Securing Postfix with TLS

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe the encryption features available for use with SMTP.
2. Configure Postfix to use TLS encryption with email.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- SMTP Security
  - SMTP does not support encryption
  - Designed to relay email
  - Email can be intercepted, read, and even modified
  - Transport Layer Security (TLS)
    - Provides encryption for any protocol
    - Allows encrypting SMTP without changing the standard
- Postfix security
  - Postfix was designed to add security features to sendmail
  - Postfix manages the encryption
  - Still conforms to the SMTP standard
- TLS Certificates
  - TLS requires a public/private key pair for authentication and encryption
  - Should not be self-signed
    - No one will trust it
  - Can be purchased
    - DigiCert
    - GoDaddy
  - Let's Encrypt
    - `sudo ufw allow 80`
    - `sudo certbot certonly --standalone --rsa-key-size 4096 --agree-tos --preferred-challenges http -d lab.itpro.tv`
    - Certificate is output to `/etc/letsencrypt/live/lab.itpro.tv`
- Postfix configruation
  - View the current values
    - `postconf | grep 'smtpd_tls_cert\|smtpd_tls_key'`
  - Update the values
    - `sudo postconf -e 'smtpd_tls_cert_file=/etc/letsencrypt/live/lab.itpro.tv/fullchain.pem'`
    - `sudo postconf -e 'smtpd_tls_key_file=/etc/letsencrypt/live/lab.itpro.tv/privkey.pem'`
  - Restart Postfix to apply
    - `sudo systemctl restart postfix`
- Opportunistic encryption
  - Postfix announces TLS support with the `STARTTLS` prompt
    - `postconf smtpd_tls_security_level`
    - Returns `may`
  - It is up to the client to accept

        - If TLS is not requested, email is exchanged unencrypted

- Forcing email encryption
    - It can be done, but it violates the SMTP standard
    - May result in dropped email
    - Recommended for internal use only
    - Configuring
        - `sudo postconf -e 'smtpd_tls_security_level=encrypt'`