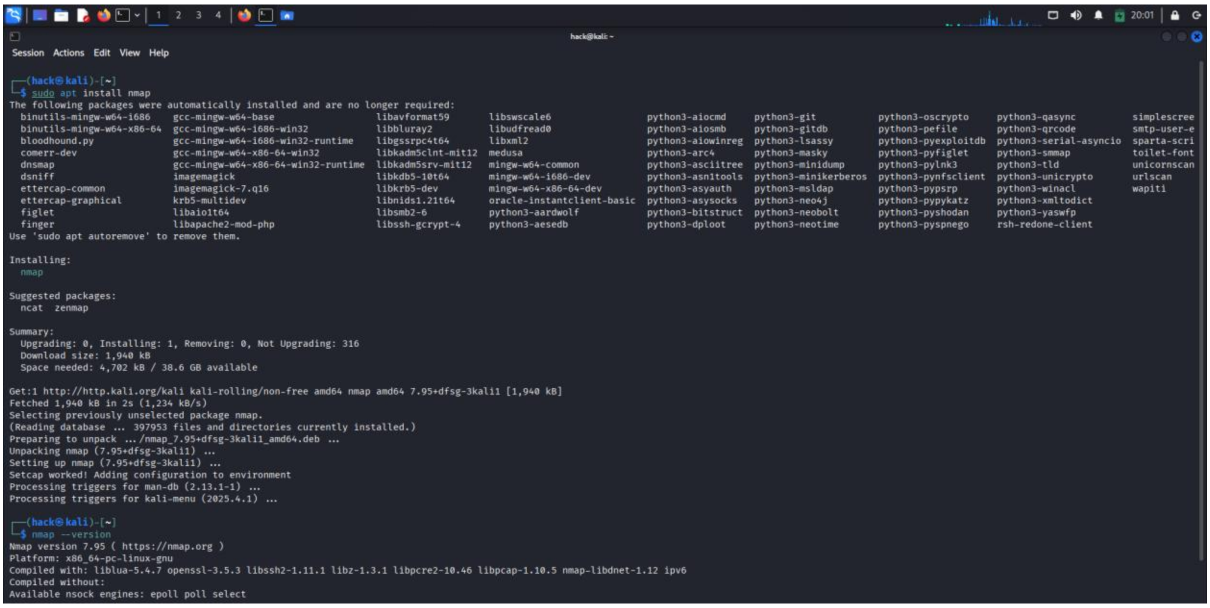
Task 1: Basic Network Scanning with Nmap

Nmap installation:

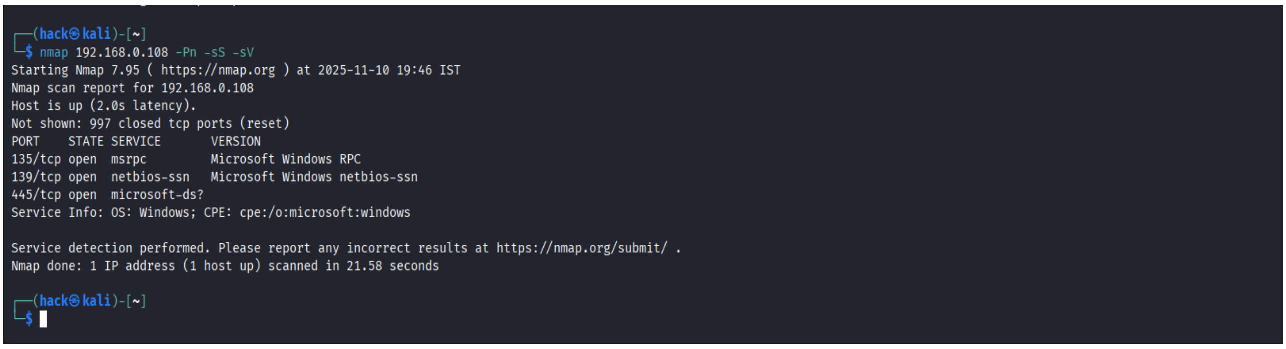
To install Nmap on Kali Linux, first update your package list with ` sudo apt update` , then install Nmap using ` sudo apt install -y nmap` . After installation verify it with ` nmap --version` (or ` sudo nmap --version` to confirm root-capable features). Remember to run scans with ` sudo` for raw SYN scans (e.g. ` sudo nmap -sS <target-ip>`) and only target systems you own or have explicit permission to test.



```
┌──(hack㉿kali)-[~]
└─$ sudo apt install nmap
The following packages were automatically installed and are no longer required:
  binutils-mingw-w64-i686    gcc-mingw-w64-base                  libavformat59       libswscale6                 python3-aiocmd     python3-git           python3-oscrypto     python3-qasync          simplescree
  binutils-mingw-w64-x86-64  gcc-mingw-w64-i686-win32            libbluray2          libudfread0                 python3-aiosmb     python3-gitdb         python3-pefile       python3-qrcode          smtp-user-e
  bloodhound.py              gcc-mingw-w64-i686-win32-runtime    libgssrpc4t64       libxml2                     python3-aiowinreg  python3-lsassy        python3-pyexploitdb  python3-serial-asyncio  sparta-scri
  comerr-dev                 gcc-mingw-w64-x86-64-win32          libkadm5clnt-mit12  medusa                      python3-arc4       python3-masky         python3-pyfiglet     python3-smmap           toilet-font
  dnsmap                     gcc-mingw-w64-x86-64-win32-runtime  libkadm5srv-mit12   mingw-w64-common            python3-asciitree  python3-minidump      python3-pylnk3       python3-tld             unicornscan
  dsniff                     imagemagick                         libkdb5-10t64       mingw-w64-i686-dev          python3-asn1tools  python3-minikerberos  python3-pynfsclient  python3-unicrypto       urlscan
  ettercap-common            imagemagick-7.q16                   libkrb5-dev         mingw-w64-x86-64-dev        python3-asyauth    python3-msldap        python3-pypsrp       python3-winacl          wapiti
  ettercap-graphical         krb5-multidev                       libnids1.21t64      oracle-instantclient-basic  python3-asysocks   python3-neo4j         python3-pypykatz     python3-xmltodict
  figlet                     libaio1t64                          libsmb2-6           python3-aardwolf            python3-bitstruct  python3-neobolt       python3-pyshodan     python3-yaswfp
  finger                     libapache2-mod-php                  libssh-gcrypt-4     python3-aesedb              python3-dploot     python3-neotime       python3-pyspnego     rsh-redone-client
Use 'sudo apt autoremove' to remove them.

Installing:
  nmap

Suggested packages:
  ncat  zenmap

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 316
  Download size: 1,940 kB
  Space needed: 4,702 kB / 38.6 GB available

Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-3kali1 [1,940 kB]
Fetched 1,940 kB in 2s (1,234 kB/s)
Selecting previously unselected package nmap.
(Reading database ... 397953 files and directories currently installed.)
Preparing to unpack .../nmap_7.95+dfsg-3kali1_amd64.deb ...
Unpacking nmap (7.95+dfsg-3kali1) ...
Setting up nmap (7.95+dfsg-3kali1) ...
Setcap worked! Adding configuration to environment
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.1) ...

┌──(hack㉿kali)-[~]
└─$ nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.3 libssh2-1.11.1 libz-1.3.1 libpcre2-10.46 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Nmap Scan:

Nmap scan is the process that is done with the help of the Nmap tool. The Nmap scan is used to scan the open ports in the connected network of the system, for the security purpose.



```
┌──(hack㉿kali)-[~]
└─$ nmap 192.168.0.108 -Pn -sS -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 19:46 IST
Nmap scan report for 192.168.0.108
Host is up (2.0s latency).
Not shown: 997 closed tcp ports (reset)
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?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.58 seconds

┌──(hack㉿kali)-[~]
└─$ 
```

Open Ports & Its definitions:

1) Port 135/tcp (msrpc)

- **Service:** Microsoft RPC (Remote Procedure Call)
- **Purpose:** Used for Microsoft RPC services, which allow programs to execute processes on remote systems.
- **Commonly Found On:** Windows systems
- **Security Note:** Often targeted in attacks due to vulnerabilities in RPC services.

2) Port 139/tcp (netbios-ssn)

- **Service:** NetBIOS Session Service
- **Purpose:** Used for file and printer sharing across a network (NetBIOS over TCP/IP). It enables networked computers to communicate.
- **Commonly Used By:** Windows file and printer sharing
- **Security Note:** Should be blocked from the internet as it may expose sensitive shares.

3) Port 445/tcp (Microsoft-ds)

- **Service:** Microsoft Directory Services (SMB over TCP)
- **Purpose:** Supports file and printer sharing and network browsing. It runs the SMB (Server Message Block) protocol directly over TCP (without NetBIOS).
- **Used By:** Modern Windows networking, Active Directory, file sharing.

- **Security Note:** Frequently targeted by malware (e.g., WannaCry ransomware) and should not be exposed to untrusted networks.

Summary:

All these ports are associated with Microsoft network services and are typically found open on Windows servers. For security, these should not be exposed to the public internet unless strictly necessary, and should be protected by firewalls and proper security configurations.