Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Basic Pentesting – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Basic Pentesting – Isabella Passarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 02/10/2025 |
| **Link** | <https://tryhackme.com/room/basicpentestingjt> |

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

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 09/09/2025 | Produção |
| **1** | 02/10/2025 | Revisão |
| **2** | 02/10/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | SMB, hydra, SUID |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

Contextualização 3

Desenvolvimento 3

Pergunta 1 - What is the name of the hidden directory on the web server(enter name without /)? 3

Pergunta 2 - What is the username? 3

Pergunta 3 - What is the password? 4

Pergunta 4 - What service do you use to access the server(answer in abbreviation in all caps)? 4

Pergunta 5 - What is the name of the other user you found(all lower case)? 5

Pergunta 6 - What is the final password you obtain? 5

Conclusão 8

Referências 8

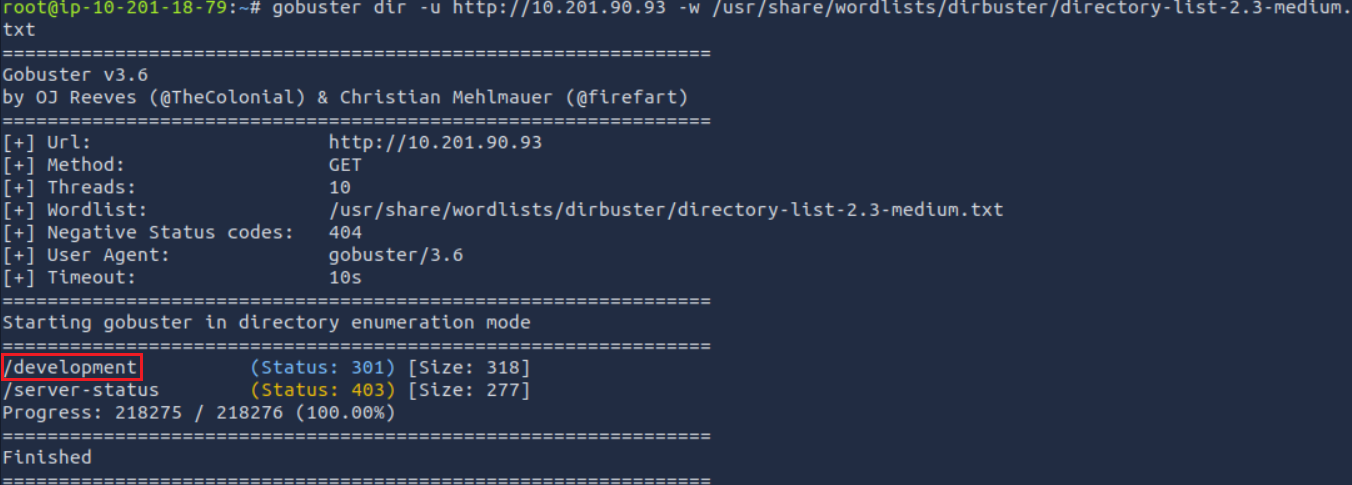
**Contextualização**

O CTF aborda assuntos sobre conceitos básicos como criptografia básica, privilege escalation e enumeração mostrando como aplicar na prática essas ferramentas essenciais para a solução de um CTF.

**Desenvolvimento**

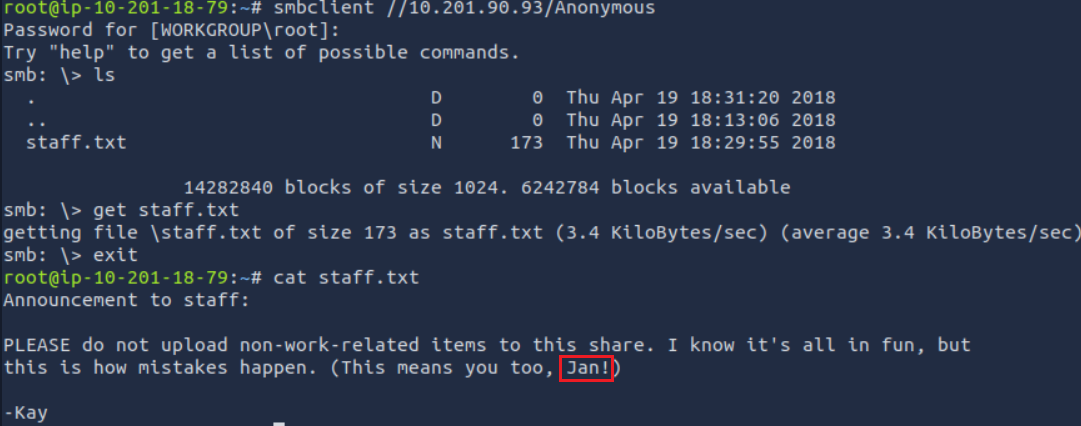
**Pergunta 1 - What is the name of the hidden directory on the web server (enter name without /)?**

Para resolver foi utilizado o comando **gobuster dir -u http://10.201.90.93 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt** para encontrar o diretório oculto. Ao testar uma lista de palavras contra o servidor, foi revelado o diretório que estava escondido.



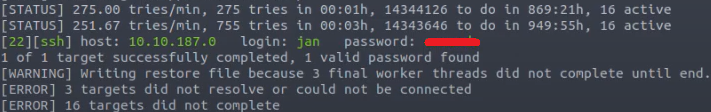
**Pergunta 2 - What is the username?**

Para descobrir o nome do usuário, inicialmente foi utilizado a ferramenta **enum4linux**. O objetivo desse comando é enumerar informações sobre o sistema, como usuários, grupos e compartilhamentos SMB. Ao realizar a enumeração, foi identificado um compartilhamento de nome "Anonymous" do tipo "Disk". A partir daí, a próxima ação foi usar o comando **smbclient** para se conectar a esse compartilhamento. Após a conexão, o comando **ls** foi executado para listar o conteúdo do diretório, e o arquivo "staff.txt" foi encontrado. O arquivo foi então baixado para a máquina local usando o comando **get staff.txt**. Por fim, ao visualizar o conteúdo do arquivo com o comando **cat staff.txt**, foram encontrados dois usuários: Jan e Kay.



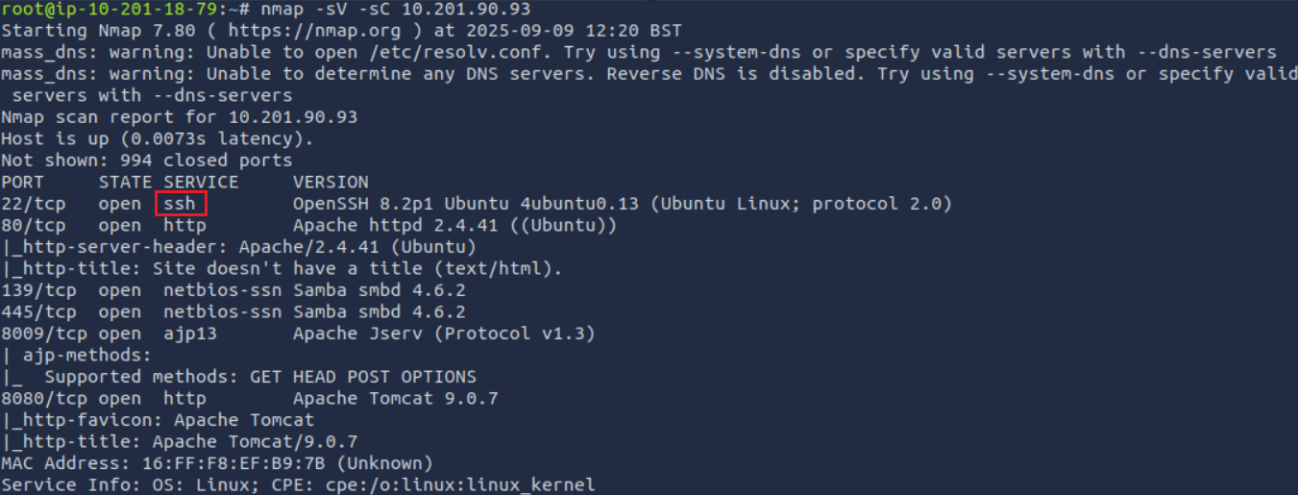
**Pergunta 3 - What is the password?**

Sabendo que o nome do usuário é Jan, para descobrir a senha foi utilizado o comando **hydra -l jan -P /usr/share/wordlists/rockyou.txt 10.10.187.0**.



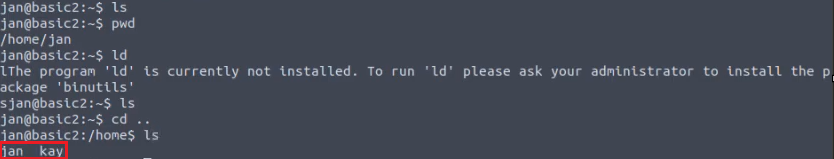
**Pergunta 4 - What service do you use to access the server (answer in abbreviation in all caps)?**

Para identificar o serviço usado para acessar o servidor, foi utilizado o comando **nmap -sV -sC 10.201.90.93**. A análise do resultado do Nmap revelou que a porta 22 estava aberta e o serviço associado era o SSH.



**Pergunta 5 - What is the name of the other user you found (all lower case)?**

Para descobrir o nome do outro usuário encontrado, foi necessário acessar o servidor com o comando **ssh jan@10.201.90.93** e a senha que foi encontrada anteriormente. Após a conexão com o sistema, foi utilizado o comando **pwd** para mostrar o caminho completo do diretório, em seguida o comando **cd ..** foi utilizado para voltar para o diretório /home. Ao executar **ls** nesse novo diretório, foram listados os diretórios dos usuários do sistema: Jan e Kay**,** onde é possível encontrar o outro usuário.



**Pergunta 6 - What is the final password you obtain?**

A tentativa inicial de acessar o arquivo pass.bak no diretório /home/kay falhou devido a permissões. Isso direcionou a busca para uma exploração mais profunda, focando no diretório .ssh de Kay. Lá, foram encontrados os arquivos id\_rsa e id\_rsa.pub, que são chaves SSH.

A chave privada, id\_rsa, foi copiada para a máquina do atacante. Em seguida, foi utilizado o **ssh2john.py**, um script que converte a chave privada SSH em um formato de hash compatível com a ferramenta de cracking de senhas John the Ripper. Com o comando **john id\_rsa.hash --wordlist=/usr/share/wordlists/rockyou.txt**, foi possível encontrar a senha da chave SSH.

Por fim, com a senha da chave SSH foi possível realizar o acesso com o comando **ssh -i id\_rsa kay@10.201.90.93**, usando a chave e a senha descobertas. Uma vez logado como **Kay**, o comando **cat pass.bak** foi executado com sucesso, revelando a senha final.

Texto

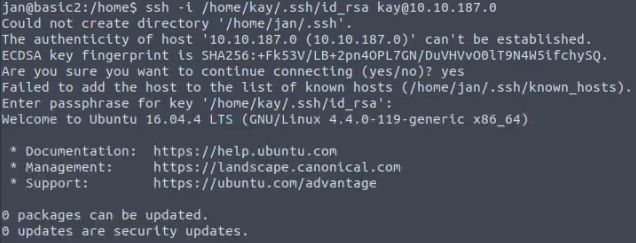
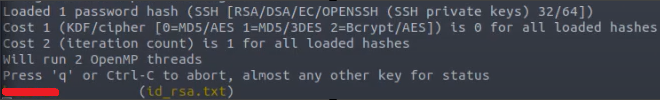
O conteúdo gerado por IA pode estar incorreto.

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.Texto

O conteúdo gerado por IA pode estar incorreto.Texto

O conteúdo gerado por IA pode estar incorreto.



**Conclusão**

O CTF no geral apresentou um nível de dificuldade fácil e é ótimo para treinar ferramentas básicas para a resolução de desafios.

**Referências**

* HACKTRICKS. **Linux Privilege Escalation Checklist**. Disponível em: [https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist](https://www.google.com/search?q=https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist). Acesso em: 9 set. 2025.
* JOHN THE RIPPER documentation. Openwall. Disponível em: <https://www.openwall.com/john/doc/>. Acesso em: 9 set. 2025.