|  |  |  |  |
| --- | --- | --- | --- |
| F:\BTS cours\portfolio\logoIMC.jpg | **BTS SIO**  **Services Informatiques aux Organisations** | | F:\BTS cours\portfolio\logolaposte.jpg |
| **Option** | **SISR** |
| **Session** | **2015** |

|  |  |  |
| --- | --- | --- |
| **Costes Antoine** | **Activité professionnelle N°** | 6 |

|  |  |
| --- | --- |
| **NATURE DE L'ACTIVITE** | Projet personnel réalisé en formation : Secure Shell |
| **Contexte** | Pour pallier à certaines failles de sécurité relative à l’administration à distance des différents équipements constituant le réseau, l’administrateur a décidé de refondre son outil d’administration à distance en utilisant un protocole sécurisé empêchant ainsi de possibles prises de contrôle sur les équipements par des utilisateurs non autorisés. L’administrateur décide d’utiliser l’application SSH pour administrer son réseau. |
| **Objectifs** | Mise en place d’une communication sécurisée |
| **Lieu de réalisation** | IMC - Paris |

|  |
| --- |
| **SOLUTIONS ENVISAGEABLES** |
| Telnet |

|  |  |
| --- | --- |
| **DESCRIPTION DE LA SOLUTION RETENUE** | |
| **Conditions initiales** | Communication non sécurisé |
| **Conditions finales** | Communication sécurisé grâce au cryptage |
| **Outils utilisés** | Protocole Secure Shell de l’outil Putty |

|  |  |
| --- | --- |
| **CONDITIONS DE REALISATION** | |
| **Matériels** | Routeur, switch, machine |
| **Logiciels** | Putty |
| **Durée** | 2 heures |
| **Contraintes** | Respect des commandes CISCO |

|  |  |  |
| --- | --- | --- |
| **COMPETENCES MISES EN OEUVRE POUR CETTE ACTIVITE PROFESSIONNELLE** | | |
| A3.3.3  A3.3.1  A3.1.3  A1.4.1  A1.1.1 | - Productions relatives à la mise en place d’un dispositif de veille technologique et à l’étude d’une technologie, d’un composant, d’un outil ou d’une méthode  - Participation à un projet d’évolution d’un SI (solution applicative et d’infrastructure portant prioritairement sur le domaine de spécialité du candidat)  Gestion des identités et des habilitations  Administration sur site ou à distance des éléments d'un réseau, de serveurs, …  Prise en compte du niveau de sécurité nécessaire à une infrastructure  Participation à un projet  Analyse du cahier des charges d'un service à produire | |
| **DEROULEMENT DE L'ACTIVITE** | |
| **Mise en place du protocole Secure Shell :**  **Secure Shell :**  SSH est un protocole de communication sécurisé, qui permet, grâce à un programme informatique de se connecter à distance, communiquer, en toute sécurité grâce à la cryptographie. Cette fonction peut être utile en cas de problème sur une machine d’un parc informatique qui nécessite une intervention, cela facilite la tâche de l’administrateur.  En SSH, les données sont sécurisées par des algorithmes de cryptage symétrique et asymétrique :   * **Le cryptage asymétrique :** Le cryptage asymétrique, utilise une clé dite « publique » qui sert à crypter, une clé dite « privée » qui sert à décrypter. Avec ce type d'algorithme, on ne peut décrypter un message que si l'on connaît la clé privée. * **Le cryptage symétrique :** Avec cette méthode, on utilise une clé (un mot de passe secret) pour crypter un message la même est utiliser pour décrypter le message. Il faut donc que la personne qui crypte et celle qui décrypte connaissent toutes deux cette clé qui sert à crypter et décrypter.   Tout d’abord en utilisant le cryptage asymétrique pour échanger discrètement une clé de cryptage symétrique. Ensuite le cryptage symétrique crypte les échanges. Le symétrique est utilisé pour communiquer car il utilise moins de ressource, asymétrique juste pour l’échange de la clef privé du cryptage symétrique. En pratique il vous suffira d’entré un login et un mot de passe pour se connecter à distance.  **SSH et Telnet :**  SSH fait appel à la cryptographie forte pour protéger votre connexion contre les écoutes, les détournements et autres attaques. Telnet est un protocole plus ancien, qui offre une sécurité minimale.  SSH vous permet de vous connecter au serveur et de passer une commande dans la foulée, de façon à ce que le serveur exécute la commande et ferme la connexion tout seul, ce qui permet d'utiliser SSH pour des traitements automatisés, sans intervention humaine ce qui facilite le travail de l’administrateur.  Si la machine cliente et le serveur sont tous deux sur le même réseau, et si ce réseau est protégé par un pare-feu, il y a moins de danger à utiliser Telnet.  **SSH avec putty : mise en place du canal sécurisé :**  Processus de négociation client/serveur pour les méthodes de chiffrement (même algorithme)   * Spécifier la version du protocole SSH: Les options -1 et -2 forcent PuTTY à utiliser la version 1 ou la version 2 du protocole SSH.   C:\Users\Anto^n\AppData\Local\Microsoft\Windows\INetCache\Content.Word\versionSSH.PNG   * Choisir un numéro de port local, sur votre machine à vous, sur lequel PuTTY doit se mettre à l'écoute des connexions entrantes. Il y a probablement plein de numéros de port disponibles au-delà de 3000. * Avant de vous connecter en SSH à la machine distante, allez dans le panneau Tunnels. * Tapez le nom d'hôte et le numéro de port à utiliser sur la machine distante dans la case Destination, en les séparant par un deux-points (exemple : popserver.exemple.com:110 pour vous connecter à un serveur POP-3). * Spécifier une clé privé SSH: l'option -i vous permet d'indiquer le nom d'un fichier de clé privée au format \*.PPK, que PuTTY utilisera pour l'authentification auprès du serveur. * Nombre de tentative en cas d’échec de connection   C:\Users\Anto^n\AppData\Local\Microsoft\Windows\INetCache\Content.Word\nbrtentatives.png   * PuTTYgen est un générateur de clés. Il génère des paires de clés publiques et privées. Lorsque vous lancez PuTTYgen, vous obtenez une fenêtre où vous avez le choix entre 'Generate'.   C:\Users\Anto^n\AppData\Local\Microsoft\Windows\INetCache\Content.Word\PuTTYgen-Lancement.png  **Choix de la taille et donc de la solidité de la clé:** La clé RSA est générée en cherchant deux nombres premiers qui font chacun la moitié de la longueur demandée, et en les multipliant l'un avec l'autre. Si vous demandez à PuTTYgen une clé RSA de 1024 bits, il va prendre deux nombres premiers de 512 bits chacun et les multiplier ensemble. Le résultat de cette multiplication peut faire 1024 bits de long, mais il peut aussi n'en faire que 1023. Il se peut donc que vous n'obteniez pas exactement la longueur de clé que vous avez demandée.   * Délai renouvellement des clés :   C:\Users\Anto^n\AppData\Local\Microsoft\Windows\INetCache\Content.Word\delairenouvellementclef.png  Lorsque la connection sécurisée est établie, le client doit s’identifié au serveur par deux méthode : l’utilisation d’un ID et d’un mdp pour l’authentification.  **Sur le switch (ou routeur) :**  - Tout d’abord configurer un nom et déclarer le switch ou routeur dans un domaine.  - Puis on configure les mots de passe d’entrée enable et username  - Ensuite on génère les clés utilisées par SSH en spécifiant leur taille et leur type (ex: RSA).  - A ce stade, le routeur (ou switch) crée un couple de clé (clé publique et clé privée) sur la base des informations nom de domaine, username et loging.  - On termine de configurer les paramètres de base de SSH. | |

|  |
| --- |
| **CONCLUSION** |
| Secure Shell est un protocole de communication sécurisé. |

|  |
| --- |
| **EVOLUTION POSSIBLE** |
| OpenSSH, SSH File Transfer Protocol (pour le transfert de fichier) |