Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Tomghost – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Tomghost – Sérgio Guidi Trovo |
| **N° Revisão** | 1 |
| **Data de publicação** | 12/10/2024 |
| **Link** | https://tryhackme.com/r/room/tomghost |

|  |  |  |
| --- | --- | --- |
| **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](#_Toc179623463)

[Desenvolvimento 3](#_Toc179623464)

[Pergunta 1 - Compromise this machine and obtain user.txt 3](#_Toc179623465)

[Pergunta 2 - Escalate privileges and obtain root.txt 6](#_Toc179623466)

[Conclusão 6](#_Toc179623467)

[Referências 7](#_Toc179623468)

Contextualização

O CTF tomghost é um CTF de nível de dificuldade fácil da plataforma TryHackMe que aborda todas as etapas do processo de pentesting. Ele é interessante para aprender a como utilizar exploits já conhecidos para ganhar acesso a um servidor.

Desenvolvimento

Pergunta 1 - Compromise this machine and obtain user.txt

Começamos o CTF realizando um mapeamento do servidor com o comando *nmap* para verificar possíveis portas abertas e seus serviços.

Texto

Descrição gerada automaticamente

Encontramos seis portas abertas. Na porta 8009, encontramos o serviço ajp13 que se trata de uma versão otimizada do protocolo HTTP. Pesquisando vulnerabilidades relacionadas a esse serviço, encontramos a vulnerabilidade *Ghostcast* que permite a leitura e escrita de arquivos no servidor.

Podemos utilizar o *metasploit* para exploitar essa vulnerabilidade.

Primeiro, procuramos pela vulnerabilidade e a acessamos no console do *metasploit*.

Texto

Descrição gerada automaticamente

Em seguida, definimos as variáveis a serem utilizadas.

Texto

Descrição gerada automaticamente

Por fim, executamos o exploit.



Fazendo isso, encontramos as credenciais de um usuário.



Podemos nos conectar com o servidor via ssh com os dados encontrados.

Texto

Descrição gerada automaticamente

Explorando o servidor, encontramos duas files.



A primeira se trata de uma file encriptada, e a segunda, é a chave para desencriptar.

Transferimos as files para a nossa máquina com o comando *scp*.

Texto

Descrição gerada automaticamente

Podemos utilizar o *john the ripper* para desencriptar a file credential.pgp. Primeiro convertemos a file tryhackme.asc para uma file que pode ser lida pelo *john*.

Texto

Descrição gerada automaticamente

Em seguida, utilizamos o *john* para desencriptar a file convertida utilizando uma wordlist de senhas comuns.

Texto

Descrição gerada automaticamente

Encontramos a chave “alexandru”. Agora, utilizamos a chave para acessar a outra file, credential.pgp.

Texto

Descrição gerada automaticamente

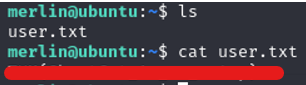
Encontramos um novo usuário “merlin”.

Nos conectamos ao servidor como o novo usuário encontrado.

Texto

Descrição gerada automaticamente

Explorando as files, encontramos a primeira flag.



Pergunta 2 - Escalate privileges and obtain root.txt

Verificando as files executáveis como sudo, encontramos /usr/bin/zip.

Texto

Descrição gerada automaticamente

Acessando o site gtfobins, encontramos uma forma simples de escalar privilégios utilizando o seguinte comando:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Utilizando o comando, conseguimos nos tornar o usuário root.

Texto

Descrição gerada automaticamente

Agora, basta acessarmos a flag de root para finalizar o CTF.



Conclusão

O CTF tomghost é um CTF muito interessante para aprender a como utilizar exploits já conhecidos. A ferramenta *metasploit* pode ser muito útil para exploitar vulnerabilidades comuns em servidores. O CTF também é interessante para aprender a manipulação de files criptografadas.

Referências

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

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

https://book.hacktricks.xyz/