# **Java rmi vulnerabilità**

Abbiamo scansionato la macchina Meta con il tool Nmap per analizzare le porte aperte e quali servizi girassero dietro di esse. Dopo la scansione, abbiamo notato la presenza di una porta aperta con servizio Java RMI, sulla porta 1099.

**Cos'è Java RMI?**

RMI è una tecnologia potente che consente di creare applicazioni distribuite in Java. RMI è spesso utilizzata per creare applicazioni Client-Server, ma può essere utilizzata anche per creare applicazioni distribuite in cui più computer collaborano per eseguire un'attività comune.

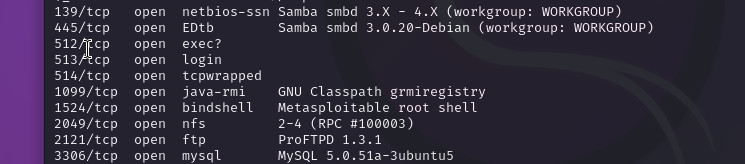
**Perché è pericoloso l'exploit?**

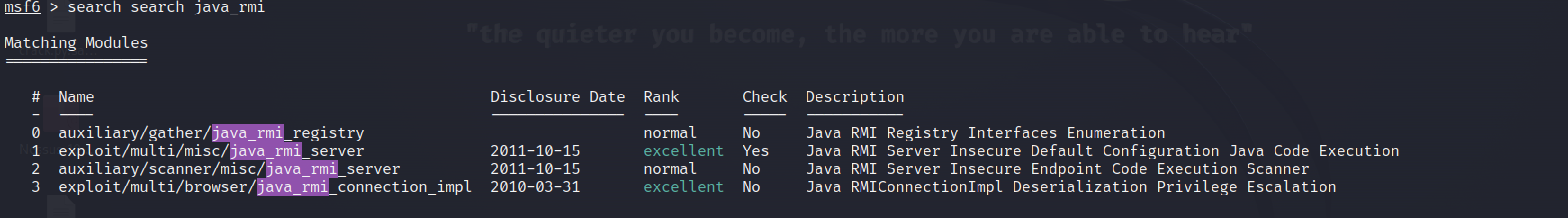
L'exploit è molto pericoloso in quanto permette a un black hat di caricare un payload e avere accesso su una determinata macchina. Dopo di che, potrebbe collegarsi a un processo primario e prenderne completamente il controllo. Tutto ciò sarebbe di difficile individuazione, permettendo anche a quest'ultimo di accendere qualsiasi volta lui voglia.

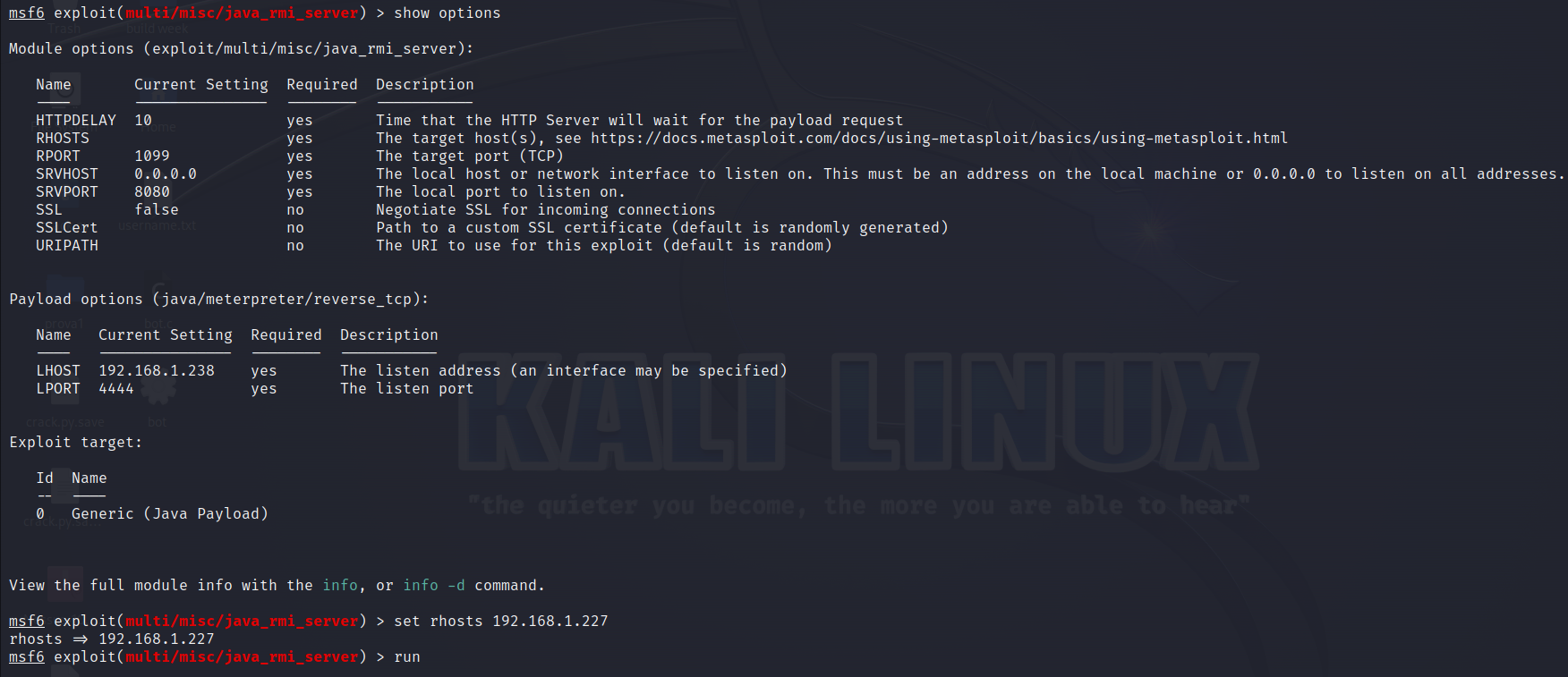
Spiegazione dell'exploit

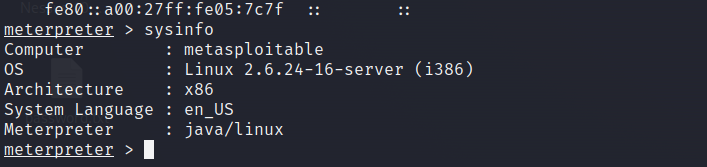
L'exploit sfrutta una vulnerabilità nota in Java RMI. Questa vulnerabilità consente a un utente malintenzionato di inviare un messaggio dannoso a un server RMI. Il messaggio dannoso può contenere un payload, che è un codice che viene eseguito dal server RMI.

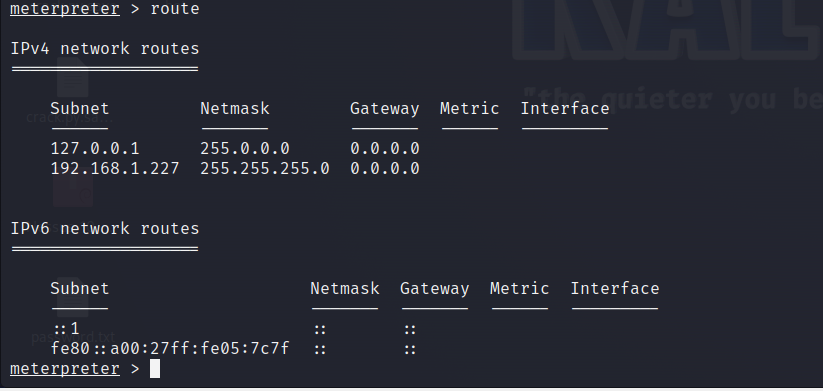
Quando il server RMI esegue il payload, il black hat può ottenere l'accesso al server. Il black hat può quindi utilizzare il server per eseguire qualsiasi azione che desideri, come rubare dati, installare malware o interrompere il servizio. Ora vi allego gli screen dei vari processi e poi vi darò dei consigli per mitigare le vulnerabilità

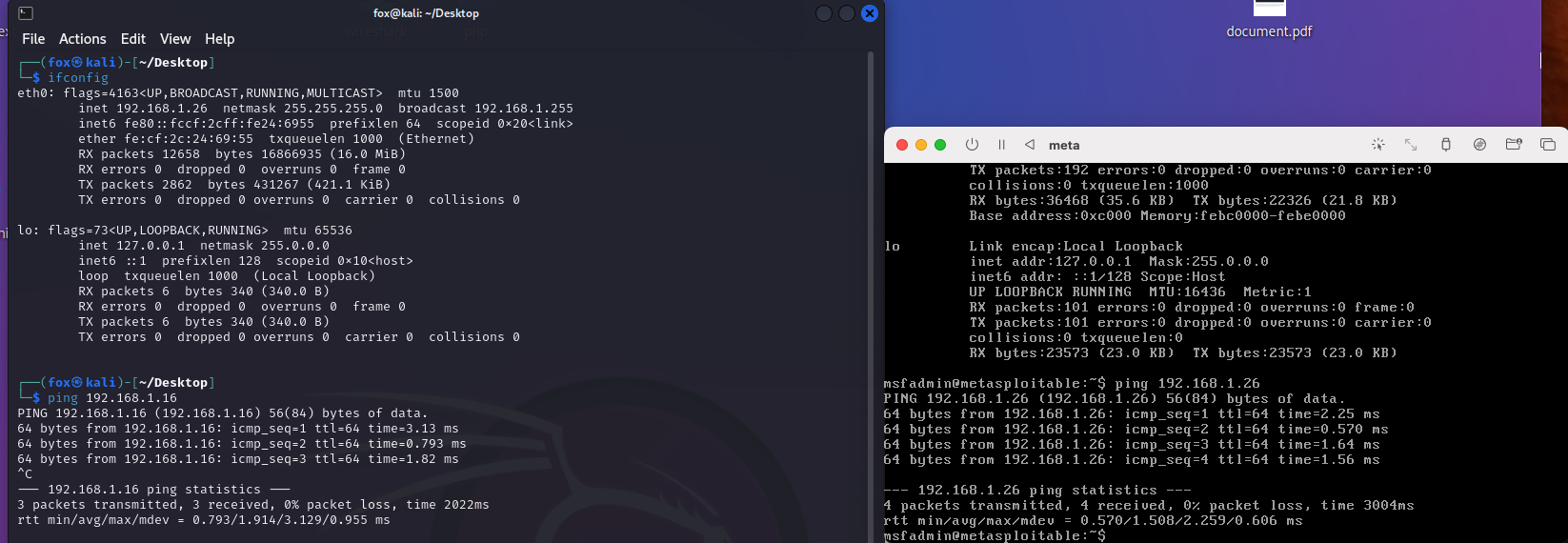












CONSIGLI

Eccovi una lista sulle metodologie da attuare per mitigare questa vulnerabilità

* Tenere aggiornato il software RMI. Oracle rilascia regolarmente aggiornamenti per RMI per correggere le vulnerabilità. È importante installare questi aggiornamenti il prima possibile per proteggersi da attacchi informatici.
* Utilizzare un firewall per limitare l'accesso a RMI. Un firewall può aiutare a bloccare gli attacchi informatici che mirano a RMI.
* Utilizzare la crittografia per proteggere i dati scambiati tramite RMI. La crittografia può aiutare a proteggere i dati da attacchi informatici che mirano a rubare dati.
* Implementare controlli di accesso rigorosi per RMI. I controlli di accesso possono aiutare a limitare l'accesso a RMI solo a utenti autorizzati.
* Eseguire audit regolari di RMI. Gli audit regolari possono aiutare a identificare e correggere eventuali vulnerabilità che potrebbero essere presenti in RMI.