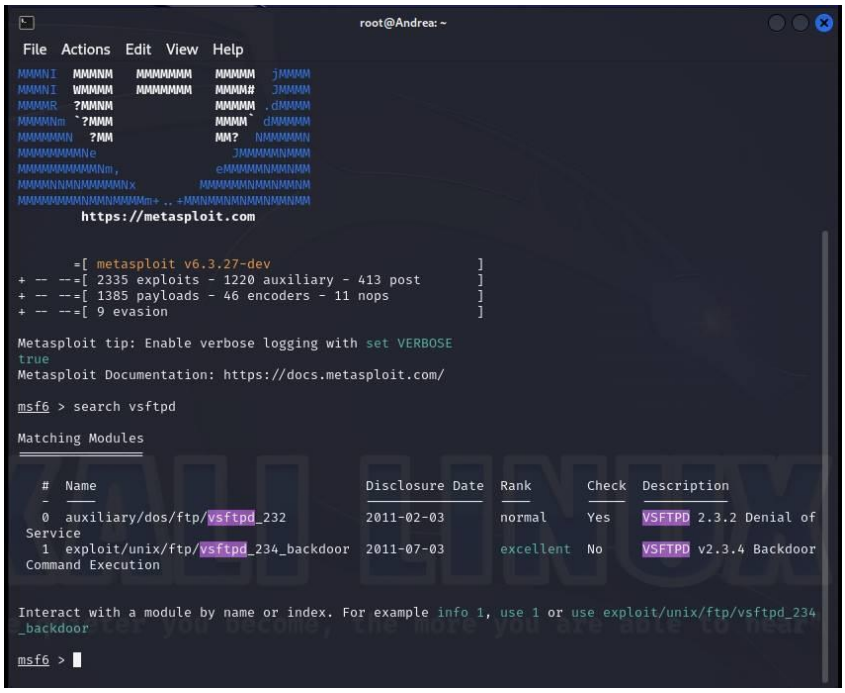
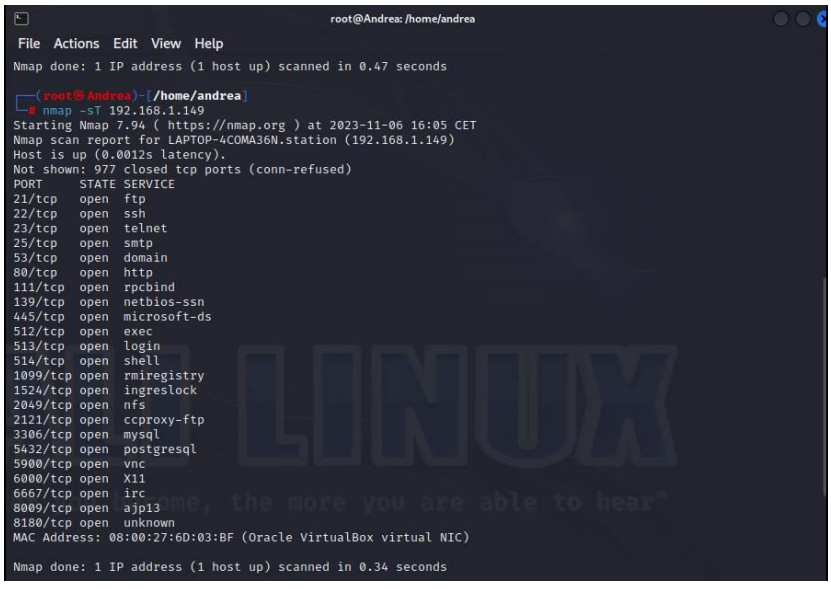
# Esercizio 1 Settimana 7

## Metasploit

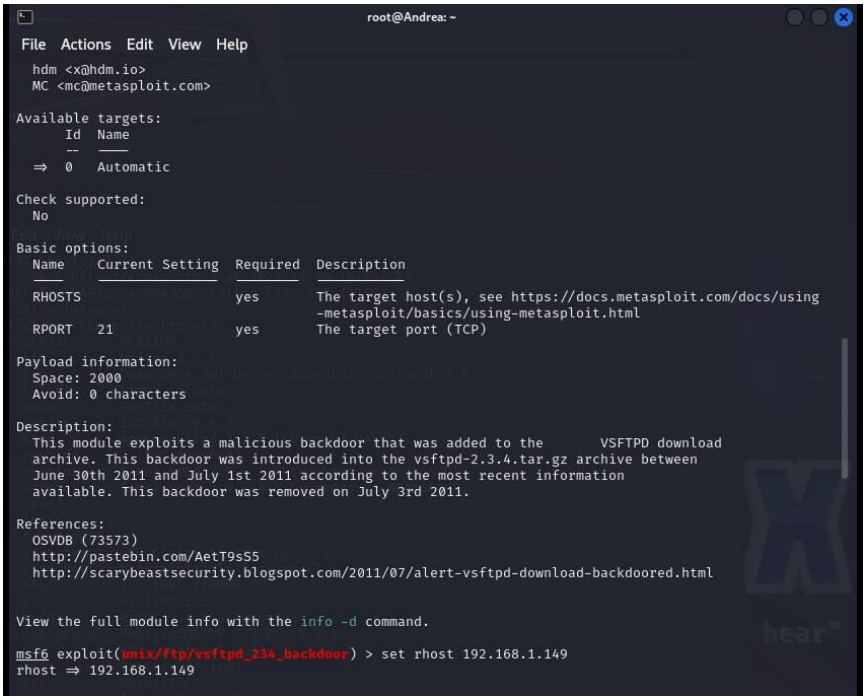
Oggi andiamo a prendere confidenza con una sessione di hacking utilizzando Metasploit sulla nostra macchina Metasploitable.
Per prima cosa andiamo a cambiare l'indirizzo IP di Meta in 192.168.1.149 e verifichiamo che comunichi con Kali effettuando un ping.
Andiamo quindi a startare Metasploit da terminale con il comando *'msfconsole'* e cerchiamo il servizio vsftpd dato in consegna con il comando *'search vsftpd'* generando la seguente schermata:

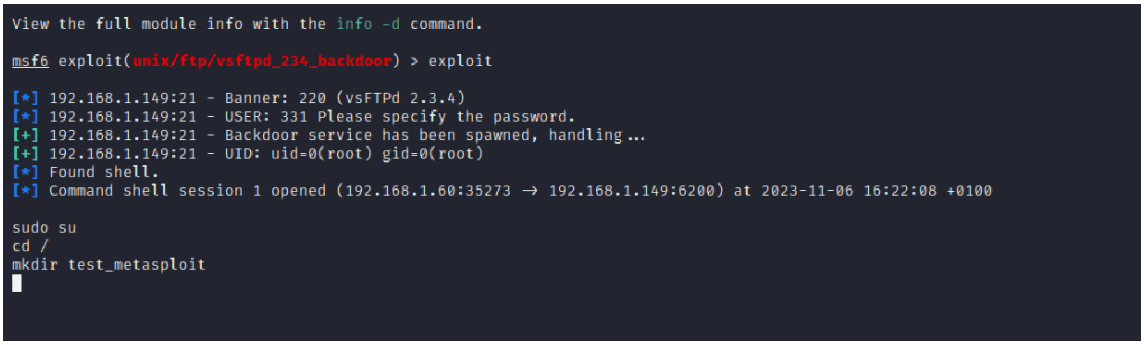



A questo punto selezioneremo la versione adatta alla macchina vittima e, per conoscerne la versione in ascolto sulla porta, faremo una scansione nmap con comando *'sudo nmap -sV 192.168.1.149 21'* (in questo caso abbiamo la versione 2.3.4):



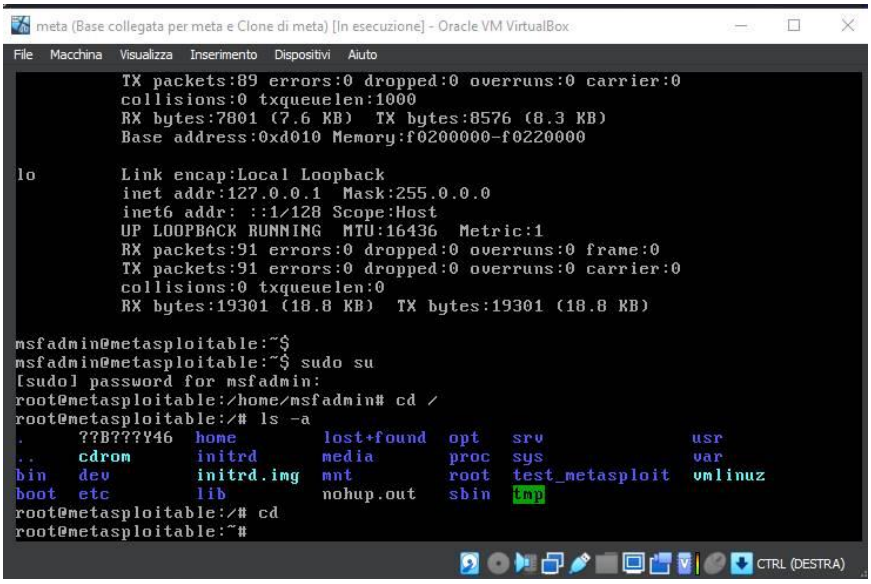
Con il comando *'use 1'* su metasploit andiamo ad utilizzare questo payload (diverso da un Malware poiché non ha bisogno delle azioni dell'utente).
Con *'info*' vediamo le impostazioni dell'attacco e andiamo a settare *'RHOSTS'* con l'IP di Meta o macchina vittima e facciamo partire il tutto con exploit: una volta finito il processo e stabilita la creazione della Shell il gioco è fatto e un eventuale BlackHat può agire indisturbato:




Nella figura sopra possiamo notare che la connessione è avvenuta e a questo punto possiamo inserire comandi specifici come la creazione di cartelle e la navigazione tra le directory.
È molto importante settare le informazioni su attacchi e target che presentano la denominazione *'required : yes'*, esse sono indispensabili per poter eseguire il tutto con successo.

.




Possiamo quindi notare che all’interno della root è stata creata la directory che abbiamo nominato test_metasploit direttamente dal terminale di Kali.