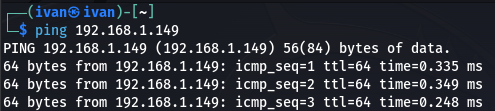
**HACKING CON METASPLOIT**

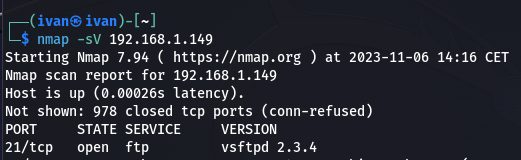
**TRACCIA**  
1) Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd».   
2) Configurare l’indirizzo della vostra macchina Metasploitable come di seguito: 192.168.1.149/24.   
3) Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/).   
4) Chiamate la cartella test\_metasploit. Mettere tutto su un report, spiegare cosa si intende per exploit, cos’è il protocollo attaccato, i vari step.  
  
**LEGENDA**

**Exploit**: Un exploit è un attacco che sfrutta le vulnerabilità già presenti in un software. L'attacco è composto da 3 fasi:  
1) **Exploit** consiste nell’atto vero e proprio di bucare un dispositivo.  
2) **Payload** è il codice contenuto nell’exploit utile a creare una connessione (Shell) con la macchina vittima.  
3) **Shell** (**Bind o Reverse**) è la connessione vera e propria; può essere di due tipi: Bind e Reverse  
Bind parte dall’attaccante, Reverse dalla vittima.  
L’obiettivo è quello di acquisire il controllo di un dispositivo e rubare i dati memorizzati su una rete.  
 **VSFTPD** (**Very Secure FTP Daemon**): è un servizio che per mezzo del protocollo FTP (File Transfer Protocol) permette il trasferimento di file.

Abbiamo configurato il nostro laboratorio virtuale settando l’ip di Metasploitable (macchina vittima) su “192.168.1.149” e l’abbiamo fatto pingare con Kali (macchina attaccante).

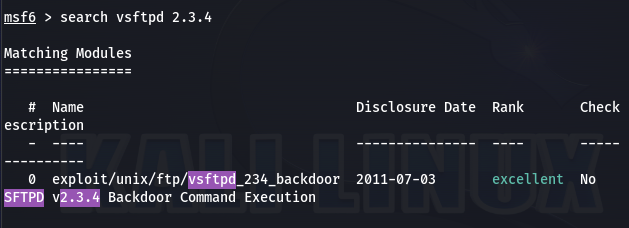


Successivamente, tramite NMAP, abbiamo scansionato tutte le porte aperte su Metasploitable, incluse anche le versioni del loro servizio.  
Troviamo la porta 21 FTP, quella che utilizzeremo per l’exploit.

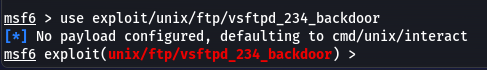


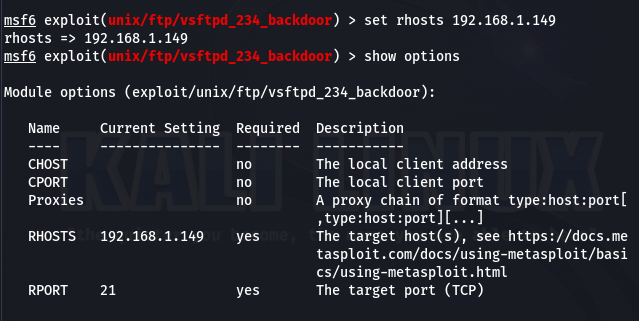
Avviamo Metasploit (software per la gestione di exploit) tramite il comando “msfconsole” e tramite il comando “search” andiamo a trovare l’exploit utile a bucare quel servizio.

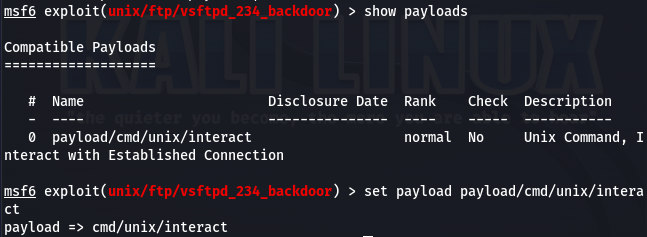


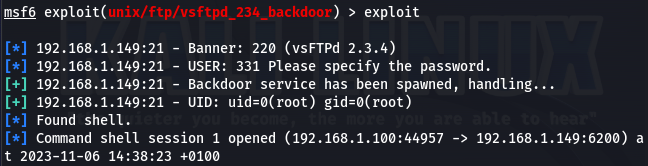


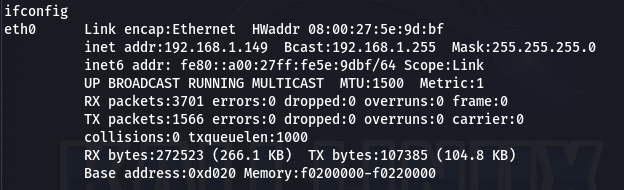
In questo caso scegliamo l’unico exploit disponibile e iniziamo la sua configurazione tramite il comando “use”

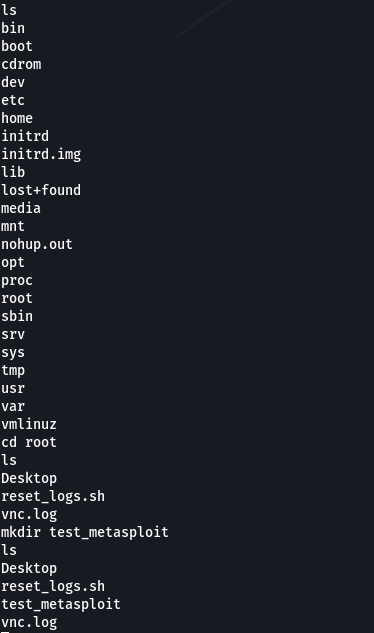


Tramite il comando “show options” notiamo tutti i parametri che ci servono per poter avviare l’attacco. In questo caso, l’unico parametro mancante è l’ip della macchina vittima. Lo andiamo ad impostare col comando “set rhosts” e facciamo un secondo check per verificare che sia tutto corretto.

Passiamo alla seconda fase impostando un payload per il nostro exploit.   
Cerchiamo quelli disponibili tramite il comando “show payloads”.  
Anche in questo caso selezioniamo l’unico disponibile e lo ‘installiamo’ tramite il comando “set payload”.

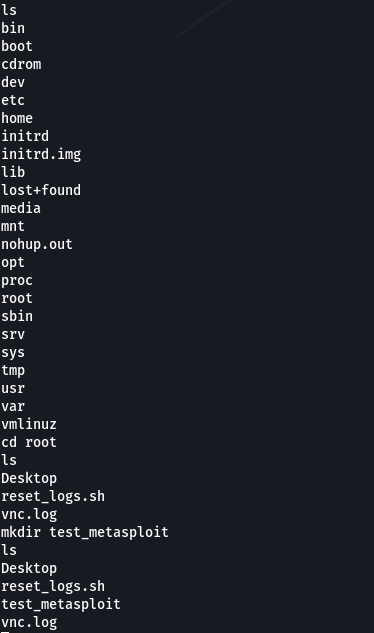
Ora è tutto pronto, eseguiamo l’attacco tramite il comando “exploit”.  
Verrà creata una Shell tra l’attaccante e la vittima. Siamo dentro.

Per controllare se l’attacco ha effettivamente avuto successo, eseguiamo il comando “ifconfig”. Se ci da come risultato l’IP di Metasploitable significa che stiamo controllando la macchina vittima.

A) Tramite i comandi “ls”1-3 (visualizza i contenuti in una directory)   
e “cd”2 (ci permette di spostarci tra le directory), arriviamo alla   
cartella root.

1

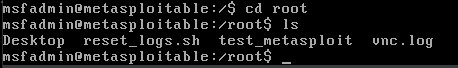


  
B) Andiamo a creare la cartella   
“test\_metasploit” tramite il   
comando “mkdir”.

3



2

  
  
C) Passiamo sulla macchina vittima per controllare se  
le azioni precedenti hanno avuto successo. Possiamo  
vedere che la directory è stata creata tramite l’exploit.