Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

chocolatefactory – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | chocolatefactory – Enrico Santarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 06/09/2024 |
| **Link** | <https://tryhackme.com/r/room/chocolatefactory> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Enrico Santarelli | Membro |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 06/09/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

Contextualização 3

Desenvolvimento 3

Enter the key you found! 3

What is Charlie's password? 4

Enter the user flag 5

Enter the root flag 6

Conclusão 7

Referências 7

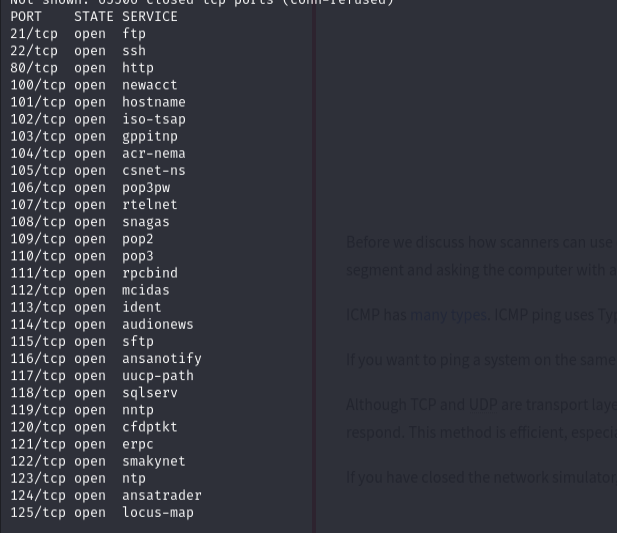
**Contextualização**

Este CTF de nível fácil é ideal para iniciantes que desejam aprender os fundamentos de segurança cibernética. É uma oportunidade prática para quem está começando no mundo dos CTFs e quer se familiarizar com ferramentas e técnicas essenciais de pentesting.

**Desenvolvimento**

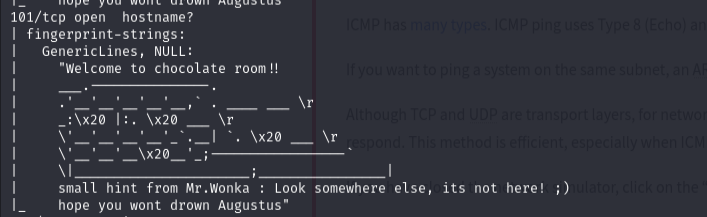
**Enter the key you found!**

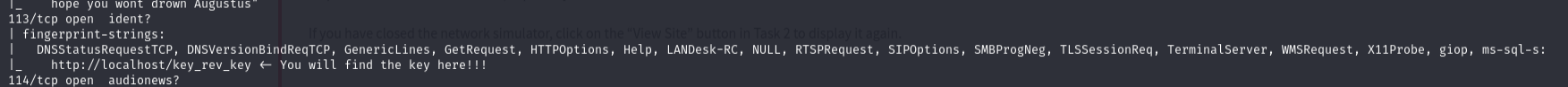
Mapeamento de todas as portas com Nmap com flag –p-.



O mapeamento de forma profunda com –A mostrou informações importantes:

* FTP com login Anonymous
* Sequência de portas 100-125 mostrou mensagens para procurar em outro lugar com exceção da porta 113 que indicou o caminho da chave.



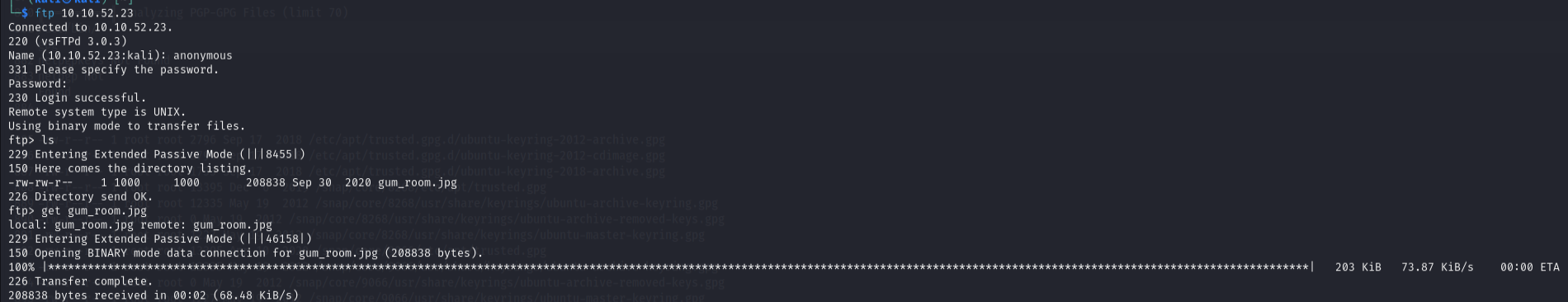


Acessando o path /key\_rev\_key o browser baixa um arquivo chamada key\_rev\_key que possui a chave da questão.



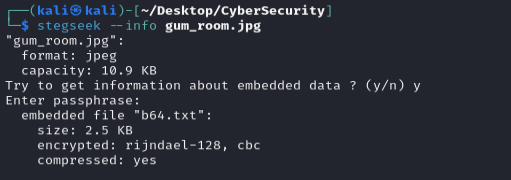
**What is the Charlie’s password?**

Conectando via FTP utilizando o usuário Anonymous encontramos um arquivo chamado gum\_room.jpg.

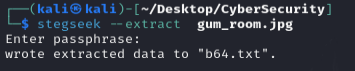


A imagem parece ocultar informações usando estenografia.

Usando a ferramenta stegseek para verificar as informações encontramos um arquivo chamado b64.txt que indica que está criptografado em base64.



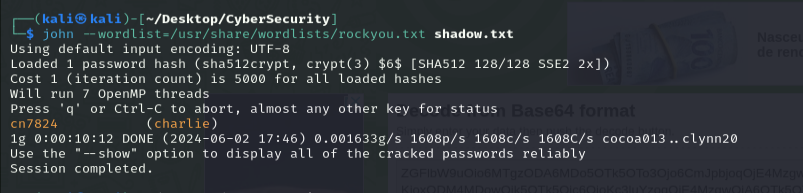
Extraindo o arquivo usando o stegseek não foi necessário o uso de senha.



Decriptografando o arquivo usando o website base64decode descobrimos que o arquivo era o /etc/shadow. Ref: https://www.base64decode.org.



Usando o john é possível decriptografar e descobrir a senha do usuário charlie.



**Enter the user flag.**

Fazendo login no website usando o usuário Charlie encontramos um input que realiza RCE no bash da máquina.



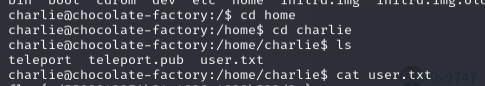
Procurando nas pastas, encontramos dentro da pasta do usuário Charlie chaves RSA pública e privada.



Tendo isso podemos conectar via ssh utilizando o usuário charlie e sua chave privada.



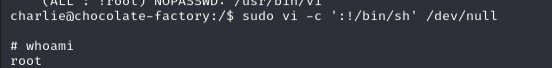
A flag do usuário está presente no diretório do usuário em /home/charlie.



**Enter the root flag.**

Procurando comandos que podem ser executados em modo sudo encontramos o vi.

Buscando no website gtfobins conseguimos realizar o escalonamento do privilégio para root. Ref: <https://gtfobins.github.io/gtfobins/vi/#sudo.>



Dentro da pasta root há apenas um arquivo root.py que ao rodar ele apenas pede a chave obtida no ínicio para liberar a chave.





**Conclusão**

Esse CTF é de nível fácil, aborda os conhecimentos iniciais de realização de CTFs, como: análise de port scanning, decriptografia de base64, reverse shell em RCE e privesc com sudo.

**Referências**

* <https://gtfobins.github.io/gtfobins/vi/#sudo.>
* https://www.base64decode.org