Magic

nmap

```
└─$ nmap -sC -sV -oN nmap/init.nmap 10.10.10.185
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 18:20 EDT
Nmap scan report for 10.10.10.185
Host is up (0.086s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
|   256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
|_  256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Magic Portfolio
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

Looks like a simple web challenge

foothold

Starting at the website, there is a login page which requires authentication to perform file uploads

We can bypass this login page using a simple sql injection payload:

username: admin

passowrd: ' OR 1=1-- -

Note: had to intercept the request and edit it in order to add spaces. probably some sort of javascript preventing spaces

Now we are at a file upload

using gobuster, we find a directory called /images, which is probably where uploaded images are stored. doing another gobuster on /images, we find a /images/uploads directory

We want to upload an “image” which actually contains php code. We can do this by starting a file with the magic bytes of an image, and then writing the php code after

lateral movement

from www-data, we need to find a way to become a user with more privileges

There is a file /var/www/Magic/db.php5 which contains code to connect to a database. This file includes plaintext credentials for the db login as well as the db name “Magic”

theseus:iamkingtheseus

mysql client is not installed on the box, but mysqldump is.
using
```
mysqldump Magic -u theseus -p
```
we get a dump of the database, which reveals more creds:

admin:Th3s3usW4sK1ng

The password is reused for theseus on the box, so we get can su to become theseus

priv esc

now that we are logged into the box as theseus, time to find a way to priv esc

for a better shell, we can generate an ssh key pair and ssh in.

there is an SUID binary /bin/sysinfo which uses `cat` without the full path

writing a reverse shell to /tmp/cat and export PATH=/tmp:$PATH, then executing /bin/sysinfo gets us a root shell