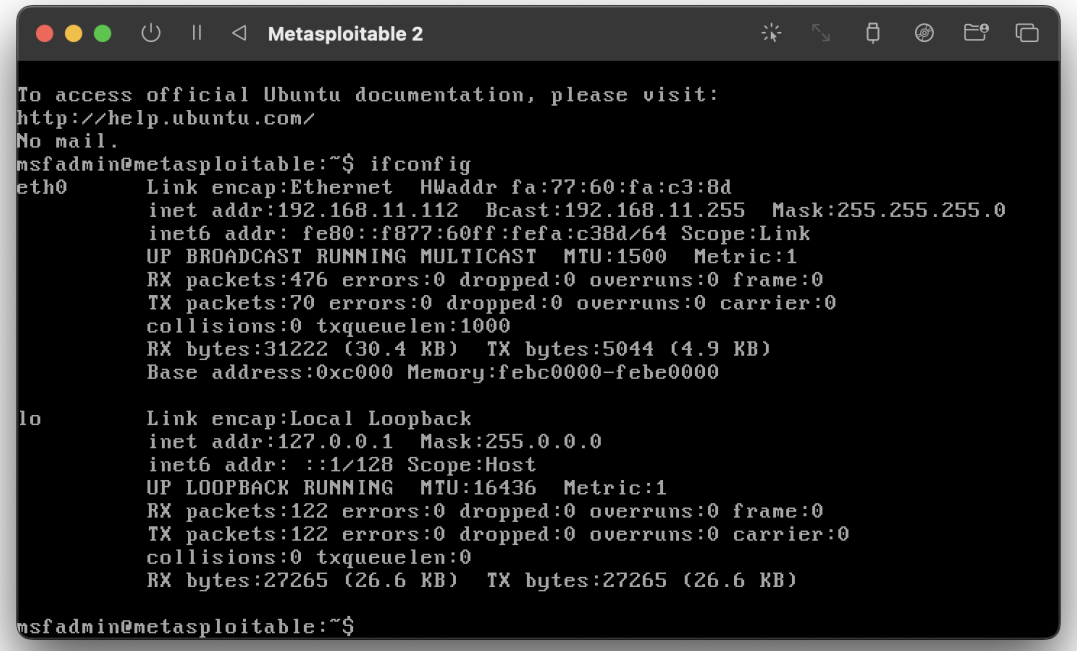
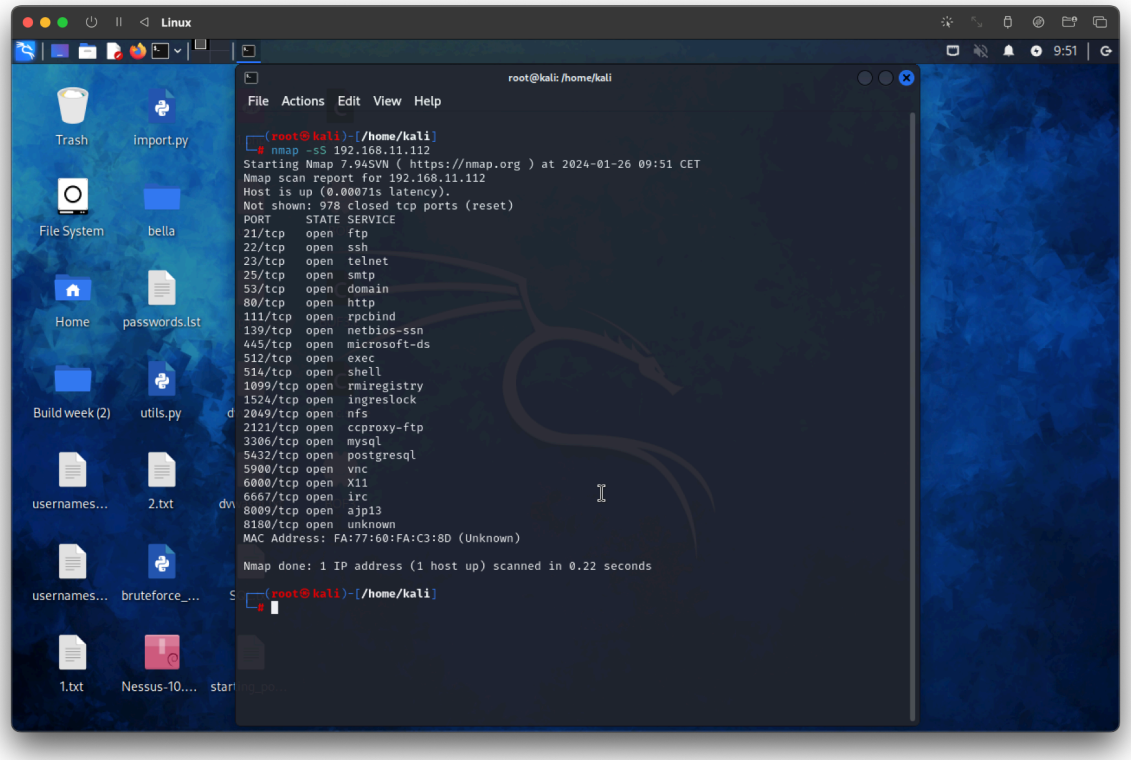
## Exploit della vulnerabilità sulla porta 1099 di Metasploitable 2

Per questo progetto utilizzerò due macchine virtuali con queste configurazioni di rete:
Kali Linux con IP: 192.168.11.111


Metasploitable 2 con IP: 192.168.11.112



Eseguendo una scansione delle varie porte con nmap, questo è il risultato:

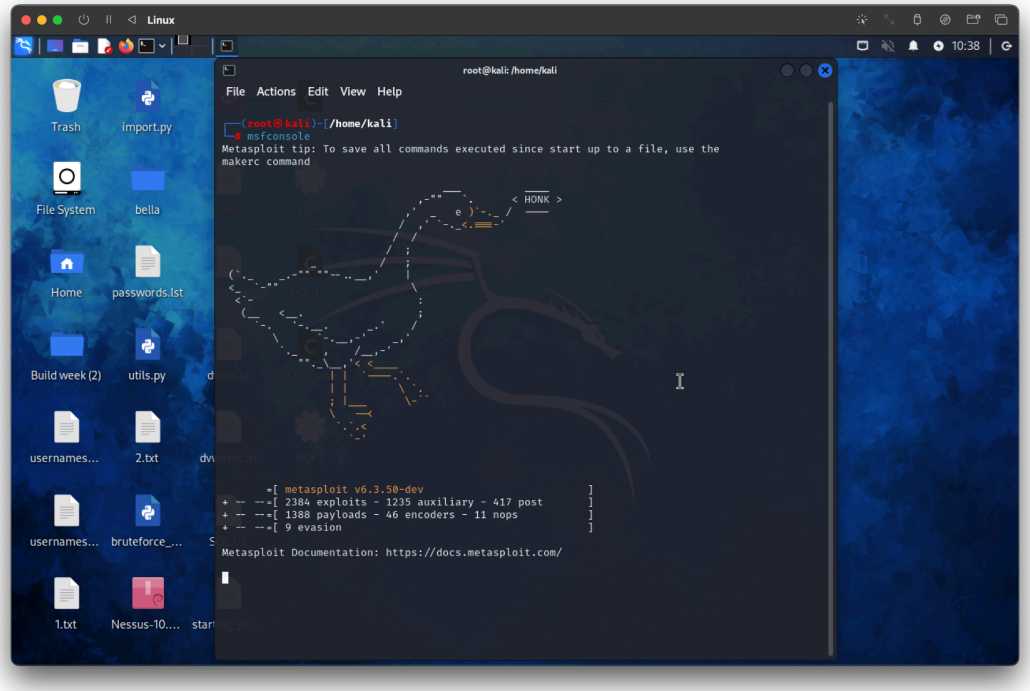



Per questo progetto mi focalizzerò sulla porta 1099/tcp.
É possibile notare che il servizio di questa porta è **rmiregistry**.

Il servizio rmiregistry è un componente del Java Remote Method Invocation (RMI), che è una tecnologia di Java per la comunicazione tra oggetti distribuiti su reti. RMI consente a oggetti Java di invocare metodi su oggetti remoti, consentendo così la comunicazione tra applicazioni distribuite.
Quando un oggetto RMI si registra presso rmiregistry, viene associato a un nome univoco all'interno del registro. Gli oggetti RMI possono essere cercati e ottenuti da altri oggetti utilizzando il loro nome registrato presso rmiregistry.
RMI registry funge quindi  da servizio di registrazione centralizzato in cui gli oggetti RMI possono registrarsi in modo che altri oggetti possano localizzarli.

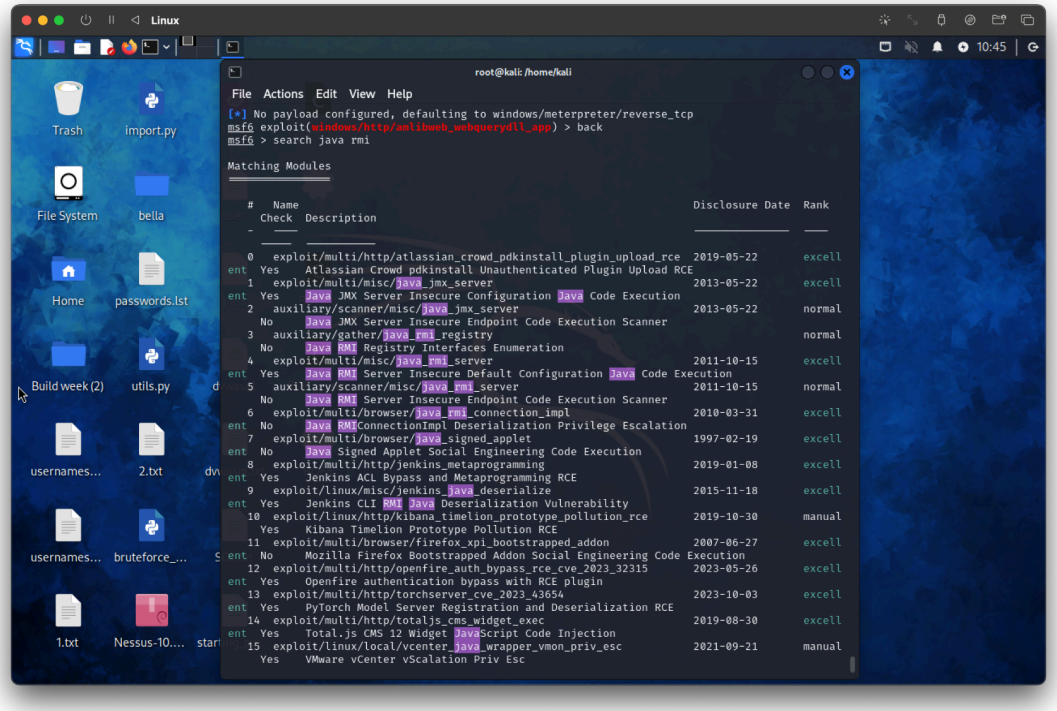
Per procedere all'exploit di questa porta occorre utilizzare un tool chiamato Metasploit.
Metasploit  è un framework open-source usato per il penetration testing e lo sviluppo di exploit.
Fornisce una vasta gamma di exploit creati dalla comunità e numerosi vettori di attacco che si possono utilizzare contro diversi sistemi e tecnologie.
Inoltre, può essere utilizzato per creare ed automatizzare i propri exploit.

Per avviare Metasploit utilizziamo il comando **msfconsole** su linux.

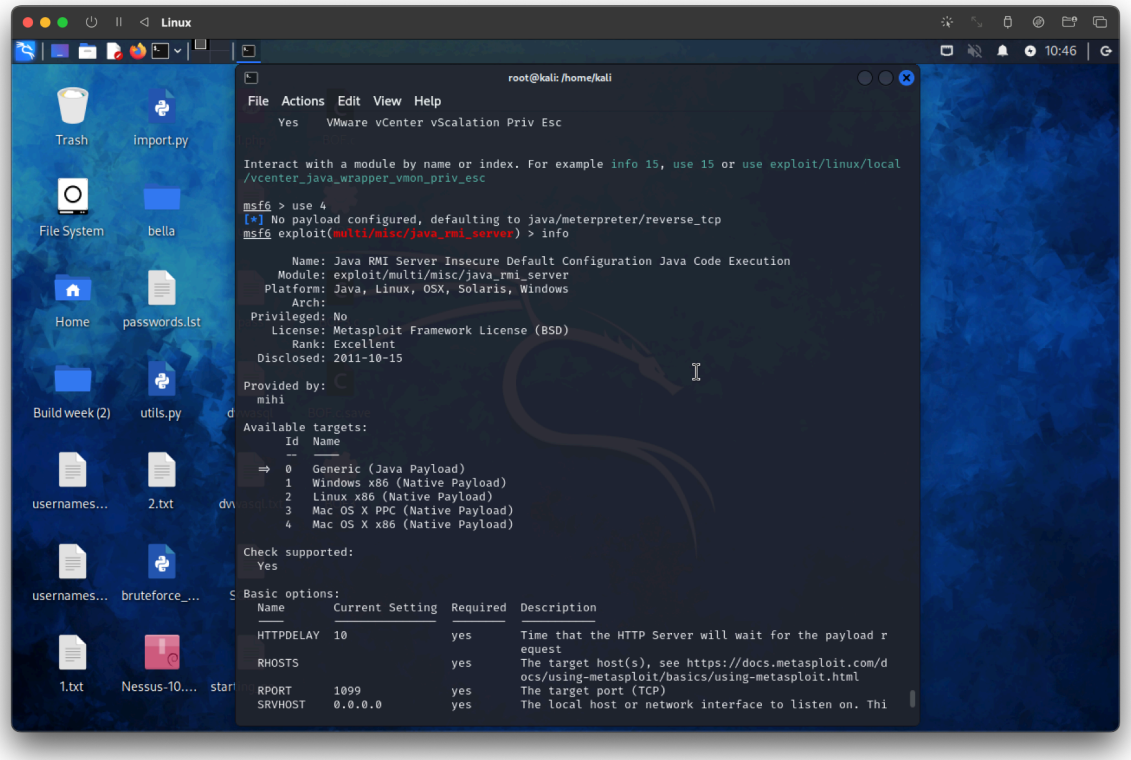


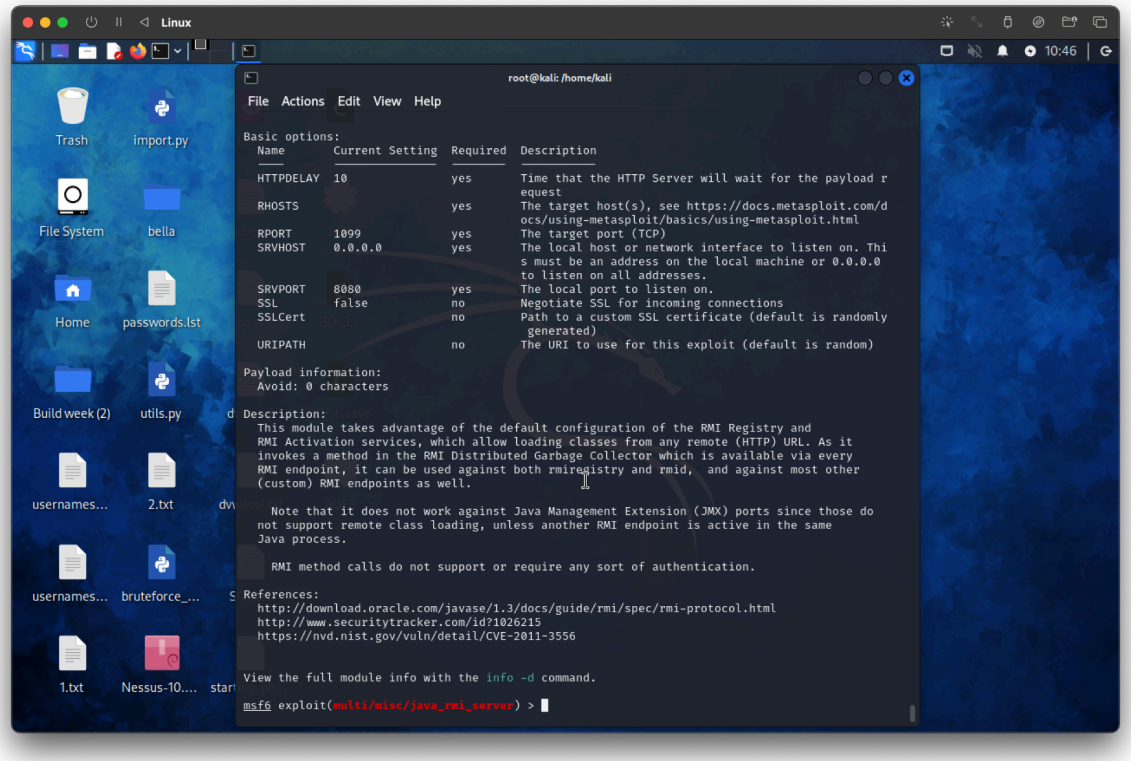

Questa è l'interfaccia di Metasploit da terminale.

Per procedere occorre cercare l'exploit di riferimento al servizio interessato:

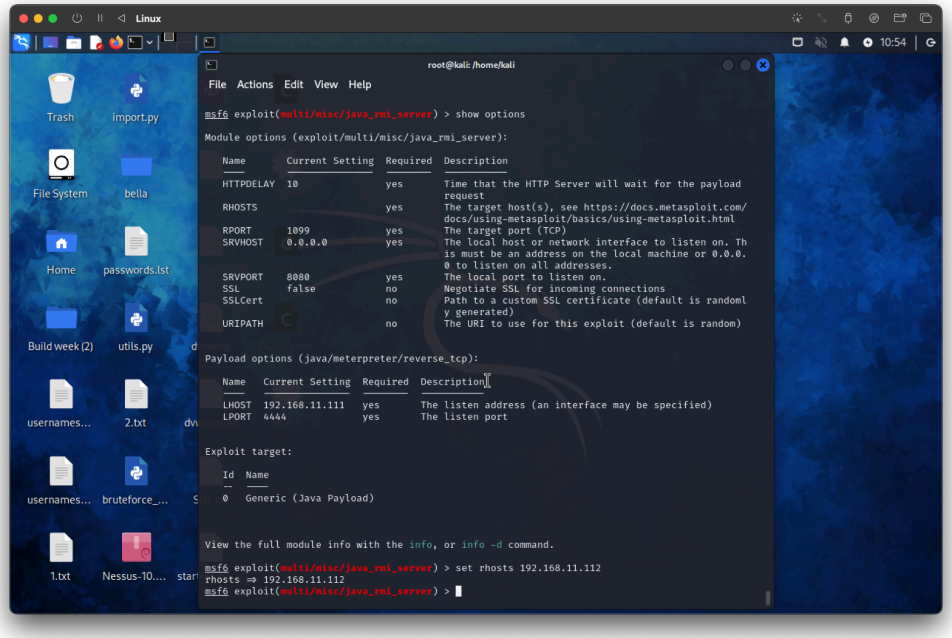


L’exploit a cui sono interessato è il numero 4:

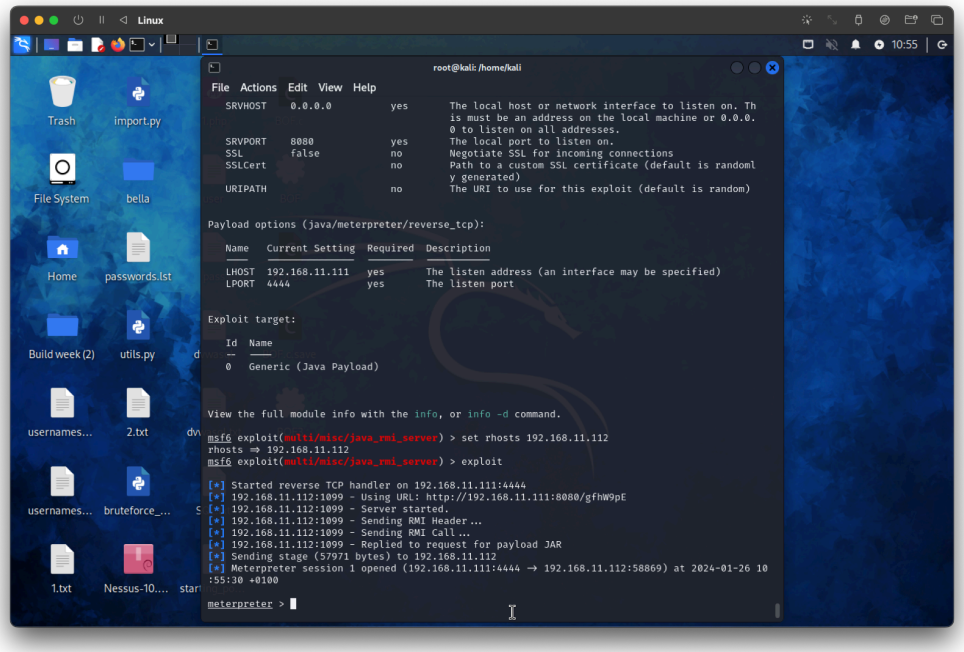


Come è possibile notare, utilizzando il comando **info,** Metasploit restituisce le informazioni riguardo l'exploit e le impostazioni che si possono modificare in base al target di riferimento.
Ora che ho identificato l'exploit da utilizzare occorre impostare il target dell'exploit; in questo caso utilizzeremo la macchina virtuale Metasploitable 2 come target con indirizzo IP: 192.168.11.112
Per impostare il target utilizzerò il comando **show options**, seguito da **set rhosts 192.168.11.112.**




Una volta modificate le impostazioni è possibile avviare l'exploit con il comando **exploit**.



Come è possibile notare l'exploit è riuscito infatti è stata avviata una sessione meterpreter nella macchina target.
Con alcuni comandi è possibile ottenere informazioni sulla macchina target.
Con il comando **ifconfig** otteniamo le informazioni sulla configurazione di rete della macchina target e con il comando **route** la tabella di routing della macchina target.