## Tarefa Prática 7 (15%) “Segurança na WEB”

Grupo: 2 Alunos

Alunos: -----------------------------------------------------------

 -----------------------------------------------------------
**Assunto:**
Configurar a segurança de um Servidor Web utilizando o software APACHE, (ou outro que você queira) com suporte para SSL. Trabalhar com a ferramenta OpenSSL; obter um certificado auto-assinado para servidor; instalar e testar o funcionamento.

### Bibliografia Básica

* Página do Apache, disponível em: <http://www.apache.org/>
* Página do OpenSSL, disponível em: <http://www.openssl.org/>
* SANTOS, Leonel Filipe Simões, e JACINTO, Nuno Filipe Pedro. Artigo: Autenticação Web com certificados digitais, 2006, disponível em: <http://www.inf.ufsc.br/~bosco/ensino/ine5630/material-cripto-seg/3_Autenticacao_Web_com_certificados_digitais.pdf>

### Objetivos

Compreender a necessidade e situações que demandam a utilização de páginas seguras. Aplicar o uso de segurança, baseado em certificados auto-assinados em um Servidor Web. Compreender como se passa a autenticação de um usuário numa página HTTPS.

### Seleção do Conteúdo

Mostre seu experimento com um conteúdo mínimo, seguindo o roteiro.
Procure um site em que possa verificar as vulnerabilidades sem causar problemas sobre ameaças ou ataques. Use a ferramenta Nikto e mostre um relatório proporcionado pela ferramenta, relatando vulnerabilidades descobertas.

Visando a prática da tarefa, trabalhe com o Apache2 (ou outro) e o OpenSSL

* Criar os certificados auto-assinados e habilitando-os no Apache para SSL;
* Criar um AC no OpenSSL;
* Habilitar o Apache para SSL;
* Testar em um navegador, acessando a página segura em “[https://](https://localhost)”, e verificando o certificado.

Para contemplar o conteúdo prática, o aluno deverá seguir os passos, na ordem abaixo:

1. $ openssl req $@ -new -x509 -days 365 -nodes -out /etc/apache2/apache.pem -keyout /etc/apache2/apache.pem → Criando o Certificado e habilitando-o no Ap$ chmod 600 /etc/apache2/apache.pem → Modificar as permissões do arquivo:



 Exemplos de dados para criar o certificado no OpenVPN.

1. $ gedit /etc/apache2/ports.conf → Modificar o arquivo ports.conf para habilitar o Apache para “escutar” a porta 443, conforme o quadro 2.

<IfModule mod\_ssl.c>

Listen 443

</IfModule>

Quadro 2: Modificação do ifModule no arquivo ports.conf

1. $ a2enmod ssl → Habilitar o Apache para SSL;
2. $ gedit /etc/apache2/sites-available/default – Modificar o arquivo *default* conforme o quadro 3:
3. $ gedit /etc/apache2/sites-available/default – Modificar o arquivo *default* conforme o quadro 3:

<VirtualHost \*:80>

ServerAdmin webmaster@localhost

DocumentRoot /var/www/

<Directory />

Options FollowSymLinks

AllowOverride None

</Directory>

<Directory /var/www/>

Options Indexes FollowSymLinks MultiViews

AllowOverride None

Order allow,deny

allow from all

</Directory>

</VirtualHost>

<VirtualHost \*:443>

DocumentRoot /var/www-ssl/

<Directory />

Options FollowSymLinks

AllowOverride None

</Directory>

<Directory /var/www-ssl/>

Options Indexes FollowSymLinks MultiViews

AllowOverride None

Order allow,deny

allow from all

</Directory>

ErrorLog /var/log/apache2/error.log

CustomLog /var/log/apache2/access.log combined

SSLEngine on

SSLEngine on

ServerSignature on

SSLCertificateFile /etc/apache2/apache.pem

</VirtualHost>

Quadro 3: Modificação no arquivo default

1. $ mkdir /var/www-ssl → Criar diretório para variáveis;
2. $ /etc/init.d/apache2 restart → Reiniciar o Apache;
3. Testar em um navegador, inserindo “https://localhosso do mesmo computador.



Navegador Mozilla Firefox demonstrando segurança com certificado em pagina https.

A sua apresentação deve ser similar a este roteiro, precisando melhorar as explicações no texto.