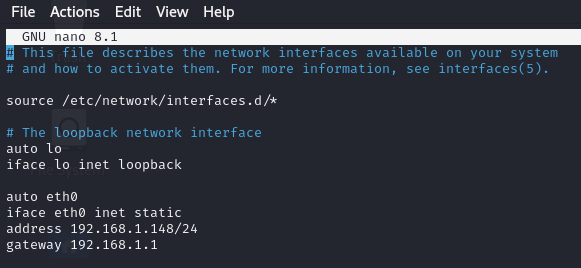
**PRATICA 11 NOVEMBRE 2024**

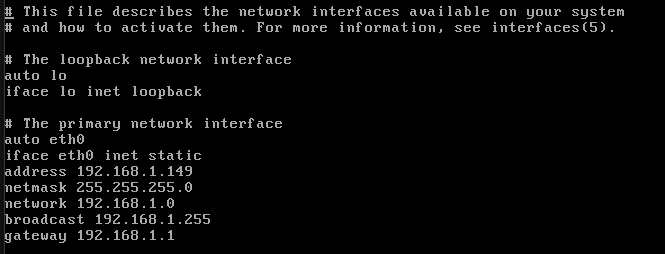
**Hacking con Metasploit**

L’obiettivo di oggi è utilizzare **Metasploit** su Kali Linux per accedere da remoto alla macchina vittima designata (Metasploitable2)

Per prima cosa andremo a settare gli indirizzi IP delle due macchine per metterle in comunicazione:

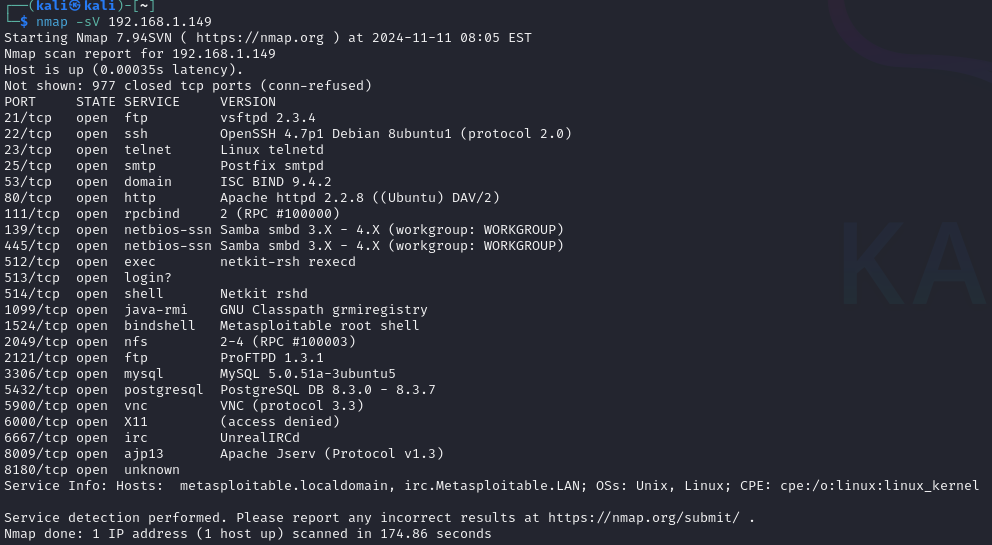
**Configurazione IP Kali Linux**

****

**Configurazione IP Metasploitable2  
**

Appurato che le due macchine comunicano, iniziamo la simulazione d’attacco.

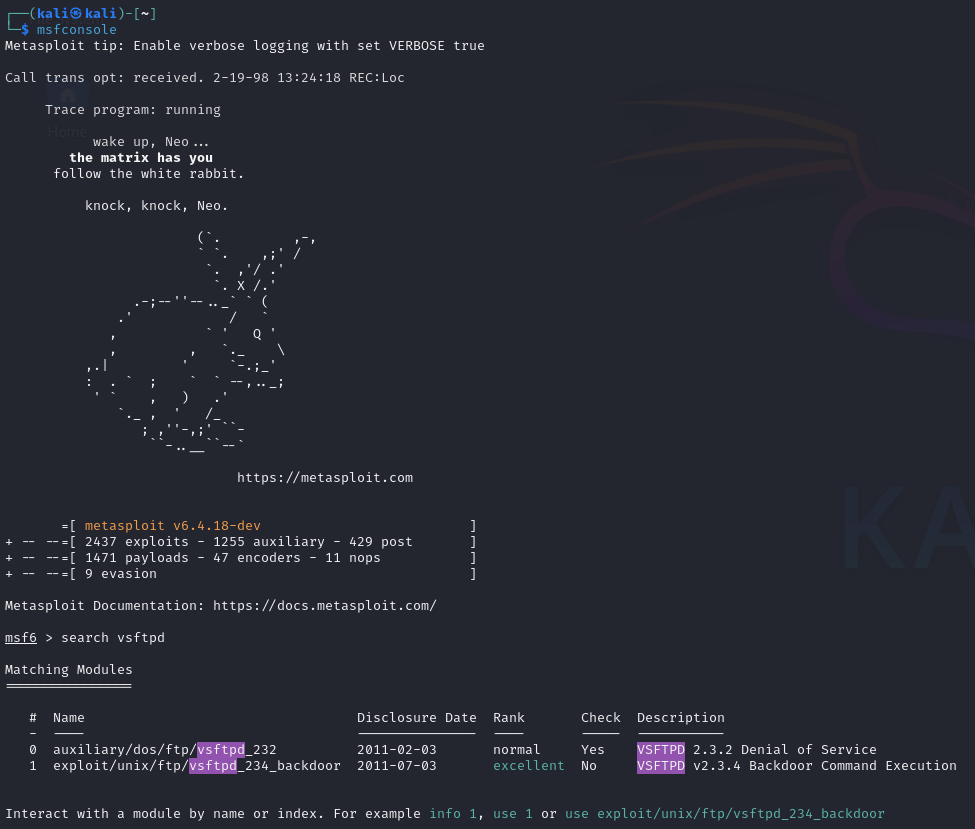
**SCANSIONE PORTE NMAP**

Per prima cosa andremo a controllare quali sono le porte aperte sulla macchina vittima utilizzando nmap:  
  


Tramite questa procedura decidiamo di utilizzare la porta 21 FTP per portare avanti il nostro attacco.

**AVVIO DI METASPLOIT**

Avviando il programma tramite terminale utilizzando il comando **“msfconsole”**, andremo a ricercare le vulnerabilità presenti sulla porta 21 tramite il comando **“search vsftsp”:**

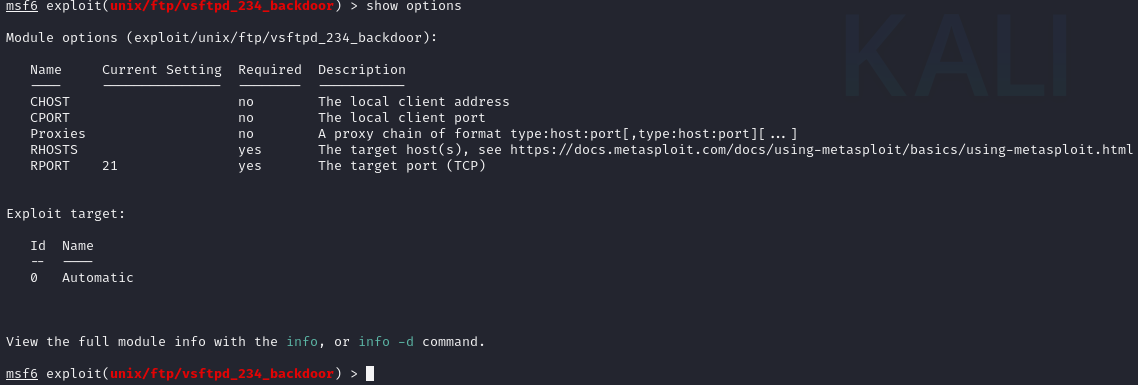


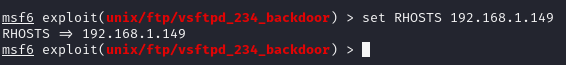
Possiamo vedere che sulla porta 21 è presente un exploit per accedere alla macchina vittima tramite backdoor.

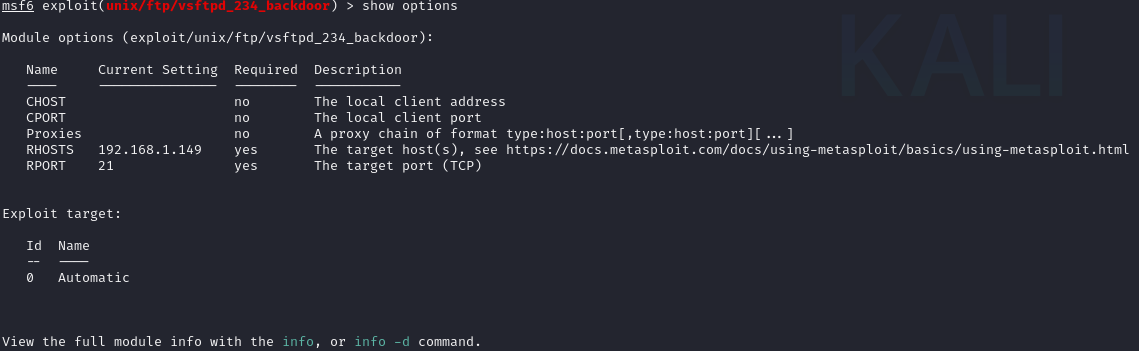
Proseguiamo con il comando “use” seguito dal path dell’exploit che vogliamo utilizzare:

Immagine che contiene testo, Carattere, schermata, Elementi grafici

Descrizione generata automaticamente

Fatto ciò, andremo a controllare i parametri disponibili utilizzando il comando **“show options”**:  


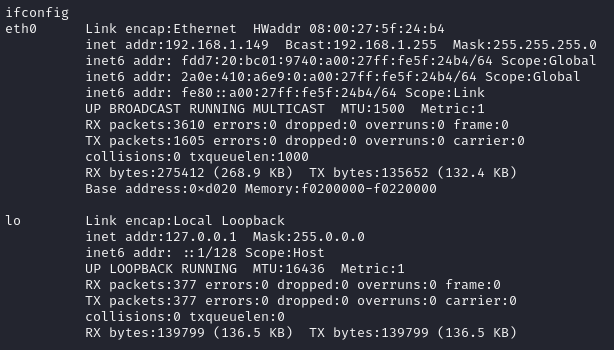
Quello che dobbiamo fare adesso è settare l’indirizzo IP della vittima nel parametro RHOSTS per tentare il collegamento:  


Ricontrolliamo i parametri con “show options” per vedere se è andato tutto a buon fine:  


Possiamo vedere che il parametro adesso è settato con l’indirizzo IP della vittima.

Sistemati questi parametri possiamo procedere all’exploit vero e proprio tramite il comando **“exploit”**:



Per avere conferma utilizzeremo il comando ifconfig:  
  


Possiamo vedere che il nostro indirizzo IP, adesso, corrisponde a quello della macchina vittima.

Per concludere andremo a creare la cartella **test\_metsploit** nella directory root della macchina vittima:

