TD1 - Sécurité

1 - Voici quelques manipulations sous Windows

A – Démarrages divers

Essayez diverses formes de démarrage de votre machine :
Démarrage en mode sans échec sous Windows
Démarrage à partir d'une clé USB

B - Commande « arp » (Attention, il faut être administrateur)

- Quel est le résultat de la commande : arp
- Modifier l'adresse « Mac » de votre machine :
commande : arp –s @ip @mac
Aller sur google, que se passe-t-il ?

C- Modification des tables de routage (Attention, il faut être administrateur)

La commande « route » modifie le contenu d'une table de routage. A l'aide de la commande man consultez les options de « route » puis supprimez quelques routes de la table et essayer le navigateur.

D - Les traces sur le net

Dans le panneau de configuration, cliquez sur Options Internet. Dans l'onglet général rubrique Historique de Navigation sélectionnez l'option « paramètres » puis demandez à afficher les fichiers. Que voyez-vous ?

Les visites de sites Web laissent beaucoup de traces sur votre machine. Pour vérifier cela allez sur différents sites : www.anonymat.org/vostraces/index.php

E - Commande « ipconfig »

Grâce à cette commande il est possible de :
- visualiser le contenu du cache DNS de la machine (/displaydns)
- vider le cache (/flushdns)

Essayez ces commandes.

F – Aspirateur de site

Téléchargez l'aspirateur de site httrack à l'adresse suivante :
http://www.httrack.com/page/2/fr/
Apres l'avoir installé, lancer l'application sur un site de votre choix.
Que se passe-t-il ?

G – TELNET

L'échange « Telnet » repose généralement sur une authentification par login et mot de passe. Mais il n'assure pas la protection des mots de passe contre l'écoute d'un sniffer. Les mots de passe associés du login circulent en clair sur le réseau.
Lancez le mode « invite de commande » Dos, et executez la commande Telnet pour vous connecter sur des services différents.
La syntaxe est : telnet www.site.fr N°port

Exemple 1 :
telnet www.free.fr 80
puis taper : GET / http/1.0

Exemple 2 :
telnet ftpperso.free.fr 21

220 Serveur de mise a jour des pages perso de Free.fr version [Sep 27 2007 15:55:37]
USER ffctlr
331 Password required for ffctlr.

PASS toto
230 User ffctlr logged in.
PWD
257 "/" is current directory.

QUIT

H – Analyseur de trames

Téléchargez wireshark à l'adresse suivante :
http://www.01net.com/telecharger/windows/Utilitaire/reseau/fiches/3590.html
Apres l'avoir installé, lancer l'application, et observez ce qui se passe. Que se passe-t-il ?
Allez sur un site web et observez ce qui se passe. Essayez d'identifier les paquets relatifs à cette connexion au site.
Lancez une application qui doit aller sur le web (et si possible qui nécessite une connexion par login), essayez d'identifier les paquets relatifs à cette connexion. Que voyez vous ?

I – Scanner
Téléchargez Avanced port Scanner à l'adresse suivante :
http://www.01net.com/telecharger/windows/Utilitaire/reseau/fiches/101523.html
Apres l'avoir installé, lancer l'application. Que se passe-t-il ?
Choisissez une plage d'adresses de votre choix. Que se passe-t-il ?

J – Keylogger
Téléchargez Keylogger gratuit à l'adresse suivante :
http://www.01net.com/telecharger/windows/Multimedia/webcam_et_surveillance/fiches/125094.html
Apres l'avoir installé l'application, faites quelques manipulations sur votre machine (saisie d'un texte, navigation sur le web, connexion a une site, etc …)
Ouvrez l'application, à partir de l'icône située dans la barre en bas de votre machine. Que voyez-vous ?

K – Fichiers cachés
Le système garde une multitude de fichiers non visibles car cachés. Ces fichiers ont pour objectif de mémoriser des paramètres ou de garder des informations pour optimiser le système.

Sous windows :
Lancez le mode « invite de commande » Dos. Avec la commande « dir /a » ,
Visualisez le contenu du dossier « AppData\Local\Microsoft\Windows\Temporary Internet Files» et des sous répertoires qui s'y trouvent (vous pouvez utiliser la commande : dir /a /s | more)
Recommencez pour les dossiers ci-dessous :
C:\Users\xxx\AppData\Local\Mozilla\Firefox
C:\Users\xxx\AppData\Local\Mozilla\Firefox\Profiles\ie9r0dog.default\thumbnails

Sous Linux :
Lancez le « terminal » et visualisez le contenu du répertoire :
/home/xxxx/.cache/mozilla/firefox/xxxxxx.default (ou xxx est votre nom de login).

Remarque : s'il le faut demander à afficher les fichiers cachés dans l'option « affichage »