Network Administration HW4 Checkpoints

tzute

Overview (1/3)

A. Check DNS record (8%, 2% for each)
   a) Check A record to mail.<student-id>.nasa. (mail)
   b) Check MX record to <student-id>.nasa. (@)
   c) Check SPF/TXT record on @
   d) Check DMARC record on @

B. Protect connections with STARTTLS (12%, 6% for each)
   a) Connect to IMAP with STARTTLS
   b) Connect to SMTP with STARTTLS

C. User test (12%, 4% for each)
   a) Login as TA
   b) Login as TA2
   c) Receive mails for TA and TA2

Overview (2/3)

D. Greylisting (8%)
E. Virtual alias
   a) TA3@ to TA@ (4%)
   b) <sth>|<user>@ to <user>@ (8%)
F. Ingoing mail filter
   a) Add "***SPAM***" in front of the subject (8%)
   b) Check SPF/DKIM/DMARC (8%)
G. Sender rewrite (4%)
   a) Rewrite @mail to @
H. Signing with DKIM (10%)
I. Outgoing mail filter (8%)

Overview (3/3)

J. No open relay (10%)

Checkpoint A (1/3)

a) Check A record to mail
   - $ dig A mail.<student-id>.nasa

b) Check MX record to @
   - $ dig MX <student-id>.nasa

Checkpoint A (2/3)

c) Check SPF/TXT record on @

- Using modified spf-tools
  - https://github.com/nctuna2018/spf-tools
- $ ./despf.sh <student-id>.nasa
- $ ./despf.sh –x <student-id>.nasa
- Output should be:
  - ip4:<ip-address-of-mail>
  - -all

Checkpoint A (3/3)

c) Check DMARC record on @

- Use dmarc rubygem (with Ruby 2.5.1)
  - https://github.com/trailofbits/dmarc
- $ ruby -rdmarc -e "DMARC::Record.query('<student-id>.nasa')&.tap { |r| puts r.v, r.p }"
- Output should be:
  - DMARC1
  - reject

Checkpoint B

a) Connect to IMAP with STARTTLS
   - $ openssl s_client -connect mail.<student-id>.nasa:imap -starttls imap

b) Connect to SMTP with STARTTLS
   - $ openssl s_client -connect mail.<student-id>.nasa:smtp -starttls smtp

Checkpoint C (1/2)

a) Login as TA
- Log-in to IMAP
  - A LOGIN TA <TAs-password>
- Log-in to SMTP
  - AUTH LOGIN
  - VEE=
  - <TAs-password-base64-encoded>

b) Login as TA2
- Log-in to IMAP
  - A LOGIN TA2 <TA2s-password>
- Log-in to SMTP
  - AUTH LOGIN
  - VEEy
  - <TA2s-password-base64-encoded>

Checkpoint C (2/2)

c) Receive mails for TA and TA2

a) Send mail to TA@ and log-in IMAP to check mail exists

b) Send mail to TA2@mail and log-in IMAP to check mail exists

Checkpoint D

- For new incoming mail server, greylist for 30 seconds
  - You should reply 451 4.7.1 on first time
  - After 30 seconds, reply 250 to the same server
  - TA will use different IP to test your server to avoid greylist trusted cache

Checkpoint E

a) TA3@ to TA@
   - Send e-mail to TA3@
   - Login TA to check the mail exists

b) <sth>|<user>@ to <user>@
   - Send e-mail to i-am-a|TA@ and check mail exists in TA's mailbox
   - Send e-mail to <random-string>|TA2@ and check mail exists in TA'2 mailbox

Checkpoint F

a) Add "***SPAM***" in front of the subject
   - Send e-mail to TA@ contains eicar.com
   - Check if subject is prepended with "***SPAM***"
   - eicar.com from http://www.eicar.org/download/eicar.com

b) Check SPF/DKIM/DMARC
   - Send mails with valid/invalid SPF/DKIM from variant domains with different DMARC policy (p=none or p=reject)

Checkpoint G

a) Rewrite @mail to @

- Send mail from TA@mail and TA2@mail
- Receive the mail and check if sender is TA@ and TA2@

Checkpoint H

- Sending e-mail from TA@ and check DKIM validation
  - Using opendkim
    - $ opendkim -t mail.eml
  - Output should be like:
    - opendkim: mail.eml: verification (s=<selector>, d=<student-id>.nasa, <any>-bit key) succeeded

Checkpoint I

- Sending mail from TA@ with subject-contained "小熊維尼"
  - Reject the mail

Checkpoint J

- Sending mail to mail which is:
  - FROM: other@tzute.nasa
  - TO: another@mail.tzute.nasa
- And you have to reject it

Help!

- Email to ta@nasa.cs.nctu.edu.tw
  - Don't send email by E3new
- EC 3F CSCC

- Demo will be hold on 6/20 18:30