Contenu

Introduction

Ce document explique comment utiliser le générateur principal pour le mastic (PuTTYgen) pour générer des clés autorisées par Protocole Secure Shell (SSH) et l'authentification RSA pour l'usage sur le système de détection d'intrusion Cisco Secure (ID). L'enjeu majeur quand vous établissez des clés autorisées par SSH est que seulement le format plus ancien de la clé RSA1 est acceptable. Ceci signifie que vous devez dire votre générateur principal de créer une clé RSA1, et vous doit limiter le client SSH pour utiliser le protocole SSH1.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Mastic récent - 7 février 2004
- Cisco Secure IDS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

Configurez

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

Remarque: Utilisez le Command Lookup Tool (clients enregistrés seulement) pour trouver les informations complémentaires sur les commandes des utilisations de ce document.

Configurez PuTTYgen

Terminez-vous ces étapes pour configurer PuTTYgen.

1. Lancement PuTTYgen.
2. Cliquez sur le type de la clé **SSH1** et placez le nombre de bits dans la clé générée à **2048** dans le groupe de paramètres au bas de la boîte de dialogue.
3. Cliquez sur **génèrent** et suivent les instructions.L'information principale est affichée dans la section supérieure de la boîte de dialogue.
4. Effacez la case d'éditer principale de commentaire.
5. Sélectionnez tout le texte dans la clé publique pour coller dans des authorized_keys classent et appuient sur le **CTRL-C**.
6. Tapez un mot de passe dans le mot de passe principal et confirmez les cases d'éditer de mot de passe.
7. **Clé privée de sauvegarde de** clic.
8. Sauvegardez le fichier principal privé de mastic dans un répertoire privé à votre procédure de connexion de Windows (dans le sous-arbre de documents et de documents Settings/(userid)/My dans Windows 2000/XP).
9. Mastic de lancement.
10. Créez une nouvelle session de mastic comme vu ici :**Session :Adresse IP :** Adresse IP du capteur d'ID**Protocol :** SSH**Port :** 22**Connexion :nom d'utilisateur d'Automatique-procédure de connexion :** Cisco (peut également être la procédure de connexion que vous utilisez sur le capteur)**Connection/SSH :Version SSH préférée :** 1 seulement**Connection/SSH/Authentic :Fichier principal privé pour l'authentification :** Parcourez au fichier stocké .PPK dans l'étape 8.**Session :** (de nouveau au dessus)**Sessions enregistrées :** (écrivez le nom de capteur, la **sauvegarde de** clic)
11. Clic **ouvert** et authentification de mot de passe d'utilisation à connecter au capteur CLI, puisque la clé publique n'est pas sur le capteur encore.
12. Sélectionnez la commande CLI de **configure terminal** et l'appuyez sur **entrent**.
13. Sélectionnez la commande CLI de **mykey d'autoriser-clé de ssh**, mais ne faites pas appuient sur entrent à ce moment. Assurez-vous et tapez un espace à l'extrémité.
14. Clic droit dans le terminal window de mastic.Le contenu de presse-papier copié dans l'étape 5 est tapé dans le CLI.
15. Appuyez sur **Entrée**.
16. Sélectionnez la **commande exit** et l'appuyez sur **entrent**.
17. Confirmez la clé autorisée est entré correctement. Sélectionnez la commande de **mykey d'autoriser-clés de show ssh** et l'appuyez sur **entrent**.
18. Sélectionnez la **commande exit** de quitter les ID CLI et l'appuyez sur **entrent**.

Vérifiez

Authentification RSA

Procédez comme suit :

1. Mastic de lancement.
2. Localisez la session enregistrée créée dans l'étape 10 et double-cliquer là-dessus. Un terminal window de mastic s'ouvre et ce texte paraît :
3. Tapez le mot de passe de clé privée que vous avez créé dans l'étape 6 et l'appuyez sur **entrent**.Vous êtes automatiquement ouvert une session.

Dépannez

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

Informations connexes

- Pages de Soutien technique de détection d'intrusion de réseau
- Support et documentation techniques - Cisco Systems