Internship Final Report

Student Name: Daniel Muthama

University: Maseno University

Major: Computer Science

Internship Duration: April 10th, 2025 - May 3rd, 2025

Company: Hack Secure

Domain: Cyber Security (Red Team Operations)

Mentor: Mr. Aman Pandey

Assistant Mentor: Mr. Shivam Kapoor

Coordinator: Mr. Nishant Prajapati

Objectives

My primary objectives for this internship were to:

Master practical Red Team operations, including vulnerability exploitation and adversarial simulation.

Develop proficiency in tools like Metasploit, Wireshark, and Python for cybersecurity tasks.

Execute simulated attacks to understand attacker methodologies and defenses.

Tasks and Responsibilities

During my internship, I performed the following tasks:

Vulnerability Assessment:

Scanned testphp.vulnweb.com using Nmap to identify open ports (e.g., port 80 running Apache).

Conducted directory brute-forcing with Gobuster, uncovering /admin, /login, and /search.php.

Penetration Testing:

Exploited SQL injection (SQLi) on the login page using payload ' OR 1=1 -- to bypass authentication.

Tested for XSS vulnerabilities by injecting <script>alert('XSS')</script> into input fields, confirming reflected XSS.

Network Traffic Analysis:

Intercepted HTTP POST requests using Wireshark during login, capturing plaintext credentials.

Red Team Simulation (CTF: PickleRick):

Gained initial access via a PHP reverse shell and established persistence with cron jobs.

Performed lateral movement using stolen credentials and exfiltrated data via Meterpreter.

Python Tool Development:

Built a port scanner, password strength checker, and file encryption tool using Python.

Published code on GitHub.

Outcomes

Key Findings:

Open ports: 80/tcp (HTTP).

Sensitive directories: /admin, /login.php.

SQLi vulnerability in listproducts.php?cat=1 leading to database extraction (acuart).

Credentials captured via Wireshark: admin:password.

Tools Used:

Nmap, Gobuster, Wireshark, sqlmap, Metasploit, Mimikatz, Python.

GitHub Project:

https://github.com/danielmuthama23/Red-Team_Hack-Secure-Internship-Project.git

Learning Outcomes

Technical Proficiency: Advanced skills in penetration testing tools (Metasploit, sqlmap) and Python scripting.

Red Team Tactics: Hands-on experience in initial access, lateral movement, and persistence.

Problem-Solving: Overcame challenges like bypassing authentication and decrypting traffic.

Professional Growth: Improved teamwork and time management during simulated attacks.

Challenges and Solutions

Complex Tool Usage: Struggled with Meterpreter payloads initially; resolved via Metasploit documentation and mentor guidance.

Traffic Decryption: Learned SSL/TLS decryption techniques in Wireshark for HTTPS analysis.

Python Scripting: Debugged port scanner threading issues using ThreadPoolExecutor.

Conclusion

This internship at Hack Secure deepened my expertise in offensive security and Red Team operations. The hands-on experience with real-world tools and attack simulations has prepared me for advanced roles in cybersecurity. I am now confident in executing ethical hacking protocols and developing defensive strategies.

Acknowledgments

I thank Mr. Aman Pandey (Mentor) and Mr. Shivam Kapoor (Assistant Mentor) for their invaluable guidance. Gratitude to Maseno University for fostering my technical foundation and Hack Secure for this transformative opportunity.

Screenshots

(Attached in Appendix)

Nmap scan results.

Gobuster directory enumeration.

SQLi exploitation via sqlmap.

XSS alert pop-up.

Meterpreter reverse shell session.

Submitted by: Daniel Muthama

Date: May 3rd, 2025

This report adheres to ethical guidelines and reflects work performed on authorized targets.

Appendix

[saved in the **ATTACHED** ‘screenshots’ **AND** ‘output_files’ folder]