



SCAN YOUR LOCAL NETWORK FOR OPEN PORTS

Learn to discover open ports on devices in your local network to understand network exposure.

01





1. INSTAL NMAP FROM OFFICIAL WEBSITE.

I downloaded the Nmap application from a Google search and successfully installed it on my system.

A screenshot of the Nmap official website's homepage. The page has a dark purple header with the text "Npcap.com - Seclists.org" on the right. Below the header is a navigation bar with buttons for "Site Search", "Reference Guide", "Book", "Docs", and "Zenmap G". A prominent button labeled "Get Nmap 7.98 here" is centered on the page. Below this button is a "News" section containing several news items. One item mentions the release of Npcap 1.00 with performance improvements and bug fixes. Another item discusses the 7-year development of Nmap and its public pre-releases. Other news items mention DEFCON 27, the original Phrack #51 article, the Icons of the Web project, and the use of Nmap in movies like Elysium. At the bottom of the news section, there are links for Nmap 6.40 and 6.25 releases, including NSE scripts, OS detection details, and download links.

02





3. FIND YOUR LOCAL IP RANGE (E.G., 192.168.1.0/24).

To find my local IP address, I opened the Command Prompt from the Start menu, typed “ipconfig”, and got the IPv4 address details.

```
Command Prompt
Microsoft Corporation. All rights reserved.

\Users\ADMIN>"ipconfig"

Windows IP Configuration

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 10:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . .
IPv6 Address . . . . . : 2409:40f2:352:e06d:b56e:4998:f461:8eb4
Temporary IPv6 Address . . . . . : 2409:40f2:352:e06d:e438:84c5:a255:edda
Link-local IPv6 Address . . . . . : fe80::8600:4f7:e313:f8d5%11
IPv4 Address . . . . . : 10.0.0.10
Subnet Mask . . . . . : 255.255.255.0
```





4. RUN: NMAP -SS 192.168.1.0/24 TO PERFORM TCP SYN SCAN.

To perform a TCP SYN scan, I opened the Nmap application and entered the IPv4 address in the target section. Then, in the profile section, I selected 'Intense scan, all TCP ports' and started the scan.

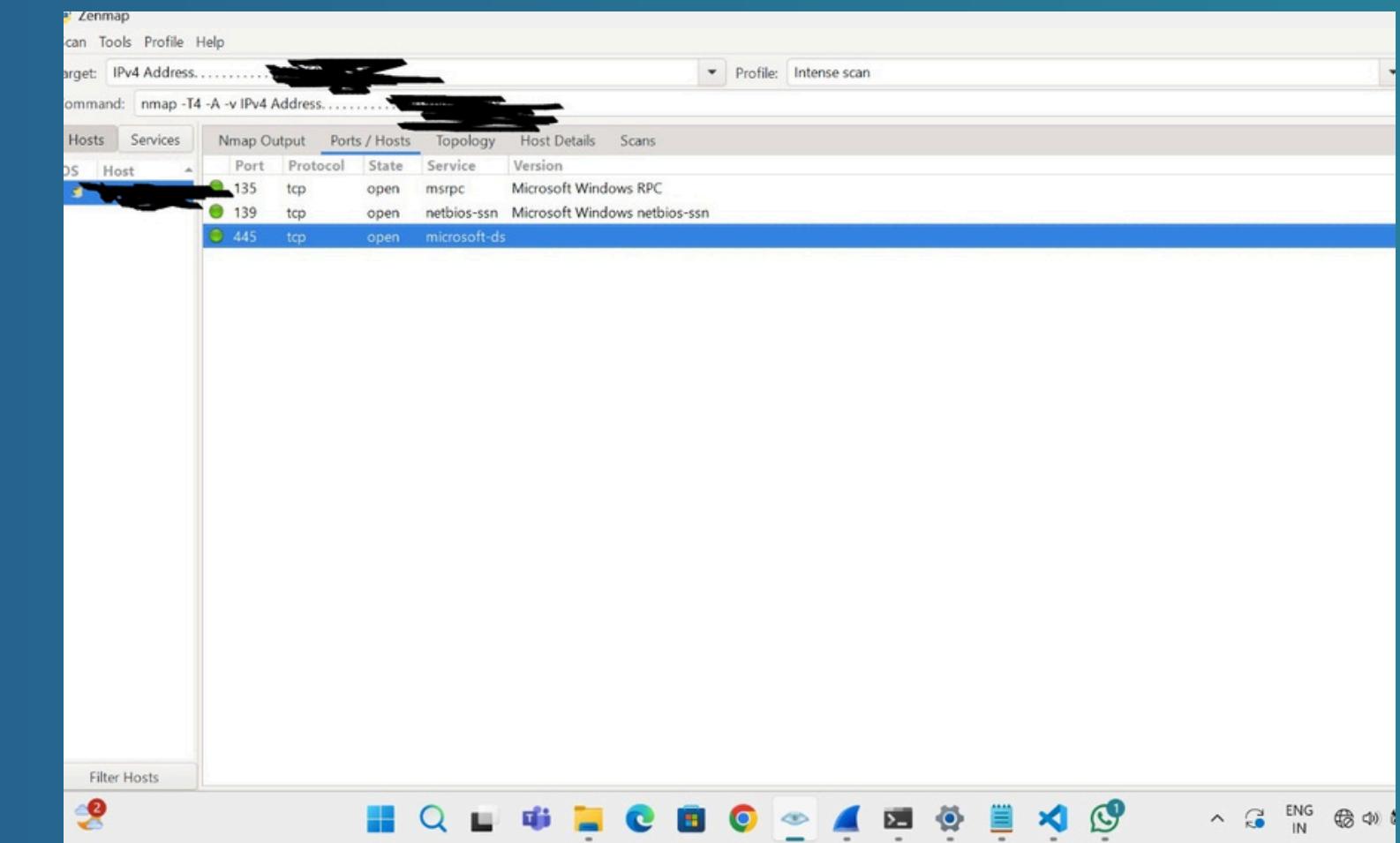
A screenshot of the Nmap application interface. The top bar shows the target as [REDACTED] and the command as nmap -p 1-65535 -T4 -A -v [REDACTED]. The profile is set to 'Intense scan, all TCP ports'. The main window has tabs for Hosts, Services, Nmap Output, Ports / Hosts, Topology, Host Details, and Scans. The Nmap Output tab is active, displaying the scan log. The log shows the start of the scan at 15:50, the loading of 158 scripts, and the initiation of various NSE (Script) scans. It details the discovery of open ports 135/tcp, 139/tcp, 445/tcp, 5357/tcp, and 7070/tcp. The SYN Stealth Scan completes at 15:50. The Service scan finds 5 services (HTTP, Microsoft-DNS, MSRPC, NetBIOS-SSN, and RealServer). The OS detection scan identifies the host as DESKTOP-NM20IAM. The final report states the host is up with 0 latency and 995 closed ports.

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-13 15:50 +0530
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:50
Completed Parallel DNS resolution of 1 host. at 15:50, 2.02s elapsed
Initiating SYN Stealth Scan at 15:50
Scanning DESKTOP-NM20IAM [1000 ports]
Discovered open port 135/tcp on [REDACTED]
Discovered open port 139/tcp on [REDACTED]
Discovered open port 445/tcp on [REDACTED]
Discovered open port 5357/tcp on [REDACTED]
Discovered open port 7070/tcp on [REDACTED]
Completed SYN Stealth Scan at 15:50, 0.16s elapsed (1000 total ports)
Initiating Service scan at 15:50
Scanning 5 services on DESKTOP-NM20IAM [1]
Completed Service scan at 15:50, 11.19s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against DESKTOP-NM20IAM [REDACTED]
NSE: Script scanning [REDACTED]
Initiating NSE at 15:50
Completed NSE at 15:50, 14.23s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.18s elapsed
Initiating NSE at 15:50
Completed NSE at 15:50, 0.00s elapsed
Nmap scan report for DESKTOP-NM20IAM (192.168.1.7)
Host is up (0.00076s latency).
Not shown: 995 closed tcp ports (reset)
```





5. NOTE DOWN IP ADDRESSES AND OPEN PORTS FOUND.



PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	

No exact OS matches for host (If you know what OS is running on the host, edit the OS guess)

TCP/IP fingerprint:





6. RESEARCH COMMON SERVICES RUNNING ON THOSE PORTS.

Port 135/tcp – MSRPC (Microsoft RPC)

- Used for Remote Procedure Calls in Windows.
- Supports services like DCOM, WMI, and remote management.

Port 139/tcp – NetBIOS Session Service

- Used for file sharing and printer sharing on older Windows systems.
- Supports SMB over NetBIOS.





07

6. RESEARCH COMMON SERVICES RUNNING ON THOSE PORTS.

Port 445/tcp – Microsoft-DS (SMB Direct)

- Used by SMB (Server Message Block) protocol.
- Handles:
 - file sharing
 - printer sharing
 - Windows authentication
 - Active Directory communication





7. IDENTIFY POTENTIAL SECURITY RISKS FROM OPEN PORTS.

Port 135 – MSRPC

Risk:

- Frequently targeted for DDoS amplification and remote code execution attacks.
- Historically vulnerable (e.g., MS Blaster worm).

Recommendation:

- Block externally on firewall
- Allow only inside LAN if necessary





7. IDENTIFY POTENTIAL SECURITY RISKS FROM OPEN PORTS.

Port 139 – NetBIOS

Risk:

- Can expose:
 - computer name
 - domain
 - network shares
- Vulnerable to:
 - NBNS poisoning
 - SMB relay attacks

Recommendation:

- Disable if not needed
- Use SMBv2/SMBv3 instead





7. IDENTIFY POTENTIAL SECURITY RISKS FROM OPEN PORTS.

Port 445 – SMB

Risk:

This is one of the most dangerous ports to leave open.

- Used in:
 - WannaCry ransomware
 - EternalBlue exploit
 - SMB relay attacks
 - Unauthorized file access
- Allows attackers to enumerate:
 - shared folders
 - users
 - passwords (via SMB brute force)

Recommendation:

- NEVER expose 445 to the internet
- Apply Windows patches
- Enable SMB signing





11

THANK YOU!

