Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Brooklyn Nine Nine – TryHackMe

|  |  |
| --- | --- |
| **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** | João Branco | Presidente |
| **Aprovação** | João Branco | Presidente |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 02/09/2024 | Produção |
| **1** | 02/09/2024 | Revisão |
| **2** | 02/09/2024 | Aprovação |

**Sumário**

[Contextualização](#_heading=h.gjdgxs) 2

[Desenvolvimento](#_heading=h.1fob9te) 2

[User Flag](#_heading=h.3znysh7) 2

[Root Flag](#_heading=h.2et92p0) 4

[Conclusão](#_heading=h.1t3h5sf) 4

[Referências 4](#_heading=h.4d34og8)

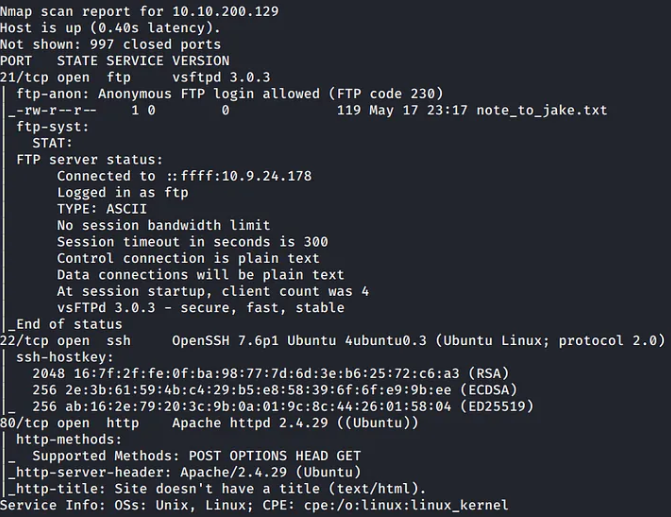
**Contextualização**

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

**Desenvolvimento**

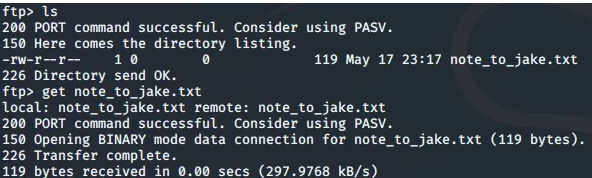
**User Flag**

Usando o nmap na máquina vemos:



E podemos ver o usuário Anonymous está habilitado

Entrando como usuário anonymous vemos:



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

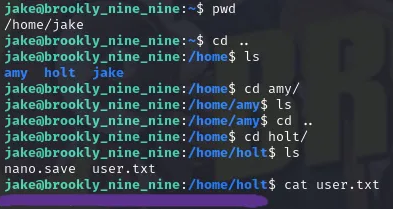
hydra -l jake -P /usr/share/wordlists/rockyou.txt <machine-ip> ssh -t 4

E obtemos

Usuário: Jake

Senha: ------

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



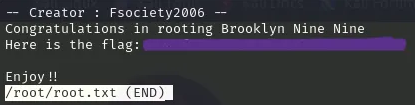
**Root Flag**

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

**Referências**