Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF WgetCTF – Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 02/03/2025 |
| **Link** | tryhackme.com/r/room/wgetctf |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 28/08/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Enumeração, cracking de senhas e privilege escalation. |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[User flag 3](#_heading=h.3znysh7)

[Root flag](#_heading=h.3dy6vkm) 6

[Conclusão](#_heading=h.1t3h5sf) 7

[Referências](#_heading=h.4d34og8) 7

**Contextualização**

O WgetCTF é um Capture The Flag (CTF) disponível na plataforma TryHackMe, voltado para iniciantes que desejam aprimorar suas habilidades em pentest e cybersecurity. Esse desafio foca em explorar vulnerabilidades comuns em aplicações web, exigindo dos participantes conhecimento em enumeração, cracking de senhas e privilege escalation.

**Desenvolvimento**

**User flag?**

Começamos utilizando o nmap para poder descobrir as portas que estão abertas no servidor, temos a porta 22 (ssh) e a 80 (http)

Comando usado: ***nmap –sS <ip\_machine>***

**Texto

O conteúdo gerado por IA pode estar incorreto.**

Acessando o site, já podemos analisar a página web que é um padrão apache. Olhando o “inspecionar” podemos ver que há o nome Jessie, como uma boa informação.

Texto

O conteúdo gerado por IA pode estar incorreto.

Usando o gobuster, podemos então ver outras páginas, como o /sitemap.

**Comando usado:** gobuster dir -w /usr/share/dirb/wordlists/common.txt -u http://<ip\_target>

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Então, não há muitas informações que botemos obter aqui. Usando novamente o mesmo comando do gobsuster, podemos ter acesso ao /.ssh

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Tabela

O conteúdo gerado por IA pode estar incorreto.

Acessando e dando uma olhada nesse arquivo, temos uma chave em RSA. Provavelmente podemos usar ela no ssh.

Texto

O conteúdo gerado por IA pode estar incorreto.

Criando um arquivo com o nome “id\_rsa” e colando a chave dentro dele, podemos dar uma permissão maior para usar no ssh.

Texto

O conteúdo gerado por IA pode estar incorreto.

Podemos então acessar o ssh da Jessie.

Texto

O conteúdo gerado por IA pode estar incorreto.

Fazendo uma busca muito simples nos diretórios, podemos então achar a “user” flag.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

**Root.flag?**

Testando qual comando pode ser executado, temos um “wget”. Podemos então executar ele de algum jeito para termos o acesso Root.Texto

O conteúdo gerado por IA pode estar incorreto.

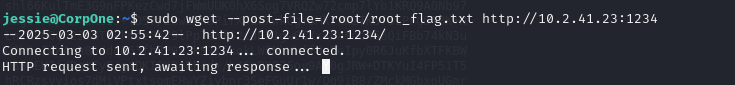
Executando o netcat para podermos ter um acesso de dentro do servidor.

**Comando usado:** nc -lvpn <port>

Texto

O conteúdo gerado por IA pode estar incorreto.

Executando uma linha de comando para poder acessar a root flag.



A informação da root.txt é enviada para o netcat e pronto, temos a flag.

Texto

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

O WgetCTF é um excelente desafio para iniciantes em pentest, proporcionando uma experiência prática e realista na exploração de vulnerabilidades comuns em aplicações web.

**Referências**

[**https://gtfobins.github.io**](https://gtfobins.github.io)