Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Root Me – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Root Me – Sérgio Guidi Trovo |
| **N° Revisão** | 1 |
| **Data de publicação** | 07/09/2024 |
| **Link** | <https://tryhackme.com/r/room/rrootme> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Sérgio Guidi Trovo | Estudante |
| **Revisão** | João Branco | Presidente |
| **Aprovação** | João Branco | Presidente |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 07/09/2024 | Produção |
| **1** | 02/10/2024 | Revisão |
| **2** | 02/10/2024 | Aprovação |

**Sumário**

[Contextualização 3](#_Toc176508087)

[Desenvolvimento 3](#_Toc176508088)

[Pergunta 1 - Scan the machine, how many ports are open? 3](#_Toc176508089)

[Pergunta 2 - What version of Apache is running? 3](#_Toc176508090)

[Pergunta 3 - What service is running on port 22? 3](#_Toc176508091)

[Pergunta 4 - What is the hidden directory? 3](#_Toc176508092)

[Pergunta 5 – user.txt 4](#_Toc176508093)

[Pergunta 6 – Search for files with SUID permission, which file is weird? 7](#_Toc176508094)

[Pergunta 7 – root.txt 7](#_Toc176508095)

[Conclusão 8](#_Toc176508096)

[Referências 8](#_Toc176508097)

Contextualização

O CTF Root Me é um CTF de nível de dificuldade fácil que aborda etapas básicas do processo de pentesting. Ele tem foco em manipulação de request com *Burpsuite* e escalação de privilégio.

Desenvolvimento

Pergunta 1 - Scan the machine, how many ports are open?Parte superior do formulário

Começamos o CTF realizando um mapeamento da máquina com o comando *nmap*.

Texto

Descrição gerada automaticamente

A partir do resultado encontramos duas portas abertas com os serviços ssh e http.

Pergunta 2 - What version of Apache is running?

Parte superior do formulário

Com o nmap realizado, é possível verificar que a versão do Apache é 2.4.29.

Pergunta 3 - What service is running on port 22?

Parte superior do formulário

Com o nmap realizado, é possível verificar que o serviço rodando na porta 22 é ssh.

Pergunta 4 - What is the hidden directory?

Parte superior do formulário

Executamos o comando gobuster para verificar os diretórios no serviço web.

Texto

Descrição gerada automaticamente

Com o gobuster, encontramos o diretório escondido */panel/.*

Pergunta 5 – user.txt

Acessando a página */panel/* encontramos um local para fazer upload de arquivos.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Podemos tentar fazer o upload de um reverse shell para ganhar acesso remoto ao sistema.

Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

Descrição gerada automaticamente

Ao tentar fazer upload de um php-reverse-shell, percebemos que o sistema não aceita upload de files *php*. Para contornar esse problema, podemos utilizar o *Burpsuite* para verificar quais tipos de extensão de arquivo são aceitos para envio.

Tabela

Descrição gerada automaticamente

Fazendo isso, encontramos que o tipo de arquivo aceito é .phtml. Então, alteramos a extensão do arquivo reverse shell e fazemos o upload.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Podemos, então, nos conectar com o servidor via *netcat*.



Texto

Descrição gerada automaticamente

Dentro da máquina invadida, utilizamos o comando *find* para encontrar a file user.txt.

Texto

Descrição gerada automaticamente

Com o caminho para file encontrado, basta utilizar o comando *cat* para verificar o conteúdo da file.



Pergunta 6 – Search for files with SUID permission, which file is weird?

Procurando por files com permissão *suid*, encontramos um binário */python*.





Pergunta 7 – root.txt

Procurando no site *gtfobins*, encontramos um script de python para escalação de privilégio.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Utilizando esse comando conseguimos acessar o servidor como root e acessar a última flag.

Interface gráfica do usuário

Descrição gerada automaticamente com confiança média

Conclusão

O CTF Root Me é um CTF recomendado para explorar conceitos básicos do processo de pentesting. Esse CTF auxilia no entendimento de manipulação de arquivos com Burpsuite e nas técnicas de escalação de privilégios.

Referências

<https://book.hacktricks.xyz/>

[https://gtfobins.github.io/#](https://gtfobins.github.io/)