Activity 2: Reconnaissance Practice

Objective

Perform Open Source Intelligence (OSINT) gathering and map the target's attack surface using passive and active reconnaissance techniques.

Tools Used

- Maltego: Visual link analysis and data mining
- Shodan: Internet-connected device search engine
- Sublist3r: Subdomain enumeration tool
- Wappalyzer: Technology stack identification
- WHOIS: Domain registration information
- Google Docs: Documentation and collaboration

Reconnaissance Methodology

Reconnaissance Types

1. **Passive Reconnaissance:** Gathering information without directly interacting with target
2. **Active Reconnaissance:** Direct interaction with target systems (requires authorization)

PTES Reconnaissance Phases

1. Information Gathering
2. Target Identification
3. Service Enumeration
4. Service Fingerprinting
5. Asset Mapping

Workflow Steps

Step 1: Domain Information Gathering (WHOIS)

1.1 WHOIS Lookup

Cmd Whois example.com

1.2 Google Docs Template - Domain Info

Target Domain: example.com

Assessment Date: January 28, 2026

Analyst: VAPT Team

1. DOMAIN REGISTRATION
   - Registrar: GoDaddy LLC
   - Registration Date: 2010-03-15
   - Expiration Date: 2027-03-15
   - Last Updated: 2025-11-20
   - Status: clientTransferProhibited

2. NAME SERVERS
   - ns1.example.com (192.168.1.10)
   - ns2.example.com (192.168.1.11)
   - ns3.example.com (192.168.1.12)

3. ADMINISTRATIVE CONTACTS
   - Organization: Example Corp
   - Email: admin@example.com (privacy protected)
   - Phone: +1-555-0100 (privacy protected)

4. DNSSEC STATUS
   - DNSSEC: Enabled
   - DS Records: Present

5. HISTORICAL RECORDS
   - Previous registrar: Network Solutions
   - Transfer date: 2015-06-10

Step 2: Subdomain Enumeration

2.1 Using Sublist3r

```
sublist3r -d example.com
```

```
 ____        _     _ _     _   _____
/ ___| _   _| |__ | (_)___| |_|___ / _ __
\___ \| | | | '_ \| | / __| __| |_ \| '__|
 ___) | |_| | |_) | | \__ \ |_ ___) | |
|____/ \__,_|_.__/|_|_|___/\__|____/|_|
              # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for example.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] DNSDumpster module failed: Could not find CSRF token on DNSDumpster page
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 7
AS207960 Test Intermediate - example.com
www.example.com
dev.example.com
m.example.com
products.example.com
support.example.com
m.testexample.com
```

2.2 Subdomain Documentation

Subdomain	IP Address	Purpose	Technologies	Risk Level
www.example.com	192.168.1.20	Main website	Apache, PHP	Medium
dev.example.com	192.168.1.50	Development	Nginx, Node.js	High
api.example.com	192.168.1.30	API endpoint	Express.js	Critical
admin.example.com	192.168.1.40	Admin panel	WordPress	Critical

Web Interface Queries

https://www.shodan.io/

Search examples:

- hostname:example.com
- ssl.cert.subject.cn:example.com
- org:"Example Corp"
- net:192.168.1.0/24 port:80

3 Asset Mapping Log (Slack-friendly format)

```
Timestamp           | Tool      | Finding
--------------------|-----------|----------------------------------
2026-01-28 10:00:00 | Shodan    | Exposed SSH on 192.168.1.50
2026-01-28 10:15:00 | Shodan    | Open RDP port 3389 on 192.168.1.60
2026-01-28 10:30:00 | Shodan    | Elasticsearch on 192.168.1.70:9200
2026-01-28 10:45:00 | Shodan    | MongoDB on 192.168.1.80:27017
2026-01-28 11:00:00 | Shodan    | Webcam interface on 192.168.1.90
```

4: Technology Stack Identification

4.1 Using Wappalyzer (Browser Extension)

1. Install Wappalyzer extension for Chrome/Firefox
2. Visit target website
3. Click Wappalyzer icon
4. Review detected technologies
5. Export results

4.2 Technologies to Identify

- **Web Server:** Apache, Nginx, IIS, Tomcat
- **Programming Language:** PHP, Python, Node.js, Ruby, Java
- **Framework:** Laravel, Django, Express, Rails, Spring
- **CMS:** WordPress, Drupal, Joomla
- **JavaScript Libraries:** jQuery, React, Angular, Vue.js
- **Analytics:** Google Analytics, Matomo
- **CDN:** Cloudflare, Akamai, AWS CloudFront
- **Security:** ModSecurity, Wordfence, Sucuri

4.3: Visual Asset Mapping with Maltego

4.4 Create New Investigation

1. File → New Graph
2. Name: "Example.com Reconnaissance"
3. Add domain entity: Drag "Domain" to canvas
4. Enter: example.com

Transform Execution

Run these transforms sequentially:

1. **To DNS Name - NS (Name Server)**
   - Right-click domain → DNS → To DNS Name - NS
   - Identifies authoritative name servers
2. **To DNS Name - MX (Mail Exchanger)**
   - Right-click domain → DNS → To DNS Name - MX
   - Identifies mail servers
3. **To IP Address**
   - Right-click domain → DNS → To IP Address
   - Resolves domain to IP
4. **To Website**
   - Right-click domain → To Website
   - Identifies associated websites
5. **To Email Address**
   - Right-click domain → To Email Address
   - Finds email addresses (from public sources)
6. **To Person**
   - Right-click email → To Person
   - Identifies personnel

4.5 Maltego Graph Analysis

Document relationships found:

example.com

```
├── Name Servers
│   ├── ns1.example.com → 192.168.1.10
│   ├── ns2.example.com → 192.168.1.11
│   └── ns3.example.com → 192.168.1.12
├── Mail Servers
│   ├── mail1.example.com → 192.168.1.15
│   └── mail2.example.com → 192.168.1.16
├── Subdomains
│   ├── www.example.com → 192.168.1.20
│   ├── dev.example.com → 192.168.1.50
│   ├── api.example.com → 192.168.1.30
│   └── admin.example.com → 192.168.1.40
├── Email Addresses
│   ├── admin@example.com → John Doe (IT Manager)
│   ├── support@example.com → Sarah Smith (Support Lead)
│   └── security@example.com → Mike Johnson (CISO)
└── Technologies
    ├── Cloudflare CDN
    ├── AWS Hosting
    └── WordPress CMS
```

5: Documentation and Logging

5.1 Comprehensive Reconnaissance Template (Google Docs)

Target Organization: Example Corp

Primary Domain: example.com

Assessment Period: January 28, 2026

Analyst: VAPT Team

EXECUTIVE SUMMARY

Comprehensive OSINT assessment conducted on Example Corp infrastructure. Identified 12 subdomains, 8 exposed services, and multiple outdated technologies presenting potential attack vectors.

1. DOMAIN INFORMATION

Domain: example.com

Registrar: GoDaddy LLC

Registration: 2010-03-15

Expiration: 2027-03-15

DNSSEC: Enabled

Name Servers:

- ns1.example.com (192.168.1.10)
- ns2.example.com (192.168.1.11)
- ns3.example.com (192.168.1.12)

2. SUBDOMAINS DISCOVERED

Total Identified: 12

Critical Risk Subdomains:

- dev.example.com (Development environment - publicly accessible)
- admin.example.com (Admin panel - weak authentication detected)
- api.example.com (API endpoint - no rate limiting)

Medium Risk Subdomains:

- www.example.com (Main site)
- mail.example.com (Webmail interface)
- vpn.example.com (VPN portal)

Low Risk Subdomains:

- blog.example.com
- support.example.com
- cdn.example.com

3. EXPOSED SERVICES (SHODAN FINDINGS)

Timestamp: 2026-01-28 10:00:00

Tool: Shodan

Critical Findings:

- SSH on 192.168.1.50:22 (dev.example.com) - Password auth enabled
- RDP on 192.168.1.60:3389 - Weak encryption detected
- Elasticsearch on 192.168.1.70:9200 - No authentication

- MongoDB on 192.168.1.80:27017 - Default configuration

Medium Findings:

- Apache Tomcat on 192.168.1.100:8080
- MySQL on 192.168.1.110:3306 - Accessible from internet

4. TECHNOLOGY STACK

Web Server: Apache 2.4.41 (Ubuntu)

Programming: PHP 7.4.3, Node.js 14.17.0

CMS: WordPress 6.1.1

Database: MySQL 8.0.28

CDN: Cloudflare

Hosting: AWS us-east-1

Identified Vulnerabilities:

- WordPress plugins outdated (3 critical updates pending)
- PHP version approaching EOL
- Missing security headers (CSP, HSTS)

5. PERSONNEL IDENTIFIED

Through email enumeration and LinkedIn:

- John Doe - IT Manager (admin@example.com)
- Sarah Smith - Support Lead (support@example.com)

- Mike Johnson - CISO (security@example.com)

- 15+ developers identified via GitHub

6. ATTACK SURFACE SUMMARY

Total Assets Identified: 45

- 12 Subdomains

- 18 IP Addresses

- 8 Exposed Services

- 7 Email Addresses

High Priority Targets:

1. dev.example.com - Exposed development environment

2. admin.example.com - Weak admin panel

3. 192.168.1.70 - Unauthenticated Elasticsearch

4. 192.168.1.80 - Open MongoDB instance

RECOMMENDATIONS

1. Immediately secure exposed databases (Elasticsearch, MongoDB)

2. Implement VPN for development environment access

3. Update all WordPress plugins

4. Enable security headers on all web properties

5. Review and restrict SSH/RDP access

6. Implement network segmentation

APPENDICES

A. Complete subdomain list

B. Shodan search results

C. Maltego relationship graph

D. Technology stack details

E. Raw tool outputs

5.2 Timestamp Logging Format

For all findings, use this CSV format:

```
Timestamp,Tool,Finding,IP Address,Port,Severity
2026-01-28 10:00:00,Shodan,Exposed SSH,192.168.1.50,22,High
2026-01-28 10:15:00,Shodan,Open RDP,192.168.1.60,3389,Critical
2026-01-28 10:30:00,Maltego,Subdomain: dev.example.com,192.168.1.50,N/A,Medium
2026-01-28 10:45:00,Sublist3r,Subdomain: api.example.com,192.168.1.30,N/A,High
2026-01-28 11:00:00,Wappalyzer,WordPress 6.1.1,192.168.1.20,80,Low
2026-01-28 11:15:00,Shodan,Elasticsearch,192.168.1.70,9200,Critical
```

8 Word Reconnaissance Summary

Reconnaissance of example.com revealed 12 subdomains with critical exposures: unauthenticated Elasticsearch, publicly accessible MongoDB, and weak SSH configuration on development server. WordPress installation requires updates.

Attack surface includes 45 assets across 18 IP addresses. Immediate database hardening and development environment isolation recommended. Technology stack: Apache, PHP, WordPress, MySQL on AWS infrastructure.