Universidade de Brasília - UnB

Faculdade do Gama – FGA

Fundamentos de Redes de Computadores: Prof. Fernando W. Cruz

Laboratório sobre Certificados Digitais e Autoridades Certificadoras

Gabriel Avelino Freire – 18/0100831

Ítalo Fernandes Sales de Serra – 18/0102613

Samuel Nogueira Bacelar – 18/0130722

Antonio Rangel Chaves– 18/0098021

Enzo Gabriel Guedes Queiroz Saraiva – 16/0119006

Introdução

Este relatório do laboratório tem como objetivo proporcionar a oportunidade de aprimorar os conhecimentos sobre Certificados Digitais por meio de atividades práticas. Os Certificados Digitais desempenham um papel crucial na segurança da comunicação e na autenticação de identidades online. Neste laboratório, tivemos a chance de explorar e experimentar as diferentes aplicações e tecnologias envolvidas nesse campo, adquirindo habilidades práticas que são essenciais para profissionais da área de segurança da informação. Dessa forma, conseguimos compreender os conceitos fundamentais por trás dos Certificados Digitais, aprender a gerar, instalar e gerenciar certificados, além de explorar tópicos avançados, como criptografia e assinatura digital. Essa abordagem prática permitiu aprofundar nossos conhecimentos teóricos e desenvolver habilidades.

Metodologia

A equipe se reuniu para realizar as pesquisas descritas no arquivo do laboratório, dividindo as tarefas entre os membros para que cada um pesquisasse um tópico e avançasse passo a passo. Além disso, um membro da equipe ficou responsável por executar os comandos para gerar os certificados e configurar o servidor Apache2. As soluções encontradas foram compartilhadas com os outros membros e documentadas em um arquivo Word, facilitando o acesso a todos.

Descrição da solução

As pesquisas realizadas pelos membros da equipe levaram aos seguintes passos para a geração de um certificado digital e uma autoridade certificadora:

Primeiro passo – Criar um endereço associado a um IP

1 – Abrir arquivo “hosts” para associar um endereço a um IP;

```
sudo nano /etc/hosts
```

2 – Adicionar no arquivo o IP e o endereço;

```
0.0.0.0        www.lab-frc.com.br
```

Segundo passo – Gerar chave para o certificado

Essa etapa serve para gerar as chaves dos certificados que serão usados pelo servidor apache2. Esses comandos geram as chaves e seus respectivos certificados.

```
openssl genrsa -des3 -out ca.key 4096

openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
```

openssl genrsa -des3 -out server.key 4096

openssl req -new -key server.key -out server.csr

openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 10102014 -out server.crt

Terceiro passo – Configurar o apache

1 - Instalar apache e pacotes;

$ apt-get install apache2 openssl

2 - Ativação;

2.1 - Ativar módulo do Apache chamado: Mod_ssl;

$ a2enmod ssl

2.2 - Ativar módulo do Apache chamado: Mod_rewrite;

$ a2enmod rewrite

3 - Editar o arquivo de configuração do Apache;

vim /etc/apache2/apache2.conf

4 - Adicionar estas linhas no final do arquivo;

<Directory /var/www/html>

AllowOverride All

</Directory>

5 - Criar uma chave privada e o certificado do website usando o comando OpeSSL;

mkdir /etc/apache2/certificate

cd /etc/apache2/certificate

openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes –out apache-certificate.crt -keyout apache.key

Enter the requested information.

6 - Entrar com as informações solicitadas;

Na opção COMMON_NAME é necessário entrar com o endereço IP ou nome do host

7 - Editar o arquivo de configuração do Apache para o padrão;

vim /etc/apache2/sites-enabled/000-default.conf

antes da configuração:

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
   DocumentRoot /var/www/html
  ErrorLog ${APACHE_LOG_DIR}/error.log
   CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

depois da configuração:

```
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile /etc/apache2/certificate/apache-certificate.crt
        SSLCertificateKeyFile /etc/apache2/certificate/apache.key
</VirtualHost>
```

para redirecionar de http para https:

```
<VirtualHost *:80>
        RewriteEngine On
        RewriteCond %{HTTPS} !=on
        RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R=301,L]
</virtualhost>
```

<VirtualHost *:443>

ServerAdmin webmaster@localhost

DocumentRoot /var/www/html

ErrorLog ${APACHE_LOG_DIR}/error.log

CustomLog ${APACHE_LOG_DIR}/access.log combined

SSLEngine on

SSLCertificateFile /etc/apache2/certificate/apache-certificate.crt // alterar para o certificado criado

SSLCertificateKeyFile /etc/apache2/certificate/apache.key // alterar para a chave criada

</VirtualHost>

8 - Reiniciar o serviço apache;

sudo service apache2 restart

9 - Abrir o navegador e acessar a versão https do website;

10 – Gerar certificado para o apache2;

mkdir /etc/apache2/certificate

cd /etc/apache2/certificate

openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out apache-certificate.crt -keyout apache.key

Quarto passo – Protocolo SSL/TLS

Após a aula, os membros da equipe pesquisaram sobre os conceitos desse protocolo, e as seguintes conclusões foram encontradas. O Protocolo SSL (Secure Sockets Layer) e seu sucessor TLS (Transport Layer Security) são protocolos criptográficos que fornecem segurança na comunicação pela Internet. Eles são projetados para proteger a integridade, confidencialidade e autenticidade dos dados transmitidos entre um cliente (como um navegador da web) e um servidor. O SSL/TLS estabelece uma conexão segura entre um cliente (navegador) e um servidor (site), negociando parâmetros criptográficos, autenticação e troca de chaves de criptografia. Isso garante a confidencialidade, autenticidade e integridade dos dados transmitidos. Os benefícios do SSL/TLS incluem criptografia dos dados, autenticação do servidor, verificação da integridade dos dados e conformidade com padrões de segurança. Sendo assim, o TLS é uma evolução do SSL, garantindo ainda mais segurança e eficácia.

Conclusão

A abordagem prática permitiu aprofundar nossos conhecimentos teóricos e desenvolver uma compreensão sólida dos Certificados Digitais. Essas habilidades e conhecimentos adquiridos são extremamente valiosos em um mundo digital onde a segurança da informação é uma preocupação constante. Ao concluir esta atividade, estamos melhor preparados para enfrentar os desafios e aproveitar as oportunidades que surgem no campo dos Certificados Digitais. Acreditamos ser capazes de aplicar nossos conhecimentos e habilidades em situações reais, contribuindo para a segurança e autenticidade da comunicação online.

Opiniões Pessoais

Gabriel Avelino Freire:

- Sobre o projeto: Achei muito interessante essa aula prática, visto que não tinha conhecimento nenhum sobre certificados digitais, utilizei uma vez no trabalho, mas não entendia como funcionava de verdade. Além disso, foi muito interessante ver o funcionamento do apache e criar um servidor a partir dele, sempre ouvi falar muito sobre, mas nunca tinha mexido com ele.
- Participação: Fiz a parte de criar um certificado e autenticar ele com uma autoridade, criando um servidor apache que usa esses certificados. Além disso, contribui para as pesquisas de como criar o certificado e a autoridade bem como também, a pesquisa do SSL/TSL.
- Autoavaliação: Muito boa. Participei em todas as partes das atividades do laboratório.

Ítalo Fernandes Sales de Serra:

- Sobre o projeto: O projeto foi bastante interessante, pois pude aprender sobre Certificados Digitais e sua importância na segurança da comunicação online. Foi uma oportunidade de aplicar os conhecimentos teóricos em uma atividade prática, o que ajudou a consolidar o aprendizado.
- Participação: Contribuí na pesquisa sobre os conceitos fundamentais dos Certificados Digitais e na elaboração dos passos para a geração de um certificado e uma autoridade certificadora. Também participei das discussões em grupo e compartilhei minhas descobertas com os demais membros da equipe.
- Autoavaliação: Considero minha participação satisfatória. Colaborei ativamente no desenvolvimento do trabalho, cumprindo minhas responsabilidades e contribuindo para a conclusão bem-sucedida das tarefas propostas.

Samuel Nogueira Bacelar:

- Sobre o projeto: O projeto foi importante para o entendimento de como funcionam os certificados digitais e como criar um servidor com o apache. Isso é algo importante e

interessante pois, mostra alguns fluxos de trabalho que não vemos no nosso cotidiano, tanto no dia a dia quanto no ambiente profissional. No ambiente profissional já estamos acostumados com as facilidades que terceiros nos disponibilizaram e por isso não ficamos a par do que acontece por debaixo dos panos.

- Participação: Minha participação consistiu também na criação de um servidor apache que utiliza os certificados, na criação do DNS e também nas pesquisas do protocolos SSL/TLS
- Autoavaliação:

Antonio Rangel:

- Sobre o projeto: A aula prática foi importante para ver como podem ser geradas as chaves e certificados e como aplicá-las em um servidor web. Para nós alunos, aulas práticas como essa ajudam a consolidar a teoria que foi passada em aulas expositivas.
- Participação: Ajudei o grupo a configurar o servidor apache 2, fornecendo os passos para que o servidor pudesse receber requisições https.
- Autoavaliação: Boa, consegui ajudar o grupo nas tarefas e todos conseguimos completar o que foi solicitado.

Enzo Gabriel:

- Sobre o projeto: A aula foi muito interessante, pois diferente das outras, a gente conseguiu ver na prática alguns conhecimentos e pudemos botar a mão na massa, configurando de fato certificados digitais.
- Participação: Ajudei o grupo principalmente na parte dos certificados digitais e na parte da assinatura digital, que foi onde mais pesquisei sobre também.
- Autoavaliação: Boa, participei juntamente com outras pessoas no início do projeto.

Referências

Gerando um Certificado Digital Próprio - https://www.devmedia.com.br/gerando-um-certificado-digital-proprio/31506

TLS e SSL: saiba o que são estes certificados de segurança e suas diferenças - https://rockcontent.com/br/blog/tls-ssl/

Ativando HTTPS no Apache - https://techexpert.tips/apache/enable-https-apache/