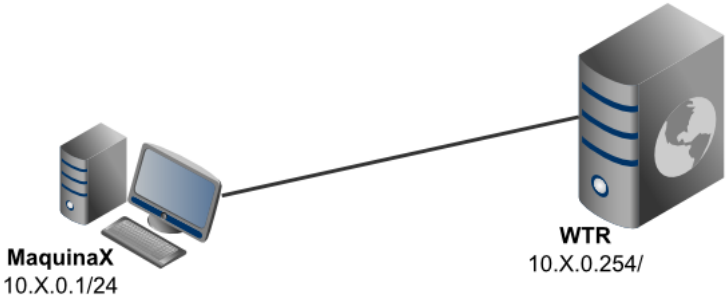
I WTR do POP-BA

I Workshop de Tecnologias de Rede
Ponto de Presença da RNP na Bahia
Instrutor: Italo Valcy
Monitor: Ibirisol Fontes

Prática 01: Configurando SSL no Apache2



Este laboratório visa apresentar aos alunos os passos para configuração de SSL em um servidor web com Apache2. A figura acima ilustra a topologia lógica para configuração do ambiente. Nessa figura, a máquina ***MaquinaX*** representa a estação de trabalho do aluno, enquanto que ***WTR*** representa uma máquina virtual que funcionará como o servidor web com Apache2.
Obs.: Substitua o ***X*** abaixo por um identificador único fornecido pelo instrutor (valor natural de 0 à 255).

Objetivo da Prática

- Entender a necessidade de configuração da criptografia no protocolo HTTP para aplicações críticas, por exemplo, autenticação em sites através de login/senha.
- Criar uma Autoridade Certificadora (CA) para emissão de certificados SSL e adicioná-la nos clientes.
- Criar um certificado SSL para www.exemplo.pop-ba.rnp.br e configurá-lo no Apache2.

Parte 01: Configurações iniciais de rede

Para configurar a rede na máquina ***MaquinaX***, inicie o gerenciador de configurações de rede do Windows e edite a interface de rede física da máquina, seção do *Protocolo TCP/IP versão 4 (TCP/IPv4)*, e adicione as seguintes configurações:
- Usar o seguinte endereço IP:
  - Endereço IP: ***10.X.0.1***
  - Máscara de sub-rede: ***255.255.255.0***
  - Gateway padrão: ***10.X.0.254***
  - Servidor DNS preferencial: ***8.8.8.8***

Adicionalmente, edite o arquivo `c:\WINDOWS\system32\drivers\etc\hosts` e acrescente o seguinte (substitua o X pelo valor apropriado):

Apoio:

10.X.0.254 ***www.exemplo.pop-ba.rnp.br***

Inicie a máquina virtual ***WTR*** e edite as configurações de rede do sistema:

sed -i 's/10.0.0./10.X.0./g' /etc/network/interfaces
/etc/init.d/networking restart

Parte 02: Entendendo o problema

Para entendermos a motivação em usar SSL em sites que trafegam dados críticos vamos configurar um sniffer de tráfego e capturar alguns pacotes de autenticação via HTTP de um site exemplo. Para isso siga os passos abaixo listados.

- Inicie o *Wireshark* e configure-o para capturar o tráfego da interface de rede da máquina ***MaquinaX*** (CRTL+i)
- Inicie um navegador web de sua preferência (*Internet Explorer*, *Mozilla Firefox*, etc.) e digite www.exemplo.pop-ba.rnp.br. Na tela de login, forneça o login ***wtr*** e a senha ***wtr2010***
- Volte para o *Wireshark* e verifique os pacotes capturados. Veja que o *login* e *senha* do usuário passam em texto puro na conexão (procure por pacotes em que o campo Info contenha: ***`POST /logar.php ...`*** e veja a sessão do cabeçalho "Line-based text data").

Parte 03: Criando sua própria Autoridade Certificadora (CA)

Para que possamos habilitar SSL em nosso servidor web, precisaremos de uma chave privada e um certificado para nosso servidor. No caso de servidores comerciais, pode ser interessante comprar um certificado junto a alguma CA reconhecida e já inclusa nos navegadores web mais populares. Em algumas situações, uma alternativa mais viável pode ser criar sua própria CA e divulgar o certificado da CA aos clientes, solicitando para que eles o incluam em seus navegadores antes de iniciar a conexão SSL. Nessa prática utilizaremos a segunda alternativa. Para criar nossa CA e emitir os certificados, usaremos a ferramenta OpenSSL (***aptitude install openssl***). Siga os passos abaixo para criação da CA.

- Criando um diretório para armazenar os certificados e chaves privadas.

mkdir /root/CA
chmod 0770 /root/CA
cd /root/CA

- Criando uma chave privada para nossa CA. Essa chave privada deve ser mantida em segredo.

root@wtr:~/CA# ***openssl genrsa -des3 -out wtr-ca.key 2048***
Generating RSA private key, 2048 bit long modulus
..+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for wtr-ca.key: ***wtr2010***
Verifying - Enter pass phrase for wtr-ca.key: ***wtr2010***

- Criando o certificado x509 para nossa CA. Este certificado será distribuído para nossos clientes.

root@wtr:~/CA# ***openssl req -new -x509 -days 3650 -key wtr-ca.key -out wtr-ca.crt***
Enter pass phrase for wtr-ca.key: ***wtr2010***

Apoio:

RNP UFBA CENTRO DE PROCESSAMENTO DE DADOS UFBA extreme networks D-Link Building Networks for People

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:***BR***
State or Province Name (full name) [Some-State]:***Bahia***
Locality Name (eg, city) []:***Salvador***
Organization Name (eg, company) [Internet Widgits Pty Ltd]:***I WTR do POP-BA***
Organizational Unit Name (eg, section) []:***Autoridade Certificadora***
Common Name (eg, YOUR name) []:***WTR CA***
Email Address []:***wtr@pop-ba.rnp.br***

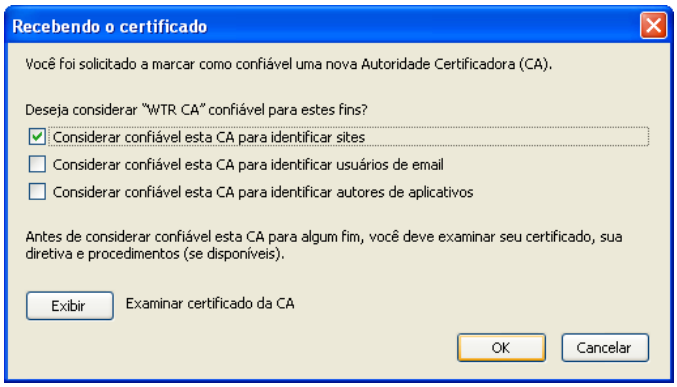
- O comando acima deve gerar o arquivo `wtr-ca.crt` na pasta local. Para visualizar seu conteúdo, execute o seguinte comando:

openssl x509 -in wtr-ca.crt -text -noout

- Vamos copiar esse certificado para a pasta `/var/www/` e deixá-lo disponível para que os clientes possam instalar em seus navegadores. Para isso execute o seguinte comando:

cp wtr-ca.crt /var/www/

- Na máquina ***MaquinaX***, instale o certificado da nossa CA para que os certificados emitidos por ela sejam automaticamente aceitos no navegador utilizado. Para isso inicie um navegador web de sua preferência (*Internet Explorer*, *Mozilla Firefox*, etc.) e digite http://10.X.0.254/wtr-ca.crt (substitua o X pelo valor adequado). Dependendo do navegador escolhido você será questionado sobre "Confiar na Autoridade Certificadora WTR CA", você deve concordar. Abaixo um exemplo usando o *Mozilla Firefox*:



Parte 04: Criando uma chave e um certificado para nosso servidor web

De volta à máquina ***WTR***, precisamos agora criar uma chave privada e um certificado para nosso servidor web. Invés de criar o certificado diretamente (certificado auto-assinado), criaremos uma requisição de certificado (*certificate request*) e assinaremos tal certificado com a chave de nossa CA, criada na *Parte 03*. Para isso, execute os passos abaixo:

- Criando uma chave privada e uma requisição de certificado para nosso servidor:

root@wtr:~/CA# ***openssl req -nodes -new -keyout exemplo.key -out exemplo.csr***
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'exemplo.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:***BR***
State or Province Name (full name) [Some-State]:***Bahia***
Locality Name (eg, city) []:***Salvador***
Organization Name (eg, company) [Internet Widgits Pty Ltd]:***I WTR do POP-BA***
Organizational Unit Name (eg, section) []:***Time de Seguranca***
Common Name (eg, YOUR name) []:***www.exemplo.pop-ba.rnp.br***
Email Address []:***wtr@pop-ba.rnp.br***

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

O comando acima deve gerar dois arquivos na pasta local: `exemplo.key` é a chave privada (desencriptada) de nosso certificado que deve ser mantida de forma segura; `exemplo.csr` é a requisição de certificado que assinaremos pela nossa CA .

- Precisamos agora assinar a requisição de certificado e gerar o certificado propriamente dito usando a CA criada anteriormente (veja que a requisição de certificado não precisa ser feita na mesma máquina em que a CA foi criada; o fizemos aqui apenas para simplificar o laboratório). Para isso execute o seguinte comando:

root@wtr:~/CA# ***openssl x509 -req -in exemplo.csr -out exemplo.crt -sha1 -CA wtr-ca.crt -CAkey wtr-ca.key -CAcreateserial -days 3650***
Signature ok
subject=/C=BR/ST=Bahia/L=Salvador/O=I WTR do POP-BA/OU=Time de Seguranca/CN=www.exemplo.pop-ba.rnp.br/emailAddress=wtr@pop-ba.rnp.br
Getting CA Private Key
Enter pass phrase for wtr-ca.key: ***wtr2010***

- Por questões de segurança, vamos modificar as permissões de acesso dos arquivos de chave privada.

chmod 0400 *.key

Apoio:


- Agora vamos copiar as chaves e certificados para o local apropriado do sistema:

cp wtr-ca.crt /etc/ssl/certs/
cp exemplo.crt /etc/ssl/certs/
cp exemplo.key /etc/ssl/private/

Parte 05: Configurando o apache

Uma vez que já temos o certificado e a chave SSL, precisamos configurar o Apache para usá-los na criptografia SSL de nosso site. Execute os passos abaixo para tal configuração.

- Edite o arquivo `/etc/apache2/sites-available/exemplo` e deixe-o como mostrado a seguir (em negrito o que deve ser inserido):

```
<VirtualHost *:80>
        ServerAdmin wtr@pop-ba.rnp.br
        ServerName www.exemplo.pop-ba.rnp.br
        DocumentRoot /var/www/exemplo-wtr
        ErrorLog /var/log/apache2/exemplo-error.log
        CustomLog /var/log/apache2/exemplo.log combined
        RedirectMatch ^/+(.*) https://www.exemplo.pop-ba.rnp.br/$1
</VirtualHost>
<VirtualHost *:443>
        ServerAdmin wtr@pop-ba.rnp.br
        ServerName www.exemplo.pop-ba.rnp.br
        DocumentRoot /var/www/exemplo-wtr
        ErrorLog /var/log/apache2/exemplo-error.log
        CustomLog /var/log/apache2/exemplo.log combined

        SSLEngine on
        SSLCertificateFile    /etc/ssl/certs/exemplo.crt
        SSLCertificateKeyFile /etc/ssl/private/exemplo.key
        SSLCertificateChainFile /etc/ssl/certs/wtr-ca.crt
        SSLCACertificateFile /etc/ssl/certs/wtr-ca.crt
</VirtualHost>
```

- Habilite o módulo SSL do apache e reinicie-o para carregar essas novas configurações:

a2enmod ssl
/etc/init.d/apache2 restart

Parte 06: Testando a configuração

- Inicie o *Wireshark* e configure-o para capturar o tráfego da interface de rede da máquina ***MaquinaX*** (CRTL+i). Caso já tenha iniciado (devido à *Parte 02*) reinicie a captura (CTRL+r).
- Volte para o navegador web utilizado na *Parte 03* e digite www.exemplo.pop-ba.rnp.br. Na tela de login, forneça o usuário ***wtr*** e a senha ***wtr2010***
- Volte para o *Wireshark* e verifique os pacotes capturados. Veja que agora o trafego é criptografado, impedido que dados sensíveis (no exemplo, usuário e senha) sejam acessíveis na Internet.

Boa prática! Em caso de dúvidas, não hesite em consultar o instrutor.

Apoio: