

Penetration Testing Lab Using Nmap

Tool Used: Nmap

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

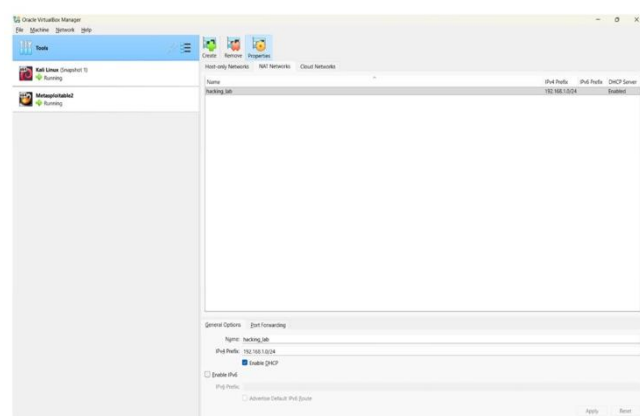
Host OS: Windows

Virtualization Tool: VirtualBox

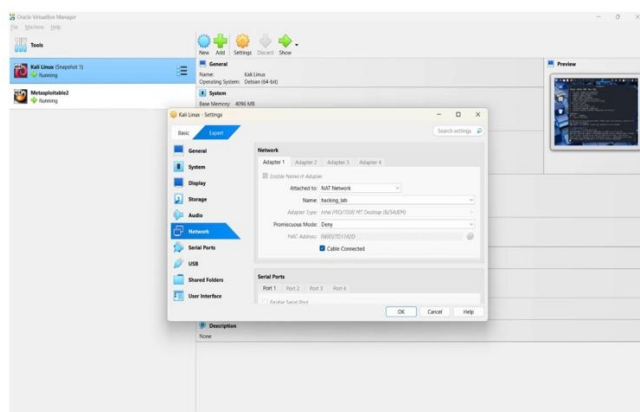
Step 1: Lab Environment Setup

VirtualBox showing Kali & Metasploitable2 running

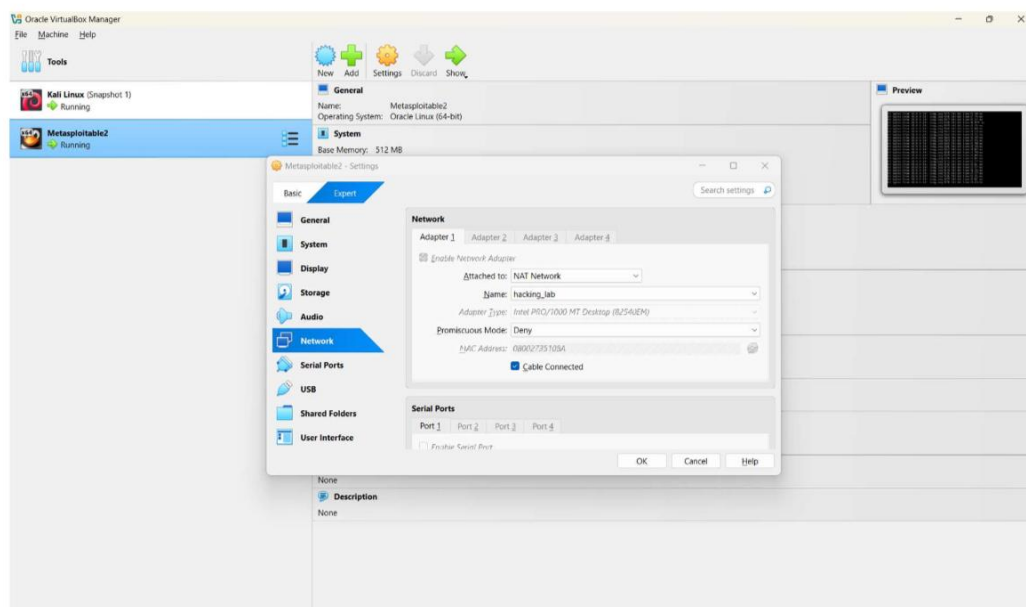
hacking_lab network



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

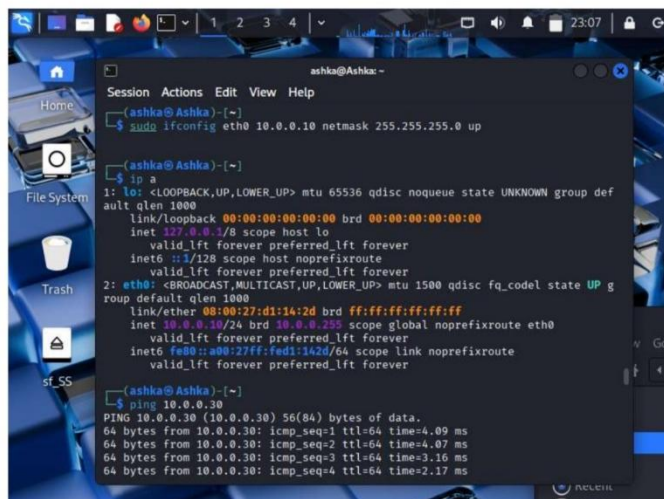
Both machines were connected to the same virtual network to allow communication.

Step 2: Verifying Network Connectivity

Kali terminal showing IP address

Metasploitable2 terminal showing IP address

Kali ping to 10.0.0.30



```

ashka@Ashka: ~
Session Actions Edit View Help
Try: sudo apt install <deb name>

(ashka@Ashka)-[~]
$ sudo ifconfig
[sudo] password for ashka:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.10 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 fe80::a00:27ff:fed1:142d prefixlen 64 scopeid 0<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 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4331 bytes 198292 (193.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4331 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

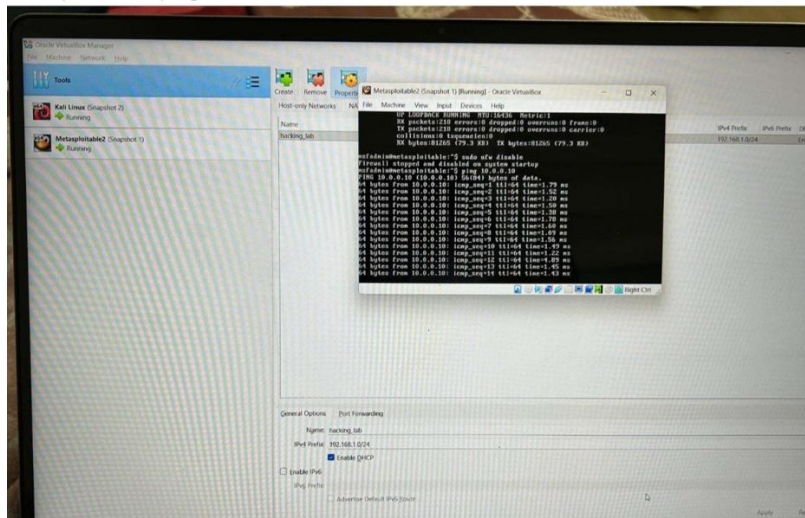
```

ashka@Ashka: ~
Session Actions Edit View Help

(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
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

```

Metasploitable2 ping to 10.0.0.10



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`

```

Session Actions Edit View Help
~$ sudo 19.8.0-18
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 22:09 PST
Hosts are scanned sequentially. Order of scans may vary from command-line order.
Warning: Ignoring hostnames because you did not specify --hostnames or --no-hostnames
Warning: Ignoring OS detection because you did not specify --osdetect or --no-osdetect
Nmap scan report for 19.8.0-18
Host is up (0.0075s latency).
Not pinged: 192.168.1.1
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  nmap
25/tcp    open  smtp
59/tcp    open  ftp
80/tcp    open  http
111/tcp   open  rcpdnet
129/tcp   open  netbios-ssn
143/tcp   open  microsoft-ds
152/tcp   open  esee
153/tcp   open  login
154/tcp   open  shell
1899/tcp  open  rmiplugltry
224/tcp   open  csmrpack
2843/tcp  open  nfs
4223/tcp  open  cisco-scp
1066/tcp  open  mpscd
4422/tcp  open  postgresql
1066/tcp  open  msf
1066/tcp  open  All
1066/tcp  open  lvs
1069/tcp  open  xjsid
1069/tcp  open  subman
MAC Address: 08:00:27:35:1B:8A (PCI Systemtechnik/Uracle VirtualBox virtual W
C)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

~$ cat /etc/nmap/nmap.conf
#--sudo -o 19.8.0-18
#--script=ssh-auth
Usage: nmap [Scan Type(s)] [Options] [Target specification]
Targets specification:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.zenmap.org, microsoft.com/24, 192.168.1.1 19.0.0.255.1-254
-iL: Specify interface: Select from list of hosts/networks
-iK: Connect kernel: Choose random targets
--exclude {hostname|host[IP]|host[IP]}: --to Exclude hosts/networks
--excludefile exclude_file: Exclude list from file
HOST DISCOVERY
--sn: List Scan - simply list targets to scan
--pi Ping Scan - disable port scan
--Pn: Treat all hosts as online - skip host discovery
-O: OS Detection (portinfo): TCP SYN, TCP ACK, UDP or ICMP discovery to given po
It's
--PS:PortSpec: UDP echo, timestamp, and network reset discovery probes
--PP:PortSpec: IP Protocol ping
--O: Server or OS detection/OS fingerprint (default: sometimes)
--os-servers {server[,server],...}: Specify custom OS servers
--system-down: Stop OS & DNS resolution
--traceroute: Trace how path to each host
SCAN TECHNIQUES
--S:SYN/ACK/SYN/FIN: TCP SYN/Connect()/ACK/Window/Jackpot scans
--T:TCP Scan
--X:XMAS/TCP Reset, FIN, and Xmas scans
--scanflags -f{flags} Customize TCP scan flags
--x:combine host() commands into safe scan
--AZI: SETIP INET/INET6/ICMP/ICMP6 scans
--OI: IP protocol scan
--h:rfp relay hosts: RFP 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 < zombie host[:probeport]>: Idle scan
-sV/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: ID protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
  Ex: -p21,-p1-65535 -p U:53,111,137,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
--top-ports <number>: Scan <number> most common ports
--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: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
--sc: Equivalent to --script=default
--script <lua scripts>: <lua scripts> is a comma separated list of
  directories, script-files or script-categories
--script-args <on-v1[,n2,v2,...]>: Provide arguments to scripts
--script-args-file <filename>: Provide NSE script args in a file
--script-trace: Show all data sent 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:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
--tcp-bc: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
  probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> 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 <decoy[,decoy[,ME],...>: Cloak a scan with decoys
-S <IP_address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url1[,url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN <file> -oX <file> -oG <file>: Output scan in normal, XML, sICRpt kIdl3,
  and Greppable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats 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
--sI <enable|disable|probe|script>: IDle scan
--sV/sZ: SCTP INIT/COOKIE-EXCH scan
--sO: IP protocol scan
--b <ip>: relay hosts: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <ports>: Only scan specified ports
Ex: -p22 -sI-65535 -p U:55,111,137,T:21-25,80,139,8080,819
--exclude-ports <port ranges>: Exclude the specified ports from scanning
--F: Fast mode - Scan fewer ports than the default scan
--ri: Scan ports sequentially - don't randomize
--top-ports <number>: Scan numbers most common ports
--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: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
--sC: equivalent to --script=default
--sC <script[,...]>: <script> is a comma separated list of
  directories, script files or script-categories
--script-args <arg1>[<arg2> ...]: provide arguments to scripts
--script-args <file>: provide NSE script args in a file
--script-trace: Show all data sent and received
--script-update: update the script database
--script-help <script>: Show help about scripts.
  <script> is a comma-separated list of script-files or
  script-categories.
OS DETECTION:
--O: Enable OS detection
--oscan: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 300s).
--tcp-sS: Set timing template (higher is faster)
--min-hostgroup <min>/max-hostgroup <time>: Parallel host group sizes
--min-parallelism <min>/max-parallelism <connections>: Probe parallelization
--min-rtt-timeout <min>/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
  probe round trip time
--max-retries <retries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
--f: <file>: <file>: Fragment packets (optionally w/given MTU)
--d <delay>: Delay between packets
--S <IP address>: Spoof source address
--e <iface>: Use specified interface
--g/--source-port <portnum>: Use given port number
--proxies <url1[,url2],...>: Relay connections through HTTP/SOCKS proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified IP options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address>[<privs>|<vendor name>]: Spoof your MAC address
--badsrc: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
--oX <ext>|<file>: Output scan in normal, XML, or script k&id3;
  and Graphable format, respectively, to the given filename.
--oA <filename>: Output in the three major formats of one
--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

```

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 10.0.0.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 22:12 PST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.38
Host is up (0.0023s 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
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  logreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:35:10:0A (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
ng/submit/.
Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds

ashka@Ashka:~$ nmap -sA 10.0.0.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 22:13 PST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.0.38
Host is up (0.0038s latency).
Not shown: 972 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-stat:
|_ftp-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`

```

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 Subuntu (protocol 2.0)
| ssh-hostkey:
| 1024 68:8f:cf:e1:08:5f:6a:7a:d6:00:24:fa:c4:d5:6c:cd (DSA)
| 2048 56:56:2a: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
| smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
| ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN
| ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=O
| C=US/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| sslv2:
| sslv2 supported
| ciphers:
| SSL2_RC4_128_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| ssl-date: 2025-11-22T06:13:25+00:00; -1s from scanner time.
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
| 100003 1,2,3 20996/tcp mountd
| 100003 1,2,3 47596/udp mountd
| 100021 1,3,4 47512/tcp nlockmgr
| 100021 1,3,4 37659/udp nlockmgr
| 100024 1 43409/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 3.0.2a-Debian (workgroup: WORKGROUP)
512/tcp open exec      netkit-rsh rexecd
513/tcp open login      Netkit rshd
514/tcp open shell      Netkit rshd
1099/tcp open java-rmi    GNU Classpath gmiiregistry
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-Subuntu5
| mysql-info:
|_ Protocol: 10
|_ Version: 5.0.51a-Subuntu5
|_ Thread ID: 0
|_ Capabilities: Flags: 43544
|_ Some Capabilities: SupportsTransactions, Support4Auth, SupportsCompressi
|_ on, LongColumnFlag, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, ConnectW
|_ rDatabase
|_ Status: Autocommit
|_ Salt: t cUg8SVe8"K-w0l-xx
5632/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=O
| C=US/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45

```

An aggressive scan was conducted to gather detailed system information:

Command used:

`nmap -A <Target_IP>`

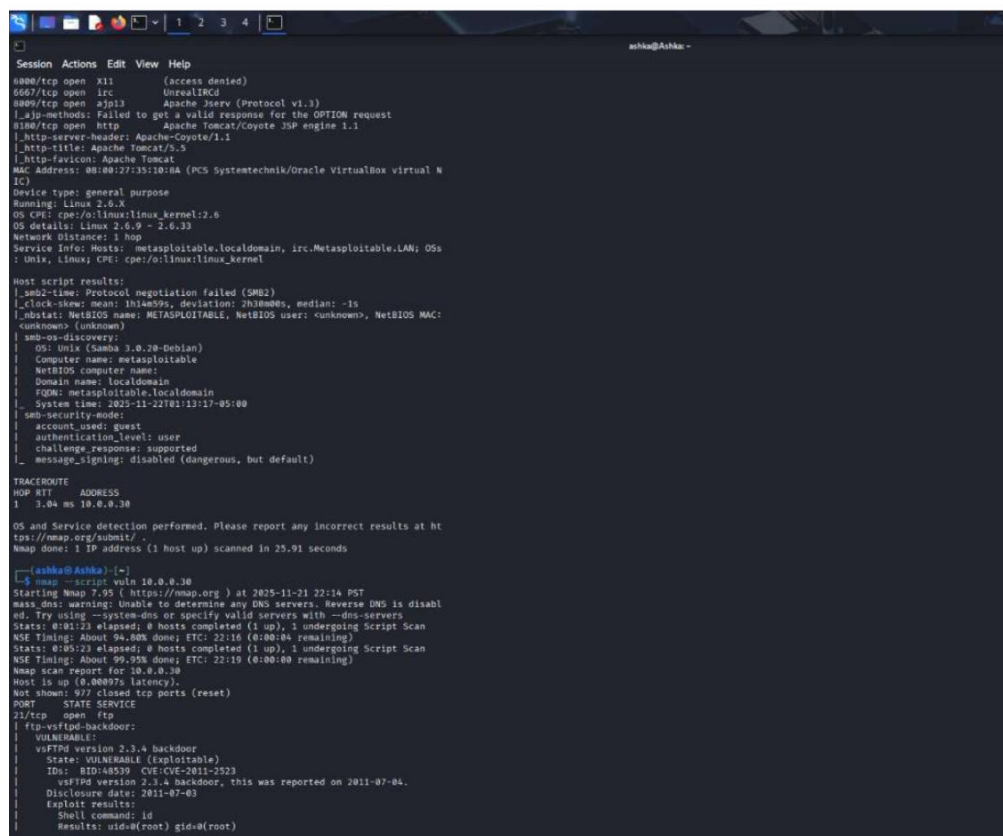
Shows:

- 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 --`



```

Session Actions Edit View Help
6000/tcp open x11 (access denied)
6067/tcp open irc UnrealIRCd
8080/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTIONS request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:35:10:0A (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
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: -1s
|_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: 2025-11-22T01:13:17-05:00
|_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 10.0.0.30

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 25.91 seconds

ashba@ashba:~$
ashba@ashba:~$ nmap --script vuln 10.0.0.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-21 22:14 PST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.80% done; ETC: 22:16 (0:00:04 remaining)
Stats: 0:05:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 22:19 (0:00:00 remaining)
Nmap scan report for 10.0.0.30
Host is up (0.00097s latency).
Not shown: 971 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-vsftpd-backdoor:
|_ VULNERABLE:
| vsftpd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDS: BID:48539 CVE:CVE-2011-2523
| vsftpd 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
22/tcp open  telnet
22/tcp open  stp
|_ssl-v2-down: ERROR: Script execution failed (use -d to debug)
|_ssl-dh-params:
|_VULNERABLE:
|_Anonymous Diffie-Hellman Key Exchange MITM Vulnerability
|_State: VULNERABLE
|_Transport Layer Security (TLS) services that use anonymous
|_Diffie-Hellman key exchange only provide protection against passive
|_eavesdropping, and 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_RC4_128_MD5
|_Modulus Type: Safe prime
|_Modulus Source: postfix builtin
|_Modulus 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 when handling 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 more 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
|_Modulus Type: Safe prime
|_Modulus Source: Unknown/Custom-generated
|_Modulus 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
|_Modulus Type: Safe prime
|_Modulus Source: postfix builtin
|_Modulus Length: 1024
|_Generator Length: 8
|_Public Key Length: 1024
|_References:
|_https://weakdh.org
|_ssl-poodle:
|_VULNERABLE:

```

The penetration test revealed the following key vulnerabilities:

- Weak services
- Open ports
- Possible entry points

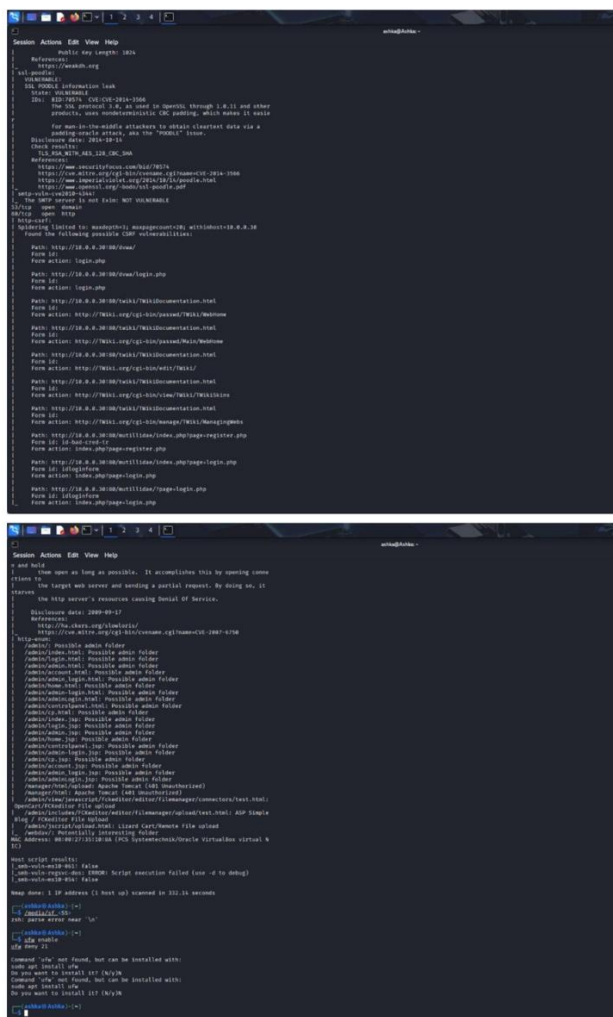
A clear list of high-risk services like:

- 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