Hacker Highschool

SECURITY AWARENESS FOR TEENS



LECON 2

LES COMMANDES ESSENTIELLES

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

AVERTISSEMENT

Le **Projet Hacker High School** est un outil didactique et comme tous les autres outils de son genre, il présente des inconvénients ou dangers. Certaines leçons, lorsqu'elles sont utilisées abusivement, peuvent engendrer des dommages physiques. Il se peut que d'autres dangers existent lorsqu'une recherche approfondie sur les effets possibles émanant de certaines technologies n'est pas faite. Les étudiants qui se servent de ces cours, doivent être surveillés et encouragés à apprendre, à essayer et le mettre en pratique. Cependant ISECOM ne peut endosser la responsabilité de toute utilisation abusive faite des informations ci-présent.

Les leçons suivantes et leurs exercices sont disponibles ouvertement au public sous les termes et conditions de **ISECOM**:

Tous les travaux du **Projet Hacker High School** sont fournis pour une utilisation non-commerciale dans les écoles primaires, les collèges et les lycées, voir dans les institutions publiques ou privées, et même pour les études à domicile. Ce matériel didactique ne doit en aucun cas être reproduit à des fins commerciales. L'utilisation de ce matériel didactique dans des séminaires, ou des ateliers de formation qui sont payants est formellement interdite à moins que vous n'obteniez une licence. Il en est de même pour les formations payantes dans les collèges, lycées, universités et camp d'informatique, ou autres. Pour l'achat d'une licence, veuillez visiter la section LICENSE sur la page de Hacker High School (HHS) qui se trouve à l'adresse suivante: http://www.hackerhighschool.org/licensing.html.

Le **Projet Hacker High School** est le fruit de l'effort d'une communauté ouverte et si vous appréciez ce projet, nous vous demandons de nous supporter en achetant une licence, ou en faisant un don, ou en nous sponsorisant.

Sommaire

Introduction et Objectifs..... 5
Les Prérequis et le Paramétrage..... 6
Les Prérequis..... 6
Le Paramétrage..... 6
Le Système d'Exploitation: Windows..... 7
Comment Ouvre t-on une fenêtre d'Invite de Commandes ?..... 7
Les Commandes et les Outils (Windows/DOS)..... 7
Les Commandes..... 10
Les Outils..... 12
Le Système d'Exploitation: Linux..... 16
Comment ouvre t-on une fenêtre Terminal?..... 17
Les Commandes et les Outils sous Linux..... 17
Les Commandes..... 18
Les Outils..... 21
Début du Jeu: les Options des Commandes..... 22
Le Système d'Exploitation: OSX..... 23
Comment ouvre t-on la fenêtre Terminal..... 23
Les Commandes et les Outils (OSX)..... 24
Les Commandes..... 25
Les Outils..... 28
Les Commandes Essentielles et leur Equivalence pour Windows, OSX et Linux..... 32

Les Contributeurs

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Bob Monroe, ISECOM
Marco Ivaldi, ISECOM
Greg Playle, ISECOM
Simone Onofri, ISECOM
Kim Truett, ISECOM
Jaume Abella, ISECOM
Tom Thomas, ISECOM
Jairo Hernández
Aneesh Dogra

Les Traducteurs

Koffi « Willy » Nassar

ISECOM

Introduction et Objectifs

Que vous ayez suivi un acte de "hacking" dans le film *Hackers* en 1995 ou vu Trinity entrain de pirater un système UNIX dans le film *The Matrix Reloaded*, lorsque vous observez un hacker, ils travaillent toujours en mode ligne de commandes. Pour de bonnes raisons.

Vous pouvez faire des choses énormes, très puissantes à partir de la ligne de commande (**CLI** : Command Line interface). Vous n'avez pas besoin d'être un maître de la ligne de commande mais vous devriez vous sentir à l'aise en l'utilisant.

Une fois que vous avez maîtrisé les notions essentielles de la ligne de commande, vous pouvez commencer à utiliser ces commandes dans des fichiers textes (nommés **scripts**) ; c'est la manière la plus facile de programmer.

Nous parlerons des commandes et des outils essentiels des systèmes d'exploitation suivant : Windows, Mac OS X, et Linux. Vous aurez besoin de les apprendre pour résoudre les exercices des leçons à venir. À la fin de cette leçon, vous vous familiariserez avec :

- Les commandes essentielles sous Windows, Linux et OSX
- Les commandes et les outils réseau essentiels, y compris:

```
ping
tracert/traceroute
netstat
ipconfig/ifconfig
route
```

Les Prérequis et le Paramétrage

Les Prérequis

Pour comprendre et bien terminer cette leçon, vous aurez besoin:

- D'un PC fonctionnant sous Linux
- D'un PC fonctionnant sous Windows
- Facultativement d'un Mac fonctionnant sous OS X
- D'un Accès Internet

Le Paramétrage

Figure 2.1: Configuration Générale du Réseau

Voici le réseau sur lequel nous allons effectuer la plupart de nos travaux. Il comprend votre PC, l'Internet et le réseau de test de ISECOM destiné à Hacker High School, auquel vous aurez accès via l'Internet.

Notez que l'accès au réseau de test de ISECOM est restreint. Pour y avoir accès, votre instructeur doit contacter l'administrateur, comme le stipule les détails sur le site http://www.hackerhighschool.org.

Cependant, vous pouvez aussi remplacer ce réseau de test par un autre juste pour les exercices. N'effectuez **JAMAIS** des tests sur des ordinateurs qui ne vous appartiennent pas ! Il se peut que ce soit un acte criminel, et peut être dangereux dans plusieurs cas.

Si vous voulez monter votre propre réseau de tests, cela peut être facile comme le fait de faire un test sur un autre ordinateur en classe ou chez vous à la maison. Il n'y aura pas besoin de faire des réglages spéciaux. Si vous voulez bien sûr quelque chose de plus robuste ou quelque chose qui vous permet de relever des défis et de résoudre les imperfections dans l'accès d'un autre ordinateur qui se trouve sur Internet, alors vous aurez besoin d'un réseau de test connecté à Internet. Ceci peut être réalisé en ayant des partenariats avec d'autres écoles ou ménages qui vous permettrons d'avoir mutuellement accès aux ordinateurs de part et d'autre. Mais rassurer vous de cerner ce que vous faites en paramétrant ce réseau de test parce que ce que vous ne souhaitez pas pour ces ordinateurs ouverts, c'est qu'ils soient détournés par des personnes malintentionnées sur Internet qui causent des dommages dont vous serez responsables par après.

Le Système d'Exploitation: Windows

Autrefois, si nous ne travaillions pas sous UNIX, nous travaillions tous sous DOS (Disk Operatiing System). Nous n'avions pas besoin de ligne de commandes ; parce que nous y sommes déjà. Ensuite UNIX a développé des interfaces sous forme de "fenêtres", une idée qui a été éventuellement épousée par le monde des PC grâce à Microsoft Windows.

Une fois que Windows est né, nous avons accès à DOS via une fenêtre ouverte sur notre bureau et nous appelons cette dernière **Invite de Commandes** (**command prompt**). Après que Windows soit passé au-delà des fonctionnalité de DOS, il possède toujours une invite de commandes, et plusieurs personnes l'appellent toujours la **fenêtre DOS.** Il ne s'agit plus du tout réellement de DOS, mais concernant nos objectifs, cela importe peut. Voici comment on ouvre une invite de commandes.

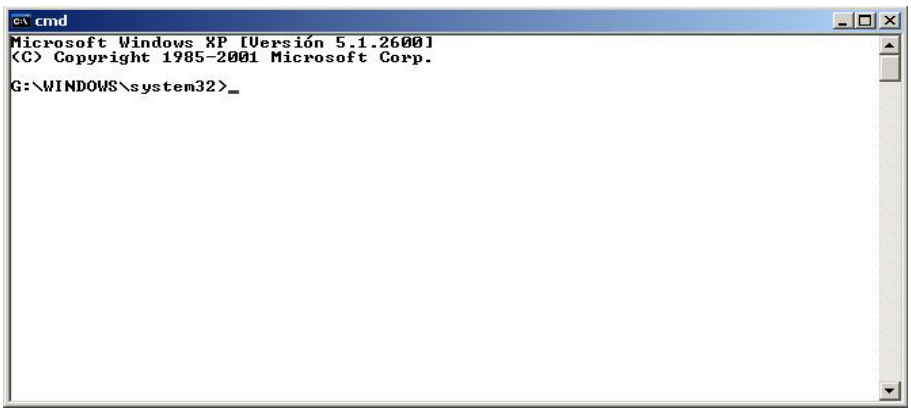
Comment Ouvre t-on une fenêtre d'Invite de Commandes ?

La procédure est pareille sous toutes les versions de Windows.

1. Cliquez sur le bouton DEMARRER.

Choisissez l'option EXECUTER (éviter ceci sous Vista et les versions ultérieures)

2. Saisissez **command** si vous utilisez Windows 95/98 ou **cmd** pour les autres versions de Windows et appuyez sur Entrer ou cliquez sur OK.
3. Une fenêtre semblable à la suivante apparaîtra:



4. A présent vous pouvez vous utiliser les commandes et les outils listés ci-après.

Les Commandes et les Outils (Windows/DOS)

Les commandes fournissent les fonctions prédéfinies d'un système d'exploitation. Les outils en font plus : ils sondent le réseau, recherche des **hôtes** (ce terme désigne les machines connectées à un réseau), et permettent de voir ou de régler les paramètres de routage de votre hôte.

Les Commandes

Les mots en italic représentent des options que vous devez saisir.

Certaines commandes existent sous une forme courte ou longue, et toutes les commandes ne sont pas disponibles sous toutes les versions de Windows.

Commandes	Fonction
date	Affiche ou règle la date
time	Affiche ou règle l'heure
ver	Affiche la version de MS-DOS ou de Windows.
dir	Affiche la liste des sous-dossiers et des fichiers d'un dossier.
cls	Efface le contenu de la fenêtre
mkdir *nom_dossier* ou **md *nom_dossier***	Crée un dossier dont le nom est *nom_dossier:* `md outils`
Chdir *chemin_vers_dossier* ou **cd *chemin_vers_dossier***	Effectue un déplacement de l'emplacement actuel vers un autre dossier: `cd outils`
rmdir *nom_dossier* ou **rd *nom_dossier***	Efface un dossier: `rd outils`
tree *nom_dossier*	Affiche la structure des dossiers et des fichiers sous un format graphique en mode texte: `tree c:\outils`
chkdsk	Vérifie un disque et renvoie un rapport d'état.
mem	Affiche la quantité de mémoire utilisée et libre sur le système.
rename *source destination* *ou* **ren *source destination***	Change le nom des fichiers: `ren images MesImages`
copy *source destination*	Copie un ou plusieurs fichiers vers un autre emplacement: `copy c:\outils\monfichier.txt c:\tmp\`
move *source destination*	Déplace les fichiers; renomme les fichiers et les dossiers: `move c:\outils c:\tmp`
type *file*	Affiche le contenu d'un ou de plusieurs fichiers texte: `type c:\outils\monfichier.txt`
more *file*	Affiche les informations pas à pas `more c:\outils\monfichier.txt`

Commandes	Fonction
delete *nom_fichier* ou **del *nom_fichier***	Efface un ou plusieurs fichiers: `del c:\outils\monfichier.txt`

Les Outils

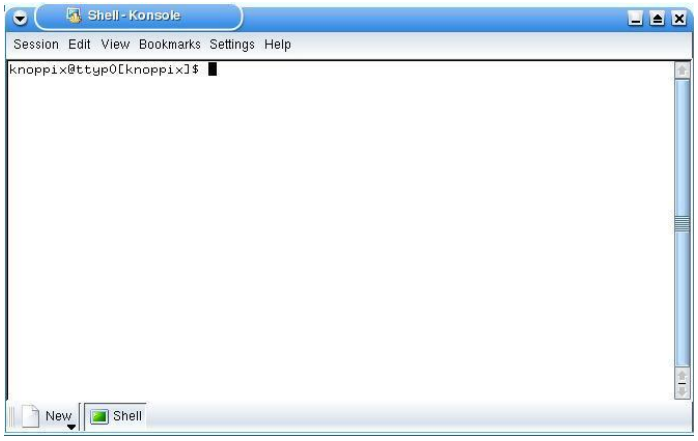
Les mots en italic sont des options que vous devez saisir. Tous les outils ne sont pas présents dans toutes les versions de Windows.

Outil	Fonction

`ping` ***`hôte`***	Vérifie l'interconnexion avec la machine *hôte*.
	
	Cette commande envoie des paquets ICMP (Internet Control Message Protocol) vers un autre ordinateur pour voir combien de temps ce dernier mettra pour répondre, ou s'il ne répond pas du tout. Vous pouvez utiliser un nom d'hôte ou une adresse IP:
	
	`ping hackerhighschool.org`
	
	`ping 216.92.116.13`
	
	Quelques Options :
	
	`ping -n 100 hackerhighschool.org`
	
	envoie 100 paquets ping et
	
	`ping -t 216.92.116.13`
	
	envoie continuellement des paquets ping vers l'hôte jusqu'à ce qu'elle ne soit interrompue avec CTRL+C.
	
	Pour voir plus d'options, faites:
	
	`ping /h`

`tracert` ***`hôte`***	Affiche les routes par lesquelles passent les paquets pour atteindre la machine *hôte*.
	
	La commande **tracert** est une adaptation de la commande **traceroute** du Système UNIX. (Les commandes DOS ne pourraient contenir que huit caractères, à l'époque.) les deux vous permettent de déterminer les routes par lesquelles passe un paquet en partant de votre hôte vers l'hôte de destination, **tracert** détermine aussi le temps de passage par chaque nœud et le nombre de nœuds par lequel passent les paquets, au maximum, 30 nœuds. Très souvent vous pouvez voir les noms d'hôte des machines par lesquelles passent les paquets:
	
	`tracert hackerhighschool.org`
	
	`tracert 216.92.116.13`
	
	Quelques options sont:
	
	`tracert -n 25 hackerhighschool.org`
	
	pour spécifier N, le nombre maximum de passages, et
	
	`tracert -d 216.92.116.13`
	
	pour cacher les noms d'hôtes.
	
	Pour voir plus d'options, faites:
	`tracert /?`

Outil	Fonction

ipconfig	Utilisée seule, elle affiche les informations concernant les interfaces actives de chaque hôte (ethernet, ppp, etc...). Elle est semblable à la commande **ifconfig** sous Linux.
	
	Quelques options sont:
	
	`ipconfig /all`
	pour afficher plus de détails.
	
	`ipconfig /renew`
	pour réinitialiser la connexion lorsque la configuration automatique avec DHCP est utilisée, et
	
	 
	
	`ipconfig /release`
	pour désactiver la connexion réseau lorsque DHCP est activé.
	
	Pour afficher plus d'options:
	
	`ipconfig /?`

Outil	Fonction

route print	Affiche la table de routage. **Route** peut être utilisée pour créer ou effacer des routes statiques.
	
	Quelques options :
	
	`route print`
	pour afficher la liste des routes,
	
	`route delete`
	pour effacer une route, et
	
	`route add`
	pour ajouter une route.
	
	Pour voir plus d'options:
	
	`route/?`

netstat	Affiche les informations concernant l'état du réseau et des connexions établies avec les machines distantes.
	
	Quelques options:
	
	`netstat -a`
	pour vérifier toutes les connexions et les ports en écoute,
	
	`netstat -n`
	pour afficher les adresses et les numéros de port sous un format numérique, et
	
	`netstat -e`
	pour échantillonner les Statistique Ethernet.
	
	Les options peuvent être combinées:
	
	`netstat -an`
	Pour voir plus d'options:
	
	`netstat/?`

Pour avoir des informations complémentaires concernant ces commandes et ces outils, essayez ces options :

command /h

command /?

help *command*

à partir de la fenêtre de l'Invite de Commandes.

Par exemple, pour obtenir des informations complémentaires concernant l'outil **netstat**, vous avez trois possibilités:

netstat /h

```
netstat /?
help netstat
```

Exercises

2.1 Ouvrez un fenêtre d'Invite de Commandes.

2.2 Identifiez la version de DOS ou de Windows que vous utilisez.

2.3 Détectez la date et l'heure du système. S'ils ne sont pas corrects, corrigez-les.

2.4 Détectez tous les Dossiers et les fichiers qui se trouvent dans C:\

2.5 Créez le dossier c:\hhs\leçon2. Copiez dans ce dossier, tous les fichiers ayant pour extension .sys et qui se trouvent sous c:\

2.6 Détectez l'adresse IP de votre hôte.

2.7 Tracez le chemin vers www.hackerhighschool.org. Identifiez les adresses IP des routeurs intermédiaires.

Le Système d'Exploitation: Linux

Tout comme dans Windows, lorsque vous utilisez Linux, vous exécutez des commandes dans une fenêtre d'invite de commandes. Cette fenêtre est souvent désignée sous les termes **console**, **terminal** ou **shell**.

Etoffez vos Connaissances : Que veut dire Console, Terminal ou Shell ?

Émerveillez vos amis en faisant la différence.

- La **console** désignait en réalité l'ensemble écran et clavier connecté directement à l'arrière d'un ordinateur pendant que les anciens utilisent aujourd'hui des **terminaux virtuels** pour accéder à un ordinateur distant.
- Vous avez réellement la possibilité de choisir votre **shell** (interpréteur de commandes) sous Linux, y compris **bash, tcsh** et **zsh**, parmi tant d'autres. Chaque shell vous permet d'accomplir des tâches différentes, et le fait de préférer un shell est l'objet d'une politique d'utilisation. Dans la plupart des cas, vous utiliserez bash. Lorsque vous vous connectez au réseau de test de hackerhighschool, vous aurez accès à un **shell vide.**
- Lorsque vous ouvrez une **fenêtre de console**, vous ouvrez, techniquement parlant un **émulateur de terminal** ou une **fenêtre terminale**, c'est un "faux" terminal virtuel fonctionnant dans une fenêtre sur votre ordinateur.

Que pouvez vous faire avec la ligne de commande Linux ? Vous pouvez faire tout ce que vous faites en interface graphique et même plus. Demandez à vos amis qui utilisent Windows de configurer votre adresse IP : ils doivent passer par toute une panoplie de fenêtres pour le faire. Sous Linux vous pourriez le faire avec la commande suivante :

```
ifconfig eth0 192.168.1.205
```

Mais vous pouvez saisir cela plus vite qu'il ne clique !

Comment ouvre t-on une fenêtre Terminal?

Étant donné qu'il existe plusieurs versions de Linux, il existe plusieurs façons de démarrer une fenêtre de console.

1. Cliquez sur le bouton Démarrer.
2. Si vous voyez une option nommée "Exécuter Commande", cliquez dessus et saisissez "konsole", ensuite Entrée.
3. Ou recherchez Accessoires, ensuite choisissez Terminal.
4. Ou sur plusieurs système, vous pouvez exécuter la combinaison de touche suivante: CTL-ALT-T.
5. Une fenêtre semblable à celle ci-dessus apparaîtra.
6. A présent vous pouvez vous servir des commandes et des outils listés ci-dessous.

Les Commandes et les Outils sous Linux

Les Commandes

Les mots en italique désignent des options que vous devez saisir

Commande	Fonction
date	Affiche ou règle la date
time	Affiche ou règle l'heure
fsck	Vérifie un système de fichiers et renvoie un rapport d'état.
cat *nom_fichier*	Affiche le contenu d'un ou de plusieurs fichiers textes: `cat /etc/passwd`
pwd	Affiche le nom du dossier dans lequel vous vous trouvez actuellement.
hostname	Affiche le nom de l'ordinateur que vous utilisez actuellement.
finger *nom_utilisateur*	Affiche les informations concernant un utilisateur: `finger root`

ls	Affiche le contenu du dossier actuel:
	
	`ls -la`
	Affiche le contenu d'un autre dossier:
	
	`ls -la /etc`

cd *chemin_vers_dossier*	Effectue un déplacement de l'emplacement actuel vers un autre dossier. Si le nom d'aucun dossier n'est mentionné, elle effectue un déplacement vers le dossier parent (home directory).
	
	Pour le nom d'utilisateur "fred" la commande
	
	`$cd`
	effectue un déplacement vers /home/fred, et
	
	`$cd -`
	effectue un déplacement vers le dossier auquel vous avez récemment accédé (pensez à la "soustraction" d'un dossier), et
	
	`$cd /tmp`
	effectue un déplacement vers le dossier /tmp.

cp *source destination*	Copie le fichier *source* vers le fichier *destination*. Exemple: `cp /etc/passwd /tmp/bunnies`

Commande	Fonction
rm *nom_fichier*	Supprime des fichiers. Seuls les utilisateurs munis d'un droit d'accès adéquat (ou root) peuvent supprimer des fichiers sensibles `rm lettre.txt`
mv *source destination*	Déplace ou renomme les fichiers et les dossiers. Exemple: `mv secrets.zip innocent.zip`
mkdir *nom_dossier*	*Crée un dossier dont le nom est nom_dossier*. Exemple: `mkdir tools`

Commande	Fonction
rmdir *nom_dossier*	Supprime un dossier si et seulement si ce dernier n'est pas vide: `rmdir tools` Question bonus: comment supprime t-on un dossier non vide c'est à dire qui contient des fichiers?
find / -name *nom_fichier*	Recherche les fichiers, à partir de /, qui contiennent *nom_fichier*. `find / -name myfile`
echo *string*	Affiche une *chaîne de caractères* à l'écran: `echo hello`
commande* > *fichier	**Redirige** l'affichage normale de l'exécution de *commande* vers *fichier*: `ls > listing.txt` Si ce fichier existe déjà, il sera **écrasé**, c'est à dire que son contenu sera remplacé!
commande >> *fichier*	Redirige l'affichage normale de l'exécution de *commande* vers *fichier*. Si ce fichier existe déjà, le résultat sera **ajouté** à la suite du contenu du fichier. Exemple: `ls >> listing.txt`
man *command*	Affiche l'aide ou le manuel en ligne d'une commande: `man ls`

Pour avoir des informations complémentaires sur ces commandes et outils, essayez ces options:

`command -h`

`command --help`

`man command`

`help command`

`info command`

Par exemple, pour avoir des informations complémentaires concernant la commande *ls*, saisissez l'une des deux possibilités suivantes:

```
ls --help
man ls
```

Les Outils

Les mots en italic sont les options que vous devez saisir.

Tool	Purpose
ping *hôte*	Vérifie l'interconnexion avec la machine *hôte*: `ping www.google.com`
traceroute *hôte*	Affiche la chemin que suivent les paquets pour atteindre la machine *hôte*: `tracert www.google.com`
ifconfig	Affiche les informations concernant les interfaces réseau actives (ethernet, ppp, etc.).
route	Affiche la table de routage
netstat	Affiche les informations concernant vos connexions réseau. `netstat -an`

Exercices

2.8 Identifiez le propriétaire du fichier **passwd**. (Note: localisez premièrement l'emplacement de ce fichier.)

2.9 Créez le dossier **travail** dans votre propre dossier d'accueil (home directory) (par exemple, si votre nom d'utilisateur est **fred**, créez dans le dossier /home/fred), et copiez le fichier passwd dans le dossier travail que vous venez de créer. Identifier le propriétaire du fichier passwd copié.

2.10 Créez le dossier **.caché** à votre emplacement actuel (notez que le nom du fichier commence par un point). Affichez le contenu de ce dossier. Qu'aviez-vous à faire pour afficher le contenu du dossier .caché?

2.11 Créez le fichier **test1** ayant le contenu, "Voici le contenu du fichier test1" dans le dossier actuel de travail. Créer le fichier test2 ayant le contenu, "Voici le contenu du fichier test2" dans le dossier actuel de travail. Copiez dans un fichier nommé **test,** les contenus des deux fichiers précédents..

Début du Jeu: les Options des Commandes

A seize ans, Jace oubliait quelques fois de respirer lorsqu'elle vivait dans les données. Peut être que cela était mieux à présent que l'air a eu un odeur de café torréfié. Le Directeur Adjoint, Mr. McGurky, l'a fixée avec un regard impatient pendant qu'elle le suppliait. "Mais les options de la ligne de commande sont la meilleure partie du système d'exploitation !" Les cheveux en couleur d'un expresso marron recouvraient la partie droite de son visage. Elle a baissé sa tête comme si elle allait cogner le moniteur sur son banc. Il ne s'est pas encore écarté d'une manière ou d'une autre de sa route, elle était déjà sur son clavier et défiait son ordinateur pour qu'il révèle les secrets de sa ligne de commandes.

"Regardez, voici comment nous pouvons trouver les commandes qui sont disponibles et ce qu'elles font. Nous pouvons saisir *help* ou la commandes suivi de *help* pour voir les options et ce qu'elles font. Regardez ça : nous pouvons combiner un lot d'options pour une seule commande qui en est séparée par une barre oblique (ou slash /)". Jace s'adressait directement au moniteur.

L'une des secrétaires était entrain d'appeler le département de la police locale, pensant que cette fille, hacker, allait les infecter avec un virus. Mais la police a juste sourit lorsqu'elle leur a expliqué la situation. L'officier de police a dit, "Jace, oui nous connaissons Jace. Elle est un bon enfant et elle connaît réellement les choses de son ordinateur. Il n'y a rien a craindre." Mais il pouvait dire que la secrétaire confuse n'était pas convaincu. "Elle était ici le mois dernier pour nous aider à paramétrer notre réseau. Dites lui juste que l'Officier Hank a dit qu'elle doit prendre une pause parce qu'elle le fait encore. Elle sait de quoi je parle, la dernière fois que je devait intervenir pour calmer un groupe de bibliothécaires après qu'elle soit entrée en conflit avec le groupe de technologie sur le fait que le port TCP zéro soit un port valide ou non."

La secrétaire ne s'est pas senti rassurée au moment où elle raccrochait. Elle n'était pas assez sûre de ce que cette fille faisait sur leurs ordinateurs. Et la dernière chose qu'elle a voulu c'était un autre virus qui couperait sa connexion Internet. Donc en essayant de ne pas trop s'accorder assez d'attention, en tremblant comme un petit enfant après une nuit de ruse et de menace, elle s'est dirigée vers l'interrupteur d'alimentation à côté de l'armoire à dossiers de Mr McGurky et elle a appuyé sur le bouton rouge, coupant l'alimentation du système informatique, de l'imprimante, du destructeur de papier, et autre. Jace est restée inactive lorsque l'écran s'est éteint. Elle a remarqué qu'elle l'a encore fait. Alors elle s'est rappelée de prendre un souffle. Mais c'était trop tard. Mr McGurky était déjà entrain d'écrire son nom sur des bouts de papiers pour une détention d'une semaine.

Fin du Jeu.

Le Système d'Exploitation: OSX

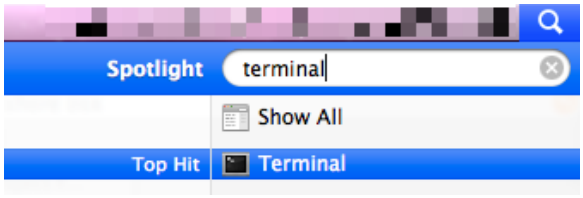
Comme dans Linux, lorsque vous travaillez sous OS X, vous exécutez les commandes dans une fenêtre d'Invite de commandes. Sous OS X cette application est désignée sous le nom de **Terminal**.

OS X est basé sur les versions NetBSD et FreeBSD d'UNIX, des ancêtres de Linux. Son interface graphique et sa Ligne de Commandes sont semblables à celle de Linux : vous pouvez faire tout ce que vous faites en interface graphique, via la ligne de commandes, et même plus.

> Certaines personnes pensent que Windows a voilé toute l'idée de l'interface graphique de Mac. En fait, les interfaces graphiques et les pointeurs de souris étaient utilisés dans des systèmes d'exploitation plus ancien. Vous pouvez savoir pratiquement plus que n'importe qui, de quel système d'exploitation s'agit-il.

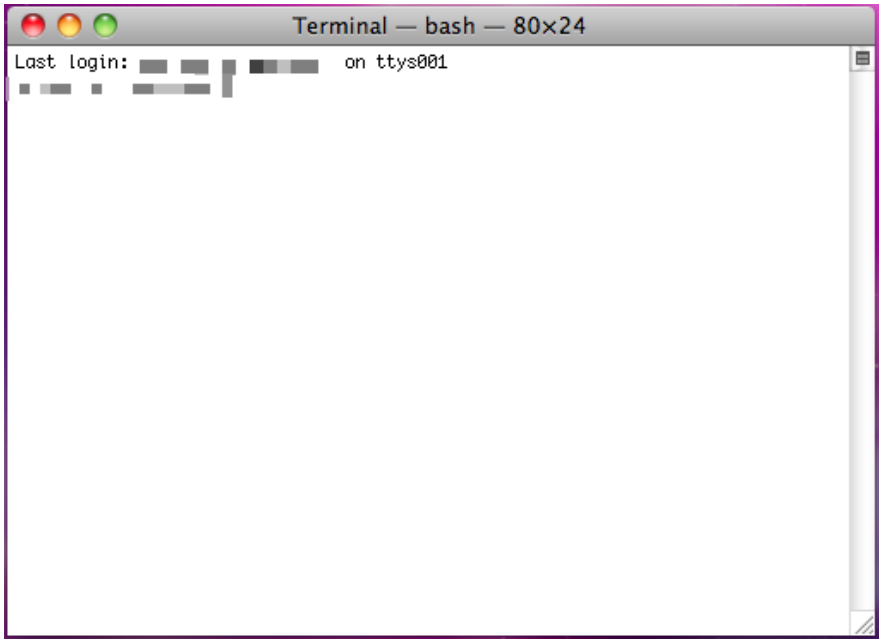
Comment ouvre t-on la fenêtre Terminal

1. Cliquez sur l'icône **Spotlight**, l'icône d'une loupe habituellement situé à l'angle supérieur droit de votre écran, recherchez **Terminal**.



2. Ensuite appuyez sur Entrer ou cliquez dessus. Vous verrez apparaître la fenêtre Terminal.

Habituellement Terminal se situe à l'emplacement suivant **Applications > Utilitaires**. Impressionnez vos amis en modifiant l'apparence du Terminal conformément à vos préférences. Appuyez simultanément sur la touche *commande* et *virgule* pour afficher la boîte de dialogue *Préférences* du Terminal et choisissez vos couleurs préférées. Habituellement ce raccourci clavier vous donne accès à la boîte de dialogue *Préférences* d'un programme sous OS X.



Les Commandes et les Outils (OSX)

Les systèmes Mac sont munis d'un shell bash, donc la plupart des commandes Linux fonctionnent aussi bien sous OS X.

Les Commandes

Les mots en italic sont des options que vous devez saisir.

Commande	Fonction
date	Affiche ou règle la date du système
time *command*	Affiche le temps nécessaire à l'exécution d'une *commande*.
fsck	effectue une vérification du système de fichiers et renvoie un rapport d'état. Si vous utilisez un système OSX qui comporte un journal tel que Mac OSX 10.3 ou ultérieur, dans lequel le journal est activé par défaut, vous n'aurez pas probablement besoin d'exécuter cette commande.
cat *file*	Affiche le contenu d'un ou de plusieurs fichiers textes: `cat /etc/passwd`
pwd	Affiche le nom du dossier dans lequel vous êtes actuellement.
hostname	Affiche le nom de l'ordinateur que vous utilisez actuellement.
finger *user*	Affiche les informations à propos d'un utilisateur: `finger root`

ls	Affiche le contenu du dossier actuel:
	
	`ls -la`
	Affiche le contenu d'un autre dossier:
	
	`ls -la /etc`

cd *chemin_vers_dossier*	effectue un déplacement, de l'emplacement actuel vers un autre dossier qui est spécifié par <*chemin_vers_dossier*>. Si le chemin vers un dossier n'est pas précisé, alors cette commande effectue un déplacement vers le dossier d'accueil de l'utilisateur en cours.
	
	Pour le nom d'utilisateur "fred" la commande
	
	`cd`
	effectue un déplacement vers /Users/fred, et
	
	`cd -`
	effectue un déplacement vers le dossier auquel vous avez eu accès récemment (pensez à la "soustraction" d'un dossier), et
	
	`cd /tmp`
	effectue un déplacement vers le dossier /tmp.

Commande	Fonction
cp *source destination*	Copie le fichier *source* vers le fichier *destination*. `cp /etc/passwd /tmp/bunnies`
rm *file*	Efface des fichiers. Seuls les utilisateurs ayant des droits d'accès appropriés (ou l'administrateur ou root) peuvent supprimer des fichiers spécifiques. `rm letter.txt`
mv *source dest*	déplace ou renomme des fichiers ou des dossiers. `mv secrets.zip innocent.zip`
mkdir *nom_dossier*	Crée un dossier dont le nom est <*nom_dossier*>. `mkdir tools`
rmdir *directory*	efface un dossier y compris son nom si et seulement si le dossier est vide `rmdir tools` Question Bonus: comment peut-on supprimer un dossier qui contient des fichiers ?
find / -name *nom_fichier*	recherche un fichier dont le nom est spécifié par <*nom_fichier*> à partir de la racine (/) du système. `find / -name myfile`
echo *chaîne_de_caractères*	affiche *chaîne_de_caractères* à l'écran : `echo hello`
commande > fichier	redirige l'affichage normal de l'exécution de *commande* vers *fichier*. `ls > listing.txt` Si le fichier existe déjà, l'exécution de cette commande écrasera le contenu du fichier !
command >> *fichier*	**Redirige** l'affichage normal de l'exécution de *commande* vers *fichier*. Si *fichier* existe déjà, son contenu ne sera pas écrasé ; l'affichage de la commande sera à la **suite** de l'ancien contenu. Exemple: `ls >> listing.txt`
man *command*	affiche l'aide d'une commande. Elle permet de voir l'explication des options d'une commande, sa syntaxe et autre : `man ls`

Pour avoir des informations complémentaires à propos d'une commande, essayez ce qui suit

```
command -h
command --help
man command
help command
info command
```

Par exemple, pour obtenir des informations complémentaires à propos de la commande *ls*, essayez les deux options suivantes :

```
ls --help
man ls
```

Les Outils

Les mots en italic sont des options à saisir.

Outil	Fonction

`ping` ***`host`***	*Vérifie* la connectivité avec la machine hôte.
	
	Cette commande envoie des paquets ping en utilisant le protocole ICMP (Internet Control Message Protocol) vers un autre ordinateur pour vérifier combien de temps ce dernier met pour répondre, ou bien s'il ne répond pas du tout. Vous pouvez utiliser un nom d'hôte ou une adresse IP comme paramètre pour la commande ping:
	
	`ping www.hackerhighschool.org`
	
	`ping 216.92.116.13`
	
	Les options sont:
	
	`ping -c 100 www.hackerhighschool.org`
	
	qui envoie 100 paquets ping, et
	
	`ping -t 216.92.116.13`
	
	envoie continuellement des paquets ping vers un hôte jusqu'à ce que la commande ne soit interrompue avec la combinaison CTRL+C.
	
	Pour voir plus d'obtions:
	
	`man ping`

Outil	Fonction

`traceroute` ***`host`***	Affiche les routeurs par lesquels passent les paquets avant d'atteindre l'*hôte* de destination.
	
	Traceroute : a le même champ d'actions que la commande *tracert* mais utilise des protocoles différents : *traceroute* utilise le *protocole UDP (User Datagram Protocol)* et *tracert* utilise le *protocole ICMP (Internet Control Message Protocol)*. Il se peut que vous obteniez des résultats différents en utilisant tracert ou traceroute à partir d'une même interface réseau
	
	Ces deux commandes vous permettent de vérifier les routeurs par lesquels passent les paquets pour joindre l'hôte de destination. Chacune de ces commandes vérifie le temps mis par un paquet pour atteindre l'hôte de destination, avec un nombre maximum de 30 routeurs. Habituellement vous verrez le nom des routeurs par lesquels passent les paquets :
	
	`traceroute www.hackerhighschool.org`
	
	`traceroute 216.92.116.13`
	
	Pour spécifier le nombre maximum (-m) de nœuds par lesquels doit passer un paquet traceroute, faites ceci :
	
	`traceroute -m 25 www.hackerhighschool.org`
	
	Pour interdire à la commande traceroute d'effectuer des résolutions de noms DNS, afin qu'elle affiche seulement les adresses IP au lieu des noms d'hôte, faites ceci :
	
	`traceroute -n 216.92.116.13`
	
	Pour voir plus d'obtions:
	`man traceroute`

Outil	Fonction

ifconfig	Cette commande lorsqu'elle est utilisée seule, elle affiche des informations à propos des interfaces réseau actives (ethernet, ppp, etc, ..) de votre système. Son fonctionnement est similaire à celui de la commande **ipconfig** sous Windows .
	
	Pour afficher plus de détails, c'est à dire le mode **verbeux**:
	
	`ifconfig -v`
	Pour afficher seulement les informations concernant l'interface réseau *en1:*
	
	`ipconfig en1`
	Pour désactiver l'interface:
	
	`ifconfig en1 down`
	Pour activer l'interface:
	
	`ifconfig en1 up`
	
	Note : vous devez avoir des droits d'administrateur pour exécuter cette commande ; donc il se peut que vous ayez besoin de saisir la commande **sudo** avant de saisir le reste. Ensuite le système vous demandera votre *mot de passe* avant de passer à l'exécution de la commande. **Servez-vous de la commande *sudo* avec précaution** !
	
	`sudo ifconfig en1 up`
	
	Pour voir plus d'options:
	
	`man ifconfig`

netstat	Affiche des informations concernant l'état du réseau et des connexions établies avec des machines distantes. Sur les systèmes dérivés de BSD, **netstat** permet aussi d'afficher la table de routage.
	
	Pour échantillonner toutes les connexions et les ports en écoute:
	
	`netstat -a`
	Pour afficher la table de routage:
	
	`netstat -r`
	Utilisez l'option -n pour afficher les adresses sous une forme numérique:
	
	`netstat -nr`
	Pour afficher les information concernant l'interface réseau *en1 :*
	
	`netstat -r -ii en1`
	Pour voir plus d'options:
	
	`man netstat`

Exercices

2.12 Identifiez le nom et l'adresse IP de votre machine.

2.13 Tracer le chemin vers www.hackerhighschool.org. Identifiez les adresses IP des routeurs intermédiaires et retrouver votre chemin.

2.14 Sous Windows utilisez **tracert** pour tracer le chemin entre vous et www.hackerhighscool.org tel que le verrait Windows, et redirigez l'affichage vers un fichier nommé **output.txt** pour une analyse ultérieure.

2.15 Ensuite exécutez l'équivalent de la commandes traceroute sous OSX et Linux à partir du même réseau, en envoyant respectivement les affichages vers les fichiers **output2OSX.txt** et **output2Linux.txt**. Analysez attentivement les fichiers contenant les affichages :

1. Les voies sont elles les même ou il y a des différences?
2. Avez-vous vu une ligne contenant:

* * *

Qu'est-ce que cela veut dire?

3. Répétez ceci au moins une heure plus tard. Est-ce que les résultats sont toujours les mêmes?

Les Commandes Essentielles et leur Equivalence pour Windows, OSX et Linux

Words in italics are options that you must enter.

Linux	OSX	Windows
command --help	command --help	*command* /h, *command* /?
man *command*	man *command*	help *command*
cp	cp	copy
rm	rm	del
mv	mv	move
mv	mv	ren
more, less, cat	more, less, cat	type
lpr	lpr	print
rm -R	rm -R	deltree
ls	ls	dir
cd	cd	cd
mkdir	mkdir	md
rmdir	rmdir	rd
netstat -r	netstat -r	route print
traceroute	traceroute	tracert
ping	ping	ping
ifconfig	ifconfig	ipconfig

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM