Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEÇON 2: QUELQUES COMMANDES ESSENTIELLES SOUS LINUX ET WINDOWS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Conditions d'utilisation de ce support

Ces leçons et supports sont gratuits et disponibles pour le public sous les conditions suivantes d'ISECOM:

Tous les travaux menés dans le cadre du "Hacker HighSchool" sont disponibles à usage non commercial auprès d'élèves du collège, du lycée, dans le cadre d'écoles publiques ou privées, ou encore lors de scolarisations à domicile. Ces supports ne peuvent être reproduits en vue d'un usage commercial. Il est expressément interdit d'utiliser ces supports dans le cadre de cours, leçons et/ou stages payants, à moins d'obtenir une licence pour cela (dans ce cas, veuillez aller sur *www.hackerhighschool.org/license*).

Le projet HSS (Hacker HighSchool) est un outil de travail et d'apprentissage, et en tant que tel, son utilisation relève de la personne qui l'utilise, et non de l'outil lui-même. ISECOM ne peut être mis en cause si cet outil est utilisé à mauvais escient ou de manière illégale.

Le projet HSS est aussi le fruit de l'effort de toute une communautés, et si vous trouvez ce projet intéressant, nous vous serions plus que reconnaissants de votre aide, soit par l'achat d'une licence, soit par un don, soit encore par un quelconque parrainage.

Table des matières

"License for Use" Information....2
Conditions d'utilisation de ce support....2
Personnes ayant contribué à ce projet....4
Traduction....4
2.1. Introduction et objectifs....5
2.2 Pré requis et démarrage....6
2.3 Environnement Windows....7
2.4 Linux....10
2.5 Exercices....12
Pour en savoir plus....13

Personnes ayant contribué à ce projet

Daniel Fernández Bleda, Internet Security Auditors

Jairo Hernández, La Salle URL Barcelona

Jaume Abella, La Salle URL Barcelona - ISECOM

Kim Truett, ISECOM

Pete Herzog, ISECOM

Marta Barceló, ISECOM

Traduction

Bénoni Martin

2.1. Introduction et objectifs

Cette leçon va vous rendre familier avec quelques commandes et outils essentiels utilisés sous Windows et Linux qui vous serviront ensuite pour mener à bien les exercices proposés.

A la fin de cette leçon, vous devriez maîtriser:

- Les commandes classiques sous Windows et Linux,
- Les utilitaires classiques comme :
    - ping
    - tracert
    - netstat
    - ipconfig
    - route

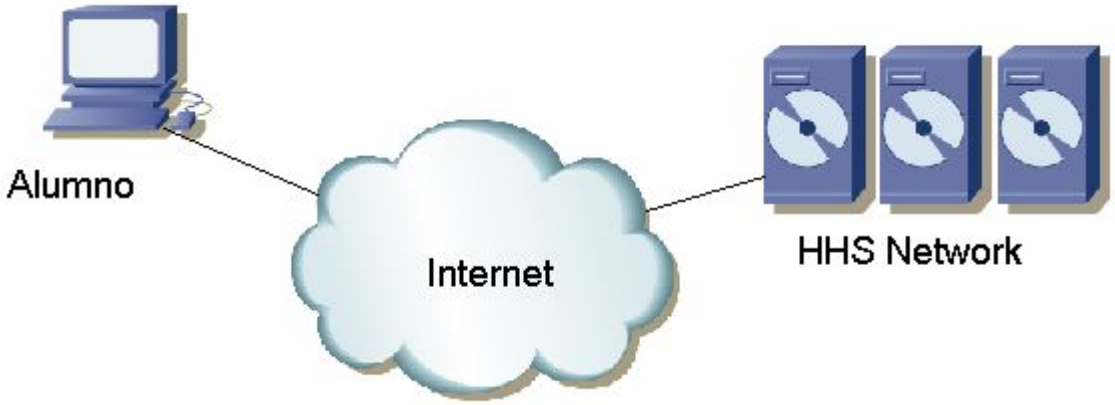
2.2 Pré requis et démarrage

2.2.1 Pré requis

Pour la leçon, nous aurons besoin:

- d'un PC avec Windows 98/Me/2000/NT/XP/2003
- d'un PC avec Linux Suze/Debian/Knoppix
- et d'un accès Internet

2.2.2 Démarrage



Ci-dessus votre environnement de travail. Il est composé de votre PC (avec accès Internet) et du réseau ISECOM Hacker HighSchool (auquel vous accéderez via Internet), réseau sur lequel vous ferez la plupart de vos tests.
Veuillez noter que l'accès au réseau de test d'ISECOM est restreint. Pour y avoir accès, votre instructeur doit contacter au préalable notre administrateur système, comme détaillé sur www.hackinghighschool.org.

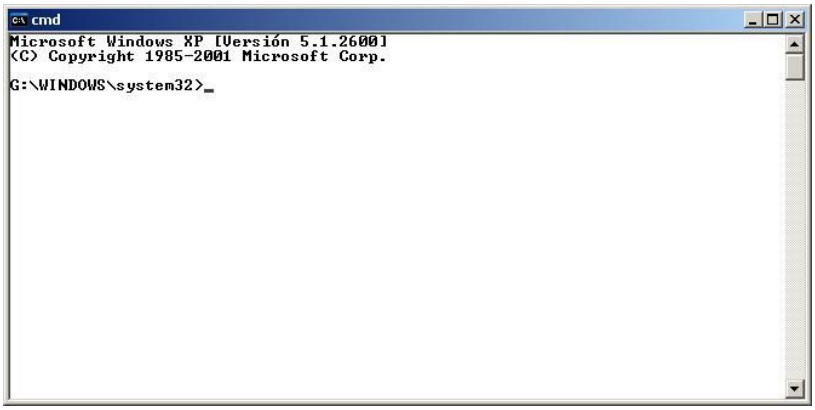
2.3 Environnement Windows

Beaucoup des outils utilisés ici sont des commandes internes à Windows. Par conséquent, nous allons vous expliquer comment ouvrir une fenêtre de commandes sous Windows.

2.3.1 Comment ouvrir une fenêtre MS-DOS Windows

Pour pouvoir lancer une commande interne, il vous faut au préalable ouvrir une fenêtre MS-DOS comme ci-dessous:

1. Cliquez sur "Démarrer",
2. Choisissez "Exécuter"",
3. Tapez "command" si vous utilisez Windows 95/98 ou "cmd" pour toutes les autres versions de Windows, puis cliquez sur OK.
4. Une fenêtre comme celle ci-dessous devrait s'ouvrir:



5. Maintenant, les commandes et utilitaires listés ci-dessous peuvent être lancés.

2.3.2 Utilitaires et outils (Windows)

Utilitaires

date	Affiche / permet de régler la date du système.
time	Affiche / permet de régler l'heure du système.
ver	Affiche la version MS-DOS utilisée.
dir	Affiche le contenu d'un répertoire.
cls	Rafraîchit l'écran
mkdir, md *répertoire*	Créé un répertoire de nom "répertoire". Ex : md outils.
chdir, cd *<répertoire>*	Affiche le nom du répertoire courant, ou permet d'aller dans le répertoire "répertoire".
rmdir, rd *<répertoire>*	Supprime le répertoire "répertoire". Ex: rd outils.
tree *<répertoire>*	Affiche l'arborescence d'un répertoire. Ex: tree C:\outils.
chkdsk	Vérifie un disque et affiche le résultat.
mem	Donne des informations sur l'utilisation de la mémoire du système

rename, ren *<src.> <dest.>*	Renomme certains fichiers. Ex: ren ancienFichier nouveauFichier
copy *<source> <destination>*	Copie un ou plusieurs fichiers d'un endroit à un autre. Ex: copy C:\outils\monfichier.txt C:\tmp
move *<source> <destination>*	Déplace des fichiers et renomme des fichiers/répertoires. Ex: move C:\outils C:\tmp
type *<fichier>*	Affiche le contenu d'un fichier texte. Exemple: type C:\outils\monfichier.txt
more *<fichier>*	Affiche le contenu d'un fichier écran par écran. Exemple: more c:\outils\monfichier.txt
delete, del *<fichier>*	Supprime un ou plusieurs fichiers. Exemple: del c:\outils\monfichier.txt

Remarque. Les mots en italique dans le tableau ci-dessus ne sont pas des commands et doivent donc être remplacées par les valeurs souhaitées. Certaines de ces commandes peuvent être exécutées soit en tapant la commande entière, soit son abréviation, par exemple "delete" et "del" sont la même commande.

ping *cible*	Vérifie si la machine cible répond. Cette commande envoie des paquets ICMP (Internet Control Message Protocol) à un autre ordinateur afin de savoir si ce dernier est sur le réseau. En plus, il affiche certaines statistiques comme le pourcentage de paquets qui n'ont pas reçu de réponse ainsi que le temps de réponse pour les autres. Comme cible, nous pouvons utiliser aussi bien le nom de la machine que son adresse IP. Exemples: ping www.google.com ou ping 193.145.85.2 Quelques options de cette commande sont: -n N. On envoie N paquets. -f. On envoie des pings tant qu'un CTRL + C n'arrête l'envoi. Pour voir les autres options: ping /h.
tracert *cible*	Montre la route que les paquets suivent pour atteindre la machine *cible*. La commande *tracert* est l'abréviation de trace route, qui permet de connaître le chemin à suivre pour atteindre la cible, avec le temps mis pour chaque étape. Le maximum d'étapes pouvant être affichées est de 30. Il est en effet quelque fois intéressant de connaître le nom des machines via lesquelles ont transité nos messages avant d'atteindre leur cible. Exemples: - h N. Spécifie le nombre maximal de sauts (N). -d. N'affiche pas le nom des machines. Pour plus d'options: tracert
ipconfig	Affiche des informations sur les interfaces actives (ethernet, ppp, etc.) de l'ordinateur. Quelques options: /all. Affiche plus de détails. /renew *nom*. Renouvelle la connexion "nom" (si la carte est en DHCP). /release *nom*. Désactive toutes les connexions correspondant à *nom* (toujours si DHCP est utilisé). Pour plus d'informations: ipconfig /?

route print	Affiche la table de routage. Cette commande sert à définir/effacer des routes statiques ou simplement lister les routes actives. Quelques options: print. Affiche la liste des routes. delete. Supprime une route. add. Ajoute une route. Pour plus d'options: route / ?
netstat	Affiche des informations sur l'état d'un réseau et établit des connexions vers des machines distantes. Quelques options: -a. Liste les connexions courantes avec les ports associés. -n. Liste les connexions courantes avec les ports associés (). -e. Affiche des statistiques Ethernet. Par exemple: netstat -an Pour plus d'options: netstat /?

Pour plus d'informations sur ces commandes et outils, tapez "command /h" ou "command / ?", ou encore "help commande" d'une fenêtre MS-DOS.

Par exemple, pour obtenir plus d'informations sur la commande netstat, nous avons 3 possibilités:

- netstat /h
- netstat /?
- help netstat

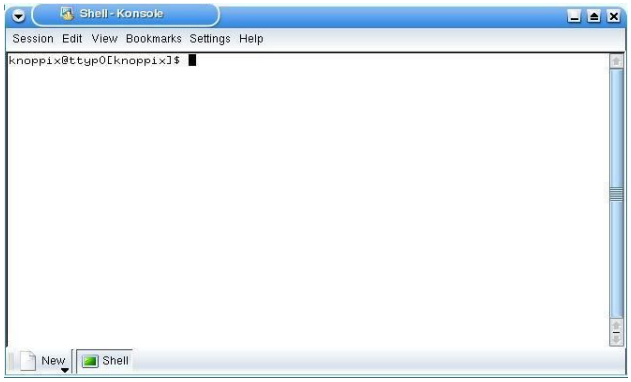
2.4 Linux

De même que sous Windows, la plupart des commandes exécutées sous Linux se font à partir d'une console. Ainsi, nous allons maintenant voir comment faire pour ouvrir une telle console sous Linux.

2.4.1 Comment ouvrir une console

Pour pouvoir lancer une commande interne, il vous faut au préalable ouvrir une console:

1. Cliquez sur le bouton "Démarrer l'application",
2. Choisissez "Exécuter la commande",
3. Tapez "konsole".
4. Une fenêtre comme celle ci-dessous devrait s'ouvrir:



5. Maintenant, les commandes et utilitaires listés ci-dessous peuvent être lancés.

2.4.2 Utilitaires et outils (Linux)

pwd	Affiche le chemin du répertoire courant.
hostname	Affiche le nom réseau de notre ordinateur.
finger *user*	Affiche des informations système sur user.
ls	Liste le contenu des répertoires.
cd *répertoire*	Change le nom du répertoire courant en *repertoire*. Si aucun nom n'est spécifié, il nous place dans le répertoire racine. Exemple: Pour le login "monlogin", la commande "$cd" change le répertoire en "/home/monlogin" Exemple: "$cd -" nous redirige vers le dernier répertoire visité. Exemple: "$cd /tmp" nous redirige vers le répertoire tmp.
cp source dest	Copie des fichiers. Copie le fichier *source* vers le fichier *dest*. Exemple: cp /etc/passwd /tmp
rm *fichier*	Supprime des fichiers. Copie le fichier *source* vers le fichier *dest*.
mv *source dest*	Déplace ou renomme des fichiers/répertoires. Exemple: mv anciennom nouveaunom
mkdir *répertoire*	Créé un répertoire appelé répertoire. Exemple: mkdir outils
rmdir *répertoire*	Supprime le répertoire appelé répertoire s'il est vide. Exemple: rmdir outils

find / -name *fichier*	Cherche un fichier se nommant "fichier" en partant de la racine. Exemple: find / -name monfichier
echo *chaine*	Ecrit la chaîne chaine sur la sortie standard. Exemple: echo chaine
commande > fichier	Redirige la sortie de "commande" vers le fichier "fichier" Exemple: ls > monls
commande >> fichier	Redirige la sortie de "commande" vers le fichier "fichier". Si le fichier existe, il rajoute la sortie à la fin de ce fichier. Exemple: ls >> monls
man *commande*	Affiche les pages d'aide sur la commande "commande". Exemple: man ls

Remarque. Les mots en italique dans le tableau ci-dessus ne sont pas des commands et doivent donc être remplacées par les valeurs souhaitées. Pour plus d'informations sur l'utilisation de ces commandes et outils, tapez "commande -help" ou "man commande" dans la console.

Par exemple, pour plus d'informations sur la commande "ls", vous avez deux possibilités:

1. ls –help
2. man ls

ping *cible*	Vérifie si la machine cible répond. Exemple: ping www.google.com
traceroute *cible*	Montre la route que les paquets suivent pour atteindre la machine *cible*. Exemple : tracer
ifconfig	Affiche des informations sur les interfaces actives (ethernet, ppp, etc.) de l'ordinateur.
route	Affiche la table de routage.
netstat	Affiche des informations sur l'état d'un réseau et établit des connexions vers des machines distantes. Par exemple: netstat -an

Quelques équivalences entre les commandes Windows et Linux

Les équivalences entre quelques commandes basiques entre Linux et Windows sont regroupées dans le tableau ci-dessous. Les commandes sont exécutées à partir d'un shell (sous Linux) ou d'une fenêtre MS-DOS (sous Windows):

Linux	Windows
command --help	command /h, command /?
man command	help command
cp	copy
rm	del
mv	move
mv	ren
more, less, cat	type
lpr	print
rm -R	deltree
ls	dir
cd	cd

mkdir	md
rmdir	rd
route	route print
traceroute –I	tracert
ping	ping
ifconfig	ipconfig

2.5 Exercices

2.5.1 Exercices sous Windows

1. Ouvrez une fenêtre MS-DOS
2. Identifiez la version MS-DOS que vous êtes en train d'utiliser. Quelle version avez-vous détectée ? Quelle commande avez-vous lancée ?
3. Regardez l'heure et la date de votre système. Si nécessaire, mettez-les à jour. Avec quelle commande l'avez-vous fait ?
4. Listez tous les répertoires se trouvant dans "C:\". Quelle commande avez-vous utilisé ?
5. Créez le répertoire C:\hhs\lecon0 et copiez-y tous les fichiers de C:\ avec une extension ".sys". Quels fichiers avez-vous trouvé et quels outils avez-vous utilisés ?
6. Trouvez votre adresse IP. Quelle commande avez-vous utilisé et quelle est votre adresse IP ?
7. Identifiez la route qui sépare votre machine de www.google.com et recherchez les adresses IP des routeurs intermédiaires.

2.5.2 Exercices sous Linux

1. Identifiez le propriétaire du fichier "passwd" après avoir cherché son emplacement. Quelle commande avez-vous utilisé ?
2. Créez un répertoire "travail" dans votre répertoire personnel: par exemple si vous vous connectez en tant que "monlogin", créez alors le répertoire "/home/monlogin", et copiez le fichier "passwd" dans ce répertoire "travail". Identifiez le propriétaire du fichier "passwd" qui a été copié.
3. Créez un sous répertoire".cache" dans le répertoire "travail" et listez le contenu de ce répertoire. Qu'avez-vous du faire pour afficher le contenu de ce répertoire ?
4. Créez le fichier "test1" dans le répertoire "travail" et écrivez-y "ceci est le contenu du fichier 1". Faites de même avec un fichier "test2". Puis copiez le contenu des deux précédents fichiers dans un troisième fichier "test". Quelles commandes avez-vous utilisé ?
5. Trouvez votre adresse IP. Quelle commande avez-vous utilisé et quelle est votre adresse IP ?
6. Identifiez la route qui sépare votre machine de www.google.com et recherchez les adresses IP des routeurs intermédiaires.

2.5.3. Exercice 3

Complétez la table suivante avec les équivalences Linux / Windows. Par exemple la commande Linux "commande -help" équivaut à "commande / ?" sous Windows, ou encore le pendant sous Windows de "cp" est "copy".

	
command --help	command / h
cp	copy
	del
mv	
more	
	print
	deltree
ls	
cd	
	md
	rd
route	
	tracert
Ping	
	ipconfig

Pour en savoir plus

Pour un glossaire exhaustif consultez :

- http://www.matisse.net/files/glossary.html
- http://www.uic.edu/depts/accc/inform/v106.html
- http://www.catb.org/~esr/jargon/

La commande Windows "-" vous permet d'avoir plus d'informations sur les commandes existantes, de même que les commandes "commande / ?", "commande /h" ou "help commande" depuis une fenêtre MS-DOS.

La commande Linux "-" vous permet d'avoir plus d'informations sur les commandes existantes, de même que les commandes "commande --help" ou "man commande".