

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كليـــة الكـــويت للعلـــــوم والتكـنولـوجيا
Private University
جامعـــــة خـاصـة

CS 440

CYBER SECURITY

LECTURE 04: RECONNAISSANCE & ATTACK LIFECYCLE

Dr. Mohamad Hoda,

Lecture Objectives



By the end of this lecture, you will be able to:

- Explain the cyber attack lifecycle
- Describe reconnaissance objectives
- Distinguish between active and passive recon
- Relate recon to later attack stages

Typical Attack Lifecycle

- **Pre-Intrusion:**
  - Reconnaissance (gather intel on target)
  - Scanning & Enumeration (map vulnerabilities and assets)
- **Intrusion:**
  - Initial Access (establish first foothold)
  - Exploitation (execute attack against vulnerability)
  - Privilege Escalation (gain higher-level permissions)
- **Post-Intrusion:**
  - Persistence (maintain access over time)
  - Covering Tracks (erase evidence of activity)

Reconnaissance



Reconnaissance is:

- Information gathering
- About the target
- Conducted *before* any exploitation

Purpose:

- To understand how the target works
- To identify possible weaknesses
- To reduce guesswork later in the attack
- **In other words:** "*Reconnaissance is about learning — not attacking yet.*" *Attackers observe, research, and map the target before making a move.*

Simple example:

- Visiting a company's website
- Checking employee roles on LinkedIn
- Identifying publicly exposed servers or services

(Better reconnaissance → more effective attacks later)

Reconnaissance Goals



During reconnaissance, attackers aim to:

- Identify systems (servers, websites, networks)
- Identify users (employees, admins, contractors)
- Identify technologies (OS, software, cloud platforms)
- Identify weaknesses (misconfigurations, outdated software)
- **In other words:** "*Attackers ask simple questions:*" *What systems exist? Who uses them? What software runs on them?*"

Types of Reconnaissance



There are two main types of reconnaissance:

- Passive reconnaissance
- Active reconnaissance

Big Picture:

- Passive recon = low risk, low visibility
- Active recon = higher risk, more detailed information
- **In other words:** *"Reconnaissance can be silent or noisy."*
  The difference is whether the target notices.

Passive Reconnaissance



Passive reconnaissance involves:

- No direct interaction with target systems
- Use of publicly available information
- Very low chance of detection.

Common sources:

- Company websites.
- Social media platforms
- Public documents (PDFs, job postings, reports)
- In other words: *"Passive recon does not touch the target system directly."*
  It is usually legal and very difficult to detect.

Active Reconnaissance



Active reconnaissance involves:

- Direct interaction with target systems
- Sending packets to the target
- Higher chance of detection

Common techniques:

- Network scanning
- DNS queries
- Service enumeration
- **In other words:** "Active recon involves touching the target."

  This is where attackers start leaving traces.

Reconnaissance in Practice



Through reconnaissance, attackers may discover:

- Open ports
- Running services
- Software versions
- Usernames

What this enables:

- Identifies entry points
- Reveals outdated or misconfigured systems
- Narrows down viable attack paths
- **In other words:** "Most successful attacks begin because attackers found something they should not have been able to see."

Why Reconnaissance Matters



Reconnaissance:

- Reduces guesswork.
- Increases attack success rate.
- Guides exploitation choices

Impact:

- Helps attackers choose the easiest path.
- Avoids unnecessary noise and failed attempts
- **In other words:** "Exploitation without reconnaissance is mostly luck."

"Reconnaissance turns luck into planning."

Reconnaissance & CIA Triad



Reconnaissance impacts:

- **Confidentiality:** exposes sensitive information
- **Integrity & Availability:** sets up attacks that may alter or disrupt systems

Why it matters:

- Understanding this helps defenders prioritize monitoring of information leaks
- Shows how recon connects to the broader security context
- **In other words:** "Reconnaissance itself may not damage systems, but it prepares attacks that will."

How Defenders See Recon



Reconnaissance can be detected through:

- System and network **logs**
- Security **alerts**
- **Anomalous traffic** patterns
- **IDS/IPS** warnings

Why it matters:

- Early detection can prevent exploitation
- Even small recon activity can reveal attacker intent
- **In other words:** "Everything attackers do can be seen — if defenses are in place."

"Reconnaissance is often the first detectable sign of an attack."

While Performing the test, Ask Yourself



Questions to guide you:

- What information did I discover?
- Why is this information useful?
- How could defenders detect this?

Focus:

- Observation and analysis
- Thinking like both attacker and defender
- **In other words:** "The goal is not to run commands — it's to interpret results."

Detection Indicators

Reconnaissance can be spotted through:

- Repeated connection attempts
- Port scans
- Unusual DNS queries

Why it matters:

- Early detection allows defenders to block or mitigate attacks
- Small anomalies often indicate a larger attack plan
- **In other words:** "Blue Teams spend a lot of time identifying reconnaissance activity before damage occurs."

Example 1: Passive Recon – Website & Metadata



Command:

curl -I http://target

- Passive
- No scanning
- Information leakage
- **In other words:** "This does not attack anything. We're just asking the web server for basic information."

Example 2: Passive Recon – Public DNS Information



Command:

nslookup target

Or

dig target

- Passive
- Naming reveals structure
- **In other words:** "DNS alone can tell attackers where systems live and how infrastructure is organized."

Example 3: Passive Recon – robots.txt



Command:

curl http://target/robots.txt

- Passive
- Human mistakes create exposure
- **In other words:** "This file is meant for search engines, but attackers read it too. Sometimes it literally lists sensitive directories."

Example 4: Active Recon – Host Discovery



Command:

nmap -sn 192.168.1.0/24

- Active
- Detectable
- First network interaction
- **In other words:** "Now we're touching the network. We're asking: who is alive? This already creates logs."

Example 5: Active Recon – Port Scanning



Command:

nmap target

- Active
- High signal for defenders
- **In other words:** "Each open port is a possible door. Reconnaissance tells attackers which doors exist — not which ones are unlocked yet."

Example 6: Active Recon – Service & Version Detection



Command:

Nmap -sV target

- Direct link to exploitation
- Recon → attack planning
- **In other words:** "This is where recon becomes dangerous. Knowing versions allows attackers to search for exact exploits."

Example 7: Blue Team Perspective



Command:

Nmap -p 22,80,443 target

- Defender visibility
- Early detection opportunity
- **In other words:** "If I'm a defender, I will see this in my logs. Recon is often the first warning sign before a real attack."
- **Final Thoughts:** "None of these commands break anything.
  But every serious cyber attack starts with commands like these."

Questions???