Terna Engineering College

Computer Engineering Department

Class: TE **Sem.: VI**

Course: System Security Lab

PART A

(PART A: TO BE REFERRED BY STUDENTS)

Experiment No.07

A.1 Aim:

Download and install Nmap. Use it with different options to scan open ports, perform OSfingerprinting, do a ping scan, TCP port scan, UDP port scan, Xmas scan etc.

A.2 Prerequisite:

Basic Knowledge of Ports, TCP, UDP, Ping

A.3 Outcome:

After successful completion of this experiment, students will be able to Install and use Nmap and use it for gathering detailed network and remote host information.

A.4 Theory:

➔ Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

- Host Discovery – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
- Port Scanning – Enumerating the open ports on one or more target hosts.
- Version Detection – Interrogating listening network services listening on remote devices to determine the application name and version number.
- OS Detection –Remotely determining the operating system and some hardware characteristics of network devices.

Basic commands working in Nmap:

- For target specifications: Nmap <target's URL or IP with spaces between them>
- For OS detection: Nmap -O <target-host's URL or IP>
- For version detection: Nmap -SV <target-host's URL or IP>

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections.

A5.Procedure:

Installation of Nmap:

$ sudo apt-get install nmap

Commands:

- **nmap -sP <10.0.0.0/24>**

  Ping scans the network, listing machines that respond to ping.

- **FIN scan (-SF)**

  Sets just the TCP FIN bit.

- **-sV (Version detection) .**

  Enables version detection, as discussed above. Alternatively, can use -A, which enables version detection among other things.

- **-sO (IP protocol scan).**

  IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn´t technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers.

- **-O (Enable OS detection).**

  Enables OS detection, as discussed above. Alternatively, you can use -A to enable OS detection along with other things.

- **-p port ranges (Only scan specified ports).**

  This option specifies which ports you want to scan and overrides the default. Individual port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively.

- **--top-ports <integer of 1 or greater>**

  Scans the N highest-ratio ports found in the Nmap-services file.

- **Nmap –-iflist**

  host interface and route information with nmap by using —–iflistǁ option.

PART B

(PART B: TO BE COMPLETED BY STUDENTS)

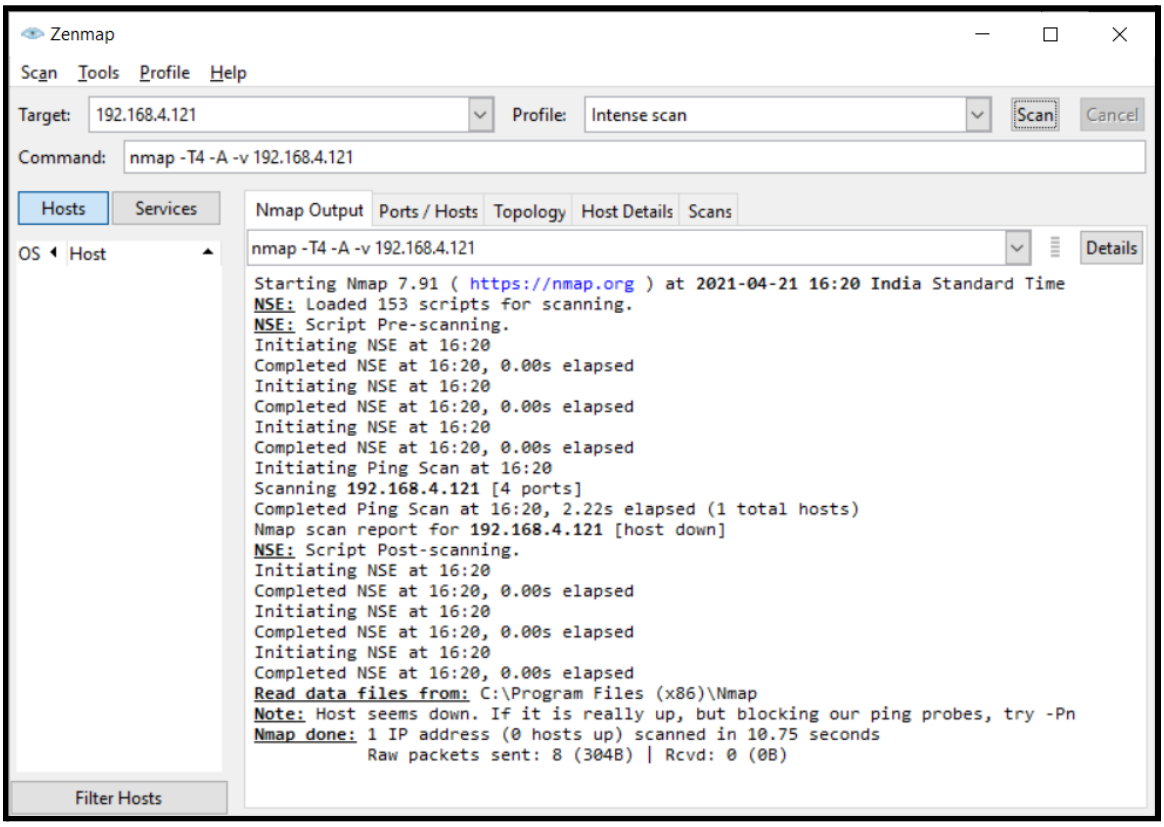
(Students must submit the soft copy as per the following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Blackboard access available)

Roll No. 50	**Name:** AMEY THAKUR
Class: Comps TE B	**Batch:** B3
Date of Experiment: 20/04/2021	**Date of Submission:** 20/04/2021
Grade:	

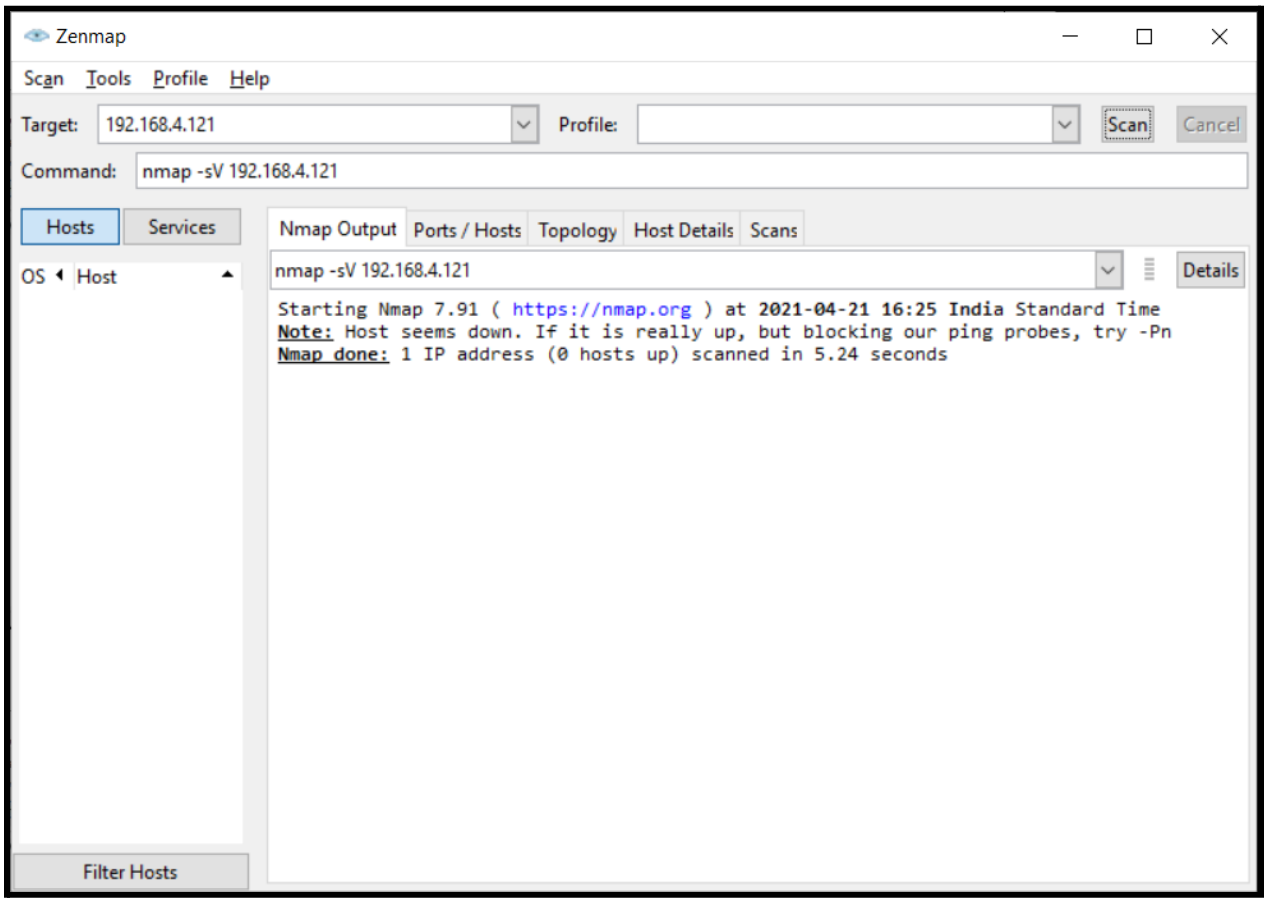
B.1 Output

(add a snapshot of output)

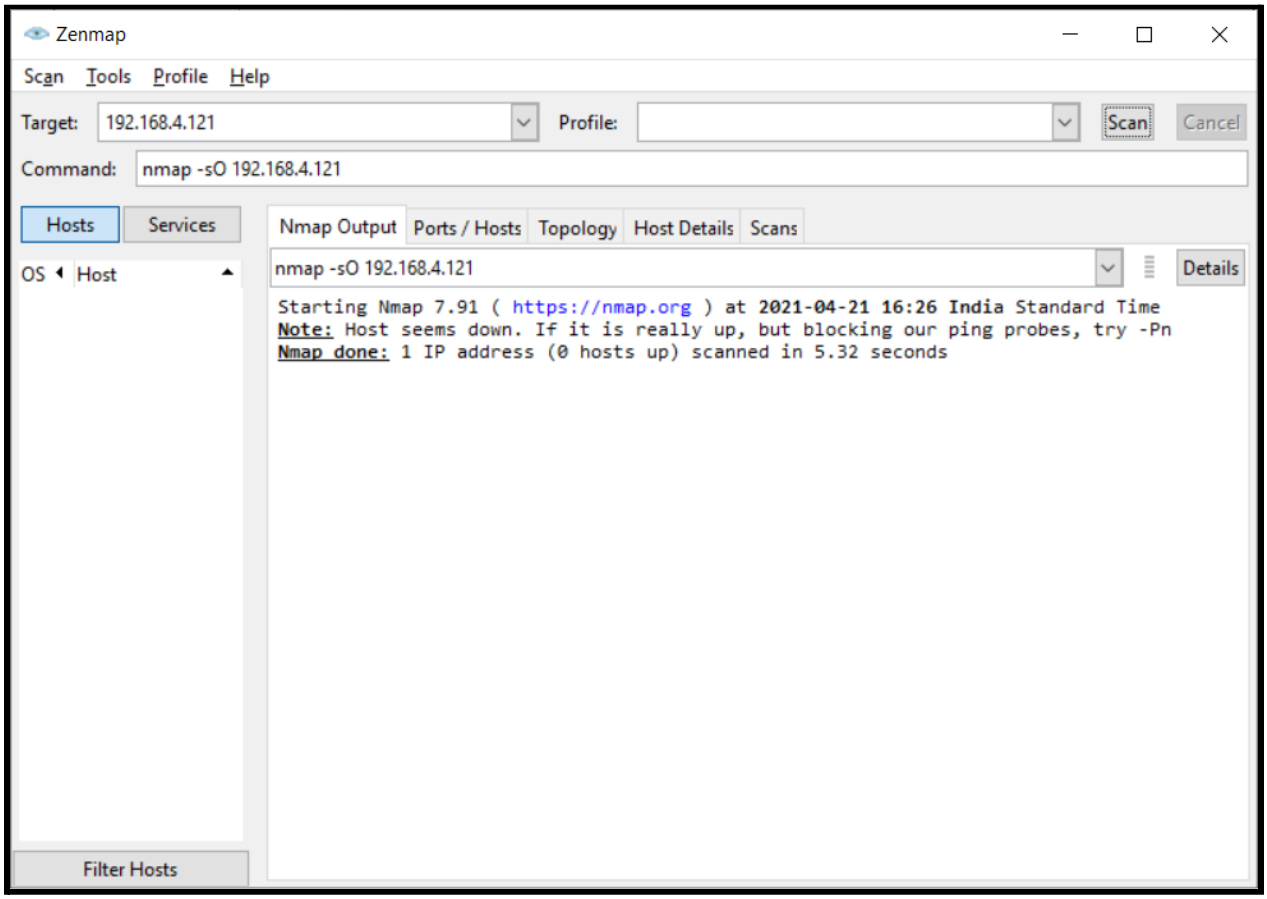
Target: 192.168.4.121
Command: nmap -T4 -A 192.168.4.121



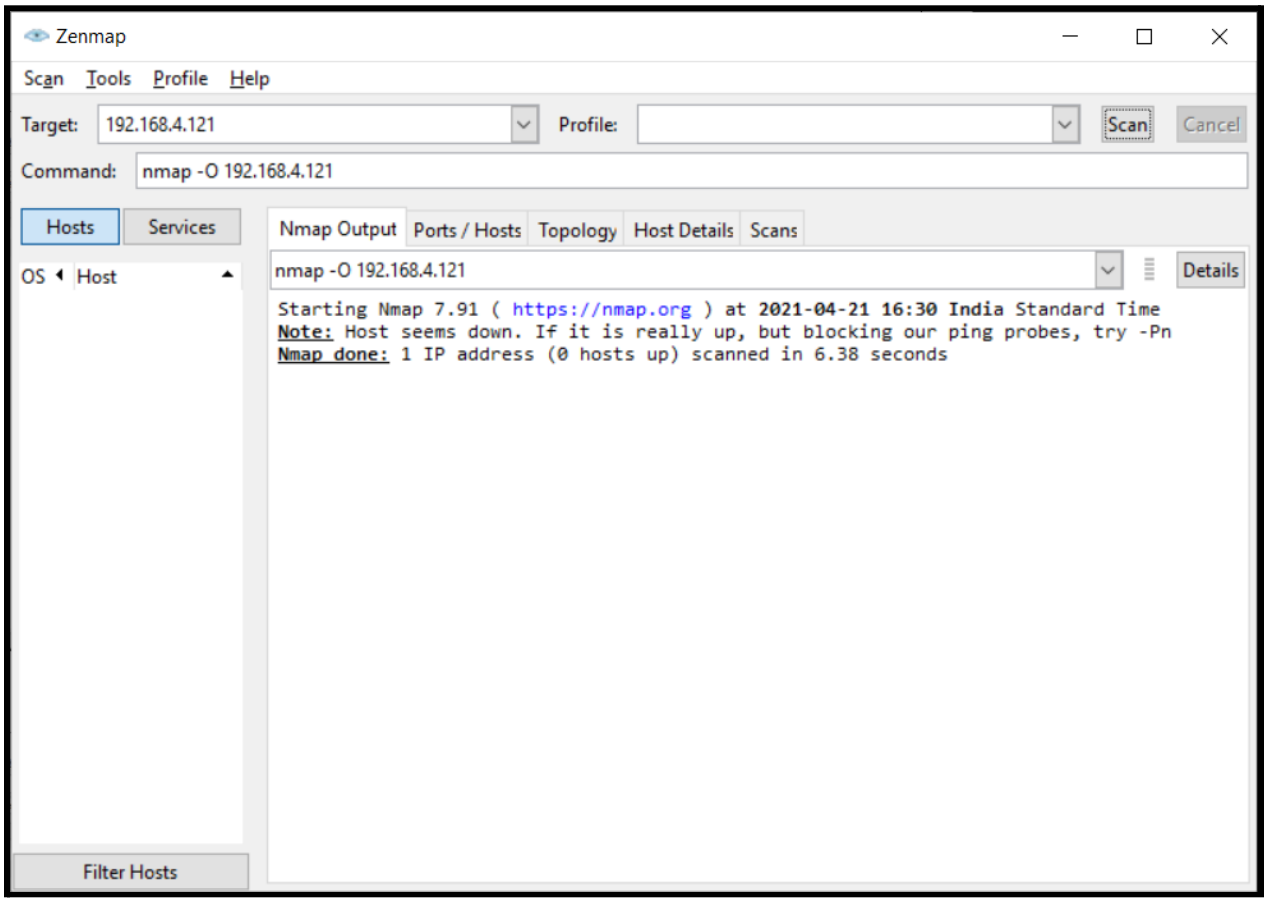
Target: 192.168.4.121
Command: nmap -sV 192.168.4.121



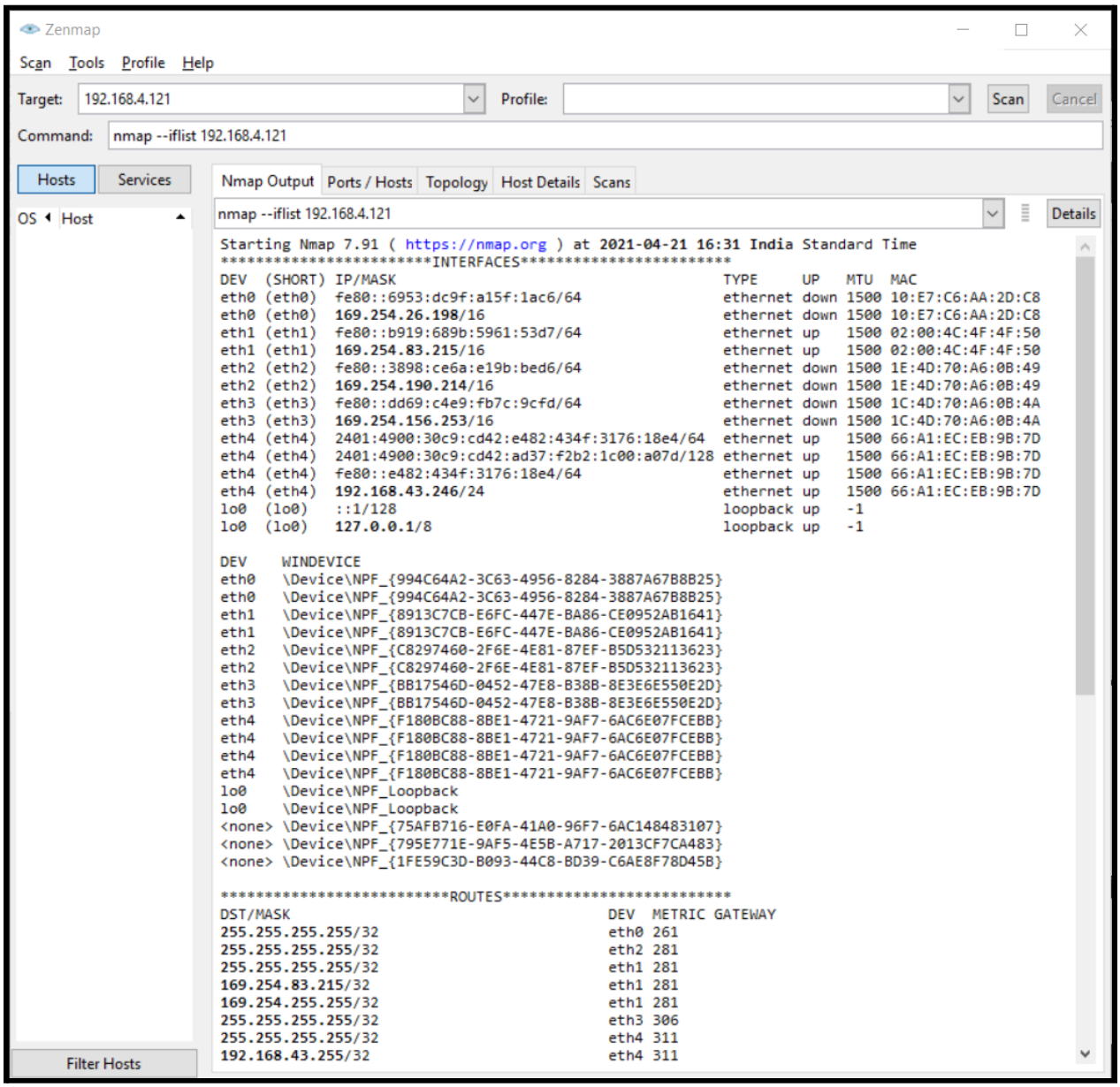
Target: 192.168.4.121
Command: nmap -sO 192.168.4.121

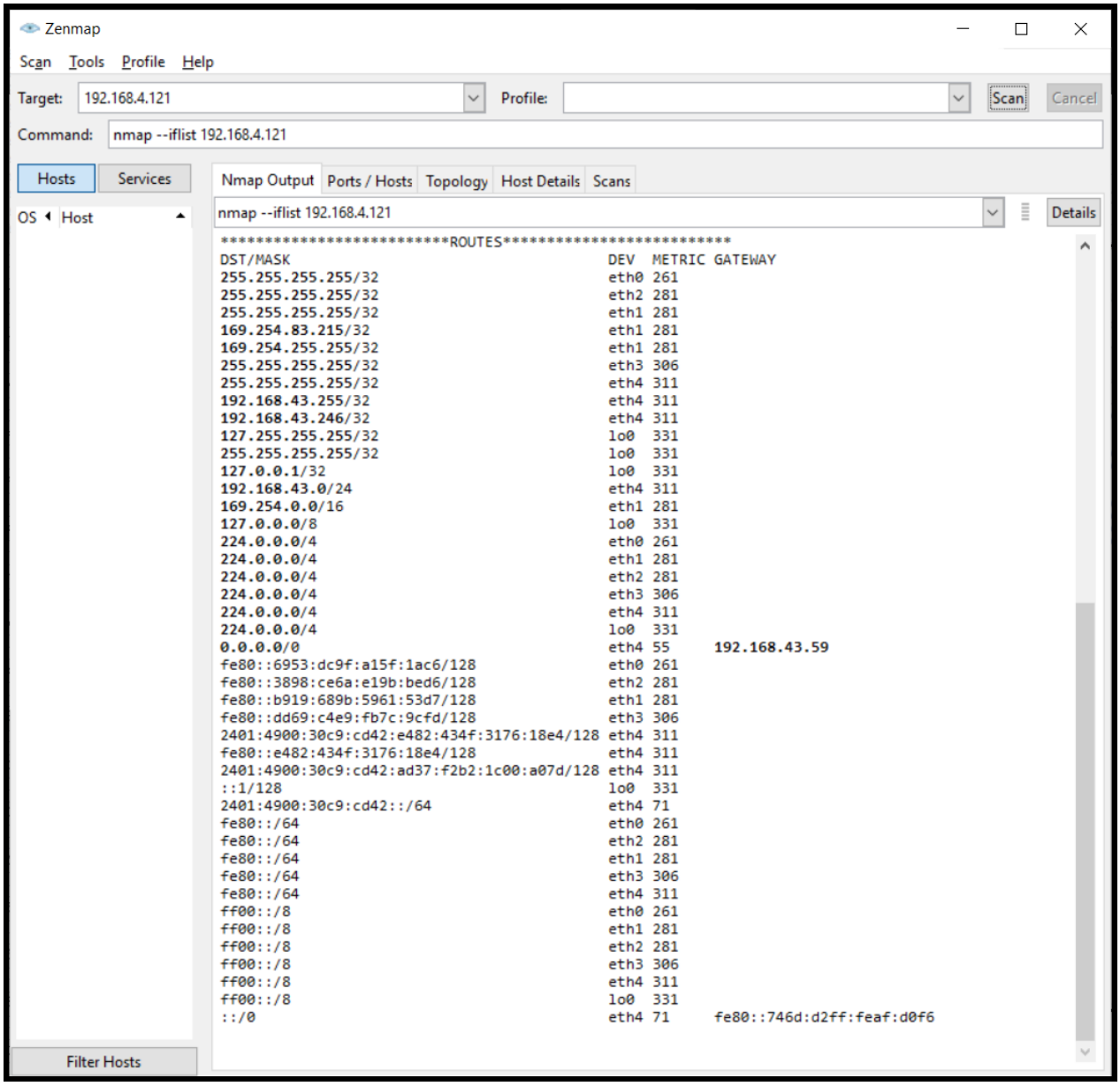


Target: 192.168.4.121
Command: nmap -O 192.168.4.121



Target: 192.168.4.121
Command: nmap --iflist 192.168.4.121





B.2 Commands/tools used with the syntax:

Target: 192.168.4.121

Commands:

- ➔ nmap -T4 -A 192.168.4.121
- ➔ nmap -sV 192.168.4.121
- ➔ nmap -sO 192.168.4.121
- ➔ nmap -O 192.168.4.121
- ➔ nmap --iflist 192.168.4.121

B.3 Question of Curiosity:

1. What is SQL injection?

Ans:

- ➔ SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour.
- ➔ In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure or perform a denial-of-service attack.

2. What is the query that makes SQL injection possible?

Ans:

- ➔ It is a simple example of authenticating with a username and a password. The example database has a table named users with the following columns: username and password.

```
# Define POST variables

    uname = request.POST['username']

    passwd = request.POST['password']

# SQL query vulnerable to SQLi

    sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"

# Execute the SQL statement

    database.execute(sql)
```

- ➔ These input fields are vulnerable to SQL Injection. An attacker could use SQL commands in the input in a way that would alter the SQL statement executed by the database server. For example, they could use a trick involving a single quote and set the password field to password' OR 1=1

3. Explain " OR 1 = 1" and what happens to SQL when this condition is used in the query.

Ans:

➔ As a result, the database server runs the following SQL query:

SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'

➔ Because of the OR 1=1 statement, the WHERE clause returns the first id from the user's table no matter what the username and password are. The first user id in a database is very often the administrator. In this way, the attacker not only bypasses authentication but also gains administrator privileges. They can also comment out the rest of the SQL statement to control the execution of the SQL query further.

B.4 Conclusion:

(Write an appropriate conclusion.)

After successful completion of this experiment, we have Installed and used Nmap for gathering detailed network and remote host information.