ECE 518 Grad Project 1

Alan Palayil Due Date: 12/04/2022

Section I Objective

In this project, we are introduced in how to secure a website with HTTPS connections and craft an attack to understand its vulnerabilities.

Section II Apache Web Server

After installing the VM, we login to the machine using the username and password provided. We then check if the machine is installed with Apache web server using the following command:

```
netstat -tan
```

After which we use ‘wget’ to obtain the homepage which confirms Apache works.

```
wget localhost
```

Section III Work with Certificate

We download and extract the project file which will be used to sign a certificate for the server using a simulated CA.

```
wget http://www.ece.iit.edu/~jwang/ece443-2022f/prjg1-src.tgz
tar -zxf prjg1-src.tgz
cd prjg1-src/
```

The CA is created and identify our sever at ‘localhost’ using openssl.

```
./create-ca.sh
./localhost-csr.sh
./sign-localhost.sh
```

Section IV Enable HTTPS Connections

We enable SSL/TLS support in Apache.

```
cd /etc/apache2/mods-enabled/
sudo ln -s ../mods-available/ssl.* .
sudo ln -s ../mods-available/socache_shmcb.load .
```

We copy the configuration file 'apache-ssl-localhost.conf’ to Apache's configuration directory and to restart Apache so it will see the changes.

cd ~/prjg1-src/

sudo cp apache-ssl-localhost.conf /etc/apache2/sites-enabled/

sudo service apache2 restart

We use the following command to verify that the HTTPS port 443 is in use and then fire 'wget https://localhost'. After which we use wget to trust our CA by providing the certificate.

```
netstat -tan
wget https://localhost
wget https://localhost --ca-certificate=ece443-CA.pem
```

Section V Attack

In this section we are looking over the vulnerabilities in HTTPS connections by crafting an attack in our virtual machine. Following the lab, we must get ece443.hacked to be recognized as a valid certificate. We are hinted to modify localhost.cnf, localhost-csr.sh, and sign-localhost.sh. I create a copy of each of the files using the command sudo cp filename new-filename within the directory.

```
sudo cp filename new-filename
```

For the copy files, I added old at the end of the filename like: localhostold.cnf, localhostold-csr.sh, and sign-localhostold.sh. We then open the files using vim to modify them.


```
sudo vim filename
```

In localhost.cnf, the line with commonName_default was changed from localhost to ece443.hacked and under alternate_names heading DNS.1 was change from localhost to ece443.hacked. After changing localhost.cnf, localhost-csr.sh and sign-localhost.sh was ran to create new private key and sign the certificate. Using the command in Section III:

```
./localhost-csr.sh
./sign-localhost.sh
```

After which the Apache server is restarted with the command:

```
sudo service apache2 restart
```

Once restarted we can check if our modifications are done correctly by using ping.

```
ping ece443.hacked
```

We then put the wget command to run https://ece443.hacked which yields a successful connection to ece443.hacked, however localhost could then not be connected to as the keys were overwritten.

- Consider the four files: 'ece443-CA.key', 'ece443-CA.pem', 'ece443-localhost.key', 'ece443-localhost.pem'. Which one is the secret of the CA? Which one is the secret of the server? Which one(s) should be released to public? Why?
  - The server's secret is ece443-localhost.key, while the CA's secret is ece443-CA.key.The certificates ece443-CA.pem and ece443-localhost.pem, which users will use to verify who they are connecting to, ought to be made available to the public. Because they are private keys and are used to sign the certificates, the Key files should not be released.
- Run 'wget https://www.google.com' in the VM. Does wget complain? Where is the CA of Google's server certificate located in the VM?

- The hostname is resolved when running "wget https://www.google.com," and the connection to Google is established successfully. When connecting, there is no complaint form for wget. A file called ca-certificates.crt houses the Google certificate authority. The location of this file is /etc/ssl/certs.

- What is the purpose of the file '/etc/hosts'? Where is '/etc/hosts' located in your own computer? (Yes, Windows and MacOS both use that file too.) Check that file and see if there is anything unusual there.
  - A file called /etc/hosts contains some IP addresses for known hostnames. It lets the computer resolve the hostname without using a DNS server. The hosts file is in C:/Windows/System32/drivers/etc/ on my Windows computer. Everything is commented out, and a comment says that it is a sample hosts file. There are two localhost entries that have been commented out, as well as some examples of how to format the hosts.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
```

Section VI Appendix

Connecting successfully to localhost before the attack

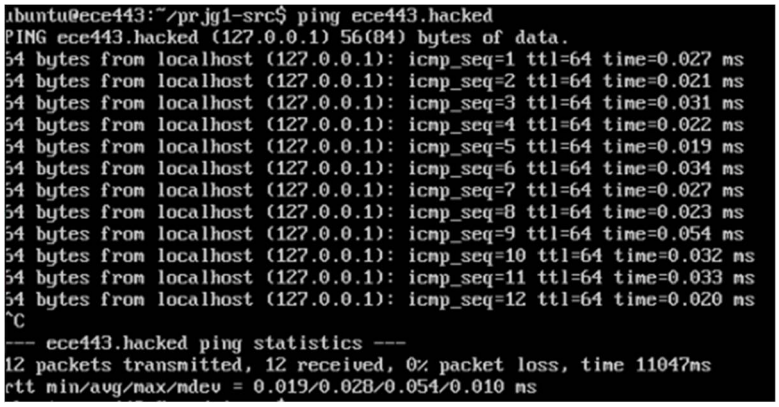
```
ubuntu@ece443:~/prjgl-src$ wget https://localhost --ca-certificate=ece443-CA.pem

--2022-12-01 21:09:39--  https://localhost/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11321 (11K) [text/html]
Saving to: 'index.html'

index.html          100%[===================>]  11.06K  --.-KB/s    in 0s

2022-12-01 21:09:39 (70.5 MB/s) - 'index.html' saved [11321/11321]
```

Pinging ece443.hacked



Connecting successfully to ece443.hacked after the attack

Failure to connect to localhost after the attack