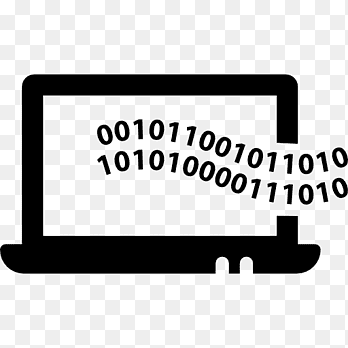
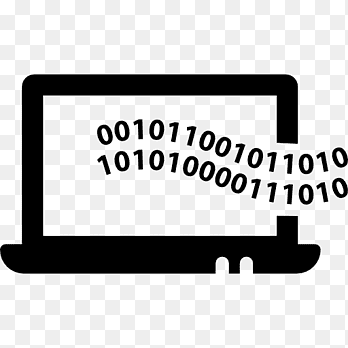
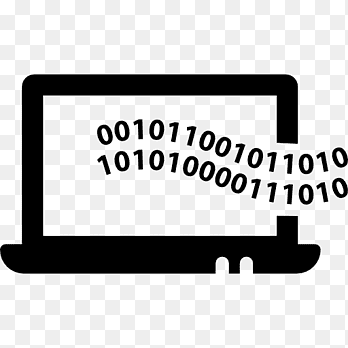
La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

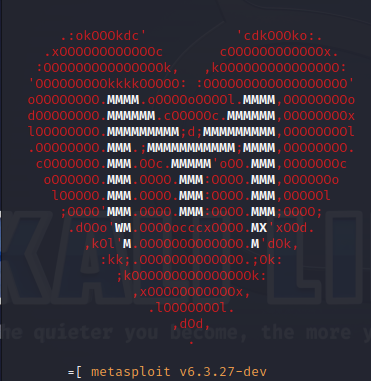
Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:

1) configurazione di rete.

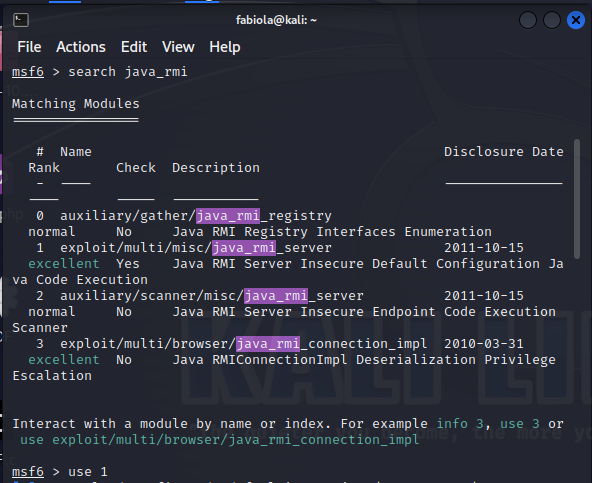
2) informazioni sulla tabella di routing della macchina vittima.

Sulla porta 1099 TCP della nostra Metasploitable è attivo un servizio Java-RMI, che è una tecnologia che consente a diversi processi Java di comunicare tra di loro attraverso una rete. La vulnerabilità in questione è dovuta ad una configurazione di default errata che permette ad un potenziale attaccante di eseguire codice arbitrario sul sistema bersaglio, potenzialmente prendendo il controllo completo del sistema o eseguendo altre attività malevole.

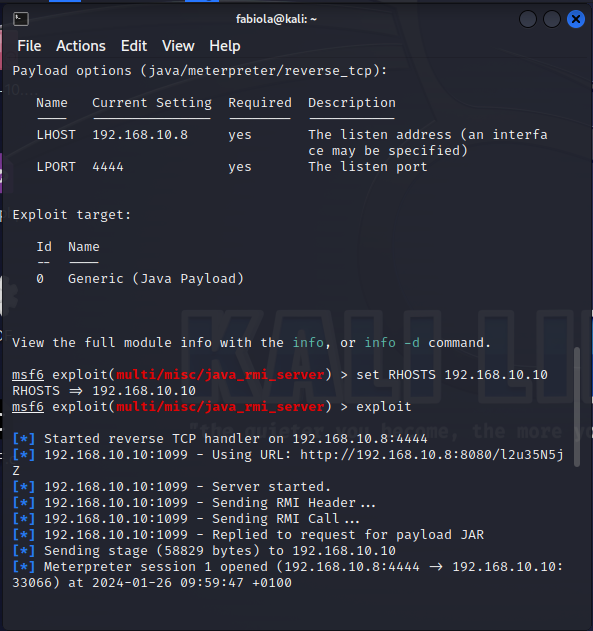


Facciamo partire **Metasploit** da console con il comando **msfconsole**, e cerchiamo utilizzando la keyword «**search**», un exploit che possa fare al nostro caso. Nella fattispecie, utilizziamo il comando «**search java\_rmi**». Il più interessante per noi sembra essere l’exploit in **riga 1** che nella descrizione riporta «default configuration code execution». Utilizziamolo con il comando «**use**» seguito dal path dell’exploit:



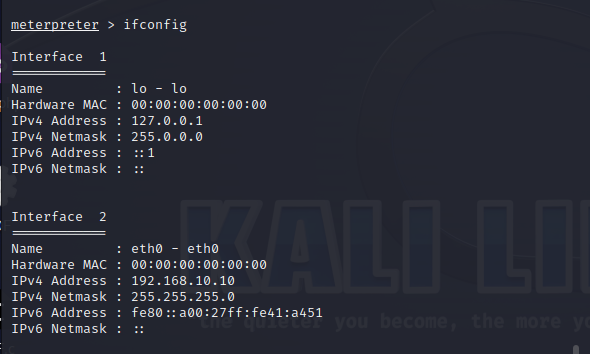
Controlliamo le opzioni da inserire utilizzando come al solito il comando «**show options**», e configuriamo il parametro **RHOSTS** con l’indirizzo della macchina target, ed il parametro **LHOST** con l’indirizzo della macchina attaccante (che in questo caso ha già impostato per conto suo).

Una volta che abbiamo configurato tutte le impostazioni ed i parametri, possiamo lanciare l’attacco con il comando «**exploit**»:

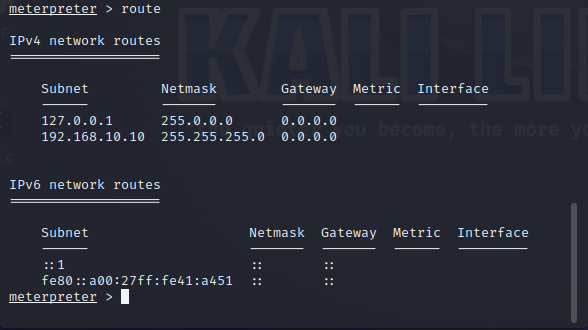
 

Abbiamo ricevuto una shell di Meterpreter. Facciamo un paio di test per confermare che siamo sulla macchina target.

Il comando «**ifconfig**» che come abbiamo visto ci restituisce la configurazione di rete della macchina, indica che siamo sulla macchina con IP 192.168.10.10 che sappiamo essere la nostra macchina Metasploitable nel nostro laboratorio virtuale.:



Per ottenere informazioni sulla tabella di routing della macchina vittima utilizzando Meterpreter, puoi sfruttare il comando «**route**»:



Facciamo un po’ di chiarezza su alcuni punti. Prima di tutto cos’è Metasploit?

**Metasploit** è un framework open-source per lo sviluppo e l'esecuzione di exploit. È una delle suite di strumenti più utilizzate nel campo della sicurezza informatica, utilizzata per testare la sicurezza dei sistemi, per la ricerca delle vulnerabilità e per l'esecuzione di operazioni di penetration testing.

È **modulare**, il che significa che è composto da una serie di moduli che possono essere utilizzati in modo flessibile per sfruttare le vulnerabilità, eseguire l'accesso remoto ai sistemi, raccogliere informazioni, eseguire attacchi di phishing e molto altro ancora; dispone di un **database** integrato per archiviare informazioni su host, vulnerabilità e risultati degli attacchi e include una vasta raccolta di exploit, che coprono una vasta gamma di sistemi operativi, servizi e applicazioni.

Questo rende Metasploit una risorsa preziosa per gli operatori di sicurezza informatica per testare la vulnerabilità dei sistemi.

Per **Exploit** si indicano moduli progettati per *sfruttare vulnerabilità specifiche* nei software o nei sistemi operativi al fine di ottenere l'accesso non autorizzato o eseguire determinate azioni sul sistema bersaglio.

Si distingue dal **Malware**, che è progettato per *danneggiare o compromettere i sistemi attraverso l'installazione di software* dannoso. Entrambi sono pericolosi per la sicurezza informatica e richiedono una risposta rapida e adeguata a mitigare i danni potenziali.

Ad un attacco di successo segue l’apertura di una sessione di **Meterpreter,** strumentoprogettato per consentire a un attaccante di *mantenere l'accesso persistente* a un sistema compromesso, offrendo una vasta gamma di funzionalità per eseguire attività dannose, raccogliere informazioni, sfruttare vulnerabilità e altro ancora.