Nocturnal

- nmap shows two open ports 22 80
- port 80 redirects to nocturnal.htb so added to `/etc/hosts`
- fuzzing shows `backup` directory and `admin.php`
- **A FAIRY TOLD US ABOUT LOGIN DETAILS OF AMANDA**
- login as `amanda`
- download backup
- unzip the backup
- Now we can read the `nocturnal_database.db`

```
cat nocturnal_database.db
```

- shows a username and password hash

```
{"username": "tobias", "password_hash": "55c82b1ccd55ab219b3b109b07d5061d"}
```

- 55c82b1ccd55ab219b3b109b07d5061d md5 decoded with https://crackstation.net/
- decoded password is `slowmotionapocalypse`
- ssh with the password

```
ssh tobias@10.10.11.64
slowmotionapocalypse
```

- user flag `cat user.txt`
- **MATRIX TOLD THAT IT IS VULNERABLE TO CVE-2023-46818**
- Vulnerable to CVE 2023 46818, got a available exploit https://github.com/bipbopbup/CVE-2023-46818-python-exploit
- save exploit as `exploit.py` https://raw.githubusercontent.com/bipbopbup/CVE-2023-46818-python-exploit/refs/heads/main/exploit.py with nano in tobius shell
- Run the exploit `python3 exploit.py http://127.0.0.1:8080 admin slowmotionapocalypse` in tobius ssh shell
- root flag `cat /root/root.txt`