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 4**

*OpenVAS / UltraTech1 / Physical Security Intro*

Internship Report Submitted By:
Vikash Upadhyay

**Table of Contents**

## Executive Summary

This report documents my hands-on internship/training experience combining TryHackMe guided rooms, supervised lab access from Shentinelix Sphere Pvt. Ltd., and a scoped penetration test engagement against ACME's infrastructure. Over the internship I completed multiple practical exercises (OSINT/SINT enumeration, web and network testing, service exploitation, and physical security fundamentals), produced lab writeups and a final engagement summary, and followed formal Rules of Engagement (ROE) and ethical procedures. Key outputs include discovery and exploitation of application and service misconfigurations, recovery of credentials from a leftover database, a successful scoped engagement on ACME, and gains in both technical tool use and reporting/communication skills.

## Introduction

The objective of this internship was to convert theoretical cybersecurity knowledge into practical capability by performing guided labs and a real-world style penetration testing engagement. Training focused on three pillars: (1) offensive skills — reconnaissance, scanning, exploitation, post-exploitation and reporting; (2) defensive awareness — detection and incident response fundamentals; and (3) physical security awareness — basic bypass and entry techniques relevant to red-team operations. All activities were performed under supervision and within explicit scope and legal agreements.

Specific aims:

- Learn and apply reconnaissance/OSINT techniques, including extracting metadata and contextual clues from a single image.
- Perform active scanning and enumeration of target hosts and services.
- Identify and validate vulnerabilities within scope; exploit only when permitted by ROE.
- Perform safe post-exploitation analysis to demonstrate impact.
- Produce clear, prioritized reporting and remediation recommendations.
- Gain introductory knowledge of physical security bypass techniques relevant to red-team operations.

Scope boundaries:

- All offensive actions were restricted to lab environments provided by Shentinelix/ACME lab and the TryHackMe rooms.
- No testing was performed against any real public infrastructure or third-party services.
- Social engineering (phishing or direct contact) was prohibited unless specifically allowed in ROE.

**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 was responsible for:

Daily responsibilities and concrete tasks performed:

1. Reconnaissance & OSINT
   - Task: Analyze a single image for metadata and visual clues.
   - Tools/process: exiftool for metadata, manual visual inspection, reverse-image search, GitHub/Google searches.
   - Outputs: username/email, location, Wi-Fi SSID, social links, holiday images, exposed passwords visible in images.
2. Network Scanning & Enumeration
   - Task: Map network surface and identify listening services.
   - Tools/commands:
     - nmap -sV -p- -T4 <target> — full port/service discovery.
     - nmap -sV -p 8081,31331 <target> — focused scanning.
     - curl -I http://<target>:8081/ and curl http://<target>:8081/api/route for REST endpoints.
   - Outputs: Node.js on port 8081 (REST API), Apache listening on 31331, OS fingerprint (Ubuntu).
3. Web Application Testing
   - Task: Interact with web application and REST API, enumerate routes and parameters.
   - Tools: Burp Suite (proxy), browser devtools, curl.
   - Actions: Enumerated API routes, tested endpoints for parameter validation,

inspected client code for used routes.

4. Artifact & Database Analysis
   - Task: Locate and analyze local artifacts; extract credentials.
   - Tools/commands:
     - find / -name "utech.db.sqlite" (lab environment)
     - sqlite3 utech.db.sqlite ".tables" and SQL queries to dump user table.
     - Extracted hash f357a0c52799563c7c7b76c1e7543a32.
5. Credential Cracking
   - Task: Crack retrieved password hash.
   - Tools: John the Ripper / Hashcat.
   - Example command (John): john --format=md5crypt --wordlist=/usr/share/wordlists/rockyou.txt hashfile
   - Output: plaintext n100906 (example result from lab).
6. Post-exploitation (Scoped & Safe)
   - Task: Use valid credential to demonstrate impact within scope (limited shell commands, read-only artifact verification).
   - Tools: sqlite3, web interface login simulation.
   - Always ensured no persistence/backdoors and all actions were logged.
7. Physical Security Awareness
   - Training: watched videos and practiced identification of bypass tools and scenarios.
   - Tools learned about: Under-the-Door Tool, Air Wedge, Shims, Traveler Hook, Double Door Tool.
8. Reporting
   - Output: full engagement report with Executive Summary, technical findings, risk ratings (High/Medium/Low), remediation guidance, and appendices (commands, screenshots, proof-of-concept descriptions).

**Accomplishments**

- Completed guided TryHackMe rooms and answered embedded assessment items correctly across offensive, defensive and physical security topics.
- OSINT / Image analysis (OhSINT-style): extracted multiple data points from one image file — user avatar (cat), location (London), Wi-Fi SSID (UnileverWiFi), personal email

(OWoodflint@gmail.com), source site (GitHub), holiday destination (New York), and an exposed password (pennYDr0pper.!). These demonstrated how much actionable intelligence can be harvested from a single image and associated metadata/artefacts.

- Service enumeration and exploitation: discovered services and ports on a lab machine — Node.js service on port 8081, Apache on non-standard port 31331, and the host running Ubuntu. Located a local SQLite database (utech.db.sqlite) containing user records; recovered a stored password hash (f357a0c52799563c7c7b76c1e7543a32) and cracked it to reveal the plaintext password n100906.
- Conducted a scoped penetration test on ACME infrastructure following the defined methodology and ROE: information gathering, scanning/enumeration, vulnerability assessment, safe exploitation (limited to scope), privilege escalation, and drafting remediation advice.
- Physical security training: reviewed common bypass tools and concepts (Under-the-Door Tool, Double Door Tool, Air Wedge, Shim, Traveler Hook, film improvisation techniques, REX sensor bypass considerations, and shielding for Adams Rite hardware).

**Skills Learned**

Technical Skills:

- Use of penetration-testing and research tools: Burp Suite, steghide, searchsploit, Linux networking utilities.
- Vulnerability research and mapping using CVE, NVD, and ExploitDB.
- Linux fundamentals: man pages, scp, fdisk, nano, netcat.
- Understanding and practical application of DNS concepts, hierarchy, and record types.
- Hashing knowledge: NTLM and Unix formats (e.g., sha512crypt).

Soft Skills:

- Structured research methodology for problem-solving.
- Technical documentation and evidence collection.
- Time management and task prioritization.

**Challenges Faced**

- Legal/ethical boundaries — differentiating actions that were legally allowed by the ROE from actions that, while technically possible, would be out of scope or ethically dubious (e.g., phishing/emails targeting real users). This required frequent consultation with supervisors and careful documentation.

- Time management during full-scope enumeration — balancing breadth of coverage versus deep exploitation of high-impact targets. Prioritization for remediation and reporting was essential.

- Ambiguity in application behaviours — some observed behaviors could be legitimate features rather than vulnerabilities; these required additional safe testing and corroboration before reporting.

- Password and credential handling — ensuring secure and responsible handling of recovered

### Conclusion

This internship effectively bridged theoretical coursework and practical cybersecurity tasks. Guided rooms and real-world style engagements improved my technical proficiency with reconnaissance, enumeration, exploitation, and reporting, and reinforced the importance of a methodical, research-first approach. The experience yielded concrete artifacts (lab notes, exploited findings, remediation recommendations) suitable for inclusion in a professional portfolio. Going forward I plan to deepen expertise in advanced exploitation techniques, defensive monitoring and incident response, and participate in more complex CTF challenges to broaden both depth and breadth.

### 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.