# **OSS LAB PROJECT**



***SUBMITTED TO*: MS. RICHA KUMARI**

***SUBMITTED BY*: MUSKAN - 2021UCP1356**

**PRASANSHA - 2021UCP1386**

**DATE: APRIL 10th may, 2024**

# 

# 

# **TCP SYN Flood Attack using Hping3 on Metasploitable2**

### **Introduction**

In the realm of computer network security, understanding the vulnerabilities and threats is paramount to safeguarding systems from malicious attacks. One such attack vector is the TCP SYN flood attacks a potent technique utilised by attackers to overwhelm and disrupt network resources. This report delves into the practical demonstration of a TCP SYN flood attack using hping3 on the vulnerable target, Metasploitable2. The objective is to provide insights into the mechanics of the attack, its impact on network infrastructure, and the measures to mitigate such threats.

## Prerequisites:

* **Kali Linux:** Your trusted weapon in the ethical hacking arsenal (You can use Parrot Security OS too).
* **Metasploitable2:** The unsuspecting victim of our digital assault.
* **Wireshark:** The all-seeing eye of the network.
* A thirst for knowledge and a passion for understanding the intricate world of network security.

### **Project Overview**

#### **Description**

The project demonstrates a TCP SYN flood attack employing hping3 on Metasploitable 2. It showcases the relentless barrage of SYN packets directed towards the target, along with real-time network traffic visualisation using Wireshark.

### **Setting the Stage**

1. **Armament**:

Install *hping3* on Kali Linux using the command “sudo apt install hping3”.

1. **Target Acquisition**:

Boot up Metasploitable 2 and identify its IP address using the “ifconfig” command.



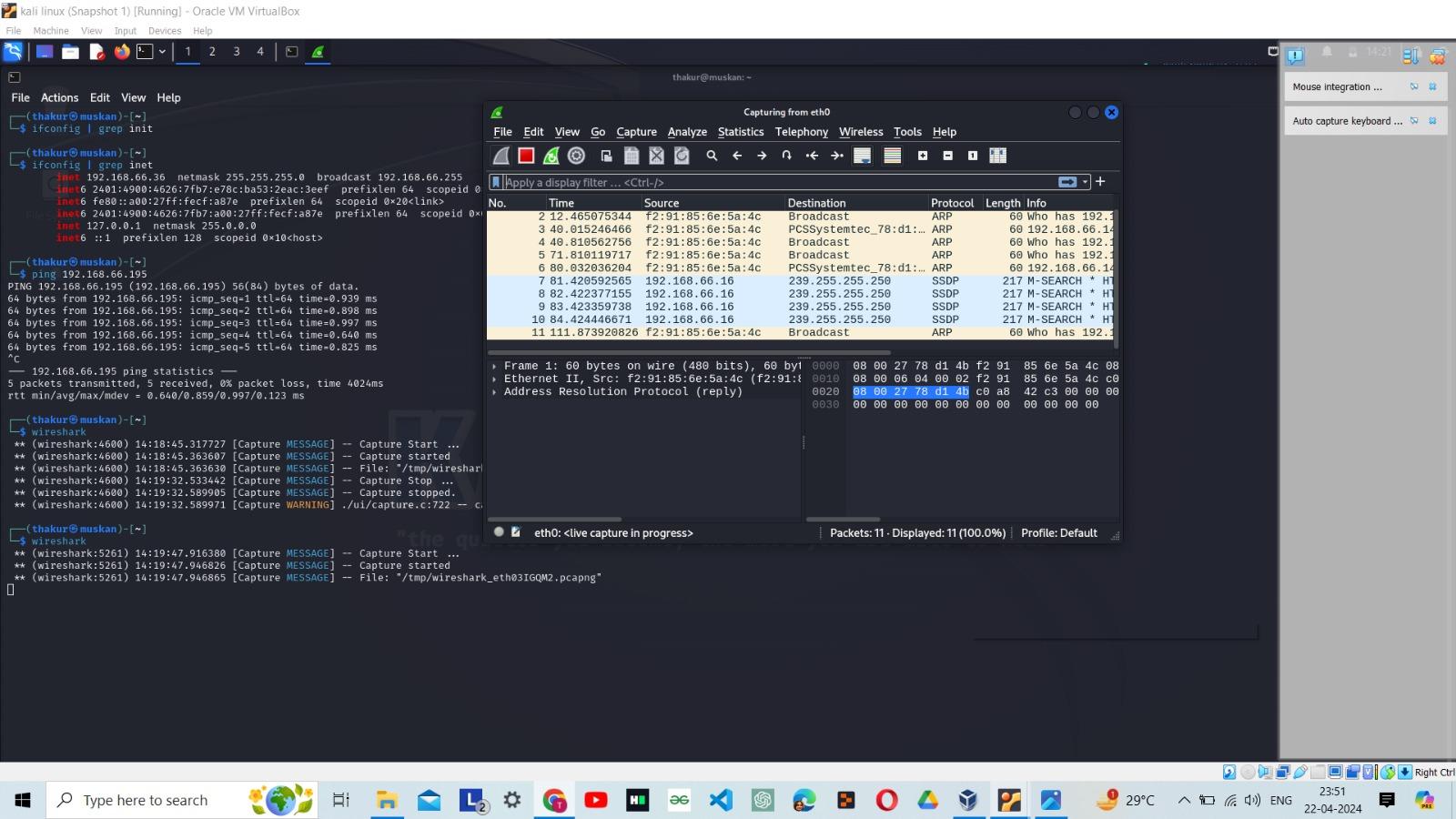
1. **Communication Establishment**:

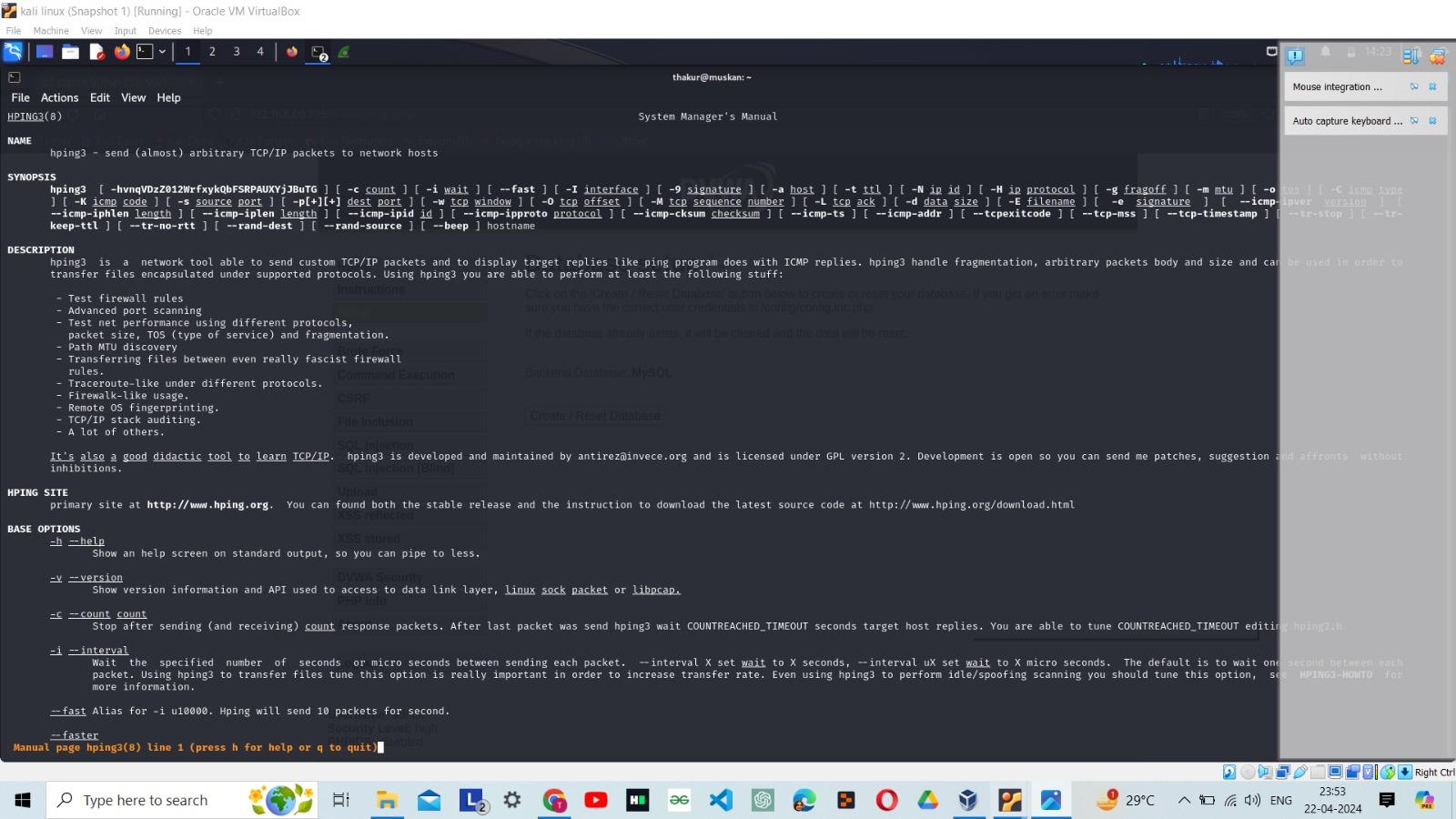
Ensure network connectivity between Kali and Metasploitable using the ping command.



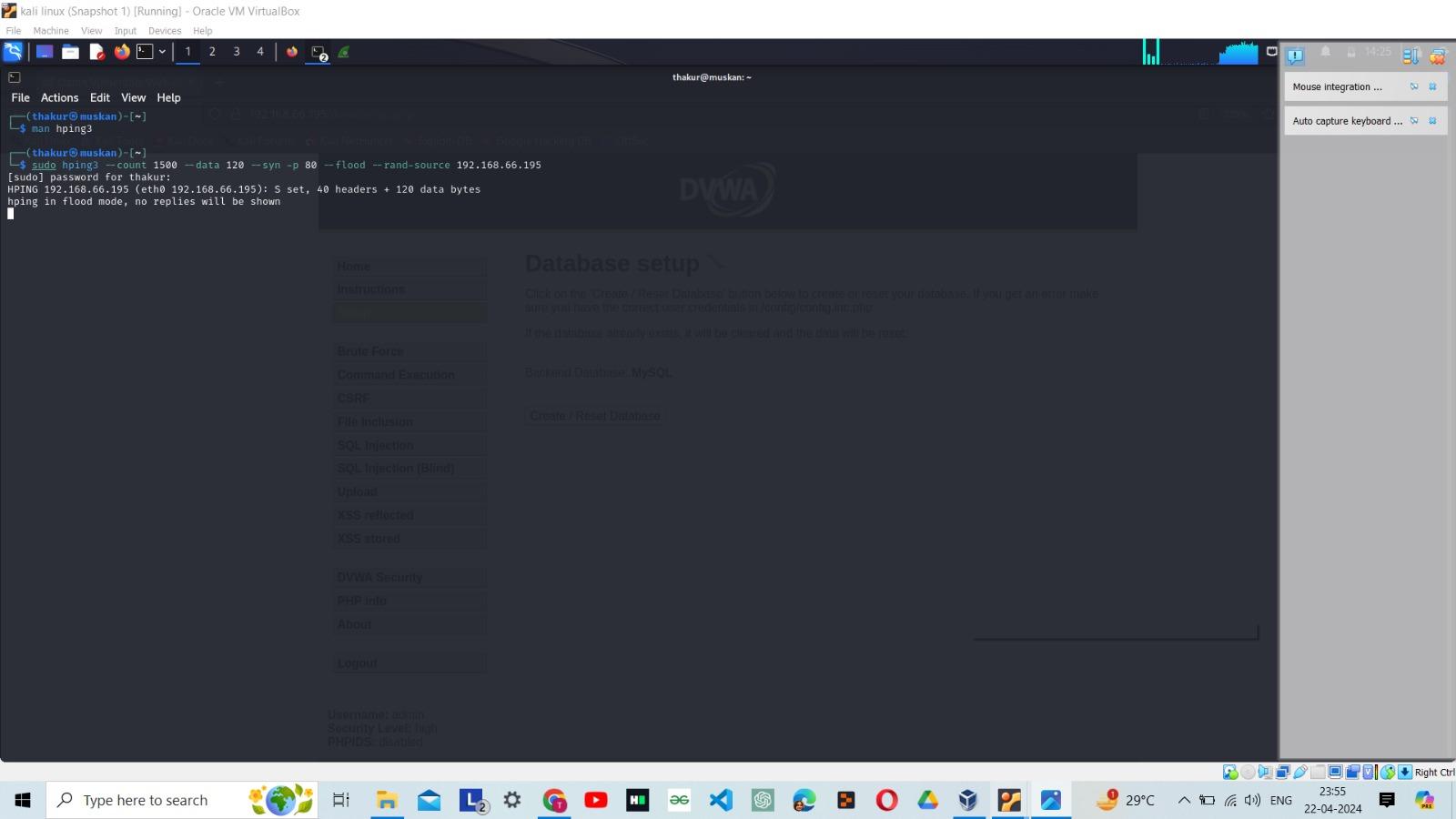
1. **Reconnaissance:**

Open Wireshark and select the appropriate network interface to monitor.





**Hping in flood , no replies will be shown :**



### **Unleashing the Storm**

1. **Command Center:** Open a terminal on Kali Linux.
2. **Execution:** Execute the SYN flood attack using hping3 with specified parameters.
3. css
4. Copy code

suding3 --count 1500 --data 120 --syn --flood -p 80 --rand-source <target

* + --count: Number of SYN packets to send
  + --data: Packet size
  + --syn: Set SYN flag
  + --flood: Send packets as fast as possible
  + -p: Destination port
  + --rand-source: Anonymize the source IP address

### **Witnessing the Devastation**

1. **Observation**:

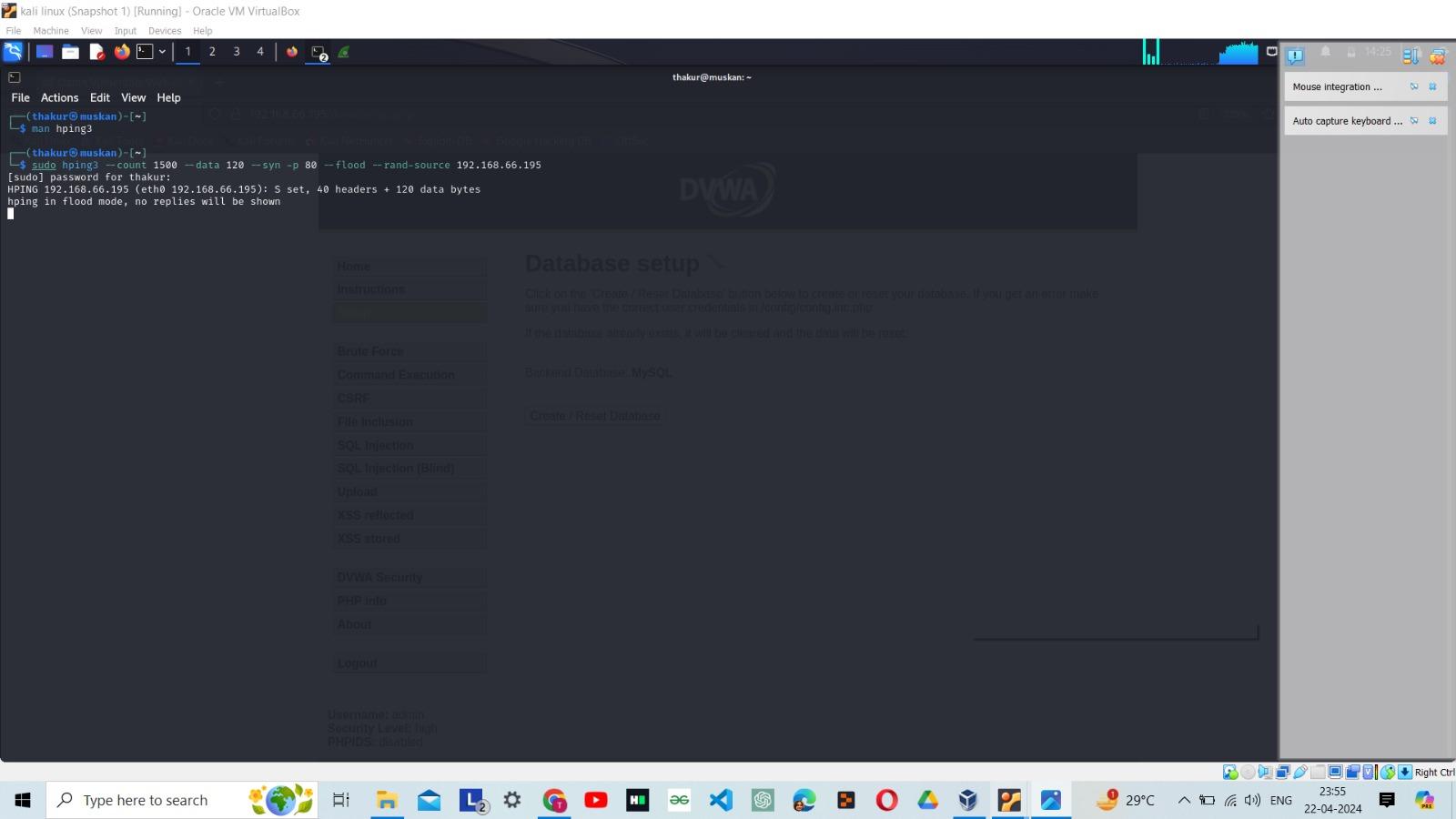
Monitor Wireshark to witness the flood of SYN packets leaving the attacker's machine.

1. **Impact Assessment**:

Observe Metasploitable's defences succumb to the onslaught, leading to disruption

1. **Acknowledgment of Success:**

Confirm the effectiveness of the attack by observing the disruption on Metasploitable's terminal.



### **Bringing the Storm to a Close**

1. **Termination:**

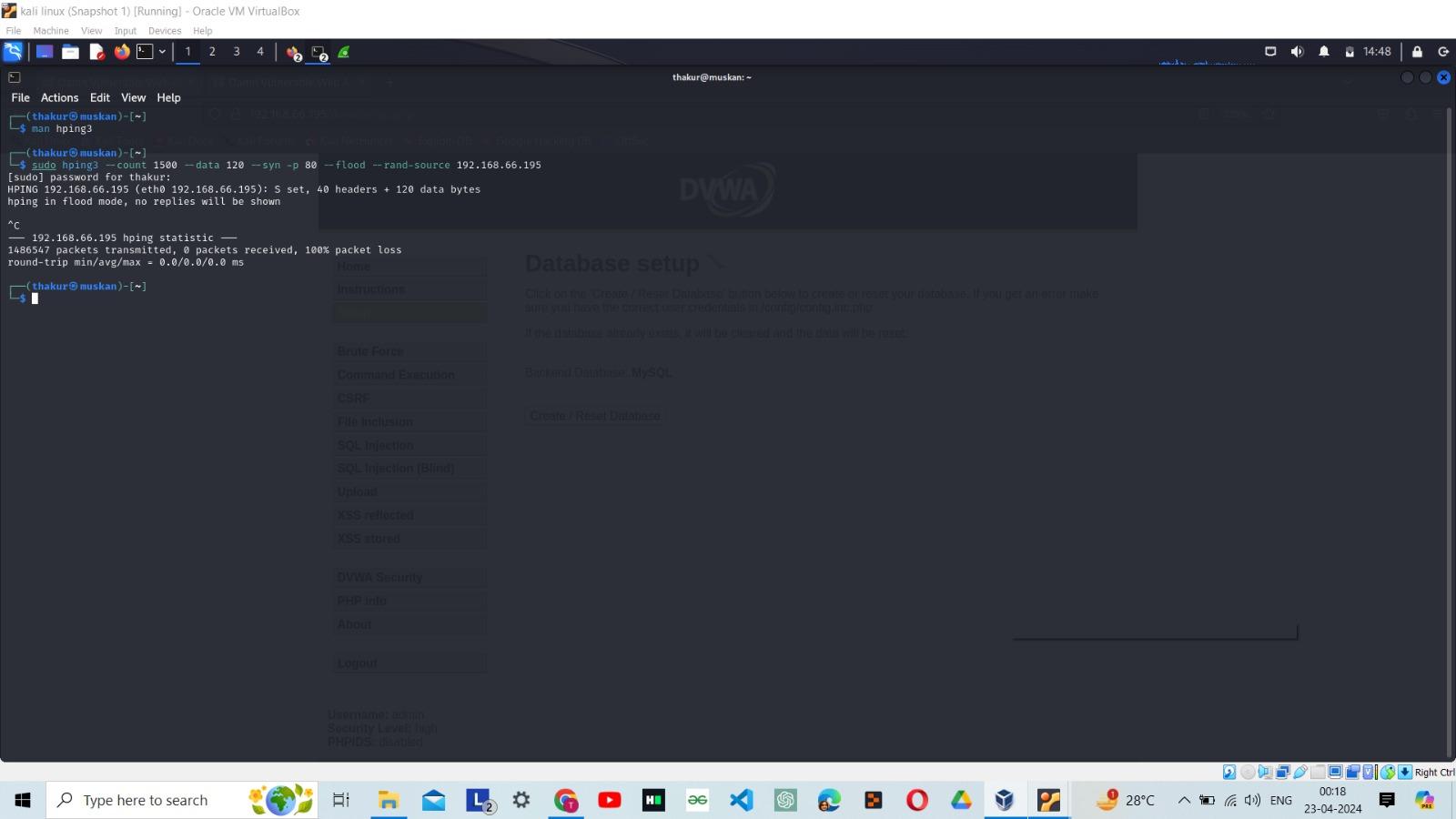
Halt the attack by pressing Ctrl + C and allow Metasploitable to recover.

1. **Analysis:**

Analyse the network traffic in Wireshark to observe the subsiding storm.

1. **Validation:**

Verify the restoration of Metasploitable's functionality post-attack.



### **BRIEF INTRO OF WHAT WE KNOW**

### 

The TCP SYN flood attack is a form of **Denial of Service (DoS)** attack that exploits the TCP protocol's three-way handshake mechanism. In a typical TCP connection initiation, the client sends a **SYN (synchronise) packe**t to the server, the server responds with a **SYN-ACK** (synchronise-acknowledgment) packet, and finally, the client acknowledges this response with an ACK packet, establishing the connection.

### **Attack Mechanism**

The SYN flood attack manipulates this process by inundating the target server with a large number of SYN requests, overwhelming its ability to respond. Instead of completing the handshake by sending the final ACK packet, the attacker neglects to respond further after receiving the SYN-ACK packets from the server. This leaves the server's resources tied up, waiting for the final acknowledgment that never arrives, eventually leading to resource exhaustion and denying service to legitimate users.

### **Impact**

The TCP SYN flood attack can have severe consequences, including:

* Service Disruption
* Resource Exhaustion
* Network Congestion

**Detection and Mitigation**

Detecting and mitigating SYN flood attacks require proactive measures such as:

* Traffic Analysis:
* Rate Limiting:
* SYN Cookies:
* Intrusion Detection Systems (IDS):

### **Conclusion**

The TCP SYN flood attack using hping3 exemplifies the potency of network-based attacks and underscores the importance of robust security measures. By comprehending the techniques employed by attackers, defenders can fortify network infrastructures against such threats. This project serves as a hands-on exploration of network security vulnerabilities and emphasises the ethical use of hacking techniques for defensive purposes.

----------------------------------**END**----------------------------------