Enabling SSL Encryption with Apache

LPIC-2: Linux Engineer (202-450)

Objectives:

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

1. Configure TLS encryption for a web site hosted on the Apache web server.

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

- SSL
  - TLS support for Apache
  - Requires OpenSSL
  - Basic steps:
    1. Create a certificate
    2. Create a secure virtual host
- Step 1: Creating a certificate
  1. Elevate access
     - `sudo -s`
  2. Generate a private key
     - `cd /etc/ssl/private`
     - `openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out lab.itpro.tv.key`
  3. Secure the key (if needed)
     - `sudo chmod 600 /etc/ssl/private/lab.itpro.tv.key`
  4. Generate a certificate signing request
     - `openssl req -new -key lab.itpro.tv.key -out lab.itpro.tv.csr`
     - Provide details as prompted
  5. Sign the request
     - `openssl x509 -req -days 365 -in lab.itpro.tv.csr -signkey lab.itpro.tv.key -out lab.itpro.tv.crt`
- Step 2: Creating a secure virtual host
  1. Edit the configuration file
     - `sudoedit /etc/apache2/sites-available/lab.itpro.tv`
  2. Create a secure virtual host
     - `<VirtualHost 10.0.222.51:443>`
       - `ServerName lab.itpro.tv`
       - `ServerAlias www.lab.itpro.tv`
       - `DocumentRoot "/var/www/html/lab.itpro.tv"`
     - `</VirtualHost>`
  3. Define the certificate and key
     - `<VirtualHost 10.0.222.51:443>`
       - `SSLEngine on`
       - `SSLCertificateFile /etc/ssl/private/lab.itpro.tv.crt`
       - `SSLCertificateKeyFile /etc/ssl/private//lab.itpro.tv.key`
     - `</VirtualHost>`
- Followup activities

- Many SSL versions are compromised and/or weak
- Disable any protocols you do not wish to support
    - `SSLProtocol -all +TLSv1.2 +TLSv1.3`
- Test with the OpenSSL client
    - `openssl s_client -connect localhost:443 -tls1_1`
    - `openssl s_client -connect localhost:443 -tls1_2`