NETWORK SCANNER

UNDERSTANDING VULNERABILITIES WITH NMAP

PRESENTED BY:

PATTAPU KUSHWANTH

UNDER THE GUIDANCE OF:

ANANYA MAM

OBJECTIVE

- The objective of this project is to use Nmap (Network Mapper) on Kali Linux to scan a controlled test network and collect information about:
  - ✓ Open ports and services
  - ✓ Service/Versions Detection
  - ✓ Operating system detection
- This exercise helps demonstrate practical skills in network discovery and foot printing in a safe, legal lab environment.
- Gain hands-on experience in Linux-based penetration testing environment.

TOOLS & ENVIRONMENT

- **VMware Workstation Pro** (host): VMware Workstation Pro is a desktop (Type-2) hypervisor that runs on your host OS (Windows or Linux) and lets you create, run, snapshot, and manage multiple virtual machines (VMs) on the same physical computer.
- **Kali Linux** (guest): Kali Linux is a Debian-based operating system designed for cybersecurity professionals and ethical hackers. It comes preloaded with powerful tools and widely used for learning and performing real-world security assessments.
- **Target VMs / Devices**: Own Device (Laptop)

STEP-BY-STEP PROCEDURE

1. Configure VMware network to Host-Only or NAT to create an isolated lab network.

2.Open Kali Linux inside VMware Workstation 17 Pro.

2. Find the target IP address of the target.

3. Use Nmap commands to perform different types of scans:

- ✓ Basic Scan: nmap <target IP>
- ✓ Service Version Detection: nmap –sV <target IP>
- ✓ Operating System Detection: nmap –O <target IP>

4. Take screenshots of each scan result.

5. And analyse them.

Safety and legal reminder: Only scan networks and devices for which you have explicit permission. Use an isolated lab.

COMMANDS USED

- **BASIC SCAN:**
  - **Command:** nmap 192.168.199.1

  What it does: This is the basic scan command. It scans the common TCP ports on the target IP to see which ports are open, closed, or filtered. Gives a quick overview of what services might be running on the device.

- **SERVICE/VERSION DETECTION:**
  - **Command:** nmap –sV 192.168.199.1

  What it does: Attempts to determine service name and version running on open ports.

COMMANDS USED

- **OS DETECTION:**

  Command: nmap –O 192.168.199.1

What it does: It uses TCP/IP fingerprinting to guess the target's operating system and device type (server, router, printer, etc.) by analyzing subtle differences in network responses.

RESULT & ANALYSIS

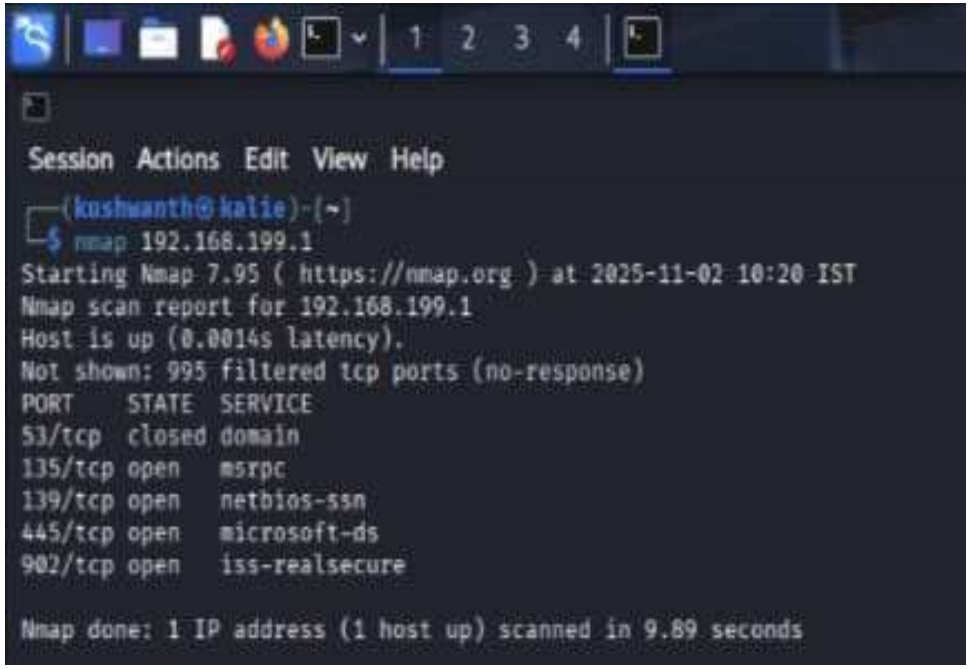
- **BASIC SCAN:**

  Command: nmap 192.168.199.1

Analysis:

This is a basic Nmap network scan.
It sends packets to the target IP (192.168.199.1) to identify:

- Which ports are open or closed
- What services are running on those ports
- Whether the host is reachable
- No advanced detection is performed (like OS or version), just a port scan.



RESULT & ANALYSIS

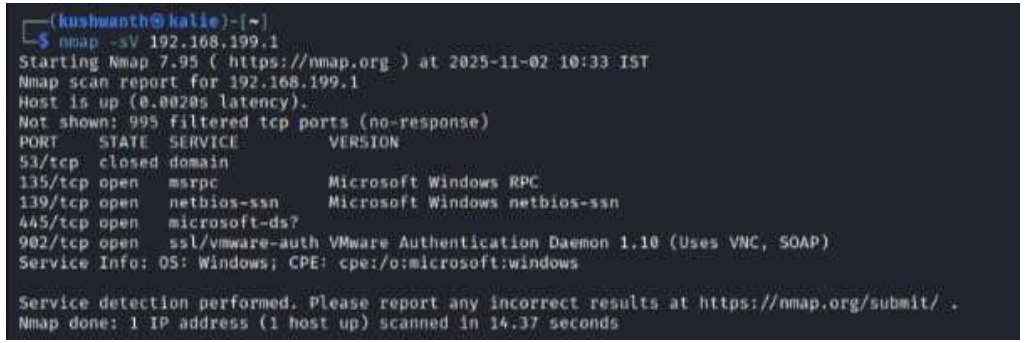
- **SERVICE/VERSION DETECTION:**

  Command: nmap 192.168.199.1

Analysis:

This tells Nmap to:

- Scan the target for open ports.
- Detect the services running on those ports.
- Identify the software version of each detected service.



RESULT & ANALYSIS

- **OS DETECTION:**

  Command: nmap –O 192.168.199.1

Analysis:

- The image displays the results of an Nmap network scan performed on the IP address 192.168.199.1.
- The scan indicates that the host is online.
- The highest confidence guess (98%) suggests the target is running "Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012".

CONCLUSION

- The Nmap scans successfully identified active hosts and open ports within the network. The target system (192.168.199.1) was found to be running Windows services such as Microsoft RPC, NetBIOS, and SMB, along with VMware authentication ports, indicating it is a virtualized Windows environment.
- Through OS detection and service version scanning, detailed insights were gathered about the system configuration and network behavior. Most other ports were filtered, suggesting the presence of firewall or security filtering mechanisms.
- Overall, this project demonstrated how Nmap can be effectively used for network exploration, device identification, and vulnerability assessment, highlighting its importance in network security auditing and penetration testing.

THANK YOU