Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

CyberLens – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CyberLenz – João Branco |
| **N° Revisão** | 1 |
| **Data de publicação** | DD/MM/AAAA |
| **Link** | https://tryhackme.com/r/room/cyberlensp6 |

|  |  |  |
| --- | --- | --- |
| **Redação** | João Branco | Presidente |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 07/09/2024 | João Branco |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

# Sumário

[Contextualização 3](#_Toc176618934)

[Desenvolvimento 3](#_Toc176618935)

[What is the user flag? 3](#_Toc176618936)

[What is the admin flag? 6](#_Toc176618937)

[Conclusão 7](#_Toc176618938)

[Referências 8](#_Toc176618939)

# Contextualização

Este CTF de nível fácil no TryHackMe apresenta um contexto de um site que extrai informações de arquivos. Neste ambiente, de servidor Windows, foi obtido duas flags no sistema. É necessário conhecimento de busca por vulnerabilidades, e Windows Privilege Escalation.

# Desenvolvimento

## What is the user flag?

Inicialmente, vale ressaltar a observação do enunciado: deve-se associar o domínio *cyberlens.thm* ao IP da máquina no arquivo */etc/hosts.*

Realizando um Port Scanning nas portas mais comuns, tem-se:  
Texto

Descrição gerada automaticamente

Verificando a página web, tem-se:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Ao analisar o código fonte, tem-se:

Texto

Descrição gerada automaticamente

Verificando que existe uma outra porta aberta (61777), é possível enumerá-la:

Texto

Descrição gerada automaticamente

Ao analisar tal diretório, tem-se:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

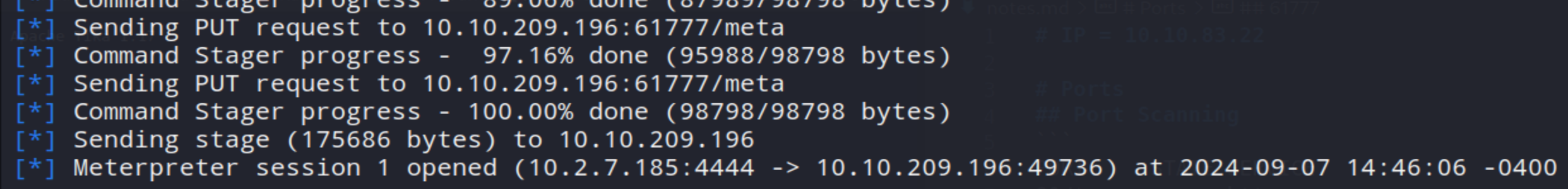
Ao procurar tal versão no *msfconsole*, tem-se:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Utilizando tal módulo, e configurando as opções, tem-se:

Texto

Descrição gerada automaticamente 

Entrando no diretório */Desktop* do nosso usuário, tem-se a primeira flag

Texto

Descrição gerada automaticamente

## What is the admin flag?

Após isso, é possível utilizar o módulo post/multi/recon/local\_exploit\_suggester dentro do *Meterpreter* para buscar vulnerabilidades:

Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente

Procurando pelo primeiro exploit apresentado, tem-se:

Texto

Descrição gerada automaticamente

Ao configurá-lo e rodá-lo, tem-se acesso à *NT AUTHORITY*:

Texto

Descrição gerada automaticamente

Por fim, no diretório *Desktop* do usuário *Administrator* tem a última flag:  
Texto

Descrição gerada automaticamente

# Conclusão

A exploração da máquina virtual permitiu aplicar técnicas fundamentais de pentesting, como exploração de vulnerabilidades em um servidor Apache Tika e elevação de privilégios no Windows. O CTF, embora de nível fácil, reforçou habilidades essenciais em segurança da informação, oferecendo uma prática valiosa em um ambiente controlado.

# Referências

- <https://www.exploit-db.com/exploits/47208>

- <https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/post/multi/recon/local_exploit_suggester.md>