RECONNAISSANCE & INFO GATHERING

📘 MODULE 2 — RECONNAISSANCE & INFORMATION GATHERING

Official Xsploit Hackademy Coursebook Chapter

🧭 CHAPTER OUTLINE

18. Recon Lab Exercises

⭐ 1. Introduction to Reconnaissance

Reconnaissance (recon) is the **first and most important stage** of any penetration test.

> "Your exploitation is only as powerful as your reconnaissance."

In recon, you learn:

- how the target works
- what technologies it uses
- what assets exist
- what is exposed
- potential attack surfaces
- vulnerabilities without touching the main application

Recon is divided into:

✔ Passive Recon (No direct interaction)

— Safe, stealthy, no logs generated

— Performed via:

- search engines
- public records
- certificates
- metadata
- OSINT tools

✔ Active Recon (Direct interaction)

— The target server sees your requests

— Includes:

- directory enumeration
- port scanning

- banner grabbing
- technology probing

⭐ 2. Passive Reconnaissance (Deep Theory)

Passive recon is **collecting information without sending packets to the target's server**.

Think of it as "researching without knocking on the door."

Benefits:

- No logs
- Almost no risk
- High signal, low noise
- Reveals forgotten or unknown assets

🌐 2.1 WHOIS Analysis

WHOIS reveals domain ownership details.

🔧 Tool:

```
whois example.com
```

📌 Information Gained:

- Registrant
- Creation/expiry dates
- Nameservers
- Registrar
- Contact email

Example Output Interpretation:

```
Domain Name: example.com
Registrar: GoDaddy
Updated Date: 2024-06-10
Name Server: ns1.server.com
```

Security Insight:

Old domains → often have forgotten subdomains.

🌐 2.2 DNS Lookup & Records

🔧 Tool:

```
dig any example.com
host example.com
nslookup example.com
```

DNS Records & Insights:

Record	Meaning	Pentest Value
A	IPv4 Address	Target IP
AAAA	IPv6 Address	Alternative path
MX	Mail Servers	Email spoofing tests
TXT	SPF/DMARC	Email security
NS	Nameservers	DNS hijack vectors
SOA	Admin details	Contact & config
CNAME	Alias	Internal host mapping
PTR	Reverse lookup	Fingerprint server

🌐 2.3 SSL/TLS Certificate OSINT

Every HTTPS website leaves behind **certificate transparency logs**.

🔧 Tools:

- https://crt.sh
- https://transparencyreport.google.com
- https://censys.io

Example crt.sh query:

```
domain:example.com
```

What you find:

- Forgotten subdomains
- Internal development portals
- Staging servers
- Legacy systems

🌐 2.4 Search Engine OSINT (Google Dorking)

Google indexes hidden paths.

Examples:

```
site:example.com ext:sql
site:example.com "password"
site:example.com intitle:"index of"
site:example.com inurl:/admin
```

What you find:

- Backup files
- Open directories
- Debug logs
- API keys
- Config files

⭐ 3. OSINT Techniques in Extreme Detail

OSINT = Open-Source Intelligence

Goal: gather maximum information without interacting with the target server.

🔎 3.1 Social Media Profiling

Targets:

- LinkedIn employees
- GitHub developers
- StackOverflow accounts
- Twitter/X engineering posts

Tools:

- Sherlock
- Holehe
- Photon
- GHunt

🔎 3.2 Metadata Extraction

Documents uploaded on websites often contain leaked metadata.

🔧 Tools:

```
exiftool file.pdf
```

Findings:

- Creator name
- Software version
- Internal machine names

- GPS (in images)

🔎 3.3 Github OSINT

Developers accidentally leak:

- API keys
- Tokens
- Internal URLs
- Passwords

Tools:

```
git-dumper https://github.com/user/repo
trufflehog
gitleaks
```

⭐ 4. Subdomain Enumeration (FULL DEEP DIVE)

Subdomains expand the attack surface.

Example:

- `api.example.com`
- `dev.example.com`
- `beta.example.com`
- `test.example.com`
- `portal.example.com`

🔽 4.1 Passive Subdomain Enumeration

Tools:

```
subfinder -d example.com
assetfinder example.com
amass enum -passive -d example.com
crt.sh
virustotal.com
```

No packets go to target → stealth.

🔽 4.2 Active Subdomain Enumeration

Sends DNS queries.

Tools:

```
amass enum -active -d example.com
dnsrecon -d example.com -t brt
```

🔽 4.3 Bruteforce Subdomain Enumeration

Tool:

```
ffuf -w subdomains.txt -u https://FUZZ.example.com
```

⭐ 5. DNS Recon (In Professional Depth)

🧩 5.1 Zone Transfer Attack

Attempt:

```
dig axfr @ns1.example.com example.com
```

If succeeds → **Critical vulnerability**.

🧩 5.2 Reverse DNS Enumerations

```
dnsrecon -r 192.168.1.0/24
```

Reveals:

- Hostnames
- Internal systems

⭐ 6. Email & Credential OSINT

📧 6.1 Harvest Email Addresses

Tools:

```
theHarvester -d example.com -b all
```

📧 6.2 Breach Lookup

Tools:

- Dehashed
- LeakCheck
- HaveIBeenPwned
- BreachDirectory

Manual test:

```
breach-parse breaches.txt
```

📧 6.3 Password Spraying

Using gathered emails:

```
hydra -L emails.txt -p Welcome@123 smtp.example.com
```

⭐ 7. Technology Fingerprinting (Detailed)

Goal: Identify:

- Backend language
- CMS
- Framework
- Web server
- Database

🔥 Tools

Wappalyzer

(Browser extension)

WhatWeb

```
whatweb https://example.com
```

Nmap scripts

```
nmap -sV --script=http-enum, http-headers, http-git example.com
```

⭐ 8. Cloud Asset Discovery

Many companies use:

- AWS
- Azure
- GCP
- Cloudflare

Tools:

```
cloud_enum --aws example.com
s3scanner
```

⭐ 9. Active Reconnaissance (Deep Practice)

🎯 9.1 Directory Enumeration

Dirsearch:

```
dirsearch -u https://example.com -e php,html,txt
```

Gobuster:

```
gobuster dir -u https://example.com -w wordlist.txt
```

ffuf:

```
ffuf -u https://example.com/FUZZ -w wordlist.txt
```

🎯 9.2 File Extension Discovery

```
gobuster dir -u example.com -x php,html,asp,txt,old,bak
```

⭐ 10. Virtual Host Discovery

```
ffuf -u http://example.com -H "Host: FUZZ.example.com" -w subdomains.t
xt
```

⭐ 11. Port Scanning Foundations

Even for web tests, port scanning matters.

```
nmap -sV -Pn -p- example.com
```

⭐ 12. Banner Grabbing

```
nc example.com 80
HEAD / HTTP/1.1
Host: example.com
```

⭐ 13. WAF Detection

Tools:

```
wafw00f https://example.com
```

⭐ 14. Reporting Recon Data

Include:

- Subdomains
- Technologies
- DNS structure
- Cloud assets
- Exposed directories
- Version numbers
- Attack surface summary

⭐ 15. Case Study Example

I will include a full case study if you want.

⭐ 16. Mistakes to Avoid

- Over-scanning
- Missing subdomains
- Skipping passive recon
- Not checking cloud assets
- Missing JS file leaks