Practical Networking

Practical TLS – Lab Guide

A deep dive into SSL and TLS – the protocols that secure the Internet

Lab 3.2 – Matching Certificate and Private Keys

In this lab, you will be performing two tasks. First, you will inspect the contents of a Private Key file and validate the fields within which were discussed in the lesson. Second, you will match five different Private Key files to their appropriate Certificate files.

Create working directory and acquire lab files

1. Navigate to the folder you created in Lab 0.0 named Practical-TLS
   - `$ cd Practical-TLS`

2. Create a new directory for Lab 3.2 files:
   - `$ mkdir "LAB3.2 – Matching Certificate and Private Keys"`

3. Download one of the following lab files and place it in the newly created folder:
   - **LAB 3.2 Files - Matching Certificates and Private Keys - Practical TLS.tar.gz**
   - **LAB 3.2 Files - Matching Certificates and Private Keys - Practical TLS.zip**

   The lab files are in `.zip` or `.tar.gz` format – the contents within are identical, use whichever file is easier for you

4. Unzip or Untar the file you downloaded into your LAB 3.2 working directory:
   - For the TAR.GZ file, you will use the Linux command: `tar -xvzf "LAB 3.2 ...`
   - For the ZIP file, it should be something like right clicking the file and selecting "Extract All..."

5. When finished, you should have the following 12 files in the LAB 3.2 directory:

```
Rainbow.cert        Blue.cert          key1.key
Rainbow.key         Green.cert         key2.key
                    Orange.cert        key3.key
                    Violet.cert        key4.key
                    Yellow.cert        key5.key
```

Inspect the content of a Private Key file

1. Use the `cat` utility to view the content of the file `Rainbow.key`
   - `cat Rainbow.key`
2. Feed `Rainbow.key` into the `openssl rsa` utility:
   - `openssl rsa` **`-in Rainbow.key`**
3. Feed `Rainbow.key` into the `openssl rsa` utility and request the text output:
   - `openssl rsa -in Rainbow.key` **`-text`**
4. Repeat the command above, but add the argument to disable the Base64 output of the file
   - `openssl rsa -in Rainbow.key -text` **`-noout`**
     NOTE: The order of the `-in <file>`, `-text`, and `-noout` arguments are irrelevant
5. From the previous output, try to identify the fields we discussed in the lesson:
   - Modulus
   - Public Exponent
   - Private Exponent
   - Prime 1
   - Prime 2
   - Exponent 1
   - Exponent 2
   - Coefficient
6. Compare the Modulus in the Private Key file with the Modulus in the Certificate file:
   - `openssl` **`x509`** `-in Rainbow`**`.cert`** `-text -noout`
     - *How did the Modulus in the Certificate compare to the Modulus in the Private Key file?*
7. Modify the commands above to only request the Modulus of either file:
   - `openssl` **`rsa`** `-in Rainbow`**`.key`** `-noout` **`-modulus`**
   - `openssl` **`x509`** `-in Rainbow`**`.cert`** `-noout` **`-modulus`**
     - *What can you determine about the Moduli in matching Certificate and Key files?*

Match Private Key files to their respective Certificates

Other than the two files you inspected in the previous task (`Rainbow.cert` and `Rainbow.key`), the remaining ten files should exist in your working directory:

```
Blue.cert       key1.key
Green.cert      key2.key
Orange.cert     key3.key
Violet.cert     key4.key
Yellow.cert     key5.key
```

Each Key file maps to one certificate. **Your task is to find which Key file matches which certificate.**

Use the commands you practiced in the previous task along with what was taught in the accompanying lesson to accomplish this task.