Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

RootMe – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF de estudo – Isabela Tamie |
| **N° Revisão** | 1 |
| **Data de publicação** |  |
| **Link** | [RootMe](https://tryhackme.com/r/room/rrootme) |

|  |  |  |
| --- | --- | --- |
| **Redação** | Nome do realizador | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 03/09/2025 | Produção |
| **1** | 18/09/2025 | Revisão |

**Sumário**

[Contextualização](#_gjdgxs) [3](#_30j0zll)

[Desenvolvimento 3](#_1fob9te)

Escaneie a máquina, quantas portas estão abertas? [3](#_3znysh7)

Qual é o diretório oculto? [3](#_2et92p0)

Encontre um formulário para fazer upload e obter um shell reverso e encontre a bandeira. [4](#_tyjcwt)

Procure arquivos com permissão SUID, qual arquivo é estranho? [7](#_3dy6vkm)

[Conclusão 9](#_1t3h5sf)

[Referências 9](#_4d34og8)

**Contextualização**

A ctf for beginners, can you root me?

**Desenvolvimento**

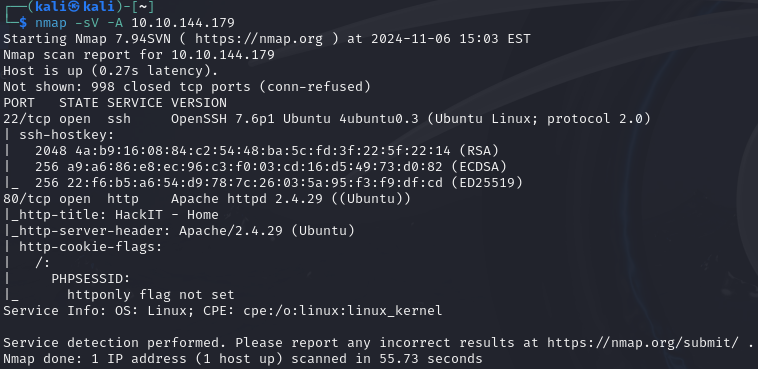
1. Escaneie a máquina, quantas portas estão abertas?

O primeiro passo é **enumerar** a máquina, ou seja, descobrir quais serviços estão rodando. Para isso, usamos o comando do **Nmap**

### **O que é Nmap?** Nmap é uma ferramenta de código aberto usada para explorar uma rede e realizar auditorias de segurança. Ele pode varrer portas e identificar serviços que estão rodando em um servidor.

**nmap -sV -A [endereço de IP]**

* **-sV**: Detecta a versão dos serviços que estão rodando nas portas abertas.
* **-A**: Habilita detecção do sistema operacional, versão dos serviços, e realiza outros testes avançados.



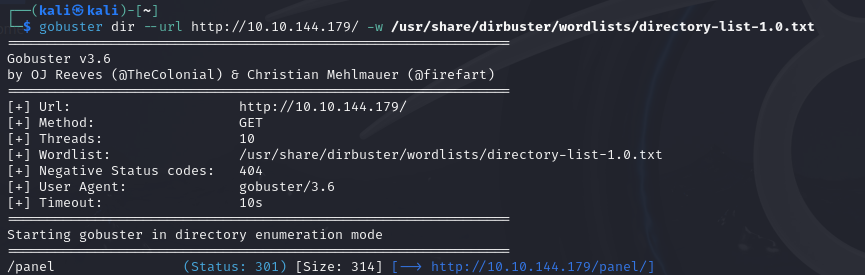
1. Qual é o diretório oculto?

### **O que é Gobuster?** Gobuster é uma ferramenta de brute-force usada para enumerar diretórios e arquivos em servidores web. Ela compara uma lista de possíveis diretórios com os disponíveis no servidor.

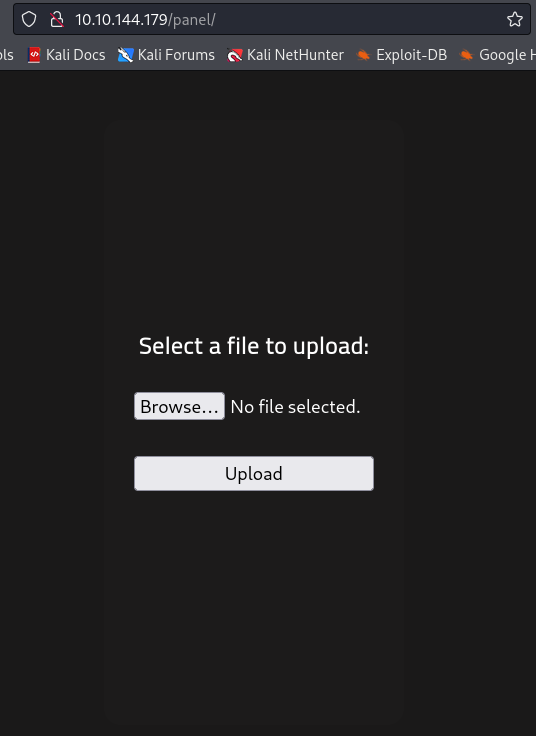
(Também é possível usar outras ferramentas, como próprio dirbuster, dirsearch, nikto, dirb, etc)

**gobuster dir --url [url] -w [diretório onde está a lista]**

* **dir**: Informa que estamos buscando por diretórios.
* **--url**: Especifica a URL do servidor.
* **-w**: Define a lista de palavras que será usada para testar nomes de diretórios.



O diretório oculto é /panel/

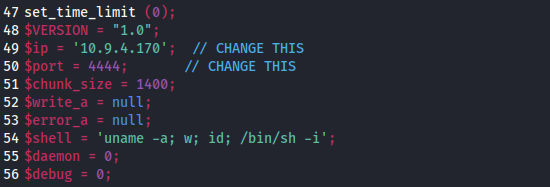


1. Encontre um formulário para fazer upload e obter um shell reverso e encontre a bandeira.

### **O que é um shell reverso?**

Um shell reverso (ou **reverse shell**) é uma técnica usada em redes e segurança de computadores, onde um sistema remoto (normalmente uma máquina atacante) consegue obter acesso a uma máquina vítima. Ao contrário de uma shell normal, onde o atacante tenta se conectar a um computador vulnerável, o shell reverso inverte esse fluxo de comunicação, ou seja, a máquina comprometida se conecta ao atacante, permitindo-lhe executar comandos e obter controle remoto da máquina.

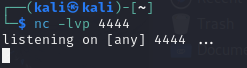
Buscamos um reverse shell em php, baixei um [aqui](https://github.com/pentestmonkey/php-reverse-shell) e editei o endereço IP do arquivo para o de minha máquina. Também editei a porta para 4444, mas fica à sua escolha.



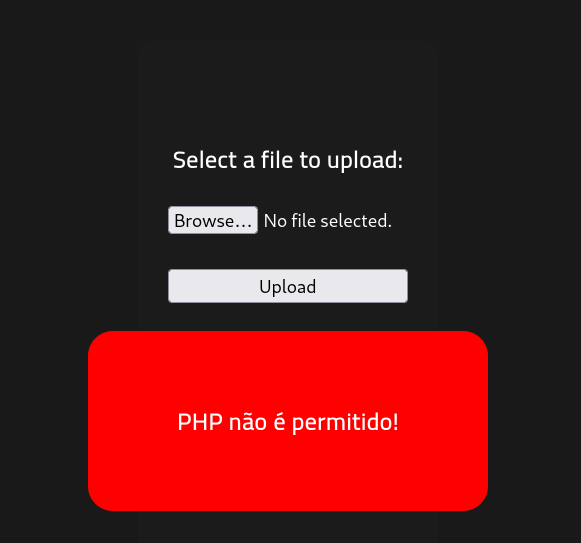
Use o **Netcat** para escutar a porta escolhida:

**nc -lvp [porta escolhida]**

* **nc**: Abreviação de Netcat, a ferramenta em si.
* **-l**: Entra no modo *listen*, onde o Netcat "escuta" conexões que chegam na porta especificada, em vez de iniciar uma conexão de saída.
* **-v**: Ativa o modo *verbose* (detalhado), exibindo mais informações sobre a conexão, o que ajuda a entender melhor o que está acontecendo.
* **-p [porta escolhida]**: Especifica a porta para a qual o Netcat deve escutar.



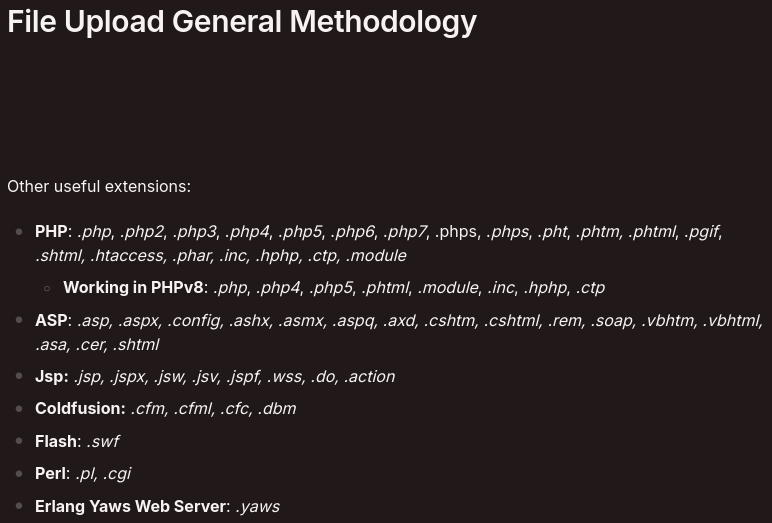
Faço o upload no servidor web mas…



Buscamos então por um file upload bypass:

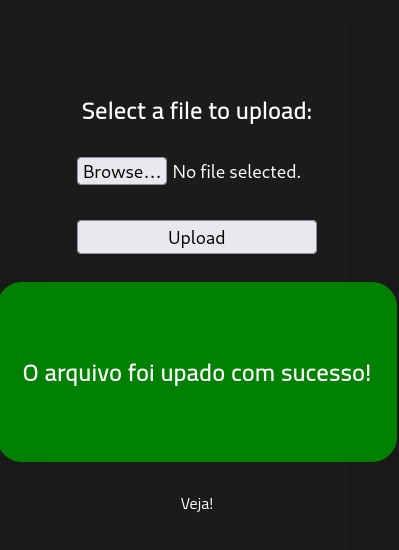
O *file upload bypass* (ou *bypass de upload de arquivos*) é uma técnica usada em ataques de segurança cibernética para contornar restrições de upload de arquivos em aplicações web. Em muitos sistemas, há controles para impedir que arquivos maliciosos, como scripts executáveis ou arquivos de configuração, sejam enviados e executados. Contudo, um atacante pode tentar contornar esses controles para fazer o upload de arquivos potencialmente prejudiciais que poderiam comprometer o servidor.

Encontrei este [site](https://book.hacktricks.xyz/pentesting-web/file-upload#file-upload-general-methodology) que dá algumas opções.



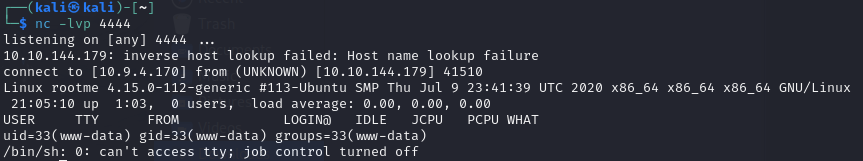
Altere o nome do arquivo para alguma dessas extensões (de PHP). Testei algumas e o que funcionou para mim foi o .php5;

Faça upload do arquivo e…



Clique em “Veja!”.

E então...



E temos acesso à máquina graças ao script do reverse shell.

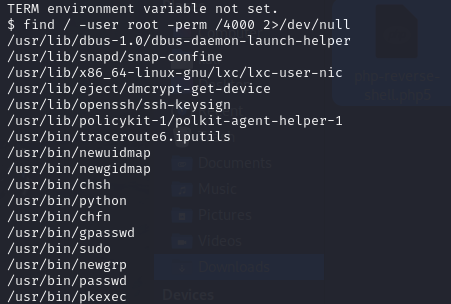
Procurando um pouco (ou rodando o comando **find / -name user.txt 2>/dev/null**) encontramos a flag.



1. Procure arquivos com permissão SUID, qual arquivo é estranho?

**find / -user root -perm /4000 2>/dev/null**

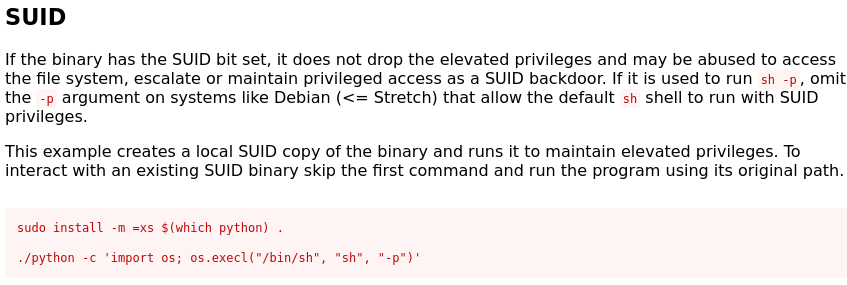
* **find /**: Isso indica que a busca começa na raiz do sistema (/), ou seja, o comando irá procurar por arquivos em todo o sistema de arquivos.
* **-user root**: Este filtro limita a busca a arquivos que pertencem ao usuário root.
* **-perm /4000**: Aqui, o comando busca arquivos com o bit **setuid** ativado, ou seja, arquivos executáveis que, quando executados, assumem as permissões do usuário root.
* **2>/dev/null**: Esta parte do comando é responsável por redirecionar as mensagens de erro para o "buraco negro" /dev/null, que descarta qualquer saída de erro.
  + O 2> é a maneira de redirecionar a **saída de erro padrão** (stderr).
  + O /dev/null é um dispositivo especial que descarta qualquer coisa enviada a ele. Portanto, qualquer erro (como "permissão negada" ou "acesso proibido") que normalmente seria exibido no terminal será ignorado.

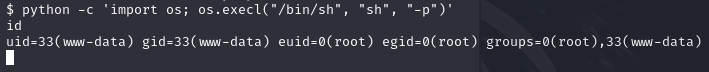


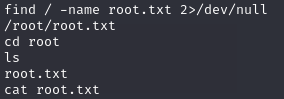
O arquivo “estranho” seria o /usr/bin/python pois, se o arquivo **/usr/bin/python** tiver a permissão SUID, pode ser possível explorá-lo para escalar privilégios. Por exemplo, no [GTFOBins](https://gtfobins.github.io/gtfobins/env/), há maneiras documentadas de usar o **python** para executar comandos arbitrários e obter uma shell privilegiada.

### **O que é o GTFOBins?** O GTFOBins é um repositório que documenta como binários comuns no sistema podem ser usados para escapar de ambientes restritos, executar comandos arbitrários e escalar privilégios. Cada entrada no GTFOBins mostra como esses binários podem ser usados de maneiras criativas para ganhar privilégios administrativos.

Vamos dar uma olhada em como isso funciona:







**Conclusão**

Considerações finais a respeito do CTF.

**Referências**

<https://youtu.be/fYUvIyjgs4Y?si=AayprDAR037-cc9v>