Simulation of DoS Attack

This presentation details the simulation of a Denial of Service (DoS) attack, exploring its mechanisms, impact, and essential mitigation strategies. We'll delve into the technical aspects of DoS versus Distributed Denial of Service (DDoS) attacks, focusing on packet patterns and system behaviour under duress.

Akshay Badshah

Roll No: TEC/IIT/SS25/003 B-Tech CSE (4th Sem)

Internship at IIT JammuConducted by: Techible & Department of CSE

Internship Context

1

Program Duration

A comprehensive 6-week Summer School Internship & Training Program in 2025.

2

Host Institution

Conducted at the prestigious Indian Institute of Technology Jammu.

3

Core Focus

Specialised training in Ethical Hacking & Cybersecurity domains.

4

Key Project

In-depth simulation and analysis of a Denial of Service (DoS) Attack.

Objectives of the Project

DoS Mechanism

To gain a thorough understanding of how DoS attacks function at a fundamental level.

Offensive Tools

To practically apply offensive security tools for network flooding scenarios.

Traffic Analysis

To effectively analyse network traffic patterns using Wireshark during an attack.

Performance Impact

To quantify and observe the performance degradation on target systems.

Mitigation Techniques

To familiarise ourselves with various strategies for defending against DoS attacks.

Tools & Technologies Used

Operating Systems

- Kali Linux: Utilised as the primary attacker machine for launching DoS attacks.
- Windows 10: Configured as the target system to observe attack impact.

Attack Tools

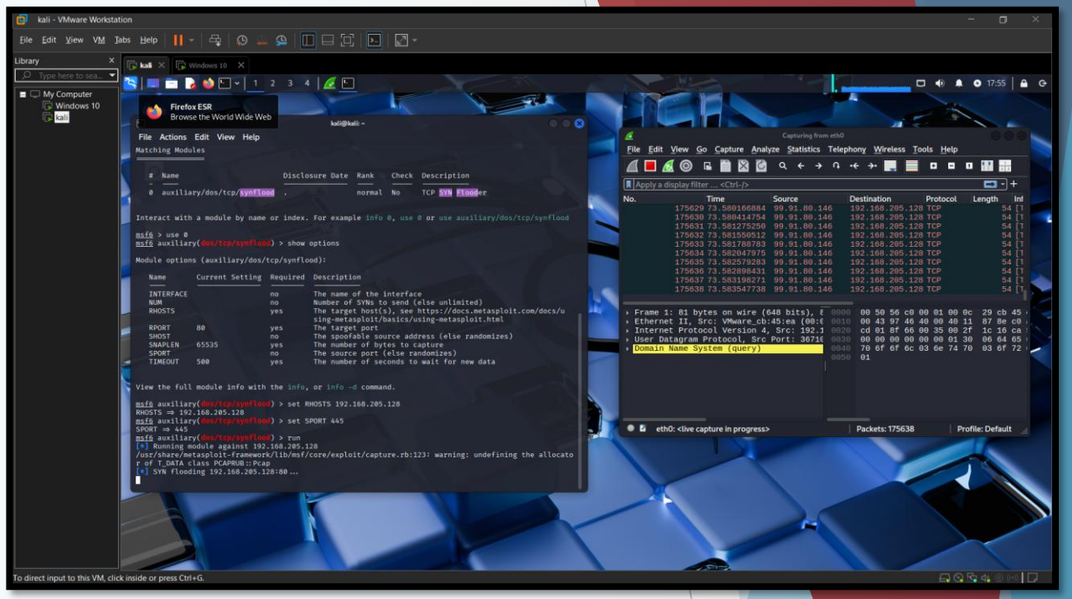
- hping3: A powerful command-line tool for crafting and sending custom TCP/IP packets.
- Metasploit Framework: Employed for leveraging various exploit modules, including SYN flood attacks.

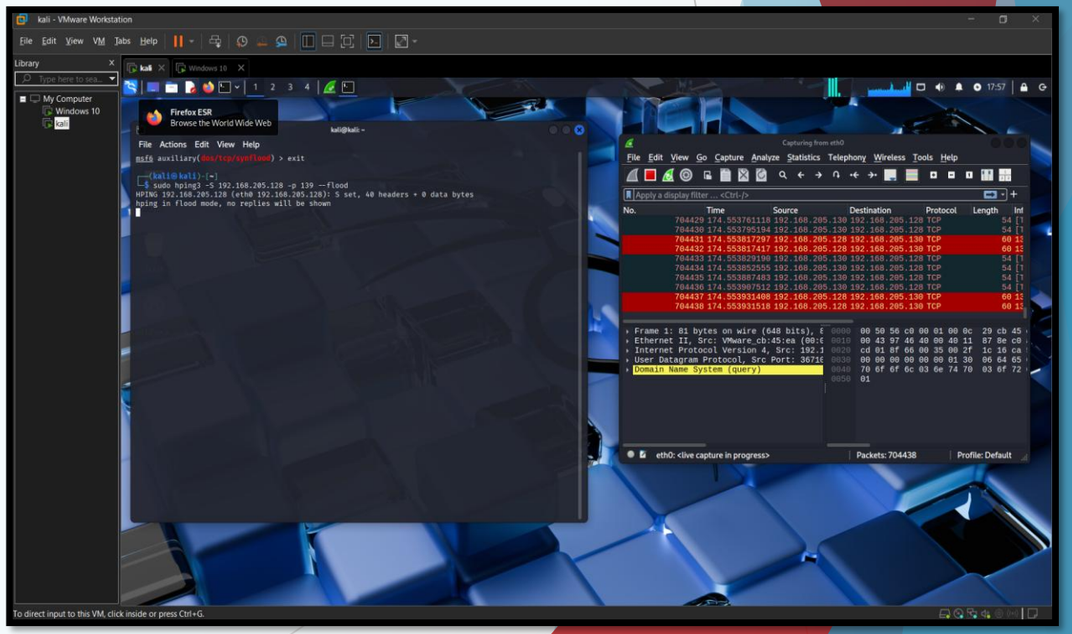
Network Analysis

- Wireshark: An essential network protocol analyser for capturing and inspecting packet flow.

Virtual Environment

- VMware Workstation: Used to set up an isolated virtual network for safe experimentation.





Methodology – Steps

1

Step 1: Environment Setup

Installed Kali Linux (attacker) and Windows 10 (target) in VMware. Configured both VMs on the same virtual network segment. Verified IP addresses using `ifconfig` (Kali) and `ipconfig` (Windows) to ensure connectivity.

2

Step 2: Firewall Configuration

Temporarily disabled the Windows Defender Firewall on the target system to allow unrestricted inbound traffic, crucial for the DoS attack to succeed and demonstrate its impact.

3

Step 3: Pre-attack Baseline

Conducted preliminary network checks using `ping` to assess baseline latency and packet loss. Captured initial network traffic with Wireshark to establish a normal operational baseline for comparison.

4

Step 4: DoS Attacks with hping3

Executed a TCP SYN Flood on Port 135 (NetBIOS Session Service) and a Large Packet SYN Flood on Port 22 (SSH). Observed significant CPU usage spikes, system unresponsiveness, and network saturation on the target.

5

Step 5: DoS with Metasploit

Utilised the `synflood` module within Metasploit Framework. Set the Remote Host (RHOST) to the target's IP and Remote Port (RPORT) to a common service port. The target system experienced severe freezing and lag, confirming service degradation.

Monitoring & Observations

Wireshark Analysis

Wireshark captures confirmed an overwhelming volume of SYN packets directed at the target, clearly demonstrating the flood's success. This high volume choked the network interface.

CPU Utilisation

The target system's CPU usage consistently peaked at 100%, indicating that the operating system was struggling to process the excessive incoming connection requests.

System Unresponsiveness

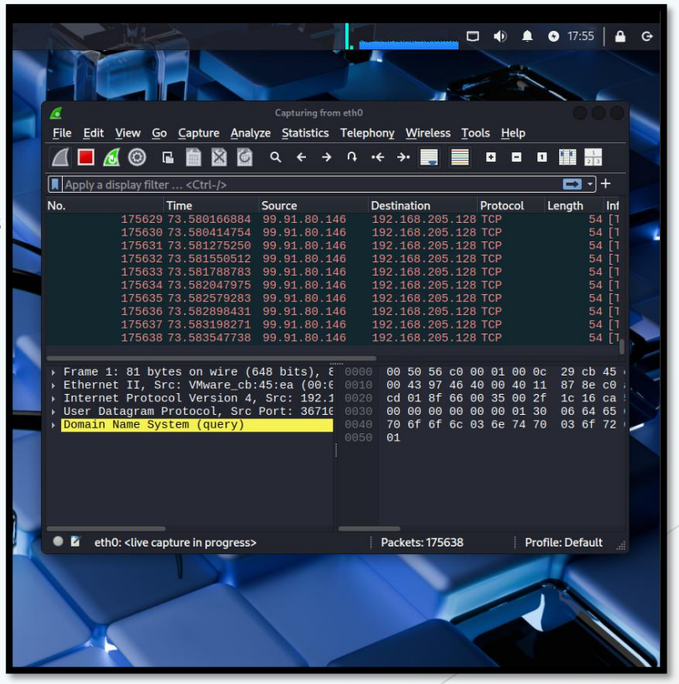
The Windows 10 target became completely unresponsive, with applications freezing and input delays, simulating a real-world DoS impact.

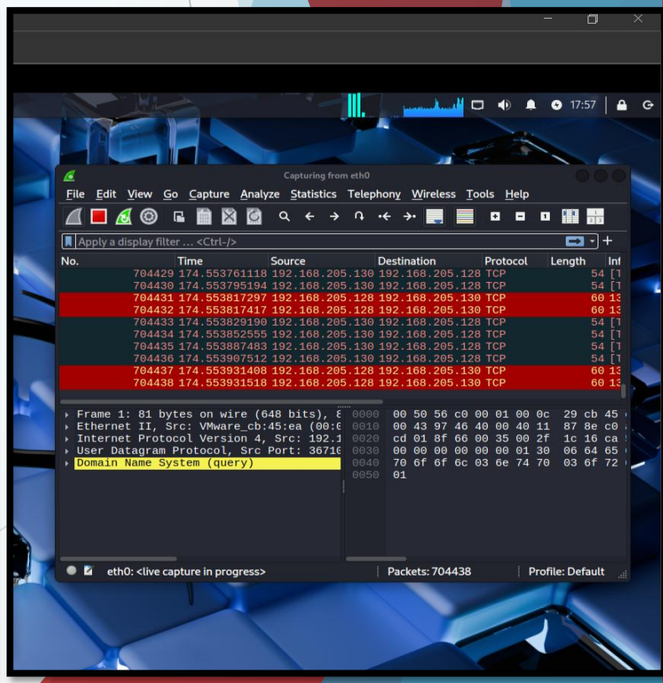
Network Latency

Observed a drastic increase in network latency and packet loss, disrupting normal network communication to and from the target.

Resource Impact

While memory impact was minimal, the primary resource contention was on the CPU and network stack, which were saturated by the flood.





Skills Learned & Challenges Faced

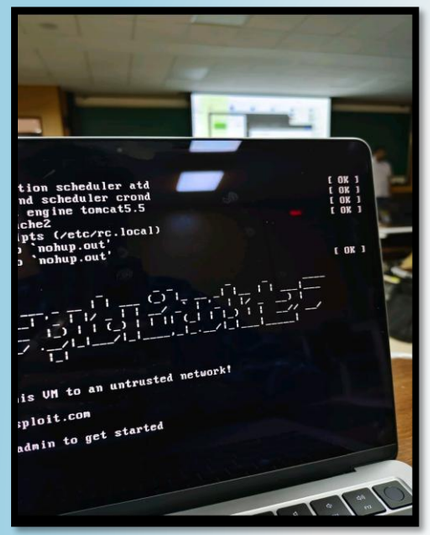
Skills Learned

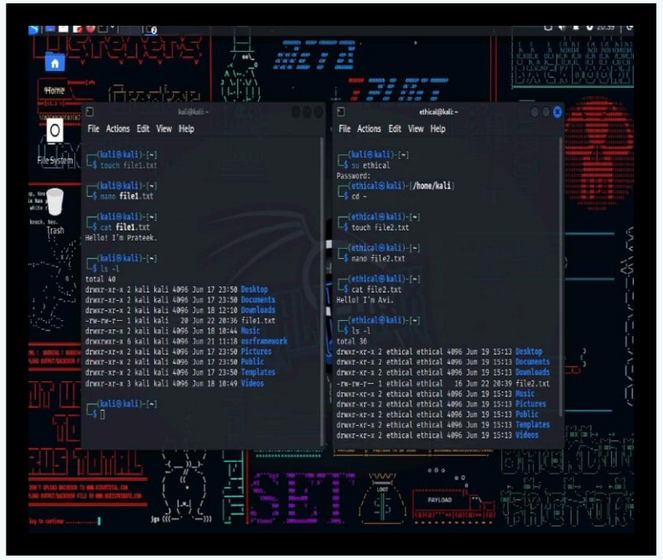
- Deepened understanding of DoS attack methodologies and their network-level implications.
- Proficient use of `hping3` for crafting and launching various types of packet floods.
- Execution and parameterisation of Metasploit modules, specifically for network attacks.
- Enhanced awareness of firewall configurations and their critical role in network security.
- Advanced skills in using Wireshark for real-time network traffic analysis and anomaly detection.
- Techniques for monitoring system resources (CPU, network) under attack conditions.

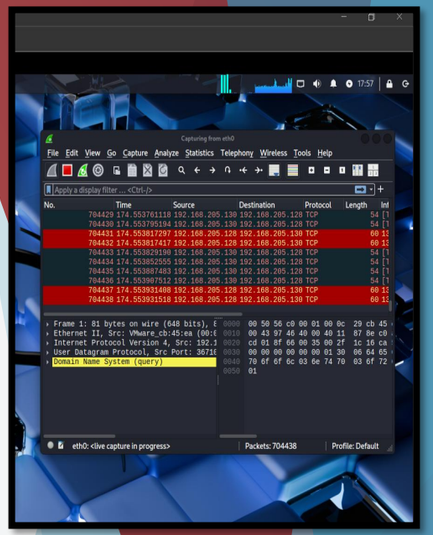
Challenges Faced

- Navigating and bypassing firewall restrictions, requiring a deep understanding of network rules.
- Dealing with significant network lag and packet loss, which complicated attack execution and monitoring.
- Optimising command parameters for `hping3` and Metasploit to achieve desired attack intensity.
- Overcoming the initial complexity of Metasploit Framework's vast array of modules and options.
- Ensuring accurate monitoring and verification of attack impact, distinguishing between attack-induced and environmental issues.

Key Takeaways







1 Hands-on Simulation

Gained invaluable practical experience in simulating DoS attacks, moving beyond theoretical knowledge.

2 Theory to Practice

Successfully bridged the gap between academic understanding and real-world application of cybersecurity concepts.

3 Defence Importance

Understood the paramount importance of robust defensive strategies in protecting against network attacks.

4 Ethical Considerations

Reinforced the critical ethical considerations and responsibilities inherent in cybersecurity practices.

Conclusion

Technical & Problem-Solving Growth

This internship significantly enhanced both technical skills in networking and cybersecurity, as well as crucial problem-solving abilities when encountering real-world attack scenarios.

Penetration Testing Expertise

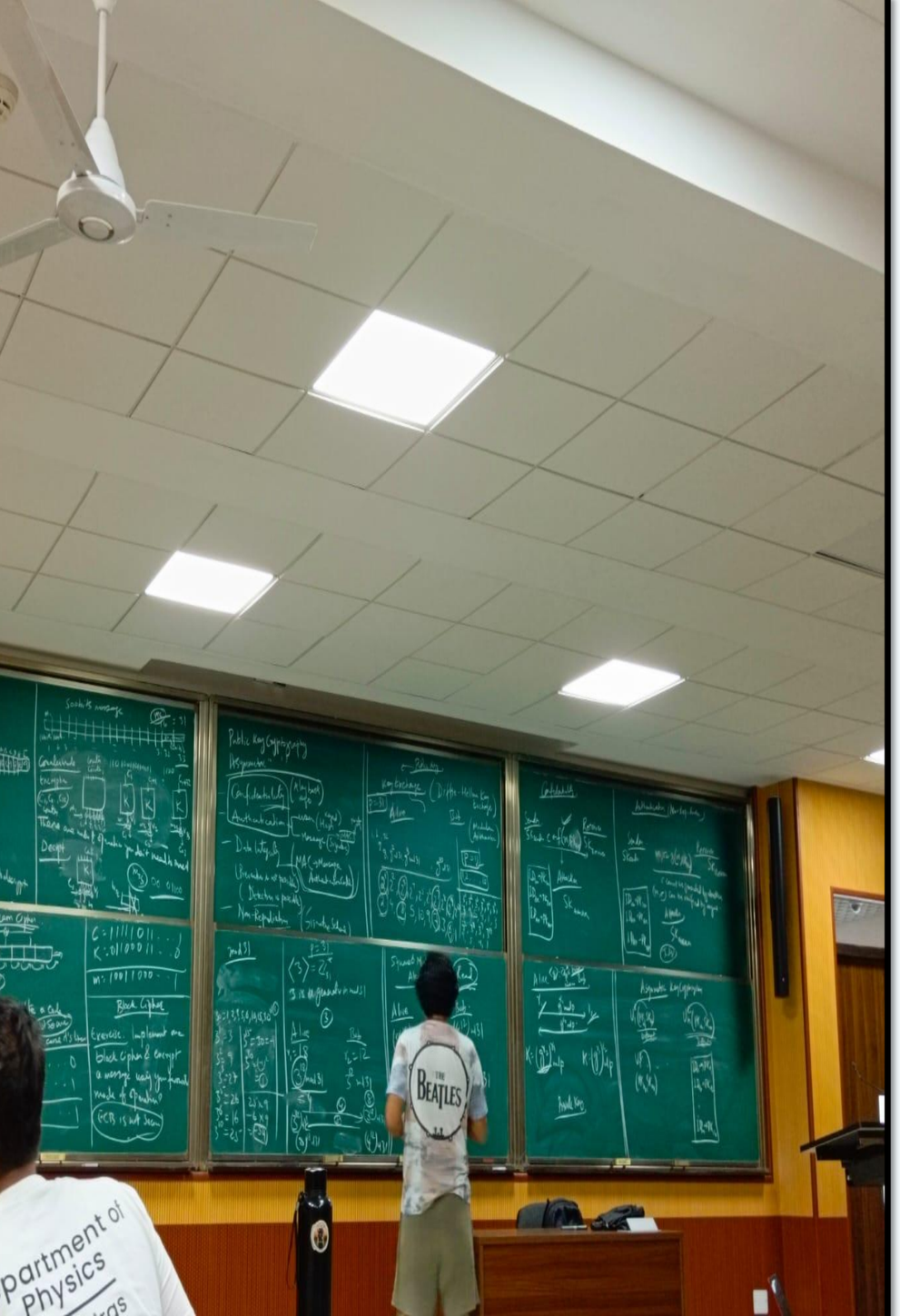
Gained practical expertise in penetration testing methodologies, specifically concerning denial of service attacks and their detection.

Defensive Measures Appreciation

Developed a deeper appreciation for the design and implementation of effective defensive security measures and protocols.

Future Role Preparation

The experience has prepared me for future roles encompassing both offensive and defensive aspects of cybersecurity.



Acknowledgement

I extend my sincere gratitude to:

- **Mentors:** Mr. Ankit Pulkit, Mrs. Aishwarya Upadhyay, and Dr. Sumit Kumar Pandey for their invaluable guidance and support throughout this project.
- **Institutions:** Indian Institute of Technology Jammu, Techible, and I3C-IIT Jammu for providing this incredible learning opportunity and the necessary resources.
- **Peers & Coordinators:** For their collaborative spirit, unwavering support, and insightful discussions that greatly contributed to the success of this internship.