Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Mr Robot – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Mr Robot – Isabella Passarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 30/10/2025 |
| **Link** | [https://tryhackme.com/room/mrrobot#](https://tryhackme.com/room/mrrobot) |

|  |  |  |
| --- | --- | --- |
| **Redação** | Isabella Passarelli | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 17/09/2025 | Produção |
| **1** | 30/10/2025 | Revisão |
| **2** | 30/10/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | searchsploit, john, SUID |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

Contextualização 3

Desenvolvimento 3

What is key 1? 3

What is key 2? 4

What is key 3? 8

Conclusão 9

Referências 9

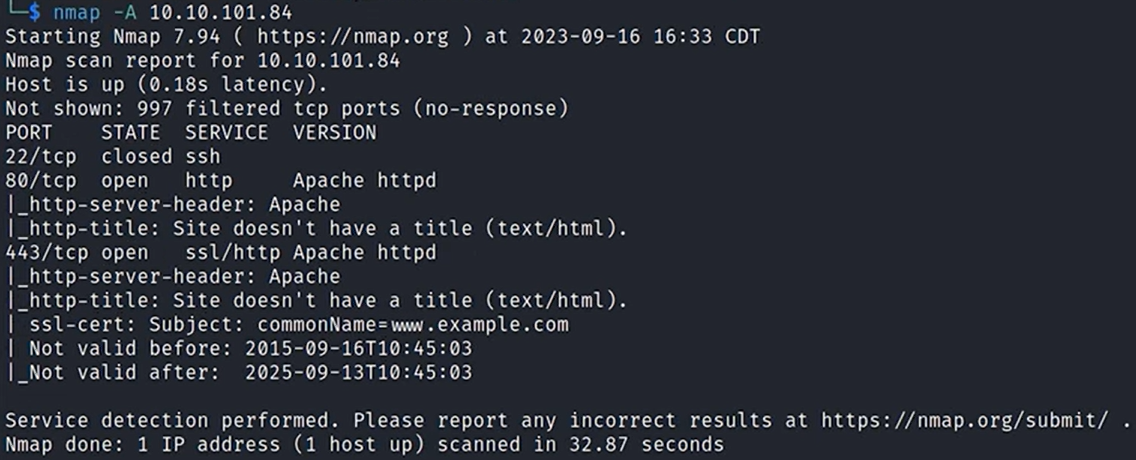
**Contextualização**

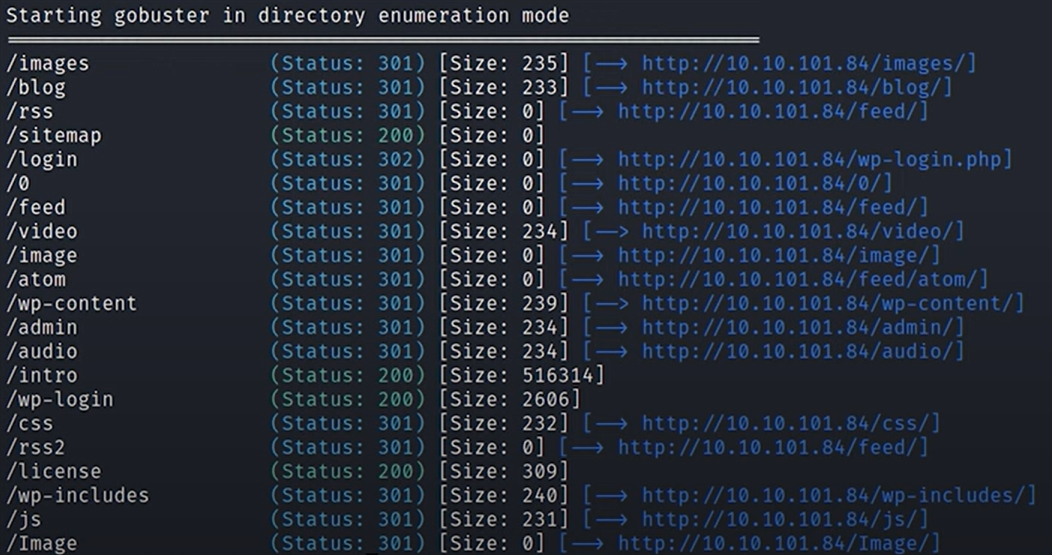
O CTF aborda assuntos sobre escaneamento de portas e serviços, enumeração de diretórios, escalonamento de privilégios e exploração web, ferramentas essenciais para a solução de um CTF.

**Desenvolvimento**

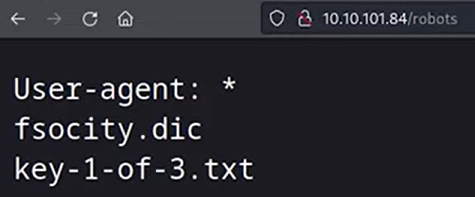
**Pergunta 1 - What is key 1?**

Inicialmente foi utilizado o comando **nmap -A <IP>** para verificar se existe um servidor web.



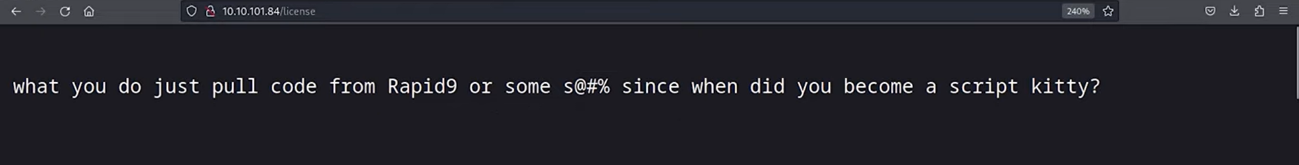
Em seguida foi utilizado o comando **gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt** para enumerar os diversos diretórios que existe no site.

Dentre os diretórios encontrados foi utilizado o diretório **/robots**. Acessando esse diretório encontramos o arquivo **key-1-of-3.txt** que ao acessarmos encontramos a primeira flag.

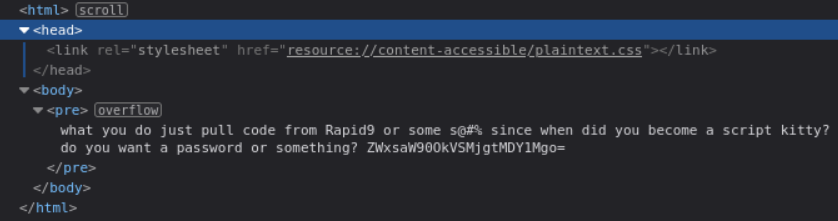


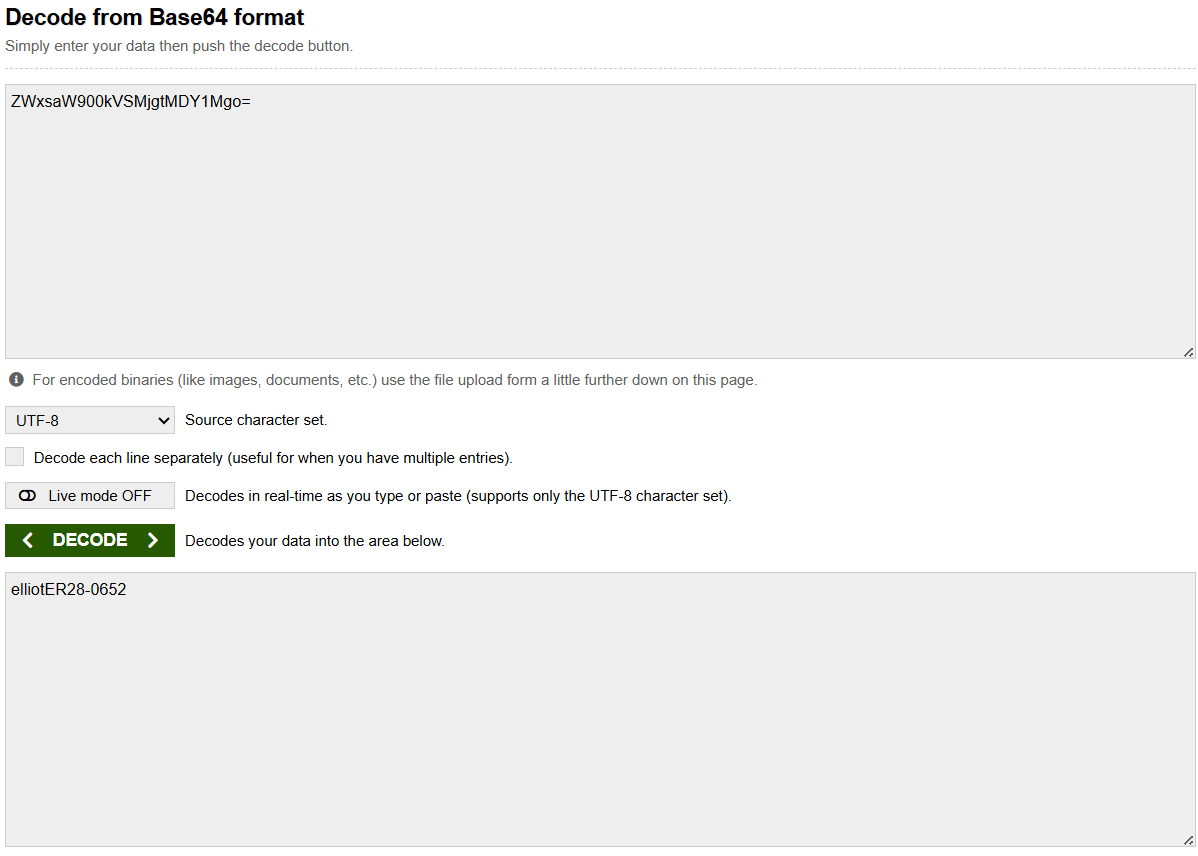
**Pergunta 2 - What is key 2?**

O próximo passo foi acessar o diretório **/license**. Ao acessar, encontramos a frase “what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?”.

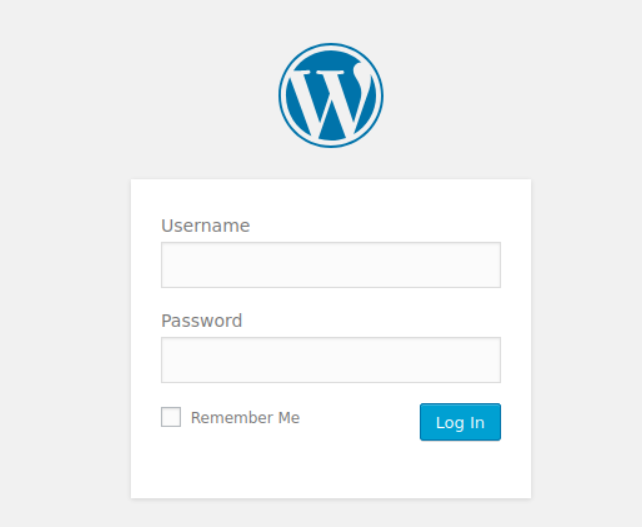


Em seguida inspecionamos a página e encontramos a informação **ZWxsaW900kVSMjgtMDY1Mgo=** criptogafada. Utilizando o site base64 para discriptografar a informação, foi possivel encontrar **elliot:ER28-0652**, um possível usuário e senha de algum login.

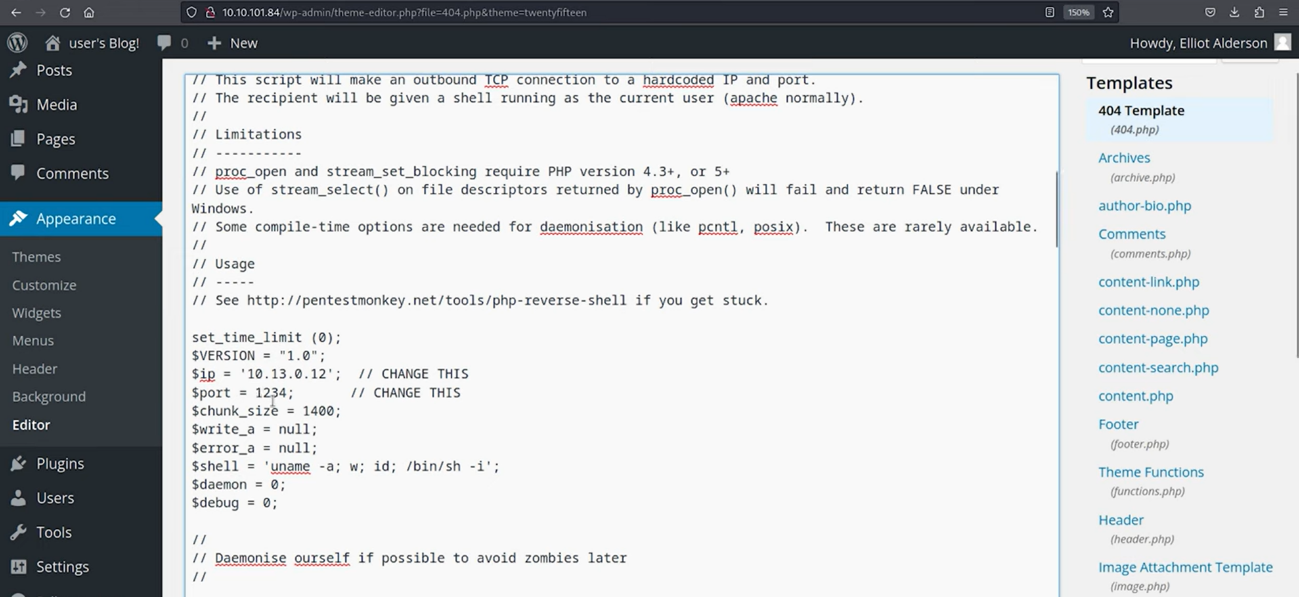
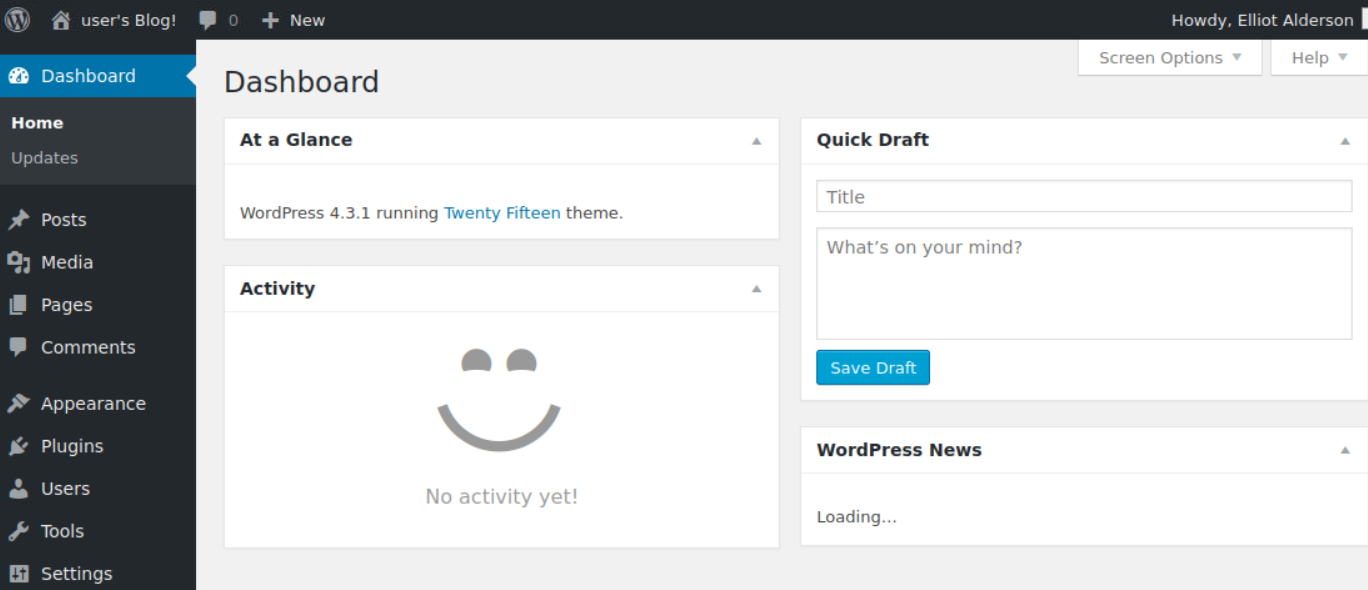




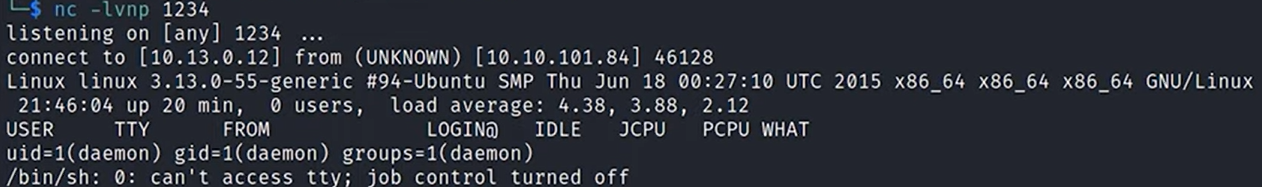
Ao entrar no diretório **wp-login.php**, somos direcionados para uma página de login de um wordpress. Com a informação encontrada anteriormente, podemos realizar o login da página.



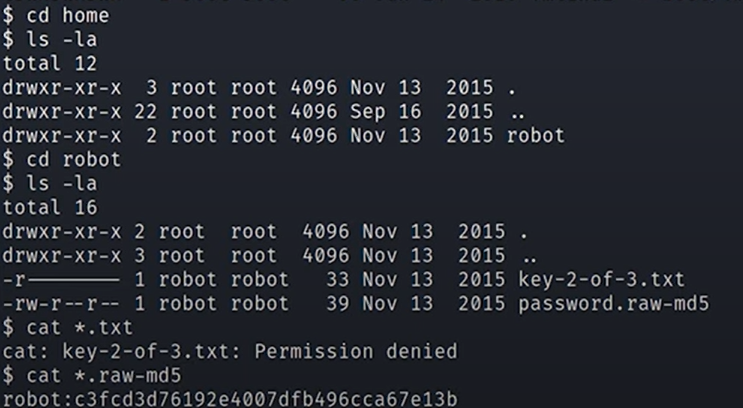
Em seguida, ao entrar em appearance, depois em editor e por último, em template 404.php, podemos ter acesso ao código. Utilizando o site pentestmonkey podemos colar uma reverse shell dentro do código e alteramos o IP e a porta que será utilizada.

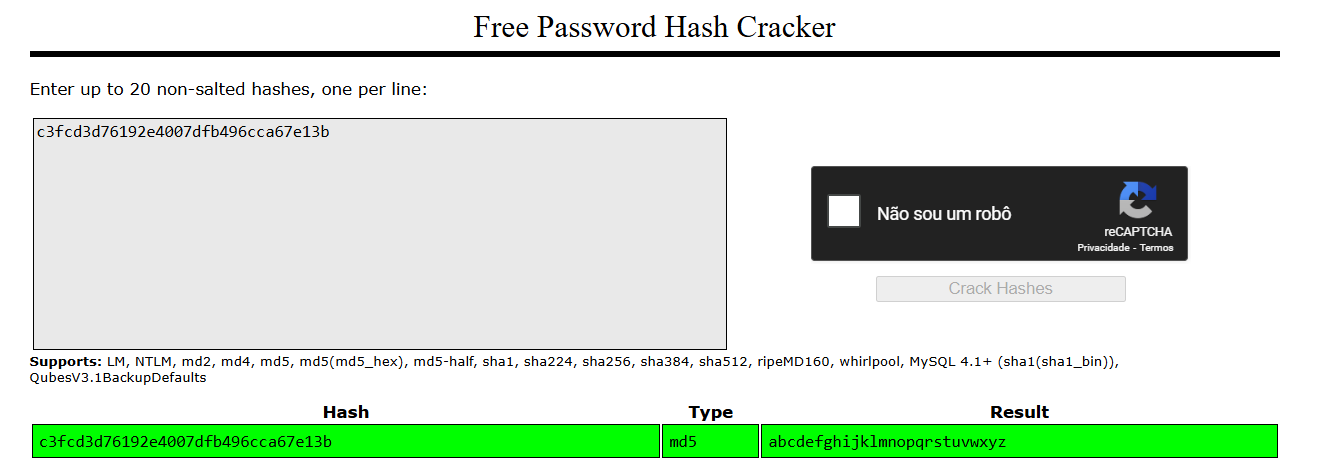


Antes de disparar a requisição rodamos o comando **nc –lvnp 1234**. Quando o servidor remoto executar o reverse shell, a conexão chega no nc e obtém uma shell remota interativa.

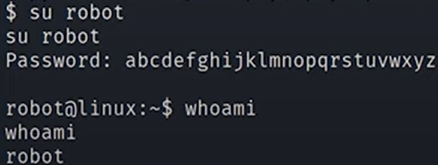


Em seguida entramos em robot e listamos todos os diretórios. Ao rodar o comando encontramos o conteúdo password.raw-md5 e ao tentar acessá-lo obtemos um hash.

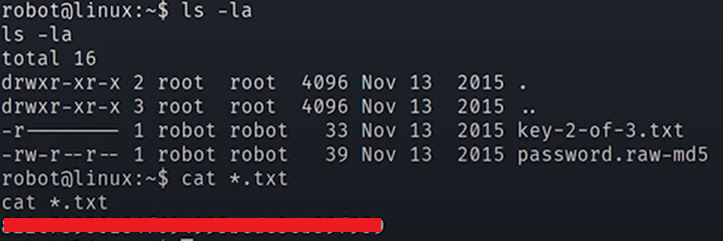


Para descobrir a senha correspondente, colocamos esse hash em um serviço de quebra de hashes como o site *CrackStation* e obtemos a senha. 

Com a senha obtida é possível mudar para o usuário robot no sistema.

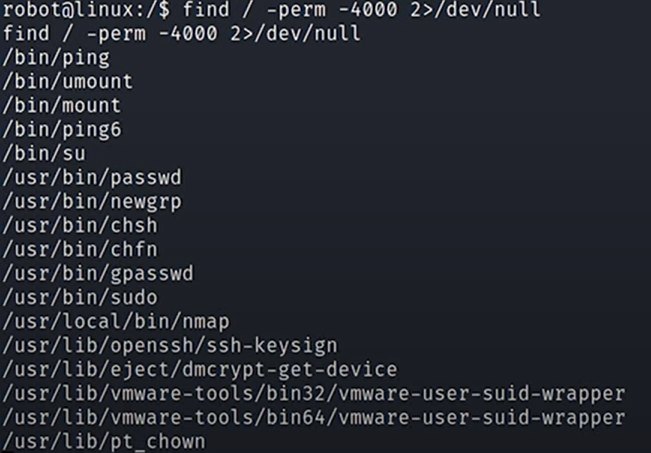


Em seguida listamos os diretórios e encontramos o arquivo key-2-of-3.txt que ao acessarmos encontramos a segunda flag.



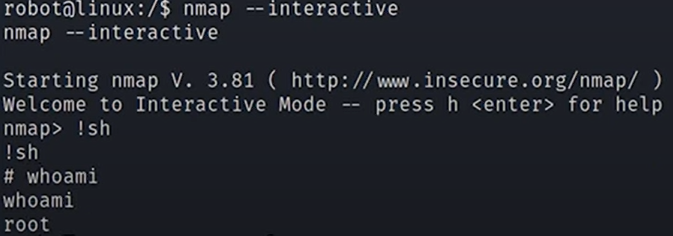
**Pergunta 3 - What is key 3?**

Com o comando **find / -perm +6000 2>/dev/null | grep '/bin/'** procuramos por binaries com permissões SUID em todo o sistema.

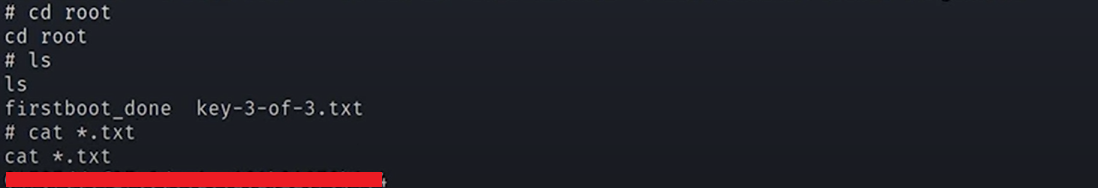


Ao entrar no site *GTFOBins* e pesquisar por nmap, consultamos um repositório que documenta métodos conhecidos para escalar privilégios usando programas que possuem funcionalidades interativas.

Executando o comando **nmap --interactive** é possível iniciar o modo interativo do nmap e logo em seguida com o comando **!sh** é possível acionar o escape documentado, fazendo com que o nmap execute um shell do sistema.



Em seguida listamos os diretórios de root e encontramos o arquivo key-3-of-3.txt que ao acessarmos encontramos a última flag do CTF.



**Conclusão**

O CTF no geral apresentou um nível de dificuldade média, pois trata de conceitos básicos e inclui alguns desafios que precisam um pouco mais de prática.

**Referências**

* BASE64 DECODE AND ENCODE. **Base64 Decode and Encode - Online.** Disponível em: <https://www.base64decode.org/>. Acesso em: 17 set. 2025.
* REVSHELLS. **Revshells**. Disponível em: <https://www.revshells.com/>. Acesso em: 17 set. 2025.
* GTFOBins. **GTFOBins**. Disponível em: <https://gtfobins.github.io/>. Acesso em: 17 set. 2025.
* CRACKSTATION. **CrackStation**. Disponível em: <https://crackstation.net/>. Acesso em: 17 set. 2025.