Homework 04 Hint

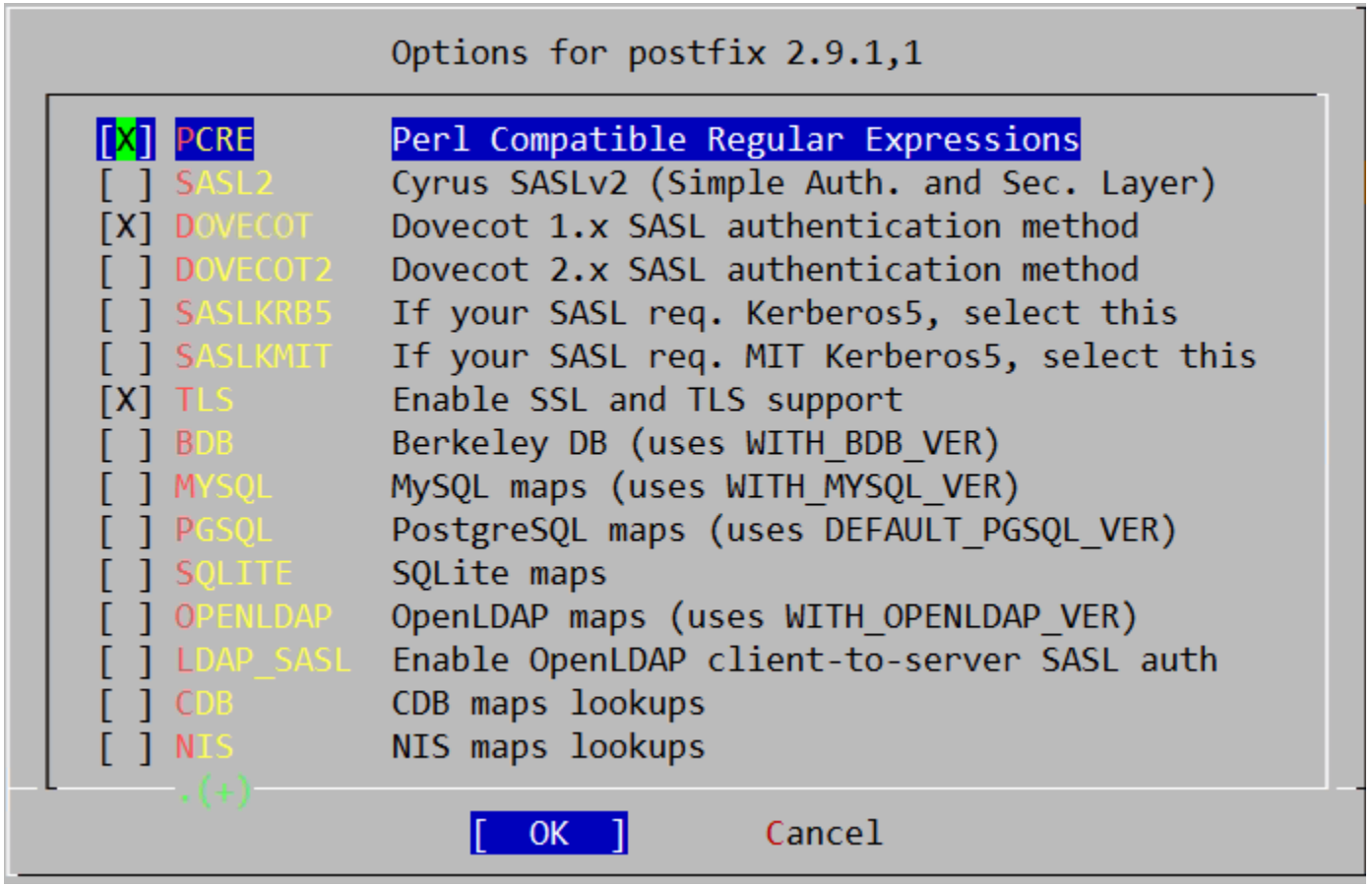
Mail System

Software

- Postfix
  - mail/postfix
- POP/IMAP
  - mail/dovecot
- MTA filter
  - security/amavisd-new
- MDA filter
  - mail/procmail
- Greylisting
  - mail/postgrey
- Anti-virus
  - security/clamav
- DKIM signature
  - mail/dkimproxy
- SPF
  - mail/sid-milter
  - mail/postfix-policyd-spf-perl
  - mail/postfix-policyd-spf-python
- Webmail
  - www/horde-base
  - mail/roundcube
  - mail/squirrelmail

Postfix – Installation

- Options
  - make config



Postfix – Installation (Cont.)

- Execute the Postfix sendmail program

```
install  -o root -g wheel -m 555
/tmp/WRKDIR/usr/ports/mail/postfix/work/postfix-
2.9.1/auxiliary/rmail/rmail /usr/local/bin/rmail
install  -o root -g wheel -m 555
/tmp/WRKDIR/usr/ports/mail/postfix/work/postfix-
2.9.1/auxiliary/qshape/qshape.pl /usr/local/bin/qshape
install  -o root -g wheel -m 444
/tmp/WRKDIR/usr/ports/mail/postfix/work/postfix-2.9.1/man/man1/qshape.1
/usr/local/man/man1
===> Installing rc.d startup script(s)
Would you like to activate Postfix in /etc/mail/mailer.conf [n]?y
```

Postfix – Configuration

- Stop sendmail

```
/etc/rc.d/sendmail stop
```

- Edit /etc/rc.conf

```
sendmail_enable="NO"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO "
postfix_enable="YES"
```

- Edit /etc/periodic.conf
  - If it does not exist please create it
  - Disable some sendmail specific daily maintenance routines

```
daily_clean_hoststat_enable="NO"
daily_status_mail_rejects_enable="NO"
daily_status_include_submit_mailq="NO"
daily_submit_queuerun="NO"
```

Postfix – Configuration (Cont.)

- Edit /usr/local/etc/postfix/master.cf
  - Enable postscreen
    - Whitelist
    - RBL
- Edit /usr/local/etc/postfix/main.cf
  - smtpd_client_restrictions
    - Deny from dynamic host
- Start Postfix

```
/usr/local/etc/rc.d/postfix start
```

- Troubleshooting
  - Check log
    - /var/log/maillog
    - /var/log/messages

Postfix – Postscreen

- postscreen_dnsbl_sites
  - Allows to weigh black/whitelists
- postscreen_dnsbl_threshold
  - When a client's score is equal to or greater than threshold, the message will be rejected

```
postscreen_dnsbl_threshold = 2
postscreen_dnsbl_sites = zen.spamhaus.org*2,
                         bl.spamcop.net*1,
                         b.barracudacentral.org*1,
                         list.dnswl.org*-1,
                         swl.spamhaus.org*-1,
                         dwl.spamhaus.org*-1
```

Dovecot

- POP3(s)/IMAP(s)
  - SSL support
- SASL Authentication
  - SASL support in the SMTP server

```
zfs [~] -wangth- postconf  -a
dovecot
```

- Configuring the following files
  - /usr/local/etc/dovecot.conf
  - /usr/local/etc/postfix/main.cf
- Edit /etc/rc.conf

```
dovecot_enable="YES"
```

- Start Dovecot

```
/usr/local/etc/rc.d/dovecot start
```

Amavisd-new

- Interface to MTA
- Anti-virus
  - supports daemonized virus and scanners accessible via Perl modules
- Anti-spam
  - SpamAssassin
- DKIM signing and verification
- SPF verification check

Amavisd-new (Cont.)

- Configuring the following files
  - /usr/local/etc/amavisd.conf
  - /usr/local/etc/postfix/main.cf
  - /usr/local/etc/postfix/master.cf
- Run the *sa-update* command at the first time
  - Automate SpamAssassin rule updates
- Edit /etc/rc.conf

```
amavisd_enable="YES"
```

- Start Amavisd

```
/usr/local/etc/rc.d/amavisd start
```

Procmail

- Configuring the following file
  - /usr/local/etc/procmailrc
- mmencode
  - converters/mmencode
  - Translate to and from mail-oriented encoding formats
    - Base64

```
zfs [~] -wangth- echo –n "蘭迪" | mmencode
6Jit6L+q
```

    - Quote-Printable

```
zfs [~] -wangth- echo –n "蘭迪" | mmencode -q
=E8=98=AD=E8=BF=AA=
```

- zh-pm-lib
  - https://github.com/linpc/zh-pm-lib

DKIM signing

- Create configuration files

```
zfs [/usr/local/etc] -wangth- sudo cp dkimproxy_in.conf.sample\
dkimproxy_in.conf
zfs [/usr/local/etc] -wangth- sudo cp dkimproxy_out.conf.sample\
dkimproxy_out.conf
```

- Configuring the following files
  - /usr/local/etc/dkimproxy_out.conf
  - /usr/local/etc/postfix/master.cf
- Edit /etc/rc.conf

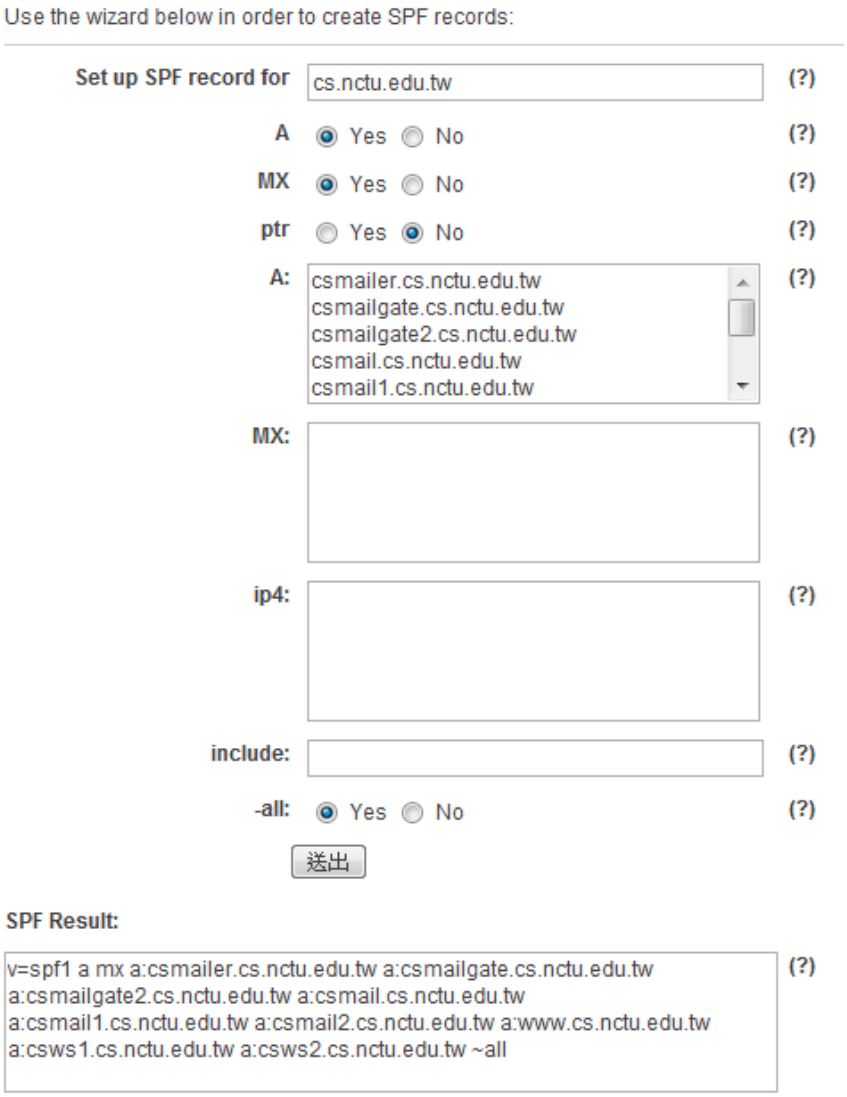
```
dkimproxy_out_enable="YES"
```

- Start dkimproxy

```
/usr/local/etc/rc.d/dkimproxy_out start
```

SPF

- SPF record
  - Add a TXT record to your zone file
  - SPF wizard
    - http://www.mailradar.com/spf/
- SPF check
  - sid-milter
    - An sid and spf milter for Sendmail
  - Postfix configuration parameter
    - smtpd_milters



DNSBL filtering – Spamhaus

- http://www.spamhaus.org
- Safe DNSBLs for safe filters
  - IP-based blacklist
    - SBL (Spamhaus Block List)
    - XBL (Exploits Blocks List)
    - PBL (Policy Block List)
    - **ZEN** (禪)
  - Domain-based blacklist
    - DBL

DNSBL filtering – Spamhaus (Cont.)

- SBL
  - Static UBE sources, verified spam services and ROKSO spammers
- XBL
  - Illegal 3rd party exploits, including proxies, worms and trojan exploits
- PBL
  - End-user Non-MTA IP addresses set by ISP outbound mail policy
- **ZEN**
  - The combination of all Spamhaus IP-based DNSBLs
    - SBL, SBLCSS, XBL and PBL blocklists

UBE: Unsolicited Bulk Email
ROKSO: The Register of Known Spam Operations
SBLCSS: Spamhaus Block List Composite SnowShoes

OpenSSL s_client

- A generic SSL/TLS client which connects to a remote host using SSL/TLS
  - very useful diagnostic tool for SSL servers.

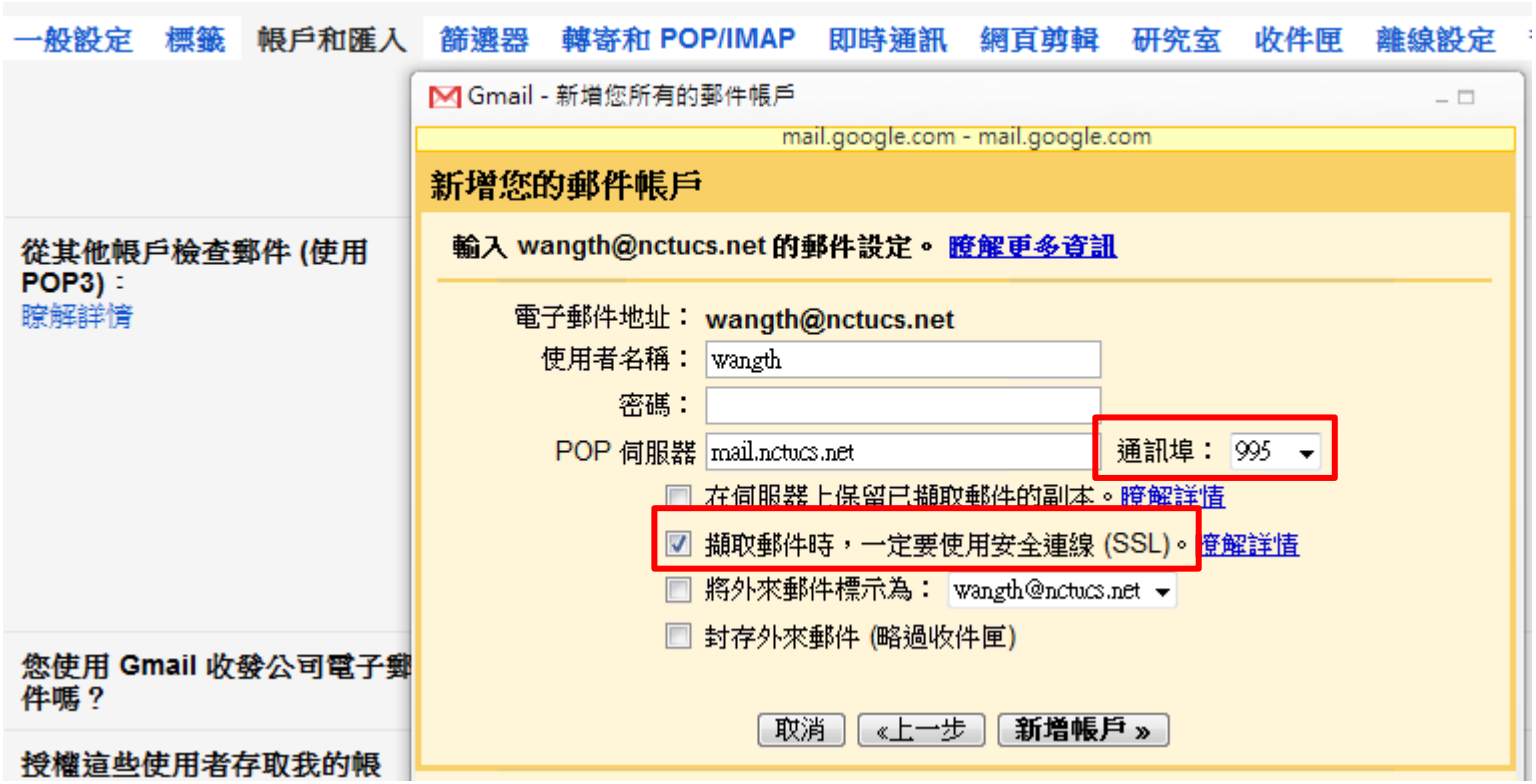
```
zfs [/usr/local/etc] -wangth- openssl s_client -connect mail.cs.nctu.edu.tw:993
CONNECTED(00000004)
…
---
SSL handshake has read 3859 bytes and written 337 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: 5A29EC41C046F1A1090F5304229149A98FC8738FF9708176FDC4912DA0BF296E
    Session-ID-ctx:
    Master-Key: ...
    Key-Arg   : None
    Start Time: 1337751796
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
---
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE
AUTH=PLAIN AUTH=LOGIN] NCTU CS Dovecot ready.
```

Webmail – Gmail

- SMTP over SSL
- SMTP authentication

Webmail – Gmail

- POP3 over SSL
- IMAP over SSL



Reference

- Postfix Postscreen Howto
  - http://www.postfix.org/POSTSCREEN_README.html
- Postfix SASL Howto
  - http://www.postfix.org/SASL_README.html
- 設定 - 郵件過濾設定
  - http://help.cs.nctu.edu.tw/help/index.php/設定_-_郵件過濾設定
- Mail-DKIM and DKIMproxy
  - http://dkimproxy.sourceforge.net/usage.html
- Setting up DKIM mail signing and verification
  - http://www.ijs.si/software/amavisd/amavisd-new-docs.html#dkim