Lab-04

1. **As a member of Blue team experts in Monitoring and Technical Support of a medium sized company, you have been asked to assess the security posture of the internal network. Use Nmap for network discovery, Port scanning, Service version detection and vulnerability detection. Then Document your findings, including the identified vulnerabilities, their severity levels.**

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

Nmap Scanning:

• Open Kali Linux and the Metasploitable2 virtual machine. • Obtain

the IP address of the target machine (Metasploitable2 VM). • Open

the terminal in Kali Linux.

• Perform scanning using the following commands with nmap:

1. nmap 192.168.62.129

2. sudo nmap -v 192.168.62.129—(v-verbose-detailed output)

3. man nmap

4. nmap -V 192.168.62.129—(V-version)

5. nmap 192.168.62.129 192.168.62.130

6. nmap 192.168.62.0/24 --exclude 192.168.62.130

7. nmap --open 192.168.62.129(showing only the open ports)

8. nmap -A 192.168.62.129(Aggressive scan)

9. nmap -sA 192.168.62.129(The packets sent to target machine are getting

filtered or not)

10.nmap -p 80 192.168.62.129(Port 80)

11.nmap --packet-trace 192.168.62.129 ((Complete tracing of packets)

12.nmap --top-ports 10 192.168.62.129

OS Detection:-

• nmap -O 192.168.62.129

• nmap -v -O 192.168.62.129—revealing additional info.. •

nmap -O --osscan-guess 192.168.62.129(proposed option)

Service Detection:-

• nmap -sV -O 192.168.62.129

• Nmap -sV --version-trace 192.168.62.129

Advanced Scan:-

• nmap -sS 192.168.62.130 (TCP Syn Scanning)

• nmap -sT 192.168.62.129 (TCP Connect scan)

• nmap -sU 192.168.62.129(UDP scans..)

• sudo nmap -sN 192.168.62.129(TCP null Sync scan)

• sudo nmap -sF 192.168.62.129(TCP FIN scan—Setting the FIN bit)

Custom scan:-

nmap -sS --scanflags SYNFIN -T4 www.google.com

nmap -sO 192.168.62.129(IP protocol scan)

Send Ethernet packets:

nmap --send-eth 192.168.62.129

Send IP packets

nmap --send-ip 192.168.62.129