**Relatório – Configuração de um Servidor Web Seguro com HTTPS e SSL/TLS**

**1. Objetivo**

Configurar um servidor web seguro utilizando HTTPS e SSL/TLS para proteger a comunicação entre clientes e o servidor, garantindo criptografia, integridade e segurança.

**2. Pré-requisitos**

1. **Sistema Operacional**: Distribuição Linux (ex: Ubuntu Server 20.04).
2. **Servidor Web**: Apache ou Nginx.
3. **Certificado SSL/TLS**: Pode ser autoassinado ou emitido por uma CA confiável como o Let's Encrypt.
4. **Conexão SSH ao servidor** (para configuração remota).
5. **Acesso root ou sudo**.

**3. Etapas de Configuração**

**3.1. Instalação do Servidor Web**

No exemplo, usaremos o **Apache**:

Uma imagem contendo Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

**3.2. Instalação do Certbot para Let's Encrypt**

Instale o Certbot, que automatiza a obtenção de certificados SSL/TLS:

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

**3.3. Obtenção do Certificado SSL/TLS**

Use o Certbot para solicitar o certificado:

Uma imagem contendo Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

Siga as instruções interativas do Certbot e forneça o domínio da empresa.

**3.4. Configuração de Redirecionamento HTTP para HTTPS**

Certifique-se de que o Certbot configure o redirecionamento automático. Caso contrário, edite o arquivo de configuração do Apache:

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Adicione as seguintes linhas:

Texto

O conteúdo gerado por IA pode estar incorreto.

Substitua example.com pelo domínio da empresa.

**3.5. Boas Práticas de Segurança**

* **Desativar TLS 1.0 e 1.1**: Edite o arquivo de configuração SSL:

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Altere para:

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

* **Adicionar Cabeçalhos de Segurança HTTP**: No mesmo arquivo ou na configuração do VirtualHost, adicione:

Texto

O conteúdo gerado por IA pode estar incorreto.

**3.6. Teste da Configuração**

1. **Usar OpenSSL**: Execute o comando para verificar o certificado:

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

1. **SSL Labs**: Acesse o site SSL Labs e insira o domínio para obter um relatório detalhado.
2. **Navegadores Web**: Acesse o site no navegador e verifique o cadeado seguro.

**4. Capturas de Tela**

Inclua imagens de:

1. **Execução dos comandos no terminal** (ex: instalação e configuração).
2. **Teste SSL Labs** com o relatório de avaliação.
3. **Visualização do site em HTTPS no navegador**.

**5. Código de Configuração**

Exemplo de arquivo /etc/apache2/sites-available/000-default-le-ssl.conf:

Texto

O conteúdo gerado por IA pode estar incorreto.

**6. Conclusão**

Com esta configuração, o servidor web está seguro e em conformidade com as melhores práticas de segurança. O HTTPS com SSL/TLS protege as comunicações entre clientes e o servidor, garantindo a integridade e confidencialidade dos dados.