إنشاء برنامج PuTTY للمفاتيح المعتمدة RSA ومصادقة (SSH) لبروتوكول طبقة الأمان من Cisco على مثال تكوين معرفات الأمان

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
تكوين PuTTYgen
التحقق من الصحة
مصادقة RSA
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يشرح هذا المستند كيفية إستخدام مولد المفاتيح ل PuTTY (PuTTYgen) لإنشاء المفاتيح المعتمدة لقشرة الأمان (SSH) ومصادقة RSA للاستخدام على نظام اكتشاف الاقتحام الآمن (IDS) من Cisco. المشكلة الأساسية عند إنشاء مفاتيح SSH المعتمدة هي أن تنسيق مفتاح RSA1 القديم فقط هو المقبول. وهذا يعني أنك بحاجة إلى إبلاغ مولد المفاتيح لديك بإنشاء مفتاح RSA1، ويجب عليك تقييد عميل SSH لاستخدام بروتوكول SSH1.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- خط tty الحديث - 7 فبراير 2004
- Cisco Secure IDS

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

يقدم لك هذا القسم معلومات تكوين الميزات التي يصفها هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على معلومات إضافية حول الأوامر التي يستخدمها هذا المستند.

تكوين PuTTYgen

أكمل الخطوات التالية لتكوين PuTTYgen.

1. بدء تشغيل PuTTYgen.
2. انقر فوق نوع مفتاح **SSH1** وحدد عدد وحدات بت في المفتاح الذي تم إنشاؤه على **2048** في مجموعة المعلمات في أسفل الشاشة.
3. طقطقة **يخلق** واتبع التعليمات.يتم عرض معلومات المفتاح في القسم العلوي من الشاشة.
4. امسح مربع تحرير التعليق الرئيسي.
5. حدد كل النص في المفتاح العام للصقه في ملف allowed_keys واضغط **Ctrl-C**.
6. اكتب عبارة مرور في مربع تحرير عبارة المرور الخاصة بالمفتاح ثم قم بتأكيد عبارة المرور.
7. انقر فوق **حفظ المفتاح الخاص**.
8. قم بحفظ ملف المفتاح الخاص ب PuTTY في دليل خاص إلى تسجيل الدخول إلى Windows (في الشجرة الفرعية المستندات والإعدادات/(userID في Windows 2000/XP)/My Documents).
9. بدء تشغيل خط tty.
10. قم بإنشاء جلسة عمل PuTTY جديدة كما هو موضح هنا:**جلسة العمل:عنوان IP:** عنوان IP الخاص بمستشعر IDS**البروتوكول:** SSH**المنفذ:** 22**الاتصال:اسم المستخدم لتسجيل الدخول التلقائي:** Cisco (يمكن أيضا أن يكون تسجيل الدخول الذي تستخدمه على المستشعر)**الاتصال/SSH:إصدار SSH المفضل:** 1 فقط**الاتصال/SSH/المصادقة:ملف مفتاح خاص للمصادقة:** تصفح إلى ملف .ppk المخزن في الخطوة 8.**الجلسة:** (رجوع إلى الأعلى)**الجلسات المحفوظة:** (أدخل اسم المستشعر، انقر فوق **حفظ**)
11. انقر فوق **فتح** واستخدام مصادقة كلمة المرور للاتصال ب CLI الخاص بالمستشعر، نظرا لأن المفتاح العام غير موجود على المستشعر بعد.
12. أدخل أمر واجهة سطر الأوامر (**configure terminal** CLI) ثم اضغط على مفتاح **Enter**.
13. أدخل أمر واجهة سطر الأوامر mykey **SSH allowed-key**، ولكن لا تضغط على Enter في هذا الوقت. تأكد من ذلك واكتب مسافة في النهاية.
14. انقر بزر الماوس الأيمن في نافذة المحطة الطرفية PuTTY.تتم كتابة مادة الحافظة المنسوخة في الخطوة 5 في CLI.
15. اضغط على المفتاح **Enter**.
16. أدخل الأمر **exit** واضغط على **إدخال**.
17. تأكد من إدخال المفتاح المعتمد بشكل صحيح. أدخل الأمر **show ssh authorized-keys mykey** واضغط **enter**.
18. أدخل الأمر **exit** لإنهاء CLI لمعرف فئة المورد (IDS) واضغط على **إدخال**.

التحقق من الصحة

مصادقة RSA

أكمل الخطوات التالية.

1. بدء تشغيل خط tty.
2. حدد مكان الجلسة المحفوظة التي تم إنشائها في الخطوة 10 وانقر عليها نقرا مزدوجا. يتم فتح نافذة وحدة PuTTY الطرفية ويظهر هذا النص:

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

3. اكتب عبارة مرور المفتاح الخاص التي قمت بإنشائها في الخطوة 6 واضغط على **إدخال**.يتم تسجيل دخولك تلقائيا.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- صفحات الدعم التقني لاكتشاف إقتحام الشبكة
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).