

# SawCTF Write-up: Clara

## Sinopse

CTF inspirado em Jogos Mortais, criado pelo OFFSEC para a SATECH/UFSC. Dentro deste CTF, está rodando uma máquina com os serviços HTTP e ssh rodando com vulnerabilidades, utilizou-se, principalmente, a análise dos códigos fontes e quebra de hashes para obter um usuário e senha.

## 1 Enumeração

O reconhecimento inicial foi feito com um scan Nmap para identificar portas e serviços abertos na máquina.

```
> nmap -sV -sC -v <IP_MAQUINA>
```

```
Nmap scan report for 10.10.1.134
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey:
|   256 37:d1:6f:b5:a4:96:e8:78;18:c7:77:d0:3e:20:4e:55 (ECDSA)
|   256 cf:5d:90:f3:37:3f:a4:e2:ba:d5:d7:25:c6:4a:a0:61 (ED25519)
80/tcp    open  http     Apache httpd 2.4.57 ((Debian))
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: SawCTF
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning a ilusão
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.13 seconds
Raw packets sent: 1022 (44.944KB) | Rcvd: 1019 (40.768KB)

(kali㉿kali)-[~/Downloads]
```

Figure 1: Resultado do scan Nmap.

A varredura mostrou as portas 22 (SSH) e 80 (HTTP) abertas.

Acessando a porta 80, encontramos a página principal http e uma analise no código fonte revelou um diretório em /trap.

```

38     <div class="text-box top-box">
39     <!-- O criador das provas não fala, apenas observa, mas deixa uma mensagem clara: todos são convidados. web_flag: 4c657454686547616d65734265676960 -->
40     Que os jogos começem! Você deve passar pela armadilha para encontrar a chave. Faça a sua escolha.
41   </div>
42   <div class="text-box bottom-box">
43     <!-- GO /trap -->
44   </div>

```

Figure 2: Analise do código fonte.

Ao acessar um diretório oculto, encontramos uma página de login. A análise do seu código fonte revelou outro diretório: /trap/jigsaw

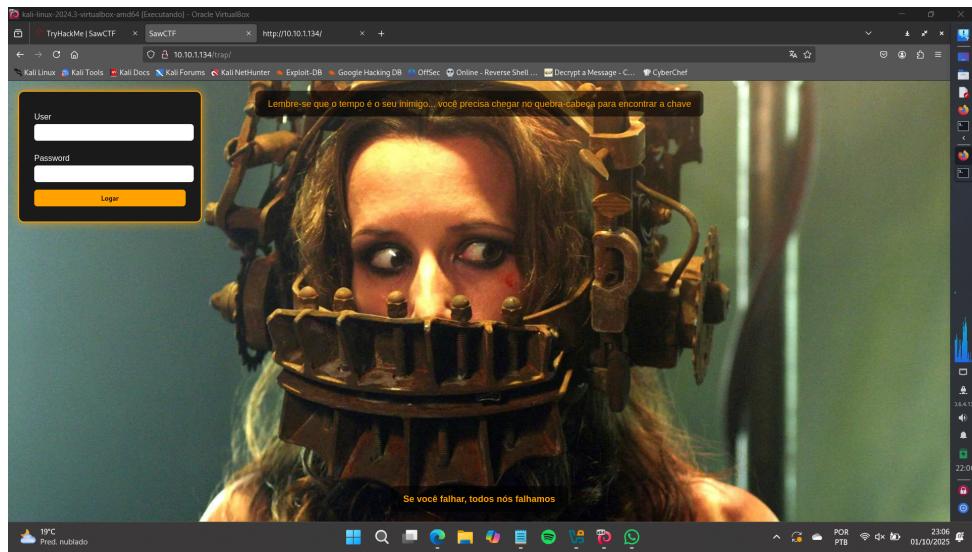


Figure 3: Página de login.

Nesse novo diretório achamos uma senha em Hexadecimal e um código morse, os quais revelam um usuário e uma senha. Com a senha e o usuário podemos fazer login no sistema por meio do ssh.

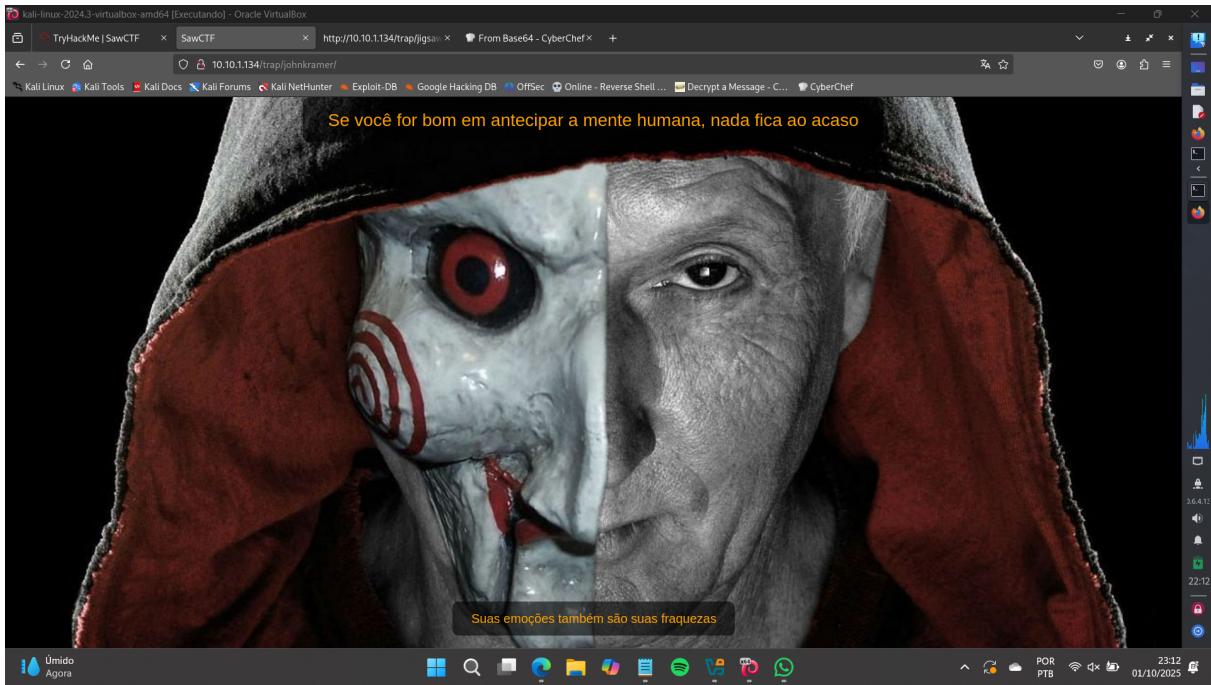


Figure 4: Site encontrado após fazer login.

## 2 Acesso Inicial

### 2.1 Acesso Inicial e Primeira Flag

Nosso ponto de partida foi o acesso com a usuária amanda. Uma rápida varredura em seu diretório pessoal nos recompensou com a primeira flag, localizada em user.txt. O próximo passo era escalar nossos privilégios.

```
(kali㉿kali)-[~/Downloads]
$ ssh amanda@10.10.1.134
The authenticity of host '10.10.1.134 (10.10.1.134)' can't be established.
ED25519 key fingerprint is SHA256:LwWOf4O2aDb/w6V7Z5VEAcjNfkxMmP0zyEIC7HMr91o.
This host key is known by the following other names/addresses:
  -/.ssh/known_hosts:23: [hashed name]
  -/.ssh/known_hosts:26: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.1.134' (ED25519) to the list of known hosts.
amanda@10.10.1.134's password:
Linux sawctf 6.1.0-11-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-4 (2023-08-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
Task 1 0 Início do Jogo
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
amanda@sawctf:~$
```

Figure 5: Acesso com ssh.

### 2.2 Descoberta e Análise do Usuário John

Sabíamos da existência de outro usuário, john, mas sua senha era um mistério. A chave para o avanço estava escondida no servidor web. Acessando a URL [http://\[IPMAQUINA\]/trap](http://[IPMAQUINA]/trap) como amanda, mergulhamos no código-fonte da página e, lá, a senha de john foi revelada.

### 3 Escalação de Privilégios para Root

Armados com o novo par de credenciais (john e sua senha), conseguimos nos conectar via SSH. A partir desse ponto, exploramos as vulnerabilidades do sistema para escalar nossos privilégios, o que nos garantiu acesso à senha de root.

O login final como root nos deu acesso total à máquina. Com isso, não apenas capturamos a flag final, como também encontramos o link que nos levaria ao próximo desafio.

```
root@sawctf:~# cat next_game.txt
FROM_Hex( N
)
From_Base85
Next game in: https://tryhackme.com/jr/pr0m3th3us
Make Your Choice!
root@sawctf:~#
```

Figure 6: URL próximo desafio.

E assim termina o CTF Saw do CTF da satech 2025.