Exemplo de Geração PuTTY de Chaves Autorizadas SSH e Autenticação RSA no Cisco Secure IDS Configuration

Contents

Introdução

Este documento explica como usar o gerador de chaves para PuTTY (PuTTYgen) para gerar chaves autorizadas Secure Shell (SSH) e autenticação RSA para uso no Cisco Secure Intrusion Detection System (IDS). O principal problema ao estabelecer chaves autorizadas SSH é que somente o formato de chave RSA1 mais antigo é aceitável. Isso significa que você precisa dizer ao gerador de chaves para criar uma chave RSA1, e você deve restringir o cliente SSH para usar o protocolo SSH1.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- PuTTY recente - 7 de fevereiro de 2004
- Cisco Secure IDS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Esta seção apresenta informações para configurar as características que este documento descreve.

Observação: use a Command Lookup Tool (somente clientes registrados) para encontrar informações adicionais sobre os comandos usados neste documento.

Configurar PuTTYgen

Conclua estas etapas para configurar o PuTTYgen.

1. Inicie o PuTTYgen.
2. Clique no tipo de chave SSH1 e defina o número de bits na chave gerada como 2048 no grupo Parâmetros na parte inferior da caixa de diálogo.
3. Clique em Gerar e siga as instruções.

   As informações principais são exibidas na seção superior da caixa de diálogo.
4. Desmarque a caixa de edição Comentário principal.
5. Selecione todo o texto na chave pública para colar no arquivo authorized_keys e pressione Ctrl-C.
6. Digite uma senha nas caixas de edição Key passphrase e Confirm passphrase.
7. Clique em Save private key.
8. Salve o arquivo de chave privada PuTTY em um diretório particular para o login do Windows (na subárvore Documents and Settings/(userid)/My Documents do Windows 2000/XP).
9. Inicie o PuTTY.
10. Crie uma nova sessão PuTTY como visto aqui:

    - Sessão:

- Endereço IP: endereço IP do sensor IDS
- Protocolo: SSH
- Porta: 22
- Conexão:
- Nome de usuário de login automático: cisco (também pode ser o login usado no Sensor)
- Conexão/SSH:
- Versão preferida do SSH: 1 apenas
- Conexão/SSH/Autenticação:
- Arquivo de chave privada para autenticação: procure o arquivo .PPK armazenado na etapa 8.
- Sessão: (voltar ao topo)
- Sessões salvas: (insira o nome do sensor e clique em Salvar)

11. Clique em Open e use a autenticação de senha para se conectar ao Sensor CLI, já que a chave pública ainda não está no Sensor.
12. Insira o comando CLI configure terminal e pressione Enter.
13. Insira o comando CLI ssh authorized-key mykey, mas não pressione Enter neste momento. Certifique-se de digitar um espaço no final.
14. Clique com o botão direito do mouse na janela do terminal PuTTY.

    O material da área de transferência copiado na etapa 5 é digitado na CLI.
15. Pressione Enter.
16. Insira o comando exit e pressione Enter.
17. Confirme se a chave autorizada foi inserida corretamente. Insira o comando show ssh authorized-keys mykey e pressione Enter.
18. Insira o comando exit para sair do IDS CLI e pressione Enter.

Verificar

Autenticação RSA

Siga estas etapas.

1. Inicie o PuTTY.
2. Localize a Sessão Salva criada na etapa 10 e clique duas vezes nela. Uma janela de terminal PuTTY é aberta e este texto é exibido:

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

3. Digite a senha da chave privada criada na etapa 6 e pressione Enter.

   Você está conectado automaticamente.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Páginas de Suporte Técnico de Detecção de Intrusão de Rede
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.