

Packet Tracer – Como usar as verificações de integridade de arquivos e dados

Tabela de Endereçamento

Dispositivo	Endereço IP privado	Endereço IP público	Máscara de sub-rede	Site
Servidor FTP/Web	10.44.1.254	209.165.201.3 http://www.cisco.corp	255.255.255.0	Metropolis Bank HQ
Servidor de arquivos de backup	N/D	209.165.201.10 https://www.cisco2.corp	255.255.255.248	Internet
Mike	10.44.2.101	N/D	255.255.255.0	Healthcare at Home
Sally	10.44.1.2	N/D	255.255.255.0	Metropolis Bank HQ
Bob	10.44.1.3	N/D	255.255.255.0	Metropolis Bank HQ

Objetivos

Parte 1: Baixar os arquivos do cliente para o computador do Mike

Parte 2: Baixar os arquivos do cliente do servidor de arquivos de backup para o computador do Mike

Parte 3: Verificar a integridade dos arquivos do cliente usando hash

Parte 4: Verifique a integridade dos arquivos importantes usando HMAC

Histórico

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.

Parte 1: Baixe os arquivos do cliente para o computador do Mike

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

- Clique no site **Gotham Healthcare Branch** e depois clique no computador **Mike**.
- Clique na guia **Desktop (Área de Trabalho)** e depois clique em **Web Browser (Navegador Web)**.
- Digite a URL **http://www.cisco.corp** e clique em **Go (Ir)**.
- Clique no link para baixar os arquivos mais recentes.

Qual protocolo foi usado para acessar essa página da Web no servidor de arquivos de backup? _____

Passo 2: O servidor de arquivos foi invadido, notifique a Sally.

- No site **Gotham Healthcare Branch**, clique no computador **Mike**.

- b. Clique na guia **Desktop** (Área de Trabalho) e depois clique em **E-mail** (E-mail).
- c. Crie um e-mail e envie para Sally@cisco.corp contando sobre o servidor de arquivos.

Parte 2: Baixe os arquivos do cliente do servidor de arquivos de backup para o computador do Mike

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

- a. No site **Gotham Healthcare Branch**, clique no computador **Mike**.
- b. Clique na guia **Desktop** (Área de Trabalho) e depois clique em **Web Browser** (Navegador Web).
- c. Digite a URL **https://www.cisco2.corp** e clique em **Go (Ir)**.
- d. Clique no link para visualizar os arquivos mais recentes e os respectivos hashes.

Qual protocolo foi usado para acessar essa página da Web no servidor de arquivos de backup? _____

Quais são os nomes e hashes dos arquivos do cliente no servidor de backup? (copie e cole-os abaixo)

Passo 2: Baixe os arquivos do cliente para o computador do Mike.

- a. No site **Gotham Healthcare Branch**, clique no computador **Mike**.
- b. Clique na guia **Desktop** (Área de Trabalho) e depois clique em **Command Prompt** (Prompt de Comando).
- c. Conecte-se ao servidor de **arquivos de backup**, digitando **ftp www.cisco2.corp** no prompt de comando.
- d. Digite o nome do usuário **mike** e a senha **cisco123**.
- e. No prompt **ftp>**, digite o comando **dir** para visualizar os arquivos armazenados atualmente no servidor FTP remoto.
- f. Baixe os seis arquivos do cliente (NEclients.txt, NWclients.txt, Nclients.txt, SEclients.txt, SWclients.txt e Sclients.txt) para o computador do Mike, digitando o comando **get FILENAME.txt**, substitua FILENAME pelo nome de um dos seis arquivos do cliente.

```
ftp> get NEclients.txt
```

```
Reading file NEclients.txt from www.cisco2.corp:
File transfer in progress...
```

```
[Transfer complete - 584 bytes]
```

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

- g. Após o download de todos os arquivos, digite o comando **quit** no prompt **ftp>**.

- h. No prompt **PC>**, digite o comando **dir** e verifique se agora os arquivos do cliente estão no computador do Mike.

Parte 3: Verifique a integridade dos arquivos do cliente usando hash

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

- a. No site **Gotham Healthcare Branch**, clique no computador **Mike**.
- b. Clique na guia **Desktop (Área de Trabalho)** e depois clique em **Text Editor (Editor de Texto)**.
- c. Na janela Text Editor (Editor de Texto), clique em **File > Open (Arquivo > Abrir)**.
- d. Clique no primeiro documento **NEclients.txt** e clique em **OK**.
- e. Copie todo o conteúdo do documento de texto.
- f. Abra um navegador da Web em seu computador pessoal e navegue para o site https://www.tools4noobs.com/online_tools/hash/
- g. Clique no espaço em branco e cole no conteúdo do documento de texto. Verifique se o algoritmo está configurado para md2. Clique em **Hash this! (Executar hash!)**.
- h. Para assegurar que um arquivo não foi modificado, você comparará o hash resultante com as informações de nome/hash do arquivo encontradas na Parte 2, Passo 1.
- i. Repita os Passos d até h para cada arquivo do cliente e compare o hash gerado com o hash original mostrado na Parte 2, Passo 1.

Qual arquivo foi modificado e tem um hash incorreto? _____

Passo 2: Baixe o arquivo suspeito para o computador da Sally.

- a. Clique no site **Metropolis Bank HQ** e depois clique no computador **Sally**.
- b. Clique na guia **Desktop (Área de Trabalho)** e depois clique em **Command Prompt (Prompt de Comando)**.
- c. Conecte-se ao servidor de **arquivos de backup**, digitando **ftp www.cisco2.corp** no prompt de comando.
- d. Digite o nome do usuário **sally** e a senha **cisco123**.
- e. No prompt **ftp>**, digite o comando **dir** para visualizar os arquivos armazenados atualmente no servidor FTP remoto.
- f. Baixe o arquivo que foi encontrado modificado na Parte 3, Passo 1.
- g. No prompt **ftp>**, digite o comando **quit**.
- h. No prompt **PC>**, digite o comando **dir** e verifique se agora o arquivo do cliente modificado está no computador da Sally, para ser analisado posteriormente.

Parte 4: Verifique a integridade dos arquivos importantes usando HMAC

Passo 1: Calcule o HMAC de um arquivo importante.

- a. No site **Metropolis Bank HQ**, clique no computador **Bob**.
- b. Clique na guia **Desktop (Área de Trabalho)** e depois clique em **Command Prompt (Prompt de Comando)**.
- c. No prompt **PC>**, digite o comando **dir** e verifique se o arquivo crítico denominado **income.txt** está no computador do Bob.

- d. Na guia **Desktop (Área de Trabalho)**, clique em **Text Editor (Editor de Texto)**.
- e. Na janela Text Editor (Editor de Texto), clique em **File > Open (Arquivo > Abrir)**.
- f. Clique no documento **income.txt** e clique em **OK**.
- g. Copie todo o conteúdo do documento de texto.
- h. Abra um navegador da Web em seu computador pessoal e navegue para o site <http://www.freeformatter.com/hmac-generator.html>
- i. Clique no espaço em branco e cole no conteúdo do documento de texto. Digite a chave secreta **cisco123**. Verifique se o algoritmo está configurado para **SHA1**. Clique em **Compute HMAC (Calcular HMAC)**.

Qual é o HMAC calculado para o conteúdo do arquivo?

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

Passo 2: Verifique o HMAC calculado.

- a. No site **Metropolis Bank HQ**, clique no computador **Bob**.
- b. Clique na guia **Desktop (Área de Trabalho)** e depois clique em **Web Browser (Navegador Web)**.
- c. Digite a URL **https://www.cisco2.corp** e clique em **Go (Ir)**.
- d. Clique no link para visualizar os arquivos mais recentes e os respectivos hashes.

O hash HMAC para o arquivo income.txt file coincide? _____

Pontuação Sugerida

Seção da Atividade	Etapas da Pergunta	Pontos Possíveis	Pontos Obtidos
Parte 1: Baixar os arquivos do cliente para o computador do Mike	Etapa 1	2	
Parte 2: Baixar os arquivos do cliente do servidor de arquivos de backup para o computador do Mike	Etapa 1	2	
	Etapa 1	6	
Parte 3: Verificar a integridade de arquivos do cliente usando hash	Etapa 1	5	
Parte 4: Verificar a integridade de arquivos importantes usando HMAC	Etapa 1	5	
	Etapa 1	5	
	Etapa 2	5	
Perguntas		30	
Pontuação do Packet Tracer		70	
Pontuação Total		100	