Internship Task 1 Report

Task Title :

Footprinting with Nmap

Objective :

To find live hosts and open ports on a local virtual network through the use of Nmap. This task seeks to replicate the reconnaissance stage of ethical hacking by conducting a ping sweep and port scan on a locally installed VM setup.

Tools & Technologies Used :

-Nmap – A reliable network scanning utility .

-Windows Command Prompt – Used to execute Nmap commands in a windows environment.

-VirtualBox – Used to host virtual machines for testing in an isolated network .

Steps Performed :

1.Identify Live Hosts (Ping Sweep)

Run the following Nmap command to perform a ping sweep across the local subnet:

```
Nmap -sn 192.168.29.38/24
```

The -sn option instructs Nmap to do a “ping scan” . This command identifies which hosts are up and accessible .

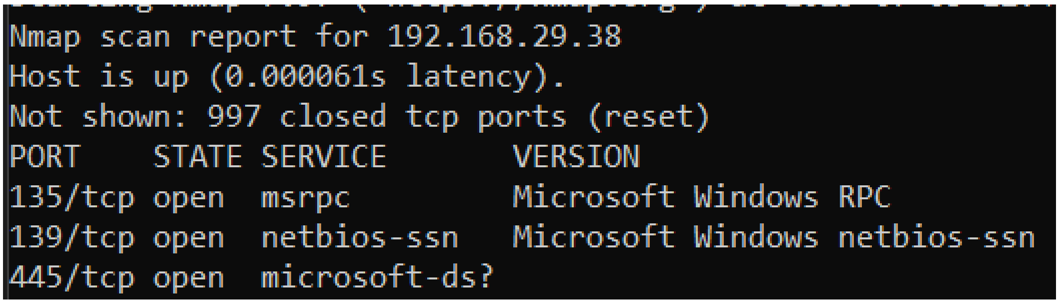
2.Scan Open Ports on Live Hosts

Scan common ports (1-1000) on a live host (ip : 192.168.29.38) :

```
nmap -sS -p 1-1000 192.168.29.38
```

- -sS scans using the TCP SYN method .
- -p defines the port range .

Output :



```
Nmap scan report for 192.168.29.38
Host is up (0.000061s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
```

Findings :

IP Address	Host Status	Open Ports	Services
192.168.29.38	Live	135, 139, 445	msrpc, netbios-ssn, Microsoft-ds?

Conclusion :

This exercise gave direct experience with Nmap to find devices on a network and scan them for listening services . Knowing how to footprint a network is imperative in defencive and offensive cyber security operations .