Experiment 2: Nmap tool

Aim: To Install and use NMAP to for gathering information.

Learning Outcomes:
After completion of this experiment, student should be able to

1. Perform port scanning
2. Identify services running on the target system
3. Identify OS available of the target system.

Theory:

Nmap is a security scanner 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. The software provides a number of features for probing computer networks, including host discovery and service and operating system detection. Nmap is a free open source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, IP address detection, and operating system detection. Nmap has the benefit of scanning of large number of machines in a single session. It's supported by many operating systems, including Unix, Windows, and Linux.

Setup:
To perform this lab, you will need two host systems. One system will be running nmap where as other system will be running wireshark for capturing packet.

Procedure:

1. Open virtual box.
2. Start SEEDUbuntu1 VM.
3. Start SEEDUbuntu2 VM.
4. Note the IP of SEEDUbuntu1 and 2 using *ifconfig* command.
5. Verify the connectivity between SEEDUbuntu1 and 2 using *ping* command.
6. Verify installation of nmap on SEEDUbuntu1 VM.
7. Verify installation of wireshark on SEEDUbuntu2 VM.
8. Start packet capturing using wireshark on SEEDUbuntu2 VM.
9. Execute following nmap commands and document the output.

Description	Nmap command	Output
Scan a single IP	nmap 192.168.1.1	
Scan a host	nmap www.testhostname.com	
Scan a range of IPs	nmap 192.168.1.1-20	
Scan a subnet	nmap 192.168.1.0/24	

Scan targets from a text file	nmap -iL list-of-ips.txt	
Scan a single Port	nmap -p 22 192.168.1.1	
Scan a range of ports	nmap -p 1-100 192.168.1.1	
Scan 100 most common ports (Fast)	nmap -F 192.168.1.1	
Scan all 65535 ports	nmap -p- 192.168.1.1	
Scan a single Port	nmap -p 22 192.168.1.1	
Note: Replace IP address with that of SEEDUbuntu 2 VM		

10. Perform port scanning using various types of scanning techniques as mentioned in the table below:
    a. Before start of any scan, do the following:
        i. Start packet capturing on SEEDUbuntu2 VM
        ii. Set filter to ip.addr= = SEEDUbuntu1 VM IP
        iii. Execute nmap commands on SEEDUbuntu1 VM
        iv. Follow TCP stream for at least one open port and one closed port in each case and note the flag status.

Scanning technique	Command	Output
Scan using TCP connect	nmap -sT 192.168.1.1	
Scan using TCP SYN scan (default)	nmap -sS 192.168.1.1	
Scan UDP ports	nmap -sU -p 123,161,162 192.168.1.1	
Scan using FIN flag	nmap –sF 192.168.1.1	
Null Scan	nmap –sN 192.168.1.1	
XMAS scan	nmap –sX 192.168.1.1	
Ping Scan	nmap –sP 192.168.1.1	
ACK scan	nmap –sA 192.168.1.1	
Scan selected ports - ignore discovery	nmap -Pn -F 192.168.1.1	
Note: Replace IP address with that of SEEDUbuntu 2 VM		

11. Perform the above mentioned scan on your host machine and note the difference in output.
12. Execute following commands for OS detection.

Command	Output
nmap -O -v 192.168.1.1	
nmap -sV –O -v 192.168.1.1	
nmap -A 192.168.1.1	

13. Interpret the result. (Refer online documentation at http://nmap.org/docs.html)
14. Identify which ports are open
15. Identify various services available on open ports.

16. Identify OS installed on the target system
17. Document your result.

Review question:

1. What is the difference between open, filtered and unfiltered port?
2. What are the different scans possible with Nmap?
3. Explain NSE script with an example.