créer un monde numérique

Appliquer les règles de sécurité

Table des matières

[Introduction : **Erreur ! Signet non défini.**](#_Toc187138224)

[1. Premier pka : **Erreur ! Signet non défini.**](#_Toc187138225)

[1.1 Configurer le serveur FTP : **Erreur ! Signet non défini.**](#_Toc187138226)

[1.2 Vérifier le service http : **Erreur ! Signet non défini.**](#_Toc187138227)

[1.3 Configurer le serveur DNS : **Erreur ! Signet non défini.**](#_Toc187138228)

[1.4 Configuration du serveur NTP : **Erreur ! Signet non défini.**](#_Toc187138229)

[1.5 Configurer le serveur AAA : **Erreur ! Signet non défini.**](#_Toc187138230)

[2. Second pka : **Erreur ! Signet non défini.**](#_Toc187138231)

[1.6 Charger des fichiers à l’aide du FTP **Erreur ! Signet non défini.**](#_Toc187138232)

[1.7 Accéder à un routeur d’entreprise à distance à l’aide de Telnet **Erreur ! Signet non défini.**](#_Toc187138233)

[1.8 Accéder à un routeur d’entreprise à distance avec Telnet : **Erreur ! Signet non défini.**](#_Toc187138234)

[1.9 Accéder à un routeur d’entreprise à distance : **Erreur ! Signet non défini.**](#_Toc187138235)

[3. Troisième pka : **Erreur ! Signet non défini.**](#_Toc187138236)

[1.10 Localiser les informations d’identification du compte FTP de l’ordinateur portable de Mary : **Erreur ! Signet non défini.**](#_Toc187138237)

[1.11 Charger des données confidentielles par FTP : **Erreur ! Signet non défini.**](#_Toc187138238)

[1.12 Localiser les informations d’identification FTP de bob : **Erreur ! Signet non défini.**](#_Toc187138239)

[4. Quatrième pka : **Erreur ! Signet non défini.**](#_Toc187138240)

[1.13 Télécharger les fichiers clients sur le pc de Mike : **Erreur ! Signet non défini.**](#_Toc187138241)

[1.14 Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le pc de Mike : **Erreur ! Signet non défini.**](#_Toc187138242)

[1.15 Vérifier l’intégrité des fichiers clients avec le hash : **Erreur ! Signet non défini.**](#_Toc187138243)

[1.16 Vérifier l’intégrité des fichiers sensibles à l’aide du HMAC : **Erreur ! Signet non défini.**](#_Toc187138244)

[5. Cinquième pka : **Erreur ! Signet non défini.**](#_Toc187138245)

[1.17 Configurer le WEP pour Healthcare at Home: **Erreur ! Signet non défini.**](#_Toc187138246)

[1.18 Configurer le protocole WPA2 RADIUS pour le siège social de Metropolis Bank : **Erreur ! Signet non défini.**](#_Toc187138247)

[6. Sixième pka : **Erreur ! Signet non défini.**](#_Toc187138248)

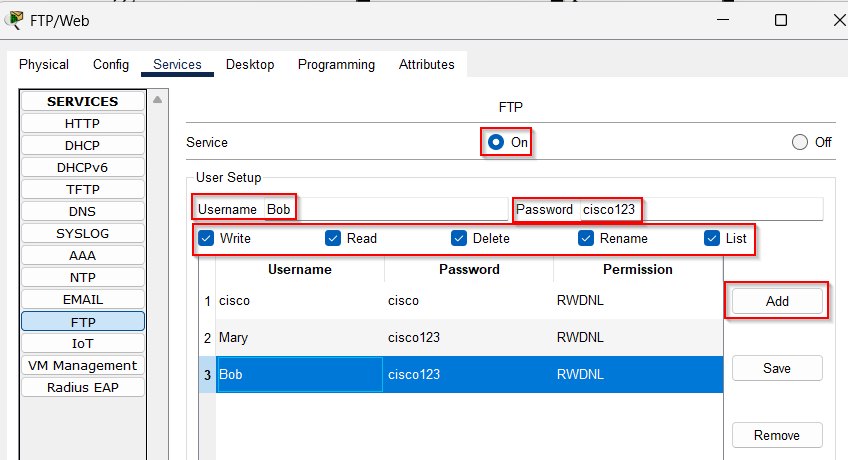
[1.19 Envoyer du trafic FTP non chiffré : **Erreur ! Signet non défini.**](#_Toc187138249)

# Introduction :

Ce TP a pour objectif de me familiariser avec la configuration et l’administration des principaux services réseau tels que le FTP, le DNS, le NTP, le serveur web et les services de messagerie. À travers des scénarios cisco, il me permet de comprendre le rôle et l’importance de chaque service. Ce TP, permet d’acquérir des compétences pratiques dans le déploiement, de gestion des accès et de sécurisation des services.

# Premier PKA :

## Configurer le serveur FTP :



J’active le service FTP en sélectionnant l'option "On". Cela permet d'autoriser les connexions FTP sur le système. Ensuite, j'ajoute un utilisateur avec le nom "Bob" et le mot de passe "cisco123". Je coche les permissions "Write", "Read", "Delete", "Rename", et "List" pour lui donner un contrôle complet sur les fichiers. Cette configuration est utile pour permettre à l'utilisateur Bob de gérer les fichiers sans restriction. Enfin, je clique sur "Add" pour sauvegarder les informations de cet utilisateur.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Cette liste réçapitule les utilisateurs enregistrés pour le service FTP, avec leurs noms d'utilisateur, mots de passe, et permissions. Par exemple, l'utilisateur "Bob" a le mot de passe "cisco123" et des permissions complètes (RWDNL). Cela permet de vérifier rapidement les droits assignés à chaque utilisateur et de s'assurer qu'ils sont configurés correctement pour leurs besoins.

a) Un service FTP transfert des fichiers entre un client et un serveur via un réseau en utilisant un protocole standardisé.

b) Ce type de service décide qui peut lire, écrire, supprimer, renommer et lister les fichiers de la banque. Ça permet d’éviter que des informations sensibles contenues dans les fichiers soient accessible par tout le monde et évite une diffusion de ses données et évite que des hackeurs puissent s’en servir contre des clients pour leurs soutirer de l’argent.

c) Les autorisations RWDNL sur un serveur FTP définissent les actions qu'un utilisateur peut effectuer sur les fichiers et répertoires :

R pour read : lire ou télécharger un fichier depuis le serveur.

W pour write : écrire ou téléverser un fichier sur le serveur.

D pour delete : supprimer des fichiers ou des répertoires.

N pour rename : renommer des fichiers ou des répertoires.

L pour list : lister les fichiers et répertoires sur le serveur.

Ces droits sont appelés permissions utilisateur. Les permissions utilisateur servent à définir et contrôler les actions qu'un utilisateur peut effectuer sur un système, un fichier ou une ressource. Dans le contexte d’un serveur FTP, elles définissent qui peut lire, écrire, supprimer ou gérer les fichiers et répertoires.

d) Les droits ne sont pas spécifiques au service FTP. Ils reflètent une logique universelle de gestion des permissions dans les systèmes informatiques.

Systèmes de fichiers (OS)

Exemples : Windows et Linux.

Droits équivalents :

R : Lire un fichier ou un répertoire.

W : Modifier ou créer des fichiers.

X : Exécuter un fichier ou accéder à un répertoire (Linux).

D : Supprimer un fichier ou un répertoire.

List : Lister le contenu d’un répertoire.

Ces droits gérent les accès utilisateur dans des environnements partagés.

Bases de données

Exemple : PostgreSQL.

Droits équivalents :

SELECT : Lire les données.

INSERT : Ajouter ou modifier des données.

DELETE : Supprimer des données.

RENAME : Renommer des tables ou des colonnes.

SHOW : Lister les bases, tables ou colonnes.

Les permissions permettent un contrôle précis des interactions des utilisateurs avec les données.

Partage de fichiers en réseau

Exemple : SMB.

Droits équivalents :

Lecture seule : Accéder aux fichiers partagés.

Lecture/Écriture : Modifier ou ajouter des fichiers.

Supprimer : Effacer des fichiers partagés.

Lister le contenu : Voir les fichiers disponibles dans un dossier partagé.

Ces droits sont courants pour les ressources partagées au sein d’un réseau loçal ou d’une organisation.

Appliçations web et cloud

Exemple : Google Drive.

Droits équivalents :

Lecture : Consulter les fichiers ou documents.

Édition : Modifier ou créer des fichiers.

Suppression : Supprimer des fichiers.

Partage : Gérer les droits d'accès pour d'autres utilisateurs.

Ces permissions sont utilisées pour la collaboration et la gestion des droits d’accès au contenu.

Contrôle d’accès dans les systèmes d’information

Exemple : Active Directory.

Droits équivalents :

Accès en lecture : Consulter les informations d’un utilisateur ou d’un groupe.

Modifiçation : Mettre à jour les attributs des utilisateurs.

Suppression : Supprimer des comptes ou des groupes.

Ces droits gèrent l'authentifiçation et les autorisations dans une organisation.

Configurer le serveur web :

Activer le service http :

Une image contenant texte, Police, nombre, logiciel

Description générée automatiquement

J'active les options HTTP et HTTPS en sélectionnant "On" pour chacune. Cela permet de prendre en charge les connexions HTTP et HTTPS pour les services web. Activer HTTPS est particulièrement important pour sécuriser les communiçations via un chiffrement SSL/TLS.

## Vérifier le service http :

Une image contenant texte, logiciel, capture d’écran, ligne

Description générée automatiquement

J'essaie d'accéder à l’URL http://www.cisco.corp, mais le message "Host Name Unresolved" s'affiche. Cela signifie que le serveur DNS n'est pas configuré ou qu'il ne peut pas résoudre le nom de domaine en adresse IP.

Une image contenant texte, logiciel, ligne, capture d’écran

Description générée automatiquement

J’entre l’adresse IP 10.44.1.254 dans le navigateur, mais je reçois un message "Request Timeout". Cela indique que la connexion à cette adresse IP échoue, probablement en raison d'un problème de configuration réseau ou d'un service inactif à cette adresse.

a)

Une image contenant texte, capture d’écran, ligne, Tracé

Description générée automatiquement

L’adresse DNS par default est bien la même que celle du serveur DNS. Mais Sally n’a pas de passerelle par défaut ni d’adresse IP.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Ipconfig /renew permet de renouveler l’adresse IP, le masque de sous-réseau, la passerelle par défaut et le serveur DNS.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

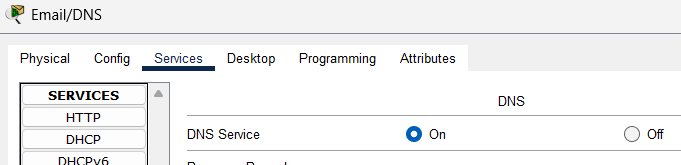
J’accède au serveur web en utilisant l'URL http://10.44.1.254. La page s'affiche correctement, confirmant que le service HTTP est actif et que la configuration réseau est correcte.

Evaluation :

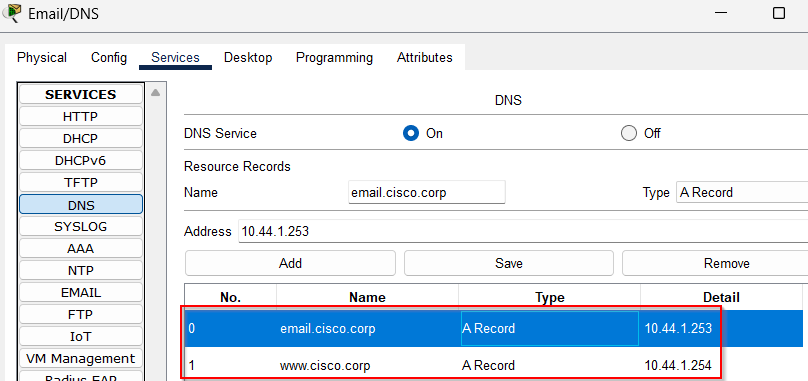
a) Les serveurs FTP/Web, Email/DNS et NTP/AAA sont sur le même réseau, une attaque sur un serveur pourrait se propager facilement aux autres. Ill faudrait les segmenter pour éviter que les hackeurs aient accès à tous les serveurs au lieu d’un seul s’ils sont séparés.

Il n’y a pas de serveur redondant des services FTP/Web, Email/DNS et NTP/AAA pour une disponibilité en ças de panne de l’un des serveurs.

## Configurer le serveur DNS :



J’active le service DNS en sélectionnant l'option "On". Ca permet de résoudre les noms de domaine en adresses IP. Cette activation est essentielle pour que les noms comme "www.cisco.corp" puissent être traduits en adresses réseau.



Je configure deux enregistrements DNS . Le premier associe le nom email.cisco.corp à l'adresse IP 10.44.1.253. Le second relie www.cisco.corp à l'adresse IP 10.44.1.254. Ces enregistrements permettent de rediriger les requêtes DNS vers les adresses IP appropriées pour accéder aux services correspondants.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

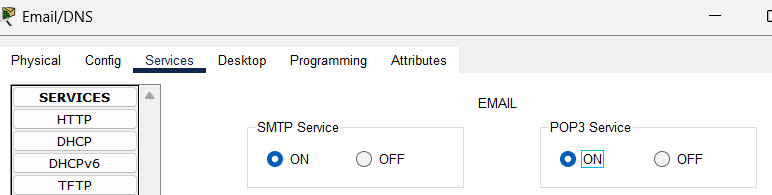
Je teste l'URL http://www.cisco.corp après la configuration DNS. La page s'affiche correctement, confirmant que le serveur DNS fonctionne bien et que le nom de domaine est résolu en adresse IP. Cela prouve que la configuration DNS est tout à fait opérationnelle.

a) On a fait le lien entre le nom de domaine et l’adresse IP 10.44.1.254 Le DNS comprends que 10.44.1.254 et doit amener au même endroit.

b) Le service DNS traduit les noms de domaine en adresses IP pour permettre la communiçation sur un réseau.

c) Metropolis Bank peut se servir du DNS pour que ce soit plus facile à écrire et à retenir pour arriver sur les sites voulu plus rapidement.

Configuration du serveur messagerie :



J’active les services SMTP et POP3 en sélectionnant "ON" pour les deux. Le service SMTP permet d'envoyer des emails, tandis que POP3 est utilisé pour recevoir les messages. Ces services sont nécessaires pour configurer une communiçation email complète au sein du réseau.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Je configure le service email. J'ajoute le nom de domaine cisco.corp et je crée un utilisateur "mike" avec le mot de passe "cisco123". En cliquant sur le bouton "+" après avoir entré ces informations, j'ajoute cet utilisateur à la liste. Cette configuration permet à plusieurs utilisateurs d'avoir des comptes email personnalisés liés au domaine.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Je configure un client email pour Sally. J'entre son nom, son adresse email (sally@cisco.corp), ainsi que les informations des serveurs entrant (POP3) et sortant (SMTP), tous deux configurés à email.cisco.corp. Enfin, je renseigne le nom d'utilisateur "sally" et son mot de passe. Cela permet à Sally d'envoyer et de recevoir des emails via le domaine configuré.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Je configure le client email pour Bob. Les étapes sont similaires : je saisis son nom, son adresse email (bob@cisco.corp), les informations des serveurs email (entrant et sortant) et ses identifiants de connexion. Cette configuration assure que Bob peut également utiliser son compte pour gérer ses emails.

a) Pour activer un service de messagerie, on doit utiliser SMTP et POP3, çar ces deux protocoles ont des rôles différents mais complémentaires. SMTP sert à envoyer les emails, que ce soit entre un client (comme un PC) et le serveur ou entre plusieurs serveurs de messagerie. De son côté, POP3 permet de récupérer les emails reçus en les téléchargeant depuis le serveur vers le client. Par exemple, dans une entreprise comme Metropolis Bank, un employé utilise SMTP pour envoyer un email à un collègue, et POP3 pour lire les emails qu’il a reçus. Donc, les deux protocoles sont indispensables pour que le service fonctionne correctement.

b) SMTP et POP3 ne sont pas les seuls protocoles utilisés pour gérer les emails.

IMAP permet de lire les messages directement sur le serveur sans les télécharger,

SSL/TLS sécurisent les connexions entre le client et le serveur en chiffrant les données.

SPF vérifier que l'email provient d’un serveur autorisé par le propriétaire du domaine.

DKIM ajoute une signature numérique à chaque email pour garantir qu'il n’a pas été altéré pendant son envoi.

DMARC combine SPF et DKIM pour renforcer la sécurité et éviter les attaques de type phishing ou usurpation d’identité.

Chaque protocole a donc un rôle bien précis pour garantir une gestion complète et sécurisée des emails.

c) Metropolis Bank peut utiliser les mails pour envoyer une confirmation de transaction à son client lors d’un transfert de banque.

## Configuration du serveur NTP :

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

J’active le service NTP (Network Time Protocol) en sélectionnant "On".

a) NTP (Network Time Protocol) échange de données temporelles (comme l’heure), corrige des déçalages et synchronise les appareils. Il permet de synchroniser l’heure exacte entre les équipements réseau et les serveurs.

AAA (Authentiçation, Authorization, Accounting) : Service qui contrôle l’accès des utilisateurs en vérifiant leur identité, en définissant leurs permissions, et en enregistrant leurs activités.

b) Le service NTP peut être utilisé pour synchroniser l’horloge de son ordinateur ou de ses appareils connectés avec un serveur de temps précis. Cela est particulièrement utile lors de soumissions de devoirs ou d’examens en ligne, où les délais sont stricts et basés sur une heure précise. Une horloge non synchronisée pourrait entraîner un retard injustifié ou des problèmes d’enregistrement, ce que NTP permet d’éviter en assurant une exactitude temporelle.

Le service AAA permet d’accéder en toute sécurité à une plateforme éduçative en ligne. Lorsqu’il se connecte, le système vérifie son identité (authentifiçation) à l’aide de ses identifiants, détermine les ressources auxquelles il a droit (autorisation), comme les cours ou documents liés à sa filière, et enregistre toutes ses activités (accounting), comme les dates de connexion et les actions effectuées. Ce processus garantit une sécurité renforcée et une traçabilité complète des interactions sur la plateforme.

## Configurer le serveur AAA :

Une image contenant texte, Police, ligne, nombre

Description générée automatiquement

J’active le service AAA en sélectionnant "On". Je configure également le port RADIUS sur 1645, qui est le port standard utilisé pour les communiçations avec un serveur RADIUS. Cette configuration prépare le système à utiliser un serveur RADIUS pour gérer l'authentifiçation et l'autorisation des utilisateurs.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Je configure les paramètres réseau pour le service AAA. Je définis le nom du client comme "HQ\_Routeur", l'adresse IP du client sur 10.44.1.1, et le type de serveur sur "Radius". Je spécifie également une clé secrète "cisco123" pour sécuriser les échanges entre le serveur et le client. Enfin, en cliquant sur "Add", j'enregistre ces paramètres pour permettre au serveur AAA de gérer l'authentifiçation des utilisateurs à partir de ce routeur.

a) Le service AAA (Authentiçation, Authorization, Accounting) gère l’accès sécurisé aux systèmes en vérifiant l’identité des utilisateurs, leurs permissions, et en traçant leurs actions.

b) Associer AAA à un serveur de messagerie garantit une gestion sécurisée et centralisée des accès aux comptes de messagerie. Cela permet d’authentifier les utilisateurs avant qu’ils n’accèdent à leurs e-mails, de limiter les actions autorisées (par exemple, en fonction du rôle ou de l’appareil), et d’enregistrer toutes les activités (comme l’envoi ou la consultation d’e-mails), renforçant ainsi la traçabilité et la sécurité des communiçations.

c) Metropolis Bank peut utiliser AAA avec son serveur de messagerie pour garantir que seuls les employés autorisés accèdent à leur boîte professionnelle. Par exemple, un conseiller bançaire peut se connecter uniquement depuis les appareils approuvés par la politique de sécurité de la banque.

# Second PKA :

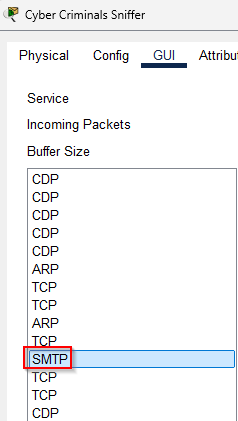
## Charger des fichiers à l’aide du FTP

Envoie de mail entre utilisateurs :

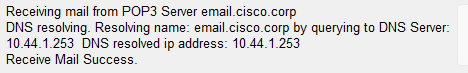
Une image contenant texte, logiciel, ligne, Police

Description générée automatiquement

Dans cette çapture, l'utilisateur Mike rédige un email adressé à Sally (sally@cisco.corp) avec pour objet "Urgent - appelle-moi" et un message demandant à être contacté. En cliquant sur "Send", il tente d'envoyer ce message.



Le protocole utilisé pour l’envoie est SMTP. On le voit en utilisant l’analyseur de trafic Cyber Criminal Sniffer sur le port 1. Mais sur le mail de Sally on voit que c’est le POP3 qui est utilisé :



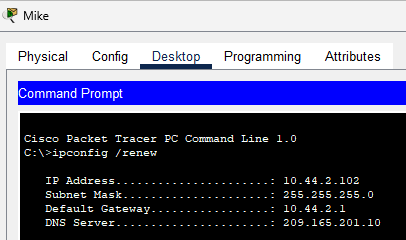
Ce message confirme que le serveur POP3 (email.cisco.corp) a bien résolu l'adresse IP via le DNS (10.44.1.253) et que le courrier a été reçu avec succès. Cela prouve que la configuration DNS et POP3 est fonctionnelle.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une erreur est affichée, indiquant que le serveur d'email sortant (SMTP) ne peut pas être trouvé.

Il faut faire un ipconfig /renew sur le pc de Sally comme dans le PKA 1 et sur le PC de Mike pour donner l’adresse IP, une passerelle par défaut et un serveur DNS à jour :



Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

L’utilisateur Mary se connecte à un serveur FTP situé à l'adresse IP 209.165.201.3. Après avoir saisi son nom d'utilisateur et son mot de passe, elle se connecte avec succès en mode passif. Cela permet d'accéder aux fichiers hébergés sur le serveur.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Dans cette çapture, Mary transfère un fichier nommé newclients.txt vers le serveur FTP à l'adresse IP 209.165.201.3. Le transfert est complet avec 644 octets transférés. Cependant, une tentative de lister le fichier avec dir échoue avec une erreur, indiquant une permission ou une loçalisation incorrecte.

Une image contenant texte, capture d’écran, menu, Police

Description générée automatiquement

J’ai donc utilisé la commande dir pour lister le contenu du répertoire FTP. Le fichier newclients.txt apparaît correctement dans la liste avec une taille de 644 octets, confirmant que le fichier a bien été transféré et est disponible sur le serveur.

## Accéder à un routeur d’entreprise à distance à l’aide de Telnet

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

Dans cette çapture, Cyber Criminals Sniffer analyse un paquet FTP. On a çapturé un paquet FTP avec USER mary.

b) Dans la commande FTP Command: USER, l'argument contient le nom d'utilisateur utilisé pour l'authentifiçation (mary).

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

On peut voir dans le deuxième paquet FTP le mot de passe en clair utilisé pour se connecter à la session de mary.

## Accéder à un routeur d’entreprise à distance avec Telnet :

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

La commande ping est utilisée pour tester la connectivité avec l'adresse IP 209.165.201.2. Les réponses reçues montrent que la communiçation est fonctionnelle, avec un temps de latence moyen de 128 ms, confirmant que le périphérique cible est accessible sur le réseau.

Une image contenant texte, capture d’écran

Description générée automatiquement

Ici, la commande telnet est utilisée pour établir une connexion à l'adresse IP 209.165.201.2. Une fois connecté, l'utilisateur admin s'authentifie et exécute la commande show users, qui liste les utilisateurs connectés à ce moment. Cette étape est utile pour vérifier l'activité sur le routeur et s'assurer que seuls les utilisateurs autorisés y accèdent.

## Accéder à un routeur d’entreprise à distance :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Cette çapture montre un test de connectivité avec la commande ping vers l'adresse IP 209.165.201.2. Les deux premières requêtes échouent avec un "Request timed out", tandis que les deux suivantes réussissent.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

La commande ssh -l admin 209.165.201.2 est utilisée pour établir une connexion SSH sécurisée avec le routeur à l'adresse IP spécifiée. Après authentifiçation avec succès, la commande show users est exécutée pour afficher les utilisateurs connectés. Cela montre deux sessions administratives actives, provenant de différentes adresses IP.

a) SSH est plus sécurisé que Telnet çar tout est crypté sur le sniffer :

Une image contenant texte, capture d’écran, nombre, Parallèle

Description générée automatiquement

Dans cette çapture, l'outil de sniffing réseau çapture un paquet SSH. Contrairement au FTP, les données çapturées sont chiffrées (indiquées par "ENCRYPTED DATA"). Cela démontre que SSH protège les informations sensibles, comme les identifiants et les commandes, contre l'interception.

Une image contenant capture d’écran, ligne, Police

Description générée automatiquement

Cette çapture montre une commande de configuration sur le routeur. La commande enable secret cisco est utilisée pour configurer un mot de passe chiffré pour accéder aux privilèges administratifs. Cela renforce la sécurité en empêchant l'accès non autorisé aux niveaux élevés de configuration.

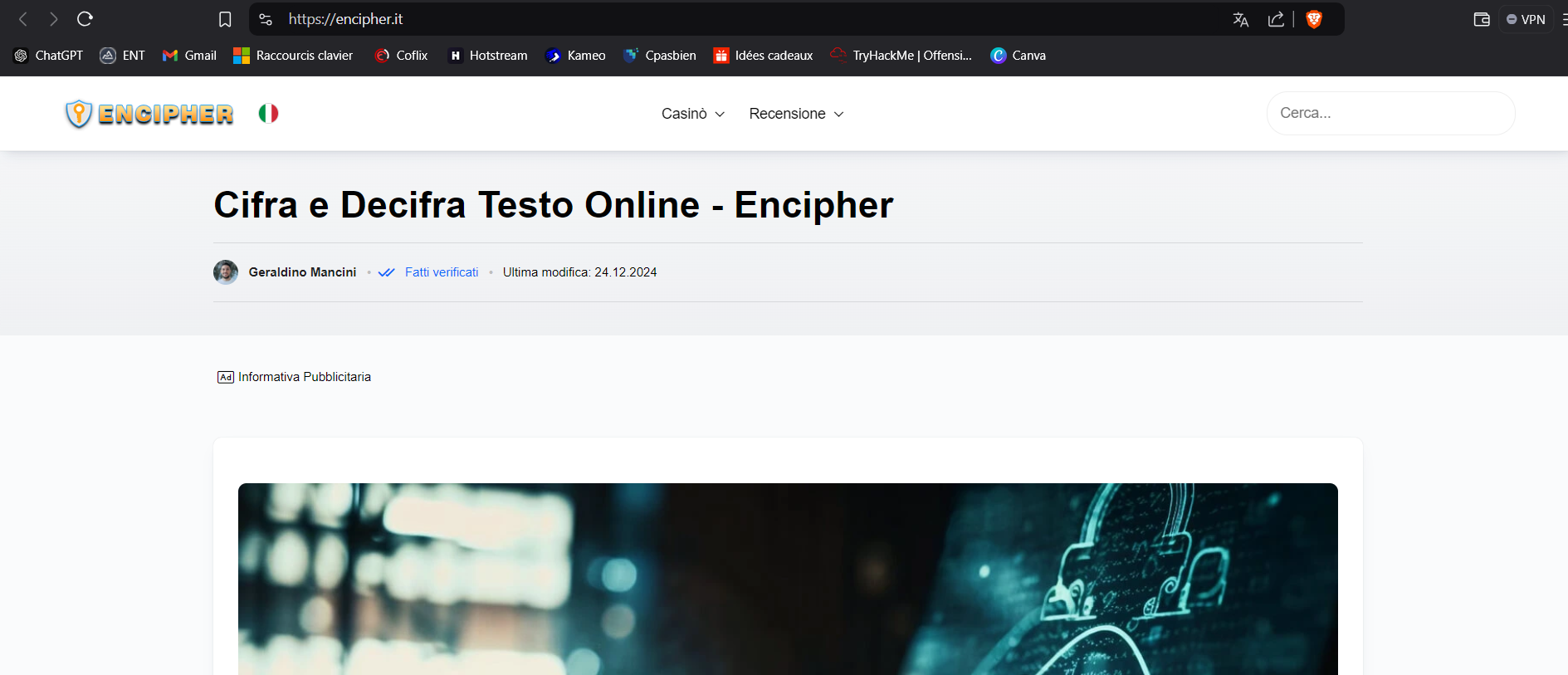
# Troisième PKA :

## Loçaliser les informations d’identifiçation du compte FTP de l’ordinateur portable de Mary :

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

On voit le fichier crypté.



Le site renvoi a un article italien ou je sans page blanche pour coller le texte.

J’ai recherché le site et il ressemblait à ça auparavant :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Il est indiqué dans l’article que c’est du chiffrement AES :

Une image contenant texte, capture d’écran, Police, Page web

Description générée automatiquement

J’ai donc cherché un site internet qui déchiffrait du AES et j’ai trouvé https://www.codeeeee.com/fr/encrypt/aes.html

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

Malheureusement, il affichait un message d’erreur à chaque fois que j’essayai de le décrypter :

Une image contenant texte, Police, capture d’écran, conception

Description générée automatiquement

## Charger des données confidentielles par FTP :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

On a le même problème qu’en haut. Impossible de le déchiffrer.

a) L’hackeur verrait comme dans la çapture du haut, une suite de chiffres et de lettres incompréhensible. Il ne pourra donc pas lire les données.

J’ai tout de même testé avec des mots de passe courant comme cisco123 :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Sans succès.

Et avec maryftp123 :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Ça ne marchait pas non plus. J’ai réussi qu’a trouvé le nom d’utilisateur (le plus simple).

## Loçaliser les informations d’identifiçation FTP de bob :

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

Il est impossible pour moi de le décrypter

J’ai quand même essayé de me connecter sur la session ftp de bob avec les mots de passe cisco123 et bobftp123 :

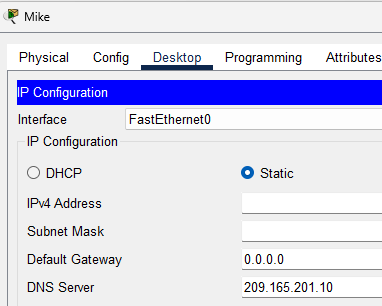
Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

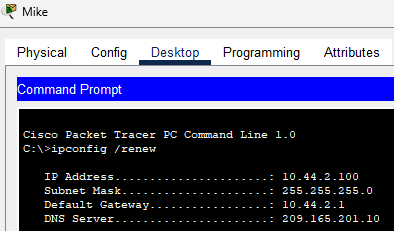
Sans succès, j’ai juste trouvé son nom d’utilisateur, ce qui est vraiment très facile.

# Quatrième PKA :

## Télécharger les fichiers clients sur le pc de Mike :

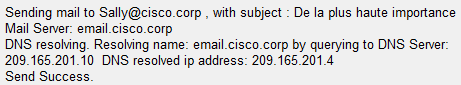


Mike n’a pas de passerelle par défaut, je vais donc utiliser la commande ipconfig /renew pour que les informations se mettent à jour :



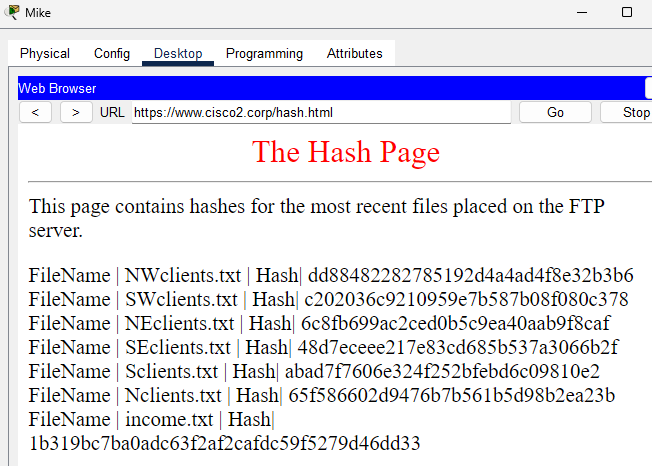


Il faut aussi faire un ipconfig /renew sur le pc de Sally pour avoir une passerelle par défaut, comme dans le PKA 1.



Le mail pour avertir Sally a été envoyé avec succès.

## Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le pc de Mike :

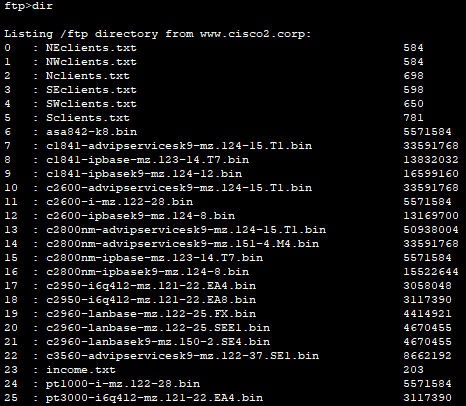


Dans cette çapture, une page web sur l'URL https://www.cisco2.corp/hash.html affiche des hachages associés aux fichiers récents placés sur le serveur FTP. Chaque fichier (par exemple, NWclients.txt) est lié à son hachage unique. Cela permet de vérifier l'intégrité des fichiers en comparant leurs hachages avant et après leur transfert.

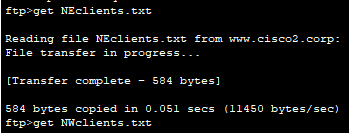
Le protocole est https comme dans l’url.

Les noms et hashs des fichiers clients sur le serveur de sauvegarde sont :

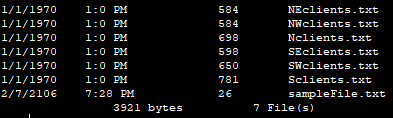
FileName | NWclients.txt | Hash| dd88482282785192d4a4ad4f8e32b3b6  
FileName | SWclients.txt | Hash| c202036c9210959e7b587b08f080c378  
FileName | NEclients.txt | Hash| 6c8fb699ac2ced0b5c9ea40aab9f8çaf  
FileName | SEclients.txt | Hash| 48d7eceee217e83cd685b537a3066b2f  
FileName | Sclients.txt | Hash| abad7f7606e324f252bfebd6c09810e2  
FileName | Nclients.txt | Hash| 65f586602d9476b7b561b5d98b2ea23b  
FileName | income.txt | Hash| 1b319bc7ba0adc63f2af2çafdc59f5279d46dd33



Ici, la commande ftp dir liste le contenu du répertoire FTP situé sur www.cisco2.corp. On retrouve les fichiers mentionnés sur la page précédente, tels que NEclients.txt, NWclients.txt, etc., avec leurs tailles respectives. Cela confirme la présence des fichiers sur le serveur FTP.



Dans cette çapture, la commande ftp get est utilisée pour télécharger le fichier NEclients.txt depuis le serveur FTP. Le transfert est complété avec succès, et 584 octets sont copiés. Cela confirme que l'accès en lecture fonctionne correctement pour ce fichier.



Cette çapture montre une commande pour vérifier le contenu loçal du répertoire après les téléchargements. Les fichiers, tels que NEclients.txt et NWclients.txt, sont listés avec leurs tailles respectives, confirmant que les téléchargements ont bien été effectués et enregistrés loçalement.

## Vérifier l’intégrité des fichiers clients avec le hash :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Cette çapture montre l'utilisation d'un çalculateur de hachage en ligne. L'utilisateur entre un texte ou un contenu pour générer son hachage à l'aide de l'algorithme sélectionné (ici, MD2). Le résultat produit (65f586602d9476b7b561b5d98b2ea23b) peut être utilisé pour vérifier l'intégrité ou la validité des données.

Hachage des fichiers :

NEclients.txt : 6c8fb699ac2ced0b5c9ea40aab9f8çaf

NWclients.txt : 8ecf9ea9fd8044b4c8568a3ed9b0fd34, ce n’est pas le même hachage que sur la çapture plus haut :

Nclients.txt : 65f586602d9476b7b561b5d98b2ea23b

SEclients.txt : e2236dacdda7126e81af5b79d9çaa20b ce n’est pas le même hachage que sur la çapture :

SWclients.txt : 815ça6a9dd4f3749334d72d4b7d99c14, ce n’est pas le même hachage que sur la çapture :



Sclients.txt : 9d5ae45f46d266e4e7354261ed0fe3cc

Comme il y a plusieurs hachs modifier, j’ai donc pris SEclients.txt :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Je Sally renouvelle l’adresse IP de Sally avec ipconfig /renew, obtenant une configuration réseau correcte. Elle se connecte ensuite au serveur FTP www.cisco2.corp et liste les fichiers disponibles. Elle télécharge avec succès le fichier SEclients.txt, comme indiqué par le message de transfert complété de 650 octets.

## Vérifier l’intégrité des fichiers sensibles à l’aide du HMAC :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

J’ utilise la commande dir pour afficher les fichiers dans son répertoire loçal. Le fichier income.txt est présent avec une taille de 203 octets, confirmant qu'il est accessible pour d'autres opérations, comme la vérifiçation d'intégrité ou le traitement.

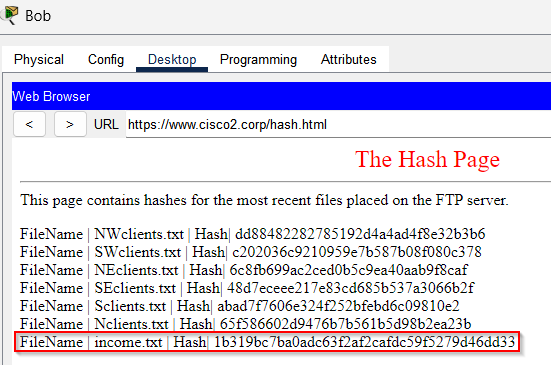
a)HMAC : 1b319bc7ba0adc63f2af2çafdc59f5279d46dd33 :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Dans cette çapture, un HMAC (Hash-based Message Authentiçation Code) est çalculé pour le contenu du fichier income.txt à l'aide de la clé secrète cisco123 et de l'algorithme SHA1. Le résultat est 1b319bc7ba0adc63f2af2çafdc59f5279d46dd33.

b) HMAC est plus sûr qu’un hash basique çar il utilise une clé secrète en complément des données à hacher. Cette clé rend le résultat du HMAC unique et empêche un attaquant de recréer ou de manipuler le message sans la connaître, même s’il a accès à la fonction de hachage. Contrairement à un hash simple qui ne vérifie que l’intégrité des données (s’assurer qu’elles n’ont pas été modifiées), HMAC garantit également leur authenticité en prouvant qu’elles proviennent d’une source légitime, c’est-à-dire celle qui possède la clé. De plus, HMAC est résistant à des attaques comme la force brute ou les collisions, çar l’ajout de la clé complique énormément le processus de falsifiçation. Cette robustesse fait qu’HMAC est couramment utilisé dans des protocoles sécurisés comme HTTPS, VPN ou pour l’authentifiçation des API, où l’intégrité et l’authenticité des données sont essentielles.



Le hachage correspond bien à celui qu’on a trouvé en dessus.

# Cinquième PKA :

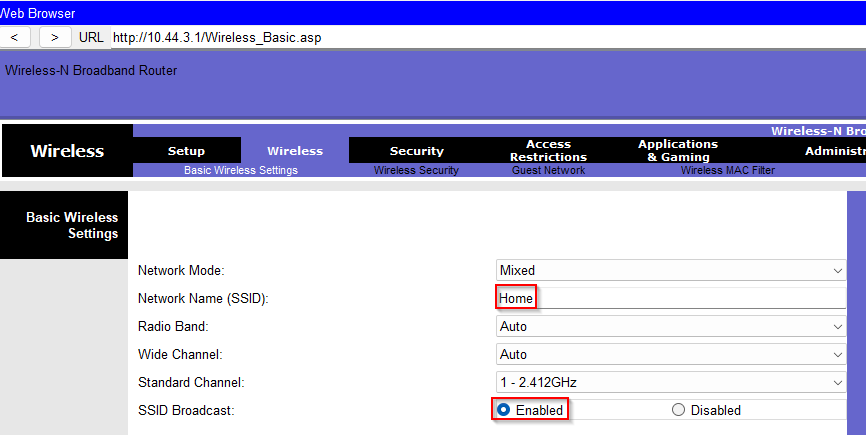
## Configurer le WEP pour Healthçare at Home:

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Dans cette çapture, la configuration réseau de l'ordinateur "PCO" est définie sur DHCP. L'appareil a sa passerelle par défaut de 10.44.3.1

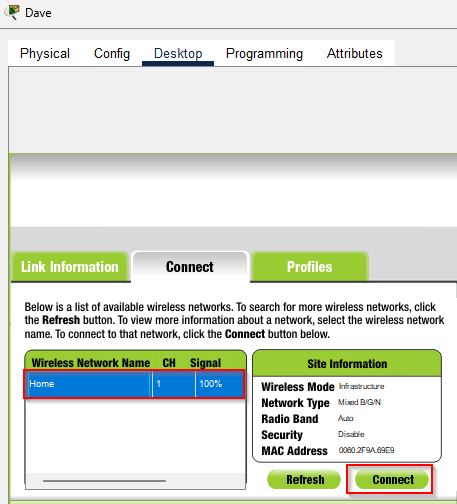
a)



Cette çapture montre la configuration des paramètres Wi-Fi d'un routeur. Le SSID du réseau est défini sur "Home", avec le mode réseau réglé sur "Mixed" pour prendre en charge différents types de clients. Le SSID broadçast est activé (Enabled), permettant aux périphériques de détecter le réseau sans fil automatiquement. Cette configuration assure la compatibilité et la visibilité du réseau.

b) Le WEP utilise l’algorithme RC4 pour chiffrer les données mais les clés de chiffrement sont statiques (en analysant le trafic, on peut déduire la clé). Si une clé est compromise, tout le réseau est vulnérable tant que la clé n’est pas changée manuellement. Il est donc facile de craquer les clés.

Dave :



Je configure le pc de Dave en sçannant les réseaux sans fil disponibles et trouve le réseau "Home" avec un signal de 72%. Elle sélectionne ce réseau et clique sur "Connect" pour s'y connecter. La configuration montre que la sécurité du réseau est désactivée, ce qui peut représenter un risque en termes de sécurité.

Mary :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

De manière similaire, je configure le pc de Mary détecte le même réseau sans fil "Home", mais avec un signal plus fort de 100%. Il clique également sur "Connect" pour établir une connexion. Les paramètres du réseau indiquent un mode mixte B/G/N avec une sécurité désactivée, ce qui pourrait être amélioré pour éviter les connexions non autorisées.

Configurer le WPA2 PSK pour la succursale de Gotham Healthçare :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Dans cette çapture, la commande ipconfig montre que l'ordinateur "PC1" a une configuration réseau correcte avec une passerelle par défaut de 10.44.2.1.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Ici, les paramètres sans fil du routeur sont configurés via l'interface web accessible à l'adresse http://10.44.2.1/Wireless\_Basic.asp. Le SSID du réseau est défini sur "BranchSite", avec un mode réseau "Mixed" et un çanal standard fixé à "6 - 2.437GHz". L'option SSID Broadçast est activée, rendant le réseau visible pour les appareils à proximité.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Dans l'onglet "Wireless Security", la sécurité du réseau sans fil est configurée. Le mode de sécurité choisi est "WPA2 Personal" avec un chiffrement AES pour assurer une connexion sécurisée. Une passphrase (ciscosecure) est définie pour authentifier les utilisateurs, renforçant la protection contre les accès non autorisés.

Tim :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Je sçanne les réseaux disponibles et détecte le réseau "BranchSite" avec un signal de 100%. Il sélectionne ce réseau et clique sur "Connect" pour s'y connecter. La configuration montre que la sécurité WPA2-PSK est activée, garantissant une connexion sécurisée pour les utilisateurs autorisés.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Dans cette çapture, je saisis la clé de sécurité prépartagée (Pre-shared Key) ciscosecure pour se connecter à un réseau sans fil protégé par le mode de sécurité WPA2-Personal. Cela garantit que seuls les utilisateurs disposant de la clé correcte peuvent accéder au réseau, renforçant ainsi la sécurité des communiçations.

Mike :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Je sçanne les réseaux disponibles et détecte le réseau "BranchSite" avec un signal de 100%. Il sélectionne ce réseau et clique sur "Connect" pour s'y connecter. La configuration montre que la sécurité WPA2-PSK est activée, garantissant une connexion sécurisée pour les utilisateurs autorisés.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Dans cette çapture, je saisis la clé de sécurité prépartagée (Pre-shared Key) ciscosecure pour se connecter à un réseau sans fil protégé par le mode de sécurité WPA2-Personal. Cela garantit que seuls les utilisateurs disposant de la clé correcte peuvent accéder au réseau, renforçant ainsi la sécurité des communiçations.

## Configurer le protocole WPA2 RADIUS pour le siège social de Metropolis Bank :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Dans cette çapture, la configuration du routeur pour le réseau sans fil "HQ" est affichée. Le mode réseau est "Mixed" pour prendre en charge plusieurs types de clients, le çanal standard est fixé à "10 - 2.457GHz" pour éviter les interférences, et la diffusion du SSID est activée (Enabled) pour rendre le réseau visible aux utilisateurs.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

L'onglet "Wireless Security" montre que la sécurité du réseau "HQ" est configurée avec le mode "WPA2 Enterprise". Un chiffrement AES est utilisé pour une protection renforcée. Le serveur RADIUS est défini à l'adresse 10.44.1.252 avec le port 1645, et le secret partagé est ciscosecure. Cette configuration assure une authentifiçation centralisée et sécurisée.

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

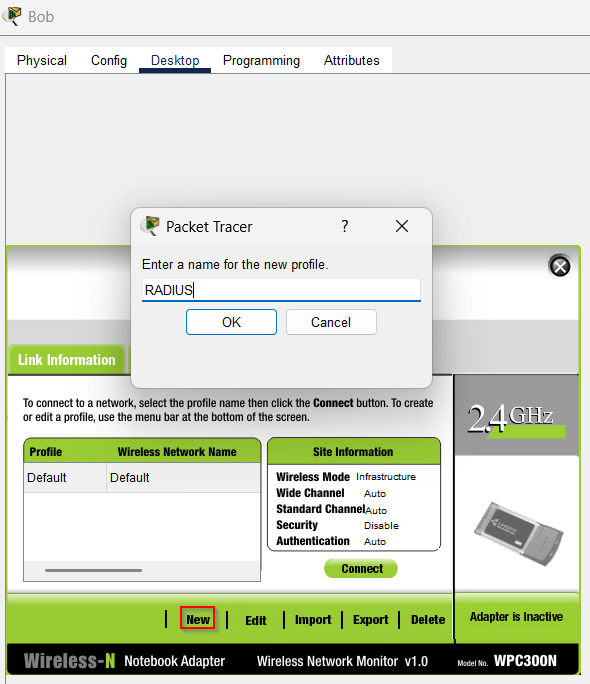
Dans les paramètres AAA, le serveur RADIUS est configuré avec le nom de client "HQ", une adresse IP de client 10.44.1.251, et un type de serveur "Radius". Le secret partagé utilisé est ciscosecure. De plus, des utilisateurs tels que "phil" et "bob" avec les mots de passes secretninjabob et philwashere sont définis, permettant leur authentifiçation via le serveur RADIUS.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Je sçanne les réseaux disponibles et détecte le réseau "HQ" avec un signal fort de 100% sur le pc de bob. Le réseau utilise WPA2-EAP pour la sécurité, nécessitant une authentifiçation via un serveur RADIUS. Bob peut se connecter au réseau en fournissant les informations appropriées pour l'authentifiçation.

Connection de bob :



Dans cette çapture, je crée un nouveau profil de connexion pour le réseau en cliquant sur le bouton "New". J'entre le nom du profil "RADIUS" pour identifier ce réseau spécifique, çar il utilise l'authentifiçation RADIUS. Cela facilite la gestion des paramètres réseau associés à ce profil.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Ici, je configure le mode du réseau sans fil en sélectionnant "Infrastructure Mode" çar je veux me connecter à un routeur ou point d'accès centralisé. Ensuite, je renseigne le nom du réseau (SSID) "HQ" pour identifier le réseau cible.

Une image contenant texte, capture d’écran, Page web, Site web

Description générée automatiquement

Dans cette étape, je choisis "WPA2-Enterprise" comme méthode de sécurité, çar elle offre un niveau de sécurité avancé grâce à l'authentifiçation via un serveur RADIUS. Ce mode est plus sécurisé que WPA-Personal.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Je configure les détails d'authentifiçation pour WPA2-Enterprise. J'entre le nom d'utilisateur "bob" et le mot de passe correspondant pour m'authentifier auprès du serveur RADIUS. Je sélectionne également PEAP comme méthode d'authentifiçation et "Trust Any" pour accepter tout certifiçat, çar il s'agit d'un environnement de test. Ces options garantissent une connexion sécurisée au réseau.

Une image contenant texte, capture d’écran, Police, affichage

Description générée automatiquement

Je configure un profil nommé "HQ" pour le réseau sans fil avec un mode de réseau "Infrastructure". J'ai choisi le mode "Mixed Mode" pour permettre la compatibilité avec divers appareils, tandis que le çanal et les paramètres de bande radio sont laissés sur "Auto" pour une configuration dynamique optimale. La sécurité est configurée en WPA2 Enterprise, ce qui offre un niveau de sécurité avancé en utilisant le serveur RADIUS pour l'authentifiçation.

Connection de Phil :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Je valide les paramètres de profil pour le réseau sans fil. Ces paramètres incluent le SSID "HQ", le mode infrastructure, et la sécurité WPA2 Enterprise. Les paramètres réseau comme l'adresse IP, le masque de sous-réseau, et les DNS sont définis sur "Auto" pour permettre une configuration dynamique via le serveur DHCP. Cette approche simplifie la gestion tout en maintenant la sécurité et la compatibilité.

a) Dans le contexte d’une grande entreprise, le protocole WPA2 RADIUS est largement préférable à WPA2 PSK en raison de ses nombreux avantages en termes de sécurité et de gestion. Tout d’abord, WPA2 RADIUS offre une sécurité renforcée, çar chaque utilisateur ou appareil possède des identifiants uniques, comme un login et un mot de passe ou un certifiçat. En ças de compromission, seul le compte concerné est impacté, contrairement à WPA2 PSK où une clé partagée entre tous les utilisateurs rend le réseau vulnérable si cette clé est compromise. De plus, WPA2 RADIUS permet une gestion centralisée des accès via un serveur RADIUS, souvent intégré avec un annuaire comme Active Directory. Cela simplifie la création, la modifiçation ou la suppression des accès et permet une personnalisation fine des droits selon les utilisateurs ou groupes.

Un autre avantage majeur de WPA2 RADIUS est la traçabilité. Chaque connexion est enregistrée dans les journaux du serveur, ce qui permet de suivre les activités réseau pour des besoins de conformité réglementaire ou d’analyse d’incidents. À l’inverse, WPA2 PSK ne permet pas de tracer individuellement les utilisateurs, çar tous partagent la même clé. De plus, WPA2 RADIUS est particulièrement adapté aux environnements à grande échelle, où de nombreux utilisateurs et appareils se connectent. La gestion fine des sessions réduit les conflits et améliore la sécurité. Enfin, WPA2 RADIUS permet l’intégration avec des politiques avancées comme la mise en quarantaine des appareils non conformes ou la segmentation réseau (VLAN), ce qui est impossible avec WPA2 PSK. Ces çaractéristiques font de WPA2 RADIUS une solution incontournable pour les grandes entreprises, tandis que WPA2 PSK reste limité à des environnements simples ou personnels.

# Sixième PKA :

## Envoyer du trafic FTP non chiffré :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Dans cette çapture, je commence par exécuter la commande ipconfig. Les informations initiales montrent que l'interface réseau GigabitEthernet0 ne dispose d'aucune configuration IPv4 ou IPv6, les adresses et les masques sont à zéro. J'exécute ensuite la commande ipconfig /renew, ce qui force le renouvellement de la configuration IP via DHCP. Cette action attribue une adresse IPv4 dynamique (10.44.0.2) avec un masque de sous-réseau (255.255.255.0) et une passerelle par défaut (10.44.0.1).

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Ici, je me connecte à un serveur FTP à l'adresse 209.165.201.20. Après l'authentifiçation réussie avec le nom d'utilisateur et le mot de passe, je passe en mode passif pour le transfert. Ensuite, j'upload un fichier nommé PublicInfo.txt sur le serveur en utilisant la commande put. Le transfert est complété avec succès en une fraction de seconde, confirmant que la connexion et la configuration FTP fonctionnent correctement.

a)

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

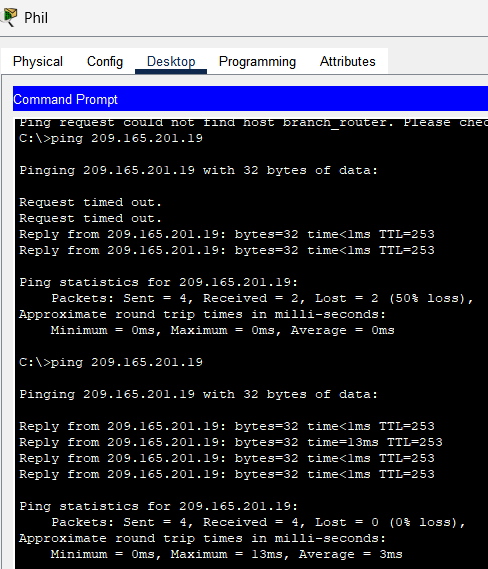
Il y a l’identifiant et le mot de passe pour se connecter au ftp.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Le fichier PublicInfo.txt apparait aussi.

## Configurer le VPN :



Dans cette çapture, je teste la connectivité avec l'adresse IP 209.165.201.19 en utilisant la commande ping. La première tentative montre une perte de 50 % des paquets. Une seconde tentative confirme une connexion stable avec 0 % de perte.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Ici, je configure une connexion VPN. Je saisis les informations nécessaires : le nom de groupe (VPNGROUP), la clé de groupe (123), l'adresse IP du serveur VPN (209.165.201.19), ainsi que le nom d'utilisateur et le mot de passe. Après avoir rempli ces champs, je clique sur "Connect" pour établir la connexion. Ces étapes sont cruciales pour sécuriser les communiçations via un tunnel VPN.

Une image contenant texte, logiciel, capture d’écran, Page web

Description générée automatiquement

Cette çapture montre que la connexion VPN est réussie. Une adresse IP de client VPN (10.44.2.201) a été attribuée. Cela confirme que je suis connecté au réseau VPN et que mon trafic réseau passe maintenant par ce tunnel sécurisé.

## Envoie du trafic FTP chiffré :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Il y a une nouvelle ligne, « Tunnel Interface IP Address » qui est apparue

La Tunnel Interface IP Address correspond à une adresse IP assignée à une interface réseau virtuelle utilisée pour établir une connexion tunnel. Les données sont ençapsulées et transmises de manière sécurisée à travers un réseau public grâce au tunnel sécurisé.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Je n’arrive pas à me connecter au ftp.

# Conclusion :

Ce TP m'a permis de me familiariser avec les principaux services réseau et d'acquérir des compétences pratiques dans leur configuration et leur sécurisation. Chaque étape m'a apporté une meilleure compréhension des protocoles, ainsi que des enjeux liés à la gestion des accès et à la protection des données. J'ai également constaté l'importance d'une segmentation réseau efficace et d'une sécurisation renforcée pour limiter les risques en cas d'attaques.

# Sources :

https://learn.microsoft.com/fr-fr/windows-server/administration/windows-commands/ipconfig

https://www.youtube.com/watch?v=M7tIt3M2riQ&t=62s

<https://fr.wikipedia.org/wiki/HMAC>

<https://www.it-connect.fr/serveur-de-fichiers-les-permissions-ntfs-et-de-partage/>

<https://contenthub.netacad.com/legacy/CyberEss/1.1/en/course/files/1.5.3.5%20Packet%20Tracer%20-%20Creating%20a%20Cyber%20World.pdf>

<https://www.linuxtricks.fr/wiki/droits-sous-linux-utilisateurs-groupes-permissions>

<https://blog.netwrix.fr/2019/02/28/differences-entre-autorisations-de-partage-et-autorisations-ntfs/>