

Task 1: Scan Your Local Network for Open Ports Objective: Learn to discover open ports on devices in your local network to understand network exposure. Tools: Nmap (free), Wireshark (optional)

STEP 1: open Metasploit and login into it

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:35:8f:b1
          inet addr:192.168.0.105  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe35:8fb1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4938 (4.8 KB)  TX bytes:6968 (6.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

We get Metasploit Ip : 192.168.0.105

Step 2: Install nmap on kali Linux with the command :

Apt install nmap

```
(root@kali)-[/home/kali]
# apt install nmap
nmap is already the newest version (7.95+dfsg-3kali1).
nmap set to manually installed.
The following packages were automatically installed and are no longer required:
crackmapexec      libgfrpc0          libopenh264-7      python3-aioconsole
firebird3.0-common libgfxdr0           libpaper1           python3-appdirs
firebird3.0-common-doc libgl1-mesa-dev     libperl5.38t64      python3-dunamai
fonts-liberation2 libglapi-mesa       libplacebo338       python3-hatch-vcs
freerdp2-x11       libgles-dev        libplist3           python3-hatchling
hydra-gtk          libgles1           libpoppler134       python3-jose
ibverbs-providers libglusterfs0       libpostproc57       python3-lib2to3
icu-devtools       libglvnd-core-dev  libpython3.11-dev   python3-ntlm-auth
```

Step 3 : Nmap command to tcp scan port:

nmap -sT 192.168.0.105

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 11:36 EDT
Nmap scan report for 192.168.0.105
Host is up (0.0060s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
```

This command gives open port state and services use by ports.

Step 4: `nmap service version scan with this command:

`nmap -sV 192.168.0.105`

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 11:45 EDT
Nmap scan report for 192.168.0.105
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
```

This command give services version which is used by host.

Step 5: Os detection scan using nmap:

`nmap -sS -O 192.168.0.105`

```
(root@kali)-[/home/kali]
# nmap -sS -O 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 11:50 EDT
Nmap scan report for 192.168.0.105
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
```

```
File Actions Edit View Help
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
1099/tcp   open  rmiregistry
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2121/tcp   open  ccproxy-ftp
3306/tcp   open  mysql
5432/tcp   open  postgresql
5900/tcp   open  vnc
6000/tcp   open  X11
6667/tcp   open  irc
8009/tcp   open  ajp13
8180/tcp   open  unknown
MAC Address: 08:00:27:35:8F:B1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds
```

This scan also detect host os.

Step 6: all port scan using nmap:

`nmap -sS -p- 192.168.0.105`

```
(root@kali)-[/home/kali]
# nmap -sS -p- 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 11:57 EDT
Nmap scan report for 192.168.0.105
Host is up (0.00080s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp   open  rmiregistry
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2121/tcp   open  ccproxy-ftp
3306/tcp   open  mysql
3632/tcp   open  distccd
5432/tcp   open  postgresql
```

This scan all port of the host system and provide details.

Step 7: specific port scan of victim :

`nmap -sS -p21,80,445, 100-1000, 192.168.0.105`

(here 21,80, 445 are port number and 100-1000 is the range we have given)

```
(root@kali)-[/home/kali]
# nmap -sS -p21,80,445,100-1000, 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 12:05 EDT
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt
Nmap scan report for 192.168.0.105
Host is up (0.00044s latency).
Not shown: 895 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
MAC Address: 08:00:27:35:8F:B1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
```

Step8: default script scan:

nmap -sC 192.168.0.105

```
(root@kali)-[/home/kali]
# nmap -sC 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 12:07 EDT
Nmap scan report for 192.168.0.105
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.0.106
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh
|_ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet
```

Step 9: Aggressive scan (which include services, os and default scripting scan)

nmap -A 192.168.0.105



```
(root@kali) - [/home/kali]
# nmap -A 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 12:14 EDT
Nmap scan report for 192.168.0.105
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.0.106
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
| End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
```

```
File Actions Edit View Help
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|   program version  port/proto  service
|   100000  2             111/tcp     rpcbind
|   100000  2             111/udp     rpcbind
|   100003  2,3,4         2049/tcp    nfs
|   100003  2,3,4         2049/udp    nfs
|   100005  1,2,3         43320/tcp   mountd
|   100005  1,2,3         58691/udp   mountd
|   100021  1,3,4         42298/tcp   nlockmgr
|   100021  1,3,4         45489/udp   nlockmgr
|   100024  1             41173/tcp   status
|   100024  1             59746/udp   status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
```

```
Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2025-07-05T12:15:37-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h01m04s, deviation: 2h00m00s, median: 1m04s

TRACEROUTE
HOP RTT ADDRESS
1 1.52 ms 192.168.0.105

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.46 seconds
```

Key learning: how to scan vulnerabilities using Nmap different scan