Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Anonymous – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Anonymous – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 16/08/2024 |
| **Link** | https://tryhackme.com/r/room/anonymous |

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

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 12/08/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

[Contextualização 3](#_Toc174726135)

[Desenvolvimento 3](#_Toc174726136)

[Enumerate the machine.  How many ports are open? 3](#_Toc174726137)

[What service is running on port 21? 3](#_Toc174726138)

[What service is running on ports 139 and 445? 3](#_Toc174726139)

[There's a share on the user's computer.  What's it called? 4](#_Toc174726140)

[User.txt: 4](#_Toc174726141)

[ROOT.txt: 7](#_Toc174726142)

[Conclusão 8](#_Toc174726144)

[Referências 8](#_Toc174726145)

Contextualização

O CTF Anonymous foca em uma vulnerabilidade no protocolo FTP que permite a conexão ao servidor sem a necessidade de credenciais. Para se autenticar, basta inserir "anonymous". Para completar o desafio, é necessário realizar um escalonamento de privilégios para obter acesso como administrador do sistema.

Desenvolvimento

Enumerate the machine.  How many ports are open?

Realizando o seguinte *Port Scanning*, tem-se:

Texto

Descrição gerada automaticamente

What service is running on port 21?

O resultado do Scanning anterior mostra que a porta 21 está rodando um serviço FTP.

Texto

Descrição gerada automaticamente

What service is running on ports 139 and 445?

Realizando o Scanning completo dos serviços, nota-se que as portas 139 e 445 estão rodando um protocolo de compartilhamento de arquivos em rede (SMB).

Texto

Descrição gerada automaticamente

There's a share on the user's computer.  What's it called?

Usando o enum4linux para fazer uma enumeração mais completa, é possível achar o sharename pics.

Texto

Descrição gerada automaticamente

User.txt:

Para procurar o arquivo user.txt precisamos nos conectar ao protocolo FTP para transferência de arquivos. Usando o scan agressivo do nmap, podemos encontrar a vulnerabilidade Anonymous, que nos permite conectar ao serviço FTP sem o uso de uma senha.

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Copiando o arquivo “clean.sh”, percebemos uma abertura para executar um comando *Reverse Shell* na linha 7:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Então, iremos substituir o arquivo original pelo arquivo modificado:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Usando NetCat para escutar a porta 9001:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

ROOT.txt:

Texto

Descrição gerada automaticamente

Visto que não temos permissão de root, vamos fazer um *Privilege Escalation*:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Conclusão

Esse CTF trata-se de um desafio de nível fácil e curto. Além disso, é ideal para colocar em prática habilidades de *Port Scanning*, exploração de vulnerabilidades e escalonamento de privilégios.

Referências

* <https://book.hacktricks.xyz/linux-hardening/privilege-escalation>
* <https://www.revshells.com/>
* <https://gtfobins.github.io/gtfobins/env/>