Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF Basic Pentesting |
| **N° Revisão** | 1 |
| **Data de publicação** | 14/08/2025 |
| **Link** | https://tryhackme.com/room/basicpentestingjt |

|  |  |  |
| --- | --- | --- |
| **Redação** | Gabriel Lippi da Costa | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | 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, Linux Enumeration |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

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

[Subtítulo caso necessário 3](#_heading=h.30j0zll)

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

[Pergunta 1 3](#_heading=h.3znysh7)

[Pergunta 2 3](#_heading=h.2et92p0)

[Pergunta 3 3](#_heading=h.tyjcwt)

[Pergunta N 3](#_heading=h.3dy6vkm)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

Este é um CTF de testagem de penetração: um laboratório prático de segurança que ensina a encontrar vulnerabilidades simples em sistemas e aplicações, explorando serviços, senhas fracas e arquivos ocultos para capturar 'flags'.

**Desenvolvimento**

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

Texto

O conteúdo gerado por IA pode estar incorreto.

É necessário executar o Gobuster para achar o diretório escondido.

**What is the username?**

**Username:** Jan.

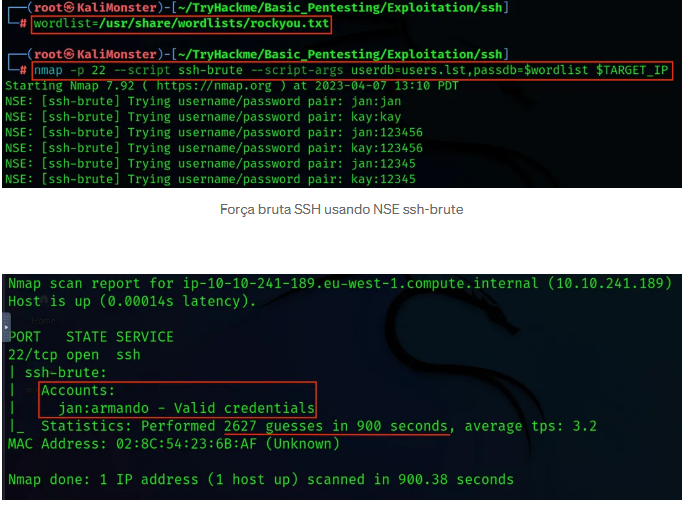
**What is the password?**

**Password:** Armando

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

**SSH** -> Comando para achar o SSH: nmap -sC -sV -sS “PING”.

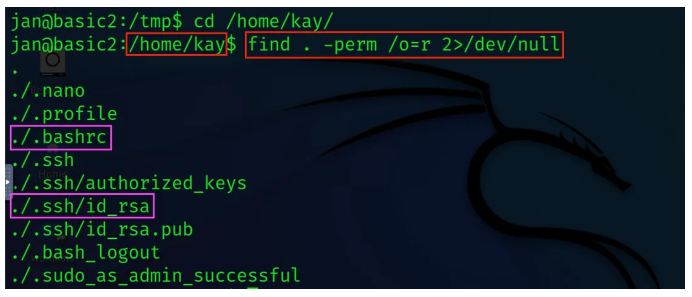
**What is the name of the other user you found(all lower case)?**

****

Basta fazer apenas fazer um **Brute-Force** via **NMAP** para descobrir a credencial.

**Username:** kay

**What is the final password you obtain?**

****

Se dermos “whoami” assim que entramos no SSH podemos ver que somos o usuário “jan” que não tem privilégios o suficiente.



Consegui descobrir a senha da chave privada. Vou tentar fazer login na conta do Jay:

Texto

O conteúdo gerado por IA pode estar incorreto.

**Password:**

heresareallystrongpasswordthatfollowsthepasswordpolicy$$

**Conclusão**

O **CTF Basic Pentesting** simula um teste de penetração básico, passando pelas etapas de enumeração, exploração e elevação de privilégios para capturar a flag final, servindo como prática introdutória de pentest.

**Referências**

OPENAI. ChatGPT. Disponível em: <https://chat.openai.com/>. Acesso em: 14 ago. 2025.

**0liverFlow.** *Basic Pentesting: TryHackMe*. Medium, 15 abr. 2023. Disponível em: <https://olivierkonate.medium.com/basic-pentesting-tryhackme-easy-cf88f2223e7b>.