INFO 2411 - Self-Signed SSL Lab

Submission Requirements

Document all the commands and all the required screenshots in the main markdown file of your submission. Ensure that all commands are entered in plain text as well and that all your screenshots show up in your markdown file.

```
SslLab-hi-89/
    ├── SSLLab-shi-89.md
    ├── KaliHosts-shi-89
    ├── SSLConfigDiff-shi-89
    ├── (appropriate files for your certificate setup here... you have to do
research as to what file(s) you should submit)
    └── img/ # All your screenshots here
```

The purpose of this lab is to become familiar with a webserver (real one) and installing an SSL certificate. On an apache server and then routing DNS to match the FQDN...

Pre-requisites

Students will need to have the Virtual Lab network setup, see the "Setting up a Lab environment in VirtualBox" document located in the same week.

Students will also need to setup an Ubuntu server. Using the provided ISO file, setup a server the the following provisions:

Some information about the setup you will need to pay attention to:

In Virtualbox [*] skip unattended in stallation Do not encrypt your home folder

Item	**Value**	**Comment**
Hostname	ubuntu-shi-89	
Username	shill	
Network	The NAT network you setup, from the previous aforementioned documentation	
CPU	1	
RAM	2 GB	
Storage	25 GB	All the files in one partition is fine. *Remember to write the changes to disk*

Item	Value	Comment
Default Packages	OpenSSH LAMP Server	You will get to select these during the installation. Because you are installing a LAMP server you will be prompted to set a password for MySQL, set this to something you will remember.

Verifying network connectivity

Students will need to verify network connectivity between their Kali Linux machine and Ubuntu. You can use `ping` to verify basic connectivity and then `ssh` to ssh to the server where you will do the work. You will notice that there is no gui to do the rest of this lab. You will find the same at work in a non-windows environment.

Instructions

How you are all set to do the lab.

```
Complete the following steps in your Ubuntu Server.  You will need to "ssh" into
your server or you can use the console.  Be sure to record all the relevant com-
mands and take screenshots to include them in your lab submission file.
```

Setting up the hosts file

Edit the /etc/hosts file. Add a line to connect to your ubuntu server:

> Of course your line will be different based on your naming convention and the network address of your ubuntu machine.

```
10.0.89.5   ssllab-shi-89.kpu.ca
```

Take a screenshot of your `/etc/hosts file` and include it in your submission.

Creating the SSL Certificate

1. Create the key and certificate on your Ubuntu Server

   sudo openssl req -x509 -nodes -days 14 -newkey rsa:4096 -keyout /etc/ssl/private/apache-ssllab-shi-89.key -out /etc/ssl/certs/apache-ssllab-shi-89.crt

> Students should pay attention to the above command argments days, keyout, out and the file name.

Here are some requirements for generating your SSL certificate. You will of course adjust for the naming convention.

Field	Value
Common Name	ssllab-shi-89.kpu.ca
Name	Your Name
Email	Your student email
Organizational Unit	CSIT

Submit the appropriate certificate file(s) for your submission, do some research, which file(s) should be submitted and while file should not

Take a note of the location of the files you will need them for later.

Enabling the certificate in Apache

```
Its always a good idea to backup a config file before you modify it, go ahead for any file use the cp command to backup the file to a different name so that you can reference the original.
```

---

1. Enabling the required config, generally with the ubuntu style apache config there is "available" and "enabled".

   ```
   cd /etc/apache2/sites-enabled
   ln -s ../sites-available/default-ssl.conf
   ```

2. Turn on the SSL key and certificate file that you generated in the previous step.

2a. Backup the `default-ssl.conf` file to `default-ssl.conf.shi-89`. Remember where you are in the file system. Use the `cp` command, record the relevant commands your markdown file for submission.

2b. Modify the default-ssh.conf file and comment out the two following key/value pairs, then add your own below. Adjust the values for where you put your key file and certificate file that you generated.

```
# SSLCertificateFile
# SSLCertificateKeyFile
```

> Remember: a key **is private** and should never leave the server that it was created on.

3. Check the config file is correct, use the command `apachectl configtest`. You may ignore any warnings about ServerName.

4. You can restart the server to test the changes have taken affect `apachectl restart`

5. Once you are sure it works then use the `diff` unix command and show the changes for `default-ssl.conf`. Redirect the output of the diff command to a file called `SSLConfigDiff-shi-89.txt`, include it with your submission. Record the comamnd you used in your submission file.

Verifying the setup on your Kali machine with a real web browser

---

```
Complete the following steps in your Kali Linux File
```

---

10. In your browser go to https://ssllab-shi-89.kpu.ca. View the certificate that is presented to the browser, take the appropriate screenshots and highlight the host name, the email address that is contained in the SSL certificate and the certificate thumbprint and the expiry date. Save the Screenshot as `SSLCertificateScreenshot-shi-89.xxx` include it in your submission.

Reflective Questions

In a the `SSLLab-shi-89.md` file answer the following questions:

1. What is `ln -s` why are we using it?
2. Why is it better to "ssh" into a server than using console?
3. What is the key strength of your certificate? What command would use to change it?
4. What was the hardest part of this lab? Why?
5. What are the most important items in an SSL certificate that will help you to identify its identity, authenticity and validity? Explain your answer.

References
