Network Administration Practice
Homework4 – Mail System

lctseng / Liang-Chi Tseng

Requirement – Prepare Your Environment

- Get you own domain
  - http://nctucs.net
  - Add a MX record for your mail server
- You must have different hostname and domain name
- Example
  - Assume your domain name is “nasa.lctseng.nctucs.net”
  - Then your server’s hostname should be “myhost.nasa.lctseng.nctucs.net”
  - DO NOT use your domain name as your hostname
- Some parts of this homework need a dedicated DNS server you should build your own BIND DNS server
  - You can use the server in homework 3

Requirement - Overview

- Build a mail system (Total 100%)
  - SMTP Server (15%)
  - POP3/IMAP Server (16%)
  - MTA Filter: Spam/virus Filter (12%)
  - MDA Filter: procmail (5%)
  - Address Rewriting (16%)
  - Multi-Domain (4%)
  - (Advanced) Client-based Anti-spam (12%)
  - (Advanced) DKIM (10%)
  - (Advanced) SPF + SRS (10%)
- Bonus: (10%)
  - Webmail

Requirement – SMTP Server

- SMTP (5%)
  - Can send mail via telnet
- Authentication (5%)
  - SASL
  - Allow your system accounts to send mails to other domain
  - Test from other machines (bsd1~6 or linux1~6)
- SMTPs
  - STARTTLS (2%)
    - Only need to show “STARTTLS” in EHLO reply
  - SMTPs (3%)
    - Can send mail via openssl s_client

Requirement – POP3/IMAP Server

- POP (5%)
  - Retrieve mails via POP protocol
  - Must prove you can receive mails
    - Using MUA or Webmail. Any method you can prove it is ok
  - 1% for only showing in telnet
- IMAP (5%)
  - Same as POP
- POP3s and IMAPs (3% each, total 6%)
  - Use openssl s_client to show your service is working
  - Zero point here if you do not finish the corresponding plain text protocol part
- Remark
  - If you can retrieve mails via POP3s or IMAPs, then you don't need to show plain text POP3 and IMAP

Requirement – MTA Filter

- Setup amavisd-new and install filter services
- SpamAssassin (6%)
  - Send (or forward) a spam mail to your mail server
  - Must show spam tag in subject or envelope

```
X-Virus-Scanned: amavisd-new at nasa.lctseng.ncatucs.net
X-Spam-Flag: YES
X-Spam-Score: 4.85
X-Spam-Level: ****
X-Spam-Status: Yes, score=4.85 tagged_above=2 required=3
```

- ClamAV
  - Send EICAR to your server
  - Must discard the virus(5%)
  - Forward alert mails from virusalert to your own mailbox (1%)

Requirement – MDA Filter

- Use procmail
- ASCII Text Filter (2%)
  - Discard mails containing keyword “Best price today”
- Chinese Filter (2%)
  - Discard mails containing keyword “五五六六”
- Logging (1%)
  - Record all log to /var/log/procmail.log

Requirement – Address Rewriting (1)

- Transport (4%)
  - The next-hop destination of nasa.cs.nctu.edu.tw would be nahw4.nctucs.net
  - Your mail server shouldn't reject mails for @ nasa.cs.nctu.edu.tw
    - You may have to modify $mydestination
  - When demo, telnet to your mail server and send mail to nasa.cs.nctu.edu.tw
  - In your mail log, should have

```
to=<lctseng@nasa.cs.nctu.edu.tw>, relay=nahw4.nctucs.net[140.113.17.225]:25
```

- Alias (4%)
  - demo@your.domain → <demo-name>@nasa.cs.nctu.edu.tw
    - <demo-name> will be replace by names that assigned by TAs
    - You should be able to change it during demo
    - Example: forward to y3nch@nasa.cs.nctu.edu.tw

Requirement – Address Rewriting (2)

- Rewriting (4%)
  - Redirect user+demo@your.domain to user@your.domain
- Address masquerading (4%)
  - When sending mail using ‘mail’ command
  - From user@your.domain instead of user@hostname.your.domain
  - All users except root

```
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
867F126D*       383 Tue Mar 22 00:03:52  root@demo1.nasa.lctseng.nctucs.net
                                         lctseng@cs.nctu.edu.tw

DF287285*       377 Tue Mar 22 00:04:00  lctseng@nasa.lctseng.nctucs.net
                                         lctseng@cs.nctu.edu.tw
```

- Remark
  - “user” should be replaced with any account on your server

Requirement – Multi-Domain

- Create two virtual domain:
  - demo1.nasa.org
  - demo2.nasa.org
  - Do not need to register them, test them via telnet/openssl s_client
- Mailbox directory
  - Store all mails under /var/vmail
- Forward mails (2% each, total 4%)
  - For admin@demo1.nasa.org, store mails in /var/vmail/nasa1-domain/admin (Mailbox)
  - For admin@demo2.nasa.org, store mails in /var/vmail/nasa2-domain/admin/ (MailDir)

Requirement – Client-based Anti-spam

- Deny SMTP clients from linux1~6 (4%)
  - bsd1~6 are allow
  - Must show something like:

```
rcpt to: lctseng@nasa.lctseng.nctucs.net
554 5.7.1 <linuxhome.cs.nctu.edu.tw[140.113.235.150]>:
          Client host rejected: Access denied
```

- Deny hosts from Real-time Blackhole List (RBL) (4%)
  - Show your configuration in main.cf
  - Reference: http://www.spamhaus.org/
- Greylisting (4%)
  - When TA sends mails from new host, your log file must show something like:

```
450 4.2.0 <lctseng@nasa.lctseng.nctucs.net>:
Recipient address rejected: Greylisted,
see http://postgrey.schweikert.ch/help/nasa.lctseng.nctucs.net.html
```

Requirement – DKIM (10%)

- Make sure mails send from your domain have correct DKIM signature
- You should have a dedicated DNS server to finish this part

```
smtp.mailfrom=lctseng@nasa.lctseng.nctucs.net;
       dkim=pass header.i=@nasa.lctseng.nctucs.net;
       dkim=pass header.i=@nasa.lctseng.nctucs.net
Received: from demo1.nasa.lctseng.nctucs.net (localhost [127.0.0.1])
        by localhost (Postfix) with ESMTP id AF1AF28C;
        Thu, 10 Mar 2016 16:44:40 +0800 (CST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
        d=nasa.lctseng.nctucs.net; s=default; t=1457599480;
        bh=q5cyARPl5zX/knmvCnEy11G7/r6gcljJ44qrvv5DErY=;
        h=To:From:Subject:Date;
        b=A9hItAg0uAU3Fj2UsQeNcdl8YisfX5O/qnp4KM210bMEw3u4acdRvx79ByOJ2fPiz
         //0VhBDRKn80NjpnJVNeAU7t9ChEi2RABbI7Kj1VDfs2b/OmJqdbs9G2jaCoellzvj
         hPUn8YvP4zPA8VFz+Hxph6czMEAozoM6YJP3s6mQ=
```

Requirement – SPF + SRS

- Enable SPF check for incoming mails (3%)

```
Received-SPF: pass (demo1.nasa.lctseng.nctucs.net:
 domain of gmail.com designates 209.85.161.182 as permitted sender)
client-ip=209.85.161.182; envelope-from=lctseng@gmail.com;
helo=mail-yw0-f182.google.com;
```

- Add SPF into your DNS server (4%)

```
Received-SPF: pass (google.com: domain of
lctseng@nasa.lctseng.nctucs.net designates 140.113.168.238 as permitted
sender) client-ip=140.113.168.238;
```

- Enable SRS (3%)

```
Received-SPF: pass (google.com: domain of
SRS0=o35H=PH=cs.nctu.edu.tw=lctseng@demo1.nasa.lctseng.nctucs.net
designates 140.113.168.238 as permitted sender) client-
ip=140.113.168.238;
```

Bonus – Webmail

- Install one of these webmail systems
  - Horde
  - Roundcube
  - Squirrelmail
- Can receive mails (via POP or IMAP) – 5%
- Can send mails (via SMTP) – 5%
- You may need a dedicated HTTP server to finish this part

Deadline

- Demo week: 5/23~5/27
  - Subject to minor adjustment
- Please start your work ASAP!

Help!

- CSCC (EC building 3F)
- ta@nasa.cs.nctu.edu.tw
- IRC channel #nctuNASA
  - passwd: ILoveCSCC
  - Use screen or tmux to stay online, so TAs can tag you to answer your questions.
- Before you ask a question…
  - 提問的智慧: How To Ask Questions The Smart Way
  - http://mis.ndhu.edu.tw/docu/question.htm