Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Cowboyhacker – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Cowboyhacker – Sérgio Guidi Trovo |
| **N° Revisão** | 1 |
| **Data de publicação** | 22/08/2024 |
| **Link** | https://tryhackme.com/room/cowboyhacker |

|  |  |  |
| --- | --- | --- |
| **Redação** | Sérgio Guidi Trovo | Estudante |
| **Revisão** | João Branco | Presidente |
| **Aprovação** | João Branco | Presidente |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 22/08/2024 | Produção |
| **1** | 25/08/2024 | Revisão |
| **2** | 25/08/2024 | Aprovação |

Sumário

[Contextualização 3](#_Toc174364849)

[Desenvolvimento 3](#_Toc174364850)

[Pergunta 1 - Find open ports on the machine 3](#_Toc174364851)

[Pergunta 2 - Who wrote the task list? 3](#_Toc174364852)

[Pergunta 3 - What service can you bruteforce with the text file found? 5](#_Toc174364853)

[Pergunta 4 - What is the users password? 5](#_Toc174364854)

[Pergunta 4 - user.txt 6](#_Toc174364855)

[Pergunta 5 - root.txt 6](#_Toc174364856)

[Conclusão 7](#_Toc174364857)

[Referências 7](#_Toc174364858)

Contextualização

O CTF *Cowboy Hacker* foi introduzido na capacitação da entidade na aula 6 de PrivEsc 1. Este CTF tem dificuldade fácil.

Desenvolvimento

Pergunta 1 - Find open ports on the machine

Realizando um *nmap* para encontrar as portas abertas:

Texto

Descrição gerada automaticamente

Pergunta 2 - Who wrote the task list?

Verificando o conteúdo da página web:

Tela de celular com publicação numa rede social

Descrição gerada automaticamente com confiança média

Utilizando o login FTP anônimo:

Texto

Descrição gerada automaticamente

Utilizando o comando *ls* para listar os diretórios:

Texto

Descrição gerada automaticamente

Utilizando o comando *get* para fazer download das files encontradas na própria máquina:

Texto

Descrição gerada automaticamente

Verificando o conteúdo das files encontradas:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

O escritor da lista *task* foi o usuário “lin”.

Pergunta 3 - What service can you bruteforce with the text file found?

O serviço possível de bruteforce é o ssh na porta 22.

Pergunta 4 - What is the users password?

Utilizando o comando *hydra* para penetrar a máquina utilizando a lista de senhas encontradas anteriormente na file *locks.txt* e o nome de usuário lin.

Texto

Descrição gerada automaticamente

Senha para o login lin: RedDr4gonSynd1cat3

Pergunta 4 - user.txt

Utilizando os dados encontrados para acessar o servidor via ssh:

Texto

Descrição gerada automaticamente

Verificando as files e diretórios presentes:



Utilizando o comando *cat* para acessar o conteúdo da file user.txt:



Pergunta 5 - root.txt

Verificando os comandos executáveis com sudo:

Texto

Descrição gerada automaticamente

Verificando o comando *tar* no site gtfobins:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Utilizando o comando encontrado para ganhar acesso ao diretório root:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Conclusão

O CTF Cowboy Hacking é um CTF simples e muito bom para aprender os conceitos básicos de *pentesting*.

Referências

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

<https://book.hacktricks.xyz/>