Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Brute It – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Brute It – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 31/08/2024 |
| **Link** | https://tryhackme.com/r/room/bruteit |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | João Branco | Orientador |
| **Aprovação** | João Branco | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 31/08/2024 | Produção |
| **1** | 02/09/2024 | Revisão |
| **2** | 02/09/2024 | Aprovação |

**Sumário**

[Contextualização 3](#_Toc176021358)

[Desenvolvimento 3](#_Toc176021359)

[How many ports are open? 3](#_Toc176021360)

[What version of SSH is running? 3](#_Toc176021361)

[What version of Apache is running? 4](#_Toc176021362)

[Which Linux distribution is running? 4](#_Toc176021363)

[What is the hidden directory? 4](#_Toc176021364)

[What is the user:password of the admin panel? 5](#_Toc176021365)

[What is John's RSA Private Key passphrase? 6](#_Toc176021366)

[User.txt: 7](#_Toc176021367)

[What is the root's password? 9](#_Toc176021368)

[Conclusão 10](#_Toc176021369)

[Referências 11](#_Toc176021370)

Contextualização

O CTF Brute It te desafia a explorar uma máquina com vulnerabilidade de serviço SSH e ataque de força bruta em uma página web afim de descobrir dados de credenciais de um usuário. Além disso, explora outros diversos conceitos da prática de pentesting.

Desenvolvimento

How many ports are open?

Com o **Nmap,** usando o parâmetro agressivo (-A) podemos fazer a enumeração da máquina. Dessa forma descobrimos que há 2 portas abertas.

Texto

Descrição gerada automaticamente

What version of SSH is running?

Usando o resultado da enumeração anterior, podemos responder essa e as próximas duas perguntas. Então, é possível observar que a máquina está rodando a seguinte versão do protocolo SSH:

Texto

Descrição gerada automaticamente

What version of Apache is running?

Com o **Nmap,** descobrimos que a máquina roda o Apache 2.4.29.

Texto

Descrição gerada automaticamente

Which Linux distribution is running?

A máquina está rodando Ubuntu como sistema operacional.

Texto

Descrição gerada automaticamente

What is the hidden directory?

Para descobrir o diretório web escondido, usaremos a ferramenta **Dirb** com uma *wordlist*. Caso o site retorne o código de resposta HTTP 200, significa que o Dirb acessou a página com sucesso:

Texto

Descrição gerada automaticamente

Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente

What is the user:password of the admin panel?

Com a ferramenta **Hydra**, podemos fazer um *Brute-Force* para descobrir a senha do usuário. O nome de usuário podemos encontrar inspecionando o código HTML da página.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Comando Hydra:

``` hydra -l admin -P /usr/share/wordlists/rockyou.txt {$IP} http-post-form "/admin/:user=^USER^&pass=^PASS^:Username or password invalid" -V ```



admin:x\*\*\*\*r

What is John's RSA Private Key passphrase?Parte superior do formulário

Autenticando no site com o usuário e senha que descobrimos anteriormente, vemos que há um download de uma chave RSA privada, usada para proteger dados criptografados.



Texto

Descrição gerada automaticamente

Para quebrar essa criptografia, devemos adicionar essa chave privada a um documento padrão de texto que eu chamei de “rsa\_key” e criar um hash dessa chave com o **John-the-Ripper** com o seguinte comando:

``` python3 /usr/share/john/ssh2john.py rsa\_key > rsa\_key\_hash ```

Então, será criado o arquivo hash chamado “rsa\_key\_hash”. Com isso, podemos descobrir a palavra-chave quebrando a criptografia do arquivo hash com o comando:

``` john --wordlist=/usr/share/wordlists/rockyou.txt rsa\_key\_hash ```

Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente

User.txt:

Agora, usaremos a porta 22 com o serviço SSH aberto (serviço de conexão remota) para se autenticar na máquina usando a chave privada. Mas, precisamos primeiro dar permissões de leitura e escrita para a chave RSA com o comando “chmod”:

``` sudo chmod 600 rsa\_key ```

E então, nos conectamos na máquina usando o SSH com o parâmetro “-i” para se credenciar a partir da chave privada. Assim, iremos digitar a senha descoberta pelo John para entrar:

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

What is the root's password?

Primeiro precisamos fazer o escalonamento de privilégios, visto que não conseguimos acessar a pasta “/root”. Podemos verificar nossas permissões acessando o arquivo “sudoers”, que coincidentemente dará certo tendo em vista que o usuário john tem acesso ao comando “cat” como administrador sem a necessidade de senha:

Texto

Descrição gerada automaticamente

Então, podemos verificar o arquivo “/etc/shadow” que contém informações de senhas dos usuários do sistema:Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Dado que a senha do usuário root está criptografada, podemos usar a ferramenta john para quebrar essa criptografia e ter acesso à senha:

Texto

Descrição gerada automaticamente

Então, logado no usuário john, podemos solicitar a troca de usuário para root e digitar a senha que descobrimos anteriormente e acessar o arquivo “/root/root.txt”:

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente com confiança média

Conclusão

Esse CTF, se adequa perfeitamente para a prática de força bruta em páginas web e aperfeiçoamento da ferramenta Hydra. Também aborda conceitos comuns de pentesting, como enumeração e criptografia. Importante ressaltar, que o Brute It pode ser um bom CTF para desenvolver os conhecimentos do sistema Linux, visto a notoriedade das pastas “/etc/shadow” e “/etc/sudoers” usadas no desafio.

Referências

* <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>
* <https://www.openwall.com/john/doc/>
* <https://hydra.cc/docs/intro/>