Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 04

Aim: To use nmap for network discovery and security auditing

Theory :

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) 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. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up ordown and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

• **Host Discovery –** Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
• **Port Scanning –** Enumerating the open ports on one or more target hosts.
• **Version Detection –** Interrogating listening network services listening on remote devices to determine the application name and version number.
• **OS Detection –** Remotely determining the operating system and some hardware characteristics of network devices.

The usage of Nmap depends on the target machine because there is a difference between simple (basic) scanning and advance scanning. There is need to use some advanced techniques to bypass the firewall and intrusion detection/preventative software to get the right result.

Table 1: Scanning Techniques

Scanning Technique	Syntax	Use
TCP SYN	-sS	Stealth scan
TCP connect()	-sT	Scan without root privileges
FIN	-sF	Stealth scan
Xmas	-sX	Stealth scan
Null	-sN	Stealth scan
Ping	-sP	Identify live hosts
Version Detection	-sV	Identify services
UDP	-sU	Find UDP services
IP Protocol	-sO	Discover supported protocols
ACK	-sA	Identify firewalls
Window	-sW	Advanced ACK scan
RPC	-sR	Information on RPC services
List	-sL	Dummy for test purposes
Idle	-sI	Scan via third party
FTP Bounce	-b	Historic

Scan Type	Syntax	Example
TCP SYN Scan	-sS	nmap –sS 10.20.3.100
TCP Connect Scan	-sT	nmap –sT 10.20.3.100
Fin Scan	-sF	nmap –sF 10.20.3.100
XMAS Scan	-sX	nmap –sX 10.20.3.100
Null Scan	-sN	nmap –sN 10.20.3.100
Ping Scan	-sP	nmap –sP 10.20.3.100
Version Detection	-sV	nmap –sV 10.20.3.100
UDP Scan	-sU	nmap –sU 10.20.3.100
IP Protocol Scan	-sO	nmap –sO 10.20.3.100
ACK Scan	-sA	nmap –sA 10.20.3.100
Windows Scan	-sW	nmap –sW 10.20.3.100
List Scan	-sL	nmap –sL 10.20.3.100

OS Detection by using Nmap :

One of the most important feature that Nmap has is the ability to detect remote operating systems and software. It is very helpful during a penetration test to know about the operating system and the software used by the remote computer because you can easily predict the known vulnerabilities from this information.

The Nmap operating system discovery technique is slightly slower then the scanning techniques because OS detection involves the process of finding open ports.
Nmap OS fingerprinting technique discovers the:
•Device type (router, work station, and so on)
•Running (running operating system)
•OS details (the name and the version of OS)
•Network distance (the distance in hops between the target and attacker)

Conclusion: Nmap has ability to cover the very first aspects of penetration testing, which include information gathering and enumeration. It is also powerful utility that can be used as a vulnerability detector or a security scanner.