Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Year of the Rabbit – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Year of the Rabbit – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 27/10/2024 |
| **Link** | https://tryhackme.com/r/room/yearoftherabbit |

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

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 14/10/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

[Contextualização 3](#_Toc181038159)

[Desenvolvimento 3](#_Toc181038160)

[What is the user flag? 3](#_Toc181038161)

[What is the root flag? 11](#_Toc181038162)

[Conclusão 13](#_Toc181038163)

[Referências 13](#_Toc181038164)

Contextualização

Esse CTF tende ao nível intermediário, possuindo uma variedade de assuntos relacionados ao pentesting. Traz temas como *Port Scanning*, enumeração, análise de requisições HTTP, conexões FTP e SSH, *Brute Force* e escalonamento de privilégios.

Desenvolvimento

What is the user flag?

Parte superior do formulário

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

Texto

Descrição gerada automaticamente

É possível ver que há 3 portas abertas, a porta 21 rodando um serviço FTP, a 22 rodando um serviço SSH (Conexão Remota) e a 80 para um servidor web em HTTP.

A aplicação web é uma página do Apache, sem informações adicionais.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Para continuar, enumere os diretórios dessa página usando o **Gobuster** com uma wordlist. Assim, a ferramenta mostrará diferentes ‘paths’ para o endereço HTTP:

Texto

Descrição gerada automaticamente

Com a enumeração, foi possível descobrir um diretório chamado ‘/assets’ acessível. Então, navegue para esse diretório web para encontrar mais informações.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Há dois arquivos, o primeiro aparenta ser um vídeo relacionado a uma piada de internet, enquanto o segundo é um arquivo CSS responsável pela formação e estilo do site.

Ao abrir o arquivo CSS, é possível encontrar uma mensagem comentada que revela um diretório escondido.

Texto

Descrição gerada automaticamente

Analisando o diretório mencionado, o navegador leva até a música “Never Gonna Give You Up” novamente. Então, use o **BurpSuite** no modo ‘proxy’ para capturar as requisições HTTP e recarregue a página.

Dessa forma, a ferramenta irá capturar um diretório secretoInterface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Nesse diretório há apenas uma imagem, faça o download dela para continuar explorando.

Tabela

Descrição gerada automaticamente

Tela de celular com foto de mulher

Descrição gerada automaticamente

Use um comando Linux para visualização de texto (cat, less ou vi) nessa imagem para encontrar mensagens escondidas.

Após os códigos binários, haverá um nome de usuário e diversas senhas (apenas uma é a correta) para as credenciais FTP:

Texto

Descrição gerada automaticamente

Copie as possíveis senhas e crie um arquivo de texto que servirá de wordlist.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Então, use o **Hydra** para fazer um *Brute-force* para testar o arquivo de senhas com o usuário encontrado com tentativas de requisições FTP. Caso o **Hydra** encontre as credenciais corretas, ele retornará no terminal.  




Use essas informações para conectar à porta 21, responsável pelo serviço FTP.

Texto

Descrição gerada automaticamente

Explorando os arquivos FTP, haverá um arquivo chamado “Eli’s\_Creds.txt”, nele conterá um código escrito em *BrainF\*ck*, uma linguagem de programação criada para desafiar os programadores.

Texto

Descrição gerada automaticamente com confiança média

Use um decodificador online para ter acesso ao texto original, que é um usuário e senha para autenticação na porta 22 (SSH) para conexões remotas:

Uma imagem contendo Diagrama

Descrição gerada automaticamente

Realizando a conexão SSH, obtém-se acesso ao terminal da máquina alvo no usuário de ‘eli’.

Texto

Descrição gerada automaticamente

Use o comando ‘find’ do Linux para encontrar o diretório da primeira flag:

Texto

Descrição gerada automaticamente

O terminal mostra que a flag está no diretório ‘/home/gwendoline’ mas que não temos acesso para visualização. Onde, provavelmente apenas o usuário ‘gwendoline’ tem acesso.

Porém, no início da conexão SSH, apareceu uma mensagem incomum escrita pelo root para gwendoline, ele diz que deixou uma mensagem para ela no diretório secreto dela. Use novamente o comando ‘find’ para encontrar o diretório secreto e ter acesso a mensagem do root.

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

A mensagem do root é uma recomendação para que gwendoline use uma senha mais forte e não apenas uma senha simples. Com isso, obtém-se a atual senha do usuário gwendoline.

Usando o comando ‘su’ do Linux, é possível trocar de usuário. E assim, permitindo acesso a flag ‘user.txt’:

Texto

Descrição gerada automaticamente

What is the root flag?

Para ter acesso a flag final, será necessário fazer um escalonamento de privilégios a partir de um usuário de menor privilégio. Então, consulte as permissões do usuário gwendoline usando o comando ‘sudo -l’.

Texto

Descrição gerada automaticamente

Com isso, é possível saber que qualquer usuário (menos o root) pode acessar o arquivo ‘user.txt’ a partir do vi (visual editor, semelhante ao less). Porém, não é comum esse tipo de permissão onde todos podem ter acesso menos o root.

Pesquisando sobre, é notável que essa característica faz parte de um exploit de *Spawn Shell*, permitindo que o usuário crie um terminal que pode ter, ou não permissões de root.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Execute o comando acima para ter acesso ao vi, e assim, criar outro terminal para root e garantir acesso a flag final.

(sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt)

Interface gráfica do usuário

Descrição gerada automaticamente

Fundo preto com letras brancas

Descrição gerada automaticamente

Conclusão

Visto que o nível do CTF tende a ser um pouco mais alto, pode ser uma oportunidade para desafiar os conhecimentos em *Web-Hacking*, praticar e concretizar o conhecimento na área de cibersegurança.

Referências

* <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>
* [https://www.dcode.fr/brainfuck-language](https://www.dcode.fr/brainfuck-language%20) <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web>
* <https://www.exploit-db.com/exploits/47502>