USE OF NMAP

Nmap: Nmap is a tool used to discover hosts and services an a computer network by sending packets and analysing the responses. Also called as “Swiss Army Knife” for Network scanning.

Host discovery

Port Scanning

Service detection

OS Detection

Vulnerability Scanning

To scan a single host

**nmap 192.168.xx.xx**

To scan a range of Ips

**nmap 192.168.1.1-50**

To detect Services and OS

**nmap -sV -O 192.168.x.x**

COMMON NMAP SCAN TYPES

-sT = TCP connect (simple, but noisy)

-sS = SYN scan (fast + stealthy, default)

-sU = UDP scan (for UDP services)

-sF, -sX, -sN = stealth scans (bypass some firewalls)

-sn = host discovery

-sV, -O, NSE = advanced service/OS/vulnerability detection

A screenshot of a computer

AI-generated content may be incorrect.

Here the packet transferring through the own device means the connection is good, By using ping command we can check the speed of the packet, TTL (Time to live).

Here by using the nmap is network mapping used to check which ports are open, which services are running including OS information sometimes.

The Wireshark will capture all the packets with port numbers and destination ports.

We can filter and identify the packets.

