Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Basic Pentesting – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Basic Pentesting – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 27/08/2024 |
| **Link** | https://tryhackme.com/r/room/basicpentestingjt |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 23/08/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

[Contextualização 3](#_Toc175597672)

[Desenvolvimento 3](#_Toc175597673)

[Find the services exposed by the machine: 3](#_Toc175597674)

[What is the name of the hidden directory on the web server(enter name without /)?´ 3](#_Toc175597675)

[User brute-forcing to find the username & password 4](#_Toc175597676)

[What is the username? 4](#_Toc175597677)

[What is the password? 4](#_Toc175597678)

[What service do you use to access the server(answer in abbreviation in all caps)? 5](#_Toc175597679)

[Enumerate the machine to find any vectors for privilege escalation 5](#_Toc175597680)

[What is the name of the other user you found(all lower case)? 5](#_Toc175597681)

[If you have found another user, what can you do with this information? 6](#_Toc175597682)

[What is the final password you obtain? 7](#_Toc175597683)

[Conclusão 10](#_Toc175597684)

[Referências 10](#_Toc175597685)

Contextualização

O CTF Basic Pentesting aborda conceitos básicos como escaneamento de portas, enumeração, escalonamento de privilégios e criptografia básica, auxiliando a prática do uso de ferramentas essenciais para a solução de um CTF.

Desenvolvimento

Find the services exposed by the machine:

Usando o **Nmap** no parâmetro agressivo para realizar o *Port Scanning,* é possível observar que a máquina está rodando os seguintes serviços:

***Texto

Descrição gerada automaticamente***

What is the name of the hidden directory on the web server(enter name without /)?´

Para descobrir qual o diretório secreto rodando na página web, basta usar a ferramenta **Dirb** com uma wordlist. Nesse caso, descobrimos que o diretório secreto se chama “development”.

***Texto

Descrição gerada automaticamente***

User brute-forcing to find the username & password

Antes de realizar o *Brute-Force* é necessário fazer uma enumeração para descobrir o nome de usuário, e então descobrir a senha.

What is the username?

Para descobrir o usuário, vamos realizar a enumeração usando o **Enum4Linux**:

***Texto

Descrição gerada automaticamente***

Com isso, descobrimos que há dois usuários no sistema: jan e kay.

What is the password?

Visto que temos os nomes de usuário, basta usar o **Hydra**com a wordlist “rockyou.txt” para descobrir os dados de login da porta SSH.

Texto

Descrição gerada automaticamente

What service do you use to access the server(answer in abbreviation in all caps)?

Para descobrir qual serviço dará acesso ao servidor, é necessário voltar ao *Port Scanning* feito pelo **Nmap**:

***Texto

Descrição gerada automaticamente***

Enumerate the machine to find any vectors for privilege escalation

Com os resultados da enumeração anterior, vimos que há uma porta rodando o serviço SSH que poderá ser usado futuramente para o escalonamento de privilégios.

What is the name of the other user you found(all lower case)?

Conectando ao serviço SSH usando a senha obtida anteriormente, é possível acessar a máquina no nome de “jan”. Então, encontramos o outro perfil chamado “kay” que já foi encontrado na enumeração.

Texto

Descrição gerada automaticamente

If you have found another user, what can you do with this information?

No usuário de kay, encontramos um arquivo interessante (pass.bak) onde provavelmente está a flag, mas que não temos acesso para abrir.

Texto

Descrição gerada automaticamente

Porém, ainda no mesmo diretório há uma pasta oculta chamada “ssh” que possui credenciais para autentificação. O arquivo id\_rsa e id\_rsa.pub são arquivos de credenciais, na qual buscam facilitar o login. Porém, visto que a chave privada (id\_rsa) está criptografada, teremos que quebrar essa criptografia para ter acesso a senha e conseguir acesso ao arquivo “pass.bak”

***Texto

Descrição gerada automaticamente***

What is the final password you obtain?Parte superior do formulário

É possível copiar a chave pública e criar um arquivo idêntico para usar o **JohnTheRipper** para descriptografar e criar um documento hash:

Imagem em preto e branco com texto preto sobre fundo branco

Descrição gerada automaticamente

Use o **ssh2john** para transformar a criptografia em hash:

Interface gráfica do usuário, Site

Descrição gerada automaticamente

Use o **John** para quebrar a senha:

Tela preta com letras brancas

Descrição gerada automaticamente

E então, é possível se autentificar no usuário “kay” usando o arquivo de credencial criptografado por meio do protocolo SSH no usuário de “jay”:

Texto

Descrição gerada automaticamente

Conclusão

O CTF em questão, apesar de tratar de conceitos básicos, pode ser um pouco desafiador para quem está começando com *pentesting.* Porém, é um CTF ótimo para treinar ferramentas básicas para resolução de desafios.

Referências

* <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>
* <https://www.openwall.com/john/doc/>
* <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web>