Administration d'un réseau local

I. Sécurité :

La sécurité est avant tout un ensemble de préconisations qu'il faut adapter aux besoins de chaque cas recontré. Il n'y a pas une seule méthode mais un ensemble de notions à prendre en compte. Ce chapitre tache d'en établir une liste qui ne peut être considérée comme exhaustive.

La sécurité à mettre en oeuvre dépend principalement des moyens qui seront mis en oeuvre pour les attaques et donc principalement de ce qui est à sécuriser. Il s'agit de trouver un juste équilibre entre le coût de la sécurité et les risques à assumer.

Lors de la mise en place d'une politique de sécurité, il est important de se rappeler que la sécurité doit être au service des utilisateurs, que ceux-ci ne doivent pas être gênés dans leur travail. Une sécurité qui ne se soucie pas des utilisateurs trouve très souvent là sa principale faille car le facteur humain reste toujours le maillon faible de la sécurité.

Une politique de sécurité prend en compte non seulement la sécurisation de l'accès aux données mais aussi la protection des données et de l'outils de production face à des évènements éventuellement destructeurs comme le vol, l'incendie ...

a – *Sécuriser l'accès physique au matériel*

- Protéger les locaux au travers d'une politique globale de sécurité : filtrage des accès à l'entreprise, mise à l'écart du matériel sensible (serveur, éléments actifs du réseau ...)
- Protéger le matériel et les données des agressions extérieures : utilisation de prises para-foudre, sauvegardes délocalisées, système anti-incendie. Prenez en compte l'ensemble des risques éventuels comme les inondations car le matériel réseau n'est pas évident à déplacer.
- Protéger le matériel du vol : les équipements critiques (serveurs, éléments actifs et passifs du réseau) ne doivent pas être accessible à tous.
- Prévoir des connexions réseaux de secours : un câble peut être victime d'un engin de chantier, de rats ... La réparation peut être une opération longue, bloquant la production.

b – *Sécuriser les données*

- Sauvegarder toutes les données : implique la mise en place de systèmes de stockage centralisés, plus sûrs que la sauvegarde de nombreux répertoires sur de nombreuses machines. Implique aussi d'être à même de pouvoir restaurer les sauvegardes faites.
- Sortir les données de l'entreprise pour les protéger d'un incendie par exemple. Ceci doit être fait dans le respect des règles de confidentialité éditées dans la politique générale de sécurité... Des entreprises proposent ce type de service.
- Utiliser des systèmes de stockage redondants, de type RAID, permettant de récupérer les données lors du crash d'un disque sans rupture du service.
- Utiliser des antivirus qui seront régulièrement mis à jour. Sensibiliser le personnel sur la provenance des virus et les règles simples à suivre pour les éviter.

c – *Garantir la continuté du service*

- Utiliser des serveurs aux services redondants (contrôleurs de domaine principaux/secondaires par exemple) pour palier aux problèmes liés à l'interruption de service.
- Utiliser des systèmes de sauvegarde permettant un changement de support à chaud (Hot-Plug) en cas de problème.
- Utiliser des systèmes intégrant une alimentation redondante, élément souvant le plus faible.
- Prévoir des solutions contre les micros-coupures et coupures de courant pour, à la fois éviter un arrêt non sécurisé des serveurs, éviter un redémarrage long des services et ainsi permettre une utilisation continu du matériel, y compris durant une coupure de courant. Dans ce dernier cas, tous les éléments doivent être sécurisés : oublier le matériel réseau par exemple rendrait la démarche totalement inefficace.
- Prévoir la reconstruction rapide d'un système détruit : création d'une image du système de base.
- Investir dans du matériel de qualité.

d – Sécuriser l'accès au réseau

- Ne pas brasser (activer) les prises non utilisées de sorte à éviter les connexions imprévues et l'écoute du réseau (des mots de passe peuvent circuler en clair, comme bon nombre d'informations stratégiques).
- Eviter ou plutôt restreindre l'allocation dynamique d'adresses IP de sorte à ne pas simplifier la tâche d'un éventuel pirate. Limiter et surveiller les adresses MAC (adresses physiques des cartes réseau, difficiles à modifier) de sorte à prévenir de la connexion d'un appareil non autorisé.
- Utiliser au maximum des équipements de commutation (switch) de sorte à limiter les possibilités d'écoute sur le réseau.
- Utiliser avec précaution les technologies sans fil, toujours activer le maximum de protections possibles (cryptage, restriction d'accès...)

e – *Sécuriser l'accès aux données et logiciels*

- Limiter les accès aux personnes en ayant besoin : mettre en oeuvre une politique de gestion de comptes utilisateurs, associés à des mots de passe.
  La politique de gestion des mots de passe est un point important de la politique de sécurité : le choix des mots de passe doit être de préférence à l'origine des utilisateurs de sorte à simplifier leur mémorisation. Un mot de passe difficile à mémoriser est un mot de passe écrit à côté de l'ordinateur ! Toutefois, certaines règles doivent être mises en place pour contraindre à l'utilisation de mots non disponibles dans un dictionnaire : utilisation de minuscules, majuscules, caractères spéciaux et taille minimale... Les mots de passe ne doivent pas être changé trop souvent pour être bien acceptés, toutefois, il est impératif de maintenir la base des mots de passe (et des utilisateurs) à jour : le départ d'une personne doit impérativement avoir pour effet la suppression (ou la désactivation) de son compte. Testez vous même les outils des pirates sur vos propres bases.
- Restreindre au maximum les plages d'accès possible : de nombreuses attaques ont lieu lorsque personne n'est présent (nuit, week-end) autant interdire tous les accès à ces moments là.

- Utiliser des moyens d'identification forts si le besoin se présente : carte à puce, biométrie...
- Empécher les accès aux lecteurs de disquettes ou CDROM qui peuvent être utilisés pour démarrer un système permettant de cracker le système présent sur le disque. Généralement une protection du Bios associé à la suppression du demarrage sur ces périphériques aura un effet suffisant... toutefois, le mot de passe du bios est simple à supprimer... Empêcher alors l'ouverture du micro-ordinateur (solution permettant de limiter également les vols).

f – *Sécuriser l'accès au réseau*

Le réseau est un point sensible du système : du fait de sa connexion vers le monde entier il offre à des individus physiquement éloignés, comme aux employés, un accès à vos données.

- Séparer le réseau interne de l'accès externe en utisant des éléments dédiés à celà : les FireWall. Préférez l'utilisation d'un équipement spécifique ou dédié plutôt que l'activation de cette fonctionnalité sur un serveur proposant d'autres services.
- Mettre en place un système de suivi des intrusions de sorte à évaluer le risque à un moment donné.
- Mettre en place un système de suivi des connexions de sorte à détecter d'éventuelles anomalies.
- Séparer le réseau interne (privé) du réseau public (ensemble des services mis à dispodition depuis Internet) . La partie publique de l'entreprise est placée dans une zone non sécurisée appelée (DMZ Zone DéMilitarisée). Cette DMZ peut toutefois être filtrée au travers d'un FireWall. Un FireWall beaucoup plus sécurisé sera mis en place entre le réseau privé et le réseau public. Le but de cette démarche et de protéger le réseau privé d'une attaque provenant de la DMZ. En effet, il est plus difficile de protéger un serveur qui doit être public.
- Suivre les mises à jours de logiciels et systèmes ainsi que les rapports de bugs publiés fréquement. Prévenir étant toujours mieux que de guérir.

Malgrès la mise en oeuvre de toutes ces règles et de sans doute bien d'autres encore, la sécurité d'un système ne peut être assurée qu'avec l'aide des utilisateurs. Ceux-ci doivent donc être sensibilisés aux risques et connaitre les règles de base de la sécurité comme par exemple ne **jamais** donner son mot de passe, y compris à l'administrateur qui, normalement, ne doit jamais en avoir besoin. La façon la plus simple de pénétrer un système étant bien souvent d'en demander l'accès à un utilisateur non averti.

Une nouvelle fois, gardez toujours en tête que l'administrateur système doit être au service de l'utilisateur de l'informatique, toutes les règles mises en oeuvre, aussi restrictives qu'elles soient doivent être accompagnées d'un service irréprochable de votre part les rendant ainsi transparentes et surtout non contraignantes.

II.Mise en place de serveurs :

a – *choix du matériel*

Le mot serveur, n'est pas à associer avec ordinateur dernier cri... comme pour tout système il est nécessaire d'évaluer le besoin exact de sorte à obtenir le service désiré à un coût adapté. Le choix du matériel doit surtout se faire suivant des critères d'évolutivité et de qualité. Les puissances et quantités de mémoire nécessaires sont généralement évaluée par les éditeurs de logiciels et fonctions du nombre d'utilisateurs ou connexions attendu. S'y référer est l'assurance d'une puissance suffisante sans exagération.

b – *choix des logiciels*

Il est important de s'élever au dessus des guerres de clochers entre solutions libres ou propriétaires pour choisir un système en fonction de ses besoins. Il est important que le système réponde exactement au besoin et n'entraine pas de ralentissement de la production. Il est tout aussi important que le logiciel soit conforme aux besoins, établis, de sécurité.

Il est de l'attribution de l'administrateur de gérer correctement les licenses des logiciels. Les risques encourus par l'entreprise en cas d'utilisation frauduleuse de logiciels sont conséquents. Vous devez donc veiller à tenir à jour la liste des logiciels installés et vous assurer que l'entreprise possède bien toutes les licences associées. Les licenses peuvent être établies par siège ou par serveur. Dans le premier cas, vous devez posséder une licence par utilisteur potentiel du logiciel. Il s'agit du mode généralement rencontré lorsque le logiciel est installé directement sur le poste client. Dans le second cas, la license limite le nombre d'utilisateurs simultanés du logiciel. Ce mode est courant dans une utilisation de serveurs d'applications. Le nombre des accès à un serveur Windows est aussi contraint par le même système de licence, ainsi, il faut veillez, en plus de l'achat du système à l'enregistrement de suffisemment de licences pour permettre aux utilisateurs un accès simultané.

Il est important que les utilisateurs ne puissent pas installer de logiciels sur leurs ordinateurs, sans quoi vous ne pourrez maîtriser la gestion des licences. Il est tout aussi évident que vous devez trouver pour eux des solutions à leur besoin. Les logiciels libres sont souvent une solution gratuite et de bonne qualité. Refuser de trouver une solution est sans nul doute le meilleur moyen de s'exposer à des installations anarchiques d'outils piratés.

c – *mise en oeuvre de technologies RAID*

Les normes RAID (Redundant Array of Independent Disks) sont employées lors de l'utilisation de grappes de disques :

- RAID0 : permet l'utilisation de plusieurs disques physiques comme un seul disque logique de très grande taille. Cette norme permet de s'affranchir de la limite d'espace offert par les disques dur du marché.
- RAID1 : utilisation de 2 disques comme un seul (miroir). Ce système offre deux avantages : augmenter le débit du disque logique ainsi créé (deux accès concurents possibles en lecture) et sécuriser les données. En effet, la destruction d'un disque n'entraine pas la perte de la copie présente sur le second.

- RAID2 : répartition de l'information sur plusieurs disques et ajout de codes de détection/correction d'erreurs sur d'autres disque. Cette architecture est peu utilisée du fait qu'elle n'apporte pas grand chose par rapport aux autres systèmes RAID.
- RAID3 : stockage des données sur plusieurs disques en parallèle, un disque supplémentaire est utilisé pour stocker la parité. Cette information est suffisante pour récupérer l'information totale lors de la destruction d'un disque. Cette technologie est obsolète.
- RAID4 : version améliorée de RAID3, elle aussi obsolète. Le principal problème des configuration RAID3 et RAID4 vient du fait que le disque de parité constitue un goulot d'étranglement car il doit être mis à jour lors de chaque écriture.
- RAID5 : fonctionne sur le même principe que RAID3/4 hors mis le fait que chaque disque contient à la fois des données et des informations de parité, du coup l'écriture de la parité ne constitue plus un goulot d'étranglement.

Les normes RAID peuvent être mises en oeuvre de façon matérielle avec des cartes spécifiques (parfois aussi présentes sur les cartes mère) ou de façon logicielle sur les systèmes WindowsNT/2K et Linux. Des systèmes dédiés au stockage (NAS Network Attached Storage) peuvent aussi être déployés. Le système RAID autorise le changement de disque à chaud (Hot-Plug) toutefois, ceci n'est possible que lorsque le matériel le permet, d'où une préférence pour du matériel SCSI ou NAS.

d – *intégration des serveurs dans le réseau*

Les serveurs sont normalement les éléments qui concentrent le plus d'informations et d'accès au sein du réseau. Il doivent donc être privilégiés. En général, il est interressant d'offir aux serveurs un débit réseau supérieur au débit offert aux autres utilisateurs. Cette dissymétrie permettra d'offrir un accès plus équitable, entre les utilisateurs, aux serveurs.
Les transferts de fichiers vont par exemple monopoliser une grande partie de la bande passante disponible. Si celui-ci est contraint par un débit faible au niveau utilisateur, il ne dégradera que peu le débit global offert par le serveur.
L'utilisation de réseaux utilisateur 10Mbits reste souvent suffisant dès lors qu'il n'y pas pas d'échange de fichiers volumineux. Toutefois, les investissements doivent d'orienter vers des solutions 100Mbits qui pourront être bridées par exemple. Le coté serveur sera, lui, privilégié en utilisant la technologie supérieure : 100Mbits pour 10Mbits coté utilisateurs ou 1GBits pour 100Mbits coté utilisateurs.

III.Plan d'adressage IP

Pour tout réseau doit être mis en place un plan d'adressage IP. Il s'agit de savoir quelles sont les adresses attribuées et quels sont les services offerts sur ces adresses. Le but est d'être capable de trouver de nouvelles adresses disponibles et de retrouver la liste des services offerts. Les adresses IP doivent permettrent de localiser des équipements et donc des utilisateurs qui pourront ainsi être surveillés.

Il peut être important de garder une certaine marge quant au nombre des adresses IP disponibles. Vous ne savez pas forcement quelle va être l'évolution de la société ou de ses services. Ainsi, la restriction des plages libres risque d'entrainer une modification votre plan d'adressage à brève échéance. Cette opération pouvant être fastidieuse elle conduit souvent à une étape intermédiaire où l'attribution d'adresses devient déstructurée (attribution d'adresse sur des sous réseaux non adaptés pour palier au manque d'adresses libres).

Il ne faut pas hésiter à mettre en oeuvre plusieurs sous réseaux de sorte à isoler physiquement certain brins et ainsi optimiser l'utilisation de la bande passante. La création de sous réseaux doit se faire suivant deux critères : les permissions d'accès octroyées à un groupe et les besoins d'accès aux données et serveurs. La mise en oeuvre de sous-réseaux demande l'installation de routeurs, qui peuvent être des équipements spécifiques ou des ordinateurs.

L'utilisation de système tels que le DHCP permet de rendre la configuration des postes clients automatique, du coup, il sera plus aisé de réaliser des modifications sur la plan d'adressage. Le DHCP permet de parametrer de façon globale l'ensemble de la couche IP. De sorte à concerver les notions de localisation et pour éviter l'arrivée sur le réseau de nouvelles machines non désirées, le DHCP doit être bridé pour qu'une adresse IP soit toujours attribuée à une machines clairement identifiées.

Les équipements, tels que les serveurs et les routeurs doivent utiliser des adresses choisies soit en début, soit en fin de réseaux de façon à les mémoriser simplement et les isoler des autres. Ceci est une convention plus qu'une obligation.

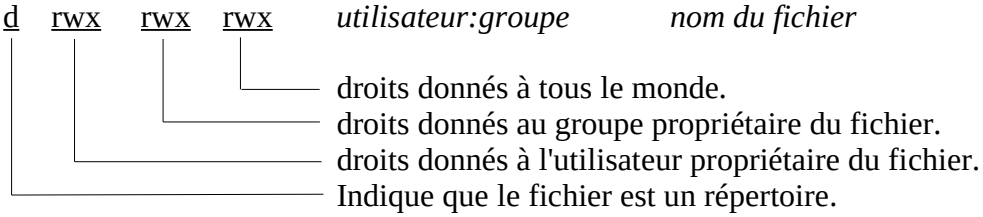
Le plan d'adressage est un document papier qui doit être tenu à jour et concervé.

Un serveur de nom (DNS-WINS) peut être mis en oeuvre pour identifier les serveurs et les postes clients autrement que par des adresses IP : celles-ci sont toujours sujettes à modification et difficiles à retenir.

IV.Gestion des utilisateurs

a – *Gestion des droits :*

Chaque fichier d'un système est associé à des droit d'accès. Ceux-ci permettent de restreindre les posibilités de lecture, d'écriture et d'exécution. Un fichier (ou programme, ou répertoire) appartient à un utilisateur et à un groupe. Les droits d'un fichier, dans le monde Unix sont présentés sous la forme suivante :



Ainsi, un programme peut être rendu exécutable pour l'utilisateur propriétaire et lui seul :

rwx --- --- *utilisateur:groupe* *nomdufichier*

Un document peut être mis à la disposition de tous mais resteaint, pour ce qui est des modifications, au créateur et ceux de son groupe.

rw- rw- r-- *utilisateur:groupe* *nomdufichier*

Notez que pour un document, l'exécution n'est pas apparente.

Rq : un repertoire possède des droits en exécution, ce droit est vérifié pour lister le repertoire. Les restrictions appliquées sur un répertoire s'appliquent à tous les fichiers qu'il contient mais aussi à tous ses sous-répertoires.

b – *Création de comptes utilisateurs*

Chaque utilisateur pouvant se connecter sur un système doit posséder un compte, celui-ci lui autorise l'accès au travers d'un identifiant (login) et d'un mot de passe. Cette utilisateur est aussi généralement associé à un espace disque qui lui sera propre.

Chaque utilisateur possède à un groupe principal. Géréralement les groupes principaux sont créés en fonction des besoin d'échange : les fichiers créés par l'utilisateur auront comme propriétaire celui-ci et comme groupe propriétaire le groupe principal de l'utilisateur. Il sera donc simple d'autoriser à tous les utilisateurs d'un groupe la consultation de ce document. Réciproquement, il sera simple d'interdire l'accès à ces même données si l'existance de plusieurs groupe principaux existe.

Les groupes principaux peuvent être par exemple *profs, élèves, compta, direction ...*

Exemple : *Nous souhaitons que les utilisteurs de la direction aient leur propre repertoire personnel et que celui-ci soit protégé contre la consultation par des tiers. Toutefois pour l'echange de fichiers, nous souhaitons ajouter un repertoire commun de partage.*

Dans le repertoire *home* où se trouve l'ensemble des repertoires utilisateurs, nous trouvons.

Utilisateur	***Groupe***	***Tous***	***utilisateur:groupe***	***nomDuRepertoire***
drwx	---	---	*grandchef : direction*	*grandchef*
drwx	---	---	*petitchef : direction*	*petitchef*
drwx	---	---	*souschef : direction*	*souschef*
drwx	*rwx*	---	*root:direction*	*partage_direction*

c – *Droits d'utilisation de logiciels :*

La gestion des droits d'utilisation d'un logiciel, mais aussi celle d'accès à certain répertoires ou périphériques fonctionne sur un principe similaire : Par exemple, si l'on souhaite restreindre l'accès de StarOffice à certains utilisateurs, il suffira de créer un groupe pour ce logiciel (so*_users*) . Ensuite, les utilisateurs autorisés à lancer ce logiciel seront ajoutés à ce nouveau groupe. En effet, un utilisateur possède un groupe principal mais il peut aussi appartenir à plusieurs groupes secondaires.

Suivant cet exemple nous aurons :

droits de l'exécutable de starOffice :

- rwx	*rwx*	*---*	*root:so_users*	*staroffice*

note: le fichier appartient à l'administrateur et fait parti du groupe su_users. Tous les utilisateurs devant accéder à ce logiciel seront rattachés à ce groupe :

utilisateur	***groupe principal***	***groupes secondaires***	***remarque***
grandchef	*direction*	*so_users*	*peut utiliser StarOffice*
petitchef	*direction*	*epb_users*	*ne peux pas utiliser StarOffice*
moyenchef	*direction*		*ne peux pas utiliser StarOffice*
comptable	*comptable*	*so_users, ebp_users*	*peut utiliser StarOffice*

Il en est de même pour le partage des répertoires :

droits du repertoire des données financières :

d rwx	*rwx*	*---*	*root:finances*	*données_financières*

groupes des utilisateurs :

utilisateur	***groupe principal***	***groupes secondaires***	***remarque***
grandchef	*direction*	*so_users, finances*	*peut acceder au repertoire*
petitchef	*direction*	*epb_users*	*ne peux pas accéder au repertoire.*
moyenchef	*direction*	*finances*	*peut accéder eu repertoire*
comptable	*comptable*	*so_users, ebp_users, finance*	*peut accéder eu repertoire*

d – *Configuration des droits*

Sur les systèmes Windows, la gestion de ces droits se fait de façon graphique au travers de cases à cocher correspondant aux diférents droits de lecture, écriture et exécution. Mais, comme tout n'est pas fichier (contrairement au monde Unix), un utilisateur peut avoir des droits lui étant directement associés comme le réglage de l'heure, l'arrêt de la station....

Sur les systèmes Unix, la manipulation graphique des droits est aussi possible, toutefois l'utilisation de la ligne de commande reste un outil plus puissant permettant entre autre la mise au point de scripts utiles s'il est necessaire de modifier l'organisation complète des droits. Tout étant fichier sous Unix, l'application de droits comme l'arrêt de la station se fait simplement par l'autorisation ou non d'exécution de la commande *reboot* par exemple...

Pour plus d'informations, se référer aux commandes *chown (choix du proprietaire d'un fichier), chmod (modification des droits d'un fichier), useradd, groupadd (ajout d'utilisateurs et de groupes).* Voir aussi les fichiers */etc/passwd (Liste des utilisateurs)* et */etc/group(Liste des groupes).*

e – *Le super-utilisateur :*

Le super utilisateur est appelé *root* dans le monde Unix et *Administrateur* dans le monde Windows Francophone. Cet utilisateur possède tous les pouvoirs, y compris et surtout ceux de détruire le système. Par conséquent, l'utilisation de cet utilisateur lors d'une utilisation classique du système doit être clairement bannie !.

Il est généralement plus interessant de se connecter à un système en temps qu'utilisateur classique (aux pouvoirs restreints) puis, pour certaines tâches le nécessitant, de devenir super-utilisateur en changeant d'identité. Ce changement étant possible au travers de la commande *su* dans les environnements UNIX.

Le super utilisateur doit être le seul à pouvoir modifier les fichiers concernant le coeur du système. Il doit aussi le seul à pouvoir tuer les processus de tous les utilisateurs.

Le super utilisateur peut consulter toutes les données d'un système y compris les répertoires personnels des utilisateurs.

f – *Suppression d'utilisateurs :*

Un utilisateur qui n'a plus de raison ou plus le droit de se connecter doit être supprimé, si toutefois vous souhaitez maintenir son compte existant, vous devez tout de même le désactiver.

V.Administration distante des serveurs

a – *Les outils d'administration à distance par prise de contrôle*

La prise à contrôle d'un poste à distance permet de l'administrer en profitant pleinement des outils de l'interface graphique. Cette methode est aussi très souvent utilisée pour le dépannage d'un utilisateur : la prise de contrôle de son poste permet de lui montrer, sans se déplacer mais tout en manupulant “son” clavier et “sa” souris, comment régler son problème.
Il existe plusieurs solutions pour celà, elles sont de deux types :

- La copie de l'image de l'écran distant sur le poste local : ce système existe sous forme de produits commerciaux ou gratuits (VNC). Il permettent de manipuler l'ordinateur distant sous les yeux de l'utilisateur. Ce système est généralement très gourmand en bande passante, le rafraichissement peut donc être long, rendant les manupilations fastidieuses.
- L'utilisation des fonctionnalités des systèmes d'exploitation : les serveurs X et Windows sont prévus pour que l'affichage d'élements graphiques générés en local puissent être déportés sur un autre poste (ou terminal) ainsi, il est possible de se connecter à distance sur un autre équipement. Ce mode est en fait l'utilisation des systèmes ancestraux utilisant un serveur d'application commandant à des terminaux l'affichage des éléments. Cette solution réduit les besoin en bande passante : lors du déplacement d'une fenêtre, seules les nouvelles coordonnées sont transmises... Par contre, elle ne permet pas toujours la gestion de l'affichage simultané sur les deux postes.

b – *Les outils d'administration à distance en ligne de commande :*

La ligne de commande est souvent le moyen idéal pour contrôler un système, les possibilités sont généralement (sur les systèmes Unix) plus complètes que l'utilisation des interfaces graphiques. Il existe de multiples outils, les plus anciens sont *telnet, rlogin, rsh* qui permettent de se connecter à un système distant pour y exécuter des commandes. Ces systèmes avaient un prolème majeur tenant au fait que les mots de passes sont émis en clair sur le réseau ! Par conséquent, l'utilisation n'en est pas à bannir, mais la connexion en tant qu'administrateur, est à proscrire.
Des outils plus récents comme *ssh* solutionnent ce problème en cryptant la communication. *Ssh* permet une connexion distante pour l'exécution de commande mais aussi pour le transfert de fichiers et le lancement d'applications graphiques.

L'administration d'un système UNIX par ce moyen peut se faire à 100%, les serveurs pour Windows sont beaucoup plus rare, toutefois Microsoft oriente ses futurs développement dans ce sens.

c – *Les outils d'administration à distance utilisant le web :*

De nombreux outils existent pour administrer un ordinateur à distance au travers d'un navigateur web. Ils reposent sur la création d'une interface graphique commandant l'exécution de scripts appliquant les modifications. Ces outils sont généralement moins puissant que la ligne de commande mais ils ont l'avantage d'être simples et peuvent être uniformisés pour plusieurs systèmes ou plusieurs distributions d'un système.

d – *Les outils de surveillance à distance :*

Un protocole est dédié à l'administration et surtout la surveillance d'équipements à distance. Il s'agit de SNMP. Ce protocole repose sur des méthodes *get* et *set* permettant d'interroger un équipement sur une de ses valeurs, voir de modifier celle-ci. Les possibilités de configuration sont toutefois souvent limitées car le protocole SNMP ne prévoit aucune protection, aucun système de mot de passe ou autre, si ce n'est un paramètre *communauté* laissé au libre choix de l'administrateur.
Les informations interrogeables sont décrites dans une *MIB* et peuvent être différentes pour chaque équipement toutefois, les *MIB* sont généralement proches les unes des autres. Les informations sont identifiées dans la *MIB* au travers d'une adresse identifiant le noeud de l'information.
Ces outils sont très souvent mis en oeuvre pour la surveillance de la charge d'un système et son bon fonctionnement. SNMP permet à ce sujet, l'envoie de *traps*, c'est à dire de messages indiquant pas exemple la coupure d'une ligne, un problème, la connexion d'un utilisateur .... Ces *traps* sont utiles pour surveiller le réseaux, déceler des pannes ou des intrusions.

La majeure partie des éléments composant un réseau sont administrables : les serveurs, bien sûr, mais aussi les éléments actifs comme les routeurs, les firewall, les switchs. Les éléments passifs, comme les hubs, peuvent aussi l'être. Il est important lorsqu'un élément est configurable de regarder comment l'adapter au mieux a votre réseau : une grande partie des équipements est “plug and play”, c'est à dire qu'il fonctionnent dès la mise sous tension grâce à une configuration par défaut simpliste. Dans de très nombreux cas, cette configuration entraine d'énormes trous de sécurité.