Relazione sull'attività di sfruttamento di una vulnerabilità tramite Metasploit

L'obiettivo dell'esercizio è stato quello di sfruttare una vulnerabilità presente sulla porta 1099, relativa al servizio Java RMI della macchina Metasploitable. Attraverso l'uso del framework Metasploit, si richiede di ottenere una sessione **Meterpreter** sulla macchina remota, permettendo così l'accesso per eseguire comandi e raccogliere informazioni di rete.

Ambiente di lavoro e configurazione:

- **Macchina attaccante (Kali Linux)**:
  - Indirizzo IP: **192.168.11.111**
- **Macchina vittima (Metasploitable)**:
  - Indirizzo IP: **192.168.11.112**

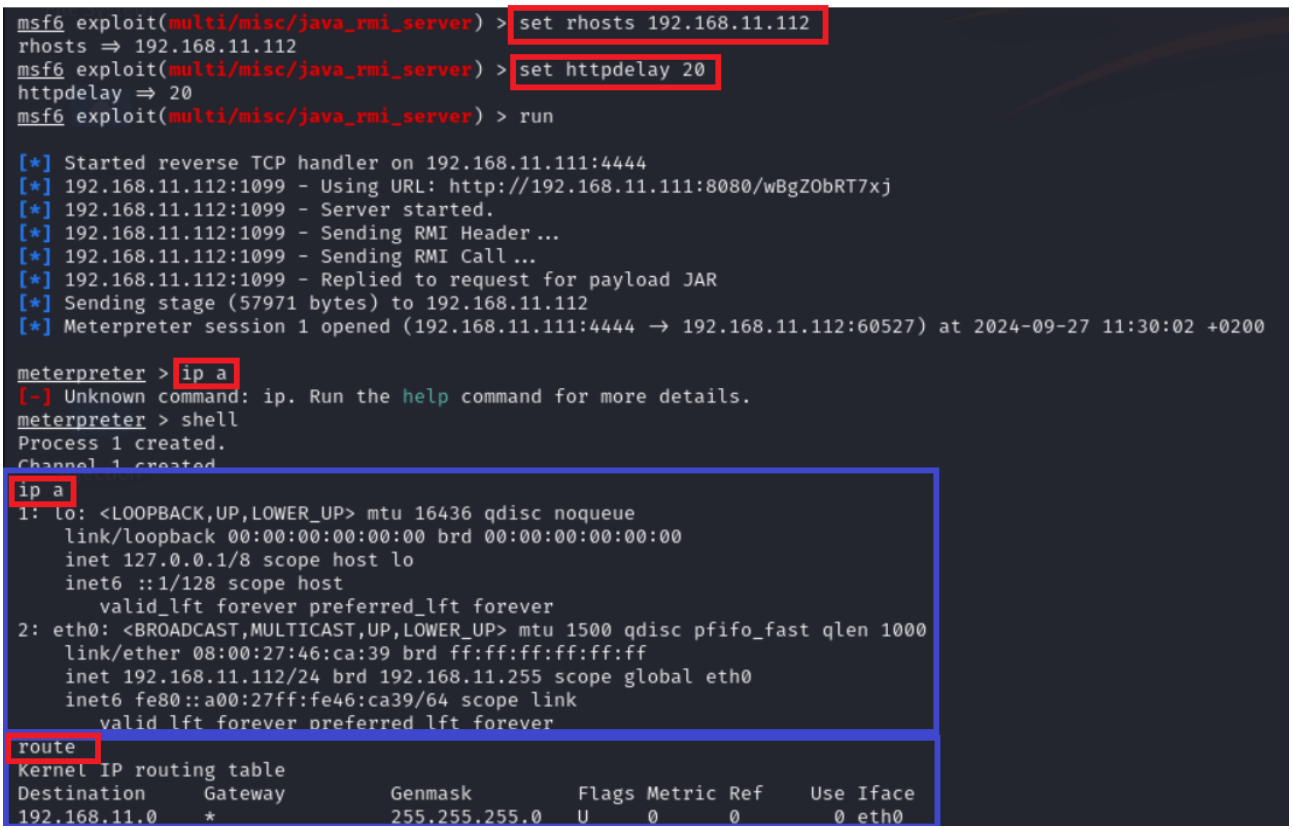
```
msf6 > search Java RMI

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent  Yes    Atlassian Crowd p
dkinstall Unauthenticated Plugin Upload RCE
   1   exploit/multi/http/crushftp_rce_cve_2023_43177        2023-08-08       excellent  Yes    CrushFTP Unauthen
ticated RCE
   2     \_ target: Java                                     .                .          .      .
   3     \_ target: Linux Dropper                            .                .          .      .
   4     \_ target: Windows Dropper                          .                .          .      .
   5   exploit/multi/misc/java_jmx_server                    2013-05-22       excellent  Yes    Java JMX Server I
nsecure Configuration Java Code Execution
   6   auxiliary/scanner/misc/java_jmx_server                2013-05-22       normal     No     Java JMX Server I
nsecure Endpoint Code Execution Scanner
   7   auxiliary/gather/java_rmi_registry                    .                normal     No     Java RMI Registry
 Interfaces Enumeration
   8   exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server I
nsecure Default Configuration Java Code Execution
   9     \_ target: Generic (Java Payload)                   .                .          .      .
   10    \_ target: Windows x86 (Native Payload)             .                .          .      .
   11    \_ target: Linux x86 (Native Payload)               .                .          .      .
   12    \_ target: Mac OS X PPC (Native Payload)            .                .          .      .
   13    \_ target: Mac OS X x86 (Native Payload)            .                .          .      .
   14  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server I
nsecure Endpoint Code Execution Scanner
   15  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectio
nImpl Deserialization Privilege Escalation
   16  exploit/multi/browser/java_signed_applet              1997-02-19       excellent  No     Java Signed Apple
t Social Engineering Code Execution
   17    \_ target: Generic (Java Payload)                   .                .          .      .
   18    \_ target: Windows x86 (Native Payload)             .                .          .      .
   19    \_ target: Linux x86 (Native Payload)               .                .          .      .
   20    \_ target: Mac OS X PPC (Native Payload)            .                .          .      .
   21    \_ target: Mac OS X x86 (Native Payload)            .                .          .      .
   22  exploit/multi/http/jenkins_metaprogramming            2019-01-08       excellent  Yes    Jenkins ACL Bypas
s and Metaprogramming RCE
   23    \_ target: Unix In-Memory                           .                .          .      .
   24    \_ target: Java Dropper                             .                .          .      .
   25  exploit/linux/misc/jenkins_java_deserialize           2015-11-18       excellent  Yes    Jenkins CLI RMI J
ava Deserialization Vulnerability
   26  exploit/linux/http/kibana_timelion_prototype_pollution_rce  2019-10-30       manual     Yes    Kibana Timelion P
```

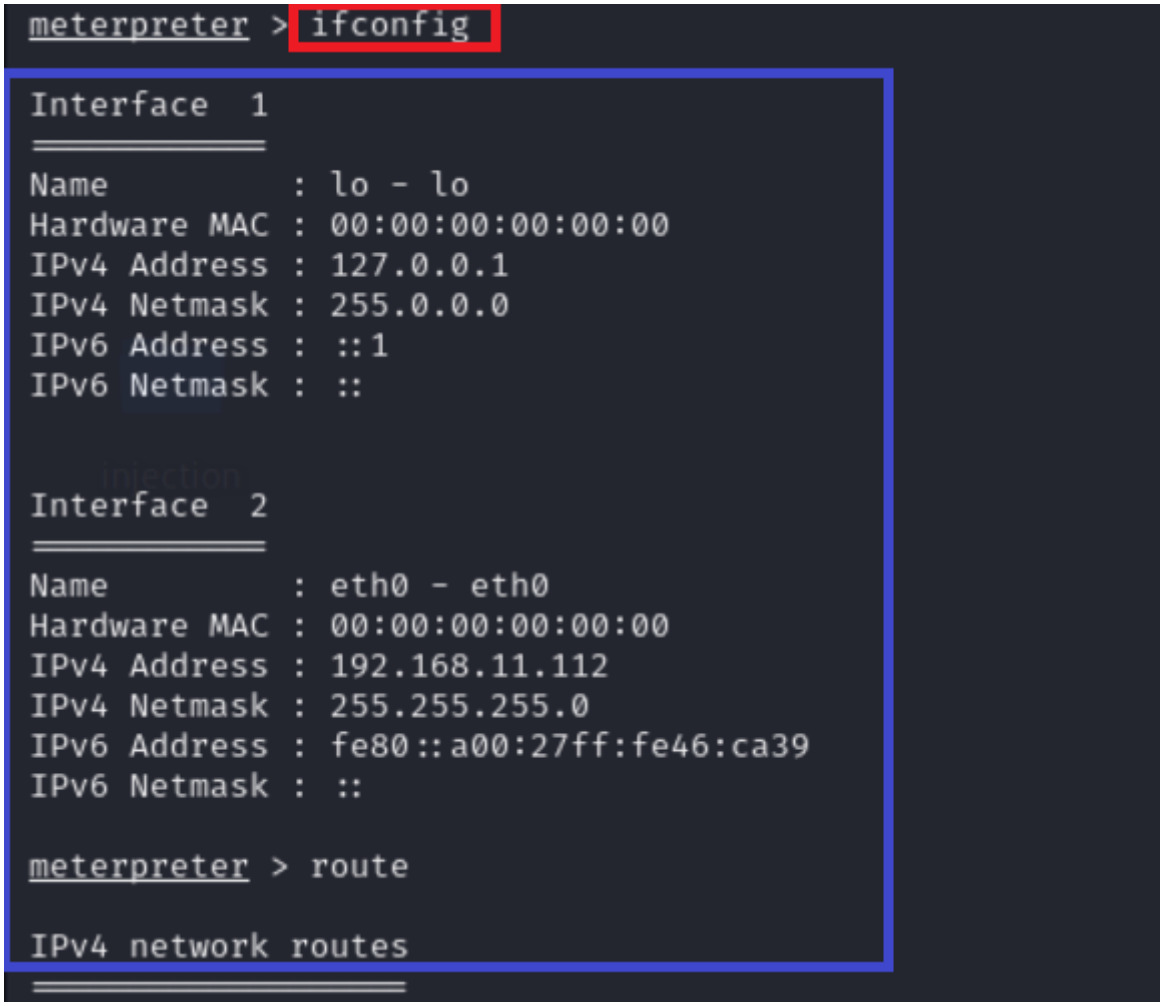
Procedura eseguita:

- **Sfruttamento della vulnerabilità**: Utilizzando **Metasploit**, è stato caricato il modulo per il servizio Java RMI sulla porta 1099. Successivamente, è stato configurato l'indirizzo IP della macchina attaccante (*192.168.11.111*) come **LHOST** e la macchina vittima (*192.168.11.112*) come **RHOST**. Dopo aver verificato i parametri, l'exploit è stato eseguito con successo, consentendo di ottenere una sessione **Meterpreter** sulla macchina Metasploitable.



- **HTTPDELAY**: Durante l'esecuzione dell'exploit, il valore di **HTTPDELAY** è stato configurato a **20**, per ritardare l'esecuzione di eventuali operazioni HTTP, garantendo una stabilità migliore della sessione Meterpreter.

- **Raccolta delle evidenze**: Una volta ottenuta la sessione *Meterpreter*, sono state eseguite le seguenti operazioni per raccogliere le evidenze richieste:



- **Configurazione di rete**: è stato eseguito il comando *ifconfig* per visualizzare i dettagli della configurazione di rete della macchina vittima, inclusi gli indirizzi IP, gateway, e subnet.
- **Tabella di routing**: il comando *route* ha permesso di ottenere le informazioni sulla tabella di routing della macchina, fornendo dettagli sui percorsi di rete attivi e le relative destinazioni.

Conclusioni:

L'attività è stata completata con successo, con lo sfruttamento della vulnerabilità del servizio *Java RMI* sulla *porta 1099* della macchina Metasploitable. È stata stabilita una connessione remota attraverso Meterpreter, permettendo di raccogliere le informazioni richieste, tra cui la configurazione di rete e la tabella di routing della macchina vittima.