HACKING CON METASPLOIT

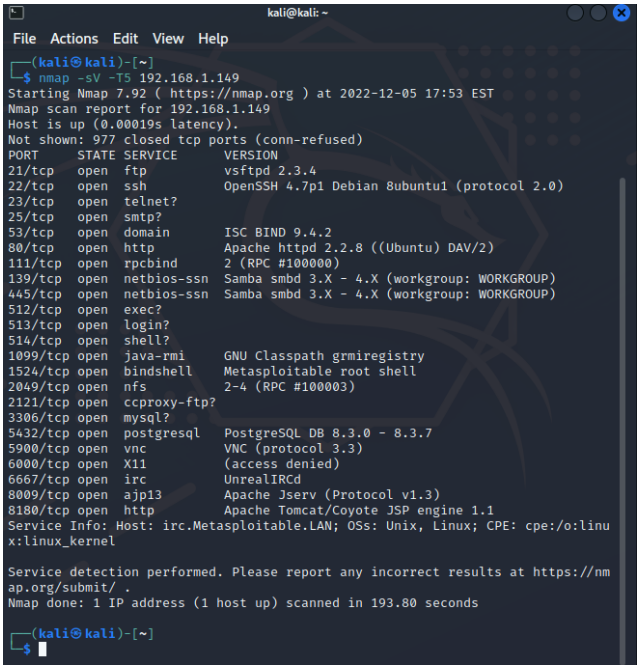
Nella lezioni pratica di oggi vedremo una sessione di hacking con Metasploit sulla macchina Metasploitable

FASE 1

Nella prima fase abbiamo preparato l'ambiente.

Usando il comando **nmap –sV –T5 192.168.1.149** abbiamo effettuato una scansione alla ricerca del servizio vsftpd come richiesto.

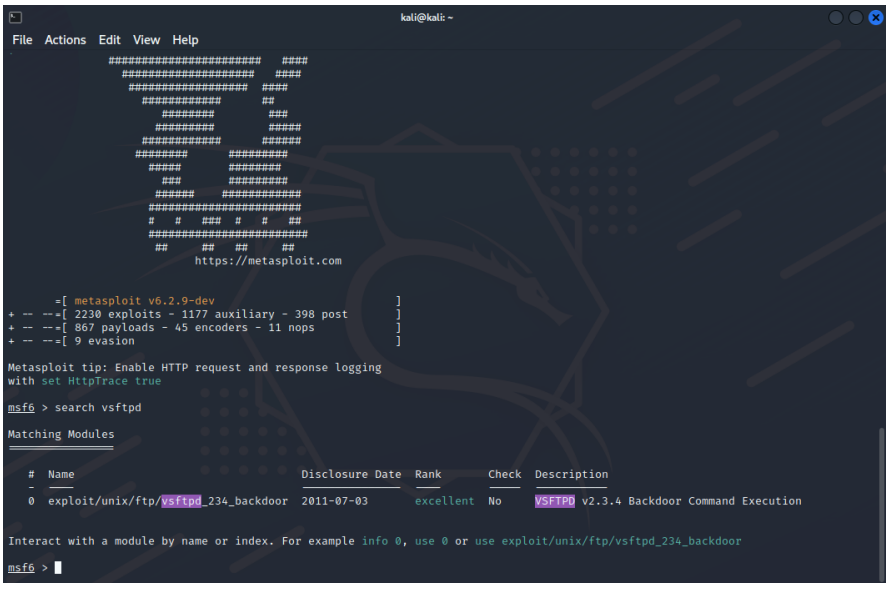
Notiamo che la prima voce che ci appare sulla porta **21** ha quel servizio.



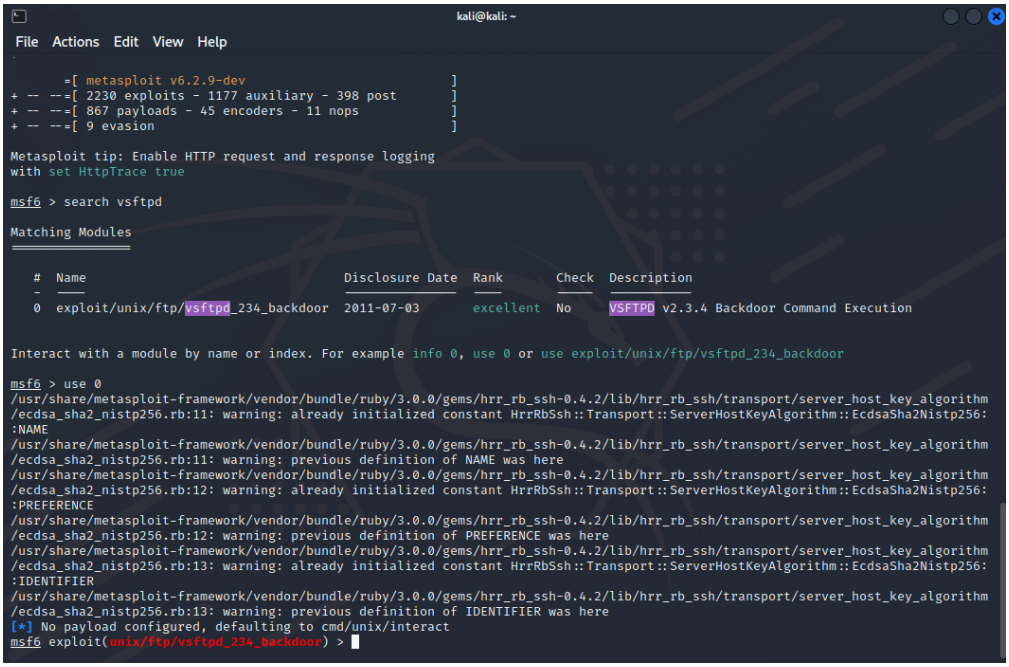
FASE 2

Nella seconda fase abbiamo preparato l'exploit e il payload tramite il comando "**msfconsole**".

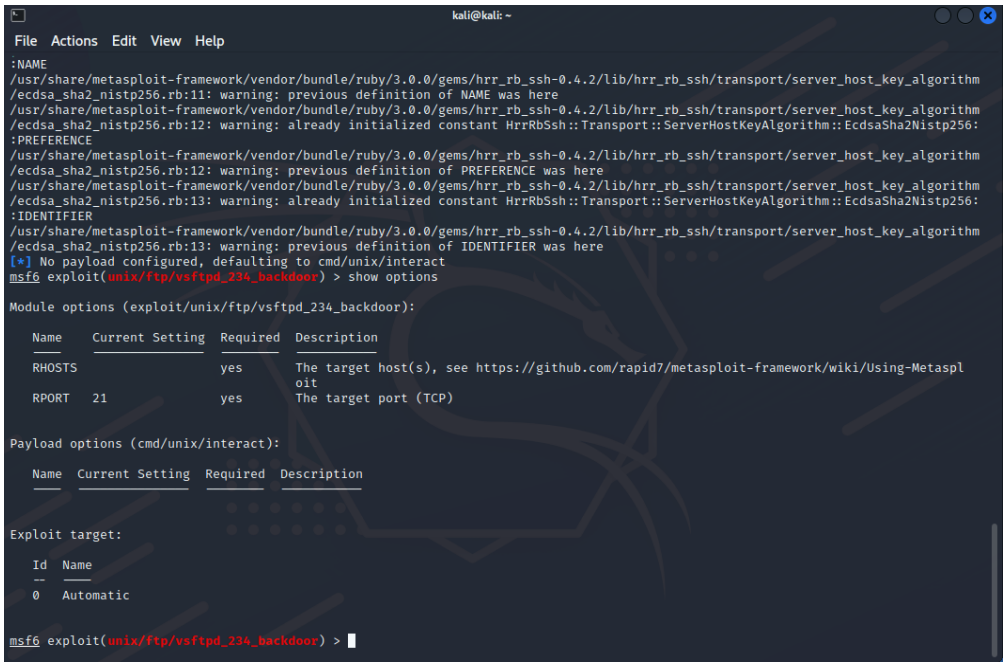
Avviando metasploit abbiamo iniziato la configurazione cercando tramite il comando **"search vsftpd**". Questa ricerca ci ha resituito un exploit per il servizio che cercavamo



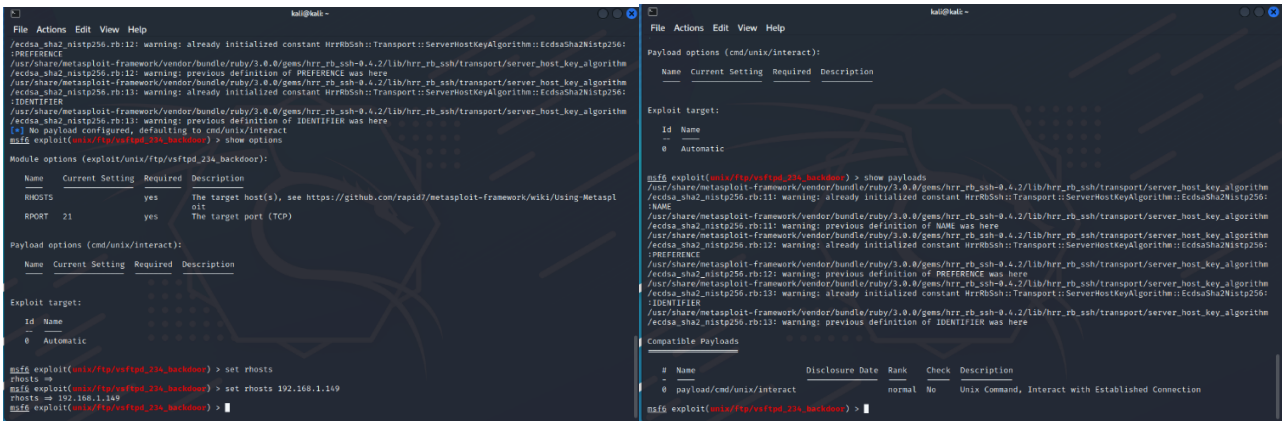
Tramite il comando **use 0** abbiamo selezionato il nostro exploit.



Una volta scelto abbiamo dovuto settarlo per il nostro target. Con il comando **show options** possiamo vedere tutti i parametri che possiamo modificare

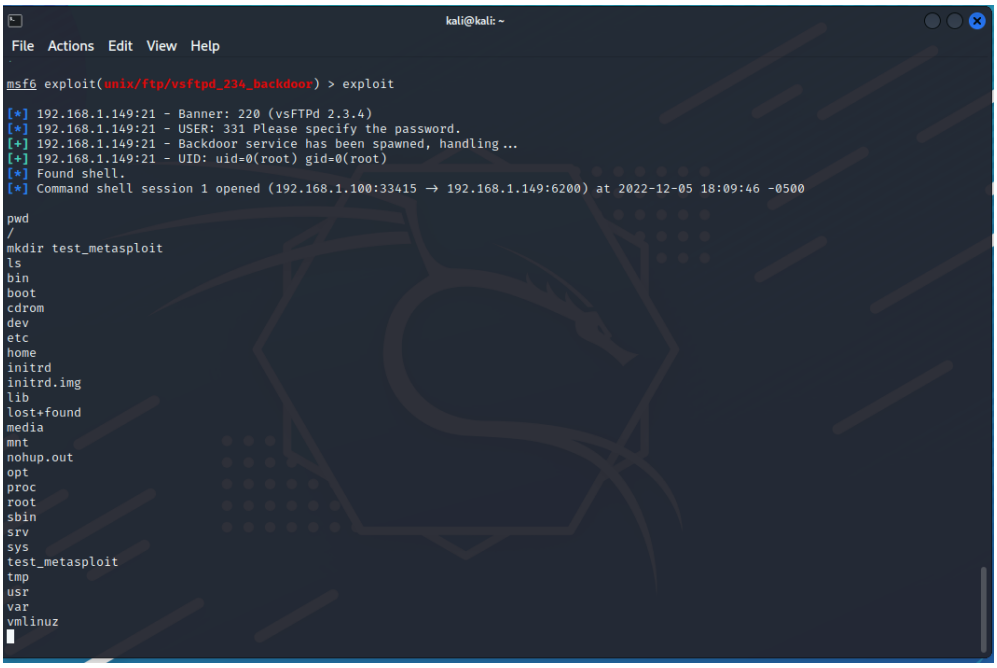


Una volta scelto abbiamo dovuto settarlo per il nostro target. Con il comando **set rhosts 192.168.1.149** abbiamo dato come IP host Metaspoitable.



FASE 3

Nella terza fase lanciamo il nostro exploit con il payload verso il nostro bersaglio con il comando **exploit**



Una volta stabilita la connessione abbiamo potuto usare dei comandi shell per muoverci tra le directory.

Tramite il comando **pwd** abbiamo visto la directory e con il comando **mkdir** abbiamo creato un'ulteriore directory chiamata **test_metasploit**