Laboratório de Sistemas Operacionais II:

Nome: Sham Vinicius Fiorin

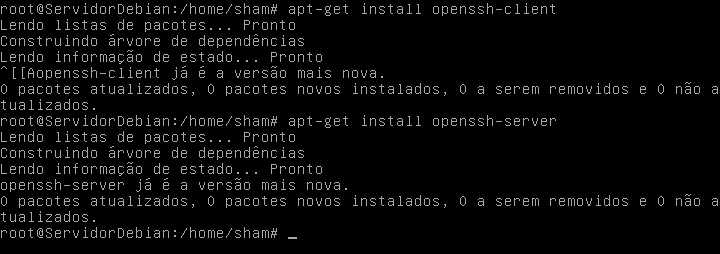
* Instalar e configurar o SSH (Servidor e Cliente).

Imagem 1: Instalando SSH servidor e cliente.

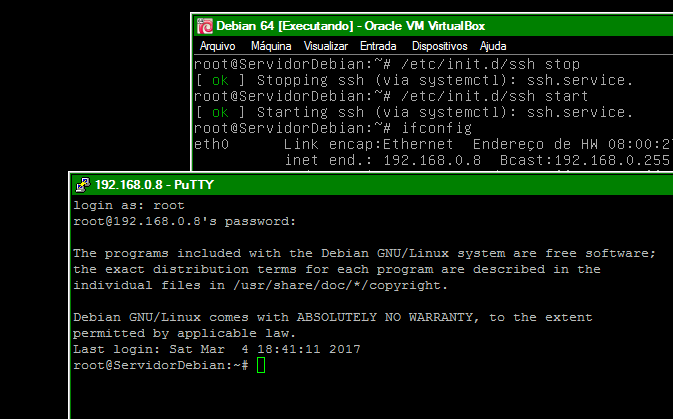
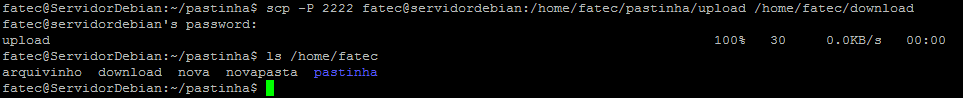
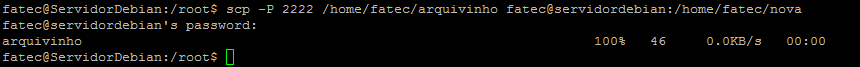
* Fazer a conexão remota com o usuário (root).

Imagem 2: Fazendo login com usuário root no Cliente Windows via Putty.

* Explorar o comando SCP:
  + Copie diretórios e arquivos para o servidor.





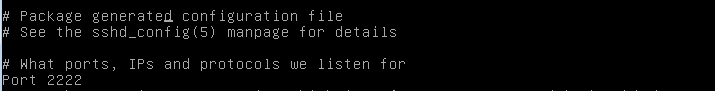
* Explicar os arquivos e seus conteúdos de configurações:
  + sshd\_config: local aonde ficam as configuração da emulação do servidor SSH
  + ssh\_config: local aonde se encontra os arquivos de configuração do cliente SSH.
* Alterar sua porta padrão (de 22 para 2222); 

Imagem X: Configurando Porta de comunicação do SSH.

* É possível o acesso remoto sem a utilização de senhas? Se sim demonstre?

Sim, através de salvar as chaves da criptografia RSA.

* Criar túnel criptografados (Tunelamento).
* Limitar o acesso ao SSH.
* Discorra sobre SSH X TELNET?

Quando se usa o protocolo TELNET para acessar remotamente servidores, a troca de informações não se tem proteção, consequentemente, quando interceptado não tem proteção dos dados enviados e recebidos.

Servidores SSH podem criptografar os dados fazendo que os dados sejam bem mais seguros ao realizar essa troca de informações.

* Conecte ao servidor SSH (Debian ou Ubuntu) com a Máquina hospedeira (Windows) via Putty.

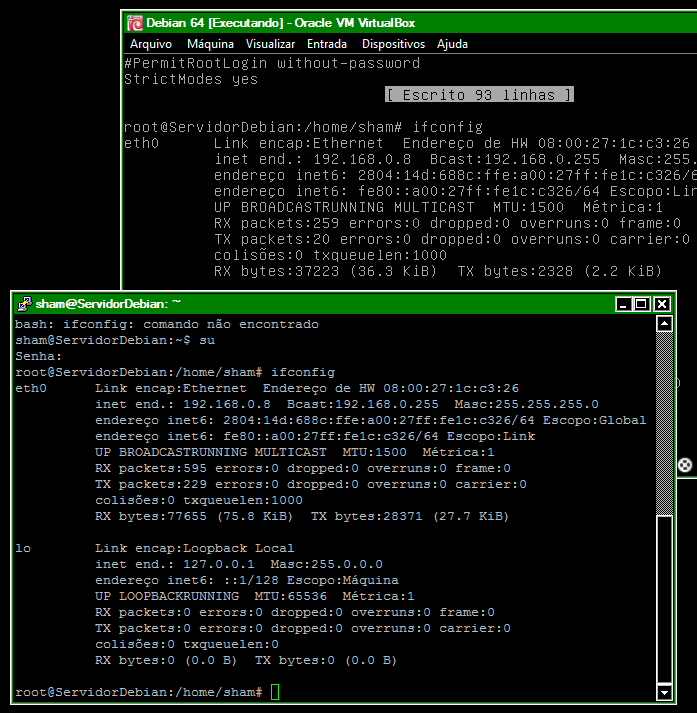


Imagem 1: Servidor SSH Debian conectado com o Cliente Windows via Putty.

* Criar um usuário (fatec).

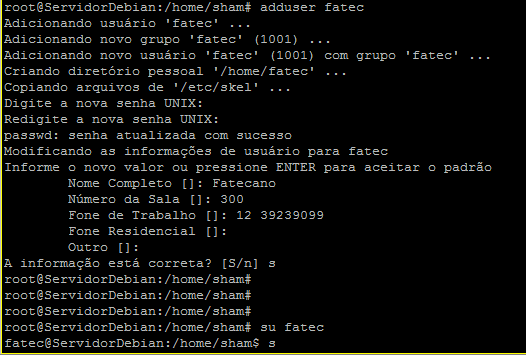


Imagem 2: Criando usuário fatec com o cliente Windows via Putty e conectando no mesmo.

* Bloquear o usuário root.
* Permitir o acesso ao servidor SSH somente com o usuário fatec.

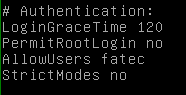


Imagem 3: Configurando para bloquear root e configurando quais usuários podem acessar o servidor.

* Faça download e upload do servidor SHH