Lab 1: Reconnaissance Basics with Python
COMPSFI 212
Due: 09/02/2025 @ 11:59pm

Pre-Lab

- Python 3.9+ installed
- Install the following libraries: python -m pip install scapy dnspython
- A test target: use your own machine (127.0.0.1) or a lab VM.
- Internet access for DNS lookups (e.g., google.com).

Part 1: Active Reconnaissance (Port Checking/Scanning)

Goal: See which common ports respond on a target.

Tasks:

- Create a Python script that:
- - Asks the user for an IP address.
- - Tries to connect to these ports: 80, 443, 22, 53.
- - Prints whether the connection succeeded or failed.

Hint: You can use Python’s built-in socket library instead of scapy to keep it simple.

Deliverable 1: Screenshot of your script running and a short explanation of results.

Part 2: Passive Reconnaissance (DNS Lookup)

Goal: Learn what DNS reveals without touching the target directly.

Tasks:

- Use dnspython to look up the IP address of: www.google.com and mail.google.com.
- Perform a reverse DNS lookup on one of those IPs to see if it maps to another name.

Deliverable 2: Copy the output of your DNS lookups and write a short explanation.

Part 3: Defensive Thinking (No coding required)

Goal: Consider how defenders might respond to reconnaissance.

Answer the following in 3–4 sentences each:

- Why can’t defenders stop all reconnaissance?
- How could a honeypot help during reconnaissance?
- What’s one way to make DNS entries less useful to attackers?

Deliverable 3: Written answers in paragraph form.