PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
Ministry of Higher Education and Scientific Research
University of Skikda — Department of Computer Science
Master's in Information Security — Semester 3 (M2) — UEF322
Web and Mobile Application Security
Updated on 2026-09-23 at 06:36:05

Lab 1 — Reconnaissance and Enumeration

Background

This lab extends section 1.3 of the course ("Intrusion phases"). Before exploiting any flaw at all, an attacker – or a legitimate pentester – always starts by **mapping the target**: which services are running, on which ports, with which versions, and what information is publicly available about it. This step does not "break" anything: it only observes what is already exposed. That is exactly why it is often neglected by defensive teams, even though it gives the attacker most of their roadmap. By practicing it yourself, you will understand why section 1.4 (vulnerabilities and CVEs) stresses the direct link between an *exposed software version* and an *exploitable attack surface*.

Objective

Reproduce, in an authorized environment, the first two phases of the Cyber Kill Chain (section 1.3 of the course handbook).

Prerequisites

Have studied chapter 1: types of hackers, intrusion phases, the concept of vulnerability and CVE/CVSS.

Tools and installation

On Linux (Ubuntu/Debian or Kali, already included in most lab VMs):

```
sudo apt update
sudo apt install -y nmap whois theharvester
```

On Windows, install Nmap from `https://nmap.org/download.html` (`whois` is not bundled: use the online `whois` lookup at `https://www.whois.com` instead); `theHarvester` requires Python 3 and installs with `pip install theHarvester`.

- `nmap` (port and service scanner)
- `whois` (domain registry lookup)
- `theHarvester` (OSINT collection)
- A Web browser

Authorized target

`scanme.nmap.org` is a host explicitly made available by the `nmap` authors for scanning practice. It is the only target to use for this lab – **never scan a target without prior written authorization** (chapter 1, ethical framework).

Procedure

1. **Identify the domain owner.** Run:

   ```
   whois nmap.org
   ```

   Note the owning organization and the domain's registration information (`whois` queries the registered domain `nmap.org`, not the `scanme` subdomain, which has no entry of its own).

2. **Map ports and services.** Run:

   ```
   nmap -sV -p- scanme.nmap.org
   ```

   This command scans all 65,535 ports (`-p-`) and attempts to identify the service version behind each open port (`-sV`). Record each open port and its associated service.

3. **OSINT collection.** Run:

   ```
   theHarvester -d nmap.org -b crtsh,duckduckgo
   ```

   Record the email addresses and subdomains publicly associated with the parent domain.

4. **Search for known vulnerabilities.** For each service identified in step 2, check whether a published CVE matches its exact version, using `https://www.cve.org` or the local `searchsploit` tool. Note the CVSS score of any CVE found (see chapter 1, section 1.4).

Comprehension questions

1. Which phase(s) of the Cyber Kill Chain (chapter 1, section 1.3) correspond to steps 2 and 3 of this lab, respectively?
2. An open port is not in itself a vulnerability. What, in the information gathered, turns an exposed service into a concrete risk?
3. Why do automated scanners (Nessus, OpenVAS, chapter 1 section 1.4) systematically perform an enumeration step before testing exploits?

Deliverable

A one-page report containing:

- the list of ports/services discovered in step 2;
- the OSINT information collected in step 3;
- for each service, a risk-level assessment (low/medium/high), justified by the CVEs found in step 4.