Esempio di generazione di PuTTen di chiavi autorizzate SSH e autenticazione RSA su Cisco Secure IDS

Sommario

Introduzione

Questo documento spiega come usare il generatore di chiavi per PuTTY (PuTTYgen) per generare chiavi autorizzate SSH (Secure Shell) e l'autenticazione RSA per l'uso con Cisco Secure Intrusion Detection System (IDS). Il problema principale quando si stabiliscono le chiavi autorizzate SSH è che è accettabile solo il formato della chiave RSA1 precedente. Ciò significa che è necessario chiedere al generatore di chiavi di creare una chiave RSA1 e limitare il client SSH all'uso del protocollo SSH1.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Ultime notizie - 7 febbraio 2004
- Cisco Secure IDS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte nel documento.

Nota: per ulteriori informazioni sui comandi **usati** nel presente documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Configurare PuTTYgen

Completare la procedura seguente per configurare PuTTYgen.

1. Avviare PuTTYgen.
2. Fare clic sul tipo di chiave **SSH1** e impostare il numero di bit nella chiave generata su **2048** nel gruppo Parametri nella parte inferiore della finestra di dialogo.
3. Fare clic su **Genera** e seguire le istruzioni.Le informazioni principali vengono visualizzate nella sezione superiore della finestra di dialogo.
4. Deselezionare la casella di modifica Commento chiave.
5. Selezionare tutto il testo nella chiave pubblica da incollare nel file authorized_keys e premere **Ctrl-C**.
6. Digitare una passphrase nelle caselle di modifica Passphrase chiave e Conferma passphrase.
7. Fare clic su **Salva chiave privata**.
8. Salvare il file della chiave privata PuTTY in una directory privata per l'accesso a Windows (nella sottostruttura Documents and Settings/(userid)/My Documents in Windows 2000/XP).
9. Avviare PuTTY.
10. Creare una nuova sessione PuTTY come mostrato di seguito:**Sessione:Indirizzo IP:** Indirizzo IP del sensore IDS**Protocollo:** SSH**Port:** 22**Connessione:Nome utente accesso automatico:** cisco (può essere anche l'account di accesso utilizzato per il sensore)**Connessione/SSH:Versione SSH preferita:** Solo 1**Connessione/SSH/Auth:File di chiave privata per l'autenticazione:** Individuare il file PPK memorizzato nel passaggio 8.**Sessione:** (torna all'inizio)**Sessioni salvate:** (immettere il nome del sensore, fare clic su **Salva**)
11. Fare clic su **Open** (Apri) e utilizzare l'autenticazione tramite password per connettersi alla CLI del sensore, poiché la chiave pubblica non è ancora presente sul sensore.
12. Immettere il comando **configure terminal** CLI e premere **Invio**.
13. Immettere il comando **ssh authorized-key** CLI, ma non premere Invio. Assicurarsi di digitare uno spazio alla fine.
14. Fare clic con il pulsante destro del mouse nella finestra del terminale PuTTY.Il materiale

copiato negli Appunti al punto 5 viene digitato nella CLI.

15. Premere **Invio**.
16. Immettere il comando **exit** e premere **Invio**.
17. Verificare che la chiave autorizzata sia stata immessa correttamente. Immettere il comando **show ssh authorized-keys** e premere **Invio**.
18. Immettere il comando **exit** per uscire dalla CLI di IDS e premere **Invio**.

Verifica

Autenticazione RSA

Attenersi alla seguente procedura.

1. Avviare PuTTY.
2. Individuare la sessione salvata creata nel passaggio 10 e fare doppio clic su di essa. Viene visualizzata una finestra del terminale PuTTY con il seguente testo:
   ```
   Sent username "cisco"
   Trying public key authentication.
   Passphrase for key "":
   ```
3. Digitare la passphrase della chiave privata creata al passaggio 6 e premere **Invio**.L'accesso viene eseguito automaticamente.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Pagine di supporto tecnico per il rilevamento delle intrusioni nella rete
- Documentazione e supporto tecnico – Cisco Systems