Como usar chaves SSH para conectar-se sem uma senha.

OpenSSH é uma maneira muito segura de se conectar remotamente a uma máquina Slackware. Mas a maneira mais fácil de usar o SSH é usar seu recurso principal.

O conceito de chaves públicas/privadas pode ser difícil de explicar; tentaremos analisá-lo da maneira mais simples possível.

Permita-me dizer isso novamente, para todos vocês, nerds de criptografia por aí: sim, eu sei que esta é uma versão muito simplificada do SSH. Isso é criado para todos os novatos em SSH... mmmmkay?

Essencialmente, as chaves SSH são baseadas na criptografia de chave pública. Isso significa que você cria two keys: um é chamado de chave pública e é usado para criptografar dados que somente você pode descriptografar. Você pode dar sua chave pública a qualquer pessoa, pois sua única função é criptografar dados - não há muito mais que você possa fazer com ela. A outra chave é chamada de chave PRIVATE e é essa chave usada para descriptografar dados criptografados com a chave pública.

Até aí tudo bem ... Agora, como isso é usado com o SSH?

Sempre que você entrar em contato com uma máquina Slackware (ou qualquer outra máquina executando o OpenSSH, na verdade) através do protocolo SSH, seu SSH client o programa instalado no computador à sua frente que você usa para se conectar) conversará com o SSH server instalado na máquina distante. Eles determinarão juntos os recursos que os dois podem usar e a versão do protocolo que devem usar para se comunicar com segurança.

Em seguida, eles tentarão determinar como você (o usuário) fará login na máquina remota. Se as chaves não forem usadas, o SSH normalmente (mas nem sempre) assume como padrão a solicitação de uma senha. Por outro lado, se chaves forem usadas, as máquinas as usarão na seguinte ordem:

1. O servidor SSH criptografará uma mensagem curta (tecnicamente um valor de hash) com sua chave pública e a enviará ao seu computador.
2. Seu cliente SSH descriptografará esta mensagem com a chave privada (cuja única cópia deve estar no seu computador) e a enviará de volta ao servidor SSH.
3. O servidor SSH ficará convencido de que você “é você”, por assim dizer, já que você é teoricamente a única pessoa capaz de descriptografar a mensagem enviada e concederá acesso imediatamente.

Se tudo isso parecer um pouco complicado, lembre-se do seguinte: você tem uma chave pública e uma chave privada. A chave pública deve estar no computador ao qual você deseja acessar ou no computador “remoto”. A chave privada deve estar no seu computador.

Vamos seguir esse processo passo a passo!

Crie o par de chaves pública/privada

Para criar uma chave pública e uma chave privada, use o utilitário OpenSSH `ssh-keygen`. Isso gerará automaticamente um par de chaves, usando os valores padrão. Aqui está um pequeno exemplo:

```
noryungi@mypc:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/noryungi/.ssh/id_rsa): TEST.rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in TEST.rsa.
Your public key has been saved in TEST.rsa.pub.
The key fingerprint is:
1a:99:51:a6:12:69:53:aa:d8:f6:c2:56:66:6e:68:5a noryungi@udon
The key's randomart image is:
+--[ RSA 2048]----+
|    .o. o        |
|    +o +         |
|   .o.o          |
| o . . +         |
|. + + + S        |
| o B   o         |
|  E + .          |
| = o             |
|.                |
+-----------------+
noryungi@mypc:~$ ls TEST*
TEST.rsa  TEST.rsa.pub
```

OK, o que está acontecendo aqui? Primeiro, `ssh-keygen` irá gerar um par de chaves. Até agora, tudo bem, certifique-se de ler o ssh-keygen man page para entender todas as opções, e existem muitas.

Próximo, `ssh-keygen` responderá que está criando o par de chaves RSA (chave pública e privada). RSA é o nome do algoritmo de criptografia usado. Existem três dessas criptografias possíveis: DSA, RSA e ECDSA. Qual é o melhor é deixado como um exercício para o leitor ... 

Em seguida, ele perguntará onde salvar a chave. Aqui, `TEST.rsa` é inserido, pois existem outras chaves no sistema. É importante dar um nome adequado à chave, pois torna muito mais fácil lembrar qual chave se conecta ao que.

Por exemplo, se você tivesse uma conta em uma máquina chamada: `stang.slackware.com`, um bom nome para o par de chaves seria `stang_slackware_com.rsa` ou algo parecido.

Em seguida, `ssh-keygen` solicita uma senha. É sempre uma boa ideia digitar uma senha. Isso permite que você proteja sua chave privada, mesmo que ela caia nas mãos erradas. Se você estiver absolutamente 100% certo de que sua chave privada ** não vai cair em mãos erradas (quão otimista você é!), Basta pressionar `Enter` aqui.

O restante são apenas mensagens informativas e você observará que o par de chaves foi salvo da

seguinte maneira:

1. A chave privada é nomeada TEST.rsa.
2. A chave pública - aquela que você deseja copiar na máquina remota - é nomeada TEST.rsa.pub

Parabéns! Você está no meio do caminho!

Configure sua chave pública no computador remoto

Tudo bem, agora, como usar a chave pública/privada? Isso é simples: copie a chave pública (denominada TEST.rsa.pub como vimos) no computador remoto. A melhor maneira de fazer isso é usar scp o programa de cópia segura do OpenSSH. Por exemplo:

```
noryungi@mypc$ scp TEST.rsa.pub
nr@test.example.com:/home/nr/.ssh/authorized_keys
```

No exemplo acima, copio a chave public TEST.rsa.pub na máquina remota denominada test.example.com, como usuário nr. O arquivo é renomeado allowed_keys, que é o nome do arquivo que contém todas as chaves públicas autorizadas a se conectar ao servidor.

Uma palavra de cautela aqui: não execute o comando scp acima se você já possui um arquivo allowed_keys no computador remoto! Isso substituirá o conteúdo do arquivo pela sua chave pública !! Se você já possui um arquivo allowed_keys, execute um cat TEST.rsa.pub » allowed_keys na máquina remota para adicionar sua chave pública ao final das chaves autorizadas

Como todas as chaves SSH que você usa devem ser colocadas no diretório .ssh , é para onde elas vão na máquina remota.

Então, nós terminamos? Na verdade, não há apenas uma pequena coisa a fazer, mas é realmente importante, pois é a fonte de muitos problemas...

Verifique as permissões de chave pública na máquina remota

Como as chaves pública e privada são muito sensíveis, elas devem ser protegidas contra olhares indiscretos. Para fazer isso, em both no computador remoto e na máquina local, digite o seguinte comando:

```
nr@test.example.com$ chmod -R -v g-rwx,o-rwx ./.ssh/
mode of `./.ssh/' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of `./.ssh/authorized_keys' changed from 0644 (rw-r--r--) to 0600 (rw-
------)
```

Este comando permite garantir que ninguém (exceto você e o servidor SSH) possa ler a chave pública.

Observe: se as permissões no arquivo `allowed_keys` OU no diretório `.ssh` não estiverem corretas, o OpenSSH não utilizará as chaves! Se você tiver algum problema com uma chave pública/privada, verifique as permissões e ou execute o comando acima para verificar se estão corretas!

Conecte-se usando sua chave SSH recém-criada

Vamos tentar conectar, de volta à máquina local, ao servidor remoto chamado`test.example.com`:

```
noryungi@mypc$ ssh -i TEST.rsa nr@test.example.com
```

Observe que entrei na opção `-i` logo após o comando `ssh`: essa opção seleciona a chave privada a ser usada para conectar-se, como usuário `nr`, ao servidor remoto denominado `test.example.com`.

Se você optou por proteger a chave privada com uma senha, `ssh` solicitará essa senha antes de conectar. Caso contrário ... Bem, se as permissões estiverem corretas (veja acima), você deverá ver o equivalente ao seguinte:

```
nr@test.example.com$
```

É isso aí! Você está conectado a uma máquina remota, sem nunca digitar uma senha e com uma segurança muito melhor do que com uma senha - que pode ser adivinhada, enquanto uma chave é muito longa para ser adivinhada.

O que poderia dar errado neste momento?

Bem, na verdade não muito, exceto a possibilidade de o administrador do sistema não querer que você se conecte com um par de chaves pública/privada ...

Nesse caso, convenhamos, ele não é um administrador de sistema muito bom. Isso pode ser verificado, no entanto, com o seguinte comando na máquina remota:

```
nr@test.example.com$ grep -i pubkeyauth /etc/ssh/sshd_config
#PubkeyAuthentication yes
```

Observe a linha `#PubkeyAuthentication yes`: este é o valor padrão para autenticação de chave pública e, como você pode ver, está definido como `yes`. Você está pronto para usar sua chave! Por outro lado, se você vir algo assim:

```
nr@test.example.com$ grep -i pubkeyauth /etc/ssh/sshd_config
PubkeyAuthentication no
```

Então você não tem permissão para se conectar à máquina remota (`test.example.com` acima) com uma chave pública. Hora de entrar em contato com o administrador do sistema ou com o administrador de segurança e pedir educadamente para poder usá-los.

(Sim, existem outras maneiras, mais sorrateiras, de se conectar sem digitar uma senha, mas nenhuma delas é tão segura quanto um par de chaves pública/privada - talvez em outra documentação neste wiki?) 

Você chegou ao final desta breve documentação - vá em frente e use as teclas OpenSSH!

Veja também

- The OpenSSH manual pages (online)

Sources

- Originally written by Noryungi

- — *slackjeff 2020/06/23 18:31 (BRT)*

howtos, security, ssh, sshkeys, author noryungi