Lab 2: Network Scanning & Enumeration – Python Nmap Port Scanner

---

Course: FSCT 8561 – Security Applications
Instructor: Dr. Maryam R. Aliabadi
Lab Duration: 3 Hours

Overview

This lab builds on the Python networking fundamentals introduced in previous labs. Students will use the Python Nmap library to perform basic network scanning and port enumeration. The focus is on understanding how scanners work, how results are interpreted programmatically, and the security implications of network reconnaissance.

Learning Objectives

- Understand the role of network scanning and enumeration in cybersecurity
- Use the Python Nmap library to perform port scans
- Interpret scan results programmatically
- Analyze security risks revealed through open ports

Pre-requisite

Completed Lab 1

Required Reading & Tutorials

- Mastering Python for Networking and Security – **Chapter 8**
    - https://learning.oreilly.com/library/view/mastering-python-for/9781839217166/
    - Source code on: https://github.com/PacktPublishing/Mastering-Python-for-Networking-and-Security-Second-Edition
- Python-Nmap Documentation
    - https://pypi.org/project/python-nmap/
- Nmap Official Documentation
    - https://nmap.org/book/man.html

Lab Scenario

You are acting as a junior security analyst tasked with assessing a host for exposed network services. Using Python and Nmap, you will scan a target system to identify open ports and running services. All scans must be performed only on systems you own or have explicit permission to test.

Part 1 – Environment Setup

1. Ensure Python 3 is installed on your system

2. Install Nmap on your operating system

3. Install the python-nmap library using pip

4. Verify installation by importing nmap in a Python shell

Part 2 – Basic Port Scanning with Python Nmap

1. Create a new Python file named scanner.py
2. Import the nmap module
3. Initialize a PortScanner object
4. Define a target host (localhost or a permitted IP)
5. Perform a TCP port scan on a small port range (e.g., 20–1024)
6. Print the scan results in a readable format

Part 3 – Interpreting Scan Results

Enhance your script to:

- List all discovered open ports
- Display port states (open/closed/filtered)
- Identify detected services if available
- Handle cases where the host is unreachable

Part 4 – Robustness and Error Handling

You must demonstrate handling of the following:

- Invalid IP address or hostname
- No open ports found
- Nmap not installed or inaccessible
- Permission or privilege errors
- Network timeout

Part 5 – Reflection Questions

1. What information does port scanning reveal to an attacker?

2. Why is port scanning often the first step in an attack?

3. How can defenders detect or limit scanning activities?

4. What are the limitations of basic port scanning?

Part 6 – Security Analysis

In 300–400 words, analyze the security implications of your scan results. Your analysis must reference:

- Discovered open ports and services
- Potential risks associated with exposed services
- How attackers could abuse this information
- Defensive measures to reduce exposure

Deliverables

- `scanner.py`
- A single recording demonstrating successful client–server communication and robustness testing (mp3 format)
- Security analysis and reflection report
- Submit **one PDF file only**. This PDF is the Security analysis and Reflection Report and must include cloud links to all required technical artifacts (code base, recordings.).
- Filename format:

Lab2-FirstName-LastName-StudentNumber.pdf

Lab Rubric

Component	Criteria	Excellent (Full Credit)	Partial Credit	No Credit	Points
Environment Setup & Readiness	Python 3, Nmap, python-nmap installed; nmap imported & PortScanner initialized	All tools installed and verified; import and initialization correct	Minor setup or verification issues	Environment not functional	10
Port Scanning Implementation	scanner.py structure, target definition, TCP scan, output formatting	Clean, readable file; valid target; TCP scan 20–1024; clear output	Functional but poorly structured, minor errors	Incomplete or non-functional	30

Component	Criteria	Excellent (Full Credit)	Partial Credit	No Credit	Points
Scan Result Interpretation	Open port enumeration, port states, service detection, host reachability	All open ports identified; states and services correctly reported; unreachable hosts handled	Partial identification or reporting	Missing or incorrect	20
Robustness & Error Handling	Handles invalid IP/hostname, no open ports, missing Nmap, permission errors, network timeout	All error cases handled gracefully with informative messages	Most cases handled	Few or no cases handled	20
Reflection Questions	Technical accuracy, depth of insight, clarity	Correct, insightful answers showing attacker/defender perspective; concise & structured	Minor inaccuracies; partially descriptive	Misunderstanding or missing answers	15
Security Analysis Report (300–400 words)	Use of scan results, risk analysis, defensive measures, writing quality	Explicit references; thorough risk & attack vector analysis; practical defenses; clear & professional	General references; limited depth; minor writing issues	Missing or poor analysis	15

Good Luck!