Recon_Notes

Reconnaissance Overview

The reconnaissance phase focused on gathering publicly available information about the target environment before performing active scanning or exploitation.

Target Information

The target consisted of test domains and intentionally vulnerable lab systems designed for security learning purposes.

Tools Used for Reconnaissance

- Shodan
- Maltego
- WHOIS
- Sublist3r
- Wappalyzer

Reconnaissance Steps & Commands

1. WHOIS Lookup

whois example.com

This command was used to gather domain registration details such as registrar name, creation date, and ownership information. This helps understand who controls the domain and possible administrative contacts.

2. DNS Resolution

nslookup example.com

Used to resolve the domain name into IPv4 and IPv6 addresses. This helps identify backend infrastructure and hosting providers.

3. Subdomain Enumeration

sublist3r -d example.com

Sublist3r was used to enumerate publicly available subdomains using search engines, SSL certificates, and passive DNS sources. Identified subdomains expand the attack surface.

4. OSINT Graph Mapping

Maltego was used to visually map relationships between the domain, subdomains, IP addresses, and DNS records. Graph-based OSINT helps correlate assets and identify infrastructure dependencies that may not be obvious in text-based results.

Key Findings

- Primary domain resolved to Cloudflare IP addresses
- Multiple subdomains identified (dev, support, mobile)
- CDN protection detected

Reconnaissance Activity Log

Timestamp	Tool	Activity Performed	Finding
2026-01-06 10:00:00	WHOIS	Domain ownership lookup	Domain registered via test registrar
2026-01-06 10:10:00	Shodan	Service exposure search	HTTP service detected on port 80
2026-01-06 10:25:00	Maltego	Domain to DNS enumeration	Multiple DNS entities identified
2026-01-06 10:40:00	Sublist3r	Subdomain enumeration	7 subdomains discovered
2026-01-06 10:55:00	Wappalyzer	Technology stack identification	CDN and web server detected

Reconnaissance Summary

The reconnaissance phase identified the target's domain infrastructure, resolved IP addresses, and multiple subdomains using OSINT tools. Passive techniques revealed hosting details and CDN usage, expanding the overall attack surface and providing inputs for further scanning and exploitation phases.