Homework #05
SSL and TLS

Announce: 20081209

Due: 20081216

OpenSSL

- http://www.openssl.org/
- In system
  - /usr/src/crypto/openssl
- In ports
  - security/openssl

ports/Mk/bsd.openssl.mk

```
# WITH_OPENSSL_BASE=yes - Use the version in the base system.
# WITH_OPENSSL_PORT=yes - Use the port, even if base is up to date
# WITH_OPENSSL_BETA=yes - Use a snapshot of recent openssl
# WITH_OPENSSL_STABLE=yes   - Use an older openssl version
(...)
# honor obsolete options for a bit
.if defined(USE_OPENSSL_BASE) && !defined(WITH_OPENSSL_BASE)
WITH_OPENSSL_BASE=yes
.endif
.if defined(USE_OPENSSL_PORT) && !defined(WITH_OPENSSL_PORT)
WITH_OPENSSL_PORT=yes
.endif
.if defined(WITH_OPENSSL_097) && !defined(WITH_OPENSSL_STABLE)
WITH_OPENSSL_STABLE=yes
.endif

#   if no preference was set, check for an installed base version
#   but give an installed port preference over it.
.if !defined(WITH_OPENSSL_BASE) && \
    !defined(WITH_OPENSSL_BETA) && \
    !defined(WITH_OPENSSL_PORT) && \
    !defined(WITH_OPENSSL_STABLE) && \
    !exists(${DESTDIR}/${LOCALBASE}/lib/libcrypto.so) && \
    exists(${DESTDIR}/usr/include/openssl/opensslv.h)
WITH_OPENSSL_BASE=yes
.endif
```

Root CA (25%)

- Be a Certificate Authority yourself
- Issue certifications for your services

FTP-over-TLS (25%)

- Server
  - ftp/pure-ftpd
  - ftp/ftpd-tls
  - ftp/bsdftpd-ssl
- Client
  - ftp/lftpd
    - OPENSSL "With OpenSSL support" on
  - ftp/ftp-tls
- Able to download file via FTP-over-TLS

HTTPS (25%)

- /usr/local/etc/apache22/httpd.conf
  - Include etc/apache22/extra/httpd-ssl.conf
- Able to browse your web site via HTTPs

IMAPs & POP3s (25%)

- Server
  - mail/imap-uw
  - mail/dovecot
- /etc/aliases:
  - root: (your account), sysadm
- `$ newaliases`
- Able to access mailbox via IMAPs/POPs

Bonus

- Apache Client Authentication (6%)
- PGP for your mail (4%)
  - Encrypt
  - Sign

Requirements

- A shell account
  - Username: sysadm
  - Password: (your student ID)
- Your RootCA Certification (.crt)
- https://your.hostname
- ftps://your.hostname
- imaps://your.hostname
- pop3s://your.hostname
- Bonus (if available)
- Mail to hw5@sysadm.cs.nctu.edu.tw