Cisco Secure IDS で使用する SSH 認証キーおよび RSA 認証を PuTTYgen で生成する設定例

内容

はじめに

このドキュメントでは、PuTTY のキー ジェネレータ（PuTTYgen）を使用して、Cisco Secure Intrusion Detection System（IDS; 侵入検知システム）で使用する Secure Shell（SSH; セキュアセル）認証キーや RSA 認証を生成する方法について説明します。SSH 認証キーを作成するときの第一の問題は、旧式の RSA1 キー形式だけが受け付けられる点です。つまり、使用しているキー ジェネレータに RSA1 キーを作成するよう指定する必要があり、SSH クライアントに対して SSH1 プロトコルを使用するよう制限する必要があります。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 最新の PuTTY - 2004 年 2 月 7 日
- Cisco Secure IDS

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報について記載しています。

注：このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

PuTTYgen の設定

PuTTYgen を設定するには、次の手順をすべて実行します。

1. PuTTYgen を起動します。
2. キーのタイプとして SSH1 をクリックして、ダイアログボックスの下部にある Parameters グループで、生成されるキーのビット数を 2048 に設定します。
3. Generate をクリックして、説明に従います。

   ダイアログボックスの上部にキーの情報が表示されます。
4. Key Comment エディット ボックスをクリアします。
5. authorized_keys file に貼り付ける公開キーの全テキストを選択して、Ctrl-C を押します。
6. Key passphrase にパスフレーズを入力し、passphrase エディット ボックスの内容を確認します。
7. Save private key をクリックします。
8. PuTTY 秘密キー ファイルを、使用している Windows ログインの個人ディレクトリに保存します (Windows 2000/XP の場合は Documents and Settings/(userid)/My Documents サブツリー) 。
9. PuTTY を起動します。
10. 次の内容で新しい PuTTY セッションを作成します。

    - Session:
    - IP Address:IDSセンサーのIPアドレス

- プロトコル：SSH
- ポート：22
- Connection:
- 自動ログインユーザ名：cisco (センサーで使用するログインも可)
- Connection/SSH:
- 推奨されるSSHバージョン：1のみ
- Connection/SSH/Auth:
- 認証用の秘密キーファイル：ステップ8で保存した.PPKファイルを参照します。
- セッション：(トップに戻る)
- 保存済みセッション：(センサー名を入力して、保存をクリック)

11. Open をクリックし、パスワード認証を使用して Sensor の CLI に接続します。これは、Sensor 上ではまだ公開キーが設定されていないためです。
12. configure terminal CLI コマンドを入力して、Enter キーを押します。
13. ssh authorized-key mykey CLI コマンドを入力しますが、この時点では Enter キーを押さないでください。最後にスペースを入力します。
14. PuTTY のターミナル ウィンドウを右クリックします。

    ステップ 5 でクリップボードにコピーした内容が、CLI に入力されます。
15. Enter を押します。
16. exit コマンドを入力して、Enter キーを押します。
17. 認証キーが正しく入力されているか、確認します。show ssh authorized-keys mykey コマンドを入力して、Enter キーを押します。
18. exit コマンドを入力して IDS CLI を終了し、Enter キーを押します。

確認

RSA 認証

次に示す手順を実行します。

1. PuTTY を起動します。
2. ステップ 10 で作成した Saved Session を探し、これをダブルクリックします。PuTTY のターミナル ウィンドウが開き、次のテキストが表示されます。

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

3. ステップ 6 で作成した秘密キーのパスフレーズを入力して、Enter キーを押します。

   自動的にログインします。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ネットワークへの侵入検知に関するテクニカル サポート ページ
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。