Exercise 9.5: Enable StartTLS for Postfix, and force Plain-Text logins to use Start-TLS

Use the following information to create a certificate.

- Private-key pass phrase: `this is a long passphrase`
- Country Name: `US`
- State Name: `Awesome`
- Locality Name: `Awesometown`
- Organization Name: `Example Incorporated`
- Organizational Unit Name: `IT`
- Common Name: `smtp.example.com`
- Email Address: `admin@smtp.example.com`

Solution 9.5

1. Create a new PEM certificate:
   - For **CentOS**:
     ```
     # cd /etc/pki/tls/certs
     # make postfix.pem
     ```
   - For other distributions:
     ```
     # /usr/bin/openssl req -utf8 -newkey rsa:2048  -keyout /tmp/postfix.key -nodes \
                            -x509 -days 365 -out /tmp/postfix.crt -set_serial 0
     # cat /tmp/postfix.key > /etc/postfix/postfix.pem
     # echo "" >> /etc/postfix/postfix.pem
     # cat /tmp/postfix.crt >> /etc/postfix/postfix.pem
     # rm -f /tmp/postfix.crt /tmp/postfix.key
     ```
   - Change the **Postfix** configuration to enable and enforce TLS:
     ```
     # postconf -e "smtpd_tls_auth_only = yes"
     # postconf -e "smtpd_tls_security_level = may"
     # postconf -e "smtpd_tls_cert_file = /etc/postfix/postfix.pem"
     # postconf -e "smtpd_tls_key_file = /etc/postfix/postfix.pem"
     ```
   - Restart **Postfix**:
     ```
     # systemctl restart postfix
     ```
   - Test SMTP StartTLS:
     Note: You may have to do this twice to get the key data.
     Note: After the **starttls** command use the ”control + d” key combination.


```
$ gnutls-cli --crlf --starttls --insecure --port 25 <IP ADDRESS>
ehlo <HOSTNAME>
starttls
^d
auth plain AHNOdWRlbnQAc3R1ZGVudA==
mail from:student
rcpt to:root@<LOCAL IP ADDRESS>
data
Subject: I sent this using SASL SMTP auth protected by TLS

Cool no?
And secure!
.
quit
```

NOTE: There is no option for AUTH until after you start the TLS session.

NOTE: Relay access is still denied until after the AUTH step.

