Atividade Prática 18: Servidor FTP

Objetivo: Tutorial Prático Configurar o seu próprio servidor FTP no Ubuntu

Introdução

Antes de iniciar a configuração do seu servidor FTP, você deve escolher o software adequado. O sistemas operacional Ubuntu, também na versão 24, já inclui no gerenciador de pacotes o vsftpd, solução pronta para uso.

Objetivo: Configurar o VSFTPD para suportar conexões criptografadas (FTPS), instalar quatro arquivos para transferência, e aplicar as configurações de segurança de forma profissional.

Materiais por Dupla

- 2 Computadores com **Ubuntu 24.04.3 LTS** (Servidor e Cliente).
- Cliente **FileZilla** instalado na máquina Cliente.
- Endereço IP fixo configurado na máquina Servidora (Ex: 192.168.1.100).

Fase 1: Preparação, Instalação e Criação de Certificado SSL

O **Aluno A** (Servidor) deve configurar a segurança para a criptografia.

1. **Instalação VSFTPD:**

Bash

sudo apt update

sudo apt install vsftpd

2. **Criação do Certificado SSL/TLS:** Crie o certificado autoassinado (a chave privada RSA de 2048-bit e o certificado .pem válido por um ano).

Bash

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

Quando solicitado, insira os detalhes pessoais (nome da organização, país, etc.).

3. **Criação de Arquivos para Transferência:** Crie quatro arquivos para o teste de transferência (usaremos a pasta Home do usuário logado no Servidor).

Bash

cd ~

touch relatorio_seguranca.pdf

touch backup_config.zip

touch imagem_logo.png

touch lista_clientes.txt

Fase 2: Configuração do FTPS (Segurança Criptografada)

1. **Backup e Edição:** Faça o backup do arquivo e abra para edição.

Bash

sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original

sudo nano /etc/vsftpd.conf

2. **Ajustes de Segurança e FTPS:**
    - ***Desativar Anônimo:*** *anonymous_enable=NO*
    - ***Ativar Local:*** *local_enable=YES*
    - ***Habilitar Escrita:*** *write_enable=YES*
    - ***Restrição (Chroot):*** *chroot_local_user=YES*

Adicione as linhas para habilitar o SSL/TLS e apontar para o certificado criado:

- *ssl_enable=YES*
- *rsa_cert_file=/etc/ssl/private/vsftpd.pem*
- *rsa_private_key_file=/etc/ssl/private/vsftpd.pem*
- *allow_anon_ssl=NO*
- *force_local_data_ssl=YES (Força a criptografia para a transferência de dados)*
- *force_local_logins_ssl=YES (Força a criptografia para o login)*

3. **Reiniciar:** Salve, saia e reinicie o serviço para aplicar o FTPS.

Bash

sudo systemctl restart vsftpd

Fase 3: Teste de Acesso e Validação (Aluno B)

O **Aluno B** valida o FTPS usando o FileZilla.

1. **Instrução no FileZilla:**

    - *Abra o **FileZilla** (Cliente).*
    - *Clique no **Gerenciador de Sites** (Site Manager).*

    - **Protocolo:** Mude de "FTP" para **"FTP ESXPLÍCITO sobre TLS/SSL"**.
    - **Host:** Endereço IP do Servidor.
    - **Usuário/Senha:** Credenciais do Servidor.

2. **Teste de Transferência:**

    - **Objetivo:** O Aluno B deve realizar o download dos **quatro arquivos** criados na Fase 1 (relatorio_seguranca.pdf, backup_config.zip, etc.).
    - **Teste de Segurança:** O FileZilla deve exibir um aviso sobre o certificado autoassinado (que é a validação de que a criptografia está funcionando, mesmo que o certificado não seja de uma autoridade reconhecida).

Relatório e Conclusão

Documente a saída do comando openssl e a **comprovação de segurança**. Explique por que o FTPS é superior ao FTP tradicional e qual porta (21 ou 20) recebe a chave de criptografia.