Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

LazyAdmin – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | LazyAdmin – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 07/11/2024 |
| **Link** | https://tryhackme.com/r/room/lazyadmin |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 22/10/2024 | Produção |
| **1** | 07/11/2024 | Sérgio Guidi Trovo |
| **2** | 07/11/2024 | Sérgio Guidi Trovo |

**Sumário**

[Contextualização 3](#_Toc180518995)

[Desenvolvimento 3](#_Toc180518996)

[What is the user flag? 3](#_Toc180518997)

[What is the root flag? 8](#_Toc180518998)

[Conclusão 9](#_Toc180518999)

[Referências 9](#_Toc180519000)

Contextualização

O CTF LazyAdmin é um desafio de nível fácil. Ele aborda assuntos básicos do pentesting, como: *port scanning*, enumeração e análise de script SQL e procura e uso de exploit, *reverse shell* e escalonamento de privilégios.

Desenvolvimento

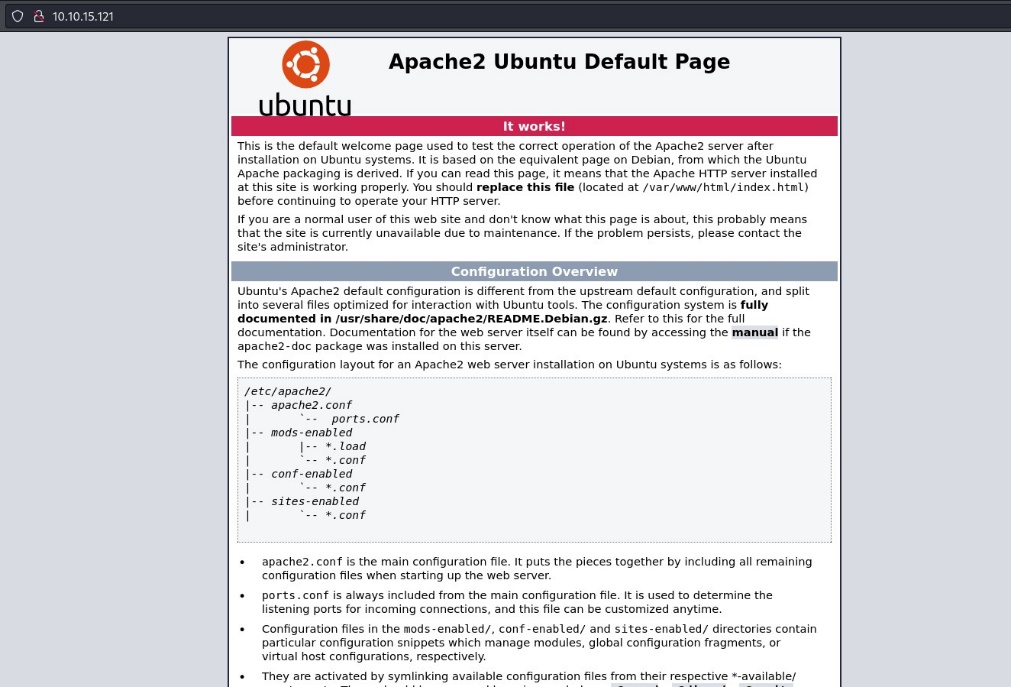
What is the user flag?

Para começar o CTF, use o **Nmap** com o parâmetro ‘*Agressive’* (-A) para fazer a enumeração da máquina.

Texto

Descrição gerada automaticamente

O resultado da enumeração aponta que a porta 22 está rodando um serviço SSH para conexões remotas e a porta 80 está rodando um serviço HTTP para uma página web. A página é apenas um site de documentação:



Para continuar a enumeração, use o ***Gobuster*** com uma *wordlist* para procurar diretórios no endereço do site:

Texto

Descrição gerada automaticamente

Além do ‘index.html’ que é o site padrão, há um diretório chamado ‘content’.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

A página indica que o site ainda não está pronto. Portanto, há uma possibilidade de existir outros diretórios expostos nessa página. Use o **Gobuster** novamente, mas dessa vez no diretório ‘/content’.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

A ferramenta exibe um diretório chamado ‘/as’ que é uma página de autenticação, onde mais tarde poderá ser de utilidade:

Interface gráfica do usuário

Descrição gerada automaticamente

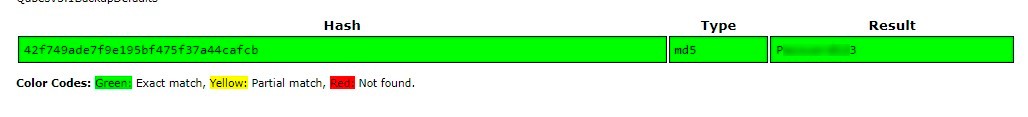
O diretório ‘/attachment’ é comumente usado para armazenar arquivos, como scripts, bibliotecas etc. Ao abrir ele, encontra-se um arquivo com a extensão ‘.sql’ na pasta de backup do banco de dados.

Dessa forma é possível fazer o download do arquivo e examinar o script do banco de dados:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

O script entrega um nome de usuário e uma senha, use uma ferramenta para descobrir a senha original.



Então, use essas credenciais (manager:P\*\*\*\*\*\*\*\*\*3) para adquirir acesso ao sistema a partir da página de login encontrada anteriormente.

Interface gráfica do usuário, Texto, Aplicativo, Email, Teams

Descrição gerada automaticamente

O site é um dashboard que está indicando rodar a versão 1.5.1 do SweetRice. Com isso, use a ferramenta ***Searchsploit*** para buscar um exploit da versão dessa aplicação e faça o download do script:

Texto

Descrição gerada automaticamente

A ferramenta apontou diversos exploits para essa aplicação, use a opção para fazer um upload de arquivo. Nesse caso, o arquivo de upload será uma *Reverse Shell* em php. Então, crie um arquivo na máquina local e copie o script alterando o IP e a porta padrão do script para o da máquina local.

Após isso, execute o script do exploit em python e siga as instruções:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Dessa forma, deverá aparecer o seu arquivo no menu ‘Media Center’ do dashboard.

Para continuar a *Reverse Shell*, inicie no terminal local o ***NetCat*** com a porta escolhida e execute o código php no site. Assim, o ***NetCat*** ficará “escutando” a requisição feita pelo arquivo do script ao ser executado, permitindo acesso à máquina alvo: Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Então, ao garantir o acesso à máquina use o comando ‘cat’ para visualizar a flag ‘user.txt’.

What is the root flag?

Para acessar o usuário root, será necessário fazer um escalonamento de privilégios a partir de um usuário padrão. Use o comando ‘sudo -l’ para verificar as permissões do usuário.

Texto

Descrição gerada automaticamente

O resultado mostra que qualquer usuário consegue rodar um script *perl*, que por sua vez, invoca um terminal para executar o script ‘copy.sh’. Dentro desse script, há um *Reverse Shell* com um IP privado para a porta 5554. Reescreva o script substituindo o IP anterior para o IP da máquina local com o comando:

echo “{*reverse shell*}” > /etc/copy.sh

Após isso, execute o ***NetCat*** em outro terminal local, mas dessa vez na porta 5554 e o script *perl* na máquina:

Texto

Descrição gerada automaticamente

Agora o outro da *Reverse Shell* possuí acesso root. Portanto, basta navegar até a pasta root e capturar a flag final:

Texto

Descrição gerada automaticamente

Conclusão

Por tratar de assuntos básicos, o CTF em questão pode ser uma boa escolha de desafio para iniciantes no mundo do pentesting e perfeito para treinar ferramentas e aprimorar os conhecimentos de ferramentas e Linux.

Referências

* <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>
* <https://crackstation.net/>
* <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web>