Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Chill Hack – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Chill Hack – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 16/03/2025 |
| **Link** | https://tryhackme.com/room/chillhack |

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

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 16/03/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio/Difícil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | FTP Anonymous, enumeração de diretórios, RCE, escalonamento de privilégios, estenografia e quebra de senhas com o JohnTheRipper. |
| **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)

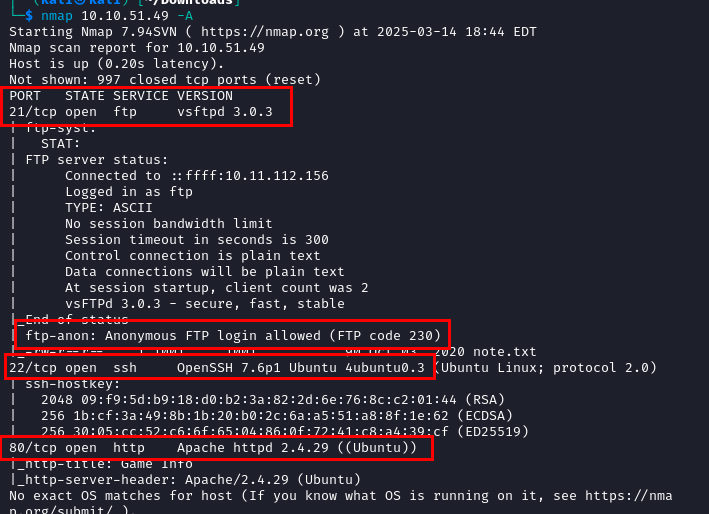
Contextualização

O Chill Hack é um CTF de nível médio/difícil a depender do nível de conhecimento. Ele aborda diversos temas extensos que podem parecer complicados de início.

Desenvolvimento

What is the user flag?

Para começar, use o **Nmap** para fazer um *Port Scanning* na máquina do TryHackMe.



Com esse resultado, é possível concluir que as portas 21, 22 e 80 estão abertas e rodando os serviços FTP (para transferência de arquivos), SSH (para conexões remotas) e HTTP (para Website). Além disso, há uma vulnerabilidade na máquina, chamada ‘Anonymous FTP’ onde é possível realizar uma conexão FTP sem credenciais, basta digitar ‘anonymous’ no usuário.

Texto

O conteúdo gerado por IA pode estar incorreto.

Com a autenticação realizada, é notável um arquivo chamado ‘note.txt’. Faça o download desse arquivo para a máquina local com o comando ‘get’.

Texto

O conteúdo gerado por IA pode estar incorreto.

O arquivo é uma mensagem dita por apaar, ele diz que há algo filtrando as strings do comando. Guarde essa informação para mais tarde.

O **Nmap** apresentou também a porta 80 aberta e executando uma página web. Use o navegador para investigar.

Interface gráfica do usuário, Site

O conteúdo gerado por IA pode estar incorreto.

Não há nada de interessante nesse site. Use o **Gobuster**ou **Dirb** para fazer uma enumeração de diretórios web.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

A ferramenta apontou que o diretório ‘/secret’ está presente entre os diretórios. Então, consulte esse diretório.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Nele está condido um RCE (Remote Code Execution), onde possivelmente aceita comandos bash.

Tela de computador com jogo

O conteúdo gerado por IA pode estar incorreto.

Ao testar outros comandos, será possível notar que há uma filtragem de string como foi dito anteriormente.

Uma imagem contendo Logotipo

O conteúdo gerado por IA pode estar incorreto.

Para enganar o filtro, use uma contrabarra (“\”) nas palavras filtradas.

Tela de computador com jogo

O conteúdo gerado por IA pode estar incorreto.

Use o **Burpsuite** no modo ‘proxy’ para fazer *requests* e facilitar a visualização da resposta do site. Então,comando ‘cat’ no arquivo ‘index.php’ para descobrir que tipo de filtro está atuando no site. Não esqueça de colocar a contrabarra no comando ‘cat’.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

O filtro está atuando nas palavras acima, então ao usar qualquer destes comandos, coloque a contrabarra.

Verifique se o python3 está instalado na máquina com o comando ‘which’

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

O **Burpsuite** mostra na *response* do site, que está instalado.

Então, use um comando em python3 para fazer uma fazer uma *request* de *Reverse Shell*, consulte o site [https://www.revshells.com/](https://www.revshells.com/%20) para isso. E use o **Netcat** na máquina local para escutar qualquer pedido de conexão na porta especificada.

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Uma *Reverse Shell* é o ato de injetar um código em um sistema, com o objetivo de fazer com que o sistema alvo se conecte de volta na máquina local. Em vez do atacante fazer o pedido para conectar à máquina alvo, a máquina alvo que faz o pedido ao atacante.

Use o comando do site na *request* e envie.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

A conexão foi bem-sucedida e foi autenticado como usuário ‘www-data’, um usuário sem privilégios. Para facilitar, faça uma *Spawn Bash*para facilitar a visualização do terminal. Então, use o parâmetro ‘-l’ no comando ‘sudo’ para exibir a lista de comandos que usuários sem privilégios podem executar como administrador.

Texto

O conteúdo gerado por IA pode estar incorreto.

É possível rodar o arquivo ‘helpline.sh’ como o usuário ‘apaar’. Navegue para o diretório ‘/home/apaar’ para investigar.

Texto

O conteúdo gerado por IA pode estar incorreto.

Nele há um arquivo de texto e um executável. Com o comando ‘cat’ veja o código do arquivo ‘helpline.sh’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Nele, é perguntado o nome de uma pessoa para o usuário ser atendido e uma mensagem. Porém, essa mensagem será executada pelo sistema.

Texto

O conteúdo gerado por IA pode estar incorreto.

Esse arquivo pode ser usado para realizar um escalonamento de privilégios.

Use o comando ‘sudo -u apaar /home/apaar/.helpline.sh’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Quando é rodado esse comando, a mensagem é executada como usuário ‘apaar’. Então, ao invés de digitar ‘whoami’, digite ‘/bin/sh’ para gerar um terminal no nome ‘apaar’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Com esse usuário, verifique o arquivo ‘local.txt’ e lá estará a *User flag.*

Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

What is the root flag?

Para acessar a flag *root* deve-se escalonar novamente os privilégios, visto que o usuário ‘apaar’ não possui essa permissão.

Navegando entre os arquivos do sistema. Encontra-se uma pasta ‘files’ responsável por outro servidor web.

Texto

O conteúdo gerado por IA pode estar incorreto.

Ao acessar o código da página ‘hacker.php’, é visto uma mensagem.

Texto

O conteúdo gerado por IA pode estar incorreto.

“Olhe no escuro! Você encontrará sua resposta”.

Pode ser uma dica para consultar as imagens presentes nos diretórios.

Texto

O conteúdo gerado por IA pode estar incorreto.

Há dois arquivos, inicie um servidor python na máquina alvo, e na máquina local faça o download do arquivo.

Texto

O conteúdo gerado por IA pode estar incorreto.

Com a foto, use a ferramenta**Steghide** para procurar arquivos escondidos na foto. A ferramenta irá pedir uma senha, basta pressionar ‘enter’ para prosseguir.

Texto

O conteúdo gerado por IA pode estar incorreto.

A ferramenta foi capaz de extrair o arquivo ‘backup.zip’. Com o **Unzip** procure extrair os arquivos comprimidos.

Texto

O conteúdo gerado por IA pode estar incorreto.

A ferramenta solicita uma senha que é desconhecida. Para descobri-la, use a ferramenta **John2zip** para criar um hash da senha que o **JohnTheRipper** será capaz de quebrar.

Texto

O conteúdo gerado por IA pode estar incorreto.

O hash foi direcionado com o caractere ‘>’ para o arquivo ‘hash.txt.

Então, com o **John** especifique o arquivo da hash e um wordlist.

Texto

O conteúdo gerado por IA pode estar incorreto.

Ele foi capaz de quebrar a senha, use ela para descomprimir o arquivo.

Texto

O conteúdo gerado por IA pode estar incorreto.

No arquivo oriundo da descompressão, foi exposto uma possível senha criptografada em base64. Faça a conversão para descobrir a senha original.

Texto

O conteúdo gerado por IA pode estar incorreto.

Essa pode ser a possível senha para o usuário mais privilegiado que o ‘apaar’, o ‘anurodh’. Voltando para a máquina alvo, com o comando ‘sudo -u anurodh’ troque de usuário. Será solicitado uma senha, digite a senha descoberta recentemente.

Texto

O conteúdo gerado por IA pode estar incorreto.

Agora, foi possível acessar o usuário ‘anurodh’ e que pertence ao grupo a um grupo que tem acesso ao ‘docker’. No site [https://gtfobins.github.io/](https://gtfobins.github.io/%20) é possível encontrar um script referente a um binário **SUID** que permite escalonar privilégios.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Agora, com o acesso ao ‘root’, navegue para a pasta ‘/root’ e visualize o arquivo referente a *flag*.

Texto

O conteúdo gerado por IA pode estar incorreto.

Conclusão

Esse desafio pode ser um bom candidato para quem busca desafiar o próprio conhecimento, pode ser excelente para concretizar conhecimentos caso seja um usuário mais avançado de CTFs.

Referências

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

<https://gtfobins.github.io/>

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