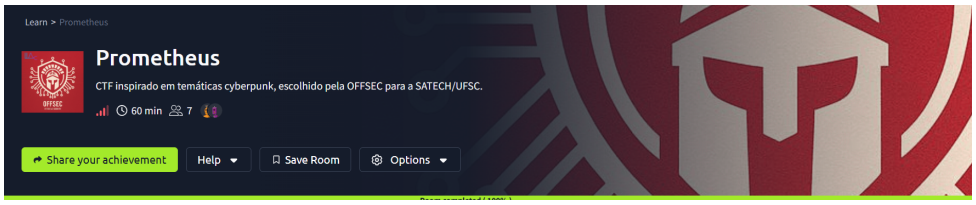

Prometheus CTF Write-up

Sinopse

CTF inspirado em temáticas cyberpunk, escolhido pela OFFSEC para a SATECH/UFSC 2025. Dentro deste CTF, está rodando uma máquina vulnerável à SQL Injection, permitindo obter um usuário e uma senha por meio do banco de dados, podendo se conectar a shell e escalar privilégios a partir de uma má configuração das permissões sudo.

1 Enumeração

O reconhecimento inicial foi feito com um scan Nmap para identificar portas e serviços abertos na máquina `10.10.144.113`.

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

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
|   256 48:42:7a:cf:38:19:20:86:ea:fd:50:88:b8:64:36:46 (ECDSA)
|_  256 9d:3d:85:29:8d:b0:77:d8:52:c2:81:bb:e9:54:d4:21 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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. Uma segunda página, index2.php, foi encontrada, por meio do comando:

```
> gobuster dir -u <IP_MAQUINA> -w /usr/share/wordlists/dirbuster/
   directory-list-2.3-medium.txt -x php,txt,html
```

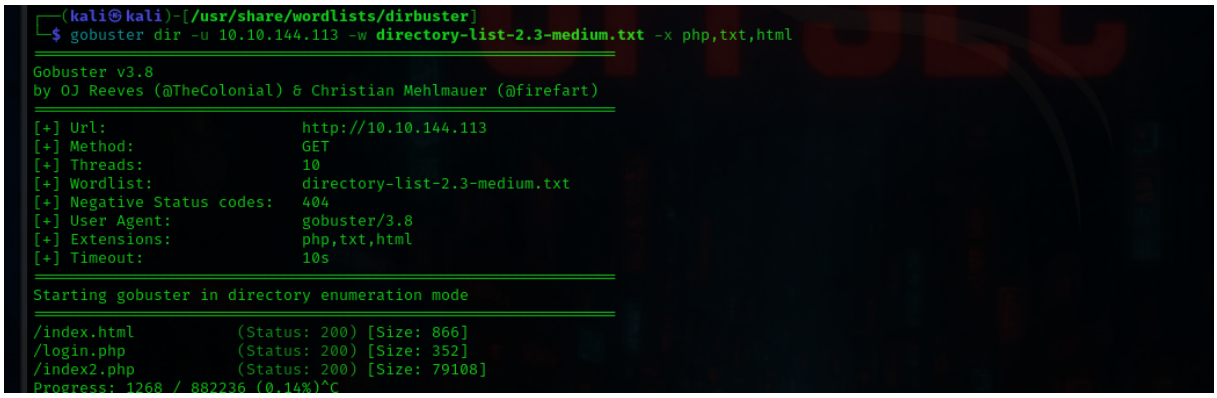

Figure 2: Resultado do Gobuster.

Ao acessar o diretório escondido, nos deparamos com a seguinte página nesse estilo cyberpunk.

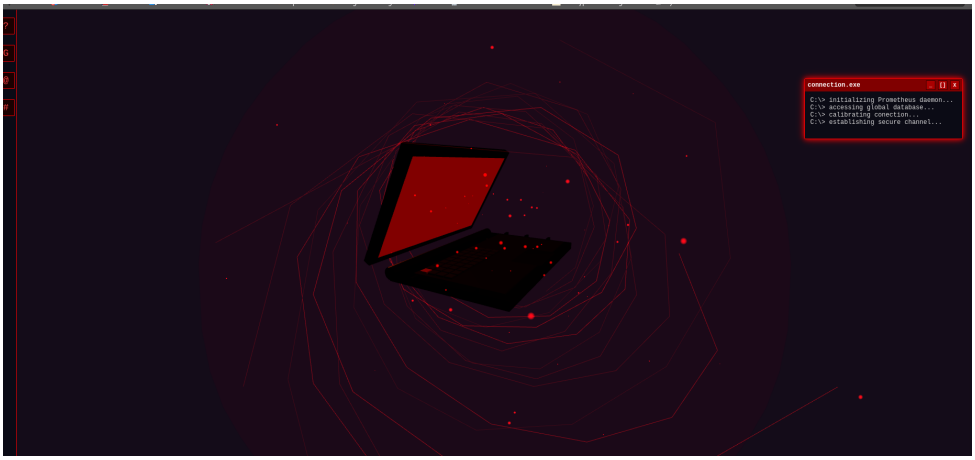

Figure 3: Página index2.php.

Ao analisar o código fonte da página, encontramos, no meio do código, uma mensagem em hexadecimal que, quando decodificada, responde a uma das perguntas feitas no desafio. Essa analise mostrou, também, um novo diretório que, ao que tudo indica, é uma página de login.

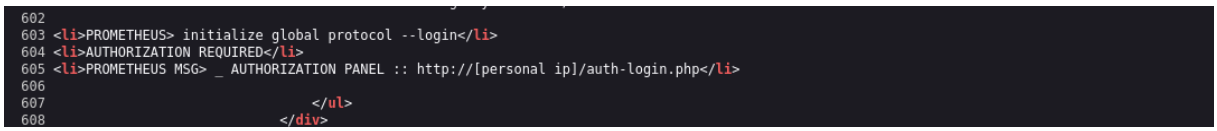

Figure 4: Novo diretório.

2 Vulnerabilidade e Exploração

Ao injetar o comando [’ OR ’1’=’1’] no campo user da nova aba encontrada, um erro de SQL foi retornado, confirmando uma vulnerabilidade de SQL Injection.

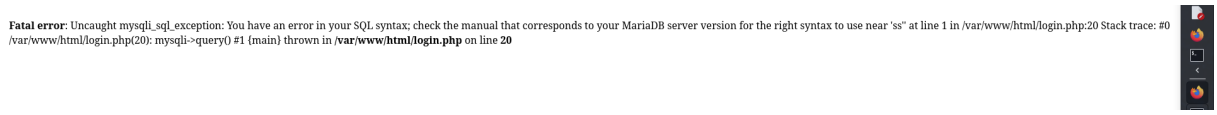

Figure 5: Erro de SQL confirmando a vulnerabilidade.

Para explorar essa vulnerabilidade, utilizei a ferramenta sqlmap para tentar extrair alguma informação extra que pudesse ajudar a fazer login pelo ssh.

```
> sqlmap -u "http://<IP_MAQUINA>/auth-login.php" --forms --crawl=1 --
    dump
```

Nesse comando, –forms instrui o sqlmap a procurar formulários HTML na URL alvo. quando encontramos esse formulário, o sqlmap identifica automaticamente os campos vulneráveis. Já o –crawl=1 ativa a funcionalidade de crawling do site, ou seja o sqlmap vai seguir os links encontrados na página alvo para descobrir outros potenciais pontos de injeção. O =1 define a profundidade do rastreamento, dessa forma, ele irá analisar a página inical e todos os links que encontrar nela. A flag –dumpé a flag que realmente age;;ela diz à ferramenta o que fazer depois de encontrar a vulnerabilidade.. Ela instrui especificamente o sqlmap a extrair todo o conteúdo das tabelas do banco de dados, e é exatamente aí que conseguimos o nosso login e nossa senha para acessar a porta 22.

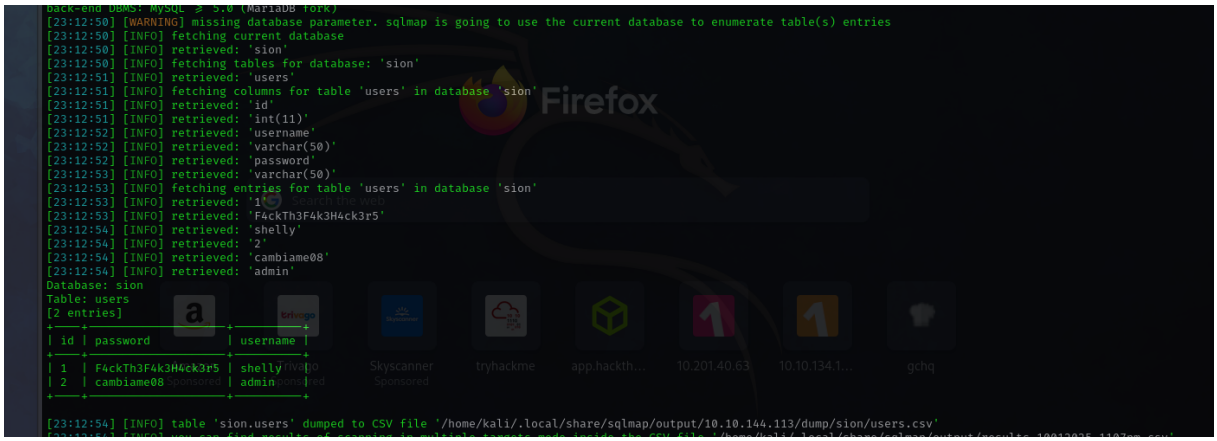

Figure 6: Sqlmap extraindo usuários e hashes de senhas.

O sqlmap obteve os hashes dos usuários `shelly`.

3 Acesso Inicial

Com a senha e o usuário podemos fazer login no sistema por meio do ssh.

```
> ssh shelly@10.10.144.113
```

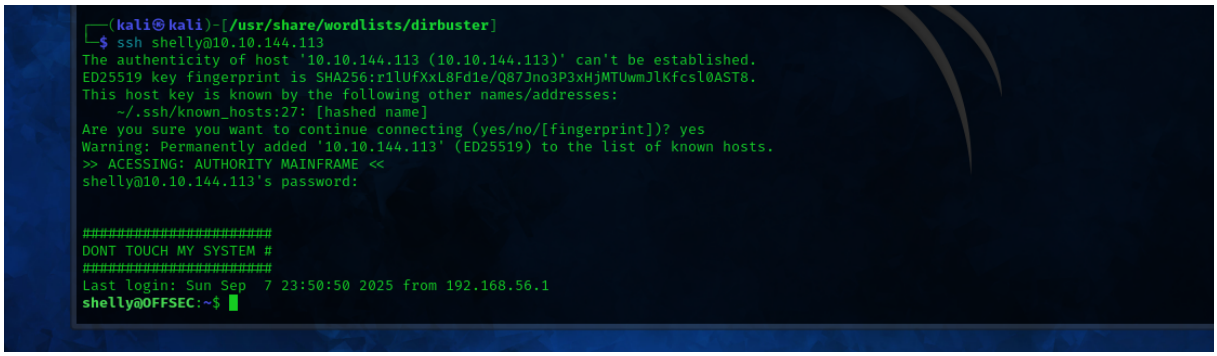

Figure 7: Sinto muito Shelly, mas agora já é tarde.

Uma vez dentro do sistema, só dar um cat para obtermos a flag do usuário.

Figure 8: Conteúdo do arquivo `user-flag.txt`.

4 Escalação de Privilégios

O comando -l revelou que o usuário shelly podia executar o comando <find> como sudo. Consultando o GTFObins, foi encontrado um método para escalar privilégios.

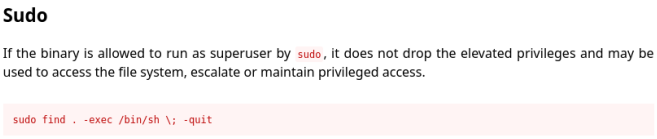

Figure 9: Comando para escalação de privilégios com `find`.

O comando foi executado na máquina alvo, concedendo um shell de root.

```
> sudo find . -exec /bin/sh \; -quit
```

Figure 10: Execução do comando e obtenção de acesso root.

Com acesso de root, a flag final foi encontrada dentro de um arquivo de imagem, sendo extraída com o comando `strings`.

Figure 11: Flag de root extraída do arquivo.

E assim termina o CTF Pr0m3th3us do CTF da satech 2025.