bandwidth, making it unavailable.

- **Disruption of Service:**
  The overwhelming traffic disrupts the normal flow of data, preventing legitimate users from accessing the service.

Types of DoS Attacks:

- **Network DoS:**

  Floods the target with network traffic, often using spoofed IP addresses to mask the source.

- **Application DoS:**

  Targets specific applications or services, such as websites or web applications, by exploiting vulnerabilities in the application code or protocols.

- **Volume-Based DoS:**

  Uses large amounts of network traffic to exhaust the target's bandwidth.

- **Resource Exhaustion DoS:**

  Overloads the target's resources, such as memory or CPU, to cripple its performance.

- **Distributed DoS (DDoS):**
  A type of DoS attack where the traffic comes from multiple sources, often using a network of compromised computers (botnets).

Examples:

- A hacker flooding a website with fake traffic to make it inaccessible to legitimate users.
- Sending a large number of email messages to a server, causing it to crash.
- Exploiting a vulnerability in a network service to crash it.

Defense:

- **Firewalls:** Filter network traffic and block malicious requests.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Detect and prevent DoS attacks.
- **Load Balancing:** Distributes traffic across multiple servers, preventing any single server from being overwhelmed.
- **Content Delivery Networks (CDNs):** Distribute content across multiple servers, making it harder to target a single server.
- **Rate Limiting:** Restricts the number of requests a user or IP address can make within a given time period.

Name : kunal Jawale

DDOS Attack :-

A DDoS (Distributed Denial-of-Service) attack is a cyberattack where an attacker uses multiple compromised systems to overwhelm a target network, service, or website with traffic, making it unavailable to legitimate users. This is done by flooding the target with malicious traffic, such as fake connection requests or data packets, which exhausts the target's resources and prevents it from responding to real users.

Here's a more detailed breakdown:

- **How it works:**

  Attackers use a network of compromised devices, often referred to as a botnet, to launch the attack. These devices, unknowingly controlled by the attacker, send massive amounts of traffic to the target.

- **Impact:**

  DDoS attacks can cause significant disruptions to online services, including websites, applications, and network infrastructure. This can lead to downtime, loss of revenue, damage to reputation, and customer dissatisfaction.

- **Types of attacks:**

  DDoS attacks can vary in their approach and the layer of the network they target. Some common types include volumetric attacks, which overwhelm the target with traffic, and application-layer attacks, which target the target's application logic.

- **Mitigation:**

  Organizations can take steps to protect against DDoS attacks, such as implementing robust security measures, using DDoS protection services, and regularly monitoring network traffic.

- **Legal consequences:**
  Participating in DDoS attacks or using DDoS-for-hire services is illegal and can be investigated by law enforcement agencies like the FBI.

In essence, a DDoS attack is a cyberattack designed to disrupt online services by overloading them with traffic, making them unavailable to legitimate users.

Name : kunal Jawale

DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

/ Here we perform the DDOS attack using ISB (i`m so bored)

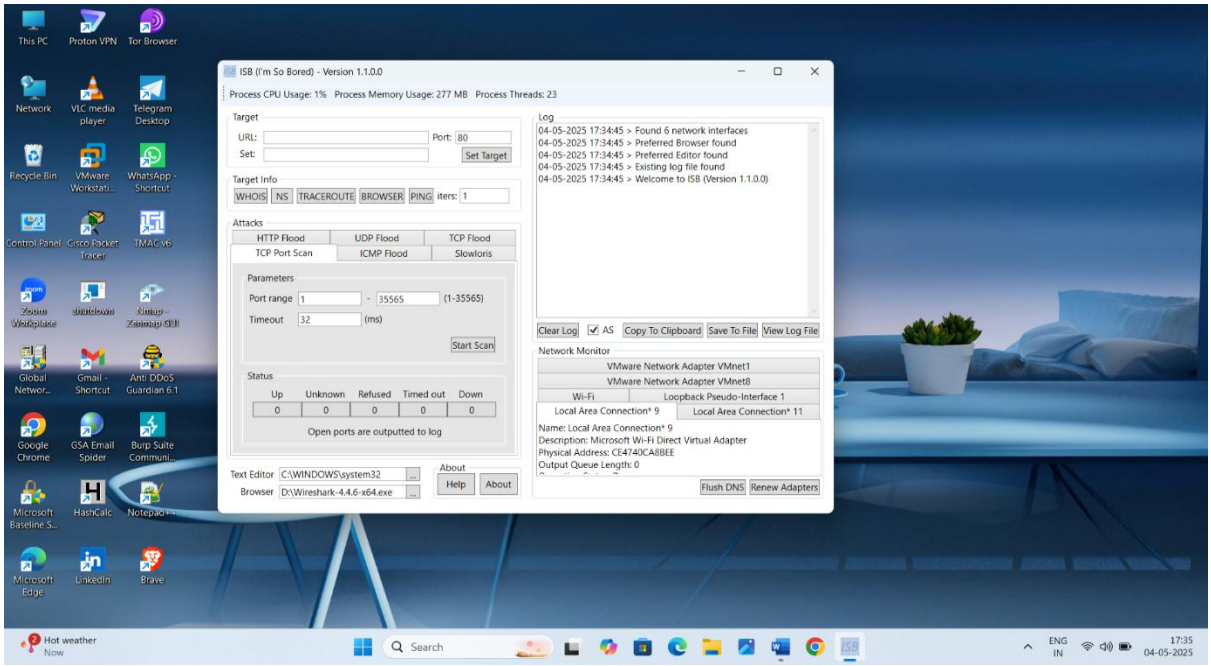
ISB :-

ISB stands for im so bored . this tool is usually used for do some dos /ddos attack on the target. This attack is illegal in india and both of countries this attack does not collect any information about the target . this attack is only use for down some network or website for no motive .

Here we show the lab

Step 1 : download ISB

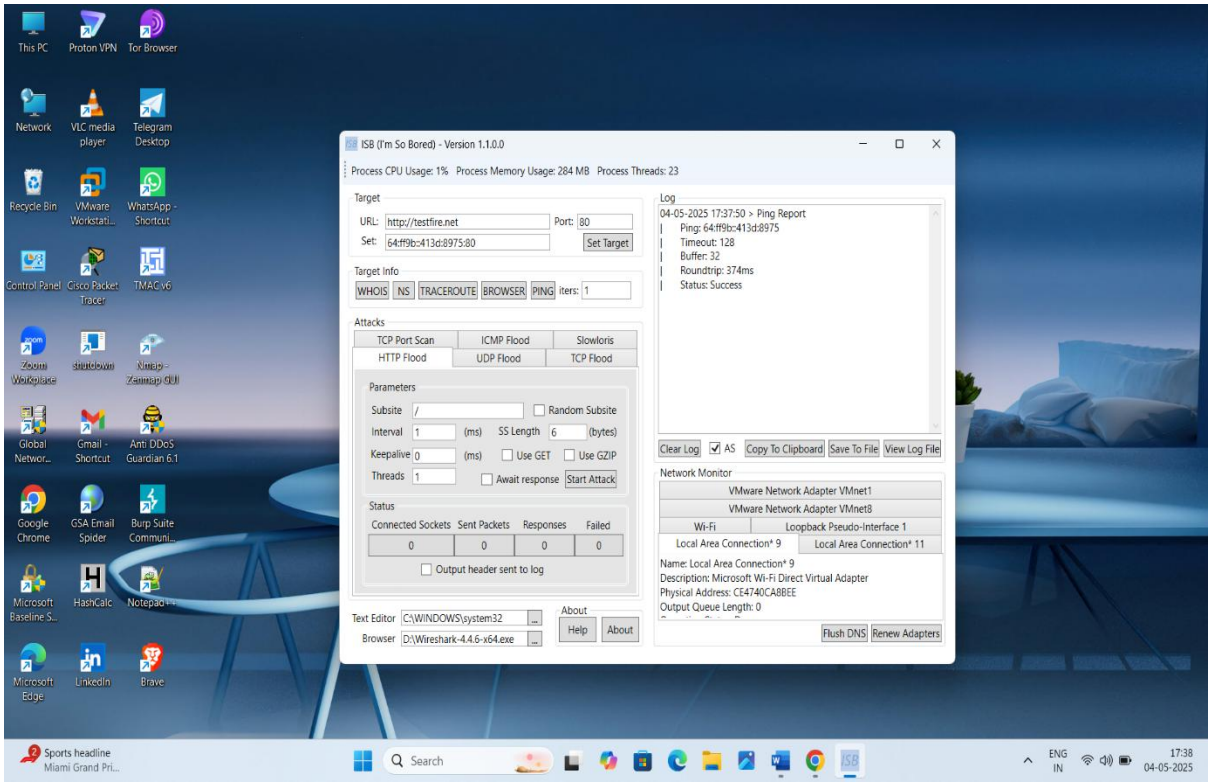
Step 2: open the ISB.exe



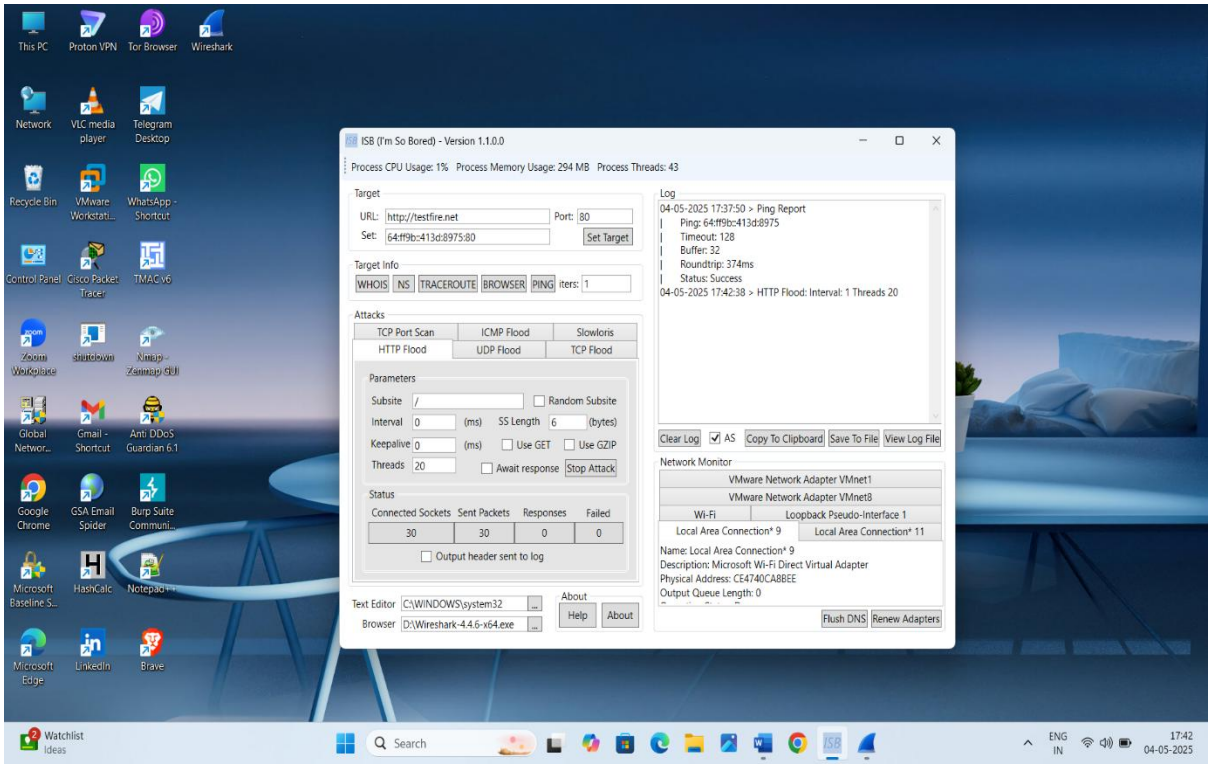
Name : kunal Jawale

Step 3 : click the set target

Step 4 : go for which type of attack you do I go for http

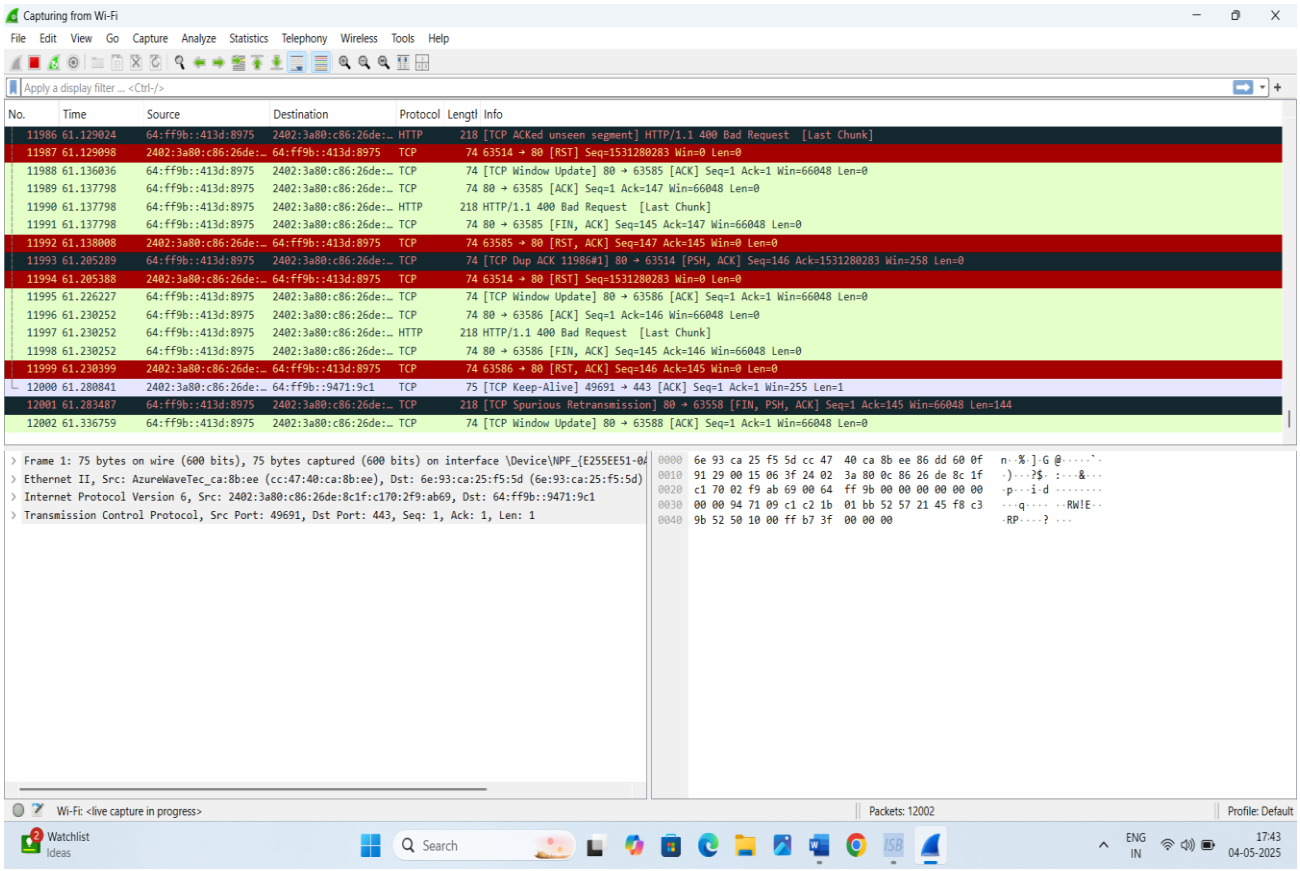


Step 5 : click on start attack then attack is start



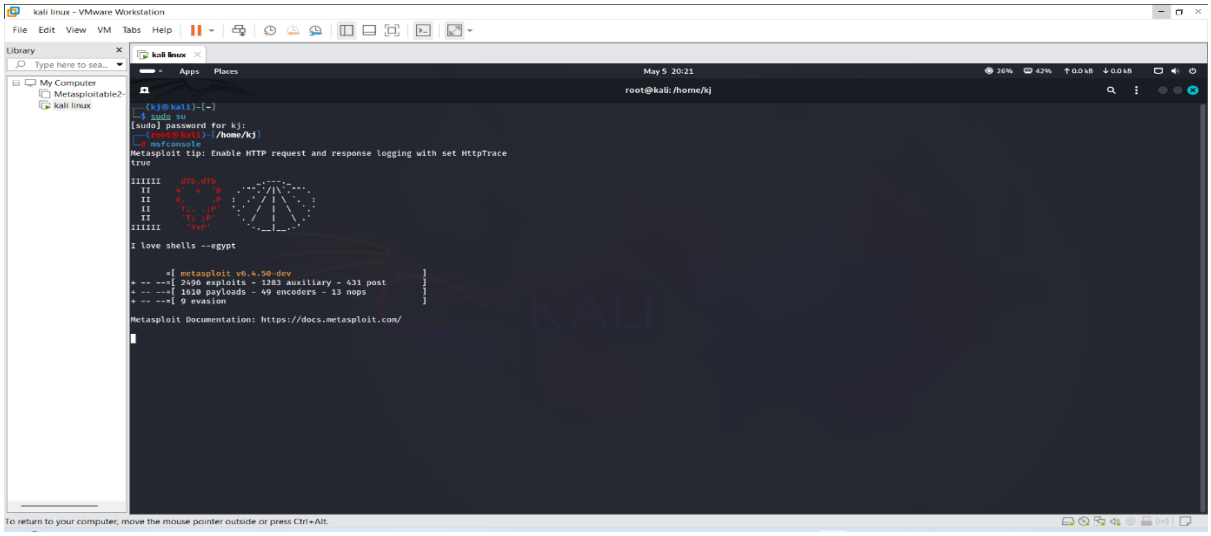
Name : kunal Jawale

Step 6: run wireshark and see attack is running on target .



/ perform DDOS attack using Botnet

Step 1 : on kali linux and run msfconsole



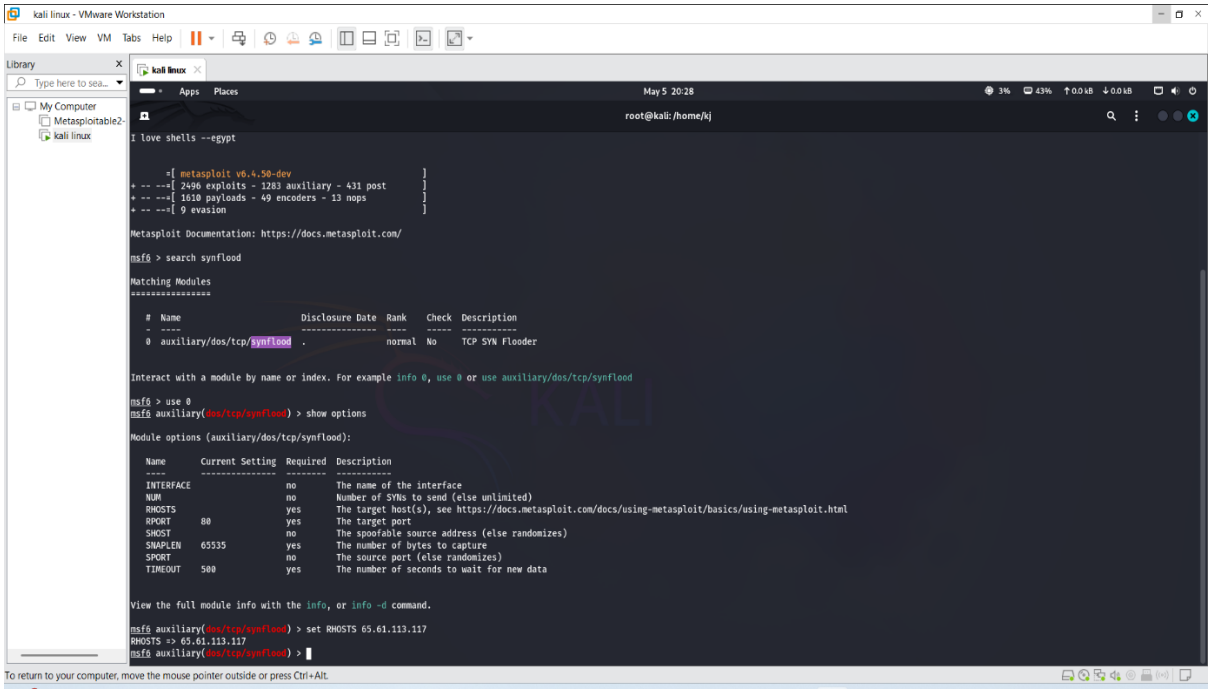
Name : kunal Jawale

Step 2 : search synflood

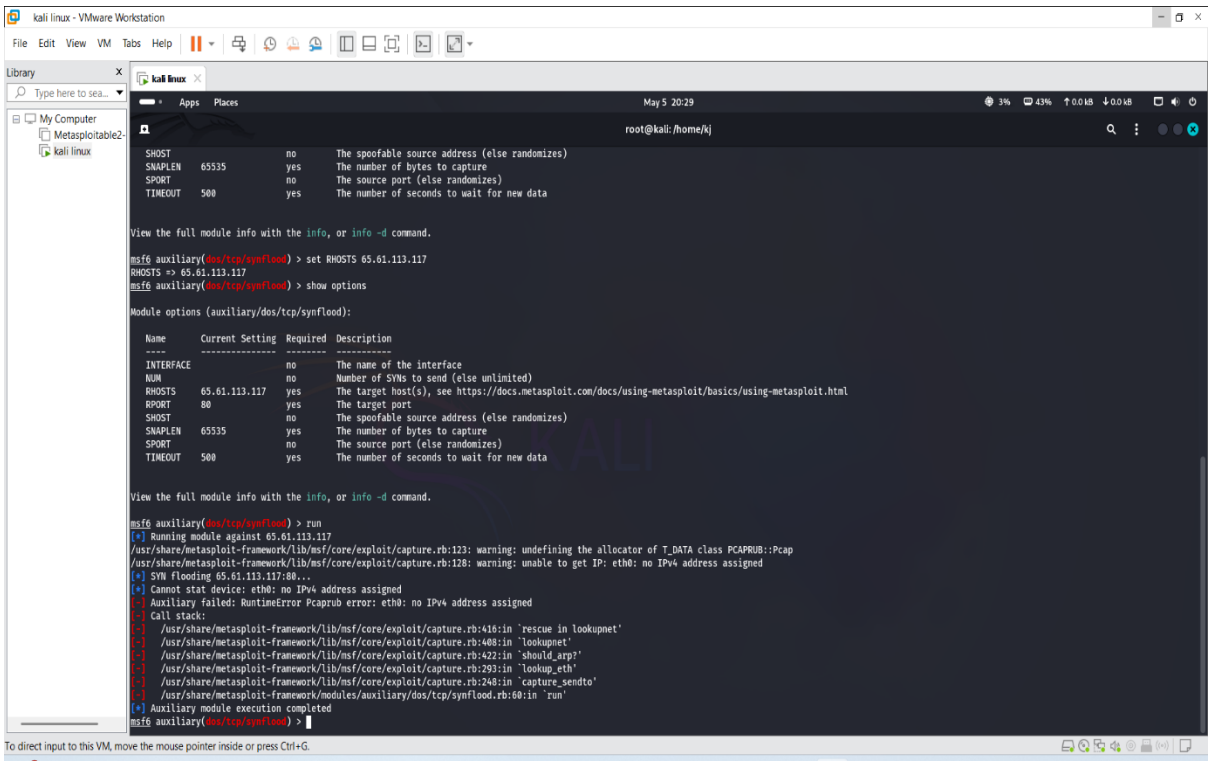
Use 0

Step 3 : show options

Step 4 : set RHOSTS

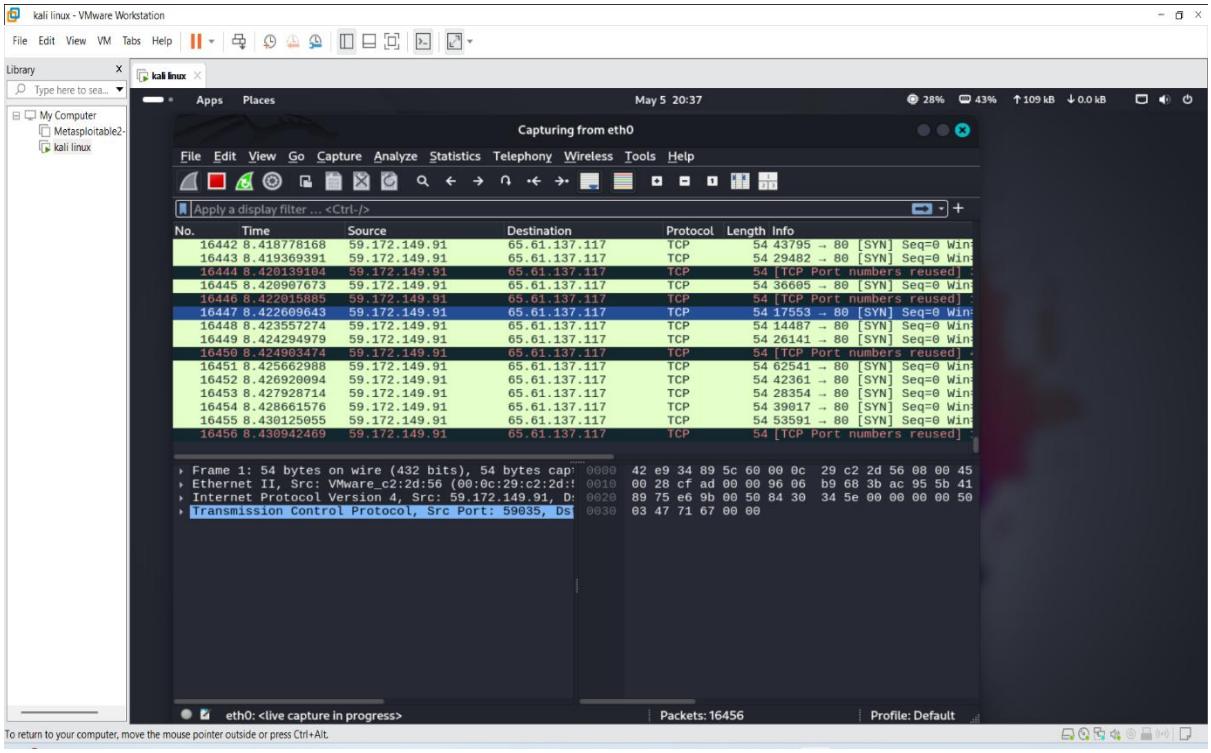


step 6 : run



Name : kunal Jawale

Step 7 : run wireshark and see attack is running

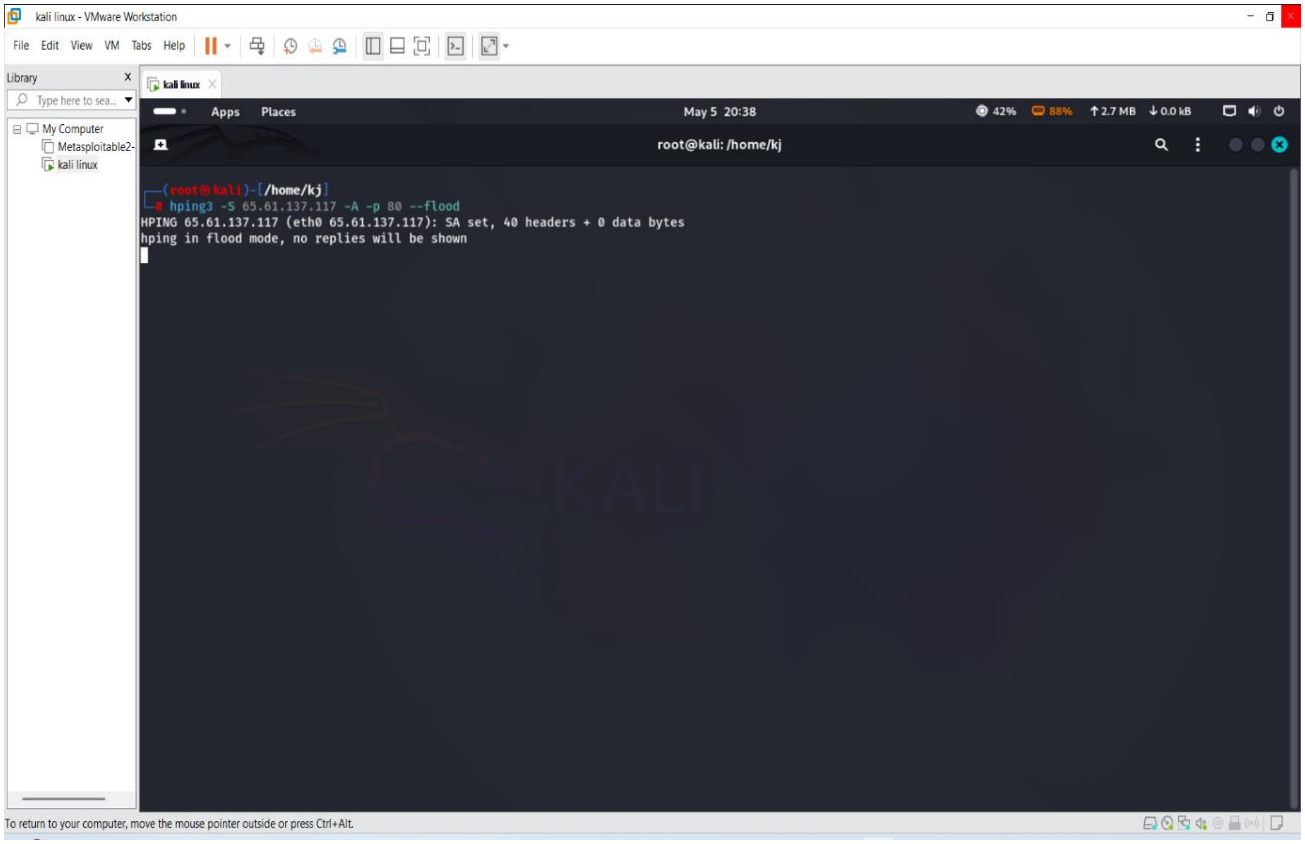


Here we see the attack run .

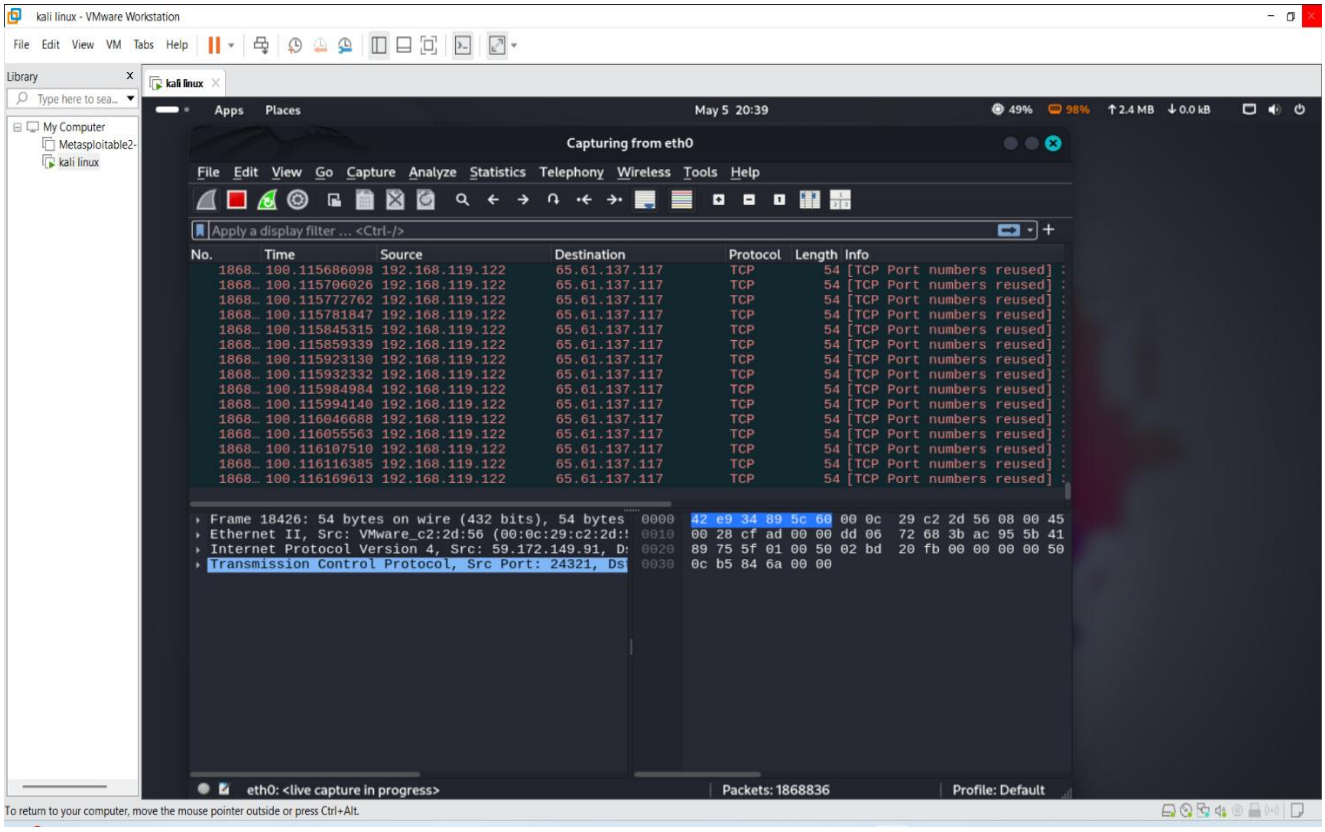
/ Here we are see DDOS attack using Hping3

Command : # hping3 -S <target IP> -A -p 80 –flood

Name : kunal Jawale



Run wireshark and see attack using hping3

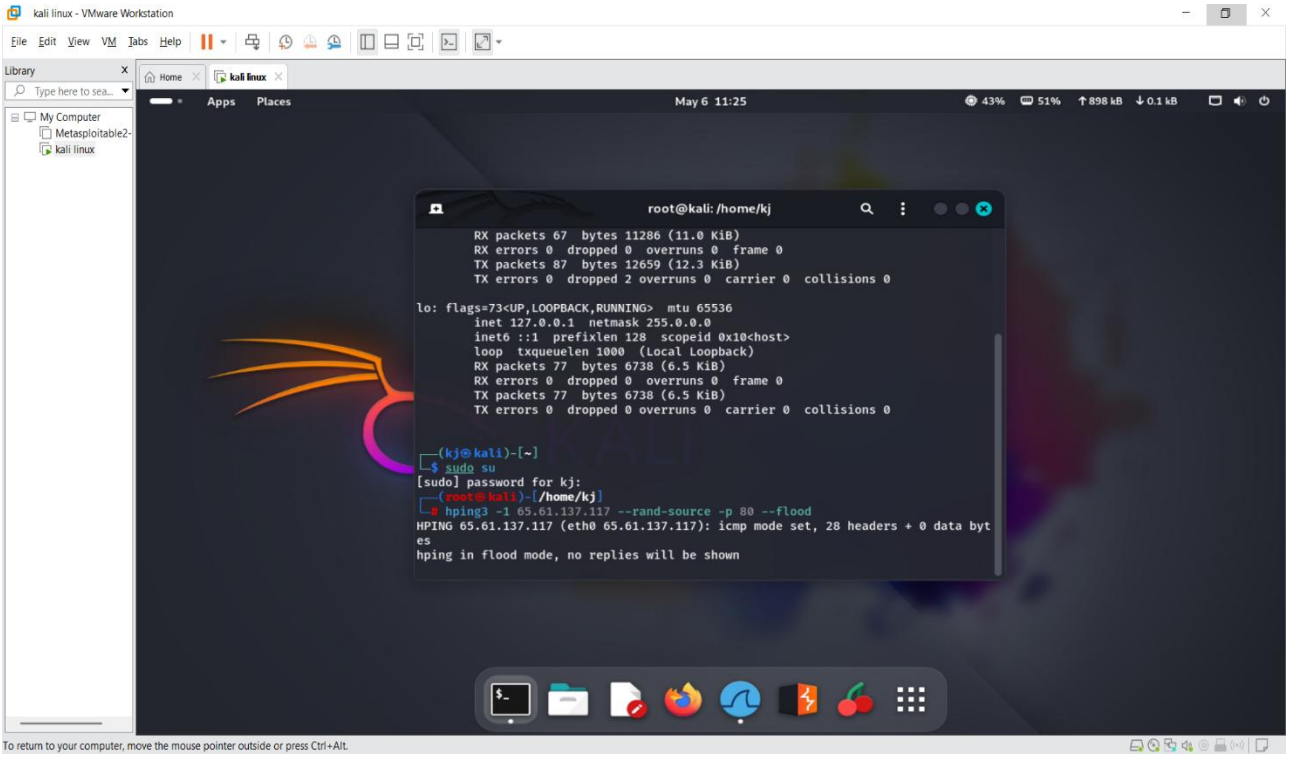


Name : kunal Jawale

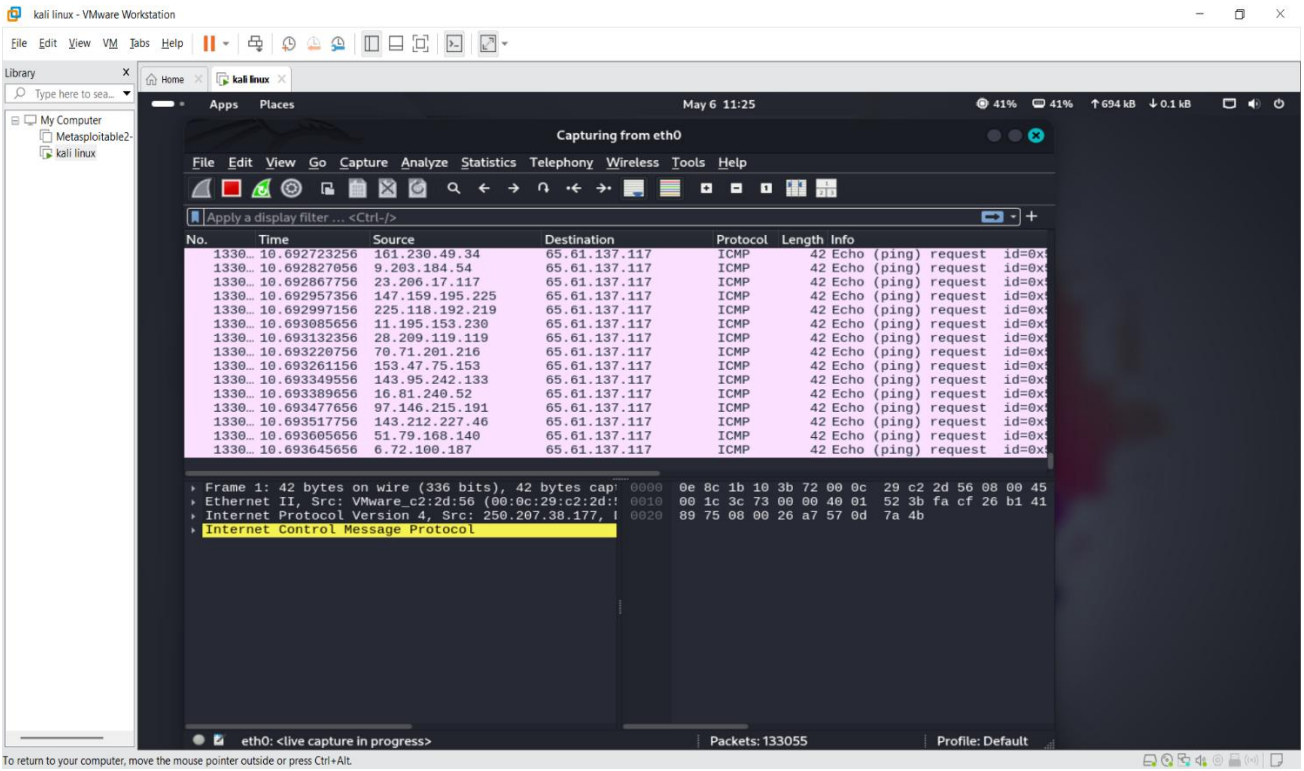
Command : # hping3 -1 <target IP> -a   -p 80 –flood

-1 for ICMP

-a for spoofing

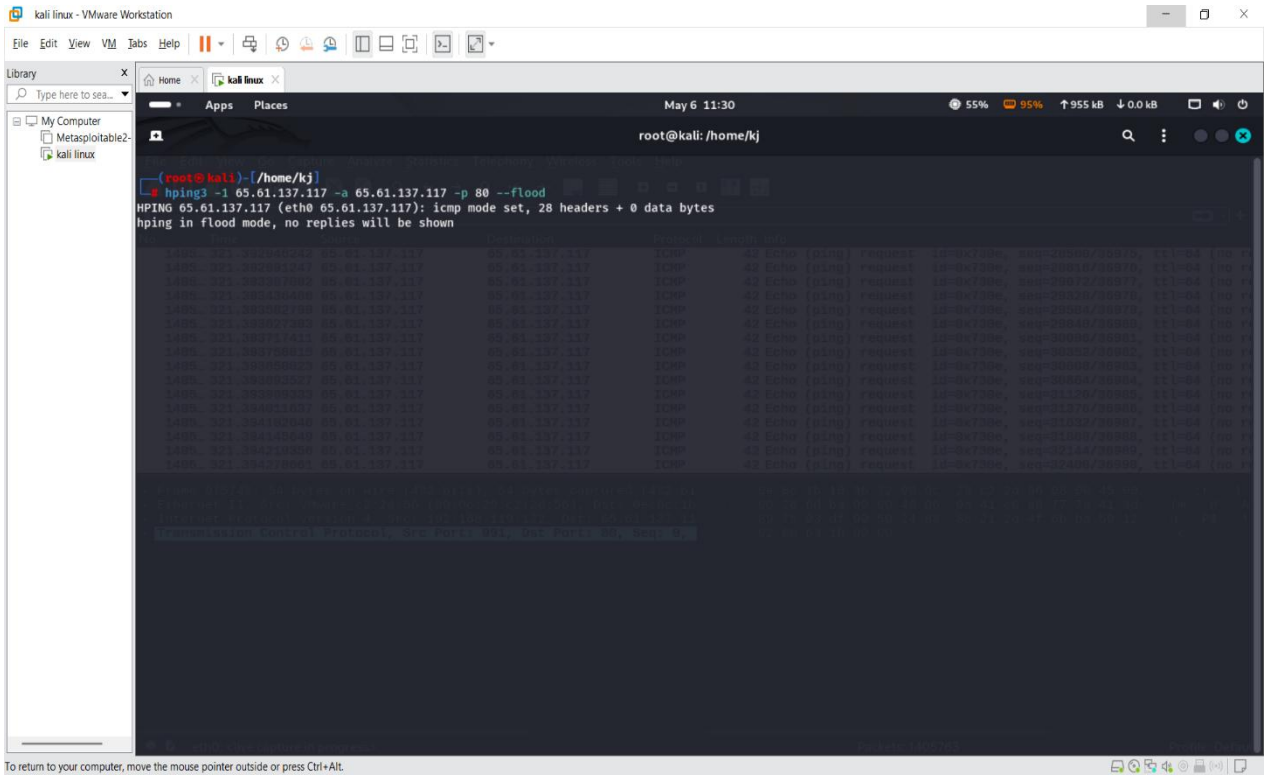


Output

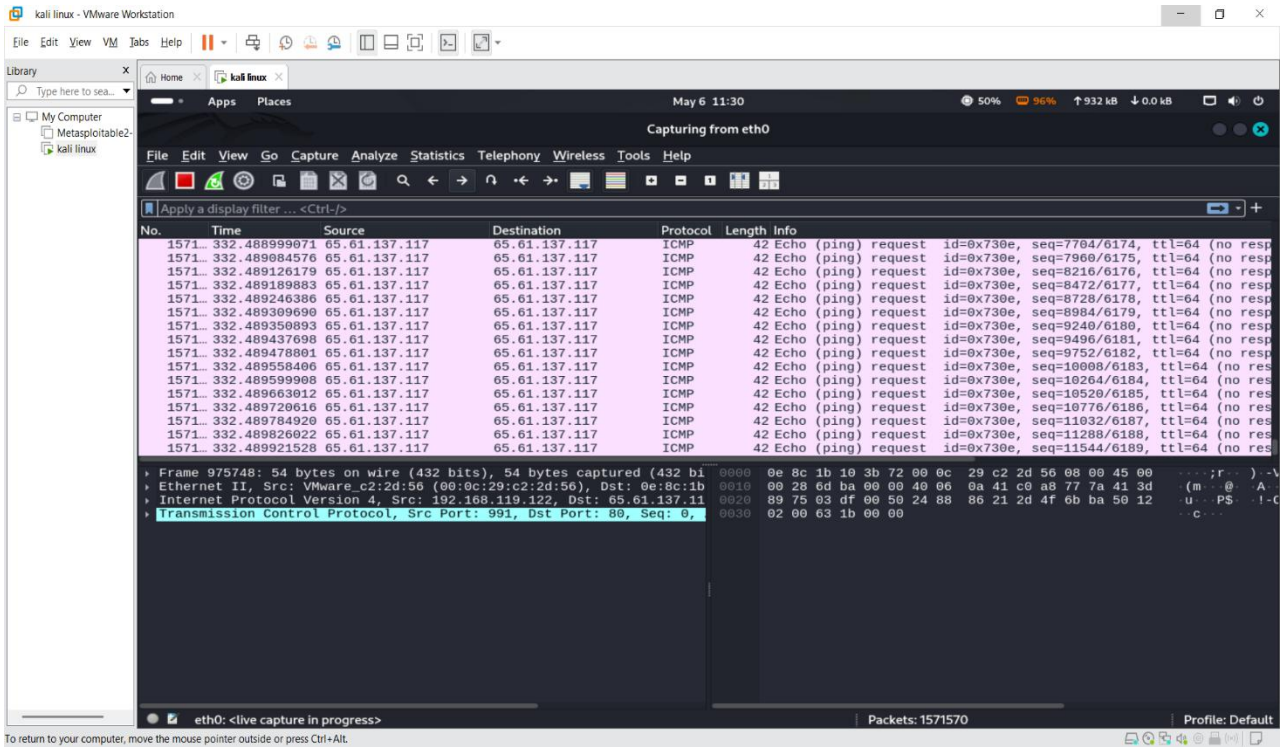


Name : kunal Jawale

Command : # hping3 -1 < target IP > -a <same target IP> -p 80 –flood



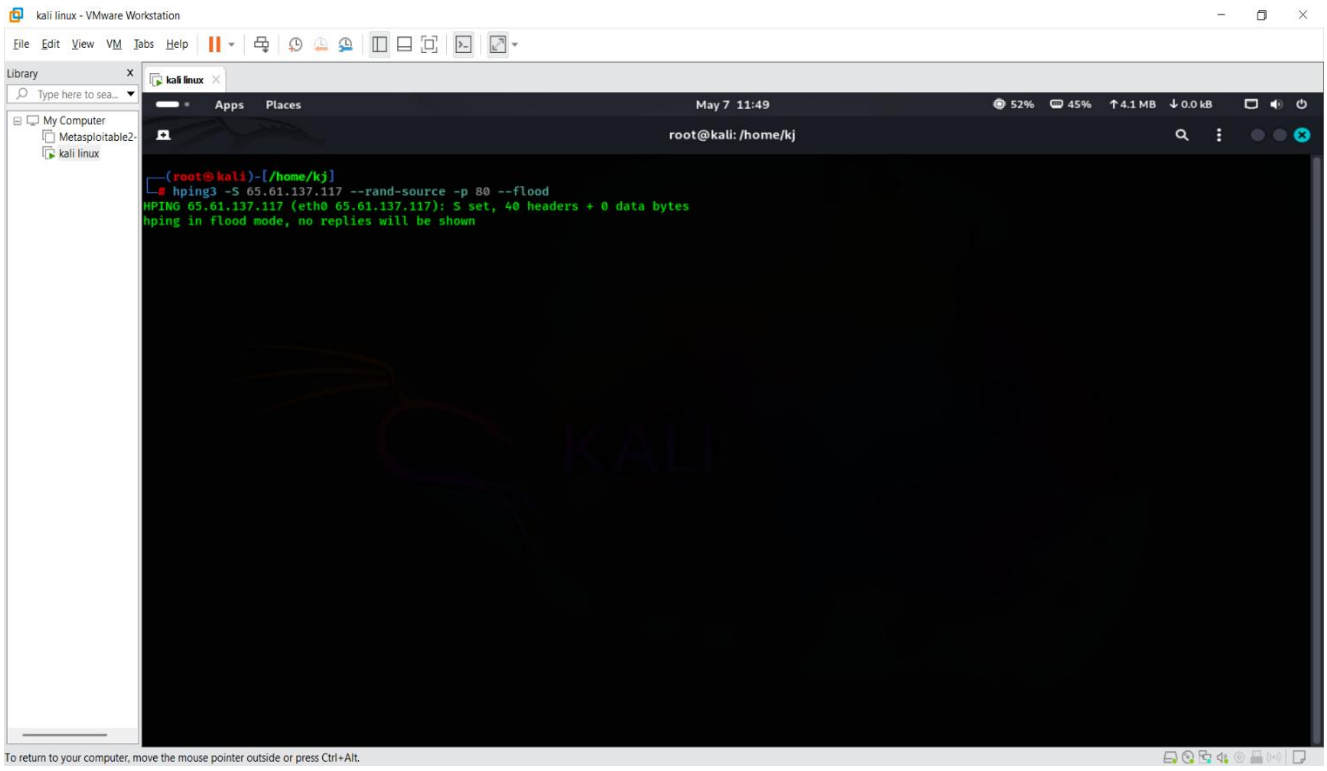
Output



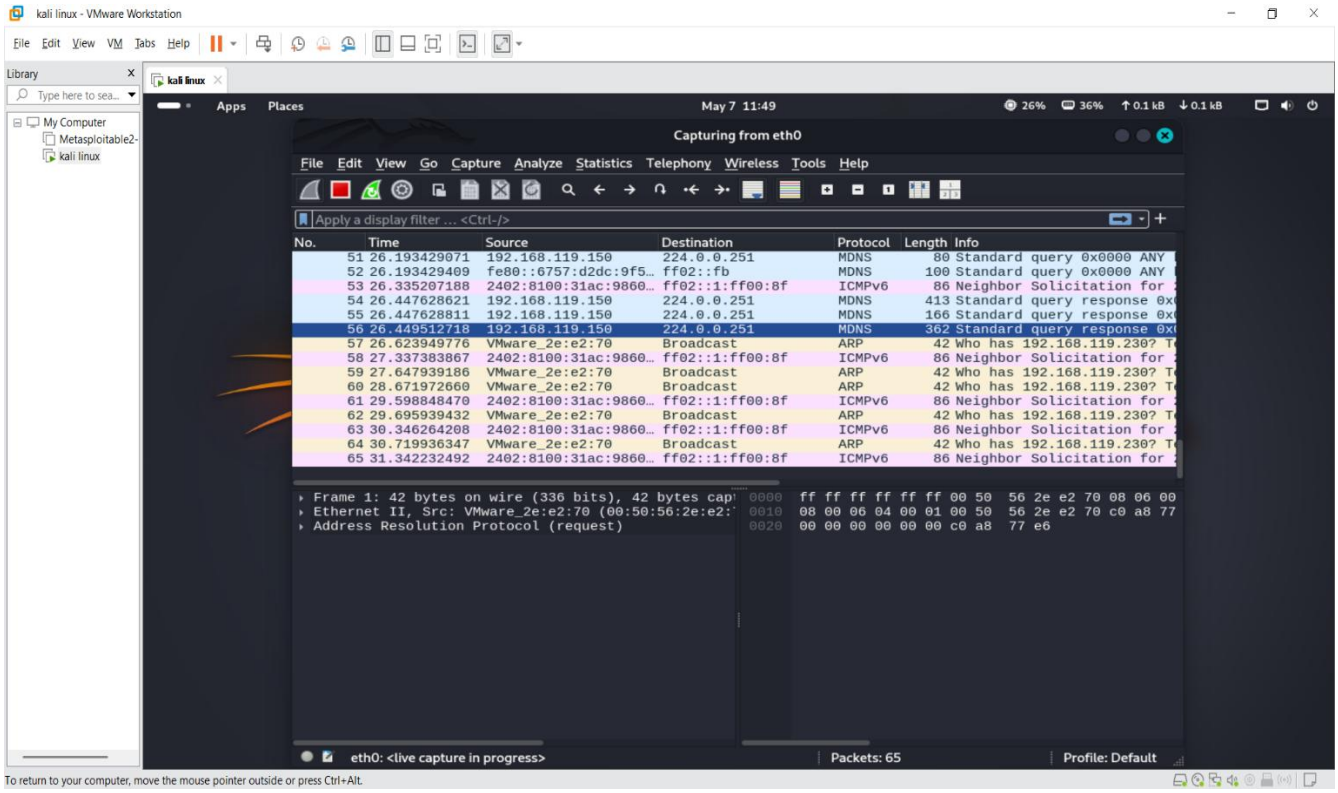
Name : kunal Jawale

Command : hping3 -S <target IP> --rand-source -p 80 –flood

--rand-source : for random source



Output



/ Information about Raven-Storm

Features

Raven Storm is a powerful application layer DDoS tool with the following features:

- Attacks layers 3, 4, and 5 of the application layer.
- Coded Python3 and can efficiently deal with robust servers.
- Requires multiple instances like botnets to operate successfully.
- Uses a CLIF framework to operate.
- Does not require any **'sudo', 'su', or root** permissions.
- The backbone of the primary python file 'main.py' is the modules script which is:
    - **L3**: Ping target host using ICMP protocol
    - **L4**: Ping target host using UDP/TCP protocol
    - **L7**: Ping target host over HTTP Protocol
    - **Server**: To launch DDoS attacks against a target website.
    - **ARP**: For ARP Spoofing
    - **Wifi**: To launch the attack module for Wifi attacks.

Attack Modules

- 8 different modules are present for carrying out different types of attacks such as **server takedown, wifi attack, application layer attack**, etc.

- The table below contains the list of attacks along with the module used to execute them.

Method	Module
Ping	**L3**
UDP/TCP Services	**L4**
Websites	**L7 (Flood Module)**
Local Devices	**ARP**
Wifi	**Bl**
Botnet	**Server**

- The tool is capable of taking down hosts and servers.
- It can be optimized and integrated to perform more substantial attacks.

Execution

- To a successful DDoS attack via botnet requires the following:
    - A URL is provided to the user while executing a DDoS attack, to connect to the botnet.
    - The user has to execute the command **“server”** and define a custom password for using this botnet, thereby preventing others from interfering.
- The ARP module uses a lot of Nmap features to scan for local devices. Hence, this module requires the user to have Nmap pre-installed.

- The attack begins once the user enters the required code (L3, L4, etc) and the target host (IP address).
- A request is sent to the target host to see if it is responsive; if it is, the attack is launched.

DDoS Module

- The server module (that carries out the DDOS Attacks) takes the following as input from the user:
    - Server password configured by the user.
    - Host IP
- The server then sends a GET packet to the host.
- An error message is returned if the session code is not 200. Here, 200 session code means that the host was reachable and able to communicate.
- Once confirmed, the server module begins the attack. The server module can carry out **500 GET requests at a time.**
- If it is unable to, then the sleep function is invoked to have a pause of a second.

Impact & Mitigation

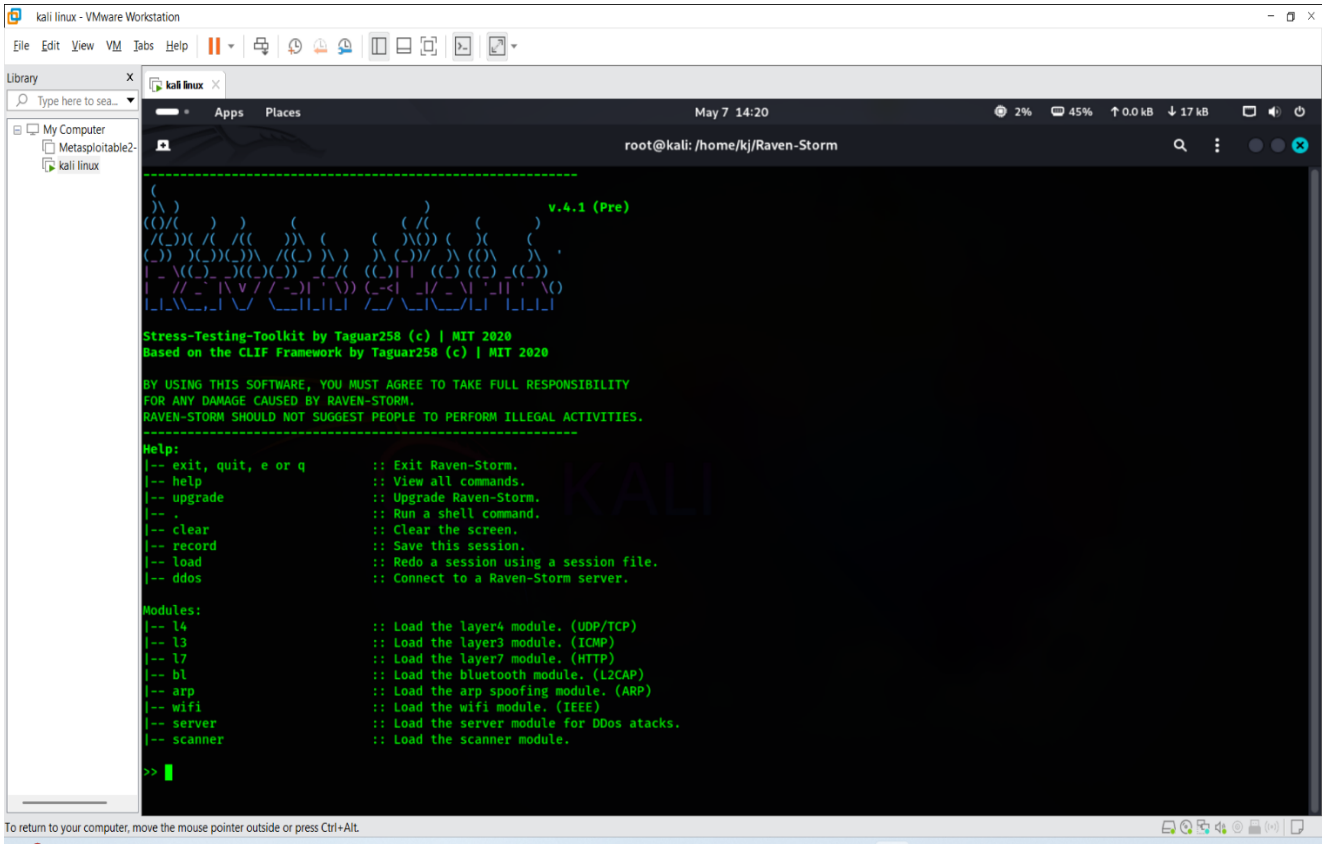
Impact	Mitigation
• **Significant amount of downtime for the website and the hosting server.** • **Loss of brand reputation and image.** • **Server and hosting issues for other websites hosted on the same server.** • **Follow-up attack by the threat actor groups abusing a vulnerability on the domain side or server side.**	• **Implement anti-DDoS protection on the server.** • **Use IP geo-blocking in case of an attack** • **Patch vulnerable and exploitable endpoints.** • **Monitor for anomalies in user accounts, which could indicate possible account takeovers.** • **Monitor cybercrime forums for the latest tactics employed by threat actors**

/ DDOS Attack using Raven-Storm

Step 1 : install Raven-storm through command in kali linux

Step 2 : after installation go to this directory and run python3 main.py command

Name : kunal Jawale



Screenshot of the Raven Storm tool being used by Mysterious Team for DDoS attacks[/caption] [caption id="attachment_20405" align="aligncenter" width="967"]

Step 3 : go for l4

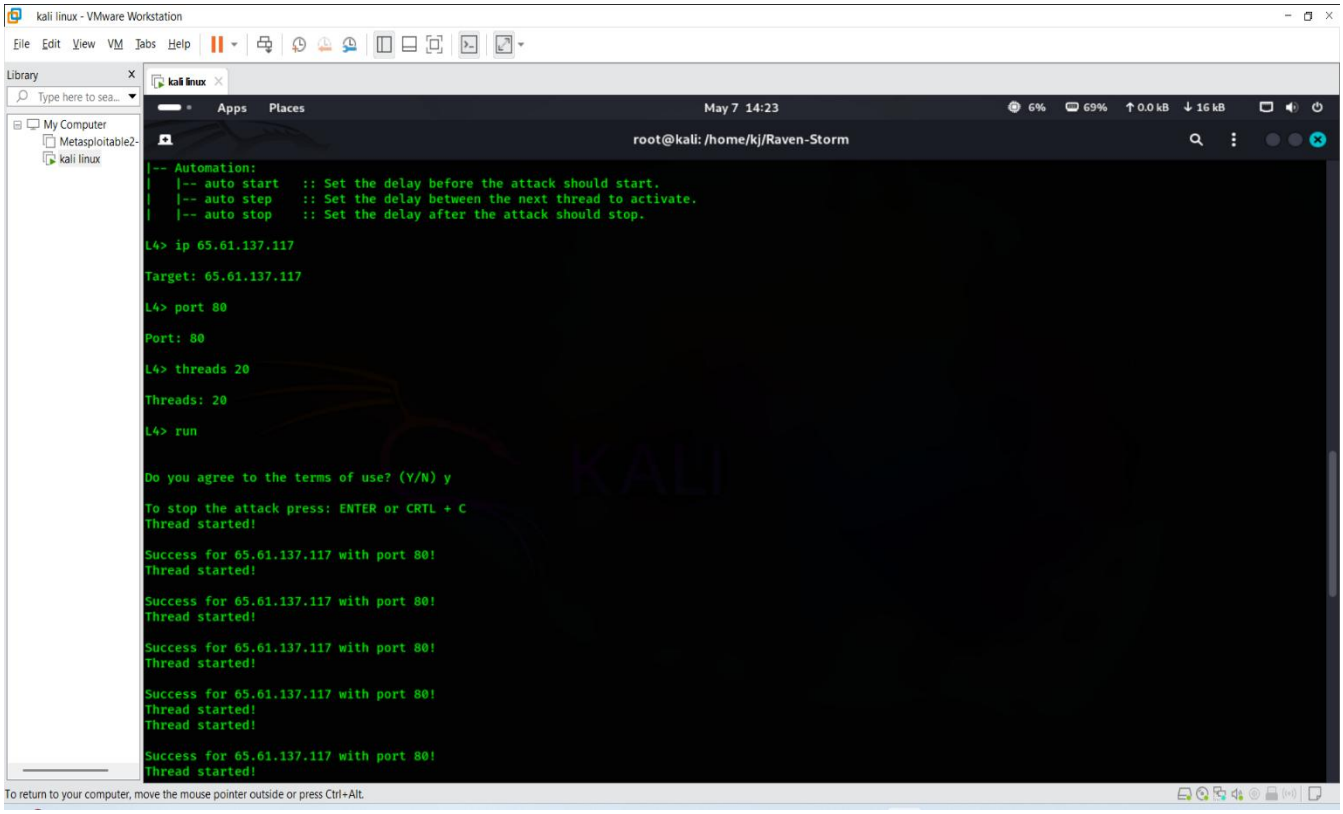
Step 4 : give the target ip

give Port 80

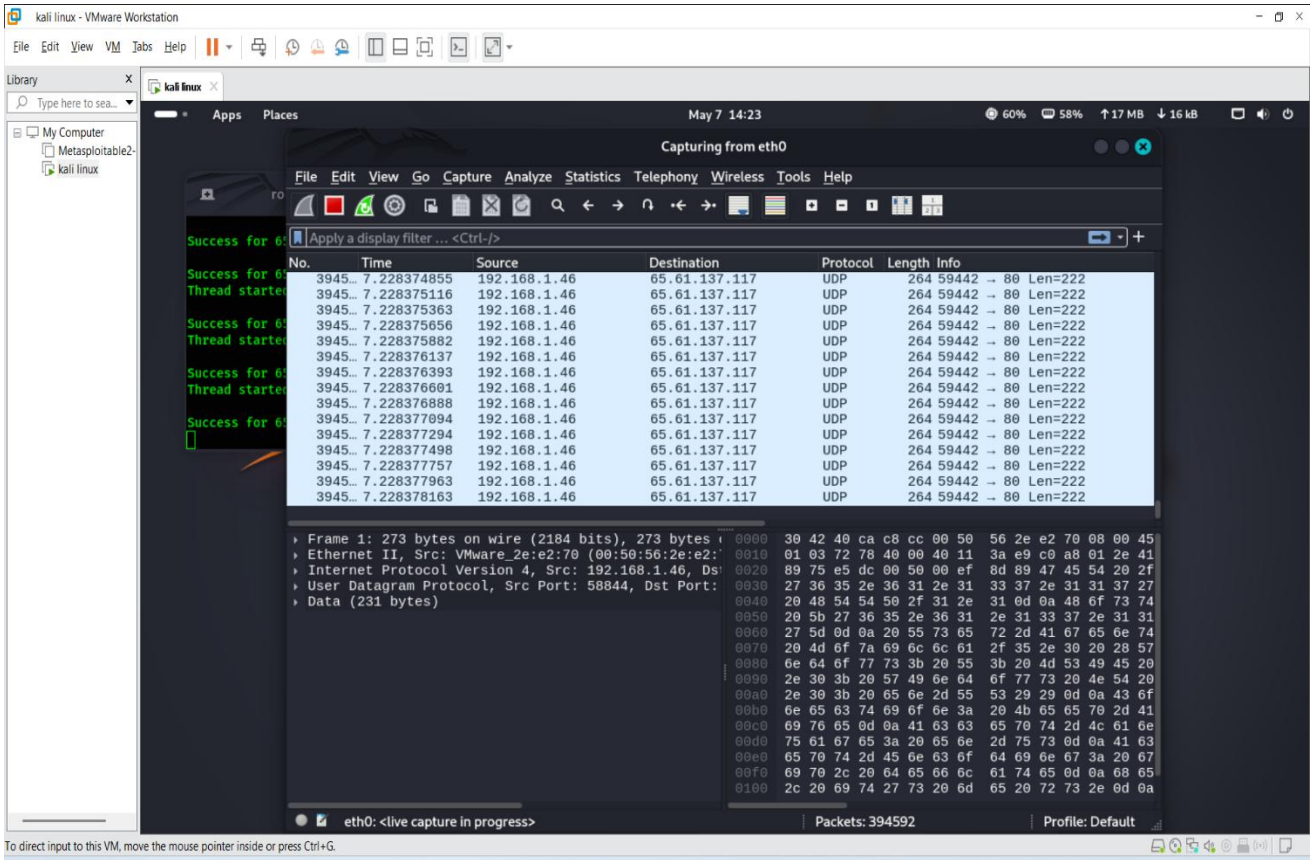
give Threads 20 (whatever you want)

Step 5 : run

Name : kunal Jawale



After getting the attack go to wireshark and check attack is running



Name : kunal Jawale

➢ Slowloris :-

- Slowloris DDoS attacks are dangerous because they can be carried out with relatively few resources and can effectively take down even large and robust web servers.
- Slowloris attacks are called “slow” because they don’t rely on sending a high traffic volume like other DDoS attacks but rather on keeping a low-level stream of connections open for as long as possible.
- As logs cannot be written until a request is completed, Slowloris can immobilize a server and go undetected for a long time. This happens without raising a red flag for anyone who actively monitors logs for any changes.
- Because Slowloris attacks only require a small amount of bandwidth and can be carried out by a single machine, they are often difficult to detect and defend against.
- Overall, Slowloris DDoS attacks are dangerous because they can be highly effective at taking down web servers, are difficult to detect and defend against, and can be launched with minimal resources
- **Slowloris Attack Vs. UDP Flood Vs. SYN Flood Vs. Ping of Death**

Types of Attacks	Method	Objective	Layer of Operation	Targets	Stealth and Detection
Slowloris Attack	Keeps numerous connections open to a web server with incomplete HTTP requests, gradually consuming server resources.	Overwhelm the server’s resources, leading to a denial of service for legitimate users.	Application layer (Layer 7) of the OSI model.	Primarily effective against web servers.	More stealthy and harder to detect due to mimicking legitimate user behavior.

UDP Flood	Floods the target server with a high volume of UDP **packets**, targeting specific ports or services vulnerable to such attacks.	Overwhelm network resources, causing the server to become unresponsive to legitimate traffic.	Transport layer (Layer 4) of the OSI model.	Can target a wide range of services and protocols relying on UDP.	More straightforward and easily recognizable due to the volume of traffic generated.
SYN Flood	Floods the target server with a large number of TCP connection requests but doesn't complete the connection handshake.	Fill the server's connection queue with half-open connections, preventing it from accepting legitimate connections.	Transport layer (Layer 4) of the **OSI model**.	Any service or protocol relying on TCP, such as web servers.	Intense and rapid, aiming to quickly overwhelm the server's capacity to handle new connections.
Ping of Death	Sends oversized or malformed ICMP packets to the target system, exploiting vulnerabilities in network protocol handling.	Crash or destabilize the target system by causing it to process malformed or oversized packets.	Network layer (Layer 3) of the OSI model.	Any system vulnerable to ICMP packet vulnerabilities.	Relatively rare in modern systems due to improvements in network protocol implementations.

Why Are Slowloris DDoS Attacks Dangerous?

Slowloris DDoS attacks are dangerous because they can be carried out with relatively few resources and can effectively take down even large and robust web servers.

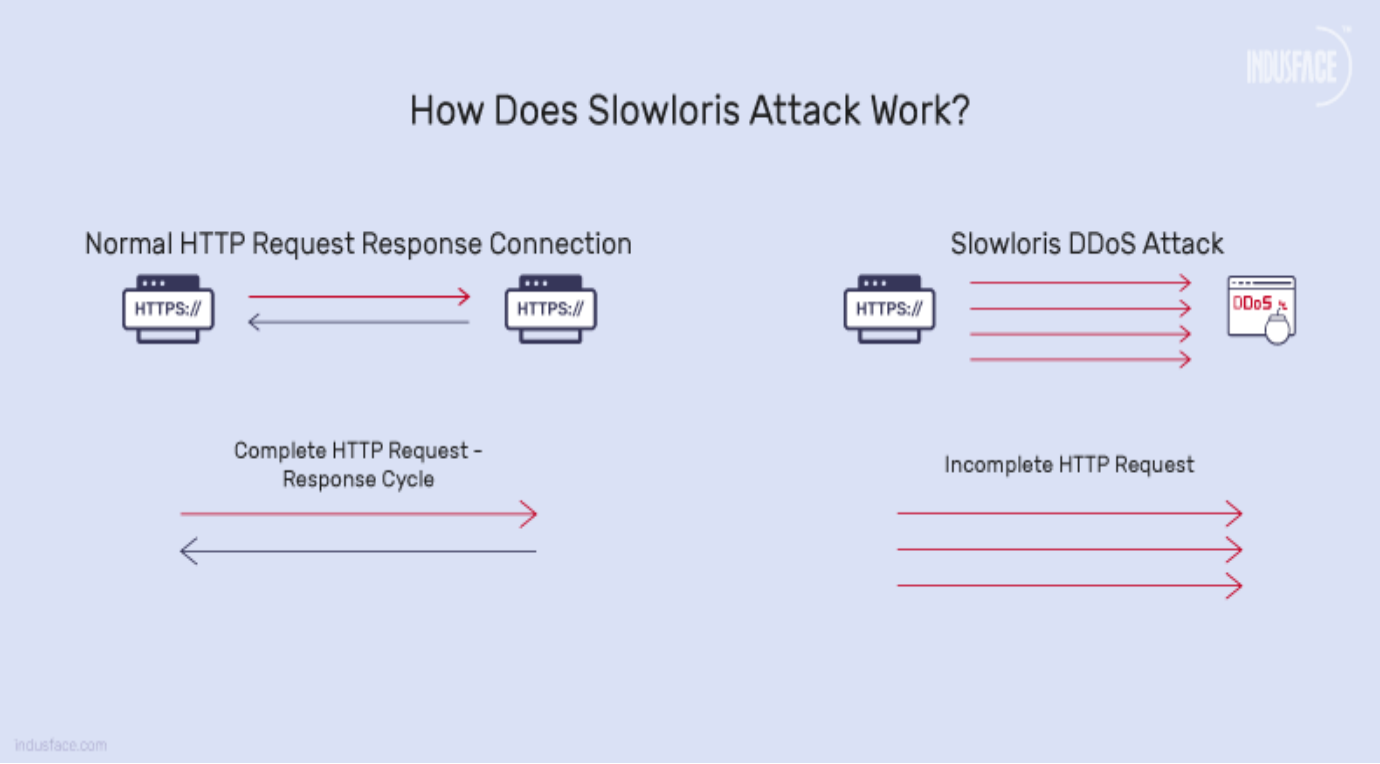
Slowloris attacks are called "slow" because they don't rely on sending a high traffic volume like other DDoS attacks but rather on keeping a low-level stream of connections open for as long as possible.

As logs cannot be written until a request is completed, Slowloris can immobilize a server and go undetected for a long time. This happens without raising a red flag for anyone who actively monitors logs for any changes.

Because Slowloris attacks only require a small amount of bandwidth and can be carried out by a single machine, they are often difficult to detect and defend against.

Overall, Slowloris DDoS attacks are dangerous because they can be highly effective at taking down web servers, are difficult to detect and defend against, and can be launched with minimal resources.

How Does a Slowloris Attack Work?

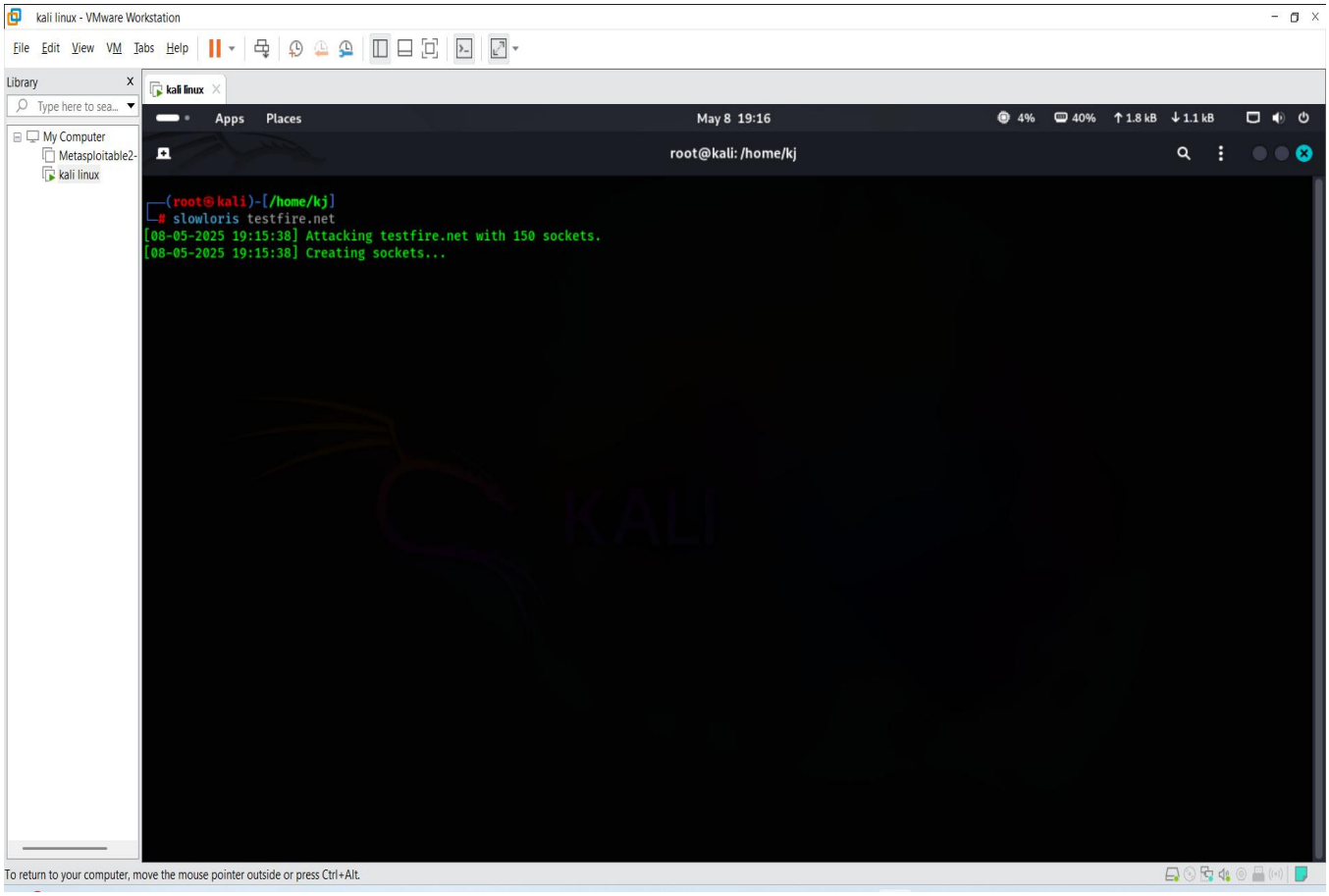


Here is a step-by-step process of how a Slowloris attack is carried out

1. **Connection Initiation:** The attacker initiates connections to the target web server, just like a legitimate user would.
2. **Incomplete Requests:** Instead of completing the HTTP requests quickly, the attacker sends partial HTTP requests to the server.
3. **Header Injection:** Periodically, the attacker sends additional HTTP headers to the server, but doesn't complete the requests by sending the necessary data.

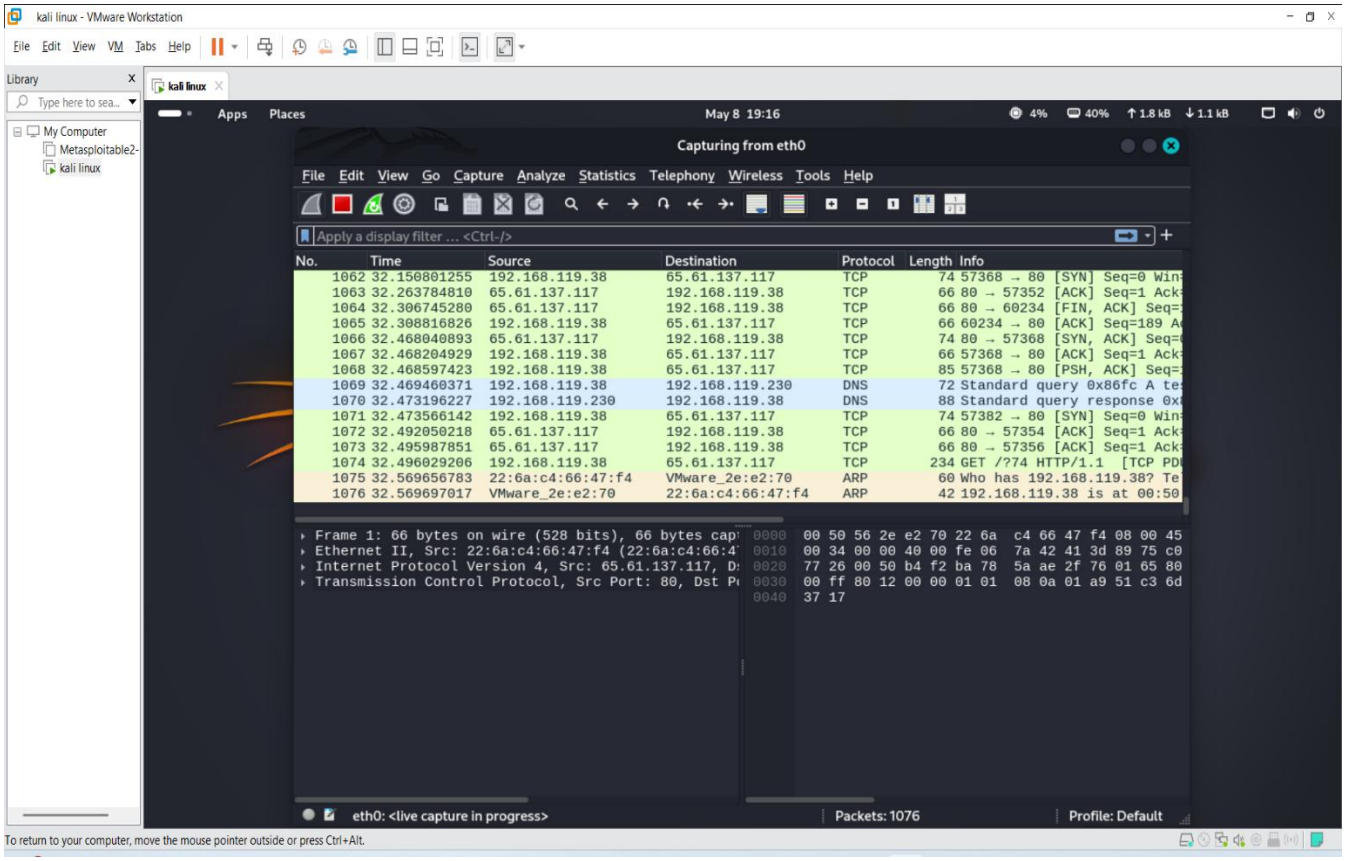
4. **Persistent Connections:** The attacker keeps these connections open by occasionally sending additional header lines, ensuring that the connections remain active.
5. **Resource Exhaustion:** As the server is programmed to wait for the completion of these requests, each open connection consumes server resources such as sockets, memory, and processing power.
6. **Server Overload:** With a large number of connections kept open simultaneously, the server's resources become exhausted, and it's unable to handle legitimate requests from other users.
7. **Denial of Service:** Eventually, the server becomes overwhelmed and can no longer respond to legitimate user requests, effectively denying service to legitimate users.
8. **Persistence:** Slowloris can maintain this attack for an extended period, as long as the attacker keeps sending periodic header updates to keep the connections alive.

/ here are some screenshot of slowloris attack and result



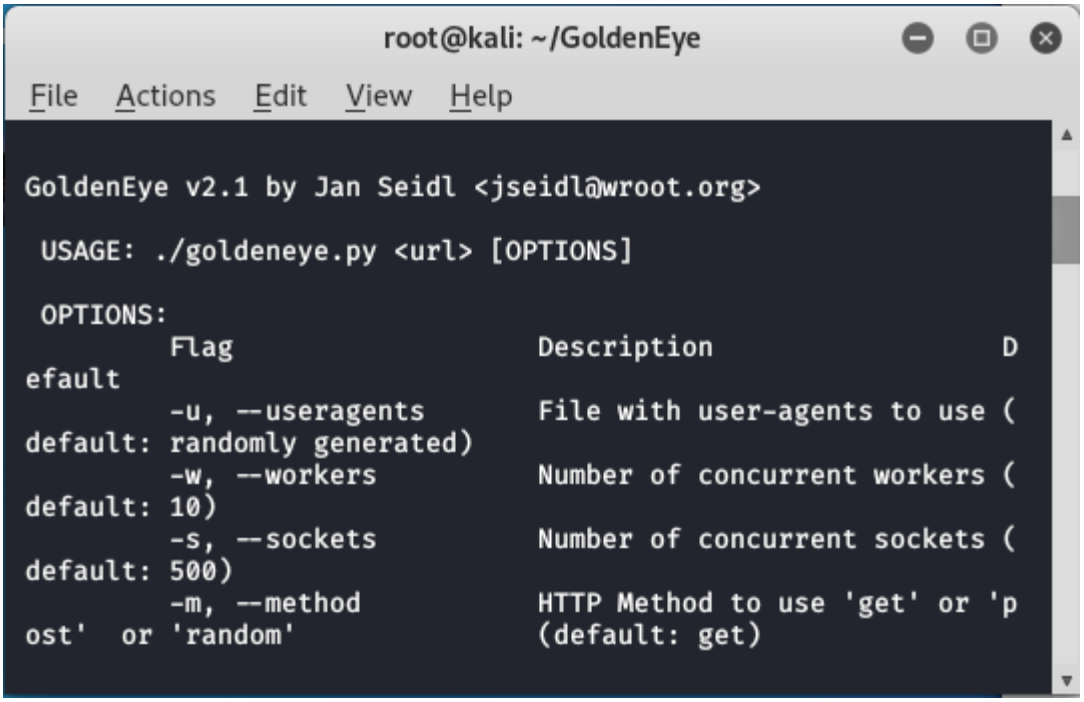
Name : kunal Jawale

Result :



Golden eye : **Goldeneye** is a free and Open source tool available on **GitHub**. We can perform a denial of service attack using this tool. It's a framework written in .NET Core. This tool provides many base classes and extensions to use with your daily work. This tool allows a single machine to take down another **machine's web server** it uses perfectly legitimate HTTP traffic. It makes a full TCP connection and then requires only a few **hundred requests** at long-term and regular intervals. As a result, the tool doesn't need to use a lot of traffic to exhaust the available connections on a server.

Name : kunal Jawale

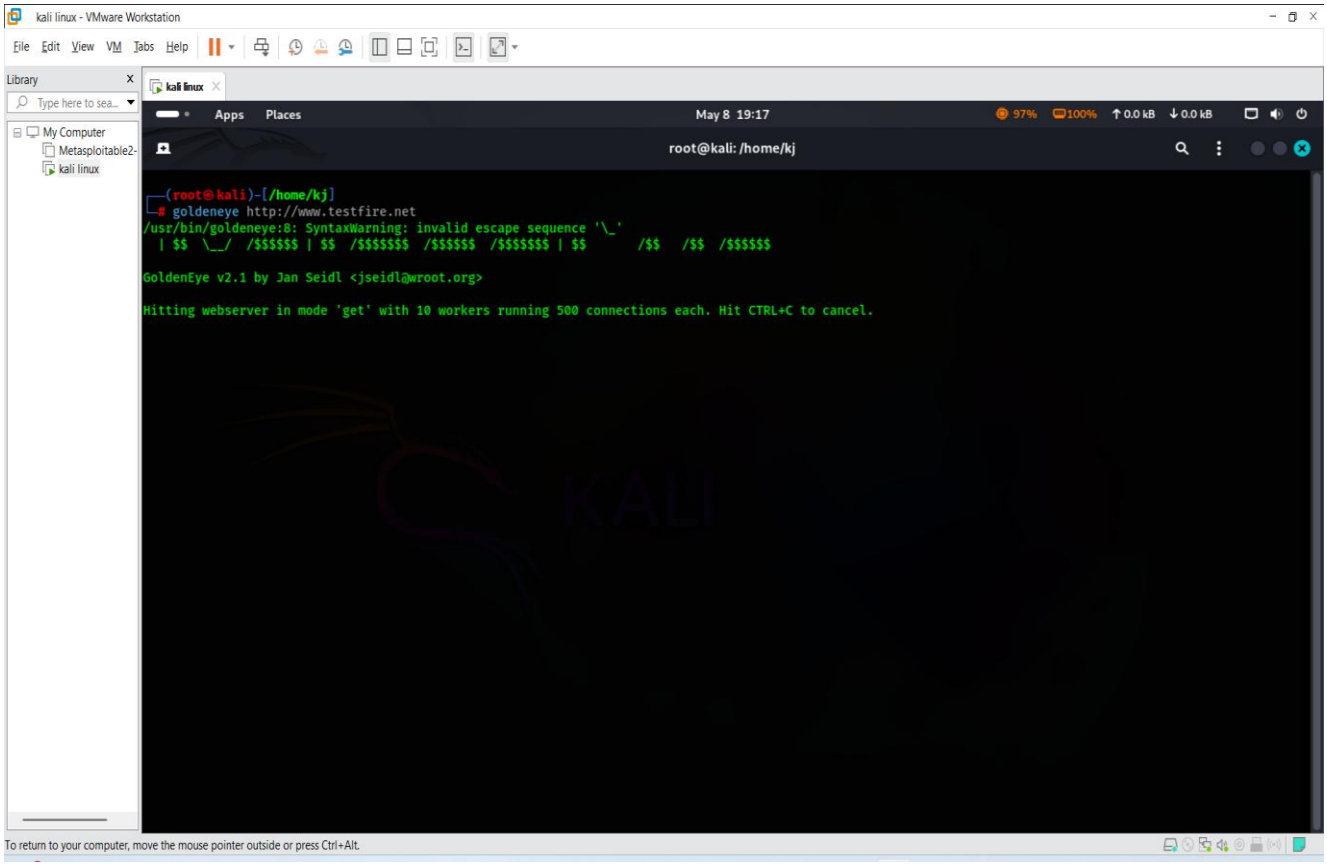


Uses of Goldeneye:

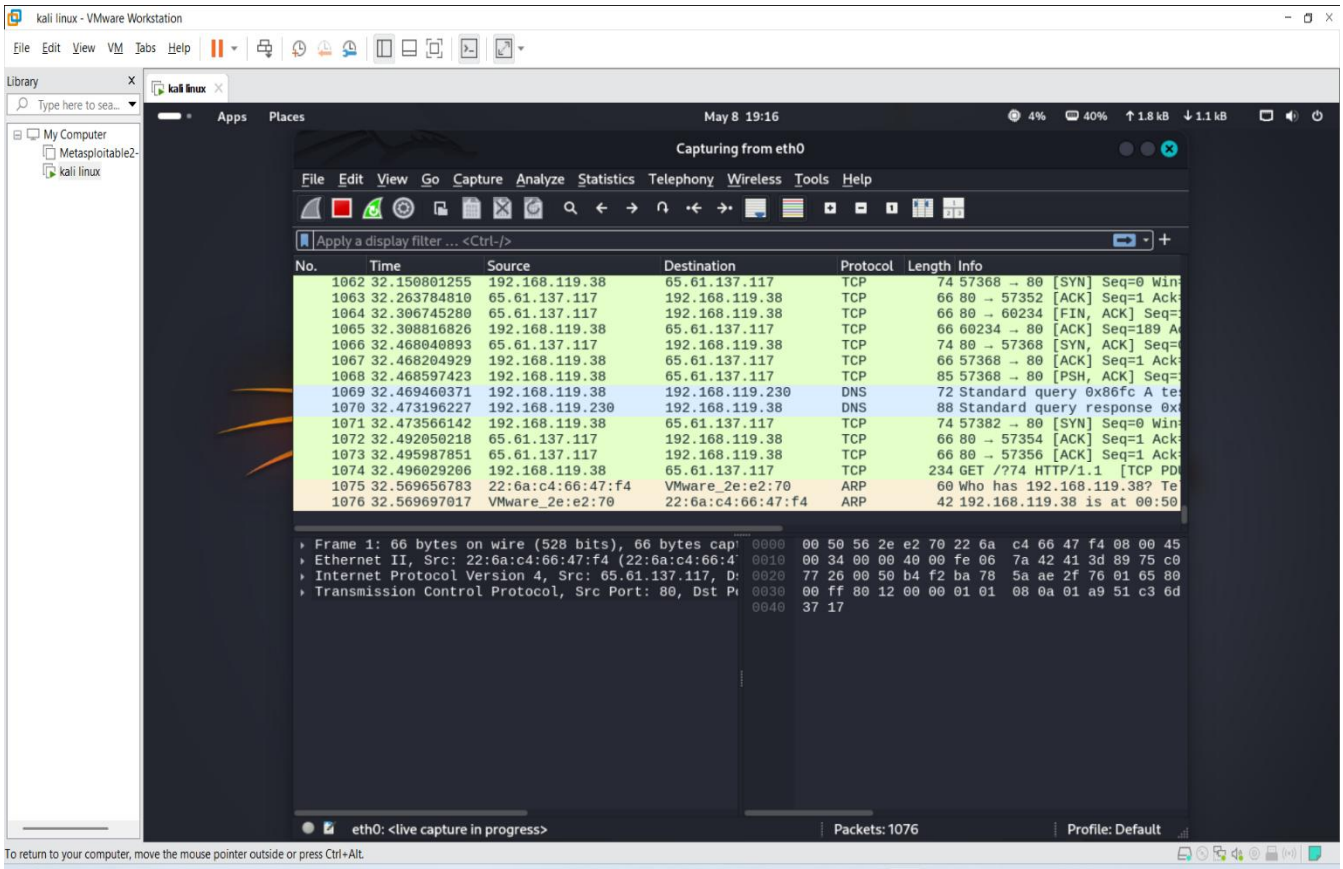
1. Goldeneye uses perfectly legitimate HTTP traffic.
2. Denial of service attack can be executed with the help of Goldeneye by generating heavy traffic of botnets.
3. Goldeneye sends multiple requests to the target as a result generates heavy traffic botnets.
4. Goldeneye is an open-source tool, so you can download it from GitHub free of cost.
5. Goldeneye can be used to perform DDoS attacks on any webserver.

Screenshot of goldeneye:

Name : kunal Jawale



Result :



HOIC :- The High Orbit Ion Cannon (HOIC) is an open-source web application designed to carry out distributed denial-of-service (DDoS) attacks. HOIC enables an attacker to launch floods of HTTP requests to overload web servers and take down websites or online services.

What is HOIC

HOIC is a network stress testing tool written in programming languages like C# and Visual Basic. It was created as an open-source alternative to replace the original Low Orbit Ion Cannon (LOIC) application that was used to perform volume-based DDoS attacks.

Key features provided by HOIC include:

- Generating high volumes of GET and POST web requests
- Support for targeting multiple URLs/domains concurrently
- Graphical and command-line attack interfaces
- Scripting capabilities to customize attack parameters
- SOCKS proxy support to obfuscate traffic
- TLS 1.2 encryption to bypass restrictions
- Automated update capability to evade blacklist blocking

While ostensibly designed for stress testing, in practice, HOIC is predominantly used maliciously to overload and disrupt websites and web applications via DDoS attack.

Using HOIC for DDoS Attacks

HOIC provides a simple interface accessible to novice users for performing application-layer DDoS attacks:

- The visual dashboard allows entering target URLs, configuring request rates, and initiating attacks.
- Command-line options support automation with scripts and proxies.
- Web-based lists provide up-to-date targets and attack details to participants.

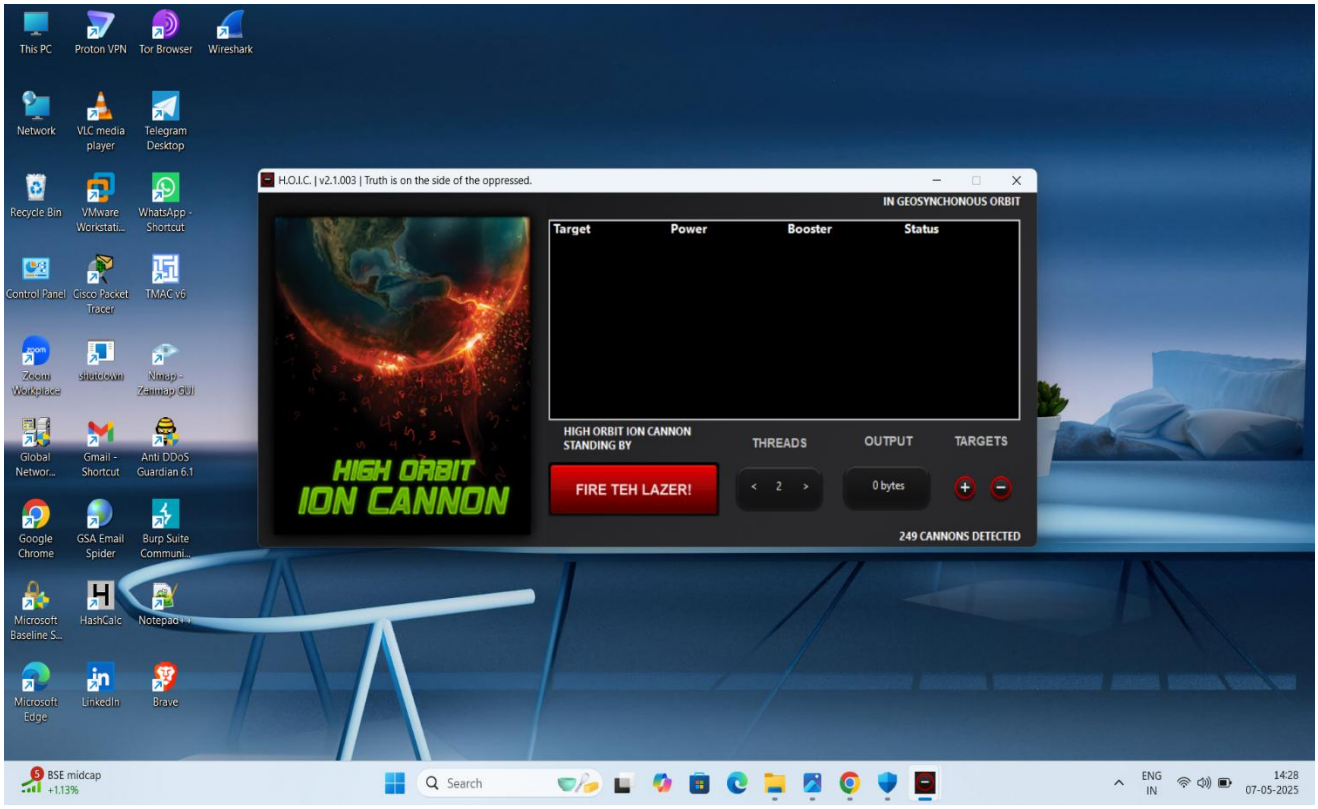
Name : kunal Jawale

Users join voluntary botnets by running HOIC to contribute attack traffic against published targets. This combines multiple HOIC instances into potent DDoS swarms.

However, these uses typically violate laws against computer hacking, abuse, and denial-of-service.

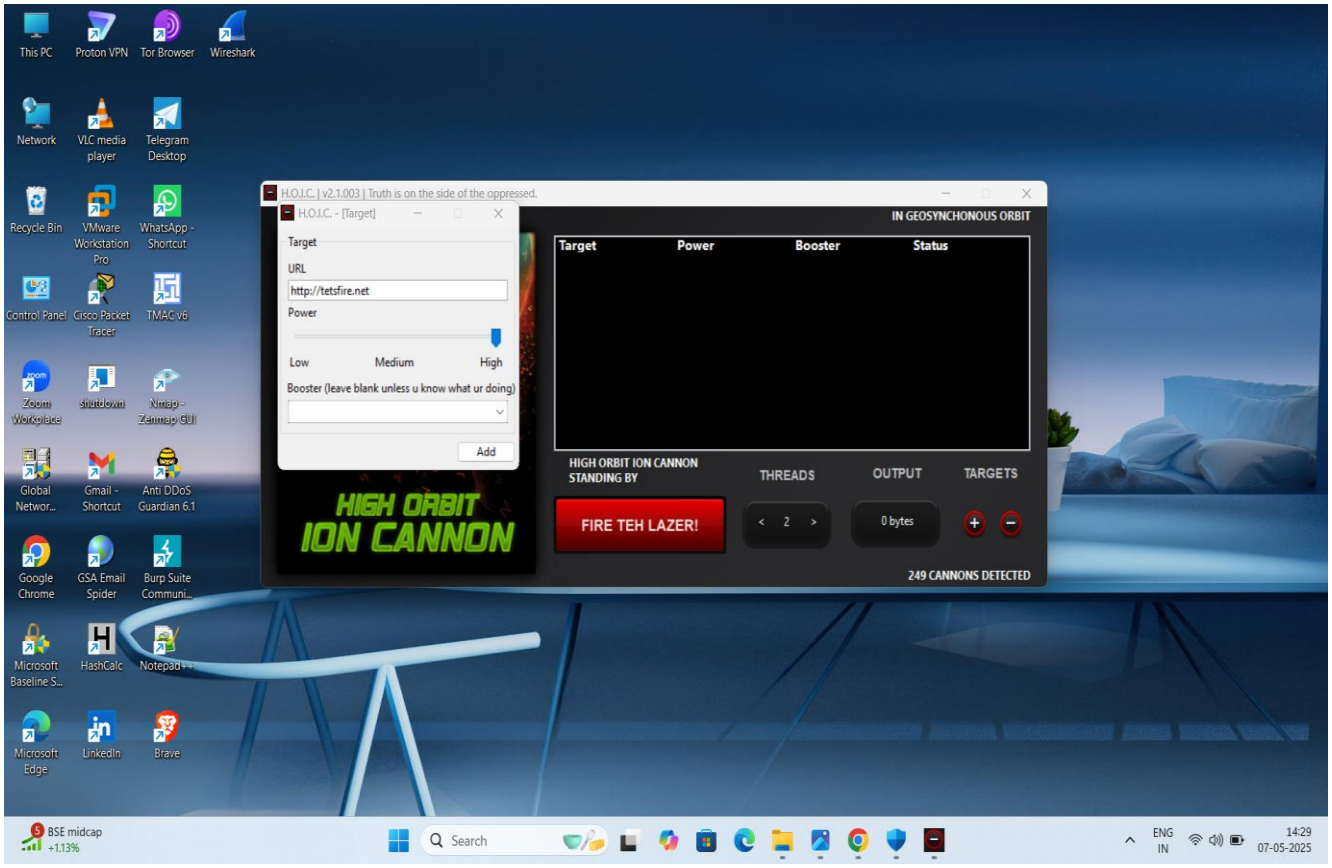
Screenshots of HOIC:

Step 1 : run HOIC on window

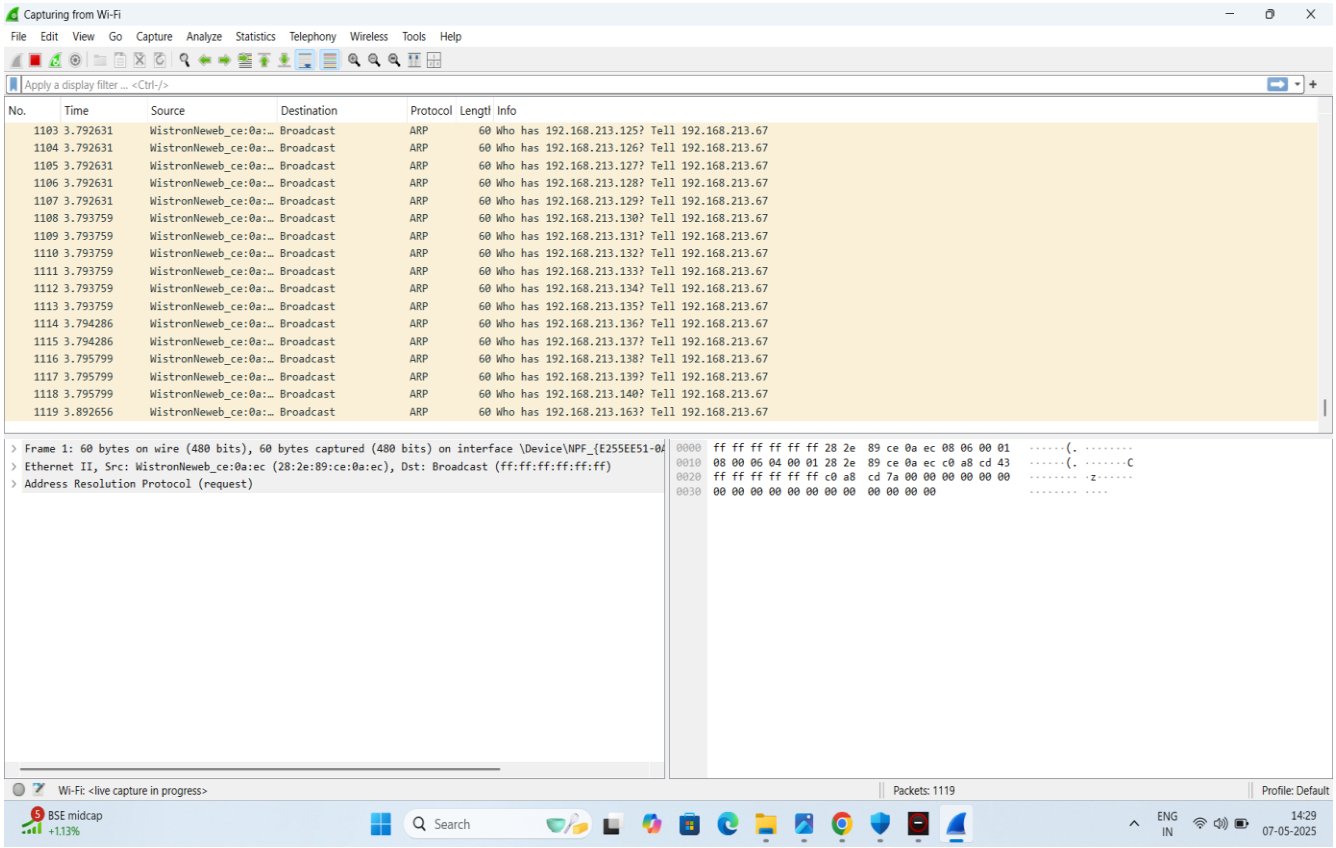


Step 2 : click on + symbol and add target url

Name : kunal Jawale



Step 3: attack is running check on wireshark



Name : kunal Jawale

/ detect and protect against DOS and DDOS Attack using Anti DDOS guardian tool :

Anti-DDoS Guardian is a software solution designed to protect Windows servers from DDoS attacks and DoS attacks by managing network traffic and limiting malicious activity. It monitors network activity in real-time, detects various attack types, and takes actions to mitigate them, including blocking malicious IPs and controlling traffic flow.

Here's a more detailed look at its features and capabilities:

Protection:

- **DDoS/DoS Mitigation:**

  Anti-DDoS Guardian protects against a wide range of attacks, including SYN floods, TCP floods, ICMP floods, UDP floods, slow HTTP Get&Post attacks, application-level attacks (Layer 7), brute-force password guessing, and others.
- **Real-time Monitoring:**

  It monitors network activity in real-time, detecting and alerting users to potential attacks.
- **Attack Detection:**

  It identifies and distinguishes DDoS attacks from legitimate traffic, allowing for effective mitigation.
- **IP Blocking:**

  Anti-DDoS Guardian can automatically block malicious IP addresses, helping to prevent further attacks.
- **Traffic Control:**

  It limits network flow, bandwidth, connections, and packet rates to prevent overload and disruption, especially for TCP half-open connections, which are effective against SYN attacks.
- **Network Flow Management:**
  Anti-DDoS Guardian manages network flows and blocks malicious traffic, especially for advanced attacks like layer 7 attacks.

Additional Features:

- **Lightweight Firewall:**

  It acts as a lightweight firewall with TCP/IP rules, allowing for customization based on IP address, port, protocol, and other factors.

Name : kunal Jawale

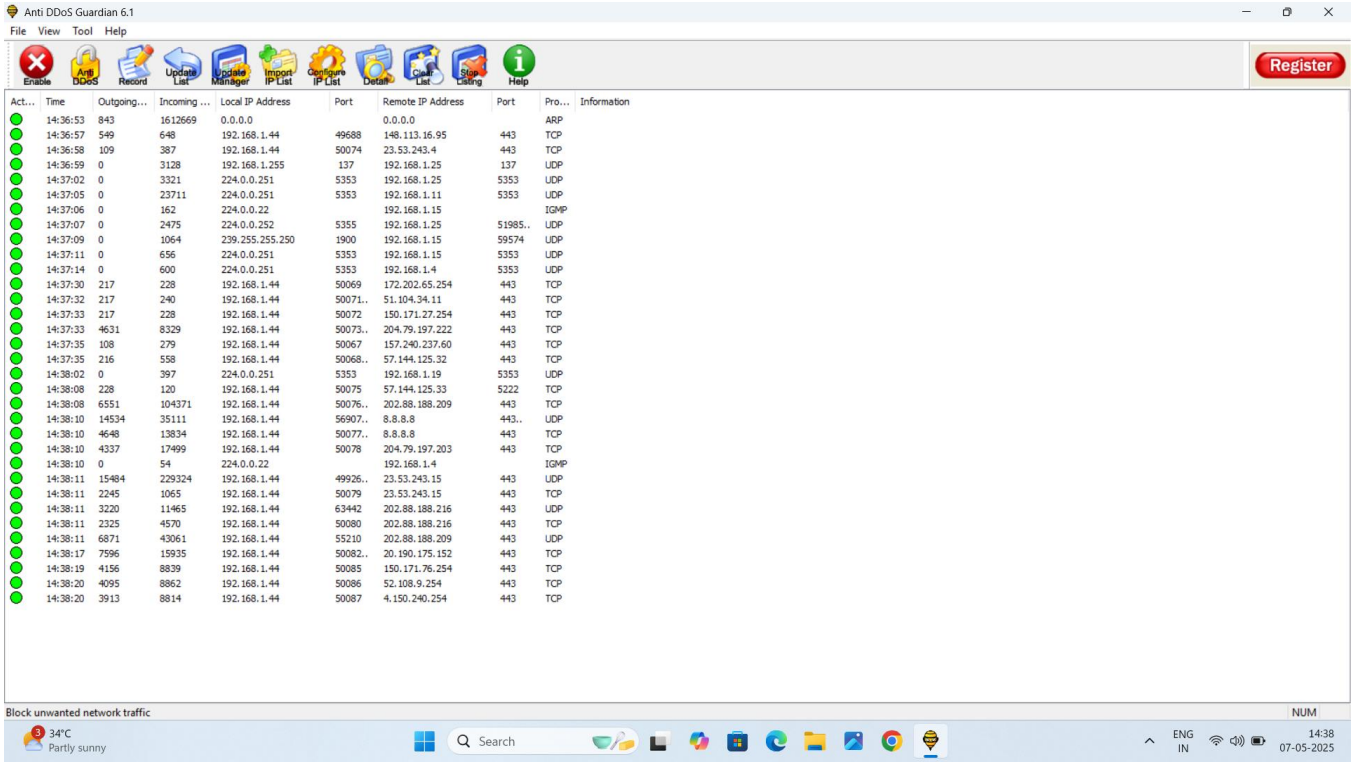
- **Production Deployment:**

  It can be deployed on Windows servers in a production environment.
- **Targeted Protection:**

  Anti-DDoS Guardian can protect various online servers, including Apache servers, IIS servers, game servers, mail servers, and more.
- **Customization:**
  Users can customize configurations to address specific attacks efficiently.

In essence, Anti-DDoS Guardian is a software solution that provides a layer of protection for Windows servers against various types of DDoS and DoS attacks by managing network traffic, detecting malicious activity, and taking actions to mitigate the impact of attacks.

Screenshot of this tool :



Name : kunal Jawale