Que faz “alguém está tentando sequestrar o erro da conexão criptografada” significa?

Índice

Introdução

Este documento descreve o erro “que é possível que alguém está tentando sequestrar a conexão criptografada ao host remoto,” e as etapas corretivas a tomar em seu Cisco enviam por correio eletrónico a ferramenta de segurança (ESA) e o dispositivo do Gerenciamento do Cisco Security (S A).

Que faz “alguém está tentando sequestrar o erro da conexão criptografada” significa?

Quando você configura sua comunicação ESA com seu S A, você pôde ver este erro:

```
Error - The host key for 172.16.6.165 appears to have changed.
It is possible that someone is trying to hijack the encrypted
connection to the remote host.
Please use the logconfig->hostkeyconfig command to verify
(and possibly update) the SSH host key for 172.16.6.165.
```

Isto pode ocorrer quando um ESA é substituído e usa o mesmos hostname e/ou endereço IP de Um ou Mais Servidores Cisco ICM NT que o ESA original. As chaves previamente armazenadas SSH usadas em uma comunicação e na autenticação entre o ESA e o S A são armazenadas no S A. O S A vê então que o trajeto de comunicação ESA mudou, e acredita que um origem não autorizada está agora no controle do endereço IP de Um ou Mais Servidores Cisco ICM NT assocaited ao ESA.

A fim corrigir isto, o início de uma sessão ao CLI do S A, e terminar estas etapas:

1. Incorpore o comando do **logconfig**.
2. Incorpore o **hostkeyconfig**.
3. Incorpore a **supressão** e escolha o número associado na lista atualmente instalada da chave Host para o IP ESA.
4. Retorne à alerta principal CLI e inscreva o **comando commit**.

```
mysma.local> logconfig
```

```
Currently configured logs:
Log Name Log Type Retrieval Interval
-----------------------------------------------------------------------------
1. authentication Authentication Logs FTP Poll None
2. backup_logs Backup Logs FTP Poll None
3. cli_logs CLI Audit Logs FTP Poll None
4. euq_logs Spam Quarantine Logs FTP Poll None
5. euqgui_logs Spam Quarantine GUI Logs FTP Poll None
6. ftpd_logs FTP Server Logs FTP Poll None
7. gui_logs HTTP Logs FTP Poll None
8. haystackd_logs Haystack Logs FTP Poll None
9. ldap_logs LDAP Debug Logs FTP Poll None
10. mail_logs Cisco Text Mail Logs FTP Poll None
11. reportd_logs Reporting Logs FTP Poll None
12. reportqueryd_logs Reporting Query Logs FTP Poll None
13. slbld_logs Safe/Block Lists Logs FTP Poll None
14. smad_logs SMA Logs FTP Poll None
15. snmp_logs SNMP Logs FTP Poll None
16. sntpd_logs NTP logs FTP Poll None
17. system_logs System Logs FTP Poll None
18. trackerd_logs Tracking Logs FTP Poll None
19. updater_logs Updater Logs FTP Poll None
20. upgrade_logs Upgrade Logs FTP Poll None

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig

Currently installed host keys:
1. 172.16.6.165 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA0ilM...DVc7plDQ==
2. 172.16.6.150 ssh-dss AAAAB3NzaC1kc3MAAACBAODKHq6uakiM...cooFXzLHFP
3. 172.16.6.131 ssh-dss AAAAB3NzaC1kc3MAAACBAI4LkblFtidp...WhM5XLNA==


Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> delete

Enter the number of the key you wish to delete.
[]> 1

Currently installed host keys:
1. 172.16.6.150 ssh-dss AAAAB3NzaC1kc3MAAACBAODKHq6uakiM...cooFXzLHFP
2. 172.16.6.131 ssh-dss AAAAB3NzaC1kc3MAAACBAI4LkblFtidp...WhM5XLNA==

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
```

```
- HOSTKEYCONFIG - Configure SSH host keys.
[]>

Currently configured logs:
Log Name Log Type Retrieval Interval
-----------------------------------------------------------------------------
1. authentication Authentication Logs FTP Poll None
2. backup_logs Backup Logs FTP Poll None
3. cli_logs CLI Audit Logs FTP Poll None
4. euq_logs Spam Quarantine Logs FTP Poll None
5. euqgui_logs Spam Quarantine GUI Logs FTP Poll None
6. ftpd_logs FTP Server Logs FTP Poll None
7. gui_logs HTTP Logs FTP Poll None
8. haystackd_logs Haystack Logs FTP Poll None
9. ldap_logs LDAP Debug Logs FTP Poll None
10. mail_logs Cisco Text Mail Logs FTP Poll None
11. reportd_logs Reporting Logs FTP Poll None
12. reportqueryd_logs Reporting Query Logs FTP Poll None
13. slbld_logs Safe/Block Lists Logs FTP Poll None
14. smad_logs SMA Logs FTP Poll None
15. snmp_logs SNMP Logs FTP Poll None
16. sntpd_logs NTP logs FTP Poll None
17. system_logs System Logs FTP Poll None
18. trackerd_logs Tracking Logs FTP Poll None
19. updater_logs Updater Logs FTP Poll None
20. upgrade_logs Upgrade Logs FTP Poll None

mysma.local> commit

Please enter some comments describing your changes:
[]> ssh key update
```

Finalmente, do S A GUI, escolha **dispositivos centralizados do > segurança de Serivces** e selecione então o ESA na lista que tinha apresentado o erro original. Uma vez que você escolhe **estabelecer a conexão…** e a **conexão de teste**, autentica, cria um par de chave Host novo SSH, e armazena este par de chave Host no S A.

Revisite o CLI para o S A, e torne a colocar em funcionamento o **logconfig > o hostkeyconfig** a fim ver os pares de chave Host novos.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Dispositivo do Gerenciamento do Cisco Security - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems