**Traccia:**

Completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**».

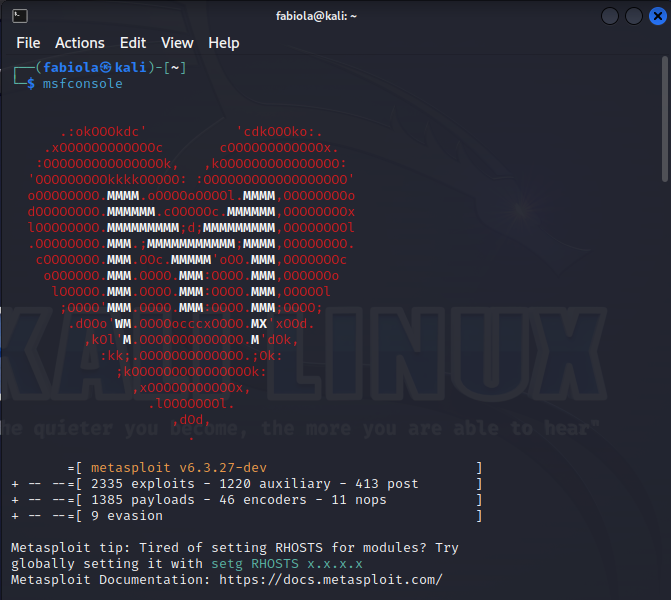
Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test\_metasploit.

Prima di tutto vediamo cos’è un Exploit.

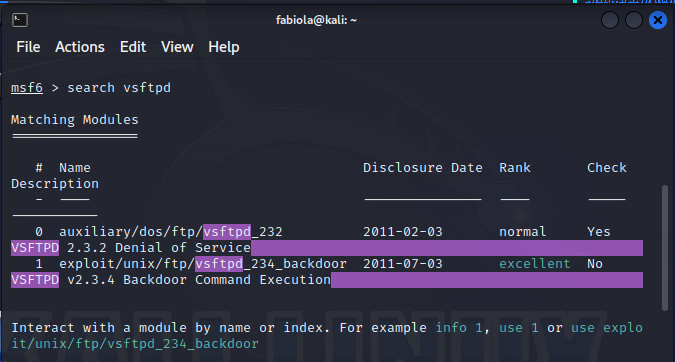
Un **exploit** è una tecnica o un codice informatico progettato per sfruttare una vulnerabilità nel software, nel sistema operativo o in un'applicazione al fine di ottenere un accesso non autorizzato o eseguire operazioni dannose. Gli exploit sono spesso utilizzati da hacker o criminali informatici per compromettere la sicurezza di un sistema e ottenere un vantaggio non consentito; è pertanto importante che gli utenti mantengano i loro sistemi sempre aggiornati e adottino pratiche di sicurezza informatica per ridurre il rischio di esserne vittime.

Per averne un idea più chiara, simuliamo un attacco sulla nostra macchina virtuale:

Sulla macchina Metasploitable, nel nostro laboratorio virtuale, ci sono diversi servizi in ascolto vulnerabili. Possiamo utilizzare i moduli di Metasploit (**msfconsole**) per sfruttare queste vulnerabilità ed ottenere accesso amministrativo alla macchina:



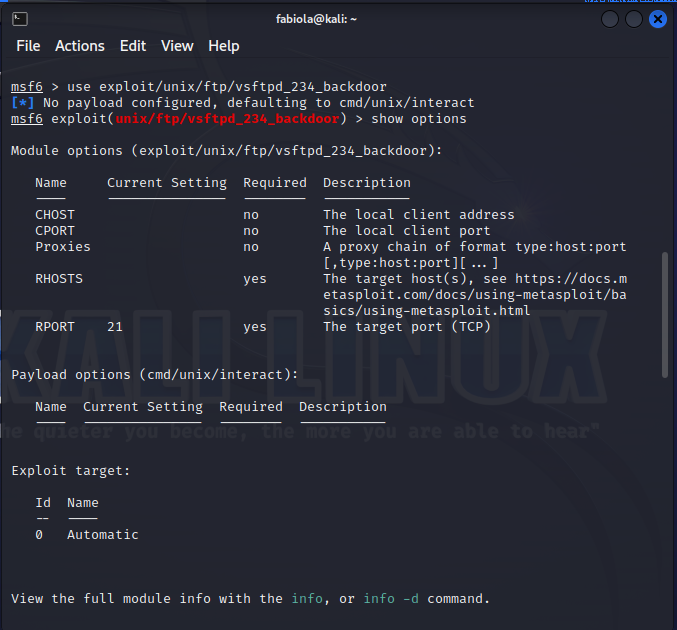
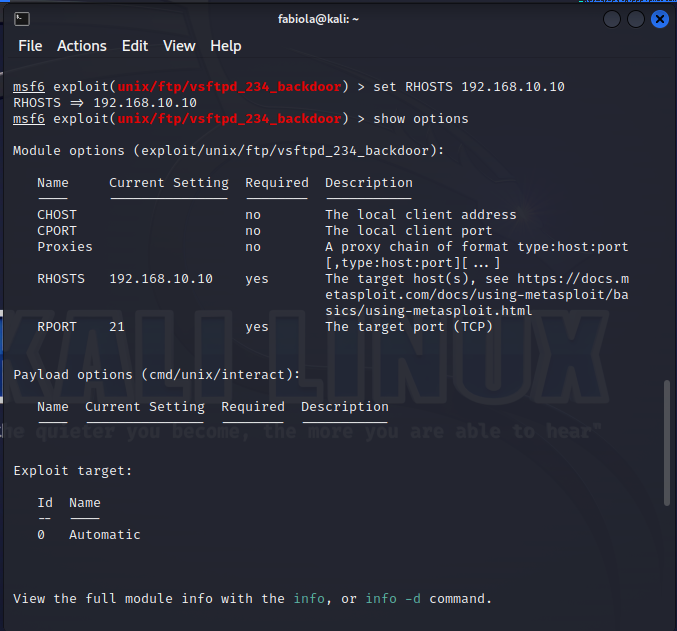
Vediamo se esiste un exploit per il servizio «vsftpd» (un server FTP (File Transfer Protocol) per sistemi operativi basati su UNIX). Possiamo fare una ricerca con il comando «**search**» seguito dal nome del servizio:



La figura ci mostra due exploit per sistemi Unix per il servizio «vsftpd». Scegliamo quello da utilizzare, in questo caso la backdoor (1).

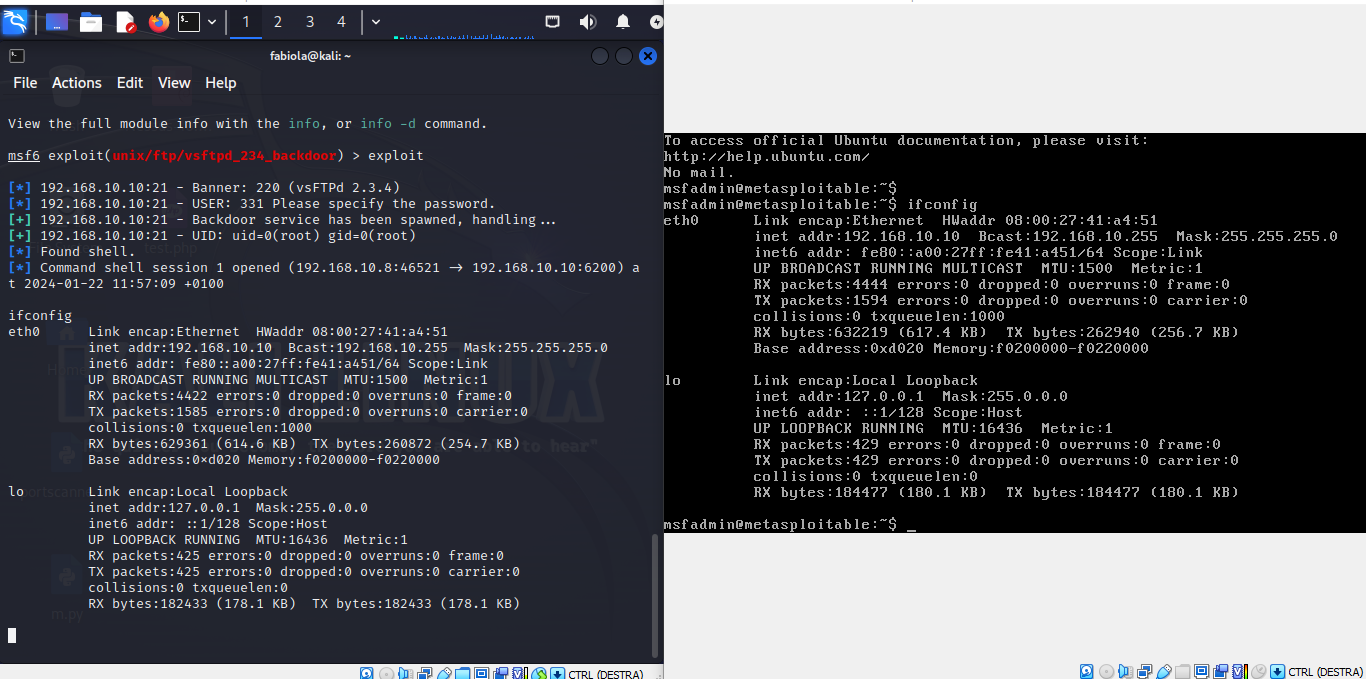
Successivamente, utilizziamo il comando «**show options**» per capire quali parametri devono essere configurati. Come si può vedere l’indirizzo della macchina vittima (RHOSTS) è necessario. Possiamo configurarlo con il comando «set» seguito da RHOSTS e l’indirizzo IP del nostro Metasploitable, quindi il comando utilizzato sarà «**set RHOSTS 192.168.10.10**».

Una volta fatto, ricontrolliamo le opzioni necessarie con il comando «show options» per vedere se abbiamo inserito tutte quelle necessarie. Come si può vedere, il campo RHOSTS è stato correttamente inserito con l’IP della nostra macchina Metasploitable.

Lanciamo quindi l’attacco con il comando «**exploit**»:

Una sessione è stata aperta, abbiamo una shell sul sistema remoto. Eseguendo il comando «ifconfig» possiamo testare se l’IP che ci restituisce la macchina è 192.168.10.10 così da essere sicuri che l’exploit è andato a buon fine e siamo effettivamente sulla macchina Metasploitable.



Possiamo provare ad eseguire qualsiasi comando, per testare l’avvenuta sessione di hacking.

Come, ad esempio, la creazione di una cartella, che chiameremo **test\_metasploit**:

