NETSEC: TP1

Jacopo Bufalino, Pengwenlong GU

October 2025

Introduction

This lab aims to give you practical experience with network analysis, reconnaissance and asset management through the use of `Wireshark` and `nmap`.

For a correct submission, provide a PDF report with the answers to both exercises.

1 Capture and analyse the protocols

In the first part of the lab, you will analyze network traces with `Wireshark`. If not yet available in your computer, you can download the tool from here: `https://www.wireshark.org/download.html`. You are encouraged to read the documentation online (`https://www.wireshark.org/docs/`).

1.1 Part1: ARP

Start a scan with Wireshark on the Ethernet interface. Apply the ARP filter on the menu and answer the following questions:

- What is your hostname?
- What is your MAC address?
- What data is exchanged in an ARP message?
- What are the source and destination in an Ethernet frame containing an ARP request?

1.2 Part2: Traceroute

Start a new scan with Wireshark on the Ethernet interface. Open a new terminal on the side and run the command `traceroute 1.1.1.1` until complete. Stop the scan and answer the following questions:

- Which protocol is used by `traceroute` ?
- What is the TTL value of the third hop?
- Some rows in the traceroute output look like `* * *`, why?

2 Network scanning

You'll perform a scan within a simulated company network to detect active devices and list the services they're running. Details on accessing the exercise platform will be sent to you via email. If you haven't received this information, please reach out to the course teachers. The credentials will allow you access to a remote SSH server where you will begin your TP.

Nmap Usage

The general syntax for an nmap command is structured as follows: `nmap [options] target`. It's essential to become familiar with the various scan types that nmap offers, along with their specific command-line options. For an in-depth reference, please consult the nmap manual at `https://nmap.org/book/man.html`. You are encouraged to find a practical tutorial on nmap online and to follow it.

As you explore different scan settings, pay particular attention to those involving protocols, ports, and timing. Remember to avoid excessive brute-force scanning, and if the virtual machine or network performance slows down, consider pausing to allow the system to recover.

Note: Please scan only private networks. Avoid scanning the Internet or any public networks. Remember that private networks, as outlined in RFC-1918, include the following ranges:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Be sure to save a copy of your findings and commands on your personal computer. The virtual machines operate in containerized environments and may be reset whenever server settings are updated or the server is rebooted.

Host Enumeration

Your objective is to scan the company network to identify the active hosts. Typically, the process begins with locating your own network interfaces and addresses then, you can use `nmap` to discover the active hosts. Here is a list of useful commands:

- ip
- ifconfig
- arp

Service discovery

Once you have found all the hosts in the company network, enumerate all the services (open ports) running on each host.

Report

- List of commands used to find the hosts and their output (you can do screenshots of your terminal). The list must contain all the IP addresses you have found.
- List of commands used to enumerate the ports open on each host and the services running on those ports, when available (you can do screenshots of your terminal).
- The topology graph of the company network.