Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Basic Pentesting – Tryhackme

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Basic Pentesting – Larissa Gomes |
| **N° Revisão** | 1 |
| **Data de publicação** | 08/09/2025 |
| **Link** | <https://tryhackme.com/room/basicpentestingjt> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Larissa Gomes | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 08/09/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | brute forcing, hash cracking, service enumeration e Linux Enumeration |
| **Plataforma** | Tryhackme |
| **Área** | Red. |

**Sumário**

[Contextualização 3](#_Toc208220274)

[Desenvolvimento 3](#_Toc208220275)

[Find the services exposed by the machine 3](#_Toc208220276)

[What is the name of the hidden directory on the web SERVER (enter name without /)? 3](#_Toc208220277)

[What is the username? 4](#_Toc208220278)

[What is the password? 4](#_Toc208220279)

[What service do you use to access the SERVER (answer in abbreviation in all caps)? 5](#_Toc208220280)

[What is the name of the other user you FOUND (all lower case)? 5](#_Toc208220281)

[If you have found another user, what can you do with this information? 5](#_Toc208220282)

[What is the final password you obtain? 6](#_Toc208220283)

[Conclusão 7](#_Toc208220284)

[Referências 7](#_Toc208220285)

Contextualização

O CTF Basic Pentesting é um desafio da plataforma TryHackMe, e aborda temas de ataque como: Brute forcing, hash cracking, service enumeration e Linux enumeration. Sendo um desafio para praticar web hacking.

Desenvolvimento

Find the services exposed by the machine

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 80 está rodando um HTTP para hospedagem de uma página web.

Texto

O conteúdo gerado por IA pode estar incorreto.

What is the name of the hidden directory on the web SERVER (enter name without /)?

Para explorar mais a página web use o **Gobuster** para enumerar os diretórios disponíveis no servidor web.

A ferramenta apontou a presença do diretório “/development”, abra o diretório.

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Dentro do diretório há dois arquivos O “dev.txt” e “j.txt”, abra eles.

Dentro desses arquivos há uma conversa entre dois usuários.

What is the username?

Para descobrir os usernames é necessário usar uma enumeração, então use o comando **enum4linux <IP>.**

A ferramenta apontou dois usuários, “kay” e “jan”.



Texto

O conteúdo gerado por IA pode estar incorreto.

What is the password?

Com os usuários encontrados, use o **Hydra** para descobrir os dados de login da porta SSH.

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

What service do you use to access the SERVER (answer in abbreviation in all caps)?

Para descobrir qual serviço dará acesso ao servidor, volte no resultado do **Nmap.**

Texto

O conteúdo gerado por IA pode estar incorreto.

What is the name of the other user you FOUND (all lower case)?

Conecte-se ao serviço SSH usando a senha e usuário obtido anteriormente, é possível entrar com o usuário “Jan”.

Texto

O conteúdo gerado por IA pode estar incorreto.Texto

O conteúdo gerado por IA pode estar incorreto.

If you have found another user, what can you do with this information?

Conectado ao serviço de SSH, busque entre os diretórios. Com isso é possível encontrar o usuário “Kay“ do qual já havia sido encontrado na enumeração.

**Parte superior do formulário**

Texto

O conteúdo gerado por IA pode estar incorreto.

What is the final password you obtain?Parte superior do formulário

Assim explore os diretórios no usuário “kay”, com isso é possível encontrar um arquivo interessante o **“pass.bak”** onde possivelmente se encontra a flag, porém não há acesso para abrir este arquivo.

Além desse arquivo também pode ser encontrado uma pasta oculta com o nome “ssh” da qual possui **credenciais para autentificação por RSA**, dos quais são os arquivos “id\_rsa” e is\_rsa.pub. Com isso é possível descobrir que a chave privada esta criptografada no arquivo “id\_rsa”.

Texto

O conteúdo gerado por IA pode estar incorreto.Texto

O conteúdo gerado por IA pode estar incorreto.Texto

O conteúdo gerado por IA pode estar incorreto.

Para quebrar o arquivo com a **rsa**, copie a chave e crie um arquivo idêntico e assim use o **JohnTheRipper** para descriptografar e descobrir a chave.

Texto

O conteúdo gerado por IA pode estar incorreto.

Assim quando descobrir a chave descriptografada conecte-se com o usuario “kay” e com isso use o **cat** para abrir a flag que está dentro do arquivo **“pass.bak”**

Tela preta com letras brancas

O conteúdo gerado por IA pode estar incorreto.lInterface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

Conclusão

O desafio de "Basic Pentesting" da plataforma TryHackMe foi uma excelente oportunidade para praticar diversas técnicas de ataque e enumeração. O documento detalha as etapas seguidas para a resolução do CTF, que abordou conceitos como brute forcing, hash cracking, service enumeration, e Linux enumeration.

Referências

* [Slide - capacitação 8](https://www.canva.com/design/DAGoyBibFf8/iIhETF-sMmBAWMIXGhuNNg/edit)
* [Capacitação 8](https://github.com/GuardianMaua/frente_registro.git)
* [ChatGPT - dúvidas](https://openai.com/pt-BR/)