**Name:** Aum Panchal

**Reg No:** 22BCE8203

**Source Code and Project Documentation**

**Install Required Platform**

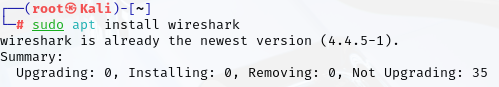
Tools Needed:

* 🐧 Kali Linux: Pre-installed with most tools.
* 🪟 Windows 7 VM: Used as the target machine for scanning/phishing.
* 📡 Both should be on the same network (use "Host-only" or "Bridged Adapter" in VirtualBox settings).

Install Wireshark on Kali (if not already):

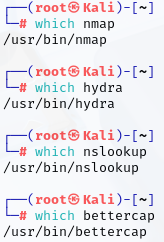
**sudo apt update**

**sudo apt install wireshark**



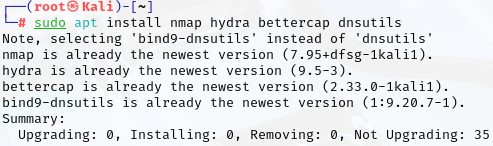
**Step 2: Import Required Libraries / Tools**

You don’t need Python libraries here. These are command-line tools, not Python scripts. But you must ensure they are installed:



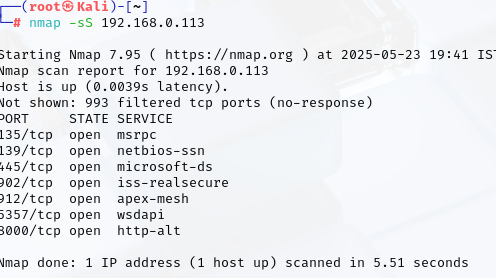
If anything is missing, install like this:

**sudo apt install nmap hydra bettercap dnsutils**

****

**Step 3: Check Manual Commands**

**nmap -sS 192.168.0.113**

****

**DDoS Attack –** A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server.

**Volume Based Attacks –** Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attacker’s goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

Volumetric attacks can also be called “floods” because an attack floods a target’s server with requests, like unwanted pings. Attacks are measured in bits per second (bps) or Gigabits per second (Gbps).

**Protocol Attacks –** Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS, and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and [load balancers](https://www.imperva.com/learn/availability/load-balancing-algorithms/), and is measured in packets per second (Pps).

Protocol attacks often work at layers 3 and 4 of the OSI model on network devices like routers. Because they are on the network layer, they are measured in packets per second (pps).

Below is a sampling of different network-layer DDoS attack types:

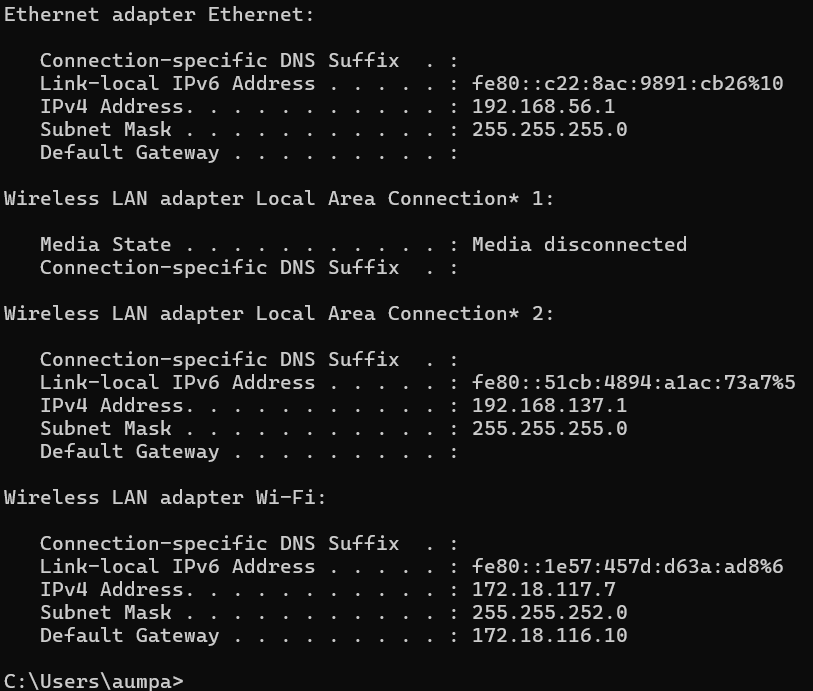
* UDP floods
* SYN floods
* NTP amplification
* DNS amplification
* IP fragmentation

**Application Layer Attacks –** Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows, or OpenBSD vulnerabilities, and more. Comprised of seemingly legitimate and innocent requests, these attacks aim to crash the web server, and the magnitude is measured in Requests per second (Rps).

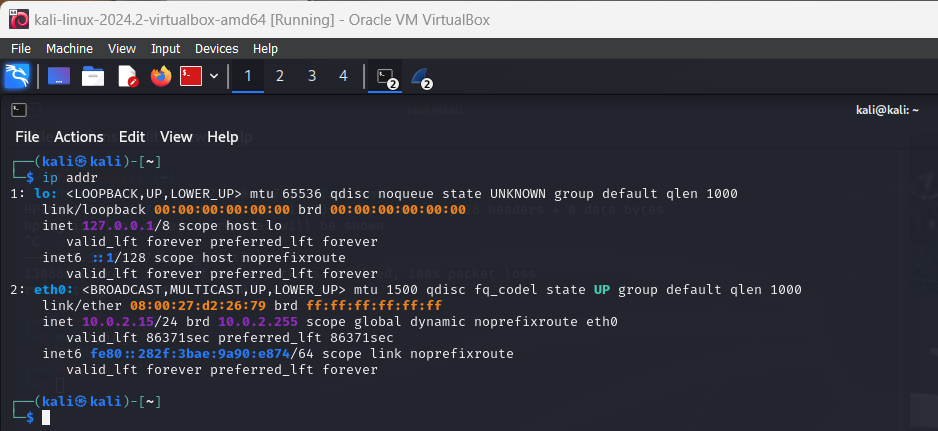
An application layer attack typically includes hitting the web server, running PHP scripts, and contacting the database to load web pages. A single HTTP request, which is simple to execute on the client side, can cause a server to execute many internal requests and load numerous files to fulfil the request, which slows the system.

An application layer attack can also be a multi-vector attack that uses a combination of volumetric and protocol attacks to increase the likelihood of taking a service offline. Because of their complexity and effectiveness, multi-vector attacks are increasingly popular among cybercriminal groups.

My Windows IP Address – 172.18.117.7



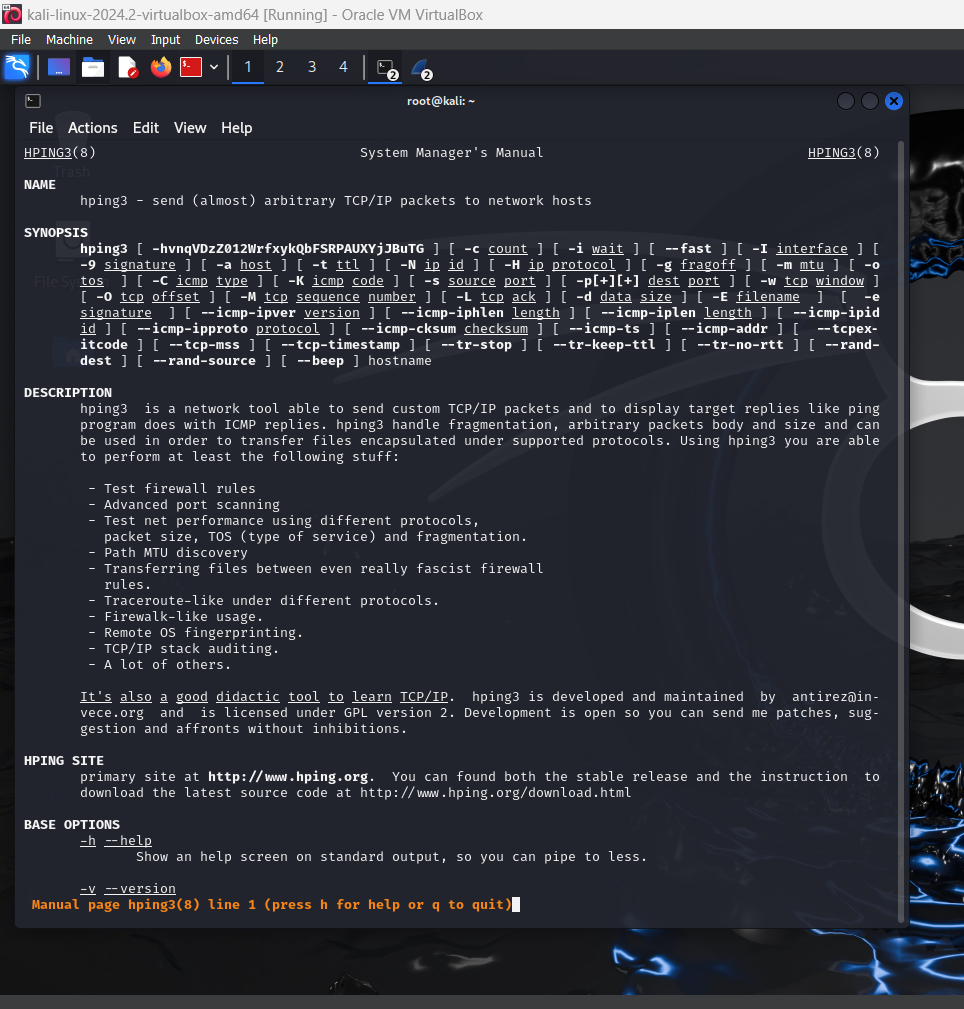
My Kali Linux VM IP Address – 10.0.2.15



**1. ICMP Flood Attack – DDoS Attack**

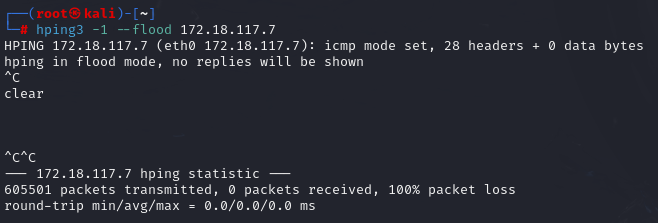
The [Internet Control Message Protocol (ICMP)](https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/), which is utilized in a Ping Flood attack, is an internet layer protocol used by network devices to communicate. The network diagnostic tools [traceroute](https://en.wikipedia.org/wiki/Traceroute) and [ping](https://en.wikipedia.org/wiki/Ping_(networking_utility)) both operate using ICMP. Commonly, ICMP echo-request and echo-reply messages are used to ping a network device for the purpose of diagnosing the health and connectivity of the device and the connection between the sender and the device.

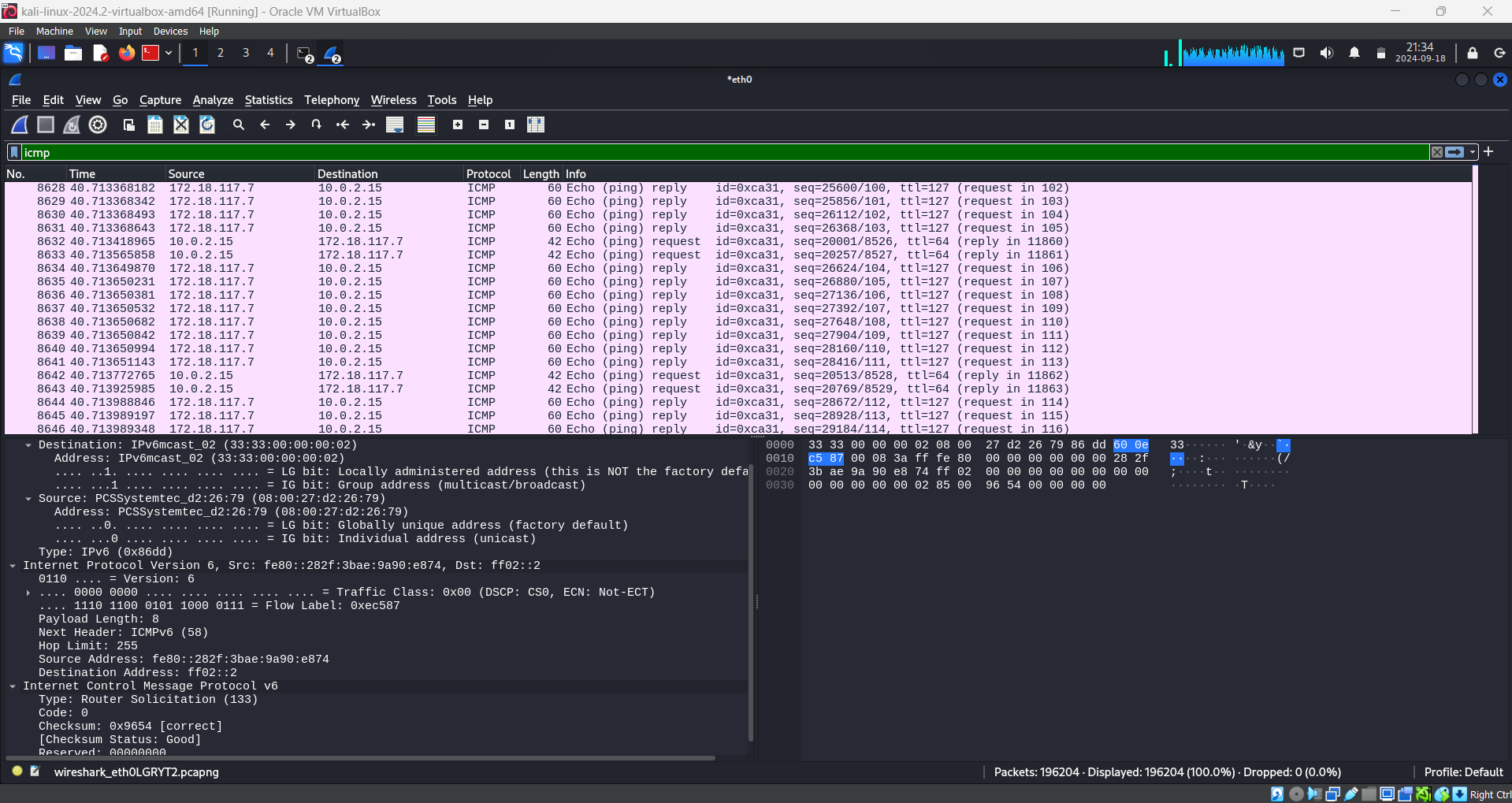
**Command - Man hping3**



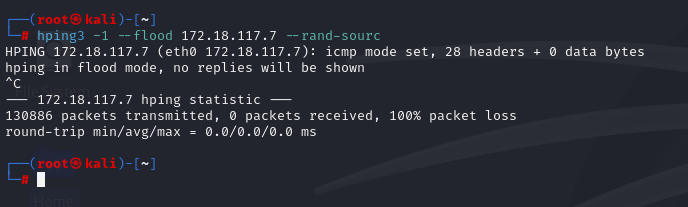
**Command – hping3 --help**



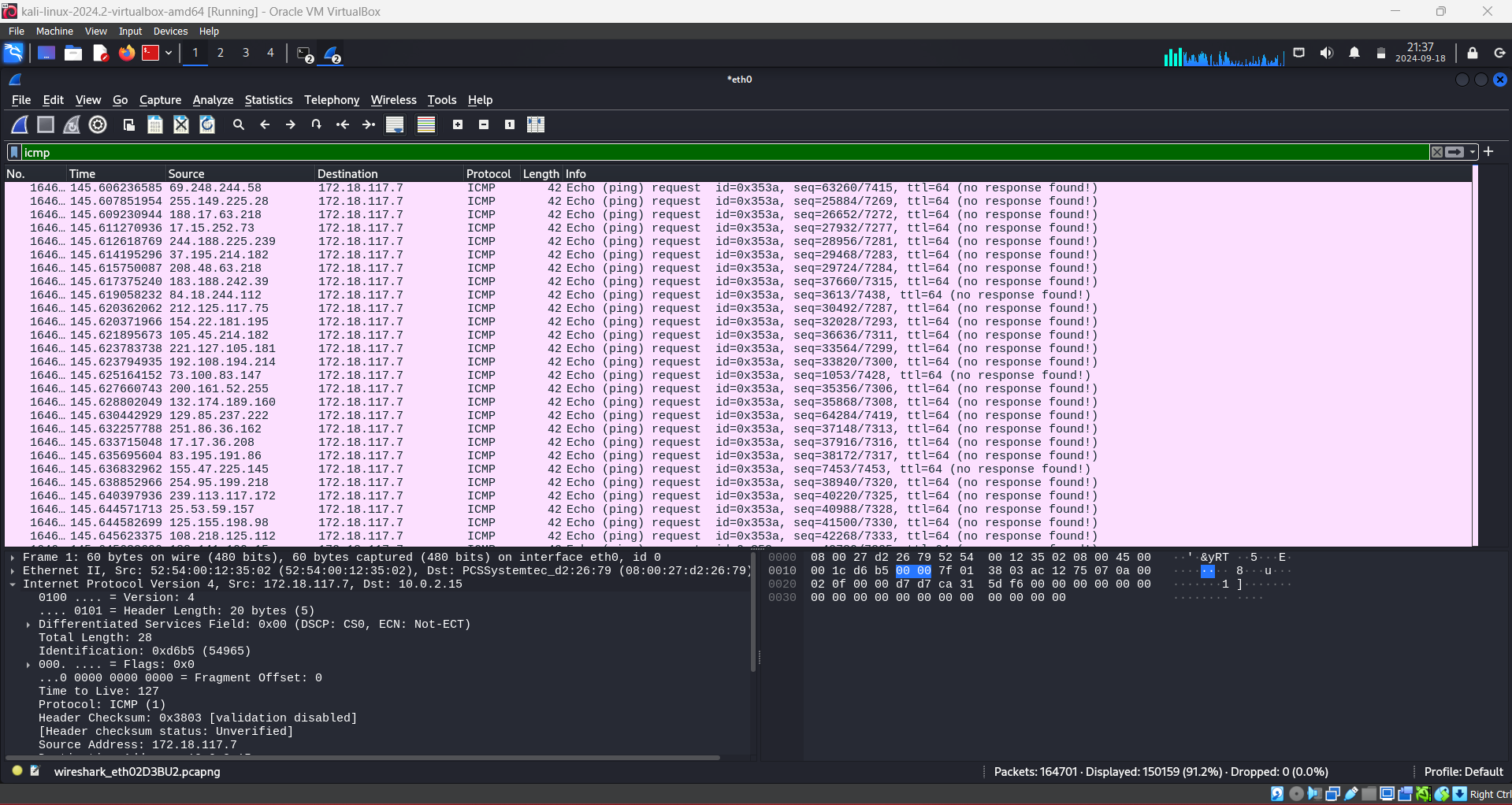
**Command – hping3 -1 –flood 172.18.117.17**



**ICMP Attacking from Random Sources –**



**Command - hping3 -1 –flood 172.18.117.17 –rand-sourc**

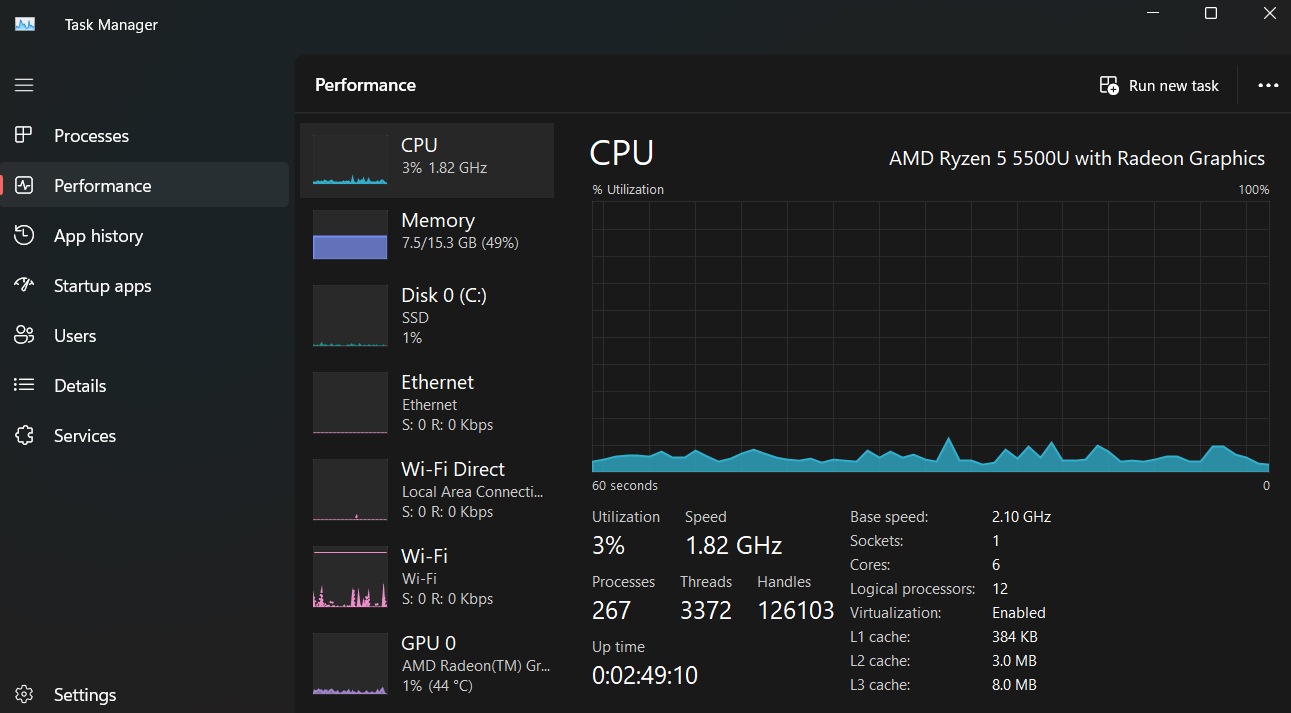


**2. UDP Flood Attack – DDoS Attack**

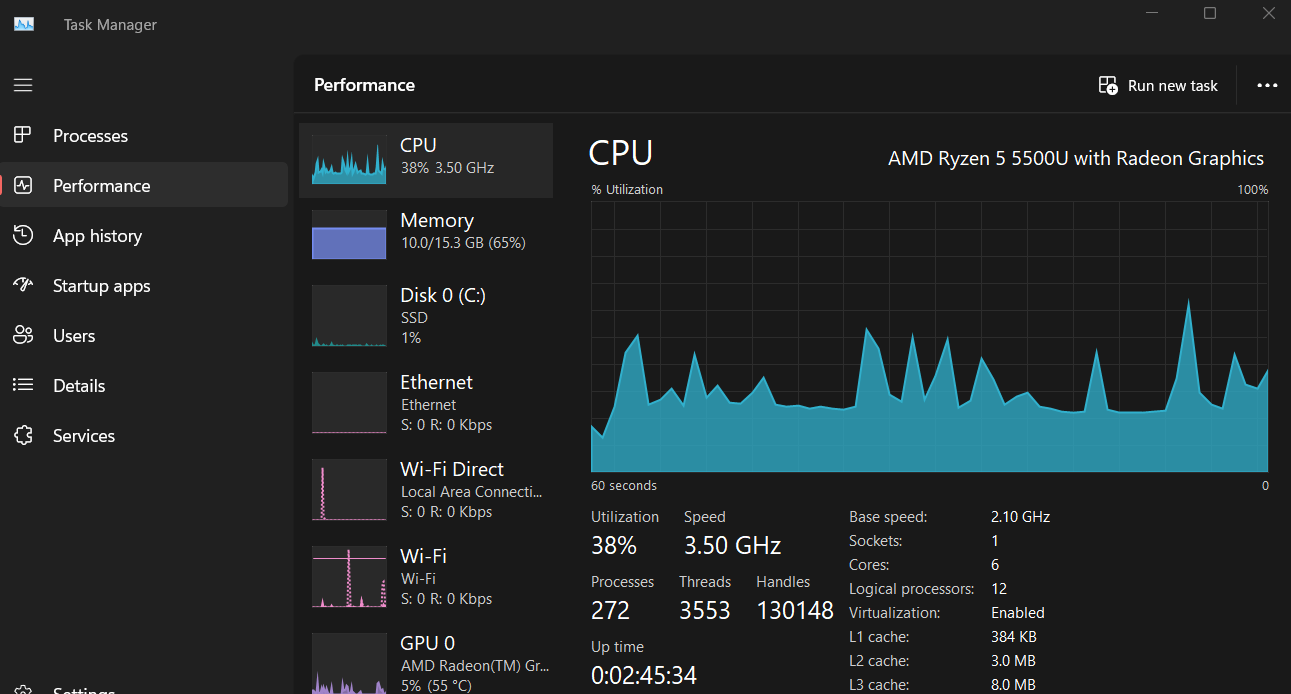
UDP flood is a type of denial-of-service (DoS) attack designed to render a system, server, bandwidth, or machine unavailable for legitimate users and requests. A sessionless protocol, UDP floods are highly effective and require few resources to execute. DoS or DDoS (distributed denial-of-service) attacks are often part of highly complex threats that combine multiple attack vectors (aka multi-vector), to target an organization’s IT environment. Unlike TCP DDoS attacks, where threat actors leverage TCP SYN packets, UDP packets can be fragmented and cause as much harm as a normal UDP flood attack.

The same commands can be use in the Kali Linux Root Terminal for UDP Flooding attack as well. We juts need to change the mode from -1(--icmp) to -2(--udp).

**Command – hping3 -2 –flood 172.18.117.17**



As we can clearly see the spikes in the CPU Utilization, hindering its usage as the UDP packets are bombarded on the target PC and hence the network is flooded

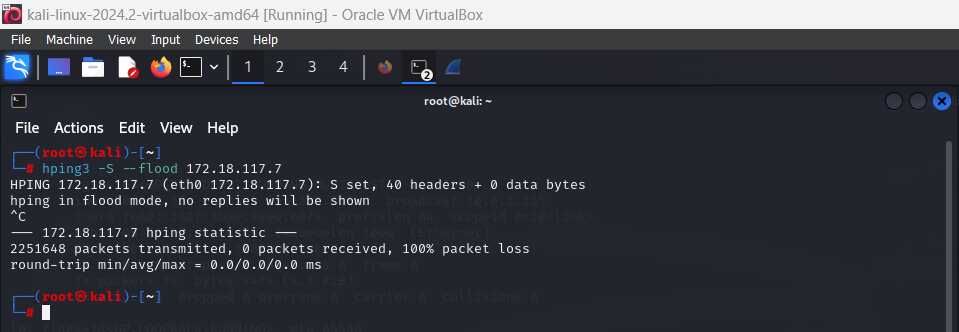


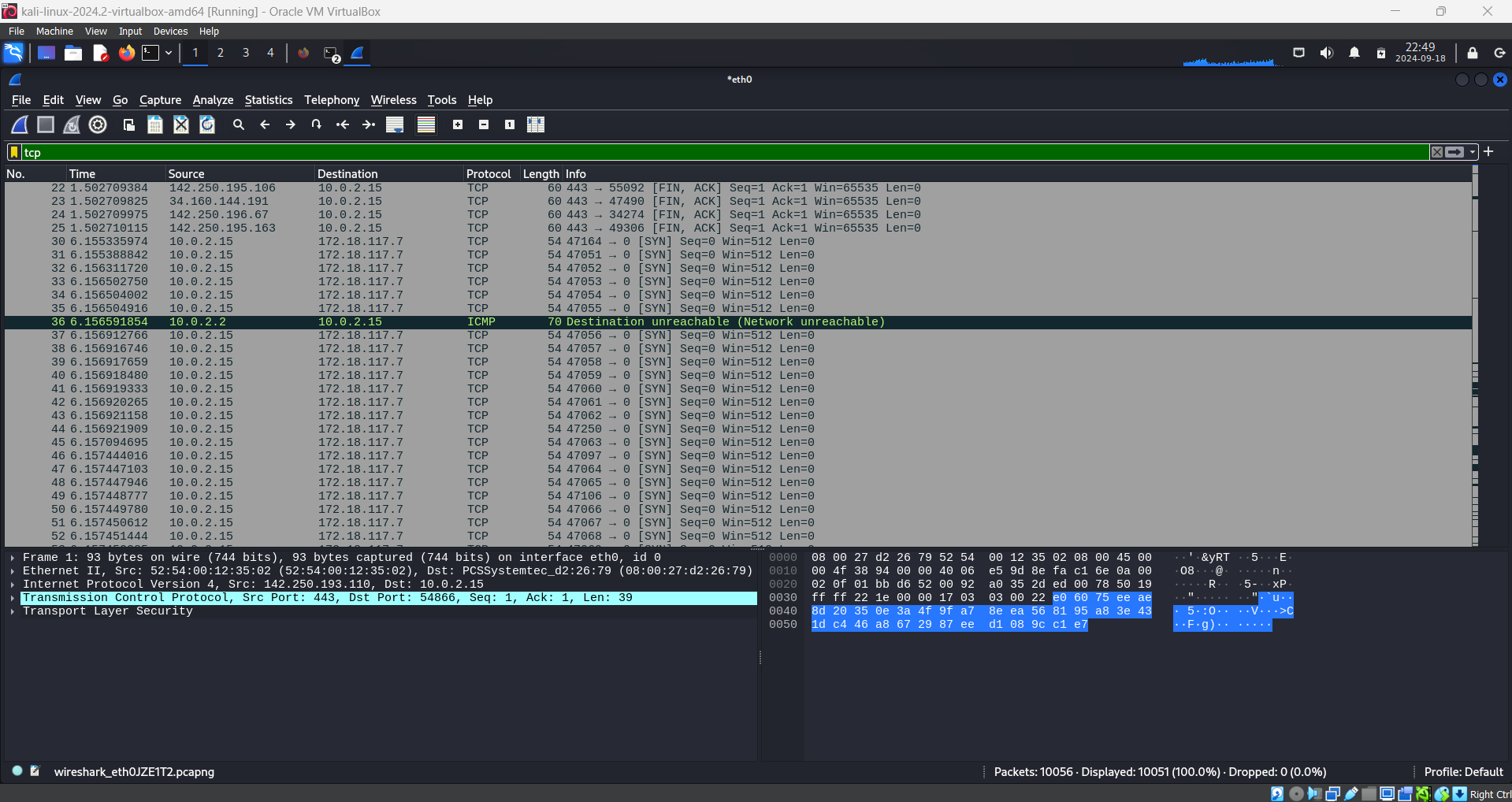
**3. TCP SYN DoS Attack –**

A TCP SYN Flood attack seeks to exploit the TCP three-way handshake mechanism, which is foundational for establishing connections in [TCP/IP](https://www.imperva.com/learn/ddos/tcp-transmission-control-protocol/) networks.

In a TCP SYN Flood attack, the malicious entity sends a barrage of SYN requests to a target server but intentionally avoids sending the final ACK. This leaves the server waiting for a response that never comes, consuming resources for each of these half-open connections.

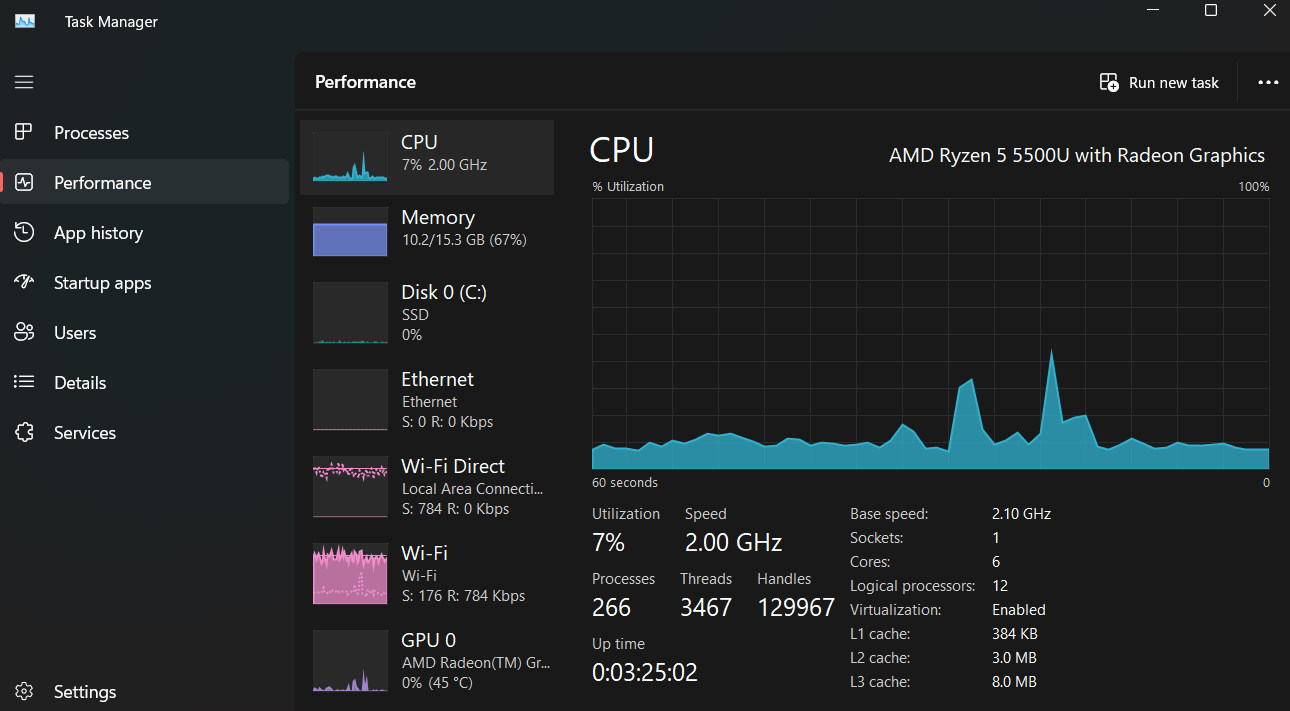
**Command – hping3 -S –flood 172.18.117.17**

****

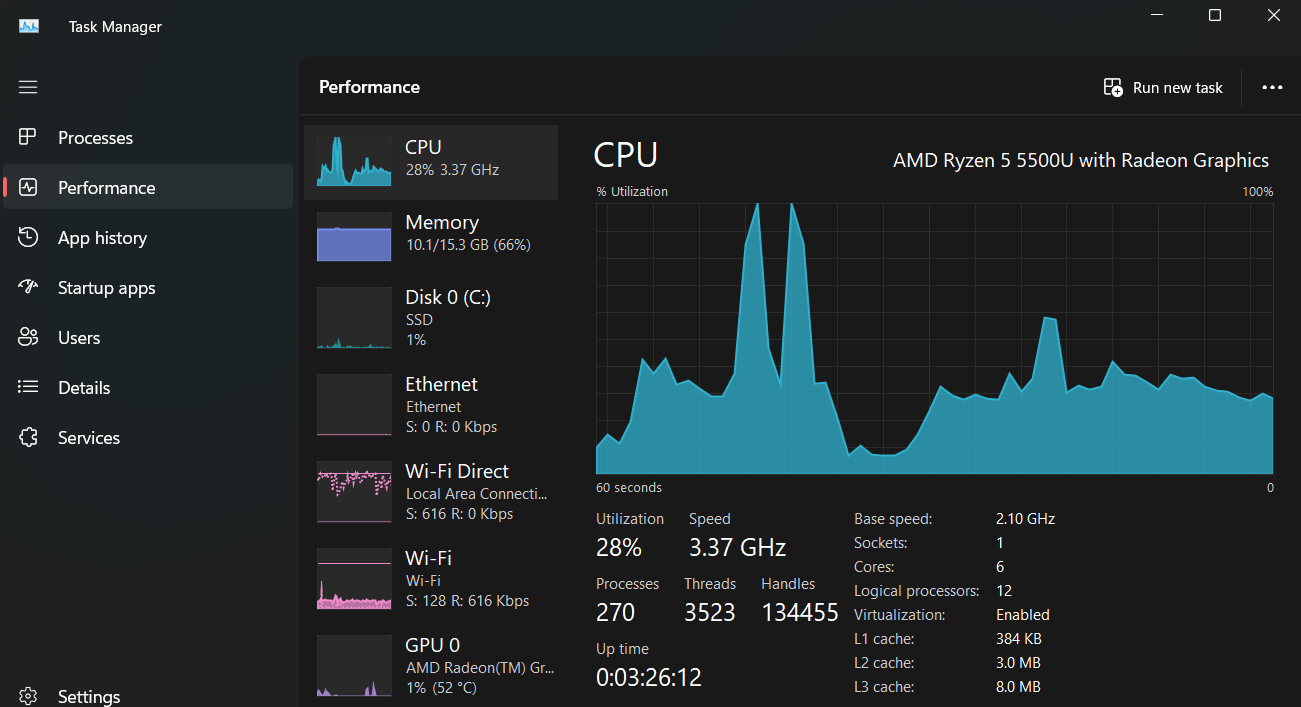
****

Only SYN Responses and no Acknowledgement in return.

Before the TCP SYN Attack –

****

After the TCP SYN Attack –

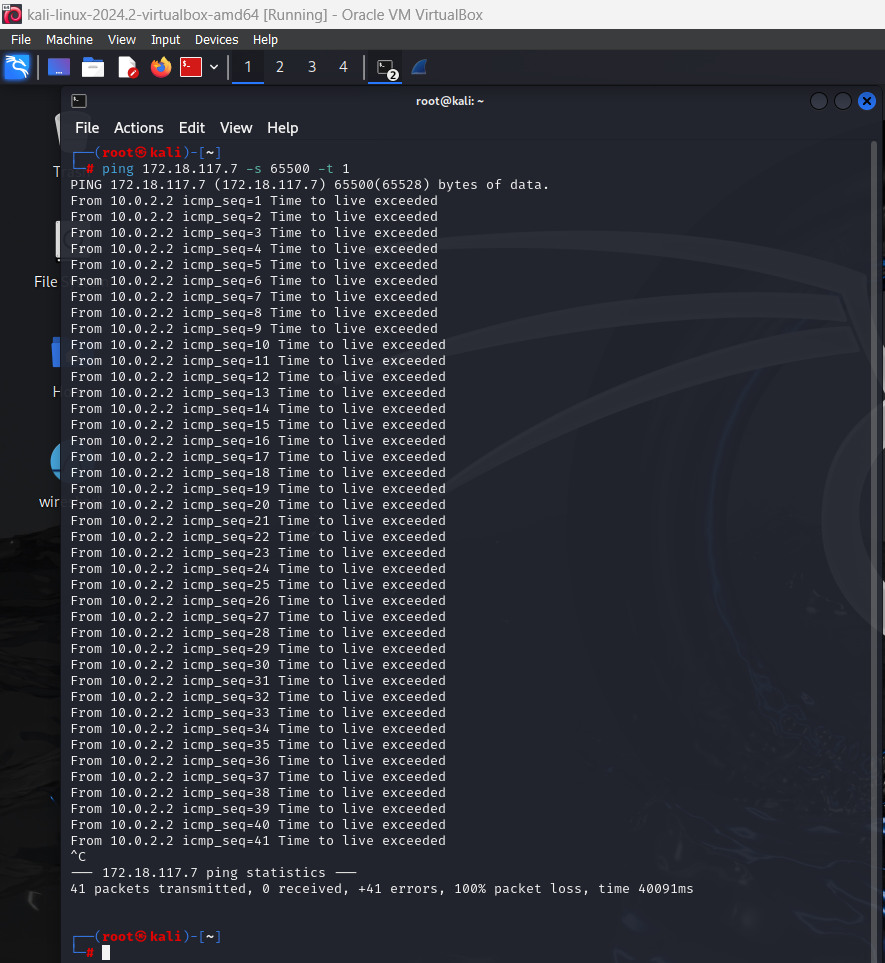
****

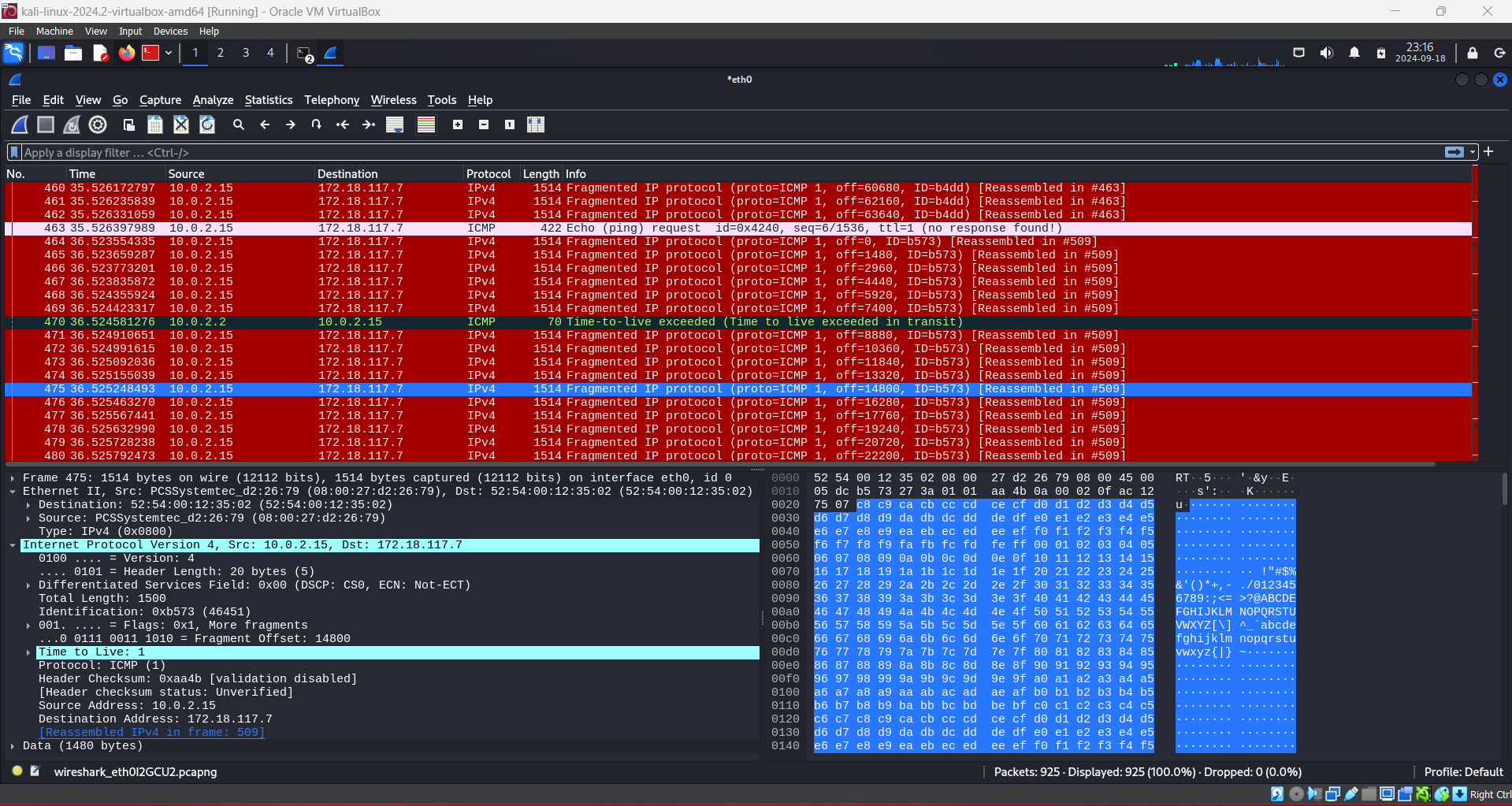
**4. Ping of Death Attack**

A ping of death attack is a type of denial-of-service (DoS) attack that uses oversized data packets to crash or destabilize a computer or service.

An [Internet Control Message Protocol (ICMP)](https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/) echo-reply message or “ping”, is a network utility used to test a network connection, and it works much like sonar – a “pulse” is sent out and the “echo” from that pulse tells the operator information about the environment. If the connection is working, the source machine receives a reply from the targeted machine.

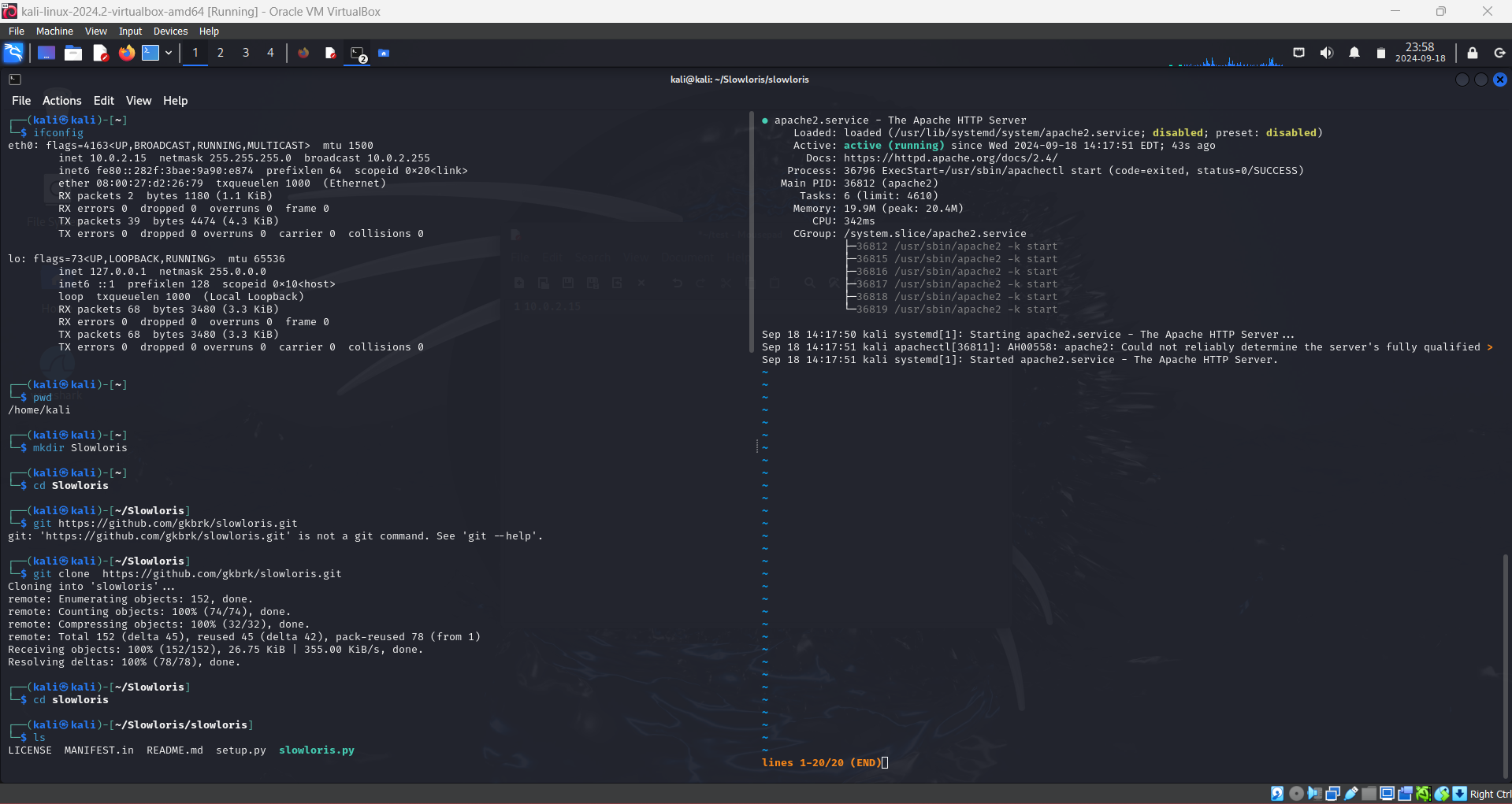
While some ping packets are very small, IP4 ping packets are much larger, and can be as large as the maximum allowable packet size of 65,535 bytes. Some [TCP/IP](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) systems were never designed to handle packets larger than the maximum, making them vulnerable to packets above that size.

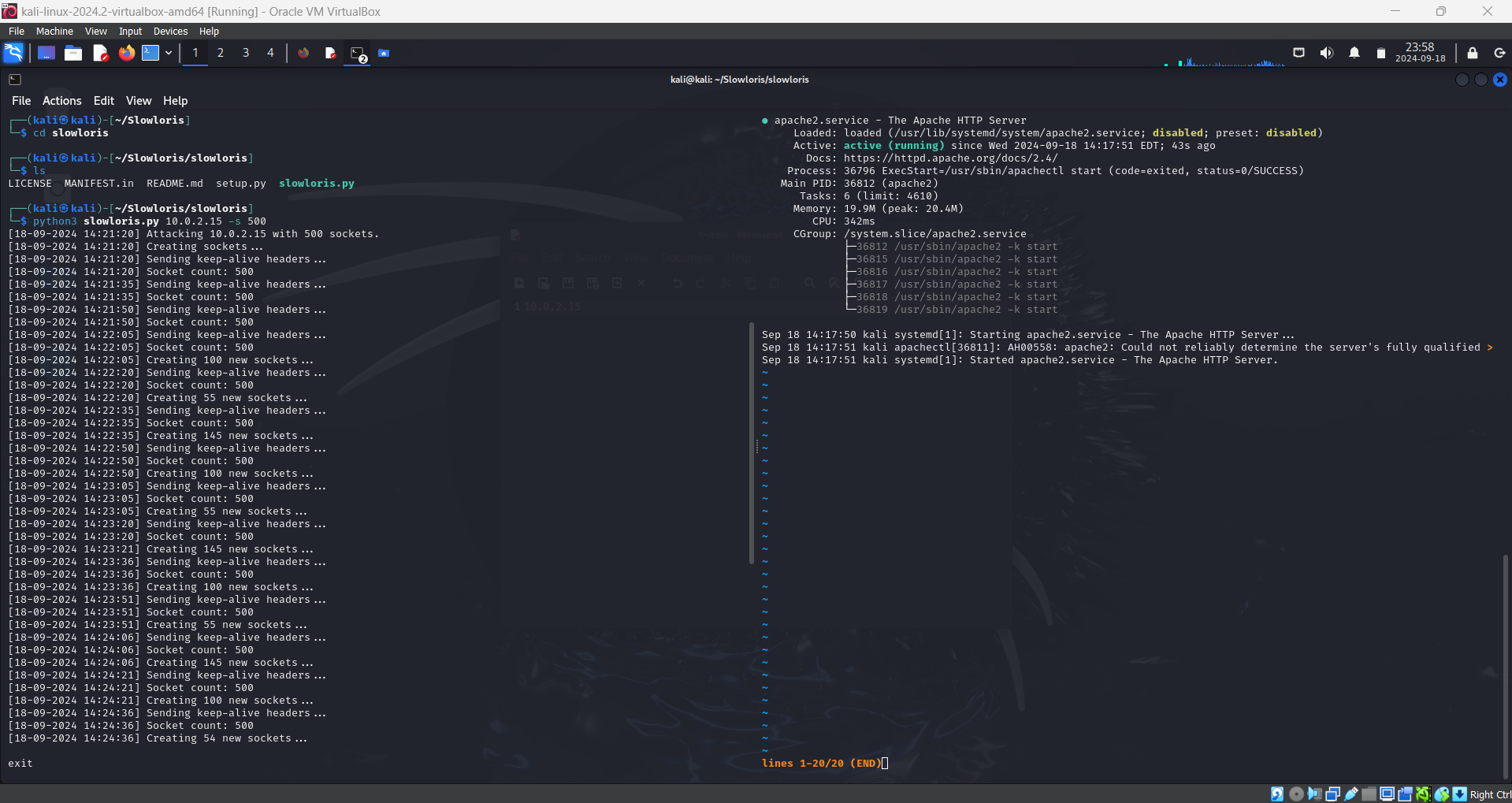


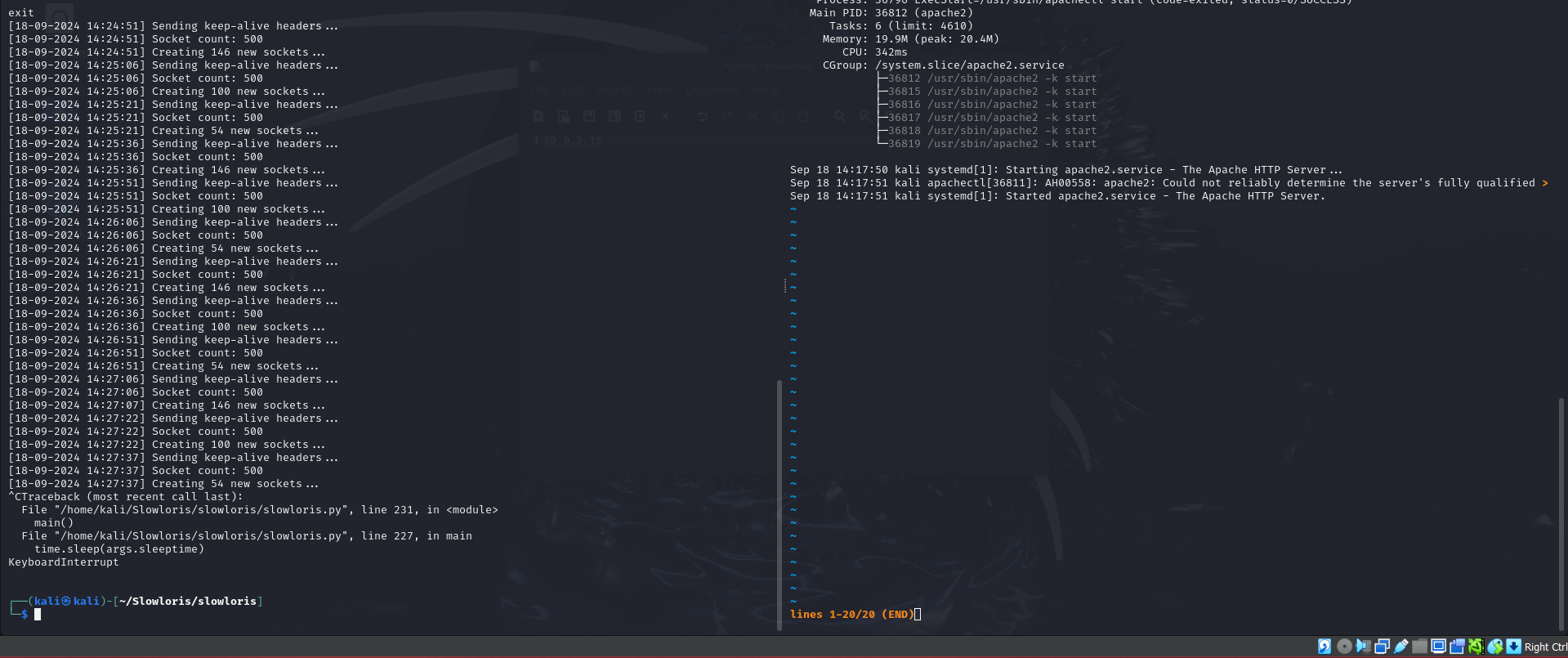


**5. Slowloris Attack –**

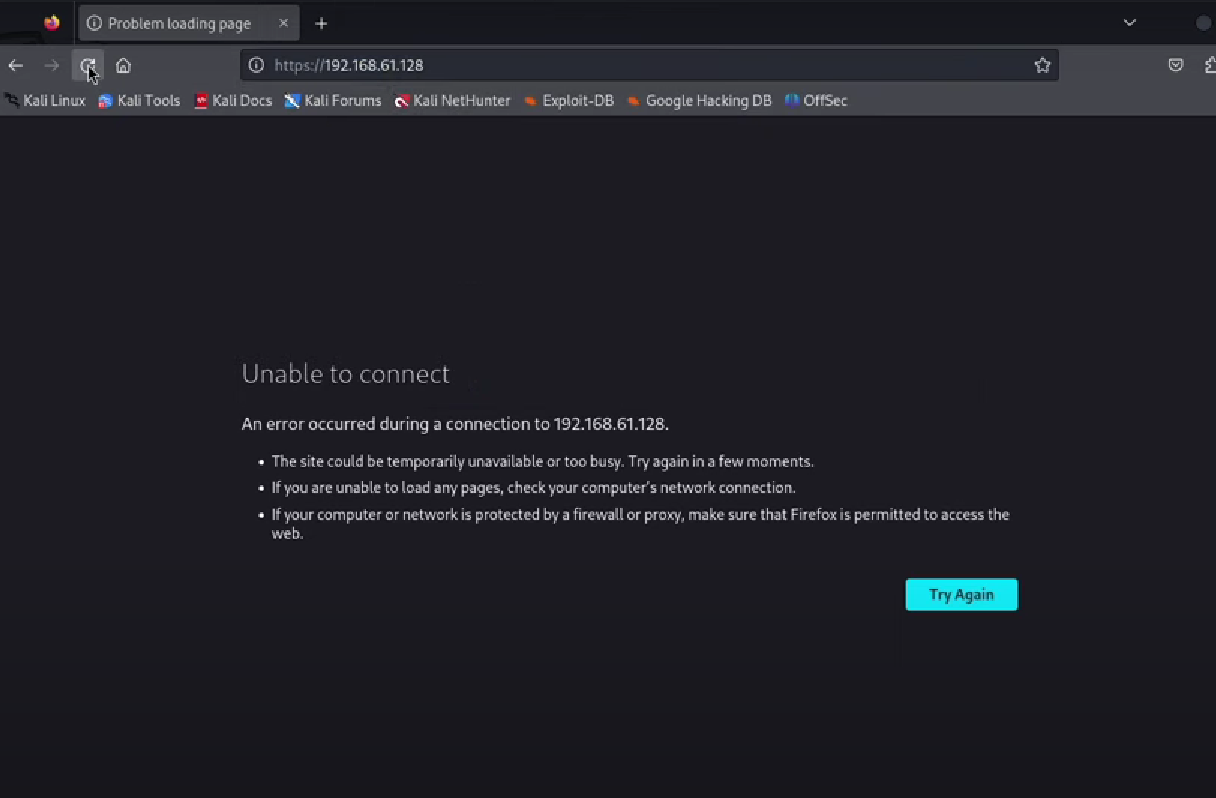
Slowloris is a type of denial-of-service attack tool which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports. Slowloris tries to keep many connections to the target web server open and hold them open as long as possible.

****

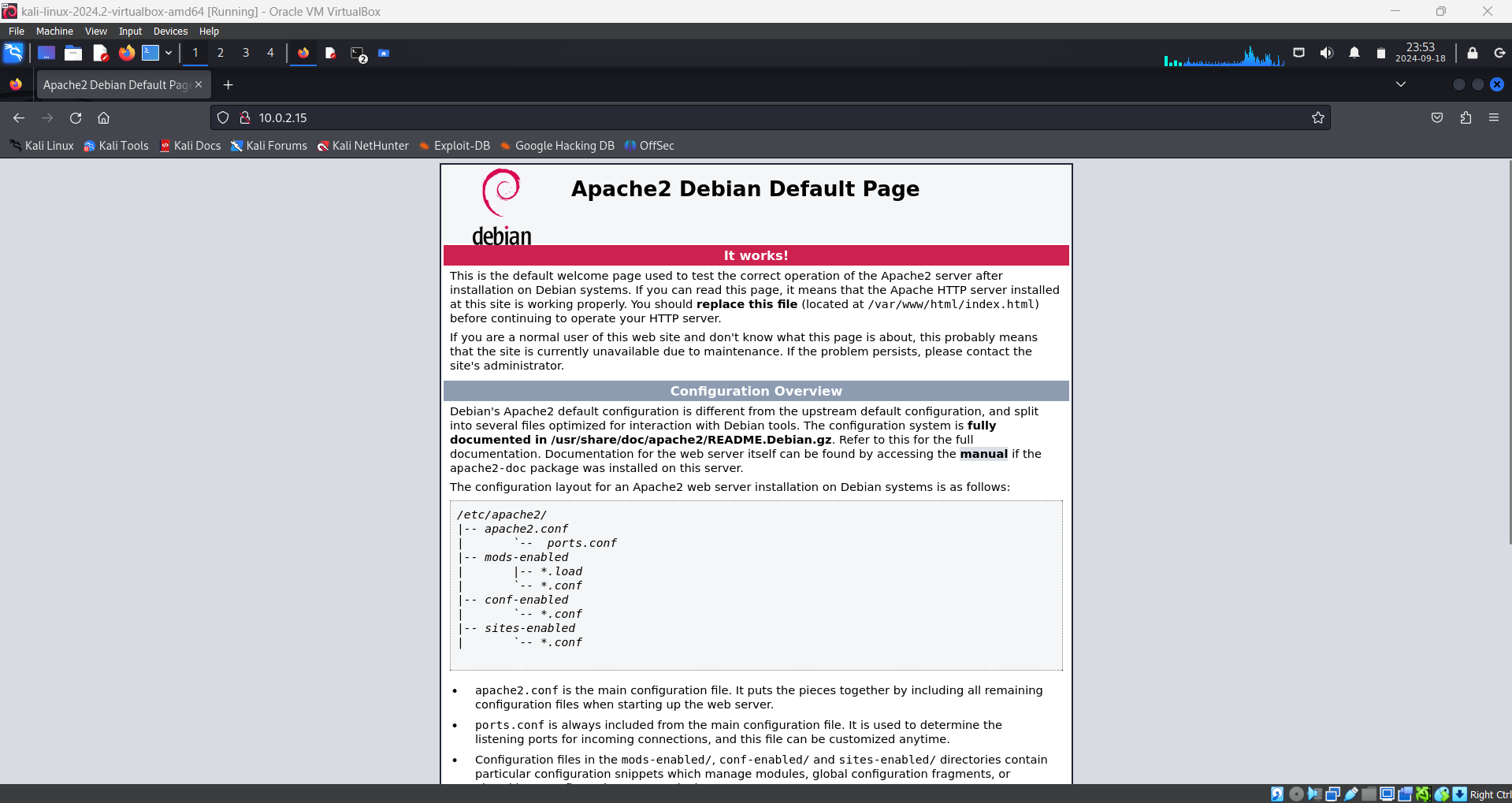
****

****

Before Slowloris Attack -

****

After Slowloris Attack -

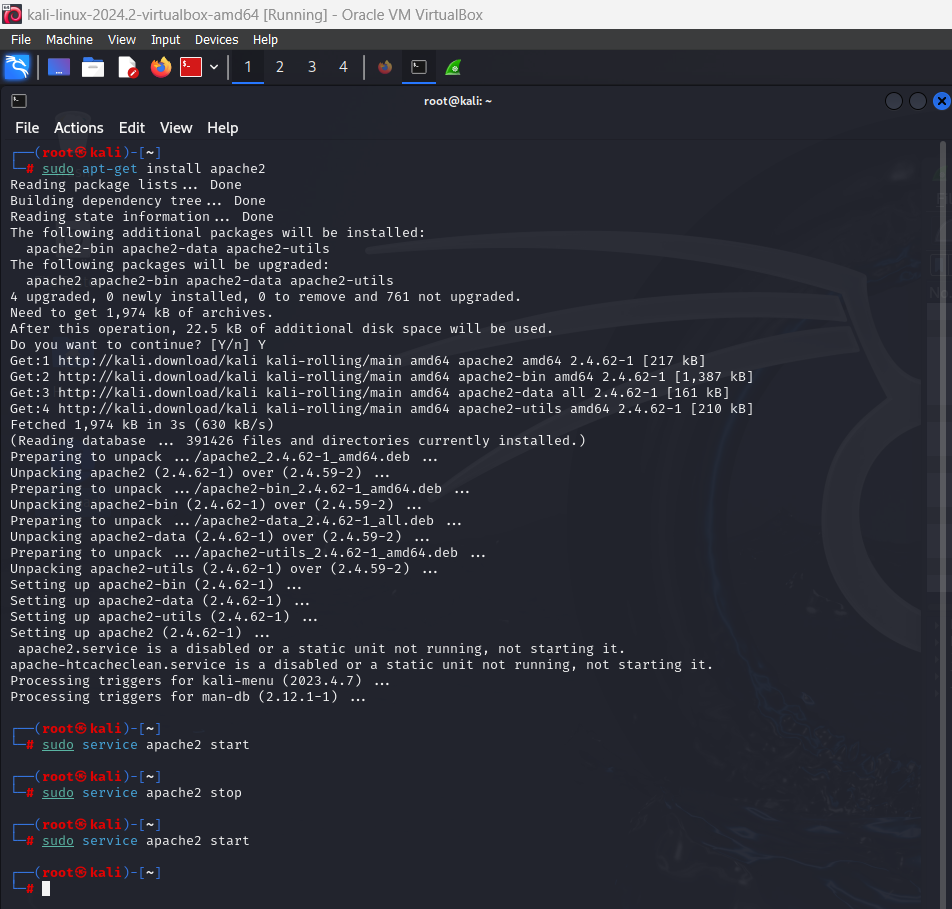


It just holds on to this page when we are executing the attack and as soon as we terminate the script, the page is no more available to connect.

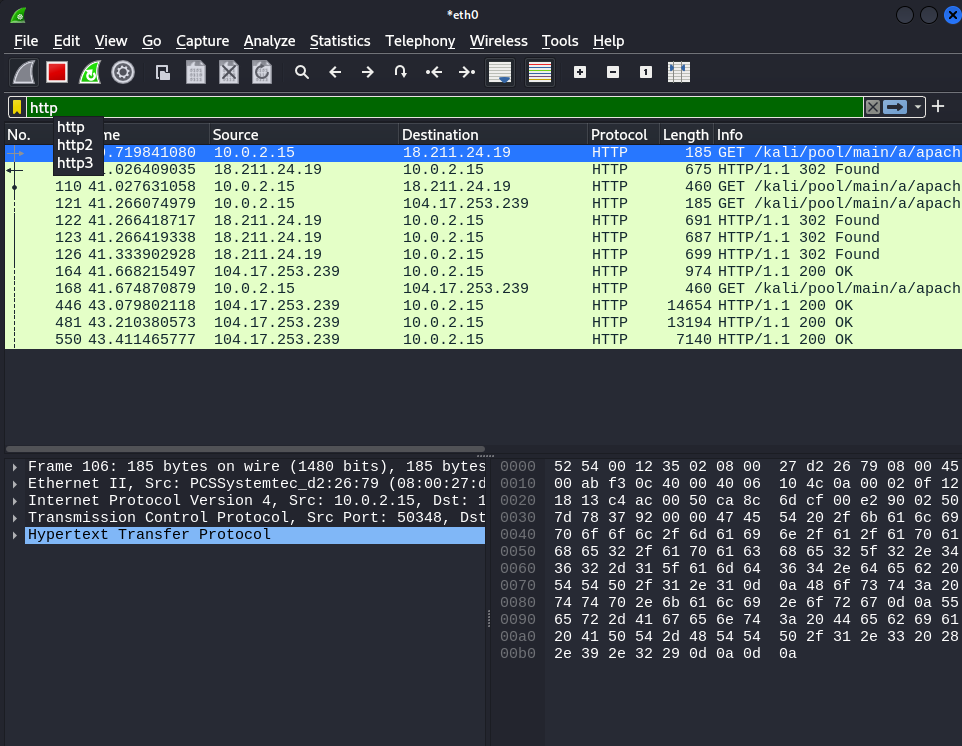
**6. HTTP Flood Attack –**

An HTTP flood attack is a type of volumetric [distributed denial-of-service (DDoS)](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/) attack designed to overwhelm a targeted server with [HTTP requests](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/). Once the target has been saturated with requests and is unable to respond to normal traffic, [denial-of-service](https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/) will occur for additional requests from actual users.

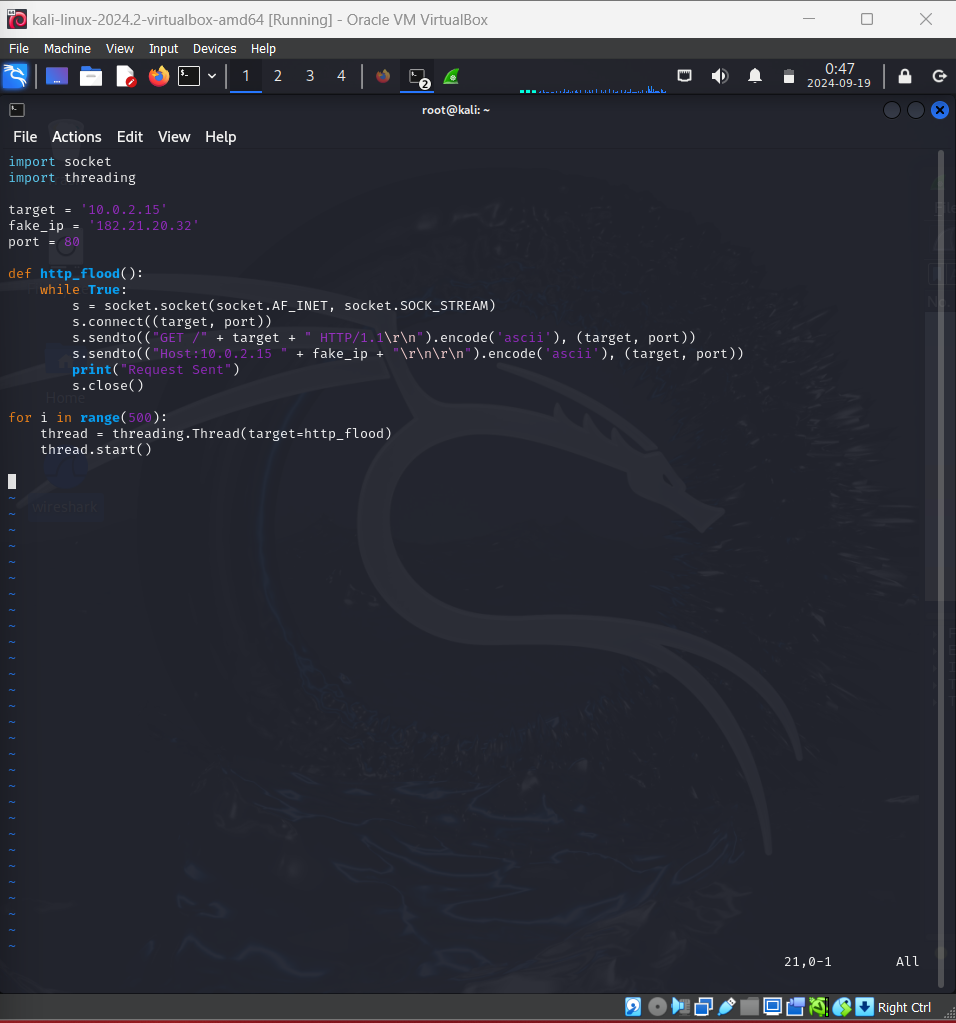
HTTP flood attacks are a type of “layer 7” DDoS attack. [Layer 7](https://www.cloudflare.com/learning/ddos/what-is-layer-7/) is the application layer of the [OSI model](https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/), and refers to internet protocols such as HTTP. HTTP is the basis of browser-based internet requests, and is commonly used to load webpages or to send form contents over the Internet. Mitigating application layer attacks is particularly complex, as the malicious traffic is difficult to distinguish from normal traffic.



Wireshark Analysis



Python Code for HTTP Flood Attack –



Output of the Code -

