TD séance n° 15
Internet et Sécurité

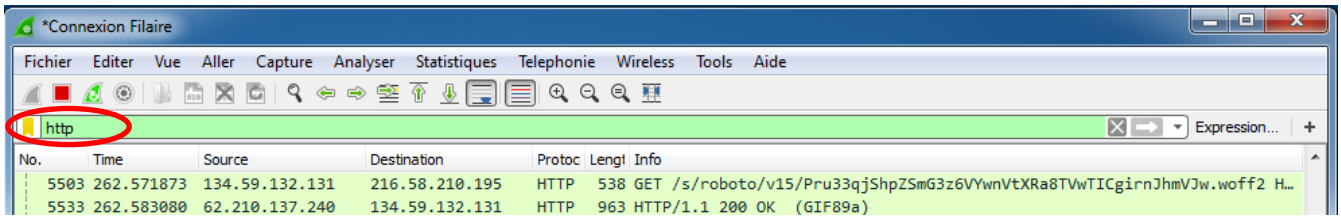
Exercices

Nous allons réaliser ce TD à la fois sous les environnements Linux et Windows. *Les premiers exercices sont à réaliser sous Windows*. Nous signalerons quand changer d'environnement, mais vous devez être à l'aise avec cela maintenant.

4 Exercices obligatoires

4.1 Ecouter les messages sur l'interface réseau d'une machine

Il est possible « d'écouter » les messages qui circulent sur l'interface réseau d'une machine. Un outil simple pour réaliser cette opération est d'utiliser le logiciel *WireShark*[1] à l'aide des ressources du TD. Installez le logiciel sur votre machine (il sera important d'ajouter l'installation de *WinPcap* si l'option n'est pas cochée). Puis au lancement du logiciel, sélectionnez la (ou les) interface(s) que vous souhaitez espionner.
Vous pouvez constater la quantité de trafic réseau qui passe sur cette interface (et pourtant vous ne faites rien de particulier). Pour éviter d'avoir trop d'informations, nous allons sélectionner le filtrage suivant le protocole HTTP et ainsi n'écouter que les échanges sur le réseau qui concernent ce protocole (ah ! c'est un peu plus calme).



Exercice n°1:

Ouvrez un navigateur Internet sur la même machine. Connectez-vous à l'adresse http://www.unice.fr/.
Que constatez-vous ? (par exemple, y'a-t-il un seul ou plusieurs message).

De nombreux messages sont échangés pour une seule requête à l'adresse http://www.unice.fr

Exercice n°2:

Remontez dans la liste des messages sur un message du type : `HTTP GET /index.html HTTP/1.1`.
A quoi correspondent les autres messages ?

L'ensemble des messages correspondent à la demande et à la réception de tous les élements qui constituent la page à afficher (les différentes images, vidéo, ...)

Exercice n°3:

Si je souhaite savoir quels sont tous les nouveaux mails qui sont consultés par la ou les personnes sur la machine, quel est le protocole que je dois surveiller à la place d'HTTP ? Et je peux vous assurer que nous serions alors capables de lire le contenu des mails reçus par la personne sur ce poste de travail. Toutefois pour gagner du temps, nous ne le ferons pas ici.

Il faut surveiller tous les messages qui tutilisent le protocole IMAP pour visualiser l'ensemble des mails reçus par le client.

Et si nous souhaitions espionner tous les mails que la personne envoie et à qui ?

Il faut alors surveiller les messages utilisant le protocole SMTP.

[1] http://www.wireshark.org/

TD séance n° 15
Internet et Sécurité

Exercice n°4:

Si je souhaite espionner tous les messages que les machines de la salle échangent avec l'extérieur du réseau local pendant la durée du TD, où dois-je écouter. Justifier avec les connaissances antérieures que vous avez acquises.

Il suffit alors d'écouter sur la passerelle qui permet de sortir du sous-réseau.

Vous comprenez maintenant l'importance de sécuriser les communications que vous avez avec les autres ? Avec l'utilisation d'un protocole sécurisé (HTTPS par exemple), on peut toujours voir les messages passer mais les lire ne sert à rien car le message est incompréhensible si l'on a pas la clé de déchiffrement.

4.2 Connexion à distance : accès à un terminal distant via SSH

Nous allons maintenant utiliser un client `ssh` pour nous connecter à un serveur `ssh`. L'établissement de cette connexion se fera donc de manière sécurisée et tous les messages qui seront échangés entre les deux machines seront cryptés (chiffrés). Installez pour cela le logiciel `putty` qui est un client `ssh` pour votre machine Windows (vous trouverez `putty` dans l'archive des ressources du TD).

Exercice n°5: Connexion avec authentification simple depuis Windows

Nous allons nous connecter sur un des serveurs ssh de Polytech'Nice Sophia. Il y a actuellement deux serveurs qui vous permettent de vous connecter en ssh : `morag.polytech.unice.fr` et `carabosse.polytech.unice.fr`.
Choisissez l'un ou l'autre des serveurs et connectez-vous à l'aide de vos identifiants Polytech'Nice Sophia (les mêmes que ceux que vous utilisez pour vous connecter sur la machine physique).
A l'aide de quel outil pouvez-vous vérifier que n'avez pas de soucis à vous faire quant à la confidentialité ?

Il est possible d'utiliser Wireshark que nous avons utilisé précédemment et de filtrer les messages concernant le protocole SSH.

Dire ce que vous voyez à l'aide de cet outil qui peut vous rassurer sur la confidentialité des messages échangés ?

Après les premiers échanges de messages sur l'initialisation du protocole (`SSH-2.0`) et l'information de clé envoyée, les messages suivants sont du type « Encrypted packet » ce qui montre bien que le contenu des mesages n'est pas compréhensible.

Nous allons maintenant tenter de faire une connexion avec authentification par clé. Il est donc nécessaire de générer nos propres clés. *Les exercices suivants sont à faire sous Linux (nous reviendrons sous Windows plus tard, cela vous sera précisé).*

Exercice n°6: Génération d'une paire de clés publique/privée depuis Linux

Quelle est la commande sous Linux pour générer la paire de clé publique/privée ? Donnez la commande qui permet de générer des clés RSA d'une longueur de `4096` bits. Attention quant à l'utilisation de cette commande : elle vous demande d'abord le nom de fichier où sauvegarder la clé (faire entrer pour conserver le fichier par défaut), puis il vous demande la passphrase pour protéger votre clé privée. Ne pas mettre une passphrase vide et évitez d'utiliser votre mot de passe de compte.

La commande sous Linux qui permet de générer les clés est `ssh-keygen`.

```
ssh-keygen -t rsa -b 4096
```

Quels sont les fichiers qui ont été créés et dans quel dossier ? Quels sont les droits sur ces fichiers ? Expliquez la raison de ces droits ?

Les fichiers créés sont `id_rsa` et `id_rsa.pub`. Les droits sur `id_rsa.pub` sont en lecture pour tous car c'est ma clé publique, donc tout le monde peut y avoir accès. Par contre les droits sur le fichier `id_rsa` sont en lecture pour moi seul car c'est ma clé privée qui doit restée secrète.

Exercice n°7: Connexion avec authentification simple depuis Linux

TD séance n° 15
Internet et Sécurité

Toujours sous Linux, donnez la commande pour vous connecter avec votre nom d'utilisateur Polytech'Nice Sophia sur la machine `morag.polytech.unice.fr`.

`ssh login@morag.polytech.unice.fr` avec `login` qui doit être remplacé par votre propre identifiant.

Comment pouvez-vous vous assurer à tout moment dans votre terminal sur quel machine vous travaillez ? Pour vous déconnecter du serveur `morag` et revenir sur votre machine, il vous suffit de taper la commande `exit`.

Le nom de la machine est inscrit dans le terminal avant le prompt (finissant par le symbole $) qui attend vos nouvelles commandes.

Exercice n°8: Copie de la clé publique sur le serveur pour une authentification par clé

Pour arriver à faire une authentification par clé, il est nécessaire d'aller enregistrer la clé publique sur le serveur. La commande permettant de faire cette copie à l'aide de `ssh` est la commande `scp`. Cette commande utilise le protocole SSH pour faire la copie d'un fichier d'une machine à une autre. Vous procéderez donc de la manière suivante :

```
scp ~/.ssh/id_rda.pub login@morag.polytech.unice.fr:mypubkey
```

Pourquoi copier la clé publique et pas la clé privée ?

La clé privée doit toujours restée secrète donc ce n'est pas celle qu'il faut fournir au serveur.

Pour que le serveur la connaisse, il est nécessaire de l'ajouter dans le fichier `.ssh/authorized_keys`. Reconnectez-vous donc sur le serveur `morag.polytech.unice.fr`.

```
ssh login@morag.polytech.unice.fr
```

Dans le cas où le fichier `.ssh/authorized_keys` n'existe pas, donnez la commande qui permet de déplacer le fichier `mypubkey` au bon endroit avec le bon nom.

```
mv ~/mypubkey ~/.ssh/authorized_keys
```

Dans le cas où le fichier `.ssh/authorized_keys` existe, donnez la commande qui permet d'ajouter à la fin du fichier existant la clé contenue dans le fichier `mypubkey`.

```
cat ~/mypubkey >> ~/.ssh/authorized_key
```

Exercice n°9: Connexion avec authentification par clé

Déconnectez-vous de `morag` et tentez de vous reconnecter. Quelle différence constatez-vous ? Pourquoi ?

```
ssh login@morag.polytech.unice.fr
```

Ce n'est pas le mot de passe qui m'est demandé, mais la passphrase de ma clé privée. Je réalise donc une connexion avec une authentifcation par clé et pas une authentification par mot de passe simple.

Exercice n°10: Connexion avec un agent sous Linux

Maintenant que nous pouvons nous connecter par clé, nous pouvons utiliser un agent qui mémorisera en mémoire la passphrase utilisée pour éviter d'avoir à la retaper à chaque connexion distante. Pour cela, il faut faire les actions suivantes :

`ssh-agent`

Copier/coller les variables d'environnement qui s'affichent

`ssh-add ~/.ssh/id_rda`

Saisir la passphrase

Maintenant, connectez-vous sur `morag`. Que constatez-vous ?

```
ssh login@morag.polytech.unice.fr
```

Lors de cette nouvelle connexion, plus aucune authentification ne m'est demandée. En fait, le programme ssh-agent a mémorisé ma passphrase (pour la durée de ma session) et répond directement lors de la demande de celle-ci sans que j'ai à la retaper.

TD séance n° 15
Internet et Sécurité

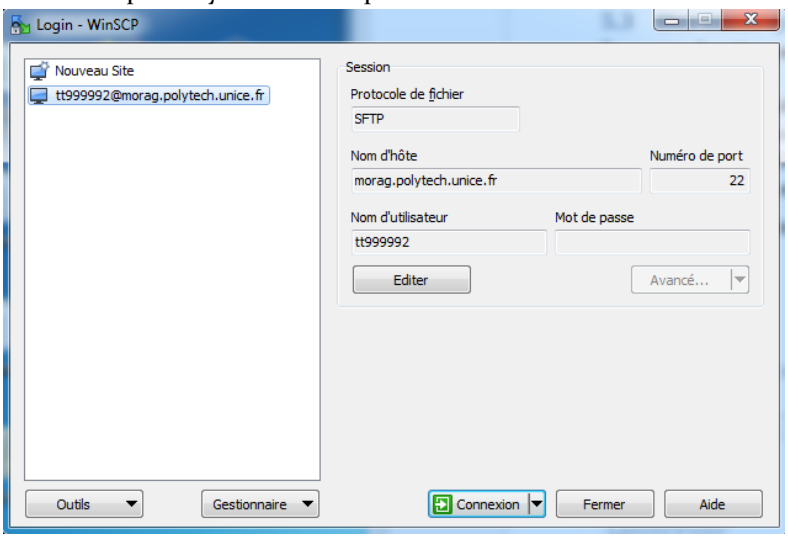
4.3 Des outils qui utilisent SSH pour copier des fichiers à distance ou les éditer

Pour cette dernière partie du TD, *nous retournons sous Windows*.

Se connecter de manière distante à une machine permet de travailler sur celle-ci. Mais il est aussi possible d'avoir accès uniquement aux fichiers qui se trouvent sur cette machine distante à l'aide du même protocole SSH. Pour cela, vous pouvez utiliser un logiciel qui vous affichera le contenu des fichiers sur la machine distante en ouvrant une connexion SSH, et donc de manière sécurisée

Exercice n°11: Accès aux fichiers d'un compte distant

Installez le logiciel WinScp qui vous est fourni dans les ressources du TD. Configurez le de manière à vous connecter sur `morag` à l'aide de votre compte Polytech'Nice Sophia.



Quel est le type d'authentification qui est utilisé si vous ne faites aucune configuration particulière ?

L'authentification par défaut est l'authentification simple avec l'identifiant et le mot de passe Polytech.

Exercice n°12: Récupération des fichiers de clés générés sous Linux depuis Windows

Une fois connecté, récupérez les fichiers de clés publique/privée de votre compte sur votre ordinateur Windows. Pourquoi le dossier .ssh n'apparaît pas ?

C'est un dossier caché car nous avons vu sous Linux que les fichiers et dossiers commençant par un point sont cachés.

Pour vous y rendre, il vous suffit de double-cliquer sur le chemin /sfe/home/... pour y ajouter .ssh. Copiez le fichier `id_rsa` sur votre machine Windows. A quoi correspond ce fichier ?

Le fichier id_rsa correspond à ma clé privée. Il faut donc faire très attention à ne pas le communiquer à qui que ce soit.

Les outils sous Windows utilisent un autre format de sauvegarde des clés. C'est l'outil `PuttyGen` permet de créer ou d'importer et convertir des clés pour une utilisation sous Windows.

Exercice n°13: Import d'une paire de clés publique/privée pour une utilisation depuis Windows

Grâce au menu conversion, importer votre clé privée. Le programme vous demande la passphrase pour garantir que vous êtes bien l'utilisateur que vous prétendez être. Sauvegardez cette clé privée dans un fichier .ppk grâce au bouton « Save Private Key ».
Détruisez le fichier `id_rsa` et vider votre corbeille pour que celui-ci ne tombe pas entre de mauvaises main.

Exercice n°14:

TD séance n° 15
Internet et Sécurité

Sous WinScp, éditez la configuration existante puis aller sur « Avancé… ». Dans la section SSH / Authentification, renseignez le chemin pour votre clé privée (fichier .ppk). Sauvegardez votre profil et tentez une connexion sur le serveur morag.polytech.unice.fr. Vous devez maintenant faire une authentification par clé. Qu'est-ce qui vous permet de vous en assurer ?

Le logiciel demande maintenant d'entrer la passphrase et plus le mot de passe du compte.

Exercice n°15: Connexion avec un agent sous Windows

Comme sous Linux, il est possible d'utiliser un programme agent sous Windows pour mémoriser votre passphrase et vous éviter de taper celui-ci à chaque nouvelle connexion. Le programme sous Windows est `Pageant`. Lancez ce programme (il démarre la zone des programmes en bas à droite de l'écran), ajoutez votre clé privée et donnez votre passphrase. Il mémorise ces informations tant qu'il s'exécute (si vous fermez la fenêtre, il continuera à s'exécuter jusqu'au prochain redémarrage de Windows).

Après avoir quitté WinScp si ce n'est déjà fait, relancez-le. Il ne doit plus vous demander votre mot de passe car `pageant` lui fournit automatiquement. Avez-vous réussi à faire cette connexion sans passphrase ni mot de passe à rentrer manuellement ?

Oui, bien sûr c'est trop facile ! ☺

Et voilà, vous avez accès sans mot de passe ou sans passphrase à votre compte Polytech'Nice Sophia depuis votre machine Windows. Durant ce TD, nous avons fait ces manipulations depuis la machine virtuelle Windows, mais bien entendu, cela pourrait être réalisé depuis votre machine à la maison pour vous permettre de récupérer vos fichiers sur votre compte Polytech'Nice Sophia à la maison ! Elle est pas belle la life !

TD séance n° 15
Internet et Sécurité

Pour aller plus loin

Pourquoi recopier un fichier depuis les serveurs de Polytech sur ma machine locale (mon PC sous Windows par exemple) alors que je pourrai directement l'éditer sur le serveur. Bien sûr, il faut que cela soit sécurisé, donc je vais le faire avec SSH, bien sûr !

Pour éditer un fichier sur la machine distante, il est toujours possible de se connecter sur celle-ci et d'utiliser un éditeur dans la console de connexion (que l'on a pu obtenir avec `putty`). Mais il est aussi possible d'éditer un fichier sur la machine distante avec un éditeur comme Notepad++, ce qui est tout de même beaucoup plus confortable à l'utilisation.

Exercice n°16: Edition à distance de fichiers avec Notepad++ sous Windows

Après avoir installé Notepad++, aller dans le menu « *Compléments* » puis « *Plugin Manager* / *Show Plugin Manager* ». Dans la liste, sélectionnez NppFTP puis Install. Après le redémarrage du logiciel, vous disposez du nouveau plugin NppFTP. Sélectionnez « *Show NppFTP Window* ». Dans la partie droite s'affiche deux nouvelles zones. Sur les paramètres (petite engrenage en haut à droite), sélectionnez « *Profile Settings* ». Vous pouvez alors configurer les paramètres de connexion en faisant « *Add New* ». Les informations à renseigner sont du même type que pour le logiciel WinScp. Pensez bien à sélectionner le protocole SFTP (Secure FTP) qui utilise SSH. Dans l'onglet authentification vous pouvez renseigner votre clé privée pour réaliser une authentification par clé au lieu de l'authentification simple. Et comme pour les exercices précédents, si pageant s'exécute, vous pourrez vous connecter dans avoir à taper ni passe phrase, ni mot de passe.

Exercice n°17: Utiliser les commandes Unix sous Windows

Et pour boucler la boucle, maintenant que vous avez apprécié les commandes Unix et tout ce qu'elles permettent, il ne reste qu'un pas à franchir pour utiliser celles-ci sous Windows. Pour cela, il vous suffit d'installer Cygwin
Rendez-vous à l'adresse http://www.cygwin.com/ et vous pourrez installer tout un environnement Unix sous Windows.

Exercice n°18: Création d'une paire de clés publique/privée pour une utilisation depuis Windows

Créez une paire de clés pour votre ordinateur sous Windows. Pourquoi l'outil vous demande de bouger frénétiquement la souris ?

> La génération des clés doit introduire des données aléatoires afin d'assurer que la clé privée n'est pas calculable à partir de la clé publique. Le programme puttygen a décidé d'utiliser les mouvement de la souris comme des données aléatoires pour la génération des clés.

Mais le problème est alors, comment ajouter la clé publique dans le format ppk à mon serveur sous Linux. Ah et bien là, je n'ai pas de solution pour le moment. C'est pourquoi, nous avons procédé autrement durant le TD.