Mini Project Report

# Project Title: Network Scanner using Nmap in PowerShell

This mini project demonstrates how to perform basic network reconnaissance by scanning for active hosts and identifying open ports in a local network using Nmap and PowerShell.

## Tools Used

- Nmap  
- Windows PowerShell  
- Local Network

## Project Steps

### 1. Ping Scan for Live Hosts

Command used:

nmap -sn 192.168.170.0/24

Sample Output:

Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-21 17:19 +0530  
Nmap scan report for 192.168.170.218  
Host is up.  
Nmap done: 1 IP address (1 host up) scanned in 2.27 seconds

### 2. Save Live Hosts to File

Command used:

nmap -sn 192.168.170.0/24 | Select-String "Nmap scan report for" | ForEach-Object { ($\_ -split " ")[-1] } > live\_hosts.txt

### 3. Scan Open Ports on Live Hosts

Command used:

Get-Content live\_hosts.txt | ForEach-Object { nmap -p 1-1000 $\_ }

Sample Output:

Nmap scan report for 192.168.170.218  
Host is up (0.0014s latency).  
Not shown: 995 closed tcp ports (reset)  
PORT STATE SERVICE  
80/tcp open http  
135/tcp open msrpc  
137/tcp filtered netbios-ns  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds

## Conclusion

This project successfully demonstrated how to detect live systems and scan their open ports on a local network. Such tools are fundamental in cybersecurity for identifying potential vulnerabilities.