Exemple de configuration de la génération PuTTYgen des touches autorisées SSH et de l'authentification RSA sur Cisco Secure IDS

Table des matières

Introduction

Ce document explique comment utiliser le générateur de clé pour PuTTY (PuTTYgen) pour générer des clés autorisées Secure Shell (SSH) et l'authentification RSA pour une utilisation sur Cisco Secure Intrusion Detection System (IDS). Le principal problème lorsque vous établissez des clés autorisées SSH est que seul le format de clé RSA1 plus ancien est acceptable. Cela signifie que vous devez demander à votre générateur de clé de créer une clé RSA1 et vous devez restreindre le client SSH à utiliser le protocole SSH1.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Récent PuTTY - 7 février 2004
- Cisco Secure IDS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Configurer

Cette section vous présente les informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour trouver des informations supplémentaires sur les commandes utilisées dans ce document.

Configuration de PuTTYgen

Complétez ces étapes pour configurer PuTTYgen.

1. Lancez PuTTYgen.
2. Cliquez sur le type de clé SSH1 et définissez le nombre de bits dans la clé générée sur 2048 dans le groupe Paramètres au bas de la boîte de dialogue.
3. Cliquez sur Generate et suivez les instructions.

   Les informations clés sont affichées dans la section supérieure de la boîte de dialogue.
4. Désactivez la zone d'édition Commentaire clé.
5. Sélectionnez tout le texte de la clé publique à coller dans le fichier authorized_keys et appuyez sur Ctrl-C.
6. Tapez une phrase de passe dans les zones Key passphrase et Confirm passphrase edit.
7. Cliquez sur Save private key.
8. Enregistrez le fichier de clé privée PuTTY dans un répertoire privé pour votre connexion Windows (dans la sous-arborescence Documents and Settings/(userid)/My Documents sous Windows 2000/XP).
9. Lancez PuTTY.
10. Créez une nouvelle session PuTTY comme indiqué ici :

    - Session :

- Adresse IP : adresse IP du capteur IDS
- Protocole : SSH
- Port : 22
- Connexion:
- Nom d'utilisateur de connexion automatique : cisco (peut également être le nom de connexion que vous utilisez sur le capteur)
- Connexion/SSH :
- Version SSH préférée : 1 uniquement
- Connexion/SSH/Auth :
- Fichier de clé privée pour l'authentification : accédez au fichier .PPK stocké à l'étape 8.
- Session : (en haut de la page)
- Sessions enregistrées : (saisissez le nom du capteur, puis cliquez sur Enregistrer)

11. Cliquez sur Open et utilisez l'authentification par mot de passe pour vous connecter à l'interface de ligne de commande du capteur, puisque la clé publique n'est pas encore sur le capteur.
12. Entrez la commande configure terminal CLI et appuyez sur Entrée.
13. Entrez la commande ssh authorized-key mykey CLI, mais n'appuyez pas sur Entrée pour le moment. Assurez-vous de taper un espace à la fin.
14. Cliquez avec le bouton droit dans la fenêtre du terminal PuTTY.

    Le contenu du Presse-papiers copié à l'étape 5 est saisi dans l'interface de ligne de commande.
15. Appuyez sur Entrée.
16. Entrez la commande exit et appuyez sur Entrée.
17. Vérifiez que la clé autorisée est entrée correctement. Entrez la commande show ssh authorized-keys mykey et appuyez sur Entrée.
18. Entrez la commande exit pour quitter l’interface de ligne de commande IDS et appuyez sur Entrée.

Vérifier

Authentification RSA

Procédez comme suit :

1. Lancez PuTTY.
2. Recherchez la session enregistrée créée à l'étape 10 et double-cliquez dessus. Une fenêtre de terminal PuTTY s'ouvre et le texte suivant apparaît :

```
Sent username "cisco"
Trying public key authentication.
Passphrase for key "":
```

3. Tapez la phrase secrète de clé privée que vous avez créée à l'étape 6 et appuyez sur Entrée.

   Vous êtes automatiquement connecté.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Pages d'assistance technique de Network Intrusion Detection
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.