# Laboratório - Criptografar e descriptografar dados usando uma ferramenta de hacker

## Objetivos

**Parte 1: Criar e criptografar arquivos**

**Parte 2: Recuperar senhas de arquivo zip criptografado**

## Histórico/Cenário

E se você trabalhar para uma grande empresa que tinha uma política corporativa sobre mídia removível? Especificamente, ele afirma que apenas documentos compactados criptografados podem ser copiados para unidades flash USB portáteis.

Nesse cenário, o Diretor Financeiro (CFO) está fora da cidade em negócios e entrou em contato com você em pânico com um pedido de ajuda de emergência. Enquanto estava fora da cidade em negócios, ele tentou descompactar documentos importantes de um arquivo zip criptografado em uma unidade USB. No entanto, a senha fornecida para abrir o arquivo zip é inválida. O diretor financeiro contatou você para ver se havia algo que pudesse fazer.

**Nota**: O cenário fornecido é simples e serve apenas como exemplo.

Pode haver algumas ferramentas disponíveis para recuperar senhas perdidas. Isto é especialmente verdadeiro em situações como esta em que o analista de segurança cibernética poderia adquirir informações pertinentes do CFO. A informação pertinente pode ser o tamanho da senha e uma idéia do que poderia ser. Conhecer informações pertinentes ajuda drasticamente ao tentar recuperar senhas.

Exemplos de utilitários e programas de recuperação de senha incluem hashcat, John the Ripper, Lopttcrack e outros. Em nosso cenário, usaremos **fcrackzip**, que é um utilitário Linux simples para recuperar as senhas de arquivos zip criptografados.

Considere que essas mesmas ferramentas podem ser usadas por cibercriminosos para descobrir senhas desconhecidas. Embora eles não tenham acesso a algumas informações pertinentes, com o tempo, é possível descobrir senhas para abrir arquivos zip criptografados. O tempo necessário depende da força da senha e do comprimento da senha. Senhas mais longas e mais complexas (mistura de diferentes tipos de caracteres) são mais seguras.

Neste laboratório, você irá:

- Criar e criptografar arquivos de texto de exemplo.
- Descriptografar o arquivo zip criptografado.

**Nota:** Este laboratório deve ser usado apenas para fins de instrução. Os métodos aqui apresentados NÃO devem ser usados para proteger dados verdadeiramente sensíveis.

## Recursos necessários

- Máquina Virtual CyberOps Workstation

## Instruções

## Parte 1: Criar e Criptografar Arquivos

Nesta parte, você criará alguns arquivos de texto que serão usados para criar arquivos zip criptografados na próxima etapa.

## Etapa 1: Criar arquivos de texto.

a. Inicie a VM CyberOps Workstation.

b. Abra uma janela de terminal. Verifique se você está no diretório home do analyst. Caso contrário, digite **cd ~** no prompt do terminal.

c. Crie uma nova pasta chamada Zip Files usando o comando **mkdir Zip-Files**.

d. Mover para esse diretório usando o comando **cd Zip-Files** .

e. Digite o seguinte para criar três arquivos de texto.

```
[analyst @secOps Zip-Files] $ echo Este é um arquivo de texto de exemplo >
sample-1.txt
[analyst @secOps Zip-Files] $ echo Este é um arquivo de texto de exemplo >
sample-2.txt
[analyst @secOps Zip-Files] $ echo Este é um arquivo de texto de exemplo >
sample-3.txt
```

f. Verifique se os arquivos foram criados usando o comando **ls** .

```
[analyst @secOps Zip-Files] $ ls -l
total 12
-rw-r—r— 1 analyst de 27 de maio de 13 10:58 sample-1.txt
-rw-r—r— 1 analyst de 27 de maio de 13 10:58 sample-2.txt
-rw-r—r— 1 analyst de 27 de maio de 13 10:58 sample-3.txt
```

## Etapa 2: Zip e criptografar os arquivos de texto.

Em seguida, criaremos vários arquivos compactados criptografados usando comprimentos de senha variados. Para fazer isso, todos os três arquivos de texto serão criptografados usando o utilitário **zip** .

a. Crie um arquivo zip criptografado chamado **file-1.zip** contendo os três arquivos de texto usando o seguinte comando:

```
[analyst @secOps Zip Files] $ zip —e file-1.zip exemplo
```

b. Quando for solicitada uma senha, insira uma senha de um caractere de sua escolha. No exemplo, a letra **B** foi inserida. Digite a mesma letra quando solicitado a verificar.

```
[analyst @secOps Zip Files] $ zip -e file-1.zip sample-*
Enter password:
Verify password:
  adicionando: sample-1.txt (armazenado 0%)
  adicionando: sample-2.txt (armazenado 0%)
  adicionando: sample-3.txt (armazenado 0%)
```

c. Repita o procedimento para criar os seguintes 4 outros arquivos

- **file-2.zip**usando uma senha de 2 caracteres de sua escolha. No nosso exemplo, usamos **R2**.
- **file-3.zip**usando uma senha de 3 caracteres de sua escolha. No nosso exemplo, usamos **0B1**.
- **file-4.zip**usando uma senha de 4 caracteres de sua escolha. No nosso exemplo, usamos **Y0Da**.
- **file-5.zip** usando uma senha de 5 caracteres de sua escolha. No nosso exemplo, usamos **C-3P0**.

d. Verifique se todos os arquivos compactados foram criados usando o comando **ls -l f***.

```
[analyst @secOps Zip-Files] $ ls -l f*
-rw-r—r— 1 analyst 643 Maio 13 11:01 file-1.zip
-rw-r—r— 1 analyst analyst 643 13 de maio 11:02 file-2.zip
-rw-r—r— 1analyst analyst 643 13 de maio 11:03 file-3.zip
```

```
-rw-r—r— 1 analyst analyst 643 13 de maio 11:03 file-4.zip
-rw-r—r— 1 analyst analyst 643 13 de maio 11:03 file-5.zip
```

e. Tente abrir um zip usando uma senha incorreta, conforme mostrado.

```
[analyst @secOps Zip Files] $ unzip file-1.zip
Archive: file-1.zip
[file-1.zip] sample-1.txt password:
password incorrect--reenter:
password incorrect--reenter:
   skipping: sample-1.txt incorrect password
[file-1.zip] sample-2.txt password:
password incorrect--reenter:
password incorrect--reenter:
   [file-1.zip] sample-2.txt password:
[file-1.zip] sample-3.txt password:
password incorrect--reenter:
password incorrect--reenter:
   [file-1.zip] sample-3.txt password:
```

## Parte 2: Recuperar senhas criptografadas de arquivos

Nesta parte, você usará o utilitário **fcrackzip** para recuperar senhas perdidas de arquivos compactados criptografados. O Fcrackzip procura cada arquivo zip fornecido para arquivos criptografados e tenta adivinhar a senha usando métodos de força bruta.

A razão pela qual criamos arquivos zip com diferentes comprimentos de senha foi para ver se o comprimento da senha influencia o tempo necessário para descobrir uma senha.

### Etapa 1: Introdução ao fcrackzip

Na janela do terminal, digite o comando **fcrackzip —h** para ver as opções de comando associadas.

Em nossos exemplos, usaremos as opções de comando **—v**, **-u e -l** . A opção -l será listada por último porque especifica o comprimento da senha possível. Sinta-se livre para experimentar outras opções.

### Etapa 2: Recuperando senhas usando fcrackzip

a. Agora tente recuperar a senha do arquivo **file-1.zip**. Lembre-se de que uma senha de um caractere foi usada para criptografar o arquivo. Portanto, use o seguinte comando **fcrackzip** :

```
[analyst @secOps Zip Files] $ fcrackzip -vul 1-4 file-1.zip
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)


PASSWORD FOUND!!!!: pw == B
```

**Observação**: o comprimento da senha pode ter sido definido para menos de 1 a 4 caracteres.

Quanto tempo demora para descobrir a senha?

b. Agora tente recuperar a senha do arquivo **file-2.zip**. Lembre-se de que uma senha de dois caracteres foi usada para criptografar o arquivo. Portanto, use o seguinte comando **fcrackzip** :

```
[analyst @secOps Zip Files] $ fcrackzip –vul 1-4 file-2.zip
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)


SENHA ENCONTRADA!!!: pw == R2
```

Quanto tempo leva para descobrir a senha?

c. Repita o procedimento e recupere a senha do arquivo **file-3.zip**. Lembre-se de que uma senha de três caracteres foi usada para criptografar o arquivo. Tempo para ver quanto tempo leva para descobrir uma senha de 3 letras. Use o seguinte comando **fcrackzip** :

```
[analyst @secOps Zip Files] $ fcrackzip –vul 1-4 file-3.zip
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)


SENHA ENCONTRADA!!!: pw == 0B1
```

Quanto tempo leva para descobrir a senha?

d. Quanto tempo demora para decifrar uma senha de quatro caracteres? Repita o procedimento e recupere a senha do arquivo **file-4.zip**. Tempo para ver quanto tempo leva para descobrir a senha usando o seguinte comando **fcrackzip** :

```
[analyst @secOps Zip Files] $ fcrackzip –vul 1-4 file-4.zip
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)
checking pw X9M~

PASSWORD FOUND!!!!: pw == Y0Da
```

Quanto tempo leva para descobrir a senha?

e. Quanto tempo demora para decifrar uma senha de cinco caracteres? Repita o procedimento e recupere a senha do arquivo **file-5.zip**. O comprimento da senha é de cinco caracteres, então precisamos definir a opção de comando **-l** para **1-5**. Novamente, tempo para ver quanto tempo leva para descobrir a senha usando o seguinte comando **fcrackzip** :

```
[analyst @secOps Zip Files] $ fcrackzip –vul 1-5 file-5.zip
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)
found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)
checking pw C-H*~

PASSWORD FOUND!!!!: pw == C-3P0
```

Quanto tempo leva para descobrir a senha?

f. Recuperar uma senha de 6 caracteres usando fcrackzip

Parece que senhas mais longas levam mais tempo para serem descobertas e, portanto, elas são mais seguras. No entanto, uma senha de 6 caracteres não dissuadiria um criminoso cibernético.

Quanto tempo você acha que o fcrackzip levaria para descobrir uma senha de 6 caracteres?

Para responder a essa pergunta, crie um arquivo chamado **file-6.zip** usando uma senha de 6 caracteres de sua escolha. No nosso exemplo, usamos **JarJar**.

```
[analyst @secOps Zip Files] $ zip –e file-6.zip exemplo
```

g. Repita o procedimento para recuperar a senha do arquivo **file-6.zip** usando o seguinte comando **fcrackzip** :

```
[analyst @secOps Zip Files] $ fcrackzip –vul 1-6 file-6.zip
```

Quanto tempo demora o fcrackzip para descobrir a senha?

A verdade simples é que senhas mais longas são mais seguras porque demoram mais tempo para serem descobertas.

Por quanto tempo você recomendaria uma senha para que ela seja segura?