

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Brooklyn Nine Nine - Edgar |
| **N° Revisão** | 1 |
| **Data de publicação** | 02/09/2024 |
| **Link** | <https://tryhackme.com/r/room/brooklynninenine> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Edgar | 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 |

**Sumário**

**Contextualização**

Nesta sala, aprenderemos a usar conhecimentos básicos de FTP no modo anonymous,bruteforce e privilege escalation

**Desenvolvimento**

**User flag**

Usando o nmap na máquina vemos:



E podemos ver o usuario Anonymous esta habilitado

Entrando como usuario anonymous vemos:



Lendo o arquivo note\_to\_jake alguem diz que a senha do jake esta fraca,portanto podemos tentar fazer um bruteforce utilizando o comando:

hydra -l jake -P /usr/share/wordlists/rockyou.txt <machine-ip> ssh -t 4

E obtemos

Usuario: Jake

Senha: ------

Usando o ssh na maquina podemos ler a user.txt DENTRO DA /HOME/HOLT



**Root flag**

Usando o comando sudo -l vemos que o comando less pode ser utlizado para ganhar acesso root usando o comando:

sudo less /etc/profile

!/bin/sh

E com isso podemos ler a root.txt



**Conclusão**

Um CTF bem fácil para testar os conhecimentos básicos