La generación del PuTTYgen de SSH autorizó las claves y la Autenticación RSA en el ejemplo de configuración del Cisco Secure IDS

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Configurar
PuTTYgen de la configuración
Verificación
Autenticación RSA
Troubleshooting
Información Relacionada

Introducción

Este documento explica cómo utilizar el generador de claves para PuTTY (PuTTYgen) para generar claves autorizadas de Secure Shell (SSH) y la autenticación RSA para su uso en el Sistema Seguro de Detección de Intrusos (IDS) de Cisco. El problema principal cuando establece claves autorizadas de SSH es que solamente es aceptable el formato de clave RSA1 más antiguo. Esto significa que necesita indicar al generador de claves que cree una clave RSA1 y debe restringir el cliente SSH para que use el protocolo SSH1.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PuTTY reciente - 7 de febrero de 2004
- Cisco Secure IDS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección se presenta información para configurar las características que este documento describe.

Nota: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para encontrar la información adicional en los comandos las aplicaciones de este documento.

Configure el PuTTYgen

Complete estos pasos para configurar el PuTTYgen.

1. Inicie el PuTTYgen.
2. Haga clic el tipo de la clave **SSH1** y fije el número de bits en la clave generada a **2048** en el grupo de parámetros en la parte inferior del cuadro de diálogo.
3. El tecleo **genera** y sigue las instrucciones.La información fundamental se visualiza en la sección superior del cuadro de diálogo.
4. Borre el recuadro de edición dominante del comentario.
5. Seleccione todo el texto en la clave pública para pegar en los authorized_keys archivo y el **Ctrl-c de la** prensa.
6. Teclee un passphrase en el passphrase dominante y confirme los recuadros de edición del passphrase.
7. Haga clic la **clave privada de la salvaguardia**.
8. Salve el archivo de clave privado del putty en un soldado del directorio a su login de Windows (en la sub-estructura de los documentos y de los documentos Settings/(userid)/My en Windows 2000/XP).
9. Inicie el putty.
10. Cree a una nueva sesión PuTTY según lo visto aquí:**Sesión:Dirección IP:** Dirección IP del sensor IDS**Protocolo:** SSH**Puerto:** 22**Conexión:nombre de usuario del Auto-login:** Cisco (puede también estar el login que usted utiliza en el sensor)**Connection/SSH:SSH versión preferido:** 1 solamente**Connection/SSH/Authentic:Archivo de clave privado para la autenticación:** Hojee al archivo .PPK salvado en el paso 8.**Sesión:** (de nuevo al top)**Sesiones guardadas:** (ingrese el nombre del sensor, la **salvaguardia del** tecleo)
11. Haga clic **abierto** y utilice la autenticación de contraseña para conectar con el sensor CLI, puesto que la clave pública no está en el sensor todavía.
12. Ingrese el comando CLI y el Presione ENTER **configurados terminal**.
13. Ingrese el comando CLI del **mykey de la autorizar-clave del ssh**, pero no haga Presione ENTER ahora. Aseegurese y teclee un espacio en el extremo.
14. Haga clic con el botón derecho del ratón en la ventana de terminal del putty.El material del

portapapeles copiado en el paso 5 se teclea en el CLI.
15. Presione Intro.
16. Ingrese el **comando exit** y el Presione ENTER.
17. Confirme la clave autorizada se ingresa correctamente. Ingrese el **comando show ssh authorized-keys mykey** y el Presione ENTER.
18. Ingrese el **comando exit** de salir el IDS CLI y Presione ENTER.

Verificación

Autenticación RSA

Complete estos pasos.

1. Inicie el putty.
2. Localice la sesión guardada creada en el paso 10 y haga doble clic en él. Una ventana de terminal del putty se abre y este texto aparece:
   ```
   Sent username "cisco" Trying public key authentication. Passphrase for key "":
   ```
3. Teclee el passphrase de la clave privada que usted creó en el paso 6 y el Presione ENTER.Le abren una sesión automáticamente.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Páginas de soporte técnico de la detección de los intrusos en la red
- Soporte Técnico y Documentación - Cisco Systems