Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF Agente Sudo |
| **N° Revisão** | 1 |
| **Data de publicação** | 22/08/2025 |
| **Link** | https://tryhackme.com/room/agentsudoctf |

|  |  |  |
| --- | --- | --- |
| **Redação** | Nome do realizador | Gabriel Lippi da Costa |
| **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** | Gratuito |
| **Conceitos envolvidos** | Enumeration, hydra, FTP, steganalysis, SUDO |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

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

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

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

[Pergunta 1 3](#_heading=h.3znysh7)

[Pergunta 2 3](#_heading=h.2et92p0)

[Pergunta 3 3](#_heading=h.tyjcwt)

[Pergunta N 3](#_heading=h.3dy6vkm)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

O CTF "Agente Sudo" simula um cenário de investigação cibernética envolvendo agentes secretos, onde o objetivo é explorar vulnerabilidades em serviços como FTP, HTTP e SSH, utilizando técnicas de enumeração, brute-force, esteganografia e escalação de privilégios para descobrir informações sensíveis e flags escondidas.

**Desenvolvimento**

**How many open ports?**

**Resposta: 3**

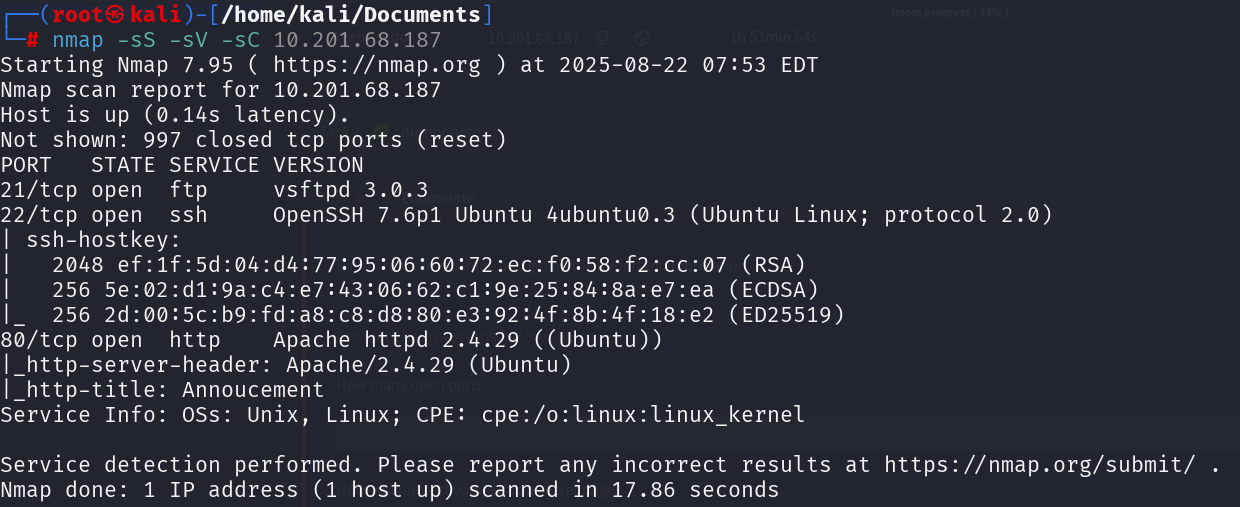
Na primeira task, era necessário utilizar o seguinte comando:

“**nmap -sS -sV -sC 10.201.68.187**”.

Com isso, é possível descobrir quantas portas estão abertas naquele IP.

Portas abertas:

* **21 – FTP**
* **22 – SSH**
* **80 – HTTP**



**How you redirect yourself to a secret page?**

**Resposta: user-agent**

Quando você acessava na URL IP:80, essa porta exibia uma página web que informava que apenas usuários com o User-Agent correto conseguiam se redirecionar para a página secreta.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

**What is the agent name?**

**Resposta: chris**

A página web da porta 80 possui outra página escondida. Para descobrir o nome do agente, é necessário usar o **Burp Suite**:

1. Abrir o **Burp Suite**.
2. Clicar na opção **Proxy** no menu superior central da janela do Burp Suite.
3. Clicar no botão **Open Browser**.
4. Inserir a URL nesse navegador do Burp Suite.
5. Clicar no botão **Intercept off**.
6. Apagar tudo do campo **User-Agent** e digitar a letra **C**.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

**FTP password**

**Resposta: crystal**

Era necessário realizar um brute force usando o Hydra no FTP. Com isso, a senha descoberta pelo Hydra foi “CRYSTAL”.

**Texto

O conteúdo gerado por IA pode estar incorreto.**

Após encontrar a senha, acessei o FTP para verificar o conteúdo e encontrei duas imagens e um arquivo .txt.

**Texto

O conteúdo gerado por IA pode estar incorreto.**

O conteúdo do arquivo .txt era o seguinte:

**Texto

O conteúdo gerado por IA pode estar incorreto.**

**Zip file password**  
**Resposta:** alien

Não encontrei nada de relevante diretamente no arquivo, então decidi analisar os **metadados** das duas imagens e acabei descobrindo algo interessante.

Uma das imagens estava em formato binário. Com isso, usei o comando:

**“binwalk -e --run-as=root cutie.png”** e encontrei um arquivo escondido.

Texto

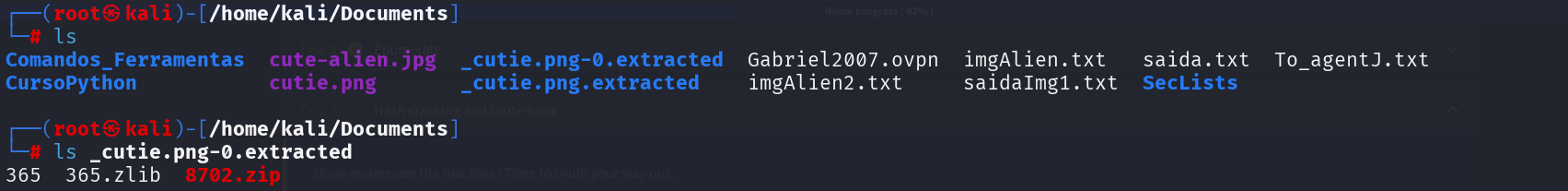
O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

O comando retornou um diretório. Ao entrar nele, encontrei um arquivo muito importante: **8702.zip**. Como o comando unzip não funcionava, usei:

**“7z e 8702.zip”.**



Ele solicitou uma senha, então realizei um **brute force** com o **John the Ripper** para descobri-la, usando:

**“zip2john 8702.zip > 8702.hash”.**

A senha descoberta foi **alien**.

Texto

O conteúdo gerado por IA pode estar incorreto.

Texto escrito dentro do arquivo:

Texto

O conteúdo gerado por IA pode estar incorreto.

**steg password**

**Resposta: Area51**

Ao abrir o arquivo **To\_agentR.txt**, encontrei uma mensagem codificada em **Base64**. Ao decodificá-la, obtive a resposta: **“Area51”**.

**Texto

O conteúdo gerado por IA pode estar incorreto.**

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

**Resposta: james**

E para achar o nome do outro agente bastava usar a ferramenta **“steghide”**

na imagem: **cute-alien.jpg.**

**Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.**

**SSH password**

**Resposta: hackerrules!**

Essa é a senha do SSH do usuário james.

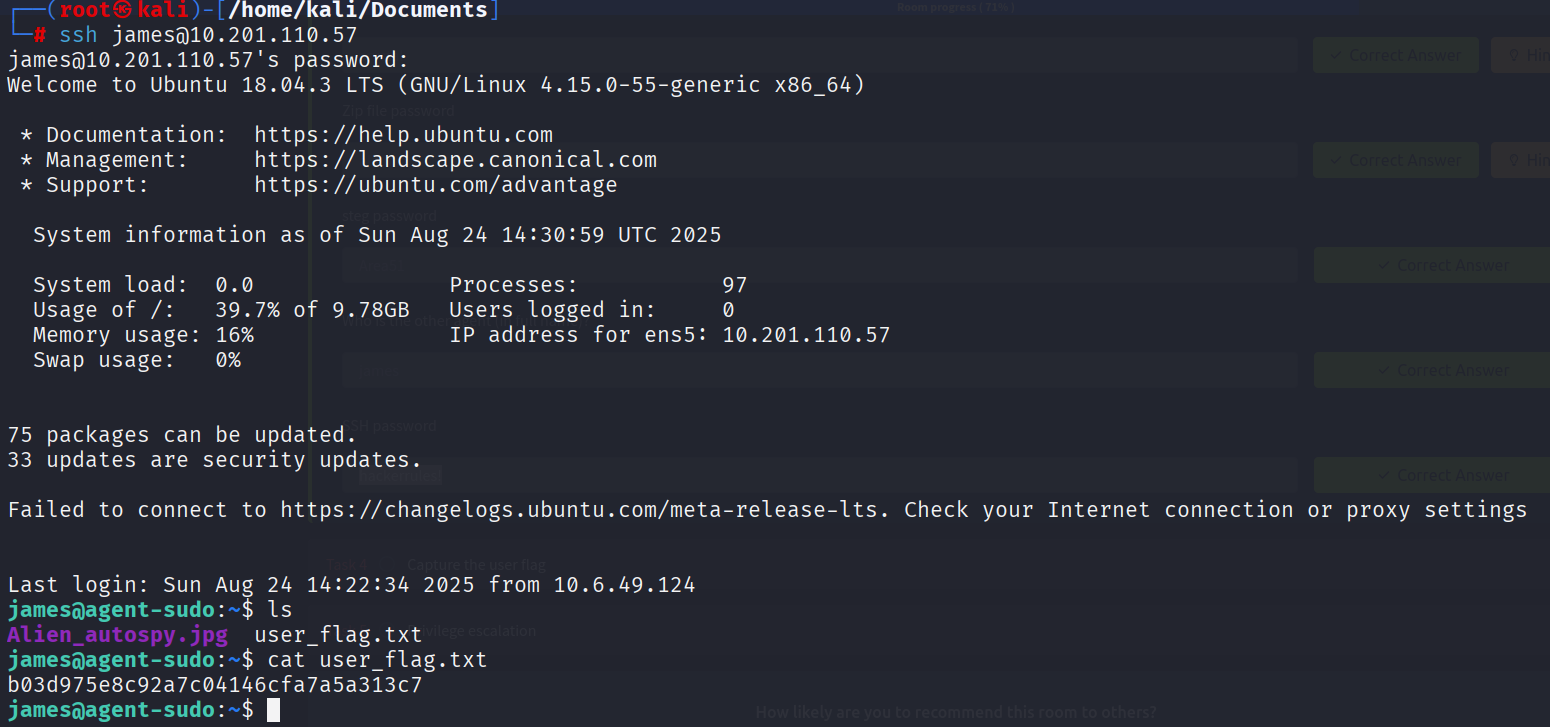
**Texto

O conteúdo gerado por IA pode estar incorreto.**

**What is the user flag?**

**Resposta: b03d975e8c92a7c04146cfa7a5a313c7**

Logo após fazermos o login no SSH do usuário james, encontramos a **user\_flag.txt**.



**What is the incident of the photo called?**

**Resposta: Roswell alien autopsy**

Junto com o arquivo da task anterior, há uma imagem que parece ser muito interessante.

Agora vamos sair do SSH e dar o seguinte comando:

**“scp james@10.201.97.102:/home/james/Alien\_autospy.jpg /home/kali/Documents/Alien\_autospy.jpg”.**

Esse comando copia a imagem do SSH para a nossa máquina local.

Tela de computador com fundo preto

O conteúdo gerado por IA pode estar incorreto.

Ao abrir a imagem, vemos um alien deitado em uma maca, possivelmente sendo examinado ou envolvido em algum tipo de procedimento.

Foto em preto e branco deitado de barriga para cima

O conteúdo gerado por IA pode estar incorreto.

Podemos usar o Google Imagens para procurar pistas ou a resposta da task.  
Após muita pesquisa em vários sites, encontrei exatamente a mesma imagem no site da Fox News:  
<https://www.foxnews.com/science/filmmaker-reveals-how-he-faked-infamous-roswell-alien-autopsy-footage-in-a-london-apartment>

Na manchete, podemos ver o nome do famoso caso: **“Roswell alien autopsy”**.

**CVE number for the escalation**

**Resposta: CVE-2019-14287**

A dica que recebemos já aponta que devemos procurar um **CVE relacionado a privilege escalation**.

Antes de iniciar a busca, é importante verificar a versão do **sudo** dentro do SSH, pois isso facilita a identificação da vulnerabilidade.

Texto

O conteúdo gerado por IA pode estar incorreto.

No SSH, utilizei o comando sudo -V para descobrir a versão instalada.  
Em seguida, pesquisei no Google por **“exploit sudo 1.8.21p2”**. Como não encontrei nada útil, continuei pesquisando no GitHub e acabei encontrando uma CVE de 2019 compatível com essa versão do sudo: **CVE-2019-14287**.

Depois disso, copiei o código do exploit, voltei para o SSH e criei um arquivo com extensão **.sh**.  
Colei o código dentro do arquivo, salvei e dei permissão de execução com:

**chmod 777 nome\_do\_arquivo.sh**

**./nome\_do\_arquivo.sh**

Texto

O conteúdo gerado por IA pode estar incorreto.

**What is the root flag?**

**Resposta: b53a02f55b57d4439e3341834d70c062**

Agora vamos para o diretório do root e pegamos a flag.

Texto

O conteúdo gerado por IA pode estar incorreto.

**(Bonus) Who is Agent R?**

**Resposta: Deskel**

Está dentro do root.txt.

**Conclusão**

O CTF **Agente Sudo** reforçou a importância de analisar serviços, explorar vulnerabilidades conhecidas e combinar diferentes técnicas. Foi uma ótima oportunidade para praticar enumeração, esteganografia, brute-force e escalonamento de privilégios de forma integrada.

**Referências**

OPENAI. ChatGPT. Disponível em: <https://chat.openai.com/>. Acesso em: 26 ago. 2025