2. Reconnaissance Practice – Detailed Documentation

Overview

The Reconnaissance Practice task focused on gathering publicly available information (OSINT) about target assets using tools such as **Maltego**, **Shodan**, and documentation platforms like **Google Docs**. The purpose of this phase was to identify external exposure, map the target's digital footprint, and understand the structure of its online presence before proceeding with deeper security testing. Reconnaissance is a crucial first step in any VAPT engagement, as it allows analysts to identify domains, subdomains, technologies, and exposed services without direct interaction that could trigger detection. The objective of this task was to perform structured reconnaissance, log findings in a repeatable format, and organize results using templates that help maintain clarity and auditability.

Activities Performed

1. OSINT Using Maltego

Maltego was used to visually map relationships between domains, subdomains, email addresses, IPs, and related infrastructure. By running standard transforms on the target domain, the tool generated a graph representation revealing potential development subdomains, linked hosting providers, and DNS associations. This helped create a clear hierarchical understanding of the target's online footprint. Maltego's ability to correlate publicly available data is particularly useful for identifying lesser-known assets that may not appear in surface-level scans.

2. Internet-Wide Search Using Shodan

Shodan was leveraged to identify **exposed services** and externally facing assets. By querying the target's IP addresses or domain, Shodan revealed open ports, running services, and version details, such as SSH, HTTP, FTP, or database services that might be publicly reachable. This enabled early detection of high-risk exposure before performing any active scanning. The findings were documented in a structured log to maintain chronological traceability.

Asset Mapping Log

All findings were logged chronologically to provide a clear audit trail for team communication:

Timestamp	Tool	Finding
2025-12-09 10:00:00	Shodan	Exposed SSH on 192.168.0.106
2025-12-09 10:30:00	Maltego	Subdomain discovered: dev.example.com
2025-12-09 11:00:00	Shodan	HTTP server with outdated Apache version
2025-12-09 11:30:00	Maltego	Identified associated mail server
2025-12-09 12:00:00	Manual	Tech stack mapped (PHP, Apache)

This format is optimized for quick posting in Slack or internal channels during collaborative engagements.

Conclusion

Through the Vulnerability Scanning Lab, we successfully used Nmap, Nikto, and OpenVAS to enumerate, detect, and prioritize vulnerabilities on multiple hosts. The evidence in our lab report confirms accurate service detection, web flaw identification, and structured risk scoring. The ability to track vulnerabilities in tables, assign CVSS scores, prepare documentation, and escalate findings.

Document Information:

Report Generated: December 12, 2025
Author: Soumendu Manna - CyArt VAPT Intern