Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Anonymous – TryHackme

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Anonymous – Larissa Gomes |
| **N° Revisão** | 1 |
| **Data de publicação** | 16/10/2025 |
| **Link** | <https://tryhackme.com/room/anonymous> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Larissa Gomes | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 29/09/2025 | Produção |
| **1** | 16/10/2025 | Revisão |
| **2** | 16/10/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Linux e Privilege escalation |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_Toc210032203)

[Desenvolvimento 3](#_Toc210032204)

[Enumerate the machine. How many ports are open? 3](#_Toc210032205)

[What service is running on port 21? 3](#_Toc210032206)

[What service is running on ports 139 and 445? 3](#_Toc210032207)

[There's a share on the user's computer. What's it called? 4](#_Toc210032208)

[user.txt 4](#_Toc210032209)

[root.txt 8](#_Toc210032210)

[Conclusão 10](#_Toc210032211)

[Referências 10](#_Toc210032212)

Contextualização

O CTF se baseia em achar duas flags, explorando arquivos e usando o conhecimento em Linux e Privilegie Escalation. Sendo uma virtual machine para iniciantes.

Desenvolvimento

Enumerate the machine. How many ports are open?

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

Com isso a ferramenta aponta que a **porta 22** está rodando o serviço de SSH para conexão remota e na **porta 21** está rodando um FTP.

Texto

O conteúdo gerado por IA pode estar incorreto.

What service is running on port 21?

O **Nmap** apontou que a **porta 21** roda um FTP.

Texto

O conteúdo gerado por IA pode estar incorreto.

What service is running on ports 139 and 445?

O Nmap apontou que a **porta 139** e a **porta 445** estão rodando smb.

Texto

O conteúdo gerado por IA pode estar incorreto.

There's a share on the user's computer. What's it called?

Use o comando **smbclient** para buscar e descobrir o usuário.

Texto

O conteúdo gerado por IA pode estar incorreto.

user.txt

Conecte-se ao serviço FTP usando o Usuário anonymous, e explore os arquivos.

Texto

O conteúdo gerado por IA pode estar incorreto.

Encontre os arquivos **“to\_do.txt”**, **“clean.sh”** e **“removed\_files.log”**, que são arquivos interessantes e baixe eles usando o comando **GET**.

Texto

O conteúdo gerado por IA pode estar incorreto.Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Abra os arquivos baixados anteriormente, e com isso é possível descobrir que o arquivo **“clean.sh”** registra uma mensagem sempre que o **“removed\_files.log”** é atualizado e isso ocorre a cada minuto.

Sabendo disso injete uma reverse shell usando um novo arquivo **“clean.sh”** criado no computador local e, assim, no FTP use o comando **PUT** para fazer upload do **“clean.sh”**.

Interface gráfica do usuário, Texto, Aplicativo, Teams

O conteúdo gerado por IA pode estar incorreto.Texto

O conteúdo gerado por IA pode estar incorreto.

Após conectar-se na máquina, busque pela flag explorando os diretórios.

Texto

O conteúdo gerado por IA pode estar incorreto.Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

root.txt

Use o comando “**find**” para buscar arquivos com o bit SUID ativado. Isso permite a identificação de executáveis que podem ser manipulados para rodar com as permissões do usuário root.

Após encontrá-lo use o **GTFOBins** para descobrir o comando para escalonar.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.Texto

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Execute o comando pego no **GTFOBins** e assim entre como root e busque pela última flag.

Texto

O conteúdo gerado por IA pode estar incorreto.

Ícone

O conteúdo gerado por IA pode estar incorreto.

Conclusão

O desafio de "Annonymous" da plataforma TryHackMe foi uma excelente oportunidade para praticar e estudar. O documento detalha as etapas seguidas para a resolução do CTF, que abordou conceitos como Linux e Privilege Escalation.

Referências

[Chat GPT](https://chatgpt.com/) – Utilizado para estudo e dúvidas

[GTFOBins](https://gtfobins.github.io/) – Utilizado para escalação de privilégios