Cisco Secure IDS上的SSH授權金鑰和RSA身份驗證的PuTTYgen生成配置示例

目錄

簡介

本文檔說明如何使用PuTTY的金鑰生成器(PuTTYgen)生成用於Cisco Secure Intrusion Detection System (IDS)的Secure Shell (SSH)授權金鑰和RSA身份驗證。建立SSH授權金鑰時的主要問題是，只能接受較舊的RSA1金鑰格式。這意味著您需要通知金鑰生成器建立RSA1金鑰，並且必須限制SSH客戶端使用SSH1協定。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 最新發佈- 2004年2月7日
- Cisco Secure IDS

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

本節提供用於設定本檔案所述功能的資訊。

附註：使用命令查閱工具(僅限註冊客戶)尋找關於本檔案所用命令的其他資訊。

配置PuTTYgen

完成以下步驟以配置PuTTYgen。

1. 啟動PuTTYgen。
2. 在對話方塊底部的「Parameters」組中按一下SSH1金鑰型別，並將生成的金鑰中的位數設定為2048。
3. 按一下Generate並按照說明操作。

   關鍵資訊會顯示在通話方塊的上方。
4. 清除「索引鍵註解」編輯方塊。
5. 選擇要貼上到authorized_keys檔案所需的公鑰中的所有文本，然後按Ctrl-C。
6. 在Key passphrase和Confirm passphrase編輯框中鍵入密碼。
7. 按一下Save private key。
8. 將PuTTY私鑰檔案儲存到Windows登入專用目錄(在Windows 2000/XP的Documents and Settings/(userid)/My Documents子目錄中)。
9. 啟動PuTTY。
10. 建立新的PuTTY會話，如下所示：
    - 工作階段：
    - IP Address： IDS感測器的IP地址
    - 協定：SSH
    - 連線埠： 22
    - 連線：
    - 自動登入使用者名稱： cisco（也可以是感測器上的登入名）
    - 連線/SSH：
    - 首選SSH版本：僅1

- 連線/SSH/身份驗證：
- 用於身份驗證的私鑰檔案：瀏覽到步驟8中儲存的.PPK檔案。
- 會話：（返回頂部）
- 儲存的會話：(輸入感測器名稱，點選儲存)

11. 由於公鑰不在感測器上，因此按一下Open並使用密碼身份驗證連線到感測器CLI。
12. 輸入configure terminal CLI命令並按Enter。
13. 輸入ssh authorized-key mykey CLI命令，但此時不要按Enter。確定並在末尾鍵入一個空格。
14. 按一下右鍵PuTTY終端窗口。

    將步驟5中複製的剪貼簿材料鍵入到CLI中。
15. 按Enter。
16. 輸入exit命令並按Enter。
17. 確認已正確輸入授權金鑰。輸入show ssh authorized-keys mykey命令並按Enter。
18. 輸入exit命令退出IDS CLI並按Enter。

驗證

RSA驗證

完成以下步驟。

1. 啟動PuTTY。
2. 找到步驟10中建立的已儲存會話，然後按兩下該會話。PuTTY終端窗口打開，並顯示以下文本：

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

3. 鍵入您在步驟6中建立的私鑰密碼短語，然後按Enter。

   您會自動登入。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Network Intrusion Detection技術支援頁
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。