1.Denial of Service (DoS) Attack Simulation Module: Simulate various types of DoS attacks, developing countermeasures to mitigate their impact.

For the Denial of Service (DoS) Attack Simulation Module, I undertook several crucial steps in the background research to understand, simulate, and counteract various DoS attacks.

Firstly, I delved into the realm of DoS attacks, comprehending the nuances of different attack types such as **ping flood** and **syn flood attacks**.

#Background Research

Understanding DoS Attacks:

- Researched and understood various types of Denial of Service (DoS) attacks, such as ping flood and syn flood attacks.

Choosing Simulation Tools:

- Selected appropriate tools for simulating DoS attacks. I used hping3 a popular tools for sending packets.

Setting Up Virtual Machines:

- Configured virtual machines (VMs) for the attack simulation, here I have used Kali Linux and Parrot Security for simulation.

Capturing Traffic with Wireshark:

- Used Wireshark to capture network traffic during the DoS attack simulations.

Developing Countermeasures:

- Worked on developing countermeasures to mitigate the impact of DoS attacks. Countermeasures can include implementing firewalls, intrusion prevention systems, rate limiting, and other security measures to protect against such attacks.

#ping-flood attack:

Ping flood, also known as ICMP flood, is a type of Denial of Service (DoS) attack where an attacker overwhelms a target system with a flood of Internet Control Message Protocol (ICMP) Echo Request (ping) packets.

The objective is to consume the target's network resources, such as bandwidth and processing power, rendering it unable to respond to legitimate network requests.

This is the demonstration video of the attack:

ping_flood.webm

#syn-flood attack:

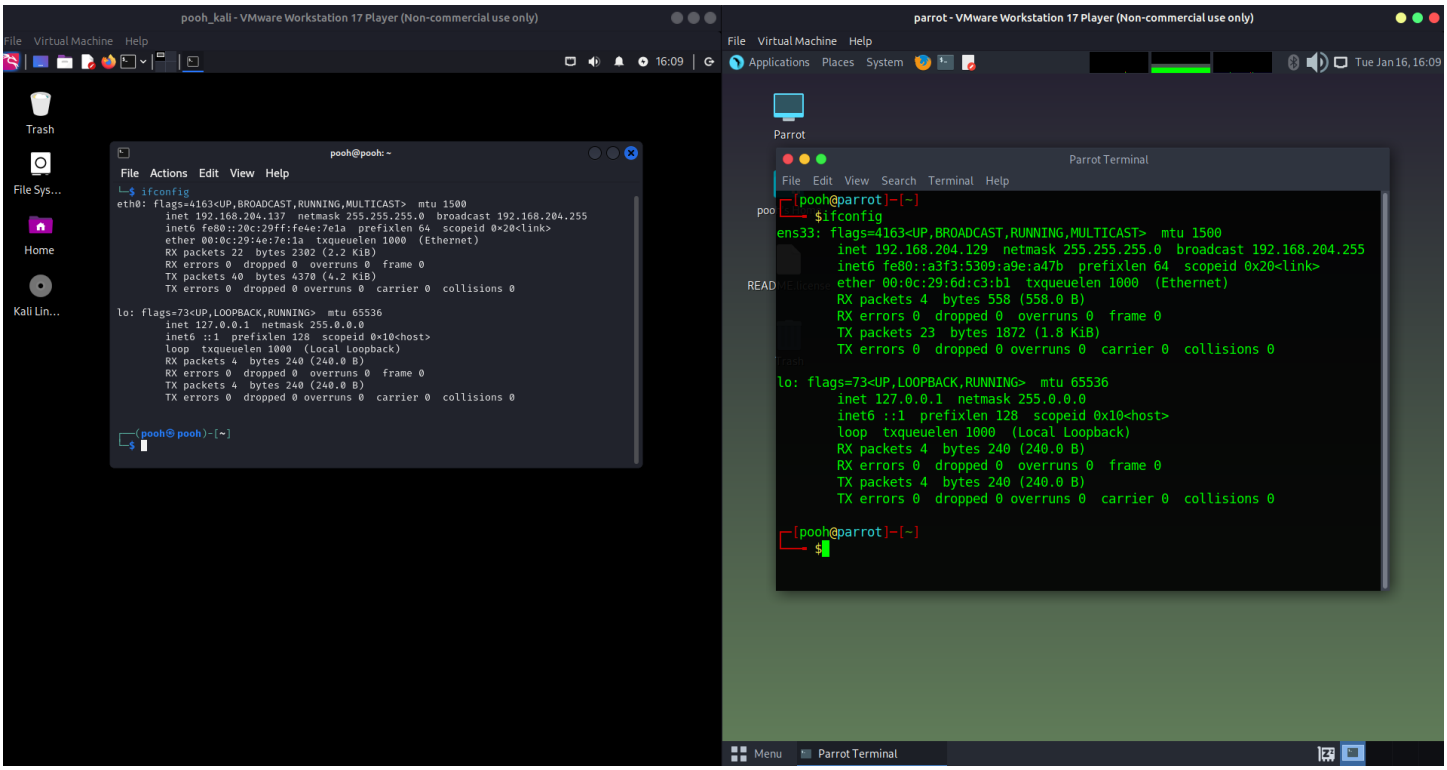
SYN flood is a form of DoS attack targeting the three-way handshake process in the Transmission Control Protocol (TCP). The attacker floods the target system with a high volume of TCP connection initiation (SYN) packets.

The goal is to overwhelm the target's ability to complete the handshake process, exhausting resources and preventing legitimate connections.

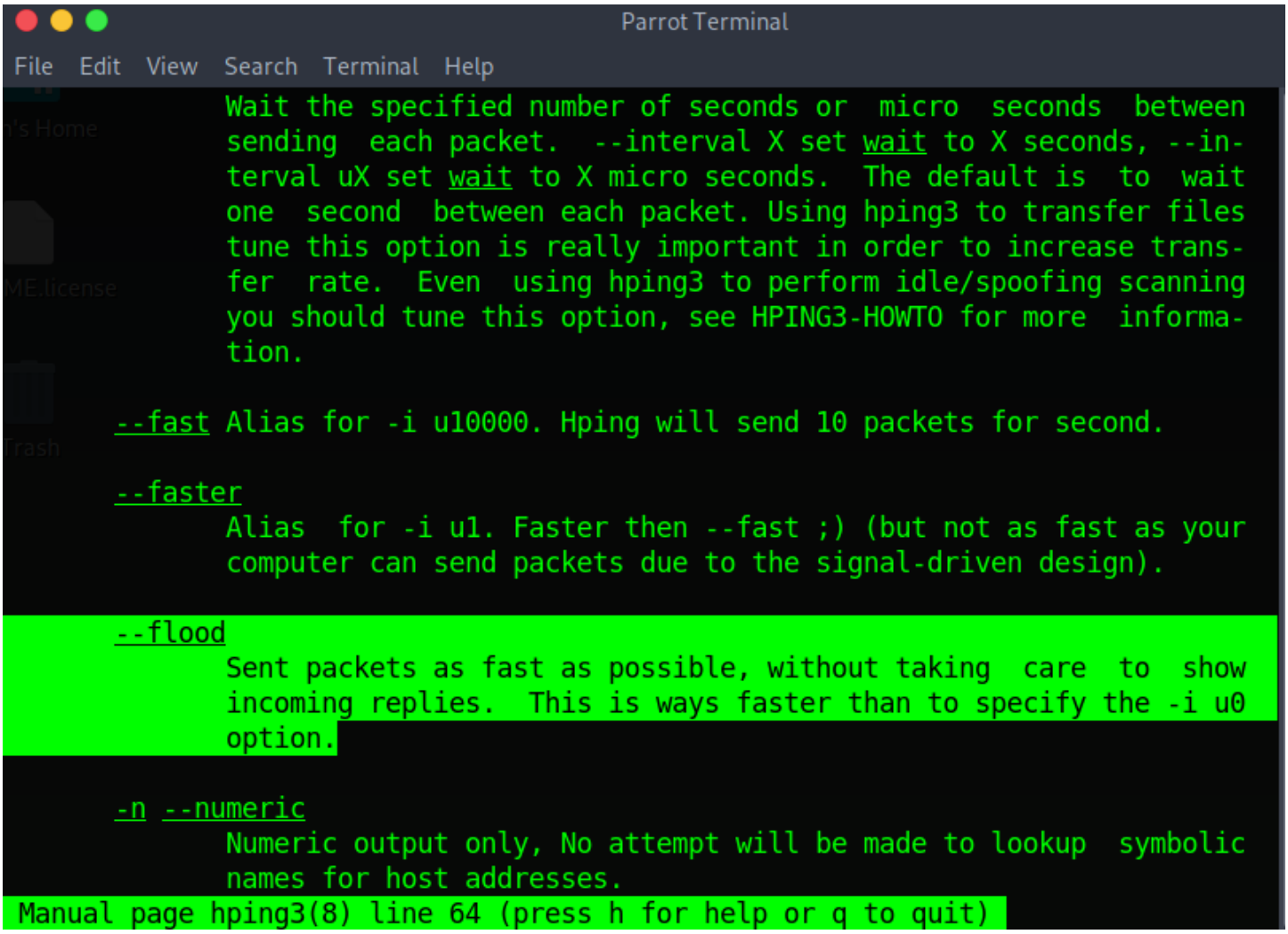
This is the video demonstration of the attack:

syn_flood.webm

Thes are the two hosts:



This is the hping3 method for flooding the packets:



#Observations:

Attack Impact:

- The simulations successfully demonstrated the significant impact of DoS attacks on network resources. Response times were severely affected, and service availability experienced disruptions during the simulated attacks.

Resource Exhaustion:

- The DoS attacks effectively exhausted network resources, leading to increased latency and potential service unavailability.

  THIS CAN BE SEEN IN THE SYN-FLOOD VIDEO WHERE I HAVE SHOWN THE INCREASED TIME TO OPEN FIREFOX AND SERVICES AS THE DENIAL Of SERVICE IS HAPPENING.

Response Time Analysis:

- Response time analysis provided insights into the network's ability to recover from DoS attacks. It was observed that response times gradually improved after the attacks ceased, emphasizing the importance of timely recovery mechanisms.