Web and Mobile Application Security

Chapter 1 — Vulnerabilities and Attack Methods

Mr Laïdi FOUGHALI

l.foughali@univ-skikda.dz

(Website ⇒ www.al-moualime.com)

University of Skikda — Computer Science Department

2nd Year Master in Information Security (IS)

Academic Year 2026-2027

Updated on 2026-09-22 at 23:40:52

Outline

Chapter objectives

By the end of this chapter, you will be able to

- Identify categories of attackers and their motivations
- Describe the organization of offensive and defensive teams
- Master the phases of an intrusion
- Understand the concept of vulnerability and "zero-day" flaws
- Distinguish the major families of attacks: malicious code, social engineering, application attacks

1.1 — Different types of hackers

A classification by intent and legality

The term "hacker" originally denotes an expert capable of repurposing a system beyond its intended use. In security, actors are classified according to their **intent** and the **legality** of their actions.

The three fundamental profiles

- **Black hat** : a malicious attacker acting without authorization, for financial gain, sabotage, or data theft
- **White hat** : a security professional (pentester, researcher) acting legally and with authorization
- **Grey hat** : an intermediate actor who discovers flaws without authorization but without clearly malicious intent

Examples: Kevin Mitnick (black hat turned consultant) – Anonymous (hacktivists) – Lazarus Group (APT, 2014 Sony Pictures hack).

1.1 — Different types of hackers (continued)

Other profiles to know

- **Script kiddies** : poorly skilled individuals reusing existing tools and exploits without understanding how they work
- **Hacktivists** : groups motivated by a political or ideological cause (defacement, leaks, DDoS)
- **Organized cybercriminals** : professional structures seeking financial profit (ransomware, fraud, data resale)
- **Insider threats** : employees or contractors abusing legitimate access
- **State-sponsored groups / APTs** : actors backed by nation-states, with significant resources, aiming at long-term espionage or sabotage

1.2 — Organization and goals of hacker teams

Three specialized teams

- **Red team** : simulates a real attacker to test an organization's resilience
- **Blue team** : defends, detects, and responds to incidents (SOC, monitoring, hardening)
- **Purple team** : coordinates red and blue to continuously improve detection and defense

Goals of offensive groups

Financial gain (extortion, fraud), industrial or state espionage, ideological statement, or reputation-seeking. Structured groups divide roles (reconnaissance, tool development, exploitation, monetization) much like a business.

1.3 — The phases of an intrusion

An intrusion generally follows a sequence of steps, formalized by models such as the **Cyber Kill Chain** or the **MITRE ATT&CK** framework.

Typical steps

1. **Reconnaissance** — passive and active information gathering about the target (OSINT, subdomain enumeration, open ports)
2. **Scanning and enumeration** — mapping services, versions, and exposed accounts
3. **Initial access / exploitation** — exploiting a vulnerability or credentials to gain a first foothold
4. **Privilege escalation** — obtaining higher-level rights (administrator, root)
5. **Persistence** — maintaining access (backdoors, scheduled tasks)
6. **Lateral movement and exfiltration** — moving through the network and stealing data
7. **Covering tracks** — deleting logs to evade detection

1.4 — Analyzing vulnerabilities and zero-day flaws

What is a vulnerability?

A **vulnerability** is a weakness in a system that can be exploited to compromise confidentiality, integrity, or availability.

- Known vulnerabilities are referenced by **CVE** identifiers and rated by a **CVSS** severity score
- Scanners (Nessus, OpenVAS, etc.) automate their detection

The "zero-day" flaw

A vulnerability unknown to the vendor, for which **no patch yet exists**. The "exposure window" — between discovery by the attacker and the release of a patch — leaves systems with no protection. These flaws are traded on a parallel market at high prices.

Example: CVE-2021-44228 (Log4Shell) – critical CVSS 10/10 flaw in the Log4j library (2021).

1.5 — Malicious code attacks

Malware families differ by propagation and payload

- **Virus** : code that attaches to a host program and spreads when it is executed
- **Worm** : spreads by itself across the network, with no host
- **Trojan horse** : a program that appears legitimate while concealing a malicious function
- **Ransomware** : encrypts the victim's data and demands a ransom
- **Spyware** : covertly collects information
- **Rootkit** : hides deep within the system to maintain stealthy access
- **Botnet** : a network of compromised machines remotely controlled (DDoS, spam)

Examples: WannaCry (ransomware + worm, 2017, exploits EternalBlue) – Mirai (IoT botnet, 2016).

1.6 — Social engineering attacks

Manipulating people rather than technology

Social engineering remains one of the most effective intrusion vectors.

- **Phishing** : fraudulent emails or websites impersonating a trusted entity
- **Spear phishing / whaling** : targeted phishing aimed at a specific person or an executive
- **Pretexting** : a fabricated scenario to obtain information
- **Baiting** : a booby-trapped device (an abandoned USB drive) exploiting curiosity
- **Vishing / smishing** : variants by phone or SMS

Defense

Relies mainly on awareness training, verification procedures, and strong authentication.

Example: the Twitter hack (July 2020) – employee accounts compromised via vishing, no technical flaw involved.

1.7 — Application attacks

Targeting the software itself

- Injections (SQL, commands)
- Buffer overflows
- Business logic attacks
- Exploitation of vulnerable third-party components

Coming up in the course

Attacks specific to **Web** applications are covered in **Chapter 3**, and those targeting **mobile** applications in **Chapter 8**.

Key takeaways

The essentials of this chapter

- Attackers are classified by intent (black/white/grey hat, hacktivists, APTs) and organize into teams (red, blue, purple)
- An intrusion follows phases: reconnaissance, exploitation, privilege escalation, persistence, exfiltration, covering tracks
- A zero-day flaw is unknown to the vendor and unpatched; its exposure window makes it critical
- Malicious code and social engineering are two major vectors, often combined

Questions and exercises

To practice

1. Compare the red team, blue team, and purple team, specifying the role and objective of each.
2. Explain why a zero-day vulnerability is more dangerous than a known vulnerability.
3. Give three social engineering techniques and one countermeasure appropriate to each.
4. Place the phases of an intrusion on a timeline and associate each with an example tool or technique.

Chapter sources

- Official module syllabus (UEF322, chapter 1)
- Publicly documented incidents: WannaCry, Log4Shell (CVE-2021-44228), the Twitter hack (July 2020)