

## Write Up máquina Crocodile HTB

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

```
(root@kali)-[/home/hmstudent]_set: mtu 1500 for tun0
# ping 10.129.1.15
PING 10.129.1.15 (10.129.1.15) 56(84) bytes of data:
64 bytes from 10.129.1.15: icmp_seq=1 ttl=63 time=146 ms
64 bytes from 10.129.1.15: icmp_seq=2 ttl=63 time=148 ms
64 bytes from 10.129.1.15: icmp_seq=3 ttl=63 time=147 ms
64 bytes from 10.129.1.15: icmp_seq=4 ttl=63 time=147 ms
64 bytes from 10.129.1.15: icmp_seq=5 ttl=63 time=154 ms
^C
— 10.129.1.15 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 145.508/148.319/154.319/3.087 ms
```

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

```
(root@kali)-[/home/hmstudent]_set: mtu 1500 for tun0
# sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.129.1.15 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2025-09-14 22:39 EDT
Initiating SYN Stealth Scan at 22:39
Scanning 10.129.1.15 [65535 ports]
Discovered open port 80/tcp on 10.129.1.15
Discovered open port 21/tcp on 10.129.1.15
Completed SYN Stealth Scan at 22:40, 14.45s elapsed (65535 total ports)
Nmap scan report for 10.129.1.15
Host is up, received user-set (0.15s latency).
Scanned at 2025-09-14 22:39:46 EDT for 14s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63
```

Logramos encontrar los puertos 21 ftp y 80 web

Se realizó un escaneo más a profundidad

```

(root@kali)-[/home/hmstudent]_set: mtu 1500 for tun0
# 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).
2025-09-14 22:35:27 net_addr_v6_addr: dead:beef:2::1029/64 dev tun0
PORT 21/tcp open  ftp      vsftpd 3.0.3
|ftp-syst:22:35:27 net_route_v4_addr: 10.129.0.0/16 via 10.10.14.43
|  STAT:
|FTP server status:add_route_ipv6(dead:beef::/64 → dead:beef:2::1029/64)
|025-09 Connected to ::ffff:10.10.14.43:21 dev tun0
|025-09 Logged in as ftp
|025-09 TYPE: ASCII
|025-09 Data Channel: cipher 'AES-256-CBC', auth 'SHA256', peer-id: 32, compression: none
|: '120 No session bandwidth limit
|025-09 Session timeout in seconds is 300
|025-09 Control connection is plain text
|n-tls Data connections will be plain text
|      At session startup, client count was 1

```

```

|vsFTPd 3.0.3 - secure, fast, stable up
|_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 cualquiera 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 22:35:27 ne (Status: 403) [Size: 276] for tun0
/.htaccess.txt 22:35:27 ne (Status: 403) [Size: 276]
/.htaccess.php 22:35:27 ne (Status: 403) [Size: 276] 2/23 dev tun0
/.htpasswd.php 22:35:27 ne (Status: 403) [Size: 276] for tun0
/.htpasswd 22:35:27 ne (Status: 403) [Size: 276]
/.htpasswd.html 22:35:27 ne (Status: 403) [Size: 276] 1029/64 dev tun0
/.htpasswd.txt 22:35:27 ne (Status: 403) [Size: 276] 0/23 via 10.10.14.1 dev [NULL] table 0
/assets 22:35:27 ne (Status: 301) [Size: 311] [→ http://10.129.1.15/assets/]
/config.php 22:35:27 ne (Status: 200) [Size: 0] 10/16 via 10.10.14.1 dev [NULL] table 0
/css 22:35:27 ne (Status: 301) [Size: 308] [→ http://10.129.1.15/css/]
/dashboard 22:35:27 ne (Status: 301) [Size: 314] [→ http://10.129.1.15/dashboard/]
/fonts 22:35:27 ne (Status: 301) [Size: 310] [→ http://10.129.1.15/fonts/]
/index.html 22:35:27 ne (Status: 200) [Size: 58565]
/index.html 22:35:27 ne (Status: 200) [Size: 58565] -CBC', auth 'SHA256', peer-id: 32,
/js 22:35:27 ne (Status: 301) [Size: 307] [→ http://10.129.1.15/js/]
/login.php 22:35:27 ne (Status: 200) [Size: 1577]
/logout.php 22:35:27 ne (Status: 302) [Size: 0] [→ login.php] protocol-flags ce-exit
/server-status 22:35:27 ne (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 Init ftp 33 Jun 08 2021 allowed.userlist
-rw-r--r-- 1 ftp Data ftp 62 Apr 20 2021 allowed.userlist.passwd
226 Directory send OK.

```

get allowed.userlist

get allowed.userlist.passwd

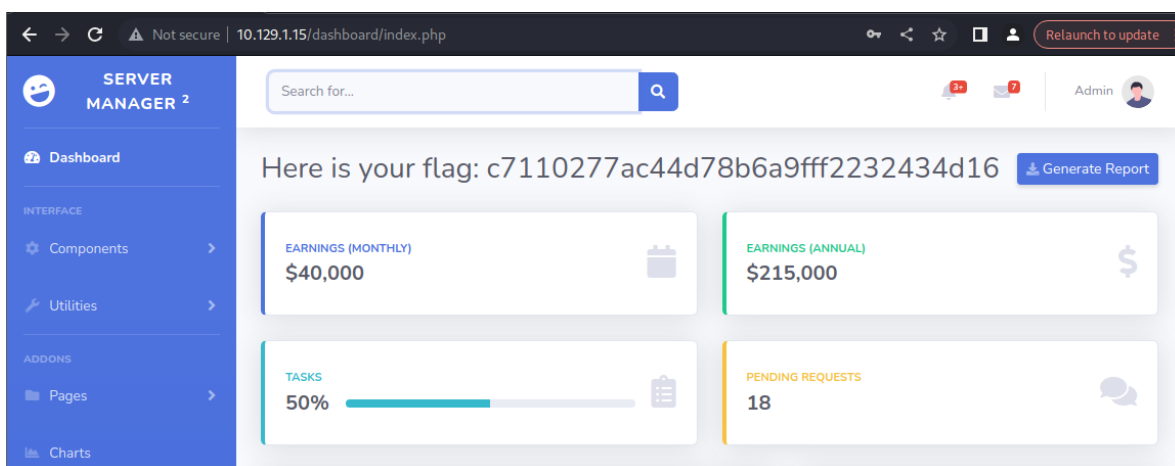
Salimos del servidor ftp y abrimos los archivos que descargamos

```
ftp> bye
221 Goodbye.

(root@kali)-[/home/hmstudent]
# cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

(root@kali)-[/home/hmstudent]
# cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd
```

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



donde obtuvimos acceso y encontramos la bandera:

c7110277ac44d78b6a9fff2232434d16

