Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Anonforce – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Anonforce – Pedro Leal Ariosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 31/08/2025 |
| **Link** | https://tryhackme.com/room/bsidesgtanonforce |

|  |  |  |
| --- | --- | --- |
| **Redação** | Pedro Leal Ariosa | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 31/08/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | FTP, Brute Force, john, gpg2john |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

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

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

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

[Root.txt 3](#_heading=h.2et92p0)

[Conclusão 5](#_heading=h.1t3h5sf)

[Referências 6](#_heading=h.4d34og8)

**Contextualização**

O CTF Anonforce é um CTF que busca desenvolver conhecimentos e técnicas de invasão em FTP, arquivos criptografados, enumeration e brute force. O cenário é estruturado de forma a representar uma aplicação web vulnerável, permitindo explorar o FTP através do login anonymous e explorar arquivos criptografados.

**Desenvolvimento**

**User.txt**

Para realizar o port scanning foi utilizado o comando “nmap -sV ip”, de modo que retornou a porta 21 aberta rodando FTP e porta 22 aberta rodando SSH.

Texto

O conteúdo gerado por IA pode estar incorreto.

Ao acessar o FTP via login anonymous, através do comando “ls” para listar os diretórios existentes o retorno observado foi “melodias”. Enumerando os diretórios dentro de melodias foi encontrado o arquivo user.txt, a primeira flag do CTF.

Texto

O conteúdo gerado por IA pode estar incorreto.

**Root.txt**

Enumerando o diretório home, o programa retornou um diretório interessante chamado “notread”. Ao acessar o diretório notread, utilizando o comando ls retornou 2 arquivos: backup.pgp e private.asc

Texto

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Com o comando “cat”, concluiu-se que ambos os arquivos estão codificados.

Dessa forma, com os comandos “gpg2john”, “john –import” e utilizando o john com parâmetro de worlists/rockyou.txt e possível realizar a importação e brute force no arquivo private.asc.

Texto

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Dessa forma, com a senha encontrada, o objetivo se tornou descriptografar o arquivo backup.pgp. Após descriptografar o arquivo, foi encontrado o hash do root, possibilitando a aplicação do brute force para encontrar a senha do root.

Texto

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Por fim, com o login e senha, tornou-se possível o acesso via ssh do root e alcançar a última flag.

Texto

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

Portanto, ao finalizar o CTF, é possível concluir que o CTF Anonforce trabalha integralmente os conhecimentos de FTP por meio do login anonymous, SSH, brute force, john the ripper e enumeração de diretórios, de modo que desenvolve e aprimora instrumentos extremamente importantes para a área de cibersegurança.

**Referências**

https://book.hacktricks.wiki/en/network-services-pentesting/pentesting-ftp/index.html

https://book.hacktricks.wiki/en/network-services-pentesting/pentesting-ssh.html