Homework 7 Postfix & Dovecot & Anti-Spoofing

hyili

Homework 7

❑ Secure your SMTP server

- SMTP over TLS
- SMTPs
- SASL

❑ Retrieve your email

- IMAP
- POP3

❑ Anti-Spoofing

- SPF
- DKIM
- DMARC

Homework 7 - Current System

❑ SMTP

- DNS Record
- Mail Service
- Forward
- No Open Relay

❑ Problem

- Plaintext
- No authentication mechanism

Homework 7 - Secure your SMTP server

- Encrypted Connection
  - SMTP over TLS (25)
    - STARTTLS
    - openssl s_client -starttls smtp -connect “{your_server}:25”
  - SMTPs (465)
    - TLS connection
    - openssl s_client -connect “{your_server}:465”
- Authentication
  - SASL
    - AUTH LOGIN (BASE64)
    - AUTH PLAIN (BASE64)
    - Run SASL only based on SMTP over TLS, or SMTPs

Homework 7 - Retrieve your email

❑ IMAP (143)

- Testing: https://wiki.dovecot.org/TestInstallation
- nc {your_server} 143

❑ IMAPs (993)

- Enable SSL support
- openssl s_client -connect "{your_server:993}"

❑ POP3 (110)

- Testing: https://wiki.dovecot.org/TestPop3Installation
- nc {your_server} 110

❑ POP3s (995)

- Enable SSL support
- openssl s_client -connect "{your_server:995}"

Homework 7 - Anti-Spoofing - SPF

- ❑ SPF
  - Prevent “Return-Path” Spoofing
  - Requirement:
    - ➢ A DNS TXT record for SPF that
      - – Allow the following domains to send mail as your domain’s user
        - » “cs.nctu.edu.tw”
      - – Deny other domains, and drop these invalid mail
    - ➢ Do SPF policy check to the in-coming email

- ❑ {your_mail_domain} {TTL} IN TXT {SPF_rules}

Homework 7 - Anti-Spoofing - DKIM

❑ DKIM

- Ensure Integrity of mail and Identity of Sender
- Requirement:
  - ➢ Signing your out-going email with your private key
  - ➢ A DNS TXT record for DKIM
  - ➢ Do DKIM policy check to the in-coming email

❑ {selector}._domainkey.{your_mail_domain} IN TXT “DKIM_information”

Homework 7 - Anti-Spoofing - DMARC

- ❑ DMARC
  - Prevent “From” Spoofing
  - Requirement:
    - ➢ A DNS TXT record for DMARC
      - – When others receive mail that does not pass DMARC policy check
        - » Drop all the invalid email
    - ➢ Do DMARC policy check to the in-coming email
      - – When receiving mail that does not pass DMARC policy check
        - » Bcc an association report to “sa@nasa.cs.nctu.edu.tw”

❑ _dmarc.{your_mail_domain} IN TXT “DMARC_rules”