Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

TakeOver – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | TakeOver – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 10/11/2024 |
| **Link** | https://tryhackme.com/r/room/takeover |

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

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 10/11/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

[Contextualização 2](#_Toc182324863)

[Desenvolvimento 3](#_Toc182324864)

[What's the value of the flag? 3](#_Toc182324865)

[Conclusão 7](#_Toc182324866)

[Referências 7](#_Toc182324867)

Contextualização

O CTF TakeOver é um desafio de nível fácil que envolve apenas exploração web, precisando de poucos conhecimentos em Linux para resolvê-lo. Para realizar esse desafio, será necessário conhecer sobre *Port Scannig,* enumeração de diretórios e subdomínios e o básico de arquivos Linux.

Desenvolvimento

What's the value of the flag?

Para garantir acesso ao site citado, será necessário adicionar o IP do TryHackMe no arquivo ‘/etc/hosts’, ele é responsável por mapear um endereço IP para seu respectivo host antes de consultar um DNS externo.

Use o comando Linux ‘nano’ para modificar o arquivo hosts:

Texto

Descrição gerada automaticamente

Então, execute o **Nmap** para fazer o *Port Scanning,* encontre as portas abertas e seus respectivos serviços usando o parâmetro ‘-sV’.

Texto

Descrição gerada automaticamente

O **Nmap** mostrou que há três portas abertas, rodando um serviço SSH para conexão remota, HTTP para conexão web e um SSL/HTTP para conexão web segura.

Ao entrar no site, é exibido apenas uma página simples sobre astrologia:

Tela de celular com aplicativo aberto

Descrição gerada automaticamente

Faça a enumeração dos diretórios web usando o **Gobuster**:  
Texto

Descrição gerada automaticamente

Nada foi descoberto com essa ferramenta, provavelmente o diretório está sendo diferenciado como subdomínio para ser diferenciado no arquivo de DNS local. Para descobrir subdomínios, use a ferramenta **FFUF** com o parâmetro ‘-fs 0, 4605’ para esconder respostas de 0 e 4605 bytes (mensagens de erro):Texto

Descrição gerada automaticamente

A ferramenta retornou dois subdomínios, ‘blog’ e ‘support’. Altere o arquivo ‘hosts’ novamente:

Texto

Descrição gerada automaticamente

Agora, consulte as páginas ‘blog’ e ‘support’, será possível encontrar um erro dizendo que a página não pode ser segura pois não apresenta um certificado confiável. Isso pode ser uma pista para encontrar algo mais tarde. Ignore o erro, e prossiga em ambas as páginas.

Blog:  
Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Support:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente com confiança média

Não há nada nas páginas em si, procure pelo certificado de cada uma.

Na página ‘support’, há um detalhe no certificado de segurança:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Texto

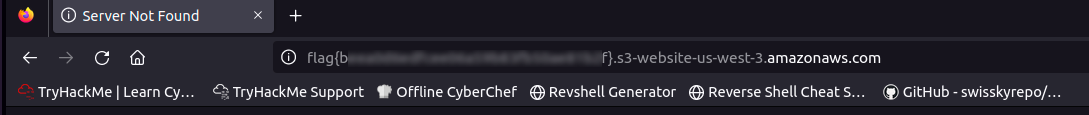
Descrição gerada automaticamente

Existe um DNS diferente do nome comum. Novamente, edite o arquivo ‘hosts’ da máquina local para ter acesso à essa página.

Texto

Descrição gerada automaticamente

Ao abrir esse DNS no navegador, automaticamente a URL aparecerá exibindo a flag do desafio.



Conclusão

O CTF em questão pode parecer confuso a princípio, por adotar uma abordagem "fora da caixa" ao explorar subdomínios, em vez de diretórios web, como é mais comum em desafios desse tipo. Todavia, essa abordagem oferece uma excelente oportunidade para testar e expandir o conhecimento em exploração de aplicações web.

Referências

* <https://www.kali.org/tools/ffuf/>
* <https://www.kali.org/tools/gobuster/>
* <https://book.hacktricks.xyz/network-services-pentesting/pentesting-web>