EC7020: COMPUTER AND NETWORK SECURITY
LABORATORY EXPERIMENT: 05
WIRELESS NETWORK SECURITY

Reg No: 2019/E/118 29/11/2023, from 13:00 to 16:00

AIM: Students will learn the fundamental principles of wireless networks and wireless network security by using network auditing tools.

OBJECTIVES:

- To understand the wireless networks.
- To understand the functionalities of network auditing.
- To understand the fundamentals of wireless network security.

Following are the tasks for this lab session. (30 Marks)

(Group Task)

1. Select a network security audit tool that works with Wi-Fi networks. You have to do a detailed analysis of a Wi-Fi network which you have to create using a mobile hot-spot.

   The report you submit must include details

   A. About the tool and its features.

One of the most exceptional instruments for scrutinizing network security is Nmap. Nmap, which stands for Network Mapper, is an open-source command-line tool designed for Linux that is employed to examine IP addresses and ports within a network, as well as to identify installed applications. It enables network administrators to ascertain which devices are operational on their network, discover exposed ports and services, and detect vulnerabilities. Several fundamental features of Nmap encompass:

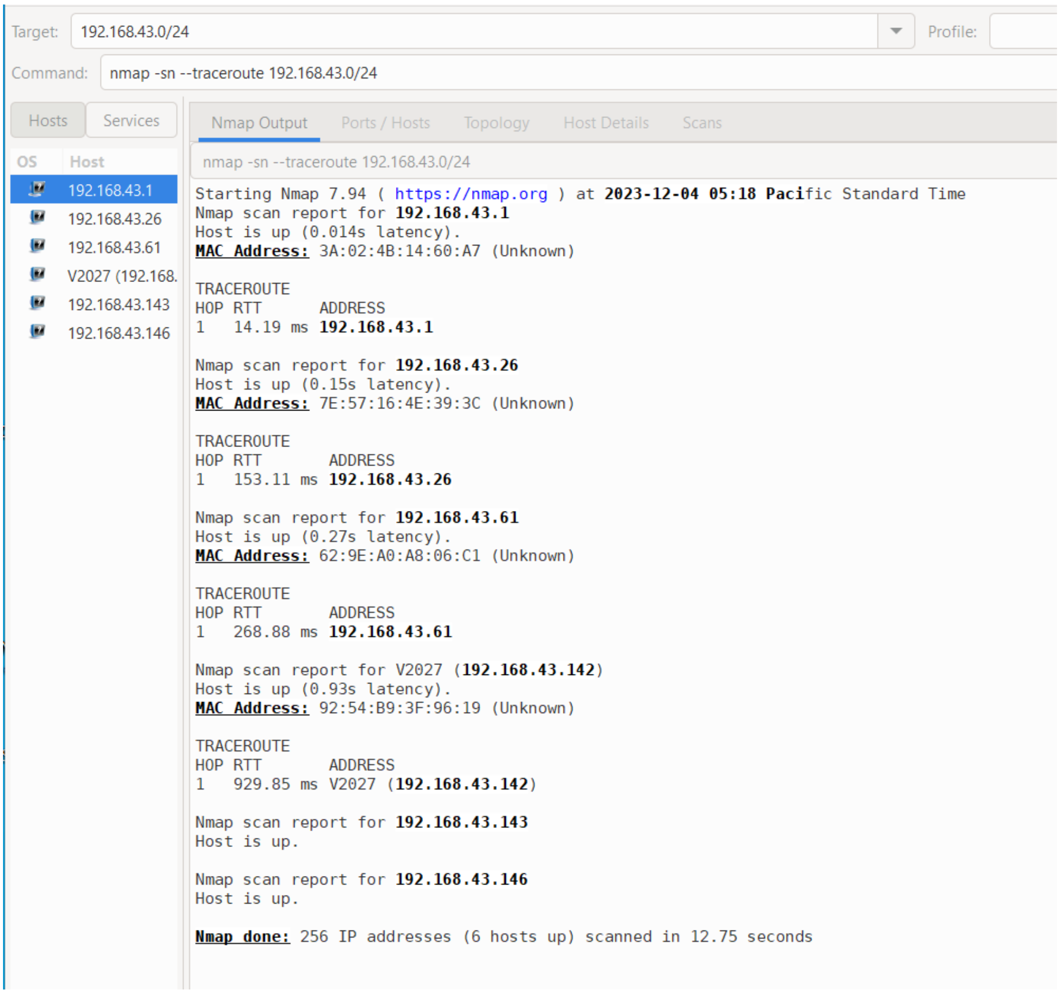
- Aptitude to promptly recognize all the devices, such as servers, routers, switches, mobile devices, etc., within a solitary or multiple networks. - Assists in identifying services running on a system, including web servers, DNS servers, and other ubiquitous applications. - Nmap can also accurately determine the versions of applications to aid in the detection of existing vulnerabilities. - It has the capability to obtain information about the operating system utilized by devices. It can furnish comprehensive details such as OS versions, thereby streamlining the planning of additional approaches during penetration testing. - During security auditing and vulnerability scanning, Nmap allows for the utilization of existing scripts from the Nmap Scripting Engine to launch attacks on systems. - Nmap encompasses a graphical user interface known as Zenmap, which facilitates the development of visual mappings of a network, thereby enhancing usability and reporting.

   B. Alternative tools available in the industry and reason for your selection

There exist numerous alternative tools, such as Zenmap, Angry IP Scanner, Fing, Advanced IP Scanner, and Port Authority. Nevertheless, Nmap is selected due to its extensive array of features and user-friendly nature. And it is open source , so it is totally free.

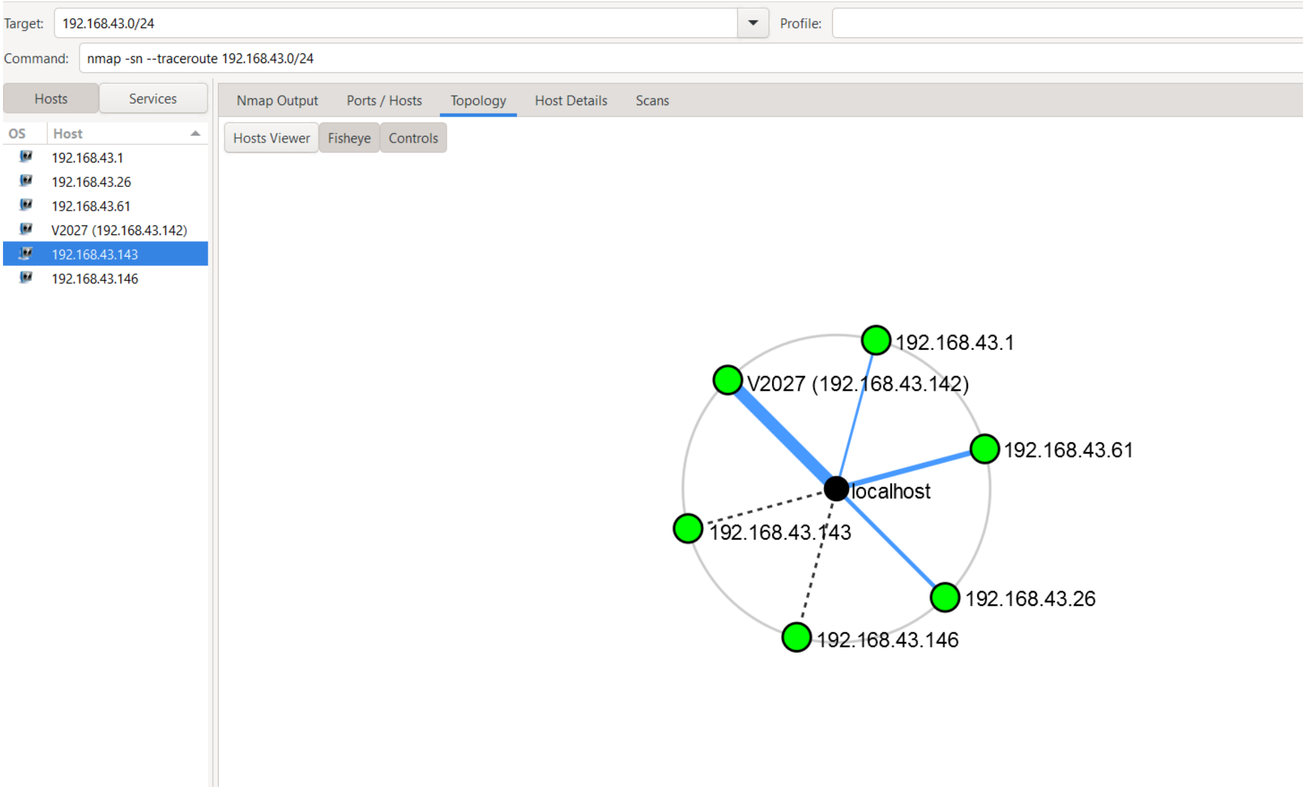
   C. The Details of Wi-Fi Hotspot.

Network topology denotes the arrangement of distinct network components within a communication network. It can manifest as physical, representing the tangible connections in a network, or logical, illustrating how data circulates within a network. Tools such as Auvik, Datadog Live Network Monitoring, and Zenmap can be employed to visualize the network topology.



```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-04 05:18 Pacific Standard Time
Nmap scan report for 192.168.43.1
Host is up (0.014s latency).
MAC Address: 3A:02:4B:14:60:A7 (Unknown)

TRACEROUTE
HOP RTT      ADDRESS
1   14.19 ms 192.168.43.1

Nmap scan report for 192.168.43.26
Host is up (0.15s latency).
MAC Address: 7E:57:16:4E:39:3C (Unknown)

TRACEROUTE
HOP RTT       ADDRESS
1   153.11 ms 192.168.43.26

Nmap scan report for 192.168.43.61
Host is up (0.27s latency).
MAC Address: 62:9E:A0:A8:06:C1 (Unknown)

TRACEROUTE
HOP RTT       ADDRESS
1   268.88 ms 192.168.43.61

Nmap scan report for V2027 (192.168.43.142)
Host is up (0.93s latency).
MAC Address: 92:54:B9:3F:96:19 (Unknown)

TRACEROUTE
HOP RTT       ADDRESS
1   929.85 ms V2027 (192.168.43.142)

Nmap scan report for 192.168.43.143
Host is up.

Nmap scan report for 192.168.43.146
Host is up.

Nmap done: 256 IP addresses (6 hosts up) scanned in 12.75 seconds
```

D. Network Topology.

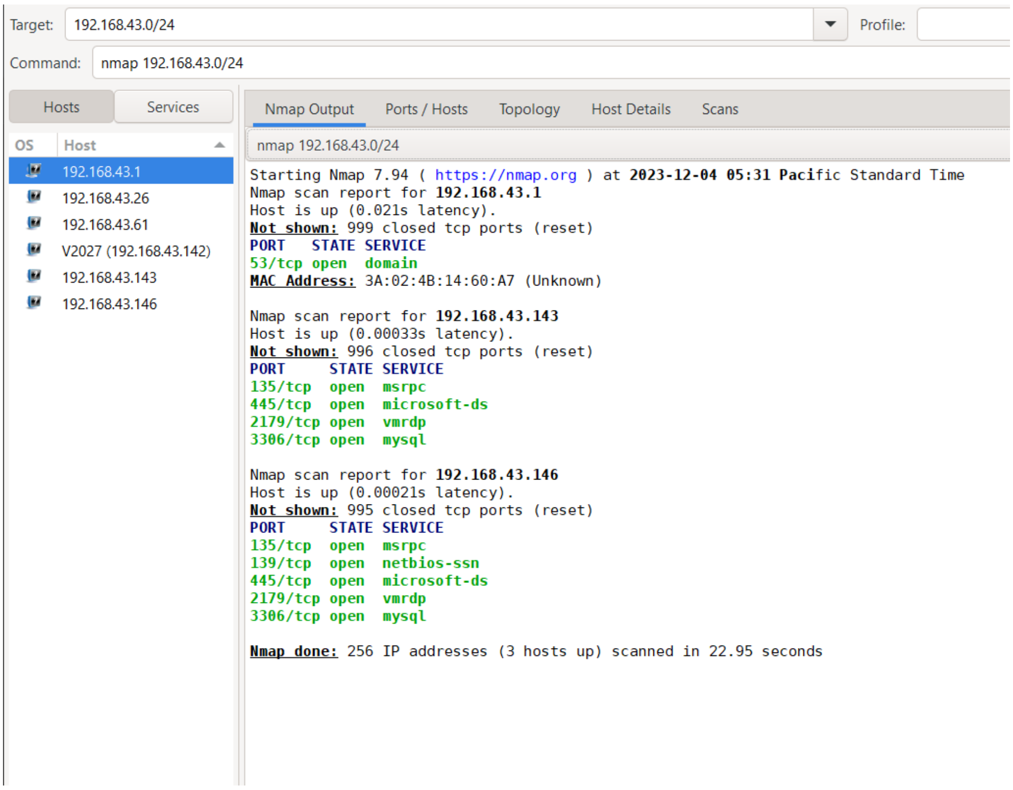


Target: 192.168.43.0/24

Command: nmap -sn --traceroute 192.168.43.0/24

192.168.43.1
192.168.43.26
192.168.43.61
V2027 (192.168.43.142)
192.168.43.143
192.168.43.146

E. Host Details.



Target: 192.168.43.0/24

Command: nmap 192.168.43.0/24

192.168.43.1
192.168.43.26
192.168.43.61
V2027 (192.168.43.142)
192.168.43.143
192.168.43.146

nmap 192.168.43.0/24

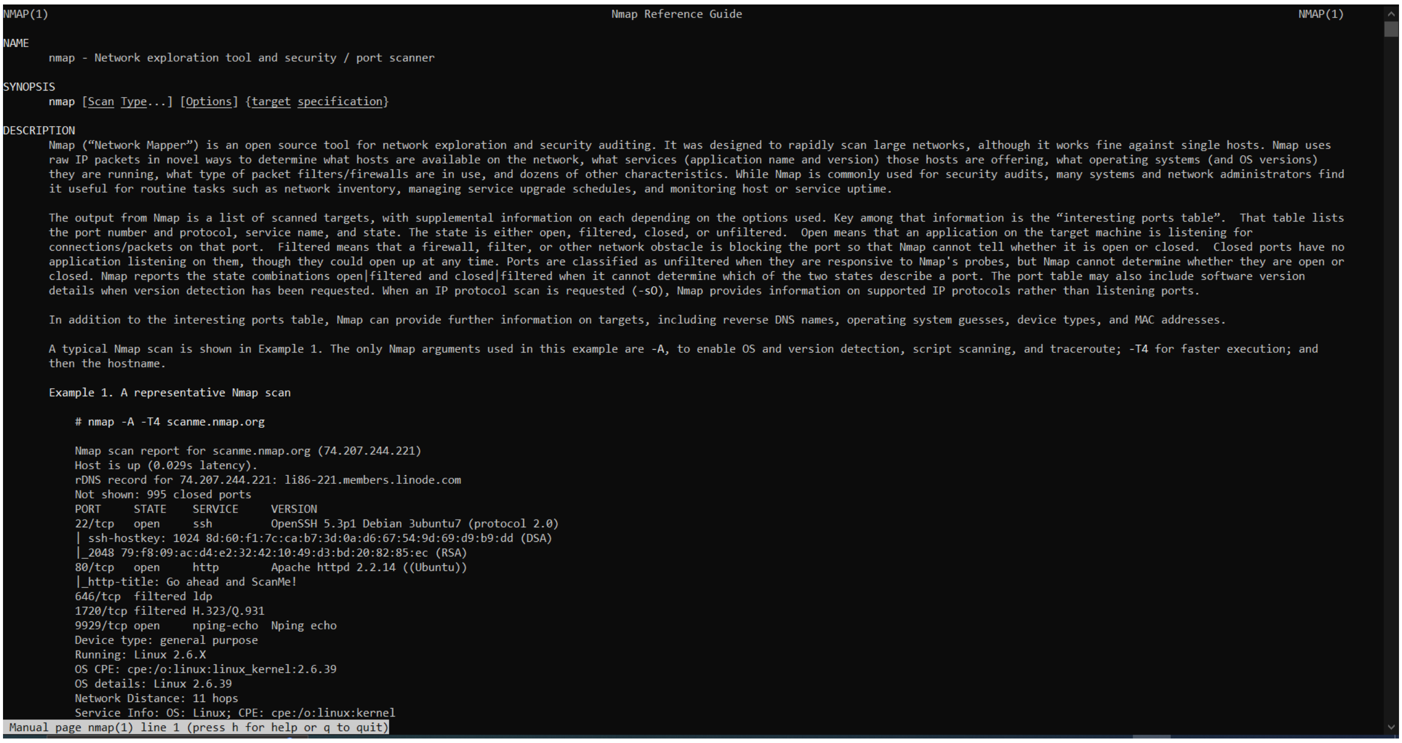
```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-04 05:31 Pacific Standard Time
Nmap scan report for 192.168.43.1
Host is up (0.021s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 3A:02:4B:14:60:A7 (Unknown)

Nmap scan report for 192.168.43.143
Host is up (0.00033s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3306/tcp open  mysql

Nmap scan report for 192.168.43.146
Host is up (0.00021s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3306/tcp open  mysql

Nmap done: 256 IP addresses (3 hosts up) scanned in 22.95 seconds
```

F. Network Analysis.

nmap [scan type] [options] {target}

there have different ways to analize using zennmap, like intense scans, ping scans,tracert scans, reguler scans are present in this tool. But The nmap command has the scan types and options and target as above structure.

Most of the detail can be seen form the tool itself using “man nmap” command



```
NMAP(1)                                                                      Nmap Reference Guide                                                                      NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses
       raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions)
       they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find
       it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the “interesting ports table”.  That table lists
       the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered.  Open means that an application on the target machine is listening for
       connections/packets on that port.  Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.  Closed ports have no
       application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or
       closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version
       details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

       In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

       A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and
       then the hostname.

       Example 1. A representative Nmap scan

           # nmap -A -T4 scanme.nmap.org

           Nmap scan report for scanme.nmap.org (74.207.244.221)
           Host is up (0.029s latency).
           rDNS record for 74.207.244.221: li86-221.members.linode.com
           Not shown: 995 closed ports
           PORT     STATE    SERVICE     VERSION
           22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
           | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
           |_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
           80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
           |_http-title: Go ahead and ScanMe!
           646/tcp  filtered ldp
           1720/tcp filtered H.323/Q.931
           9929/tcp open     nping-echo  Nping echo
           Device type: general purpose
           Running: Linux 2.6.X
           OS CPE: cpe:/o:linux:linux_kernel:2.6.39
           OS details: Linux 2.6.39
           Network Distance: 11 hops
           Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
 Manual page nmap(1) line 1 (press h for help or q to quit)
```

Attach Screenshots and explain content if necessary.

Work Flow:

- Refer to the following links,
    - https://www.ictshore.com/hacking/nmap-tutorial/
    - https://nmap.org/book/zenmap.html
    - Nmap Cheat Sheet 2023: All the Commands, Flags & Switches (stationx.net)
- Use one laptop for analyzer
- You can use as much as devices for scanning.
- Connect multiple devices with a same hotspot. The laptop should be connected with the same hotspot.
- Then scan the network and report the results.

(Individual Tasks)

2. You have to describe the Evolution of Wireless security protocols clearly. And include comparison. (30 Marks)

WEP, also known as Wired Equivalent Privacy, was introduced in 1997 as a component of the original 802.11 standard. It employed a static key for encryption, which unfortunately proved to be easily deciphered. Consequently, WEP exhibited inadequate security measures and was susceptible to numerous vulnerabilities.

In an attempt to rectify the shortcomings of WEP, WPA, or Wi-Fi Protected Access, was developed in 2003. This iteration of wireless security introduced the Temporal Key Integrity Protocol (TKIP) to enhance encryption. Additionally, WPA implemented a Message Integrity Check, which effectively prevented packet forgery.

Following the introduction of WPA, WPA2, or Wi-Fi Protected Access II, was certified in 2004 and subsequently mandated in 2006 for all new devices. Notably, WPA2 replaced TKIP with the more robust Advanced Encryption Standard (AES) protocol, thereby bolstering security measures. Consequently, WPA2 emerged as the preeminent security protocol for Wi-Fi networks.

Building upon the foundation laid by its predecessor, WPA3, or Wi-Fi Protected Access III, was released in 2018 as a replacement for WPA2. This iteration of wireless security provides enhanced protection against offline password guessing attacks. Additionally, WPA3 employs individualized data encryption to safeguard data transmitted over open networks.

WPA3 employs encryption methods that are more resilient, namely AES-128 and AES-256, when juxtaposed with its predecessors.

WPA3 provides enhanced defense mechanisms against brute-force attacks through the utilization of Simultaneous Authentication of Equals (SAE).

WPA3 offers support for forward secrecy, which signifies that in the event that an adversary manages to intercept encrypted data, they would be incapable of deciphering it, even if they acquire knowledge of the network password at a later point in time.

3. Compare the difference between Wired LAN and Wireless Network security protocols. (10 Marks)

The ease of interception pertains to the capability of wireless signals to be intercepted by any individual within the vicinity, thereby rendering wireless networks intrinsically less secure in comparison to wired networks. The security protocols established on wired networks are contingent upon physical security measures, in contrast to wireless networks which necessitate the implementation of intricate encryption algorithms to ensure the safeguarding of data transmission. The aspect of maintenance mandates that wired networks necessitate infrequent alterations to security settings when juxtaposed with wireless networks, which require periodic updates in order to sustain their security against novel threats.

4. Briefly describe about packet tracing. And explain how packet tracer helps to crack Wi-Fi passwords. (10 Marks)

Packet tracing is a technique employed to trace the trajectory of packets throughout a network. It aids in the identification and diagnosis of network problems, comprehension of network traffic patterns, and detection of possible security infringements. Packet tracing utilities seize and scrutinize the packets traversing the network, furnishing valuable insights into the data transmission and reception, as well as the network's efficiency.

Discussion (Write the analysis of this lab experiment) (10 Marks)

Nmap provides a comprehensive set of features for network analysis, including topology and address details1. Different network protocols offer security suitable for various situations, and the appropriate protocol should be selected based on the context2. Some devices, particularly those running Apple OS, may not reveal connected device data to Nmap.

Conclusion (Include the concise summary of those which have already been presented in the report) (10marks)

Nmap’s extensive features facilitate detailed network analysis, allowing for the extraction of information such as network topology and addresses1. The lab experiment highlights the importance of selecting the right network protocol for specific security needs and situations. The experiment also demonstrates that while Nmap is a powerful tool, it may have limitations in detecting certain devices, emphasizing the need for continuous tool evaluation and updates.

Write your answers in this Lab Instruction sheet with the file name EC7020_L5_YourRegNo. Submit it as a PDF document archive all files and upload it to the teams. The same name conversion applies to the Zip.