



Si Linux m'était conté

Si vous pensiez vaguement que **Linux** est une marque de mouchoir ou de lessive comme le montre l'image.

Mais Linux ce n'est pas seulement une marque de lessive. C'est aussi le système qui fait fonctionner les serveurs de la planète entière !



Le 16 septembre 2004, Linux est sorti tout fidèle du crâne de son inventeur **Mark Shuttleworth**, revêtu de son armure et prêt à conquérir le monde.

Au commencement était Unix

Linux ? Unix ? Logiciels libres ? Faisons un petit voyage dans le temps pour y voir un peu plus clair.

Les premiers ordinateurs construit à l'époque du XXe siècle étaient de véritables monstres. Leurs force de calcul était constituée de dizaines de milliers de tubes électroniques. Ils occupaient l'équivalent d'un terrain de foot, consommaient autant d'électricité qu'un village entier et dégageaient plus de chaleur qu'une mare de geysers en activité.

Vers le début des années 1960, la taille des machines a pu être réduite de façon considérable avec l'avènement des semi-conducteurs. Les tubes électroniques ont été successivement remplacés par des transistors, puis par des circuits intégrés. Cette nouvelle génération de machines occupait à peine l'espace d'une collection d'armoires normandes. Malheureusement, tous souffraient toujours du même défaut majeur.

Chacun de ces ordinateurs disposait en effet de son propre système d'exploitation, conçu en même temps que la machine et taillé sur mesure par la force des choses. Un ingénieur qui avait appris à se servir de l'une d'entre elles et qui souhaitait travailler sur un autre type de machine était contraint de jeter par-dessus bord tout son savoir-faire pour revenir à la case départ et tout réapprendre depuis le début. Si seulement toutes ces machines pouvaient parler le même langage... Il fallait trouver une solution.

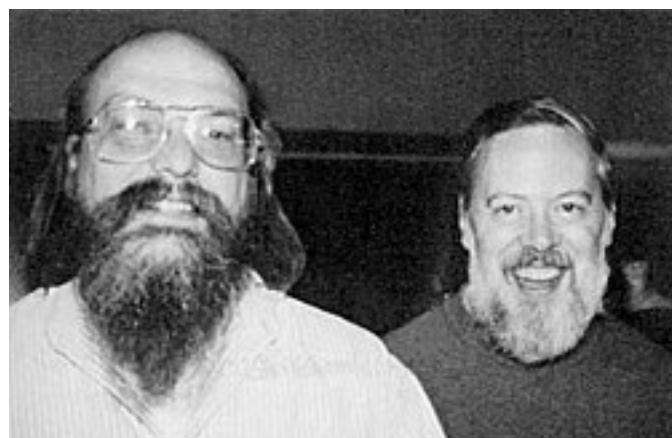
Un système d'exploitation ou OS (Operating System) est un ensemble de logiciels qui gère les fonctions les plus élémentaires d'une machine. D'une part, il contrôle les périphériques entrée(input)/sortie(output) comme le clavier et l'écran, ce qui permet à un humain de communiquer avec l'ordinateur. D'autre part, il s'occupe de la répartition intelligente des ressources de la machine comme le processeur et la mémoire. Une machine dépourvue de système d'exploitation ne sera donc même pas capable de démarrer un programme.

Le projet **Multics** (Multiplexed Information and Computing Service) a été initié en 1964 pour apporter précisément cette solution. L'ambition de Multics consistait à fournir un système d'exploitation **portable**, c'est-à-dire capable d'être porté sur la plupart des machines existantes ; ambition

énorme car, si le projet réussissait, il mettrait fin à la confusion gigantesque des systèmes d'exploitation.

Multics n'a connu qu'un succès modeste, comme cela arrive parfois avec les projets pharaoniques. Hormis quelques thésards en informatique et une poignée de vétérans, l'humanité à même fini par l'oublier. Ce qui nous reste de Multics, c'est une série de bonnes idées, mais qui a fini par connaître un succès incroyable.

1969, l'année où l'astronaute Neil Armstrong se promène sur la Lune, deux ingénieurs des laboratoires BELL, **Dennis Ritchie et Ken Thompson**, décident d'écrire un système d'exploitation pour l'ordinateur dont ils disposent plus ou moins librement dans leur bureau. Cette machine, un **DEC PDP-7**, est considérée comme un "mini-ordinateur" à l'époque. Pour avoir une vague idée de la taille familiale de l'engin, imaginez une batterie de quatre ou cinq réfrigérateurs de taille familiale posés les un à côté des autres. Dennis Ritchie et Ken Thompson se servent des bout de code du projet Multics, mais leur ambition et bien plus modeste, pour ne pas dire purement ludique. Ce qui les motive dans l'immédiat, c'est de disposer d'une machine suffisamment fonctionnelle pour jouer à un jeu tout à fait dans l'air du temps : *Space Travel*, un jeu interactif en mode texte, où il s'agit de poser une capsule spatiale sur la Lune.



Ken Thompson et Dennis Ritchie

Étymologie : Le "x" de Unix

Le nom de "Unics" est contracté par la suite en "Unix". Cette consonne finale sera caractéristique d'un certain nombre de variantes, dérivées et clones d'Unix : XENIX, AIX, HP-UX, ULTRIX, IRIX, MINIX... sans oublier Linux et Mac OS X.

La fin des années 1960, ce n'est pas seulement la conquête spatiale, mais Les campus des universités et les entreprises qui ont une idée en tête : contribuer au code d'Unix en vue de l'améliorer. Certes, la propriété intellectuelle et les brevets existent déjà, mais cela n'empêche personne de vivre pour autant. Les *hackers* - au sens noble du terme - échangent entre eux leurs meilleures idées et les bout de code source qui vont avec. Les entreprises et les facultés ne payent pas de frais de licence pour utiliser Unix et lorsqu'elles réclament le code source à **Ken Thompson**, celui-ci a l'habitude d'ajouter un petit mot au colis de bandes magnétiques et disquettes : "Love Ken".

CULTURE

Code source et programme exécutable

Les sources d'un programme, c'est l'ensemble des fichiers qui contiennent du code et que l'on compile pour obtenir un programme exécutable. Lorsqu'on distribue un programme sous forme binaire, il est prêt à l'emploi, mais on ne peut pas le modifier.

L'AIR DU TEMPS L'informatique avant Microsoft et Apple

Imaginez-vous en 1970 : Microsoft et Apple n'existent pas encore et personne n'aurait l'idée d'associer des mots de tous les jours comme "**Windows**" ou "**Apple**" à de l'informatique. Vous apercevez le future pas trop lointain, quelques décennies plus tard. Vous annoncez solennellement qu'un jour viendra où les systèmes et les applications se vendront **sans** le code source qui va avec. Dans des cartons au graphisme léché. Des boîtes remplies majoritairement de vide comme les *cornflakes*. Ornées de fenêtres multicolores ou d'une pomme stylisée. Le prix sera conséquent, les gens devront acheter les boîtes avec le matériel et les ventes feront de vous l'homme le plus riche de la terre.

Durant les années 1970 et début des années 1980, les universités utilisent à



A quoi ressemblait l'informatique en 1970, avant Microsoft et Apple ?

peu près exclusivement Unix. Les entreprises décident d'emboîter le pas et l'adoptent également à grande échelle. Après tout, les étudiants d'aujourd'hui font les ingénieurs de demain. Techniquement, Unix est à la pointe des systèmes d'exploitation. C'est un vrai système multitâche et multi-utilisateur, robuste et transparent. Il définit clairement les droits d'accès aux fichiers, il sépare les processus bien proprement et il est conçu dès le départ pour fonctionner en **réseau**. Petit à petit, Unix est une bonne voie de faire tourner les ordinateurs du monde entier. L'âge d'or d'Unix connaît une fin abrupte et quelques peu absurde en 1983. Dans le cadre de la lutte antitrust du gouvernement **Ronald Reagan**, Les laboratoires Bell sont séparés de leur maison mère, l'entreprise de communications AT & T (American Telephone and Télégraphe). Dans la foulée des actions judiciaires qui s'ensuivent, un décret qui empêchait la commercialisation d'Unix jusqu'à ce que ce soit rendu caduc. At & T décide de sauter dans la brèche ouverte par la nouvelle législation et de s'approprier le système Unix et tout le code qui va avec, en faisant fi des nombreuses contributions externes. L'émoi

causé par cette mainmise qui - a failli sonner le glas du système - est considérable dans la communauté des *hackers*.

Les étudiants qui ont contribué au code d'Unix s'estiment doublement lésés. D'une part, AT & T "oublie" de les rémunérer alors que les licences sont monnayées au prix fort. D'autre part, ils n'ont plus accès à leur propre code ou - situation plus ubuesque encore - n'ont plus le droit de l'utiliser pour de sombres raisons de propriété intellectuelle.

Certes, At & T essaie de calmer le jeu en annonçant que les universités pourront désormais bénéficier de tarifs préférentiels pour les licences. Il n'empêche que l'accès au code source est dorénavant restreint. Du jour au lendemain, Unix est devenu un système d'exploitation rigoureusement propriétaire et commerciale.

Au niveau Marketing **Les systèmes propriétaires dans l'éducation.**

Quelques décennies plus tard, le tarif préférentiel pour les élèves et les étudiants demeure une stratégie de fidélisation populaire auprès des éditeurs de systèmes de logiciels propriétaires.

Richard Stallman et le projet GNU

La commercialisation d'Unix marque l'avènement d'un véritable âge de faire en informatique. La "culture hacker" des premières années céde la place à une logique restrictive, commerciale et propriétaire. Cette transition ne

s'est pourtant pas faite en un jour. Elle a été marquée par une série de signes avant-coureurs.

Revenons un peu en arrière, en 1980, et rendons visite à Richard Stallman dans son laboratoire d'Intelligence artificielle au Massachusetts Institute of Technology (MIT). Richard est confronté à un problème qu'il n'arrive pas à résoudre. La nouvelle imprimante lasser du laboratoire, une Xerox 9700, se bloque régulièrement et refuse d'imprimer suite à des erreurs de bourrage papier. En bon hacker qui se respecte, Richard aime relever les défis techniques et le dysfonctionnement d'un périphérique tombe dans cette catégorie.

La précédente imprimante, une Xerox XGP, avait connu exactement le même problème de bourrage papier et Richard l'avait résolu comme un



informaticien de l'époque pouvait le faire : il avait réclamé le code source du pilote à Xerox et s'était plongé dans sa lecture. Après avoir identifié l'erreur, il lui avait suffit de modifier et recompiler le code pour que l'imprimante fonctionne correctement. Or, le problème auquel Richard se heurte cette fois-ci n'est pas d'ordre technique. Le fabricant Xerox vient en effet d'opposer un refus à sa demande, estimant que le code source est désormais un secret de fabrication. Richard ne peut donc pas y accéder,

encore moins l'étudier ou le corriger. En revanche, Xerox l'invite à "envoyer un rapport d'erreurs", afin que les ingénieurs de l'entreprise étudient le problème à sa place et mettent à disposition une mise à jour qui corrigera éventuellement le dysfonctionnement. Richard a effectivement soumis le rapport d'erreurs suggéré par Xerox. Il n'a jamais reçu de réponse.

Richard sent naître en lui un mélange de colère et d'impuissance. Les constructeurs de matériel informatique tendent visiblement à ne plus livrer que des pilotes au format binaire, sans le code source qui va avec. L'utilisation de licences logicielles restrictives s'impose manifestement comme une nouvelle norme. C'est une véritable gangrène qui touche le monde de l'informatique et le pourrit de l'intérieur. Il faut donc trouver une solution, une force nouvelle qui puisse contrecarrer cette tendance funeste.

Le 27 septembre 1983, quelques mois après la mainmise d'AT & T sur Unix, Richard poste un message sur Usenet pour annoncer la naissance du projet GNU, un système d'exploitation libre compatible avec Unix.

GNU signifie GNU's Not Unix, c'est-à-dire "GNU n'est pas Unix". C'est un acronyme récursif, l'équivalent linguistique d'un chat qui se mord la queue. L'acronyme récursif est assez répandu en informatique.

Pour Richard comme pour beaucoup d'autres, Unix reste le système d'exploitation de référence, pour toutes les raisons. Son seul défaut, c'est qu'il n'est pas libre. L'ambition du projet GNU consiste ni plus ni moins qu'à réinventer la roue et propose un système d'exploitation libre 100% compatible Unix mais qui, justement, n'est pas Unix, c'est-à-dire qu'il ne contient aucune ligne de code. Un système comme Unix n'est pas un block monolithique. Il est composé d'une multitude de petits programmes, dont chacun s'acquitte d'une tâche bien définie. Cette modularité va considérablement faciliter la tâche du projet GNU, qui se pose comme but concret de remplacer l'un après l'autre chacun des composants d'UNIX par un équivalent libre.

C'est donc un projet d'envergure, une vaste mosaïque qu'il s'agit de compléter avec beaucoup de patience, morceau par morceau. Richard Stallman lui-même démissionne de son poste au MIT en janvier 1984 pour se consacrer entièrement au projet GNU et développer quelques logiciels significatifs : un compilateur, un débogueur, une collection d'outils basiques et l'éditeur de texte Emacs.

Richard comprends très vite que le projet GNU a besoin d'une infrastructure légale pour assurer sa pérennité et lui éviter d'être cannibalisé par les éditeurs de logiciels propriétaires. En 1985, il crée la FSF (Free Software Fondation), une organisation à but non lucratif pour la défense et la

promotion du logiciel libre. Cette même année, il publie le Manifeste GNU, un texte fondateur qui porte aussi bien sur l'aspect technique et social du projet que sur sa philosophie.

Linus Torvalds et le noyau Linux

Au début des années 90 (20 ans après UNIX), un autre personnage important de notre histoire, Linus Torvalds, cherche à développer des outils de production sur une version d'UNIX qui fonctionne sur des PC domestiques ; à destination des particuliers, donc... Vous l'aurez peut-être deviné, il appelle cette version Linux, en gardant le X en hommage à UNIX. Linux est donc : Un descendant direct d'une longue lignée de systèmes d'exploitation qui remonte jusqu'à UNIX, leur ancêtre commun. Il a gardé la même philosophie initiale : des programmes qui font une seule opération essentielle du système, mais qui la font parfaitement. Il est totalement intégré dans le mouvement du libre, ce qui en fait un système d'exploitation ouvert et gratuit !

Ce que les gens ne savent pas toujours, c'est que l'on retrouve Linux un peu partout aujourd'hui. Par exemple, Android est un cousin proche de Linux, avec le même grand-père UNIX. Linux est également dans la box de votre fournisseur Internet, mais aussi dans les robots de la NASA et notamment "Ingenuity" qui s'est posé sur Mars en février 2021 !



Premier pas en ligne de commande

Commencer par taper n'importe quoi et regardez la réaction de votre système. Par exemple : *make test*.

Vous venez de taper une commande au hasard, tout en choisissant bien, et vous vous retrouvez à votre premier message d'erreur. Que s'est-il passé exactement ?

- L'interpréteur de commandes vous affiche une un vite **[javier@serveur- linux ~]\$**. Il vous ainsi signifié qu'il était prêt à recevoir une ou plusieurs commandes.
- Vous avez tapé une commande : ***make***.
- Vous avez fait suivre cette dernière d'un argument : ***test***.
- L'interpréteur a essayé en vain d'exécuter ce que vous lui avez demandé de faire et vous a dit plus ou moins clairement ce qu'il en pense, en l'occurrence : *make: *** Aucune règle pour fabriquer la cible « test ».* Arrêt.
- L'interpréteur vous affiche à nouveau l'invite, pour vous indiquer qu'il est prêt à recevoir d'autres commandes.

A présent, nous n'avons qu'à essayer avec des commandes qui ont un peu plus de sens pour votre machine.

Afficher le contenu d'un répertoire avec **ls**

La commande **ls** (comme list) affiche la liste des fichiers dans un répertoire. Pour afficher le contenu de la racine du système de fichier, saisissez ceci : **ls /** et pour voir ce qu'il ya dans **/usr**, il suffit d'invoquer la commande suivante : **ls /usr**.

Déchiffrer les résultats de votre ordinateur

Qu'est-ce qui est quoi là-dedans ?

Les différentes couleurs de l'affichage nous suggère qu'il ne s'agit peut-être pas d'éléments du même type. Essayez : **ls /etc**

Le résultat de cette commande dépassera éventuellement la taille d'un écran. Certains éléments apparaissent en bleu, d'autres en turquoise, d'autres en noir et blanc et il y a même un peu de rouge. Pour avoir le coeur net, il va falloir utiliser **ls** avec l'option **-F** **ls -F /etc**.

Réinvoquez **ls -F** pour afficher le contenu de **/etc/ppp**. Vous constatez que certains éléments sont suivis d'une barre oblique **/**, d'autres d'une arobase **@** ou d'un astérisque ***** ; le reste des éléments ne contient aucun suffixe.

- La barre oblique **/** (couleur bleu par défaut) désigne un répertoire.
- L'absence de suffixe (couleur par défaut : noire, blanc ou gris, selon votre terminal) indique qu'il s'agit d'un fichier régulier non exécutable.
- L'arobase **@** (couleur par défaut : turquoise) montre qu'il s'agit d'un lien symbolique, ce qui constitue l'équivalent d'un raccourci sous Windows.
- L'astérisque ***** (couleur par défaut : vert) indique qu'il s'agit d'un fichier régulier exécutable.

Mais encore ?

Ces informations paraissent un peu maigre. Nous pouvons en afficher davantage en utilisant l'option **-l** (comme long).

ls -l /etc/sysconfig

L'utilisateur non averti trouvera cet affichage quelque peu énigmatique. En fait, il est facile à lire une fois que l'on sait à quoi corresponds chaque terme.

Tout à fait à gauche, vous avez une série de dix caractères. Le tout premier vous indique s'il s'agit d'un fichier (tiret -) ou d'un répertoire (d comme directory). Ensuite, la série de neuf caractères indique les droits d'accès au fichier ou au répertoire. Les caractères **r**, **w**, **x** et - décrivent ce que l'on a le droit de faire avec le fichier ou le répertoire :

- lire : **r** comme read ;
- écrire : (modifier) **w** comme write ;
- exécuter : **x** pour e[x]ecute ;
- rien du tout : -

Je disais : ce que l'on a le droit de faire. Ce on est en fait assez bien spécifique : les trois premières caractères de la série concernent le propriétaire du fichier, les trois suivants le groupe et les trois derniers le reste du monde.

Humain, pas trop humain ?

La prochaine indication correspond à la taille du fichier. Ici l'astuce est d'invoquer **ls** avec l'option supplémentaire -h ou --human-readable.

Essayez : **ls -lh /etc/sysconfig/**
la taille des fichiers est toute de suite beaucoup plus lisible, car le système l'indique en kilooctets(K), mégaoctets(M) ou gigaoctets(G).

Splendeur et misère des fichiers cachés

Une autre option fréquemment utilisée est **-a** (ou **--all** : tout). Appliquez-la sur votre répertoire utilisateur et vous serais probablement surpris : **ls -a**. Cette option sert à afficher les fichiers et répertoires cachés. Dans un système Linux, les fichiers et répertoires dont le nom commence par un point ne s'affichent pas lorsque **ls** est invoqué normalement. Vous ne les verrez qu'en utilisant l'option **-a**.

Cachez cette configuration que je ne saurais voir

A quoi peuvent bien servir ces fichiers et quel est l'intérêt de les dissimuler ? Les fichiers cachés ou **dotfile** (de l'anglais **dot** : point) contiennent la configuration personnalisées de vos applications. Concrètement, les fichiers **.bash_logout .bash_profile .bashrc** contiennent la configuration de votre *shell* Bash (qui est une application). Quant au fichier **.bash_history**, il renferme l'historique des commandes précédemment invoquées.

Afficher les informations détaillées d'un répertoire

Il nous reste à voir une dernière option importante pour **ls**. Admettons que vous souhaitez afficher les informations détaillées pour le répertoire **/etc** : les droits d'accès, le propriétaire, le groupe etc. Vous invoquez donc hardiment **ls** suivis de l'option **-l** et de l'argument **/etc** et vous voyez... les informations détaillées de tout le contenu du répertoire, mais pas du répertoire lui-même.

Comment faire ? Tout simplement en invoquant l'option supplémentaire **-d** (comme directory, c'est-à-dire "répertoire") : **ls -ld /etc** cette commande affiche les répertoires avec la même présentation que les fichiers, sans lister leur contenu.

pwd : « Vous êtes ici ! »

La commande **pwd** (print working directory) s'acquitte d'une seule tâche. Elle vous affiche (print) quel est le répertoire courant (working directory) dans lequel vous vous situez actuellement.

On bouge avec cd !

La commande **cd** (change directory) est utilisée pour changer de répertoire courant. Il suffit de taper **cd** puis le chemin du répertoire dans lequel on veut se placer. Dans l'exemple suivant, l'invocation de la commande **pwd** après **cd** permet de vérifier que nous sommes bien dans le répertoire demandé.

```
cd /
ls
pwd
cd bin
```

Chemin relatif ou absolu ?

Lorsque je me trouve dans le répertoire racine **/** et que je souhaite me déplacer vers le répertoire **/bin**, je peux écrire **cd bin**. Cela correspond au chemin relatif c'est-à-dire celui indiqué à partir du répertoire dans lequel je me situe, en l'occurrence **/**. Quand à **cd /bin**, c'est le chemin absolu, autrement dit l'emplacement à partir du répertoire racine.

En revanche, lorsque je me trouve dans le répertoire /etc et que je veux me déplacer dans le répertoire /bin, je suis obligé - pour l'instant - d'utiliser un chemin absolu. Pour saisir la distinction, je vous donne un exemple qui illustre ce qu'il ne faut pas faire :

```
[javier@serveur-linux ~]$ cd /etc
```

```
[javier@serveur-linux etc]$  
/etc
```

```
[javier@serveur-linux etc]$ cd bin
```

-bash: cd: bin: Aucun fichier ou dossier de ce type

Ces deux exemples de la vie courante vous permettront peut-être de saisir la nuance :

- "Remontez la rue devant vous, tournez à gauche, continuez deux cents mètres, puis tournez à droite et encore à droite"(chemin relatif).
- "Partez du Vieux Port, remontez la Canebière, puis prenez le boulevard Longchamp et arrêtez-vous au Palais Longchamp"(chemin absolu).

Dans l'exemple si-dessus, nous nous situons dans le répertoire /etc. Si nous écrivons cd bin sans la barre oblique / qui précède, l'interpréteur de commandes cherche un répertoire inexistant /etc/bin et affiche une erreur.

A court d'arguments

Pour revenir dans votre répertoire d'utilisateur, il suffit d'invoquer **cd** sans arguments.

Ici et à l'étage

Voyons maintenant deux répertoires un peu particulier. Affichez la totalité du contenu de votre répertoire d'utilisateur. Vous remarquez qu'en début de

liste, vous avez un répertoire nommé "." et un autre nommé "..". Affichez maintenant le contenu d'un autre répertoire, avec les mêmes options **-aF**. Si vous répétez l'opération sur d'autres répertoires au hasard, vous constaterez que chaque liste débute invariablement par ces mêmes répertoires . et ..

- . est le répertoire courant.
- .. est le répertoire parent.

Là encore, la mise en pratique vous aidera à saisir le concept. Essayez ceci :

```
[javier@serveur-linux ~]$ cd /etc/sysconfig/network-scripts/
```

```
[javier@serveur-linux network-scripts]$ pwd
```

```
[javier@serveur-linux network-scripts]$ cd ..
```

```
[javier@serveur-linux sysconfig]$ pwd
```

```
[javier@serveur-linux sysconfig]$ cd ..
```

```
[javier@serveur-linux etc]$ pwd
```

```
[javier@serveur-linux etc]$ cd ..
```

```
[javier@serveur-linux /]$ pwd
```

Chaque appel à cd .. nous fait ainsi remonter d'un cran dans l'arborescence, jusqu'à ce que nous nous retrouvions à la racine.

Quant au point ".", il faut se le représenter comme le fameux "VOUS ETES ICI" sur le plan de la ville. Admettons que je me situe dans le répertoire /etc et que je veuille me rendre dans le sous-répertoire sysconfig. Je pourrais utiliser indépendamment ces deux notations, qui reviendraient au même :

```
[javier@serveur-linux /]$ cd etc/
```

```
[javier@serveur-linux etc]$ cd sysconfig/
```

```
[javier@serveur-linux sysconfig]$ pwd
```

```
/etc/sysconfig
```

Ou alors :

```
[javier@serveur-linux /]$ cd etc/  
[javier@serveur-linux etc]$ cd ./sysconfig/  
[javier@serveur-linux sysconfig]$ pwd  
/etc/sysconfig
```

Pour l'instant, retenez simplement que "." signifie "ici".

Remarque pwd

Si j'invoque pwd à chaque changement de répertoire, c'est simplement à des fins de démonstration, pour bien expliquer le répertoire courant.

Vous pouvez également monter de plusieurs crans, si cela est nécessaire. Si votre répertoire courant est /etc/sysconfig/network-scripts et si vous souhaitez vous rendre dans /etc/ssh, il va falloir que vous montiez de deux crans, pour ensuite entrer dans le répertoire ssh.

En pratique, cela ressemblerait à l'exemple suivant :

```
[javier@serveur-linux ~]$ cd /etc/sysconfig/network-scripts/  
[javier@serveur-linux network-scripts]$ pwd  
/etc/sysconfig/network-scripts  
[javier@serveur-linux network-scripts]$ cd ../../ssh  
[javier@serveur-linux ssh]$ pwd  
/etc/ssh
```

Méthodologie petit aperçu très bref de la philosophie UNIX

Vous venez d'apprendre en tout et pour tout trois commandes et une poignée d'options. Peut-être sentez-vous monter en vous un vague sentiment de déception. C'est donc ça Linux ? Des commandes qu'il faut taper fastidieusement dans une interface archaïque ?

Pour vous rassurer - et nous conforter dans notre démarche - je me permettrai de vous donner un exemple qui semblera familier à beaucoup d'entre vous. Imaginez que votre voiture (ou la voiture d'une autre personne) tombe en pane un jour. Vous avez en gros deux possibilités pour la faire réparer.

- Vous la faites remorquer au garage Peugeot en ville : un endroit très high tech avec beaucoup de chrome et de carrelage blanc, sans la moindre trace de cambouis ni de poussière. Les mécaniciens ressemblent à des ingénieurs en blouse blanche. Ils sont armés jusqu'aux dents d'ordinateurs portables et ne répondent à personne. Votre voiture est le seul objet sale dans cet endroit étincelant de propreté. L'ingénieur en chef dissimule à peine son dégoût, ouvre le capot et branche un câble dans une prise dont vous ignoriez l'existence jusque-là. Il retourne devant l'écran de son portable, clique sur une série de boutons dans son logiciel de diagnostic et vous annonce qu'il ne peut pas vous fixer un rendez-vous avant le début du mois prochain, mais qu'on peut déjà établir un devis.
- Vous décidez d'aller voir Tony, le mécanicien du village. En guise de bonjour, Tony vous présente son avant-bras à peine moins maculé de cambouis que ses mains. Il propose de s'occuper tout de suite de votre voiture, l'objet le plus propre dans tout le garage. Il ouvre le capot et contemple le moteur en sifflotant le refrain qui vient de passer à la radio. Puis il fouille dans sa boîte à outils et en extrait une clé tubulaire, un tournevis et une pince. A peine deux minutes plus tard, il vous annonce qu'il fallait juste nettoyer les bougies et refixer une durite qui s'était défaite. Il refuse de se faire payer malgré vos protestations réitérées.

Les commandes que nous venons d'apprendre sont certes aussi peu spectaculaires qu'une clé tubulaire, un tournevis ou une clé de douze.

Vous serez d'ailleurs probablement surpris d'apprendre que ce sont des commandes Unix, le système d'exploitation présenté en début de cette formation. Les principes de base d'Unix sont restés les mêmes pendant près de quarante ans. Douglas McIlroy, l'un des fondateurs d'Unix, a résumé la philosophie de ce système et une série de trois impératifs, catégoriques.

1. Écrivez des programmes qui font une seule chose et qui le font bien.
2. Écrivez des programmes qui se combinent les uns avec les autres.
3. Écrivez des programmes pour gérer des flux de texte, car c'est une interface universelle.

Même si vous n'avez pas l'intention d'écrire des programmes Unix (ou Linux), ces trois règles sont d'une importance capitale pour tout utilisateur de systèmes de cette famille. A partir du moment où vous maîtrisez ne serait-ce qu'une poignée de commandes Unix, vous apprendrez à les combiner pour résoudre les problèmes de manière efficace. Gardez ce principe à l'esprit lors de votre apprentissage, car nous verrons bientôt comment les tâches les plus complexes peuvent être décomposées en une série d'opérations simples.

Deux commandes de sortie simples : echo et cat

La commande echo affiche sur l'écran le texte spécifié en argument, par exemple tapez ceci depuis votre terminal : **echo Bonjour Monsieur !** puis faites entrer. Voilà un grand pas pour nous, un petit pas pour l'humanité. Continuons : *[javier@serveur-linux ~]\$ echo Bonjour Monsieur ! > bonjour.txt* Cette fois-ci, il n'y a aucun résultat immédiat. Regardons le contenu du répertoire courant avec un **ls**

Explication : la flèche **>** a redirigé la sortie standard vers un fichier, comme le formulerait quelqu'un du métier. En d'autres termes, la chaîne de caractère **Bonjour Monsieur !** a été écrite dans un fichier **bonjour.txt** au lieu de s'afficher sur l'écran. Affichons le contenu de ce fichier avec la commande **cat** : **cat bonjour.txt**. Un autre exemple tout savoir sur son processeur.

Voici un cas d'utilisation de **cat** qu'on peut rencontrer dans le quotidien d'un administrateur système. Il affiche des renseignements sur le processeur de la machine : **cat /proc/cpuinfo**

cat : afficher et concaténer

Affichons le contenu de ce fichier avec la commande **cat** *bonjour.txt*

Les arborescences en un coup d'oeil avec tree

Puisque nous sommes en plein dans les arborescences de répertoires, le moment est venu de vous présenter un cousin lointain de **ls**, la commande **tree**. Curieusement, on ne la rencontre pas souvent dans les manuels d'initiation de commande sous Linux. La commande **tree** ne fait pas partie de notre système minimal, mais il est facile de l'installer. Déconnectez-vous (**exit**) et reconnectez-vous en tant que root. Vérifiez si vous êtes bien connecté à internet.

ping -c 4 www.centos.org

ensuite installez **tree** comme ceci :

yum install tree



Avant de commencer

Envie d'apprendre à cuisiner ? Il vous faut tout d'abord... une cuisine. Un four. Un frigo. Un évier. Des ustensiles de base. Sans parler des ingrédients, pour lesquels il va falloir songer à faire quelques courses. Supermarché ou marché tout court ? Prenons le temps de répondre à toutes les questions élémentaires que l'apprenti cuistot sous Linux peut se poser. Car toute recette "aux petits oignons" demande un peu de préparation.

Petite introduction culinaire

Il existe grossièrement trois façons de concevoir la cuisine. Prenons l'exemple d'un plat de lasagnes.

1. Achetez une boîte congelées. Placez le contenu dans un four à micro-ondes et faites chauffer. Observez la transformation progressive du bloc de béton grisâtre en geyser de boue ocre en ébullition. Notez qu'à aucun moment de l'opération, la plat ne ressemble à l'illustration appétissante de l'emballage.

2. Achetez les ingrédients nécessaire pour la préparation d'un plat de lasagnes. Faites vos emplettes au marché et dans les petits commerces du quartier, en dédaignant les super marchés. Pour quatre personnes, prenez trois cent cinquante grammes de boeuf maigre, trois cent cinquante grammes de farine, quatre oeufs, un oignon, une carotte, une échalote, une branche de céleri, un bouquet garni, quelques cuillères d'huile d'olive, deux feuille de sauge et un zeste de citron. Sans oublier une grappe de tomates fraîches, un bol de parmesan râpé et un demi-litre de bouillon. Le cas échéant, les tomates en boîte, le fromage en sachet et le bouillon cube font très bien l'affaire. Épluchez, lavez, hachez finement, épluchez encore, égouttez, hachez encore, coupez en petit dès, faites chauffer, couvrez, laissez étuver, remuez, mélangez, salez, poivrez, faites bouillir, arrosez, portez à ébullition, et ainsi de suite. Au bout d'une heure, sortez les lasagnes du four et servez-les avec une petite coupelle de parmesan.
3. Inscrivez-vous à une faculté de sciences et faites des études de biochimie alimentaire. Découvrez et apprenez par coeur la composition moléculaire de quelques milliers d'aliments. Au bout de deux ans à peine, vous serez en mesure d'évaluer le pH d'une sauce tomate et cinq ans d'étude suffiront pour vous permettre d'entreprendre la modélisation moléculaire d'un plat de lasagnes *alla bolognese*.

Vous l'aurez deviné : ce premier module se propose de vous initier à l'installation, la configuration, l'administration et l'utilisation de Linux comme un cuistot vous initierait à la cuisine. Sa philosophie - son approche sera donc en tous points pratique et pragmatique, semblable à la deuxième conception culinaire énoncé précédemment.

Et maintenant, en cuisine !

Se former à Linux avec CentOS

Pour ce module, j'ai pris parti, pour toute une série de raisons, de choisir une distribution bien précise : CentOS Linux. CentOS est un système techniquement identique à Red Hat Enterprise Linux qui est une distribution Linux produite par Red Hat et orientée vers le marché commercial et les serveurs d'entreprise. La principale différence résidant dans le fait que Red Hat fournit un support technique payant pour ses clients. C'est une distribution de qualité "entreprise", solide et éprouvée, qui ne réserve pas de mauvaises surprises. CentOS fait partie de distributions les plus populaires sur les serveurs du monde entier et assure une partie significative de l'infrastructure d'internet. En dehors de CentOS et Red Hat Entreprise Linux, les entreprises et les administrations utilisent régulièrement Debian et Ubuntu LTS sur leur serveurs. Dans la famille des Unix, FreeBSD et sans conteste le système le plus populaire. Le focus sur CentOS et la famille Red Hat est donc un parti pris pédagogique. Une fois que vous aurez intégrer les concepts présentés de ce module "avec le sourire", vous pourrez vous familiariser petit à petit avec les systèmes de la famille Debian et BSD et leur manière particulière de faire les choses.

Le matériel : usine à gaz ou simple gazinière ?

Je connais un pianiste hongrois qui a une façon assez singulière de répéter. Lorsqu'on lui confie un nouveau morceau à travailler, il prends la pile partitions, s'installe dans un fauteuil confortable et étudie chaque page en sirotant un café. Suivant la durée et la complexité du morceau, l'opération peut durer quelques minutes ou quelques heures. Et c'est seulement après avoir appris, mémorisé et maîtrisé mentalement chaque note, chaque mesure et chaque passage que le maestro se lève, s'installe au piano et s'exécute. Si vous sentez un talent comparable pour l'informatique,

vous pouvez très bien vous contenter de la simple lecture d'un livre d'informatique par exemple. Dans le cas contraire, si vous doutez de vos capacités d'émulation mentale, il vous faudra songer à vous procurer l'instrument approprié pour mettre en pratique ce que nous allons apprendre dans ce premier module.

Vous aurez donc le choix de vous entraîner sur... :

- un PC faisant office de serveur;
- un vrai serveur
- une machine virtuelle

Dans notre cas nous allons utiliser une machine virtuelle.

Acheter un PC faisant office de serveur

Pas la peine de casser la tirelire pour découvrir Linux sur un ordinateur dédié. En règle générale, un PC d'occasion vieux de six ou sept ans fera très bien l'affaire. Si vous optez pour la solution PC-reconverti-en-serveur, évitez les ordinateurs portables trop modernes. Hormis le fait que l'utilisation d'un PC portable comme serveur est une aberration, vous risquez d'avoir quelques surprises avec le matériel ultra-récent et/ou exotique.

Acheter un vrai serveur

Vous pouvez partir également sur du "vrai" matériel serveur. Là encore, ce n'est pas la peine de débourser une fortune. Les serveurs reconditionnés en bon état sont vendus à partir d'une centaine d'euros. Optez plutôt pour le format tour que pour une lame, à moins que vous ne disposiez d'un rack de rangement dans vos locaux.

Un facteur que l'on oublie souvent lorsqu'on achète un serveur c'est le bruit. Certains modèles génèrent autant de bruit qu'une batterie de sèche-cheveux au démarrage, ce qui peut vite déverdir lassant lorsqu'on essaie de travailler à côté.

Lorsque j'effectue une installation dans une petite entreprise qui ne dispose pas d'un local à part pour les serveurs, j'utilise à peu près systématiquement les machines HP de la gamme Proliant Microserver. Les serveurs de cette famille sont particulièrement silencieux et vous pouvez les poser dans un espace de travail sans vous faire maudire par tout le monde. Dans mon bureau, j'ai un des premiers modèles de HP Proliant Microserver qui tourne

depuis cinq ans et j'en suis très satisfait. **C'est dans les vielles marmites qu'on fait les meilleures soupes.**

L'achat de matériel reconditionné - voire le reconditionnement de votre matériel existant - offre une série d'avantages non négligeables. Vous faites un geste pour l'environnement, puisque vous offrez une seconde vie sous Linux à votre serveur. Et un aspect que l'on oublie parfois, c'est la compatibilité. En achetant du matériel serveur qui date un peu, vous pouvez être sûr à 100% que tous vos composants seront reconnus sans problème par CentOS.

Comment obtenir la distribution CentOS ?

Rendez sur le site officiel <https://mwww.centos.org/> mais pour vous faciliter la tâche voici le lien de téléchargement de CentOS : http://centos.mirror.ate.info/7.9.2009/isos/x86_64/CentOS-7-x86_64-Minimal-2009.iso

S'entraîner sur un système virtualisé

Une solution virtualisée permet de vous entraîner sur votre ordinateur personnel sans pour autant mettre en péril votre système et vos données ; cela vous évite l'acquisition de nouveau matériel. Elle vous dispense également de la confection du support d'installation, étant donné que vous pourrez vous servir directement du fichier ISO que vous venez de télécharger.

VirtualBox ("machine virtuel") est un logiciel de virtualisation de systèmes d'exploitation. En utilisant les ressources matériels de l'ordinateur (système hôte), VirtualBox crée un ordinateur virtuel dans lequel s'installent d'autres systèmes d'exploitation (système invités). Les systèmes invités fonctionnent en même temps que le système hôte, mais seul ce dernier a accès directement au véritable matériel de l'ordinateur.

VirtualBox est un logiciel libre développé par la société Oracle. Il est disponible pour les plate-formes Microsoft Windows, Mac OS X, Linux et Solaris. Voici le lien direct de téléchargement : <https://download.virtualbox.org/virtualbox/7.0.2/VirtualBox-7.0.2-154219-Win.exe>

Une fois installé et lancé vous aurez une fenêtre comme le montre l'image.



Bienvenue dans VirtualBox !
La partie gauche de cette fenêtre contient les outils globaux et affiche la liste des machines virtuelles de votre ordinateur. Vous pouvez importer, ajouter et créer de nouvelles machines virtuelles en utilisant le bouton correspondant dans la barre d'outils. Vous pouvez afficher les outils d'un élément sélectionné à l'aide du bouton correspondant.

Vous pouvez appuyer sur F1 pour obtenir de l'aide, ou visiter www.virtualbox.org pour plus d'information et les dernières nouvelles (en anglais).



Créer et configurer une Machine Virtuel

Dans l'exemple qui suit, nous allons créer et préparer une machine virtuel pour CentOS.

1. Démarrez VirtualBox et cliquez sur **Nouvelle** pour créer une nouvelle machine virtuelle.
2. Définissez le nom (CentOS 7 64-bit), et le type (Linux) et la version (Red Hat 94-bit).

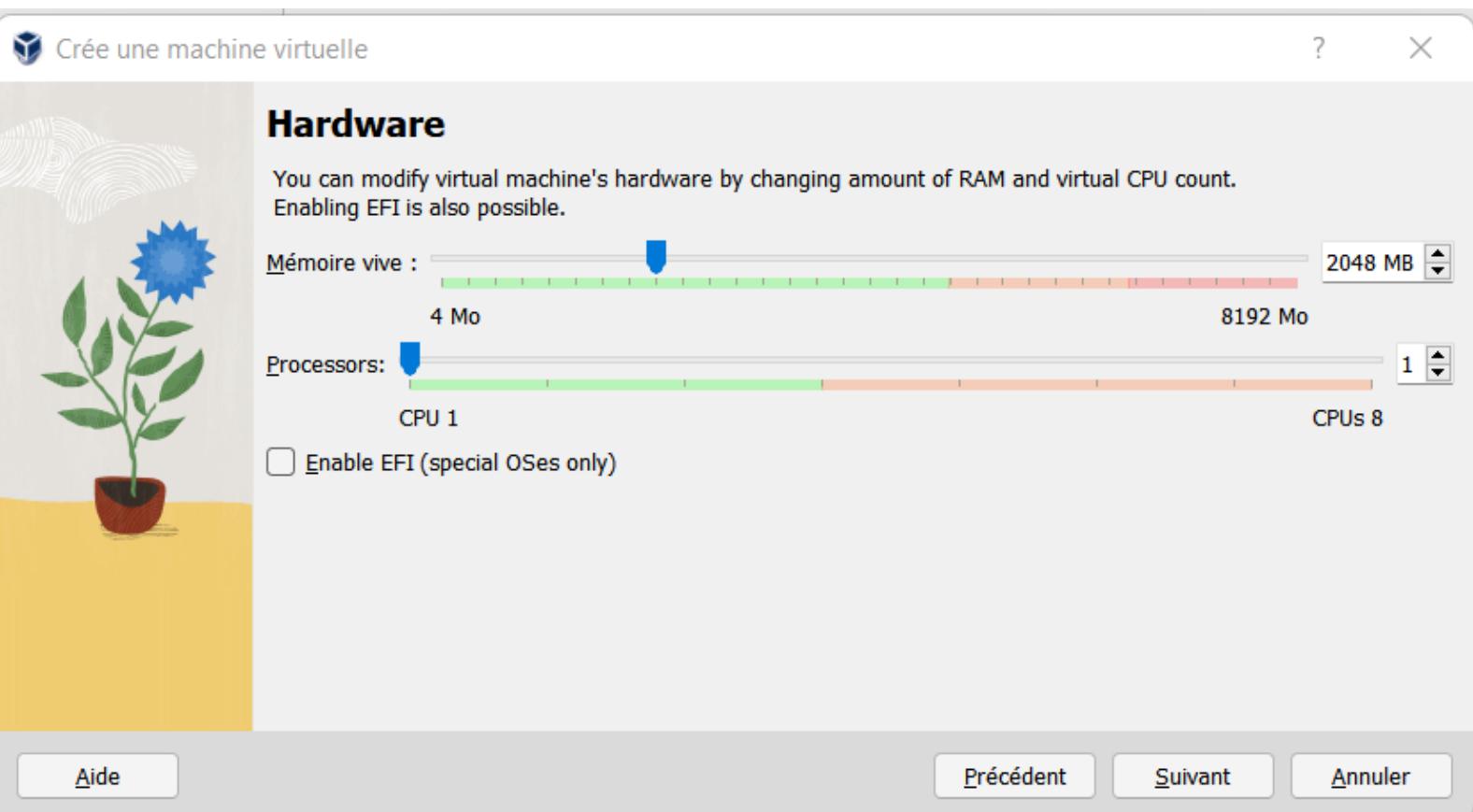
 Crée une machine virtuelle ? X

Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

	Nom : <input type="text" value="CentOS 7 64-bit"/> <input checked="" type="checkbox"/> Folder: <input type="text" value="C:\Users\JavierPerez\VirtualBox VMs"/> ISO Image: <input type="text" value="<non sélectionné>"/> Edition: Type : <input type="text" value="Linux"/> Version : <input type="text" value="Red Hat (64-bit)"/>
	<input type="checkbox"/> Skip Unattended Installation ! No ISO image is selected, the guest OS will need to be installed manually.

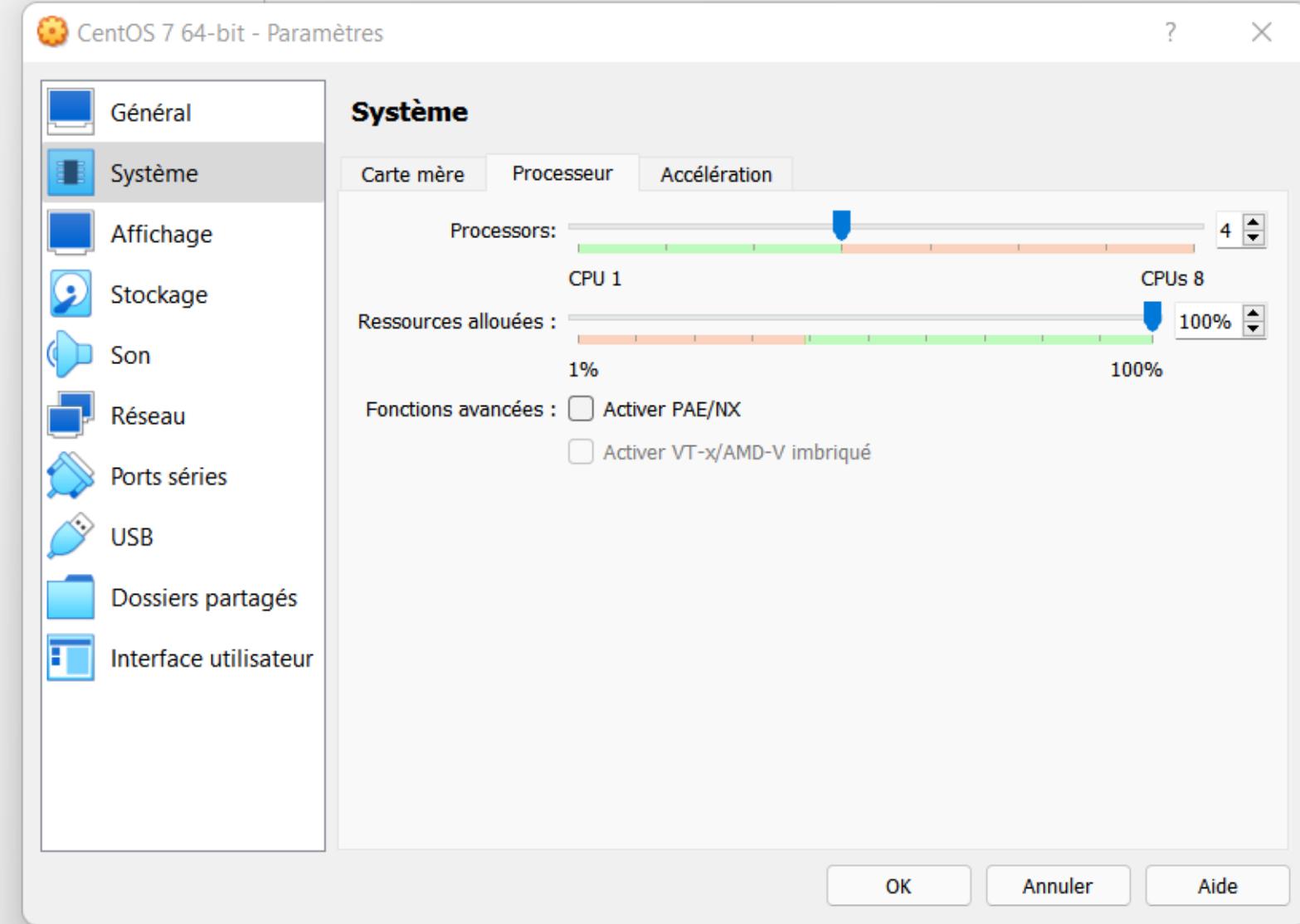
3. Faire suivant et définissez la quantité de mémoire vive que vous souhaitez allouer à la machine virtuelle. Vous pouvez laisser ce que l'assistant suggère par défaut et vous faites suivant.



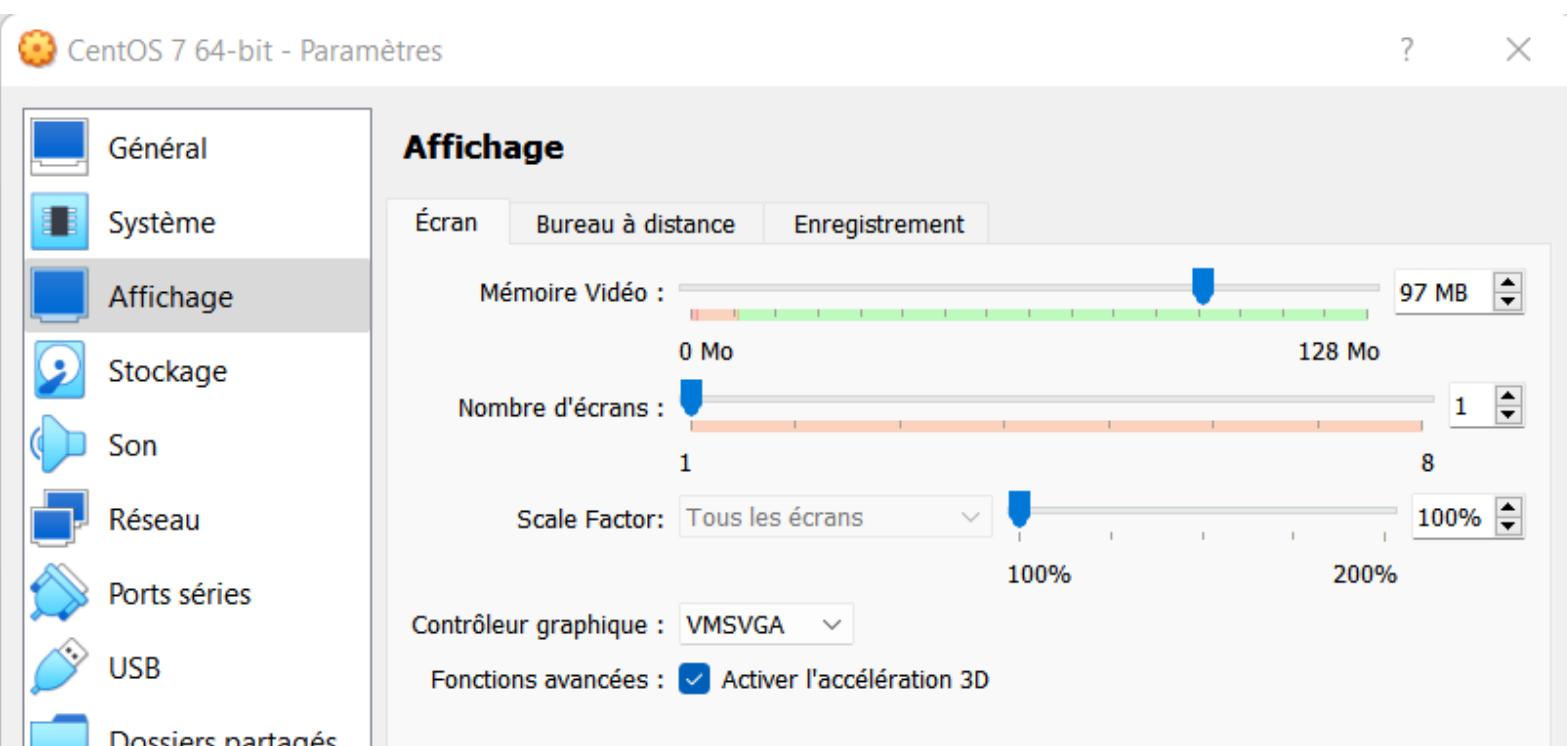
4. Créez un disque dur virtuelle. Gardez l'option par défaut et faites suivant puis cliquez sur finish.

Maintenant que la machine virtuelle est créée, nous allons la configurer. Plus exactement, nous allons définir ses caractéristiques matérielles. Suivez le guide.

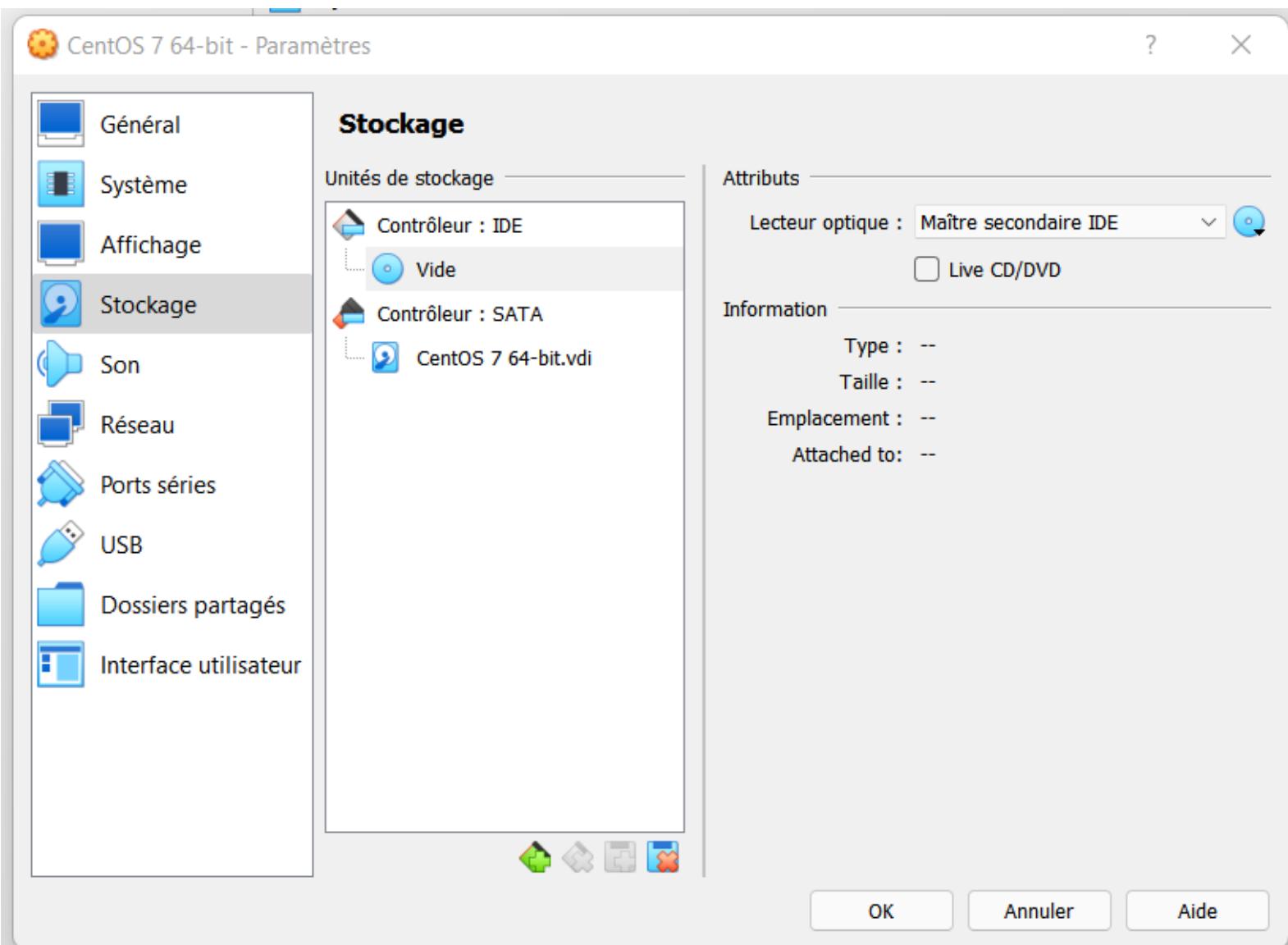
Cliquez sur le bouton **Configuration** dans section **Système** repérez l'onglet **Processeur** et augmentez éventuellement le nombre de processeur de la machine virtuelle. Vous pouvez décochez la case Activer PAE/NX qui ne concerne que les systèmes 32-bits comme le montre l'image.



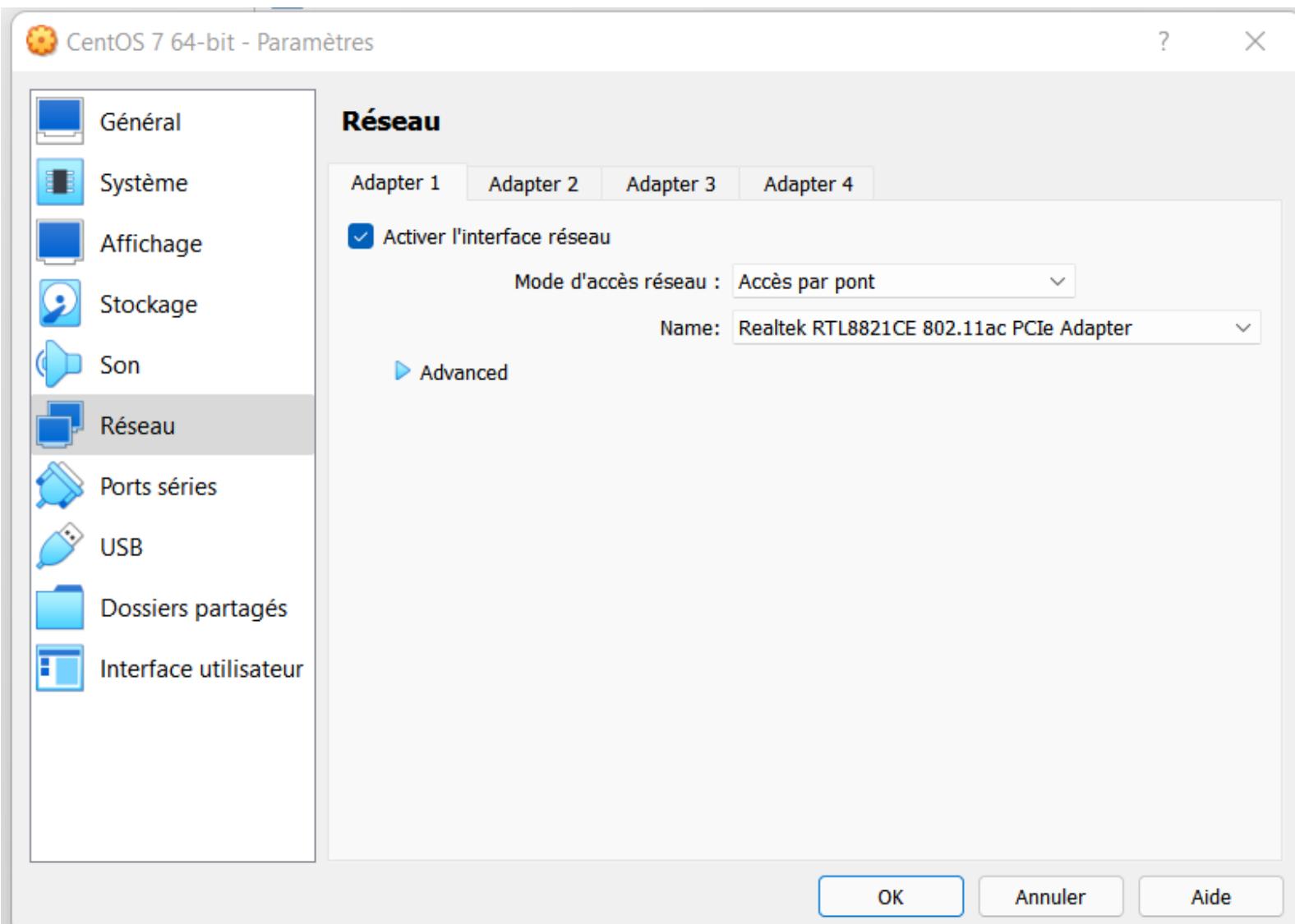
Dans la section **Affichage**, vous pouvez éventuellement augmenter la mémoire vidéo et activer l'**accélération 3D**.



Dans la section **Stockage** sélectionnez le champ Vide du Contrôleur : IDE, cliquez sur la petite flèche en dessous de l'icône du CD pour déplier le menu du lecteur optique et sélectionnez votre fichier ISO.



Dans la section **Réseau**, remplacez la configuration **NAT** par un **Accès par pont** dans le menu déroulant du mode d'accès réseau et terminez en cliquant sur Ok.



VirtualBox fait partie des applications du genre "usine à gaz" qui peuvent intimider par une myriade de fonctionnalités et d'options. Si vous souhaitez aller plus loin, n'hésitez pas à jeter un oeil sur l'excellente documentation du projet, qui existe également en traduction française. Elle a peut-être une ou deux versions de retard, mais ce n'est pas bien grave.

Enfin, notez que nous ne traitons pas ici l'installation des Addition Invité (Guset Addition) de VirtualBox, qui ne sont réellement nécessaires que sur un système invité de type poste de travail.

Et maintenant, il est temps de mettre la main à la pâte...



Installation du système Linux

Pour découvrir un système d'exploitation comme Linux il faut d'abord l'installer sur son ordinateur. C'est probablement beaucoup moins difficile que vous ne l'imaginez. Avec un peu de pratique c'est même un jeu d'enfant.

L'oeuf ou la poule ?

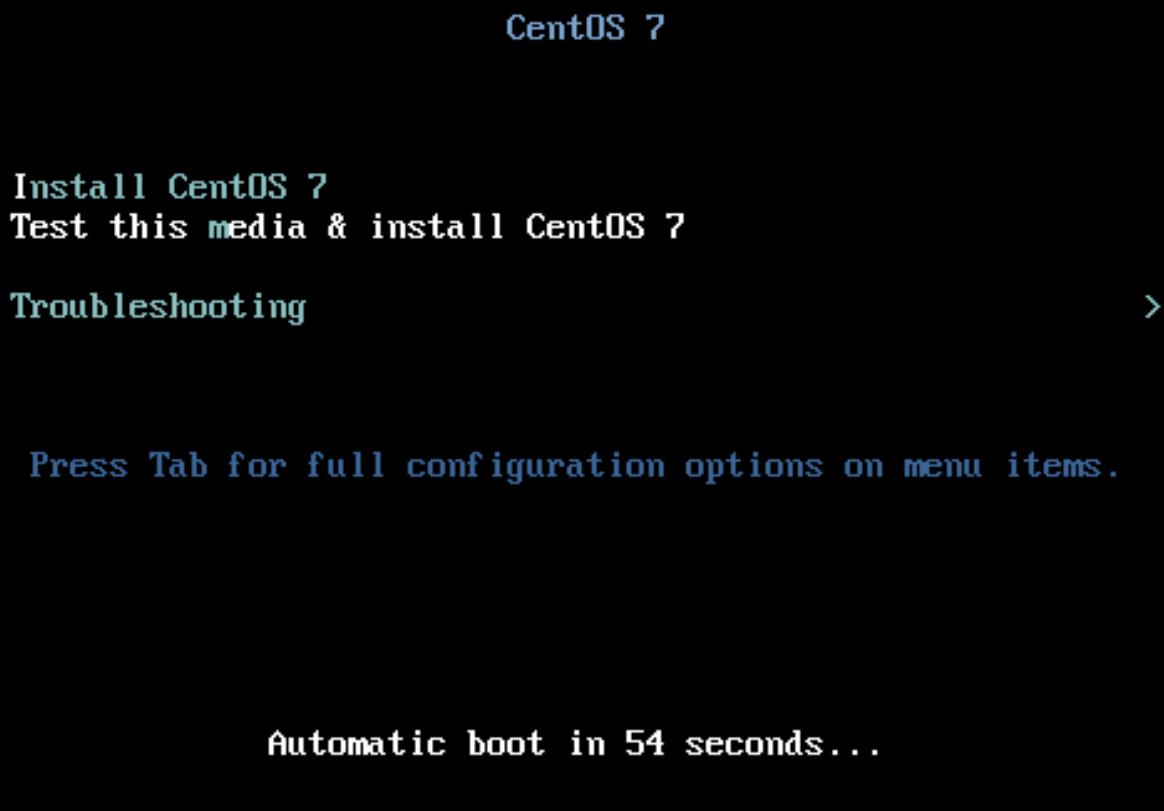
Nous voilà donc armés jusqu'aux dents de matériel, de supports d'installation et de bonne volonté. Et nous nous retrouvons face à un dilemme. Tout le monde connaît la paradoxe de l'oeuf et la poule : qui était là en premier, l'oeuf ou la poule ? L'oeuf, répondez-vous, pour vous ravisir instantanément en vous demandant quelle poule a bien pu le pondre. La poule, donc, mais non, car de quel oeuf a-t-elle bien pu éclore ? Et ainsi de suite.

Notre dilemme est analogue et peut être formulé ainsi :

- l'apprentissage de Linux par la pratique nécessite une installation fonctionnelle de ce système ;
- l'installation de Linux nécessite de connaître le système un tant soit peu.

Pour sortir de cercle vicieux, nous allons effectuer dans un premier temps ce que certains informaticiens anglophones appellent une *chicken install* : l'installation d'un système d'exploitation telle qu'une poule serait capable de réaliser. Il suffit qu'elle accepte les choix par défaut de l'installation en actionnant la touche *Entrée* avec son bec : *OK, OK, OK, OK, OK...*

A présent dans VirtualBox, mettez en surbrillance et cliquez sur le gros bouton **Démarrer** en haut de l'écran, symbolisé par une **flèche verte**. Au bout de quelques secondes, vous voyez apparaître l'écran de démarrage



que voici :
en suite vous aurez une fenêtre vous demandant de la langue comme dans l'image suivante :



CentOS

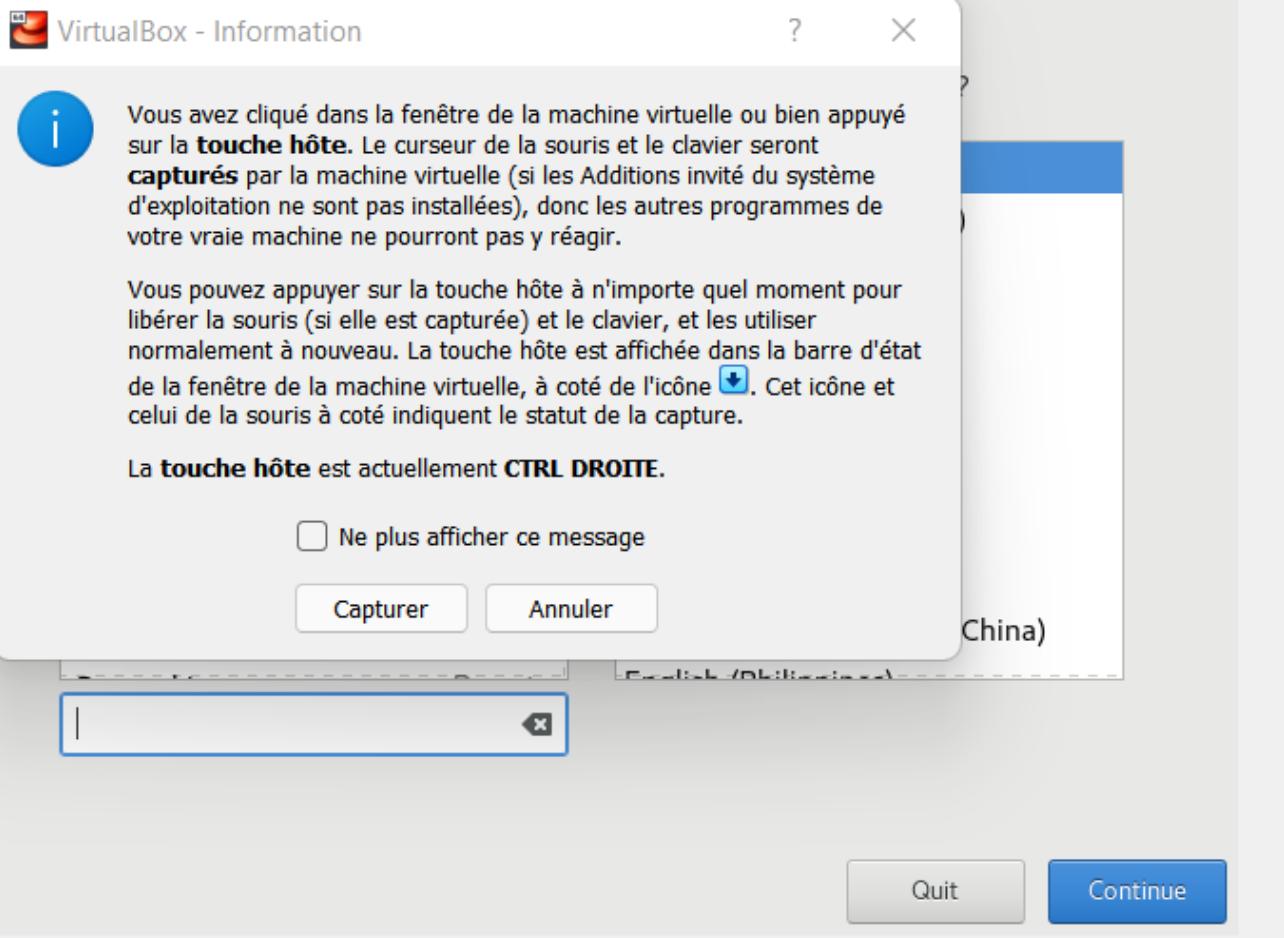
WELCOME TO CENTOS 7.

What language would you like to use during the installation process?

English	English	English (United States)
Afrikaans	Afrikaans	English (United Kingdom)
አማርኛ	Amharic	English (India)
العربية	Arabic	English (Australia)
অসমীয়া	Assamese	English (Canada)
Asturianu	Asturian	English (Denmark)
Беларуская	Belarusian	English (Ireland)
Български	Bulgarian	English (New Zealand)
বাংলা	Bengali	English (Nigeria)
Type here to search. <input type="text"/>		English (Hong Kong SAR China)

 Quit Continue

dans la barre de recherche cliquez pour choisir la langue une nouvelle fenêtre s'ouvre cette fenêtre vas nous permettre d'utiliser la souris, pour ce faire cliquez sur **Capturer**, la fenêtre vas disparaître et vous laisseras utiliser la souris, maintenant dans la barre de recherche il suffit d'écrire **fr** pour choisir la langue en français :



RÉSUMÉ DE L'INSTALLATION



CentOS

LOCALISATION



DATE ET HEURE

Fuseau horaire Europe/Paris



PRISE EN CHARGE DE LA LANGUE

Français (France)



CLAVIER

Français (variante)

LOGICIEL



SOURCE D'INSTALLATION

Média local



SÉLECTION DE LOGICIELS

Installation minimale

SYSTÈME



DESTINATION DE L'INSTALLATION



KDUMP

Quitter

Démarrer l'installation

puis nous allons voir apparaître une nouvelle fenêtre contenant tous les options de l'installateur :

Partitionner le disque dur

Pour cette première installation, nous nous simplifierons la vie et nous choisirons le partitionnement automatique.

1. Cliquez sur **Destination de l'installation**
2. Vérifiez que le disque est bien sélectionné.

CIBLE DE L'INSTALLATION

Terminé

INSTALLATION DE CENTOS 7

fr (oss) Aidez-moi !

Sélection des périphériques

Selectionnez le périphérique sur lequel vous souhaitez faire l'installation. Il restera intact jusqu'à ce que vous cliquiez sur le bouton « Commencer l'installation » du menu principal.

Disques locaux standards

20 GiO	
ATA VBOX HARDDISK	
sda / 20 GiO d'espace libre	

Les disques décochés ne seront pas modifiés.

Disques spéciaux et réseau

	Ajouter un disque...
--	----------------------

Les disques décochés ne seront pas modifiés.

Autres options de stockage

Partitionnement

Configurer automatiquement le partitionnement. Je vais configurer le partitionnement.
 Je voudrais libérer plus d'espace.

[Résumé complet du disque et du chargeur de démarrage...](#) 1 disque sélectionné ; 20 GiO de capacité ; 20 GiO d'espace libre [Rafraîchir...](#)

3. Grdez l'option **Configurer automatiquement le partitionnement.**
4. Cliquez sur **Terminer.**

Désactiver le service Kdump

Kdump est un mécanisme de capture lors du plantage d'un noyau, désactivez le en décochant la petite case **Activer Kdump** : cliquez sur Terminé.

KDUMP

Terminé

INSTALLATION DE CENTOS

fr (oss)

Aidez-moi !

Kdump est un mécanisme de capture lors du plantage d'un noyau. Kdump capture les informations de votre système qui peuvent être cruciales pour aider à déterminer la cause de l'échec. Notez que kdump requiert une partie de la mémoire système qui sera indisponible pour d'autres utilisations.

Activer Kdump

Réserve de la mémoire Kdump (en Mo) : Automatique Manuel

Mémoire à réserver (en Mo) :

160 - +

Mémoire totale du système (en Mo) : 1998

Mémoire utilisable du système (en Mo) : 1838

Activer le réseau et définir le nom d'hôte

Réseau DHCP

DHCP signifie Dynamique Host Configuration Protocole et désigne un protocole d'allocation dynamique d'adresses IP. Pour comprendre le principe de fonctionnement du DHCP, imaginez un cours d'anglais où le professeur décide de donner des noms typiquement anglais à ses élèves. Pour la durée du cours, tel élève s'appellera donc Fredy, sa voisine à droite sera Pamela et son voisin de gauche sera connu sous le nom de Brian. Pour éviter toute confusion, chaque élève portera un prénom distinct. De façon analogue et en simplifiant un tant soit peu, le modem/routeur dira à votre PC : " Pour une durée de 32 400 secondes, tu seras la machine 192.198.2.10 dans le réseau."

Si tout ce passe bien, votre serveur DHCP vous attribue vos paramètres réseau :

- une *Adresse IP* (quelque chose comme 192.168.2.10) ;
 - un *Masque de sous-réseau* (quelque chose comme 255.255.255.0) ;
 - une *Route par défaut* (quelque chose comme 192.168.2.1) ;
 - l'adresse IP d'un *serveur DNS* (quelque chose comme 192.168.2.1) ;
- mais pas forcément la même adresse IP que la route par défaut dans notre exemple.

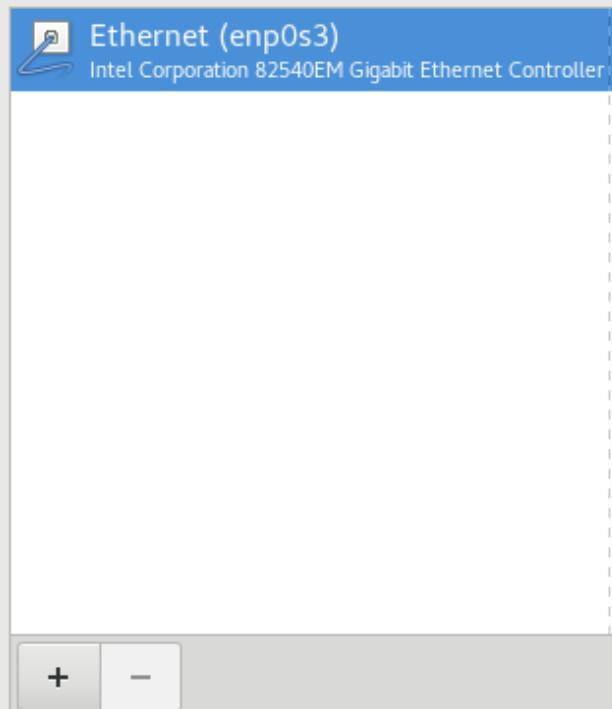
Pour le nom d'hôte de votre machine, choisissez-en un à votre convenance, en remplacement de *localhost.localdomain* par défaut. Voici quelques exemples pour vous donner une idée :

- centosbox ;
- nestor ;
- serveur-linux ;
- etc.

Terminé

fr (oss)

Aidez-moi !



Ethernet (enp0s3)
Intel Corporation 82540EM Gigabit Ethernet Controller
Déconnecté
Adresse matérielle 08:00:27:A7:96:05
Vitesse 1000 Mb/s
Masque de sous-réseau 127.0.0.1

Nom d'hôte :

Appliquer

Nom d'hôte actuel : localhost

Définir les paramètres utilisateur

L'écran *Paramètres utilisateur* nous permet de choisir un mot de passe administrateur et nous propose de créer un premier utilisateur.

Fin de l'installation et redémarrage initial

Au terme de l'installation et de la configuration du système, il ne vous reste plus qu'à *Redémarrer* la machine.

Connectez-vous en tant qu'utilisateur normal. Notez que le mot de passe ne s'affiche pas sur l'écran. Si tout se passe bien, vous vous retrouvez face à l'invite de commande.

CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64
serveur-linux login: gaby
Password:
[gaby@serveur-linux ~]\$



Linux en mode texte consolez-vous !

Introduction à la ligne de commande



C'est un fait : l'utilisation de la ligne de commande intimide la plupart des utilisateurs novices de Linux. D'après un petit sondage que j'ai effectué dans mon entourage, le travail en mode texte est associé à une période révolue et désormais archaïque de l'informatique, lorsque les souris et les interfaces graphiques n'existaient pas encore, que la notion de confort d'utilisation (la fameuse *usability*, traduite parfois par les néologismes *usabilité* ou *utilisabilité*) était encore inconnue. La manipulation de ces mystérieuses machines était alors réservée à un public averti, initié aux arcanes du métier. Les personnes qui continuent à utiliser la ligne de commande de nos jours feraient ainsi penser à de drôle d'hurluberlus à rouler en deux CV ou, pire, en traction avant ; un petit groupe de passéeiste aussi irréductibles qu'incorrigibles.

Ce refus en bloc peut se comprendre lorsqu'on voit certains ouvrages, soit-disant "pour les nuls", qui inculquent avant tout au lecteur le sentiment d'être effectivement nul en la matière, ou encore lorsqu'on considère certains ouvrages "d'introduction", "pour débutant" ou autres, qui n'ont d'autre but que de vous plonger la tête dans le cambouis en vous faisant faire le tour, complet et exhaustif, des commandes Unix de A à Z, avant de vous lancer dans un grand écart sans échauffement vers l'édition de script *shell*. Ajoutons à cela les mauvais souvenir que certains auront pu garder de la fameuse invite de commande DOS de Microsoft et les réticences s'expliquent.

Laissons là toute polémique, et même toute théorie ; concentrons-nous sur la pratique car nous attaquons la première leçon d'introduction à la ligne de commande. Pour travailler en ligne de commande, vous devez tout d'abord vous retrouver face à une "invite de commande" (en anglais : *command prompt*).

Se connecter à un serveur Linux en SSH

Le système SSH (Secure Shell) est un protocole sécurisé de connexion à distance développé par l'équipe d'OPENBSD depuis 1999. Si nous en parlons sommairement ici, c'est que, dans le cadre d'une formation en entreprise, il est pratique de pouvoir se connecter d'emblée sur un serveur Linux dans le réseau mais avant nous devons installer Open SSH Server dans notre machine avec la commande suivante :

yum install openssh-server. Pour connaître l'adresse IP du serveur il suffit de lancer la commande suivante depuis CentOS **ip addr**. Voici un exemple de l'adresse ip de la machine je l'ai mise en surbrillance pour la repérer facilement :

Mise à jour	: openssh-7.4p1-22.el7_9.x86_64	1/6
Mise à jour	: openssh-server-7.4p1-22.el7_9.x86_64	2/6
Mise à jour	: openssh-clients-7.4p1-22.el7_9.x86_64	3/6
Nettoyage	: openssh-clients-7.4p1-21.el7.x86_64	4/6
Nettoyage	: openssh-server-7.4p1-21.el7.x86_64	5/6
Nettoyage	: openssh-7.4p1-21.el7.x86_64	6/6
Vérification	: openssh-server-7.4p1-22.el7_9.x86_64	1/6
Vérification	: openssh-clients-7.4p1-22.el7_9.x86_64	2/6
Vérification	: openssh-7.4p1-22.el7_9.x86_64	3/6
Vérification	: openssh-clients-7.4p1-21.el7.x86_64	4/6
Vérification	: openssh-7.4p1-21.el7.x86_64	5/6
Vérification	: openssh-server-7.4p1-21.el7.x86_64	6/6

Mis à jour :
 openssh-server.x86_64 0:7.4p1-22.el7_9

Dépendances mises à jour :
openssh.x86_64 0:7.4p1-22.el7_9 openssh-clients.x86_64 0:7.4p1-22.el7_9

Terminé !

```
[javier@serveur-linux ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:90:44:2a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.121/24 brd 192.168.1.255 scope global noprefixroute dynamic enp0s3
        valid_lft 86142sec preferred_lft 86142sec
    inet6 2a02:8428:4d06:4601:9862:fe2b:6804:5b7c/64 scope global noprefixroute dynamic
        valid_lft 269sec preferred_lft 269sec
    inet6 fe80::4ab7:6535:8b0a:6503/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[javier@serveur-linux ~]$
```

Utiliser PuTTY sous windows

PuTTY est un client SSH libre pour Windows, écrit par Simon Tatham et publié sous licence MIT (Massachusetts Institute of Technology). Pour télécharger PuTTY rendez-vous à l'adresse suivante : <https://www.putty.org/> ensuite cliquez sur Download PuTTY. Pour ouvrir une session distante avec PuTTY, je dois lui fournir quelques paramètres de base comme le nom de hôte ou l'adresse IP, le port et le type de connexion. Voici un exemple de mon réseau local :

 PuTTY Configuration X

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
 - Features
- Window
 - Appearance
 - Behaviour
 - Translation
- + Selection
 - Colours
- Connection
 - Data
 - Proxy
 - + SSH
 - Serial
 - Telnet
 - Rlogin
 - SUPDUP

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

Connection type:

SSH Serial Other: ▼

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:
 Always Never Only on clean exit

Le saviez-vous ? Votre machine virtuelle est une machine distante !

A partir du moment où vous avez configuré correctement l'accès par pont comme mode d'accès réseau de votre machine virtuelle dans VirtualBox, votre système invité se comporte comme une machine à part entière de votre réseau. Vous pouvez donc afficher son adresse IP et vous connecter en SSH comme s'il s'agissait d'une "vrai" machine physique distante.

Un peu d'histoire

Le terme terminal est issu de l'ère préhistorique de l'informatique, où les ordinateurs personnels n'existaient pas encore. Pour se connecter à l'un de ces ordinateurs ancestraux, il fallait un terminal, c'est-à-dire un bloc sans la moindre puissance de calcul incorporée - composé uniquement d'un clavier et d'un écran, ainsi que d'un câble le reliant à l'ordinateur central.



Une pièce de musé : un "terminal", un vrai.



La carte Ethernet

Si nous procédons méthodiquement, nous devons d'abord nous poser la question ; le serveur dispose-t-il d'une carte Ethernet ? Si oui, est-elle branchée correctement ? Bien sûr, nous pouvons jeter un coup d'oeil sur les branchements de la machine, ce qui nécessite parfois de grimper derrière le meuble où il est rangé. Alternativement, nous pouvons rester assis devant et nous contenter d'invoquer la commande suivante :

lspci | grep -i eth

00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)

NOTE : pour pouvoir utiliser la commande **lspci** il faudrait l'installer
sudo yum install pciutils

La commande **lspci** nous montre qu'elle est équipée d'une carte réseau intel.

Attention : cette commande nous dit uniquement qu'une carte Ethernet est bien présente physiquement sur le serveur. Cela ne veut pas forcément dire

que la carte est effectivement gérée par le système d'exploitation. Si nous voulons savoir ce que ce dernier - en l'occurrence le noyau - "pense" du périphérique en question, nous devons utiliser la commande suivante :

```
$ dmesg | grep -i network
```

```
1.647914] drop_monitor: Initializing network drop monitor service
2.029769] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-
NAPI
2.643774] e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network
Connection
```

Le résultat de cette dernière commande nous montre que, apparemment, le kernel reconnaît La carte Ethernet. Dans le cas contraire, nous aurions eu droit à un message d'erreur de ce genre :

eth0: unknown interface: not such device

Ce n'est pas le cas (heureusement) et nous savons que le kernel est capable de gérer le matériel avec le module **e1000**. Il est peut-être utile de s'attarder un moment sur cette notion de "module".



Premier pas sur le réseau

A partir du moment où vous connectez deux ou plusieurs ordinateurs et où vous envoyez des données d'une machine à l'autre, vous fonctionnez en réseau.

La communication est un besoin essentiel pour l'être humain, au même titre que respirer, boire et manger. De nos jours, on peut filer la métaphore et légitimement considérer que la communication avec d'autres machines fait partie du minimum syndical que l'on peut exiger d'un ordinateur, à plus forte raison lorsqu'il d'un serveur. Le hic, c'est que la communication entre les ordinateurs est une chose très complexe, probablement autant que celle entre les humains. Ça parle plusieurs langues , ça utilise des patois différents, ça créer des malentendus, ça entend de travers, ça monopolise le discours, c'est sourd comme un pot et parfois stupide comme un pot.

Là encore, il existe une série d'ouvrages sur le sujet, toute la gamme allant de "pour les nuls" à "pour les pros". En règle générale, ils comprennent une histoire exhaustive des réseaux depuis la guerre froide et **ARPANET**, suivie d'une introduction détaillée à l'algèbre binaire, octal et hexadécimale. Vous feuilletez ces livres de plus en plus vite, puis vous les reposez en vous sentant progressivement envahi par une vague nausée existentielle.

MAC ? ARP ? IP ? TCP ? UDP ? DHCP ? DNS ? NTP ? HTTP ? FTP ?

Comment vous en sortir ?

Je prends donc le partie de vous initier aux réseaux et à leur fonctionnement par une approche résolument pratique, en mettant la main à la pâte, avec un minimum de théorie. Nous avancerons par étapes successives, en partant du cas de figure le plus simple. Puis, peu à peu, lorsque vous aurez digéré les notions de base, je vous présenterai des configurations un peu plus sophistiquées, quitte à rectifier le tir et reprendre les simplifications abusives dont je me serai rendu coupable.



Gérer les archives compressées

Les différents formats d'archivage

Les archives compressées sont omniprésent dans le quotidien informatique et elle sont utilisées à des fins très variées. A titre d'exemple, lorsque vous souhaitez envoyer vos photos de vacances par courrier électronique, il sera bien plus commode d'envoyer une archive plutôt que d'ajouter chaque photo individuellement en pièce jointe. Étant donné que, de nos jours, la taille moyenne des photos - c'est-à-dire leur poids en mégaoctets - est assez importante, vous utiliserez plutôt un service de transfert de fichiers en ligne et, dans certains cas, la confection préalable d'une archive sera obligatoire. Une archive compressée représente également le format idéal pour effectuer une sauvegarde de vos données. Enfin, l'utilisation de fichiers compressées pour le transfert sur Internet vous fait économiser de la bande passante. Si vous avez l'habitude de Windows, vous avez certainement déjà croisé des fichiers **.zip** et **.rar** sur votre disque. Ces types de fichiers ne sont pas inconnus à Linux, mais les deux formats d'archives compressées les plus largement répandus sous ce système sont les fichiers **.tar.gz** et **.tar.bz2**. Derrière ces extensions, quelque peu énigmatique pour un néophyte, se cachent en réalité trois programmes, trois petits outils. **tar**

rassemble plusieurs fichiers et répertoires en une archive, **gzip** et **bzip2** se chargent de la compression.

Ces formats sont très bien géré par les différents systèmes d'exploitation. Linux sait gérer les archives au format **.zip** et **.rar** grâce aux outils **unzip** et **unrar**.

Compresser et décompresser un fichier avec gzip

gzip (GNU Zip) constitue l'outil de compression standard sous Linux. Il fait une chose et une seule : gérer la compression de fichiers simples. Il ne sait pas constituer des archives, c'est **tar** qui s'en charge. Cherchons dans notre système un fichier au hasard, sur lequel nous pourrions nous entraîner :

```
$ cp /etc/services .
```

```
$ ls -lh services
```

```
-rw-r--r--. 1 ... 655K 11 déc. 17:38 services
```

L'affichage détailler nous montre qu'il s'agit d'un fichier texte assez important en terme de taille : 655 kilo-octets. C'est pour cela que je l'ai choisi. Essayons de le compacter :

```
$ gzip services
```

gzip remplace le fichier d'origine par une version plus compacte, comportant l'extension de fichier supplémentaire **.gzip** :

```
$ ls -lh services.gz
```

```
-rw-r--r--. 1 ... 133K 11 déc. 17:38 services.gz
```

Dans cet exemple, la compression est assez conséquente : le fichier résultant est environ cinq fois plus petit que l'original.

Quel type de fichiers compresser avec gzip ?

La compression varie selon un certain nombre de facteurs .gzip n'aura pas beaucoup d'effet sur des formats de fichiers comportant une compression initiale, comme le MP3 ou le JPEG. En revanche, il fonctionnera très bien avec les fichiers au format texte simple ou les images Bitmap non compressées.

Pour décompresser un fichier .gz, vous avez deux possibilités :

gzip -d services.gz

Ou alors, ce qui revient exactement au même :

gunzip services.gz

Compresser et décompresser un fichier avec bzip2

L'outil **bzip2** est un outil de compression au même titre que gzip, au détail près qu'il utilise un algorithme un peu plus performant.

L'outil **bzip2** ne fait pas partie de notre installation minimale.

\$ sudo yum install bzip2

Reprendons l'exemple précédent, avec le fichier service :

\$ bzip2 services

Il en résulte un fichier compressé pourtant l'extension de fichier supplémentaire **.bzip2**. Regardons ce fichier de plus près :

ls -lh services.bz2

-rw-r--r--. 1 ... 122K 11 déc. 17:38 services.bz2

Effectivement, le taux de compression est légèrement supérieur à celui proposé par gzip. Le fichier compressé ne pèse plus que 122 kilo-octets, contre 133 avec gzip.

Pour décompresser un fichier compacté à l'aide de bzip2, nous avons également le choix entre deux commandes, qui ont exactement le même effet :

\$ bzip2 -d services.bz2

Ou alors :

\$ bunzip2 services.bz2

Manipuler les archives avec tar

Créer une archive avec tar

gzip et **bzip2** ne gèrent que la compression d'un seul fichier fourni en argument. Pour créer une archive, nous aurons recours à la commande **tar**. Là aussi, un exemple pratique nous aidera à comprendre le fonctionnement de l'outil en question.

Pour commencer, il nous faut un répertoire contenant quelques fichiers. Je crée donc, au hasard, un répertoire **~/config** et j'y place tous les fichiers ***.conf** que je trouve dans l'arborescence de **/etc** en faisant **find .** des avertissements relatifs aux droits d'accès. Notez que la barre, antislash après la commande **find** indique un passage à la ligne, étant donné que la commande ne tient pas en une seule ligne.

```
$ mkdir config
```

```
find /etc/ -name '*.conf' 2> /dev/null \
-exec cp {} ~/config/ \;
```

```
$ ls config/
```

Nous allons rassembler tous ces fichiers contenus dans **~/config** pour en constituer une archive avec la commande **tar** :

```
$ tar cvf config.tar config/
```

Le nom du programme (tape archiver) révèle son utilisation initiale : tar a servi en premier lieu à la gestion d'archives sur bande magnétique. Voici une petite explication de l'exemple que nous venons de voir :

- tar reçoit l'ordre de créer (create) une archive avec l'option **-c** ;
- la commande nous dit ce qui se passe en coulisse avec l'option **-v** ;
- le premier argument (**config.tar**) sera interprété comme le nom de l'archive grâce à l'option **-f** (file).

Voici un exemple plus générale pour vous familiariser avec la syntaxe de tar pour la création d'une archive. Nous créons trois fichiers **fichier1**, **fichier2** et **fichier3** et les rassemblons dans un fichier **archive.tar** :

```
$ touch fichier{1,2,3}
```

```
$ tar -cvf archive.tar fichier1 fichier2 fichier3
```

Extraire les fichiers d'une archive

Avant de "déballer" notre archive, nous allons le déplacer dans un répertoire nouvellement créé. En effet, étant donné que les fichiers d'origine sont toujours en place, une extraction dans le même répertoire ne changerait rien et écraserait tous les fichiers existants.

```
$ mkdir Repertoire
```

```
$ mv config.tar Repertoire/
```

```
$ cd Repertoire/
```

```
$ tar -xvf config.tar
```

Dans l'autre sens, c'est donc l'option **-x** (extract) qui procède au dépaquetage de l'archive.

Combiner l'archivage et la compression

Essayons de créer une archive compressée en reprenant l'exemple du début. Nous pouvons très bien :

- créer l'archive avec tar ;
- compresser l'archive avec gzip ou bzip2.

tar comporte une série d'options qui servent à créer une archive et la compresser à la volée :

```
$ tar -cvjf config.tar.bz2 config/
```

```
$ tar -cvzf config.tar.gz config
```

Notez la différence de taille entre les deux archives :

```
$ ls -lh config.tar*
```

Extraire une archive compressée

Inversement, l'extraction d'une archive compressé peut également s'effectuer d'une traite :

- pour une archive .tar.gz :

```
$ tar -xvzf config.tar.gz
```

- et pour une archice .tar.bz2 :

```
$ tar -xvjf config.tar.bz2
```



Les pilotes sous Linux

Un module, ce n'est rien d'autre que ce que vous connaissez peut-être par ailleurs sous le nom de pilote (driver, en anglais), c'est-à-dire un bout de code qui permet au système d'exploitation de communiquer avec le matériel et dont de la gérer. Sur un système Linux, la commande **lsmod** sert à afficher le statut des modules.

\$ lsmod

Filtrons ce résultat il trop long :

\$ lsmod | grep e1000

Les modules se trouvent dans **/lib/modules**, dans le répertoire correspondant à la version du noyau en cours. Concrètement, le pilote de notre carte se trouve donc dans l'arborescence **/lib/modules/3.10.0-957.e17.x86_64**, dans le sous-répertoire **kernel/drivers/net/ethernet/intel/e1000**, et c'est le fichier **e1000.ko.xz**. L'extension **.ko** signifie **kernel object** et **.xz** nous indique qu'il s'agit d'un **fichier compressé**. C'est précisément ce fichier qui est chargé par le noyau pour gérer une carte Ethernet équipée d'une puce Intel 82574L.



Créer et manipuler des liens

Jusqu'ici notre prise en main du système Linux consistait essentiellement à manipuler des fichiers et des répertoires. A l'occasion des nos travaux pratiques, peut-être avez-vous remarqué ici ou là, la présence de fichiers mystérieux qui ne semblent tomber ni dans l'une ni dans l'autre de ces deux catégories.

Créer des liens symboliques

Le meilleur moyen de maîtriser un nouvel objet, c'est de faire comme les enfants : jouer avec. Dans votre répertoire d'utilisateur, créez un répertoire **Test_Liens**, placez-vous dedans, puis créez un fichier **texte.txt** avec un peu de contenu. Maintenant, créons un lien symbolique vers ce fichier :

ln -s texte.txt lien.txt

Voyons le résultat :

```
[javier@linuxserver Test_Liens]$ ls -l
lrwxrwxrwx. 1 javier javier 9 4 déc. 14:45 lien.txt -> texte.txt
-rw-rw-r--. 1 javier javier 18 4 déc. 14:43 texte.txt
```

Arrêtons-nous là et essayons d'établir un état des lieux sommaire :

- les permissions **rwxrwxrwx** semblent pour le moins insolites ;
- les deux fichiers n'ont pas la même taille : 8 octets pour l'un et 18 octets pour l'autre ;
- dans la console, **lien.txt** apparaît en noir sur fond noir, mais en turquoise.

Nous pouvons déjà expliquer les différences de taille. Le fichier **texte.txt** comprends en gros 18 caractères, si l'on additionne y compris les retours chariot. Quant à **lien.txt**, il pointe vers "**texte.txt**", c'est-à-dire vers un nom de fichier comptant exactement 9 caractères.

Ajoutez du contenu dans le fichier **lien.txt** et regardons à nouveau le résultat détaillé :

```
lrwxrwxrwx. 1 javier javier 9 4 déc. 14:45 lien.txt -> texte.txt
-rw-rw-r--. 1 javier javier 538 4 déc. 15:15 texte.txt
```

Nous constatons que, depuis que nous avons ajouté du texte à **lien.txt**, la taille de ce dernier n'a pas changé. En revanche, c'est bien **texte.txt** qui compte désormais 538 au lieu de 18 octets.

A quoi servent les liens symboliques ?

Les liens symboliques sont omniprésents sur un système Linux. Notre installation minimale en compte déjà plus de 9 000 :

```
find / -type l 2> /dev/null | wc -l
```

La commande **wc (word count)** sert à compter les octets, les mots ou les lignes d'un fichier. Avec l'option **-l**, elle affiche le nombre de sauts de ligne.



Gestion des utilisateurs

Tout comme Unix, Linux a été conçu dès le départ comme un vrai système multi-utilisateur. Gérer les utilisateurs revient à définir qui a accès à quoi dans un système Linux.

Systèmes mono-utilisateurs et systèmes multi-utilisateurs

Linux est un vrai système multi-utilisateur, tout comme son ancêtre Unix. Pour comprendre la portée de cette assertion, imaginez un poste de travail comme on peut en trouver dans la salle d'informatique d'une grande université, fréquentée par une bonne dizaine de milliers d'étudiants. Chaque étudiant inscrit a le droit d'utiliser les machines de la salle informatique. Il possède donc son identifiant personnel et son mot de passe, qui lui permettent de se connecter à une machine pour y travailler, c'est-à-dire

effectuer ses recherches, écrire ses devoirs, rédiger son mémoire ou sa thèse, etc. Une telle installation doit répondre à quelques exigences.

- Chaque utilisateur du système doit disposer de son répertoire personnel, c'est-à-dire d'un endroit pour lui seul, utilisable par lui seul, où il peut stocker toutes ses données.
- La confidentialité doit être assurée, c'est-à-dire qu'un étudiant connecté ne pourra pas aller fouiner librement dans les données de ses collègues.
- Il ne faut pas non plus qu'un utilisateur puisse effacer par mégarde (même intentionnellement) les données qui ne lui appartiennent pas.
- Enfin, l'intégrité du système ne doit en aucun cas être mise en péril par les utilisateurs.

Si l'importance de ces points ne vous apparaît pas dans toute son ampleur, imaginez dans un tel contexte un système mono-utilisateur.

- Les données de tous les utilisateurs c'est-à-dire quelques dizaines voire centaines de milliers de fichiers, seraient stockées en vrac dans une seule arborescence.
- Chaque étudiant pourrait lire les données de ses collègues.
- Il pourrait les modifier et/ou les effacer comme bon lui semble.
- Chaque utilisateur serait libre de compromettre l'intégrité du système.

Sécurité alerte au virus belge

En mai 2001, une alerte au virus un peu spéciale a fait le tour du monde. Les utilisateurs de systèmes Microsoft Windows étaient mis en garde contre un fichier mal intentionné **SULFNBK.EXE** éventuellement présent sur leur système. L'alerte par courrier indiquant l'emplacement du fichier en question, en précisant qu'il suffisait d'effacer le fichier pour le mettre hors d'état de nuire. Le problème c'est que **SULFNBK.EXE** n'a pas été un virus, mais un fichier système de Windows. Cette alerte au virus a constitué la première occurrence de ce que les administrateurs ont baptisé plus tard

"virus belge" (parfois aussi "virus albanais") : son déploiement ne nécessite aucun effort de développement de la part des instigateurs, étant donné que les victimes se chargent elles-même de se tirer dans le pied, ce qu'elle ont tout loisir de faire sur un tel système.

Notre configuration de test sera beaucoup plus modeste qu'une série de posts de travail dans la salle d'informatique d'une université ; il n'empêche que l'approche multi-utilisateur est tout aussi pertinente, même pour un usage sur une machine locale. Après tout, peu importe si le système gère deux ou trois utilisateurs ou vingt-cinq mille.

Réseau profils itinérants

Techniquement parlant, une telle installation dans une université se différencie d'une installation domestique d'un poste de travail par la configuration *itinérante* des profiles utilisateurs. Dans une telle configuration, l'ensemble des données, les identifiant de connexion et les mots de passe sont stockés de façon centralisée sur le serveur.

A partir de là, chaque étudiant peut se connecter sur n'importe quelle machine de la salle d'informatique et retrouve son environnement, alors que, sur une installation comme un poste de travail domestique, chaque compte d'utilisateur reste lié à la machine locale. Il existe plusieurs manières de mettre en place les profils itinérants dans un réseau local lié à la machine local et nous les aborderons en temps et en heure. Pour l'instant, nous nous concentrerons sur la gestion locale des utilisateurs sur une seule machine tournant sous Linux.

Ajouter de nouveaux utilisateurs : useradd

Lors de la configuration post-installation, j'ai défini un premier utilisateur du "commun des mortels" pour mon système. Cela signifie que ma machine connaît deux comptes :

- l'administrateur **root** ;
- l'utilisateur en question (javier).

Créons quelques comptes supplémentaires :

- Diego Perez Mota (dperezmota) ;
- Leyli Perez (lperezmota) ;
- Fanny Banester (fbanester) ;
- Melissa Turpin (mturpin).

Chacun d'eux sera créé à l'aide de la commande **useradd**. L'invocation de cette commande requiert des droits administrateur. Dans un premier temps, nous allons acquérir ces droits de façon peu élégante, en mode en nous nous déconnectant et nous reconnectant en tant que **root**.

Je lance la création de mon premier utilisateur :

```
useradd -c "Diego Perez Mota" dperezmota  
passwd dperezmota
```

Pour supprimer un utilisateur on utilise la commande suivante : **userdel -r nom_utilisateur**.

Gérer les droits d'accès

Chaque employé possède son badge qui lui donne accès aux locaux de l'entreprise. Il a son bureau où il range ses affaires, éventuellement aussi son casier personnel. En principe, les employés partagent les ressources de l'entreprise, ce qui ne veut pas forcément dire que tous les employés ont accès aux même ressources. Beaucoup disposent de leur propre bureau individuel, d'autres travaillent en équipe dans de grandes pièces spacieuses, où l'accès aux ordinateurs, aux photocopieuses et aux documents est ouvert à tous les membres de l'équipe. Quelques rares privilégiés ont accès plus large : l'agent de sécurité, le PDG ou le DRH. La métaphore peut ainsi être tressée et affiné, mais vous avez compris le principe sous-jacent.

Considérons l'exemple suivant. Le système compte trois utilisateurs, chaque utilisateur dispose de son propre répertoire (-) : **ls /home**. Chacun va ranger ses données personnelles dans son répertoire utilisateur. Dans l'exemple, chacun disposera d'un document "confidentiel" confectionné comme suit par exemple : **mkdir Documents**.

Qui a accès à quoi là-dedans ? Est-ce que un utilisateur pourra lire le fichier **confidentiel.txt** d'un autre utilisateur ? Est-ce que celle-ci pourra modifier le fichier **confidentiel.txt** de un autre utilisateur ? En effet, il ne suffit pas que chaque utilisateur dispose de son propre répertoire au-dessous de **/home**. Aussi faut-il que ses données soient à l'abri des autres utilisateurs de la machine. Le but du jeu et que tout ce petit monde puisse se connecter à la machine. Le présent chapitre se propose de répondre de façon détaillé à toutes ces questions.

Un exemple pratique

Les nouveaux utilisateurs de Linux sont souvent intimidés par les questions de permissions et de droits d'accès, qu'ils perçoivent comme une nébuleuse complexe et impressionnante. Ici comme ailleurs, je vous propose de rester fidèle à la devise du grand neurologue français Charcot : "La théorie, c'est bon, mais ça n'empêche pas d'exister".

Pour commencer, créez un fichier **droits.txt** dans votre répertoire utilisateur.

```
cat > droits.txt << EOF
echo "Voici la date"
date
EOF
```

Comprendre les permissions dans l'affichage détaillé

Vous voilà donc avec votre fichier **droits.txt**. Qui est le propriétaire ? Qui peut faire quoi avec ? D'ailleurs, qu'est-ce qu'on peut bien faire avec un fichier ? En lire le contenu ? Le modifier ? L'effacer ? Et puis quoi encore ?

ls -l droits.txt

Dans la partie de droite de cet affichage détaillé, vous avez :

- **le nom du fichier**
-
- **sa date de création**
-
- **sa taille**

La partie gauche est réservée aux droits accès du fichier.

Rendre un fichier exécutable

Peut-être vous en êtes-vous déjà vaguement douté, mais notre fichier droits.txt contient du code exécutable. C'est un programme, eh oui ! Un script, plus exactement. Alors comment l'exécuter ?

Dans un premier temps nous allons définir des droits d'exécution pour le propriétaire du fichier :

chmod u+x droits.txt

ls -l droits.txt

Les droits concernant le propriétaire sont passés de **rw-** à **rwx**, qui signifie : "L'utilisateur javier a le droit de lire ce fichier, le modifier ou l'effacer, mais aussi de l'exécuter" Et c'est ce que nous allons faire :

./droits.txt

A la différence de **Windows**, la possibilité d'exécuter un fichier n'est aucunement liée à un quelconque suffixe comme **.EXE ou .COM**, sous Linux, cette caractéristique est essentiellement liée au système de droits d'accès.

Vous voyez que les membres du groupe javier ont le droit de lire et de modifier ce fichier(rw-) et que tous les autres ont seulement le droit de lire(r---). Comment empêcher complètement ces derniers d'accéder à mon fichier ? Tout simplement avec la commande : **chmod go-rw droits.txt**.

Effectivement, les classes d'utilisateurs group(g) et others(o) n'ont plus le droit de rien faire, comme le montre le -----final. Un système Linux permet d'attribuer des droits d'accès aux fichiers avec une précision quasi chirurgicale.

Ajouter et retirer les droits de lecture et d'écriture

Donnons maintenant le droit à tout le monde (**a** comme **all**) de lire le fichier.

chmod a+r droits.txt

ls -l droits.txt

Ici, les trois classes d'utilisateurs (user, group et others) obtiennent des droits de lecture. De façon analogue, pour retirer les droits de lecture au groups et aux autres, il suffit d'invoquer la commande suivante :

chmod go-r droits.txt

La méthode directive

Dans les exemples jusqu'ici, nous avons vu deux approches dans la définition de droits :

- une méthode additive, qui ajoute des droits à certaines catégories d'utilisateurs ;
- une méthode soustractive, qui retire des droits à certaines catégories d'utilisateurs.

En dehors de ces deux approches, la méthode directive définit des droits très précis pour chaque classe d'utilisateurs. Ainsi, la commande suivante donne tous les droits au seul propriétaire :

chmod u=rwx,g=o= droits.txt

Et si je veux rétablir les permissions initiales de mon fichier en utilisant la méthode directive, voici comme je dois m'y prendre :

chmod u=rw,g=rw,o=r droits.txt

Les permissions par défaut : umask

Vous vous êtes peut-être demandé d'où viennent les droits initiaux des fichiers. Créons un fichier :

touch droits2.txt

ls -l droits2.txt

Je vois que droits2.txt est créé d'emblée avec une structure rw-rw-r--. Qui ou quoi décide des permissions pour les fichiers nouvellement créé ? Il faut savoir que, sur un système Linux, il n'est pas possible de créer un fichier qui possède d'emblée les droits d'exécution. Cela signifie que les permissions maximale que je peux obtenir pour un fichier nouvellement créé, c'est -rw-rw-, autrement dit 666.

Or, si je regarde de plus près mon fichier droits2.txt, il est affublé d'une structure de droits rw-rw-r--, c'est-à-dire 664 en notation numérique. Si je pars du principe que mes droits plénier s'élèvent à 666 et que je dispose de 664, j'en conclus maussadement que je me suis fait gruger de 002 au passage. Le responsable de cette restriction se nom **umask**. Le seul rôle de ce réglage est de soustraire des droits de la création de fichiers.

**umask
002**

Il est toute fois possible de le changer :

umask 0022

La conséquence de cette redéfinition est immédiate. En effet, lorsque je crée un nouveau fichier avec un umask de 002 ses droits par défaut sont désormais de 664 :

**touch droits3.txt
ls -lI droits3.txt**

Maintenant, soyons carrément permissifs :

**umask 0000
touch droits4.txt
ls -lI droits3.txt**

Le fichier droits3.txt a les droits en lecture et écriture pour tout le monde, ce qui est le maximum possible à la création.

La valeur umask est redéfinie à chaque fois que vous vous connectez à la machine.

Gérer les droits d'accès aux répertoires

Depuis le début de cette section, nous avons essentiellement manipulé des fichiers. Qu'en est-il des répertoires ? Eh bien, voyons par nous-mêmes...

Avant de faire quoi que ce soit, assurez-vous de ne pas être en root et de redéfinir votre umask d'utilisateur à 0002.

Maintenant, créez un dossier Test :

```
mkdir Test  
ls -ld Test/
```

Tiens ! Contrairement à ce que j'ai pu énoncer plus haut, les droits d'exécution sont bel et bien définis d'emblée. Non content de cela, ils sont définis pour tout le monde !

L'explication pour cette anomalie apparente est simple, car les droits d'exécution n'ont pas la même signification pour un répertoire que pour un fichier. A y regarder de près, c'est même normal, car cela n'a pas de sens de vouloir "exécuter un répertoire". Le x ici signifie simplement qu'on a le droit de se placer dans le répertoire avec la commande cd et d'en afficher le contenu.

Faisons la preuve par l'exemple pour nous en assurer. Dans le répertoire Test, créons trois fichiers : **fichier1**, **fichier2**, **fichier3**, puis revenons au point de départ :

```
cd Test/  
touch fichier{1,2,3}  
ls -l
```

Maintenant, retirons les droits d'exécution au répertoire, pour tout le monde tant que nous y sommes. Nous avons donc le choix :

```
chmod a-x Test
```

Ou, en utilisant la notation numérique :

```
chmod 664 Test
```

Dans un cas comme dans l'autre, voici ce que nous obtenons :

ls -l Test

Voyons ce que cette dernière opération a eu comme incidence sur l'accès au répertoire :

cd Test

Dans ce cas, pouvons-nous au moins en afficher le contenu de l'extérieur ? L'entrée est bloquée, mais essayons de nous hisser sur la pointe des pieds et de jeter un oeil curieux par-dessus le mur. Est-ce que nous voyons quelque chose ?

ls -l Test

Oui, mais non. Pas vraiment. Tout ce que nous devinons, c'est que ce répertoire contient trois fichiers. Quant à obtenir des informations détaillé, il n'en est pas question.



Principe de fonctionnement des réseaux

Afficher la configuration des interfaces réseau

Après avoir vérifier que mes cartes Ethernet sont gérées, j'invoque la commande suivante :

ip addr

Invoquée sans argument, la commande **ip addr** affiche la configuration des interface réseau. Le résultat de la commande se décompose en trois sections dans notre exemple : **lo**, **enp7s4** et **enp0s3**. La partie **lo** (comme localhost) désigne la boucle locale, une interface qui représente approximativement le journal intime de votre machine et qui lui permet de soliloquer. Les interfaces qui nous intéressent plus particulièrement sont tout ce qui n'est pas **lo**. Essayons de lire les informations qui nous concernent.

```
$ ip address show enp0s3
```

L'adresse MAC de votre carte

La ligne **link/ether 08:00:27:44:ce:** identifie la carte réseau d'un point de vue purement matériel. Il s'agit d'une série de six chiffres hexadécimaux séparé par des symboles deux points qui constitue l'empreinte digitale de votre carte Ethernet, en quelque sorte. Cette empreinte ou adresse MAC (Media Acces Control).

L'adresse IP et le réseau

L'adresse IP **inet 172.18.241.16/24** caractérise ma machine dans le réseau. Autrement dit, **172.18.241.16** est l'adresse IP de mon ordinateur dans le réseau local **172.18.241.16/24**.

Le **/24** signifie ici que mon réseau peut disposer d'un maximum de 254 hôtes distincts. Vous vous demandez probablement comment j'en viens à cette conclusion. Dans le cas présent, je retire 24 de 32, j'obtiens 8, puis j'effectue l'opération $2^{32-24} = 256$. Gardez cette formule magique dans un coin de la tête, nous y reviendrons un peu plus loin.

Normalement chaque ordinateur dans un réseau possède une adresse IP, une série de quatre nombres a.b.c.d: a et d sont compris entre 1 et 254, b et c peuvent prendre toutes les valeurs comprises entre 0 et 255. Tentez l'expérience : lancez ip addr sur votre machine pour noter votre adresse IP et votre réseau. Théoriquement, tous les ordinateurs de la terre se répartissent donc des adresses IP allant de 1.0.0.1 à 254.255.255.254. J'ai bien dit théoriquement.

IPv4 et IPv6

Vous vous demandez peut-être ce que signifie **inet6 fe80::9d65:a09e:866c:6b77/64**. Il s'agit là tout simplement d'un nouveau protocole d'adressage IP, dans la mesure où un protocole réseau mis au point vers la fin des années 1990 peut être qualifié de "nouveau". Les adresses IP que nous traitons dans ce module font partie du protocole IPv4 à 32 bits : grosso modo, quatre nombres de 0 à 255 (en notation décimal), séparées par des points. Le hic avec ce protocole, c'est que le nombre d'adresses distinctes possibles et non seulement limité, mais véritablement

épuisé dans certains pays. Les adresses IP existantes y ont effectivement toutes été attribuées.

IPv6 constitue le remède à cette pénurie d'adresses. C'est un protocole à 128 bits ; le nombre d'adresses possibles passe donc de 2^{32} à 2^{128} . En contrepartie, les adresses IP du futur ressembleront à quelque chose du genre **fe80::ebc5:8c3:26c4:1413**.

Les adresses IP

Un peu de pratique ; voici une petite expérience amusante pour illustrer la notion d'adresse IP. Prenons au hasard un nom de site web suffisamment connu, par exemple www.google.fr. Ouvrons un terminal et invoquons la commande suivante :

host www.google.fr

La commande host fait partie du paquet bind-utils.

\$ sudo yum install bind-utils.

La commande me retourne deux réponses : une adresse IPv4 et une IPv6 dont je ne me préoccupe pas. Maintenant, ouvrez un navigateur web sur votre poste de travail, effacez le contenu de la barre d'adresse et mettez-y :

<http://142.250.179.227>. Que constatez-vous ?

Retenez de faire la même chose avec un autre site web.



Peaufiner l'affichage des adresses IP

L'outil ip dispose de toute une série d'options d'affichage, que nous allons explorer ici. Revenons à la commande **ip addr show** :

```
$ ip addr show
```

nous avons vu que l'option -family inet nous limite à l'affichage de l'adresse IPv4 :

```
$ ip -family inet addr show enp0s3
```

L'option -color met de la couleur dans l'affichage du résultat et le rend beaucoup plus lisible :

```
$ ip -color -family inet addr show enp0s3
```

Enfin, l'option -oneline rassemble toutes les informations en une seule ligne :

```
$ ip -color -oneline -family inet addr show enp0s3
```

Jusqu'ici, j'ai fait exprès de détailler les options longues car elles sont plus parlantes. Jetez un oeil dans la page manuel de la commande ip ; vous verrez que chaque option comprend également une version courte. La dernière commande aurait donc pu être invoquée comme ceci :

```
$ ip -c -o -4 a s enp0s3
```

Établir un contact avec une machine distante : ping

Retenons le fait que les machines d'un même réseau sont capables de communiquer entre elles.

Pour l'instant, notre réseau ne comporte que deux machines, si l'on peut dire : le serveur Linux et le routeur. En effet, le routeur est aussi une machine (ou un hôte), même s'il n'est doté ni d'un clavier ni d'un écran. Il contient un petit système d'exploitation embarqué (Linux, eh oui !) et il s'acquitte des quelques tâches simples pour lesquelles il est construit. Normalement, un routeur est livré avec une adresse IP fixe préconfigurée par défaut, indiquée sur la petite note explicative qui l'accompagne. A titre d'exemple, les Livebox de chez Orange sont souvent préconfigurées avec une adresse 192.168.1.1, le routeur Netgear livré par Nerim a une adresse IP par défaut 192.168.0.1. Voyons voir si j'arrive à établir une liaison avec le routeur. Pour cela j'utilise la commande ping, qui dit en quelque sorte "Allô, il y a quelqu'un ?" :

```
$ ping -c 4 192.168.0.1
```

Le routeur à répondu !

Le routeur : un centre de tri pour paquets numériques

Je viens d'insister sur le fait que les machines d'un même réseau peuvent communiquer entre elles. Dans ce cas, comment se fait-il qu'on puisse communiquer, par exemple, avec la machine 172.217.22.131 (en affichant la page d'accueil de Google stocké sur la machine en question), alors que celle-ci ne fait manifestement pas partie de notre réseau 192.168.1.244/24 ?

Réponse : parce que nous passons par le routeur. Ce dernier est défini en tant que passerelle (gateway), qui sert à faire communiquer votre machine avec le monde extérieur. L'information que vous envoyez ou que vous

reçoivent transite sur le réseau sous forme de paquets. Si une passerelle est définie, tous les paquets qui ne concernent pas le réseau local sont envoyés par cette porte vers le monde extérieur. La commande ip route show indique si la passerelle est définie correctement :

\$ ip route show

Sous les pavé numériques, la plage d'adresse IP privées

La commande ip addr vous a retourné votre adresse IP sous la forme inet 192.168.1.244/24. Même si le nom suggère, cette adresse n'est pas normalement "joignable" à partie d'Internet. Elle fait partie de la plage standardisée d'adresses IP privées réservées aux réseaux locaux privés :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

Bien sûr, la solution la plus simple consisterait à utiliser une adresse publique. Le hic, c'est que vous devez acheter celle-ci chez un fournisseur d'accès. Un abonnement à Internet vous fournit en général une seule adresse publique pour vous rattacher au monde extérieur. C'est largement suffisant si vous n'utilisez qu'une seule machine. Pour configurer votre réseau domestique, il vous faudrait acheter un bloc d'adresses entier, ce qui revient très cher, mais rassurez-vous, il existe une solution au problème.

Relier le public et le privé

Un routeur est un hôte un peu spécial, qui assure la communication entre deux réseaux. Il fait transiter les paquets d'un réseau à un autre. Dans les réseaux domestiques, c'est le plus souvent le modem routeur ADSL qui assume ce rôle. Dans le réseau local d'une TPE ou d'une PME c'est souvent une machine un peu spéciale, un serveur équipé d'au moins deux cartes réseau, qui fait office de passerelle vers le monde extérieur. Dans un cas comme dans l'autre, à partir du moment où nous avons un réseau local avec

plusieurs machines, tous les hôtes du réseau utilisent cette passerelle pour communiquer avec les machines en dehors du réseau.

Sans trop entrer dans les détails, l'astuce du routeur consiste à manipuler les paquets qu'il fait transiter. Côté Internet, le routeur dispose d'une adresse publique. Il se fait donc passer lui-même pour l'expéditeur de chaque paquet qu'il envoie sur Internet. La procédure s'inverse pour les paquets entrants : la passerelle remplace l'adresse de destination par l'adresse IP privée de la machine qui attend une réponse d'Internet.

A retenir : s'il ne fallait que cela ; dans un réseau local privé, la passerelle vous permet de communiquer avec Internet.

Le système de noms de domaine : l'annuaire d'Internet

Maintenant, comment s'y retrouver dans toute cette jungle d'adresses IP ? Est-ce qu'il faut se constituer un agenda, comme dans le bon vieux temps où les téléphones avaient juste un cadran et rien d'autre ? Eh non, ce n'est pas nécessaire grâce à DNS, le système de noms de domaines (Domain Name System). Les humains savent passablement mémoriser et gérer des noms comme www.google.fr. Le système de noms de domaines nous épargne donc la tâche pénible de devoir mémoriser des adresses comme 172.217.22.131 etc. Vous pouvez d'ailleurs filer la métaphore avec les numéros de téléphone en considérant DNS comme un service d'annuaire global.

Les serveurs DNS (qu'on appelle aussi "serveur de noms") sont organisées de façon hiérarchique. Lorsqu'un serveur n'arrive pas à résoudre un certain nom, c'est-à-dire à fournir une adresse IP correspondante, il envoie à son tour une requête au prochain serveur dans la hiérarchie et ainsi de suite. Chaque client doit donc connaître au moins un serveur DNS pour ensuite se faufiler dans cette hiérarchie.

Lorsque nous avons invoqué la commande host, nous avons fait exactement cela : nous avons envoyé une requête à un serveur de noms en lui fournissant un nom de domaine et il nous a gracieusement retourné une adresse IP.

Configurer une connexion à Internet

Tentons un petit récapitulatif. Quel est le minimum syndicale dont nous avons besoin pour configurer une connexion à Internet ? Ici, je vais partir sur le principe que le matériel est correctement géré par le système :

- **une adresse IP**
- **un masque de sous-réseau pour la machine**
- **l'adresse IP de la passerelle**
- **au moins une adresse IP de serveur DNS**

C'est tout. Ces quatre conditions suffisent pour vous connecter à Internet.

Dans notre exemple , nous n'avons pas vraiment configurer quoi que ce soit. Nous nous sommes contentés d'afficher les détails de la configuration. D'où viennent donc ces données ?

Un PEU DE MAGIE Configuration autonome

Il y a quelques années, un vendeur de matériel informatique local à qui je demandais des détails sur la configuration d'un de ses réseaux sur lequel je devais intervenir m'a expliqué que ses machines étaient sous Windows et qu'elles se configuraient " elles-mêmes, comme ça, toutes seules, au démarrage, c'est automatique, vous voyez ? " Notre système Linux serait-il doté du même pouvoir de configuration auto-magique que les systèmes Windows ?

Configuration dynamique DHCP

La réponse à notre question est simple et elle s'appelle DHCP (Dynamic Host Configuration Protocol). Ce sigle désigne le protocole d'allocation dynamique d'adresses IP.

Dans la configuration par défaut de CentOS, les messages de démarrage du système sont remplacés par une simple barre de progression horizontale en bas de l'écran. Lorsqu'on appuie sur la touche [Echap] pour les faire

apparaître, ils défilent à une tel allure qu'on n'a pas vraiment le temps de les lire.

Si nous voulons en savoir un peu plus sur ce qui s'est passé lors du dernier démarrage, nous pouvons jeter un oeil dans le fichier **/var/log/messages**. En cherchant un peu, nous tombons sur la partie qui nous intéresse :

```
Dec 20 17:13:55 centos-server NetworkManager[691]: <info>
[1671552835.0376] dhcpc4 (enp0s3): address 192.168.1.244
Dec 20 17:13:55 centos-server NetworkManager[691]: <info>
[1671552835.0377] dhcpc4 (enp0s3): plen 24 (255.255.255.0)
Dec 20 17:13:55 centos-server NetworkManager[691]: <info>
[1671552835.0377] dhcpc4 (enp0s3): gateway 192.168.1.1
Dec 20 17:13:55 centos-server NetworkManager[691]: <info>
[1671552835.0377] dhcpc4 (enp0s3): lease time 86400
Dec 20 17:13:55 centos-server NetworkManager[691]: <info>
[1671552835.0378] dhcpc4 (enp0s3): hostname 'centos-server'
Dec 20 17:13:55 centos-server NetworkManager[691]: <info>
[1671552835.0378] dhcpc4 (enp0s3): nameserver '192.168.1.1'
```

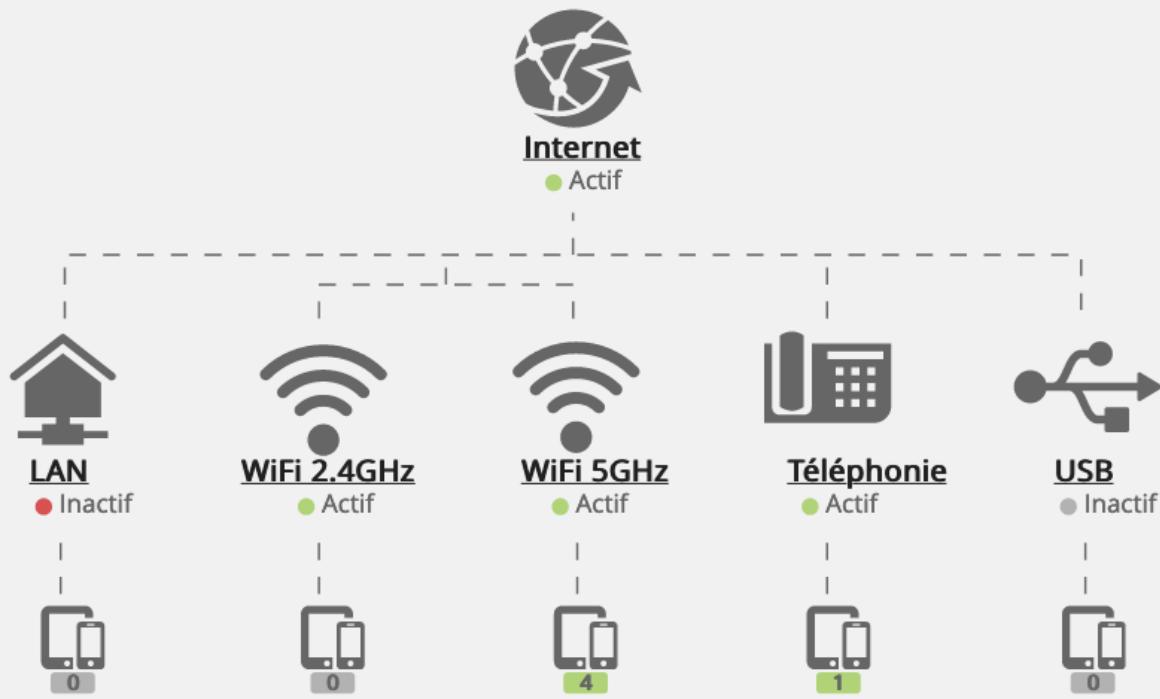
Paramétrer le serveur DHCP intégré dans le modem routeur

Votre modem routeur est un hôte à part entière, dépourvu d'un clavier et d'un écran. Ce genre de petite machine se configure en général par le biais d'une interface web, en ouvrant un navigateur à l'adresse IP de la " boîte noire ".

Page principale

Mon réseau

Cliquez sur les objets pour accéder aux paramètres correspondants.





Principes de sécurité du système d'information

Menaces, risques et vulnérabilités

La Sécurité des Systèmes d'Information (SSI) est une discipline de première importance car le système d'information (SI) est pour toute entreprise un élément absolument vital. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités. Il est possible de préciser la notion de risque en la décrivant comme le produit d'un préjudice par une probabilité d'occurrence :

$$\text{risque} = \text{préjudice} \times \text{probabilité d'occurrence}$$

Cette formule exprime qu'un événement dont la probabilité est assez élevée, par exemple la défaillance d'un disque dur, mais dont il est possible de prévenir le préjudice qu'il peut causer, par des sauvegardes régulières, représente un risque acceptable ; il en va de même pour un événement à la

gravité imparable, comme l'impact d'un météorite de grande taille, mais à la probabilité d'occurrence faible. Il va de soi que, dans le premier cas, le risque ne devient acceptable que si les mesures de prévention contre le préjudice sont effectives et efficaces : cela irait sans dire, si l'oubli de cette condition n'était très fréquent.

Si la question de la sécurité des systèmes d'information a été radicalement bouleversée par l'évolution rapide de l'Internet, elle ne saurait s'y réduire ; il s'agit d'un vaste problème dont les aspects techniques ne sont qu'une partie. Les aspects juridiques, sociaux, ergonomiques, psychologiques et organisationnels sont aussi importants, sans oublier les aspects immobiliers, mais nous commencerons par les aspects techniques liés à l'informatique.

Aspects techniques de la sécurité informatique

Les problèmes techniques actuels de sécurité informatique peuvent, au moins provisoirement, être classés en deux grandes catégories :

- ceux qui concernent la sécurité de l'ordinateur proprement dit, serveur ou poste de travail, de son système d'exploitation et des données qu'il abrite ;
- ceux qui découlent directement ou indirectement de l'essor des réseaux, qui multiplie la quantité et la gravité des menaces.

Si les problèmes de la première catégorie citée ici existent depuis la naissance de l'informatique, il est clair que l'essor des réseaux, puis de l'Internet, en a démultiplié l'impact potentiel en permettant leur combinaison avec ceux de la seconde catégorie.

Définir risques et objets à protéger

Fixer un périmètre de sécurité et élaborer une politique de sécurité

Inutile de se préoccuper de sécurité sans avoir défini ce qui était à protéger : en d'autres termes toute organisation désireuse de protéger ses systèmes et ses réseaux doit déterminer son périmètre de sécurité. Le périmètre de sécurité, au sein de l'univers physique, délimite l'intérieur et l'extérieur, mais

sa définition doit aussi englober (ou pas) les entités immatérielles qui peuplent les ordinateurs et les réseaux, essentiellement les logiciels et en particulier les systèmes d'exploitation. Une fois fixé ce périmètre, il faut aussi élaborer une politique de sécurité, c'est-à-dire décider de ce qui est autorisé et de ce qui est interdit. À cette politique viennent en principe s'ajouter les lois et les règlements en vigueur, qui s'imposent à tous. Nous disons « en principe », parce que l'identification des lois en vigueur est rien moins qu'évidente : en vigueur où ? Les casinos en ligne sont interdits en France, mais autorisés en Grande-Bretagne, or qui peut m'empêcher d'installer mon casino sur un site britannique et d'y attirer les joueurs français ?

Si avec l'aide du service juridique de votre entreprise vous avez réussi à surmonter ces difficultés et à mettre sur pieds une politique de sécurité des systèmes d'information, il vous sera possible de mettre en place les solutions techniques appropriées à la défense du périmètre selon la politique choisie. Mais déjà il est patent que les dispositifs techniques ne pourront pas résoudre tous les problèmes de sécurité, et, de surcroît, la notion même de périmètre de sécurité est aujourd'hui battue en brèche par des phénomènes comme la multiplication des ordinateurs portables et autres objets mobiles informatiques en réseau (iPhones 5G ...) qui, par définition, se déplacent de l'intérieur à l'extérieur et inversement, à quoi s'ajoute l'extraterritorialité de fait des activités sur l'Internet.

Périmètres et frontières

La notion de périmètre de sécurité, devient de plus en plus fragile au fur et à mesure que les frontières entre l'extérieur et l'intérieur de l'entreprise ainsi qu'entre les pays deviennent plus floues et plus poreuses. Interviennent ici des considérations topographiques : les ordinateurs portables entrent et sortent des locaux et des réseaux internes pour aller se faire contaminer à l'extérieur ; mais aussi des considérations logiques : quelles sont les lois et les règles qui peuvent s'appliquer à un serveur hébergé aux États-Unis, qui appartient à une entreprise française et qui sert des clients brésiliens et canadiens ?

La justice et les fournisseurs français d'accès à l'Internet (FAI) en ont fait l'expérience : un certain nombre d'organisations ont déposé devant les tribunaux français des plaintes destinées à faire cesser la propagation de pages Web à contenus négationnistes, effectivement attaquables en droit français. Mais les sites négationnistes étaient installés aux États-Unis, pays dépourvu d'une législation anti-négationniste, ce qui interdisait tout recours contre les auteurs et les éditeurs des pages en question. Les plaignants se sont donc retournés contre les FAI français, par l'intermédiaire desquels les

internautes pouvaient accéder aux pages délictueuses, mais ceux-ci n'en pouvaient pas. En effet, ainsi le filtrage de contenus sur l'Internet est une entreprise coûteuse, aux résultats incertains, et en fin de compte vaine, car les éditeurs des pages en question disposent de nombreux moyens pour déjouer les mesures de prohibition.

Ressources publiques, ressources privées

Les systèmes et les réseaux comportent des données et des programmes que nous considérerons comme des ressources. Certaines ressources sont d'accès public, ainsi certains serveurs Web, d'autres sont privées pour une personne, comme une boîte à lettres électronique, d'autres sont privées pour un groupe de personnes, comme l'annuaire téléphonique interne d'une entreprise. Ce caractère plus ou moins public d'une ressource doit être traduit dans le système sous forme de droits d'accès.

Identifier et authentifier

Les personnes qui accèdent à une ressource non publique doivent être identifiées ; leur identité doit être authentifiée ; leurs droits d'accès doivent être vérifiés au regard des habilitations qui leur ont été attribuées : à ces trois actions correspond un premier domaine des techniques de sécurité, les méthodes d'authentification, de signature, de vérification de l'intégrité des données et d'attribution de droits (une habilitation donnée à un utilisateur et consignée dans une base de données adéquate est une liste de droits d'accès et de pouvoirs formulés de telle sorte qu'un système informatique puisse les vérifier automatiquement).

La sécurité des accès par le réseau à une ressource protégée n'est pas suffisamment garantie par la seule identification de leurs auteurs. Sur un réseau local de type Ethernet où la circulation des données fonctionne selon le modèle de l'émission radiophonique que tout le monde peut capter (enfin, pas si facilement que cela, heureusement), il est possible à un tiers de la détourner. Si la transmission a lieu à travers l'Internet, les données circulent de façon analogue à une carte postale, c'est-à-dire qu'au moins le facteur et la concierge y ont accès. Dès lors que les données doivent être protégées, il faut faire appel aux techniques d'un autre domaine de la sécurité informatique : le chiffrement. Authentification et chiffrement sont indissociables : chiffrer sans authentifier ne protège pas des usurpations d'identité (comme notamment l'attaque par interposition, dite en anglais attaque de type man in the middle), authentifier sans chiffrer laisse la porte ouverte au vol de données.

Empêcher les intrusions

Mais ces deux méthodes de sécurité ne suffisent pas, il faut en outre se prémunir contre les intrusions destinées à détruire ou corrompre les données, ou à en rendre l'accès impossible. Les techniques classiques contre ce risque sont l'usage de pare-feu(firewalls) et le filtrage des communications réseaux, qui permettent de protéger la partie privée d'un réseau dont les stations pourront communiquer avec l'Internet sans en être « visibles » ; le terme visible est ici une métaphore qui exprime que nul système connecté à l'Internet ne peut de sa propre initiative accéder aux machines du réseau local (seules ces dernières peuvent établir un dialogue) et que le filtre interdit certains types de dialogues ou de services, ou certains correspondants (reconnus dangereux).

La plupart des entreprises mettent en place des ordinateurs qu'elles souhaitent rendre accessibles aux visiteurs extérieurs, tels que leur serveur Web et leur relais de messagerie. Entre le réseau privé et l'Internet, ces machines publiques seront placées sur un segment du réseau ouvert aux accès en provenance de l'extérieur, mais relativement isolé du réseau intérieur, afin qu'un visiteur étranger à l'entreprise ne puisse pas accéder aux machines à usage strictement privé. Un tel segment de réseau est appelé zone démilitarisée(DMZ), en souvenir de la zone du même nom qui a été établie entre les belligérants à la fin de la guerre de Corée. Les machines en DMZ, exposées donc au feu de l'Internet, seront appelées bastions. Certains auteurs considèrent que ces techniques de sécurité par remparts, ponts levés et échauguettes sont dignes du Moyen-Âge de l'informatique ; ils leur préfèrent les systèmes de détection d'intrusion (IDS), plus subtils.

Un projet de certification de sécurité Open Source : OSSTMM

L'Institute for Security and Open Methodologies (ISECOM), est un organisme de recherche en sécurité fondé en 2001, qui se proclame « ouvert ». Cet institut a élaboré un référentiel de mesures de sécurité et d'audit, Open Source Security Testing Methodology Manual(OSSTMM). Ce manuel, disponible librement en ligne, propose donc une méthodologie de vérification de la sûreté des systèmes. La fonction d'un référentiel, c'est de pouvoir faire des audits. Si l'on a construit son système en suivant des règles écrites dans un référentiel, l'auditeur pourra vérifier la conformité du système au référentiel, ce qui est l'essentiel du métier d'audit. Encore faut-il que le référentiel soit pertinent. Le manuel OSSTMM peut éventuellement être utilisé comme catalogue de vérifications à faire et de mesures à prendre, comme il en existe beaucoup. Mais, comme tout catalogue, il risque de se substituer à la compréhension substantielle

de la situation de sécurité à étudier et à résoudre. En outre il ne sera pas d'un emploi très commode pour un auditeur, parce qu'il mêle deux genres, le référentiel de règles et de contrôles, et le manuel explicatif. Il y a certes des listes de choses à vérifier, mais formulées dans des termes assez étroitement techniques, ce qui risque de les périmer assez rapidement. L'auteur de ces lignes n'a pas été convaincu par l'ensemble.

D'autre part, l'utilité première d'un processus de certification est de procurer au certifié une garantie institutionnelle dont il puisse se prévaloir vis-à-vis de ses partenaires, des autorités légales et de son conseil d'administration. C'est la principale qualité, par exemple, du processus de certification IS 27001, qui, au moins en France, est encadré assez rigoureusement. De ce point de vue, le processus OSSTMM, où les auditeurs sont auto-certifiés, et la communauté d'origine auto-proclamée, semble assez faible.

Législation financière et SI

Depuis les scandales financiers de la période 2001-2002 (nous ne mentionnerons ici que les affaires Enron et Worldcom), sont apparues comme champignons après la pluie des réglementations destinées à améliorer le contrôle des autorités et des actionnaires sur la gestion des entreprises. Le signal a bien sûr été donné par les États-Unis en juillet 2002 avec la loi Sarbanes-Oxley (plus familièrement SOX), qui impose aux entreprises qui font appel au capital public (c'est-à-dire cotées en bourse) toute une série de règles comptables et administratives destinées à assurer la traçabilité de leurs opérations financières, afin que les actionnaires ne courent plus le risque de voir leurs actions partir en fumée après une déconfiture que des comptes truqués n'auraient pas permis de prévoir, cependant que les dirigeants initiés auraient revendu à temps leurs stock-options pour se retirer sur leur yacht aux îles Cayman... La France a bien sûr emboîté le pas avec la loi du 1er août 2003 sur la sécurité financière (LSF) qui concerne principalement trois domaines : la modernisation des autorités de contrôle des marchés financiers, la sécurité des épargnants et des assurés et enfin le contrôle légal des comptes ainsi que la transparence et le gouvernement d'entreprise. Cette loi française ne concerne pas seulement les sociétés cotées, mais toutes les sociétés anonymes ; elle est complétée par le dispositif réglementaire européen « Bâle 2 » de 2004, qui concerne les établissements financiers.

Les différents volets de la protection du SI

L'indispensable sécurité physique Avant d'entrer plus avant dans le vif de notre propos, il convient de faire un détour par un sujet que nous ne traiterons pas en détail, mais qu'il importe d'évoquer : toute mesure de protection logique est vaine si la sécurité physique des données et des traitements n'est pas convenablement assurée. Il convient donc d'accorder un soin jaloux aux points suivants :

- qualité du bâtiment qui abrite données et traitements, à l'épreuve des intempéries et des inondations, protégé contre les incendies et les intrusions ;
- contrôles d'accès adéquats ;
- qualité de l'alimentation électrique ;
- certification adéquate du câblage du réseau local et des accès aux réseaux extérieurs ; la capacité des infrastructures de communication est très sensible à la qualité physique du câblage et des connexions ;
- pour l'utilisation de réseaux sans fil, placement méticuleux des bornes d'accès, réglage de leur puissance d'émission et contrôle des signaux en provenance et à destination de l'extérieur. Ces précautions prises, il faut néanmoins envisager qu'elles puissent se révéler insuffisantes, et que l'intégrité physique de votre système d'information soit alors compromise. La compromission d'un système d'information désigne le fait qu'un intrus ait pu, d'une façon ou d'une autre, en usurper l'accès pour obtenir des informations qui auraient dû rester confidentielles. Pour éviter que cette circonstance n'entraîne la disparition de l'entreprise, il aura fallu prendre les mesures suivantes :
 - sauvegarde régulière des données sur des supports physiques adéquats distincts des supports utilisés en production ;
 - transport régulier de copies de sauvegarde en dehors du site d'exploitation ;
 - aménagement d'un site de secours pour les applications vitales. Ces précautions seront inopérantes si elles ne font pas l'objet d'une documentation tenue à jour et d'exercices périodiques : en situation de catastrophe, il s'avère que les humains ne savent faire que ce à quoi ils sont entraînés, des actions complexes qui n'auront jamais été effectuées « à blanc » ne pourront avoir pour conséquence qu'une catastrophe encore plus

grave. Des solutions techniques existent pour toutes ces mesures, mais leur mise en œuvre est complexe et onéreuse, ce qui conduit souvent à les négliger. Le débit des réseaux modernes permet de disposer à plusieurs kilomètres du site d'exploitation un site miroir dont les données pourront être mises à jour heure par heure, ou même en temps réel si cela est vraiment indispensable, le coût n'est même pas tellement élevé, mais la conception et la réalisation d'une telle organisation sont loin d'être des tâches faciles. De même, la complexité d'un plan de sauvegarde pour quelques dizaines de serveurs en réseau ne doit en aucun cas être sous-estimée.

La sécurité des données peut également être améliorée par le recours aux possibilités des matériels modernes de stockage et de leurs logiciels de pilotage : les systèmes NAS (Network Attached Storage) offrent des possibilités intéressantes de prise d'instantanés (snapshots) et de réPLICATION à distance, les batteries de disques RAID et les systèmes de fichiers virtuels tels que Logical Volume Management (LVM) diminuent grandement les risques de perte de données en cas de défaillance d'un disque. Le lecteur sera bien avisé de s'intéresser à ces sujets, qui font l'objet de nombreux et volumineux ouvrages, et dont nous ne saurions donner ici plus que cette énumération brève et non exhaustive.

Les mesures évoquées ici sont des missions pour des ingénieurs spécialisés, de haut niveau, et surtout expérimentés. Nous n'entrerons pas plus dans les détails de ces actions, mais nous ne saurions trop mettre en garde contre la tentation de les négliger.

Protéger le principal : le système d'exploitation

Afin d'être fiable, un système d'exploitation digne de ce nom doit comporter des dispositifs et des procédures de protection des objets qu'il permet de créer et de manipuler. Les objets à protéger appartiennent à deux grandes catégories : les objets persistants tels que les fichiers, et les objets éphémères créés en mémoire pendant l'exécution d'un processus et destinés à disparaître avec lui. Les objets matériels, tels que périphériques physiques, interfaces réseau, etc., sont assimilés à des objets persistants. La protection consiste à empêcher qu'un utilisateur puisse altérer un fichier qui ne lui appartient pas sans que le propriétaire lui en ait donné l'autorisation, ou encore, par exemple, à empêcher qu'un processus en cours d'exécution ne modifie une zone mémoire attribuée à un autre processus sans l'autorisation du propriétaire de celui-ci.

Droits d'accès

De façon très générale, la question de la protection d'un objet informatique se pose dans les termes suivants, inspirés des concepts mis en œuvre par le système Multics.

- Un objet a un propriétaire identifié, généralement l'utilisateur qui l'a créé. Un objet est, sous réserve d'inventaire, soit un fichier, soit un processus, soit des structures de données éphémères créées en mémoire par un processus, mais pour Multics tous ces objets sont en fin de compte des espaces de mémoire virtuelle nommés segments ou sont contenus dans des segments.
- Le propriétaire d'un objet peut avoir conféré à lui-même et à d'autres utilisateurs des droits d'accès à cet objet. Les types de droits possibles sont en général les suivants (on peut en imaginer d'autres) :
 - droit d'accès en consultation (lecture) ;
 - droit d'accès en modification (écriture, destruction, création) ;
 - droit d'accès en exécution ; pour un programme exécutable, la signification de ce droit est évidente ; pour un répertoire de fichiers ce droit confère à ceux qui le possèdent la faculté d'exécuter une commande ou un programme qui consulte ce répertoire ;
 - droit de blocage, par exemple pour un processus en cours d'exécution ou éligible pour l'exécution.
- À chaque objet est donc associée une liste de contrôle d'accès (access control list) qui énumère les utilisateurs autorisés et leurs droits.
- Avant toute tentative d'accès à un objet par un utilisateur, l'identité de cet utilisateur doit être authentifiée.
- Pour qu'un utilisateur ait le droit d'exécuter une action sur un objet, et dans un système informatique cette action est perpétrée par l'entremise d'un processus, il faut en outre que le processus en question possède le pouvoir voulu. Le pouvoir est un attribut d'un processus, il peut prendre des valeurs qui confèrent à ce processus des priviléges plus ou moins étendus. La plupart des systèmes ne proposent que deux valeurs de pouvoir : le mode superviseur, qui confère le pouvoir absolu, et le mode utilisateur, qui limite les actions de l'utilisateur en question aux objets dont il est propriétaire. Mais nous allons voir que certains systèmes ont affiné la hiérarchie des valeurs de pouvoir.

- La valeur du pouvoir d'un processus peut changer au cours de son exécution.

Ainsi un processus qui se déroule dans un mode utilisateur peut faire une demande d'entrée-sortie, ce qui nécessite le mode superviseur. Ceci sera résolu, sous Unix par exemple, par le mécanisme de l'appel système, qui transfère le contrôle, pour le compte du processus utilisateur, à une procédure du noyau qui va travailler en mode superviseur.



La cybersécurité

La cybersécurité est la protection des ordinateurs, des réseaux, des programmes et des données contre les attaques, les dommages ou les accès non autorisés. Elle est essentielle pour protéger notre vie privée, notre identité et nos informations personnelles. Dans ce guide, vous apprendrez les bases de la cybersécurité et comment vous pouvez vous protéger en ligne.

Les types de menaces en ligne

Il existe plusieurs types de menaces en ligne que vous devez connaître : Les logiciels malveillants : ce sont des programmes conçus pour endommager ou prendre le contrôle de votre ordinateur. Les virus, les vers, les chevaux de Troie et les ransomwares sont des exemples de logiciels malveillants. Le phishing : c'est une technique utilisée pour obtenir vos informations personnelles, telles que vos identifiants de connexion ou vos numéros de carte de crédit.

Les attaquants envoient des e-mails ou des messages texte qui semblent provenir d'une source légitime, comme votre banque ou votre entreprise. Les attaques de force brute : il s'agit d'une méthode qui consiste à essayer de deviner un mot de passe en utilisant différentes combinaisons jusqu'à ce que le bon soit trouvé. Les dénis de service : il s'agit d'une attaque qui vise à rendre un site Web ou un service indisponible en le surchargeant de trafic.

Les bonnes pratiques pour se protéger en ligne

Utilisez des mots de passe forts : vos mots de passe doivent contenir au moins huit caractères, être difficiles à deviner et ne pas être utilisés sur plusieurs sites Web. Méfiez-vous des e-mails et des messages texte suspects : ne cliquez pas sur les liens ou les pièces jointes provenant d'expéditeurs inconnus ou suspects. Utilisez un logiciel antivirus : il peut vous aider à détecter et à supprimer les logiciels malveillants de votre ordinateur. Mettez à jour vos logiciels : les mises à jour peuvent inclure des correctifs de sécurité pour les vulnérabilités connues. Utilisez des réseaux Wi-Fi sécurisés : évitez les réseaux publics ou non sécurisés qui peuvent être surveillés par des attaquants. Évitez de partager des informations personnelles sensibles en ligne : cela inclut les informations de carte de crédit, les numéros de sécurité sociale et les adresses personnelles.

Les conséquences des comportements en ligne

Il est important de comprendre que les comportements en ligne peuvent avoir des conséquences graves. Voici quelques exemples :

Le vol d'identité : les informations personnelles volées en ligne peuvent être utilisées pour voler votre identité et commettre des fraudes. Les conséquences juridiques : partager des fichiers piratés ou des contenus protégés par des droits d'auteur peut entraîner des poursuites judiciaires. Les conséquences professionnelles : publier des informations inappropriées sur les réseaux sociaux peut affecter votre réputation professionnelle.

Les réseaux informatiques

Un réseau informatique est un groupe d'ordinateurs connectés les uns aux autres pour partager des données et des ressources. Les réseaux peuvent être locaux, tels que ceux que l'on trouve dans les entreprises et les écoles, ou étendus, tels que l'Internet.

Les menaces pour la sécurité des réseaux

Les réseaux informatiques peuvent être vulnérables à plusieurs menaces pour la sécurité, notamment : Les attaques de type "man-in-the-middle" : ces attaques visent à intercepter les données entre deux parties qui communiquent, afin d'obtenir des informations confidentielles. Les attaques de déni de service distribué (DDoS) : ces attaques consistent à surcharger un réseau avec du trafic malveillant pour le rendre indisponible. Les attaques de force brute : ces attaques consistent à essayer de deviner des identifiants de connexion en utilisant différentes combinaisons jusqu'à ce que le bon soit trouvé.

Les bonnes pratiques pour protéger les réseaux

Utilisez des mots de passe forts pour les appareils et les comptes : cela peut aider à empêcher les attaquants d'accéder à votre réseau. Configurez les pare-feux : les pare-feux peuvent aider à bloquer les connexions non autorisées vers votre réseau. Mettez à jour les logiciels : les mises à jour peuvent inclure des correctifs de sécurité pour les vulnérabilités connues. Restreignez l'accès aux appareils et aux données : cela peut aider à empêcher les utilisateurs non autorisés d'accéder à votre réseau. Utilisez des outils de surveillance : ces outils peuvent aider à détecter les activités suspectes sur votre réseau.

Les conséquences des attaques sur les réseaux

Les attaques sur les réseaux peuvent avoir des conséquences graves, notamment : La perte de données : les attaques peuvent entraîner la perte de données importantes, telles que des informations clients ou des fichiers d'entreprise. Les coûts financiers : la restauration et la réparation d'un réseau endommagé peuvent être coûteuses. Les conséquences juridiques : les entreprises peuvent être tenues responsables des pertes de données des clients ou des violations de la confidentialité.



Introduction à Kali et à BackTrack Linux

Il y a quelques années, une discussion ouverte sur les techniques de hacking et leur enseignement aurait fait l'objet d'un certain tabou. Les temps ont heureusement changé et la valeur d'une sécurité offensive est à présent comprise. Elle est aujourd'hui adoptée par les entreprises, quels que soient leur taille et leur secteur d'activité. Les gouvernements la prennent également au sérieux. Ils sont nombreux à avoir annoncé sa mise en place.

Un test d'intrusion doit jouer un rôle important dans la sécurité globale de l'entreprise. À l'instar des politiques, de l'évaluation du risque, de la planification de la continuité d'activité et du plan de reprise d'activité, qui font désormais partie intégrante d'une stratégie de sécurité, il faut y ajouter les tests d'intrusion. Ils permettent de voir l'entreprise au travers des yeux de l'ennemi. Ils peuvent mener à des découvertes surprenantes, en donnant le temps de corriger les systèmes avant qu'un pirate n'entre en scène.

Lorsque l'on souhaite apprendre le hacking, on a aujourd'hui à disposition de nombreux outils. Non seulement ils sont prêts à l'emploi, mais nombre d'entre eux font également preuve d'une grande stabilité car ils bénéficient de plusieurs années de développement. Pour certains d'entre vous, le plus important sera peut-être que la plupart sont disponibles gratuitement. Les outils présentés dans ce module sont tous gratuits.

S'il est facile de savoir qu'un outil est gratuit, il peut en aller tout autrement pour le trouver, le compiler et l'installer avec tous les autres utilitaires requis pour mener à bien un test d'intrusion même de base. Si la procédure se révèle relativement simple sur un système d'exploitation **Linux** moderne, elle reste un **tantinet intimidante pour les novices**. En général, les gens sont plus intéressés par apprendre à utiliser les outils qu'à explorer Internet pour les trouver et ensuite les installer.

Pour être franc, vous devrez apprendre à compiler et à installer manuellement les logiciels sur une machine Linux. Tout au moins, vous devez vous familiariser avec l'outil **apt-get** (ou équivalent).

Aller plus loin

APT (Advanced Package Tool) est un système de gestion de paquetages. Il permet d'installer, d'actualiser et de supprimer rapidement et facilement des logiciels à partir de **la ligne de commande**. Outre sa simplicité, il présente l'intérêt de résoudre automatiquement les problèmes de dépendance. Autrement dit, si le paquetage en cours d'installation a besoin d'un logiciel supplémentaire, APT va se charger de localiser et d'installer automatiquement celui-ci. Cette possibilité constitue une nette amélioration par rapport aux outils plus anciens.

L'installation d'un logiciel à l'aide d'APT est très simple. Par exemple, supposons que nous souhaitions installer l'outil **Paros Proxy** sur notre **machine Linux locale**. **Paros peut servir, entre autres, à évaluer la sécurité des applications web**. Nous examinerons les **proxies** dans ce module, mais, pour le moment, concentrons-nous sur l'installation de l'outil plutôt que sur son utilisation. Si nous connaissons le nom du paquetage, il suffit d'exécuter **apt-get install** depuis **la ligne de commande en lui précisant ce nom**. Il est toujours préférable d'exécuter **apt-get update** avant d'installer un logiciel car nous sommes ainsi certains de disposer de la dernière version. Dans le cas de Paros, il suffit de lancer les commandes suivantes :

apt-get update

apt-get install paros

Avant que l'installation du paquetage ne débute, la quantité d'espace disque requise est affichée et APT demande si nous souhaitons poursuivre. Dans l'affirmative, nous saisissons **O**

et appuyons sur la touche Entrée. Lorsque l'installation du programme est terminée, nous revenons à l'invite #. Nous pouvons alors lancer Paros en exécutant la commande suivante depuis la console : **paros** Pour le moment, fermons simplement le programme Paros, car notre objectif était non pas de lancer ou d'utiliser Paros, mais de montrer l'installation d'un nouveau logiciel.

APT nous oblige à connaître le nom exact du logiciel à installer avant d'exécuter la commande **apt-get install**. Si nous ne sommes pas certains du nom ou ne connaissons pas son orthographe exacte, la commande **apt-cache search** va nous être utile. Elle affiche tous les paquetages ou outils qui correspondent au critère de recherche et en donne une courte description. Grâce à **apt-cache search**, nous pouvons arriver rapidement au nom du paquetage que nous recherchons. Par exemple, pour obtenir le nom officiel donné au paquetage de Paros, nous commençons par exécuter la commande

suivante :

apt-cache search paros

Dans les noms et les descriptions obtenus, nous devrions trouver le paquetage recherché. Il suffira ensuite d'exécuter la commande **apt-get install appropriée**.

Si vous choisissez la distribution Kali Linux, Paros sera déjà installé. Même dans ce cas, la commande **apt-get install** reste un outil puissant pour l'installation des logiciels. Des connaissances de base sur Linux vous seront profitables et vous en tirerez de nombreux bénéfices sur le long terme. Toutefois, pour votre propre bien, n'hésitez pas à vous engager à devenir plus tard un gourou Linux. Si vous vous intéressez aux tests d'intrusion ou au hacking, vous n'avez d'autre choix que de maîtriser Linux.

Heureusement, le monde de la sécurité profite d'une communauté très active et très généreuse. Plusieurs organismes ont travaillé inlassablement

à la création de distributions Linux adaptées à la sécurité. Une distribution est de façon générale une variante, un type ou une marque dérivé de Linux.

Parmi les distributions les plus connues adaptées aux tests d'intrusion, il existe **BackTrack**. Elle représente votre guichet unique pour l'apprentissage du hacking et la mise en place de tests d'intrusion.

BackTrack Linux me fait penser à cette scène du premier épisode de **Matrix** où **Tank** demande à **Neo** : "Alors, de quoi t'as besoin, à part d'un miracle ?" **Neo** réplique alors : "Des armes, un maximum d'armes." À ce moment du film, de nombreux râteliers d'armes apparaissent. Tous les types d'armes imaginables sont proposés à **Neo** et à **Trinity** : des pistolets, des fusils, des fusils de chasse, des semi-automatiques, des automatiques, des explosifs et d'autres encore. Lorsqu'ils démarrent **BackTrack** ou **Kali**, les débutants se trouvent dans la même situation : des outils, un maximum d'outils.

BackTrack Linux et Kali Linux sont le rêve réalisé de tout hacker. Ces distributions ont été conçues pour les testeurs d'intrusion. Elles viennent avec des centaines d'outils de sécurité déjà installés, configurés et prêts à l'emploi. Qui plus est, elles sont gratuites ! Vous pouvez en télécharger

un exemplaire à l'adresse <http://www.backtrack-linux.org/downloads/>.

Info

Au printemps 2013, les membres d'Offensive Security ont sorti une version redéfinie et revue de **BackTrack** appelée "**Kali Linux**". Elle est également disponible gratuitement et est fournie avec de nombreux outils pour l'audit de la sécurité. Vous pouvez la télécharger à l'adresse <http://www.kali.org>.

Si vous débutez dans les tests d'intrusion et le hacking, les différences entre BackTrack et Kali risquent d'être confuses. Toutefois, pour apprendre les bases et expérimenter les exemples de ce module, les deux distributions feront l'affaire. Kali Linux sera parfois plus facile à utiliser que BackTrack car tous les outils sont installés de façon à pouvoir être exécutés depuis n'importe quel répertoire. Il suffit d'ouvrir une fenêtre de terminal et de saisir le nom de l'outil, avec les options souhaitées. Si vous utilisez BackTrack, il vous faudra souvent aller dans le répertoire qui correspond à un outil avant de pouvoir lancer celui-ci. Si ces explications vous laissent un tantinet perplexe, ne vous inquiétez pas. Nous y reviendrons progressivement.

Pour le moment, vous devez simplement choisir entre Kali et BackTrack. Quelle que soit votre décision, elle sera de toute façon bonne.

En vous rendant sur ce site, vous aurez le choix entre un fichier .iso et une image VMware. Si vous choisissez le fichier .iso, vous devrez le graver sur un DVD. Il vous suffira de placer ce DVD amorçable dans le lecteur et de redémarrer l'ordinateur. Dans certains cas, vous devrez d'abord modifier l'ordre de démarrage dans le BIOS afin de donner la priorité au lecteur optique.

Si vous choisissez de télécharger l'image VMware, vous aurez besoin d'un logiciel capable de l'ouvrir et de la déployer ou de l'exécuter. Par chance, il existe plusieurs outils pour y parvenir. En fonction de vos préférences, vous pouvez opter pour VMware Player de VMware, VirtualBox d'Oracle ou Virtual PC de Microsoft. Si ces propositions ne vous conviennent pas, il existe d'autres logiciels capables d'exécuter une image VMware. Prenez simplement celui qui vous correspond.

Les trois solutions de virtualisation mentionnées sont disponibles gratuitement et vous permettront d'exécuter des images de machines virtuelles. Vous devez simplement décider de la version à employer.

Mettre en place un laboratoire de hacking

Un hacker éthique doit disposer d'un endroit où pratiquer et découvrir. La plupart des débutants se demandent comment apprendre à utiliser les outils de hacking sans violer la loi ni attaquer des cibles interdites. En général, la solution consiste à créer son propre "laboratoire de hacking". Il s'agit d'un environnement isolé du trafic réseau, et les attaques n'ont aucune chance de sortir ni d'atteindre des cibles interdites ou accidentnelles. Dans cet environnement, vous avez toute liberté pour étudier les différents outils et techniques sans craindre que du trafic ou des attaques ne sortent de votre réseau. Le laboratoire comprend au moins deux machines : celle de l'assaillant et celle de la victime. Il est également possible de déployer simultanément plusieurs victimes afin de simuler un réseau plus réaliste.

Il est important que l'utilisation et la configuration du laboratoire de hacking soient correctes car il représente l'une des meilleures façons de se former à ces techniques par l'expérimentation. L'apprentissage et la maîtrise des bases des tests d'intrusion se passent de la même manière. Le seul point crucial du laboratoire réside dans l'isolation du réseau. Vous devez le configurer afin qu'il soit impossible au trafic de sortir du réseau. Tout le monde peut faire des erreurs et se tromper dans la saisie des adresses IP. Rien n'est plus facile que d'inverser des chiffres dans une adresse IP, mais cette simple erreur peut avoir des conséquences

catastrophiques pour vous et votre avenir. Il serait dommage (pour ne pas dire illégal) d'effectuer des scans et des attaques sur une cible que vous pensez présente dans votre laboratoire à l'adresse 173.16.1.1 et de découvrir ensuite que vous aviez saisi l'adresse 137.16.1.1.

Pour mettre en place un environnement isolé, l'approche la plus simple et la plus efficace consiste à débrancher physiquement votre réseau d'Internet. Si vous utilisez des machines physiques, il est préférable d'opter pour une connexion Ethernet filaire et des commutateurs pour router le trafic. N'oubliez pas de vérifier soigneusement que toutes les interfaces sans fil sont désactivées. Avant de poursuivre, inspectez et examinez toujours votre réseau à la recherche de fuites potentielles.

La création d'un laboratoire de hacking autour de machines physiques est une solution viable, mais les machines virtuelles apporteront plusieurs avantages. Tout d'abord, en raison de la puissance des processeurs actuels, il est possible de créer et de configurer un petit laboratoire sur une seule machine ou un ordinateur portable. Dans la plupart des cas, une machine de gamme intermédiaire est capable d'exécuter simultanément deux ou trois machines virtuelles car les cibles peuvent avoir une configuration réduite. Même un ordinateur portable est en mesure de supporter deux machines virtuelles. Un tel choix aura l'avantage de rendre votre laboratoire portable. Le faible coût des disques de stockage externes permet de créer des centaines de machines virtuelles sur un même disque, de les transporter et de les activer en fonction des besoins. Si vous souhaitez pratiquer ou explorer un nouvel outil, lancez simplement BackTrack, Kali ou votre machine d'attaque, et déployez une machine virtuelle sous forme de cible. La mise en place d'un laboratoire de ce type vous permet de brancher rapidement différents systèmes d'exploitation et configurations et de jouer avec.

Grâce aux machines virtuelles, il est également très simple d'isoler l'intégralité du système. Pour cela, il suffit de désactiver la carte sans fil et de débrancher le câble réseau. Si les adresses réseau ont été attribuées comme nous l'avons expliqué précédemment, la machine physique et les machines virtuelles resteront en mesure de communiquer les unes avec les autres et vous serez certain qu'aucun trafic d'attaque ne sortira de l'ordinateur physique.

Un test d'intrusion est en général un processus destructif. Un grand nombre d'outils que nous utiliserons et les exploits que nous réaliserons peuvent provoquer des dommages et conduire au dysfonctionnement des systèmes. Dans certains cas, il est plus facile de réinstaller le système d'exploitation ou un programme que de tenter une réparation.

Sur ce point, les machines virtuelles présentent un véritable avantage. Au lieu de réinstaller physiquement un programme comme SQL Server ou un système d'exploitation complet, la machine virtuelle peut être aisément réinitialisée ou restaurée dans sa configuration d'origine.

Reconnaissance

Les personnes qui participent aux ateliers ou aux formations sur le hacking ont en général des connaissances de base sur quelques outils de sécurité. Elles ont souvent employé un scanner de ports pour explorer un système ou ont pu se servir de Wireshark pour étudier un trafic réseau.

Certaines se sont même sans doute amusées avec des outils d'exploitation comme Metasploit. Malheureusement, la plupart des débutants ne comprennent pas la place de ces différents outils dans le contexte global d'un test d'intrusion. Leurs connaissances sont donc incomplètes. En suivant une méthodologie, vous respectez un plan et savez comment avancer.

Pour souligner l'importance de la méthodologie, il peut être bon de décrire un scénario qui illustre à la fois l'intérêt de cette étape et les bénéfices que l'on peut tirer du suivi d'une méthodologie complète lors d'un test d'intrusion.

Supposons que vous soyez un testeur d'intrusion éthique qui travaille pour une société de sécurité. Votre chef vient vous voir dans votre bureau et vous tend une feuille de papier : "Je viens d'avoir le PDG de cette entreprise au téléphone. Il veut que mon meilleur testeur d'intrusion, c'est-à-dire vous, intervienne sur sa société. Notre service juridique va vous envoyer un courrier électronique pour confirmer que nous avons toutes les autorisations et les garanties appropriées." Vous hochez la tête pour accepter ce travail. Il sort de votre bureau. Vous jetez un œil à la feuille de papier, sur laquelle un seul mot est écrit : Syngress. Vous n'avez jamais entendu parler de cette société et le document ne donne aucune autre information.

Que faire ?

Tout travail doit commencer par une recherche. Mieux vous serez préparé pour une opération, plus vous aurez de chances de réussir. Les créateurs de BackTrack et de Kali Linux aiment citer Abraham Lincoln : "Que l'on me donne six heures pour couper un arbre, j'en passerai quatre à préparer ma hache." Il s'agit d'une parfaite introduction aux tests d'intrusion et à la phase de reconnaissance.

La reconnaissance, ou recueil d'informations, est probablement la plus importante des quatre phases que nous allons présenter. Plus vous passerez du temps à collecter des informations sur votre cible, plus les phases suivantes auront une chance de réussir. Pourtant, la reconnaissance est également l'une des étapes les plus négligées, sous utilisées et incomprises dans les méthodologies actuelles des tests d'intrusion.

Cette phase est sans doute négligée car son concept n'est jamais formellement présenté aux débutants, tout comme ses bénéfices ou l'importance d'une bonne collecte d'informations pour les phases suivantes. Par ailleurs, il s'agit de la phase la moins technique et la moins excitante. Les novices en hacking ont souvent tendance à la considérer comme ennuyeuse et peu stimulante. Rien n'est plus éloigné de la vérité.

S'il est exact que peu de bons outils automatisés permettent de mener à bien une reconnaissance, la maîtrise de ses bases permet de voir le monde sous un autre jour. Un collecteur d'informations efficace est constitué à parts égales d'un hacker, d'un ingénieur social et d'un détective privé. L'absence de règles de conduite parfaitement définies distingue cette phase des autres. Cela contraste totalement avec les autres étapes de notre méthodologie. Par exemple, lorsque nous présenterons les scans, vous découvrirez que leur mise en place sur une cible se fait en suivant scrupuleusement une séquence d'étapes identifiées.

Apprendre à mener une reconnaissance numérique donne des compétences valorisantes pour quiconque vit dans le monde actuel. Pour les testeurs d'intrusion et les hackers, cela n'a pas de prix. Le monde des tests d'intrusion regorge d'exemples et d'histoires sur des testeurs qui ont pu compromettre un réseau ou un système simplement grâce à la reconnaissance effectuée.

Prenons l'exemple de deux criminels différents qui planifient le braquage d'une banque. Le premier achète une arme et pénètre dans la banque en criant : "Haut les mains, c'est un hold-up !" Vous imaginez sans mal le chaos qui peut s'ensuivre et, même si le voleur incompetent parvient à s'enfuir, il ne faudra pas longtemps à la police pour le retrouver, l'arrêter et l'envoyer en prison. À l'opposé, prenons n'importe quel film hollywoodien dans lequel les criminels passent plusieurs mois à planifier, à simuler, à organiser et à examiner tous les détails avant leur casse. Ils prennent du temps à acheter discrètement des armes, à prévoir des itinéraires de repli et à étudier les plans du bâtiment. Ils se rendent dans la banque pour repérer les caméras de sécurité, pour noter la place des gardes et déterminer à quel moment la banque dispose du plus d'argent et est la plus vulnérable. Ces criminels ont clairement plus de chances que le

premier de repartir avec l'argent.

La différence entre ces deux modes opératoires réside évidemment dans la préparation. Le hacking et les tests d'intrusion demandent également une préparation – il ne suffit pas d'obtenir une adresse IP et de lancer Metasploit (cette approche est possible mais sera probablement peu efficace).

Revenons à l'exemple donné au début de ce module. Vous devez effectuer un test d'intrusion mais vous disposez de très peu d'informations. Vous ne connaissez que le nom de la société. La question à un million d'euros pour tout aspirant hacker est : "Comment puis-je passer du nom d'une entreprise à un accès aux systèmes de son réseau ?"

Au début, nous ne savons pratiquement rien sur l'entreprise. Nous ne connaissons pas son site web, son adresse physique ni le nombre de ses employés. Nous ne connaissons pas ses adresses IP publiques ni son schéma IP interne. Nous ne savons rien des technologies déployées, des systèmes d'exploitation installés ni des défenses mises en place.

La première étape commence par une recherche d'informations publiques ; certaines entreprises appellent cela ROSO (renseignement d'origine source ouverte) ou, en anglais, OSINT (Open-Source Intelligence).

Dans la plupart des cas, nous pouvons récolter une quantité de données significatives sans envoyer un seul paquet vers la cible. Signalons à ce propos que certains outils ou techniques employés pour la reconnaissance envoient des informations directement à la cible. Il est important de savoir distinguer les outils qui touchent à la cible et ceux qui n'y touchent pas. Cette phase a deux objectifs principaux : premièrement recueillir autant d'informations que possible sur la cible et deuxièmement trier toutes ces informations et créer une liste d'adresses IP ou d'URL attaquables.

Les deux types de hackers réalisent une reconnaissance exhaustive de leur cible, mais les pirates n'ont pas de limites ni d'autorisation.

Lorsque les hackers éthiques effectuent leurs recherches, ils sont contraints de rester dans les limites du test. Au cours de la collecte des informations, il n'est pas rare qu'un hacker découvre un système vulnérable relié à la cible mais qui ne lui appartient pas. Même si ce système peut fournir un accès à l'organisme d'origine, sans autorisation préalable le hacker éthique s'interdira d'utiliser ou d'explorer cette option. Par exemple, supposons que vous meniez un test d'intrusion sur

une entreprise et que vous déterminiez que son serveur web (qui contient les données des clients) fasse l'objet d'une sous-traitance. Si vous identifiez une vulnérabilité importante sur le site web du client alors que vous n'êtes pas explicitement autorisé à le tester et à l'utiliser, vous devez l'ignorer. Les pirates ne sont pas contraints par de telles règles et vont employer tous les moyens possibles pour accéder aux systèmes de la cible. Dans la plupart des cas, puisque vous n'êtes pas autorisé à tester ni à examiner ces systèmes externes, vous ne pourrez pas fournir un grand nombre de détails. Cependant, votre rapport final doit inclure autant d'informations que possible sur les systèmes qui, à votre avis, font peser des risques sur l'entreprise.

Info

En tant que testeur d'intrusion, lorsque vous découvrez des risques qui sortent de l'étendue de votre accord, vous devez faire tout votre possible pour obtenir l'autorisation d'étendre celle-ci. Cela vous demandera souvent de travailler étroitement avec votre client et ses fournisseurs afin d'expliquer correctement les risques potentiels.

Pour réussir la phase de reconnaissance, nous devons mettre en place une stratégie. Pratiquement toutes les facettes de la collecte d'informations exploitent la puissance d'Internet. Une stratégie classique comprend une reconnaissance active et une reconnaissance passive.

La reconnaissance active demande une interaction directe avec la cible.

Notez que, au cours de ce processus, la cible peut enregistrer votre adresse IP et consigner vos actions. Elles ont donc de fortes chances d'être détectées, même si vous tentez de réaliser un test d'intrusion de façon furtive.

La reconnaissance passive se fonde sur les informations disponibles sur le Web. Au cours de ce travail, nous n'interagissons pas directement avec la cible, qui n'a donc aucun moyen de connaître, d'enregistrer ou de consigner nos actions.

Nous l'avons expliqué, l'objectif de la reconnaissance est de recueillir autant d'informations que possible sur la cible. À ce stade du test d'intrusion, aucun détail ne doit être ignoré, aussi inoffensif qu'il puisse paraître. Il est important de conserver les données recueillies dans un lieu central. Lorsque c'est possible, il est préférable de les mémoriser sous une forme électronique. Cela permettra d'effectuer ultérieurement des recherches rapides et précises. Chaque hacker est différent et certains préfèrent imprimer les informations obtenues.

Chaque feuille de papier doit être soigneusement classée et placée dans un dossier. Si vous adoptez la solution papier, prenez soin d'organiser minutieusement vos données.

Pour une seule cible, il est possible d'arriver rapidement à plusieurs centaines de pages.

En général, la première activité consiste à trouver le site web de l'entreprise. Dans notre exemple, nous allons utiliser un moteur de recherche pour obtenir des informations sur "Syngress".

Attention

Même si nous avons discuté précédemment de l'importance de la création et de l'utilisation d'un "laboratoire de hacking isolé" afin d'éviter que du trafic ne sorte du réseau, la mise en place de la reconnaissance exige une connexion Internet active.

HTTrack

La première phase débute souvent par un examen minutieux du site web de la cible. Dans certains cas, nous pouvons nous servir de l'outil HTTrack pour effectuer une copie de toutes les pages du site. Cet utilitaire gratuit est capable de générer une copie consultable hors connexion du site web cible. Cette copie comprendra l'ensemble des pages, liens, images et code du site d'origine, mais elle résidera sur l'ordinateur local. Grâce aux outils d'aspiration de sites web comme HTTrack, nous pouvons explorer et fouiller de fond en comble le site web hors connexion, sans avoir à passer du temps à nous balader sur le serveur web de l'entreprise.

Info

Vous devez bien comprendre que plus vous passez du temps à naviguer et à explorer le site web de la cible, plus vos actions pourront être repérées et suivies (même si vous vous contentez de parcourir le site). N'oubliez pas que chaque fois que vous interagissez directement avec une ressource détenue par la cible, il est possible que vous laissiez une empreinte digitale numérique.

Les testeurs d'intrusion expérimentés se servent également d'outils automatiques pour extraire des informations supplémentaires ou cachées à partir d'une copie locale du site web.

HTTrack est disponible en téléchargement sur le site web à l'adresse <http://www.httrack.com/>. Dans le cas de la version Windows, il suffit de récupérer le fichier d'installation et de lancer son exécution. Si vous souhaitez installer HTTrack sur Kali ou votre machine d'attaque sous Linux, connectez-vous à Internet, ouvrez une fenêtre de terminal et saisissez la commande

suivante :

```
apt-get install httrack
```

Notez qu'il existe également une version graphique de HTTrack, mais, pour le moment, nous allons nous limiter à la version en ligne de commande. Si vous préférez une interface graphique, vous pourrez toujours l'installer ultérieurement.

Après que le programme a été installé, vous pouvez le lancer en ouvrant une fenêtre de terminal et en exécutant la commande suivante :

```
httrack
```

Vous devez comprendre que le clonage d'un site web est facile à repérer et que cette activité est considérée comme fortement offensive. N'utilisez jamais HTTrack sans autorisation préalable. Après son démarrage, cet outil pose une suite de questions avant de procéder à la copie du site. Pour y répondre, il suffit en général d'appuyer sur la touche Entrée. Vous devez toutefois saisir un nom de projet et l'URL du site à copier.

Prenez le temps de lire chaque question avant d'accepter systématiquement la valeur par défaut. Lorsque le questionnaire est terminé, saisissez Y pour lancer le clonage. Le temps nécessaire à l'opération dépendra de la taille du site web. N'oubliez pas que vous devez disposer sur votre ordinateur local d'un espace disque suffisant pour contenir l'intégralité du site cible.

Les plus grands peuvent en demander une quantité très importante.

Vérifiez toujours la place disponible avant de démarrer l'opération de copie.

Après que HTTrack a terminé la copie, il affiche sur le terminal un message indiquant que l'opération est achevée et vous remerciant d'avoir utilisé HTTrack. Si vous utilisez Kali et avez accepté les options par défaut, HTTrack place le site cloné dans le répertoire

/root/websites/
nom_du_projet. Vous pouvez à présent lancer Firefox et saisir

/root/websites/nom_du_projet

dans le champ d'adresse.

nom_du_projet

doit être remplacé par le nom que vous avez indiqué lors de la configuration de l'opération de copie. Dans le navigateur, vous pouvez manipuler le site web copié en cliquant sur les liens. Le fichier index.html constitue généralement un bon point de départ.

Firefox est disponible à partir du bureau, dans le menu des applications. Vous pouvez également ouvrir un terminal et exécuter la commande suivante :

firefox

Que vous fassiez une copie du site web ou que vous le parcouriez simplement en temps réel, il est important de faire attention aux détails. Vous devez examiner attentivement toutes les informations que vous découvrez sur le site web de la cible et les enregistrer. Bien souvent, une navigation un peu approfondie conduira à des découvertes intéressantes, comme une adresse et des emplacements physiques, des numéros de téléphone, des adresses électroniques, des horaires d'ouverture, des relations professionnelles (partenaires), des noms d'employés, les connexions aux médias sociaux et d'autres données publiques.

Lors d'un test d'intrusion, il est important de prêter attention à certains éléments, comme les actualités et les annonces. Les entreprises sont souvent fières de leurs prouesses et laissent filer par mégarde des informations dans les articles. Les fusions et les acquisitions d'entreprises peuvent également fournir des données intéressantes, notamment pour augmenter l'étendue du test d'intrusion et lui ajouter des cibles supplémentaires. Même la plus petite acquisition faite en douceur peut créer des changements et des désordres dans une organisation. Il existe toujours une période de transition lors de la fusion d'entreprises. Elle nous donne des opportunités uniques de tirer parti des changements et de la confusion. Même si une fusion est ancienne ou s'est faite sans difficulté, l'information a toujours une valeur en désignant des cibles supplémentaires. Les entreprises fusionnées ou associées doivent être

autorisées et incluses dans la liste des cibles, car elles constituent une passerelle potentielle vers le client.

Enfin, il est important de rechercher et d'examiner les offres d'emploi technique proposées par la société cible. En effet, elles dévoilent souvent des informations très détaillées sur les technologies mises en œuvre au sein de la société. Vous pourrez notamment y voir mentionnés du matériel et du logiciel spécifiques. N'oubliez pas de rechercher la cible dans les offres d'emploi postées ailleurs. Par exemple, supposons que vous trouviez une annonce pour un poste d'administrateur réseau qui doit posséder une expérience sur les appareils Cisco ASA. Vous pouvez immédiatement en conclure plusieurs choses. Tout d'abord, vous êtes certain que l'entreprise utilise ou envisage d'utiliser un pare-feu Cisco ASA. Ensuite, en fonction de la taille de la société, vous pouvez en déduire qu'aucun de ses employés n'est en mesure d'utiliser et de configurer correctement un pare-feu Cisco ASA, ou que la personne compétente va s'en aller. Dans les deux cas, vous avez obtenu des informations intéressantes sur les technologies en place.

Après l'examen minutieux du site web de la cible, nous devons avoir une bonne connaissance de celle-ci, notamment qui elle est, ce qu'elle fait, où elle se trouve et quelles technologies elle emploie.

Armés de ces informations de base, nous pouvons passer à une reconnaissance passive. Pour une entreprise, il est très difficile, voire

impossible, de déterminer si un hacker ou un testeur d'intrusion effectue une telle reconnaissance. Cette activité présente un risque faible pour l'assaillant, alors qu'elle peut se révéler très enrichissante. Rappelons qu'une reconnaissance passive se fait sans envoyer un seul paquet vers les systèmes de la cible. Pour cette opération, notre arme de prédilection est évidemment Internet. Nous commençons par effectuer des recherches exhaustives de la cible dans les différents moteurs existants. Les bons moteurs de recherche disponibles aujourd'hui sont nombreux, mais, pour la présentation des bases du hacking et des tests d'intrusion, nous allons nous limiter à Google. Celui-ci fait vraiment un bon travail ; c'est pourquoi le cours de l'action de l'entreprise est si élevé. Ses robots fouillent sans relâche les moindres recoins d'Internet afin de cataloguer toutes les informations trouvées. Ils sont si efficaces que les hackers parviennent parfois à mener un test d'intrusion complet en utilisant uniquement Google.

Lors de la conférence Defcon 13, Johnny Long a ébranlé la communauté des hackers en donnant une session intitulée "Google Hacking for Penetration Testers". Elle a été suivie de la publication d'un ouvrage qui allait encore plus loin dans l'art du hacking Google.

Nous n'allons pas entrer dans les spécificités du hacking Google, mais une bonne compréhension de la manière d'utiliser correctement ce moteur est indispensable pour devenir un expert des tests d'intrusion. Si

vous posez à quelqu'un la question "comment utilises-tu Google ?", il répond généralement par "c'est simple, je lance mon navigateur web, je me rends sur la page d'accueil de Google et je saisis les termes dans le champ de recherche".

Bien que cette réponse soit pertinente pour 99 % des internautes, elle ne suffit pas pour les aspirants hackers et testeurs d'intrusion. Ils doivent apprendre à effectuer des recherches de manière plus intelligente et à mieux exploiter les résultats obtenus. En maîtrisant les moteurs de recherche comme Google, vous gagnerez du temps et vous pourrez trouver les joyaux qui se cachent dans les milliards de pages web accessibles sur Internet.

Opérateurs Google

Nous avons de la chance, Google nous donne accès à des "opérateurs" faciles d'emploi qui nous aideront à exploiter au mieux nos recherches. Ces opérateurs correspondent à des mots clés grâce auxquels nous pouvons extraire de façon plus précise des informations à partir de l'index Google.

Supposons par exemple que vous vouliez rechercher sur le site web de des informations me concernant. La solution la plus simple consiste à saisir les termes suivants dans le champ de recherche de Google : pat javier perrez mota. Cette recherche va produire plusieurs résultats, mais, au moment de l'écriture de ces lignes, seuls quatre des dix premiers sites web sont en lien avec moi.

Grâce aux opérateurs Google, nous pouvons influencer l'index Google.

Dans l'exemple précédent, nous connaissons à la fois le site web cible et les mots clés à rechercher. Plus précisément, nous voulons obliger Google à retourner uniquement les résultats qui proviennent du domaine de la cible. Dans ce cas, l'opérateur site : est notre meilleur ami. En effet, il demande à Google de retourner uniquement les résultats qui correspondent aux termes indiqués et qui proviennent directement du site web précisé.

Pour utiliser un opérateur Google, nous devons indiquer les trois éléments suivants :

1. le nom de l'opérateur ;
2. des deux-points ;
3. le terme à utiliser dans l'opérateur.

Après avoir saisi les trois éléments d'information précédents, nous pouvons effectuer une recherche normale. Pour utiliser l'opérateur site:, nous devons saisir la ligne suivante dans le champ de recherche de Google :

site:domaine terme(s) à rechercher

Vous remarquerez qu'aucune espace ne se trouve entre l'opérateur, les deux points et le domaine. Pour reprendre notre exemple précédent, nous voulons mener une recherche concernant Pat Engebretson sur le site web de DSU. Pour cela, nous saisissons la commande suivante dans le champ

de recherche de Google :

site:dsu.edu pat engebretson

Les résultats de cette recherche sont très différents de la précédente.

Tout d'abord, nous avons réduit le nombre de résultats : de plus de 30 000, nous arrivons à 147. La liste est plus facile à gérer, car une personne aura moins de difficultés à extraire des informations à partir de 147 résultats qu'à partir de 30 000. Ensuite, et c'est probablement le plus important, chaque résultat obtenu provient directement du site web cible. Grâce à l'opérateur `site:`, nous pouvons effectuer une recherche sur une cible particulière, pour ensuite trouver des informations complémentaires. Il nous permet de focaliser notre recherche et de ne pas être submergé par les résultats.

Attention

Vous devez savoir que les recherches avec Google ne sont pas sensibles à la casse. Par conséquent, "pat", "Pat" et "PAT" produiront exactement les mêmes résultats.

Les opérateurs `intitle:` et `allintitle:` sont également très intéressants. En les ajoutant à une recherche, seuls les sites web dont les titres des pages comprennent les termes indiqués sont retournés. Avec `allintitle:`, seuls les sites dont les titres des pages comprennent tous les termes sont retournés. Avec l'opérateur `intitle:`, les pages dont les titres comprennent au moins l'un des termes saisis sont retournées.

Voici un exemple classique de recherche Google avec l'opérateur

allintitle: :

allintitle:index of

Elle permet d'obtenir la liste de tous les répertoires qui ont été indexés et qui sont accessibles au travers du serveur web. Cela constitue souvent un bon point de départ pour effectuer une reconnaissance sur la cible.

Si nous voulons rechercher les sites dont les URL comprennent des mots précis, nous avons à notre disposition l'opérateur inurl:. Nous pouvons par exemple émettre la commande suivante pour localiser des pages potentiellement intéressantes sur la cible :

inurl:admin

Cette recherche pourra se révéler extrêmement utile car elle permet de révéler des pages d'administration ou de configuration sur le site web de la cible.

Il peut également être très intéressant d'effectuer des recherches dans le cache de Google plutôt que sur le site web de la cible. Cette approche non seulement permet de réduire notre empreinte numérique sur le serveur de la cible (nous sommes plus difficiles à détecter) mais nous fournit également l'opportunité de consulter des pages web et des fichiers qui ont été retirés du site web officiel. Le cache de Google mémorise une copie épurée de chaque site web qui a été examiné par ses robots. Il est important de comprendre que le cache contient à la fois le code qui a

servi à la construction du site et les nombreux fichiers qui ont été découverts au cours de l'analyse. Il peut s'agir de fichiers PDF, de documents Microsoft Office, de fichiers texte, etc.

Aujourd'hui, il n'est pas rare que des informations soient placées par erreur sur Internet. Supposons par exemple que vous soyez l'administrateur réseau d'une entreprise. Vous utilisez Microsoft Excel pour créer un classeur qui contient toutes les adresses IP, les noms et les emplacements des PC dans votre réseau. Au lieu de transporter ce document Excel avec vous, vous décidez de le publier sur l'intranet de l'entreprise afin qu'il soit accessible uniquement par son personnel.

Cependant, au lieu de le placer sur l'intranet, vous le publiez par erreur sur le site web public de la société. Si les robots de Google analysent votre site avant que vous ne retirez le document, il est possible que celui-ci réside dans le cache de Google même après que vous avez supprimé le fichier de votre site. Voilà pourquoi il est important d'effectuer des recherches dans le cache de Google.

L'opérateur `cache:` permet de limiter les résultats de recherche et de ne présenter que les informations extraites directement du cache de Google.

L'exemple suivant retourne la version de la page d'accueil de Syngress qui se trouve dans le cache :

`cache:syngress.com`

Si nous cliquons sur l'une des URL obtenues, nous arrivons non pas sur la

version qui existe dans le cache mais sur le site web actif. Pour consulter les pages mémorisées dans le cache, il faut modifier la recherche.

Le dernier opérateur mentionné dans cette section se nomme filetype::

Nous pouvons nous en servir pour préciser des extensions de fichiers et donc pour rechercher des types de fichiers sur le site web de la cible. Par exemple, pour obtenir uniquement les résultats qui concernent des documents PDF, saisissez la commande suivante :

filetype:pdf

Cet opérateur sera très utile pour trouver des liens vers des fichiers particuliers, comme ceux qui ont l'extension

.doc

,

.xlsx

,

.ppt

,

.txt

ou autres. Nos possibilités sont presque sans limites.

Pour une plus grande souplesse, il est possible de combiner plusieurs opérateurs dans la même recherche. Par exemple, voici comment rechercher toutes les présentations PowerPoint sur le site web de DSU :

site:dsu.edu filetype:ppt

Chaque résultat retourné correspond à un fichier PPT qui provient directement du domaine dsu.edu. La première utilise les opérateurs Google, tandis que la seconde correspond à une recherche classique. Les opérateurs

Google permettent de réduire énormément le nombre de résultats (de 211955).

Le hacking Google est parfois appelé "Google Dork". Lorsqu'une application souffre d'une vulnérabilité précise, les hackers et les chercheurs en sécurité placent généralement un Google Dork dans l'exploit, ce qui nous permet de rechercher des versions vulnérables en utilisant Google. Le site web Exploit Database, qui est maintenu par les créateurs de BackTrack et de Kali Linux (Offensive-Security), propose une longue liste de Google Dork et des techniques de hacking Google supplémentaires. Rendez-vous à l'URL <http://www.exploit-db.com> et cliquez sur le bouton GHDB (Google Hacking Database).

Voici une autre recherche qui pourra produire des informations intéressantes :

inurl:login

Elle peut également se faire avec les termes suivants :

Logon

Signin

Signon

Forgotpassword

Forgot

Reset

Nous pourrons ainsi trouver des pages d'ouverture de session ou similaires qui peuvent proposer du contenu dynamique. Des vulnérabilités se cachent souvent dans ce type de pages.

La recherche suivante produit une liste des répertoires qu'il est possible de parcourir afin d'en consulter le contenu :

site:syngress.com intitle:"index of"

Une telle vulnérabilité est absente du site de Syngress, mais cette méthode est souvent employée pour rechercher des fichiers supplémentaires qui ne sont normalement pas accessibles au travers des pages web.

Il existe de nombreux autres opérateurs et hacks Google avec lesquels vous devez vous familiariser. Il est également important que vous vous intéressiez aux autres moteurs de recherche que Google. En effet, chaque moteur peut produire des résultats différents, même pour des termes identiques. En tant que testeur d'intrusion qui mène une reconnaissance, vous devez être aussi rigoureux que possible. Vous serez récompensé par le temps que vous passerez à apprendre à exploiter au mieux les possibilités de recherche de Yahoo, Bing, Ask, Dogpile et les autres.

Enfin, vous devez savoir que ces recherches passives le resteront uniquement pendant les recherches. Si vous vous connectez au système cible (en cliquant sur l'un des liens du résultat), vous repassez en mode actif. Une reconnaissance active sans autorisation préalable peut être considérée comme une activité illégale.

Après que nous avons examiné minutieusement la page web de la cible et mené des recherches exhaustives avec Google et d'autres moteurs de recherche, il est important d'explorer d'autres recoins d'Internet. Les groupes de nouvelles et les BBS (Bulletin Board System) comme UseNet et Google Groupes peuvent se révéler très utiles lors du recueil d'informations sur la cible. Les forums d'aide, les systèmes de discussion et les fonctions de chat en direct avec un représentant de la société peuvent recéler des informations intéressantes. Il n'est pas rare que des personnes se servent des forums d'aide et de discussion pour publier et recevoir de l'aide sur des problèmes techniques. Malheureusement (ou heureusement selon le point de vue), les questions posées par les employés sont souvent très détaillées, avec des informations sensibles et confidentielles. Supposons qu'un administrateur réseau rencontre des difficultés à configurer correctement son pare-feu. Sur les forums publics, il arrive souvent de trouver des discussions au cours desquelles ces administrateurs postent des sections entières de leur fichier de configuration sans les censurer. Pire encore, les billets sont publiés en utilisant l'adresse électronique de la société. Ces informations sont une véritable mine d'or pour n'importe quel pirate.

Même si l'administrateur réseau est suffisamment intelligent pour ne pas fournir tous les détails de la configuration, il est difficile d'obtenir l'aide de la communauté sans laisser involontairement fuiter quelques

informations. En lisant des billets pourtant soigneusement rédigés, il est possible d'obtenir des données sur la version précise d'un logiciel, les modèles de matériels, la configuration courante et d'autres données internes aux systèmes. Tout cela doit être mis de côté pour une future utilisation au cours du test d'intrusion.

Les forums publics constituent une excellente manière de partager des informations et de recevoir une aide technique. Cependant, si vous utilisez ces ressources, faites attention à employer une adresse de courrier électronique relativement anonyme, par exemple sur Gmail ou Hotmail, à la place de votre adresse professionnelle.

La croissance explosive des réseaux sociaux, comme Facebook et Twitter, ouvre de nouvelles portes vers des données sur les cibles. Au cours d'une reconnaissance, il est bon d'employer ces sites à notre avantage. Prenons un exemple fictif qui consiste à mener un test d'intrusion sur une petite entreprise. Votre reconnaissance vous a permis de découvrir que son administrateur réseau dispose d'un compte Twitter, Facebook et Steam. Grâce à une petite ingénierie sociale, vous devenez ami avec l'administrateur peu méfiant et le suivez sur Facebook et Twitter. Après quelques semaines de billets plus ennuyeux les uns que les autres, vous gagnez le jackpot. Il envoie sur Facebook le message suivant : "Super ! Le pare-feu a grillé aujourd'hui sans prévenir personne. Un nouveau va nous être envoyé pendant la nuit. Je sens que

demain sera une longue journée à tout remettre en place."

Un autre exemple pourrait être un technicien qui publie : "J'ai eu un problème avec le dernier correctif de Microsoft. J'ai dû le désinstaller. Je les appellerai au cours de la matinée."

Vous pourriez également voir arriver un message comme : "Je viens de terminer le prochain budget annuel. J'ai l'impression que je vais rester encore un an avec ce serveur Win2K."

Bien que ces exemples puissent sembler un tantinet tirés par les cheveux, vous seriez surpris de constater la quantité d'informations que vous pouvez recueillir en surveillant simplement ce que les employés publient en ligne.



The Harvester

Pendant la phase de reconnaissance, l'outil **The Harvester** se révélera très utile. Il s'agit d'un simple **script Python** très efficace écrit par **Christian Martorella chez Edge Security**. Il permet de cataloguer rapidement et précisément les adresses de courrier électronique et les sous-domaines directement liés à la cible.

Il est important de toujours utiliser la dernière version de The Harvester car de nombreux moteurs de recherche actualisent et modifient régulièrement leurs systèmes. Même une modification subtile dans le comportement d'un moteur de recherche peut rendre inopérants les outils automatisés. Dans certains cas, les moteurs de recherche filtrent les résultats avant de renvoyer les informations. Ils sont également nombreux à mettre en place des techniques de limitation qui tentent d'empêcher les recherches automatisées.

The Harvester peut être employé avec les serveurs de Google, Bing et PGP afin de rechercher des adresses électroniques, des hôtes et des sous-domaines. Il est également compatible avec LinkedIn pour les noms d'utilisateurs. La plupart des gens pensent que leur adresse de courrier électronique présente peu d'intérêt. Nous avons déjà expliqué les dangers de publier des messages sur les forums publics en utilisant une adresse de

messagerie professionnelle, mais il existe bien d'autres risques.

Supposons que, au cours de la reconnaissance, vous découvriez l'adresse électronique d'un employé qui travaille pour l'entreprise cible. En manipulant les informations placées avant le signe "@", nous pouvons générer des noms d'utilisateurs réseau potentiels. Il n'est pas rare que les entreprises utilisent les mêmes noms d'utilisateurs au sein de leur réseau et dans les adresses électroniques. Nous pourrons nous en servir pour tenter des accès exhaustifs à certains services, comme SSH, VPN ou FTP, *que nous découvrirons au cours de la deuxième phase (les scans).

The Harvester est intégré à Kali. La façon la plus rapide d'y accéder consiste à ouvrir une fenêtre de terminal et à exécuter la commande `theHarvester`. Si vous avez besoin du chemin complet du programme et si vous utilisez Kali, The Harvester, comme pratiquement tous les autres outils, se trouve dans le répertoire `/usr/bin/`. Toutefois, n'oubliez pas que l'un des principaux avantages de Kali est qu'il est inutile de préciser le chemin complet pour exécuter ces outils. Il suffit d'ouvrir le terminal et d'entrer la commande de lancement correspondante :

`theHarvester`

Vous pouvez également préciser l'intégralité du chemin :

`/usr/bin/theharvester`

Si vous avez choisi une distribution autre que BackTrack ou Kali, ou si vous ne trouvez pas l'outil qui vous intéresse dans le répertoire indiqué, servez-vous de la commande `locate` pour vous aider à le rechercher. Avant d'invoquer cette commande, vous devez lancer `updatedb`. Pour rechercher l'endroit où est installé The Harvester sur votre système, ouvrez une fenêtre de terminal et saisissez la commande suivante :

`updatedb`

Suivie de :

`locate theharvester`

La commande `locate` peut être très verbeuse, mais un examen attentif de la liste vous aidera à déterminer l'emplacement de l'outil. Nous l'avons mentionné précédemment, sur Kali, la plupart des outils pour les tests d'intrusion se trouvent dans un sous-répertoire de `/usr/bin/`.

Attention

Si vous utilisez un système d'exploitation autre que Kali, vous pouvez télécharger l'outil directement sur le site d'Edge Security à l'adresse <http://www.edge-security.com>. Extrayez ensuite le contenu du fichier tar en exécutant la commande suivante depuis le terminal :

```
tar xf theHarvester
```

Notez le "H" en majuscule. Puisque Linux est sensible à la casse, "theHarvester" et "theharvester" ne sont pas équivalents. Faites attention au nom du fichier exécutable pour savoir si vous devez utiliser un "h" majuscule ou minuscule. En cas d'erreur, un message vous indiquera généralement que le fichier ou le répertoire n'a pas été trouvé. Revoyez alors l'orthographe du nom du fichier. Que vous ayez téléchargé The Harvester ou que vous utilisiez la version déjà installée sur la machine d'attaque, cet outil vous servira à recueillir des informations complémentaires sur la cible. Exécutez la commande

suivante :

```
theHarvester -d syngress.com -l 10 -b all
```

Elle recherche les adresses de messagerie, les sous-domaines et les hôtes qui appartiennent à syngress.com

Whois

Pour recueillir des informations supplémentaires sur une cible, une solution très simple mais efficace consiste à employer Whois. Ce service nous permet d'accéder à des informations précises sur la cible, notamment les adresses IP ou les noms d'hôtes des serveurs DNS (Domain Name System) de la société, ainsi qu'à des informations de contact qui comprennent généralement une adresse et un numéro de téléphone.

Whois est intégré au système d'exploitation Linux. Pour l'utiliser, il suffit d'ouvrir une fenêtre de terminal et d'exécuter la commande suivante :
whois domaine_cible

Par exemple, pour obtenir des informations sur Syngress, saisissez
whois syngress.com.

Il est important de conserver toutes ces informations et de prêter une attention particulière aux serveurs DNS. Si les résultats présentent uniquement les noms des serveurs, nous utiliserons la commande host pour les convertir en adresses IP (nous y reviendrons à la section suivante). La recherche Whois est également possible avec un navigateur web. Il suffit d'aller à l'adresse :

<http://www.whois.net> et d'indiquer la cible dans le champ de saisie
Examinez attentivement les informations présentées. Il peut arriver que les résultats donnent peu de détails. Dans ce cas, il est souvent possible de les trouver en interrogeant les serveurs Whois indiqués dans la sortie de la recherche initiale.

Host

Très souvent, les actions de reconnaissance produiront non pas des adresses IP mais des noms d'hôtes. Lorsque c'est le cas, la commande host se chargera d'en faire la traduction à notre place. Cet outil est intégré à la plupart des systèmes Linux, y compris Kali. Il suffit d'ouvrir une fenêtre de terminal et de saisir la commande suivante :

host nom_hôte_cible

Supposons que nos recherches précédentes nous aient amenés à découvrir un serveur DNS dont le nom d'hôte est ns1.dreamhost.com. Pour convertir celui-ci en une adresse IP, nous saisissons la commande suivante dans un terminal :

host ns1.dreamhost.com

La commande host peut également être employée dans le sens inverse, pour convertir une adresse IP en un nom d'hôte. Voici comment procéder :

host adresse_IP

Avec l'option -a, la sortie devient verbeuse et peut éventuellement révéler des informations supplémentaires. N'hésitez pas à passer du temps à consulter la documentation et les fichiers d'aide de cet outil. Vous pouvez également lire son mode d'emploi en exécutant man host dans une fenêtre de terminal. Ce fichier d'aide vous permettra de vous familiariser avec les différentes options qui vous donneront accès aux différentes fonctionnalités de hosts.

Extraire des informations du DNS

Les serveurs DNS sont des cibles de choix pour les hackers et les testeurs d'intrusion, car ils contiennent généralement des informations de forte valeur. Le DNS est un composant central des réseaux locaux et d'Internet. Il est entre autres responsable de la conversion des noms de domaine en adresses IP. En tant qu'êtres humains, il nous est plus facile de mémoriser google.fr 142.250.75.227. En revanche, les machines préfèrent l'inverse. Le DNS se charge de cette traduction. En tant que testeurs d'intrusion, nous devons nous focaliser sur les serveurs DNS qui appartiennent à notre cible. La raison en est simple. Pour que le DNS fonctionne correctement, il doit connaître à la fois l'adresse IP et le nom de domaine correspondant de chaque ordinateur du réseau. En terme de reconnaissance, obtenir un accès total au serveur DNS d'une entreprise revient à trouver le trésor au pied de l'arc-en-ciel. Ou, peut-être de façon plus précise, cela revient à trouver un plan de la société, avec la liste complète des adresses IP et des noms d'hôtes internes qui appartiennent à la cible. N'oubliez pas que l'un des principaux objectifs de la collecte d'informations est de recueillir des adresses IP qui appartiennent à la cible.

Hormis le trésor, l'intérêt de se concentrer sur le DNS est que, dans de nombreux cas, ces serveurs ont tendance à fonctionner selon le principe "si ça marche, il ne faut surtout pas y toucher".

Les administrateurs réseau peu expérimentés regardent souvent leurs serveurs DNS avec méfiance et défiance. Ils choisissent de les ignorer totalement car ils n'en maîtrisent pas le fonctionnement. Par conséquent, la mise à jour, le changement de configuration ou l'application des correctifs sur les serveurs DNS ne font pas partie des tâches prioritaires. Ajoutez à cela le fait que la plupart des serveurs DNS semblent bénéficier d'une grande stabilité (tant que l'administrateur n'y touche pas) et vous avez là une recette pour un désastre de sécurité. Ces administrateurs ont appris à tort au début de leur carrière que moins ils bricolaienr leurs serveurs DNS, moins ils risquaient de provoquer des dysfonctionnements. En raison du nombre de serveurs DNS mal configurés et non actualisés qui foisonnent aujourd'hui, il est naturel que le testeur d'intrusion suppose que de nombreux administrateurs réseau suivent le grand principe cité précédemment.

Si nos déclarations se vérifient dans un nombre d'entreprises même faible, nous disposons de cibles intéressantes qui ont une forte probabilité d'être non corrigées ou obsolètes. Logiquement, la question suivante est de savoir comment accéder à ce trésor virtuel. Avant que nous puissions démarrer l'examen d'un serveur DNS, nous avons besoin d'une adresse IP. Au cours des tâches de reconnaissance précédentes, nous avons

rencontré plusieurs références au DNS. Certaines d'entre elles correspondaient à des noms d'hôtes, tandis que d'autres étaient des adresses IP. Grâce à la commande host, nous pouvons convertir les noms d'hôtes en adresses IP et ajouter celles-ci à notre liste de cibles potentielles. À nouveau, vous devez vous assurer que les adresses IP recueillies sont couvertes par l'étendue du test.

Nous disposons à présent d'une liste d'adresses IP des serveurs DNS qui appartiennent à notre cible ou qu'elle utilise. Nous pouvons donc commencer l'interrogation du DNS afin d'en extraire des informations.

Bien que cela soit de moins en moins possible, l'une des premières actions consiste à tenter un transfert de zone.

Les serveurs DNS conservent des enregistrements qui mettent en correspondance l'adresse IP et le nom d'hôte pour tous les appareils qu'ils connaissent. Dans de nombreux réseaux, plusieurs serveurs DNS sont déployés afin assurer une redondance ou une répartition de la charge. En conséquence, ces serveurs ont besoin d'un mécanisme pour partager des informations : le transfert de zone. Au cours de ce transfert, également appelé AXFR, un serveur envoie toutes les correspondances hôte-vers-IP qu'il contient à un autre serveur DNS. C'est grâce à ces échanges que la synchronisation des serveurs DNS est assurée.

Même si nous ne parvenons pas à réaliser un transfert de zone, nous devons passer du temps à examiner tous les serveurs DNS qui entrent dans l'étendue du test.



Scans

Au terme de la phase 1, vous devez avoir développé une solide compréhension de la cible et organisé dans le détail les informations recueillies. Ces données comprennent principalement des adresses IP. Rappelez-vous que l'une des dernières étapes de la reconnaissance consiste à créer une liste des adresses IP qui appartiennent à la cible et que vous êtes autorisé à attaquer. Cette liste permet de passer de la phase 1 à la phase 2. Au cours de la première phase, nous avons transformé les informations collectées en adresses IP attaquables. Au cours de la deuxième phase, nous associerons les adresses IP à des ports et à des services ouverts.

Info

Les exemples de ce module seront mis en œuvre à partir de Kali et cibleront une machine virtuelle Windows ou Metasploitable. Après que vous aurez téléchargé et installé Metasploitable, vous aurez probablement besoin de modifier les paramètres réseau dans la configuration de VMware Player de manière à les passer de "bridged" à "NAT". Redémarrez ensuite la machine virtuelle Metasploitable pour arriver à un écran d'ouverture de session comparable à celui de Kali.

Il sera inutile de fournir un nom d'utilisateur et un mot de passe car l'objectif est de compromettre Metasploitable et d'obtenir un accès distant au système.

Il est important de comprendre que le rôle de la plupart des réseaux est d'autoriser au moins une communication entrante et sortante à leur périphérie. Les réseaux totalement isolés, sans connexion à Internet, sans services comme la messagerie électronique ou l'accès au Web, sont aujourd'hui extrêmement rares. Chaque service, connexion ou route vers un autre réseau constitue pour l'assaillant un point d'attaque potentiel.

Les scans ont pour objectif d'identifier les systèmes actifs et les services qui existent sur ces systèmes.

Dans le cadre de notre méthodologie, nous décomposons la phase 2 en quatre étapes distinctes :

1. Déterminer si un système est actif avec des paquets ping.
2. Scanner les ports du système avec **Nmap**.
3. Utiliser le moteur de scripts de Nmap (NSE,Nmap Scripting Engine) pour examiner de façon plus précise la cible.
4. Scanner le système à la recherche de vulnérabilités avec **Nessus**.

Plus loin dans ce module, nous présenterons des outils qui regroupent ces étapes au sein d'une seule procédure. Toutefois, lors de la découverte d'un nouvel outil et de son apprentissage, il est préférable de les réaliser séparément.

L'étape 2.1 consiste à déterminer si un système cible est allumé et s'il est capable de communiquer ou d'interagir avec notre machine. Elle est la moins fiable et doit toujours être suivie des étapes 2.2 à 2.4 quel que soit le résultat du test. Peu importe ce que nous allons découvrir, il faut mener à bien cette étape et noter toutes les machines qui sembleront actives. Pour être honnête, avec l'expérience, vous combinerez probablement les étapes 2.1 et 2.2 en un seul scan réalisé directement avec Nmap.

L'étape 2.2 a pour objectif d'identifier les ports et services qui s'exécutent sur un hôte donné.

Pour faire simple, un port permet à un logiciel, un service ou un réseau de communiquer avec un autre matériel, comme un ordinateur. Il s'agit d'une connexion de données qui permet à un ordinateur d'échanger des informations avec d'autres ordinateurs, logiciels ou appareils. Avant l'interconnexion des ordinateurs et des réseaux, les informations étaient transférées entre les machines en utilisant des supports physiques, comme des disquettes. Dès lors que les ordinateurs ont été connectés à un réseau, ils ont eu besoin d'une solution efficace pour communiquer les uns avec les autres. Elle a pris la forme des ports. En utilisant plusieurs ports, il est possible d'effectuer des communications simultanées sans moment d'attente.

Si vous n'êtes pas familier des ports et des ordinateurs, l'analogie suivante pourra peut-être vous aider. Imaginez que votre ordinateur soit une maison. Il existe plusieurs façons d'y entrer. Chaque ouverture qui permet de pénétrer dans la maison (ordinateur) est comparable à un port, et toutes les entrées permettent au trafic d'entrer et de sortir.

Imaginez que chaque point d'entrée dans la maison soit repéré par un numéro unique. La plupart des visiteurs passeront par la porte principale, mais les propriétaires pourront emprunter la porte du garage. Certaines personnes pénétreront dans la maison par la porte du jardin ou par une fenêtre. D'autres pourraient même passer par une fenêtre de toit ou tenter d'emprunter la chatière !

Quelle que soit la manière dont vous entrez dans votre maison, chacun de ces exemples se calque parfaitement sur les ordinateurs et les ports. Les ports jouent le rôle de passerelles vers votre ordinateur. Certains sont relativement communs et reçoivent un trafic important (la porte d'entrée principale), tandis que d'autres sont plus rarement employés (par les humains), comme la chatière.

De nombreux services réseau répandus s'exécutent sur des numéros de port standard et peuvent donner aux assaillants des indications sur le fonctionnement du système cible.

Info

Compromettre une machine et l'utiliser comme tremplin pour attaquer une autre machine se nomme "**pivoter**". Cette technique est souvent employée lorsque la machine cible est connectée à un réseau mais sans être atteignable directement depuis notre emplacement.

Les hackers et les testeurs d'intrusion auront peut-être à pivoter à plusieurs reprises avant d'atteindre la cible initiale.

Les périphériques de périmètre sont des ordinateurs, des serveurs, des routeurs, des pare-feu ou d'autres appareils qui se situent en périphérie d'un réseau protégé. Ils servent d'intermédiaires entre les ressources internes protégées et les réseaux externes comme Internet.

Comme nous l'avons mentionné, nous commençons généralement par scanner les périphériques de périmètre afin de découvrir des faiblesses ou des vulnérabilités qui nous permettront d'ouvrir une porte sur le réseau.

Ping et balayage ping

Un ping est un type de paquet réseau particulier appelé paquet ICMP. Le principe consiste à envoyer un type de trafic réseau spécial, appelé paquet de requête ICMP Echo, à une interface spécifique sur un ordinateur ou un périphérique réseau. Si l'appareil (et la carte réseau associée) qui reçoit le paquet ping est allumé et est configuré pour répondre, il renvoie à la machine d'origine un paquet de réponse ICMP Echo. Cela nous permet non seulement de savoir qu'un hôte est actif et accepte un trafic, mais également de connaître le temps total qu'il faut au paquet pour atteindre la cible et revenir. Cet échange indique également les pertes de paquets, et nous pouvons nous en servir pour estimer la fiabilité d'une connexion réseau. Pour émettre un paquet ping à partir de votre machine Linux, ouvrez une fenêtre de terminal et exécutez la commande suivante :

ping ip_cible

Vous devez remplacer ip_cible par l'adresse IP ou le nom d'hôte de la machine à laquelle les paquets ping doivent être envoyés.

Exemple : **ping google.fr**

Concentrons-nous sur la troisième ligne, qui commence par "**64 bytes from**". Elle nous indique que notre paquet de requête ICMP Echo a bien atteint la cible et que celle-ci a répondu par un paquet ICMP Reply à notre machine. Comme indiqué, la taille du paquet de la réponse est de **64 octets**. La partie "**from par03s12-in-f24.1e100.net (173.194.45.56):**" précise le nom d'hôte et l'adresse IP qui a répondu à notre ping sur google.fr. La partie "**icmp_seq=**" indique l'ordre du paquet, "**ttl=54**" correspond à une valeur de durée de vie (utilisé pour déterminer le nombre de sauts que le paquet effectuera avant d'expirer automatiquement) et "**time=29.9 ms**" correspond à la durée totale du voyage des paquets vers

et depuis la cible. Après que nous avons arrêté l'exécution de la commande ping, nous obtenons des statistiques, notamment le nombre de paquets transmis, les paquets perdus et des informations de durée. Si la cible est éteinte ou si elle bloque les paquets ICMP, vous verrez une perte de paquets de 100 % ou un message qui signale que l'hôte est inatteignable (selon le système d'exploitation). Si la connexion réseau est de mauvaise qualité, vous pourrez constater que des requêtes arrivent à expiration et que d'autres obtiennent des réponses.

Cela provient généralement de problèmes réseau sur le système destinataire. Maintenant que vous connaissez le fonctionnement de la commande ping, voyons comment l'exploiter en tant que hacker. Puisque les paquets ping peuvent nous aider à déterminer si un hôte est actif, nous utilisons ping comme un service de découverte d'hôtes. Cependant, lancer cette commande pour chaque machine potentielle, même sur un petit réseau, se révélera inefficace. Heureusement, il existe plusieurs outils qui permettent d'effectuer des balayages ping. Il s'agit d'une suite de ping envoyés automatiquement à une plage d'adresses IP.

La solution la plus simple pour effectuer un balayage ping est fournie par **FPing**. Cet outil est déjà installé sur Kali et s'exécute depuis le terminal (il est disponible en téléchargement pour Windows). Voici comment l'invoquer :

```
fping -a -g 216.58.214.67 216.58.214.67 > hôtes.txt
```

L'option **-a** permet d'inclure dans la sortie uniquement les hôtes actifs. Le rapport final sera ainsi plus clair et plus facile à consulter. L'option **-g** permet de définir la plage des adresses IP à balayer. Nous devons indiquer l'adresse IP de début et celle de fin.



Scans TCP Connect avec Nmap

Notre première action sera un scan TCP Connect. Ce type de scan est souvent considéré comme le plus simple et le plus stable car Nmap tente d'effectuer une connexion en trois étapes complète sur chaque port indiqué. Puisque ce scan va jusqu'au bout de la connexion en trois étapes et la termine ensuite proprement, il est peu probable que le système cible soit submergé et se plante.

Sans préciser une plage de ports, Nmap scannera les 1 000 ports les plus utilisés. À moins que vous ne soyez vraiment pressé, il est fortement recommandé de scanner non pas uniquement ces 1 000 ports mais tous. En effet, il arrive souvent que les administrateurs un peu rusés tentent de masquer un service en l'exécutant sur un port non standard. Pour effectuer un scan de l'intégralité des ports, vous devez ajouter l'option **-p-** lors de l'exécution de Nmap. L'option **-Pn** est également conseillée car elle désactive la découverte des hôtes et oblige Nmap à scanner chaque système comme s'il était actif. Cela sera très utile pour découvrir des systèmes et des ports supplémentaires à côté desquels nous serions sinon passés.

Pour effectuer un scan TCP Connect, il suffit d'exécuter la commande suivante depuis un terminal :

```
nmap -sT -p- -Pn 192.168.56.102
```

Prenons un peu de temps pour étudier cette commande. Le premier mot, nmap, déclenche l'exécution du scanner de ports Nmap. La deuxième partie, **-sT**, indique à Nmap d'effectuer un scan TCP Connect. Plus précisément, **-s** est utilisé pour indiquer que nous allons préciser le type scan à effectuer, tandis que **T** correspond au type TCP Connect. Nous ajoutons **-p-** pour demander un scan de tous les ports à la place des 1 000 par défaut. La dernière option, **-Pn**, évite la phase de découverte des hôtes et scanne toutes les adresses comme si le système était actif et répondait aux requêtes ping.

Très souvent, le scan doit se faire sur l'intégralité d'un sous-réseau ou une plage d'adresses IP. Dans ce cas, il suffit de préciser à Nmap la plage des adresses en ajoutant l'octet de la dernière adresse IP :

```
nmap -sT -p- -Pn 192.168.56.1-254
```

Cette commande demande à Nmap d'effectuer un scan des ports sur tous les hôtes dont les adresses IP se situent entre 192.168.56.1 et 192.168.56.254. À l'instar des balayages ping, cette technique peut énormément améliorer votre productivité au cours des opérations de scan.

Si le scan doit concerner plusieurs hôtes dont les adresses IP ne se suivent pas, il suffit de créer un fichier texte et d'y indiquer chaque adresse sur sa propre ligne. Pour passer ce fichier à Nmap, il faut alors ajouter l'option **-iL chemin_du_fichier**. Nous pouvons ainsi scanner tous les hôtes cibles à partir d'une seule commande. Lorsque c'est possible, il est préférable de créer un seul fichier texte qui comprend toutes les adresses IP cibles. La plupart des outils que nous présenterons disposent en effet d'une option ou d'un mécanisme capable de lire un tel fichier texte. Grâce à cette liste, le travail de saisie sera moindre et, plus important encore, elle permet de réduire les risques de scan sur une cible non autorisée en raison d'une erreur de saisie dans une adresse.



Introduction à la sécurité en ligne

Objectifs :

Comprendre les risques de sécurité en ligne.

Apprendre à protéger vos données en ligne.

Apprendre à identifier les menaces de sécurité en ligne.

Apprendre à utiliser des outils pour renforcer votre sécurité en ligne.

Activités :

1. Expliquez les différents risques de sécurité en ligne, tels que les virus, les logiciels malveillants, les attaques de phishing.
2. Expliquez des conséquences possibles de l'exposition de vos données en ligne, comme le vol d'identité, le piratage de compte.
3. Donnez des exemples concrets de problèmes de sécurité en ligne, tels que des histoires récentes de piratage de données.

Identifiez les menaces de sécurité en ligne

Distribuez des exemples d'e-mails de phishing, de faux sites web et de messages suspects sur les réseaux sociaux. Identifiez les éléments de ces messages qui indiquent qu'ils sont suspects ou dangereux.

Apprenez à protéger vos données en ligne

Donnez des conseils pour créer des mots de passe forts et uniques.

Expliquez comment configurer la vérification en deux étapes sur les comptes en ligne.

Quels sont les outils disponibles pour protéger votre vie privée en ligne ?

Pratiquez la sécurité en ligne

Donnez des exemples de scénarios de sécurité en ligne, tels que l'utilisation d'un Wi-Fi public ou le partage de données avec un ami en ligne.

Expliquez la meilleure façon de se protéger dans chaque situation.

Donnez des conseils pour éviter les pièges en ligne, tels que l'utilisation d'un bloqueur de publicités et la vérification des URL avant de cliquer sur un lien.

Conclusion

Récapitulez les éléments clés de la sécurité en ligne et les mesures à prendre pour se protéger.

PEREZ MOTA Javier
Formateur

Introduction à la sécurité en ligne

Objectifs :

Comprendre les risques de sécurité en ligne.

Apprendre à protéger vos données en ligne.

Apprendre à identifier les menaces de sécurité en ligne.

Apprendre à utiliser des outils pour renforcer votre sécurité en ligne.

Activités :

1. Expliquez les différents risques de sécurité en ligne, tels que les virus, les logiciels malveillants, les attaques de phishing.

Ce sont des programmes malveillants qui infectent les fichiers d'un ordinateur qui peuvent causer des pertes de fps, aussi les virus peuvent se propager par des sites web et dans les e-mails où infecter par un téléchargements des logiciels malveillants.

2. Expliquer des conséquences possibles de l'exposition de vos données en ligne, comme le vol d'identité, le piratage de compte.

- Le vol d'identité peut se produire lorsque une personne utilise vos informations personnelles pour essayer de commettre des fraudes ou des crimes en utilisant votre nom.
- Il y a aussi le piratage de comptes se produit lorsqu'une personne entre dans votre compte en ligne sans votre autorisation, les pirates peuvent vous voler des informations comme vos coordonnées bancaires ou vos informations de connexion.
- Le harcèlement en ligne, lorsque vos données personnelles sont exposées en ligne, peuvent vous intimider. Cela peut inclure des menaces ou des harcèlements sexuels où en utilisant la cyberattaques.
- Les pertes des données personnelles sont sensibles, si vous stockez des informations en ligne telles que les informations

médicales, où les coordonnées bancaires, cartes de crédit. Une exposition peut vous entraîner à une perte et elle peut vous mettre en danger financière et votre vie privée.

Il est préférable de mettre en place les facteurs de doubles authentifications pour protéger toutes vos données personnelles pour ne pas se faire pirater.

3. Donnez des exemples concrets de problèmes de sécurité en ligne, tels que des histoires récentes de piratage de données.

- En 2020 il y a un géant des logiciels malveillants SolarWinds a été victime d'une cyberattaque massive qui a commis des milliers d'entreprises gouvernementales de l'État américain.
- En 2019 Capital One c'était une grande entreprise des services financiers qui a subi violation des données et qui a exposé les informations personnelles à plus de 100 millions de clients y compris les numéros des sécurités sociales et les numéros comptes bancaires.
- En 2017, Equifax était l'une des principales agences sociales d'évaluation du crédit as été victime d'une violations des données massives qui a commis les informations personnelles plus de 149 millions de personnes y compris leurs noms, dates de naissances et leur numéros de sécurité sociaux.
- En 2016 il y avait Yahoo as relevé qu'elle avait été victime d'un piratage.

Identifiez les menaces de sécurité en ligne

Distribuez des exemples d'e-mails de phishing, de faux sites web et de

messages suspects sur les réseaux sociaux. Identifiez les éléments de ces messages qui indiquent qu'ils sont suspects ou dangereux.

Les menaces de sécurité en ligne sont nombreuses et peuvent prendre des formes. Voici quelques exemples courants de menaces de sécurité ci-dessous

Il y a le phishing qui commet une fraude technique qui vise à tromper l'utilisateur pour qu'il divulgue des informations personnelles ou financières en se faisant passer pour une entreprise de confiance ou une organisation légitime. Voici un exemple e-mails de phishing :

"Sujet: Votre compte bancaire est en danger!

Cher client,

Nous avons remarqué une activité suspecte sur votre compte bancaire. Pour des raisons de sécurité, nous vous demandons de vérifier vos informations en cliquant sur le lien ci-dessous et en vous connectant à votre compte.

Lien suspect: [Insérer un lien suspect ici]

Nous vous remercions de votre coopération.

Cordialement,

L'équipe de la banque"

Apprenez à protéger vos données en ligne

Donnez des conseils pour créer des mots de passe forts et uniques. Expliquez comment configurer la vérification en deux étapes sur les comptes en ligne.

Il faut bien mettre un mot de passe bien robuste pour pas se faire pirater je vais vous montrer des exemples ci-dessous : aussi je vais vous montrer comment faire pour la configuration en deux étapes voici les étapes générales :

1. Utilisez une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux. Évitez les mots de passe évidents tels que "123456" ou "motdepasse".
 2. Utilisez des phrases plutôt que des mots simples. Par exemple, "J'aime manger des bananes tous les jours" peut être transformé en "J@im3M@dBT0usL3sJ0urs".
 3. Utilisez des mots de passe différents pour chaque compte en ligne.
 4. Évitez d'utiliser des informations personnelles telles que votre nom, date de naissance, adresse ou numéro de téléphone comme partie de votre mot de passe.
-
5. Connectez-vous à votre compte en ligne et accédez aux paramètres de sécurité.
 6. Trouvez l'option "Vérification en deux étapes" ou "Authentification à deux facteurs" et activez-la.
 7. Choisissez le type d'authentification en deux étapes que vous préférez. Les options courantes incluent les codes envoyés par SMS, les applications d'authentification telles que Google Authenticator ou Authy, ou les clés de sécurité physique.
 8. Suivez les instructions pour configurer l'authentification en deux étapes en fonction du type choisi.

La vérification en deux étapes ajoute une sous-couche de sécurité supplémentaire à vos comptes en ligne en exigeant une deuxième forme d'identification, généralement un code unique, en plus de votre mot de passe pour accéder à votre compte. Cela rend beaucoup plus difficile pour les pirates informatiques d'accéder à vos informations, même s'ils ont réussi à obtenir votre mot de passe.

Quels sont les outils disponibles pour protéger votre vie privée en ligne ?

Pratiquez la sécurité en ligne

Donnez des exemples de scénarios de sécurité en ligne, tels que l'utilisation d'un Wi-Fi public ou le partage de données avec un ami en ligne. Expliquer la meilleure façon de se protéger dans chaque situation. Donnez des conseils pour éviter les pièges en ligne, tels que l'utilisation d'un bloqueur de publicités et la vérification des URL avant de cliquer sur un lien.

Il y a aussi le VPN (Virtual Private Network) qui crée les tunnels cryptés entre vos ordinateurs pour pouvoir voir ce que vous faites sur internet aussi les navigateurs web (Brave, Firefox) offrent leur fonctionnalité de confidentialité telles que le blocage des publicités et les trackers avec leurs logiciels de blocage de publicités des programmes tels que (alguard add block ...) peuvent être utilisés pour bloquer les publicités en ligne. La messagerie chiffré : l'utilisation de messagerie comme Signal ou Whats'ap peut protéger la confidentialité de vos communications.

Pour éviter les pièges en ligne voici quelques conseils ci-dessous :

1. Utilisez un bloqueur de publicités : Les publicités en ligne peuvent contenir des logiciels malveillants, des liens trompeurs ou des arnaques. Utilisez un bloqueur de publicités pour éviter ces risques.
2. Vérifiez les URL avant de cliquer sur un lien : Les liens frauduleux peuvent vous rediriger vers des sites malveillants ou vous inciter à télécharger des logiciels malveillants. Vérifiez l'URL avant de cliquer sur un lien pour vous assurer qu'il est légitime.

Pour pratiquer la sécurité en ligne voici quelques exemples de scénarios de sécurité en ligne et la meilleure façon de se protéger dans chaque situation de piratage :

1. Utilisation d'un Wi-Fi public : Évitez de vous connecter à des sites Web qui contiennent des informations personnelles ou financières importantes lors de l'utilisation d'un Wi-Fi public. Utilisez un VPN pour chiffrer votre trafic et éviter que les autres utilisateurs du réseau ne voient vos informations.
2. Partage de données avec un ami en ligne : Évitez de partager des informations sensibles en ligne, même avec des amis. Utilisez des plates-formes de partage de fichiers sécurisées et chiffrées, telles que Dropbox ou Google Drive, pour protéger vos données.

Conclusion

Récapitez les éléments clés de la sécurité en ligne et les mesures à prendre pour se protéger.

En conclusion il faut bien penser à bien mettre un mot de passe bien robuste pour empêcher les pirates de pirater toutes vos données personnelles comme carte de crédit, comptes bancaires... Il faut penser à mettre authentification à deux facteurs pour pas se faire pirater comme ça les pirates auront du mal à récupérer vos données personnelle.



TP de cybersécurité : Analyse d'attaques informatiques

Objectifs :

Comprendre les méthodes d'attaque informatique.

Apprendre à analyser les attaques informatiques.

Apprendre à se protéger contre les attaques informatiques

Activités :

- Expliquez les différentes menaces de sécurité informatique, telles que les attaques par déni de service, les attaques de phishing, les attaques de logiciels malveillants.
- Expliquez les conséquences possibles des attaques informatiques, telles que la perte de données, la violation de la vie privée.
- Donnez des exemples concrets d'attaques informatiques, telles que des histoires récentes de piratage de données.

Analyse d'attaques informatiques

- Distribuez des exemples d'attaques informatiques, tels que des journaux d'événements de système, des captures de paquets de réseau.
- Analysez ces exemples pour identifier les méthodes d'attaque et les vecteurs d'attaque.
- Expliquez les outils disponibles pour analyser les attaques informatiques, tels que les systèmes de gestion des événements de sécurité et les outils de détection d'intrusion.

Pratique de la sécurité informatique

- Donnez des exemples de scénarios de sécurité informatique, tels que la mise à jour des logiciels, la configuration du pare-feu.
- Réfléchissez à la meilleure façon de se protéger dans chaque situation.

- Expliquez les mesures à prendre pour éviter les attaques informatiques, telles que l'utilisation de logiciels antivirus et de pare-feu, la mise à jour régulière des logiciels.

Création d'un plan de sécurité informatique

- Créez un plan de sécurité informatique pour une entreprise ou une organisation.
- Le plan devrait inclure des mesures pour protéger les données de l'organisation, tels que la configuration du pare-feu, la formation des employés, la mise en place de politiques de sécurité.
- Incluez les mesures pour détecter et répondre aux attaques informatiques.

Conclusion

Récapitez les éléments clés de la sécurité informatique et les mesures à prendre pour se protéger contre les attaques informatiques.

PEREZ MOTA Javier
Formateur

TP de cybersécurité : Analyse d'attaques informatiques

Objectifs :

Comprendre les méthodes d'attaque informatique.

Apprendre à analyser les attaques informatiques.

Apprendre à se protéger contre les attaques informatiques

Activités :

- Expliquez les différentes menaces de sécurité informatique, telles que les attaques par déni de service, les attaques de phishing, les attaques de logiciels malveillants.

Le déni de service (DDoS) sont des attaques qui consistent à spammer un site avec plusieurs requêtes ce qui fait souvent planter. Le phishing lui usurpe l'identité d'un proche ou d'un organisme pour vous prélever des données via des liens. Le malwares lui qui est souvent installer sur votre appareil grâce au phishing pour prendre le contrôle de votre appareil.

- Expliquez les conséquences possibles des attaques informatiques, telles que la perte de données, la violation de la vie privée.

Les pertes des données personnelles sont sensibles ,si vous stockez des informations en ligne telles que les informations médicales, où les coordonnées bancaires, cartes de crédit. Une exposition peut vous entraîner à une perte et elle peut vous mettre en danger financière et votre vie privée.

- Donnez des exemples concrets d'attaques informatiques, telles que des histoires récentes de piratage de données.

En 2020 il y a un géant des logiciels malveillants Solar Winds a été victime d'une cyberattaque massive qui a commis des milliers d'entreprises gouvernementales de l'État américain.

Piratage de Colonial Pipeline : En mai 2021, le Colonial Pipeline, qui fournit près de la moitié du carburant de la côte est des États-Unis, a été piraté. Les pirates ont réussi à bloquer l'accès au système informatique de la société et ont demandé une rançon en échange d'un accès à nouveau fonctionnel.

Les pirates ont chiffré les systèmes informatiques de l'entreprise et ont demandé une rançon pour leur libération.

Attaque de ransomware contre Kaseya : En juillet 2021, un groupe de pirates informatiques a attaqué Kaseya, une entreprise qui fournit des logiciels de gestion informatique à des milliers d'entreprises.

Analyse d'attaques informatiques

- Distribuez des exemples d'attaques informatiques, tels que des journaux

Voici deux exemples des attaques informatiques dans les journaux :

Attaque de phishing contre Google :

1. En janvier 2021, des pirates ont lancé une attaque de phishing contre les utilisateurs de Gmail et Google Drive, utilisant des messages d'hameçonnage pour tenter de voler des informations de connexion et d'accéder à des comptes Google.

2. Attaque contre l'Université de Californie à San Francisco :

En juin 2021, l'Université de Californie à San Francisco (UCSF) a révélé avoir été victime d'une attaque de ransomware en juin 2020. Les pirates ont chiffré les données de l'université et ont demandé une rançon en échange de leur libération.

d'événements de système, des captures de paquets de réseau.

- Analysez ces exemples pour identifier les méthodes d'attaque et les vecteurs d'attaque.

Attaque contre SolarWinds :

Méthode d'attaque : compromission de logiciels (supply chain attack)

1. Vecteur d'attaque : les pirates ont compromis une mise à jour de logiciel distribuée par SolarWinds, ce qui leur a permis d'accéder aux systèmes des clients de l'entreprise.

Attaque contre le Colonial Pipeline :

Méthode d'attaque : ransomware

2. Vecteur d'attaque : les pirates ont exploité une vulnérabilité dans les systèmes informatiques de l'entreprise pour chiffrer les données et demander une rançon.

Attaque contre Kaseya :

Méthode d'attaque : ransomware

3. Vecteur d'attaque : les pirates ont exploité une vulnérabilité dans le logiciel de gestion informatique de Kaseya pour chiffrer les données de ses clients et demander une rançon.

• Expliquez les outils disponibles pour analyser les attaques informatiques, tels que les systèmes de gestion des événements de sécurité et les outils de détection d'intrusion.

Les outils d'analyse sont

- les pare-feux
- les antivirus
- les services à clé privée

Les outils de détection d'intrusion en deux grande catégories comme les détection par signature et détection par anomalie

Pratique de la sécurité informatique

• Donnez des exemples de scénarios de sécurité informatique, tels que la mise à jour des logiciels, la configuration du pare-feu.

Voici quatre exemples de scénarios de sécurité informatique, tels que la mise à jour des logiciels, la configuration du pare-feu ci-dessous :

1. Mise à jour des logiciels : Il est essentiel de maintenir tous les logiciels utilisés à jour pour éviter l'exploitation de vulnérabilités

connues. Les mises à jour incluent souvent des correctifs de sécurité pour combler les failles de sécurité.

2. Configuration du pare-feu : Un pare-feu est un élément essentiel de la sécurité du réseau. Il peut être configuré pour bloquer l'accès non autorisé à un réseau ou à un ordinateur, en limitant le trafic entrant et sortant.
3. Utilisation de mots de passe forts : Les mots de passe faibles peuvent être facilement devinés ou craqués par les pirates. Il est important d'utiliser des mots de passe forts, avec une combinaison de lettres majuscules et minuscules, de chiffres et de symboles.
4. Utilisation de l'authentification à deux facteurs : L'authentification à deux facteurs est une mesure de sécurité supplémentaire qui nécessite une deuxième forme d'identification, en plus du mot de passe, pour accéder à un compte.

- Réfléchissez à la meilleure façon de se protéger dans chaque situation.

Voici quelques conseils pour se protéger dans chaque situation :

1. Protection contre les attaques de phishing : Il est important d'être attentif aux emails suspects, de ne pas cliquer sur les liens ou pièces jointes non sollicités, de ne pas fournir d'informations personnelles ou financières à moins d'être certain de la légitimité de l'expéditeur.

2. Protection contre les attaques de logiciels malveillants : Pour se protéger contre les logiciels malveillants, il est recommandé de maintenir tous les logiciels à jour, d'installer des logiciels antivirus et des pare-feux, d'être prudent lors de l'installation de nouveaux logiciels.

- Expliquez les mesures à prendre pour éviter les attaques informatiques, telles que l'utilisation de logiciels antivirus et de pare-feu, la mise à jour régulière des logiciels.

Pour être protéger il faut toujours avoir un bon FAI(fournisseur d'accès d'Internet), connaître et repérer le phishing et protéger ces accès physique et surtout à distance de ces appareils.

Création d'un plan de sécurité informatique

- Créez un plan de sécurité informatique pour une entreprise ou une organisation.
- Le plan devrait inclure des mesures pour protéger les données de l'organisation, tels que la configuration du pare-feu, la formation des employés, la mise en place de politiques de sécurité.
- Incluez les mesures pour détecter et répondre aux attaques informatiques.

Voici le plan de sécurité informatique pour une entreprise ou une organisation ci -dessous :

1. Mise en place de politiques de sécurité : Élaborer des politiques de sécurité informatique solides qui couvrent tous les aspects de la sécurité, y compris l'utilisation des données, l'accès aux ressources, la gestion des appareils et des réseaux, et la gestion des incidents.
2. Sauvegarde et récupération des données : Mettre en place une stratégie de sauvegarde et de récupération des données pour s'assurer que toutes les données sont protégées contre les pertes et les dommages.

3. Surveillance des activités suspectes : Installer des outils de surveillance des activités pour détecter les activités suspectes et les attaques en temps réel.

Enfin, il est important de réévaluer régulièrement le plan de sécurité informatique pour s'assurer qu'il reste efficace et adapté aux évolutions des menaces et des technologies.

Conclusion

Récapitez les éléments clés de la sécurité informatique et les mesures à prendre pour se protéger contre les attaques informatiques.

En conclusion, pour avoir les clés de la sécurité il faut avoir les cinq points : mise à jour des logiciels, configuration du pare-feu, utilisation de mots de passe forts, utilisation de l'authentification à deux facteurs et avoir une bonne connexion sécurisée.



TP : Détection et réponse aux cyberattaques

Objectifs :

Le but de ce TP est de comprendre comment les cyberattaques peuvent affecter les entreprises et comment détecter et répondre à ces attaques.

Tâches :

- **Introduction aux types de cyberattaques** - comprendre les différents types de cyberattaques, tels que les attaques par phishing, les attaques par déni de service distribué (DDoS), les attaques de logiciels malveillants.
- **Analyse des attaques** - travail en équipe pour analyser des exemples d'attaques de sécurité. Vous devez comprendre comment les attaques ont été lancées, comment elles ont réussi et quelles ont été les conséquences pour l'entreprise.
- **Détection des cyberattaques** - Vous devez apprendre à détecter les signes d'une cyberattaque en cours. Vous pouvez vous concentrer sur la surveillance des journaux système, l'utilisation d'outils de détection de logiciels malveillants et la mise en place de systèmes d'alerte.
- **Réponse aux cyberattaques** - Vous devez apprendre à répondre aux cyberattaques en cours. Vous devez comprendre comment arrêter l'attaque, comment minimiser les dégâts et comment restaurer les systèmes affectés.
- **Prévention des cyberattaques futures** - Vous devez travailler en équipe pour mettre en place des mesures de sécurité pour prévenir les cyberattaques futures. Vous pouvez vous concentrer sur la mise à jour des logiciels de sécurité, la formation du personnel, la mise en place de politiques de sécurité solides.
- **Présentation et discussion** - Les équipes doivent présenter leurs résultats et discuter des différentes mesures de sécurité qu'ils ont mises en œuvre.

Matériel :

- Des présentations PowerPoint ou des documents PDF pour chaque section.
- Des exemples d'attaques de sécurité pour l'analyse
- Des outils en ligne pour la détection de logiciels malveillants et la surveillance des journaux système
- Des guides de bonnes pratiques de sécurité pour la prévention des cyberattaques

PEREZ MOTA Javier
Formateur

Objectifs :

Le but de ce TP est de comprendre comment les cyberattaques peuvent affecter les entreprises et comment détecter et répondre à ces attaques.

Tâches :

- Introduction aux types de cyberattaques - comprendre les différents types de cyberattaques, tels que les attaques par phishing, les attaques par déni de service distribué (DDoS), les attaques de logiciels malveillants.

Les différents types de piratages ou de cyberattaques sont :

Le phishing: Le fait de se faire passer pour une société fictive ou réelle

Pour collecter données bancaires et de vie privée

Les virus : comme les ransomware :

Qui mettent à genoux les pare feu et infectent la machine

Ou les trojan (ou chevaux de troie)

Qui sont des fichiers cleans en apparence mais dangereux si exécutés

Les malwares :

Qui parasite les fichiers système les rendant inactifs ou les supprimant

Ils existent des black hats qui piratent les bases de données de grandes entreprises pour récupérer adresses mail et identifiants

- Analyse des attaques - travail en équipe pour analyser des exemples d'attaques de sécurité. Vous devez comprendre comment les attaques ont été lancées, comment elles ont réussi et quelles ont été les conséquences pour l'entreprise.

Les cyberattaques utilisant le phishing se déroulent comme suit

Le Brouteur ou Black hat : crée un compte et un site internet d'une entreprise bidon ou réelles

Il contacte une victime par sa boîte mail et lui demande une fausse vérification d'identité sur son site

Puis une fois que la victime a entré ses infos perso et bancaire il copie – colle les info et peut débiter et utiliser son email piraté ou ses chiffres et son code de CB pour faire des achats

Pour le wannacry

L'arnaqueur injecte via un fichier .bat un programme qui bloque le pc et affiche une demande de rançon le plus souvent en BTC

Si la victime ne « paye » pas la rançon alors les fichiers systèmes seront supprimés et les activités en ligne de l'utilisateur dévoilées

Pour les malware le hacker utilise un programme en .exe qui se fait passer pour un logiciel ou un jeu

Le malware si executé peut detruire le pc via ses fichier systeme ou infecter un reseaux entreprise

Les attaques de sécurité sont des tentatives malveillants visant à accéder à donnés sans leur autorisation Il existe de nombreuses façons dont ces attaques peuvent être lancer chacune ayant ses propres méthodes et leurs conséquences ci dessous :

Elles regroupent des types d'attaque comme le phishing, les wannacry et les malwares mais aussi les attaques de grande ampleur comme celle d'amazon de 2018

- Détection des cyberattaques - Vous devez apprendre à détecter les signes d'une cyberattaque en cours.Vous pouvez vous concentrer sur la surveillance des journaux système, l'utilisation d'outils de détection de logiciels malveillants et la mise en place de systèmes d'alerte. En effet, il est important de savoir détecter les signes d'une cyberattaque en cours pour pouvoir agir rapidement et minimiser les dommages potentiels. Voici quelques éléments clés à surveiller :

Surveillez les journaux des systèmes qui contiennent des informations précieuses sur les activités du système, notamment les tentatives de connexions infructueuses sur les erreurs de connexions et les activités suspectes. Il est important de surveiller régulièrement ces journaux pour détecter toute activité inhabituelle.

Utilisez des outils de détection de logiciels malveillants : il existe de nombreux outils de détection de logiciels malveillants disponibles sur le marché, tels que les logiciels antivirus et les scanners de vulnérabilités. Ces outils peuvent aider à détecter les logiciels malveillants et les vulnérabilités du système qui pourraient être exploitées par les cybercriminels.

Mettez en place des systèmes d'alerte : des systèmes d'alerte peuvent être mis en place pour alerter les équipes de sécurité dès qu'une activité suspecte est détectée

sur le réseau ou sur un système spécifique. Ces systèmes peuvent être configurés pour envoyer des alertes par e-mail, SMS ou notification en temps réel.

- Réponse aux cyberattaques - Vous devez apprendre à répondre aux cyberattaques en cours. Vous devez comprendre comment arrêter l'attaque, comment minimiser les dégâts et comment restaurer les systèmes affectés.

Les réponses aux cyberattaques est une étape critique pour minimiser les dommages et réduire l'impact sur les systèmes et les données. Voici les cinq étapes clés à suivre lorsqu'une cyberattaque est en cours :

1. Arrêtez l'attaque : La première étape consiste à arrêter l'attaque pour éviter tout autre dommage potentiel. Cela peut impliquer de déconnecter des ordinateurs ou des réseaux spécifiques du reste du réseau, d'arrêter des processus ou de supprimer des fichiers infectés.
2. Évaluez les dégâts : Une fois l'attaque arrêtée, il est important d'évaluer les dégâts et de déterminer l'étendue des dommages. Il est possible que les données aient été volées ou corrompues, que les systèmes aient été endommagés ou que les comptes aient été compromis.
3. Isoler et sécuriser les systèmes affectés : Les systèmes affectés doivent être isolés du reste du réseau pour éviter toute contamination supplémentaire. Les mesures de sécurité doivent être renforcées pour minimiser les risques de nouvelles attaques. Les sauvegardes des données doivent être vérifiées et restaurées si nécessaire.
4. Notifyez les autorités et les parties prenantes : Si les données personnelles ont été volées ou compromises, il est important de notifier les autorités compétentes, ainsi que les clients, les fournisseurs et les partenaires concernés. Les autorités peuvent fournir des conseils sur les mesures à prendre et les parties prenantes peuvent prendre des mesures pour protéger leurs propres systèmes.
5. Analysez l'attaque et apprenez-en : Après l'incident, une analyse détaillée de l'attaque doit être menée pour comprendre comment elle s'est produite et comment elle peut être évitée à l'avenir. Les leçons apprises doivent être utilisées pour renforcer les mesures de sécurité et réduire les risques de futures cyberattaques.

- Prévention des cyberattaques futures - Vous devez travailler en équipe pour mettre en place des mesures de sécurité pour prévenir les cyberattaques futures. Vous pouvez vous concentrer sur la mise à jour des logiciels de sécurité, la formation du personnel, la mise en place de politiques de sécurité solides.

La prévention des cyberattaques est une tâche continue qui nécessite une collaboration étroite entre les équipes de sécurité informatique, les employés et les parties prenantes concernées. Voici cinq étapes clés à prendre pour prévenir les cyberattaques du futurs :

1. Mettez à jour les logiciels de sécurité : Les logiciels de sécurité, tels que les antivirus, les pare-feu et les logiciels de détection de logiciels malveillants, doivent être régulièrement mis à jour pour rester efficaces contre les nouvelles menaces. Les correctifs de sécurité doivent également être installés dès qu'ils sont disponibles.
2. Formez le personnel : Les employés doivent être formés à la sécurité informatique pour éviter les erreurs humaines qui pourraient exposer l'entreprise à des cyberattaques. La formation doit inclure la sensibilisation aux attaques par phishing, aux mots de passe sécurisés et aux bonnes pratiques de navigation sur Internet.
3. Mettez en place des politiques de sécurité solides : Des politiques de sécurité strictes doivent être mises en place pour guider les employés sur la façon de traiter les informations sensibles et d'utiliser les systèmes informatiques. Les politiques doivent inclure des mesures de sécurité telles que l'authentification à deux facteurs, la sauvegarde régulière des données et la limitation de l'accès aux informations sensibles.
4. Utilisez des outils de sécurité avancés : Les outils de sécurité avancés, tels que la détection des menaces en temps réel et la protection des points de terminaison, peuvent aider à prévenir les attaques de logiciels malveillants et les tentatives d'intrusion.
5. Effectuez des audits de sécurité réguliers : Les audits de sécurité réguliers peuvent aider à identifier les vulnérabilités du système et les mesures de sécurité qui doivent être renforcées. Les audits doivent être effectués par des professionnels de la sécurité informatique pour garantir l'efficacité et l'objectivité de l'analyse.

- Présentation et discussion - Les équipes doivent présenter leurs résultats et discuter des différentes mesures de sécurité qu'ils ont mises en œuvre.

Matériel :

- Des présentations PowerPoint ou des documents PDF pour chaque section.
- Des exemples d'attaques de sécurité pour l'analyse
- Des outils en ligne pour la détection de logiciels malveillants et la surveillance des journaux système
- Des guides de bonnes pratiques de sécurité pour la prévention des cyberattaques



Scan de vulnérabilités

À présent que nous disposons d'une liste d'adresses IP, de ports ouverts et de services sur chaque machine, il est temps de scanner ces cibles à la recherche de vulnérabilités. Une vulnérabilité correspond dans le logiciel ou la configuration du système à une faiblesse que nous pouvons exploiter. Elles peuvent prendre différentes formes, mais elles sont souvent liées à des correctifs non appliqués. Les fournisseurs publient des correctifs qui suppriment des vulnérabilités ou des problèmes connus. Avec les logiciels et les systèmes auxquels les correctifs n'ont pas été appliqués, les tests d'intrusion arrivent souvent rapidement à leur conclusion car certaines vulnérabilités permettent l'exécution d'un code à distance. Cette possibilité est le Saint-Graal du hacking.

L'exécution de code à distance permet à un assaillant ou à un testeur d'intrusion de contrôler totalement l'ordinateur distant comme s'il était assis devant lui. Cela lui permet notamment de copier, de modifier et de supprimer des documents ou des fichiers, d'installer de nouveaux logiciels, de modifier ou de désactiver des logiciels de défense, comme le pare-feu ou l'antivirus, d'installer des enregistreurs de frappe ou des portes dérobées, et d'utiliser le nouvel ordinateur compromis pour attaquer d'autres machines.

Il est important de comprendre cette étape, car ses résultats alimenteront directement la phase 3, au cours de laquelle nous tenterons un exploit afin d'obtenir un accès au système. Pour rechercher les vulnérabilités sur un système, nous utilisons un scanner de vulnérabilités. Plusieurs outils sont disponibles, mais, dans ce module, nous nous limiterons à Nessus.

Nessus est un très bon outil disponible gratuitement (tant que son utilisation reste dans un cadre personnel) sur son site web à l'adresse <http://www.tenable.com/products/nessus>. Tenable, le créateur de Nessus, vous autorise à télécharger une version complète et à obtenir une clé gratuitement. Si vous souhaitez utiliser Nessus dans un cadre professionnel, vous devez choisir l'inscription Professional Feed à la place de Home Feed. Il vous en coûtera 1 500 dollars par an.

Pour installer Nessus sur Kali Linux, vous pouvez suivre les étapes suivantes :

Tout d'abord, téléchargez la dernière version de Nessus sur le site officiel de Tenable : <https://www.tenable.com/downloads/nessus> Une fois le téléchargement terminé, ouvrez un terminal et allez dans le dossier où vous avez téléchargé le fichier Nessus.

Exécutez la commande suivante pour installer Nessus :

`sudo wget https://www.tenable.com/downloads/nessus`

après l'installation, vous devez configurer Nessus en accédant à son interface web.

Ouvrez un navigateur Web dans Kali Linux et accédez à l'adresse suivante : <https://localhost:8834/> Vous devrez accepter le certificat de sécurité pour continuer.

Suivez les instructions à l'écran pour configurer Nessus en créant un utilisateur administrateur et en configurant les paramètres.

Après avoir configuré Nessus, vous pouvez lancer des analyses de vulnérabilité en utilisant l'interface web de Nessus.
Assurez-vous que la machine virtuelle VirtualBox a une connexion réseau active pour accéder à l'interface web de Nessus.

PEREZ MOTA Javier
Formateur



TP : Déchiffrer des mots de passe

Objectifs :

Le TP a pour objectif de comprendre les concepts de base des techniques de déchiffrement de mots de passe, d'identifier les méthodes courantes de déchiffrement de mots de passe et d'apprendre à utiliser des outils pour déchiffrer des mots de passe chiffrés.

Instructions :

Expliquez les concepts de base de la cryptographie.

Expliquez comment les mots de passe sont chiffrés et comment les attaquants peuvent utiliser des techniques de déchiffrement pour récupérer les mots de passe.

Voici un ensemble de mots de passe cryptés que vous devez décrypter :

25f9e794323b453885f5181f1b624d0b

a64cd8062eaa4562c0ba463f2ee7c828

f7c3bc1d808e04732adf679965ccc34ca7ae3441

426a6cb167cad750ac07eb9b5aac2334e97ec801

**df5e963e06213ab7a2235e3ea47fdc7ee51e393eaf2bc675882dcdba5b978
85b**

**9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a
08**

Exécutez les outils de déchiffrement et vérifiez les résultats. Vous devrez signaler tous les mots de passe déchiffrés avec succès.

Identifiez les méthodes courantes de déchiffrement de mots de passe.

Expliquez comment améliorer la sécurité des mots de passe en utilisant des techniques de hachage de mots de passe plus robustes et en imposant des politiques de mots de passe plus strictes.

Conclusion :

Le déchiffrement de mots de passe est une technique courante utilisée par les attaquants pour accéder à des comptes et à des systèmes protégés par mot de passe.

Vous devez comprendre les concepts de base des techniques de déchiffrement de mots de passe, savoir identifier les méthodes courantes de déchiffrement de mots de passe et savoir utiliser des outils pour déchiffrer des mots de passe chiffrés.

Les outils de déchiffrement de mots de passe peuvent aider à renforcer la sécurité en testant la robustesse des politiques de mots de passe.

Cependant, il est important de souligner que la meilleure façon de protéger les mots de passe est d'utiliser des techniques de hachage de mots de passe robustes et d'imposer des politiques de mots de passe strictes.

PEREZ MOTA Javier
Formateur

TP : Déchiffrer des mots de passe

Objectifs :

Le TP a pour objectif de comprendre les concepts de base des techniques de déchiffrement de mots de passe, d'identifier les méthodes courantes de déchiffrement de mots de passe et d'apprendre à utiliser des outils pour déchiffrer des mots de passe chiffrés.

Instructions :

Expliquez les concepts de base de la cryptographie.

Expliquez comment les mots de passe sont chiffrés et comment les attaquants peuvent utiliser des techniques de déchiffrement pour récupérer les mots de passe.

Les mots de passes sont chiffrés à l'aide d'un algorithme de hachage. Cette empreinte de hachage est stocké dans la base de données du système, plutôt que le mot de passe soit réel pour les raisons de sécurité.

Voici un ensemble de mots de passe cryptés que vous devez décrypter :

25f9e794323b453885f5181f1b624d0b

a64cd8062eaa4562c0ba463f2ee7c828

f7c3bc1d808e04732adf679965ccc34ca7ae3441

426a6cb167cad750ac07eb9b5aac2334e97ec801

**df5e963e06213ab7a2235e3ea47fdc7ee51e393eaf2bc6
75882dcdba5b978 85b**

**9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822
cd15d6c15b0f00a 08**

Exécutez les outils de déchiffrement et vérifiez les résultats. Vous devrez signaler tous les mots de passe déchiffrés avec succès.

Identifiez les méthodes courantes de déchiffrement de mots de passe.

Il existe plusieurs méthode courante pour les déchiffrement du mot de passe voici les 4 étapes à suivre :

1. Force brute : cette méthode consiste à essayer toutes les combinaisons possibles de caractères jusqu'à ce que le mot de passe soit découvert. Cela peut prendre beaucoup de temps et nécessite souvent des ressources informatiques importantes.
2. Attaque par dictionnaire : cette méthode consiste à utiliser une liste de mots couramment utilisés, des noms propres, des phrases et d'autres combinaisons de mots pour essayer de deviner le mot de passe.
3. Attaque par rainbow tables : cette méthode utilise des tables précalculées de hachages de mots de passe connus pour essayer de trouver la correspondance avec le hachage du mot de passe cible. Cette méthode peut être très rapide mais nécessite une grande quantité de stockage pour stocker les tables précalculées.
4. Ingénierie sociale : cette méthode consiste à obtenir des informations sensibles telles que des mots de passe en manipulant les personnes plutôt que les systèmes. Par

exemple, un attaquant peut se faire passer pour un membre du personnel de support technique et demander à un utilisateur de divulguer son mot de passe.

Expliquez comment améliorer la sécurité des mots de passe en utilisant des techniques de hachage de mots de passe plus robustes et en imposant des politiques de mots de passe plus strictes.

Les mots de passes sont l'une des formes plus courantes d'authentification, mais leur sécurité est souvent compromise en raison de leur faible complexité. Il existe 4 méthodes pour améliorer la sécurité des mots de passes :

1. Utiliser des fonctions de hachage de mots de passe robustes : Les fonctions de hachage de mots de passe comme PBKDF2, bcrypt et scrypt peuvent être utilisées pour renforcer la sécurité des mots de passe. Ces fonctions sont conçues pour rendre le hachage des mots de passe plus difficile à casser en utilisant des itérations et des sels. Les sels sont des données aléatoires qui sont ajoutées aux mots de passe avant le hachage pour rendre les attaques par dictionnaire plus difficiles.
2. Imposer des politiques de mots de passe strictes : Les politiques de mots de passe peuvent être utilisées pour encourager les utilisateurs à choisir des mots de passe forts et à les changer régulièrement. Les politiques peuvent inclure des exigences telles que la longueur minimale du mot de passe, la complexité, l'utilisation de caractères spéciaux, l'interdiction d'utiliser des mots courants, l'expiration régulière du mot de passe, etc.
3. Utiliser la vérification en deux étapes : La vérification en deux étapes ajoute une couche supplémentaire de sécurité en obligeant les utilisateurs à saisir un code d'authentification

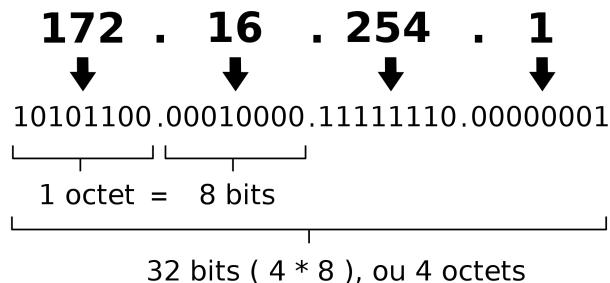
Les adresses et leur écritures

Une adresse IPv4 est composée de 4 octets. Chaque octet contient 8 bits.

Les octets ont une valeur variant de 0 à 255 en écriture décimale, soit de 0000 0000 à 1111 1111 en écriture binaire.

Voici un exemple d'une adresse IPv4 :

Une adresse IPv4 (notation décimale à point)



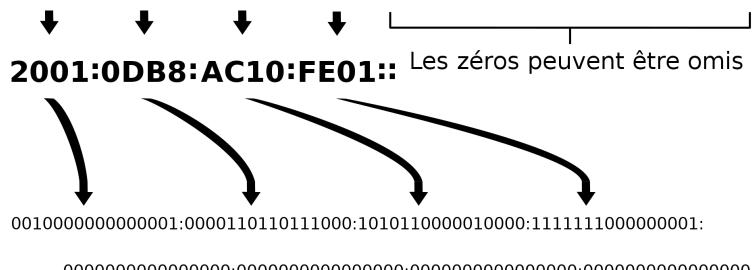
Une adresse IPv6 est composée de 16 octets. Chaque octet contient 8 bits.

Les octets ont une valeur variant de 00 à FF en écriture hexadécimale, soit de 0000 0000 à 1111 1111 en écriture binaire.

Voici un exemple d'une adresse IPv6 :

Une adresse IPv6 (en hexadécimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000



Comme vous pouvez le voir sur l'exemple, les octets qui sont à 0 peuvent être omis en notant ::

L'écriture binaire est une succession de puissance de 2. Chaque valeur qui correspond à 1 est une valeur de puissance de 2.

Exemple : Si on prend la valeur maximale d'un octet d'une adresse IPv4, soit 255 et qu'on convertit celle-ci en binaire soit 1111 1111, on peut traduire cela par $2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$ soit $128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$

Si on prend le dernier octet de l'adresse IP 192.168.1.10 qui correspond au nombre 10, on le convertit de cette façon en binaire : 0000 1010 soit $2^3 + 2^1$ ou $8 + 2$

Pour une adresse IPv6, on peut en exemple un octet qui correspond à B8. Pour convertir la valeur hexadécimale B8 en binaire, nous devons convertir chaque chiffre hexadécimal (B et 8) en binaire. Le chiffre B correspond à 1011 en binaire et le chiffre 8 correspond à 1000 en binaire. Nous combinons ensuite ces deux séquences de bits pour obtenir la valeur binaire complète 10111000.

Une adresse MAC (Media Access Control) est une adresse physique unique attribuée à chaque carte réseau d'un appareil, telle qu'une carte Ethernet ou Wi-Fi. L'adresse MAC est un identifiant unique, généralement composé de 48 bits, qui identifie de manière précise un appareil au sein d'un réseau local (LAN).

L'adresse MAC est également appelée adresse physique ou adresse Ethernet. Elle est généralement assignée par le fabricant de la carte réseau, et est gravée dans le matériel de la carte elle-même. L'adresse MAC est souvent représentée sous forme de 12 chiffres hexadécimaux, séparés par des tirets ou des deux-points. Par exemple, une adresse MAC typique peut ressembler à ceci : 00:1A:2B:3C:4D:5E.

L'adresse MAC est utilisée pour acheminer des données sur un réseau local. Les protocoles de communication tels que Ethernet utilisent l'adresse MAC pour acheminer les données de l'émetteur vers le destinataire. Contrairement aux adresses IP qui peuvent être changées ou masquées, l'adresse MAC est considérée comme étant "unique" pour chaque carte réseau et est généralement fixe tout au long de la vie de la carte.

Un masque de sous-réseau (ou subnet mask en anglais) est un nombre binaire qui permet de délimiter les parties d'une adresse IP qui correspondent à l'identification du réseau et à l'identification de l'hôte. En d'autres termes, il permet de définir la taille du réseau et du sous-réseau auquel appartient une adresse IP.

Le masque de sous-réseau est généralement représenté sous la forme d'une série de bits à 1 suivis d'une série de bits à 0. Les bits à 1 correspondent à la partie de l'adresse IP qui identifie le réseau et les sous-réseaux, tandis que les bits à 0 correspondent à la partie de l'adresse IP qui identifie l'hôte.

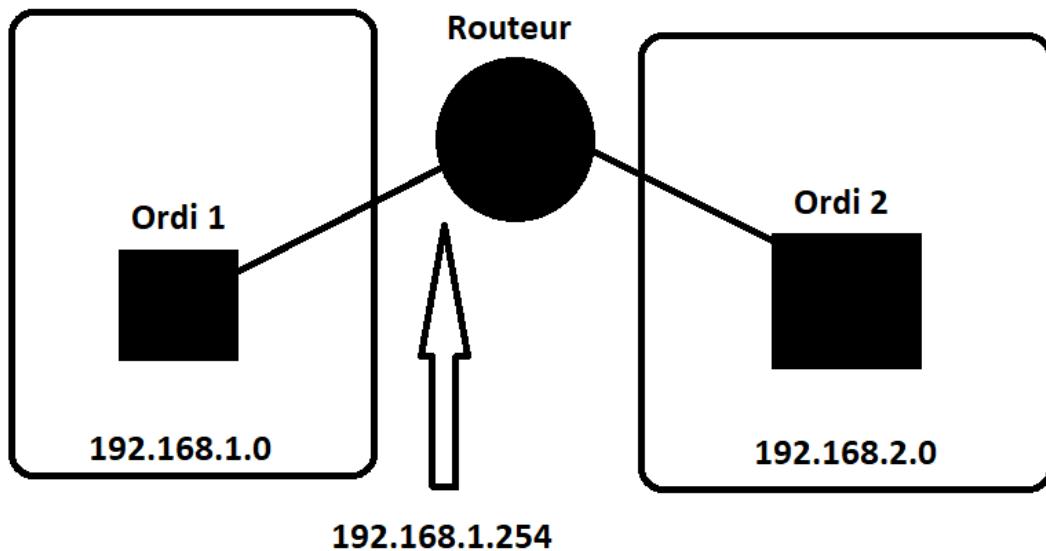
Par exemple, si le masque de sous-réseau est "255.255.255.0" pour une adresse IP de la forme "192.168.0.X", cela signifie que les trois premiers octets de l'adresse IP (192.168.0) identifient le réseau et le dernier octet (X) identifie l'hôte. En d'autres termes, il y a 256 adresses IP disponibles pour les hôtes (de 192.168.0.1 à 192.168.0.254), car un octet contient 8 bits et que le dernier octet est réservé pour l'identification de l'hôte.

Une passerelle par défaut (ou default gateway en anglais) est une adresse IP de l'équipement réseau qui sert de point de sortie pour les communications à destination d'autres réseaux.

Lorsqu'un appareil, comme un ordinateur ou un routeur, doit communiquer avec une adresse IP qui ne fait pas partie de son réseau local, il envoie le paquet à la passerelle par défaut. Cette dernière est généralement configurée sur l'appareil comme l'adresse IP de la première interface du routeur qui mène à un réseau externe, tel que l'Internet.

La passerelle par défaut est donc l'adresse IP de l'équipement qui permet à un appareil de sortir de son réseau local pour accéder à d'autres réseaux. Elle joue un rôle crucial dans le routage des paquets et est souvent configurée lors de la mise en place d'un réseau ou d'un système informatique.

Par exemple, mon ordinateur a une adresse IP qui est configurée dans le réseau 192.168.1.0. L'adresse IP de l'interface réseau du routeur qui est connecté à ce réseau est 192.168.1.254. Mon ordinateur aura donc cette adresse IP en passerelle par défaut pour pouvoir communiquer avec les autres réseaux.



Les adresses IP sont divisés en 3 parties :

- **Les adresses réseaux** : Une adresse réseau est une adresse IP qui identifie un réseau particulier dans un système informatique. Elle est utilisée pour diriger les données à destination et en provenance du réseau, ainsi que pour déterminer si un hôte est membre de ce réseau. Une adresse réseau est généralement obtenue en appliquant un masque de sous-réseau à une adresse IP. Le masque de sous-réseau permet de définir la plage d'adresses IP qui sont incluses dans le réseau.

Par exemple, si une adresse IP est 192.168.1.10 et que le masque de sous-réseau est 255.255.255.0, alors l'adresse réseau correspondante serait 192.168.1.0. Cela signifie que tous les ordinateurs ayant une adresse IP commençant par "192.168.1." appartiennent au même réseau et peuvent communiquer directement les uns avec les autres sans passer par un routeur.

- **Les adresses de diffusion** : Une adresse de diffusion est une adresse IP spéciale qui permet d'envoyer des données à tous les ordinateurs d'un réseau en une seule opération. Lorsqu'un ordinateur envoie des données à une adresse de diffusion, celles-ci sont envoyées à tous les ordinateurs du réseau qui écoutent sur cette adresse.

En général, l'adresse de diffusion est déterminée en fixant tous les bits de l'adresse IP qui représentent l'identifiant de l'hôte à 1. Par exemple, si l'adresse IP de l'hôte est 192.168.1.10, alors l'adresse de diffusion correspondante serait 192.168.1.255.

L'utilisation d'adresses de diffusion est courante dans les protocoles de réseau pour la diffusion de messages, tels que la découverte de services, les mises à jour de configuration, les annonces de route, etc. Cela permet aux ordinateurs de communiquer plus efficacement et de manière fiable sur un réseau local.

- **Les adresses IP hôtes** : Une adresse IP hôte est une adresse unique qui identifie un ordinateur ou un périphérique sur un réseau. C'est une adresse IP qui est attribuée à un nœud spécifique sur le réseau et qui permet à d'autres ordinateurs sur le réseau de communiquer avec lui.

Les adresses IP hôtes sont utilisées dans les communications entre les ordinateurs sur un réseau, que ce soit sur Internet ou dans un réseau local. Les adresses IP hôtes sont attribuées de manière dynamique ou statique, selon le mode de configuration du réseau. Les adresses IP statiques sont souvent utilisées pour les serveurs et les périphériques de réseau, tandis que les adresses IP dynamiques sont utilisées pour les ordinateurs clients sur le réseau.

Maintenant que l'on a vu comment est constitué une adresse IP, on va voir les types d'adresses IP :

- **Les adresses IP statiques** : Une adresse IP statique est une adresse IP qui est fixe et ne change pas. L'adresse IP statique est configurée manuellement par un administrateur réseau et elle reste la même, même après le redémarrage de l'appareil ou la déconnexion du réseau.

Les adresses IP statiques sont souvent utilisées pour les serveurs, les imprimantes réseau, les routeurs, les pare-feu et autres équipements réseau, car ces appareils ont besoin d'une adresse IP fixe pour une gestion et une accessibilité à distance plus facile. Les adresses IP statiques sont également utiles pour les applications qui nécessitent une adresse IP constante pour fonctionner correctement.

Cependant, l'utilisation d'adresses IP statiques peut présenter des inconvénients en termes de gestion et de sécurité, car les adresses IP statiques doivent être configurées manuellement, ce qui peut être fastidieux pour les grands réseaux. De plus, les adresses IP statiques sont plus faciles à cibler pour les attaques de sécurité car elles sont facilement reconnaissables et peuvent être plus vulnérables aux attaques de type "ping flooding" ou "port scanning".

- **Les adresses IP dynamiques** : Une adresse IP dynamique est une adresse IP qui est attribuée automatiquement par un serveur DHCP (Dynamic Host Configuration Protocol) lorsqu'un appareil se connecte à un réseau.

Les adresses IP dynamiques sont souvent utilisées pour les ordinateurs de bureau, les ordinateurs portables et autres appareils clients, car elles permettent à plusieurs appareils de partager une plage limitée d'adresses IP sans qu'il soit nécessaire de configurer manuellement chaque adresse IP. Les adresses IP dynamiques sont également utiles pour les fournisseurs de services Internet (FSI) qui doivent attribuer des adresses IP à leurs clients de manière efficace.

Cependant, l'utilisation d'adresses IP dynamiques peut présenter des inconvénients en termes de gestion et de sécurité. Par exemple, les adresses IP dynamiques peuvent être plus difficiles à localiser si un problème de réseau survient, car elles peuvent changer régulièrement. Les adresses IP dynamiques peuvent également rendre la configuration de la sécurité réseau plus complexe car elles sont plus difficiles à surveiller et à filtrer en raison de leur nature dynamique.

- **Les adresses IP publiques** : Une adresse IP publique est une adresse unique attribuée à un appareil connecté à Internet, très souvent un routeur, qui permet à cet appareil d'être identifié et de communiquer avec d'autres appareils sur Internet.

Les adresses IP publiques sont fournies par les fournisseurs d'accès Internet (FAI) et sont visibles depuis Internet. Chaque appareil connecté à Internet possède une adresse IP publique unique qui lui est attribuée par le FAI. Cette adresse IP est utilisée pour acheminer les données entre cet appareil et les autres appareils sur Internet.

Les adresses IP publiques sont essentielles pour permettre aux appareils connectés à Internet de communiquer entre eux. Par exemple, lorsqu'un utilisateur envoie un e-mail ou visite un site web, son appareil utilise son adresse IP publique pour communiquer avec le serveur du destinataire.

Le protocole IPv4 dispose d'un espace d'adressage de 32 bits, ce qui permet un total théorique de 4,3 milliards d'adresses IP uniques. Cependant, en réalité, la plupart de ces adresses IP sont réservées pour des utilisations spéciales, ce qui réduit le nombre d'adresses IP publiques utilisables.

On estime donc qu'il y a environ 800 millions d'adresses IP publiques utilisables en pratique avec le protocole IPv4.

Le protocole IPv6 a été conçu pour éviter une pénurie d'adresses IP publiques utilisables car celui-ci a une plage d'adresses de $2,81 \times 10^{28}$ adresses IP publiques utilisables soit 28 100 000 000 000 000 000 000 000 000 adresses. Cela représente un nombre extrêmement élevé d'adresses IP, bien au-delà de ce dont nous avons besoin actuellement.

Pour mieux comprendre à quel point ce nombre est grand, voici un exemple de comparaison :

Si chaque atome de la Terre avait une adresse IPv6 unique, il resterait encore plus de $3,5 \times 10^{27}$ adresses inutilisées.

En bref, le nombre d'adresses IPv6 disponibles est suffisamment élevé pour répondre aux besoins futurs d'adressage IP pendant de nombreuses années.

- **Les adresses IP privés** : Une adresse IP privée est une adresse IP réservée pour une utilisation à l'intérieur d'un réseau privé. Contrairement aux adresses IP publiques, les adresses IP privées ne sont pas routables sur Internet, ce qui signifie qu'elles ne peuvent pas être utilisées pour accéder à des ressources Internet depuis l'extérieur du réseau privé.

Les adresses IP privées sont souvent utilisées dans les réseaux domestiques, les réseaux d'entreprise et les réseaux locaux. Elles permettent à de nombreux appareils sur un même réseau de communiquer entre eux en utilisant des adresses IP uniques, même si ces adresses ne sont pas accessibles depuis Internet.

Il existe trois blocs d'adresses IP privées réservées pour une utilisation interne :

- 10.0.0.0 à 10.255.255.255 (masque de sous-réseau 255.0.0.0)
- 172.16.0.0 à 172.31.255.255 (masque de sous-réseau 255.255.0.0)
- 192.168.0.0 à 192.168.255.255 (masque de sous-réseau 255.255.0.0)

Les adresses IP privées sont souvent utilisées en conjonction avec la traduction d'adresses réseau (NAT) pour permettre aux appareils sur un réseau privé d'accéder à Internet en utilisant une adresse IP publique partagée.

En IPv6, contrairement à IPv4, il n'y a pas de plage d'adresses IP réservées pour un usage privé. Au lieu de cela, une adresse IPv6 privée est générée en utilisant une technique appelée "Unique Local Address" (ULA) ou "Local-Use IPv6 Address".

Une ULA est un préfixe d'adresse IPv6 qui est choisi aléatoirement localement et qui ne peut pas être routé sur Internet public. Ces préfixes commencent par le bloc d'adresse FC00::/7 (qui inclut les préfixes FD00::/8 réservés pour une utilisation privée) et sont destinés à être utilisés pour les réseaux privés à grande échelle (comme les réseaux d'entreprise) ainsi que pour les réseaux plus petits (comme les réseaux domestiques).

En résumé, les adresses IPv6 privées sont générées à partir des préfixes ULA, qui sont choisis aléatoirement localement et qui ne peuvent pas être routés sur Internet public.

Voici un exemple d'adresse IPv6 privée générée à l'aide d'un préfixe ULA :

FD12:3456:789A:1::1

généré par un appareil ou une application tiers après avoir saisi leur nom d'utilisateur et leur mot de passe.

4. Utiliser des gestionnaires de mots de passe : Les gestionnaires de mots de passe sont des outils qui stockent en toute sécurité les mots de passe de l'utilisateur et les saisissent automatiquement lorsqu'ils accèdent à un site ou à une application. Les gestionnaires de mots de passe peuvent également générer des mots de passe forts pour l'utilisateur.

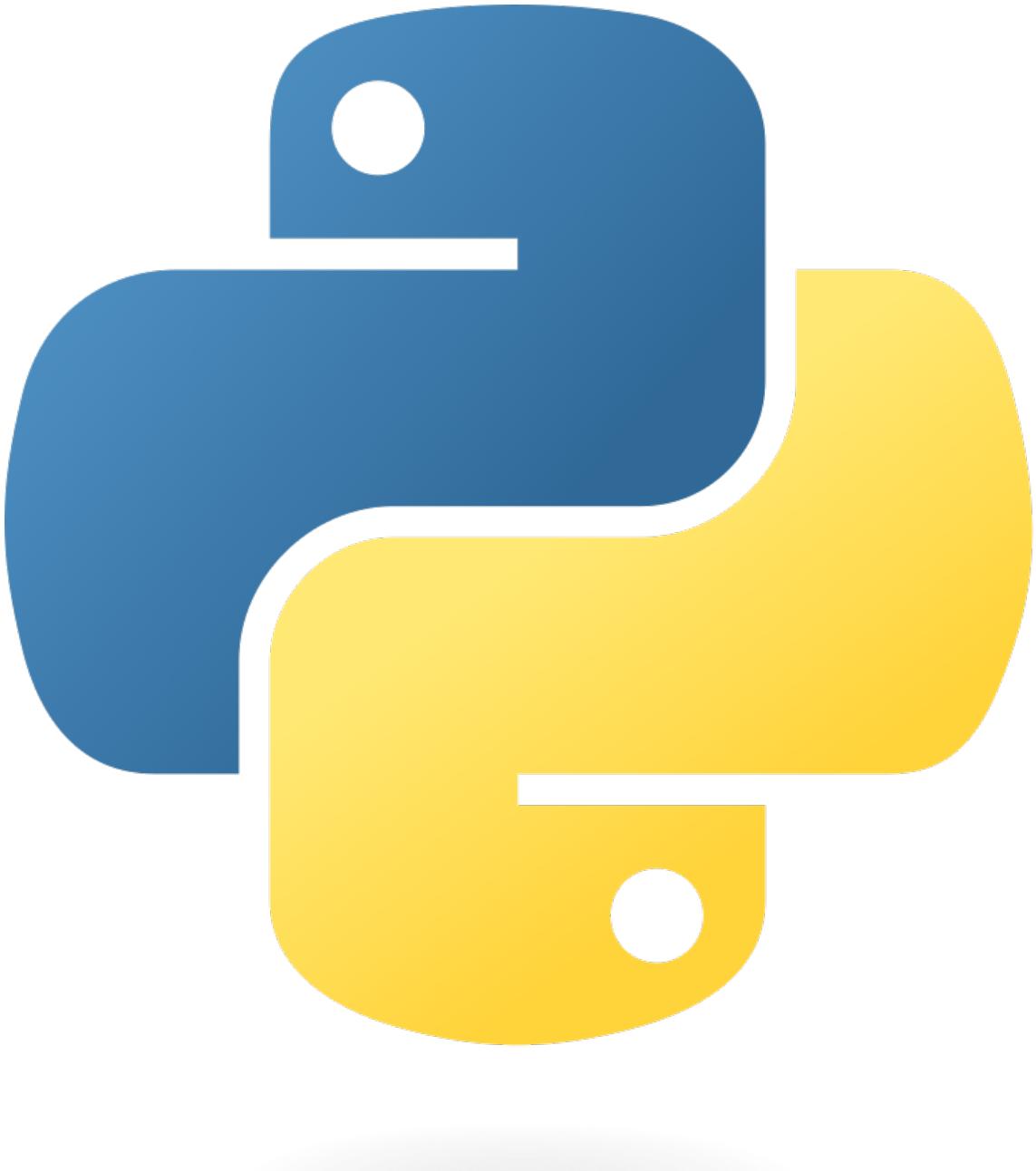
Conclusion :

Le déchiffrement de mots de passe est une technique courante utilisée par les attaquants pour accéder à des comptes et à des systèmes protégés par mot de passe.

Vous devez comprendre les concepts de base des techniques de déchiffrement de mots de passe, savoir identifier les méthodes courantes de déchiffrement de mots de passe et savoir utiliser des outils pour déchiffrer des mots de passe chiffrés.

Les outils de déchiffrement de mots de passe peuvent aider à renforcer la sécurité en testant la robustesse des politiques de mots de passe.

Cependant, il est important de souligner que la meilleure façon de protéger les mots de passe est d'utiliser des techniques de hachage de mots de passe robustes et d'imposer des politiques de mots de passe strictes



TP : Création de variables en Python

Objectifs :

Comprendre ce qu'est une variable en Python

Apprendre à créer et à affecter des variables en Python

Savoir comment utiliser les variables dans des calculs et des opérations en Python

Exercice 1 : Création et affectation de variables

Créez une nouvelle variable appelée "nom" et affectez-lui une chaîne de caractères contenant votre nom.

Créez une deuxième variable appelée "age" et affectez-lui votre âge en utilisant un nombre entier.

Créez une troisième variable appelée "taille" et affectez-lui votre taille en utilisant un nombre décimal.

Affichez le contenu de ces variables en utilisant la fonction print().

Exercice 2 : Utilisation des variables dans des opérations

Créez une quatrième variable appelée "poids" et affectez-lui votre poids en utilisant un nombre décimal.

Calculez votre indice de masse corporelle (IMC) en utilisant la formule suivante : IMC = poids / (taille * taille)

Affichez le résultat de l'IMC en utilisant la fonction print().

Exercice 3 : Modification des valeurs des variables

Modifiez la valeur de la variable "taille" en utilisant une nouvelle valeur.

Recalculez l'IMC en utilisant la nouvelle valeur de la variable "taille".

Affichez le nouveau résultat de l'IMC en utilisant la fonction print().

Exercice 4 : Utilisation de variables dans des chaînes de caractères

Créez une cinquième variable appelée "ville" et affectez-lui le nom de votre ville de résidence.

Créez une chaîne de caractères en utilisant les variables "nom", "age", "taille", "poids" et "ville".

Affichez cette chaîne de caractères en utilisant la fonction print().

Exercice 5 : Utilisation de variables dans des opérations mathématiques

Créez une sixième variable appelée "x" et affectez-lui une valeur entière.

Créez une septième variable appelée "y" et affectez-lui une valeur entière différente de "x".

Calculez la somme de "x" et "y" et affectez-la à une huitième variable appelée "somme".

Calculez la différence entre "y" et "x" et affectez-la à une neuvième variable appelée "difference".

Affichez les valeurs des variables "somme" et "difference" en utilisant la fonction print().

Conclusion :

Dans ce TP, vous avez appris à créer des variables en Python et à les utiliser dans des opérations mathématiques et des chaînes de caractères. Les variables sont des éléments essentiels de la programmation en Python et vous permettent de stocker des données.