भारतीय प्रौद्योगिकी संस्थान जम्मू
INDIAN INSTITUTE OF TECHNOLOGY JAMMU
विद्याधनं सर्वधन प्रधानम्

Techible

INSTITUTE INCUBATION & INNOVATION COUNCIL

INTERNSHIP REPORT

SUBMITTED BY

AKSHAY BADSHAH (TEC/IIT/SS25/003)

B-Tech 'CSE '(4TH SEM)

Submiitted In The Partial Fulfilment Of The Certification Requirements

For The

Summer Internship 2025.

SUPERVISED BY

Mr. ANKIT PULKIT
Ms. AISHWARYA UPADHYAY
Dr. SUMIT KUMAR PANDEY

INTERNSHIP TITLE

ETHICAL HACKING & CYBERSECURITY

CONDUCTED BY

INDIAN INSTITUTE OF TECHNOLOGY, JAMMU
in collaboration with **TECHILBLE & I3C**-IIT JAMMU

DEPARTMENT OF INFORMATION TECHNOLOGY AND ENGINEERING
BABA GHULAM SHAH BADSHAH UNIVERSITY, RAJOURI, J&K-185234

INTERNSHIP DURATION: (**15TH JUNE 2025 – 1ST AUGUST 2025**)

ACKNOWLEDGEMENT

I, **AKSHAY BADSHAH**, a second-year B-Tech student in COMPUTER SCIENCE AND ENGINEERING at Baba Ghulam Shah University, Rajouri J&K, feel privileged to express my sincere gratitude to all those who made my internship experience in the **Summer School Internship & Training Program 2025** at **IIT Jammu** both enriching and memorable.

I am sincerely thankful to **Dr. Navneet Kumar**, Program Advisor, for granting me this opportunity to be a part of such a prestigious program. His vision in designing a forward-looking internship that blends theoretical knowledge with real-world applications in **Ethical Hacking & CyberSecurity** has been truly inspiring. This platform not only expanded my technical expertise but also exposed me to innovative approaches and collaborative problem-solving.

My special appreciation goes to **Mr. Ankit Pulkit**, **Ms. Aishwarya Upadhyay**, and **Dr. Sumit Kumar Pandey**, our primary mentors, whose exceptional teaching skills, deep subject knowledge, and constant guidance made complex concepts accessible and engaging. Their ability to challenge our thinking while providing unwavering support has left a lasting impact on my learning journey.

I would also like to acknowledge **Indian Institute of Technology Jammu**, **Techible** and **I3C-IIT Jammu** for building a vibrant learning environment that encouraged curiosity, teamwork, and hands-on experimentation with cuttingedge technologies.

To my fellow interns and coordinators, I am grateful for the knowledge exchange, teamwork, and positive energy that made every day of this internship inspiring and productive.

This experience has not only strengthened my technical skills but has also instilled in me a renewed determination to explore, innovate, and contribute meaningfully to my field in the future.

CERTIFICATE

AKSHAY BADSHAH

B-Tech 2nd Year (ICOMPUTER SCIENCE AND ENGINEERING)
Baba Ghulam Shah Badshah University
Rajouri, Jammu & Kashmir – 185234

TABLE OF CONTENTS

S. No.	Title	Page
1	INTERNSHIP REPORT	1
2	ACKNOWLEDGEMENT	2
3	CERTIFICATE	3
4	TABLE OF CONTENTS	4
5	EXECUTIVE SUMMARY	5
6	INTRODUCTION	6
7	INTERNSHIP OBJECTIVES	7-8
8	LEARNING OUTCOMES	9-10
9	PROJECT	11-14
10	SKILLS LEARNED	15-16
11	CHALLENGES FACED	17-18
12	KEY TAKEAWAYS	19-20
13	CONCLUSION	21
14	APPENDIX	

EXECUTIVE SUMMARY

As a part of my academic curriculum, I had the privilege of completing a six-week internship under the **Summer School Internship & Training Program 2025**, organized by the **Indian Institute of Technology Jammu**, in collaboration with **Techible** and **I3C-IIT Jammu**. The internship was thematically focused on ***Ethical Hacking and CyberSecurity*** and was designed to provide hands-on exposure to modern cybersecurity tools, ethical hacking techniques, vulnerability assessments, and realworld penetration testing practices.

Throughout the program, I engaged in daily learning sessions covering key topics such as cybersecurity fundamentals, including network security protocols and ethical hacking methodologies, practical penetration testing tools and vulnerability assessment techniques, cryptography and encryption algorithms, as well as real-world cyber-attack simulations like privilege escalation and many more, incident response strategies, and the development of security measures to mitigate potential threats. I actively participated in workshops, practical labs, and project work, which enabled me to apply theoretical knowledge to realistic scenarios, enhancing my problem-solving skills, technical expertise, and understanding of incident response and security measures to mitigate potential threats.

This internship has significantly enriched my understanding of cybersecurity principles and practical applications. It has equipped me with valuable technical skills and a problem-solving mindset essential for tackling contemporary cybersecurity challenges. The exposure to real-world scenarios and expert mentorship from **Mr. Ankit Pulkit**, **Ms. Aishwarya Upadhyay**, and **Dr. Sumit Kumar Pandey** has strengthened my confidence and motivated me to pursue further specialization in the field of Ethical Hacking and Cybersecurity. I am confident that the knowledge and experience gained during this internship will greatly contribute to my academic growth and future career aspirations in the cybersecurity domain.

INTRODUCTION

I am AKSHAY BADSHAH, currently a second-year B.Tech student in COMPUTER SCIENCE AND ENGINEERING at Baba Ghulam Shah Badshah University, Rajouri J&K. Throughout my academic journey, I have developed a strong interest in Cybersecurity and Ethical Hacking, driven by the growing importance of securing digital systems in today's technology-driven world.

My keen interest lies in **Cyber Forensics**, which motivated me to choose this internship. Although the program primarily focused on Ethical Hacking and Cybersecurity techniques, I saw this as an invaluable opportunity to build foundational skills and gain practical exposure in the broader field of cybersecurity. I believe the experience and knowledge gained during this internship will serve as a strong stepping stone toward specializing in cyber forensics in the future.

My coursework has provided me with a solid foundation in computer networks, programming, and information security concepts. However, I recognized the need to gain practical, hands-on experience to deepen my understanding and better prepare myself for real-world challenges in cybersecurity.

The primary purpose of undertaking the **Summer School Internship & Training Program 2025** at the **Indian Institute of Technology Jammu** was to bridge the gap between theoretical knowledge and practical application. This internship offered an excellent platform to learn about advanced cybersecurity tools, ethical hacking techniques, and real-world vulnerability assessment and penetration testing practices. My goal was to enhance my technical skills, gain industry-relevant experience, and develop problem-solving abilities essential for a career in cybersecurity.

INTERNSHIP OBJECTIVES

During my internship, my primary learning goals were to deepen my understanding of cybersecurity concepts and develop practical skills that would prepare me for real-world challenges in the field. I aimed to bridge the gap between theoretical knowledge from my coursework and hands-on experience with current cybersecurity tools and methodologies. Additionally, I wanted to improve my problem-solving abilities and gain insights into industry-standard practices for identifying and mitigating security threats.

The skills and knowledge I aimed to gain included:

- **Network Security Fundamentals:** Gaining a thorough understanding of VLANs, subnets, firewall configurations, and their correlations to effectively design and secure network infrastructures. This also included learning about common network vulnerabilities and mitigation techniques.

- **Virtualization Technologies:** Practical experience with VirtualBox and virtual machine management to simulate various network environments and safely conduct penetration testing and security assessments without risking real systems.

- **Linux System Administration:** Developing command-line proficiency and managing file system permissions, user accounts, and processes on Linux-based systems, which form the backbone of many servers and security tools.

- **Security Tools and Frameworks:** Hands-on experience with industry-standard cybersecurity tools such as Nmap for network scanning, Wireshark for packet analysis, Metasploit for exploit development, and Burp SuCSE for web vulnerability testing. This also involved learning to interpret tool outputs to identify security weaknesses.

- **Cryptographic Principles:** Deepening my understanding of encryption algorithms, hashing techniques, digital certificates, and secure communication protocols, essential for protecting data confidentiality and integrity.

- **Practical Ethical Hacking:** Applying real-world penetration testing techniques to identify and exploit vulnerabilities in various systems, including reconnaissance, scanning, exploitation, and reporting. This included simulations like DoS attack, privilege escalation, and web application firewall bypass techniques.

- **Incident Response Strategies:** Learning the fundamentals of incident detection, containment, eradication, and recovery to effectively manage and mitigate cybersecurity incidents. This included exposure to creating incident reports and understanding forensics basics.

- **Communication and Collaboration:** Enhancing soft skills by participating in group projects, presentations, and knowledge-sharing sessions, which fostered teamwork and improved my ability to communicate complex technical information clearly and effectively.

LEARNING OUTCOMES

The **Summer School Internship & Training Program 2025** at the **Indian Institute of Technology Jammu**, conducted in collaboration with **Techible** and **I3C-IIT Jammu**, provided a highly structured, multidisciplinary learning environment focused on practical applications of Ethical Hacking and CyberSecurity. The program offered a comprehensive exploration of cybersecurity, beginning with foundational networking concepts and progressing to advanced security implementations. During the internship, I gained valuable insights into virtualization and networking technologies, including VLANs, subnets, VirtualBox, and SSH protocols. The Linux system administration module further enhanced my understanding of file systems, permissions, user management, and essential security practices.

The cryptography segment of the program was particularly enlightening, covering fundamental concepts such as hash functions, symmetric encryption, Message Authentication Codes (MAC), digital signatures, and public key encryption. In-depth discussions also encompassed HTTPS and TLS protocols, Shannon's perfect secrecy, probability theory applications, one-time pad encryption, and the distinction between true random and pseudorandom number generators. These topics collectively strengthened my theoretical foundation and practical knowledge critical for a career in cybersecurity.

The internship followed a structured schedule with sessions three days a week, each lasting about three hours. Each session combined theoretical lessons with practical demonstrations. Daily activities involved hands-on practice with the tools introduced during the classes. Weekly tasks included solving Capture The Flag (CTF) challenges, vulnerability assessments, penetration testing exercises, and collaborative work on a final group project focused on real-world cybersecurity scenarios.

Throughout the internship, I gained proficiency in a variety of industrystandard tools and platforms, including:

- **Learning Platforms:** TryHackMe for interactive cybersecurity exercises, and PicoCTF for competitive Capture The Flag (CTF) challenges.

- **Development Tools:** GitHub for version control and collaboration; Sublime Text and Notepad++ for code editing and scripting.

- **Security Tools:** Wireshark for packet capture and network traffic analysis; Nmap for network scanning; Metasploit for penetration testing; Burp SuCSE for web vulnerability scanning; Cisco Packet Tracer for network simulation.

- **Virtualization:** VirtualBox for managing virtual machines, running isolated environments to safely conduct penetration tests and simulations; Ubuntu as the primary Linux distribution for server deployments and system administration practice.

- **Cloud Services:** Google Cloud Platform to deploy and test server infrastructure in a cloud environment.

- **Analysis Tools:** Recon-ng for reconnaissance and information gathering; static and dynamic code analysis tools; fuzzing techniques for automated vulnerability discovery.

PROJECT

Title: Simulation of DoS Attack

Introduction:

A Denial of Service (DoS) Attack is a malicious attempt to make a machine, service, or network resource unavailable to its intended users by overwhelming it with a flood of requests or traffic. Unlike distributed DoS (DDoS) attacks, where multiple systems are involved, a DoS attack generally originates from a single machine.

In this project, I simulated a DoS attack in a controlled lab environment to study the attack behaviour, packet patterns, and the effect on target system performance. The primary aim was to understand the working of such attacks, analyse their network footprint, and explore Preventive measure.

The simulation was performed using **Kali Linux** as the attacking machine, targeting a Windows-based system. Before initiating the attack, I disabled the firewall on the target machine to allow unrestricted packet flow. The attack was executed with tools such as **hping3** (for packet flooding) and **Metasploit Framework** (for exploiting network weaknesses).

Objectives:

- To understand the working mechanism of a DoS attack in a safe, controlled environment.
- To explore and use different offensive security tools for network flooding.
- To analyse the network traffic generated during the attack using Wireshark.
- To study the impact of a DoS attack on system performance.
- To develop an awareness of mitigation techniques and defensive strategies.

Tools & Technologies Used:

Operating Systems:

- **Kali Linux** – Attacker Machine.
- **Windows 10** – Target Machine.

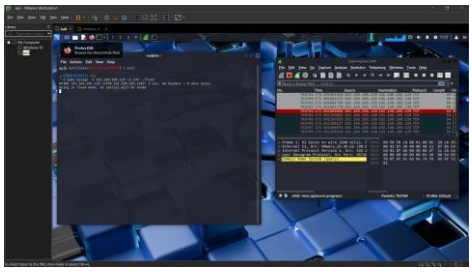
Tools:

- **hping3** – Used for generating custom TCP/UDP packets and simulating packet floods.
- **Metasploit Framework** – Used for launching auxiliary DoS modules.
- **Wireshark** – For monitoring and analysing network traffic during the attack.

Network Setup:

- Virtualized environment using VMware/UTM.
- Host machine running Window 11.

Methodology:



Step 1: Environment Setup

- Installed **Kali Linux** as the Attacking Machine.
- Installed **Windows 10** as the Target Machine.
- Ensured both machines were connected to the same virtual network.
- Verified IP addresses of both machines using ifconfig and ipconfig respectively.

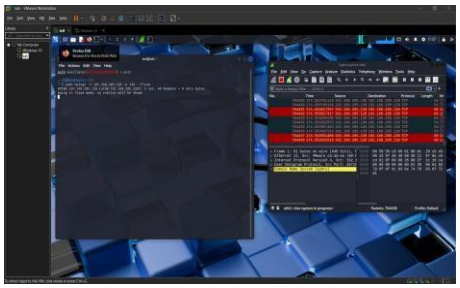
Step 2: Disabling the Firewall on the Target

- On the Windows 10 machine, the firewall was turned off using:
  - **Control Panel → Windows Firewall → Turn Windows Firewall Off**
- This step was necessary to ensure the DoS traffic could bypass built-in packet filtering.

Step 3: Pre-Attack Analysis

- Verified network connectivity between attacker and victim using ping command.
- Recorded normal network traffic patterns using Wireshark for baseline analysis.

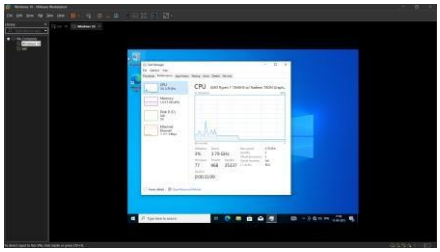
Step 4: Performing DoS Attack Using hping3



Two different types of flooding techniques were tested:

i. TCP SYN Flood on Port 135

- Identified the target's IP address, e.g., 192.168.1.105.
- Launched a TCP SYN flood attack using hping3:
  'hping3 -S <victim-ip> -p 135 --flood'
- **-S** → Sends TCP packets with the SYN flag set.
- **-p 135** → Targets port 135 (commonly used by Microsoft RPC service).
- **--flood** → Sends packets as fast as possible without waiting for replies.
- **Purpose** → This simulates a SYN Flood DoS attack, overwhelming the TCP handshake process on the target system.



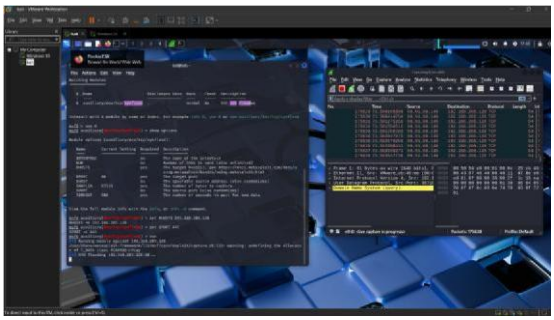
ii. Large Packet Flood on Port 22

- Identified the target's IP address, e.g., 192.168.1.105.
- Launched a SYN flood attack using hping3:
  'hping3 -d 65538 -S -p 22 --flood <victim-ip>'

- **-d 65538** → Sets a custom packet size (very large in this case, which can strain the target's processing and bandwidth).
- **-S** → Again, sets SYN flag for TCP connection requests.
- **-p 22** → Targets port 22 (commonly used for SSH).
- **--flood** → Sends the packets continuously at maximum speed.
- **Purpose** → This variant not only initiates a SYN flood but also uses oversized packets, increasing resource consumption and amplifying the denial-of-service effect.

Observed **CPU usage reaching 100%** on the target machine, causing freezing and unresponsiveness.

Step 5: Performing the Attack Using Metasploit



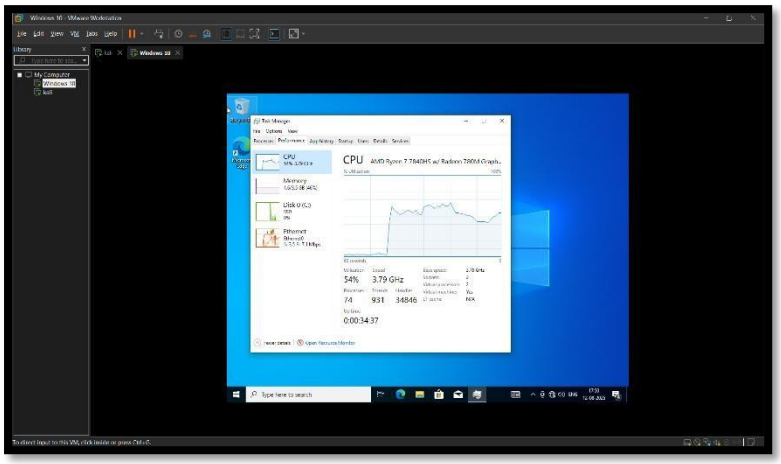
i. Opened Metasploit console:
'msfconsole' ii. Selected a DoS auxiliary module:
'use auxiliary/dos/tcp/synflood' iii. Set target IP and port:
'set RHOST 192.168.1.105'
'set RPORT 80'
'run' iv. Observed similar system freeze on the target.

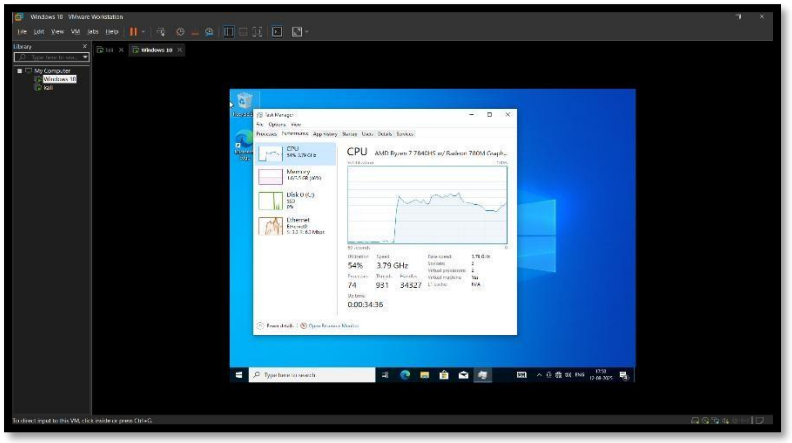
Step 6: Monitoring the Attack

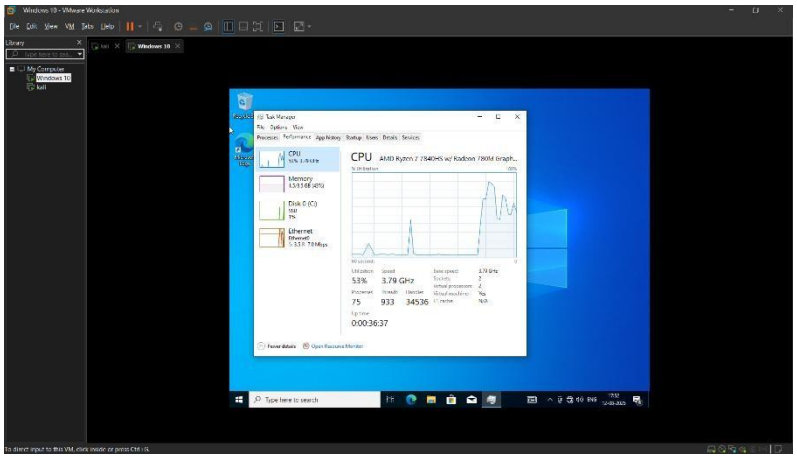
- **Wireshark** was run on Kali Linux to monitor outgoing packet flow.
- Observed high CPU usage on the Windows 10 machine (100%), causing severe lag and unresponsiveness.

Observations:

- CPU utilization on the target reached **100%**, freezing the display.
- The system became unresponsive, with mouse and keyboard lag.
- Network latency increased significantly; legitimate requests failed.
- In Wireshark, a massive volume of SYN packets from the attacker was recorded.
- Even though **physical memory usage** was low (~18%), CPU saturation caused the crash.
- Proving DoS primarily affected CPU/network stack.







SKILLS LEARNED

During the execution of the **"Simulation of DoS Attack"** project, I gained a comprehensive set of technical and analytical skills that enhanced my understanding of offensive security techniques and network vulnerabilities. The key skills learned are outlined below:

1. Practical Understanding of Denial-of-Service (DoS) Attacks

- Learned how DoS attacks overwhelm network resources and disrupt legitimate services by consuming bandwidth, CPU cycles, and memory.
- Understood the difference between **DoS** and **Distributed DoS (DDoS)** attacks, including their real-world implications on security and service availability.

2. Hands-on Experience with hping3

- Mastered the usage of **hping3** to craft and send custom TCP/IP packets for simulating network floods.
- Practiced two key commands:
  - *'hping3 -S <victim-ip> -p 135 –flood'* for SYN flood attacks on port 135.
  - *'hping3 -d 65538 -S -p 22 --flood <victim-ip>'* for large-payload SYN flood attacks on port 22.
- Learned how to manipulate packet size, ports, and flags to achieve specific attack behaviours.

3. Metasploit Framework Proficiency

- Learned to configure and execute DoS attack modules available in the **Metasploit Framework**.
- Gained experience in setting parameters, running exploit modules, and analysing the target's response.

4. Firewall and Security Configuration Awareness

- Understood how firewalls can detect and block abnormal traffic.
- Practiced disabling firewall protections in a controlled lab environment to allow attack simulation, learning the importance of secure firewall policies.

5. Packet Analysis with Wireshark

- Gained experience in capturing and analysing live network traffic during the attack.
- Identified patterns of abnormal traffic, packet rates, and SYN request floods in the captured logs.

6. System Resource Monitoring

- Learned to use system tools like Task Manager (Windows) and top/htop (Linux) to monitor CPU, memory, and network usage under attack conditions.

7. Documentation and Reporting Skills

- Improved ability to document methodologies, commands, and results in a clear and structured manner. Developed a deeper understanding of how to present technical findings in a formal report format for academic or professional purposes.

CHALLENGES FACED

During the execution of the **"Simulation of DoS Attack"** project, several technical and practical challenges were encountered. These challenges tested my problem-solving skills, adaptability, and ability to think critically in real-time. Below is a detailed account of the major challenges faced and the strategies I used to overcome them.

1. Firewall Restrictions

- **Challenge:**
  Initially, the target machine was protected by a firewall that automatically filtered and blocked incoming suspicious traffic. This prevented the ***hping3*** packets and the Metasploit payload from reaching the target effectively, making the attack appear unsuccessful during the first few attempts.

- **Solution:**
  I manually disabled the firewall on the target system before conducting the simulation. This allowed the attack traffic to bypass the filtering rules and directly hit the target, enabling me to accurately observe the effect of a DoS attack.

2. Network Lag and Packet Loss

- **Challenge:**
  While performing the flood attack using **hping3**, I experienced significant packet loss and delay in command execution. This was due to heavy CPU and bandwidth consumption caused by the flood. In some instances, the attacking system's terminal became unresponsive.

- **Solution:**
  To address this, I ran the attack from a dedicated virtual machine in Kali Linux, isolated from other tasks. This ensured that maximum resources were allocated to the attack process, reducing lag and preventing interference with other applications.

3. Command Parameter Optimization

- **Challenge:**
  Understanding the correct parameters for hping3 was not straightforward. The two main commands I used:
  a. *'hping3 -S <victim-ip> -p 135 –flood'*
  b. *'hping3 -d 65538 -S -p 22 --flood <victim-ip>'* initially caused confusion, especially regarding the -d (data size) parameter, which can significantly impact performance and detectability.

- **Solution:**
  I referred to the official **hping3** documentation and community forums to fully understand how each flag worked. Experimenting with different payload sizes helped me determine optimal configurations for achieving maximum traffic load without crashing the attacking system.

4. Metasploit Framework Complexity

- **Challenge:**
  Using the Metasploit Framework for a DoS module required a proper understanding of auxiliary modules, payload selection, and target configuration. A mistake in the configuration phase often resulted in failed attempts, wasting time.

- **Solution:**
  Using the Metasploit Framework for a DoS module required a proper understanding of auxiliary modules, payload selection, and target configuration. A mistake in the configuration phase often resulted in failed attempts, wasting time.

5. Monitoring and Verifying the Attack

- **Challenge:**
  Observing the real impact of the DoS attack was challenging. Although the target machine's CPU usage and responsiveness were visibly affected, measuring packet flow accurately in **Wireshark** was difficult due to lag.

- **Solution:**I used both **Wireshark** and **System Resource Monitor** to cross-verify the impact. By filtering traffic by source IP and protocol, I could better visualize the flood in Wireshark despCSE occasional packet capture lag.

KEY TAKEAWAYS

This project on the **"Simulation of DoS Attack"** has been a transformative learning experience, offering not just technical growth but also professional development. By working with tools such as hping3 and Metasploit, I gained a hands-on understanding of how denial-of-service attacks operate, how they can disrupt systems, and why preventive security measures are crucial in a real-world environment.

From a professional growth perspective, this internship bridged the gap between theoretical academic knowledge and its practical industry application. While classroom lessons taught me the definitions, properties, and classifications of cyberattacks, this project enabled me to simulate and observe them in action. I learned to set up virtual environments, identify vulnerabilities, remove existing firewalls for controlled testing, and execute targeted flood attacks using different configurations. This practical engagement enhanced my problem-solving skills, attention to detail, and adaptability in unexpected scenarios.

Moreover, I developed a deeper **awareness of network security** and system performance monitoring. Observing the CPU usage spike to 100% and the target system freeze demonstrated how resource exhaustion can cripple a service. It reinforced the importance of proper firewall configurations, intrusion detection systems, and proactive monitoring in any organization.

The project also gave me a **better understanding of the ethical considerations** in cybersecurity. Conducting attacks in a controlled, legal environment highlighted the responsibility of ethical hackers to use their skills for defence, not harm.

In conclusion, this internship improved my technical competence, boosted my professional confidence, and provided valuable industry insights. I now feel more prepared to contribute to **offensive security testing**, vulnerability assessments, and network defence strategies in real-world projects.

CONCLUSION

My experience during this internship, particularly while working on the **"Simulation of DoS Attack"**, has been both transformative and enriching. This project allowed me to apply my academic knowledge in a real-world, practical scenario while deepening my understanding of offensive security concepts.

The process of setting up the target environment, removing the firewall for the simulation, and successfully executing multiple variations of the DoS attack gave me a strong grasp of both the theoretical and technical aspects of cybersecurity. I learned how to craft precise attack commands, analyse the impact using network monitoring tools, and interpret the behaviour of the target system under stress. This has not only improved my technical skills but also my problem-solving abilities, especially when facing challenges like system freezes, network delays, and lag in monitoring tools.

From a professional perspective, this project has enhanced my confidence in handling penetration testing tools, understanding attack vectors, and following ethical hacking methodologies. It has also helped me appreciate the importance of defensive measures like firewalls, intrusion detection systems, and rate-limiting configurations, which I encountered firsthand by intentionally disabling protection for the simulation.

The knowledge gained during this internship will directly benefit my future career in **Cybersecurity** and **Offensive Security**. It has reinforced my interest in pursuing advanced studies and certifications in penetration testing and red teaming, and I now feel more prepared to handle both offensive and defensive security challenges in professional environments.

This internship has been a valuable step toward my goal of becoming an expert in offensive security, providing me with both technical competence and industry-level awareness to excel in my future endeavours.