SSH授权密匙的PuTTYgen生成与Cisco Secure IDS上的RSA认证配置示例

目录

简介

本文档说明如何使用PuTTY密钥生成器(PuTTYgen)生成安全外壳(SSH)授权密钥和RSA身份验证，以便在思科安全入侵检测系统(IDS)上使用。建立SSH授权密钥时的主要问题是只能接受较旧的RSA1密钥格式。这意味着您需要告知密钥生成器创建RSA1密钥，并且您必须限制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 - 2004年2月7日
- 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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

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(仅注册客户)查找有关本文档使用的命令的其他信息。

配置PuTTYgen

完成以下步骤以配置PuTTYgen。

1. 启动PuTTYgen。
2. 单击对话框底部的“Parameters”组中的SSH1密钥类型并将生成的密钥中的位数设置为2048。
3. 单击Generate并按照说明操作。

   关键信息显示在对话框的上部。
4. 清除Key Comment编辑框。
5. 选择要粘贴到authorized_keys文件的所有公钥文本，然后按Ctrl-C。
6. 在Key passphrase和Confirm passphrase编辑框中键入密码。
7. 单击Save private key。
8. 将PuTTY私钥文件保存到Windows登录专用目录中(位于Windows 2000/XP中的Documents and Settings/(userid)/My Documents子树中)。
9. 启动PuTTY。
10. 创建新的PuTTY会话，如下所示：
    - 会话：
    - IP Address： IDS传感器的IP地址
    - 协议：SSH
    - 端口：22
    - 连接:
    - 自动登录用户名：cisco（也可以是您在传感器上使用的登录名）
    - 连接/SSH：
    - 首选SSH版本：仅1

- 连接/SSH/身份验证：
- 用于身份验证的私钥文件：浏览到步骤8中存储的.PPK文件。
- 会话：（返回顶部）
- 保存的会话：(输入传感器名称，点击保存)

11. 由于公钥不在传感器上，因此单击Open并使用密码验证来连接到传感器CLI。
12. 输入configure terminal CLI命令并按Enter。
13. 输入ssh authorized-key mykey CLI命令，但此时不要按Enter键。确保并在末尾键入空格。
14. 右键单击PuTTY终端窗口。

    将步骤5中复制的剪贴板材料键入到CLI中。
15. Press Enter.
16. 输入exit命令并按Enter。
17. 确认已正确输入授权密钥。输入show ssh authorized-keys mykey命令并按Enter。
18. 输入exit命令退出IDS CLI，然后按Enter。

验证

RSA身份验证

完成下面这些步骤。

1. 启动PuTTY。
2. 找到在步骤10中创建的已保存会话，然后双击它。PuTTY终端窗口打开，显示以下文本：

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

3. 键入在步骤6中创建的私钥密码短语，然后按Enter。

   您将自动登录。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。