The exercises are designed for students to finish in an individual capacity. The exercises are not designed to be completed in tutorial sessions but rather to give you some tasks and a starting point to continue and complete on your own.

1 TCP Scanning Techniques

TCP scanning is a fundamental technique used in network security for enumerating open ports on a target machine. Different types of TCP scans exploit the behaviour of the TCP three-way handshake to detect the status of ports (open, closed, filtered). Understanding these methods is crucial for both network defence and penetration testing.

Learning Objectives:

- Understand the theory behind various TCP scanning techniques.
- Perform practical TCP scanning using common tools.
- Analyze network traffic to identify different scanning methods.

1.1 Understanding various TCP scanning techniques

1. Explain the TCP three-way handshake process.
2. For each of the following TCP scanning methods, describe how the scan works, its typical use cases, and its strengths and weaknesses. Consider how each technique interacts with the TCP handshake process and what kind of response it seeks from the target.
   - SYN Connect Scan
   - TCP SYN Scan (Half-open scan)
   - ACK Scan
   - FIN Scan
   - Xmas Tree Scan
   - NULL Scan
3. Discuss the legal and ethical implications of using TCP scanning techniques in real-world environments. When and where is it appropriate to use these scans?

1.2 Practical Application of scanning techniques

1.2.1 Setting up the lab environment

Open SecureCorp project and start all nodes (you can use an existing SecureCorp project from the previous labs). You will need an Attacker and a Server node for this lab. These can be any 2 nodes in your SecureCorp project. Let's use `Internal-Client` as the Server and the `Internal-Attacker` as the Attacker.

- Prepare the server
  Run the provided server.py script on the Internal-Client as below. This will open a set of random ports on the server that we can scan.

```
python3 server.py 123456
```

- Prepare the Internal-Attacker
  Run the below commands to install Namp on the Attacker node.

```
apt update
apt install nmap -y
```

1.2.2 Perform the TCP scans

Nmap (Network Mapper) is a powerful and widely-used open-source tool designed for network discovery and security auditing. It is highly versatile and supports various types of scanning techniques, including TCP connect scans, SYN scans, FIN scans, and more. It can also detect vulnerabilities and misconfigurations within a network, making it an essential tool for both network administrators and security professionals.

Perform the above discussed TCP scans using Nmap. Below is the basic syntax for performing a TCP Connect Scan for all ports. Refer to Namp documentation to find out how to perform other types of TCP scans using Namp. (ref: `https://nmap.org/book/scan-methods.html`)

```
nmap -sT -p- <target-ip>
```

1.2.3 Analyse the scanning traffic

Observe the traffic between the Internal-Server and Internal-Attacker using Wireshark. Can you find the traffic patterns discussed in previous task?