***MN502 Network Security***

# NMap Lab Manual [1]

## **Description:**

After the lab exercises, the students should be able to use NMAP in command line to scan a host/network, so to find out the possible vulnerable points in the hosts. You should be using the Kali Linux on VM.

**Pre-work:**

1. **Launch Virtual Box**
2. **Launch your Kali Linux VM**
3. **Do all your exercises in the VM**

## **NMAP - the Network MAPper**

Nmap is the scanning tool that provides the ability to crack a computer system by finding a target machine vulnerable to attacks. Intruders can scan for UDP and TCP listening ports and can design their attacks accordingly. Our lab exercise will focus on using Nmap in the **command-line**.

## How to use NMAP?

Nmap is a simple tool to use and is accessed via command line. Usage syntax is:

Nmap –sflag IP-address/network address

Flag are according to the purpose, for example:

Icmp ping                     # nmap -sP 172.16.63.0/24

tcp ping                        # nmap -sP -PT80 172.16.63.0/24

TCP connect                # nmap -sT 172.16.63.n

Stealth Scanning           # nmap -sS 172.16.63.n

UDP Scanning             # nmap -sU 172.16.63.n

Stealth FIN                  # nmap -sF 172.16.63.n

**(n is the host number)**

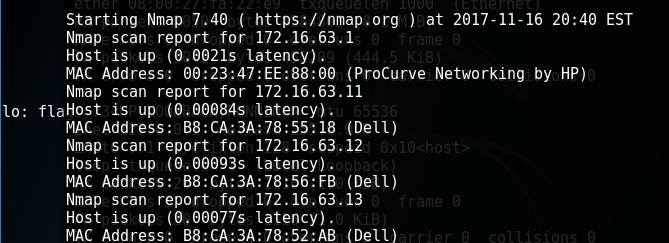
To run most commands in Nmap, root privileges are required.

## **Task 1: Ping Sweeping: To check what hosts are UP**

Ping sweeping can be used with option of ”-sP” for finding all the running hosts in the network. The network address and the subnet mask need to be given. Nmap sends an ICMP echo and a TCP ACK to each host it scans. Hosts that respond to either are considered to be up.

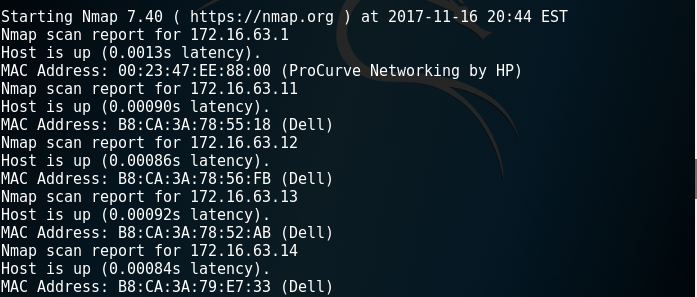
**You need to use ifconfig on the terminal to find your host address and then use that to figure out your network address.**

**Example output is shown in the following figure for port scanning using Nmap:**



TCP ping sweep with flag of “-sP –PT” can be used to check the hosts responding to TCP connection request and to find out the running hosts as some hosts may not reply back to ICMP messages.

**Example output is shown in the following figure for port scanning with TCP using Nmap:**



Once intruder knows which machines on a network are up, ususlly the next step is port scanning.

Text

Description automatically generated

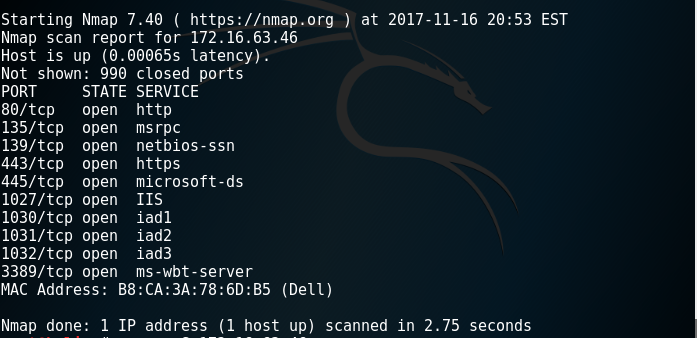
## **Task 2: Port Scanning**

Different types of port scans are provided by Nmap: TCP connect, TCP SYN, Stealth FIN, UDP scans.

TCP connect

One form of port scanning is TCP connect which uses the connect() system call to open connections to interesting ports on the target host and complete the 3-way TCP handshake. An important issue is that the probe is easily detected by the target host. "-sT" flag is used for this purpose.

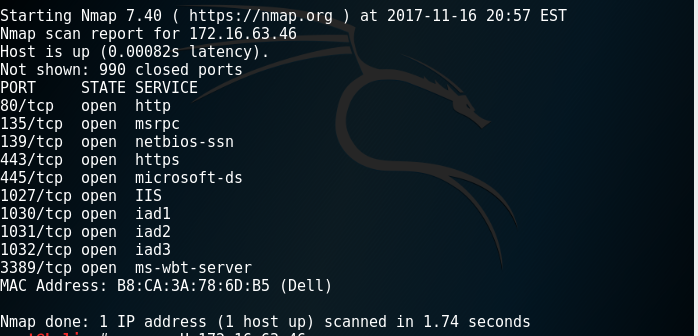
**Example output is shown in the following figure for TCP connect port scanning using Nmap:**



Stealth Scanning

When attacker does not want to be logged in at the target system while port scanning then the best option is to use Stealth Scanning. TCP SYN scans are less prone to logging on the target's machine, because a full handshake never completes. A SYN scan starts by sending a SYN packet, which is the first packet in TCP negotiation. Any open ports will respond with a SYN|ACK, as they should. However, the attacker sends a RST instead of an ACK, which terminates the connection. The "-sS" flag will launch a SYN scan against a host or network.

**Example output is shown in the following figure for Stealth scanning using Nmap:**



UDP Scanning

Using the UDP scan "-sU" a 0-byte UDP packet is sent to each port for finding open UDP ports. If the port is closed the host will return an ICMP error message. This task may take long time, if it won’t finish in 5-6 minutes cancel it using Ctrl+C

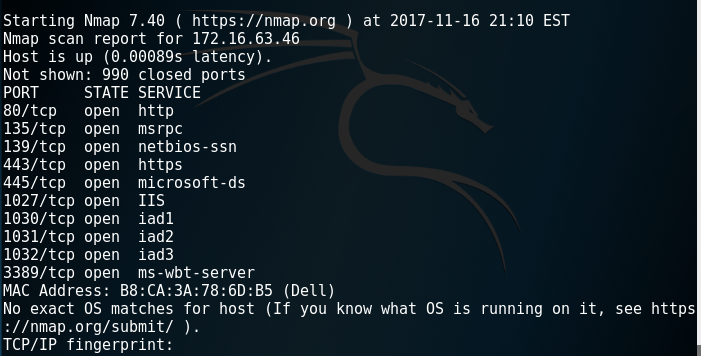
Text

Description automatically generated

## **Task 3: OS Fingerprinting: Which OS is running on the host?**

Finding the operating system of the target host is a simple task with Nmap using “-sS -O” flag. This information can be used to customize attacks based on the vulnerability of each OS. This has to be combined with a port scan and not a ping scan. Nmap accomplishes this by sending different types of probes to the host, which will narrow the target operating system. Fingerprinting the TCP stack includes such techniques as FIN probing to see what kind of response the target has, BOGUS flag probing to see the remote host's reaction to undefined flags sent with a SYN packet, TCP Initial Sequence Number (ISN) sampling to find patterns of ISN numbers, as well as other methods of determining the remote operating system.

**Example output is shown in the following figure for OS scanning using Nmap:**



For a complete list of the options for Nmap, you can see the manual of the NMAP in website <http://www.insecure.org/nmap>. Also “**man nmap”** provides complete list of options for nmap.

Graphical user interface, text

Description automatically generated

**Laboratory 1**: Introduction to Security 1

**Description of the laboratory exercise**:

In this laboratory, student will analyse a security tool (Nmap on Kali Linux), and also analyse and discuss common threats/attacks and mitigation techniques for networked information systems. Student needs to complete the exercises in the manual and do the following tasks related to Nmap tool in Kali

**Lab Exercise:**

After completing the exercises in manual (which is based on Kali Linux running on Virtual Box), answer the following questions.

1. From your observations how many hosts are running in LAN? Please list IP addresses of at least five running hosts.

Text

Description automatically generated

1. For the five identified running hosts in question 1, which services (TCP and UDP) are open on those machines?

Graphical user interface, text

Description automatically generated

1. Can you determine the Operating system and its possible version that is running on those five machines?

Text

Description automatically generated

**Analysis 1:** **From your experience with Nmap** discuss and analyse the potential security threats we all face while connected in the network.

**Scanning devices with anti virus technologies may be blocked and not be able to be scanned with Nmap.**

**Analysis 2:** Propose suitable risk mitigation techniques for the threats identified in the previous part.

**Risk identification, Risk Impact Assessment, Risk Tracking and Risk Prioritization Analysis**

# References

|  |  |
| --- | --- |
| [1] | “NMap Lab Exercise,” [Online]. Available: https://discovery.csc.ncsu.edu/Courses/csc474-S05/lab/Lab-nmap.html. [Accessed 17 November 2017]. |
| [2] | “Nmap Manual,” [Online]. Available: https://nmap.org/book/man.html. [Accessed 17 November 2017]. |