CHANDIGARH UNIVERSITY, GHARUAN

Department of Computer Science and Engineering

INTERNSHIP REPORT

Submitted in Partial Fulfilment of the
Requirements for the Degree of
Bachelor of Engineering (B.E.) in Computer Science and Engineering

Internship Program (20 Sep-25 Dec):

Cybersecurity Internship Program – Shentinelix Sphere Pvt Ltd

Task 2

DNS in Detail Pentesting Fundamentals

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

Executive Summary

This internship report summarizes the work completed by Vikash Upadhyay during the internship period at **Shentinelix sphere Pvt Ltd** from **20 Sep** to **25 Dec**. The focus of the internship was practical learning and hands-on exposure to information security research methodologies, vulnerability discovery resources, Linux tooling, and CTF-style problem solving. Key activities included completing guided TryHackMe modules (notably the Research Methodology room), using tools such as Burp Suite, steganography utilities, searchsploit/ExploitDB, and exploring Linux man pages. The internship strengthened applied research skills, introduced practical exploitation-research workflows, and produced demonstrable outcomes (task completions, writeups, and practical exercises). This report highlights duties performed, accomplishments, new skills, challenges faced, and final reflections.

Introduction

The primary objective of this internship was to develop practical cybersecurity research and network analysis skills. Tasks were designed to simulate real-world scenarios, requiring independent research, tool usage, and problem-solving. During the internship, I learned how to extract hidden data from files, investigate vulnerabilities, identify CVEs, use penetration-testing tools such as Burp Suite Repeater, and explore Linux command-line utilities. Additionally, I gained knowledge about the Domain Name System (DNS), its hierarchy, record types, and query resolution process.

Simultaneously, the TryHackMe "Starting Out in Cybersecurity" module provided foundational knowledge of cybersecurity career paths, introducing the major branches—offensive security (penetration testing, exploit research) and defensive security (SOC monitoring, incident response, malware analysis). This combination of theoretical orientation and practical training enhanced my investigative mindset, provided structured research skills, and prepared me for independent problem-solving in real-world scenarios.

Overview of the Company

Shentinelix Sphere Pvt. Ltd. is a cybersecurity training and solutions provider that specializes in delivering practical exposure in information security, penetration testing, and cyber defense. The company focuses on empowering students and professionals with real-world skills through structured labs, Capture-the-Flag (CTF) style challenges, and guided mentorship.

During the internship, I was assigned to the Cybersecurity Research and Training Department The organization strongly emphasizes hands-on learning by offering lab environments, curated challenges, and continuous support from experienced security practitioners, ensuring that interns develop both technical competence and a strong research methodology.

Description of Duties

During the internship, I performed the following duties:

- Completed structured hands-on modules on TryHackMe (Research Methodology, DNS and Welcome to Cybersecurity rooms).
- Researched cybersecurity techniques, tools, and exploits (e.g., steganography, Burp Suite workflows, ExploitDB/NVD/CVE).
- Practiced Linux command-line utilities and consulted man pages for tool options.
- Identified CVEs and correlated them with software versions.
- Learned and applied DNS concepts, including domain hierarchy, TLDs, subdomains, and record types.
- Performed a supervised penetration test engagement on ACME’s infrastructure, following a Rules of Engagement (ROE).
- Documented task completions, captured screenshots, and maintained clear technical notes.

Accomplishments

- Successfully completed TryHackMe modules covering research methodology, DNS, and cybersecurity career awareness.

- Extracted hidden data from images using steganography tools and tested HTTP requests via Burp Suite Repeater.

- Identified multiple CVEs (e.g., CVE-2020-10385, CVE-2016-1240, CVE-2007-0017, CVE-2019-18634) and understood their practical implications.

- Gained hands-on experience with DNS fundamentals, including record types (A, AAAA, MX, CNAME, TXT), TTL, and query resolution.

- Executed a scoped penetration test on ACME’s infrastructure: reconnaissance, scanning, vulnerability identification, exploitation (where permitted), and documentation of findings.

- Built a reproducible research workflow: **question → search → tool identification → test → document**.

- Produced professional technical documentation suitable for academic submission and portfolio use.

Skills Learned

Technical Skills:

- Penetration-testing and research tools: Burp Suite, steghide, searchsploit, Linux networking utilities.
- Vulnerability research using CVE, NVD, and ExploitDB.
- Linux fundamentals: scp, fdisk, nano, netcat, man pages.
- DNS concepts: hierarchy, TLDs, subdomains, record types, query resolution.
- Hashing: NTLM, sha512crypt formats.

Soft and Process Skills:

- Structured research methodology for problem-solving.
- Technical documentation and evidence collection.
- Time management, task prioritization, and adherence to ROE in practical engagements.
- Communicating findings to both technical and non-technical stakeholders.

Challenges Faced

- Information Overload: Filtering relevant sources from the vast internet resources.
- Tool Familiarity: Learning new options and workflows in unfamiliar tools.
- Version Mismatches: Correlating CVEs with specific software versions.
- Time Constraints: Balancing deep research with submission deadlines.

Conclusion

This internship provided hands-on exposure to cybersecurity research, penetration testing, Linux tools, and DNS fundamentals. By completing guided TryHackMe modules and supervised lab exercises, I developed practical problem-solving skills, enhanced technical knowledge, and built a reproducible methodology for independent research. The experience strengthened my foundation for future cybersecurity roles, cultivated a research-first mindset, and provided tangible outputs for academic and professional purposes. Moving forward, I plan to advance in offensive and defensive techniques, explore advanced exploitation, and contribute to more complex CTF challenges.

Acknowledgments

I would like to thank the team at **Shentinelix Sphere Pvt. Ltd.** for providing access to lab environments, learning resources, and a supportive environment that encouraged practical learning and skill development. Special thanks to the **TryHackMe platform** and the authors of the Research Methodology room for providing structured, hands-on lessons that significantly enhanced my research and problem-solving skills. Finally, I extend my gratitude to my peers and family for their continuous support and encouragement throughout the internship period.