Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Team – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Team – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 10/05/2025 |
| **Link** | https://tryhackme.com/room/teamcw |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 10/05/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Enumeração de diretórios e subdomínios, análise de código bash, escalonamento de privilégios. |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 2](#_Toc191235304)

[Desenvolvimento 3](#_Toc191235305)

[What is the user flag? 3](#_Toc191235306)

[What is the root flag? 8](#_Toc191235307)

[Conclusão 14](#_Toc191235308)

[Referências 14](#_Toc191235309)

Contextualização

O CTF Team é um desafio da plataforma TryHackMe, e que aborda vetores de ataque como: Arquivos e credenciais expostos e LFI. Um desafio que exemplifica os possíveis erros de segurança ao desenvolver uma aplicação em time, caso não seja tomado os devidos cuidados.

Desenvolvimento

What is the user flag?

Use o **Nmap** para escanear as portas abertas na máquina (*Port Scanning*).

Texto

O conteúdo gerado por IA pode estar incorreto.

A ferramenta aponta que a porta 21, 22 e 80 estão rodando os serviços de FTP para transferência de arquivos, SSH para conexão remota e HTTP para hospedagem de uma página web, respectivamente.

No navegador, abra a página web.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

O site mostra uma página padrão do Apache, um servidor web. Ao consultar o código fonte HTML, é possível ver uma mensagem deixada pelo desenvolvedor.

Texto

O conteúdo gerado por IA pode estar incorreto.

A mensagem é uma instrução para vincular o IP fornecido ao nome de domínio ‘team.thm’. Para isso, é necessário modificar o arquivo de texto ‘/etc/hosts’ da máquina local.

Texto

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Agora, ao acessar ‘http://team.thm/’ aparecerá a seguinte *Landing Page*.

Interface gráfica do usuário, Site

O conteúdo gerado por IA pode estar incorreto.

Trata-se de um simples blog, para continuar a exploração, use uma ferramenta de *Fuzzing* para enumerar os diretórios disponíveis no servidor web.

Texto

O conteúdo gerado por IA pode estar incorreto.

A ferramenta aponta a presença do arquivo ‘robots.txt’. No navegador, abra o arquivo ‘robots.txt’ responsável por informar aos buscadores quais partes de um site não devem ser indexadas.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Há apenas um texto que aparenta ser o nome de um usuário.

Para continuar a exploração, novamente com a ferramenta de *Fuzzing* procure por subdomínios na aplicação web.

Texto

O conteúdo gerado por IA pode estar incorreto.

Nesse caso, há um subdomínio notável (‘dev’). Adicione ao arquivo ‘/etc/hosts’ da máquina local.

Texto

O conteúdo gerado por IA pode estar incorreto.

Agora, será possível acessar esse domínio.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Há uma mensagem de que o site ainda está sendo construído. Ao clicar no link, o site redireciona para outra página que aparenta possuir uma vulnerabilidade.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

A vulnerabilidade em questão é chamada de LFI (Local File Inclusion), onde é possível explorar arquivos local de uma máquina a partir de uma requisição remota.

Visto que há um possível nome de usuário chamado ‘dale’, é possível deduzir um diretório para encontrar a primeira flag. Teste o diretório padrão ‘/home/dale’ e procure pelo arquivo ‘user.txt’.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

What is the root flag?

Para garantir a flag final, será necessário acessar a máquina do desafio e escalar privilégios. Para isso, use a vulnerabilidade descoberta anteriormente para procurar arquivos de credenciais SSH.

Texto

O conteúdo gerado por IA pode estar incorreto.

Há um arquivo exposto chamado ‘sshd\_config’ dentro do diretório ‘/etc/ssh’ que pode ser explorado, para melhor visualização abra o código fonte da página.

Texto

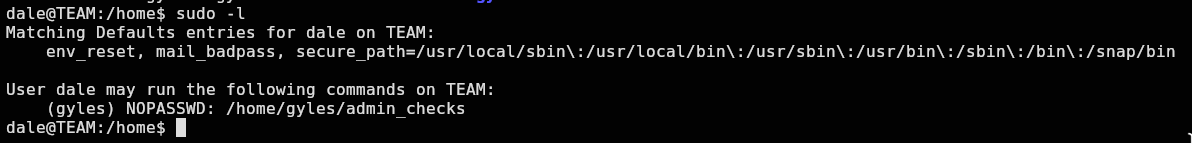
O conteúdo gerado por IA pode estar incorreto.

Nesse arquivo, é possível entrar a chave privada do usuário ‘dale’, copie e insira em um arquivo para usar posteriormente em uma conexão SSH. Use o comando ‘chmod’ para alterar as permissões da chave e usá-la como credenciais.

Texto

O conteúdo gerado por IA pode estar incorreto.

Credenciado como ‘dale’, consulte as permissões de usuário usando o comando ‘sudo -l’.



É possível ver o usuário ‘gyles’ consegue executar o script ‘admin\_checks’. Entre no diretório do usuário ‘gyles’ e use o comando ‘cat’ no script para descobrir o que faz o código.

Texto

O conteúdo gerado por IA pode estar incorreto.

O código solicita ao usuário um nome e uma data para fazer backups de arquivos. Mas a variável ‘error’ é executada ao final do código, permitindo a execução de comandos arbitrários. Use isso para fazer uma *Spawn Bash* usando python para criar uma bash como ‘gyles’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Como ‘gyles’, agora é possível executar scripts variados. Então, na máquina local baixe o **linPEAS** (ferramenta responsável por escanear vetores de escalonamento de privilégios) e hospede na máquina local com o comando ‘python -m http.server’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Então, execute a ferramenta para começar a escanear.

Uma imagem contendo Diagrama

O conteúdo gerado por IA pode estar incorreto.

Uma imagem contendo Texto

O conteúdo gerado por IA pode estar incorreto.

O **linPEAS** apontou um script chamado dev\_backup.sh. Navegue até o diretório para explorar o script de backup.

Texto

O conteúdo gerado por IA pode estar incorreto.

De acordo com as permissões, esse arquivo pode ser escrito e modificado. Então, faça uma *Reverse Shell* em bash para garantir acesso ao root.

Interface gráfica do usuário, Aplicativo, Teams

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Na máquina local, execute o comando **Netcat** ‘nc -lvnp {porta}’ para servir como *Listener* na porta especificada*.*

Texto

O conteúdo gerado por IA pode estar incorreto.

Ao acessar o usuário root, basta navegar até o diretório ‘/root’ e abrir a flag final do desafio.

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Conclusão

Esse CTF pode ser categorizado como de nível fácil, e que explora falhas simples que um sistema pode conter. Ele é ideal para iniciantes que desejam praticar técnicas básicas de *web hacking* e entender diferentes vulnerabilidades.

Referências

<https://www.revshells.com/>

<https://www.cloudflare.com/pt-br/learning/security/what-is-remote-code-execution/>

<https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS>