Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF de estudo – Guilherme Thomasi Ronca |
| **N° Revisão** | 1 |
| **Data de publicação** | 25/10/2025 |
| **Link** | https://tryhackme.com/room/res |

|  |  |  |
| --- | --- | --- |
| **Redação** | Guilherme Thomasi Ronca | 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** | Pago |
| **Conceitos envolvidos** | Linux, Redis, Privilege Escalation |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

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

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

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

Scan the machine, how many ports are open? [3](#_heading=h.3znysh7)

What is the database management system installed on the server? [3](#_heading=h.2et92p0)

What port is the database management system running on? [3](#_heading=h.tyjcwt)

What is the version of management system installed on the server? 3

Compromise the machine andlocate user.txt 3

Wha tis the local user account password? 4

Escalate privileges and obtain root.txt5

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

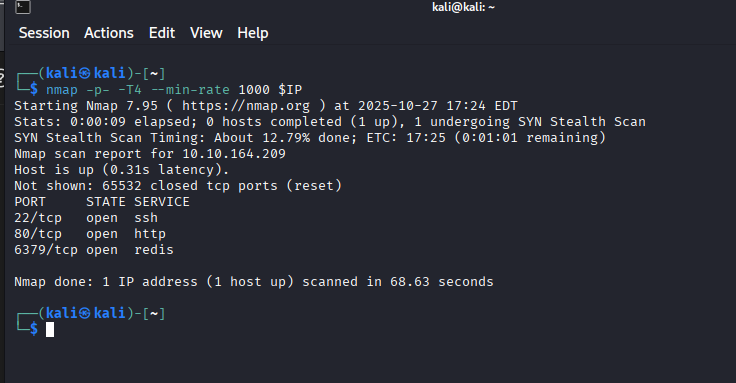
**Contextualização**

Desafio pago da plataforma TryHackMe, que tem como objetivo principal invadir uma máquina Linux.

**Desenvolvimento**

**Scan the machine, how many ports are open?**

Primeiramente, fiz um nmap para checar todas as portas.

****

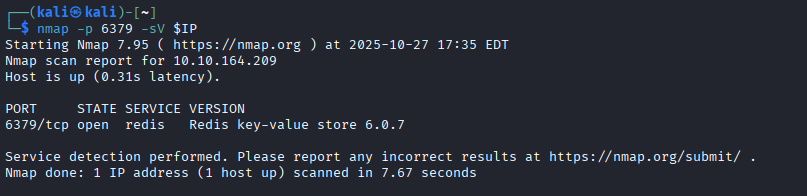
**What is the database management system installed on the server?**

R: Redis

**What port is the database management system running on?**

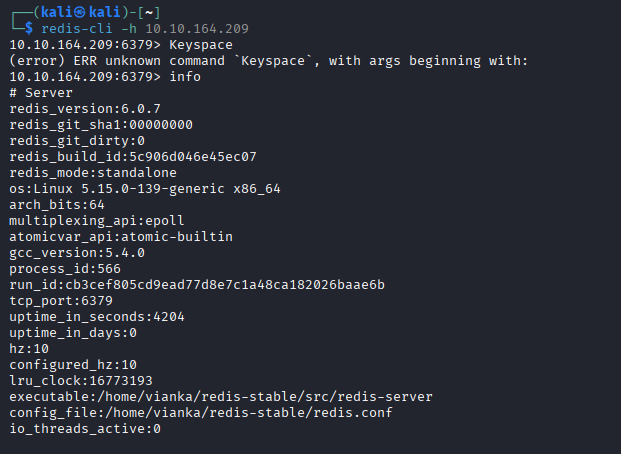
R: 6379

**Wha is the version of the management system installed on the server?**

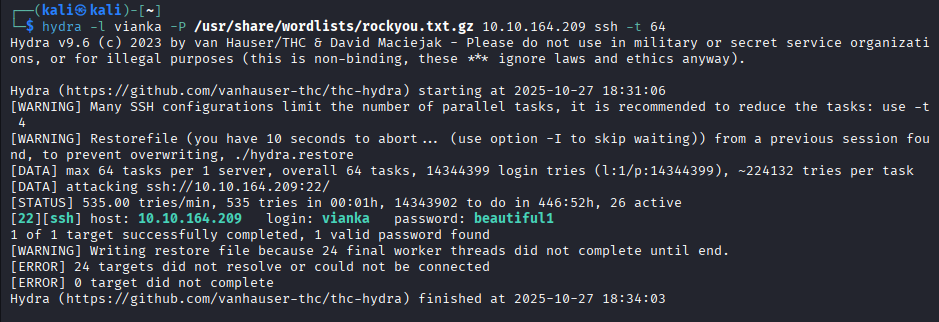


**Compromise the machine and locate user.txt**

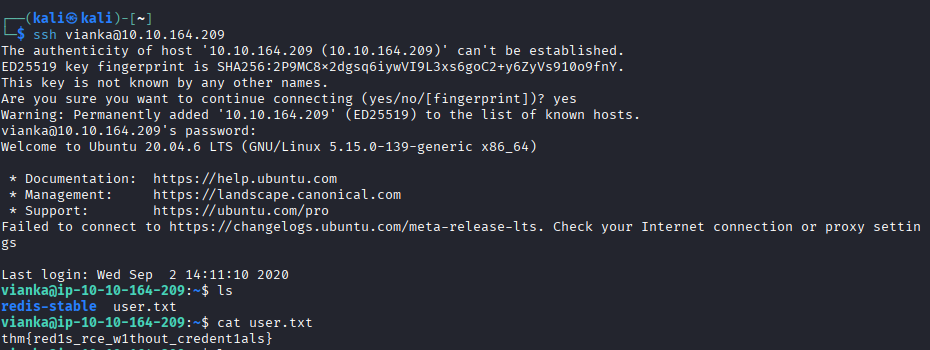
Utilizando o redis-cli e o host da máquina, entrei dentro do serviço, pois não foi necessário uma senha. Depois disso rodei um info para descobrir informações dos sistema. Com isso descobri um possível usuário em /home/vianka.



Com o usuário, utilizei o hydra com rockyou.txt para fazer o brute force da senha pelo ssh.



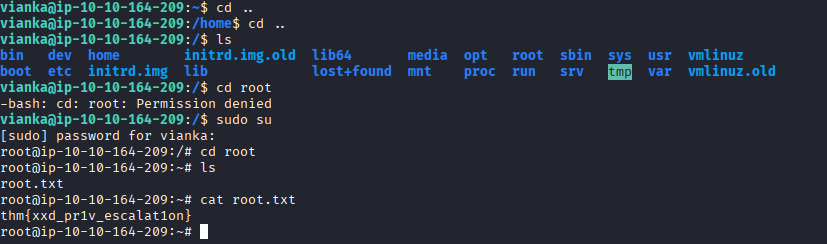
Conseguindo a senha, entrei no sistema e consegui o user.txt.



**What is the local user account password?**

**R: beautiful1**

**Escalate privileges and obtain root.txt**

Já dentro do sistema, fiz uma navegação de diretórios para encontrar o root. Assim, com um sudo su e a senha encontrada, entrei em root e consegui a flag.

**Conclusão**

O desafio foi bem simples, porém foi interessante pois nunca havia feito um CTF utilizando redis antes.

**Referências**

<https://book.hacktricks.wiki/en/network-services-pentesting/6379-pentesting-redis.html>