Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Wgel CTF – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Wgel CTF – Sergio Guidi Trovo |
| **N° Revisão** | 1 |
| **Data de publicação** | 06/10/2024 |
| **Link** | https://tryhackme.com/r/room/wgelctf |

|  |  |  |
| --- | --- | --- |
| **Redação** | Sérgio Guidi Trovo | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

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

**Sumário**

[Contextualização 2](#_Toc179143088)

[Desenvolvimento 3](#_Toc179143089)

[Pergunta 1 - User flag 3](#_Toc179143090)

[Pergunta 2 - Root flag 6](#_Toc179143091)

[Conclusão 7](#_Toc179143092)

[Referências 8](#_Toc179143093)

Contextualização

O CTF Wgel CTF é um CTF de nível de dificuldade fácil da plataforma TryHackMe. Esse CTF aborda principalmente a manipulação de chaves RSA e escalação de privilégios utilizando comandos com permissão SUDO.

Desenvolvimento

Pergunta 1 - User flag

Iniciamos o CTF realizando um mapeamento do servidor para encontrar portas abertas e os serviços rodando nelas. Para isso utilizamos o comando *nmap*.

Texto

Descrição gerada automaticamente

Encontramos duas portas abertas: a porta 22 rodando o serviço ssh e a porta 80 rodando o serviço http.

Acessando o serviço web encontramos a página default do Apache2 Ubuntu.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Inspecionando a página encontramos uma mensagem deixada para o usuário “Jessie” em forma de comentário.

Texto

Descrição gerada automaticamente

Podemos procurar por diretórios escondidos fazendo uma enumeração com o comando *gobuster* no serviço web.

Texto branco sobre fundo preto

Descrição gerada automaticamente

Encontramos um diretório interessante chamado sitemap.

Acessando a página encontrada, encontramos outro site.

Interface gráfica do usuário, Site

Descrição gerada automaticamente

Explorando o site encontrado, não encontramos nada que possa ser útil para invadir o servidor. Então realizamos uma nova enumeração de diretórios, desta vez a partir da página encontrada, em busca de possíveis vulnerabilidades.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente com confiança média

Descobrimos, desse modo, uma nova página interessante chamada .ssh. Acessando essa página encontramos um arquivo nomeado id\_rsa.

Tabela

Descrição gerada automaticamente

Acessando o arquivo, encontramos, como esperado, uma chave RSA. Podemos tentar utilizar a ferramenta *john the ripper* para tentar obter a chave da RSA encontrada.



Fazendo isso, descobrimos que a chave RSA encontrada não tem chave. Desse modo, podemos utilizar a chave para tentar nos conectar via ssh com o servidor utilizando o usuário encontrado anteriormente: “Jessie”.

Texto

Descrição gerada automaticamente

Conseguimos nos conectar com o servidor.

Explorando o servidor encontramos a flag de usuário user\_flag.txt.

Interface gráfica do usuário, Site

Descrição gerada automaticamente

Pergunta 2 - Root flag

Para conseguir a flag de root, precisamos tentar escalar privilégios no servidor. Para isso, começamos utilizando o comando *sudo -l* para verificar files executáveis com permissões de sudo no servidor.

Texto

Descrição gerada automaticamente

Descobrimos que podemos utilizar o comando *wget* com permissões de sudo. Pesquisando formas de escalar privilégio com o comando *wget* encontramos uma forma de enviar arquivos do servidor invadido para a nossa máquina.

Primeiramente abrimos um netcat na nossa máquina para ouvir por conexões.



Em seguida, executamos o seguinte comando na máquina invadida para enviar a flag de root para a nossa máquina:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Ao fazer isso, recebemos via netcat o conteúdo da file *root\_flag.txt*.

Texto

Descrição gerada automaticamente

Conclusão

O CTF Wgel é um CTF interessante para aprender os procedimentos básicos do processo de pentesting. Ele é indicado para desenvolver novas habilidades de escalação de privilégios.

Referências

<https://www.exploit-db.com/>

<https://gtfobins.github.io/>

https://book.hacktricks.xyz/