Packet Tracer – Explore a criptografia de dados e de arquivos

# Objetivos

**Parte 1: Localize as credenciais da conta FTP do notebook da Mary**

**Parte 2: Carregue os dados confidenciais usando FTP**

**Parte 3: Localize as credenciais da conta FTP do computador do Bob**

**Parte 4: Baixe os dados confidenciais usando FTP**

**Parte 5: Descriptografar o conteúdo de um arquivo confidencial**

# Contexto

Nesta atividade, você acessará o conteúdo criptografado de vários arquivos e transferirá um arquivo pela Internet para um servidor FTP centralizado. Em seguida, outro usuário baixará o arquivo do servidor FTP e descriptografará o conteúdo dos arquivos. O endereçamento IP, a configuração de rede e as confirmações de serviço já foram realizados. Você usará os dispositivos clientes nas diferentes regiões geográficas, para transferir um arquivo com os dados criptografados para outro dispositivo.

Para descriptografar o texto e os arquivos nessa atividade, você usará o OpenSSL. OpenSSL é um projeto de código aberto que fornece um kit de ferramentas robusto, comercial e completo para os protocolos Transport Layer Security (TLS) e Secure Sockets Layer (SSL). É também uma biblioteca de criptografia de uso geral.

**Observação**: Embora o OpenSSL seja a biblioteca de criptografia de fato hoje, o uso apresentado neste laboratório NÃO é recomendado para proteção robusta. Abaixo estão dois problemas de segurança com este laboratório:

o    O método descrito neste laboratório usa uma função de derivação de chave fraca. A ÚNICA segurança é introduzida por uma senha muito forte.

o    método descrito neste laboratório não garante a integridade do arquivo de texto.

Esta atividade deve ser usada apenas como uma ferramenta de aprendizagem. Os métodos aqui apresentados NÃO devem ser usados para proteger dados verdadeiramente sensíveis.

# Recursos

O **CSE-LABVM** instalado no VirtualBox

**Observação**: é recomendável usar o **CSE-LABVM** para as tarefas de descriptografia nesta atividade. O **CSE-LABVM** foi instalado durante o **laboratório - Instalar uma máquina virtual em um computador pessoal**.

# Instruções

## Parte 1: Descubra as credenciais de conta de FTP para Mary

O laptop de Mary se chama **Laptop BR-1** na **filial**. Mary tem um documento em seu laptop com as informações de login do FTP criptografadas. O conteúdo deve ser descriptografado para permitir o acesso ao **servidor BR** que está localizado no **armário de cabeamento da filial**.

### Passo 1: Acesse o documento de texto no notebook da Mary.

a.     Clique em **Laptop BR-1** > **Área de trabalho** > **Editor de texto**.

b.     Na janela do **Editor de Texto**, clique em **File > Open**(Arquivo >Abrir).

c.     Clique no documento **maryftplogin.txt** e clique em **OK**.

### Passo 2: Descriptografe as informações da conta FTP da Mary.

a.     Selecione todo o texto no arquivo **maryftplogin.txt** e copie.

b.     Inicie o **CSE-LABVM**.

c.     Clique duas vezes no ícone **Terminal** para abrir um terminal.

d.     Use o comando a seguir para descriptografar o conteúdo do arquivo e revelar as informações de login de FTP para Mary.

cisco@labvm:~$ **echo 'U2FsdGVkX1+sKwL7uceALGKqAQ78WWown3ok73zicO8GLYu2SpMvLEwCB7HsyRC3MeimUjiXRCLwOSSahAraUrnEtkClGK4tytP9hludc6k=' | openssl aes-256-cbc -pbkdf2 -a -d**

Este comando envia o texto criptografado para o aplicativo OpenSSL. A opção **aes-256-cbc** diz ao OpenSSL para usar o sistema de criptografia avançado com um comprimento de chave de 256 bits e encadeamento de blocos de criptografia. A opção **pbkdf2** ativa a Função de derivação de chave com base em senha 2, que aplica um código de autenticação de mensagem com base em hash ou HMAC à senha junto com o salt. A opção **-a** diz ao OpenSSL para codificar a mensagem criptografada usando um método de codificação diferente do Base64 antes de armazenar os resultados em um arquivo. A opção **-d** diz ao aplicativo para descriptografar os dados.

e.     Quando a senha de descriptografia for solicitada, use **maryftp123**.

enter aes-256-cbc encryption password: **maryftp123**

#### Pergunta:

Qual é o nome de usuário e senha da conta FTP da Mary?

Digite suas respostas aqui.

## Parte 2: Carregue os dados confidenciais usando FTP

Mary trabalha para uma agência de cartão de crédito e precisa enviar à agência um arquivo que contenha os dados de alguns clientes. Na parte 2, você verificará se os dados estão criptografados antes de carregá-los no **servidor BR**.

### Passo 1: Visualize o documento confidencial no notebook da Mary.

a.      Volte para o **notebook BR-1.** Abra o **Editor de texto**, se necessário, e clique em **Arquivo** > **Abrir**.

b.     Clique no documento **clientinfo.enc** e clique em **OK**.

#### Pergunta:

Em que forma estão os dados?

Digite suas respostas aqui.

### Passo 2: Conecte-se ao servidor FTP.

a.     Feche o **Editor de texto** e clique no **Prompt de comando**.

b.      No prompt, digite o comando **ftp 10.0.3.30** para se conectar ao **servidor BR.**

c.     Use as credenciais de Mary que você descriptografou cedo para autenticar.

### Passo 3: Carregue um arquivo para o servidor FTP.

a.     No prompt **ftp>** entre o comando **dir** para ver os arquivos atuais armazenados no servidor FTP remoto.

b.     Use o comando **put** para carregar o arquivo **clientInfo.enc** no servidor.

c.     No prompt **ftp>**, digite o comando **dir** e verifique se agora o arquivo **clientinfo.en**c está no servidor FTP.

d.     Insira **quit** para sair da sessão.

#### Pergunta:

Se criminosos virtuais interceptassem a transferência do arquivo pela Internet, o que estaria no texto claro?

Digite suas respostas aqui.

## Parte 3: Localize as credenciais da conta FTP do computador do Bob

Bob precisa acessar o conteúdo do arquivo que Maria armazenou no **BR Server** para verificar algumas informações do cliente. Como Mary, Bob precisa descriptografar as informações de login do FTP para acessar o **BR Server** e baixar o arquivo.

### Passo 1: Acesse o documento de texto no notebook da Mary.

a.     Na **Filial**, clique em **Laptop BR-2** e abra o **Editor de texto**.

b.     Na janela do **Editor de Texto**, clique em **File** > **Open**(Arquivo >Abrir).

c.     Clique no documento **bobftplogin.txt** e clique em **OK**.

### Passo 2: Descriptografe as informações da conta FTP do Bob.

a.     Selecione todo o texto no arquivo **bobftplogin.txt** e copie.

b.     Retorne à janela do terminal no **CSE-LABVM**.

c.     Use o comando a seguir para descriptografar o conteúdo do arquivo e revelar as informações de login de FTP para Bob.

cisco@labvm:~$ **echo 'U2FsdGVkX1/+3jGTemCqs3e4dK8+b0xfXJiq4eoU0lQgRV9aZQPqJCBsYJWc9lDQwiB2svhiWSUVhCRS5qBrjgmDZF3q/dXqaCrZRR5prjE=' | openssl aes-256-cbc -pbkdf2 -a -d**

d.     Quando a senha de descriptografia for solicitada, use **bobftp123**.

Entre com a senha de descriptação aes-256-cbc: **bobftp123**

#### Pergunta:

Qual é o nome de usuário e senha da conta FTP do Bob?

Digite suas respostas aqui.

## Parte 4: Baixe os dados confidenciais usando FTP

Nesta parte, você vai baixar e descriptografar os dados confidenciais armazenados no **BR Server**.

### Passo 1: Conecte-se ao servidor FTP.

a.     Na Filial no laptop BR-2, feche a janela do **Editor de texto** e clique em **Prompt de comando.**

b.      No prompt, digite o comando **ftp 10.0.3.30** para se conectar ao **servidor BR.**

c.      Use as credenciais de Bob que você descriptografou cedo para autenticar.

### Passo 2: Baixe o arquivo para o computador do Bob.

a.     No prompt **ftp>** entre o comando **dir** para ver os arquivos atuais armazenados no **servidor BR**.

b.      Use o comando **get** para baixar o arquivo **clientinfo.enc** do servidor.

c.     Insira **quit** para encerrar a sessão FTP.

d.     No prompt **C:\>**, digite o comando **dir** e verifique se agora o arquivo **clientinfo.enc** está no **Laptop BR-2**.

#### Pergunta:

Se criminosos virtuais interceptassem a transferência do arquivo pela Internet, o que estaria no texto claro?

Digite suas respostas aqui.

## Parte 5: Descriptografar o conteúdo de um arquivo confidencial

Nesta parte, você descriptografará o arquivo **clientinfo.enc**.

### Passo 1: Obter a chave de descriptografia.

Agora que Bob tem o arquivo, ele precisa descriptografá-lo para que possa lê-lo. Anteriormente, Mary enviou um e-mail a Bob com a chave de descriptografia do arquivo. Use o programa de e-mail para recuperar a chave de criptografia do arquivo **clientinfo.enc**.

a.     Feche a janela do **Prompt de comando**, e então clique em **E-mail**.

b.     Clique no E-mail com o assunto “ **Decryption Key** ” (“Chave de Descriptografia”) e anote a chave de descriptografia abaixo.

#### Pergunta:

Qual é a chave de descriptografia para acessar as informações confidenciais no arquivo **clientinfo.txt**?

Digite suas respostas aqui.

### Passo 2: Descriptografe o conteúdo do arquivo clientinfo.txt.

a.     Feche a janela E-mail e clique em **Editor de texto.**

b.     Na janela do Editor de texto, clique em **Arquivo** > **Abrir**, clique no documento **clientinfo.enc** e clique em **OK**.

c.     Selecione todo o texto no arquivo **clientinfo.txt** e copie.

d.      No **CSE-LABVM**, clique no botão **Menu** e, em seguida, clique em **Editor de texto Pluma**.

e.     Clique em **Editar** > **Colar** e, em seguida, clique em **Arquivo** > **Salvar**.

f.      Salve o arquivo com o nome **clientinfo.enc**.

g.     Feche o **Pluma**.

h.     No terminal, insira o comando **ls** para verificar se **clientinfo.enc** está no diretório atual. Caso contrário, navegue até o diretório em que **clientinfo.enc** está armazenado.

i.      Use o comando a seguir para descriptografar o arquivo **clientinfo.enc**.

cisco@labvm:~$ **openssl aes-256-cbc -pbkdf2 -a -d -in clientinfo.enc -out clientinfo.txt**

j.      Quando a senha de descriptografia for solicitada, use a senha que você descobriu no e-mail de Mary.

Entre com a senha de descriptação aes-256-cbc:

cisco@labvm:~$

k.     Insira o comando **ls** para ver se um novo arquivo, **clientinfo.txt**, foi adicionado ao diretório.

l.      Use qualquer método que você deseja abrir o arquivo **clientinfo.txt** para ver o conteúdo descriptografado.

#### Pergunta:

Qual é o primeiro nome da conta no arquivo **clientinfo.txt**?

Digite suas respostas aqui.

Fim do documento