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 10 - 16

Traffic Analysis Essentials, Python Playground and Peak Hill

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.

During this training period, I successfully completed three highly practical cybersecurity rooms on TryHackMe — **Traffic Analysis Essentials**, **Python Playground**, and **Peak Hill**. Each room was designed to strengthen a different but interconnected area of cybersecurity: network monitoring and analysis, application exploitation through Python, and privilege escalation techniques in a controlled environment. Collectively, they provided a hands-on understanding of both the offensive and defensive sides of cybersecurity.

This combined internship experience helped me bridge theoretical knowledge with practical investigation skills. I learned how to analyze network traffic patterns, decode obfuscated or serialized data structures, and identify misconfigurations in real-world systems that could lead to unauthorized access. The completion of all three rooms required structured problem-solving, critical thinking, and technical proficiency in both network and system-level operations.

Additionally, the program emphasized the significance of security architecture design and defensive engineering. It taught me how proper access control, policy management, and system hardening contribute to a secure network environment. By working on both attack simulation and defense strategies, I gained a holistic perspective on cybersecurity operations — one that focuses equally on prevention, detection, and response.

Introduction

The purpose of this internship was to develop an in-depth understanding of **Network Security** and **Traffic Analysis**, alongside learning how vulnerabilities in systems and applications can be exploited using tools and coding techniques. The **Traffic Analysis Essentials** room introduced me to the fundamentals of network monitoring, anomaly detection, and the classification of control levels — physical, technical, and administrative. The **Python Playground** and **Peak Hill** rooms expanded this foundation into applied cybersecurity, focusing on exploitation and privilege escalation techniques.

These rooms followed a structured learning path: theory, hands-on labs, and simulation. The **Traffic Analysis Essentials** section taught how real-time monitoring can detect intrusions and data leaks, while **Python Playground** exposed me to the inner workings of code exploitation

through the manipulation of Python's serialization mechanisms. **Peak Hill**, on the other hand, was a culmination of these skills — involving reconnaissance, decompilation, privilege escalation, and secure shell persistence.

Together, these modules created a learning flow from detection to exploitation and mitigation. The knowledge gained from the labs helped me understand how attackers identify vulnerabilities and how defenders can build better protections. This balanced exposure improved both my red-team (offensive) and blue-team (defensive) cybersecurity competencies.

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

- Performed network traffic analysis to identify malicious IP addresses, suspicious flows, and packet anomalies using real-time monitoring techniques.
- Analyzed and categorized security controls into physical, technical, and administrative layers for effective protection strategies.
- Captured and investigated network packets to detect potential attacks and data exfiltration patterns.
- Executed Python exploitation exercises to bypass blacklisted functions and gain restricted shell access in simulated environments.
- Conducted source code analysis to find vulnerabilities in web-based Python applications and serialization logic.
- Utilized tools such as Wireshark, Nmap, Netcat, and Uncompyle6 for reconnaissance, enumeration, and reverse engineering.
- Decoded pickled credential files and safely extracted sensitive data without executing malicious payloads.
- Performed privilege escalation tasks in the Peak Hill room by exploiting misconfigurations and improper file permissions.
- Documented each step, methodology, and command used during exploitation and analysis for future reference.

- Proposed mitigation strategies and secure coding practices to prevent exploitation of identified vulnerabilities.
- Collaborated with online TryHackMe community discussions to cross-verify solutions and enhance analytical accuracy.

Maintained detailed logs and progress reports for every completed challenge, ensuring traceability and professional documentation standards. Accomplishments
During the course of this internship, I achieved several major milestones. In the Traffic Analysis Essentials module, I successfully identified malicious network activity and captured both flags — THM{PACKET_MASTER} and THM{DETECTION_MASTER} — demonstrating proficiency in network traffic filtering and pattern recognition. This accomplishment reflected my ability to apply theory to practice in identifying anomalous data flow.

In the Python Playground room, I managed to bypass a blacklisted Python environment using creative import techniques and achieved command execution in a restricted shell environment. This experience greatly improved my understanding of Python-based web applications and how insecure coding practices can be exploited. In Peak Hill, I went further by decoding serialized data, gaining user access, and escalating privileges to root — completing the room with all required flags.
Another accomplishment was my ability to compile detailed, step-by-step documentation for each challenge. This not only proved my technical understanding but also helped me build a structured reporting style suitable for professional cybersecurity operations, penetration testing, and research documentation.

Skills Learned
Through this internship, I acquired a broad range of technical and analytical skills. I became proficient in Network Security concepts, such as authentication, authorization, access control, intrusion detection, and anomaly monitoring. The exercises enhanced my understanding of how different control levels (physical, technical, administrative) are applied to protect data, users, and network infrastructure.I also developed advanced Python exploitation and debugging skills, particularly around safe handling of pickled objects, bypassing restrictions using built-in functions, and analyzing serialized data. The labs strengthened my command-line skills, use of Linux utilities, and experience with tools like nmap, netcat, and uncompyle6. These tools were crucial for enumeration and reverse engineering tasks.

Additionally, I improved my soft skills, including time management, technical writing, and analytical reasoning. I learned how to think like both an attacker and a defender — evaluating vulnerabilities from multiple perspectives and documenting outcomes in a professional format suitable for academic and industry purposes.

Challenges Faced

One of the biggest challenges was adapting to the depth of network data during the Traffic Analysis Essentials exercises. Understanding packet headers, flow statistics, and anomaly detection patterns required continuous research and hands-on practice. Another challenge was interpreting encrypted or compressed data during flow analysis, as it limited the ability to identify precise threat vectors without decryption.

In Python Playground, I initially struggled with the filtering system that restricted certain keywords, making it difficult to execute standard commands. This challenge forced me to think creatively and experiment with alternative syntax and hidden Python functionalities to achieve the desired outcome. Similarly, the Peak Hill room tested my ability to decode and safely handle pickled credential files without executing them maliciously.

Overcoming these challenges taught me patience, persistence, and resourcefulness. I learned that in cybersecurity, every failure or dead-end is an opportunity to refine methods and gain new insights. These challenges significantly improved my confidence in troubleshooting, problem-solving, and working under pressure.

Conclusion

Completing the **Traffic Analysis Essentials**, **Python Playground**, and **Peak Hill** rooms collectively provided me with a strong and diverse foundation in cybersecurity. I developed both theoretical knowledge and practical proficiency in network security, data analysis, and ethical hacking. The hands-on simulations helped me understand the lifecycle of cyber incidents — from detection to exploitation and mitigation.The experience also reinforced my commitment to cybersecurity as a career path. It taught me that security is not only about tools but also about mindset, methodology, and continuous learning. Through these rooms, I learned to approach problems systematically and maintain ethical standards while performing security research.

In conclusion, this internship has been transformative. It has helped me build a professional-level understanding of cyber defense and offense, improve my problem-solving approach, and gain real-world readiness. I now feel equipped to take on more advanced cybersecurity challenges and pursue certifications or roles focused on network defense, ethical hacking, and threat analysis.

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.