Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Silver Platter– Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 07/05/2025 |
| **Link** | https://tryhackme.com/room/silverplatter |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 07/05/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Directory, ports enumaration, busca por diretórios, IDOR, brute force, Priv Escalation |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[What is the user flag? 3](#_heading=h.3znysh7)

[What is the root flag? 3](#_heading=h.2et92p0)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

Silver Platter é um CTF divertido e prático, ele é nível fácil, e há diversos conceitos que vamos praticar, como por exemplo “idor” e “priv Escalation”

**Desenvolvimento**

**What is the user flag?**

Começando com um simples nmap, sem parâmetro algum, para poder ver as portas que estão abertas neste servidor.

Texto

O conteúdo gerado por IA pode estar incorreto.

Vemos que temos 3 portas abertas, que são a porta 80 (http), 22 (ssh) e a porta 8080 (http-proxy). Primeiro vamos focar na 80.

Acessando então o ip na rede, temos esse simples site:

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.  
Não há nada de interessante no inspecionar, porém, temos a página contatos, onde nos mostra o User do “scr1ptkiddy”, e um tal de Silverpeas meio estranho, mas vamos continuar.

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

Utilizando a ferramenta feroxbuster para fazer enumeração de diretório, infelizmente não achamos nada interessante, porém na porta 8080, temos coisas interessantes como o “website”, porém, é restrito

Texto

O conteúdo gerado por IA pode estar incorreto.

Mas se colocarmos o Silverpeas, que achamos antes, temos uma página interessante de login. Podemos testar algum tipo de Brute force com o user “scr1ptkiddy”

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Utilizando o Burp suit para poder pegar a requisição e preparar o brute force com o Hydra, algo não muito difícil

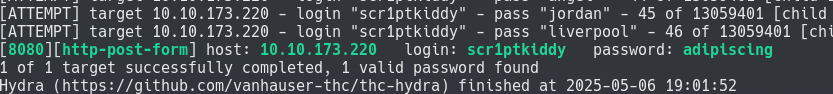
Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Pegando as informações que precisamos, podemos então começar o brute force.

Texto

O conteúdo gerado por IA pode estar incorreto.



Senha um pouco estranha, mas o user também não é nada normal, então relevamos.

Acessando então, vamos para a página principal após logar.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Clicando no nosso User e indo para a página de notificação, e acessando a primeira notificação que aparece, podemos ver que a URL, é alterada e ainda aparece um “id”, podemos então mandar um “IDOR” de sempre.

Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Tentando diversos números, quando chegamos no 6, podemos ver que há uma notificação nova, nos informando a senha e o user do ssh. Então, já sabemos nosso próximo alvo

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Então, usando as infos que nos foram dadas, podemos fazer um simples acesso ao SSH

Texto

O conteúdo gerado por IA pode estar incorreto.

E pronto, estamos dentro do sistema, agora vamos atrás das flags.

Fazendo uma simples busca pelos diretórios e pelos arquivos, é possível achar a primeira flag.

Texto

O conteúdo gerado por IA pode estar incorreto.

**What is the root flag?**

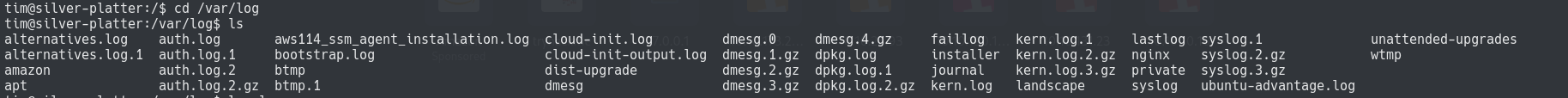
Agora, vai ser um pouco mais chato do que o normal. Usando um cat e acessando o “/etc/passwd” podemos ver que o User Tyler, tem direito root, temos que tentar acessa-lo então.

Texto

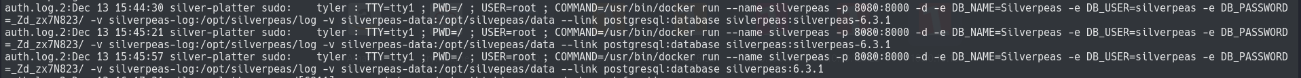
O conteúdo gerado por IA pode estar incorreto.



Usando agora o comando cd nos diretórios “/var/logs” e filtrando por “password” é possível achar algumas credenciais, como a própria senha do user Tyler, sendo ela “\_Zd\_zx7NB23/”







Agora temos o acesso a o user do Tyler, acessando este usuário, e indo até o diretório /root, temos a nossa segunda flag.

Texto

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

Silver Platter é um CTF simples que engloba diversos conceitos para se praticar e aprimorar suas habilidades.

**Referências**

Não há