PROGETTO S5L5

Exploit: l'exploit è una tecnica attraverso la quale usando un programma o un codice o comandi che sfruttano la vulnerabilita di un sistema ai fini di attaccare per reperire niformazioni, prendere il controllo o danneggiare una macchina.

Nel exploit di oggi attaccheremo la porta 1099 java rmi che fornisce accesso ai registri del dispositivo.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 08:21 EST
Nmap scan report for 192.168.11.112
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 14.31 seconds
```

Accediamo a msfconsole e accediamo per cercare exploit appropriato, configuriamo e attacchiamo. Avendo successo nel attacco osserviamo la configurazione di rete e la 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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fec0:6ac7
IPv6 Netmask : ::
```

```
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:fec0:6ac7 ::       ::
meterpreter >
```

Identificare la rete ci aiuta a conoscere in che dispositivo ci troviamo.

La tabella di routing contiene informazioni sulle reti disponibili e le interfacce di rete attraverso le quali i pacchetti devono essere inoltrati. Entrare a conoscenza della tabella ci permette identificare: la rete, ulteriori dispositivi collegati che possono essere attaccati, i percorsi di rete dove passano i dati , i percorsi poco sicuri, ulteriori ip, risorse accesibili direttamente e quali richiedono un percorso.
La tabella di routing può rivelare informazioni sensibili sulla rete.

Questo ci da a conoscere che la rete è esposta perche questo exploit da a conoscere tutte le informazioni di rete ed espone anche altri dispositivi, in questo caso mostra solo 1 dispositivo perche è una rete chiusa.