***SSH***

**O que é SSH?**

SSH é um protocolo de rede que se encontra na Camada 3 do Modeo OSI, usado para criptografar os dados permitindo uma comunicação segura entre dois ou mais computadores, geralmente usado para acessar e gerenciar servidores de forma remota.

O usuário pode se autenficar no servidor de duas maneiras. A primeira seria com senha, onde ele digitaria seu nome de usuário e a senha, sendo a forma menos segura, pois as senhas podem ser adivinhadas. E a outra maneira mais segura seria gerando uma **Chave SSH**. Aqui é gerado duas chaves, sendo uma pública e uma privada, permitindo que o usuário use a chave pública para se autenficar no servidor.

A chave pública é basicamente a chave que será cadastrada no lado do servidor, e a chave privada é chave que fica no computador do cliente provando que ele realmente é o dono da chave pública gerada naquele servidor.

Configurando as chaves corretamente é possível acessar o servidor sem precisar ficar digtando a senha sempre que entrar, permitindo o acesso mais seguro e confiável na hora de acessar o servidor.

****Gerando uma chave SSH:****

**Para gerar uma chave SSH digitaremos o seguinte comando:**

ssh-keygen -t rsa -b 4096 -f ~/.ssh/nome\_da\_chave.id\_rsa

**Esse comando gerará dois arquivos, sendo um com a extenção **id\_rsa.pub** que é a chave pública e um arquivo **id\_rsa** que seria a chave privada.**

**RSAé basicamente o tipo da chave, sendo a comumente usada, e **4096** é o tamanho da chave em bits, considerado um tamanho seguro.**

**Agora o próximo passo é copiar a chave pública para o servidor. E para isso utilizaremos o seguinte comando:**

ssh-copy-id nome\_do\_usuário@ip\_ou\_domínio\_do\_servidor

**Esse comando gerará a chave pública dentro do arquivo authorized\_keys** dentro da pasta SSH do servidor, permitindo assim o acesso direto sem usar senha nas próximas conexões.

Utilizamos agora o seguinte comando para se conectar:

ssh nome\_do\_usuario@ip\_ou\_dns\_do\_servidor

****O que é SSH Agent?****

Depois de tudo configurado, ao se conectar no servidor será pedido uma senha, essa senha é a senha da chave privada registrada dentro do computador do cliente.

O **SSH Agent** basicamente guarda essa senha na memória do computador em cache, permitindo que não seja necessário digitar a senha novamente.

Para configurar o Agent SSH seguiremos o seguintes passos:

**1. Íniciar o SSH Agent:**

eval $(ssh-agent -s)

**2. Adicionar a chave privada ao Agent:**

ssh-add ~/.ssh/nome\_da\_chave

**3. Listamos as chaves registradas para verificação:**

ssh-add -l

**4. Se quiser remover a chave do Agent use:**

ssh-add -d ~/.ssh/nome\_da\_chave

**5. Se quiser finalizar a sessão do Agent:**

ssh-agent -k

****Segurança Adicional no SSH:****

É possível adicionar ainda a **Autenficação de Dois Fatores (2FA)**. Assim além de ter a chave privada e ser necessário digitar a senha ao se conectar a primeira vez na sessão com o servidor, será pedido uma outra autentificação como uma chave gerada em seu smartphone.

****Configurações Avançadas:****

Dentro da pasta **.ssh** existe um arquivo de configuração chamado **config**. Nesse arquivo podemos configurar algumas opções para controlar o acesso SSH.

**Desabilitar Login com Senha:**

PasswordAuthentication no

**Permitir ou Bloquear usuários específicos:**

AllowUsers usuario1 usuario2

DenyUsers usuario3 usuario4

**Desabilitar o Login como Root:**

PermitRootLogin no

**Limitar o número de tentativas de login:**

MaxAuthTries numero\_de\_tentativas

**Forçar o uso da SSH com a versão 2:**

Protocol 2

Após editarmos o arquivo de configuração devemos reniviar o serviço SSH, utilizando o seguinte comando:

sudo systemctl restart ssh