WIKIPÉDIA

Secure Shell

Secure Shell (**SSH**) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un *sniffer* pour voir ce que fait l'utilisateur.

Le protocole SSH a été conçu avec l'objectif de remplacer les différents protocoles non chiffrés comme rlogin, telnet, rcp et rsh.

Secure Shell

Informations

Fonction	Session à distance sécurisée
Sigle	SSH
Date de création	1995
Port	TCP/22
RFC	RFC 4251[1]

Sommaire

Le protocole

Le protocole SSH existe en deux versions majeures : la version 1.0 et la version 2.0.

- La première version permet de se connecter à distance à un ordinateur afin d'obtenir un shell ou ligne de commande. Cette version souffrait néanmoins de problèmes de sécurité dans la vérification de l'intégrité des données envoyées ou reçues, la rendant vulnérable à des attaques actives. En outre, cette version implémentait un système sommaire de transmission de fichiers, et du *port tunneling*.
- La version 2 qui était à l'état de brouillon jusqu'en janvier 2006 est déjà largement utilisée à travers le monde.

Cette version est beaucoup plus sûre au niveau cryptographique, et possède en plus un protocole de transfert de fichiers complet, le SSH file transfer protocol.

Habituellement le protocole SSH utilise le port TCP 22. Il est particulièrement utilisé pour ouvrir un shell sur un ordinateur distant. Peu utilisé sur les stations Windows (quoiqu'on puisse l'utiliser avec PuTTY, mRemote, cygwin ou encore OpenSSH), SSH fait référence pour l'accès distant sur les stations Linux et Unix.

SSH peut également être utilisé pour transférer des ports TCP d'une machine vers une autre, créant ainsi un tunnel. Cette méthode est couramment utilisée afin de sécuriser une connexion qui ne l'est pas (par exemple le protocole de récupérations de courrier électronique POP3) en la faisant transférer par le biais du tunnel chiffré SSH.

Il est également possible de faire plusieurs sauts entre consoles SSH, c'est-à-dire ouvrir une console sur un serveur, puis, de là, en ouvrir une autre sur un autre serveur.

Historique

La première version de SSH (SSH-1) a été conçue par Tatu Ylönen, à Espoo, en Finlande en 1995. Il a créé le premier programme utilisant ce protocole et a ensuite créé une entreprise, SSH Communications Security **(en)** pour exploiter cette innovation. Cette première version utilisait certains logiciels libres comme la bibliothèque Gnu libgmp, mais au fil du temps ces logiciels ont été remplacés par des logiciels propriétaires. SSH Communications Security **(en)** a vendu sa licence SSH à F-Secure (anciennement connue sous le nom de Data Fellows).

La version suivante a été nommée SSH-2. Le groupe de recherche de l'IETF « secsh » a défini en janvier 2006 le standard Internet SSH-2, que l'on retrouve actuellement dans la plupart des implémentations. Cette version permet une compatibilité ascendante avec les implémentations du brouillon de SSH-2 qui étaient en version 1.99.

SSH avec authentification par clés

Avec SSH, l'authentification peut se faire sans l'utilisation de mot de passe ou de phrase secrète en utilisant la cryptographie asymétrique. La clé publique est distribuée sur les systèmes auxquels on souhaite se connecter. La clé privée, qu'on prendra le soin de protéger par un mot de passe, reste uniquement sur le poste à partir duquel on se connecte. L'utilisation d'un « agent ssh **(en)** » permet de stocker le mot de passe de la clé privée pendant la durée de la session utilisateur.

Cette configuration profite aussi à SCP et à SFTP qui se connectent au même serveur SSH.

Implémentations logicielles

- *OpenSSH*, le projet libre d'outils SSH. OpenSSH est l'implémentation ssh la plus utilisée, y compris par les distributions GNU/Linux.
- *Portable OpenSSH*, une implémentation OpenSSH multiplateforme.
- *lsh*[2], une implémentation distribuée par le projet GNU selon les termes de la licence GNU GPL.
- *MacSSH*[3], une implémentation *lsh* pour Mac OS classic 68k et PPC.
- *FRESH*[4], une implémentation ssh en environnement JBoss.
- *SSHWindows*[5], une implémentation pour Windows non maintenue.
- *Dropbear*[6], une implémentation libre ayant pour but de remplacer OpenSSH sur les systèmes Unix ayant peu de ressources (processeur, mémoire, etc.) comme les systèmes embarqués.
- PuTTY, un client SSH multi-OS.
- TTyEmulator - Émulateur de terminal propriétaire, en français sous Windows incluant un grand nombre de fonctionnalités.

Notes et références

1. **(en)** « The Secure Shell (SSH) Protocol Architecture (https://tools.ietf.org/html/rfc4251) », Request for Comments n° 4251, janvier 2006.
2. **(en)** Implémentation GNU (http://www.lysator.liu.se/~nisse/lsh/).
3. **(en)** MacSSH (http://sourceforge.net/projects/macssh/) sur la plateforme SourceForge.
4. **(en)** FRESH (https://issues.jboss.org/browse/FRESH).
5. **(en)** SSHWindows (http://sshwindows.sourceforge.net/) sur la plateforme SourceForge.
6. **(en)** Dropbear (https://matt.ucc.asn.au/dropbear/dropbear.html).

Voir aussi

Articles connexes

Sur les autres projets Wikimedia :