

# Packet Tracer – Utiliser des vérifications d'intégrité des données et des fichiers

## Table d'adressage

Appareil	Adresse IP privée	Adresse IP publique	Masque de sous-réseau	Site
FTP/Serveur web	10.44.1.254	209.165.201.3 http://www.cisco.corp	255.255.255.0	Metropolis Bank HQ
Serveur de sauvegarde des fichiers	S/O	209.165.201.10 https://www.cisco2.corp	255.255.255.248	Internet
Mike	10.44.2.101	S/O	255.255.255.0	Healthcare at Home
Sally	10.44.1.2	S/O	255.255.255.0	Metropolis Bank HQ
Bob	10.44.1.3	S/O	255.255.255.0	Metropolis Bank HQ

## Objectifs

**Partie 1 : Télécharger les fichiers clients sur le PC de Mike**

**Partie 2 : Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le PC de Mike**

**Partie 3 : Vérifier l'intégrité des fichiers clients à l'aide du hash**

**Partie 4 : Vérifier l'intégrité des fichiers sensibles à l'aide du HMAC**

## Contexte

Durant cette activité, vous vérifierez l'intégrité de plusieurs fichiers à l'aide des hashes pour vous assurer que les fichiers n'ont pas été falsifiés. Si vous suspectez un fichier d'avoir été falsifié, vous devez l'envoyer sur le PC de Sally pour une analyse approfondie. L'adresse IP, le réseau et le service ont déjà été configurés. Vous utiliserez les appareils du client dans différentes régions géographiques pour vérifier et transférer les fichiers suspects.

## Partie 1 : Télécharger les fichiers clients sur le PC de Mike

### Étape 1 : Accédez au client de messagerie sur le PC de Mike.

- Cliquez sur le site **Gotham Healthcare Branch**, puis sur le PC **Mike**.
- Cliquez sur l'onglet **Poste de travail**, puis sur **Navigateur web**.
- Saisissez l'URL **http://www.cisco.corp**, puis cliquez sur **Go**.
- Cliquez sur le lien pour télécharger les fichiers les plus récents.

Quel protocole a été utilisé pour accéder à cette page web sur le serveur de sauvegarde des fichiers ? \_\_\_

### Étape 2 : Le serveur de fichiers a été piraté. Avertissez Sally.

- Sur le site **Gotham Healthcare Branch**, cliquez sur le PC **Mike**.
- Cliquez sur l'onglet **Poste de travail**, puis sur **Messagerie**.
- Créez un e-mail et envoyez-le à [Sally@cisco.corp](mailto:Sally@cisco.corp) pour l'avertir du piratage du serveur de fichiers.

## Partie 2 : Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le PC de Mike

### Étape 1 : Accédez au serveur FTP hors site sur le PC de Mike.

- Sur le site **Gotham Healthcare Branch**, cliquez sur le PC **Mike**.
- Cliquez sur l'onglet **Poste de travail**, puis sur **Navigateur web**.
- Saisissez l'URL **https://www.cisco2.corp**, puis cliquez sur **Go**.
- Cliquez sur le lien pour afficher les fichiers les plus récents et leurs hashes.

Quel protocole a été utilisé pour accéder à cette page web sur le serveur de sauvegarde des fichiers ? \_\_\_

Quels sont les noms et hashes des fichiers clients sur le serveur de sauvegarde ? (Copiez et collez-les ci-dessous.)

---

---

---

---

---

---

---

---

### Étape 2 : Téléchargez les fichiers clients sur le PC de Mike.

- Sur le site **Gotham Healthcare Branch**, cliquez sur le PC **Mike**.
- Cliquez sur l'onglet **Poste de travail**, puis sur **Invite de commande**.
- Connectez-vous au serveur **Fichier de sauvegarde** en saisissant **ftp www.cisco2.corp** sur l'invite de commande.
- Saisissez le nom d'utilisateur **mike** et le mot de passe **cisco123**.
- À l'invite **ftp>**, saisissez la commande **dir** pour afficher les fichiers actuellement stockés sur le serveur FTP à distance.
- Téléchargez les six fichiers clients (**NEclients.txt**, **NWclients.txt**, **Nclients.txt**, **SEclients.txt**, **SWclients.txt** et **Sclients.txt**) sur le PC de Mike en saisissant la commande **get FILENAME.txt**. Remplacez **FILENAME** par l'un des six noms de fichiers clients.

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

```
Lecture du fichier NEclients.txt depuis www.cisco2.corp :  
Transfert du fichier en cours...
```

```
[Transfert terminé - 584 octets]
```

```
584 octets copiés en 0,05 seconde (11680 octets/sec)
```

- Une fois que vous avez téléchargé tous les fichiers, saisissez la commande **quit** à l'invite **ftp>**.
- À l'invite **PC>**, saisissez la commande **dir** et vérifiez que les fichiers clients se trouvent désormais sur le PC de Mike.

## Partie 3 : Vérifier l'intégrité des fichiers clients à l'aide du hash

### Étape 1 : Vérifiez les hashes sur les fichiers clients sur le PC de Mike.

- Sur le site **Gotham Healthcare Branch**, cliquez sur le PC **Mike**.
- Cliquez sur l'onglet **Poste de travail**, puis sur **Éditeur de texte**.
- Dans la fenêtre de l'éditeur de texte, cliquez sur **Fichier > Ouvrir**.
- Cliquez sur le premier document **NEclients.txt**, puis sur **OK**.
- Copiez l'intégralité du contenu du document texte.
- Ouvrez un navigateur web sur votre ordinateur, puis rendez-vous sur le site [https://www.tools4noobs.com/online\\_tools/hash/](https://www.tools4noobs.com/online_tools/hash/).
- Cliquez dans le champ vide, puis collez le contenu du document texte dans ce champ. Vérifiez que l'algorithme sélectionné est bien md2. Cliquez sur **Hasher le contenu**.
- Pour vous assurer que le fichier n'a pas été modifié, comparez le hash obtenu avec les informations relatives au nom du fichier et au hash fournies à l'étape 1 de la partie 2.
- Répétez les étapes de d à h pour chaque fichier client, puis comparez le hash généré avec le hash d'origine fourni à l'étape 1 de la partie 2.

Quel fichier a été modifié et présente un hash incorrect ? \_\_\_\_\_

### Étape 2 : Téléchargez le fichier suspect sur l'ordinateur de Sally.

- Cliquez sur le site du **siège social de la Metropolis Bank**, puis sur l'ordinateur de **Sally**.
- Cliquez sur l'onglet **Poste de travail**, puis sur **Invite de commande**.
- Connectez-vous au serveur **Fichier de sauvegarde** en saisissant **ftp www.cisco2.corp** sur l'invite de commande.
- Saisissez le nom d'utilisateur **sally**, puis le mot de passe **cisco123**.
- À l'invite **ftp>**, saisissez la commande **dir** pour afficher les fichiers actuellement stockés sur le serveur FTP à distance.
- Téléchargez le fichier modifié identifié à l'étape 1 de la partie 3.
- À l'invite **ftp>**, saisissez la commande **quit**.
- À l'invite **PC>**, saisissez la commande **dir**, puis vérifiez que le fichier client modifié se trouve bien sur l'ordinateur de Sally, où il pourra être analysé ultérieurement.

## Partie 4 : Vérifier l'intégrité des fichiers sensibles à l'aide du HMAC

### Étape 1 : Calculez le HMAC d'un fichier sensible.

- Sur le site **Metropolis Bank HQ**, cliquez sur le PC **Bob**.
- Cliquez sur l'onglet **Poste de travail**, puis sur **Invite de commande**.
- À l'invite **PC>**, saisissez la commande **dir**, puis vérifiez que le fichier **income.txt** se trouve bien sur l'ordinateur de Bob.
- Sous l'onglet **Bureau**, cliquez sur **Éditeur de texte**.
- Dans la fenêtre de l'éditeur de texte, cliquez sur **Fichier > Ouvrir**.
- Cliquez sur le document **income.txt**, puis sur **OK**.

- g. Copiez l'intégralité du contenu du document texte.
- h. Ouvrez un navigateur web sur votre ordinateur, puis rendez-vous sur le site <http://www.freeformatter.com/hmac-generator.html>.
- i. Cliquez dans le champ vide, puis collez le contenu du document texte dans ce champ. Saisissez la clé secrète **cisco123**. Vérifiez que l'algorithme sélectionné est bien **SHA1**. Cliquez sur **Calculer le HMAC**.

Quel HMAC obtenez-vous pour le contenu du fichier ?

---

Pourquoi est-il plus sûr d'utiliser le HMAC que le hash basique ?

---

### Étape 2 : Vérifiez le HMAC calculé.

- a. Sur le site **Metropolis Bank HQ**, cliquez sur le PC **Bob**.
- b. Cliquez sur l'onglet **Poste de travail**, puis sur **Navigateur web**.
- c. Saisissez l'URL **https://www.cisco2.corp**, puis cliquez sur **Go**.
- d. Cliquez sur le lien pour afficher les derniers fichiers et leur hash.

Le hash HMAC obtenu correspond-il à celui du fichier income.txt ? \_\_\_\_\_

### Suggestion de barème de notation

Section d'exercice	Emplacement de la question	Nombre maximum de points	Points obtenus
Partie 1 : Télécharger les fichiers du client sur l'ordinateur de Mike	Étape 1	2	
Partie 2 : Télécharger les fichiers du client depuis le serveur de fichiers de sauvegarde vers l'ordinateur de Mike	Étape 1	2	
	Étape 1	6	
Partie 3 : Vérifier l'intégrité des fichiers des clients à l'aide du hash	Étape 1	5	
Partie 4 : Vérifier l'intégrité des fichiers sensibles à l'aide du HMAC.	Étape 1	5	
	Étape 1	5	
	Étape 2	5	
<b>Questions</b>		<b>30</b>	
<b>Score relatif à Packet Tracer</b>		<b>70</b>	
<b>Score total</b>		<b>100</b>	