SSHD

Marcar como feito

O ssh é um serviço muito utilizado para acesso remoto de sistemas e equipamentos de redes e por isso precisamos ter certos cuidados com ele. Em equipamentos de redes, provavelmente você não verá o que vou descrever mas você pode utilizar essas dicas em servidores GNU/Linux rodando o serviço **sshd** e aumentar a segurança do serviço contra um ataque conhecido como **brute force**. O ideal é sempre limitarmos os acessos mas se for inevitável que o serviço fique aberto na Internet, pelo menos mantenha este sempre atualizado e procure seguir as dicas abaixo:

O que nós vamos fazer é dizer ao nosso serviço ssh para aceitar somente conexões com **chaves ssh** e por favor quando for gerar sua chave ssh, crie esta com uma senha que só você conheça. Antes de habilitar as configurações no servidor, teste se está funcionando o acesso remoto usando as chaves ssh, porque após mudar a configuração e reiniciar o serviço sshd, se a chave não funcionar, você perderá o acesso remoto ao sistema.

Atualmente o tipo mais forte de chave é o **ed25519**, contudo sistemas antigos não aceitarão a conexão pela falta do suporte mas se os sistemas que for administrar forem servidores GNU/Linux mais recentes, provavelmente funcionará.

Gerando um par de chaves fortes

No shell de sua distribuição GNU/Linux execute algo como no exemplo abaixo mas trocando o **<user>** pelo seu login ou nome que queira dar. O comando irá gerar um par de chaves, a chave privada e a pública. A pública é a que você usará nos servidores que for administrar, em **~/.ssh/authorized\_keys**.

# ssh-keygen -t ed25519 -q -f ~/.ssh/<user>\_ed25519

Configurando o servidor sshd

Em **/etc/ssh/sshd\_config** fazer as alterações nos seguintes parâmetros:

PermitRootLogin prohibit-password

PubkeyAuthentication yes

PasswordAuthentication no

Após a configuração você precisará reiniciar o serviço sshd para que passe a valer nossa alteração.

Criando uma lista de acesso ssh

Se você utiliza um Desktop GNU/Linux com bash, pode ser que queira criar uma lista com seus servidores remotos e utilizar o comando ssh seguido de **<TAB>** para listar todos e escolher qual acessar. Para isso é bem simples basta criar o arquivo **~/.ssh/config** com um conteúdo conforme o exemplo abaixo:

Host <nome\_servidor>

Hostname <IP>

Port <porta>

User <login>

IdentityFile ~/.ssh/<user>\_ed25519

No exemplo acima trocamos o **<nome\_servidor>** pelo nome que queremos dar ao servidor remoto, **<IP>** do servidor remoto, **<porta>** pela porta ssh utilizada naquele servidor, **<login>** pelo username de conexão e por último o apontamento da chave ssh privada que será utilizada naquela conexão.

Identificando quem acessou o servidor pela chave ssh

Para identificar no **/var/log/auth.log** pelo **fingerprint hash** basta listar o **authorized\_keys** com o comando exemplo abaixo:

# ssh-keygen -l -f ~/.ssh/authorized\_keys

O comando acima irá mostrar um resultado parecido, conforme exemplo abaixo. Esse seria o **fingerprint** da chave do zezinho@gmail.com

256 SHA256:2WaBto4tzZWf/tt5rNHzFqB3cD7e3T8LepMRZBNZDpM zezinho@gmail.com (ED25519)

De posse dos **fingerprints** só olhar em **/var/log/auth.log** pelos **fingerprints** e ver quem fez o acesso ao servidor. Pode ser que no seu sistema não exista o **/var/log/auth.log** ou tenha um outro nome.

Para liberar o acesso no servidor ssh

Adicione a sua chave pública em **~/.ssh/authorized\_keys** conforme exemplo abaixo:

ssh-ed25519 AAAAC3NzaC1lZDI1TNE5AAAAIMUA6bpdkJxu6Xk+ayHmimGcC5s3G49gkF+t8jX6Sgu2 zezinho@gmail.com