PuTig-generatie van SSH-geautoriseerde toetsen en RSA-verificatie op Cisco Secure IDS-configuratievoorbeeld

Inhoud

Inleiding

Dit document legt uit hoe u de Key generator voor PuTTY (PuTTYgen) kunt gebruiken om beveiligde Shell (SSH)-geautoriseerde toetsen en RSA-verificatie te genereren voor gebruik op Cisco Secure Inbraakdetectiesysteem (IDS). Het primaire probleem wanneer u SSH geautoriseerde toetsen instelt is dat alleen het oudere RSA1 sleutelformaat acceptabel is. Dit betekent dat u uw sleutelgenerator moet vertellen om een RSA1-toets te maken en u moet de SSH1-client beperken om het SSH1-protocol te gebruiken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Recente PuTTY - 7 februari 2004
- Cisco beveiligde IDS-systemen

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

In deze sectie wordt u voorzien van de informatie om de functies te configureren die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om aanvullende informatie te vinden over de opdrachten die dit document gebruikt.

PuTTYgen configureren

Volg deze stappen om PuTTYgen te configureren.

1. Start PuTTYgen.
2. Klik op het sleuteltype **SSH1** en stel het aantal bits in de gegenereerde toets in op **2048** in het vak Parameters onder in het dialoogvenster.
3. Klik op **Generate** en volg de instructies.De belangrijkste informatie wordt weergegeven in het bovenste gedeelte van het dialoogvenster.
4. Schakel het invoervakje voor hoofdcommentaar uit.
5. Selecteer alle tekst in Openbare toets voor het plakken in geautoriseerd_keys bestand en druk op **Ctrl-C**.
6. Typ een wachtwoord in het hoofdwachtwoord en bevestig het wachtwoord.
7. Klik op **Opslaan privé-toets**.
8. Sla het privé-sleutelbestand van PuTTY in een directory privé met uw Windows-inlognaam op (in de substructuur Document en Settings/(gebruikersnaam)/Mijn documenten in Windows 2000/XP).
9. Start PuTTY.
10. Maak een nieuwe PuTTY-sessie zoals hier te zien is:**Sessie:IP-adres:** IP-adres van de IDS-sensorProtocol: SSHPort: 22**Verbinding:Gebruikersnaam voor auto-inloggen:** cisco (kan ook de inlognaam zijn die u op de Sensor gebruikt)**Verbinding/SSH:Voorkeuren van SSH-versie:** Alleen 1**Verbinding/SSH/augustus:Private key file voor verificatie:** Bladeren naar het .PPK-bestand dat in stap 8 is opgeslagen.**Sessie:** (terug naar boven)**Opgeslagen sessies:** (voer de naam van de sensor in en klik op **Opslaan**)
11. Klik op **Open** en gebruik wachtwoordverificatie om verbinding te maken met de Sensor CLI, omdat de openbare toets nog niet op de Sensor is ingeschakeld.
12. Typ de opdracht **configureerbare terminal** CLI en druk op **ENTER**.
13. Typ de opdracht **mykey** CLI van de **ssh met geautoriseerde toets**, maar druk op dit moment niet op ENTER. Zorg ervoor dat u een ruimte aan het einde intypt.
14. Klik met de rechtermuisknop in het aansluitvenster van PuTTY.Het klembord materiaal dat in stap 5 is gekopieerd, wordt in de CLI getypt.
15. Druk op **ENTER**.
16. Typ de opdracht **afsluiten** en druk op **ENTER**.

17. Bevestig dat de geautoriseerde toets correct is ingevoerd. Typ de opdracht **voor** de **sneltoetsen ssh geautoriseerd en druk op ENTER**.
18. Typ de opdracht **afsluiten** om de IDS CLI te verlaten en druk op **ENTER**.

Verifiëren

RSA-verificatie

Volg deze stappen.

1. Start PuTTY.
2. Pak de opgeslagen sessie die in stap 10 is gemaakt en dubbelklik op deze sessie. Er wordt een venster met de tekst PuTTY geopend en deze tekst verschijnt:
```
Sent username "cisco"
Trying public key authentication.
Passphrase for key "":
```
3. Typ het particuliere wachtwoord dat u in stap 6 hebt gemaakt en druk **op ENTER**.U wordt automatisch aangemeld.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Pagina's voor technische ondersteuning van netwerkinbraakdetectie
- Technische ondersteuning en documentatie – Cisco Systems