

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 7

Win AD Basics , SearchLight OSINT and Sakura

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

1. Title Page
2. Table of Contents
3. Executive Summary
4. Introduction
5. Overview of the Company
6. Description of Duties
7. Accomplishments
8. Skills Learned
9. Challenges Faced
10. Conclusion
11. Acknowledgments

Executive Summary

During my internship, I was provided with extensive hands-on experience in cybersecurity, focusing on three key areas: Windows Active Directory (AD) administration, SearchLight IMINT/GEOINT, and Sakura OSINT Room investigations.

The internship helped me understand the practical implementation of corporate network management, the use of visual intelligence for geolocation, and the use of passive OSINT techniques to trace cybercriminals. By the end of the program, I was able to perform AD management tasks, geolocate images based on visual clues, and track digital footprints to gather evidence for investigative scenarios.

This experience not only strengthened my technical skills but also enhanced my analytical thinking, problem-solving, and understanding of cybersecurity workflows.

Introduction

Cybersecurity is an essential discipline in today's technology-driven world, as organizations increasingly rely on digital systems for operations, communications, and data storage. Protecting these systems requires not only technical knowledge but also investigative skills to detect and respond to threats.

During this internship, I had the opportunity to work with three key cybersecurity areas: Windows Active Directory (AD) administration, SearchLight IMINT/GEOINT, and Sakura OSINT investigations. Each of these areas provided a unique perspective on managing digital environments and analyzing cyber threats:

1. **Windows Active Directory (AD):** Provided experience in managing users, computers, groups, and security policies in a centralized network. This environment simulates real-world corporate networks, where efficient management of hundreds of users and devices is critical.
2. **SearchLight IMINT/GEOINT:** Introduced image intelligence and geospatial intelligence techniques. I learned to analyze visual data, extract clues, and geolocate images accurately, skills crucial in cyber investigations, reconnaissance, and threat intelligence.
3. **Sakura OSINT Room:** Focused on real-world digital investigations using passive OSINT techniques. I explored tracking attackers through usernames, analyzing metadata, and investigating cryptocurrency activity, thereby gaining insight into investigative workflows used in cybersecurity operations.

This internship strengthened both my technical abilities and analytical thinking, enabling me to

apply classroom knowledge to practical cybersecurity scenarios. It also highlighted the importance of attention to detail, methodical investigation, and ethical considerations when handling sensitive digital information.

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

Windows AD Basics

- Managed users, groups, and machines in a simulated corporate environment
- Created and organized Organizational Units for departments such as Sales, Marketing, and IT
- Delegated control of specific OUs to lower-level administrators
- Configured Group Policy Objects to enforce security policies and baseline configurations
- Implemented Kerberos authentication and understood NetNTLM legacy support
- Explored multi-domain environments, trees, forests, and trust relationships
- Applied real-world scenarios to control access between different branches of a company

SearchLight IMINT/GEOINT

- Analyzed images for contextual clues such as street signs, vehicle types, architectural styles, and natural features
- Used reverse image searches and Google dorking techniques to pinpoint locations
- Evaluated environmental characteristics like road types, vegetation, and infrastructure
- Solved multiple challenges requiring geolocation and context-based problem-solving
- Learned to use methodology frameworks to systematically analyze images

Sakura OSINT Room

- Conducted passive reconnaissance to gather digital evidence without interacting directly with targets

- Traced attacker activity using usernames across social media and professional platforms
- Analyzed metadata and extracted hidden information from images left behind by attackers
- Explored cryptocurrency transactions to identify wallets, mining pools, and exchanged tokens
- Investigated edited or deleted content using archival and caching tools
- Documented findings in a structured investigative workflow

Accomplishments

- **Active Directory Mastery:** Successfully organized users, machines, and departments into OUs, delegated administrative privileges, and implemented GPOs to enforce security standards across a multi-domain environment.
- **Advanced Image Geolocation:** Solved multiple SearchLight IMINT challenges by accurately geolocating images using visual intelligence techniques.
- **OSINT Investigation Success:** Identified cybercriminal digital footprints, tracked cryptocurrency wallets, and retrieved previously deleted content to reconstruct investigative evidence.
- **Real-World Workflow Application:** Applied structured investigative methodologies to simulate corporate cybersecurity incident responses.
- **Enhanced Analytical Skills:** Developed the ability to analyze incomplete, complex, and sometimes misleading data to reach accurate conclusions.
- **Ethical Cybersecurity Practices:** Gained experience in passive investigation techniques, respecting privacy and operational security while collecting actionable intelligence.

Skills Learned

During the internship, I acquired and strengthened a wide range of technical skills spanning network administration, investigative analysis, and intelligence techniques. Key technical skills include:

1. Windows Active Directory Skills

- **User and Group Management:** Creating, modifying, and deleting user accounts and security groups.
- **Organizational Unit (OU) Management:** Structuring OUs according to departments, delegating administrative permissions, and protecting against accidental deletion.
- **Group Policy Objects (GPO):** Configuring policies for users and computers, enforcing security baselines, and applying domain-wide settings.

- Authentication Protocols: Understanding and working with Kerberos and NetNTLM authentication methods.
- Domain Architecture: Implementing multi-domain trees, forests, and trust relationships for complex network structures.
- Security Administration: Assigning domain-level privileges, managing Domain Admins, Server Operators, and Enterprise Admins groups.

2. SearchLight IMINT/GEOINT Skills

- Image Analysis: Identifying contextual, foreground, and background clues in images.
- Geolocation Techniques: Using landmarks, architecture, road types, vegetation, and vehicle characteristics to locate images.
- Tools & Methodologies: Reverse image search, Google Dorking, and visual intelligence workflows to extract actionable information.
- Critical Thinking: Evaluating incomplete or ambiguous data to make accurate conclusions about locations and environments.

3. Sakura OSINT Investigation Skills

- Digital Footprint Tracking: Tracing usernames across platforms and identifying linked social media accounts.
- Metadata Analysis: Extracting creation dates, software used, geotags, and other hidden information from files and images.
- Cryptocurrency Investigation: Analyzing wallets, mining pools, and transaction histories for evidence of activity.
- Investigation Techniques: Using archived pages, edit histories, and passive OSINT methods to retrieve deleted or altered content.
- Reporting & Documentation: Structuring findings in a coherent investigative workflow suitable for real-world scenarios.

Challenges Faced

- Handling complex Active Directory structures with multiple domains and trust relationships
- Extracting actionable intelligence from images lacking explicit context
- Managing OSINT investigations while avoiding false positives
- Tracking digital evidence across multiple platforms and verifying its authenticity

Conclusion

This internship provided a comprehensive understanding of cybersecurity administration, image intelligence, and OSINT investigations. The experience demonstrated the importance of combining technical expertise with analytical reasoning to solve real-world challenges.

I gained practical knowledge of Active Directory management, geolocation, and investigative OSINT techniques, preparing me for professional roles in cybersecurity and digital intelligence.

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.