di Giulio Zanet

S7L5: exploit JAVA RMI

exploit java tramite Metasploit e Meterpreter

Fasi del progetto

Scansione

Scansione di porte e servizi tramite nmap.

Metasploit

Avvio del framework Metasploit

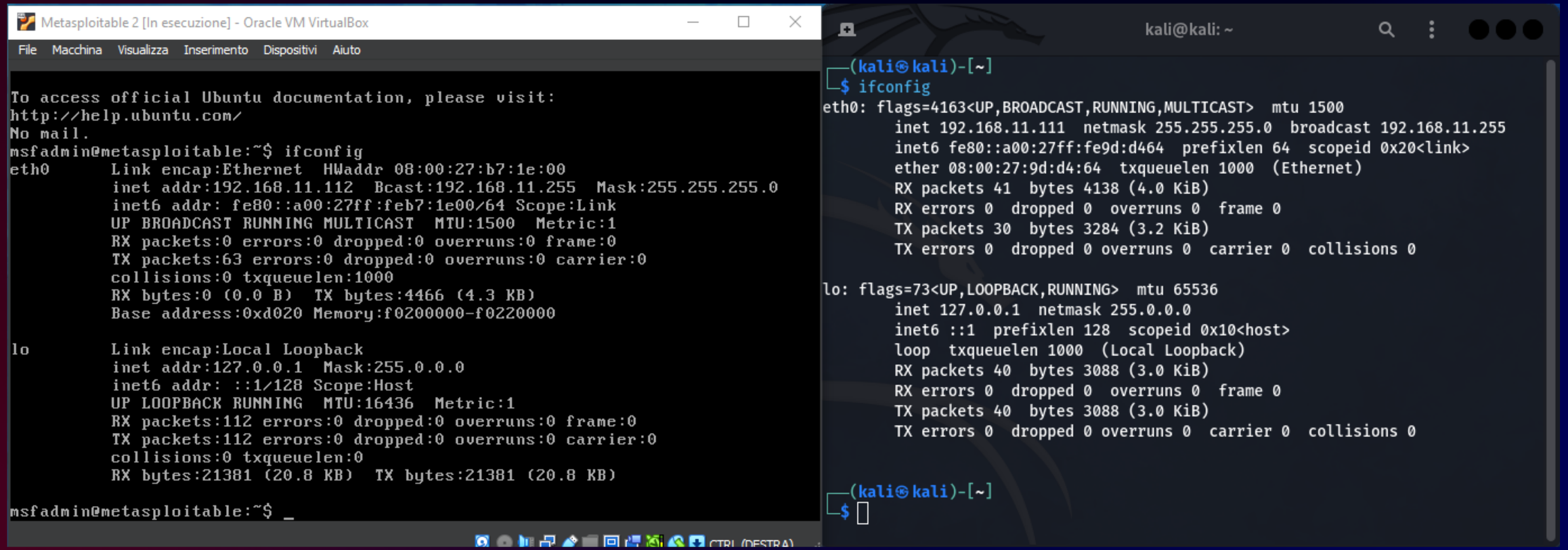
Ricerca

Ricerca e configurazione dell'exploit di java mri

Exploit

Avvio dell'exploit, conclusioni

Cambio degli indirizzi ip

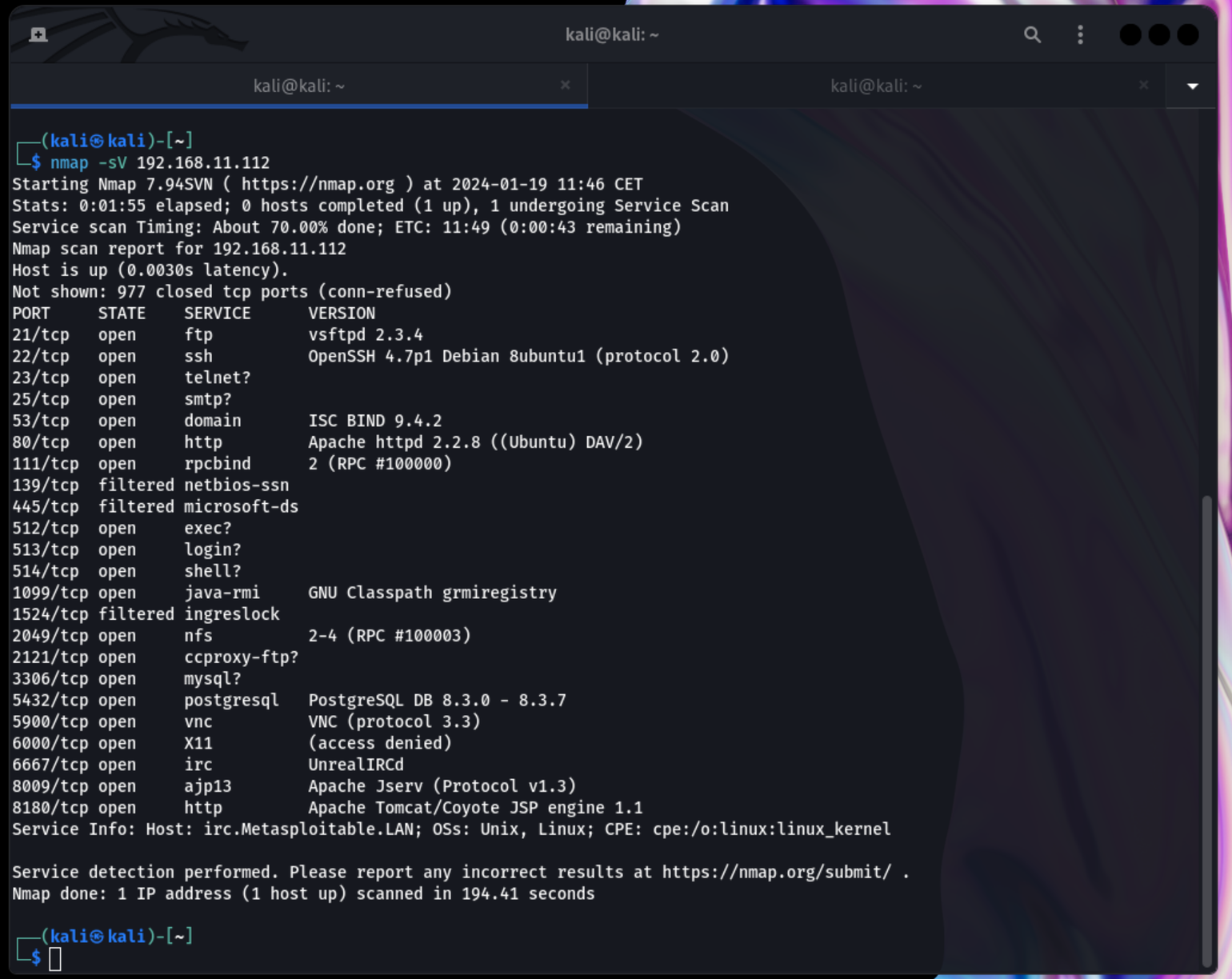


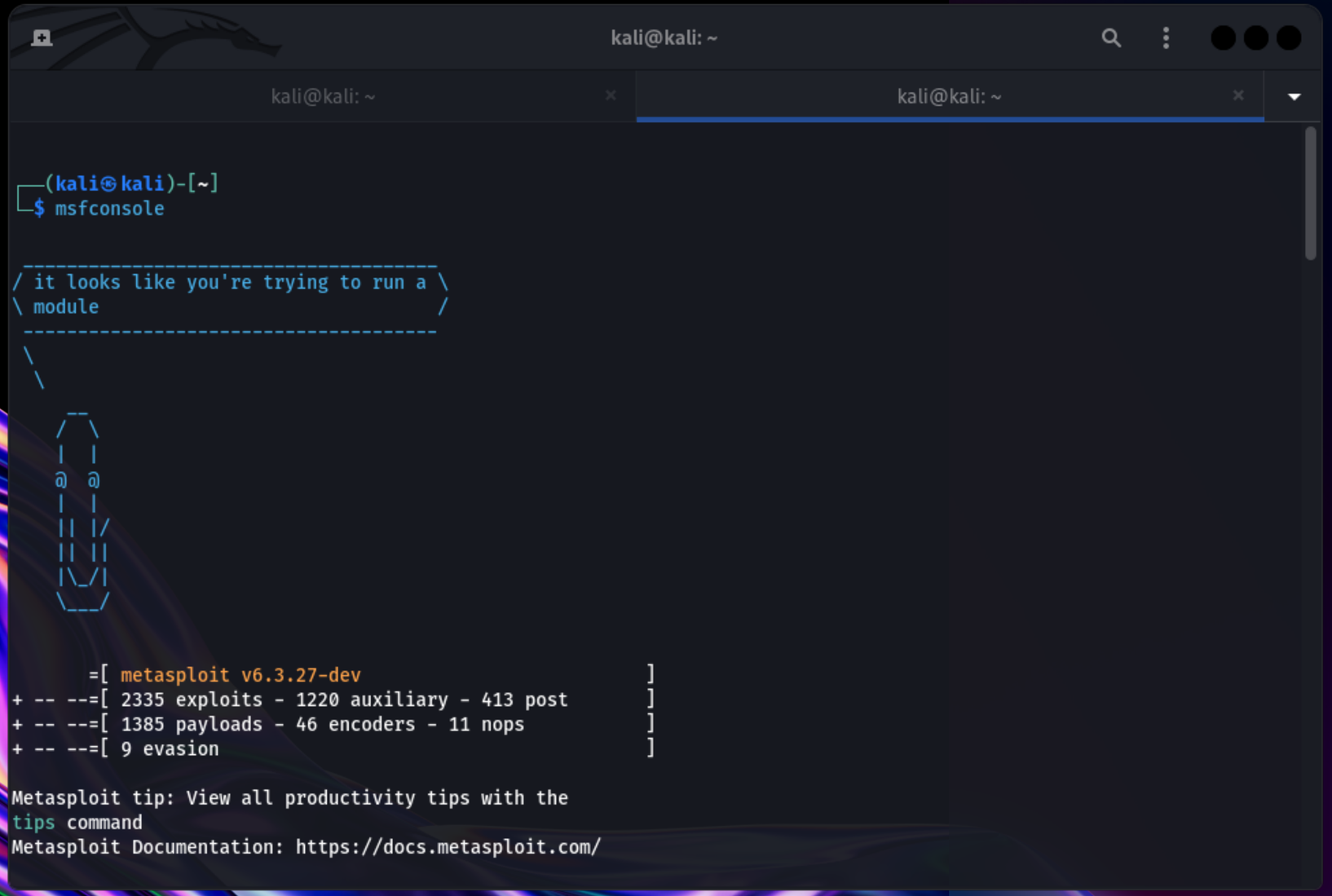
Come da consegna cambio l'indirizzo ip di entrambe le macchine: 192.168.11.111 per Kali e 192.168.11.112 per Meta

NMAP

Tramite nmap effettuo una scansione sulla macchina Meta alla ricerca del servizio java RMI; un'API Java che esegue l'invocazione di metodi remoti.

A scansione finita possiamo confermare che il servizio è attivo e in ascolto sulla porta 1099, quindi è possibile avanzare.





METASPLOIT

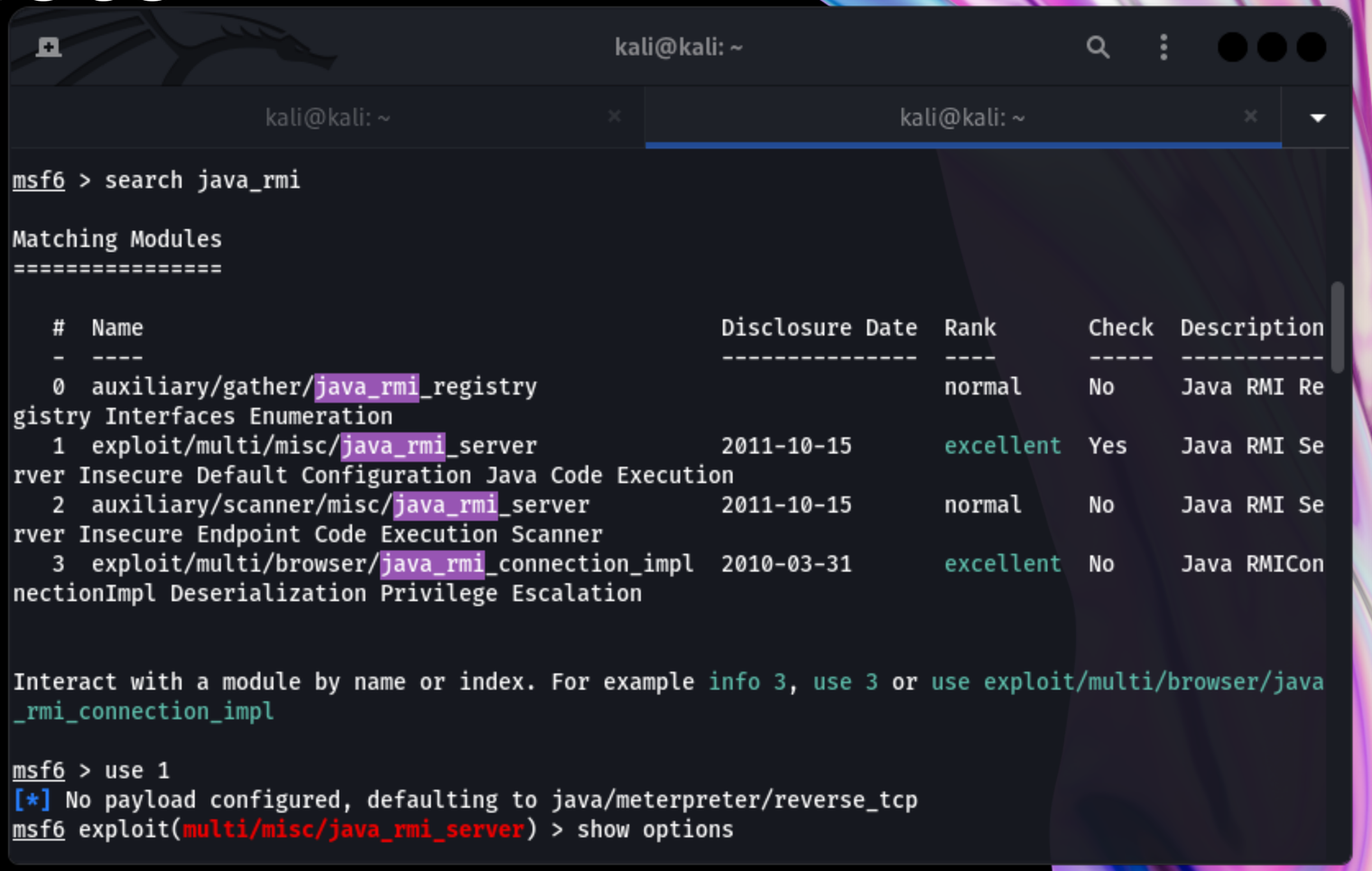
Metasploit Framework è una piattaforma open source che supporta la ricerca di vulnerabilità, lo sviluppo di exploit e la creazione di strumenti di sicurezza personalizzati.

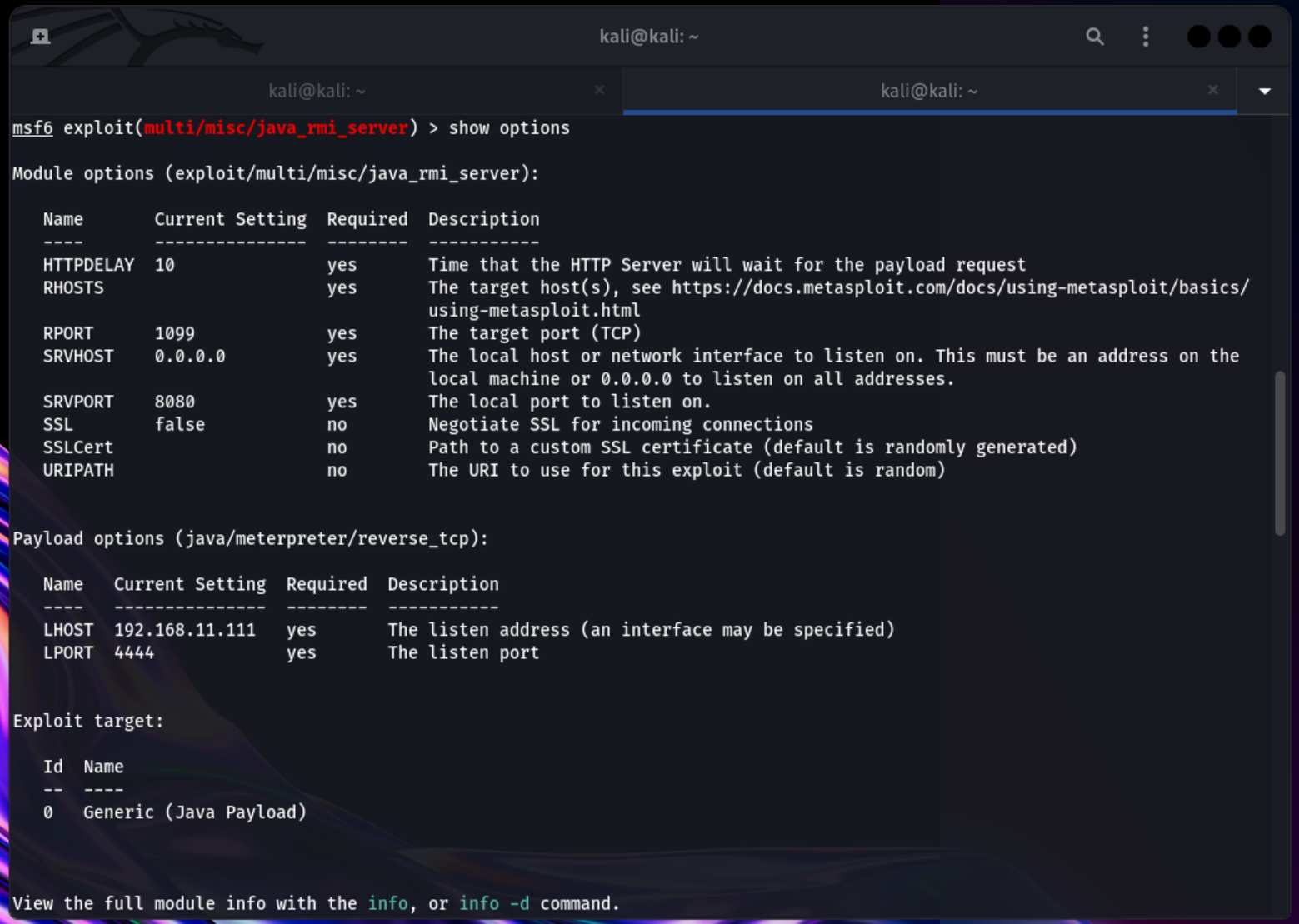
per la consegna di oggi utilizzeremo un modulo per java già presente all'interno di metasploit

Ricerca del modulo

Con il comando “search” controllo se è presente l’exploit necessario per l’esercizio di oggi. Scelgo il modulo numero 1 e lo avvio con il comando “use 1”.

Alternativamente è possibile utilizzare “use exploit/multi/misc/java_mri_server”



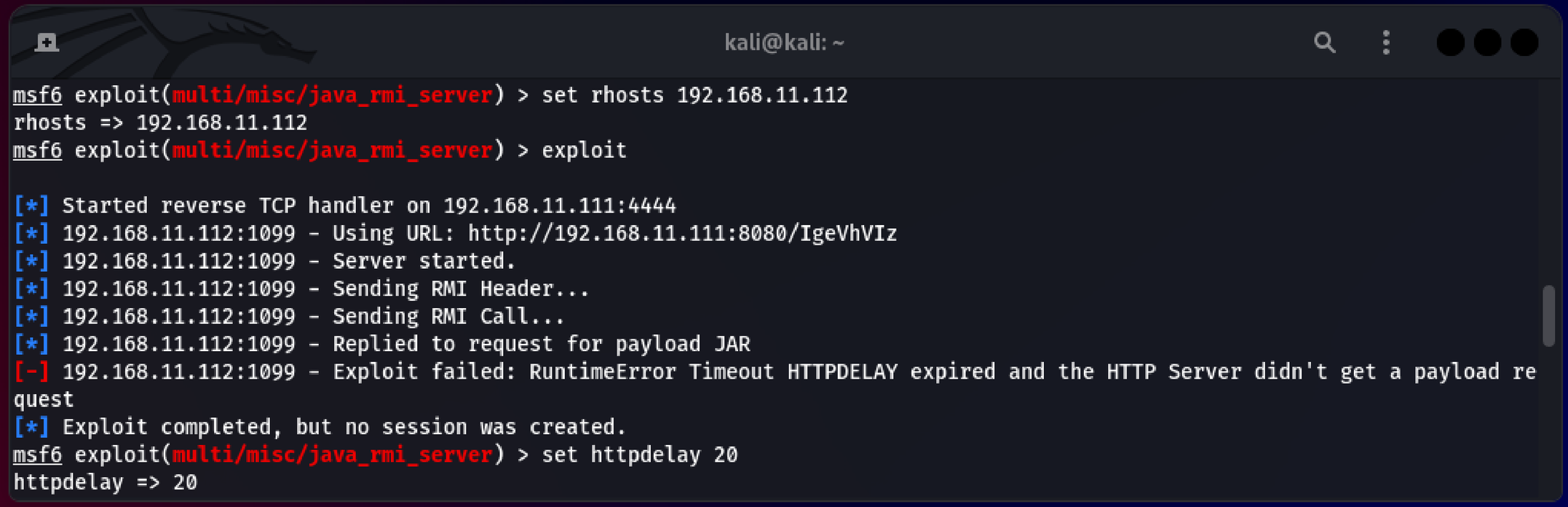


Configurazione

Tramite il comando “show options” è possibile controllare i parametri utilizzati dal modulo e dal suo payload, ovvero un frammento di codice eseguibile dall’exploit.

Nel caso di oggi utilizzerò il payload “meterpreter/reverse_tcp”.

Avvio dell'exploit



Quasi tutti i parametri posseggono già un valore di default, tranne rhost, l'indirizzo ip target, quindi procedo a cambiarlo tramite il comando "set". Procedo poi ad avviare l'exploit, ma fallisce per via di un errore di timeout.

Per risolverlo basta semplicemente aumentare l'httpdelay a 20 secondi rispetto ai precedenti 10.

Raccolta informazioni

Ritentanto l'exploit stavolta la connessione ha successo: meterpreter apre una shell avanzata che mi permette di ottenere informazioni sulla macchina bersaglio e, in questo caso, anche gli indirizzi ip delle altre macchine nella sua stessa rete.