**Lab Experiment 08**

**B. Tech CSF-CSE Semester III Course: Physical and IT Security**

**By: Dr. Gopal Singh Rawat**

**Lab Objective: Learn Network Scanning Tool - NMAP**

**Tools:**

* **NMAP**

Network Mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. Nmap is not limited to merely gathering information and enumeration, but it is also powerful utility that can be used as a vulnerability detector or a security scanner. So Nmap is a multipurpose tool, and it can be run on many different operating systems including Windows, Linux, BSD, and Mac. Nmap is a very powerful utility that can be used to:

* Detect the live host on the network (host discovery)
* Detect the open ports on the host (port discovery or enumeration)
* Detect the software and the version to the respective port (service discovery)
* Detect the operating system, hardware address, and the software version
* Detect the vulnerability and security holes (Nmap scripts)

**Steps to perform:**

1. **Check for systems and discover:**
   1. **To know my own IP Address and Network Segment: # ifconfig**
   2. **To discover others: # netdiscover –r IP/Segment**
   3. **Use this for NMAP Scanning: http://scanme.nmap.org/**
2. Scan single IP / One Target

**NMAP Target # nmap target.com # nmap 192.168.1.1**

1. Scan the entire subnet

**NMAP Target/cdir # nmap 192.168.1.1/24**

1. Scan multiple targets 🡪 separate each target via space:

**nmap target target1 target2 # nmap 192.168.1.1 192.168.1.8**

1. To scan the entire subnet but not a specific IP addresses because it might be dangerous OR that might be an IDS, then use the Nmap command with the excluding parameter:

**# nmap 192.168.1.1/24 – -exclude 192.168.1.1**

1. Scan specific port(s) on the target machines (e.g. HTTP, FTP, and Telnet port only)

**# nmap -p80,21,23 192.168.1.1 It scan the target for port number 80,21 and 23.**

**Nmap Scanning Techniques:**

### **TCP SYN Scan (-sS) 🡪** It is a basic scan, and it is also called half-open scanning because this technique allows Nmap to get information from the remote host without the complete TCP handshake process, Nmap sends SYN packets to the destination, but it does not create any sessions, As a result, the target computer can’t create any log of the interaction because no session was initiated, making this feature an advantage of the TCP SYN scan.

**# nmap -sS 192.168.1.1**

* **TCP connect() scan (-sT) 🡪** This the default scanning technique used, if and only if the SYN scan is not an option, because the SYN scan requires root privilege. Unlike the TCP SYN scan, it completes the normal TCP three way handshake process and requires the system to call connect(), which is a part of the operating system. Keep in mind that this technique is only applicable to find out the TCP ports, not the UDP ports.

**# nmap -sT 192.168.1.1**

### **UDP Scan (-sU) 🡪** this technique is used to find an open UDP port of the target machine. It does not require any SYN packet to be sent because it is targeting the UDP ports. But we can make the scanning more effective by using -sS along with –sU. UDP scans send the UDP packets to the target machine, and waits for a response—if an error message arrives saying the ICMP is unreachable, then it means that the port is closed; but if it gets an appropriate response, then it means that the port is open. **# nmap -sU 192.168.1.1**

### **FIN Scan (-sF) 🡪** Sometimes a normal TCP SYN scan is not the best solution because of the firewall. IDS and IPS scans might be deployed on the target machine, but a firewall will usually block the SYN packets. A FIN scan sends the packet only set with a FIN flag, so it is not required to complete the TCP handshaking.

### **# nmap -sF 192.168.1.8**

### **Ping Scan (-sP) 🡪** Ping scanning is unlike the other scan techniques because it is only used to find out whether the host is alive or not, it is not used to discover open ports. Ping scans require root access s ICMP packets can be sent, but if the user does not have administrator privilege, then the ping scan uses connect() call.

### **# nmap -sP 192.168.1.1**

### **Version Detection (-sV) 🡪** Version detection is the right technique that is used to find out what software version is running on the target computer and on the respective ports. It is unlike the other scanning techniques because it is not used to detect the open ports, but it requires the information from open ports to detect the software version. In the first step of this scan technique, version detection uses the TCP SYN scan to find out which ports are open.

### **# nmap -sV 192.168.1.1**

### **Idle Scan (-sI) 🡪** Idle scan is an advance scan that provides complete anonymity while scanning. In idle scan, Nmap doesn’t send the packets from your real IP address—instead of generating the packets from the attacker machine, Nmap uses another host from the target network to send the packets. Let’s consider an example to understand the concept of idle scan:

### **# nmap -sI zombie\_host target\_host**

### **# nmap -sI 192.168.1.6 192.168.1.1**

**Lab #08 File Activity:**

Perform this experiment on Kali Linux & check info for at least five different targets and report the findings for

* [**Webscantest**](file:///D:\Courses%20to%20teach\Semester%202021%2001-06\Sem%204%20-%20B3-B4%20-%20CSSF2108%20-%20IT%20Network%20Security%20Lab%20-%201%20Credit\Lab%20Experiments\webscantest.com)**.com**
* [**https://www.scanme.nmap.org**](https://www.scanme.nmap.org)
* [**http://www.itsecgames.com**](http://www.itsecgames.com/)
* [**ftp://speedtest.tele2.net/**](ftp://speedtest.tele2.net/)
* [**ftp://test.rebex.net**](ftp://test.rebex.net)
* [**ftp://ftp.swfwmd.state.fl.us**](ftp://ftp.swfwmd.state.fl.us) **(Login: Anonymous / Password: Email ID)**
* **NMAP Full Scan: # nmap scanme.nmap.org**
* **TCP Scan: # nmap –sT scanme.nmap.org**
* **UDP Scan: # nmap –sU scanme.nmap.org**
* **Half Scan: # nmap –sS scanme.nmap.org**
* **XMAS Scan: # nmap –sX scanme.nmap.org**
* **FIN Scan: # nmap –sF scanme.nmap.org**
* **ACK Scan: # nmap –sA scanme.nmap.org**
* **Version Scan: # nmap –sV scanme.nmap.org**
* **Aggressive Scan: # nmap –A scanme.nmap.org**

This should not be used in the real world for scanning as it generates a lot of noise/logs and detects the scan.

* **Firewalk scan: # nmap isl Target\_Firewall**

This gives rules of Firewall for further attack planning