System Administration Homework Five - SSL and TLS

yzlin <yzlin@sysadm.cs.nctu.edu.tw>

Introduction

In this homework, you are asked to build some services with SSL & TLS support.

Requirement

You should create a shell account "sysadm" with your student ID as the password. This account will be used to access the services below.

- Root CA: Make a Certificate Authority and issue certifications for the following services.
- FTP-over-TLS: Build FTP service with TLS support. You could use any server app such as ftp/pure-ftpd, ftp/ftpd-tls, and ftp/bsdftpd-ssl, just make sure it could satisfy the requrement.
- HTTPS: Build Web service with SSL support. We recommand you to use Apache (www/apache22). However, there are other server apps encouraged to use such as Lighttpd (www/lighttpd).
- IMAPs & POP3s: Build IMAPs & POP3s services. Also, any server app (mail/imap-uw and mail/dovecot) can satisfy the requirement is good. Make sure you added the following line to /etc/aliases:

  root: (your account), sysadm

  You can use command "newaliases" to rebuild the aliases database.

Advanced Requirement

- Apache Client Authentication
- Use PGP tools to create your own PGP key pair. Keep the private key and upload your public key to the PGP key server (pgp.mit.edu). Use the PGP public key of "ta@sysadm.cs.nctu.edu.tw" and your own private key to encrypt and sign a mail. Then, send this mail with subject "{Your_id}_sahw5_{PGP_key_ID}" (example: 9655630_sahw5_0F4DEE85). The mail sould contain some meaningful text to verify if it's encrypted correctly. Here is the PGP key info of "ta@sysadm.cs.nctu.edu.tw":

Type	bits /keyID	Date	User ID
pub	1024D/A5778DB7	2008/12/13	TA of Sysadmin (System Administration, CS, NCTU) <ta@sysadm.cs.nctu.edu.tw>

Grading Policy

- Root CA: 25%
- FTP-over-TLS: 25%
- HTTPS: 25%
- IMAPs & POP3s: 25%
- (Bonus) Apache Client Authentication: 6%
- (Bonus) PGP for your mail: 4%

Due Date

2008 12/17 (Wed.) 23:59:59. Please make sure your services would be accessable during 2008 12/18 00:00:00 and 2008 12/19 23:59:59.

How to Hand In

Send an email to "hw5@sysadm.cs.nctu.edu.tw" containing the following info:

- Server Domain Name: your.hostname
- Your Root CA Certification (.crt)
- (Bonus) Required infomations for Apache Client Authentication
- (Bonus) Your PGP key ID

Mail subject should be {Your_id}_sahw5 (example: 9655630_sahw5).

Demo

- Access https://your.hostname and check if the certificate info is correct.
- Use FTP clients (support TLS) to access ftps://your.hostname and download a file. Please make sure at least one file exists.
- Access imaps://your.hostname and delete one mail. Login "sysadm" and check if the mail exists.
- Access pop3s://your.hostname to download mails and delete one mail at client side. Login "sysadm" and check if the mail exists.
- Login "sysadm" and send a mail to root (local delivery). Verify the mail alias.
- Add your Root CA Certification to the trusted CA list and verify the services again.
- (Bonus) Check if we could use the key you provided to verify the certificate of https.
- (Bonus) Check if we could use your public key to verify your PGP key and use the private key of "ta@sysadm.cs.nctu.edu.tw" to decrypt the mail you sent.

Questions

TAs, I need heeeeeeeeeeeelp!

- Email ta@sysadm.cs.nctu.edu.tw
- Newsgroup cs.course.sysadmin
- BBS bs2.to board CS-SysAdmin
- Goto CSCC to ask professional 3F!