PuTTYgen-Generierung von autorisierten SSH-Schlüsseln und RSA-Authentifizierung auf Cisco Secure IDS - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird erläutert, wie mithilfe des Key-Generators für PuTTY (PuTTYgen) Secure Shell (SSH)-autorisierte Schlüssel und RSA-Authentifizierung für die Verwendung auf dem Cisco Secure Intrusion Detection System (IDS) generiert werden. Das Hauptproblem bei der Erstellung von autorisierten SSH-Schlüsseln besteht darin, dass nur das ältere RSA1-Schlüsselformat zulässig ist. Dies bedeutet, dass Sie Ihrem Schlüsselgenerator mitteilen müssen, dass er einen RSA1-Schlüssel erstellt, und dass Sie den SSH-Client auf die Verwendung des SSH1-Protokolls beschränken müssen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Zuletzt PuTTY - 7. Februar 2004
- Cisco Secure IDS

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den Befehlen zu finden, die dieses Dokument verwendet.

PuTTYgen konfigurieren

Führen Sie diese Schritte aus, um PuTTYgen zu konfigurieren.

1. Starten Sie PuTTYgen.
2. Klicken Sie auf den Schlüsseltyp **SSH1**, und legen Sie die Anzahl der Bits im generierten Schlüssel unten im Dialogfeld in der Gruppe Parameter auf **2048** fest.
3. Klicken Sie auf **Generate** (Generieren) und folgen Sie den Anweisungen.Die Schlüsselinformationen werden im oberen Bereich des Dialogfelds angezeigt.
4. Deaktivieren Sie das Bearbeitungsfeld Schlüsselkommentar.
5. Wählen Sie den gesamten Text im öffentlichen Schlüssel zum Einfügen in die Datei authorized_keys aus, und drücken Sie **Strg-C**.
6. Geben Sie eine Passphrase in die Felder Schlüssel-Passphrase ein, und bestätigen Sie die Passphrase-Bearbeitung.
7. Klicken Sie auf **Privaten Schlüssel speichern**.
8. Speichern Sie die private PuTTY-Schlüsseldatei in einem Verzeichnis, das in Ihrem Windows-Login privat ist (in der Unterstruktur Dokumente und Einstellungen/(userid)/Eigene Dokumente in Windows 2000/XP).
9. Starten Sie PuTTY.
10. Erstellen Sie eine neue PuTTY-Sitzung, wie hier gezeigt:**Sitzung:IP-Adresse:** IP-Adresse des IDS-Sensors**Protokoll:** SSH**Port:** 22**Verbindung:Benutzername für automatische Anmeldung:** cisco (kann auch die Anmeldung sein, die Sie auf dem Sensor verwenden)**Verbindung/SSH:Bevorzugte SSH-Version:** Nur 1**Verbindung/SSH/Auth:Private Schlüsseldatei für die Authentifizierung:** Navigieren Sie zur PPK-Datei, die in Schritt 8 gespeichert ist.**Sitzung:** (Nach oben)**Gespeicherte Sitzungen:** (Geben Sie den Sensornamen ein, und klicken Sie auf **Speichern**.)
11. Klicken Sie auf **Öffnen** und verwenden Sie die Kennwortauthentifizierung, um eine Verbindung zur Sensor-CLI herzustellen, da der öffentliche Schlüssel noch nicht auf dem Sensor gespeichert ist.
12. Geben Sie den Befehl **configure terminal** CLI ein, und drücken Sie die **Eingabetaste**.

13. Geben Sie den Befehl **ssh authorized-key mykey** CLI ein, drücken Sie aber derzeit nicht die Eingabetaste. Stellen Sie sicher, dass Sie am Ende ein Leerzeichen eingeben.
14. Klicken Sie mit der rechten Maustaste in das PuTTY-Terminalfenster.Das in Schritt 5 kopierte Clipboard-Material wird in die CLI eingegeben.
15. Drücken Sie **die Eingabetaste**.
16. Geben Sie den Befehl **exit ein**, und drücken Sie die **Eingabetaste**.
17. Bestätigen Sie, dass der autorisierte Schlüssel korrekt eingegeben wurde. Geben Sie den Befehl **show ssh authorized-keys mykey ein,** und drücken Sie die **Eingabetaste**.
18. Geben Sie den Befehl **exit** ein, um die IDS-CLI zu beenden, und drücken Sie die **Eingabetaste**.

Überprüfen

RSA-Authentifizierung

Führen Sie diese Schritte aus.

1. Starten Sie PuTTY.
2. Suchen Sie die in Schritt 10 erstellte gespeicherte Sitzung, und doppelklicken Sie darauf. Ein PuTTY-Terminalfenster wird geöffnet, und dieser Text wird angezeigt:
   ```
   Sent username "cisco"
   Trying public key authentication.
   Passphrase for key "":
   ```
3. Geben Sie die in Schritt 6 erstellte private Schlüssel-Passphrase ein und drücken Sie **die Eingabetaste**.Sie werden automatisch angemeldet.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Seiten des technischen Supports zur Erkennung von Netzwerksicherheitsrisiken
- Technischer Support und Dokumentation - Cisco Systems