Packet Tracer – Verificações de integridade de arquivos e dados

# Objetivos

**Parte 1: Recuperar arquivos após um ataque cibernético**

**Parte 2: Usando hash para verificar a integridade do arquivo**

**Parte 3: Usando o HMAC para verificar a integridade do arquivo**

# Contexto

Nesta atividade, você verificará a integridade de vários arquivos, usando hashes para assegurar que os arquivos não foram modificados. Se houver suspeita de que foram modificados, os arquivos devem ser enviados para o computador da Sally para futuras análises. 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 verificar e transferir arquivos suspeitos.

**Recursos**

O CSE-LABVM instalado no VirtualBox

**Observação**: é recomendável usar o CSE- LABVM para verificar hashes de arquivos MD5 de arquivo nesta atividade. O CSE-LABVM foi instalado durante o laboratório - Instalar uma máquina virtual em um computador pessoal.

# Instruções

## Parte 1: Recuperar arquivos após um ataque cibernético

Os dados do cliente devem ser protegidos e permanecer inalterados por pessoal não autorizado. Ao fazer a hash dos dados antes e depois do arquivamento, você pode dizer se eles foram alterados mesmo um caractere ou um pouco, porque os hashes não correspondem. Nesta parte, você tentará recuperar arquivos de um backup após um ataque digital.

### Passo 1: Acesse o servidor FTP pelo computador do Mike.

a.     Cliqueem Branch Office e, em seguida, clique em Laptop BR-1.

b.     Clique na guia Desktop (Área de Trabalho) e depois clique em Web Browser (Navegador Web).

c.     Digite a URL http://branch.corp e clique em Go (Ir).

**Observação**: o Packet Tracer pode levar vários segundos para convergir. Você pode clicar em Fast Forward Time para acelerar o processo.

d.     Clique no link para baixar os arquivos mais recentes.

### Passo 2: Copie os valores de hash da última vez que os arquivos foram arquivados.

Você precisa restaurar os arquivos ausentes de um servidor de backup localizado na sede. Mas, primeiro, você precisa dos hashes dos arquivos armazenados para garantir a integridade deles.

a.     Digite a URL http://branch.corpe clique em Go (Ir).

b.     Clique no link para visualizar os arquivos mais recentes e os respectivos hashes.

c.     Selecione e copie todo o conteúdo.

d.     Abra o CSE-LABVMe clique em Menu > Editor de texto Pluma.

e.     Cole o conteúdo da área de transferência no documento em branco. Você usará esses hashes para validar se um arquivo está corrompido.

### Passo 3: Baixar os arquivos do cliente para o computador do Mike.

a.     De volta ao Packet Tracer, feche o navegador da Web e o PC de Mike.

b.     Clique no Command Prompt. Conecte-se ao servidor HQ FTP, inserindo ftp hq.corpno prompt.

c.     Digite o nome do usuário mike e a senha cisco123.

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

e.     Baixe os seis arquivos do cliente (NEclients.txt, NWclients.txt, Nclients.txt, SEclients.txt, SWclients.txt e Sclients.txt) para o PC de Mike. Um exemplo para o primeiro arquivo é mostrado aqui:

ftp> **get NEclients.txt**

Lendo o arquivo NEclients.txt de hq.corp:

File transfer in progress...

[Transfer complete - 584 bytes]

584 bytes copied in 0,05 secs (11680 bytes/sec)

f.      Depois de baixar todos os arquivos, saia da linha de comando do FTP.

g.     Digite o comando dir e verifique se os arquivos do cliente estão agora no Laptop BR-1.

## Parte 2: Usar hash para verificar a integridade do arquivo

Nesta parte, use o CSE-LABVM para hash o conteúdo dos arquivos que você baixou. Você comparará o novo hash com o hash antigo para ver se os dados foram alterados. Todos os arquivos que foram alterados desde que foram arquivados serão enviados para Sally para que ela possa investigar as alterações posteriormente.

### Passo 1: Verifique os hashes nos arquivos do cliente no computador do Mike.

a.     Feche o prompt de comando e clique no editor de texto,

b. Clique     Cliqueem Arquivo > Abrir, selecione o primeiro documento NEclients.txt e clique em OK.

c.     Copie todo o conteúdo do documento de texto.

d.     Abra o CSE-LABVM.

e.     Clique duas vezes no ícone Terminalpara abrir um terminal.

f.      Use o Comando echo -n 'file-content' | md5 sum para criar um hash para validar os dados no arquivo NEclients.txt . Cole o conteúdo da área de transferência entre aspas simples.

cisco@labvm:~$ **echo -n '**file-content**' | md5sum**

g.     Compare o valor de hash criado aqui com os valores de hash que você copiou anteriormente para o documento de texto.

#### Pergunta:

Os dois valores de hash para NEclients.txt são iguais?

Digite suas respostas aqui.

h.     Hash o conteúdo dos cinco arquivos restantes até que um dos valores não corresponda ao hash calculado.

#### Pergunta:

Qual arquivo foi modificado e tem um hash incorreto?

Digite suas respostas aqui.

### Etapa 2: Escalar o ataque digital para a supervisora de Mike, Sally.

a.     Retorne ao Packet Tracer e feche o Editor de texto.

b.     Clique em E-mail e depois em Escrever. Escreva um e-mail e envie para sally@branch.corp para informar que o servidor de arquivos foi invadido.

### Passo 3: Baixe o arquivo suspeito para o computador da Sally.

a.     Volte para HQe clique em HQ-Laptop-1.

b.     Clique na guia Desktop > Prompt de comando e digite ftp hq.corp para se conectar ao servidor FTP do HQ (Sede).

c.     Digite o nome de usuário de sally e uma senha de cisco321.

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

e.     Baixe o arquivo que foi encontrado adulterado na Parte 3, Etapa 1.

f.      No prompt ftp> , digite o comando quit.

g.     No prompt C:\>, digite o comando dir e verifique se o arquivo de cliente adulterado está agora no HQ-Laptop-1 para análise por Sally no futuro.

## Parte 3: Use o HMAC para verificar a integridade do arquivo

Bob é o CFO de uma pequena empresa e monitora todas as finanças. Nesta parte, você computará e verificará um código de autenticação de mensagem baseado em hash (HMAC) de um arquivo essencial para garantir que sejam os mesmos dados desde a última vez que o arquivo foi usado. O HMAC requer uma chave secreta para que a integridade do arquivo possa ser validada.

a.     Clique no laptop de Bob, que é HQ-Laptop-2.

b.     Clique na guia Área de trabalho> Prompt de comando, digite o comando dir e verifique se o arquivo crítico chamado **redimentos.txt** está no laptop. Feche a janela do prompt de comando quando terminar.

c.     Clique em Editor de texto , e em Arquivo > Abrir

d.     Selecione o documento redimentos.txt e clique OK.

e.     Selecione e copie todo o conteúdo do documento.

f.      No CSE-LABVM, clique no botão Menu e, em seguida, clique em Editor de texto Pluma. Clique em Editar e clique em Colar.

g.     Clique em Arquivo e clique em Salvar. Salve o arquivo com o nome redimentos.txt. Feche o arquivo.

h.     Em uma janela de terminal na VM CSE-LABVM, use o seguinte comando para criar um HMAC para o arquivo rendimentos.txt. Digite a chave secreta cisco123.

cisco@labvm:~$ **openssl dgst -sha256 -hmac cisco123 rendimentos.txt**

#### Perguntas:

Qual é o HMAC calculado para o conteúdo do arquivo?

Digite suas respostas aqui.

O uso de HMAC é mais confiável do que o hash geral?

Digite suas respostas aqui.

O hash do HMAC para o arquivo rendimentos.txt corresponde ao hash original que você copiou para o arquivo de texto no CSE-LABVM?

Digite suas respostas aqui.

Fim do documento