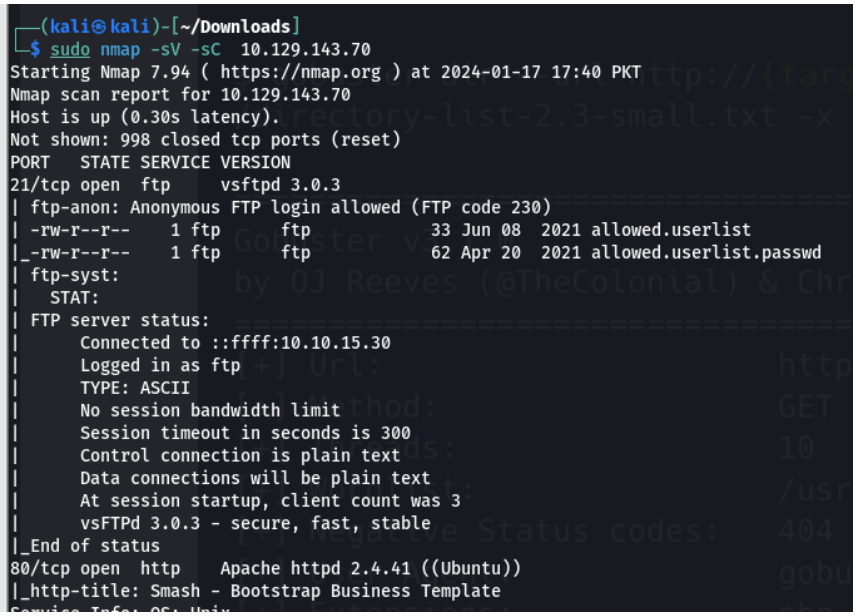
Crocodile

Enumeration

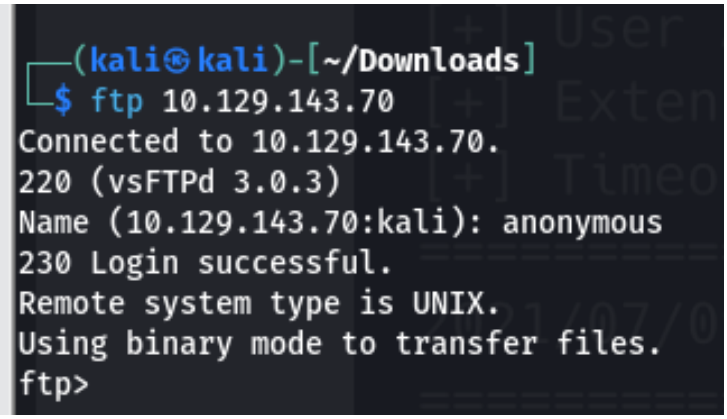
After connecting to the provided vpn and having the target ip I ran an nmap scan by following command



This scan some very useful information as

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

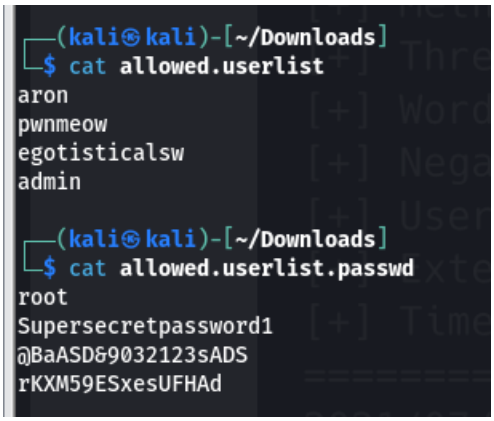
- There are also some **http services** running on this ip.
- On connecting to the ftp server I was logged into the server by adding username as anonymous



After that I listed the files available on this server

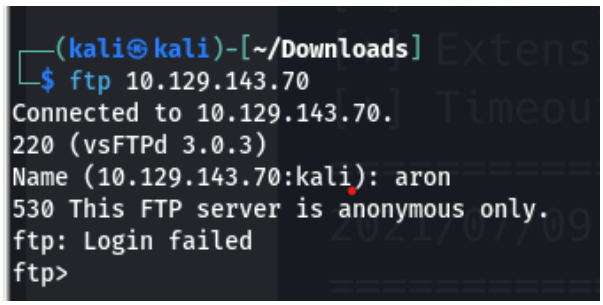
This listed two files that seemed very confidential **“allowed.userlist”** and **“allowed.userlist.passwd”**

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



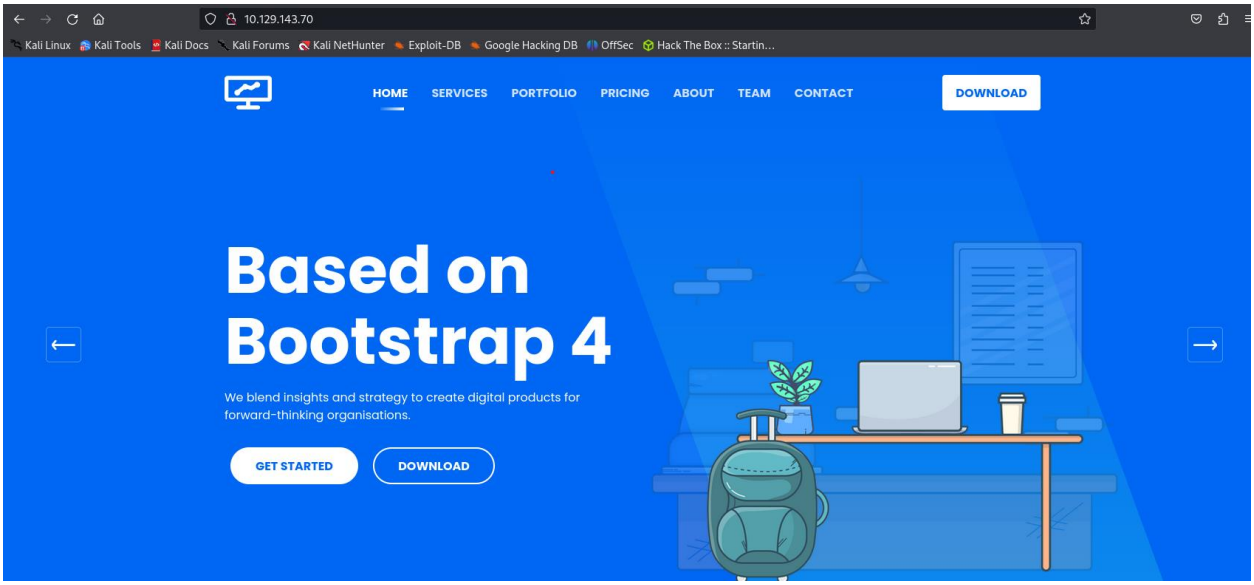
this gave me the list of allowed users and there respective passwords by which I can access this server

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



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

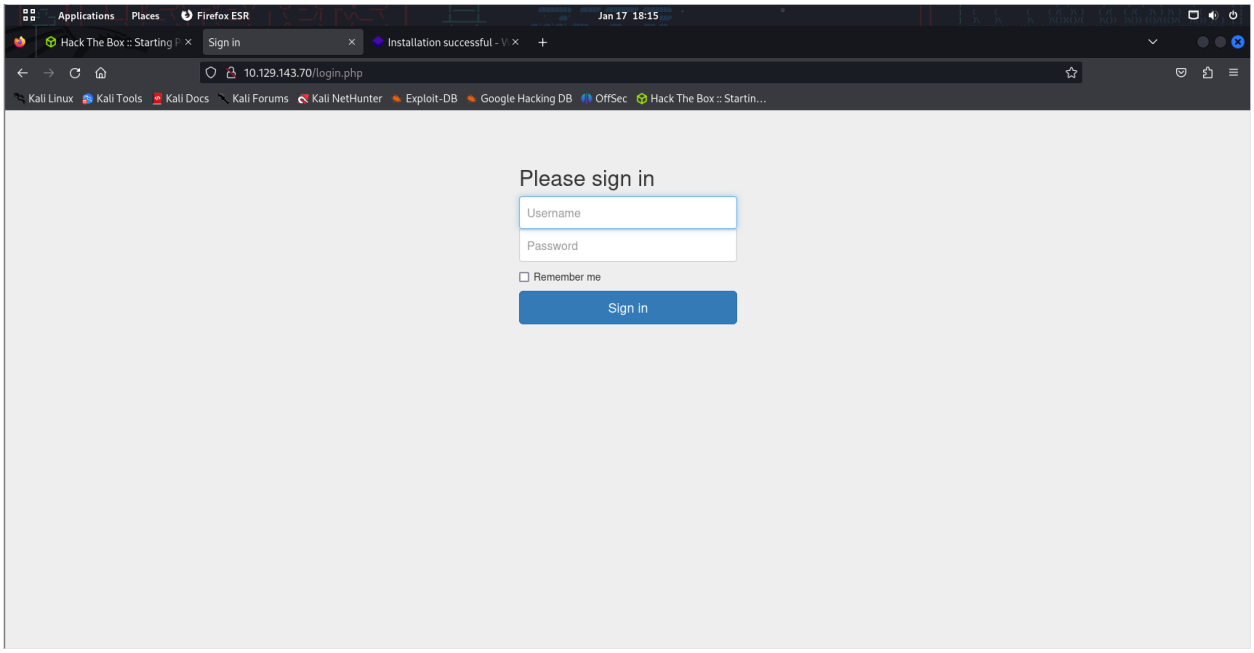
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir --url http://10.129.143.70/ -x .php,.html  --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

===============================================================
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