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 17

Introduction to Dark Web, Anonymity, Cryptocurrency

And Wifi Hacking 101

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

Executive Summary

I completed a dual-topic training module that combined an introductory course on the Dark Web, anonymity tools (Tor, Proxychains) and basic cryptocurrency concepts, with a practical WiFi security lab focused on WPA/WPA2 attack techniques using the Aircrack-ng suite. The course balanced theory (privacy risks, onion services, Bitcoin fundamentals) with hands-on labs (installing Tor on Windows/Kali, configuring Proxychains, enabling monitor mode, capturing 4-way handshakes, and cracking a provided capture). Emphasis throughout was on ethical, legal practice and defensive understanding.

The outcome of the training was twofold: (1) conceptual mastery — learners can explain the Tor architecture, Onion services, and how Bitcoin transactions enable pseudonymous payments; and (2) practical competency — learners can set up Tor/Proxychains, safely browse onion services, enable monitor mode on wireless NICs, capture handshakes with airodump-ng, and use aircrack-ng/hashcat workflows to test WPA2 PSK strength. The WiFi lab specifically reinforced that real-world attacks require the right hardware (monitor-capable NIC, injection support), appropriate wordlists, and patience.

This combined module improved my ability to perform structured, legally-sound security assessments and to produce risk-based recommendations. It also highlighted operational constraints (legal/ethical boundaries, tooling limits) and produced measurable results — successful Tor/Proxychains configuration, successful handshake capture, and extraction of the test password from the supplied capture using rockyou/hashcat technique.

Introduction

This report documents the learning objectives, tasks, and outcomes for two complementary cybersecurity topics: Dark Web/Anonymity/Cryptocurrency, and WiFi Hacking 101. Both are essential for modern security professionals: the former for understanding threat actor marketplaces and privacy tools, the latter for evaluating wireless network security posture. The training was delivered as a blended set of short videos, demonstrations, and hands-on labs.

The Dark Web portion covered what the Tor network is, how Onion Services operate, the privacy vs. anonymity distinction, risks of deanonymization, and safe browsing practices. It also introduced Proxychains as an additional routing/redirect tool for chaining proxies and Tor. The cryptocurrency section provided an accessible explanation of Bitcoin — wallets, addresses, transactions, and the role of cryptocurrencies in enabling pseudonymous transactions on darknet markets.

The WiFi Hacking 101 room focused on WPA/WPA2-PSK basics, the 4-way handshake, and the practical Aircrack-ng workflow: enabling monitor mode (airmon-ng), capturing traffic (airodump-ng), forcing re-authentication (aireplay-ng deauth), and cracking with aircrack-ng or hashcat. The pedagogical approach emphasized lab safety, legal use (test networks or explicit permission), and translating offensive techniques into defensive remediation guidance.

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

I installed and configured the Tor Browser on Windows 10 and Kali Linux, verified circuit creation, and explored Onion Services using test/benign sites. I configured Proxychains to force specific traffic through Tor and tested different proxy types. I documented safe-access guidelines (disable plugins, avoid downloaded binaries, use a VM) and created checklists for secure browsing and evidence handling.

I prepared a lab environment (hotspot with known weak password), ensured a monitor-mode capable NIC was available, and executed the Aircrack-ng workflow: airmon-ng start, airodump-ng capture with --bssid/--channel and -w options, aireplay-ng deauth to trigger re-authentication, and finally password cracking using aircrack-ng and hashcat (HCCAPX conversion) against rockyou. I also practiced capturing and analyzing pcap files and converting them for GPU cracking.

For both tracks I maintained a lab log: precise commands used, timestamps, environment details, and remediation suggestions. I ensured all testing was confined to lab systems or explicitly permitted networks. I prepared presentation slides and a short SOP for safe exploration of onion services and for conducting wireless penetration tests in a controlled, documented manner.

Some quick duty points:

- Configure Tor Browser securely (disable scripts, use fresh profile).
- Build Proxychains config and test applications through it.
- Enable monitor mode: airmon-ng start wlan0 → wlan0mon.
- Capture handshake: airodump-ng --bssid <BSSID> --channel <ch> -w <file> wlan0mon.
- Force handshake: aireplay-ng --deauth 5 -a <BSSID> -c <client> wlan0mon.
- Crack with aircrack-ng/hashcat; convert to HCCAPX if using GPU.

Acomplishments

Successfully installed and configured Tor Browser on both Windows 10 and Kali Linux; validated onion service access in a lab setting while following hardened browsing practices. Proxychains was set up to route command-line tools through Tor, and I confirmed traffic flow and DNS leakage prevention via tests.

Captured a valid WPA2 4-way handshake in the lab, performed HCCAPX conversion, and cracked the provided capture using the rockyou wordlist (password recovered: *greeneggsandham* from the supplied capture). Demonstrated the complete capture-to-crack workflow and documented performance observations (CPU vs GPU cracking speeds).

Produced: (a) a step-by-step SOP for safe Dark Web exploration, (b) a Proxychains configuration template, (c) a lab log with all Aircrack-ng commands and outputs, and (d) a remediation checklist for hardening wireless networks (strong passphrases, WPA3 where possible, client/network logging).

Accomplishment bullet points:

- Tor + Proxychains deployed and validated.
- Completed chapter quizzes and hands-on tasks with 100% lab completion.
- Successfully cracked lab capture and documented attack timeline.
- Created remediation checklist for network owners.

Skills Learned

Understanding Tor's onion routing, conceptual differences between anonymity and privacy, how onion services are published, and the common deanonymization pitfalls (timing correlation, browser/OS leaks). Grasped Bitcoin basics: keys, addresses, transactions, mempool, and how coins can be mixed/obfuscated (mixers, coinjoin) — and the limits of true anonymity with cryptocurrency.

Hands-on use of Tor Browser, Proxychains, and associated utilities. For WiFi: mastery of the Aircrack-ng suite (airmon-ng, airodump-ng, aireplay-ng, aircrack-ng), capture file handling, and the workflow to convert captures for GPU cracking with hashcat. Learned NIC selection criteria (monitor mode + injection support) and practical troubleshooting steps.

Improved lab preparation, evidence logging, and report-writing for security assessments. Enhanced judgment around legal/ethical boundaries, risk communication to stakeholders, and ability to propose prioritized mitigations (e.g., enforcing 12+ char random passphrases, enabling enterprise EAP, and monitoring for rogue APs).

Skills bullet list:

- Tor network fundamentals and safe browsing practices.
- Proxychains configuration and command-line testing.

- Aircrack-ng workflow: monitor mode → capture → deauth → crack.
- Converting pcap → hccapx and using hashcat.
- Documentation, SOP creation, and risk-based remediation.

industry purposes.

Challenges Faced

A core challenge is maintaining strict adherence to legal/ethical boundaries: practicing only on owned or explicitly authorized networks. This necessitated building isolated lab environments (hotspots, VM sandboxes) and documenting permission to avoid accidental misuse.

Not all wireless adapters support monitor mode or packet injection — finding compatible hardware was necessary. In the field, environmental noise, overlapping channels, and client mobility reduce capture success rate. Similarly, Tor browsing can be slowed by volunteer relay capacity and exit node restrictions.

Proxychains/Multi-proxy setups can leak DNS or fail silently if misconfigured; careful testing is required. Cracking WPA2 relies heavily on wordlist quality and compute resources — GPU acceleration helps, but large-scale cracking remains time and resource intensive. Also, cryptocurrency anonymity is imperfect; deanonymization techniques are a continuing concern.

Challenge bullet points:

- Ensuring use of legal test targets only.
- Procuring monitor-capable NICs and suitable GPU resources.
- Avoiding operational mistakes that leak identity (e.g., using the same browser profile across Tor and clearnet).
- Managing time/resources for cracking (wordlists, GPU vs CPU).

Conclusion

This combined module provided a robust, ethical introduction to both the Dark Web/anonymity ecosystem and practical wireless security testing. The theoretical modules demystified Tor, Onion Services, Proxychains, and the basics of Bitcoin; the labs turned concepts into actionable skills — from configuring anonymity tools to capturing and cracking WPA2 handshakes. Completing the coursework and labs improved my ability to think like both defender and attacker, which is crucial for effective penetration testing and incident response.

Moving forward, recommended next steps include: practicing defensive controls (WPA3 migration, client isolation, enterprise authentication), deeper study of deanonymization

research, experimenting with alternative anonymity tools and coin-privacy techniques (safely and ethically), and expanding wordlist and GPU cracking strategies in controlled environments. Above all, continuing to emphasize lawful, documented testing and responsible disclosure will ensure these skills are used to strengthen security rather than harm it.

Closing recommendations (concise):

- Always test only on authorized networks or lab gear.
- Harden wireless: long random PSKs, WPA3/enterprise, regular key rotation.
- For privacy research: use isolated VMs, avoid downloading unknown binaries, and keep detailed logs.
- Document findings and propose prioritized remediation for stakeholders.

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.