Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

Lab 5 – Network Surveillance

Lab Description and Instructions
We learn how to carry out basic network reconnaissance using two popular tools, namely nmap and WireShark. We will limit our reconnaissance to the local network and all of our VM's traffic (local and external). To learn about the local network we will first learn the local IP address of our VM using:

```bash
ifconfig (e.g. 192.168.13.101)
```

First, we will scan for all computers (hosts) and services on the local network using nmap as follows:

```bash
nmap 192.168.13.101/24
```

Next, we will observe traffic (network packets) on the local link using WireShark (graphical).

**Homework:**
Try all the above steps in your VM. Additionally, scan for all open ports on the host 192.168.12.2. Use WireShark to find out if and when your VM is communicating with the 192.168.12.2.