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 the SecureCorp project and start all nodes. You should have the Internal-Server node from Week 6 lab.

- Prepare the server
  Install Python3 on the Internal-Server container

  ```
  apt install python3-pip -y
  ```

  Run the provided server.py script on the Internal-Server 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?

2 Wireless Security

2.1 Understanding Wireless Security protocols

- In IEEE 802.11, open system authentication simply consists of two communications. An authentication is requested by the client, which contains the station ID (typically a MAC address). This is followed by an authentication response from the AP/router containing the success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.
  - What are the benefits of this authentication scheme?
  - What are the security vulnerabilities of this authentication scheme?
- What is a rogue AP? How to detect and prevent rogue AP risks?
- Briefly analyze different wireless security protocols (WEP, WPA, WPA2).
- Describe the key differences between WPA2 and WPA3 in terms of encryption methods, authentication mechanisms, and protection against common attacks. Why was WPA3 introduced, and what vulnerabilities in WPA2 does it address?
- Explain how the 802.11 standards (such as 802.11ac and 802.11ax) interact with WPA2 and WPA3 protocols. How do these standards enhance or complement the security features of WPA2 and WPA3?

2.1.1 War-Driving and War-Walking and RADIUS

Wireless LANs are often not secure. It is simple to bring your laptop computer into a public area and listen for wireless networks. This is called War-Driving (if you are in a car) or War-Walking (if you're walking). As long as you do not attempt to use any networks without authorization, War-Driving and War-Walking are quite legal. There are many good software tools available for War-Driving.

- NetSpot for Windows or Mac OS (`http://www.netspotapp.com`)
- Acrylic Wifi for Windows (`https://www.acrylicwifi.com/en/`)
- inSSIDer-2 for Windows (`http://bit.ly/1KcqkN2`)
- Net Stumbler for Windows (`http://www.netstumbler.com/downloads/`)

The first step is to download and install a WLAN sniffing tool on a laptop computer that has wireless capability (please install it in your host, NOT in your VM). Once you have installed the software, simply walk or drive to a public area and start it up. For each AP explore the security section and find any insecure (with WEP or WPA) APs.

- Do you see any OPEN network? What does it mean?
- Research WiFi implementation with RADIUS (Remote Authentication Dial In User Service) and discuss its security.

2.2 Adittional Review Questions

- What is the basic building block of an 802.11 WLAN?
- Define an extended service set.
- Is a Distribution System a Wireless Network?
- What security areas are addressed by IEEE 802.11i?
- What is the difference between TKIP and CCMP?