Introdução

Este documento descreve como gerar uma chave privada do Shell Seguro (ssh) e usar isso para o username e a autenticação ao registrar no comando line interface(cli) na ferramenta de segurança do email de Cisco (ESA).

Como configurar a autenticação da chave pública SSH para o início de uma sessão ao ESA sem uma senha

A autenticação da chave pública (PKI) é um método de autenticação que confie keypair público/privado gerado. Com PKI, uma “chave especial” é gerada que tenha uma propriedade muito útil: Qualquer um que pode ler a metade pública da chave pode cifra os dados que podem então somente ser lidos por uma pessoa que tenha o acesso à metade privada da chave. Desta maneira, ter o acesso à metade pública de uma chave permite que você envie a informação secreta a qualquer um com a metade privada, e igualmente verifique que uma pessoa tem de facto o acesso à metade privada. É fácil de ver como esta técnica poderia ser usada para autenticar.

Como um usuário, você pode gerar um keypair e então colocar a metade pública da chave em um sistema remoto, tal como seu ESA. Esse sistema remoto pode então autenticar seu usuário - identificação, e permite que você entre apenas tendo o demonstra que você tem o acesso à metade privada do keypair. Isto é feito a nível de protocolo dentro do SSH e acontece automaticamente.

, Contudo, significa que você precisa de proteger a privacidade da chave privada. Em um sistema compartilhado onde você não tenha a raiz isto pode ser realizado cifrando a chave privada com uma frase de passagem, que funcione similarmente a uma senha. Antes que o SSH possa ler sua chave privada a fim executar a autenticação da chave pública você estará pedido para fornecer a frase de passagem de modo que a chave privada possa ser decifrada. Em mais sistemas seguros (como uma máquina onde você seja o único usuário, ou uma máquina em sua HOME onde nenhum desconhecido terá o acesso físico) você pode simplificar este processo criando uma chave privada unencrypted (sem a frase de passagem) ou entrando em sua frase de passagem uma vez e então pondo em esconderijo a chave na memória para a duração de seu tempo no computador. OpenSSH contém uma ferramenta chamada o SSH-agente que simplifica este processo.

exemplo SSH-keygen para Linux/Unix

Termine as seguintes etapas para estabelecer seu uma estação de trabalho do linux/unix (ou o server) a conectar ao ESA sem uma senha. Neste exemplo, nós não especificaremos como a frase de passagem.

1) Em sua estação de trabalho (ou em server), gere uma chave privada usando o comando unix **SSH-keygen**:

```
$ ssh-keygen -b 2048 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/[USERID]/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
Your identification has been saved in /home/[USERID]/.ssh/id_rsa.
Your public key has been saved in /home/[USERID]/.ssh/id_rsa.pub.
The key fingerprint is:
00:11:22:77:f6:a9:1e:19:f0:ca:28:9c:ff:00:11:22 [USERID]@hostname.com
The key's randomart image is:
+--[ RSA 2048]----+
| +... +|
| o= o+|
| o o ..|
| . ..o . + |
| . ES. o + |
| o + . . |
| o . . |
| o o |
| . . |
+-----------------+
```

(o *the acima foi gerado de Ubuntu 14.04.1)

2) Abra o arquivo de chave pública (id_rsa.pub) criou em #1 e copiam a saída:

```
$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJg9W3DeGf83m+E/PLGzUFPalSoJz5F
t54Wl2wUS36NLxm4IO4Xfrrb5bA97I+ZA4YcB1l/HsFLZcoljAK4uBbmpY5kXg96A6Wf
mIYMnl+nV2vrhrODgbcicEAdMcQN3wWHXiEWacV+6u+FlHlonkSAIDEug6vfnd+bsbcP
Zz2uYnx1llxbVtGftbWVssBK3LkFp9f0GwDiYs7LsXvQbTkixrECXqeSrr+NLzhU5hf6
eb9Kn8xjytf+eFbYAslam/NEfl9i4rjide1ebWN+LnkdcE5eQ0ZsecBidXv0KNf45RJa
KgzF7joke9niLfpf2sgCTiFxg+qZ0rQludntknw [USERID]@hostname.com
```

3) Entre a seu dispositivo e configurar seu ESA para reconhecer sua estação de trabalho (ou server) que usam a chave do público SSH que você criou em #1, e **comprometa as** mudanças. Observe a solicitação da senha durante o início de uma sessão:

```
$ ssh admin@192.168.0.199
******************************
CONNECTING to myesa.local
Please stand by...
******************************

Password:[PASSWORD]
Last login: Mon Aug 18 14:11:40 2014 from 192.168.0.200
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance

myesa.local> sshconfig

Currently installed keys for admin:

Choose the operation you want to perform:
```

```
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJg9W3DeGf83m+E/PLGzUFPalSoJz5F
t54Wl2wUS36NLxm4IO4Xfrrb5bA97I+ZA4YcB1l/HsFLZcoljAK4uBbmpY5kXg96A6Wf
mIYMnl+nV2vrhrODgbcicEAdMcQN3wWHXiEWacV+6u+FlHlonkSAIDEug6vfnd+bsbcP
Zz2uYnx1llxbVtGftbWVssBK3LkFp9f0GwDiYs7LsXvQbTkixrECXqeSrr+NLzhU5hf6
eb9Kn8xjytf+eFbYAslam/NEfl9i4rjide1ebWN+LnkdcE5eQ0ZsecBidXv0KNf45RJa
KgzF7joke9niLfpf2sgCTiFxg+qZ0rQludntknw [USERID]@hostname.com

Currently installed keys for admin:
1. ssh-rsa AAAAB3NzaC1yc2EAA...rQludntknw ([USERID]@hostname.com)

Choose the operation you want to perform:
- NEW - Add a new key.
- DELETE - Remove a key.
- PRINT - Display a key.
- USER - Switch to a different user to edit.
[]>

myesa.local> commit
```

4) Retire fora do dispositivo, e do re-início de uma sessão. Observe que a solicitação da senha está removida, e o acesso está concedido diretamente:

```
myesa.local> exit

Connection to 192.168.0.199 closed.
robert@ubuntu:~$ ssh admin@192.168.0.199
******************************
CONNECTING to myesa.local
Please stand by...
******************************

Last login: Mon Aug 18 14:14:50 2014 from 192.168.0.200
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local>
```

exemplo SSH-keygen para Windows

Termine as seguintes etapas para estabelecer seu uma estação de trabalho do Windows (ou o server) a conectar ao ESA sem uma senha. Neste exemplo, nós não especificaremos como a frase de passagem.

Nota: Há uma variação no aplicativo do console usado de Windows. Você precisará de

pesquisar e encontrar a solução que trabalha melhor para seu aplicativo do console. Este exemplo usará a massa de vidraceiro e o PuTTyGen.

1) Abra PuttyGen.

2) Para o tipo de chave a gerar, selecione SSH-2 RSA.

3) Clique o botão da **geração**.

4) Mova seu rato na área abaixo da barra do progresso. Quando a barra do progresso está completa, PuTTYgen gera seu par de chaves.

5) Datilografe uma frase de passagem no campo chave da frase de passagem. Datilografe a mesma frase de passagem no campo da frase de passagem da confirmação. Você pode usar uma chave sem uma frase de passagem, mas este não é recomendado.

6) Clique o botão da **chave privada da salvaguarda** para salvar a chave privada.

Nota: Você deve salvar a chave privada. Você precisá-la-á de conectar a sua máquina.

7) Clicar com o botão direito no campo de texto etiquetado chave pública para colar em authorized_keys de OpenSSH o arquivo e escolha **seleto tudo**.

8) Clicar com o botão direito outra vez no mesmo campo de texto e escolha a **cópia**.

9) Usando a massa de vidraceiro, entre a seu dispositivo e configurar seu ESA para reconhecer sua estação de trabalho do Windows (ou server) que usam a chave do público SSH que você salvar e copiou de #6 - #8, e compromete as mudanças.

```
login as: admin
Using keyboard-interactive authentication.
Password: [PASSWORD]
Last login: Mon Aug 18 11:46:17 2014 from 192.168.0.201
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local> sshconfig

Currently installed keys for admin:

Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAj6ReI+gqLU3W1uQAMUG0620B+tpdkjkgBn
5NfYc+qrtyB93stG38O1T4s0zHnhuKJLTdwBg/JHdFuNO77BY+21GYGS27dMp3UT9/VuQ
```

```
TjP8DmWKOa+8Mpc9ePdCBZp1C4ct9oroidUT3V3Fbl5M9rL8q4/gonSi+7iFc9uOaqgDM
/h+RxhYeFdJLechMY5nN0adViFloKGmV1tz3K9t0p+jEW5l9TJf+fl5X6yxpBBDoNcaB9
jNwQ5v7vcIZBv+fl98OcXD9SNt08G0XaefyD2VuphtNA5EHwx+f6eeA8ftlmO+PgtqnAs
c2T+i3BAdC73xwML+1IG82zY51pudntknw rsa-key-20140818

Currently installed keys for admin:
1. ssh-rsa AAAAB3NzaC1yc2EAA...51pudntknw (rsa-key-20140818)

Choose the operation you want to perform:
- NEW - Add a new key.
- DELETE - Remove a key.
- PRINT - Display a key.
- USER - Switch to a different user to edit.
[]>

myesa.local> commit
```

10) Da janela de configuração da massa de vidraceiro, e de sua sessão salvar PRE-existente para seu ESA, escolha a **conexão > o SSH > o AUTH** e no *arquivo-chave privado para o* campo da *autenticação*, o clique **consulta** e encontra sua chave privada salvar da etapa #6.

11) Salvar a sessão (perfil) na massa de vidraceiro, e clique **aberto**. Entre com o username, se não já salvar ou especificado da sessão PRE-configurada. Observe a inclusão da "autenticação com chave pública "[FILE-NAME OF SAVED PRIVATE KEY]" ao entrar:

```
login as: admin
Using keyboard-interactive authentication.
Password: [PASSWORD]
Last login: Mon Aug 18 11:46:17 2014 from 192.168.0.201
Copyright (c) 2001-2013, Cisco Systems, Inc.


AsyncOS 8.5.6 for Cisco C100V build 074

Welcome to the Cisco C100V Email Security Virtual Appliance
myesa.local> sshconfig

Currently installed keys for admin:

Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new

Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAj6ReI+gqLU3W1uQAMUG0620B+tpdkjkgBn
5NfYc+qrtyB93stG38O1T4s0zHnhuKJLTdwBg/JHdFuNO77BY+21GYGS27dMp3UT9/VuQ
TjP8DmWKOa+8Mpc9ePdCBZp1C4ct9oroidUT3V3Fbl5M9rL8q4/gonSi+7iFc9uOaqgDM
/h+RxhYeFdJLechMY5nN0adViFloKGmV1tz3K9t0p+jEW5l9TJf+fl5X6yxpBBDoNcaB9
jNwQ5v7vcIZBv+fl98OcXD9SNt08G0XaefyD2VuphtNA5EHwx+f6eeA8ftlmO+PgtqnAs
c2T+i3BAdC73xwML+1IG82zY51pudntknw rsa-key-20140818
```

```
Currently installed keys for admin:
1. ssh-rsa AAAAB3NzaC1yc2EAA...51pudntknw (rsa-key-20140818)

Choose the operation you want to perform:
- NEW - Add a new key.
- DELETE - Remove a key.
- PRINT - Display a key.
- USER - Switch to a different user to edit.
[]>

myesa.local> commit
```

Informações Relacionadas

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