

Atividades – Autenticação SSH com Putty

Este guia descreve como gerar e usar um par de chaves pública/privada para efetuar login em um sistema remoto com SSH usando [PuTTY](#) . PuTTY é um cliente SSH que está disponível para Windows e Linux (embora seja mais comum em sistemas Windows).

Usando logins-chave baseados em SSH, você pode desativar o procedimento de login de usuário / senha normal, o que significa que apenas pessoas com um par válido de chaves privada/pública podem logar.

Nota Preliminar

Neste tutorial eu uso um desktop Windows para se conectar a um servidor Linux SSH (Ubuntu com endereço IP: *192.168.0.100*).

Instale PuTTY, PuTTYgen, E Pageant no sistema Windows

Primeiro nós precisamos instalar PuTTY, PuTTYgen e Pageant em nosso sistema Windows. Tudo o que precisa fazer é baixar os arquivos executáveis (.exe) e salvá-los em algum lugar, por exemplo, na área de trabalho. Nós não precisamos instalá-los visto que eles são aplicativos independentes. Para iniciá-los, basta dar um clique duplo-los.

Faça o download dos seguintes arquivos da [página de download do PuTTY](#) e salvá-los em seu sistema Windows, por exemplo, na área de trabalho:

<https://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

<https://the.earth.li/~sgtatham/putty/latest/x86/puttygen.exe>

<https://the.earth.li/~sgtatham/putty/latest/x86/pageant.exe>

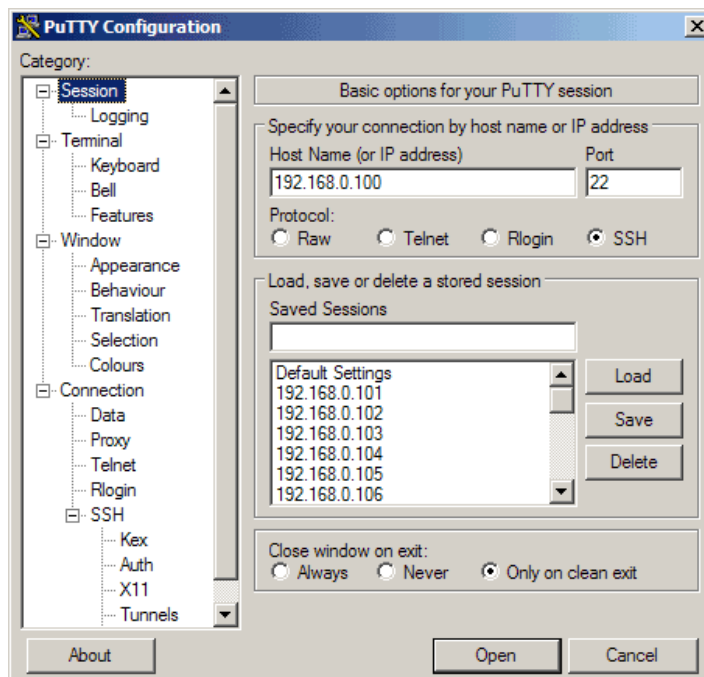


Criar um perfil com definições para o nosso servidor 192.168.0.100

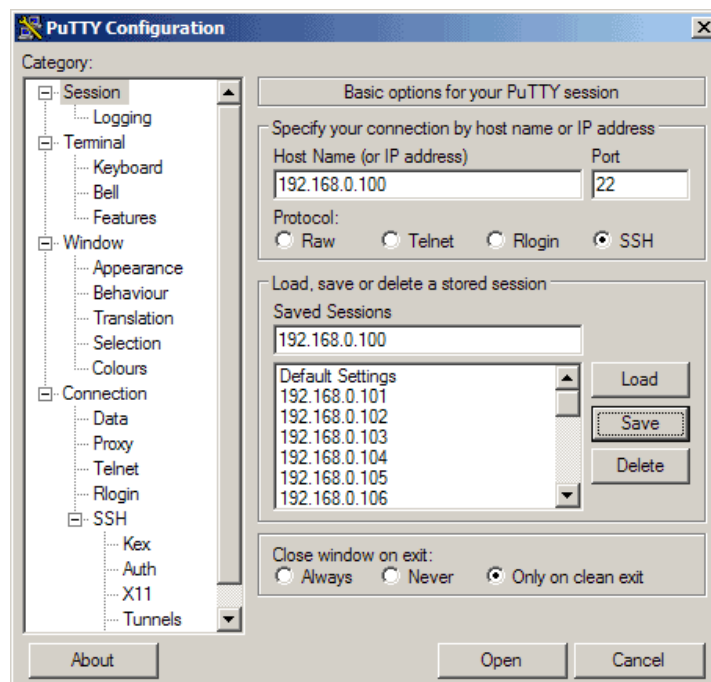
Em PuTTY, você pode criar perfis para conexões com seus vários servidores SSH, para que você não tem que digitar as configurações novamente quando você quiser se conectar a um determinado servidor novamente.

Vamos criar um perfil para o nosso servidor *192.168.0.100*. Inicie o PuTTY clicando duas vezes seu arquivo executável. Agora você está na categoria *Session* (ver a árvore no lado

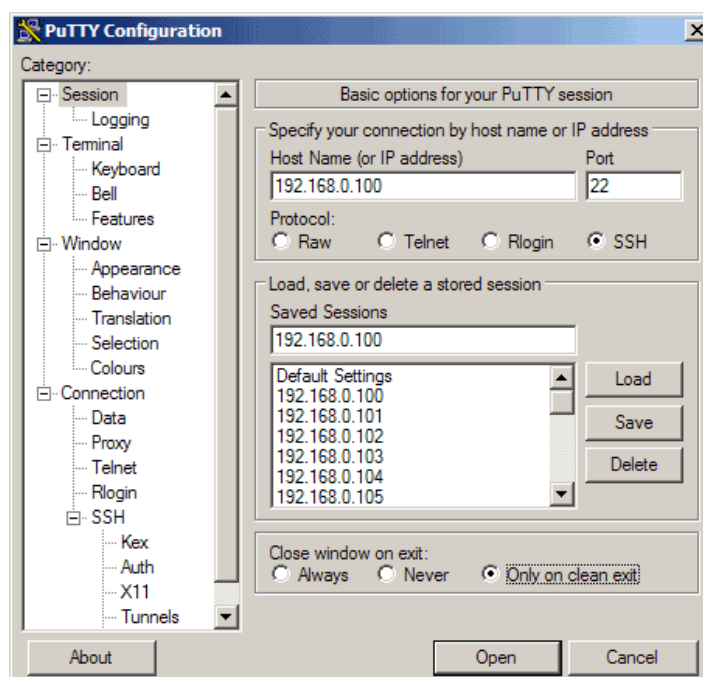
esquerdo da imagem). Digite *192.168.0.100* em *Nome do host (ou endereço IP)*, digite *22* sob *Port* e selecione *SSH* ao abrigo do *Protocol*:



Sob *Save Sessions* digite um nome para o perfil, por exemplo *192.168.0.100* ou qualquer outro nome que permite que você se lembre de qual servidor o perfil se refere. Em seguida, clique em *Salvar*:



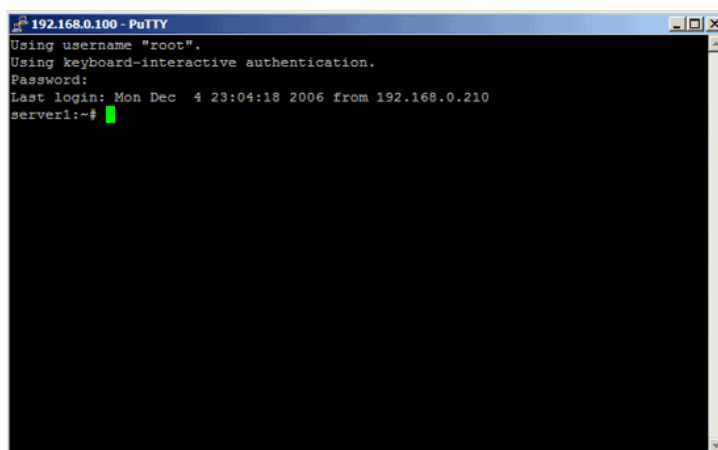
A próxima vez que você usar PuTTY, você pode simplesmente selecionar o perfil adequado em *Saved Sessions*, clique em *Carregar* e, em seguida, em *Abrir*. Agora podemos conectar ao nosso servidor SSH simplesmente clicando em *Open*.



Se você se conectar ao servidor pela primeira vez, um aviso de segurança aparece. Isso ocorre porque PuTTY não sabe a chave de host do servidor, portanto é seguro clicar em *Sim*. (Se isso acontecer novamente, mais tarde, isso pode significar que outro servidor está agora em execução sob o mesmo endereço IP, ou que alguém tenha alterado o acesso ao servidor e mudado a chave.)



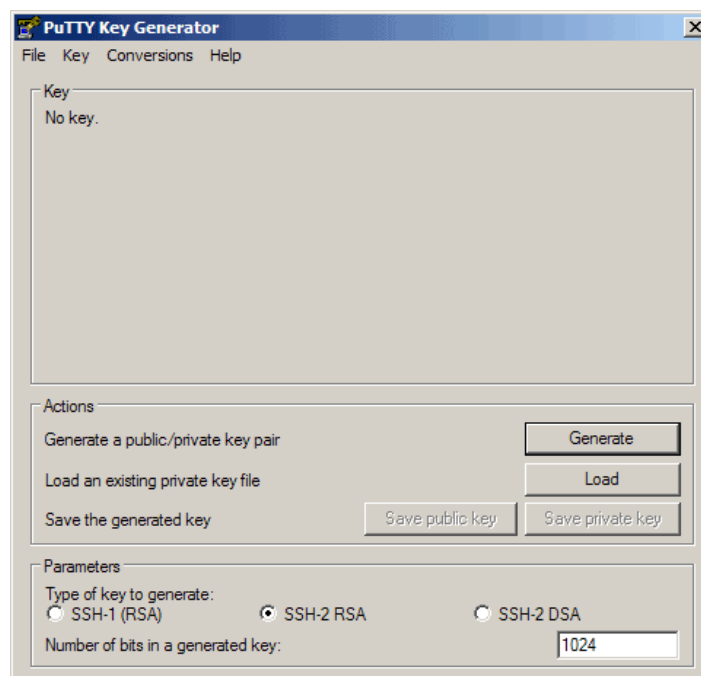
Temos guardado o nome de usuário com o qual conectar em nossas configurações de perfil, por isso, não tem que digitá-lo aqui novamente. Nós só precisamos especificar a senha do usuário:



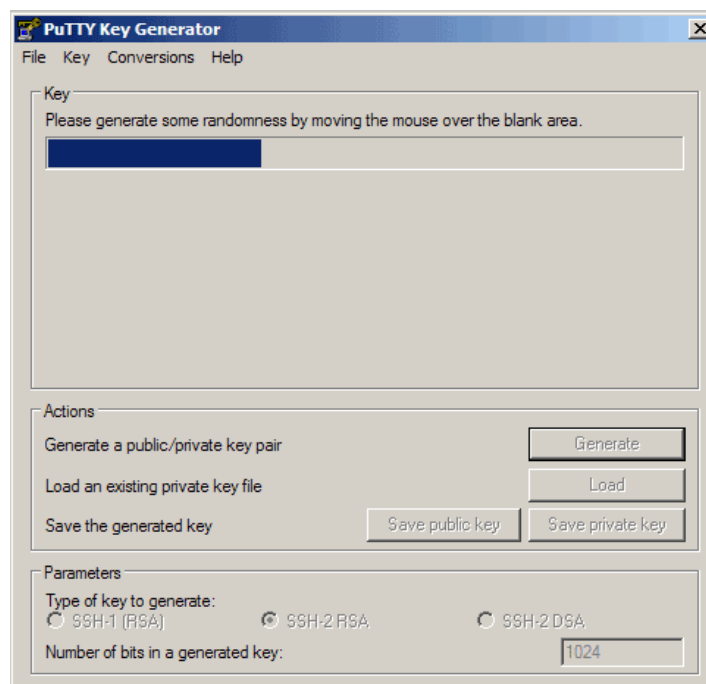
Agora, esta era a maneira "normal" de login, ou seja, com um nome de usuário e uma senha. Se alguém sabe o nome de usuário e senha, ele pode entrar também. Então se você tem senhas fracas e/ou for vítima de um ataque de bruta força, isso pode se tornar um problema. Vamos mudar isso agora.

Gerar um par de chaves pública e privado

Podemos usar PuTTYgen para criar um par de chaves pública/privada. Iniciá-lo clicando duas vezes seu arquivo executável. Certifique-se de que você selecione *SSH-2 RSA* sob o *tipo de chave para gerar* e especifique *2048* como o *número de bits em uma chave gerada*. Em seguida, clique em *Gerar*:

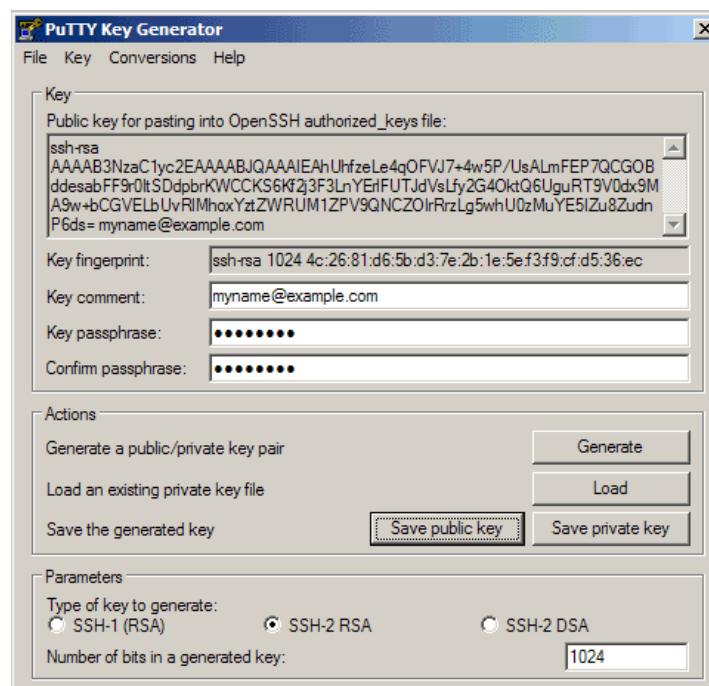


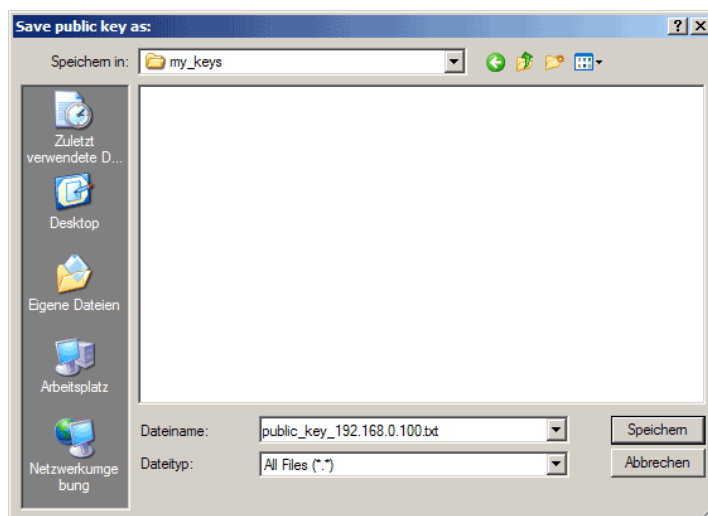
Mova o ponteiro do mouse sobre a área em branco durante a geração de chaves para gerar alguma aleatoriedade:



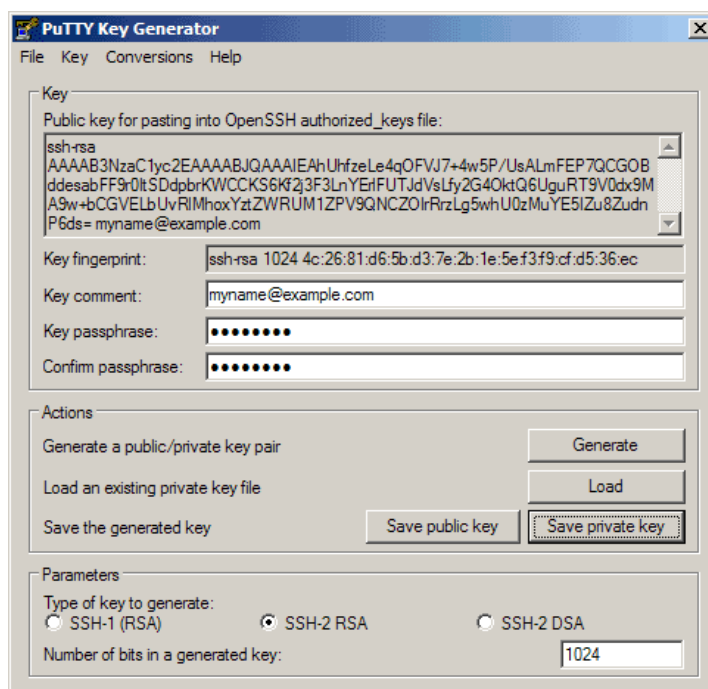
Agora, um par de chaves privada/pública foram geradas. Sob *comentário Key*, você pode inserir qualquer comentário; Normalmente você use seu endereço de e-mail aqui. Em seguida, especifique uma *senha Key* e repeti-lo sob *Confirmar senha*. Você vai precisar que frase-senha para efetuar login no SSH com a sua nova chave.

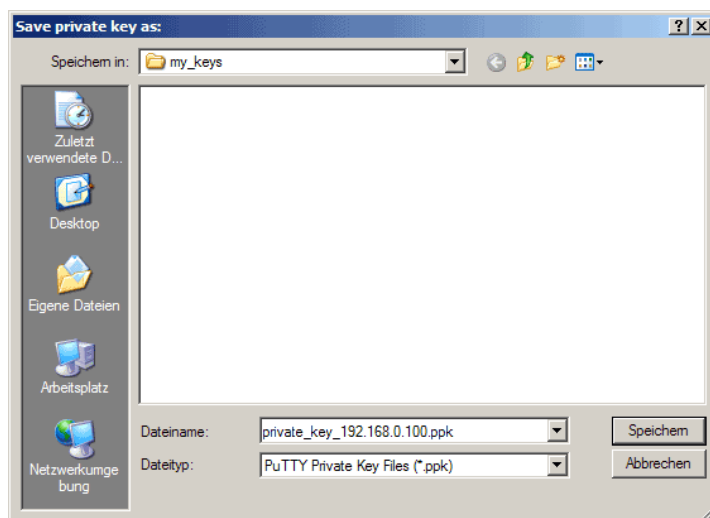
Em seguida, clique em *Save Public Key* e salvá-lo em algum local seguro no seu computador. Você é livre para escolher um nome de arquivo e extensão, mas deve ser um que permite que você se lembrar por qual sistema é.



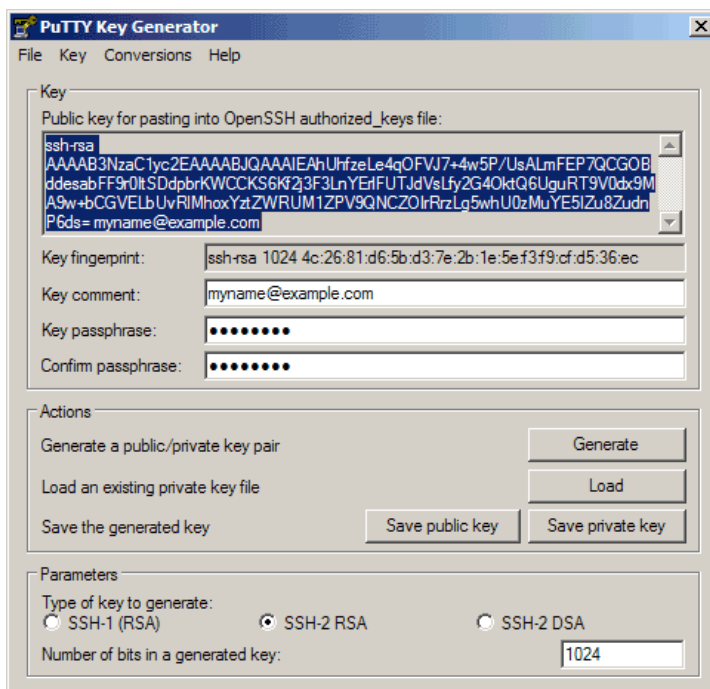


Em seguida, clique em *Save Private Key*. Você pode salvá-lo no mesmo local que a chave pública - deve ser um local que só você pode acessar. Mais uma vez, você é livre para escolher um nome de arquivo, mas desta vez a extensão deve ser *.ppk*:





Em seguida, copie a chave pública a partir da janela PuTTYgen:



Salvar a chave pública no servidor

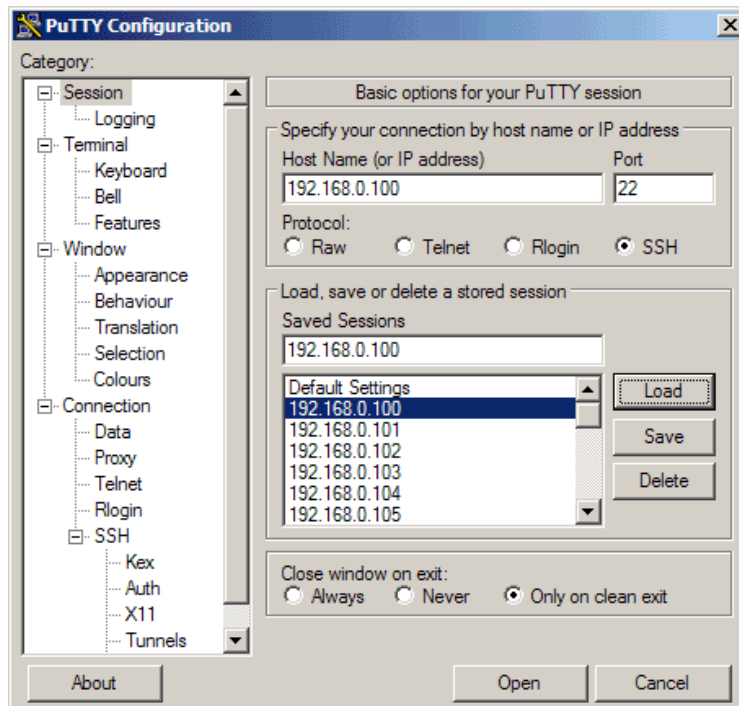
Em seguida, faça o login para o servidor SSH, ainda com o nome de usuário e senha, e cole

```
# mkdir ~/.ssh
# chmod 700 ~/.ssh
# nano ~/.ssh/authorized_keys2
# chmod 600 ~/.ssh/authorized_keys2
```

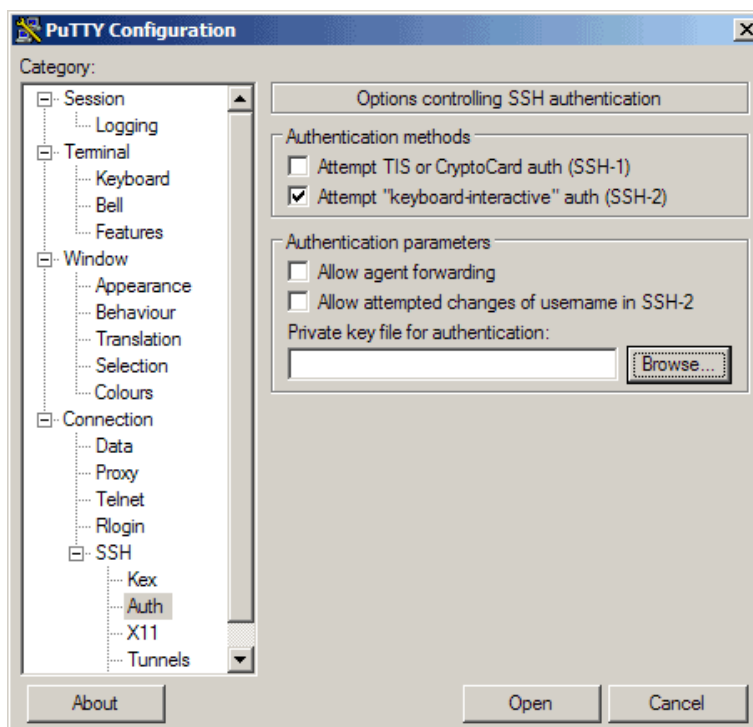
a

chave pública no arquivo `~/.ssh/authorized_keys2`, assim (em uma linha!):

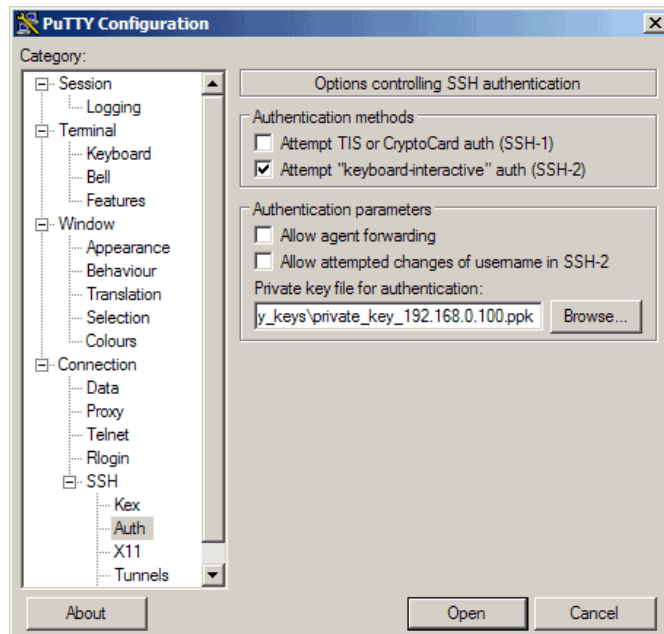
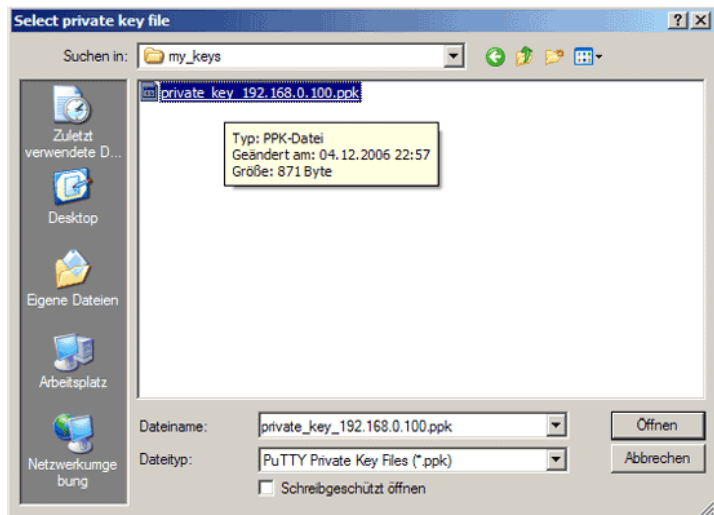
Agora abra o PuTTY novamente e carregue o perfil do seu servidor SSH (192.168.0.100):



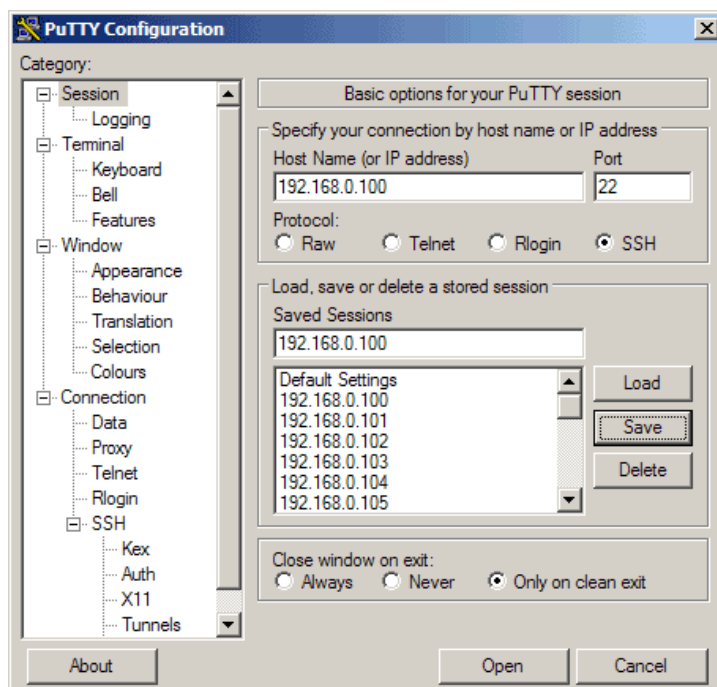
Então vá para *SSH -> Auth* e clique em *Procurar*:



Procure no seu sistema de arquivos e selecione a sua chave privada criada anteriormente:



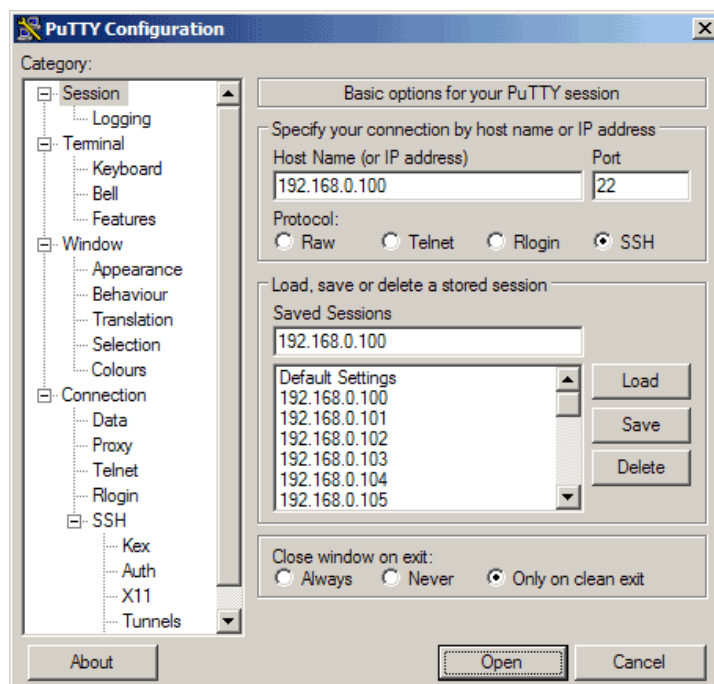
Então vá para a *sessão* novamente e clique em *Salvar*:



Agora vamos ter anexado a chave privada para o nosso perfil *192.168.0.100* PuTTY.

Nossa login baseado em Key First

Agora tudo está pronto para o nosso primeiro login baseada em chave para o nosso servidor SSH. Clique em *Abrir*:



Como você pode ver, a chave pública é agora usado para autenticação, e é solicitada a frase-senha (aquela que você especificou anteriormente):

Até agora, você pode fazer login com o seu par de chaves pública/privada e ainda com logins nome de usuário / senha, por isso, se alguém não anexar uma chave privada para a sua sessão PuTTY, ele será solicitado um nome de usuário e senha. Assim, para alcançar uma maior segurança, é preciso desativar os logins nome de usuário/senha (você deve fazer isso apenas quando você sabe que seus logins chave baseados estão funcionando, porque se eles não estão e você desativar logins nome de usuário/senha, então você tem um problema...).

Para desativar os logins nome de usuário/senha, é preciso modificar o arquivo de configuração do sshd. Em sistemas CentOS/Ubuntu, é em **/etc/ssh/sshd_config**. Você deve definir **protocolo 2** (1 é inseguro e não deve ser usado!), **PasswordAuthentication no**. Logo após reinicie o serviço de SSH:

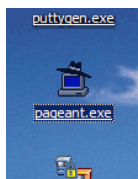
```
# vi /etc/ssh/sshd_config
...
Protocolo 2
PasswordAuthentication no
UsePAM no
...
# service sshd restart
```

Agora, se você abrir uma sessão PuTTY sem a sua chave privada em anexo, você não deve ser capaz de efetuar login mais.

Pageant lembrar sua senha de chave

Sempre que você usar o seu login baseado em chave agora, você still tem que especificar a sua senha de chave. Isso pode ser irritante se você se conectar ao servidor SSH várias vezes por dia. Felizmente, você pode dizer a senha para Pageant, que irá fornecer a senha sempre que você efetuar login no seu servidor SSH.

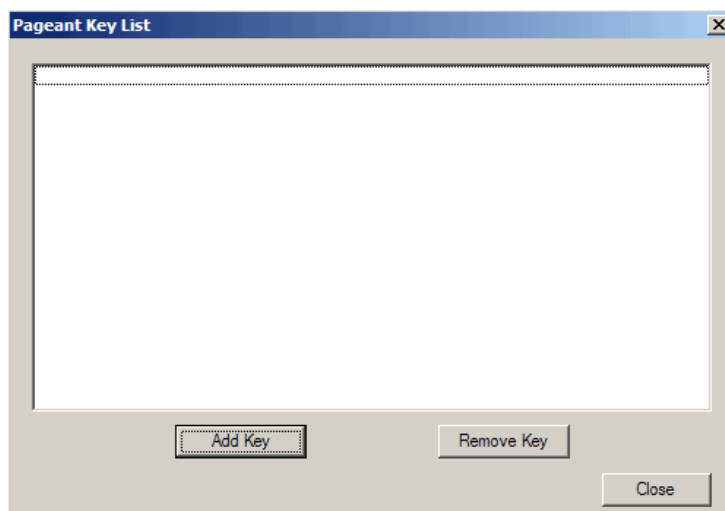
Você pode começar Pageant clicando duas vezes em seu arquivo executável:



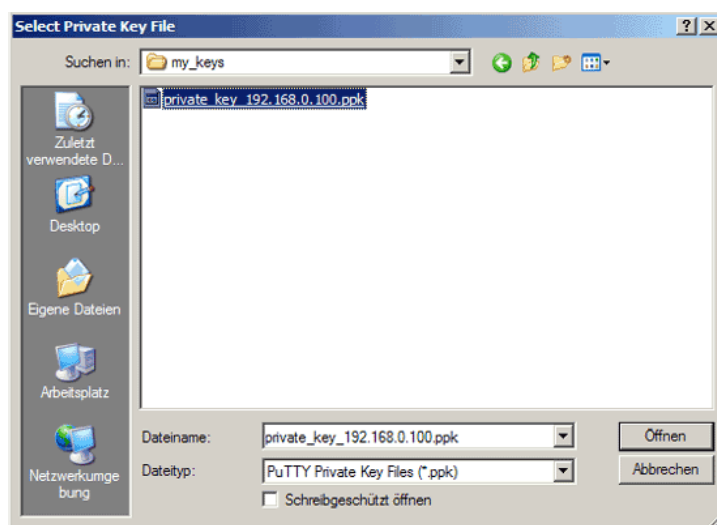
Em seguida, você deve ver correndo Pageant na barra de tarefas:



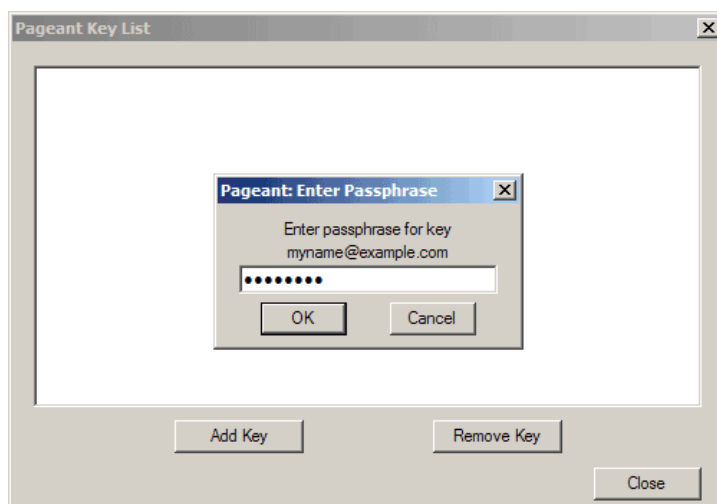
Agora dê um duplo clique no ícone Pageant na barra de tarefas. A seguinte janela aparece. Clique em *Adicionar chave*:



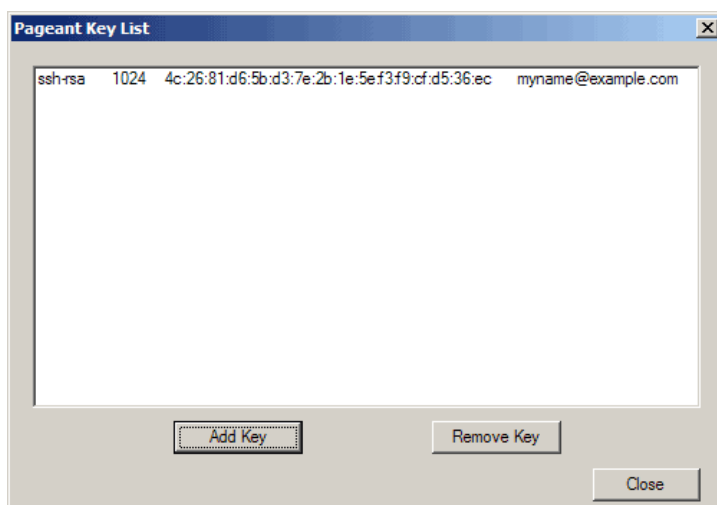
Procure no seu sistema de arquivos e selecione a sua chave privada:



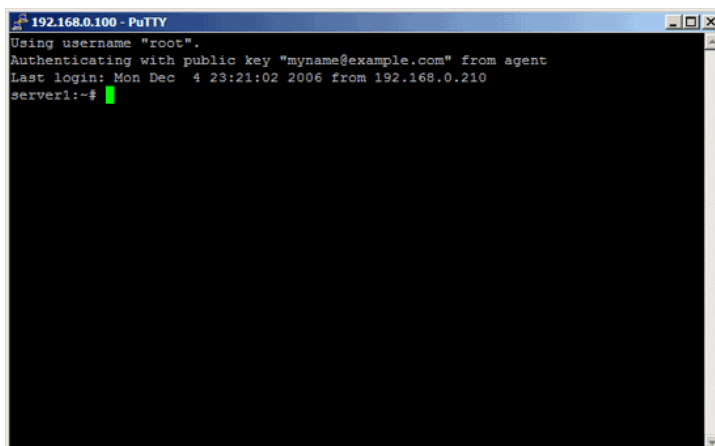
Em seguida, digite a senha para a chave privada:



A chave agora está listada na lista de chaves do Pageant. Clique em *Fechar*:



Enquanto Pageant está em execução na barra de tarefas, você pode efetuar login em seu servidor SSH sem fornecer a senha - isso é feito por Pageant:



```
192.168.0.100 - PuTTY
Using username "root".
Authenticating with public key "myname@example.com" from agent
Last login: Mon Dec  4 23:21:02 2006 from 192.168.0.210
server1:~#
```