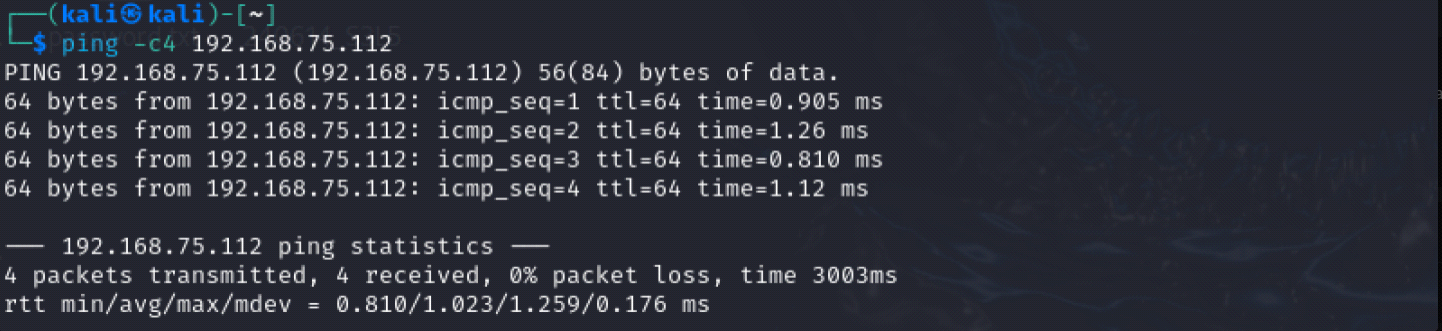
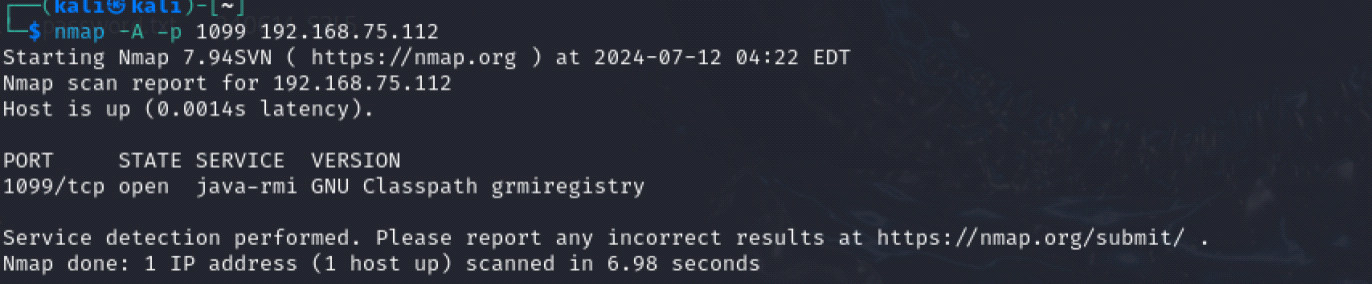
Progetto S7-L5

Traccia: La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si ric hiede allo s tudente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpretersulla macchina remota. I re quis iti dell’e s ercizio s ono: ● La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.75.111 ● La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.75.112 ● Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete. 2) informazioni sulla tabella di routing della macchina vittima.

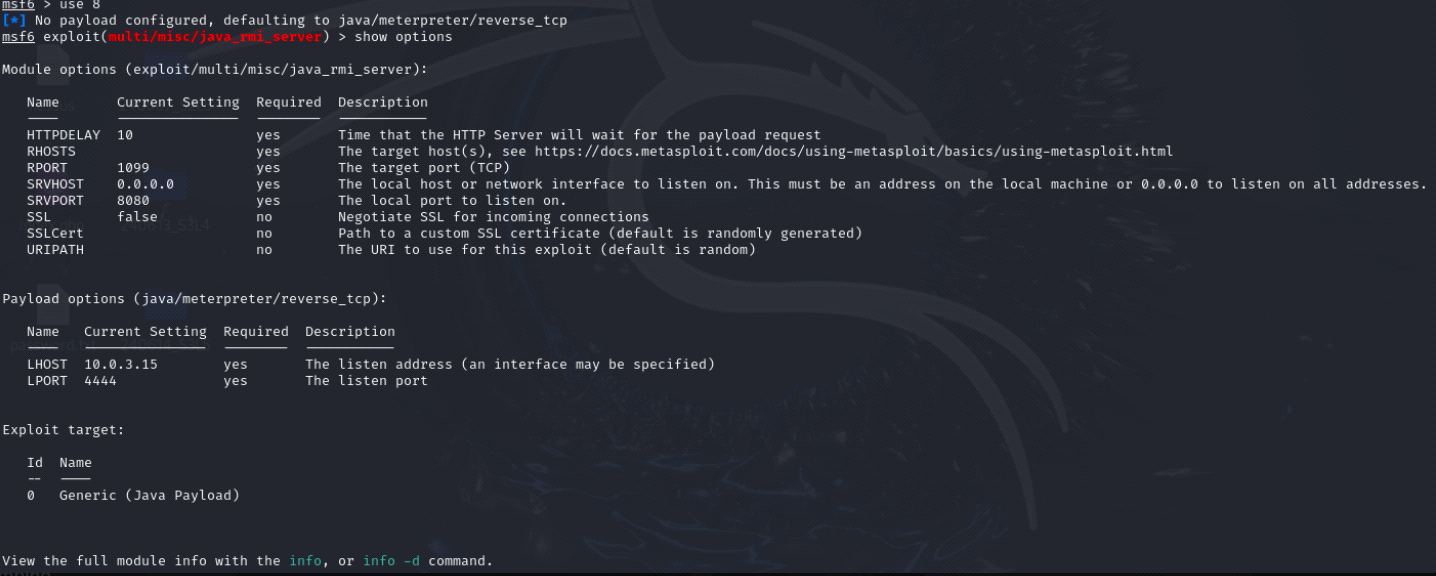
Configurazione rete



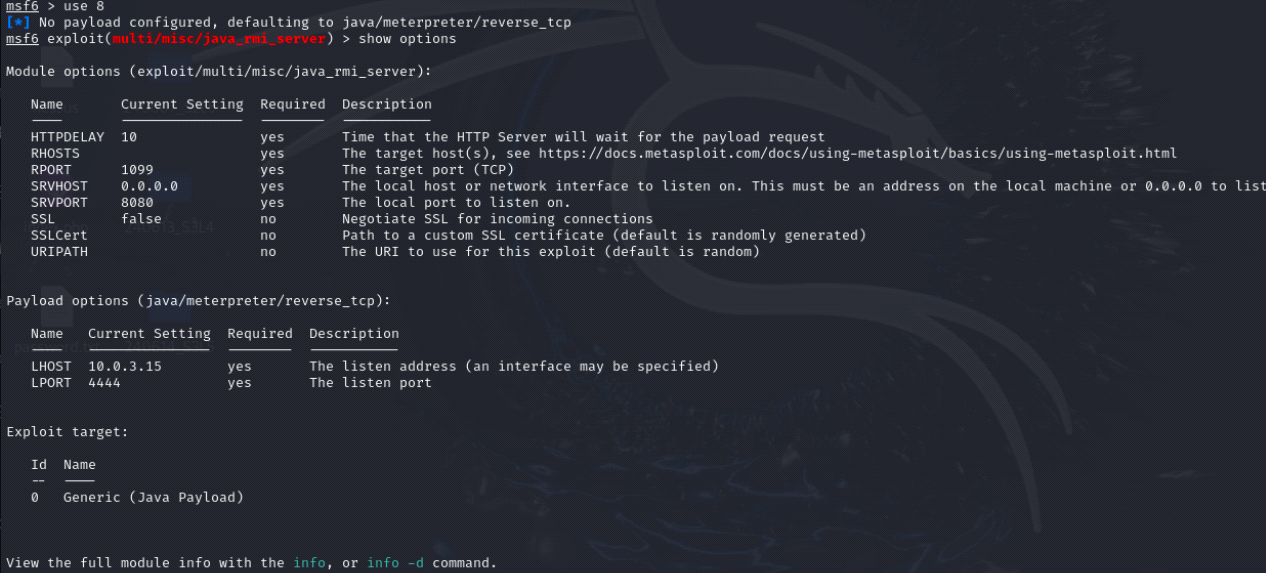


MSFCONSOLE

Cerchiamo il modulo necessario



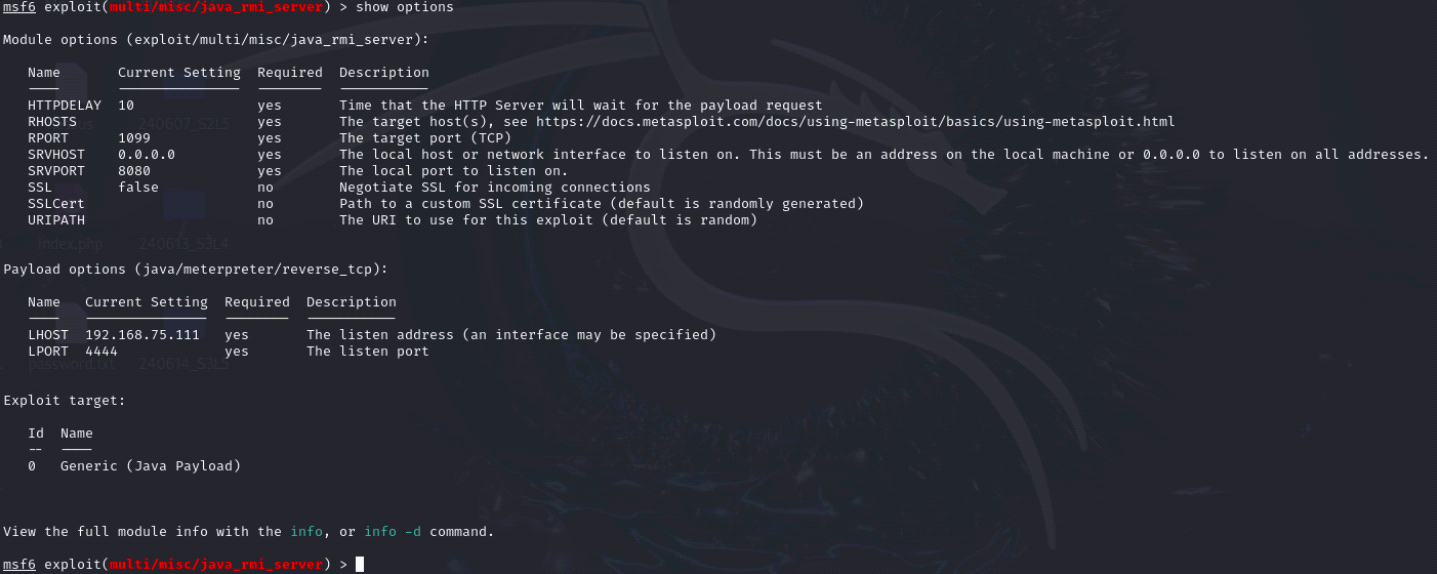
Impostiamo la macchina vittima e facciamo l exploit

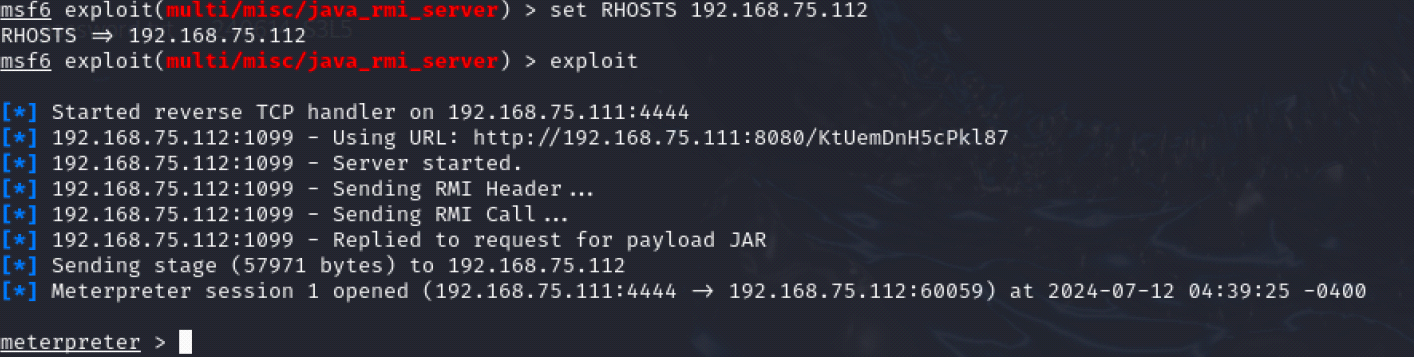


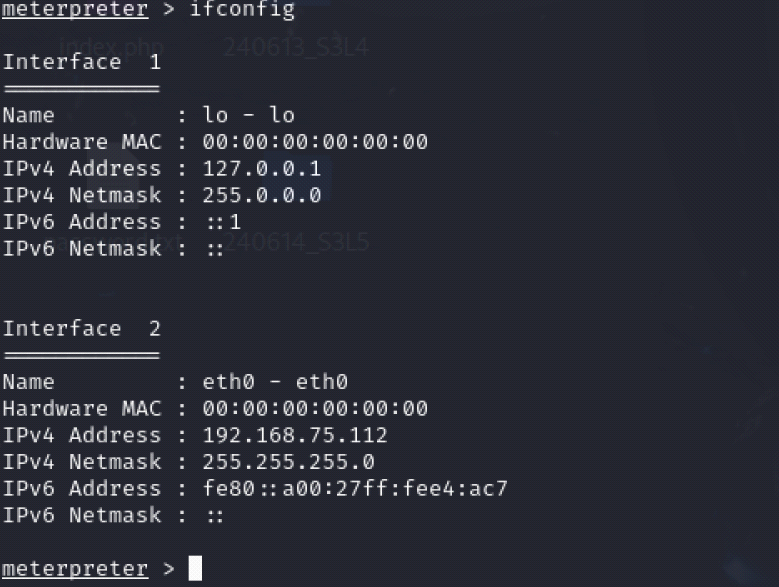
Check

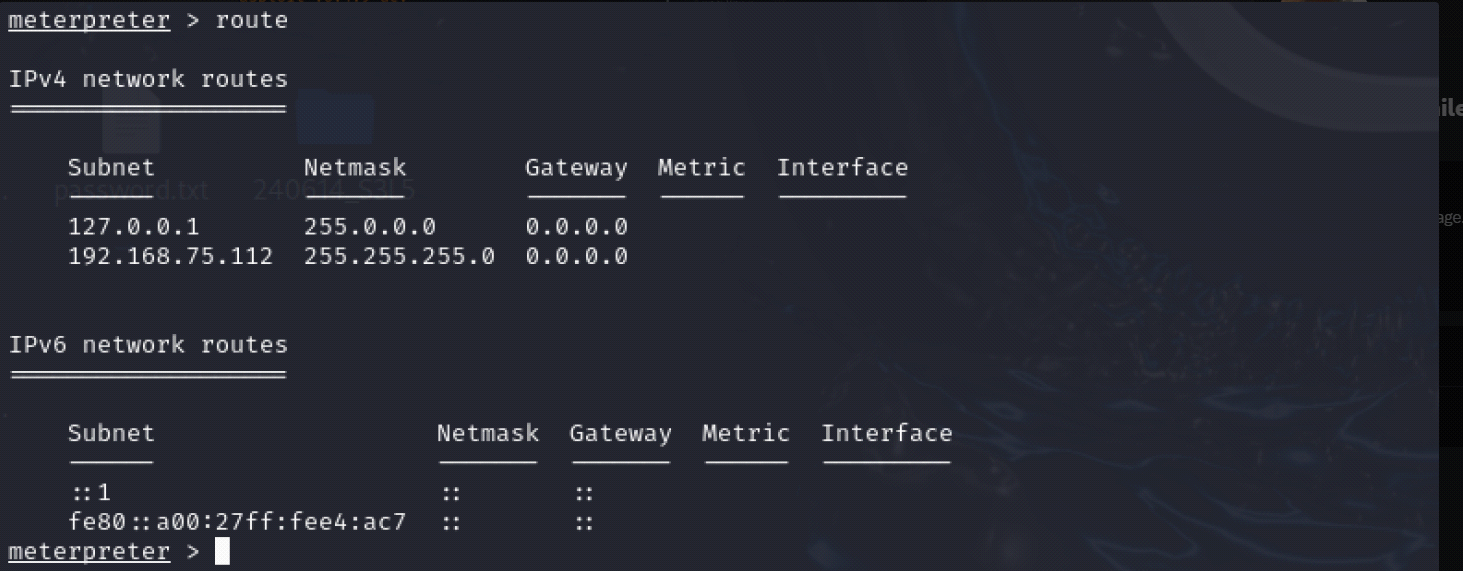
Dopo l avvenuto collegamento,controlliamo di esssere effetivamnete all interno della macchina Target con: route(info sula tabella di routing)

ifconfig









Esercizio 2: Esercizio Traccia e requisiti

Sfrutta la vulnerabilità nelservizio PostgreSQLdiMetasploitable

2. Esegui l'exploit per ottenere una sessione Meterpreter sulsistema target.

Una volta ottenuta la sessione Metarpreter,il tuo compito è eseguire un escalation di privilegi per passare da un utente limitato a root utlizzato solo i mezzi fornitida msfconsole.

Eseguire il comando getuid per verificare l identita dell utente corrente.

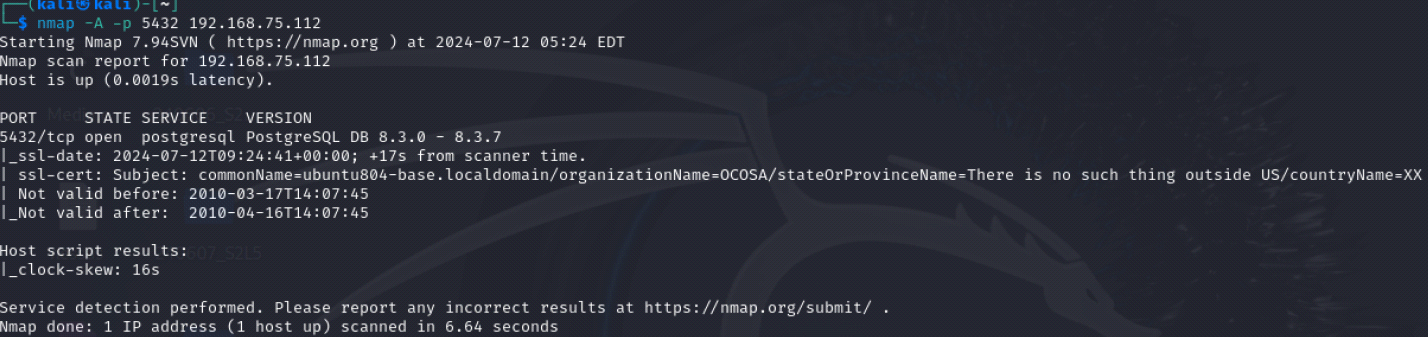
Usa il modulo post di msfconsole per identificare potenziali vulnerabilità locali che possono essere sfruttare per l escaltion di privilige.

esegui l exploit propositi e verifica ogni vulnerabiltà trovata dal modulo spracitato.

Per ogni vulnerabiltà test l escalation di privilegi eseguendo nuovamentegetuid o tentando di eseguire un comando che richiede privilegi di root.

Sempre usando msfconsole installa una backdoor e dimostra che puo accedere ad essa in un momneto successivo.

Andiamo a cercare il modulo corretto e verifichiamo cos altro esiste:



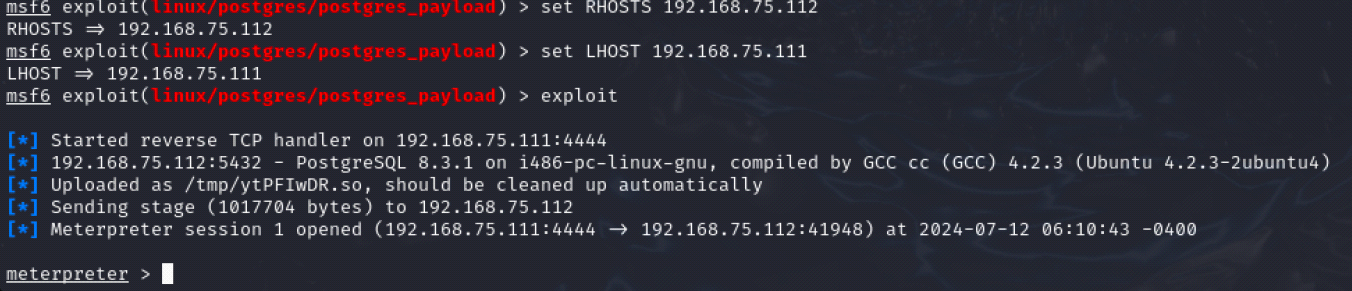
Controlliamo le options richieste da inserire



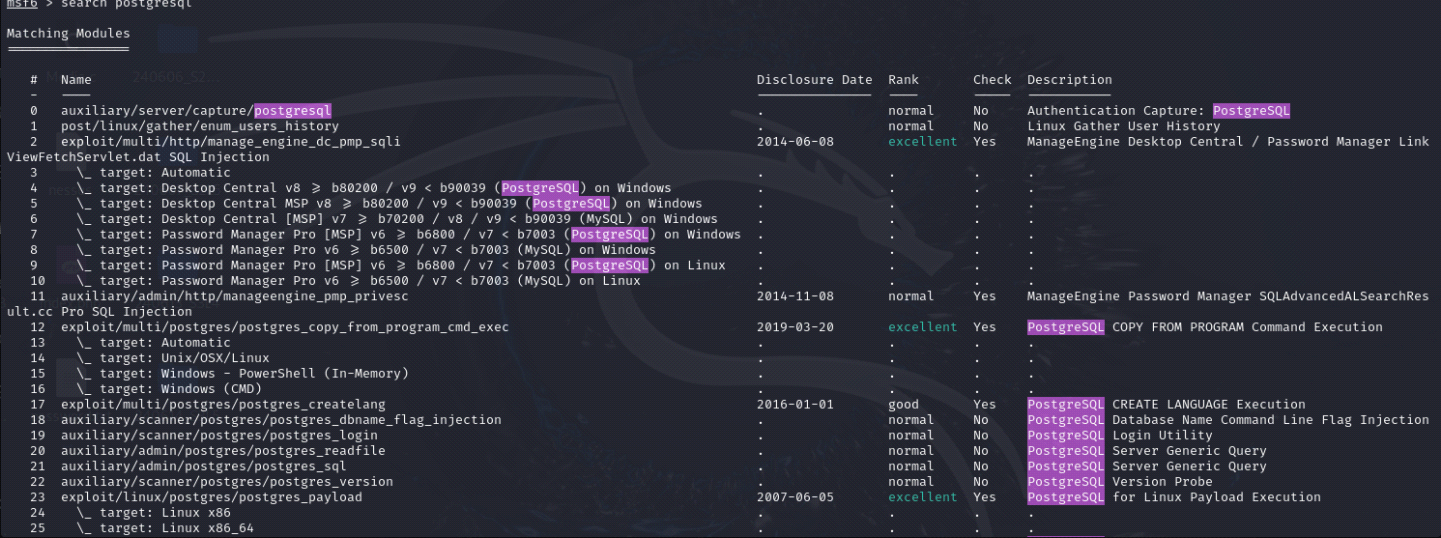
Configuriamo correttemente l exploit con

Set RHOSTS 192.168.11.112

set RHOSTS 192.168.11.111



Scegliamo il playload corretto:



Controlliamo semore la correttezza dell avvenuto exploit

