

Packet Tracer — Usando verificações de integridade de ficheiros e dados

Tabela de endereçamento

Dispositivo	Endereço IP Privado	Endereço IP Público	Máscara de sub-rede	Local
Servidor FTP/Web	10.44.1.254	209.165.201.3 http://www.cisco.corp	255.255.255.0	Metropolis Bank HQ
Servidor de ficheiros de Backup	N/A	209.165.201.10 https://www.cisco2.corp	255.255.255.248	Internet
Mike	10.44.2.101	N/A	255.255.255.0	Healthcare at Home
Sally	10.44.1.2	N/A	255.255.255.0	Metropolis Bank HQ
Bob	10.44.1.3	N/A	255.255.255.0	Metropolis Bank HQ

Objetivos

Parte 1: Descarregue os ficheiros do cliente para o PC do Mike

Parte 2: Descarregue os ficheiros do cliente, a partir do servidor de ficheiros de backup, para o PC do Mike

Parte 3: Verifique a integridade dos ficheiros do cliente usando Hashing

Parte 4: Verifique a integridade dos ficheiros críticos usando o HMAC

Contexto

Nesta atividade, você verificará a integridade de vários ficheiros usando hashes para garantir que os ficheiros não foram adulterados. Se algum ficheiro for suspeito de ser adulterado, eles devem ser enviados para o PC da Sally para análise posterior. O endereçamento IP, a configuração de rede e as configurações de serviço já foram realizados. Você usará os dispositivos cliente nas diferentes regiões geográficas para verificar e transferir quaisquer ficheiros suspeitos.

Parte 1: Descarregue os ficheiros do cliente para o PC do Mike

Passo 1. Aceda ao servidor FTP a partir do PC do Mike.

- Clique em **Gotham Healthcare Branch** e depois clique no computador do **Mike**.
- Clique na aba **Desktop** e de seguida clique em **Web Browser**.
- Digite o URL **http://www.cisco.corp** e clique em **Go**.
- Clique na ligação para transferir os ficheiros mais recentes.

Que protocolo foi usado para aceder a esta página no servidor de ficheiros de backup? _____

Passo 2. O servidor de ficheiros foi comprometido, avise a Sally.

- Dentro do **Gotham Healthcare Branch**, clique no PC do **Mike**.

- b. Clique na aba **Desktop** e depois clique em **Email**.
- c. Crie um e-mail e envie-o para Sally@cisco.corp e conte-lhe sobre o Servidor de ficheiros.

Parte 2: Descarregue os ficheiros de cliente do servidor de ficheiros de backup para o PC do Mike

Passo 1. Aceda ao servidor FTP externo a partir do PC do Mike.

- a. Dentro do **Gotham Healthcare Branch**, clique no PC do **Mike**.
- b. Clique na aba **Desktop** e de seguida clique em **Web Browser**.
- c. Digite o URL **http://www.cisco.corp** e clique em **Go**.
- d. Clique no link para visualizar os ficheiros mais recentes e seus respetivos hashes.

Que protocolo foi usado para aceder a esta página no servidor de ficheiros de backup? _____

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

Passo 2. Descarregue os ficheiros do cliente para o PC do Mike

- a. Dentro do **Gotham Healthcare Branch**, clique no PC do **Mike**.
- b. Clique na aba **Desktop** e depois em **Command Prompt**.
- c. Ligue-se ao servidor **de ficheiros de backup** usando o comando **ftp www.cisco2.corp** no prompt da linha de comandos.
- d. Introduza o nome de utilizador **mike** e a senha **cisco123**.
- e. No prompt **ftp>** introduza o comando **dir** para ver os ficheiros armazenados no servidor FTP remoto.
- f. Baixe os seis ficheiros de cliente (NEclients.txt, NWclients.txt, Nclients.txt, SEclients.txt, SWclients.txt e Sclients.txt) para o PC de Mike inserindo o comando **get FILENAME.txt**, substitua FILENAME por um dos seis nomes de ficheiro 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. Depois de descarregar todos os ficheiros, digite o comando **quit** no prompt **ftp>**.
- h. No prompt **PC**, digite o comando **dir** e verifique se os ficheiros de cliente estão agora no PC do Mike.

Parte 3: Verifique a integridade dos ficheiros do cliente usando Hashing

Passo 1. Verifique os hashes nos ficheiros do cliente no PC do Mike.

- Dentro do **Gotham Healthcare Branch**, clique no PC do **Mike**.
- Clique na aba **Desktop** e depois clique em **Text Editor**.
- Na janela do editor de texto, clique em **File > Open**.
- Clique no primeiro documento **NEclients.txt** e clique em **OK**.
- Copie todo o conteúdo do documento de texto.
- Abra um navegador web no seu computador pessoal e navegue até o site https://www.tools4noobs.com/online_tools/hash/
- Clique no espaço em branco e cole o conteúdo do documento de texto. Certifique-se de que o algoritmo está definido como md2. Clique em **Hash this!**.
- Para garantir que um ficheiro não foi adulterado, vai comparar o hash resultante com as informações de nome de ficheiro/hash que encontrou na Parte 2, Passo 1.
- Repita os passos d até h para cada ficheiro de cliente e compare o hash gerado com o hash original mostrado na Parte 2, Passo 1.

Que ficheiro foi adulterado e tem um hash incorreto? _____

Passo 2. Descarregue o ficheiro suspeito para o PC da Sally.

- Clique no **Metropolis Bank HQ** e, em seguida, clique no PC da **Sally**.
- Clique na aba **Desktop** e depois em **Command Prompt**.
- Ligue-se ao servidor **de ficheiros de backup** usando o comando **ftp www.cisco2.corp** no prompt da linha de comandos.
- Introduza o nome de utilizador **sally** e a senha **cisco123**.
- No prompt **ftp>** introduza o comando **dir** para ver os ficheiros armazenados no servidor FTP remoto.
- Descarregue o ficheiro que foi determinado ter sido adulterado na parte 3, passo 1.
- No prompt **ftp>** introduza o comando **quit**.
- No prompt **PC**, insira o comando **dir** e verifique se o ficheiro do cliente adulterado está agora no PC da Sally para análise posterior.

Parte 4: Verificar a integridade de ficheiros críticos usando o HMAC

Passo 1. Calcular o HMAC de um ficheiro crítico.

- Dentro do **Metropolis Bank HQ** clique no PC do **Bob**.
- Clique na aba **Desktop** e depois em **Command Prompt**.
- No prompt **PC>**, digite o comando **dir** e verifique se o ficheiro crítico chamado **income.txt** está no PC do Bob.
- Na aba **Desktop**, clique em **Text Editor**.
- Na janela do editor de texto, clique em **File > Open**.
- Clique no documento **income.txt** e clique em **OK**.

- g. Copie todo o conteúdo do documento de texto.
- h. Abra um navegador web no seu computador pessoal e navegue até o site <http://www.freeformatter.com/hmac-generator.html>
- i. Clique no espaço em branco e cole o conteúdo do documento de texto. Introduza a chave secreta **cisco123**. Certifique-se de que o algoritmo está definido para **SHA1**. Clique em **Compute HMAC**. Qual é o HMAC computado para o conteúdo do ficheiro?

Porque é que usar o HMAC é mais seguro do que um simples hashing?

Passo 2. Verifique o HMAC calculado.

- a. Dentro do **Metropolis Bank HQ** clique no PC do **Bob**.
- b. Clique na aba **Desktop** e de seguida clique em **Web Browser**.
- c. Digite o URL **http://www.cisco.corp** e clique em **Go**.
- d. Clique no link para visualizar os ficheiros mais recentes e seus hashes.

O hash HMAC para o ficheiro income.txt corresponde? _____

Pontuação Sugerida

Secção da Atividade	Localização da Questão	Pontos Possíveis	Pontos Ganhos
Parte 1: Descarregar os ficheiros do cliente para o PC do Mike	Passo 1	2	
Parte 2: Descarregar os ficheiros do cliente do servidor de ficheiros de backup para o PC do Mike	Passo 1	2	
	Passo 1	6	
Parte 3: Verificar a integridade dos ficheiros do cliente usando hashing	Passo 1	5	
Parte 4: Verificar a integridade dos ficheiros críticos usando o HMAC	Passo 1	5	
	Passo 1	5	
	Passo 2	5	
Perguntas		30	
Pontuação do Packet Tracer		70	
Pontuação Total		100	