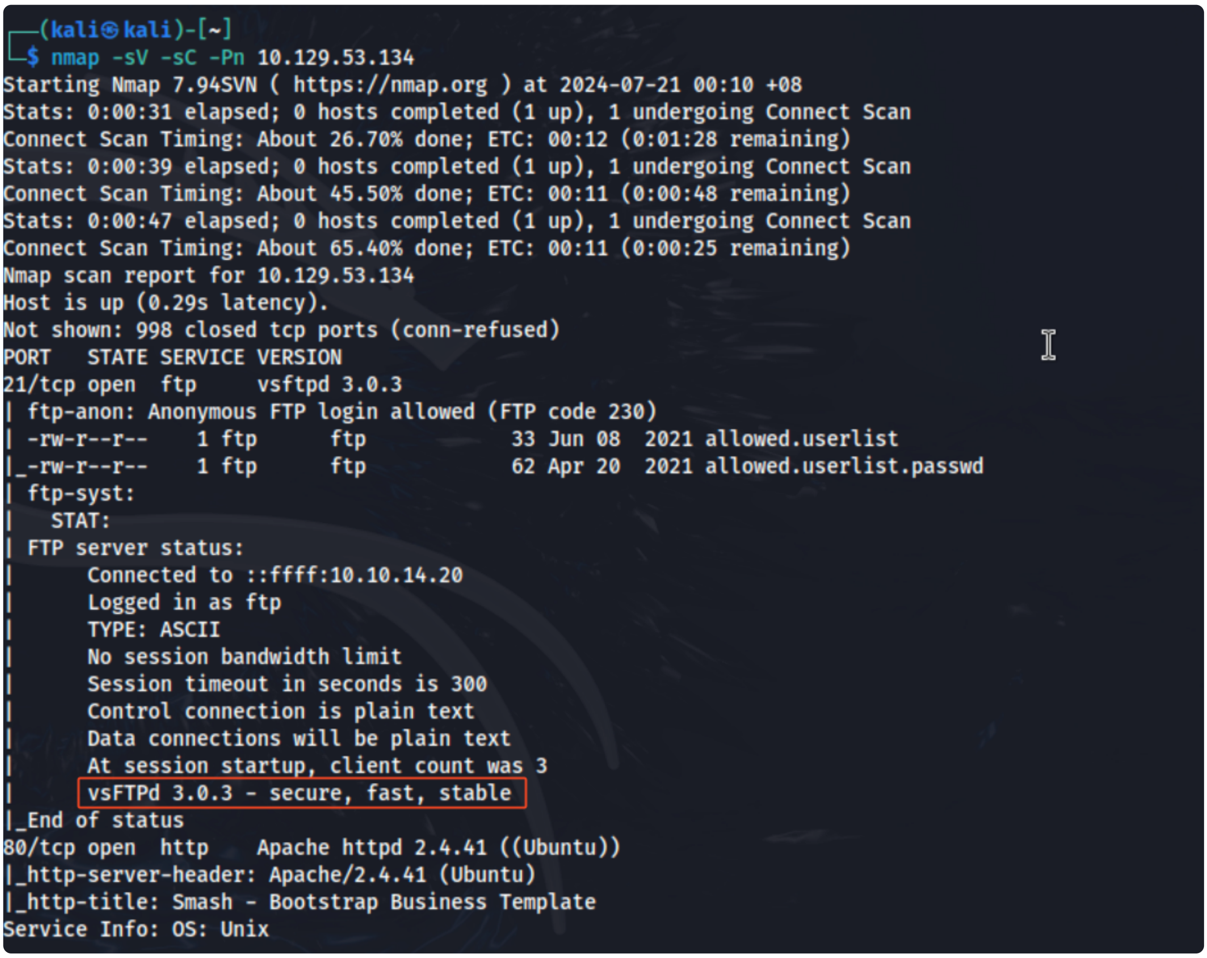
Crocodile

Task 1

- What Nmap scanning switch employs the use of default scripts during a scan?
  - `-sC`

Task 2

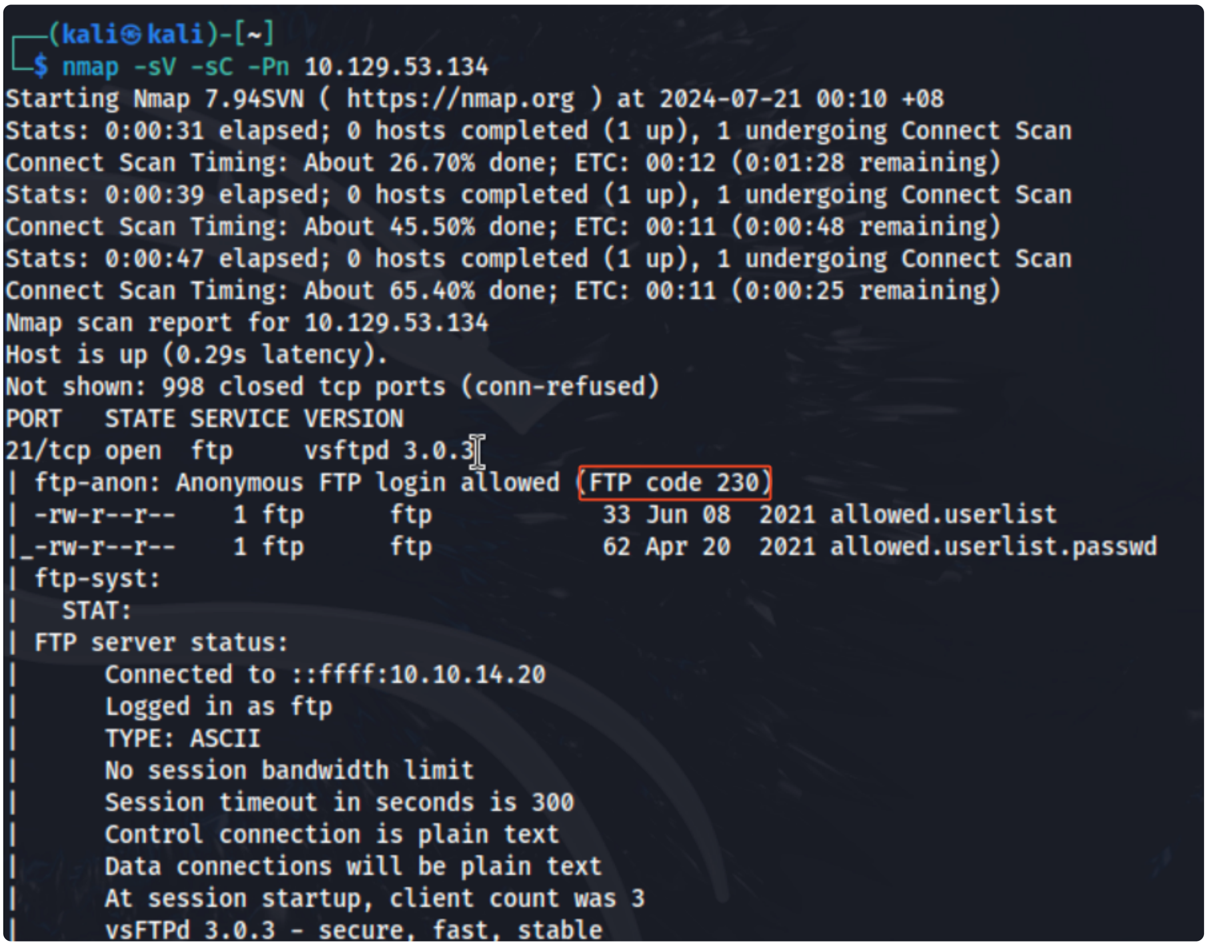
- What service version is found to be running on port 21?
  - The -Pn option in nmap is used to disable host discovery. When you use -Pn, nmap assumes that the specified hosts are up (online) without performing a preliminary ping sweep to check their status. This is useful in scenarios where you know the host is up, but it might be blocking ICMP (ping) requests or other types of probes that nmap uses for host discovery.
  - `nmap -sV -sC -Pn 10.129.53.134
  - vsFTPD 3.0.3



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -Pn 10.129.53.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-21 00:10 +08
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.70% done; ETC: 00:12 (0:01:28 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 45.50% done; ETC: 00:11 (0:00:48 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.40% done; ETC: 00:11 (0:00:25 remaining)
Nmap scan report for 10.129.53.134
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (conn-refused)
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:10.10.14.20
|      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-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Smash - Bootstrap Business Template
Service Info: OS: Unix
```

Task 3

- What FTP code is returned to us for the "Anonymous FTP login allowed" message?
  - 230



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -Pn 10.129.53.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-21 00:10 +08
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.70% done; ETC: 00:12 (0:01:28 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 45.50% done; ETC: 00:11 (0:00:48 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.40% done; ETC: 00:11 (0:00:25 remaining)
Nmap scan report for 10.129.53.134
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (conn-refused)
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:10.10.14.20
|      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
```

Task 4

- After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?
  - `anonymous`

Task 5

- After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server?
  - `get`

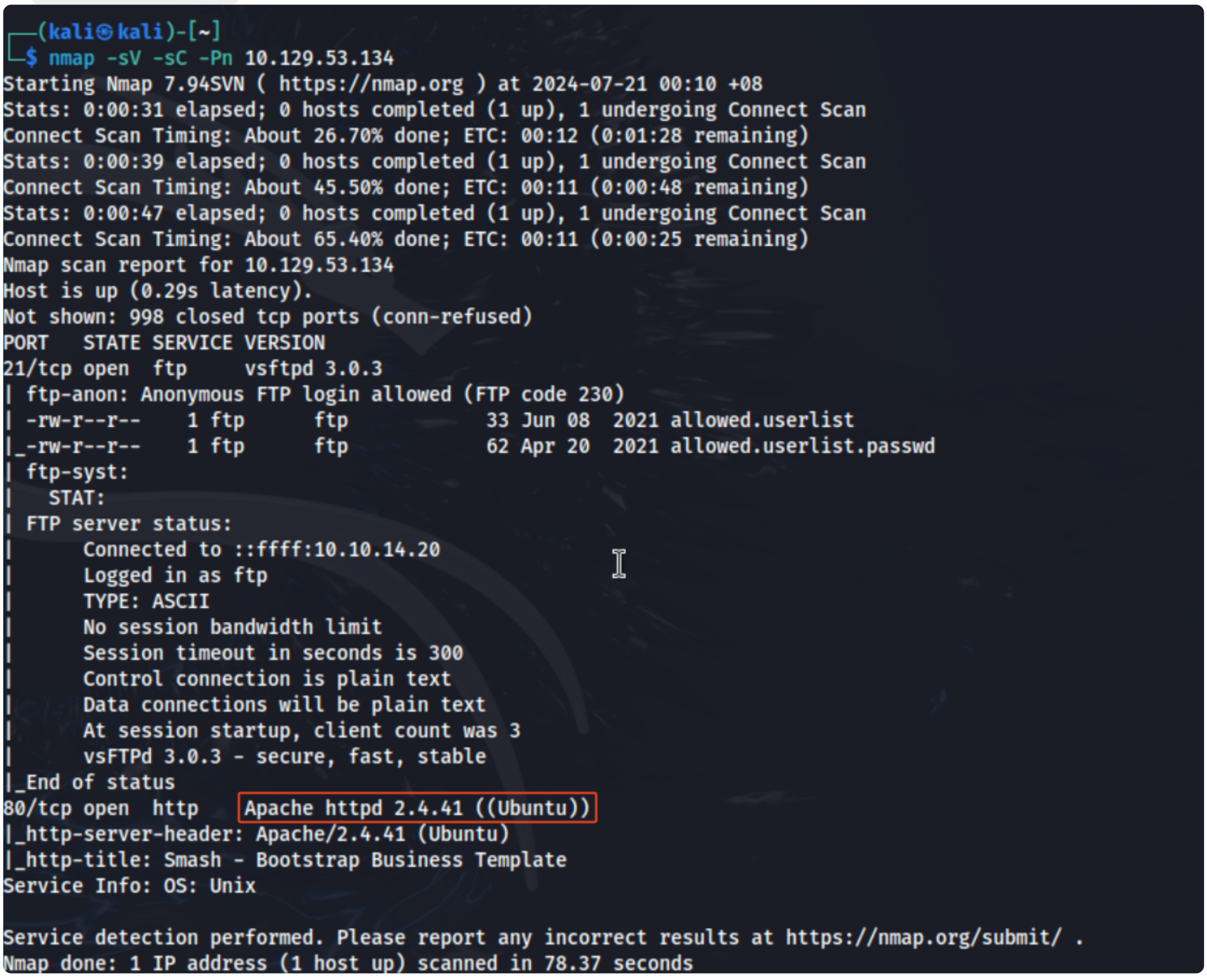
Task 6

- What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?
  - `admin`

Task 7

- What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?

- Apache httpd 2.4.41



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -Pn 10.129.53.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-21 00:10 +08
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.70% done; ETC: 00:12 (0:01:28 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 45.50% done; ETC: 00:11 (0:00:48 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 65.40% done; ETC: 00:11 (0:00:25 remaining)
Nmap scan report for 10.129.53.134
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (conn-refused)
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:10.10.14.20
|      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-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 78.37 seconds
```

Task 8

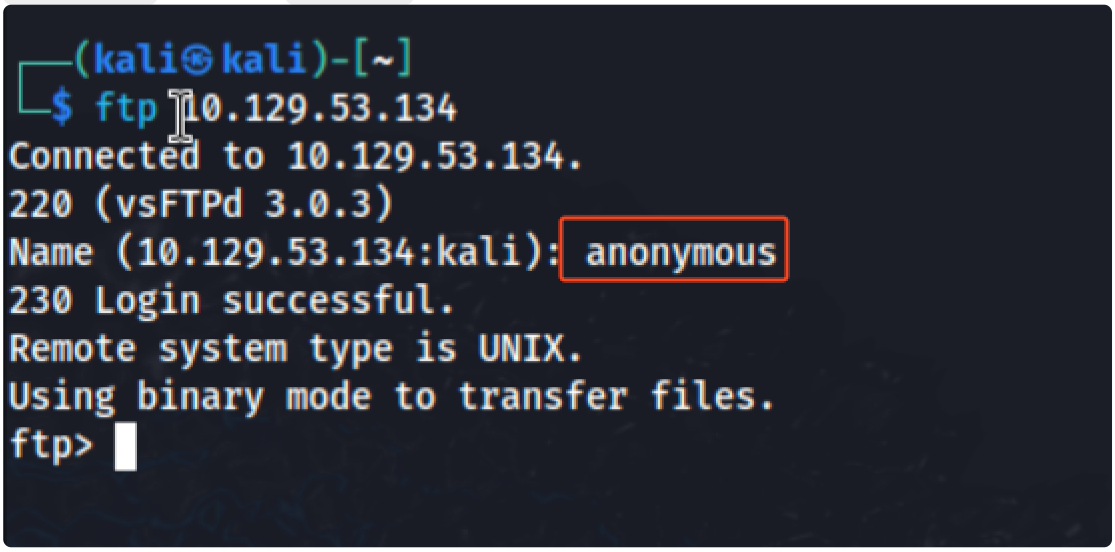
- What switch can we use with Gobuster to specify we are looking for specific filetypes?
  - -x

Task 9

- Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?
  - login.php

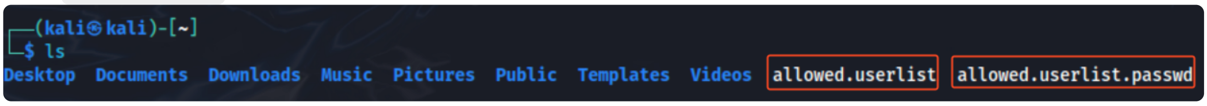
Task 10

1. `ftp {IP_Target}` | Name: `anonymous`



```
┌──(kali㉿kali)-[~]
└─$ ftp 10.129.53.134
Connected to 10.129.53.134.
220 (vsFTPd 3.0.3)
Name (10.129.53.134:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

2. get `allowed.userlist` & `allowed.userlist.-passwd

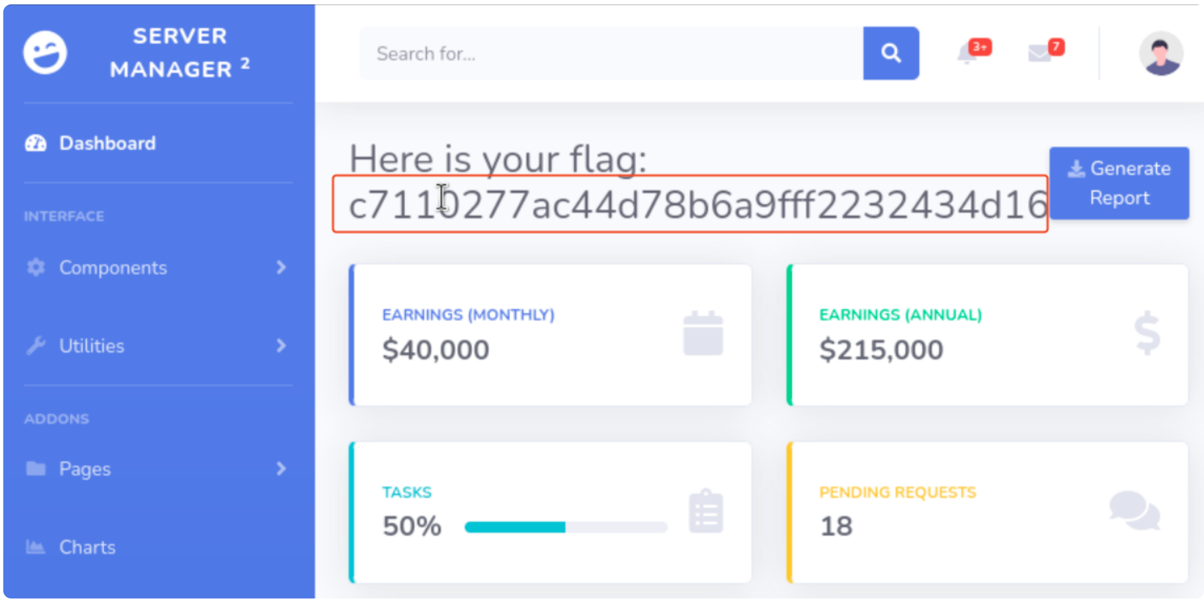


```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  allowed.userlist  allowed.userlist.passwd
```

3. Now we use gobuster to search for directories (Can just guess the directory "idk")

```
# gobluster
sudo gobuster dir -u http://10.129.53.134/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,html
```

4. cat the file that you download and login as admin



Here is your flag:
c7110277ac44d78b6a9fff2232434d16