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

目錄

簡介

本文檔介紹如何使用PuTTY金鑰生成器(PuTTYgen)生成安全外殼(SSH)授權金鑰和RSA身份驗證，以便在Cisco Secure Intrusion Detection System(IDS)上使用。 建立SSH授權金鑰時的主要問題是，只有舊的RSA1金鑰格式是可接受的。這意味著您需要告知金鑰生成器建立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：

- 最新一期PuTTY - 2004年2月7日
- Cisco安全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中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)查詢有關本文檔使用的命令的更多資訊。

配置PuTTYgen

完成以下步驟以配置PuTTYgen。

1. 啟動PuTTYgen。
2. 按一下**SSH1**金鑰型別，並在對話方塊底部的Parameters組中將生成的金鑰中的位數設定為**2048**。
3. 按一下「**Generate**」，然後按照說明操作。關鍵資訊顯示在對話方塊的上部。
4. 清除「鍵註釋」編輯框。
5. 選擇「公鑰」中的所有文本以貼上到authorized_keys檔案中，然後按**Ctrl-C**。
6. 在Key密碼和Confirm密碼編輯框中鍵入密碼短語。
7. 按一下**Save private key**。
8. 將PuTTY私鑰檔案儲存到Windows登入專用目錄中(在Windows 2000/XP的「Documents and Settings/(userid)/My Documents(文檔和設定/(userid)/My Documents)」子樹中)。
9. 啟動PuTTY。
10. 建立新的PuTTY會話，如下所示：**會話：IP 位址:**IDS感測器的IP地址**通訊協定:**SSH**連接埠**:22**Connection:自動登入使用者名稱：**cisco（也可以是您在感測器上使用的登入名）**連線/SSH:首選SSH版本：**僅1**Connection/SSH/Auth: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：**（回到頁首）**儲存的會話：**(輸入感測器名稱，按一下**Save**)
11. 按一下**Open**並使用密碼身份驗證連線到感測器CLI，因為公鑰尚未在感測器上。
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鍵。確保在結尾鍵入一個空格。
14. 按一下右鍵PuTTY終端視窗。將步驟5中複製的剪貼簿材料鍵入到CLI中。
15. 按**Enter**鍵。
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，然後按**Enter**。
18. 輸入**exit**命令退出IDS CLI，然後按**Enter**。

驗證

RSA身份驗證

請完成以下步驟。

1. 啟動PuTTY。
2. 找到在步驟10中建立的已儲存會話，然後按兩下它。PuTTY終端視窗開啟，並顯示以下文本：

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

3. 鍵入在步驟6中建立的私鑰密碼，然後按Enter。您將自動登入。

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

- 網路入侵檢測技術支援頁
- 技術支援與文件 - Cisco Systems