

Network Scanning Report

1. Objective

The main objective of this practical is to perform network scanning to identify active devices, open ports, and vulnerabilities in a network.

2. Tools Used

- Nmap (Network Mapper)
- Wireshark
- Zenmap
- Operating System: Windows/Linux

3. Methodology

Step 1: Identify IP address using ipconfig or ifconfig.

Step 2: Ping Scan using command: `nmap -sn 192.168.1.0/24`

Step 3: Port Scan using command: `nmap 192.168.1.1`

Step 4: Service Version Detection: `nmap -sV 192.168.1.1`

Step 5: OS Detection: `nmap -O 192.168.1.1`

4. Observations

- Active devices detected in network
- Open ports such as 80, 443, 22 found
- Services and OS detected successfully

5. Security Risks

- Open ports can be exploited
- Outdated services may have vulnerabilities
- Unauthorized access possible

6. Recommendations

- Close unused ports
- Enable firewall
- Update system regularly
- Monitor network traffic

7. Conclusion

Network scanning helps identify devices, ports, and vulnerabilities. Regular scanning improves security and protects systems from attacks.