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 3

Linux Fundamentals Part 1 / Linux Strength Traning

Internship Report Submitted By:

Vikash Upadhyay

Table of Contents

3. 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.

4. Introduction

The primary objective of this internship was to gain practical knowledge and hands-on experience in cybersecurity, focusing on Linux systems, data security, and network technologies. In today's digital world, where cyber threats are constantly evolving, proficiency in system administration, data protection, and security research is essential for any aspiring cybersecurity professional.

This internship provided the opportunity to:

- Build strong foundational skills in Linux, including file system navigation, file and folder management, advanced searching, and command-line efficiency.
- Understand data security concepts, such as hashing, encryption, Base64 encoding, and secure password management.
- Develop practical experience in SQL database management, including connecting to local and remote databases, querying data, and analyzing relational database structures.
- Explore DNS fundamentals, including domain hierarchies, record types, query analysis, and server configurations.
- Apply research methodology in cybersecurity, learning to locate vulnerabilities, analyze exploits, and leverage online resources such as CVE databases and ExploitDB.
- Improve analytical thinking and problem-solving skills through structured TryHackMe labs and CTF-style exercises that simulate real-world cybersecurity challenges.

During the internship, I was exposed to realistic cybersecurity scenarios, where I practiced extracting sensitive information, managing encrypted data, and understanding the workflow of ethical hacking. By combining theoretical knowledge with hands-on exercises, I developed the

ability to approach complex security problems methodically, make informed decisions, and apply tools effectively.

Overall, this internship aimed to bridge the gap between academic learning and professional cybersecurity practice, providing me with the skills, confidence, and insight necessary to pursue a career in ethical hacking, penetration testing, and cybersecurity research.

5. 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.

6. Description of Duties

6.1 Research Methodology

- Learning to conduct structured cybersecurity research.
- Using platforms like ExploitDB, CVE databases, and Linux man pages.
- Extracting hidden data from files, images, or databases for CTF challenges.
- Applying logical analysis to prioritize and verify findings.

6.2 DNS Fundamentals

- Understanding domain hierarchy: TLD, second-level domains, subdomains.
- Exploring DNS record types: A, AAAA, CNAME, MX, TXT.
- Performing DNS queries and analyzing server responses.
- Understanding recursive and authoritative DNS servers, TTL, and propagation.

6.3 Linux Fundamentals & Strength Training

6.3.1 File and Directory Management

- Navigation: cd, pwd, ls.
- Viewing files: cat [filename].

- Creating/editing files/folders: touch [filename], mkdir [foldername], nano [filename].
- Copying/moving/renaming: cp, mv, handling multiple files and directories.

Searching:

- By name: find /home/user -type f -name file.txt.
- By size: find /home/user -type f -size 10c.
- By user/group: find /etc/server -type f -user john.
- By date modified/accessed: find / -type f -newermt '2020-06-30'.
- By keyword: grep -iRl '/folderA/flag'.

Efficiency tips:

- CTRL+L to clear screen, up-arrow for previous commands.
- 2>/dev/null to ignore permission errors.

6.3.2 Hashing

- Hashing converts data to irreversible strings for integrity verification.
- Algorithms: MD5, SHA1 (weak), SHA-256 (recommended).

Cracking hashes with John the Ripper:

john --format=md5 --wordlist=rockyou.txt hash.txt

- Identifying unknown hashes with hash-identifier [hash].

6.3.3 Base64 Encoding/Decoding

Encoding converts binary data to ASCII text:

echo "example" | base64

Decoding:

cat [file] | base64 -d > output.txt

6.3.4 Encryption & Decryption

Using GPG for AES-256 encryption:

gpg --cipher-algo AES256 -c sensitive.txt

gpg sensitive.txt.gpg

Cracking encrypted files using gpg2john and John the Ripper:

gpg2john file.gpg > hash.txt

john --wordlist=rockyou.txt --format=gpg hash.txt

6.3.5 SQL Database Interaction

- Start/stop MySQL services: service mysql start/stop.
- Connect to remote MySQL: mysql -u [user] -p -h [host].

Load and view local database:

mysql -u [user] -p

source file.sql

SHOW DATABASES;

USE employees;

SHOW TABLES;

DESCRIBE table_name;

SELECT * FROM table_name;

7. Accomplishments

- Completed TryHackMe labs: Research Methodology, DNS, Linux Fundamentals, Hashing, Encryption, Base64, SQL**.**
- Developed proficiency in Linux command-line navigation and file management**.**
- Cracked password hashes and decrypted GPG files successfully.
- Queried and analyzed relational databases.
- Applied DNS knowledge to understand domain hierarchies and record types.
- Built strong analytical, problem-solving, and research skills.

8. Skills Learned

Technical Skills:

- Linux navigation, file management, and advanced search.

- Hashing, Base64 encoding/decoding, and encryption/decryption.
- SQL database operations and data analysis.
- DNS systems, queries, and record type understanding.

Soft Skills:

- Analytical and critical thinking.
- Independent research and experimentation.
- Attention to detail handling sensitive data.
- Time management while completing complex lab exercises.

9. Challenges Faced

- Adjusting to text-based Linux terminal interface.
- Understanding hash types and cracking techniques.
- Working with encrypted files without passwords.
- Grasping relational database structure and writing queries.
- Handling errors in Linux due to special characters or permission issues.
- Interpreting DNS responses and resolving queries effectively.

10. Conclusion

The internship provided extensive hands-on experience in Linux, hashing, encryption, Base64, SQL databases, research methodology, and DNS fundamentals. It strengthened technical proficiency, analytical thinking, and problem-solving skills, preparing me for real-world cybersecurity challenges and future work in penetration testing and ethical hacking.

11. 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.