Welcome to

# DNS and Email Security

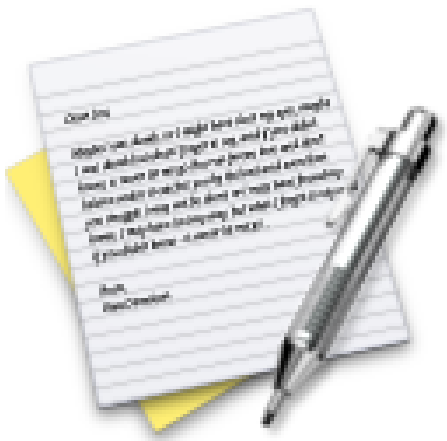
## Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramse@Github

11-DNS-and-Email-Security.tex in the repo security-courses

# Exercise



Now lets do the exercise

**??**

which is number **??** in the exercise PDF.

# SMTP Simple Mail Transfer Protocol

```
hlk@bigfoot:hlk$ telnet mail.kramse.dk 25
Connected to sunny.
220 sunny.kramse.dk ESMTP Postfix
HELO bigfoot
250 sunny.kramse.dk
MAIL FROM: Henrik
250 Ok
RCPT TO: hlk@kramse.dk
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
hejsa
.
250 Ok: queued as 749193BD2
QUIT
221 Bye
```

RFC-821 SMTP Simple Mail Transfer Protocol fra 1982

RFC-2821 fra 2001 og flere andre er idag gældende

http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

# e-mail servere

Sendmail, qmail og postfix

Tre meget brugte e-mail systemer

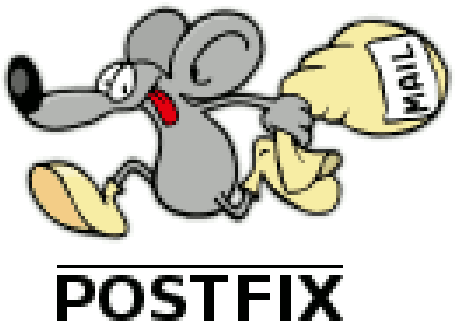
- Sendmail - den ældste og mest benyttede
- Postfix en modulært og sikkerhedsmæssigt god e-mail server
  er ligeledes nem at konfigurere
- Qmail - en underlig mailserver lavet af Dan J Bernstein, med en speciel licens - ligesom programmøren

Dertil kommer diverse andre mailservere:

Microsoft Exchange på Windows servere

Jeg anbefaler at man har en postserver mod internet, der kun sender og modtager ekstern post, og en intern postserver der opbevarer al posten

# Postfix postserveren




Lavet af Wietse Venema for IBM

Nem at konfigurere og sikker

`main.cf` findes typisk i kataloget `/etc/postfix`

# Audit af postservere

Typisk findes konfigurationsfilerne til postservere under `/etc`

- `/etc/mail`
- `/etc/postfix`

Det vigtigste er at den er opdateret og IKKE tillader relaying

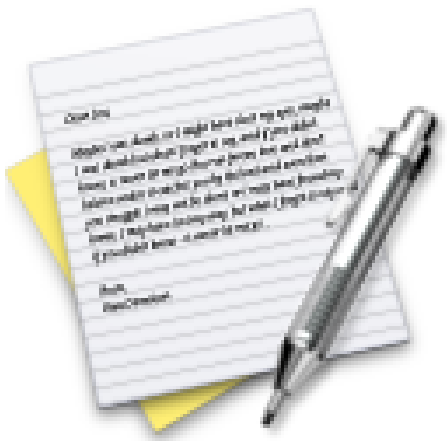
Der findes diverse test-scripts til relaycheck på internet

Husk også at checke domæne records, MX og A

# Test af e-mail server

```
[hlk]$  telnet localhost 25
Connected.
Escape character is '^]'.
220 server ESMTP Postfix
 helo test
250 server
 mail from: postmaster@pentest.dk
250 Ok
 rcpt to: root@pentest.dk
250 Ok
 data
354 End data with <CR><LF>.<CR><LF>
 skriv en kort besked
.
250 Ok: queued as 91AA34D18
 quit
```

# Exercise



Now lets do the exercise

**??**

which is number **??** in the exercise PDF.

# Postservere til klienter

SMTP som vi har gennemgået er til at sende mail mellem servere

Når vi skal hente post sker det typisk med POP3 eller IMAP

- POP3 Post Office Protocol version 3 RFC-1939
- Internet Message Access Protocol (typisk IMAPv4) RFC-3501

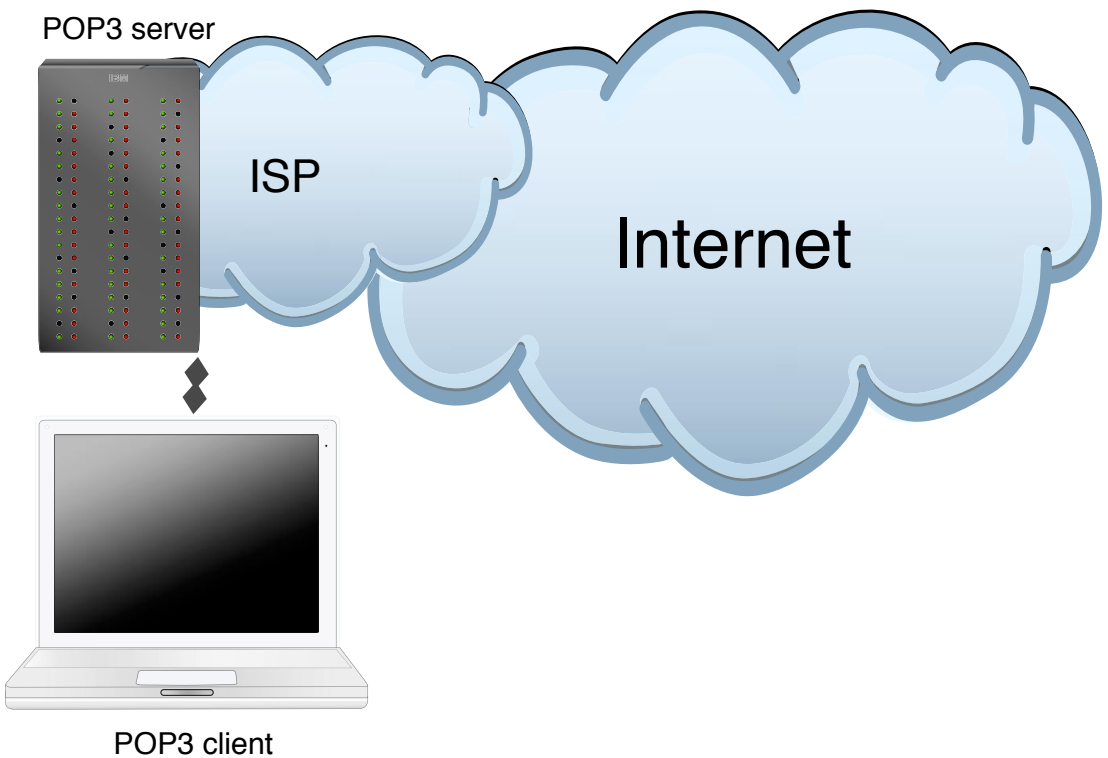
Forskellen mellem de to er at man typisk med POP3 henter posten, hvor man med IMAP lader den ligge på serveren

POP3 er bedst hvis kun en klient skal hente

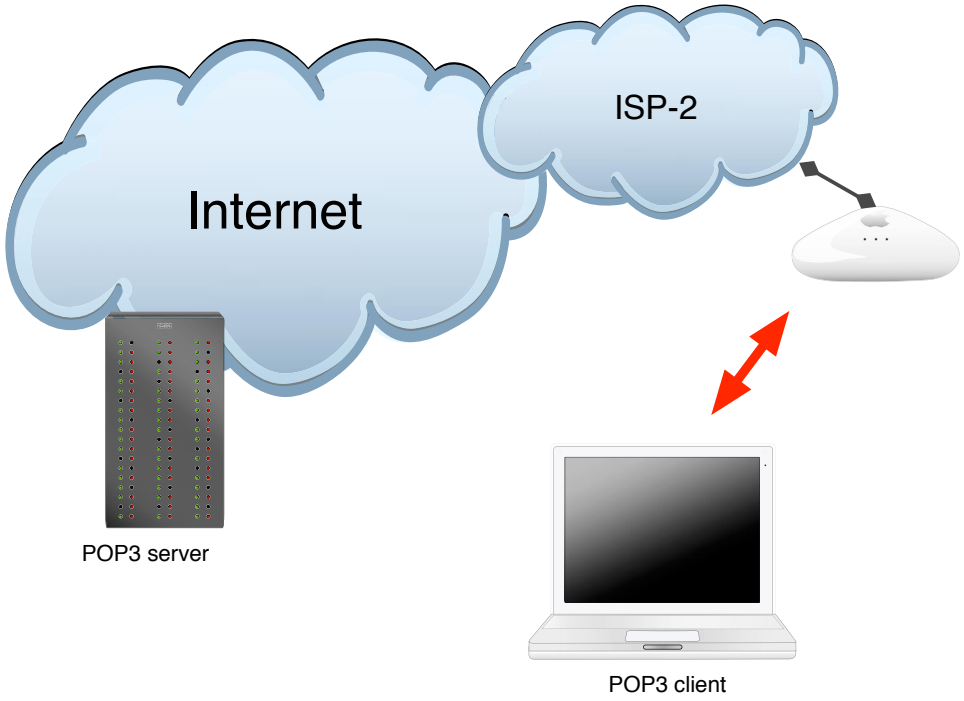
IMAP er bedst hvis du vil tilgå din post fra flere systemer

Jeg bruger selv IMAPS, IMAP over SSL kryptering - idet kodeord ellers sendes i klartekst

# POP3 i Danmark



# POP3 i Danmark - trådløst




Har man tillid til andre ISP'er? Alle ISP'er?