**Setting up Secure Websites and use of TLS/SSL**

## Objective:

1. Learn how to set up a secure website using https
2. In the process, understand how TLS/SSL works

## Preamble:

Agent X's boss Albert is impressed with the way Agent X is managing security concerns of his organization (well, one sows, another reaps, thats life!). The boss wants yet another problem tackled. Periodically he has some information that he needs to share with thousands of field agents. He could potentially send individual messages via email encrypted with their public key and signed by his private key but this is turning out to be very cumbersome. What can be done?

You decide that you can create a secure website and post this information there and these field agents can login with passwords everyday and check for new updates and retrieve the information. You know TLS/SSL is the way to go since it helps agents authenticate the server as well as server authenticate agents via passwords.

## General Guidance:

1. We will use 2 VMs for this exercise as specified below. The VM images and other details can be found at https://seedsecuritylabs.org/lab_env.html To clone and configure such that the VMs are on the same LAN, follow the instructions in Appendix A and B of the below document.
   https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf
   a) Server hosting Albert's website (VM1)
   b) Agent connecting to the website (VM2)
2. Once you start the VMs, check that their IP addresses are distinct and they can ping each other. If this fails, you did not set the NAT network correctly (see Appendix B)
3. You need the following files, which are provided as a tar.gz
   a) albert.crt (Albert's root certificate)
   b) website.crt (websites' certificate signed by Albert as root).
   c) website.pem (websites's RSA keys)
   d) albert-http (folder)
   e) albert-https (folder)

## Exercise 1: Setting up a website and configuring browser

We will setup both a HTTP as well as HTTPs server using Apache which is already installed in the VM. Also we will configure the browser to trust Albert's public key.

Be very meticulous in the steps, slight mistakes, things won’t work.

## Guidance: (Setting up a web site on VM1)

1. To setup a secure website, you will need a certificate for the website (signed by Albert as root CA) as well as public/private keys associated with the website. (How to do these, we covered in previous PKI lab, for this lab, just use the ones provided (website.crt and website.pem).
2. **You need to be root for this purpose**. So at the command line, type “sudo su”.

3. An Apache server can simultaneously host multiple websites. It needs to know the directory where the website's files are stored. This is done via its "VirtualHost" file, located in the "/etc/apache2/sites-available" directory. To add a HTTP website, we add a VirtualHost entry to the file 000-default.conf (inside /etc/apache2/sites-available). Add at the end of the file. Copy the albert-http folder to /var/www/.

```
<VirtualHost *:80>
        ServerName http://www.albert-unsecure.com
        DocumentRoot /var/www/albert-http
        DirectoryIndex index.html
</VirtualHost>
```

4. To add a HTTPS website, we need to add a VirtualHost entry to the default-ssl.conf file in the same folder. Add at the very last line. Ensure that the server name matches exactly what is in the website certificate. Copy the SSLCertificateFile (website.crt) to /etc/apache2/ssl/ and the SSLCertificateKeyFile (website.pem) to /etc/apache2/ssl/. Also, copy the albert-https folder to /var/www/. Double check that all paths below have valid files/folders.

```
<VirtualHost *:443>
      ServerName https://www.albert-secure.com
      DocumentRoot /var/www/albert-https
      DirectoryIndex index.html
      SSLEngine On
      SSLCertificateFile /etc/apache2/ssl/website.crt
      SSLCertificateKeyFile /etc/apache2/ssl/website.pem
</VirtualHost>
```

5. You need to run a series of commands to enable SSL/TLS. Note Apache will ask you to type the password used for encrypting the private key. At the command line,
    1. To test the Apache configuration file for errors, type "apachectl configtest" (It should say OK)
    2. To Enable the SSL module, type "a2enmod ssl"
    3. To Enable the site, type "a2ensite default-ssl"
    4. To (re)start Apache service, type "service apache2 restart" and enter password as "albert2" without the quotes (the website.pem file is protected with this)
6. Also, if you want to access the website locally, you have to enter the following in the "/etc/hosts" file

```
127.0.0.1       www.albert-unsecure.com
127.0.0.1       www.albert-secure.com
```

7. You can check if the site works by opening a browser and typing the URL http://www.albert-unsecure.com/. If you tried https://www.albert-secure.com/, it will say URL is not secure since Albert is not recognized as a root CA by the browser.

**Guidance: (Setting up a browser on VM2)**

1. Configuring the browser: We need to get the browser to accept the CA certificate (Albert's). Had the website certificate been assigned by say VeriSign, this comes preloaded into Firefox'scertificate repository already. Unfortunately, Albert as a CA is not recognized by Firefox. We need to do this manually. (You can do the same on VM1 too)
2. To load albert.crt into Firefox "Edit -> Preference -> Privacy & Security -> View Certificates". Use "import" and import "albert.crt" and select the following option: "Trust this CA to identify web sites". You will see that our CA's certificate is now in Firefox's list of the accepted certificates (under IIT).
3. Also, to access the website on VM1 from browser on VM2, you have to do a DNS

resolution on VM2. We will get around this by directly entering the following in the "/etc/hosts" file. **Note: You need to change the IP address below to whatever is the IP address of VM1.**

```
10.0.2.4      www.albert-unsecure.com
10.0.2.4      www.albert-secure.com
```

Once everything is set up properly, you can browse the web site.

**Exercise 2: Exploring TLS/SSL (VM1 and VM2)**

References:
https://medium.com/@ethicalevil/tls-handshake-protocol-overview-a39e8eee2cf5
https://vincent.bernat.ch/en/blog/2011-ssl-session-reuse-rfc5077

1. From the agent machine (VM2), start a wireshark trace. Then open the browser and connect to the http (insecure) website (http://www.albert-unsecure.com). Enter username/password (anything you feel like). Stop capture and save the trace and explore it and answer the questions in the quiz. In case you see no traffic, clear the cache and try again.
2. From the agent machine (VM2), start a wireshark trace. Then open the browser and connect to the https (secure) website (https://www.albert-secure.com). Enter username/password (anything you feel like). Stop capture and save the trace and explore it and answer the questions in the quiz. In case you see no traffic, clear the cache and try again.

(Once you are done, I will go through it and come up with the questions)