Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Anonymous – TryHackMe

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

| **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** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Enumeration, FTP, SMB, Reverse Shell, SUID |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[**Contextualização 3**](#_1crp6xmi3zw2)

[**Desenvolvimento 3**](#_hfu1kh836b4m)

[Enumerate the machine. How many ports are open? 3](#_gvxsdft5bi3z)

[What service is running on port 21? 4](#_sppeistm9yhp)

[What service is running on ports 139 and 445? 4](#_nta2smlo04sg)

[There’s a share on the user’s computer. What 's it called? 4](#_z0mbu080aedv)

[user.txt 5](#_z0mbu080aedv)

[root.txt 7](#_z0mbu080aedv)

[**Conclusão 8**](#_83i3wttott0d)

[**Referências**](#_hf6yq38ukzpk) 8

# Contextualização

O CTF “Anonymous” de nível médio aborda conceitos como enumeração de portas, acesso de serviços, como FTP e SMB, utilizando anonymous login, reverse shell e utilização de binários SUID para realizar o escalonamento de privilégios.

# Desenvolvimento

## Enumerate the machine. How many ports are open?

Ao realizar a enumeração de portas utilizando o nmap, obtemos quatro portas abertas:



## What service is running on port 21?

Além de ser uma convenção, é possível visualizar que o protocolo ftp está rodando na porta 21 e que é possível realizar anonymous login.

## What service is running on ports 139 and 445?

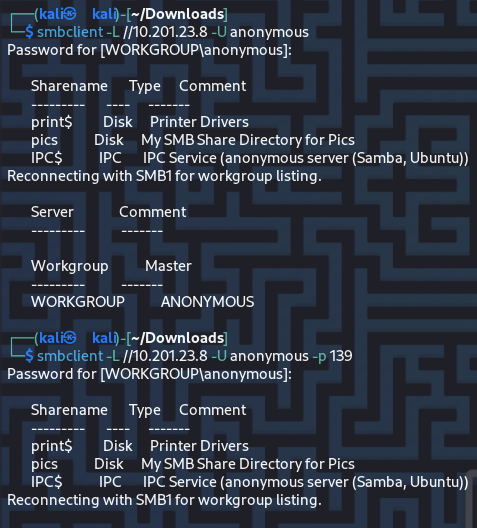
Ao realizar um reconhecimento mais profundo, com o parâmetro -A no nmap, nessas duas portas, obtém-se que ambas as portas estão rodando Server Message Block (SMB), protocolo de rede, que opera no modelo cliente-servidor, utilizado para compartilhar e acessar arquivos, diretórios e outros recursos como impressoras e roteadores. A porta padrão antiga era 139 e a 445 e a porta padrão atual.





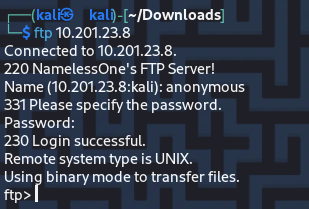
## There’s a share on the user’s computer. What 's it called?

Outra informação obtida durante o reconhecimento é a possibilidade de realizar anonymous login no smb. Assim, utilizando o comando “smbclient”, especificando IP e o usuário como anonymous e, em uma segunda tentativa para confirmar a resposta, especificando a porta 139, obtém-se a pasta compartilhada: pics.

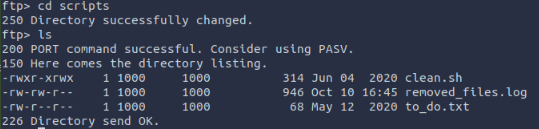


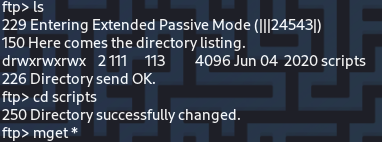
## user.txt

Como dito anteriormente, é possível realizar anonymous login no ftp.

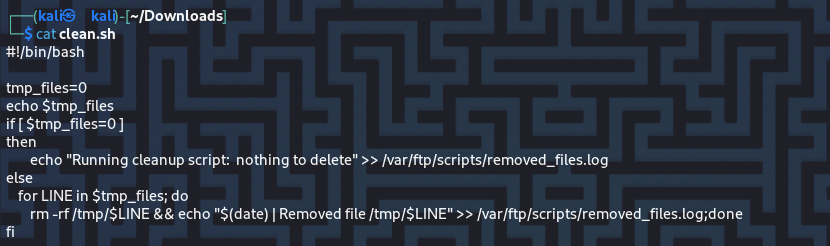


Existe o diretório “script”, dentro do diretório há os arquivos clean.sh, removed\_files.log e to\_do.txt.

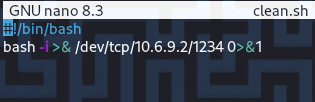




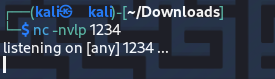
Analisando o conteúdo do script, o shebang (primeira linha) indica que o script é executado no bash. Assim, é possível substituir o script original por um reverse shell e utilizar o ftp para substituí-lo no diretório.



Alterando o conteúdo do script com a reverse shell:



Utilizando o netcat para “ouvir” conexões:



Substituindo o script original:



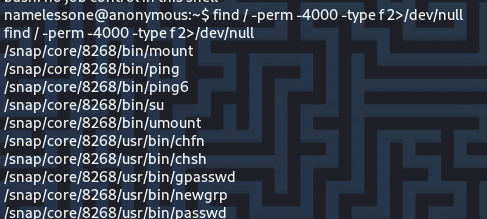
Após algum tempo, obtém-se a reverse shell na máquina da vítima.

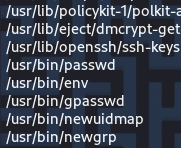


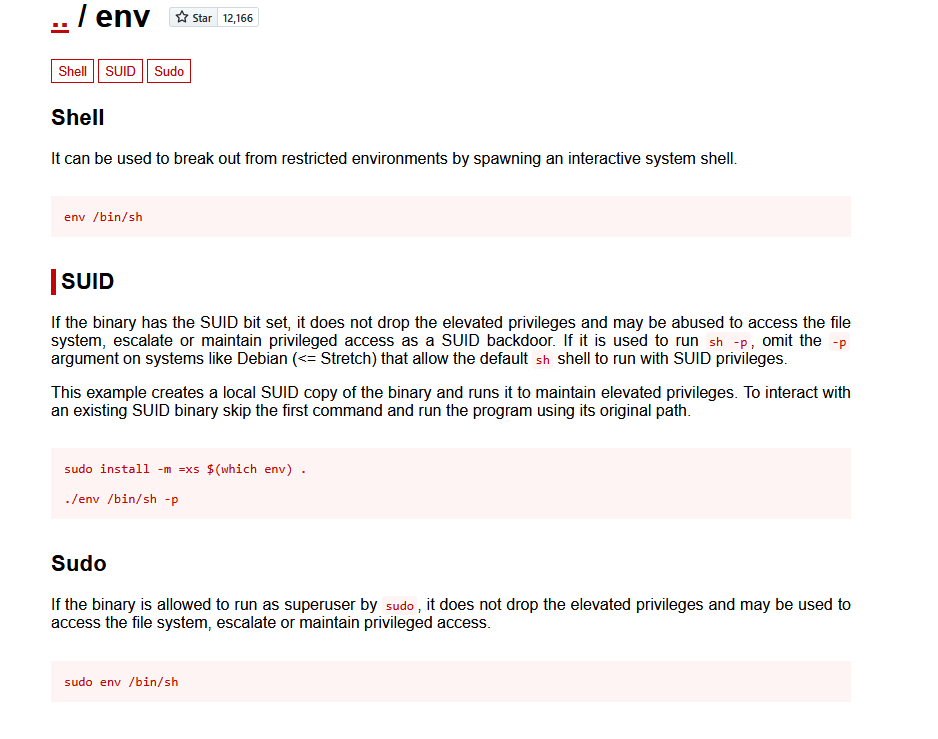


## root.txt

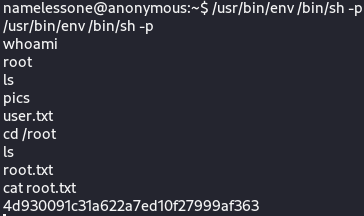
Para obter o usuário root, é preciso verificar quais binários possuem a permissão SUID, ou seja, são executados com os privilégios do dono do arquivo, e não do usuário que está executando. Um desses binários é o “env”.

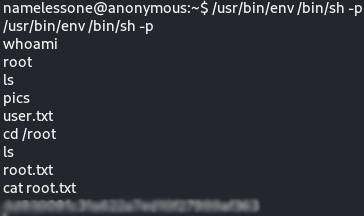






Utilizando o comando disponível no GTFOBins, mas alterando o caminho do binário, é possível escalar o privilégio até o root e, consequentemente, obter a última flag.





# Conclusão

Através do CTF, aprende-se que a possibilidade de realizar login anônimo em serviços e de execução de binários com permissões inadequadas tornam a máquina altamente vulnerável e exposta contra atacantes.

# Referências

<https://book.hacktricks.wiki/en/network-services-pentesting/pentesting-smb/index.html>

<https://gtfobins.github.io/>

https://www.revshells.com/