Travail en autonomie du lundi 9 janvier 2023

Créer un monde numérique, appliquer des règles de sécurité

1. Fichier à utiliser : <Bloc1_sem1_tp00_decouverte_des_services_01.pka>

[Fichier à utiliser : Bloc1\_sem1\_tp00\_decouverte\_des\_services\_01.pka 1](#_Toc124710841)

[Table d’adressage 2](#_Toc124710842)

[Objectifs 3](#_Toc124710843)

[Partie 1 : Configurer le serveur FTP 3](#_Toc124710844)

[Étape 1 : Activez le service FTP. 3](#_Toc124710845)

[Étape 2 : Autorisez l’utilisateur à accéder au serveur FTP. 3](#_Toc124710846)

[Étape 3 : Proposer une définition et un exemple d’utilisation en entreprise de ce type de service. 3](#_Toc124710847)

[Partie 2 : Configurer le serveur web 3](#_Toc124710848)

[Étape 1 : Activez le service HTTP. 3](#_Toc124710849)

[Étape 2 : Vérifiez le service HTTP. 4](#_Toc124710850)

[Étape 3 : Évaluation du réseau de Metropolis Bank 4](#_Toc124710851)

[Partie 3 : Configurer le serveur DNS 4](#_Toc124710852)

[Étape 1 : Activez le service DNS. 4](#_Toc124710853)

[Étape 2 : Créez l’enregistrement DNS A. 4](#_Toc124710854)

[Étape 3 : Vérifiez le service DNS. 5](#_Toc124710855)

[Étape 4 : Proposer une définition et un exemple d’utilisation en entreprise de ce type de service. 5](#_Toc124710856)

[Partie 4 : Configurer le serveur de messagerie 5](#_Toc124710857)

[Étape 1 : Activez les services de messagerie. 5](#_Toc124710858)

[Étape 2 : Créez des comptes de messagerie pour les utilisateurs. 6](#_Toc124710859)

[Étape 3 : Configurez les clients de messagerie utilisateur. 6](#_Toc124710860)

[Étape 4 : Proposer une définition et un exemple d’utilisation en entreprise de ce type de service. 6](#_Toc124710861)

[Partie 5 : Configurer le serveur NTP 7](#_Toc124710862)

[Étape 1 : Activez le service NTP. 7](#_Toc124710863)

[Étape 2 : Sécuriser le service NTP. 7](#_Toc124710864)

[Étape 3 : Proposer une définition et un exemple d’utilisation en entreprise de ce type de service. 7](#_Toc124710865)

[Partie 6 : Configurer le serveur AAA 7](#_Toc124710866)

[Étape 1 : Activez le service AAA. 7](#_Toc124710867)

[Étape 2 : Configurer le réseau AAA. 8](#_Toc124710868)

[Étape 3 : Proposer une définition et un exemple d’utilisation en entreprise de ce type de service. 8](#_Toc124710869)

[Fichier à utiliser : Bloc1\_sem1\_tp00\_decouverte\_des\_services\_02.pka 8](#_Toc124710870)

[Table d’adressage 8](#_Toc124710871)

[Objectifs 8](#_Toc124710872)

[Contexte 9](#_Toc124710873)

[Partie 7 : Envoi d’e-mails entre utilisateurs 9](#_Toc124710874)

[Étape 1 : Accédez au client de messagerie sur le PC de Mike. 9](#_Toc124710875)

[Partie 8 : Envoyer un e-mail à Sally. 9](#_Toc124710876)

[Étape 1 : Faites en sorte que Sally vérifie ses e-mails. 9](#_Toc124710877)

[Partie 9 : Charger des fichiers à l’aide du FTP 9](#_Toc124710878)

[Étape 1 : Configurez le renifleur de paquets de sorte à capturer le trafic sur le bon port. 9](#_Toc124710879)

[Étape 2 : Connectez-vous au serveur FTP à distance. 9](#_Toc124710880)

[Étape 3 : Charger le fichier sur le serveur FTP. 10](#_Toc124710881)

[Étape 4 : Analysez le trafic FTP. 10](#_Toc124710882)

[Partie 10 : Accéder à un routeur d’entreprise à distance à l’aide de Telnet 11](#_Toc124710883)

[Étape 1 : Connectez-vous à un routeur d’entreprise à distance. 11](#_Toc124710884)

[Partie 11 : Accéder à un routeur d’entreprise à distance à l’aide de SSH 12](#_Toc124710885)

[Étape 1 : Connectez-vous à un routeur d’entreprise à distance. 12](#_Toc124710886)

[Fichier à utiliser : Bloc1\_sem1\_tp00\_decouverte\_des\_services\_03.pka 12](#_Toc124710887)

[Table d’adressage 12](#_Toc124710888)

[Objectifs 13](#_Toc124710889)

[Contexte 13](#_Toc124710890)

[Partie 12 : Localiser les informations d’identification du compte FTP de l’ordinateur portable de Mary 13](#_Toc124710891)

[Étape 1 : Accédez au document texte sur l’ordinateur portable de Mary. 13](#_Toc124710892)

[Étape 2 : Déchiffrez les informations de compte FTP de Mary. 13](#_Toc124710893)

[Partie 13 : Charger des données confidentielles par FTP 13](#_Toc124710894)

[Étape 1 : Accédez au document texte sur l’ordinateur portable de Mary. 13](#_Toc124710895)

[Étape 2 : Connectez-vous au serveur FTP à distance. 14](#_Toc124710896)

[Étape 3 : Chargez le fichier sur le serveur FTP. 14](#_Toc124710897)

[Partie 14 : Localiser les informations d’identification du compte FTP du PC de Bob 15](#_Toc124710898)

[Étape 1 : Accédez au document texte sur le PC de Bob. 15](#_Toc124710899)

[Partie 15 : Télécharger des données confidentielles par FTP 15](#_Toc124710900)

[Étape 1 : Connectez-vous au serveur FTP à distance. 15](#_Toc124710901)

[Étape 2 : Téléchargez le fichier sur le PC de Bob. 15](#_Toc124710902)

[Partie 16 : Déchiffrer le contenu du fichier clientinfo.txt 16](#_Toc124710903)

[Étape 1 : Obtenez la clé de déchiffrement de la part de Mary. 16](#_Toc124710904)

[Étape 2 : Déchiffrez le contenu du fichier clientinfo.txt. 16](#_Toc124710905)

[Fichier à utiliser : Bloc1\_sem1\_tp00\_decouverte\_des\_services\_04.pka 16](#_Toc124710906)

[Table d’adressage 16](#_Toc124710907)

[Objectifs 17](#_Toc124710908)

[Contexte 17](#_Toc124710909)

[Partie 17 : Télécharger les fichiers clients sur le PC de Mike 17](#_Toc124710910)

[Étape 1 : Accédez au client de messagerie sur le PC de Mike. 17](#_Toc124710911)

[Étape 2 : Le serveur de fichiers a été piraté. Avertissez Sally. 17](#_Toc124710912)

[Partie 18 : Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le PC de Mike 18](#_Toc124710913)

[Étape 1 : Accédez au serveur FTP hors site sur le PC de Mike. 18](#_Toc124710914)

[Étape 2 : Téléchargez les fichiers clients sur le PC de Mike. 18](#_Toc124710915)

[Partie 19 : Vérifier l’intégrité des fichiers clients à l’aide du hash 19](#_Toc124710916)

[Étape 1 : Vérifiez les hashs sur les fichiers clients sur le PC de Mike. 19](#_Toc124710917)

[Étape 2 : Téléchargez le fichier suspect sur l’ordinateur de Sally. 20](#_Toc124710918)

[Partie 20 : Vérifier l’intégrité des fichiers sensibles à l’aide du HMAC 20](#_Toc124710919)

[Étape 1 : Calculez le HMAC d’un fichier sensible. 20](#_Toc124710920)

[Étape 2 : Vérifiez le HMAC calculé. 20](#_Toc124710921)

[Fichier à utiliser : Bloc1\_sem1\_tp00\_decouverte\_des\_services\_05.pka 21](#_Toc124710922)

[Table d’adressage 21](#_Toc124710923)

[Objectifs 21](#_Toc124710924)

[Contexte 21](#_Toc124710925)

[Partie 21 : Configurer le WEP pour Healthcare at Home 21](#_Toc124710926)

[Étape 1 : Configurez le SSID sans fil. 21](#_Toc124710927)

[Étape 2 : Connectez les clients. 22](#_Toc124710928)

[Partie 22 : Configurer le WPA2 PSK pour la succursale de Gotham Healthcare 22](#_Toc124710929)

[Étape 1 : Configurez le SSID sans fil. 22](#_Toc124710930)

[Étape 2 : Configurez la sécurité sans fil. 23](#_Toc124710931)

[Étape 3 : Connectez les clients. 23](#_Toc124710932)

[Partie 23 : Configurer le protocole WPA2 RADIUS pour le siège social de la Metropolis Bank 23](#_Toc124710933)

[Étape 1 : Configurez le SSID sans fil. 23](#_Toc124710934)

[Étape 2 : Configurez la sécurité sans fil. 24](#_Toc124710935)

[Étape 3 : Configurez le serveur RADIUS. 24](#_Toc124710936)

[Étape 4 : Connectez les clients. 24](#_Toc124710937)

[Fichier à utiliser : Bloc1\_sem1\_tp00\_decouverte\_des\_services\_06.pka 25](#_Toc124710938)

[Table d’adressage 25](#_Toc124710939)

[Objectifs 25](#_Toc124710940)

[Le contexte 25](#_Toc124710941)

[Partie 24 : Envoyer du trafic FTP non chiffré 25](#_Toc124710942)

[Étape 1 : Accédez au détecteur d’intrusion 25](#_Toc124710943)

[Étape 2 : Connectez-vous au serveur Public\_FTP via une connexion FTP non sécurisée. 25](#_Toc124710944)

[Étape 3 : Affichez le trafic sur le Détecteur d’intrusion. 26](#_Toc124710945)

[Partie 25 : Configurer le client VPN sur l’ordinateur de Phil 26](#_Toc124710946)

[Partie 26 : Envoyer du trafic FTP chiffré 27](#_Toc124710947)

[Étape 1 : Affichez l’adressage IP actuel sur l’ordinateur de Phil. 27](#_Toc124710948)

[Étape 2 : Envoyez du trafic FTP chiffré de l’ordinateur de Phil au serveur Private\_FTP. 27](#_Toc124710949)

[Étape 3 : Affichez le trafic sur le Détecteur d’intrusion. 27](#_Toc124710950)

[Fichier à utiliser : Bloc1\_sem1\_tp00\_decouverte\_des\_services\_07.pka 27](#_Toc124710951)

[Table d'adressage 27](#_Toc124710952)

[Objectifs 27](#_Toc124710953)

[Contexte 27](#_Toc124710954)

[Partie 27 : Envoyer du trafic FTP non chiffré 27](#_Toc124710955)

[Étape 1 : Accédez au Détecteur d'intrusion. 27](#_Toc124710956)

[Étape 2 : Connectez-vous au serveur de sauvegarde FTP à l'aide d'une connexion FTP non sécurisée. 27](#_Toc124710957)

[Étape 3 : Affichez le trafic sur le Détecteur d'intrusion. 28](#_Toc124710958)

[Partie 28 : Configurer un tunnel VPN entre Metropolis et Gotham 28](#_Toc124710959)

[Partie 29 : Envoyer du trafic FTP chiffré 29](#_Toc124710960)

[Étape 1 : Envoyez du trafic FTP du PC de Sally au serveur de sauvegarde de fichiers. 29](#_Toc124710961)

[Étape 2 : Affichez le trafic sur le détecteur d'intrusion. 29](#_Toc124710962)

1. Table d’adressage

|  |  |  |  |
| --- | --- | --- | --- |
| Appareil | Adresse IP | Masque de sous-réseau | Site |
| FTP/Serveur web | 10.44.1.254 | 255.255.255.0 | Metropolis Bank HQ |
| E-mail/Serveur DNS | 10.44.1.253 | 255.255.255.0 | Metropolis Bank HQ |
| NTP/Serveur AAA | 10.44.1.252 | 255.255.255.0 | Metropolis Bank HQ |
| Serveur de sauvegarde du fichier | 10.44.2.254 | 255.255.255.0 | Gotham Healthcare Branch |

1. Objectifs

**Configurer le serveur FTP**

**Configurer le serveur web**

**Configurer le serveur de messagerie**

**Configurer le serveur DNS**

**Configurer le serveur NTP**

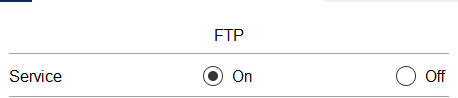
**Configurer le serveur AAA**

1. Contexte/Scénario

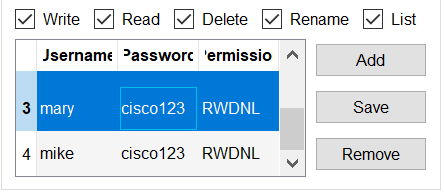
Dans cette activité, vous configurerez des éléments basiques du serveur. L’adresse IP a déjà été configurée. Vous utiliserez l’onglet Services sur plusieurs serveurs pour déployer les services FTP, web, messagerie, DNS, NTP et AAA.

1. Configurer le serveur FTP
   * 1. Activez le service FTP.

* Pour configurer un serveur FTP, nous devons d’abord procéder a son activation, pour cela suis le chemin suivant : Metropolis Bank HQ > FTP / WEB > Service > FTP. Puis on coche l’option ON :



* + 1. Autorisez l’utilisateur à accéder au serveur FTP.
* Voici les autorisations attribuées aux trois utilisateurs, et le mot de passe :



* + 1. Proposer une définition et un exemple d’utilisation en entreprise de ce type de service.

1. Donnez une définition en 1 ligne maximum d’un service FTP

* Un service FTP est un protocole de transfert de fichier sur internet (file transfert protocol).

1. Proposez un exemple d’utilisation pour **Metropolis Bank** de ce type de service.

* Ce protocole est nécessaire aux Transfer de fichier, Il peut être utile pour Métropolis Bank dans le cas ou un banquier voudrais envoyer une facture à un client.

1. Configurer le serveur web
   * 1. Activez le service HTTP.

* Pour configurer le serveur web il faut d’abord activer le service http et https, pour cela on coche l’option ON :



* + 1. Vérifiez le service HTTP.
* Pour vérifier le service http, on va se servir du PC nommé sally
* En utilisant le navigateur web et en essayant de nous rendre sur [www.cisco.com](http://www.cisco.com), on remarque que ça ne marche pas, car nous n’avons pas encore configurer le serveur DNS.
* En revanche nous avons paramétré le service http et https donc en entrant l’IP **10.44.1.254 correspondant à cisco, on peut constater que l’action se réalise correctement.**

Pourquoi un utilisateur peut-il consulter une adresse IP, mais pas un FQDN ?

* FQDN signifie fully qualified domain name, c’est tous simplement le nom de domaine complet, l’utilisateur ne peut pas le consulter car c’est une sécurité. Si ont avait la possibilité de les consulter, on pourrait voir ou sont stocké, sur quel serveur sont stocké les informations que l’on consulte.
  + 1. Évaluation du réseau de Metropolis Bank
* On peut voir la sécurité sous différent aspect, ici en premier lieu, on aborde l’aspect de la conception, effectivement Le parc des serveurs est à l’étage 1 juste a coté du parking et sans cage de faraday, on peut donc avoir accès au wifi car le routeur se trouve se trouve dans le parc de serveur, on peut facilement capter le signal. De plus sur le schéma réseau, on peut voir également la présence d’un switch dans le bureau 1, grâce à lui n’importe qui peut avoir accès au parc de serveur grâce à un branchement par câble.

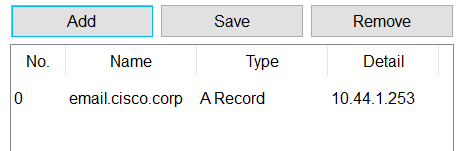
1. Configurer le serveur DNS
   * 1. Activez le service DNS.

* Pour configurer le serveur DNS on clique sur le cluster Email/DNS puis on se rend dans les services et enfin dans DNS et on coche l’option ON :

Une image contenant texte

Description générée automatiquement

* + 1. Créez l’enregistrement DNS A.
* Pour créer cet enregistrement, il suffit d’entrer le mail ci-dessus et l’adresse IP demandé et voici le résultat après avoir cliqué sur ajouter :



* + 1. Vérifiez le service DNS.
* Ont créé ensuite un second enregistrement en procédant de la même manière :

Une image contenant texte

Description générée automatiquement

* Afin de s’assurer que ce que nous avons fait est correcte, nous devons simplement cliquer sur le pc nommé Sally puis sélectionner le navigateur web. Pour faire le test on se rend sur [www.cisco.corp](http://www.cisco.corp) :

Une image contenant texte

Description générée automatiquement

* Ici il on notera que l’utilisateur peut consulter le FQDN grâce aux enregistrement réalisé ci-dessus, en effets ils ont permis d’associer les FQDN aux IP.
  + 1. Proposer une définition et un exemple d’utilisation en entreprise de ce type de service.
* Un serveur DNS (domaine name System) est un service qui permet de convertir les adresses IP en nom de domaine.

1. Proposez un exemple d’utilisation pour **Metropolis Bank** de ce type de service

* Une entreprise comme Métropolis Bank a tous intérêts à utiliser le service DNS, car celui-ci peut permettre de résoudre les noms de domaine de ses site web ou de ses applications en adresses IP pour permettre une connexion plus facile, il put également permettre d’établir des stratégies de sécurité comme la restriction d'accès à certains sites web ou IP pour la protection des données sensible. Mais le DNS peut également être utilisé pour améliorer les performances en répartissant les connexions en fonction de la géolocalisation des utilisateurs.

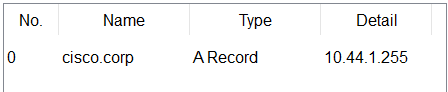
1. Configurer le serveur de messagerie
   * 1. Activez les services de messagerie.

* Pour configurer le serveur de messagerie, on commence par activer le service de messagerie. Pour cela on se rend dans le cluster de Bank HQ, puis sur le serveur Email/DNS puis dans service, et on se rend dans le service Email. Grace aux boutons situé en haut de l’interface, on active le service SMTP et POP3 :

Une image contenant texte

Description générée automatiquement

* L’activation de ses deux services pour le serveur de messagerie est indispensable, car le SMTP est le protocole utilisé pour l’envoie des mails, et enfin le POP3 est le protocole qui permet le téléchargement des e-mails d’un serveur vers le client, il permet d’assurer leur réception.
  + 1. Créez des comptes de messagerie pour les utilisateurs.
* Pour poursuivre la configuration du serveur de messagerie, il est maintenant nécessaire de créer des comptes de messageries pour les utilisateurs. Pour cela, il faut se rendre dans service, puis dans DNS, maintenant on saisie le nom de domaine « cisco.corp » que l’ont associe à l’IP 10.44.1.255 et on clique sur « add » pour finaliser la création :

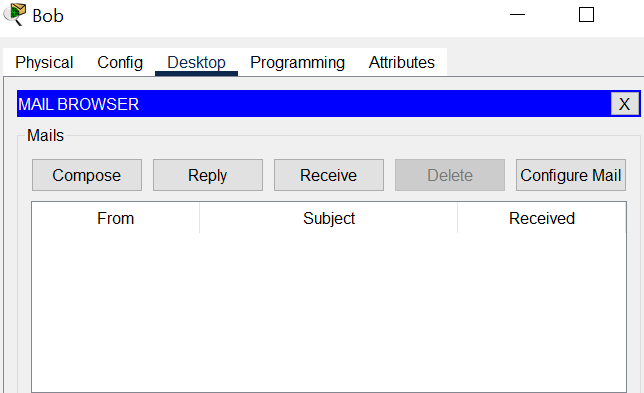


* Il faut maintenant créer les noms d’utilisateurs, on se rend dans le service FTP, on active ce service et on entre les noms souhaités que l’on assigne avec le mot de passe souhaité, dans notre cas c’est « cisco123 » :

Une image contenant texte

Description générée automatiquement

* + 1. Configurez les clients de messagerie utilisateur.
* Après la création de compte de messagerie, il faut maintenant configurer les client de messagerie, pour cela on se rend dans les pc bob et sally, puis on sélectionne la messagerie. On remplit les champs à compléter tel que => le nom, l’adresse mail, le serveur de messagerie entrant et sortant, le nom d’utilisateur, et le mot de passe, une fois ces champs rempli on sélectionne « save » et voici le résultat :



* Cette étape a été effectué sur les postes « sally & bob ».
* On notera que l’activation des protocole SMTP et POP3 sont nécessaire l’ors de l’activation du service de messagerie car le SMTP permet l’envoie des mails, et le POP3 permet d’assurer leur réception.
  + 1. Proposer une définition et un exemple d’utilisation en entreprise de ce type de service.

1. Donnez une définition en 1 ligne maximum d’un service de messagerie

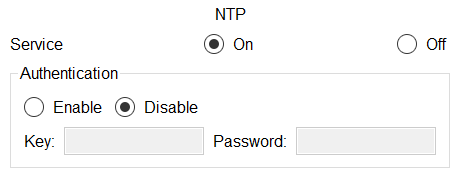
* Un service de messagerie est un système qui permet l’échange de courriel électronique entre utilisateur connecté à internet.

1. Proposez un exemple d’utilisation pour **Metropolis Bank** de ce type de service

* Métropolis Bak a tous intérêt à utiliser ce type de service, car cela leur permet de manager, de contrôler leur boite mail.

1. Configurer le serveur NTP
   * 1. Activez le service NTP.

* Pour le paramétrage du serveur NTP, on se rend dans l’onglet service, puis dans NTP et on positionne le bouton radial sur ON :

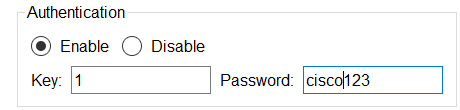


* + 1. Sécuriser le service NTP.
* Une fois l’activation de ce service réussi, il faut maintenant le sécuriser, pour cela on active la fonctionnalité d’authentification :

Une image contenant texte

Description générée automatiquement

* On peut maintenant configurer la clé 1 avec un mot de passe, dans notre cas le mot de passe sera : « cisco123 » :



* + 1. Proposer une définition et un exemple d’utilisation en entreprise de ce type de service.

1. Donnez une définition en 1 ligne maximum d’un service NTP/AAA

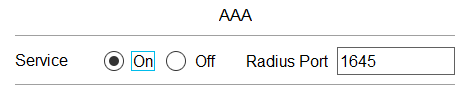
* Le service NTP (Network Time Protocol) permet de synchroniser les horloges des équipements présent sur un réseau avec une horloge source qui servira de référence.

1. Proposez un exemple d’utilisation pour **Metropolis Bank** de ce type de service

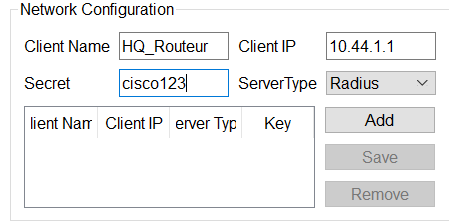
* Métropolis Bank peut utiliser ce type de service afin de synchroniser ses différents systèmes informatiques comme les serveurs de bases de données et le système de transaction en ligne.

1. Configurer le serveur AAA
   * 1. Activez le service AAA.

* Pour la configuration du serveur AAA, on se rend dans le service AAA, on l’active grâce au bouton radial :



* + 1. Configurer le réseau AAA.
* Nous pouvons maintenant configurer le réseau AAA, pour cela il faut configurer le nom de client suivant et lui attribuer une IP ainsi qu’un mot de passe :



* Il faut cliquer sur « add » pour confirmer cette configuration.
  + 1. Proposer une définition et un exemple d’utilisation en entreprise de ce type de service.

1. Donnez une définition en 1 ligne maximum d’un service AAA

* Le service AAA de son appellation complète (Authentication Authorization & Accounting) permet d’authentifier les utilisateurs et donc d’autoriser ou non leur accès à certains services.

1. Proposez un exemple d’utilisation pour **Metropolis Bank** de ce type de service

* Métropolis Bank pourrait utiliser ce type de service afin de contrôler les accès aux système de gestion des comptes bancaire par exemple.

1. Fichier à utiliser : <Bloc1_sem1_tp00_decouverte_des_services_02.pka>
2. 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 | 255.255.255.0 | Metropolis Bank HQ |
| E-mail/Serveur DNS | 10.44.1.253 | 209.165.201.4 | 255.255.255.0 | Metropolis Bank HQ |
| NTP/Serveur AAA | 10.44.1.252 | 209.165.201.5 | 255.255.255.0 | Metropolis Bank HQ |
| Serveur de sauvegarde du fichier | 10.44.2.254 | S/O | 255.255.255.0 | Gotham Healthcare Branch |

1. Objectifs

**Envoi d’e-mails entre utilisateurs**

**Charger et télécharger des fichiers à l’aide du FTP**

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

**Accéder à un routeur d’entreprise à distance à l’aide de SSH**

1. Contexte

Pendant cette activité, vous communiquerez sur des réseaux à distance à l’aide de services réseau courants. L’adresse IP, le réseau et le service ont déjà été configurés. Vous utiliserez les appareils du client dans différentes régions géographiques pour vous connecter aux serveurs et aux autres appareils du client.

1. Envoi d’e-mails entre utilisateurs
   * 1. Accédez au client de messagerie sur le PC de Mike.

* Dans cette partie nous allons aborder, l’envoie de mail entre utilisateur. Pour commencer, nous devons avoir accès au client de messagerie sur le pc de mike, pour cela on se rend dans le cluster de Gotham Healthcare Branch et ensuite sur le pc Mike, et enfin on sélectionne la messagerie.

1. Envoyer un e-mail à Sally.

* Ici nous devons rédiger un mail pour l’envoyer au pc Sally :

Une image contenant texte

Description générée automatiquement

* L’ors de l’envoie du mail par mike le protocole utiliser sera le protocole SMTP, celui-ci assurera l’arrivée du mail au serveur.
  + 1. Faites en sorte que Sally vérifie ses e-mails.
* Ici pour vérifier le bon acheminement du mail, on se rend dans le cluster de Metropolis Bank HQ puis sur le pc de sally, on ouvre la messagerie et on clique sur le bouton recevoir afin que le mail de Mike nous parvienne :

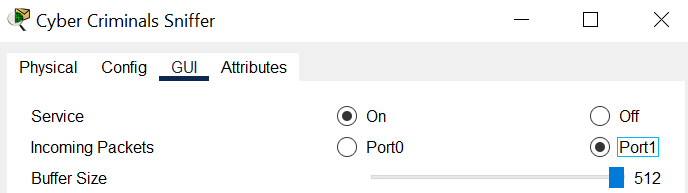
Une image contenant texte

Description générée automatiquement

* On peut voir ici que l’action c’est déroulé avec succès. On notera que le protocole utiliser ici pour l’acheminement du mail vers le receveur est le POP3.

1. Charger des fichiers à l’aide du FTP
   * 1. Configurez le renifleur de paquets de sorte à capturer le trafic sur le bon port.

* Maintenant que le service de messagerie est opérationnel, il faut maintenant configurer le FTP (File Transfert Protocol) afin que ls fichiers ne soit pas partager sur n’importe quel port. Pour cela, on se rend sur la vue global (géographique) des trois sites distants, on sélectionne le renifleur, et on sélectionne le port 1, cette action permettra de capturer les paquets présents sur ce port :



* + 1. Connectez-vous au serveur FTP à distance.
* On se rend maintenant sur le site Healthcare at home puis sur le PC Mary, on ouvre son invite de commande, puis en saisissant ftp **209.165.201.3 on se connecte au serveur FTP web de Métropolis Bank HQ, bien sûr il faudra entrer le nom d’utilisateur et le mot de passe que nous avons initialisé au paravent :**

Une image contenant texte

Description générée automatiquement

* Ici la connexion est réussi.
  + 1. Charger le fichier sur le serveur FTP.
* Maintenant que nous somme connecter sur le serveur FTP, grâce à la commande « dir » nous pouvons avoir accès a la liste de fichier stocké actuellement dans le serveur, voici un aperçu :

Une image contenant texte

Description générée automatiquement

* Ici on peut voir que les fichiers transmis par FTP ne sont pas chiffré, ils sont affiché en claire sur le réseau, on peut considérer cela comme une vulnérabilité pour une attaque « man in the midle ».
  + 1. Analysez le trafic FTP.
* On retourne maintenant sur le sniffer, dans l’onglet GUI on sélectionne le premier paquet FTP et on déroule la fenêtre de droite j’jusqu’en bas. On peut voir alors que les informations comme la commande utilisé et le prénom sont affiché en clair :

Une image contenant table

Description générée automatiquement

* On répète cette opération sur le deuxième paquet FTP, on peut alors s’apercevoir que le nom d’utilisateur du compte utilisé est également affiché en clair :

Une image contenant table

Description générée automatiquement

* Et enfin pour le troisième paquet FTP, on peut voir que le mot de passe est affiché en clair :

Une image contenant table

Description générée automatiquement

* Dans l’entête d’autres informations sensibles figurent en claire, ce sont les numéros de port sources et destination.

Dans l’en-tête FTP, quelles informations sont affichées en texte clair ?

1. Accéder à un routeur d’entreprise à distance à l’aide de Telnet
   * 1. Connectez-vous à un routeur d’entreprise à distance.

* Dans cette partie, nous étudierons le protocole Telnet afin de nous connecter à distance à un routeur d’une entreprise. Ici nous sélectionneront le site Healte at Home, puis le PC Dave, on utilise l’invite de commande en envoyant un ping a l’adresse **209.165.201.2 pour tester l’accessibilité :**

Une image contenant texte

Description générée automatiquement

* Ici on peut voir que le ping est réceptif, le test d’accessibilité est concluant.
* On se rend maintenant sur telnet pour cela on utilise la commande suivante « telnet **209.165.201.2 » dans l’invite de commande, puis on s’identifie => admin & cisco123 :**

Une image contenant texte

Description générée automatiquement

* On peut maintenant utiliser la commande « show users » on peut donc voir la connexion active de telnet :

Une image contenant texte, périphérique, mètre

Description générée automatiquement

* Il faut savoir que telnet est un protocole considéré comme non sécurisé pour gérer un appareil a distance car in n’utilise pas de chiffrement pour protéger les données transmises entre l’ordinateur client et l’appareil distant, cela signifie que les informations telles que les noms d’utilisateur et les mots de passe peuvent être intercepté et lues par des tiers malveillants lors de la transmission sur internet. De plus telnet ne verifie pas l’identité de l’appareil distant.

1. Accéder à un routeur d’entreprise à distance à l’aide de SSH
   * 1. Connectez-vous à un routeur d’entreprise à distance.

* Nous pouvons maintenant nous connecter à un routeur de l’entreprise à distance, pour cela on retourne dans Gotham Healthcare Branch, puis sur le PC Tim et on sélectionne l’invite de commande. Avant de commencer il est nécessaire de vérifier l’accessibilité du routeur, pour cela on effectue un test grâce à un ping :

Une image contenant texte

Description générée automatiquement

* Le test est concluant, on peut donc commencer, on entre la commande « ssh -l admin **209.165.201.2 » puis on s’identifie au prés du routeur avec le mot de passe « cisco123 » :**

Une image contenant texte

Description générée automatiquement

* Grace a la commande « show ssh », on peut voir la connexion active du ssh :

Une image contenant texte

Description générée automatiquement

* SSH est considéré comme un protocole sécurisé pour gérer un appareil a distance car contrairement à telnet on peut voir qu’une méthode de cryptage est utilisé Ici c’est le « HMAC ». De plus il verifie l’identité de l’appareil distant.
* Maintenant grâce au mode de configuration global accessible grâce a la commande « conf term » on peut créer un mot de passe secret d’activation :

Une image contenant texte, orange, sombre, ensemble

Description générée automatiquement

1. Fichier à utiliser : <Bloc1_sem1_tp00_decouverte_des_services_03.pka>
2. 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 | 255.255.255.0 | Metropolis Bank HQ |
| Mary | 10.44.3.101 | S/O | 255.255.255.0 | Healthcare at Home |
| Bob | 10.44.1.3 | S/O | 255.255.255.0 | Metropolis Bank HQ |

1. Objectifs

**Localiser les informations d’identification du compte FTP de l’ordinateur portable de Mary**

**Charger des données confidentielles par FTP**

**Localiser les informations d’identification du compte FTP du PC de Bob**

**Télécharger des données confidentielles par FTP**

**Déchiffrer le contenu du fichier clientinfo.txt**

1. Contexte

Dans cette activité, vous accéderez au contenu chiffré de plusieurs fichiers et transférerez un fichier vers un serveur FTP centralisé via Internet. Un autre utilisateur téléchargera ensuite le fichier du serveur FTP et déchiffrera le contenu des fichiers. L’adresse IP, le réseau et le service ont déjà été configurés. Vous utiliserez les appareils du client dans les différentes régions géographiques pour transférer un fichier avec des données chiffrées vers un autre appareil.

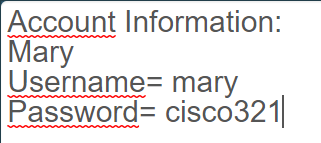
1. Localiser les informations d’identification du compte FTP de l’ordinateur portable de Mary
   * 1. Accédez au document texte sur l’ordinateur portable de Mary.

* Dans cette partie on souhaite avoir accès au document texte ftplogin.txt sur l’ordinateur de marie pour cela, on se rend d’abord sur celui-ci :

Une image contenant texte

Description générée automatiquement

* Comme on peut le voir ici les donnés son chiffré, pour remédier à cela, on utilisera un site internet => <https://encipher.it> on colle le texte crypté, on entre le mot de passe de déchiffrement => « maryftp123 », et voici le résultat :



* + 1. Déchiffrez les informations de compte FTP de Mary.
* On peut voir que le nom d’utilisateur est mary, et le mot de passe du compte FTP de Mary est cisco123.

1. Charger des données confidentielles par FTP
   * 1. Accédez au document texte sur l’ordinateur portable de Mary.

* Pour cette étape on renouvelle l’action précédente mais avec le fichier clientinfo.txt :

Une image contenant texte

Description générée automatiquement

* On peut voir ici que les données sont cryptées.
  + 1. Connectez-vous au serveur FTP à distance.
* Dans cette partie nous devons nous connecter au serveur FTP a distance, pour cela on ouvre l’invite de commande du PC Mary. Puis on se rend sur le site Métropolis Bank HQ en saisissant la commande suivante : **ftp 209.165.201.3 , puis on se connecte en entrant mary et cisco 321:**

Une image contenant texte

Description générée automatiquement

* + 1. Chargez le fichier sur le serveur FTP.
* Maintenant que la connexion sur le serveur FTP a été réalisé, nous pouvons charger le fichier sur le serveur FTP. Pour cela, nous allons d’abord utiliser la commande « dir » qui nous permettra de lister tous les fichiers présents sur le serveur FTP distant. Voici un aperçu de ces fichiers :

Une image contenant texte

Description générée automatiquement

* Pour charger le fichier voulue sur le serveur, on utilise la commande « put » suivis du fichier souhaité, dans notre cas c’est le fichier clientinfo.txt, voici le résultat :

Une image contenant texte

Description générée automatiquement

* En saisissant a nouveau la commande dir, on peut s’apercevoir que le fichier est maintenant présent sur le serveur :



* Si le transfert de fichier été intercepté via internet, on pourrait voire une suite de caractères incompréhensible, car celui-ci est crypté.

1. Localiser les informations d’identification du compte FTP du PC de Bob
   * 1. Accédez au document texte sur le PC de Bob.

* Dans cette partie, nous devons identifier l’es informations du compte FTP provenant du PC Bob. On se rend donc sur le pc de bob et on selectionne l’outil éditeur de texte et on ouvre le fichiers ftplogin.txt que l’on va copier et dechiffrer grâce au site utilisé au paravant. Ici on utilisera le mot de passe de déchiffrement bobftp123 :

Une image contenant texte

Description générée automatiquement

* On peut voir ici que le nom d’utilisateur est bob et le mot de passe est ninja123.

1. Télécharger des données confidentielles par FTP
   * 1. Connectez-vous au serveur FTP à distance.

* Ont souhaite maintenant télécharger les données confidentielle, pour cela on ouvre l’invite de commande du PC Bob et on saisie la commande ftp suivie de l’adresse du serveur pour s’y connecter :

Une image contenant texte

Description générée automatiquement

* On utilise l’’identifiant et le mot de passe décrypté ci-dessus pour se connecter.
  + 1. Téléchargez le fichier sur le PC de Bob.
* Maintenant pour télécharger le fichier sur le PC de Bob on utilise la commande « get clientinfo.txt » puis on saisit ensuite la commande quit :

Une image contenant texte

Description générée automatiquement

* Ici grâce à la commande dir, on peut voir que le fichier a été chargé correctement :



1. Déchiffrer le contenu du fichier clientinfo.txt
   * 1. Obtenez la clé de déchiffrement de la part de Mary.

* Maintenant que le transfert du fichier est terminé, il nous faut la clés de déchiffrement pour pouvoir lire le contenue du fichier. Pour cela on se rend dans la Messagerie du pc Bob, puis on clique sur receive et on sélectionne le mail avec pour objet « decryption key » et on enregistre la clé de déchiffrement :

Une image contenant texte

Description générée automatiquement

* Ici la clé qui permet de déchiffrer le fichier clientinfo.txt est « cisco123 ».
  + 1. Déchiffrez le contenu du fichier clientinfo.txt.
* On peut maintenant déchiffrer le contenue du fichier, il faut se rendre sur le PC Bob dans son éditeur de texte, on ouvre le fichier clientinfo.txt, on copie le contenue et on se rend sur le site de déchiffrement puis on utilise la clé de déchiffrement :

Une image contenant texte

Description générée automatiquement

* On peut voir que le nom du premier compte est « plato X. riggs ».

1. Fichier à utiliser : <Bloc1_sem1_tp00_decouverte_des_services_04.pka>
2. 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 |

1. Objectifs

* **Télécharger les fichiers clients sur le PC de Mike**
* **Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le PC de Mike**
* **Vérifier l’intégrité des fichiers clients à l’aide du hash**
* **Vérifier l’intégrité des fichiers sensibles à l’aide du HMAC**

1. Contexte

Durant cette activité, vous vérifierez l’intégrité de plusieurs fichiers à l’aide des hashs 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.

1. Télécharger les fichiers clients sur le PC de Mike
   * 1. Accédez au client de messagerie sur le PC de Mike.

* Dans cette partie, on souhaite télécharger les fichiers clients sur le PC Mike, Pour cela il nous faut l’accès au client de messagerie sur le PC Mike. On se rend sur le site Healthcare Branch puis sur le PC Mike, on ouvre le navigateur web et on saisit l’url suivante : [**http://www.cisco.corp**](http://www.cisco.corp) **, et on clique sur le lien de téléchargement :**

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

* Pour accéder à cette page à cette page web sur le serveur de sauvegarde, le protocole utilisé est http.
  + 1. Le serveur de fichiers a été piraté. Avertissez Sally.
* Ici dans le cas ou le serveur de fichier a été piraté, on nous demande d’avertir sally pour cela sur le site Gotham Healthcare Branche, on se rend sur le PC Mike, puis sur la messagerie, on créé un email pour l’avertir du piratage du serveur de fichiers :

Une image contenant texte

Description générée automatiquement

* Le mail est envoyé avec succès :

Une image contenant texte

Description générée automatiquement

1. Télécharger les fichiers clients du serveur de sauvegarde des fichiers sur le PC de Mike
   * 1. Accédez au serveur FTP hors site sur le PC de Mike.

* Nous devons maintenant transférer les fichiers client du serveur sur le PV Mike afin de les protéger, pour cela on accède au serveur FTP hors site sur le PC Mike, on ouvre le navigateur web et on saisit l’url suivante :

[**https://www.cisco2.corp**](https://www.cisco2.corp)**.**

* **On clique sur le lien pour afficher les fichiers les plus récents et leur hashs :**

Une image contenant texte

Description générée automatiquement

* Cette capture d’écran contient tous les hashs et les fichiers clients sur le serveur de sauvegarde.
* Ici pour accéder à cette page web, le protocole utilisé est HTTPS.
  + 1. Téléchargez les fichiers clients sur le PC de Mike.
* Il faut maintenant télécharger tous ces fichiers sur le PC Mike, pour cela on ouvre l’invite de commande, puis on se connecte au serveur de fichier de sauvegarde en saisissant ftp [**www.cisco2.corp**](http://www.cisco2.corp) **on sidentife avec mike et cisco123 :**

Une image contenant texte

Description générée automatiquement

* On peut maintenant télécharger les fichiers souhaité :

Une image contenant texte

Description générée automatiquement

* On termine en utilisant la command quit, puis dir afin de s’assurer que les fichiers sont bien présents :

Une image contenant texte, équipement électronique

Description générée automatiquement

1. Vérifier l’intégrité des fichiers clients à l’aide du hash
   * 1. Vérifiez les hashs sur les fichiers clients sur le PC de Mike.

* Il faut maintenant vérifier les fichiers hashs sur les fichiers clients sur le PC Mike pour cela sur le pc Mike on ouvre l’éditeur de texte puis on ouvre le fichiers NEclients.txt, on copie l’intégralité du contenue et on se rend sur le site <https://www.tools4noobs.com/online_tools/hash/>
* Celui-ci nous permettra d’obtenir le hashe du fichier. Une fois le texte collé, on clique sur Asher le contenue :

Une image contenant texte

Description générée automatiquement

* On répète cette opération pour les 5 autres fichiers :

NWclients.txt : Une image contenant texte

Description générée automatiquement

Nclients.txt : Une image contenant texte

Description générée automatiquement

SEclients.txt : Une image contenant texte

Description générée automatiquement

SWclients.txt : Une image contenant texte

Description générée automatiquement

Sclients.txt : Une image contenant texte

Description générée automatiquement

* Ici en comparant avec le resultat précédent :

Une image contenant texte

Description générée automatiquement

* On peut voir que tous les hashes ont été changé.
  + - 1. Sur le site **Gotham Healthcare Branch**, cliquez sur le PC **Mike**.
      2. Cliquez sur l’onglet **Poste de travail**, puis sur **Éditeur de texte**.
      3. Dans la fenêtre de l’éditeur de texte, cliquez sur **Fichier** > **Ouvrir**.
      4. Cliquez sur le premier document **NEclients.txt**, puis sur **OK**.
      5. Copiez l’intégralité du contenu du document texte.
      6. Ouvrez un navigateur web sur votre ordinateur, puis rendez-vous sur le site <https://www.tools4noobs.com/online_tools/hash/>.
      7. 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**.
      8. 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.
      9. 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 ?

* + 1. Téléchargez le fichier suspect sur l’ordinateur de Sally.
       1. Cliquez sur le site du **siège social de la Metropolis Bank**, puis sur l’ordinateur de **Sally**.
       2. Cliquez sur l’onglet **Poste de travail**, puis sur **Invite de commande**.
       3. Connectez-vous au serveur **Fichier de sauvegarde** en saisissant **ftp www.cisco2.corp** sur l’invite de commande.
       4. Saisissez le nom d’utilisateur **sally**, puis le mot de passe **cisco123**.
       5. À l’invite **ftp>**, saisissez la commande **dir** pour afficher les fichiers actuellement stockés sur le serveur FTP à distance.
       6. Téléchargez le fichier modifié identifié à l’étape 1 de la partie 3.
       7. À l’invite **ftp>**, saisissez la commande **quit**.
       8. 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.

1. Vérifier l’intégrité des fichiers sensibles à l’aide du HMAC
   * 1. Calculez le HMAC d’un fichier sensible.
        1. Sur le site **Metropolis Bank HQ**, cliquez sur le PC **Bob**.
        2. Cliquez sur l’onglet **Poste de travail**, puis sur **Invite de commande**.
        3. À l’invite **PC>**, saisissez la commande **dir**, puis vérifiez que le fichier **income.txt** se trouve bien sur l’ordinateur de Bob.
        4. Sous l’onglet **Bureau**, cliquez sur **Éditeur de texte**.
        5. Dans la fenêtre de l’éditeur de texte, cliquez sur **Fichier** > **Ouvrir**.
        6. Cliquez sur le document **income.txt**, puis sur **OK**.
        7. Copiez l’intégralité du contenu du document texte.
        8. Ouvrez un navigateur web sur votre ordinateur, puis rendez-vous sur le site <http://www.freeformatter.com/hmac-generator.html>.
        9. 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 ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Vérifiez le HMAC calculé.
       1. Sur le site **Metropolis Bank HQ**, cliquez sur le PC **Bob**.
       2. Cliquez sur l’onglet **Poste de travail**, puis sur **Navigateur web**.
       3. Saisissez l’URL **https://www.cisco2.corp**, puis cliquez sur **Go**.
       4. Cliquez sur le lien pour afficher les derniers fichiers et leur hash.

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

1. Fichier à utiliser : <Bloc1_sem1_tp00_decouverte_des_services_05.pka>
2. Table d’adressage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appareil | Adresse IP privée | Adresse IP publique | Masque de sous-réseau | Site |
| NTP/Serveur AAA | 10.44.1.252 | 209.165.201.5 | 255.255.255.0 | Metropolis Bank HQ |

1. Objectifs

**Partie 1 : Configurer le WEP pour Healthcare at Home**

**Partie 2 : Configurer le WPA2 PSK pour la succursale de Gotham Healthcare**

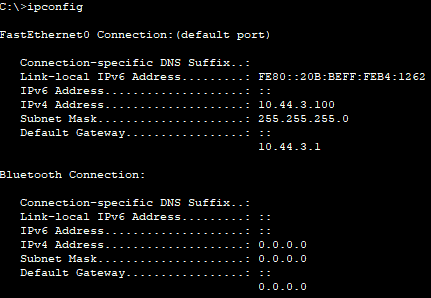
**Partie 3 : Configurer le WPA2 RADIUS pour le siège social de la Metropolis Bank**

1. Contexte

Au cours de cette activité, vous configurerez les réseaux Wi-Fi pour les trois sites. De plus, vous utiliserez à la fois le WEP, le WPA2 PSK et le WPA2 RADIUS afin de comprendre ces différentes configurations de réseaux Wi-Fi et leurs critères de sécurité. Le réseau Healthcare at Home sera configuré avec le WEP. Le réseau de la succursale de Gotham Healthcare sera configuré avec WPA2 PSK et le siège social de la Metropolis Bank utilisera WPA2 Radius. L’adresse IP, le réseau et le service ont déjà été configurés. Vous utiliserez des routeurs sans fil et des appareils client dans les diverses régions géographiques pour configurer plusieurs réseaux sans fil sécurisés.

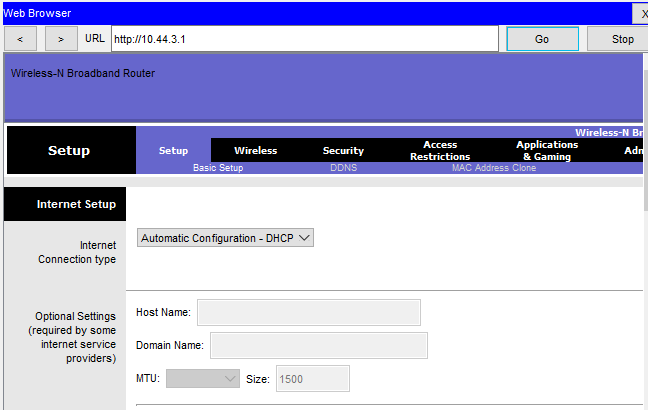
1. Configurer le WEP pour Healthcare at Home
   * 1. Configurez le SSID sans fil.

* Dans cette partie, nous devons configurer le SSID sans file, pour cela on se rend sur le site Healthcare at Home puis sur le PC0, on ouvre l’invite de commande et son saisie « ipconfig » :



* Il faut maintenant se rendre sur le navigateur web et saisir l’adresse de la passerelle par défaut :

Et on s’ydentifie => admin, admin voici, le résultat :



* On se rend dans l’onglet wirless (sans file) et on modifie le SSID en le remplassant par home :



* Et enfin on paramètre le SSID en diffusion et on sauvegarde les paramétres :



* Il faut maintenant paramétrer la sécurité sans fil, pour cela, on se rend dans l’onglet sécurité sans fil, et on sélectionne le mode de sécurité WEP, on saisie la clé **0123456789 qui correspond à la clé 1, et on enregistre les paramètres :**

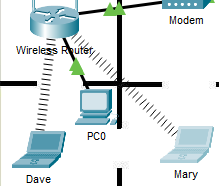
Une image contenant texte

Description générée automatiquement

* Le WEP n’est pas recommandé pour la sécurisation des réseaux sans fil car il comporte de nombreuses vulnérabilité tel que des attaques de cracking de clé, ces attaques peuvent permettre aux pirates de découvrir la clé transmises sur le réseaux.
  + 1. Connectez les clients.
* Il faut maintenant connecter le client, pour cela on utilise le portable de Dave et on se rend dans l’onglet pc wirless, on clique sur se connecter puis refresh :



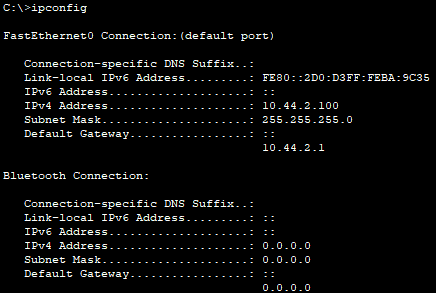
* On clique maintenant sur home puis sur connect et on entre ensuite le numéro de clé et on peut voir que le pc et connecté :



* On répète l’opération pour le pc Mary.

1. Configurer le WPA2 PSK pour la succursale de Gotham Healthcare
   * 1. Configurez le SSID sans fil.

* Nous pouvons maintenant passer à la configuration du SSID sans file, on se rend dans Gotham Healthcare Branche, puis sur le PC1, on selectionne l’onglet burreau et on ouvre l’invite de commande et on saisit ipconfig pour obtenir l’adresse de la paserelle par défaut :

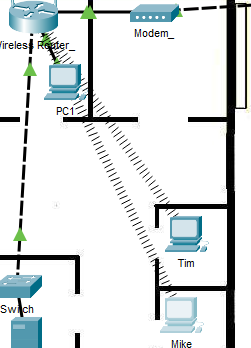


* On entre l’IP de la passerelle par défaut dans le navigateur web et on s’identifie avec admin admin on clique sur l’onglet wirless, et on modifie le SSID en l remplacent par BranchSite on modifie également la fréquence du canal standard par 6-2,437 GHz et le ssid sur diffusion, puis on sauvegarde les modifications.
  + 1. Configurez la sécurité sans fil.
* Il faut maintenant configurer la sécurité sans fil de façon optimal, pour cela on sélectionne le mode de sécurité WPA2 et on entre le mot de passe « **ciscosecure » et on sauvegarde les paramètres :**

Une image contenant texte

Description générée automatiquement

* + 1. Connectez les clients.
* Nous pouvons maintenant connecter les clients, on clique sur le pc de Tim on ouvre l’onglet « ordinateur sans fil », puis connecter et actualiser, on sélectionne le réseau BranchSite on entre **ciscosecure et on se connecte ont répète l’opération sur le pc Mike et on peut voir qu’ils sont maintenant connecté :**



1. Configurer le protocole WPA2 RADIUS pour le siège social de la Metropolis Bank
   * 1. Configurez le SSID sans fil.

* Dans cette partie, nous devons configurer le SSID sans fil su siége social de Métropolis Bank, on ouvre le pc Sally, puis le navigateur web et on entre l’IP => 10.44.1.251 et on s’identifie avec admin admin.
* On clique sur wirless on modifie le SSID en l’appelant HQ on remplace la fréquenceet on le met en mode diffusion, puis on enregistre les paramètres :

Une image contenant texte

Description générée automatiquement

* + 1. Configurez la sécurité sans fil.
* On configure maintenant le mode de sécurité :

Une image contenant texte

Description générée automatiquement

* + 1. Configurez le serveur RADIUS.
* Dans cette étape nous allons configurer le serveur RADIUS, pour cela on se rend sur le serveur NTP/AAA on sélectionne le service AAA et on saisit les infos suivantes :

Une image contenant table

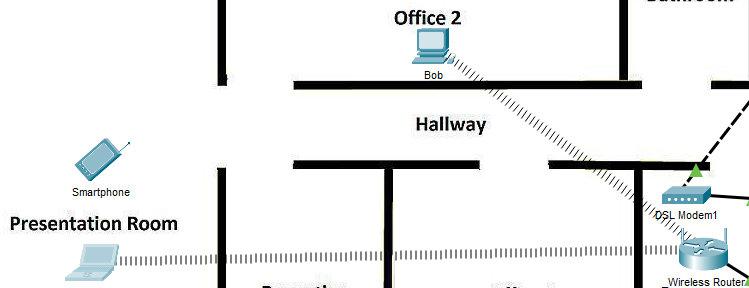
Description générée automatiquement

* Puis dans configuration de l’utilisateur, on entre les informations suivantes :

Une image contenant table

Description générée automatiquement

* + 1. Connectez les clients.
* Il faut maintenant connecter les clients :



* Dans le cadre d’une grande entreprise, le protocole WPA est préférable car car il offre une gestion centralisée des utilisateurs et des clés de chiffrement.

1. Fichier à utiliser : <Bloc1_sem1_tp00_decouverte_des_services_06.pka>
2. Table d’adressage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Appareil** | **Adresse IP privée** | **Adresse IP publique** | **Masque de sous-réseau** | **Site** |
| **Serveur Private\_FTP** | 10.44.2.254 | S/O | 255.255.255.0 | Gotham Healthcare Branch |
| **Serveur Public\_FTP** | 10.44.2.253 | 209.165.201.20 | 255.255.255.0 | Gotham Healthcare Branch |
| **Branch\_Router** | S/O | 209.165.201.19 | 255.255.255.248 | Gotham Healthcare Branch |
| **Ordinateur de Phil** | 10.44.0.2 | S/O | 255.255.255.0 | Metropolis Bank HQ |

1. Objectifs

**Partie 1 : Envoyer du trafic FTP non chiffré**

**Partie 2 : Configurer un client VPN dans Metropolis**

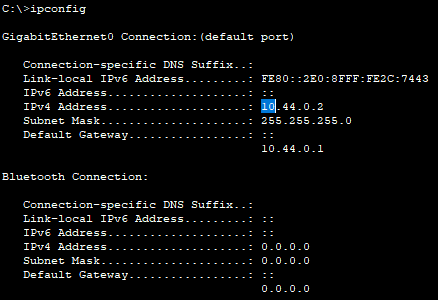
**Partie 3 : Envoyer du trafic FTP chiffré**

1. Le contexte

Au cours de cette activité, vous observerez le transfert d’un trafic FTP non chiffré entre un client et un site distant. Puis, vous configurerez un client VPN afin qu’il se connecte avec le site de la succursale de Gotham Healthcare et lui envoie un trafic FTP chiffré. L’adresse IP, le réseau et le service ont déjà été configurés. Vous utiliserez un terminal client du siège social de la Metropolis Bank pour transférer des données FTP chiffrées et non chiffrées.

1. Envoyer du trafic FTP non chiffré
   * 1. Accédez au détecteur d’intrusion

* Dans cette partie, nous devons envoyer de trafic FTP non chiffré, pour cela nous devons d’abord accéder au détecteur d’intrusion, on efface ensuite tous les éléments détecter.
  + 1. Connectez-vous au serveur Public\_FTP via une connexion FTP non sécurisée.
* Il faut maintenant que je me connecte au serveur Public\_FTP via une connexion FTP non sécurisé pour cela je me rend dans Métropolis Bank, sur le pc Phil, et j’ouvre l’invite de commande. Il faut ensuite utiliser la commande ipconfig pour connaitre l’IP actuelle de l’ordinateur :

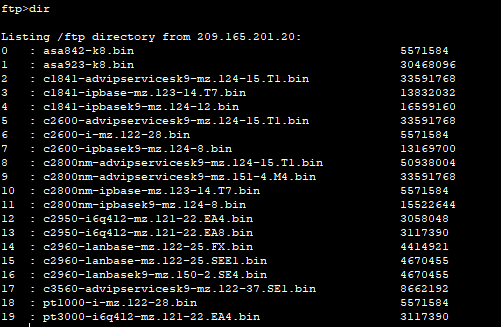


* Je saisit la commande ftp 209.165.201.20 pour me connecter au serveur public FTP => cisco, publickey :

Une image contenant texte

Description générée automatiquement

* J’utilise maintenant la commande dir pour lister les fichiers :

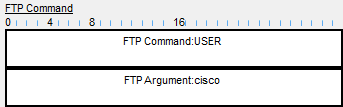


* Je peux maintenant transférer le fichier Publicinfo.txt sur le serveur FTP :

Une image contenant texte

Description générée automatiquement

* + 1. Affichez le trafic sur le Détecteur d’intrusion.
* Pour afficher le trafic du détecteur d’intrusion, je retourne sur celui-ci et je clique sur sur les messages FTP, voici un aperçu du premier :



* Dans l’ensemble des messages FTP, les informations affichées en clair sont le nom et le type fichier ainsi que les identifiants de connexions au serveur.

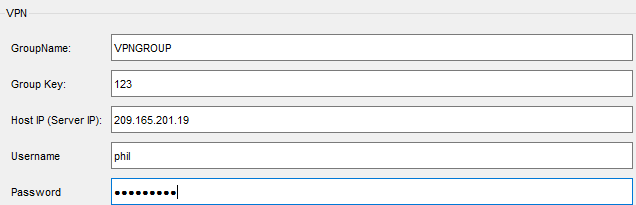
1. Configurer le client VPN sur l’ordinateur de Phil

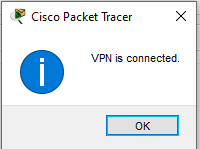
* Il faut maintenant configurer un serveur VPN sur l’ordinateur de phil, on commence par faire un test d’activité avec un ping vers le routeur :

Une image contenant texte, intérieur

Description générée automatiquement

* Ici le test est concluant. On peut donc commencer, il faut cliquer sur l’onglet VPN et saisir les caractères suivants :





* L’adresse IP du client pour la connexion est 10.44.2.200.

1. Envoyer du trafic FTP chiffré
   * 1. Affichez l’adressage IP actuel sur l’ordinateur de Phil.

* Aucune nouvelle IP ne s’affiche.
  + 1. Envoyez du trafic FTP chiffré de l’ordinateur de Phil au serveur Private\_FTP.

1. Saisissez **ftp 10.44.2.254** dans l’invite de commandes et connectez-vous au serveur **Private\_FTP** de la **succursale de Gotham Healthcare**.
2. Saisissez le nom d’utilisateur **cisco** et le mot de passe **secretkey** pour vous connecter au serveur **Private\_FTP**.
3. Transférez le fichier **PrivateInfo.txt** au serveur **Private\_FTP**.
   * 1. Affichez le trafic sur le Détecteur d’intrusion.
4. Agrandissez le **Détecteur d’intrusion** qui avait été réduit.
5. Cliquez sur les messages **FTP** affichés sur le détecteur.

Y a-t-il des messages FTP indiquant le mot de passe du réseau interne ou affichant le chargement du fichier PrivateInfo.txt ? Expliquez votre réponse.

1. Fichier à utiliser : <Bloc1_sem1_tp00_decouverte_des_services_07.pka>
2. Table d'adressage

|  |  |  |  |
| --- | --- | --- | --- |
| Appareil | Adresse IP privée | Masque de sous-réseau | Site |
| Serveur de sauvegarde du fichier | 10.44.2.254 | 255.255.255.0 | Gotham Healthcare Branch |

1. Objectifs

**Partie 1 : Envoyer du trafic FTP non chiffré**

**Partie 2 : Configurer un tunnel VPN entre Metropolis et Gotham**

**Partie 3 : Envoyer du trafic FTP chiffré**

1. Contexte

Au cours de cette activité, vous observerez le transfert de trafic FTP non chiffré entre deux sites géographiques. Vous configurerez ensuite un tunnel VPN entre deux sites géographiques, puis émettrez du trafic FTP chiffré. L'adresse IP, le réseau et le service ont déjà été configurés. Vous utiliserez les terminaux du client dans les différentes régions géographiques pour transférer des données FTP de façon sécurisée et non sécurisée.

1. Envoyer du trafic FTP non chiffré

* Dans cette partie, nous devons envoyer du trafic non chiffré, Pour cela on se rend dans le detecteur d’intrusions, dans l’onglet IU puis on efface les mouvements détéctés.
  + 1. Accédez au Détecteur d'intrusion.
       1. Cliquez sur **Détecteur d'intrusion** et sur l'onglet **IU**.
       2. Cliquez sur le bouton **Effacer** pour supprimer tous les mouvements détectés.
       3. Réduisez le **Détecteur d'intrusion**.
    2. Connectez-vous au serveur de sauvegarde FTP à l'aide d'une connexion FTP non sécurisée.
* On se rend maintenant dans Métropolis Bank et on clique sur l’ordinateur portable de phil, on uilise ensuite l’invite de commande avec la commande ipconfig pour afficher l’ip de l’ordinateur :

Une image contenant texte

Description générée automatiquement

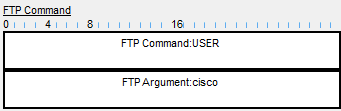
* Ont utilise ensuite la commande ftp 10.44.2.254 ET ON s’identifie avec cisco cisco :

Une image contenant texte

Description générée automatiquement

* + 1. Affichez le trafic sur le Détecteur d'intrusion.
* On retourne maintenant sur le detecteur d’intrusion et on peut voir la présence de deux messages FTP :

Message 1 :



Message 2 :

Une image contenant texte

Description générée automatiquement

* On peut voir que les informations affichées en texte claire sont les identifiants de connexions et le mot de passe et le numéro de la source de destination.

1. Configurer un tunnel VPN entre Metropolis et Gotham

* Nous devons maintenant configurer un tunnel VPN entre Métropolis et Gotham pour cela sur le site de Metroplis, on se rend sur HQ\_routeur, on copie la configuration du site VPN puis on la colle sur le routeur HQ routeur :

Une image contenant texte

Description générée automatiquement

1. Envoyer du trafic FTP chiffré
   * 1. Envoyez du trafic FTP du PC de Sally au serveur de sauvegarde de fichiers.

* Nous devons maintenant envoyer du trafic FTP du pc de Sally au serveur de sauvegarde des fichiers, pour cela sur le site du siege sociale de Metropolis Bank, on utilise le pc Sally, on ouvre l’invite de commandes, on utilise la commande ipconfig pour connaitre l’IP du poste :

Une image contenant texte

Description générée automatiquement

* On saisie ensuite la commande ftp 10.44.2.254 puis on s’identife avec cisco cisco :

Une image contenant texte

Description générée automatiquement

* Il faut maintenant utiliser la commande put pour charger le fichier FTPupload.txt sur le serveur de sauvegarde :

Une image contenant texte

Description générée automatiquement

* + 1. Affichez le trafic sur le détecteur d'intrusion.
* On retourne maintenant sur le sniffer de réseaux et on peut voir qu’il n’y a pas de message provenant de l’adresse IP de l’ordinateur de Sally car nous avons configurer une liste d’accès au serveur.