Communications sécurisées avec OpenSSH

Atelier Quand: Samedi 4 mai 2019, 13h-17h Lieu: Centre de loisirs Saint-Louis-de-France

Animé par: Sébastien Boisvert

Matériel requis pour participer aux exercices pratiques: ordinateur personnel avec Linux

Commande à taper sur le client (votre ordinateur portable):

-  `commande dans l'invite de commande` (client)

Commande à taper sur le serveur (rivendell.linuq.org)

-  `commande dans l'invite de commande` (serveur)

- Serveur pour l'atelier:
  - rivendell.linuq.org (instance du modèle B2-7 chez OVH)
  - Chacun et chacune va avoir un identifiant et un mot de passe

Rappels

- 3 parties d'un système d'exploitation: kernel (noyau), shell (invite de commande), utilities (applications)
  - Vidéo de 00:02:19: Ken Thompson and Dennis Ritchie Explain UNIX (Bell Labs)
  -  `uname -a` (client)
- Réseau Internet
  -  `hostname` (client)
- Protocole TCP/IP (Transmission Control Protocol/Internet Protocol)
- Adresse IP (IPv4: a.b.c.d)

-  `ip addr ls` (client)
- Port TCP/IP (port 22 pour SSH, 80 pour HTTP, 443 pour HTTPS)
  - 
  - `telnet linuq.org 80` (client)
  - `telnet rivendell.linuq.org 22` (client)

Le projet OpenSSH

- Communications sécurisées
- Site web officiel de OpenSSH: https://www.openssh.com/
- OpenSSH est écrit en C pour OpenBSD
  -  `ssh -V` (client)
- Pour les autres plateformes (Linux, Mac, Windows, FreeBSD, ...), c'est plutôt OpenSSH “portable”
- Dans Ubuntu: paquet opensh-client, version 1:7.6p1-4ubuntu0.3
  - Signifie: version 7.6 p1 de OpenSSH, soit la version portable 1 (p1) de OpenSSH 7.6
  -  `dpkg -l|grep openssh` (client)
- Code source: Dépôt CVS de OpenSSH
  - pas de dépôt git ou subversion ou mercurial
  - Surprenant car CVS ne garantie pas l'intégrité des fichiers comme GIT le fait.

Protocole SSH vs OpenSSH

- Protocole SSH utilise port TCP/IP 22 (comme HTTP utilise le port TCP/IP 80)
- Protocole SSH 2 versus Protocole SSH 1
- OpenSSH: implémentation très utilisée du protocole SSH
- Protocole SSH
  - Spécifications RFC sur www.openssh.com
  - ssh protocol, sur www.ssh.com (anglais)
- Autres protocoles:
  - Protocole SFTP
  - Protocole SCP

- Commande pour tester le protocole SSH:
  -  `telnet rivendell.linuq.org 22` (client)

Serveurs / démons

- sshd - serveur OpenSSH avec le protocole SSH 2
  - répond aux clients “ssh”

    - paquet openssh-server dans Ubuntu
- ssh-keyscan - Scanneur pour obtenir la liste des clés et empruntes d'un serveur sshd qui roule sur un serveur
    -  `ssh-keyscan rivendell.linuq.org` (client)
- sftp-server - serveur SFTP
    - répond aux clients “sftp”
    - paquet openssh-sftp-server dans Ubuntu

Programme client

- ssh - client SSH de OpenSSH
- Peut être utiliser pour obtenir une invite de commande sur un serveur
- paquet openssh-client dans Ubuntu
    -  `ssh -l utilisateur rivendell.linuq.org -p 22` (client)
- Commandes pour voir qui sont connectés:
    - 
    - who (serveur)
    - w (serveur)

Transfert de fichiers

- scp - programme client pour le protocole SCP
- 
    - `scp STE402P_.pdf utilisateur@rivendell.linuq.org:/tmp/` (client, téléverser fichier, client → serveur)
    - `scp utilisateur@rivendell.linuq.org:/tmp/STE402P_.pdf .` (client, télécharger fichier, serveur → client)
- sftp - programme client pour le protocole SFTP
- rsync est supérieur à scp et à sftp pour transférer / synchroniser des fichiers
- 
- `echo Bonjour > mon-fichier.txt` (client)
- `rsync -av mon-fichier.txt utilisateur@rivendell.linuq.org:` (client)

Gestion de clés d'authentification

- ssh-keygen - générer des clés d'authentification

-  `ssh-keygen -f key.pem` (client)
- ssh-copy-id (script SH) - copier une clé publique d'authentification sur un serveur
  -  `ssh-copy-id -i key.pem.pub utilisateur@rivendell.linuq.org -p 22` (client)
- Maintenant possible de s'authentifier avec la clé
  -  `ssh -i key.pem -l utilisateur rivendell.linuq.org -p 22` (client)

Agent d'authentification

- ssh-agent - un agent qui gère vos clés d'authentification pour vous
  - 
  - `ssh-agent > ssh-agent.txt` (client)
  - `source ssh-agent.txt` (client)
- ssh-add - programme client pour ajouter une clé à l'agent 'ssh-agent'
  - 
  - `ssh-add key.pem` (client)
  - `ssh-add -l` (client)
- Maintenant possible de s'authentifier avec l'agent:
  -  `ssh -l utilisateur rivendell.linuq.org -p 22` (client)

Redirection de port (avancé)

- Créer la redirection de port:
  -  `ssh -l utilisateur rivendell.linuq.org -p 22 -N -f -L 2222:serveur-secret:22` (client)
- Se connecter avec ssh sur le *serveur-secret* qui est protégé par un pare-feu:
  -  `ssh -p 2222 localhost` (client)

Programmes mystérieux de OpenSSH (si on a le temps !)

- Je n'ai jamais utilisé ces programmes.
- slogin - lien symbolique vers “ssh”
- ssh-keysign - programme pour signer des clés

    - désactivé par défaut
    - n'est pas distribué dans Ubuntu 18.04.1 LTS
- ssh-argv0 (script SH) - programme qui fait une commande qui ressemble à “exec ssh”
- ssh-import-id (script Python) - Obtenir une clé publique d'authentification
- ssh-import-id-gh (script Python) - Obtenir une clé publique d'authentification
    - pour Github.com (Microsoft)
- ssh-import-id-lp (script Python) - Obtenir une clé publique d'authentification
    - pour Launchpad.net (Canonical, compagnie derrière Ubuntu)

Liens

- Qu’est-ce que SSH ?
- Comprendre et maîtriser SSH
- Comprendre et maîtriser SSH
- Tunnel SSH pour HTTP(S)
- Cryptographie asymmétrique, voir: Présentation de GnuPG (chiffrement, cryptographie)