目录

简介

本文解释如何使用关键生成器PuTTY (PuTTYgen)生成安全壳SSH授权的密钥和RSA验证为使用在Cisco安全入侵监测系统(IDS)。主要的问题，当您设立SSH授权的密钥时是仅更旧的RSA1密钥格式是可接受。这意味着您需要告诉您的关键生成器创建RSA1密钥和您必须限制SSH客户端使用SSH1协议。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 最近的PuTTY -二月7， 2004
- Cisco 安全 IDS

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供了用于配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可查找有关本文档所用命令的其他信息。

配置PuTTYgen

完成这些步骤配置PuTTYgen。

1. 启动PuTTYgen。
2. 点击**SSH1**密钥类型并且设置位数量生成的密钥的到**2048**在参数组在对话框的底部。
3. 单击**生成**并且遵从说明。关键信息在对话框的上面的部分显示。
4. 清除关键注释编辑框。
5. 选择在公共密钥的所有文本粘贴的到authorized_keys文件并且按**ctrl-c**。
6. 键入在关键密码短语的一密码短语并且确认密码短语编辑框。
7. 点击**保存专用密钥**。
8. 保存PuTTY专用密钥文件到目录私有对您的Windows登录(在Windows 2000/XP)的本文和Settings/(userid)/My文档子树。
9. 启动PuTTY。
10. 创建一新的PuTTY会话如被看到此处：**会话：IP 地址：**IDS传感器的IP地址**协议：**SSH**波尔特：**22**连接：自动登录用户名：**cisco (可以也是您在传感器使用)的登录**Connection/SSH：首选的SSH版本：**1only**Connection/SSH/Auth ：验证的专用密钥文件：**浏览到在步骤存储的.PPK文件8。**会话：**(回到顶部)**已保存会话：**(请输入传感器名称，点击**“Save”**)
11. 因为公共密钥不在传感器，点击**开放**并且请使用密码验证连接到传感器CLI。
12. 输入CLI命令的**configure terminal**并且按回车。
13. 输入CLI命令**SSH的authorized-key mykey**，但是请勿此时按回车。确保并且键入空间在末端。
14. 用鼠标右键单击在PuTTY终端窗口。在步骤复制的剪贴板材料5被键入到CLI。
15. 按 **Enter**。
16. 输入**exit命令**并且按回车。
17. 确认已授权密钥适当地被输入。输入**show ssh authorized-keys mykey命令**并且按回车。
18. 输入**exit命令**离开IDS CLI和按回车。

验证

RSA验证

完成下面这些步骤。

1. 启动PuTTY。
2. 找出在对此的步骤10和双击创建的已保存会话。PuTTY终端窗口打开，并且此文本出版：
3. 键入您在步骤6创建的专用密钥密码短语并且按回车。您自动地登陆。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 网络入侵检测技术支持页
- 技术支持和文档 - Cisco Systems