Introduction aux attaques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une « **attaque** » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

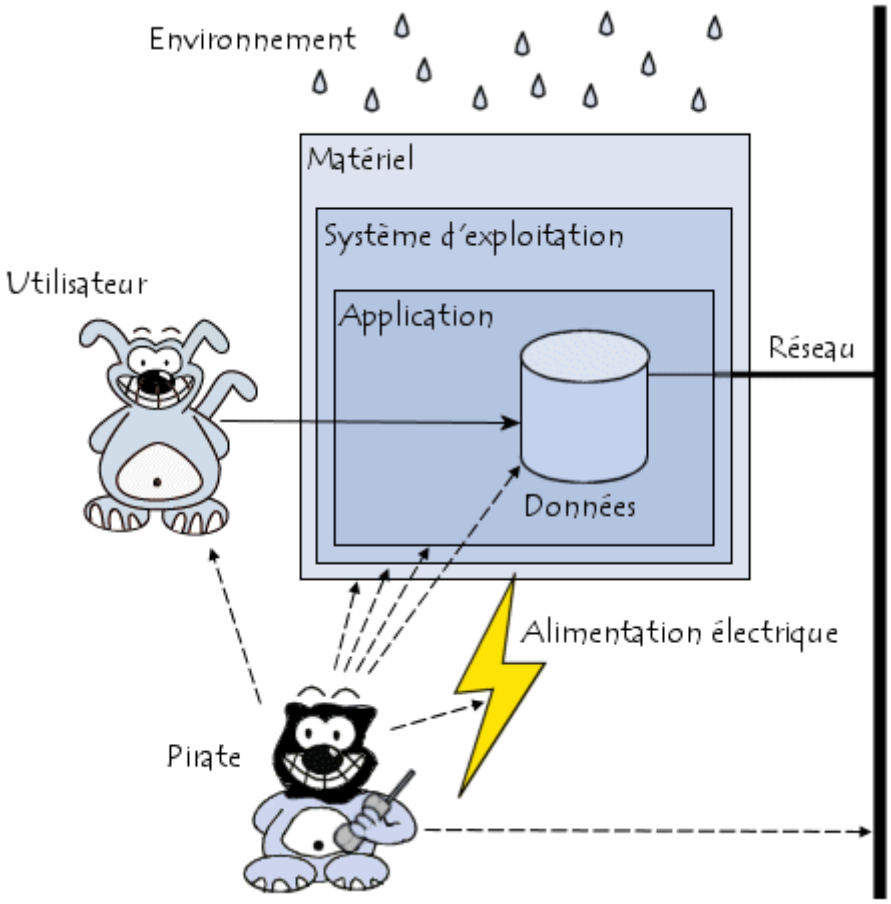
Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- glaner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

Types d'attaques

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau.

Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Le schéma ci-dessous rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe :



Il est ainsi possible de catégoriser les risques de la manière suivante :

- **Accès physique** : il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :
  - Coupure de l'électricité
  - Extinction manuelle de l'ordinateur
  - Vandalisme
  - Ouverture du boîtier de l'ordinateur et vol de disque dur
  - Ecoute du trafic sur le réseau
- **Interception de communications** :
  - Vol de session (*session hijacking*)
  - Usurpation d'identité
  - Détournement ou altération de messages
- **Dénis de service** : il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
  - Exploitation de faiblesses des protocoles TCP/IP
  - Exploitation de vulnérabilité des logiciels serveurs
- **Intrusions** :
  - Balayage de ports ;
  - Elévation de privilèges : ce type d'attaque consiste à exploiter une vulnérabilité d'une application en envoyant une requête spécifique, non

prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à un accès au système avec les droits de l'application.
    - Les attaques par **débordement de tampon** (en anglais *buffer overflow*) utilisent ce principe ;
    - Maliciels (virus, vers et chevaux de Troie).
- **Ingénierie sociale** : Dans la majeure partie des cas le maillon faible est l'utilisateur lui-même ! En effet c'est souvent lui qui, par méconnaissance ou par duperie, va ouvrir une brèche dans le système, en donnant des informations (mot de passe par exemple) au pirate informatique ou en exécutant une pièce jointe.

Ainsi, aucun dispositif de protection ne peut protéger l'utilisateur contre les arnaques, seuls bon sens, raison et un peu d'information sur les différentes pratiques peuvent lui éviter de tomber dans le piège.

- **Trappes** : il s'agit d'une porte dérobée (en anglais *backdoor*) dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur.

Pour autant, les erreurs de programmation contenues dans les programmes sont habituellement corrigées assez rapidement par leur concepteur dès lors que la vulnérabilité a été publiée. Il appartient alors aux administrateurs (ou utilisateurs personnels avertis) de se tenir informé des mises à jour des programmes qu'ils utilisent afin de limiter les risques d'attaques.

D'autre part il existe un certain nombre de dispositifs (pare-feu, systèmes de détection d'intrusions, antivirus) permettant d'ajouter un niveau de sécurisation supplémentaire.

Effort de protection

La sécurisation d'un système informatique est généralement dite « asymétrique », dans la mesure où le pirate n'a qu'à trouver une seule vulnérabilité pour compromette le système, tandis que l'administrateur se doit de corriger toutes les failles.

Attaques par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les **attaques par rebond** (par opposition aux **attaques directes**), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, il est possible de se retrouver « complice » d'une attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.

Avec le développement des réseaux sans fils, ce type de scénario risque de devenir de plus en plus courant car lorsque le réseau sans fil est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

Attaques - Méthodologie d'une intrusion sur un réseau

Méthodologie globale

Les hackers ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des **failles**, c'est-à-dire des *vulnérabilités* nuisibles à la sécurité du système, dans les protocoles, les systèmes d'exploitations, les applications ou même le personnel d'une organisation ! Les termes de **vulnérabilité**, de **brèche** ou en langage plus familier de **trou de sécurité** (en anglais *security hole*) sont également utilisés pour désigner les failles de sécurité.

Pour pouvoir mettre en œuvre un exploit (il s'agit du terme technique signifiant *exploiter une vulnérabilité*), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci.

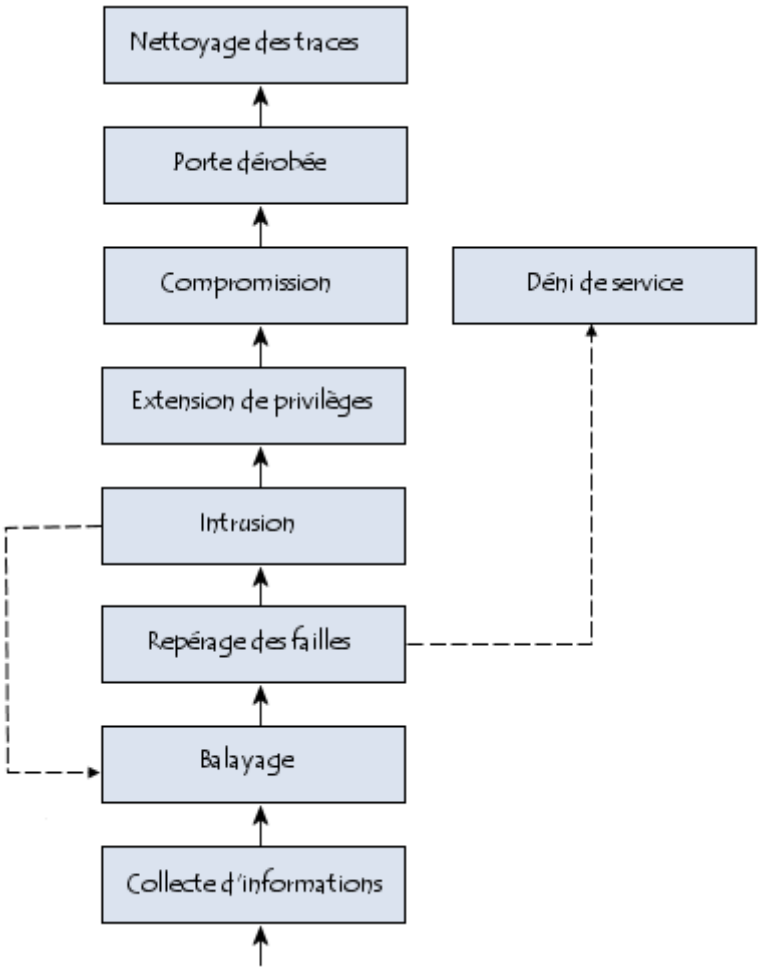
La plupart des attaques sont l'œuvre de *script kiddies* essayant bêtement des exploits trouvés sur internet, sans aucune connaissance du système, ni des risques liés à leur acte.

Une fois que le hacker a établi une cartographie du système, il est en mesure de mettre en application des exploits relatifs aux versions des applications qu'il a recensées. Un premier accès à une machine lui permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses privilèges sur la machine.

Lorsqu'un accès administrateur (le terme anglais *root* est généralement utilisé) est obtenu, on parle alors de compromission de la machine (ou plus exactement en anglais *root compromise*), car les fichiers systèmes sont susceptibles d'avoir été modifiés. Le hacker possède alors le plus haut niveau de droit sur la machine.

S'il s'agit d'un pirate, la dernière étape consiste à effacer ses traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises.

Le schéma suivant récapitule la méthodologie complète :



La récupération d'informations sur le système

L'obtention d'informations sur l'adressage du réseau visé, généralement qualifiée de **prise d'empreinte**, est un préalable à toute attaque. Elle consiste à rassembler le maximum d'informations concernant les infrastructures de communication du réseau cible :

- Adressage IP,
- Noms de domaine,
- Protocoles de réseau,
- Services activés,
- Architecture des serveurs,
- etc.

Consultation de bases publiques

En connaissant l'adresse IP publique d'une des machines du réseau ou bien tout simplement le nom de domaine de l'organisation, un pirate est potentiellement capable

de connaître l'adressage du réseau tout entier, c'est-à-dire la plage d'adresses IP publiques appartenant à l'organisation visée et son découpage en sous-réseaux.

Consultation de moteurs de recherche

La simple consultation des moteurs de recherche permet parfois de glaner des informations sur la structure d'une entreprise, le nom de ses principaux produits, voire le nom de certains personnels.

Balayage du réseau

Lorsque la topologie du réseau est connue par le pirate, il peut le scanner (le terme *balayer* est également utilisé), c'est-à-dire déterminer à l'aide d'un outil logiciel (appelé *scanner* ou *scanneur* en français) quelles sont les adresses IP actives sur le réseau, les ports ouverts correspondant à des services accessibles, et le système d'exploitation utilisé par ces serveurs.

L'un des outils les plus connus pour scanner un réseau est Nmap, reconnu par de nombreux administrateurs réseaux comme un outil indispensable à la sécurisation d'un réseau. Cet outil agit en envoyant des paquets TCP et/ou UDP à un ensemble de machines sur un réseau (déterminé par une adresse réseau et un masque), puis il analyse les réponses. Selon l'allure des paquets TCP reçus, il lui est possible de déterminer le système d'exploitation distant pour chaque machine scannée.

Il existe un autre type de scanneur, appelé **mappeur passif** (l'un des plus connus est Siphon), permettant de connaître la topologie réseau du brin physique sur lequel le mappeur analyse les paquets. Contrairement aux scanners précédents, cet outil n'envoie pas de paquets sur le réseau et est donc totalement indétectable par les systèmes de détection d'intrusion.

Enfin, certains outils permettent de capturer les connexions X (un serveur X est un serveur gérant l'affichage des machines de type UNIX). Ce système a pour caractéristique de pouvoir utiliser l'affichage des stations présentes sur le réseau, afin d'étudier ce qui est affiché sur les écrans et éventuellement d'intercepter les touches saisies par les utilisateurs des machines vulnérables.

Lecture de bannières

Lorsque le balayage du réseau est terminé, il suffit au pirate d'examiner le fichier journal (*log*) des outils utilisés pour connaître les adresses IP des machines connectées au réseau et les ports ouverts sur celles-ci.

Les numéros de port ouverts sur les machines peuvent lui donner des informations sur le type de service ouvert et donc l'inviter à interroger le service afin d'obtenir des informations supplémentaires sur la version du serveur dans les informations dites de « bannière ».

Ingénierie sociale

L'ingénierie sociale (en anglais « *Social Engineering* ») consiste à manipuler les êtres humains, c'est-à-dire d'utiliser la naïveté et la gentillesse exagérée des utilisateurs du réseau, pour obtenir des informations sur ce dernier. Ce procédé consiste à entrer en contact avec un utilisateur du réseau, en se faisant passer en général pour quelqu'un d'autre, afin d'obtenir des renseignements sur le système d'information ou éventuellement pour obtenir directement un mot de passe.

De la même façon une faille de sécurité peut être créée dans le système distant en envoyant un cheval de Troie à certains utilisateurs du réseau. Il suffit qu'un des utilisateurs exécute la pièce jointe pour qu'un accès au réseau interne soit donné à l'agresseur extérieur.

C'est la raison pour laquelle la politique de sécurité doit être globale et intégrer les facteurs humains (par exemple la sensibilisation des utilisateurs aux problèmes de sécurité) car le niveau de sécurité d'un système est caractérisé par le niveau de son maillon le plus faible.

Le repérage des failles

Après avoir établi l'inventaire du parc logiciel et éventuellement matériel, il reste au hacker à déterminer si des failles existent.

Il existe ainsi des scanneurs de vulnérabilité permettant aux administrateurs de soumettre leur réseau à des tests d'intrusion afin de constater si certaines applications possèdent des failles de sécurité. Les deux principaux scanneurs de failles sont :

- Nessus
- SAINT

Il est également conseillé aux administrateurs de réseaux de consulter régulièrement les sites tenant à jour une base de données des vulnérabilités :

- SecurityFocus / Vulnerabilities

L'intrusion

Lorsque le pirate a dressé une cartographie des ressources et des machines présentes sur le réseau, il est en mesure de préparer son intrusion.

Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valides sur les machines qu'il a recensées. Pour ce faire, plusieurs méthodes sont utilisées par les pirates :

- L'ingénierie sociale, c'est-à-dire en contactant directement certains utilisateurs du réseau (par mail ou par téléphone) afin de leur soutirer des informations concernant leur identifiant de connexion et leur mot de passe. Ceci est généralement fait en se faisant passer pour l'administrateur réseau.
- La consultation de l'annuaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des noms d'utilisateurs valides
- L'exploitation des vulnérabilités des commandes R* de Berkeley.
- Les attaques par force brute (*brute force cracking*), consistant à essayer de façon automatique différents mots de passe sur une liste de compte (par exemple l'identifiant, éventuellement suivi d'un chiffre, ou bien le mot de passe *password*, ou *passwd*, etc).

Extension de privilèges

Lorsque le pirate a obtenu un ou plusieurs accès sur le réseau en se logeant sur un ou plusieurs comptes peu protégés, celui-ci va chercher à augmenter ses privilèges en obtenant l'accès *root* (en français *super utilisateur* ou super administrateur), on parle ainsi d'**extension de privilèges**.

Dès qu'un accès *root* a été obtenu sur une machine, l'attaquant a la possibilité d'examiner le réseau à la recherche d'informations supplémentaires.

Il lui est ainsi possible d'installer un sniffeur (en anglais *sniffer*), c'est-à-dire un logiciel capable d'écouter (le terme *reniffler*, ou en anglais *sniffing*, est également employé) le trafic réseau en provenance ou à destination des machines situées sur le même brin.

Grâce à cette technique, le pirate peut espérer récupérer les couples *identifiants/mots de passe* lui permettant d'accéder à des comptes possédant des privilèges étendus sur d'autres machines du réseau (par exemple l'accès au compte d'un administrateur) afin d'être à même de contrôler une plus grande partie du réseau.

Les serveurs NIS présents sur un réseau sont également des cibles de choix pour les pirates car ils regorgent d'informations sur le réseau et ses utilisateurs.

Compromission

Grâce aux étapes précédentes, le pirate a pu dresser une cartographie complète du réseau, des machines s'y trouvant, de leurs failles et possède un accès *root* sur au moins l'une d'entre-elles. Il lui est alors possible d'étendre encore son action en exploitant les relations d'approbation existant entre les différentes machines.

Cette technique d'usurpation d'identité, appelée spoofing, permet au pirate de pénétrer des réseaux privilégiés auxquels la machine compromise a accès.

Porte dérobée

Lorsqu'un pirate a réussi à infiltrer un réseau d'entreprise et à compromettre une machine, il peut arriver qu'il souhaite pouvoir revenir. Pour ce faire celui-ci va installer une application afin de créer artificiellement une faille de sécurité, on parle alors de **porte dérobée** (en anglais **backdoor**, le terme *trappe* est parfois également employé).

Nettoyage des traces

Lorsque l'intrus a obtenu un niveau de maîtrise suffisant sur le réseau, il lui reste à effacer les traces de son passage en supprimant les fichiers qu'il a créés et en nettoyant les fichiers de logs des machines dans lesquelles il s'est introduit, c'est-à-dire en supprimant les lignes d'activité concernant ses actions.

Par ailleurs, il existe des logiciels, appelés « **kits racine** » (en anglais « *rootkits* ») permettant de remplacer les outils d'administration du système par des versions modifiées afin de masquer la présence du pirate sur le système.

En effet, si l'administrateur se connecte en même temps que le pirate, il est susceptible de remarquer les services que le pirate a lancé ou tout simplement qu'une autre personne que lui est connectée simultanément. L'objectif d'un rootkit est donc de tromper l'administrateur en lui masquant la réalité.

Conclusion

Il revient à tout responsable de réseau connecté à internet d'en assurer sa sécurité, et par conséquent d'en tester les failles.

C'est la raison pour laquelle, un administrateur réseau se doit d'être au courant des vulnérabilités des logiciels qu'il utilise et de se « mettre dans la peau d'un pirate » afin d'essayer de s'introduire dans son propre système et afin d'être continuellement dans un contexte de paranoïa.

Lorsque les compétences au sein de l'entreprise ne sont pas suffisantes pour mener à bien cette opération, il convient de faire réaliser un audit par une société spécialisée dans la sécurité informatique.

Les mots de passe

Lors de la connexion à un système informatique, celui-ci demande la plupart du temps un **identifiant** (en anglais *login* ou *username*) et un **mot de passe** (en anglais *password*) pour y accéder. Ce couple *identifiant/mot de passe* forme ainsi la clé permettant d'obtenir un accès au système.

Si l'identifiant est généralement automatiquement attribué par le système ou son administrateur, le choix du mot de passe est souvent laissé libre à l'utilisateur. Ainsi, la plupart des utilisateurs, estimant qu'ils n'ont rien de vraiment secret à protéger, se contentent d'utiliser un mot de passe facile à retenir (par exemple leur identifiant, le prénom de leur conjoint ou leur date de naissance).

Or, si les données sur le compte de l'utilisateur n'ont pas un caractère stratégique, l'accès au compte de l'utilisateur peut constituer une porte ouverte vers le système tout entier.

En effet, dès qu'un pirate obtient un accès à un compte d'une machine, il lui est possible d'élargir son champ d'action en obtenant la liste des utilisateurs autorisés à se connecter à la machine.

A l'aide d'outils de génération de mots de passe, le pirate peut essayer un grand nombre de mots de passe générés aléatoirement ou à l'aide d'un dictionnaire (éventuellement une combinaison des deux). S'il trouve par hasard le mot de passe de l'administrateur, il obtient alors toutes les permissions sur la machine !

De plus, à partir d'une machine du réseau, le pirate peut éventuellement obtenir un accès sur le réseau local, ce qui signifie qu'il peut dresser une cartographie des autres serveurs côtoyant celui auquel il a obtenu un accès.

Les mots de passe des utilisateurs représentent donc la première défense contre les attaques envers un système, c'est la raison pour laquelle il est nécessaire de définir une politique en matière de mots de passe afin d'imposer aux utilisateurs le choix d'un mot de passe suffisamment sécurisé.

Méthodes d'attaque

La plupart des systèmes sont configurés de manière à bloquer temporairement le compte d'un utilisateur après un certain nombre de tentatives de connexion infructueuses. Ainsi, un pirate peut difficilement s'infiltrer sur un système de cette façon.

En contrepartie, un pirate peut se servir de ce mécanisme d'auto-défense pour bloquer l'ensemble des comptes utilisateurs afin de provoquer un déni de service.

Sur la plupart des systèmes les mots de passe sont stockés de manière chiffrée (« cryptée ») dans un fichier ou une base de données.

Néanmoins, lorsqu'un pirate obtient un accès au système et obtient ce fichier, il lui est possible de tenter de casser le mot de passe d'un utilisateur en particulier ou bien de l'ensemble des comptes utilisateurs.

Attaque par force brute

On appelle ainsi « **attaque par force brute** » (en anglais « *brute force cracking* », parfois également *attaque exhaustive*) le cassage d'un mot de passe en testant tous les mots de passe possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération.

Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les pirates informatiques pour s'introduire dans les systèmes informatiques.

Attaque par dictionnaire

Les outils d'attaque par force brute peuvent demander des heures, voire des jours, de calcul même avec des machines équipées de processeurs puissants. Ainsi, une alternative consiste à effectuer une « **attaque par dictionnaire** ».

En effet, la plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Avec ce type d'attaques, un tel mot de passe peut être craqué en quelques minutes.

Attaque hybride

Le dernier type d'attaques de ce type, appelées « **attaques hybrides** », vise particulièrement les mots de passe constitué d'un mot traditionnel et suivi d'une lettre ou d'un chiffre (tel que « marechal6 »). Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire.

Il existe enfin des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs :

- Les **key loggers** (littéralement « enregistreurs de touches »), sont des logiciels qui, lorsqu'ils sont installés sur le poste de l'utilisateur, permettent d'enregistrer les frappes de claviers saisies par l'utilisateur.

  Les systèmes d'exploitation récents possèdent des mémoires tampon protégées permettant de retenir temporairement le mot de passe et accessibles uniquement par le système.

- L'**ingénierie sociale** consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence ;
- L'**espionnage** représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'œil par-dessus son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

Choix du mot de passe

Il est aisément compréhensible que plus un mot de passe est long, plus il est difficile à casser. D'autre part, un mot de passe constitué uniquement de chiffres sera beaucoup plus simple à casser qu'un mot de passe contenant des lettres :

Un mot de passe de 4 chiffres correspond à 10 000 possibilités (10^4). Si ce chiffre paraît élevé, un ordinateur doté d'une configuration modeste est capable de le casser en quelques minutes.
On lui préfèrera un mot de passe de 4 lettres, pour lequel il existe 456972 possibilités (26^4). Dans le même ordre d'idée, un mot de passe mêlant chiffres et lettres, voire également des majuscules et des caractères spéciaux sera encore plus difficile à casser.

Mots de passe à **éviter** :

- Votre identifiant ;
- Votre nom ;
- Votre prénom ou celui d'un proche (conjoint, enfant, etc.) ;
- Un mot du dictionnaire ;
- Un mot à l'envers (les outils de cassage de mots de passe prennent en compte cette possibilité) ;
- Un mot suivi d'un chiffre, de l'année en cours ou d'une année de naissance (par exemple « password1999 »).

Politique en matière de mot de passe

L'accès au compte d'un seul employé d'une entreprise peut compromettre la sécurité globale de toute l'organisation. Ainsi, toute entreprise souhaitant garantir un niveau de sécurité optimal se doit de mettre en place une réelle politique de sécurité de matière de mots de passe.

Il s'agit notamment d'imposer aux employés le choix d'un mot de passe conforme à certaines exigences, par exemple :

- Une longueur de mot de passe minimale ;
- La présence de caractères particuliers ;
- Un changement de casse (minuscule et majuscule).

Par ailleurs, il est possible de renforcer cette politique de sécurité en imposant une durée d'expiration des mots de passe, afin d'obliger les utilisateurs à modifier régulièrement leur mot de passe. Cela complique ainsi la tâche des pirates essayant de casser des mots de passe sur la durée. Par ailleurs il s'agit d'un excellent moyen de limiter la durée de vie des mots de passe ayant été cassés.

Enfin, il est recommandé aux administrateurs système d'utiliser des logiciels de cassage de mots de passe en interne sur les mots de passe de leurs utilisateurs afin d'en éprouver la solidité. Ceci doit néanmoins se faire dans le cadre de la politique de sécurité et être écrit noir sur blanc, afin d'avoir l'approbation de la direction et des utilisateurs.

Mots de passe multiples

Il n'est pas sain d'avoir un seul mot de passe, au même titre qu'il ne serait pas sain d'avoir comme code de carte bancaire le même code que pour son téléphone portable et que le digicode en bas de l'immeuble.

Il est donc conseillé de posséder plusieurs mots de passe par catégorie d'usage, en fonction de la confidentialité du secret qu'il protège. Le code d'une carte bancaire devra ainsi être utilisé uniquement pour cet usage. Par contre, le code PIN d'un téléphone portable peut correspondre à celui du cadenas d'une valise.

De même, lors de l'inscription à un service en ligne demandant une adresse électronique il est fortement déconseillé de choisir le même mot de passe que celui permettant d'accéder à cette messagerie car un administrateur peu scrupuleux, pourrait sans aucun problème avoir un œil sur votre vie privée.

Qu'est-ce qu'un réseau ?

Le terme générique « **réseau** » définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.

- **Réseau** (en anglais *network*) : Ensemble des ordinateurs et périphériques connectés les uns aux autres. Notons que deux ordinateurs connectés ensemble constituent à eux seuls un réseau minimal.
- **mise en réseau** (en anglais *networking*) : Mise en œuvre des outils et des tâches permettant de relier des ordinateurs afin qu'ils puissent partager des ressources en réseau.

Intérêt d'un réseau

Un ordinateur est une machine permettant de manipuler des données. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre-eux afin de pouvoir échanger des informations.

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.) ;
- La communication entre personnes (courrier électronique, discussion en direct, etc.) ;
- La communication entre processus (entre des ordinateurs industriels par exemple) ;
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau) ;
- Le jeu vidéo multi-joueurs.

Les réseaux permettent aussi de standardiser les applications, on parle généralement de **groupware** pour qualifier les outils permettant à plusieurs personnes de travailler en réseau. Par exemple la messagerie électronique et les agendas de groupe permettent de communiquer plus efficacement et plus rapidement. Voici un aperçu des avantages qu'offrent de tels systèmes :

- Diminution des coûts grâce aux partages des données et des périphériques ;
- Standardisation des applications ;
- Accès aux données en temps utile ;
- Communication et organisation plus efficace.

Similitudes entre types de réseaux

Les différents types de réseaux ont généralement les points suivants en commun :

- **Serveurs** : ordinateurs qui fournissent des ressources partagées aux utilisateurs par un serveur de réseau.
- **Clients** : ordinateurs qui accèdent aux ressources partagées fournies par un serveur de réseau.
- **Support de connexion** : conditionne la façon dont les ordinateurs sont reliés entre eux.
- **Données partagées** : fichiers accessibles sur les serveurs du réseau.
- **Imprimantes et autres périphériques partagés** : fichiers, imprimantes ou autres éléments utilisés par les usagers du réseau.
- **Ressources diverses** : autres ressources fournies par le serveur.

Les différents types de réseau

On distingue généralement les deux types de réseaux suivants :

- Les réseaux poste à poste (peer to peer / égal à égal) ;
- Réseaux organisés autour de serveurs (Client/Serveur).

Ces deux types de réseau ont des capacités différentes. Le type de réseau à installer dépend des critères suivants :

- Taille de l'entreprise ;
- Niveau de sécurité nécessaire ;
- Type d'activité ;
- Niveau de compétence d'administration disponible ;
- Volume du trafic sur le réseau ;
- Besoins des utilisateurs du réseau ;
- Budget alloué au fonctionnement du réseau (pas seulement l'achat mais aussi l'entretien et la maintenance).

Que signifie le terme « topologie »

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé **topologie physique**. On distingue généralement les topologies suivantes :

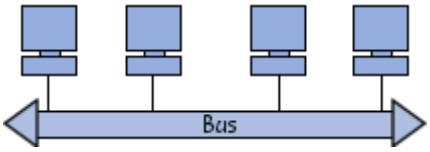
- Topologie en bus ;
- Topologie en étoile ;
- Topologie en anneau ;
- Topologie en arbre ;

- Topologie maillée.

La **topologie logique**, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont **Ethernet, Token Ring et FDDI.**

Topologie en bus

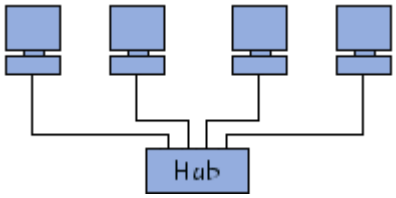
Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.



Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

Topologie en étoile

Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un système matériel central appelé **concentrateur** (en anglais *hub*, littéralement *moyen de roue*). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

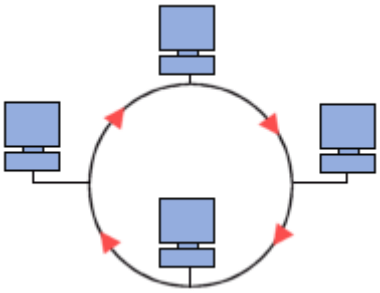


Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

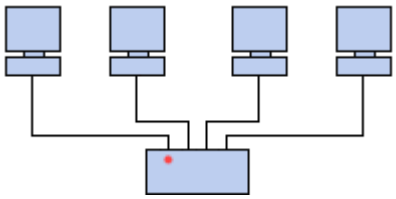
Topologie en anneau

Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.



>

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un **répartiteur** (appelé *MAU*, *Multistation Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre-eux un temps de parole.



Les deux principales topologies logiques utilisant cette topologie physique sont Token ring (anneau à jeton) et FDDI.

Les différents types de réseaux

On distingue différents types de réseaux (privés) selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. On fait généralement trois catégories de réseaux :

- **LAN** (local area network) **;**
- **MAN** (metropolitan area network) **;**
- **WAN** (wide area network).

Il existe deux autres types de réseaux : les **TAN** (Tiny Area Network) identiques aux LAN mais moins étendus (2 à 3 machines) et les **CAN** (Campus Area Network) identiques au MAN (avec une bande passante maximale entre tous les LAN du réseau).

Les LAN

LAN signifie *Local Area Network* (en français *Réseau Local*). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données? d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

En élargissant le contexte de la définition aux services qu'apporte le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement d'"**égal à égal**" (en anglais *peer to peer*), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur à un rôle similaire ;
- dans un environnement **"client/serveur**", dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

Les MAN

Les **MAN** (*Metropolitan Area Network*) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

Les WAN

Un **WAN** (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau.

Le plus connu des WAN est Internet.

Un système d'exploitation est le logiciel qui gère les applications et le matériel de l'ordinateur.il est le garant de la sécurité de toutes les ressources qui s'y trouvent. Un utilisateur accède à une ressource à travers un certain nombre de droits qui sont définis.

Un droit d'accès est la permission que possède un utilisateur par rapport à une ressource. La sécurité du système consiste à sécuriser n'importe quelle ressource du SE tel que les fichiers, le système de fichiers ou n'importe quelle autre information plus ou moins critique.

Elle doit faire partir des priorités de l'entreprise car les utilisateurs travaillent dans leur poste de travail.

Le but de ce cours est donc de comprendre les fondamentaux de la sécurité système et savoir configurer les stratégies locales de sécurité.

1.1. La gestion des ressources

Dans un ordinateur du réseau, on peut identifier deux types de ressources :

- Les ressources partagées : c'est l'ensemble des ressources disponibles via le réseau ;
- Les ressources non partagées (les ressources locales) : c'est l'ensemble des ressources accessible uniquement via le poste en local.

1.2. Méthodes d'accès aux ressources partagées

L'accès à une ressource partagée peut se faire de plusieurs manières :

- L'utilisation d'un chemin UNC (universal Name convention). Le chemin UNC a la forme suivante : \\nomserveur[\non_partage[\nom_fichier]] ;
- L'utilisation d'un favori réseau.

La convention suivante est souvent utilisée pour définir les permissions des utilisateurs par rapport aux ressources : ***U←A/P*** c'est-à-dire que l'utilisateur U reçoit la permission A par rapport à la ressource **P**

Interprétation :

U est un utilisateur ou un groupe d'utilisateur ;

A est une autorisation ou une permission par rapport à une ressource ;

P c'est la ressource partagée.

1.3. Liste des autorisations de partage

Il existe quatre niveaux d'autorisation

- **NA (No access)** c'est-à-dire que l'utilisateur ou le groupe d'utilisateur ne possède aucune permission sur la ressource concernée ;
- **R (read)** c'est-à-dire l'utilisateur ou le groupe d'utilisateur possède la permission de lecture ;
- **C (change)** l'utilisateur ou le groupe d'utilisateur peut non seulement lire la ressource mais la modifier également ;

- **FC (full control (ou control total))** l'utilisateur ou le groupe d'utilisateur a toutes les permissions.

2. Les piliers de la sécurité d'un Système d'Exploitation

La sécurité du SE se base sur les trois piliers suivants :

- Intégrité du SE
  - Seul l'utilisateur légitime doit pouvoir accéder au système.
- La confidentialité
  - Un SE est constitué d'un ou plusieurs comptes utilisateurs. Chaque compte possède des droits par rapport à chaque ressource du réseau.
- La disponibilité du SE

  C'est le SE qui fait fonctionner un ordinateur. Son instabilité rend également instable l'accès aux données ou à d'autres ressources locales ou partagées.

3. La notion de checklist

Une checklist représente l'ensemble des mesures de sécurité à appliquer afin de garantir une bonne sécurité des données et du système. N'importe quelle entreprise doit avoir une checklist. Elle permet d'élaborer et même de garantir une bonne politique de sécurité.

Les éléments de la checklist

- La désactivation des services non essentiels : un attaquant peut se servir d'un service ouvert mais non utiliser pour attaquer un service ;
- Les patchs (correctif de sécurité) et mise à jour ;
- Utilisation des mots de passe complexes ;
- Désactivation des comptes non utilisés ;
- Installation et mise à jour des antivirus ;
- Utilisation des ACL ;
- Chiffrement des fichiers et système de fichiers ;
- Configuration du pare feu de l'hôte ;
- Activation des mises à jour.

4. Les menaces qui pèsent sur l'hôte

Un hôte est exposé à plusieurs types de menaces telles que :

- Les infections de malware
  - Un malware est un programme malveillant capable de nuire au bon fonctionnement d'un hôte ou du moins un système. On distingue plusieurs types de malwares parmi lesquels :
- Les virus ;
- Les trojans ;
- Les backdoor, etc ;
- La suppression des données ;

- Elle peut se faire par une action volontaire ou involontaire ou encore illégitime.

- Les accès non autorisés
  - Les SE sont exposés à ce type de menaces. Cette menace se produit lorsqu'une tierce personne (attaquant) plus ou moins mal intentionnée utilise les failles de votre système pour entrer dans votre ordinateur.
- Hôte non patché
  - Il est toujours important de faire des mises à jour de votre système afin de renforcer sa sécurité.
- Les emails
  - Plusieurs menaces proviennent également des emails qui nous parviennent. Ça peut être un mail de fishing ou de spam.
- Le social engineering
  - Il consiste en un renseignement que fait l'attaquant sur l'entreprise de manière intelligente dont le but est d'obtenir une information qu'il pourra exploiter pour attaquer l'entreprise.
- Le partage de fichiers réseaux
  - Il est conseillé d'utiliser les protocoles sécurisés pour partager les fichiers en réseaux.
- Téléchargement sur internet
  - On court beaucoup de risque lorsqu'on effectue les téléchargements sur internet. La plupart des applications surtout celles qui sont gratuites sont le plus souvent infectées.

Généralement il est greffé à ces applications, des programmes malveillants qui pourront créer une instabilité de votre système une fois installés. Les hackers ou crackers utilisent généralement ce type de technique pour intégrer votre ordinateur dans un réseau de botnet.

5. Les bonnes pratiques en matière de sécurité système

- Changer les noms et les mots de passe par défaut ;
- Désactiver les comptes inactifs ;
- Granularité dans les droits ;
- Pas de compte partagé ;
- Mise à jour d'une politique de sécurité des mots de passe.

6. La sécurité sur Windows

Windows est un système propriétaire très connu dans la famille des SE. C'est un système très répandu et apprécié dans le monde. Il existe en mode client mais aussi en mode serveur. Comme tout système d'exploitation, la sécurité sur Windows consiste à protéger les ressources internes de l'ordinateur contre les accès non autorisés.

On fait allusion ici aux données, aux applications, aux fichiers catalogues et fichiers ordinaires qui doivent être protégés contre les personnes illégitimes.

La sécurité des systèmes Windows repose sur les points suivants :

- Les droits des utilisateurs par rapport aux ressources locales ou partagées ;
- L'utilisation du pare feu du système ;
- La base de registre ;
- L'utilisation de la stratégie locale de sécurité.

6.1. Les privilèges des utilisateurs

Privilège signifie droit d'accès, ou permission. Pour des raisons de sécurité, Chaque utilisateur doit avoir des droits pour accéder à une ressource. Sous Windows, ça se configure au niveau des propriétés de sécurité du fichier à protéger.

Clic droit sur le fichier → propriété → onglet sécurité

6.2. La base de registre

Le registre Windows est un ensemble de données structurées. En clair, il s'agit d'une base de données qui stocke les informations importantes pour Windows et les applications installées. Le registre Windows contient toute la configuration de Windows. On y trouve notamment :

- Services Windows et les programmes qui se chargent au démarrage ;
- Les associations de fichiers ;
- Les informations des comptes utilisateurs ;
- La configuration matérielle ;
- La configuration d'explorer.exe ;
- Les restrictions administrateurs ;
- Toute la configuration utilisateur (fond d'écran, les paramètres de Windows choisies par l'utilisateur etc.) ;
- La configuration des applications. Celles-ci peuvent utiliser la base de registre pour stocker certains éléments de configuration ou de fonctionnement.

Il existe deux manières d'ouvrir l'Éditeur du Registre dans Windows 10 :

- Dans la zone de recherche de la barre des tâches, tapez **regedit**, puis sélectionnez **Éditeur du Registre** (application de bureau) dans les résultats.
- Cliquez avec le bouton **droit sur Démarrer**, puis sélectionnez **Exécuter**. Tapez **regedit** dans la zone Ouvrir et sélectionnez **OK.**

Introduction à la sûreté de fonctionnement

Quel que soit le service rendu par un système informatique, il est essentiel que les utilisateurs aient confiance en son fonctionnement pour pouvoir l'utiliser dans de bonnes conditions. Le terme « **sûreté de fonctionnement** » caractérise le niveau de confiance d'un système informatique.

Une défaillance correspond à un dysfonctionnement du service, c'est-à-dire un état de fonctionnement anormal ou plus exactement non conforme aux spécifications. Du point de vue de l'utilisateur, un service possède deux états :

- Service approprié, c'est-à-dire conforme aux attentes ;
- Service inapproprié, c'est-à-dire non conforme aux attentes.

Une défaillance est imputable à une erreur, c'est-à-dire un dysfonctionnement local. Toutes les erreurs ne conduisent pas nécessairement à une défaillance du service.

Il existe plusieurs moyens de limiter les défaillances d'un service :

- La **prévention des fautes** consistant à éviter les fautes en les anticipant.
- La **tolérance aux fautes** dont l'objectif est de fournir un service conforme aux spécifications malgré les fautes en introduisant une redondance.
- L'élimination **des fautes** visant à réduire le nombre de fautes grâce à des actions correctives.
- La **prévision des fautes** en anticipation les fautes et leur impact sur le service.

Introduction à la haute disponibilité

On appelle « **haute disponibilité** » (en anglais « **high availability** ») toutes les dispositions visant à garantir la disponibilité d'un service, c'est-à-dire assurer le bon fonctionnement d'un service 24H/24.

Le terme « **disponibilité** » désigne la probabilité qu'un service soit en bon état de fonctionnement à un instant donné.

Le terme « **fiabilité** », parfois également utilisé, désigne la probabilité qu'un système soit en fonctionnement normal sur une période donnée. On parle ainsi de « **continuité de service** ».

Evaluation des risques

En effet, la panne d'un système informatique peut causer une perte de productivité et d'argent, voire des pertes matérielles ou humaines dans certains cas critiques. Il est ainsi essentiel d'évaluer les risques liés à un dysfonctionnement (faute) d'une des composantes du système d'information et de prévoir des moyens et mesures permettant d'éviter ou de rétablir dans des temps acceptables tout incident.

Comme chacun le sait, les risques de pannes d'un système informatique en réseau sont nombreux. L'origine des fautes peut être schématisée de la manière suivant :

- Origines physiques : elles peuvent être d'origine naturelle ou criminelle :
  - Désastre naturel (inondation, séisme, incendie) ;
  - Environnement (intempéries, taux d'humidité de l'air, température) ;
  - Panne matérielle ;
  - Panne du réseau ;
  - Coupure électrique.
- Origines humaines : elles peuvent être intentionnelles ou fortuites :
  - Erreur de conception (bogue logiciel, mauvais dimensionnement du réseau) ;
- Origines humaines : elles peuvent être intentionnelles ou fortuites :
  - Erreur de conception (bogue logiciel, mauvais dimensionnement du réseau) ;
- Origines opérationnelles : elles sont liées à un état du système à un moment donné :
  - Bogue logiciel ;
  - Dysfonctionnement logiciel ;

L'ensemble de ces risques peuvent avoir différentes causes telles que les suivantes :

- Malveillance intentionnelle.

Tolérance aux pannes

Puisqu'il est impossible d'empêcher totalement les pannes, une solution consiste à mettre en place des mécanismes de **redondance**, en dupliquant les ressources critiques.

La capacité d'un système à fonctionner malgré une défaillance d'une de ses composantes est appelée **tolérance aux pannes** (parfois nommée *tolérance aux fautes* », en anglais *fault tolerance*).

Lorsqu'une des ressources tombe en panne, les autres ressources prennent le relais afin de laisser le temps aux administrateurs du système de remédier à l'avarie. En anglais le terme de « **Fail-Over Service** » (noté *FOS*) est ainsi utilisé.

Idéalement, dans le cas d'une panne matérielles, les éléments matériels fautifs devront pouvoir être « **extractibles à chaud** » (en anglais « *hot swappable* »), c'est-à-dire pouvoir être extraits puis remplacés, sans interruption de service.

La sauvegarde

La mise en place d'une architecture redondante ne permet que de s'assurer de la disponibilité des données d'un système mais ne permet pas de protéger les données contre les erreurs de manipulation des utilisateurs ou contre des catastrophes naturelles telles qu'un incendie, une inondation ou encore un tremblement de terre.

Il est donc nécessaire de prévoir des mécanismes de sauvegardes, idéalement sur des sites distants, afin de garantir la pérennité des données.

Par ailleurs, un mécanisme de sauvegarde permet d'assurer une fonction d'archivage, c'est-à-dire de conserver les données dans un état correspondant à une date donnée.

Tolérance aux pannes

Puisqu'il est impossible d'empêcher totalement les pannes, une solution consiste à mettre en place des mécanismes de **redondance**, en dupliquant les ressources critiques.

La capacité d'un système à fonctionner malgré une défaillance d'une de ses composantes est appelée **tolérance aux pannes** (parfois nommée *tolérance aux fautes* », en anglais *fault tolerance*).

Lorsqu'une des ressources tombe en panne, les autres ressources prennent le relais afin de laisser le temps aux administrateurs du système de remédier à l'avarie. En anglais le terme de « **Fail-Over Service** » (noté *FOS*) est ainsi utilisé.

Idéalement, dans le cas d'une panne matérielles, les éléments matériels fautifs devront pouvoir être « **extractibles à chaud** » (en anglais « *hot swappable* »), c'est-à-dire pouvoir être extraits puis remplacés, sans interruption de service.

La sauvegarde

Néanmoins, la mise en place d'une architecture redondante ne permet que de s'assurer de la disponibilité des données d'un système mais ne permet pas de protéger les données contre les erreurs de manipulation des utilisateurs ou contre des catastrophes naturelles telles qu'un incendie, une inondation ou encore un tremblement de terre.

Il est donc nécessaire de prévoir des mécanismes de **sauvegarde** (en anglais *backup*), idéalement sur des sites distants, afin de garantir la pérennité des données.

Par ailleurs, un mécanisme de sauvegarde permet d'assurer une fonction d'archivage, c'est-à-dire de conserver les données dans un état correspondant à une date donnée.

Types de sauvegarde

Le mécanisme de sauvegarde mis en œuvre doit impérativement être pensé de manière à assurer la pérennité et la récupération de l'ensemble des données critiques de l'organisation, quel que soit le sinistre subi, sans perturber le fonctionnement du système d'information.

Ainsi, le choix du mécanisme de sauvegarde doit faire l'objet d'une stratégie de sauvegarde, définissant les données à sauvegarder, la fréquence et le mode de sauvegarde, et d'un plan de reprise sur sinistre indiquant la démarche nécessaire pour rétablir le fonctionnement normal en cas d'incident.

On distingue habituellement les catégories de sauvegardes suivantes :

- Sauvegarde totale ;
- Sauvegarde différentielle ;
- Sauvegarde incrémentale ;
- Sauvegarde à delta ;
- Journalisation.

Sauvegarde complète

L'objectif de la **sauvegarde totale** (parfois *sauvegarde totale* ou en anglais *full backup*) est de réaliser une copie conforme des données à sauvegarder sur un support séparé.

Néanmoins, pour de gros volumes de données, la sauvegarde complète peut poser des problèmes de lenteur (si les données sont modifiées en cours de sauvegarde), de disponibilité car elle crée des accès disques longs et intenses ou encore de coût étant donné la capacité nécessaire. En revanche elle permet d'obtenir une image fidèle des données à un temps t.

Sauvegarde incrémentale

La **sauvegarde incrémentale** (en anglais *incremental backup*) consiste à copier tous les éléments modifiés depuis la sauvegarde précédente. Ce type de sauvegarde est plus performant qu'une sauvegarde totale car elle permet de se focaliser uniquement sur les fichiers modifiés avec un espace de stockage plus faible, mais nécessite en contrepartie de posséder les sauvegardes précédentes pour reconstituer la sauvegarde complète.

Sauvegarde différentielle

La **sauvegarde différentielle** (en anglais *differential backup*) se focalise uniquement sur les fichiers modifiés depuis la dernière sauvegarde complète, ce qui la rend plus lente et plus coûteuse en espace de stockage qu'une sauvegarde incrémentale mais également plus fiable car seule la sauvegarde complète est nécessaire pour reconstituer les données sauvegardées.

Sauvegarde à delta

La **sauvegarde à delta** (en anglais *delta backup*) est une sauvegarde incrémentale sur des éléments de données à granularité plus fine, c'est-à-dire au niveau de chaque bloc de données et non au niveau du fichier seulement.

Equilibrage de charge

L'**équilibrage de charge** (parfois appelé *répartition de charge* ou en anglais *load balancing*) consiste à distribuer une tâche à un pool de machines ou de périphériques afin :

- De lisser le trafic réseau, c'est-à-dire de répartir la charge globale vers différents équipements ;
- De s'assurer de la disponibilité des équipements, en n'envoyant des données qu'aux équipements en mesure de répondre, voire à ceux offrant le meilleur temps de réponse.

Ce type de mécanisme s'appuie sur un élément, appelé **répartiteur de charge** (en anglais *load balancer*) chargé de distribuer le travail entre différentes machines.

Notion de cluster

Un « cluster » (en français « **grappe** ») est une architecture composée de plusieurs ordinateurs formant des nœuds, où chacun des nœuds est capable de fonctionner indépendamment des autres.

Il existe deux principaux usages des clusters :

- Les **clusters de haute disponibilité** permettent de répartir une charge de travail parmi un grand nombre de serveurs et de garantir l'accomplissement de la tâche même en cas de défaillance d'un des nœuds ;
- Les **clusters de calcul** permettent de répartir une charge de travail parmi un grand nombre de serveurs afin d'utiliser la performance cumulée de chacun des nœuds.

Introduction aux NAS

Un « **NAS** » (*Network Attached Storage*) est un dispositif de stockage en réseau. Il s'agit d'un serveur de stockage à part entière pouvant être facilement attaché au réseau de l'entreprise afin de servir de serveur de fichiers et fournir un espace de stockage tolérant aux pannes.

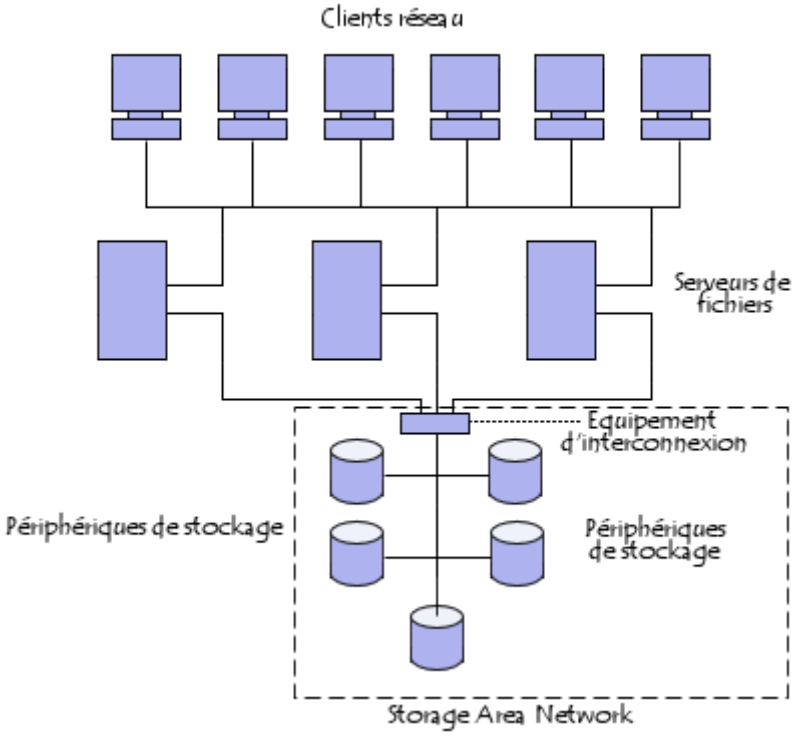
Présentation d'un NAS

- Un NAS est un serveur à part entière disposant de son propre système d'exploitation et d'un logiciel de configuration paramétré avec des valeurs par défaut convenant dans la majorité des cas.
- Il possède généralement son propre système de fichiers hébergeant le système d'exploitation, ainsi qu'un ensemble de disques indépendants servant à héberger les données à sauvegarder.

Introduction aux SAN

Un « **SAN** » (*Storage Area Network*) est un réseau de stockage à part entière. Un SAN est ainsi une architecture complète regroupant les éléments suivants :

- Un réseau très haut débit en Fiber Channel ou SCSI ;
- Des équipements d'interconnexion dédiés (switch, ponts, etc.) ;
- Des éléments de stockage (disques durs) en réseau.



Présentation d'un SAN

Le SAN est un réseau dédié au stockage attaché aux réseaux de communication de l'entreprise. Les ordinateurs ayant accès au SAN possèdent donc une interface réseau spécifique relié au SAN, en plus de leur interface réseau traditionnelle.

Avantages et inconvénients

Les performances du SAN sont directement liées à celle du type de réseau utilisé. Dans le cas d'un réseau Fibre Channel, la bande passante est d'environ 100 Mo/s (1000 Mbit/s) et peut être étendue en multipliant les liens d'accès.

La capacité d'un SAN peut être étendue de manière quasi-illimitée et atteindre des centaines, voire des milliers de téraoctets.

Grâce au SAN, il est possible de partager des données entre plusieurs ordinateurs du réseau sans sacrifier les performances, dans la mesure où le trafic SAN est complètement séparé du trafic utilisateurs. Ce sont les serveurs applicatifs qui jouent le rôle d'interface entre le réseau de données (généralement Fibre Channel) et le réseau des utilisateurs (généralement Ethernet).

En contrepartie, le coût d'acquisition d'un SAN est beaucoup plus onéreux qu'un dispositif NAS dans la mesure où il s'agit d'une architecture complète, utilisant des technologies encore chères.

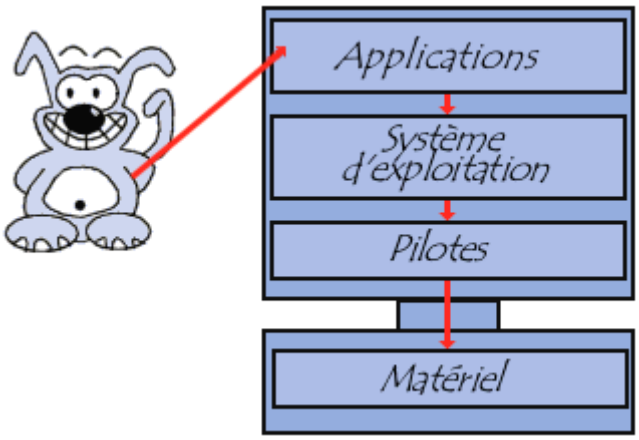
Description du système d'exploitation

Pour qu'un ordinateur soit capable de faire fonctionner un **programme informatique** (appelé parfois *application* ou *logiciel*), la machine doit être en mesure d'effectuer un certain nombre d'opérations préparatoires afin d'assurer les échanges entre le processeur, la mémoire, et les ressources physiques (périphériques).

Le **système d'exploitation** (noté *SE* ou *OS*, abréviation du terme anglais *Operating System*), est chargé d'assurer la liaison entre les ressources matérielles, l'utilisateur et les applications (traitement de texte, jeu vidéo, ...).

Ainsi, lorsqu'un programme désire accéder à une ressource matérielle, il ne lui est pas nécessaire d'envoyer des informations spécifiques au périphérique, il lui suffit d'envoyer les informations au système d'exploitation, qui se charge de les transmettre au périphérique concerné via son pilote.

En l'absence de pilotes il faudrait que chaque programme reconnaisse et prenne en compte la communication avec chaque type de périphérique.



Le système d'exploitation permet ainsi de "dissocier" les programmes et le matériel, afin notamment de simplifier la gestion des ressources et offrir à l'utilisateur une interface homme-machine (notée « IHM ») simplifiée afin de lui permettre de s'affranchir de la complexité de la machine physique.

Rôles du système d'exploitation

Les rôles du système d'exploitation sont divers :

- **Gestion du processeur** : le système d'exploitation est chargé de gérer l'allocation du processeur entre les différents programmes grâce à un **algorithme d'ordonnancement**. Le type d'ordonnanceur est totalement dépendant du système d'exploitation, en fonction de l'objectif visé.

- **Gestion de la mémoire vive** : le système d'exploitation est chargé de gérer l'espace mémoire alloué à chaque application et, le cas échéant, à chaque usager. En cas d'insuffisance de mémoire physique, le système d'exploitation peut créer une zone mémoire sur le disque dur, appelée «**mémoire virtuelle**».

La mémoire virtuelle permet de faire fonctionner des applications nécessitant plus de mémoire qu'il n'y a de mémoire vive disponible sur le système. En contrepartie cette mémoire est beaucoup plus lente.

- **Gestion des entrées/sorties** : le système d'exploitation permet d'unifier et de contrôler l'accès des programmes aux ressources matérielles par l'intermédiaire des pilotes (appelés également gestionnaires de périphériques ou gestionnaires d'entrée/sortie).
- **Gestion de l'exécution des applications** : le système d'exploitation est chargé de la bonne exécution des applications en leur affectant les ressources nécessaires à leur bon fonctionnement. Il permet à ce titre de « tuer » une application ne répondant plus correctement.
- **Gestion des droits** : le système d'exploitation est chargé de la sécurité liée à l'exécution des programmes en garantissant que les ressources ne sont utilisées que par les programmes et utilisateurs possédant les droits adéquats.
- **Gestion des fichiers** : le système d'exploitation gère la lecture et l'écriture dans le système de fichiers et les droits d'accès aux fichiers par les utilisateurs et les applications.
- **Gestion des informations** : le système d'exploitation fournit un certain nombre d'indicateurs permettant de diagnostiquer le bon fonctionnement de la machine.

Composantes du système d'exploitation

Le système d'exploitation est composé d'un ensemble de logiciels permettant de gérer les interactions avec le matériel. Parmi cet ensemble de logiciels on distingue généralement les éléments suivants :

- Le **noyau** (en anglais **kernel**) représentant les fonctions fondamentales du système d'exploitation telles que la gestion de la mémoire, des processus, des fichiers, des entrées-sorties principales, et des fonctionnalités de communication.
- L'**interpréteur de commande** (en anglais **shell**, traduisez « *coquille* » par opposition au noyau) permettant la communication avec le système d'exploitation par l'intermédiaire d'un langage de commandes, afin de permettre à l'utilisateur de piloter les périphériques en ignorant tous des caractéristiques du matériel qu'il utilise, de la gestion des adresses physiques, etc.
- Le **système de fichiers** (en anglais « *file system* », noté *FS*), permettant d'enregistrer les fichiers dans une arborescence.

Systèmes multitâches

Un système d'exploitation est dit « **multitâche** » (en anglais *multithreaded*) lorsque plusieurs « **tâches** » (également appelées *processus*) peuvent être exécutées simultanément.

Les applications sont composées en séquence d'instructions que l'on appelle « **processus légers** » (en anglais «*threads*»). Ces threads seront tour à tour actifs, en attente, suspendus ou détruits, suivant la priorité qui leur est associée ou bien exécutés séquentiellement.

Un système est dit **préemptif** lorsqu'il possède un **ordonnanceur** (aussi appelé *planificateur*), qui répartit, selon des critères de priorité, le temps machine entre les différents processus qui en font la demande.

Le système est dit à **temps partagé** lorsqu'un quota de temps est alloué à chaque processus par l'ordonnanceur. C'est notamment le cas des systèmes multi-utilisateurs qui permettent à plusieurs utilisateurs d'utiliser simultanément sur une même machine des applications différentes ou bien similaires : le système est alors dit « **système transactionnel** ». Pour ce faire, le système alloue à chaque utilisateur une tranche de temps.

Systèmes multi-processeurs

Le **multiprocessing** est une technique consistant à faire fonctionner plusieurs processeurs en parallèle afin d'obtenir une puissance de calcul plus importante que celle obtenue avec un processeur haut de gamme ou bien afin d'augmenter la disponibilité du système (en cas de panne d'un processeur).

On appelle **SMP** (*Symmetric Multiprocessing* ou *Symmetric Multiprocessor*) une architecture dans laquelle tous les processeurs accèdent à un espace mémoire partagé.

Un système multiprocesseur doit donc être capable de gérer le partage de la mémoire entre plusieurs processeurs mais également de distribuer la charge de travail.

Systèmes embarqués

Les **systèmes embarqués** sont des systèmes d'exploitation prévus pour fonctionner sur des machines de petite taille, telles que des PDA (*personal digital assistants* ou en français *assistants numériques personnels*) ou des appareils électroniques autonomes (sondes spatiales, robot, ordinateur de bord de véhicule, etc.), possédant une autonomie réduite.

Ainsi, une caractéristique essentielle des systèmes embarqués est leur gestion avancée de l'énergie et leur capacité à fonctionner avec des ressources limitées.

Les principaux systèmes embarqués «grand public» pour assistants numériques personnels sont :

- PalmOS
- Windows CE / Windows Mobile / Window Smartphone

Systèmes temps réel

Les **systèmes temps réel** (*real time systems*), essentiellement utilisés dans l'industrie, sont des systèmes dont l'objectif est de fonctionner dans un environnement contraint temporellement.

Un système temps réel doit ainsi fonctionner de manière fiable selon des contraintes temporelles spécifiques, c'est-à-dire qu'il doit être capable de délivrer un traitement correct des informations reçues à des intervalles de temps bien définis (réguliers ou non).

Voici quelques exemples de systèmes d'exploitation temps réel :

- OS-9 ;
- RTLinux (RealTime Linux) ;
- QNX ;
- VxWorks.

Les types de systèmes d'exploitation

On distingue plusieurs types de systèmes d'exploitation, selon qu'ils sont capables de gérer simultanément des informations d'une longueur de 16 bits, 32 bits, 64 bits ou plus.

Les fichiers corrompus

Il vous est forcément déjà arrivé de télécharger un fichier sur Internet et que le navigateur plante ou bien que le serveur qui héberge ce fichier coupe la communication. Si ce fichier est un fichier texte, il ne vous manquera que la fin du texte, par contre si celui-ci est un fichier binaire (un programme exécutable par exemple) son exécution pourrait très bien être dangereuse car il manque des informations.

Le système d'exploitation compare donc sa taille réelle à la taille indiquée dans l'en-tête pour vérifier la validité du fichier. On parle généralement d'intégrité. En réalité ce contrôle est réalisé à l'aide d'un algorithme plus performant appelé CRC (contrôle de redondance cyclique).

Infection par un virus

Lorsqu'un fichier est infecté par un virus, ce dernier y ajoute des lignes de code. Ainsi, l'information concernant la taille du fichier située dans l'en-tête ne correspondra plus (à moins que le virus ne soit programmé de manière à modifier l'en-tête), il pourra donc être repéré.