Servidor SSH

Prof. Jean Carlos

Servidor SSH (Secure SHell)

Objetivo da Aula

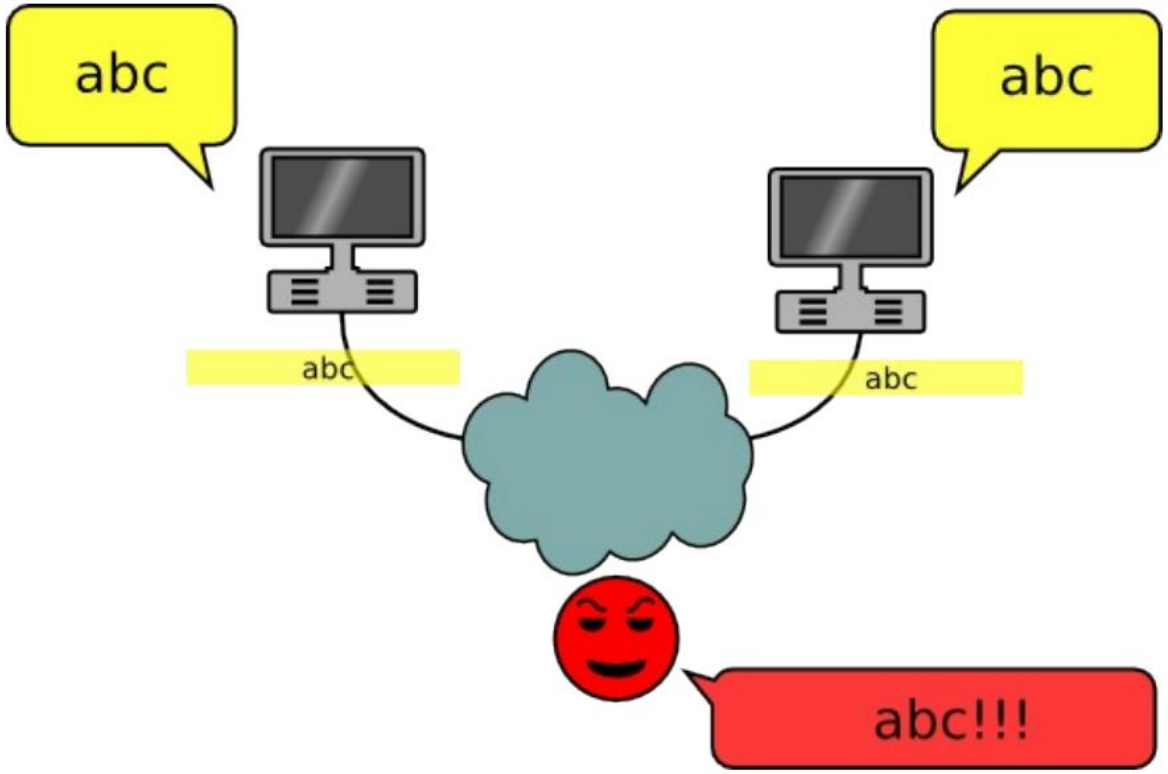
- Realizar acesso e cópias através do SSH;
- Ajustar configurações do servidor SSH;
- Configurar acesso com uso de chaves entre os servidores;
- Laboratório SSH

SSH

- O Serviço SSH é usado para realizar Acesso Remoto de forma Segura. Ele oferece as seguintes proteções:
  - Após a primeira conexão ele armazena a identidade do Servidor (know_hosts) para garantir que você sempre irá acessar o servidor correto. Caso a identidade seja alterada, ele irá te alertar;
  - O cliente transmite as informações de autenticação usando criptografia forte de 128 bits;
  - Todos os dados recebidos e enviados usa uma criptografia de 128bits tornando praticamente impossível decifrar os dados;
  - Como SSH criptografa tudo, ele pode servir de tunelamento para outros protocolos inseguros (Tunelamento).

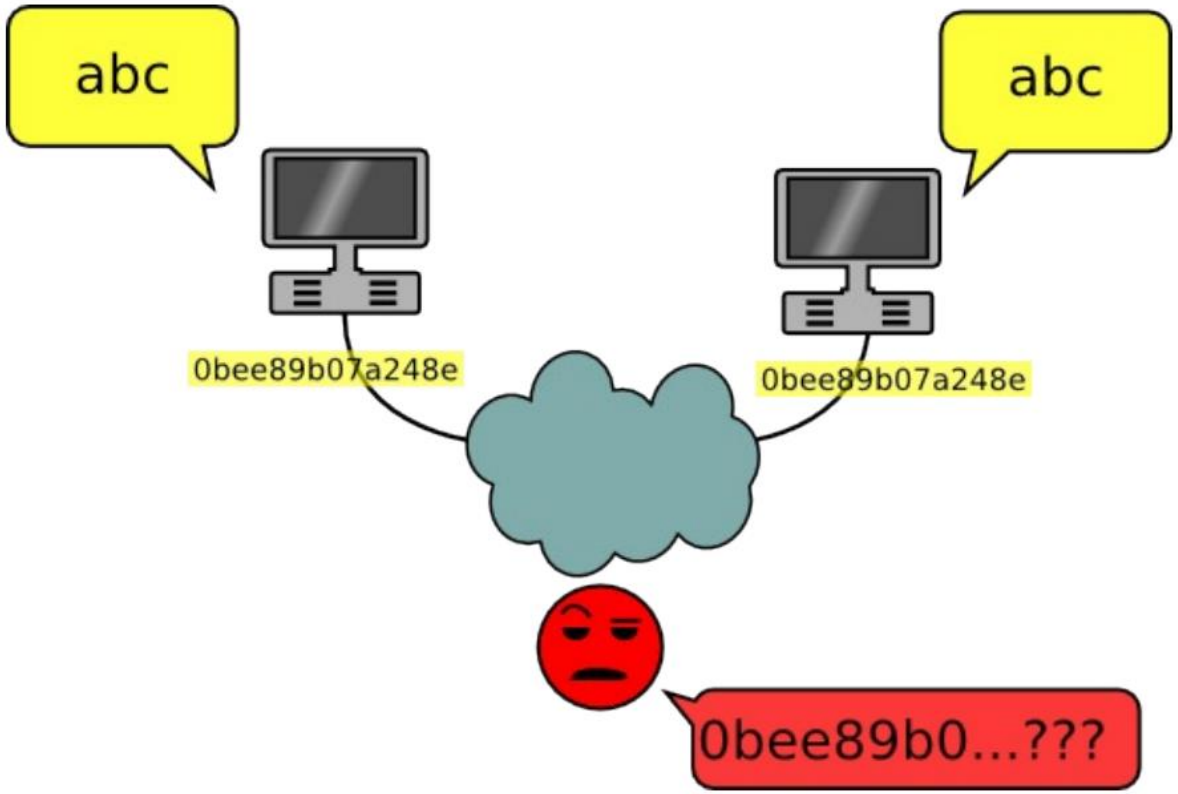
SSH

- Comunicação insegura (sem criptografia):



SSH

- Comunicação segura (com criptografia):



Porque SSH?

- Existem uma variedade de ferramentas que podem ser usadas para romper ou interceptar dados de uma comunicação com o objetivo de conseguir acesso a um sistema, como por exemplo, usar um sniffers para capturar dados que estão trafegando na rede.

Porque SSH?

- Com o SSH essa ameaça é quase nula, isso porque o cliente e o servidor SSH usam assinaturas digitais para verificar a sua identidade. Além disso, toda a comunicação entre eles é criptografada. As tentativas para falsificar a identidade de cada lado de uma comunicação não funciona, já que cada pacote é criptografado utilizando uma chave conhecida apenas pelo cliente e o servidor.

Conexão SSH


Solicitação de Conexão: Porta 22/tcp
Confirmação de Identidade
(know_hosts)
Solicitação de Autenticação
Fornecimento de Senha ou Chave
Liberação do Shell
bash
Troca de Dados (Criptografada)
DESKTOP LINUX
WebServerCloud

SSH e Cloud

- É praticamente impossível falar de Cloud sem SSH.
- Com o avanço do Mercado de Cloud o SSH passou a ser uma ferramenta vital, quando o assunto é administrar servidores remotos. É exatamente por isso que é extremamente importante configurar esse Serviço de forma correta, visando sempre a segurança do acesso ao Sistema.

Acesso Remoto

- Para usar o SSH é necessário ter o pacote instalado, tanto o pacote do Servidor, quanto o pacote do Cliente.
- A porta padrão do SSH é a 22, se o Serviço está ativo essa porta é liberada para aceitar conexões SSH no Servidor.

- Iremos ativar e configurar o Serviço SSH no Servidor (Debian ou Ubuntu) para permitir conexão SSH através do Cliente (Debian ou Ubuntu).

Acesso Remoto

- Servidor → Máquina que recebe um acesso Remoto
- Cliente → Máquina que realiza um acesso Remoto

Todos os Servidores podem ser Cliente e Servidor!

Laboratório SSH

- Instalar e configurar o SSH (Servidor e Cliente).
- Fazer a conexão remota com o usuário (root).
- Explorar o comando SCP:
  - Copie diretórios e arquivos para o servidor.
- Explicar os arquivos e seus conteúdos de configurações:
  - sshd_config;
  - ssh_config.
- Alterar sua porta padrão (de 22 para 2222);
- É possível o acesso remoto sem a utilização de senhas? Se sim demonstre?

Laboratório SSH

- Discorra sobre SSH X TELNET?.
- Conecte ao servidor SSH (Debian ou Ubuntu) com a Máquina hospedeira (Windows) via Putty.
- Criar um usuário (etec).
- Bloquear o usuário root.
- Permitir o acesso ao servidor SSH somente com o usuário etec.
- Faça download e upload do servidor SSH.

- Observação: Todos os passos acima deverão ser registrados e salvo em PDF. (Pode ser feito em dupla!!!)
  - Exemplo: DS_SSH_nome.sobrenome.PDF

Pergunta LPI

Qual arquivo de configuração você precisará editar para alterar as opções padrões do cliente SSH?

A. /etc/ssh/sshd_config

B. /etc/ssh/ssh_client

C. /etc/ssh/client

D. /etc/ssh/ssh

E. /etc/ssh/ssh_config

Pergunta LPI

Qual parâmetro no arquivo configuração do SSH define os usuários que podem se logar no servidor?

A. AllowUsers

B. DenyUsers

C. AllowUser

D. UsersAllow

E. UsersDeny