

Crocodile

Enumeration

After connecting to the provided vpn and having the target ip I ran an nmap scan by following command

```
(kali@kali)-[~/Downloads]
$ sudo nmap -sV -sC 10.129.143.70
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 17:40 PKT
Nmap scan report for 10.129.143.70
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| 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
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.10.15.30
|   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 3
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Smash - Bootstrap Business Template
|_http-headers: Server: Apache/2.4.41 (Ubuntu)
|_http-headers: Server: Apache/2.4.41 (Ubuntu)
```

This scan some very useful information as

This ip is running some ftp services and most importantly this ftp server **allows anonymous login**.

- There are also some **http services** running on this ip.
- On connecting to the ftp server I was logged into the server by adding username as anonymous

```
(kali@kali)-[~/Downloads]
$ ftp 10.129.143.70
Connected to 10.129.143.70.
220 (vsFTPD 3.0.3)
Name (10.129.143.70:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

After that I listed the files available on this server

```
ftp> help
Commands may be abbreviated.  Commands are:

!          case  [+]  
$          cd    [+]  
account   cdup  [+]  
append    chmod [+]  
ascii     close [+]  
bell      cr    [+]  
binary    debug [+]  
bye        delete  
ftp> ls
229 Entering Extended Passive Mode (|||49537|)
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>
```

This listed two files that seemed very confidential “**allowed.userlist**” and “**allowed.userlist.passwd**”

so I downloaded both these files on my machine and viewed the contents in these files

```
(kali@kali)-[~/Downloads]
$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

(kali@kali)-[~/Downloads]
$ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd
```

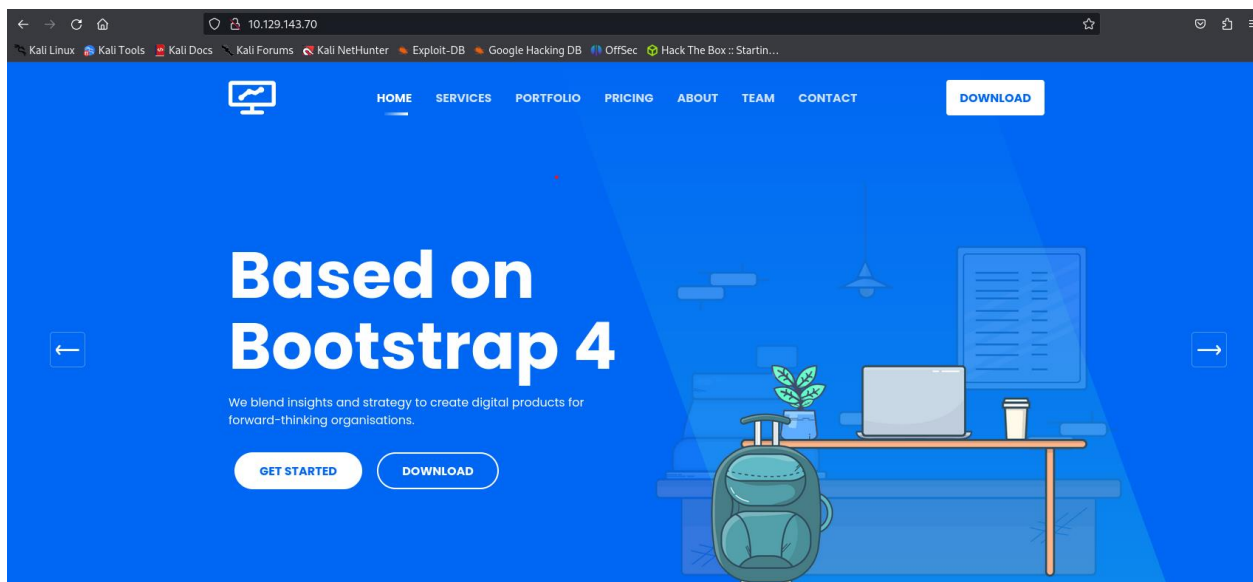
this gave me the list of allowed users and there respective passwords by which I can access this server

so then I tried connecting to the server using the allowed username I got from this list

```
(kali@kali)-[~/Downloads]
$ ftp 10.129.143.70
Connected to 10.129.143.70.
220 (vsFTPD 3.0.3)
Name (10.129.143.70:kali): aron
530 This FTP server is anonymous only.
ftp: Login failed
ftp>
```

As I tried to log in with name “aron” it displayed that this is an **anonymous only server** so which means that I cannot access this server even after having the right credentials.

Nmap scan also exposed some http services



This was the page I was welcomed with the provided ip

I scrolled through all the pages but all these pages seemed static so I decided to brute force directories so that I may some extra pages

I used gobuster to brute force directories and after the scan I had some valuable pages

```
(kali@kali)-[~]
└─$ gobuster dir --url http://10.129.143.70/ -x .php,.html --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

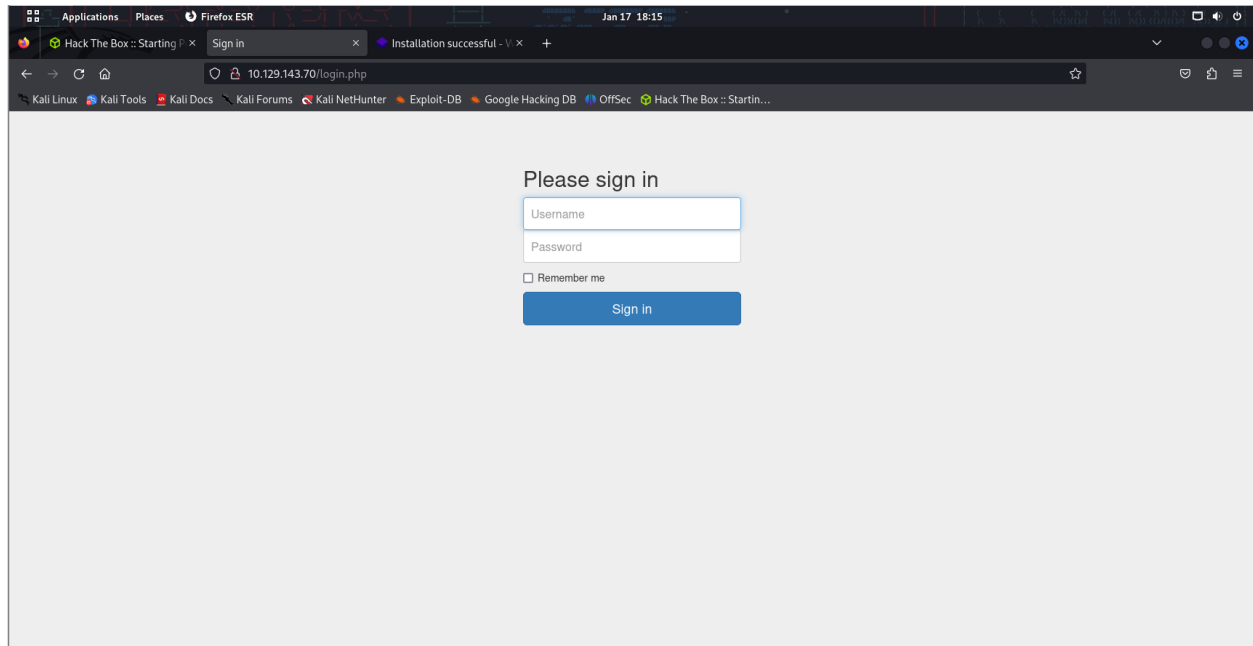
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.129.143.70/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./php (Status: 403) [Size: 278]
/index.html (Status: 200) [Size: 58565]
./html (Status: 403) [Size: 278]
/login.php (Status: 200) [Size: 1577]
Progress: 219 / 262995 (0.08%) [ERROR] Get "http://10.129.143.70/en.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.129.143.70/en.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 221 / 262995 (0.08%) [ERROR] Get "http://10.129.143.70/forum.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 230 / 262995 (0.09%) [ERROR] Get "http://10.129.143.70/security": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 231 / 262995 (0.09%) [ERROR] Get "http://10.129.143.70/security.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

- Php
- Index.html
- .html
- Login.php

Gobuster exposed these four pages so I visited them one by one

- Index.html directed me to the same home page with different url
- .html and .php were not found

But as I tried to connect to the login.php page I was directed to another page



So here I was demanded username and password, so I put the username and password I extracted from ftp server and I was handed over with the flag

