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 1

Intro to Research & Starting Out in Cybersec

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

Information security is an inherently investigative discipline: success depends less on memorising facts and more on knowing where and how to find the right information. This internship was structured to reflect that reality, with a focus on problem-based learning through TryHackMe rooms, lab exercises, and guided research questions. Tasks included extracting hidden data with steganography tools, mapping software versions to CVEs, and replaying HTTP requests in Burp Suite Repeater. Working in a Kali Linux environment, I also gained fluency with essential utilities such as nc, scp, searchsploit, and steghide, while learning to consult man pages and correlate findings across trusted sources like ExploitDB and NVD. The combination of these skills — hands-on tool use and disciplined research methodology — resulted in completed challenge rooms, documented solutions, and a portfolio of evidence suitable for academic and professional use.

At the same time, the **TryHackMe "Starting Out in Cybersecurity"** module provided a strong conceptual foundation by introducing the major branches of the field — offensive security (penetration testing, exploit research) and defensive security (incident response, SOC analysis, malware defense). This overview not only clarified how different career paths fit into the cybersecurity landscape but also gave me a roadmap for progression. By pairing theoretical orientation with practical training, the internship equipped me with both the investigative mindset and the technical toolset necessary to begin a career in cybersecurity.

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 (e.g., TryHackMe Research Methodology and Welcome to Cybersecurity rooms) and documented solutions.
- Explored cybersecurity career paths, differentiating between offensive and defensive security roles.
- Researched techniques and tools (steganography extraction, Burp Suite workflows, searching ExploitDB/NVD/CVE databases).
- Practiced Linux command-line utilities and consulted manual pages to learn flags/options for tools (scp, fdisk, nano, netcat).
- Used Kali tools such as searchsploit to map software to known CVEs and assessed exploit relevance.
- Reproduced lab exercises and created short technical notes summarizing methods and results.
- Prepared screenshots and evidence of task completion for submission and evaluation.

Accomplishments

- Successfully completed the TryHackMe Research Methodology and Welcome to Cybersecurity modules.

- Gained awareness of cybersecurity career paths including penetration testing, SOC analysis, incident response, and malware analysis.

- Identified and documented relevant CVEs (e.g., CVE-2020-10385 for WPForms, CVE-2016-1240 for Debian Apache Tomcat, CVE-2007-0017 for VLC, CVE-2019-18634 for sudo).

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

- Developed a portfolio of lab screenshots and step-by-step documentation suitable for academic evaluation and interviews.

Skills Learned

Technical:

- Practical use of penetration-testing and research tools: Burp Suite (Repeater), steghide and related steganography utilities, searchsploit/ExploitDB, Linux networking tools (netcat), and package management with apt.
- Use of penetration-testing and research tools: Burp Suite (Repeater), steghide, searchsploit, Linux networking tools.
- Vulnerability research: searching NVD, Mitre CVE, and ExploitDB for exploits and CVE details.
- Linux fundamentals: using man pages, understanding common switches (scp -r, fdisk -l, nano -B), and basic shell commands.
- Hashing knowledge: recognizing NTLM and unix crypt formats (e.g., 6 corresponds to sha512crypt).

Soft:

- Structured research methodology (breaking down complex problems, iterating on findings).
- Technical documentation and evidence collection (clear notes and screenshots).
- Time and task management to complete modules and meet internship deliverables.

Challenges Faced

- **Information overload:** With many possible sources online, identifying authoritative and relevant resources required discipline. I overcame this by prioritizing official docs, reputable security blogs, and established databases (NVD, CVE, ExploitDB).
- **Tool familiarity:** Some tools (steghide, Burp Suite) required experimentation and consultation of manuals.
- **Toolchain familiarity:** Some tools (e.g., steghide, Burp Suite) had unfamiliar options; resolving this required reading man pages and practical experimentation.

- **Version mismatches:** Finding exact exploits that match target software versions was sometimes difficult; I learned to correlate CVE year/ID with release dates and patch notes.
- **Time constraints:** Balancing depth of research with deadlines forced prioritization of the most educational tasks and documenting the rest for follow-up learning.

Conclusion

This internship provided a practical, hands-on bridge between theoretical concepts and real- world cybersecurity tasks. By completing guided rooms and conducting independent research I improved both my tool proficiency and my approach to solving unfamiliar problems. The experience solidified a research-first mindset essential for cybersecurity work and provided tangible accomplishments and documentation that I can present to future employers. I plan to continue building on this foundation by exploring advanced exploitation, defensive techniques, and contributing 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.