SIMULATE & ANALYZE DDOS ATTACK

Submitted by:

Ramesh 24109114

Sonia: 24109119

Course: Digital Forensics

Instructor: Muhammad Waqar

UDP FLOOD ATTACK

Objective:

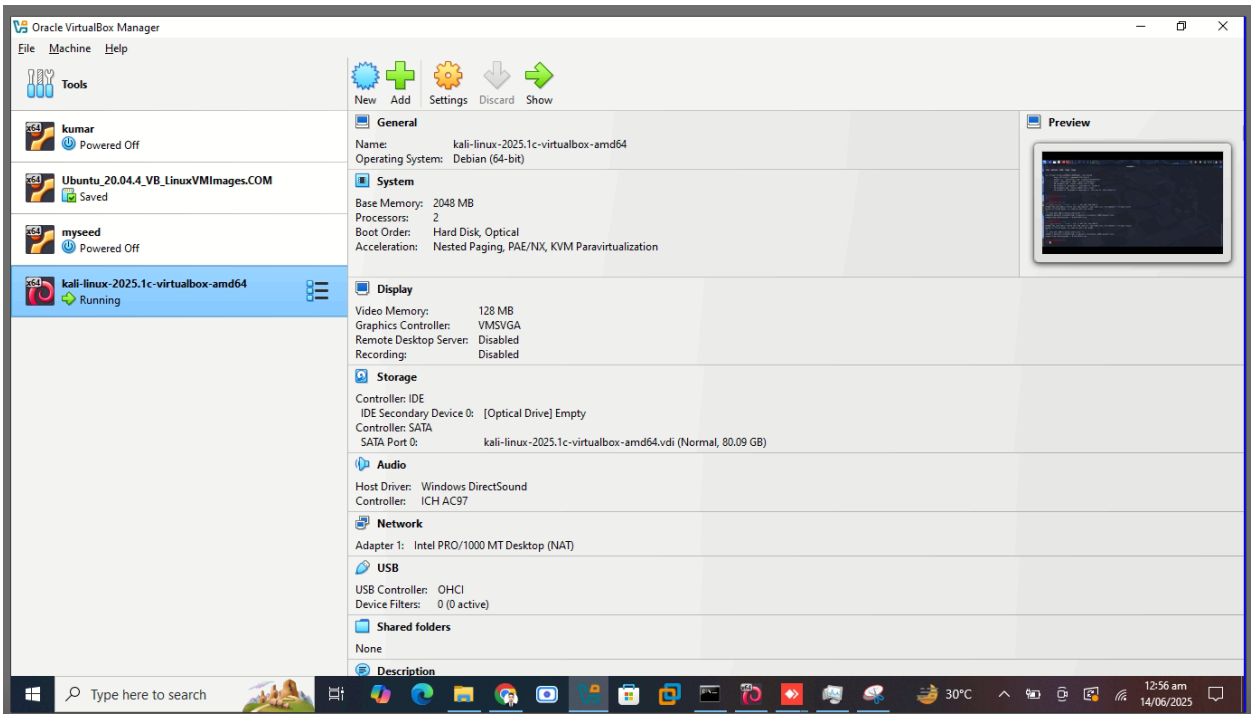
A UDP flood attack is a type of Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack where the attacker **floods** a target system with a large number of UDP (User Datagram Protocol) packets. The goal is to consume the target's resourcessuch as bandwidth or processing powercausing the system to slow down, crash, or become unavailable.

I have performed UDP flood attack Target Machine is my Windows: IP: 192.168.100.6

Victim Machine is Kali Linux:IP: 10.0.2.15.

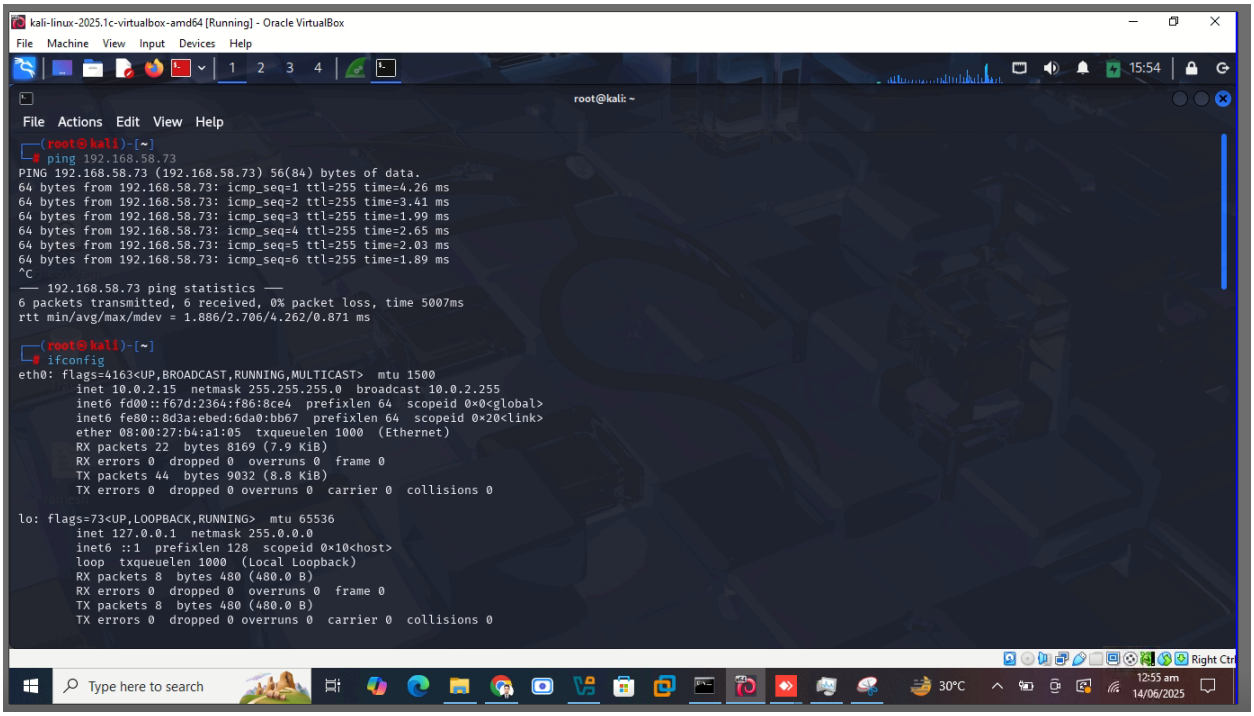
Step 1: **Open Kali linux VM in virtual box.**

This step initiates the attacker machine using Kali Linux in a virtualized environment. Kali provides essential penetration testing tools like hping3.



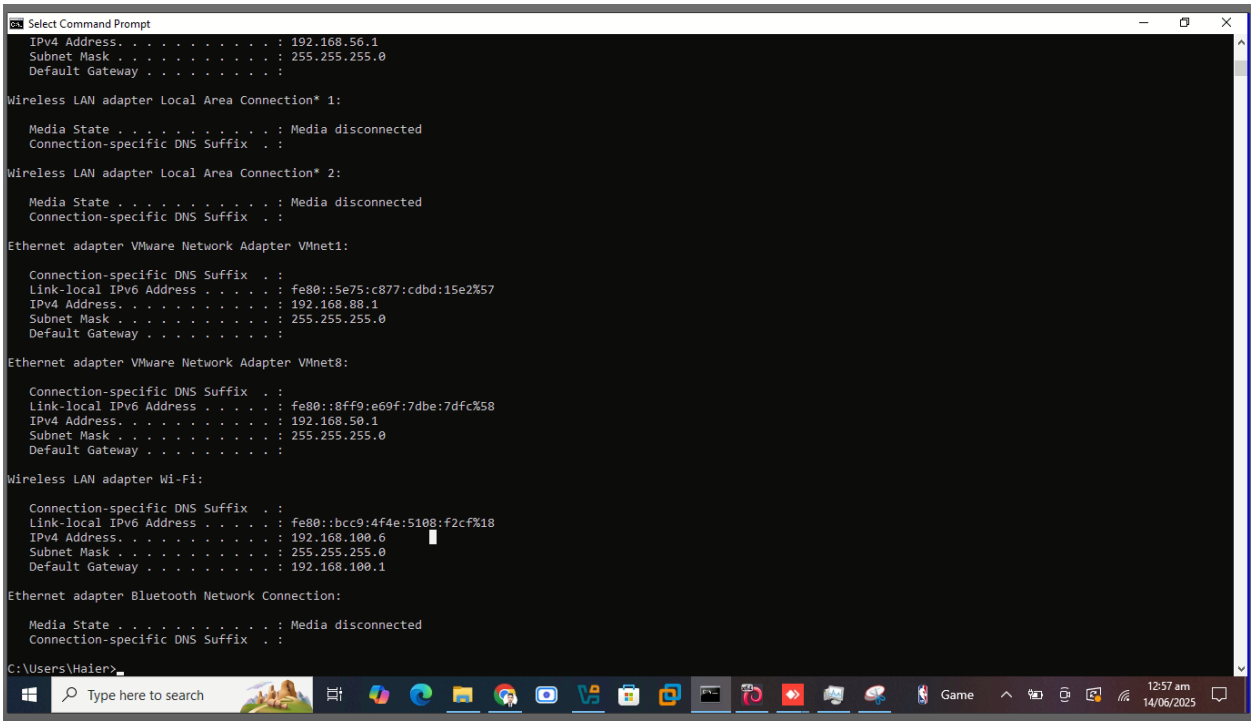
Step 2: Open terminal and run the "ifconfig" command to check ip of Kali Linux.

The ifconfig command displays the IP address of the Kali VM (10.0.2.15). This helps in confirming the network configuration of the attacker.



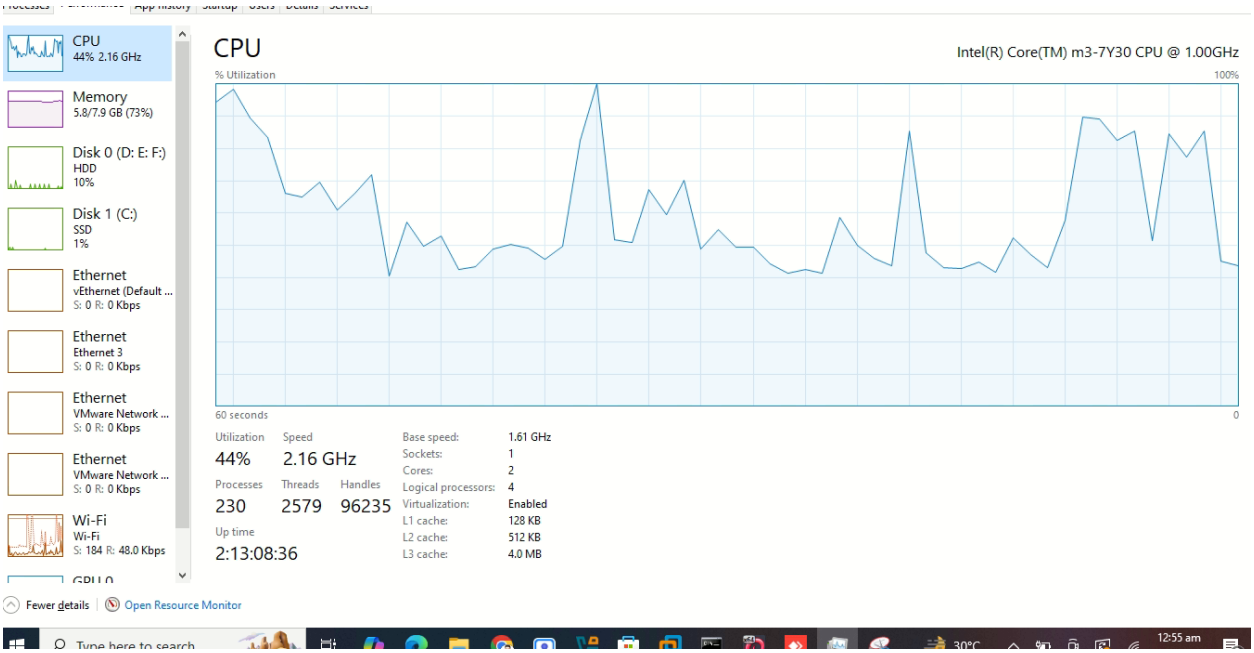
Step 3: Open CMD and run the "ipconfig" command to check ip of Windows.

Running “ipconfig” on the Windows machine shows its IP address (192.168.100.6), which is needed as the target for the UDP flood attack.



Step 4: Windows-based System performance before the attack.

This step records baseline performance (CPU, RAM, network usage) on the Windows machine. It's used for comparing the system's behavior before and after the attack.

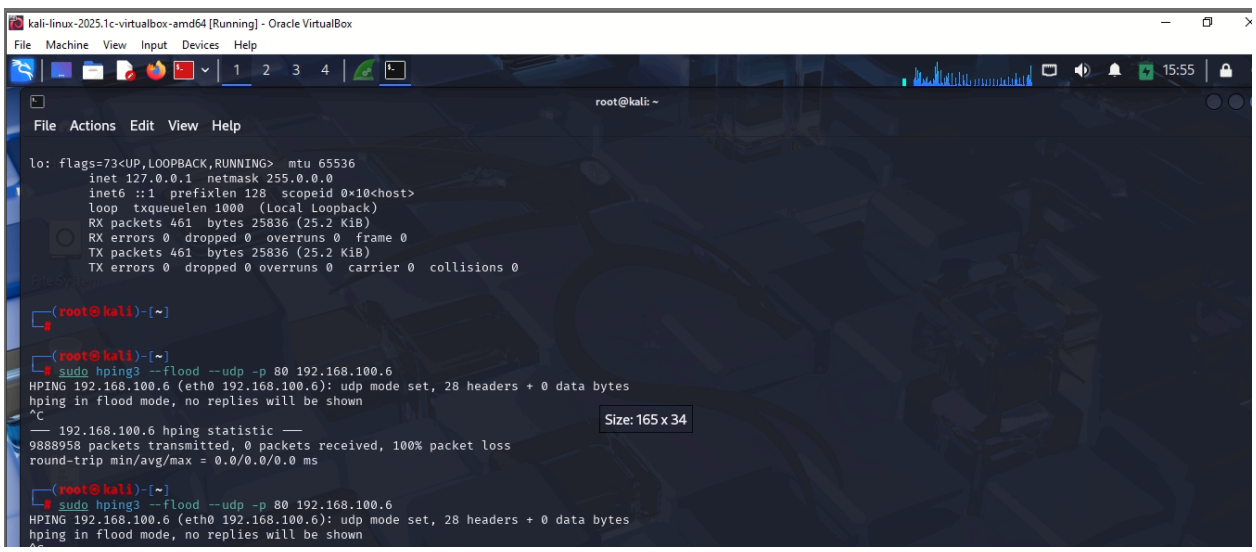


Step 5: sudo hping3 --flood --udp -p 80 192.168.100.6

This command launches a high-speed UDP flood to port 80 of the Windows machine, aiming to consume its resources and network stack.

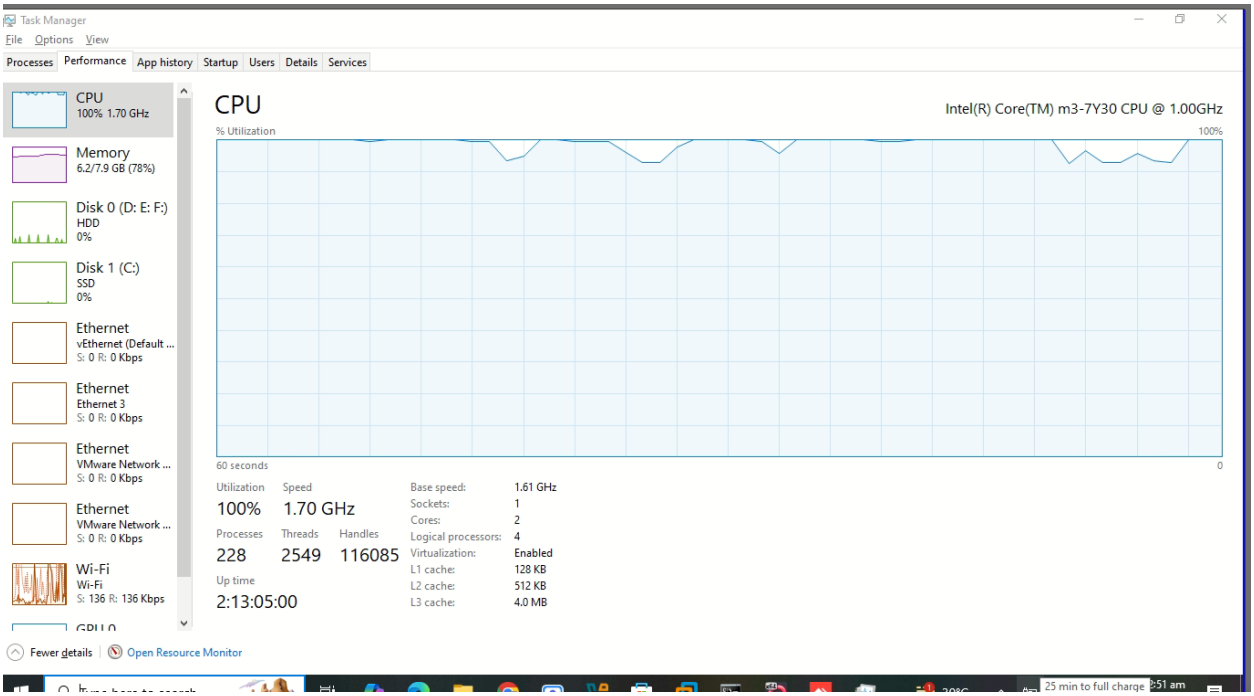
- **Hping3** is a powerful command-line network tool used primarily for packet crafting and network testing. It is often used in penetration testing to simulate various types of traffic, including DoS/DDoS simulation, firewall testing, network scanning.
- **sudo means:**
    - Run this command as an administrator (superuser).

- **flood** Sends packets as fast as possible (flooding)
    - **UDP** sends UDP packets (instead of TCP)
    - -**p** 80 Target port (80 = HTTP, you can change this)



Step 6: Windows-based System performance after attack:

Observe the impact of the DDoS attack likely a spike in CPU usage, high network activity, and potential unresponsiveness, indicating successful disruption.



Forensic Elements in this Project

1. Traffic Capture and Analysis (Using Wireshark)

- Capturing network traffic during the attack is core forensic work.
- You analyze packet volume, frequency, and source/destination IPs to identify suspicious patterns.
- Example: Detecting a sudden burst of UDP packets to a single port from one or multiple IPs.

2. Source IP Verification and Spoofing Detection

- Forensics involves examining if source IPs are real or spoofed.
- Tools like Wireshark help you identify anomalies, such as non-existent IPs or private IPs not belonging to your network.

3. System Logs and Performance Metrics

- You compare system resource usage before and after the attack.
- Forensics here includes collecting and preserving CPU, memory, and network usage data as digital evidence of impact.

Forensics in this project is about acting like a network investigator:

Capturing data, identifying what happened, who did it (or where it came from), how it happened, and what it affected.