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 6

OHsint , Shodan and Google Dorking

Internship Report Submitted By:
Vikash Upadhyay

Table of Contents

Executive Summary

This internship module focused on information gathering techniques through OSINT (Open Source Intelligence), Shodan, and Google Dorking. The OhSINT topic taught how to extract detailed personal and network-related information from a single image file. Shodan introduced techniques for discovering and analyzing publicly accessible devices on the internet, including vulnerabilities and services. Google Dorking explored advanced search queries to locate specific publicly available data efficiently. Collectively, these skills enhance reconnaissance capabilities in penetration testing and cybersecurity assessments.

Introduction

Reconnaissance is the first and one of the most critical phases in cybersecurity and penetration testing. It involves gathering as much information as possible about a target system, network, or individual before any active engagement. The quality of reconnaissance directly impacts the effectiveness of subsequent security testing or defense planning.

During this internship module, I focused on three main reconnaissance techniques: OhSINT, Shodan, and Google Dorking. These techniques fall under the broader category of OSINT (Open Source Intelligence), which is the practice of collecting information from publicly available sources.

1. **OhSINT (Open Source Intelligence on Images):**

   OhSINT focuses on analyzing digital images to extract hidden or public information about individuals, locations, or devices. Even a single image can reveal metadata, geolocation, connected networks, and sometimes personal identifiers such as email addresses. This skill is essential for digital investigations and social engineering assessments.

2. **Shodan:**

   Shodan is a specialized search engine for discovering internet-connected devices, often called the “Google for IoT.” Unlike traditional search engines, Shodan indexes services, banners, ports, and vulnerabilities of devices exposed to the internet. It is extremely useful in penetration testing to identify network weaknesses, insecure IoT devices, and potential entry points into an organization’s infrastructure.

3. **Google Dorking:**

   Google Dorking leverages advanced search operators to locate sensitive or hidden information on publicly available websites. By refining search queries, it is possible to discover exposed files, directories, documents, and other data that might not be immediately visible through regular browsing. This technique emphasizes the power of search engines in cybersecurity research and intelligence gathering.

This module provided hands-on experience using these tools and techniques in a controlled environment, emphasizing both ethical considerations and practical application. Learning to extract, interpret, and correlate information from multiple sources is a critical skill for cybersecurity professionals, whether for penetration testing, threat intelligence, or digital forensics.

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

OhSINT – Image-Based Reconnaissance

- Extracted information from a single image file.
- Techniques included metadata analysis and OSINT tools to infer personal information from images.

Shodan – Device & Network Reconnaissance

- Used IP addresses obtained via ping to search Shodan for connected services.
- Explored Autonomous System Numbers (ASN) to discover devices across IP ranges.
- Performed targeted searches using Shodan filters, e.g., vuln:ms17-010 to identify Eternal Blue vulnerabilities.
- Analyzed banners to identify services, ports, operating systems, and geographical information.
- Explored Shodan Monitor and Chrome extension to track devices and assess security exposure.

Google Dorking – Advanced Search Queries

- Used Google operators to refine search results, focusing on publicly available sensitive information.
- Key operators included:
  - site: – Limit search to a specific domain.
  - filetype: – Search for specific file extensions like PDF.
  - intitle: – Ensure keywords appear in the title.
  - cache: – Access cached versions of web pages.
- Learned to combine operators to locate data efficiently while staying within legal boundaries.

Accomplishments

- Extracted detailed personal and network data from a single image file.
- Identified services, devices, vulnerabilities, and network details using Shodan.
- Gained mastery in using advanced Google search operators for reconnaissance.
- Learned to correlate data from multiple sources to build a detailed profile of a target.

Skills Learned

Technical Skills

- OSINT data extraction from images
- Shodan searches and analysis (ASN, banners, vulnerabilities)
- Google Dorking for advanced information retrieval
- Using developer tools to inspect web content

Conceptual Skills

- Ethical considerations in reconnaissance
- Effective use of search engines and online platforms for cybersecurity
- Correlating multi-source intelligence to form actionable insights

Challenges Faced

- Understanding metadata and hidden information in images during OhSINT.
- Learning Shodan query syntax and interpreting results accurately.
- Combining Google Dorking operators efficiently to filter irrelevant data.
- Ensuring ethical and legal compliance while gathering intelligence.

Conclusion

The internship provided hands-on experience with three crucial reconnaissance methods: OhSINT, Shodan, and Google Dorking. By mastering these techniques, I can efficiently gather intelligence about individuals, networks, and systems for cybersecurity assessments while adhering to ethical and legal standards. These skills form a solid foundation for advanced penetration testing and cyber defense operations.

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.