

I. Objet

Les connexions SSH son très souvent utiliser par les administrateurs réseau. Les pirates informatiques conscient de ce moyen de connexion profite par tout les moyens d'accéder au machine avec de protocole de communication.

Pour évité cela je vais mettre en place un système dit key public/private, personnel à l'utilisateur. Les informations circulant sur le réseau entre la machine cliente et le serveur serons crypté, donc ne pourra être lu par un logiciel de capture de trame ou autre de type Wireshark.

Les connexions via un mot de passe seront refusées, uniquement l'authentification RSA le sera.

II. Domaine d'application

Cette procédure s'applique au service informatique de la société GSB.

III. Documents associés

AUCUN DOCUMENT ASSOCIE

IV. Définitions

• SSH avec authentification par clef

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 sur lesquels 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 » 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.

Source : Wikipédia



Introduction :

Le client SSH s'utilise le plus souvent avec un couple utilisateur/mot de passe sur la machine distante.

Toutefois, il est possible d'utiliser une clef RSA (authentification par clef publique) pour s'authentifier sur la machine distante. L'utilisation de cette méthode d'authentification couplée avec une *passphrase* permet de mettre en place un mécanisme d'authentification forte, et donc d'augmenter le niveau de sécurité.

Authentification RSA

Le principe de l'authentification RSA se base sur la signature de jetons d'authentification lors de la connexion. Le client dispose d'une paire de clefs d'authentification : une clef privée qu'il est le seul à détenir et une clef publique que les serveurs utiliseront pour vérifier l'identité du client. Au moment de l'authentification, le client signe un jeton avec sa clef privée et le donne au serveur sur lequel il a besoin de s'authentifier. Le serveur doit avoir accès à la clef publique du client pour décrypter le jeton d'authentification (principe de signature numérique). Le serveur, avec la clef publique, peut donc vérifier la signature du jeton d'authentification, en ayant l'assurance que seul le client a pu générer la signature (le client est le seul à détenir la clef privée).





I. Génération d'une paire de clefs sur Linux

Sur ma machine serveur je génère une paire de clef pour l'utilisateur « root »

root@srv-web1-GSB:~	\$ ssh-keygen -t rsa
Generating public/p	rivate rsa key pair.
Enter file in which	to save the key (/root/.ssh/id_rsa):"NOM DE LA CLE"
Enter passphrase (e	mpty for no passphrase):
Enter same passphra	se again:
Your identification	has been saved in /root/.ssh/
Your public key has	been saved in /root/.ssh/"NOM DE LA CLE".pub.
The key fingerprint	is:
44:1b:94:be:04:4a:3	4:ca:ad:af:16:43:a2:28:b4:8c
The key's randomart	image is:
+[RSA 2048]+	
.0 .+.	
. 00	
0 00	
0	
*00 .S.	
Eoo	
. 0.	
++	

Par défaut la clef privée est sauvegardée dans le fichier id_rsa dans un répertoire caché nommé .ssh de la homedir de l'utilisateur. La clef publique correspondante est sauvegardée dans le fichier id_rsa.pub dans le même répertoire. Lorsque l'on génère la clef privée, il est possible de protéger l'accès à cette clef par une phrase (appelée passphrase). Cela renforce la sécurité mais oblige à saisir cette phrase à chaque fois que l'on utilise la clef privée, ce qui perd tout intérêt quand l'authentification se fait dans un script.

II. Ajout de la clef publique sur le serveur

Pour permettre l'authentification par clef RSA sur le serveur, il est nécessaire d'ajouter la clef publique de l'utilisateur dans le fichier de clefs autorisées sur le serveur. Pour cela il faut connaitre le mot de passe de l'utilisateur sur le serveur et utiliser la commande suivante :

```
ssh-copy-id -i /root/.ssh/"NOM DE LE CLE".pub root@srv-web1-GSB
Password:
Now try logging into the machine, with "ssh 'root@srv-web1-GSB'", and check in:
   .ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
```

3

	Procédures informatiques administrateur	Réf. : gsb-DOC-admin-02 Version : 1
Ţ	Connexion au serveur SSH via authentification RSA	Date : 23/04/2013 Pages n°4

La clef publique (.pub) à été automatiquement ajouter au fichier « authorized_keys » du serveur.

III. Copie de la clef priver RSA sur la machine client

Après avoir installé le logiciel « WinSCP » sur la machine Windows.

Connecter vous sur la machine serveur, aller dans le répertoire ou et stocker la clef priver (/root/.ssh/ « Nom de la clef »). Pour terminer copier la sur votre machine Windows.

ssh - root@srv-web1-GSB - W	inSCP				×
Local Marquer Fichiers Com	mandes Sessi	ion Options Dista	nt Aide		
👲 💷 🕤 - 🔐 🚷	🔤 🚜 🔤	强 🛨 🖃 🔻	\$ Ø C	Défaut - 🌀 -	
root@srv-web1-GSB +					
Mes documents - 🕤	7	⇒ - 100 00 6	Ø 19	• 📾 🔽 😓 → 🖓 🕅 🖉	е. Не
C:\Users\Anthony\Documents				/root/.ssh	
Nom Evt	Taille	Type	Date de mu	Nom Ext Taille	Date
A CAL	rame	Décembries and	22/04/2012		22/
📕		Repertoire par	22/04/2013	base A42 P	22/(
Ma musique		Dossier de fich	20/00/2013	id real real pub 200 P	22/0
Mes fichiers recus		Dossier de fich	00/04/2012	id rsa root 1766 B	22/0
Mes formes		Dossier de fich	02/10/2012	authorized keys 300 B	22/(
Mes images		Dossier de fich	30/09/2012	dditionized_keys	22/1
Mes numérisations		Dossier de fich	20/04/2013		
Mes vidéos		Dossier de fich	30/09/2012		
My Safes		Dossier de fich	30/10/2012		
Native Instruments		Dossier de fich	24/11/2012		
samsung		Dossier de fich	24/03/2013		
SendBlaster2		Dossier de fich	29/10/2012		
Virtual Machines		Dossier de fich	16/04/2013		
Visual Studio 2008		Dossier de fich	30/09/2012		
\mu Visual Studio 2010		Dossier de fich	18/12/2012		
🌄 Default.rdp	2 200 B	Connexion Bur	10/04/2013		
🛍 desktop.ini	402 B	Paramètres de	30/09/2012		

IV. Modification du fichier de configuration sshd

Le service SSH doit également être configuré pour accepter l'authentification par clefs RSA. Le fichier de configuration du serveur SSH doit contenir les paramètres suivants :

nano /etc/ssh/sshd.cong RSAAuthentication yes PubkeyAuthentication yes AuthorizedKeysFile \$h/.ssh/authorized keys PasswordAuthentification no

Nous allons forcer l'authentification par clef RSA, en désactivant l'option « PasswordAuthentification no ».

Si vous avez besoin d'ajouter ces lignes de configuration ou de les dé-commenter, n'oubliez pas de redémarrer le service sshd !

service ssh restart



V. Utilisation de clefs RSA avec PuTTy sous Windows

Ensuite nous allons convertir cette clef dans un format utilisable par PuTTy avec l'outil « puttygen.exe », aurait pu être également utilisé pour générer une paire de clefs RSA, dans ce cas nous aurions dû sauvegarder la clef publique générée et ajouter cette clef dans le fichier « autorized_keys » du serveur. Ici nous allons convertir notre clef existante :

	-			
e Key	Conversions	Help		
Key —	Import key			
No key.	Export Op Export ssh	en55H key .com key		
Actions -				
Actions - Generate	e a public/priva	ate key pair		Generate
Actions - Generate Load an	e a public/private	ate key pair e key file		Generate
Actions - Generate Load an Save the	e a public/private existing private e generated ke	ate key pair a key file Y	Save public key	Generate Load Save private key
Actions - Generate Load an Save the Paramete	e a public/priva existing private e generated ke ers	ate key pair 9 key file 9	Save public key	Generate Load Save private key
Actions - Generate Load an Save the Paramete Type of I C SSH	e a public/priva existing private e generated ke ers key to generat -1 (RSA)	ate key pair a key file y e: © SSH-2 RSA	Save public key	Generate Load Save private key

On peut nommer la clef ainsi convertie et la sauvegarder au format ppk utilisé par PuTTy :

Une fois la clef sauvegardée (bouton « Save private key »), on a maintenant une clef utilisable pour nos sessions SSH. Enregistrer votre key privé dans un emplacement identifiable, pour ne pas le supprimer malencontreusement.

Putty Key Generat	0 r		<u>? ×</u>
File Key Conversions	Help		
Кеу			
Public key for pasting in	nto OpenSSH authorized	d_keys file:	
ssh-rsa AAAAB3NzaC1yc2EA J83zWdHcXQiw8KXP +VgBhMn0CtmzsIn4Id +wbxk9EEZWVLYJeII	AAADAQABAAABAQCw vOm73WYPP6Si0MY7r IO2z5CbSci9UbvNG4l6 IWOFFCViEaiq3OTnP5	vmS1Cqld1/Yzq0W0M hEflZc3Nf1Swi2VppVL iLB iVgN8Ms	f5nQ9mZyqG6aTJ
Key fingerprint:	ssh-rsa 2048 44:1b:94:	be:04:4a:34:ca:ad:af:1	16:43:a2:28:b4:8c
Key comment:	badrogh-openssh-key	>	
Key passphrase:			
Confirm passphrase:			
Actions			
Generate a public/priva	ate key pair		Generate
Load an existing private	e key file		Load
Save the generated ke	у	Save public key	Save private key
Parameters			
Type of key to generate OSSH-1 (RSA)	e: SSH-2 RSA	C SS	H-2 DSA
Number of bits in a gen	erated key:		1024



VI. Configuration de la connexion SSH avec PuTTy

Commençons par ouvrir PuTTy puis précisons le nom de login à utiliser pour la connexion SSH dans l'onglet « Connexion » > « Data »:

Session	Data ta a	and to the server
Logging Logging Logging Logging Logging Window Peatures Window Peatures Window Peatures Selection Colours Connection Data Proxy Telnet Rlogin SSH SSH Serial	Login details Auto-login usemame Terminal details Terminal type string Terminal speeds Environment variables Variable	badrogh xterm 38400,38400 Add Remove

Puis ajoutons la clef privée à utiliser pour la connexion SSH dans l'onglet « Connection » > « SSH » > « Auth » :





Procédures informatiques administrateur Connexion au serveur SSH via authentification

<u>RSA</u>

Réf. : gsb-DOC-admin-02 Version : 1 Date : 23/04/2013 Pages n°7

www.anthony-cochet.fr

