

# Penetration Testing Lab Using Nmap

**Tool Used:** Nmap

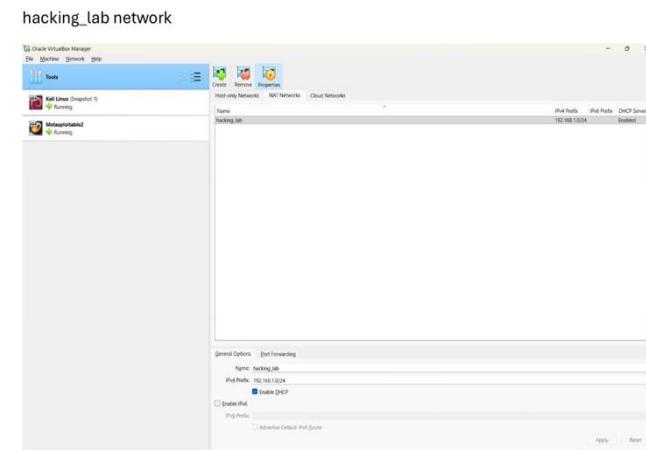
**Environment:** Kali Linux (Attacker) & Metasploitable2 (Target)

**Host OS:** Windows

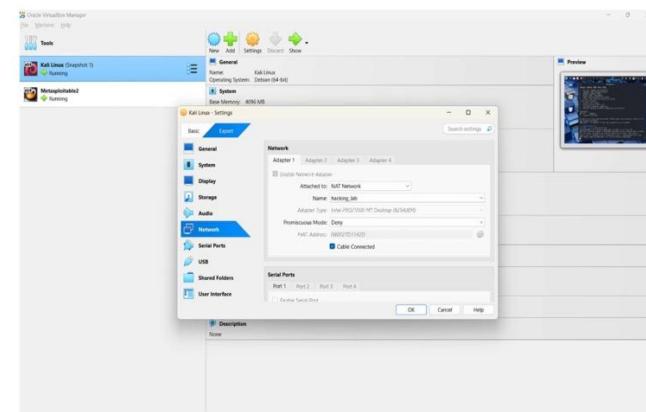
**Virtualization Tool:** VirtualBox

## Step 1: Lab Environment Setup

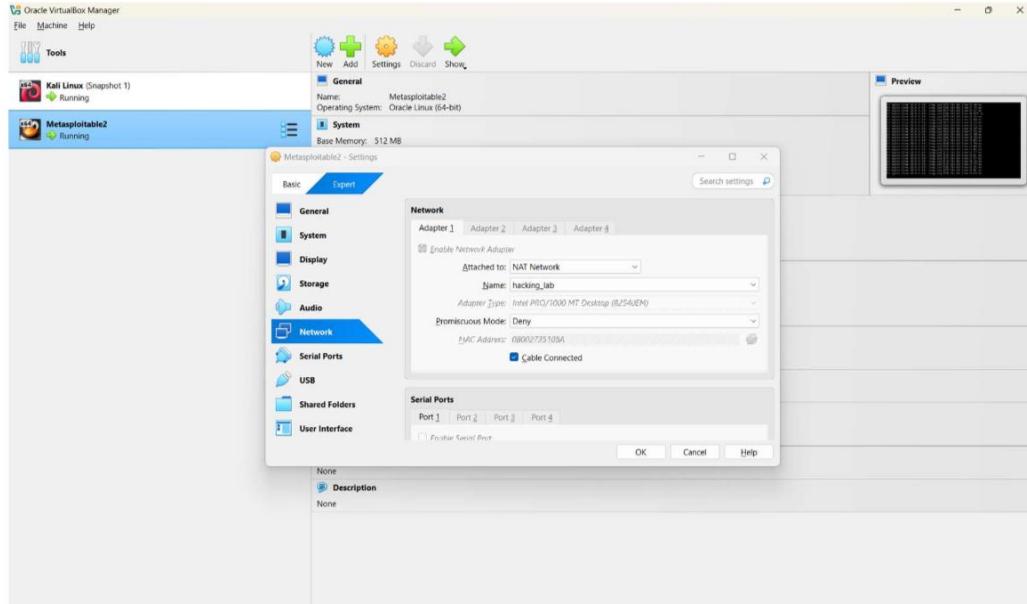
VirtualBox showing Kali & Metasploitable2 running



Kali connection to hacking\_lab



### Metasploitable2 connection to hacking\_lab



Two virtual machines were created and configured on a Windows laptop using VirtualBox:

- Kali Linux – used as the attacker machine
- Metasploitable2 – used as the vulnerable target machine

Both machines were connected to the same virtual network to allow communication.

### Step 2: Verifying Network Connectivity

Kali terminal showing IP address

Metasploitable2 terminal showing IP address

Kali ping to 10.0.0.30

```

ashka@Ashka:~$ ping 10.0.0.30
PING 10.0.0.30 (10.0.0.30) 56(84) bytes of data.
64 bytes from 10.0.0.30: icmp_seq=1 ttl=64 time=4.09 ms
64 bytes from 10.0.0.30: icmp_seq=2 ttl=64 time=4.07 ms
64 bytes from 10.0.0.30: icmp_seq=3 ttl=64 time=3.16 ms
64 bytes from 10.0.0.30: icmp_seq=4 ttl=64 time=2.17 ms

```

```

Session Actions Edit View Help
Try: sudo apt install <deb name>

(ashka㉿Ashka) ~]$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.10 brd 255.255.255.0 broadcast 10.0.0.255
        inet6 fe80::27ff:fed1:142d/128 scope link
            ether 08:00:27:d1:14:2d txqueuelen 1000 (Ethernet)
            RX packets 45704 bytes 20243991 (19.3 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 42333 bytes 4030606 (3.8 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 brd 255.0.0.0 netmask 255.0.0.0
    inet6 ::1 brd :: prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 4321 bytes 198292 (193.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 4321 bytes 198292 (193.6 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(ashka㉿Ashka) ~]$ sudo ifconfig eth0 10.0.0.10 netmask 255.255.255.0 up

```

The IP addresses of both virtual machines were identified to confirm network connectivity. The following commands were used.

ip a (on Kali)  
ifconfig (on Metasploitable2)

Each machine displays its IP address, confirming they are on the same network.

### Step 3: Ping Test (Connectivity Check)

Kali ping command

```

Session Actions Edit View Help
Try: sudo apt install <deb name>

(ashka㉿Ashka) ~]$ ping 10.0.0.30
PING 10.0.0.30(56(84) bytes of data).
64 bytes from 10.0.0.30: icmp_seq=1 ttl=64 time=4.09 ms
64 bytes from 10.0.0.30: icmp_seq=2 ttl=64 time=4.07 ms
64 bytes from 10.0.0.30: icmp_seq=3 ttl=64 time=3.16 ms
64 bytes from 10.0.0.30: icmp_seq=4 ttl=64 time=2.17 ms
64 bytes from 10.0.0.30: icmp_seq=5 ttl=64 time=4.85 ms
64 bytes from 10.0.0.30: icmp_seq=6 ttl=64 time=2.25 ms
64 bytes from 10.0.0.30: icmp_seq=7 ttl=64 time=2.04 ms
64 bytes from 10.0.0.30: icmp_seq=8 ttl=64 time=1.12 ms
64 bytes from 10.0.0.30: icmp_seq=9 ttl=64 time=2.23 ms
64 bytes from 10.0.0.30: icmp_seq=10 ttl=64 time=1.15 ms
64 bytes from 10.0.0.30: icmp_seq=11 ttl=64 time=1.02 ms
64 bytes from 10.0.0.30: icmp_seq=12 ttl=64 time=2.38 ms
64 bytes from 10.0.0.30: icmp_seq=13 ttl=64 time=2.38 ms
64 bytes from 10.0.0.30: icmp_seq=14 ttl=64 time=0.961 ms
64 bytes from 10.0.0.30: icmp_seq=15 ttl=64 time=1.79 ms
64 bytes from 10.0.0.30: icmp_seq=16 ttl=64 time=1.58 ms
64 bytes from 10.0.0.30: icmp_seq=17 ttl=64 time=1.64 ms
64 bytes from 10.0.0.30: icmp_seq=18 ttl=64 time=2.12 ms
64 bytes from 10.0.0.30: icmp_seq=19 ttl=64 time=1.63 ms
64 bytes from 10.0.0.30: icmp_seq=20 ttl=64 time=2.15 ms
64 bytes from 10.0.0.30: icmp_seq=21 ttl=64 time=3.98 ms
64 bytes from 10.0.0.30: icmp_seq=22 ttl=64 time=1.99 ms

```

```

File Machine View Input Devices Help
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:210 errors:0 dropped:0 overruns:0 frame:0
TX packets:210 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:81265 (79.3 KB) TX bytes:81265 (79.3 KB)

msfadmin@metasploitable:~$ sudo ufw disable
Firewall stopped and disabled on system startup
msfadmin@metasploitable:~$ ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
4 bytes from 10.0.0.10: icmp_seq=1 ttl=64 time=1.79 ms
4 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=1.52 ms
4 bytes from 10.0.0.10: icmp_seq=3 ttl=64 time=1.20 ms
4 bytes from 10.0.0.10: icmp_seq=4 ttl=64 time=1.50 ms
4 bytes from 10.0.0.10: icmp_seq=5 ttl=64 time=1.38 ms
4 bytes from 10.0.0.10: icmp_seq=6 ttl=64 time=1.78 ms
4 bytes from 10.0.0.10: icmp_seq=7 ttl=64 time=1.60 ms
4 bytes from 10.0.0.10: icmp_seq=8 ttl=64 time=1.09 ms
4 bytes from 10.0.0.10: icmp_seq=9 ttl=64 time=1.56 ms
4 bytes from 10.0.0.10: icmp_seq=10 ttl=64 time=1.49 ms
4 bytes from 10.0.0.10: icmp_seq=11 ttl=64 time=1.22 ms
4 bytes from 10.0.0.10: icmp_seq=12 ttl=64 time=1.89 ms
4 bytes from 10.0.0.10: icmp_seq=13 ttl=64 time=1.45 ms
4 bytes from 10.0.0.10: icmp_seq=14 ttl=64 time=1.43 ms

```

A ping test was conducted from Kali Linux to Metasploitable2 to verify communication between the machines:

Command used:

`ping <Metasploitable_IP>`

Successful ICMP responses confirmed stable connectivity between the attacker and target systems.

#### Step 4: Basic Nmap Scan (Host Discovery)

Nmap basic scan

## INFORMATION GATHERING WITH NMAP

Basic Scan (Check if target is alive) command: nmap

```
[root@rhel7 ~]# nmap -sT -p 1-65535 192.168.1.10
Starting Nmap 7.05 ( https://nmap.org ) at 2015-11-21 22:09 PST
nmap: warning: unable to determine any DNS servers. Reverse DNS is disabled
nmap: info: using --dns-servers to specify valid servers with --dns-servers
nmap scan type: SYN+ACK Scan
nmap version: 7.05 ( https://nmap.org )
nmap: up is (0.0079s latency).
nmap: scanning 192.168.1.10 [65535 ports (next)]
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
53/tcp    open  dns
5351/tcp  open  rrdcached
139/tcp   open  netbios-ssn
1394/tcp  open  rawmidi
3322/tcp  open  eesm
4000/tcp  open  httpd
5325/tcp  open  vnc
5326/tcp  open  vnc
5327/tcp  open  vnc
5328/tcp  open  vnc
5329/tcp  open  vnc
5399/tcp  open  mraeregistry
23450/tcp open  unknown
23460/tcp open  afunix
23221/tcp open  ciscoavp-vtp
23222/tcp open  ciscoavp-vtp
33422/tcp open  unknown
33423/tcp open  postgresql
50000/tcp open  x11
50001/tcp open  x11
50002/tcp open  x11
51867/tcp open  irc
51868/tcp open  irc
51869/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.90 seconds

[root@rhel7 ~]# nmap -sT -p 1-65535 192.168.1.10
Starting Nmap 7.05 ( https://nmap.org ) at 2015-11-21 22:10 PST
nmap: warning: unable to determine any DNS servers. Reverse DNS is disabled
nmap: info: using --dns-servers to specify valid servers with --dns-servers
nmap scan type: SYN+ACK Scan
nmap version: 7.05 ( https://nmap.org )
nmap: up is (0.0079s latency).
nmap: scanning 192.168.1.10 [65535 ports (next)]
[...]
[TARGET SPECIFICATION]
Can pass hostnames, IP addresses, networks, etc.
For example: 192.168.1.10, 192.168.1.1-10, 192.168.1.1-254
-IL [inputfilename]: Input from list of hosts/networks
-IL2 [inputfilename]: Input from list of hosts/networks
--excludefile [file]: Exclude hosts/networks
--excludehost [host|IP]:> Exclude hosts/networks
--excludedomain [file]: Exclude list from file
[...]
[SCANNING]
-n: disable port scanning
-UL [list]: Simply list targets to scan
-PE: Perform OS detection
-PS: Treat all ports as open
-PR: Perform TCP connect(2) probe
-PPV[PV/PV]: [parallelize] TCP SYN, TCP ACK, UDP or ICMP discovery to given po
-PRV[PV]: [parallelize] TCP SYN, TCP ACK, UDP or ICMP discovery to given po
-P[VV]: ICMP Echo, timestamp, and netmask request discovery probes
-[P]rotocol [list]: IP Protocol, Ping, TCP, UDP, ICMP, Raw, and Nmap Scripting Engine (NSE) probe
--script [script|script[,script],...]:> Specify custom NSE scripts
--script-args [key=value,...]:> Set arguments for NSE scripts
--traceroute: Trace hop path to each host
[SCAN TECHNIQUES]
--script [script|script[,script],...]:> Run NSE scripts
--script-args [key=value,...]:> Set arguments for NSE scripts
--script-timeout [time]: Set script timeout
--script-fingerprint [file]: Customize TCP scan flags
--script-timing [file]:> zombie host[prod/report]:> file scan
--script-timeout [time]: Set script timeout
--script-args [key=value,...]:> Set arguments for NSE scripts
--ohI IP protocol scan
--ohI IP protocol scan
--ohI IP relay hosts:> TCP bounce scan
```

A simple Nmap scan was performed to confirm the target is alive.

## Command used:

nmap <Target\_IP>

This revealed that the host was active and presented multiple open ports, indicating a broad attack surface.

## Nmap displays:

- Host is up
  - List of open ports such as 21, 22, 80, 139, etc.

## Step 5: Full Port Scan

Full Nmap port scan

Detailed Scan Command: nmap -sv

```

Session Actions Edit View Help
  --scanflags <flags>: Customize TCP scan flags
  -sI <zonefile>[,<port>]: Idle scan
  -sT: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>; FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <ports>[,-,+,!]<ports>: Specify ports to scan
    Ex: -p22,-p1-65535,-p U153,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -R: Scan ports sequentially - don't randomize
  -T <time>: Set timing template. See <man nmap> for details
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -SV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Try every probe (intensity 1)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -S<C>: equivalent to --script=default
  --script[=list] <script>: <Lua script> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<key1>[,<key2>,...]: provide arguments to scripts
  --script-args-file<filename>: provide NSE script args in a file
  --script-track: Track all scripts and received
  --script-updatedb: Update the script database
  --script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma-separated list of script-files or
    script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  -D<time>[,<time>]: Set timing template. <time> are in seconds, or append 'ms' (milliseconds),
    's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g., 30m).
  -T<0-5>: Set timing template (higher is faster)
  -min-hostgroup|max-hostgroup <n>: Parallel host scan group sizes
  -min-parallelism|max-parallelism <n>: Probe parallelization
  -min-rtt|initial-rtt|max-rtt<initial-rtt>: Specifies
    probe round trip time.
  --max-retries <n>: Cap number of port scan probe retransmissions.
  -host-timeout <time>: Give up on target after this long
  --scn-delay|max-scan-delay <n>: Delay between probes
  --max-rate <n>: Send packets no slower than <n> per second
  --max-rate-number: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f: --mtu <val>: Fragment packets (optionally w/given MTU)
  -D <decays>: Decay factor for a scan with decoys
  -S <IP Address>: Spoof source address
  -e <interface>: Use specified interface
  -g/<source-port ><portnum>: Use given port number
  --proxies <url1>,[<url2>,...]: Relay connections through HTTP/SOCKS4 proxies
  --http-proxy <proxy>: Use proxy to send packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <n>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --macforge <mac address>/<prefix>/<vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oG <file>: Output scan in normal, XML, srxIpt kIdl3,
  and gresB format, respectively, to the given filename.
  -oh <format>: Output scan in the given format at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  -reason: Display the reason a port is in a particular state

```

A comprehensive port scan was conducted to detect all open ports:

Command used:

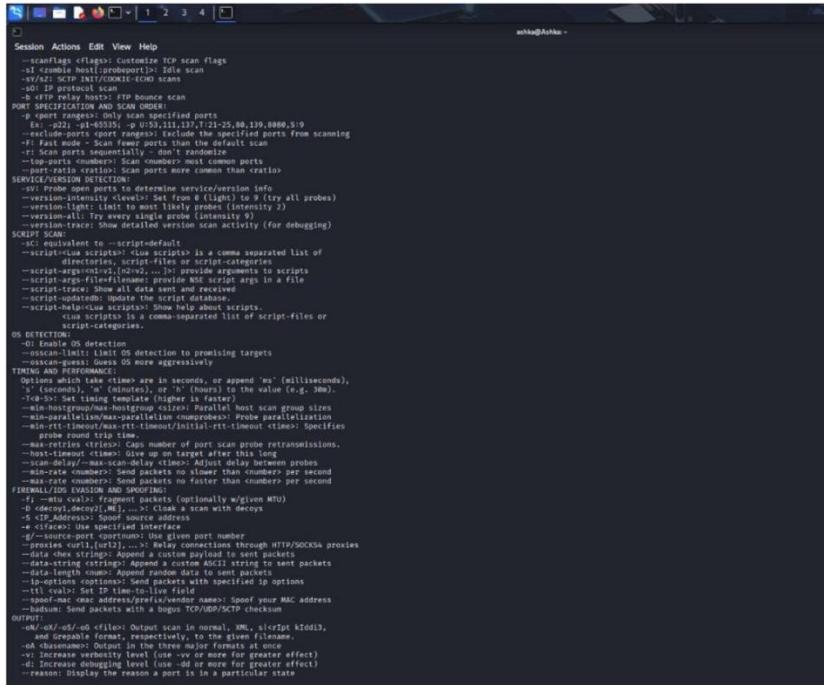
nmap -p- <Target\_IP>

All open ports on the system are displayed, revealing potential attack points.

## Step 6: Service and Version Detection

Nmap -sV output

Detailed Scan Command: nmap -sv



```

Session Actions Edit View Help
  --scanflags <flags> Customize TCP scan flags
  -A Full OS detection, service detection, and script scanning
  -Sv[+/-] SCTP INIT/CONNECT/ACK scanning
  -O IP protocol scan
  -N No SYN/ACK bounce scan
PORT SPECIFICATION AND SCAN ORDER
  -p <port ranges> Only scan specified ports
  -T <timing template> Set timing template (e.g., 25,80,120,900,5,10)
  --exclude-ports <port ranges> Exclude the specified ports from scanning
  -F Fast mode - Scan fewer ports than the default scan
  -T <timing template> Set timing template (e.g., 25,80,120,900,5,10)
  --top-ports <number> Scan <number> most common ports
  --port-ratio <ratio> Scan ports more common than <ratio>
SERVICE VERSION
  -sV Probe open ports to determine service/version info
  --version-intensity <level> Set from 0 (light) to 9 (try all probes)
  --version-light Try every probe with intensity 1
  --version-all Try every single probe (intensity 9)
  --script-trace Show detailed version scan activity (for debugging)
SCRIPTS SCAN
  --script <script> or --script <script>[,<script>...]
  --script-list <list> A comma-separated list of scripts
  --script-default <script>[,<script>...]
  --script-args <args>[,<args>...]
  --script-args-list <list> Provide arguments to scripts
  --script-timeout <seconds> Set timeout for each arg in a script
  --script-trace Show all data sent and received
  --script-updatedb Update the script database
  --script-help <script> Show help about scripts.
  --script-include <list> A comma-separated list of script-files or
  --script-categories.
OS DETECTION
  -O Enable OS detection
  --osscan-limit Limit OS detection to promising targets
  --osscan-super-aggressive Use OS detection more aggressively
TIMING
Options which take <time> are in seconds, or append 'ms' (milliseconds).
  -T<n> Set timing template (higher is faster)
  --min-tx-interval <time> Parallel host scan sizes
  --max-parallelism/max-parallel-sessions <value> Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time> Specifies
  --max-retries <tries> Caps number of port scan probe retransmissions.
  --host-timeout <time> Give up on target after this long
  --script-timeout <seconds> Set timeout for each script
  --min-rate <number> Send packets no slower than <number> per second
  --max-rate <number> Send packets faster than <number> per second
  --script-rate <number> Set rate for each script
  -f<val> Fragment packets (optionally w/given MTU)
  -D <decoy>[,<decoy>...]> Click a scan with decoys
  -S <source> Use <source> as source address
  -e <iface> Use <iface> as specified interface
  -g <source-port> <port> Use given port number
  --proxy <proxy> Use proxy to make connections through HTTP/SOCKS4 proxies
  --data <hex strings> Append a custom payload to sent packets
  --data-string <strings> Append a custom ASCII string to sent packets
  --data-length <length> Set data length for each packet
  --ip-options <options> Send packets with specified IP options
  --traceroute Traceroute to destination
  --load <mac> <mac> address/prefix/vendor name: Speed your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT
  -oN/-oX/-oG <file> Output scan in normal, XML, s|cript/kiddis,
  and Grepable format, respectively, to the given filename.
  -oh <format> Output scan in <format> (e.g., nmap.html)
  -vv Increase verbosity level (use -v or more for greater effect)
  -dI Increase debugging level (use -dd or more for greater effect)
  -r<reason> Display the reason a port is in a particular state

```

The following command was used to identify specific services and their versions:

Command used:

nmap -sV <Target\_IP>

Detailed information such as:

- FTP version
- Apache web server version
- SSH version

This revealed outdated or vulnerable software.

## Step 7: Operating System Detection

OS detection scan

OS Detection command: nmap -O

```
(ashka@Ashka)[-]
└─$ nmap -O 10.0.0.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 22:12 PST
nmap.dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
edns01: warning: Unable to determine any DNS servers. Specify valid servers with --dns-servers
Nmap scan report for 10.0.0.30
Host is up (0.0003s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  fts
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
523/tcp   open  rsh
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3128/tcp  open  http-proxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
8000/tcp  open  X11
60007/tcp open  vsftpd
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0B:27:35:10:8A (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

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.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds

[ashka@Ashka][-]
└─$ nmap -A 10.0.0.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 22:13 PST
nmap.dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
edns01: warning: Unable to determine any DNS servers. Specify valid servers with --dns-servers
Nmap scan report for 10.0.0.30
Host is up (0.0003s latency).
Not shown: 977 closed tcp ports (rset)
PORT      STATE SERVICE
2000/tcp  open  vsftpd
22/tcp    open  ssh
vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_STAT
|_FTP server status:
|_ Connected to 10.0.0.10
|_ 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
```

Nmap was used to guess the operating system of the target:

Command used:

nmap -O <Target\_IP>

Results indicated that the target system was Linux-based.

## Step 8: Aggressive Scan

Aggressive scan results

Aggressive Full Scan (Main Evidence) command: nmap -A

```

ashka@Ashka: ~
Session Actions Edit View Help
| Data connections will be plain text
| vsFTPd 2.3.4 - secure, fast, stable
|_ End of status
22/tcp open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-keygen-sshd-OpenSSH_4.7p1 Debian_8ubuntu1DSA
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open  telnet        Linux telnetd
25/tcp open  smtp         Postfix smtpd
|_ auth-command: Metasploit2.localdomain PIPELINING, SIZE 10240000, VRFY,
  EHLO, STARTTLS, ENHANCEDSTATUSCODES, RRBNMIME, DSN
|_ ssl-cert: Subject: commonName=ubuntu864-base.localdomain/organizationName=XX
  COUNTRY/STATE/PROVINCE=There is no such thing outside US/countryName=XX
| Not valid before: 2016-03-17T14:07:45
| Not valid after:  2016-04-10T14:07:45
|_ sslv2:
|_ SSLv2 supported
|_ Ciphers:
|   SSLv2_RC4_128_WITH_MD5
|   SSLv2_DES_192_EDE3_CBC_WITH_MD5
|   SSLv2_RC4_128_EXPORT40_WITH_MD5
|   SSLv2_RC2_128_CBC_WITH_MD5
|   SSLv2_DES_64_CBC_WITH_MD5
|   SSLv2_RC4_40_EXPORT40_WITH_MD5
|_ ssl-date: 2025-11-27T00:00:00+00:00 - 1s from scanner time.
53/tcp open  domain      ISC BIND 9.4.2
| dns-mxid:
|_ 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 #10000)
| rpcinfo:
|   program version port/proto service
|   10000 2           111/tcp  rpcbind
|   10000 2           111/udp rpcbind
|   100003 2,3,4     2049/tcp  nfs
|   100003 2,3,4     2049/udp nfs
|   100005 1,2,3     3399/tcp  mountd
|   100005 1,2,3     4759/tcp  mountd
|   100021 1,3,4     4752/tcp  nlockmgr
|   100021 1,3,4     57059/udp nlockmgr
|   100024 4           424/tcp  status
|   100024 1           44781/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)
513/tcp open  exec       netkit-rsh rexecd
513/tcp open  shell      netkit-rsh
514/tcp open  shell      Netkit rsh
1099/tcp open  java-rmi  GNU Classpath gmrregistry
1524/tcp open  bindshell  Metasploitable root shell
2000/tcp open  nntp      2-4 (RPC #100003)
2212/tcp open  ftp       ProFTPD 1.3.1
3306/tcp open  mysql     MySQL 5.4.30-1ubuntu5
| mysql-info:
|_ Protocol: 10
|_ Version: 5.4.30-1ubuntu5
|_ Thread ID: 8
|_ Capabilities flags: 43564
|_ Some Capabilities: SupportsTransactions, SupportsIAuth, SupportsCompressi
on, LongColumnFlag, Speaks4ProtocolNew, SwitchToSSLAfterHandshake, ConnectWi
thDB
|_ Status: Autocommit
|_ Salt: t'COLgSYU0`k-WvI=*
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-cert: Subject: commonName=ubuntu864-base.localdomain/organizationName=XX
  COUNTRY/STATE/PROVINCE=There is no such thing outside US/countryName=XX
| Not valid before: 2016-03-17T14:07:45

```

An aggressive scan was conducted to gather detailed system information:

Command used:

nmap -A <Target\_IP>

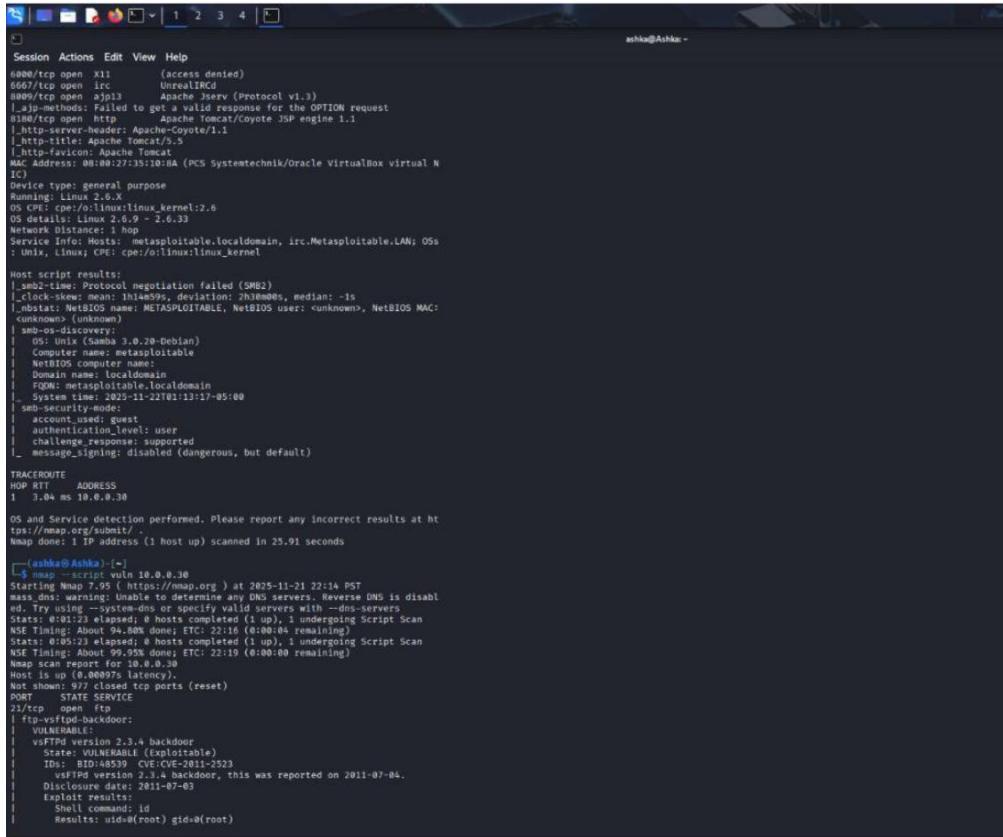
Shows:

- Open ports
- Services
- OS details
- Script results
- Comprehensive system profile is created.

## Step 9: Vulnerability Script Scan

Nmap Scripting Engine (NSE) vulnerability scan

VULNERABILITY CHECK USING NMAP SCRIPTS command: nmap --



```

ashka@Ashka: ~
Session Actions Edit View Help
5000/tcp open  X11      (access denied)
5667/tcp open  irc      UnrealIRCd
8009/tcp open  ajml3    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-user-agent: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 08:0A:27:35:10:8A (PCS Systemtechnik/Oracle virtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linus_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network card(s):
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
  : Unix, Linux; CPE: cpe:/o:linux:linus_kernel

Host script results:
|_ smb-line: protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h1m59s, deviation: 2h30m00s, median: -1s
|_mbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|  |_os-type: Linux (Ubuntu 10.04.3 LTS - 3.2.0-31-generic)
|  |_os-name: metasploitable
|  |_NetBIOS computer name:
|  |_Domain name: localdomain
|  |_FQDN: metasploitable.localdomain
|  |_Last seen time: 2025-11-22T01:13:17+05:00
|_smb-security-mode:
|  |_account_used: guest
|  |_authentication_level: user
|  |_challenge_response_supported
|  |_message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT      ADDRESS
1  3.04 ms 10.8.0.38

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 25.91 seconds
[ashka@Ashka: ~] $ nmap --script vuln 10.0.0.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 22:1a PST
nmap: dns: warning: unable to determine all DNS servers; DNS is disabled
nmap: dns: warning: unable to verify security valid responses with --dns-servers
Stats: #0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.800s done; ETC: 22:16 (0:00:04 remaining)
Stats: #0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: about 94.800s done; ETC: 22:19 (0:00:00 remaining)
Nmap scan report for 10.0.0.38
Host is up (0.00097s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
22/tcp    open  ssh
|_ftp-vsftpd-backdoor:
|  |_VULNERABLE:
|  |_vsFTPD version 2.3.4 backdoor
|    |_State: VULNERABLE (Exploitable)
|    |_ID: BID-4559 CVSS:4.0-2011-2523
|    |_vsFTFd version 2.3.4 backdoor, this was reported on 2011-07-04.
|    |_Disclosure date: 2011-07-03
|    |_Exploit results:
|      |_Shell command: id
|      |_Results: uid=0(root) gid=0(root)
```

A vulnerability script scan was performed using Nmap's NSE engine:

Command used:

nmap --script vuln <Target\_IP>

This scan identified several vulnerabilities associated with insecure service configurations and outdated software packages.

## Step 10: Results Analysis

### Summary of scan findings

```

Session Actions Edit View Help
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
|_sslv2-down: Script execution failed (use -d to debug)
ssl-dh-params:
|_ssl-dh-params:
| Anonymous Diffie-Hellman Key Exchange MITM Vulnerability
| State: VULNERABLE
| Transport Layer Security (TLS) services that use anonymous
| Diffie-Hellman key exchange or premain protection against passive
| eavesdropping are vulnerable to active man-in-the-middle attacks
| which could completely compromise the confidentiality and integrity
| of any data exchanged over the resulting session.
| Check results:
| ANONYMOUS DH GROUP 1
|   Cipher Suite: TLS_DH_anon_WITH_RCA_128_MDS
|   Modules Type: Safe prime
|   Modules Source: postfix builtin
|   Modules Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024
| References:
| https://www.ietf.org/rfc/rfc2246.txt
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM
(logjam)
| State: VULNERABLE
| IDs: BID:74733 CVE: CVE-2015-4000
| The Transport Layer Security (TLS) protocol contains a flaw that is
| triggered by sending Diffie-Hellman key exchanges defined with
| the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
| to downgrade the security of a TLS session to 512-bit export-grade
| cryptography, which is significantly weaker, allowing the attacker
| to easily break the encryption and monitor or tamper with
| the encrypted stream.
| Disclosure date: 2015-5-19
| Check results:
| EXPORT-GRADE DH GROUP 1
|   Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|   Modules Type: Safe prime
|   Modules Source: Unknown/Custom-generated
|   Modules Length: 512
|   Generator Length: 8
|   Public Key Length: 512
| References:
| https://weakdh.org
| https://www.securityfocus.com/bid/74733
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE
| Transport Layer Security (TLS) services that use Diffie-Hellman group
| of insufficient strength, especially those using one of a few common
| shared groups, may be susceptible to passive eavesdropping attacks.
| Check results:
| WEAK DH GROUP 1
|   Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
|   Modules Type: Safe prime
|   Modules Source: postfix builtin
|   Modules Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024
| References:
| https://weakdh.org
| ssl-pool:
| VULNERABLE:

```

The penetration test revealed the following key vulnerabilities:

- Weak services
- Open ports
- Possible entry points

A clear list of high-risk services like:

- Open FTP with anonymous access
- Outdated Apache server
- Exposed SMB services

These conditions significantly increase the likelihood of unauthorized access and system compromise if deployed in a real-world environment.

## **Step 11: Simulated Exploitation Preparation**

#### Identified vulnerable port focus

Vulnerable ports were selected as possible exploitation targets based on risk.

Identification of critical weaknesses to demonstrate attack potential.

## Step 12: Risk Classification

Vulnerabilities were ranked by severity:

- High Risk – Open FTP, SMB shares
- Medium Risk – Outdated services
- Low Risk – Informational ports

## Expected Result

Clear prioritization for remediation.

## Practical Summary

This penetration test simulated a real attacker lifecycle within a controlled lab environment. Kali Linux was used as the attacking machine, while Metasploitable2 was configured as the vulnerable target. Using Nmap, several scans were conducted to identify open ports, running services, operating system details, and security weaknesses.

The tests revealed multiple vulnerabilities including exposed services, outdated software versions, and insecure configurations. These findings demonstrated how attackers can exploit weak system setups and reinforced the importance of proactive security controls.

## Key Findings

- Multiple open ports increasing attack surface
- Weak service configurations
- Outdated applications vulnerable to exploitation
- Potential for unauthorized system access