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 5

Passive and Active Reconnaissance

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

Executive Summary

This internship focused on practical training in network security with a concentrated module on reconnaissance — covering both passive and active techniques. Using TryHackMe rooms, AttackBox environments, and mentorship from Shentinelix Sphere Pvt. Ltd., I practised gathering information responsibly and ethically, mapping network assets, and performing initial service enumeration. Key activities included passive data collection (WHOIS, DNS queries, Shodan, DNSDumpster) and active engagement (ping, traceroute, telnet, netcat, browser developer tools, Nmap). The module strengthened my understanding of reconnaissance methodology, legal/ethical boundaries, and the technical toolchain used in early-stage penetration testing.

Introduction

Reconnaissance is the foundational phase of any security assessment. It contains two complementary approaches: passive reconnaissance, which gathers information from public sources without interacting directly with target systems, and active reconnaissance, which uses direct interaction to discover live services and network behavior. The objective of this module was to learn how to collect, interpret, and correlate reconnaissance data while maintaining legal and ethical boundaries. Through lab exercises and controlled engagements, I developed workflows to discover assets, prioritise targets, and prepare for subsequent vulnerability analysis and exploitation stages.

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

Passive Reconnaissance

- Collected publicly available domain and infrastructure information using whois, nslookup, and dig.
- Used online resources such as DNSDumpster for DNS mapping and subdomain discovery.

- Queried Shodan to discover exposed services, devices, and server banners associated with target IPs.
- Extracted metadata and footprints from web pages and public repositories (OSINT).
- Compiled passive findings and prioritized assets for further (controlled) testing.

Active Reconnaissance

- Performed controlled host reachability and path analysis using ping and traceroute/tracert.
- Used browser developer tools (DevTools) to inspect page structure, requests, cookies, and client-side resources.
- Performed banner grabbing and basic interaction with services using telnet and netcat (nc).
- Conducted safe, scoped port and service discovery with nmap (where permitted in the lab) to identify open ports and service versions.
- Combined passive and active data to create an initial network map and test plan, all executed under lab/ROE constraints.

Documentation & Reporting

- Recorded all commands, outputs, screenshots, and notes for reproducibility.
- Distinguished which findings were passive vs. active and documented the ethical/legal stance for each action.
- Prepared lab write-ups summarizing tools used, methodology, and next recommended steps for vulnerability assessment.

Accomplishments

- Completed all lab exercises in both Passive and Active Reconnaissance modules.
- Successfully gathered domain and DNS data using whois, nslookup, and dig.
- Mapped subdomains and public assets using DNSDumpster and corroborated findings with Shodan.
- Performed traceroute and interpreted network hops to understand routing paths.
- Extracted service banners and checked open ports via telnet, nc, and nmap(within lab scope).
- Used browser DevTools to analyze web application resources and client-side behaviour.

- Produced clear, reproducible documentation (command logs, screenshots, and summaries) suitable for reporting and portfolio inclusion.

Skills Learned

Technical Skills

- Passive tools: whois, nslookup, dig, DNSDumpster, Shodan.io.
- Active tools: ping, traceroute/tracert, telnet, netcat (nc), nmap.
- Browser-based reconnaissance: Chrome/Firefox DevTools (network, console, sources).
- Interpreting DNS records (A, AAAA, MX, TXT, CNAME) and TTL implications.
- Basic banner grabbing, port/service identification, and correlating version information with public vulnerability databases.

Conceptual / Soft Skills

- Distinguishing passive vs active reconnaissance and their operational implications.
- Ethical reasoning and adhering to Rules of Engagement (ROE) and lab scope.
- Structured documentation and reproducible workflows for security assessments.
- Prioritisation of reconnaissance findings to guide subsequent vulnerability analysis.

Challenges Faced

- **Interpreting noisy OSINT:** Public data sometimes contained duplicates, stale entries, or misleading records that required cross-verification.
- **Shodan result interpretation:** Filtering Shodan output to identify truly relevant exposures required experience and context.
- **Traceroute analysis:** Mapping hop information to real-world infrastructure (e.g., CDN, ISP) needed careful analysis.
- **Tool nuance learning curve:** Understanding flags and output formats (e.g., dig vs nslookup, nmap timing/safeguards).
- **Ethical/legal constraints:** Ensuring every active test remained within the permitted lab scope a

Conclusion

The combined Passive and Active Reconnaissance module provided a comprehensive, hands-on foundation for early-stage security assessments. I developed a repeatable reconnaissance workflow: discover (passive) → verify (active) → map → prioritise → document. The practical experience improved my ability to gather reliable intelligence, understand network layouts, and

responsibly use reconnaissance tools — all essential capabilities for future penetration testing and security analyst roles. Going forward, I plan to deepen skills in automated discovery, service fingerprinting, and correlating reconnaissance outputs with vulnerability research.

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.