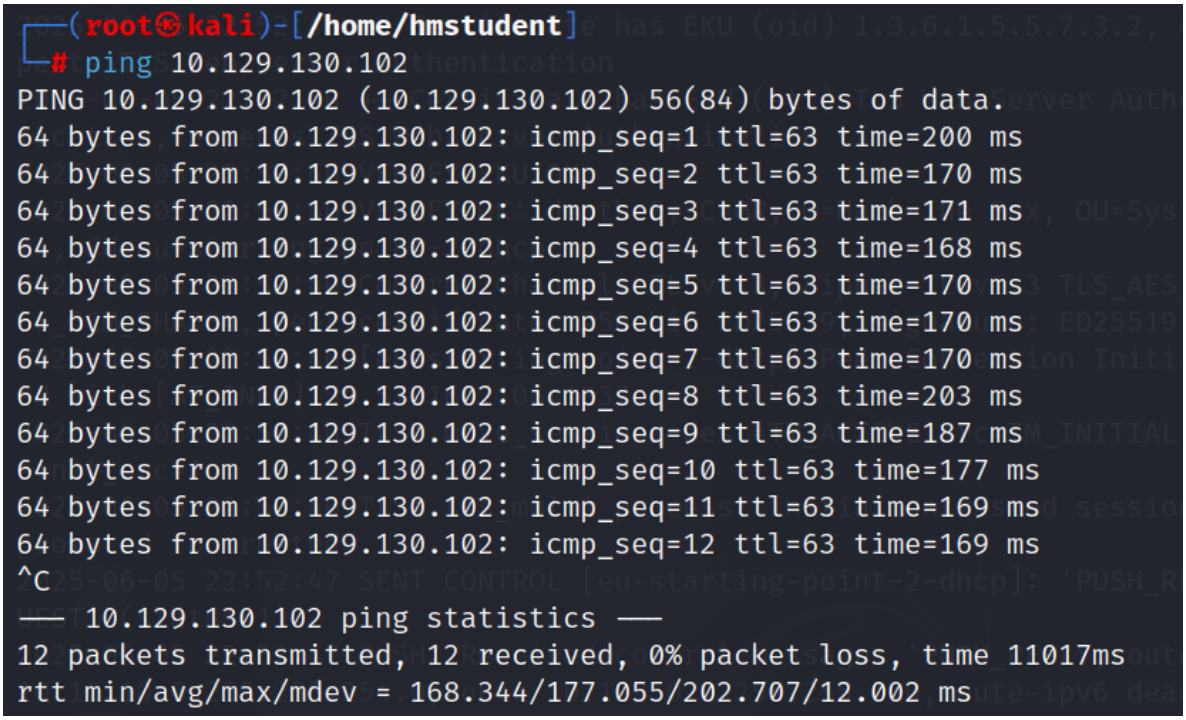
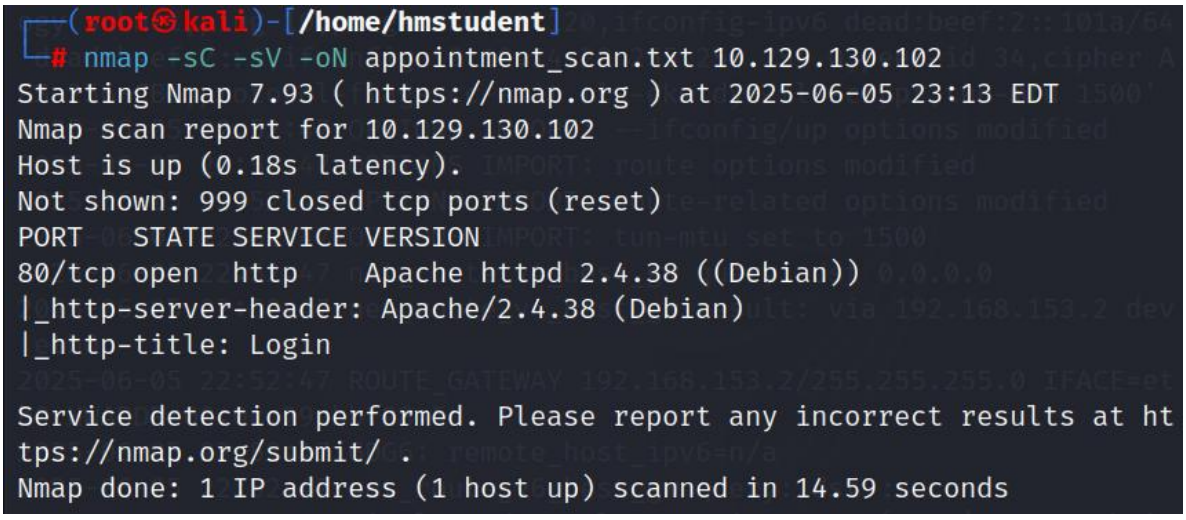
Write Up máquina Appointment HTB

Empezamos verificando si temenos acceso a la máquina, realizamos un ping:



Comprobamos que, si tenemos acceso, luego procedemos a realizar un escaneo con nmap para enumerar los puertos y servicios abiertos en la máquina



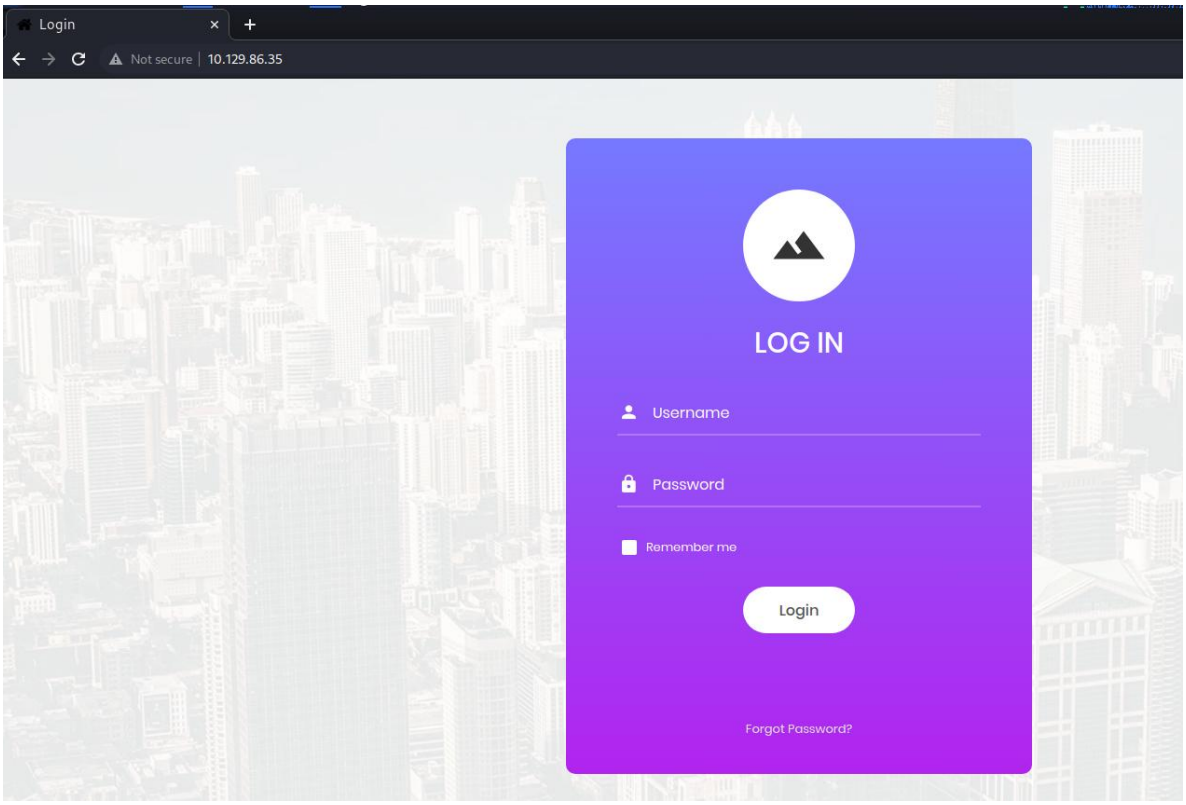
Logramos encontrar información valiosa, encontramos el puerto 80 abierto y que usa un servicio web con Apache httpd 2.4.38 Debian

Se realizo un escaneo más a profundidad

```
┌──(root㉿kali)-[/home/hmstudent]
└─# nmap -sC -sV -p80 10.129.86.35 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2025-09-11 00:13 EDT
Nmap scan report for 10.129.86.35
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.81 seconds
```

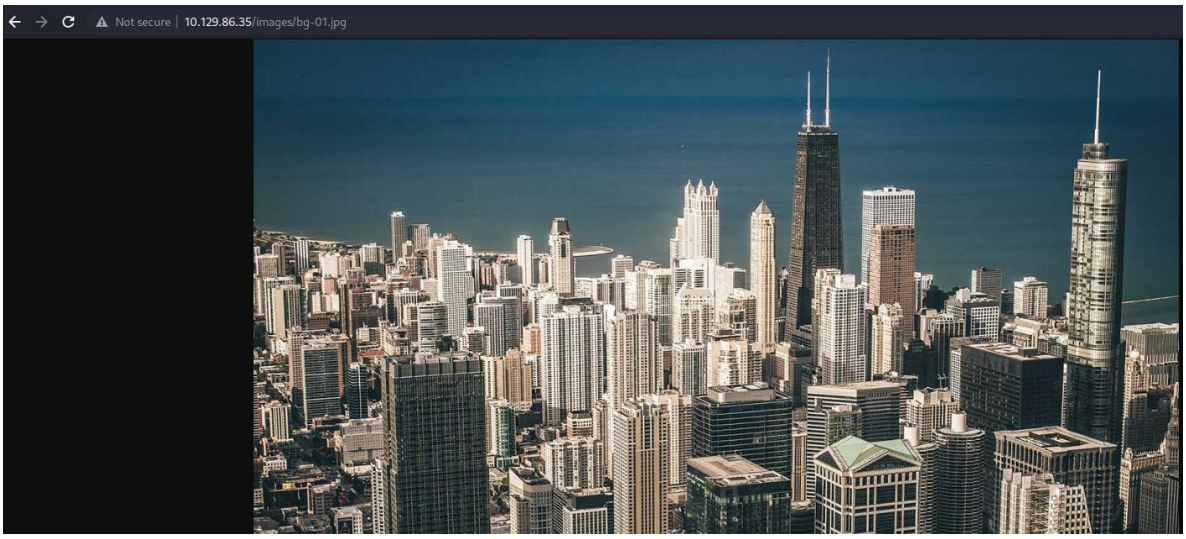
```
┌──(root㉿kali)-[/home/hmstudent]
└─# nmap -sC -sV -oN appointment_scan.txt 10.129.130.102
Starting Nmap 7.93 ( https://nmap.org ) at 2025-06-05 23:13 EDT
Nmap scan report for 10.129.130.102
Host is up (0.18s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login

Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
```

Entramos al navegador y nos encontramos con el login de una página web



Inspeccionamos el código de la pagina donde solo encontramos una url que nos lleva a una imagen publicada

```
<!--===============================================================================================-->
</head>
<body>


    <div class="limiter">
        <div class="container-login100" style="background-image: url('images/bg-01.jpg');">
            <div class="wrap-login100">
                <form class="login100-form validate-form" method="post">
                    <span class="login100-form-logo">
                        <i class="zmdi zmdi-landscape"></i>
                    </span>

                    <span class="login100-form-title p-b-34 p-t-27">
                        Log in
                    </span>

                    <div class="wrap-input100 validate-input" data-validate = "Enter username">
                        <input class="input100" type="text" name="username" placeholder="Username">
                        <span class="focus-input100" data-placeholder="&#xf207;"></span>
                    </div>

                    <div class="wrap-input100 validate-input" data-validate="Enter password">
                        <input class="input100" type="password" name="password" placeholder="Password">
                        <span class="focus-input100" data-placeholder="&#xf191;"></span>
                    </div>

                    <div class="contact100-form-checkbox">
                        <input class="input-checkbox100" id="ckb1" type="checkbox" name="remember-me">
                        <label class="label-checkbox100" for="ckb1">
                            Remember me
                        </label>
```



Probamos ingresar credenciales como admin – admin pero no funcionaron, luego probamos que la pagina sea vulnerable a sql injection ingresamos en el campo de username una inyección básica:

admin' OR '1'='1

donde obtuvimos acceso y encontramos la bandera:

e3d0796d002a446c0e622226f42e9672