Crocodile ACTIVE

VERY EASY

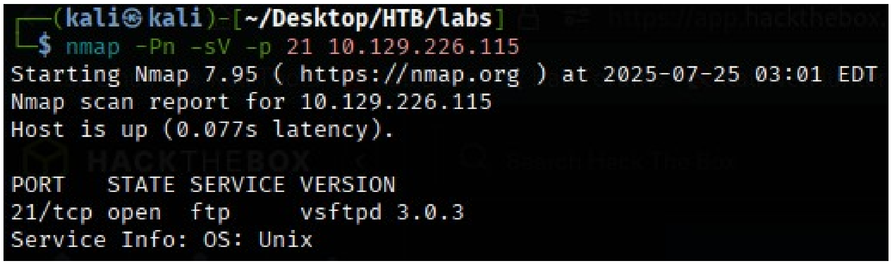
TARGET MACHINE IP ADDRESS

10.129.226.115

1. What Nmap scanning switch employs the use of default scripts during a scan?

   Answer: -sC

2. What service version is found to be running on port 21?

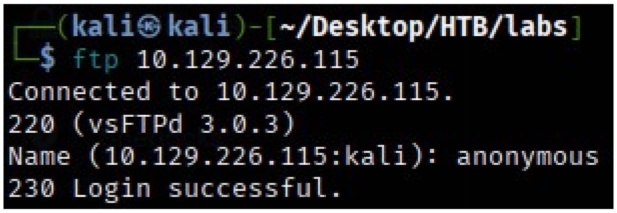


```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV -p 21 10.129.226.115
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 03:01 EDT
Nmap scan report for 10.129.226.115
Host is up (0.077s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix
```

   Answer: vsftpd 3.0.3

3. What FTP code is returned to us for the "Anonymous FTP login allowed" message?



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ ftp 10.129.226.115
Connected to 10.129.226.115.
220 (vsFTPd 3.0.3)
Name (10.129.226.115:kali): anonymous
230 Login successful.
```

   Answer: 230

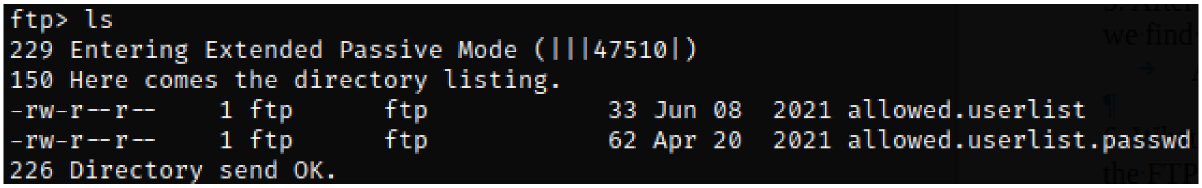
4. After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?

   Answer: anonymous

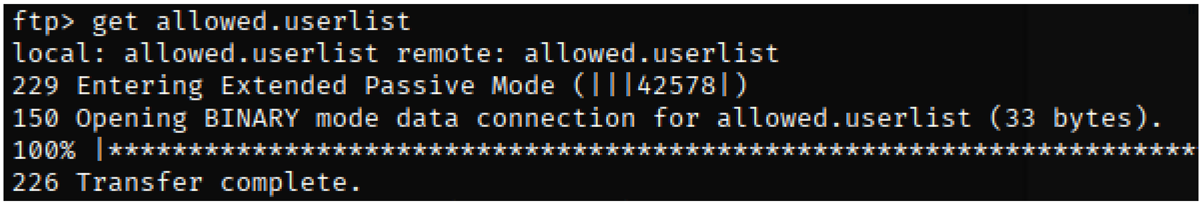
5. After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server?

   Answer: get

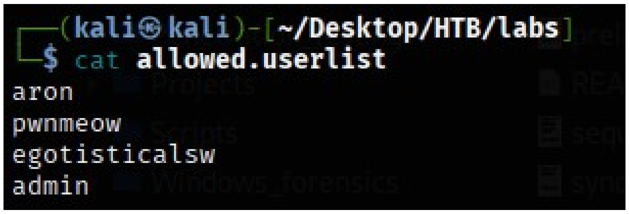
6. What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?



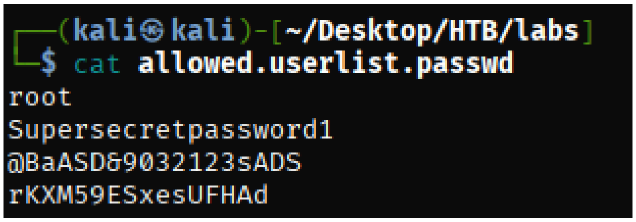
```
ftp> ls
229 Entering Extended Passive Mode (|||47510|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.
```



```
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||42578|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% |*********************************************************************
226 Transfer complete.
```



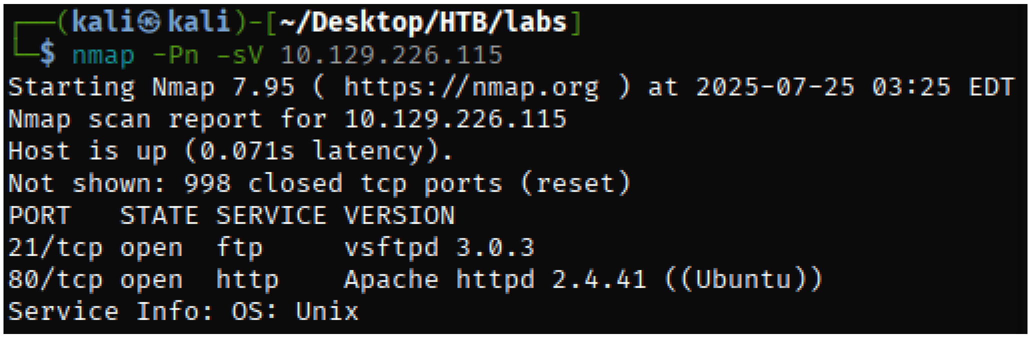
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd
```

Answer: admin

7. What version of Apache HTTP Server is running on the target host?



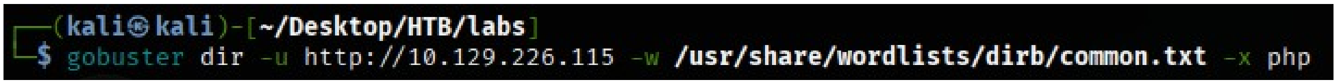
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn -sV 10.129.226.115
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 03:25 EDT
Nmap scan report for 10.129.226.115
Host is up (0.071s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Unix
```

Answer: Apache httpd 2.4.41

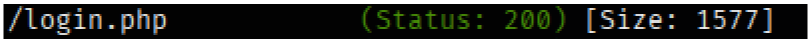
8. What switch can we use with Gobuster to specify we are looking for specific filetypes?

Answer: -x

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



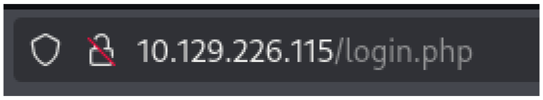
```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ gobuster dir -u http://10.129.226.115 -w /usr/share/wordlists/dirb/common.txt -x php
```



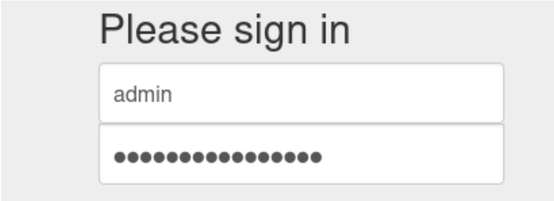
```
/login.php            (Status: 200) [Size: 1577]
```

Answer : login.php

10. Submit root flag



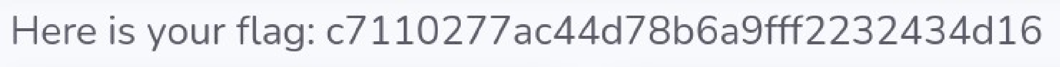
10.129.226.115/login.php



Please sign in

admin

●●●●●●●●●●●●●●●●



Here is your flag: c7110277ac44d78b6a9fff2232434d16

Answer: c7110277ac44d78b6a9fff2232434d16