Welcome to

DNS and Email Security

Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.com

Slides are available as PDF, kramse@Github

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

Basal DNS opsætning

```
domain security6.net
nameserver 212.242.40.3
nameserver 212.242.40.51
nameserver 2001:1448:81:30::2
```

`/etc/resolv.conf` angiver navneservere og søgedomæner

typisk indhold er domænenavn og IP-adresser for navneservere

Filen opdateres også automatisk på DHCP klienter

Husk at man godt kan slå AAAA records op over IPv4

NB: denne fil kan hedde noget andet på UNIX varianter!

eksempelvis `/etc/netsvc.conf`

DNS systemet

Navneopslag på Internet - centralt for IPv6

Tidligere brugte man en **hosts** fil
hosts filer bruges stadig lokalt til serveren - IP-adresser

UNIX: /etc/hosts

Windows `c:\windows\system32\drivers\etc\hosts`

Eksempel: www.security6.net har adressen 217.157.20.131

skrives i database filer, zone filer

```
ns1     IN      A       217.157.20.130
        IN      AAAA    2001:618:433::1
www     IN      A       217.157.20.131
        IN      AAAA    2001:618:433::14
```

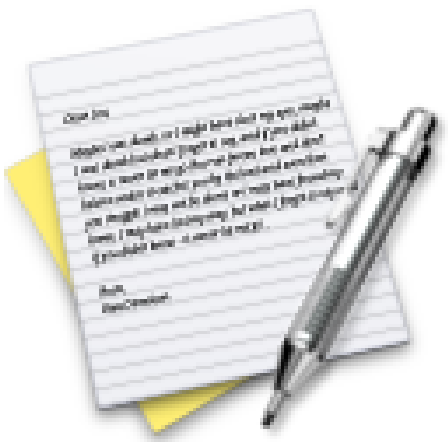
Mere end navneopslag

består af resource records med en type:

- adresser A-records
- IPv6 adresser AAAA-records
- autoritative navneservere NS-records
- post, mail-exchanger MX-records
- flere andre: md , mf , cname , soa , mb , mg , mr , null , wks , ptr , hinfo , minfo , mx ....

```
IN      MX      10      mail.security6.net.
IN      MX      20      mail2.security6.net.
```

Exercise



Now lets do the exercise

DNS og navneopslag

which is number **8** in the exercise PDF.

BIND DNS server

Berkeley Internet Name Daemon server

Mange bruger BIND fra Internet Systems Consortium - altså Open Source

konfigureres gennem `named.conf`

det anbefales at bruge BIND version 9

- *DNS and BIND*, Paul Albitz & Cricket Liu, O'Reilly, 4th edition Maj 2001
- *DNS and BIND cookbook*, Cricket Liu, O'Reilly, 4th edition Oktober 2002

Kilde: `http://www.isc.org`

BIND konfiguration - et udgangspunkt

```
acl internals { 127.0.0.1; ::1; 10.0.0.0/24; };
options {
        // the random device depends on the OS !
        random-device "/dev/random"; directory "/namedb";
         listen-on-v6  any; ;
        port 53; version "Dont know"; allow-query { any; };
};
view "internal" {
   match-clients { internals; }; recursion yes;
   zone "." {
       type hint;   file "root.cache"; };
   // localhost forward lookup
   zone "localhost." {
        type master; file "internal/db.localhost";   };
   // localhost reverse lookup from IPv4 address
   zone "0.0.127.in-addr.arpa" {
        type master; file "internal/db.127.0.0"; notify no;   };
```

```
...
}
```

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`

Vedhæftede filer kodes i MIME Multipurpose Internet Mail Extensions

Bemærk at MIME encoding forøger størrelsen med ca. 30%!

e-mail servere

Sendmail, qmail og postfix

Tre meget brugte e-mail systemer

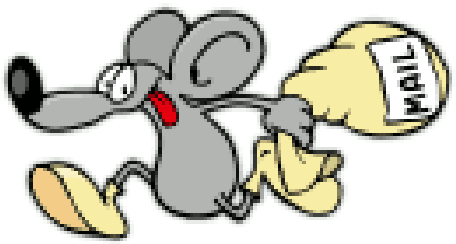
- Sendmail - den ældste og mest benyttede
- Postfix en modulært og sikkerhedsmæssigt god e-mail server
  er ligeledes nem at konfigurere
- Qmail - en underlig mailserver lavet af Dan J Bernstein, med en speciel licens - ligesom programmøren

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



POSTFIX

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

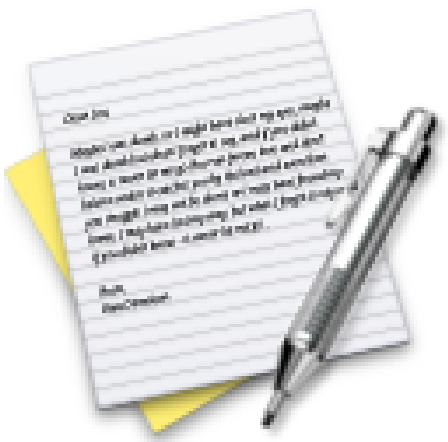
Husk også at checke domæne records, MX og A

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

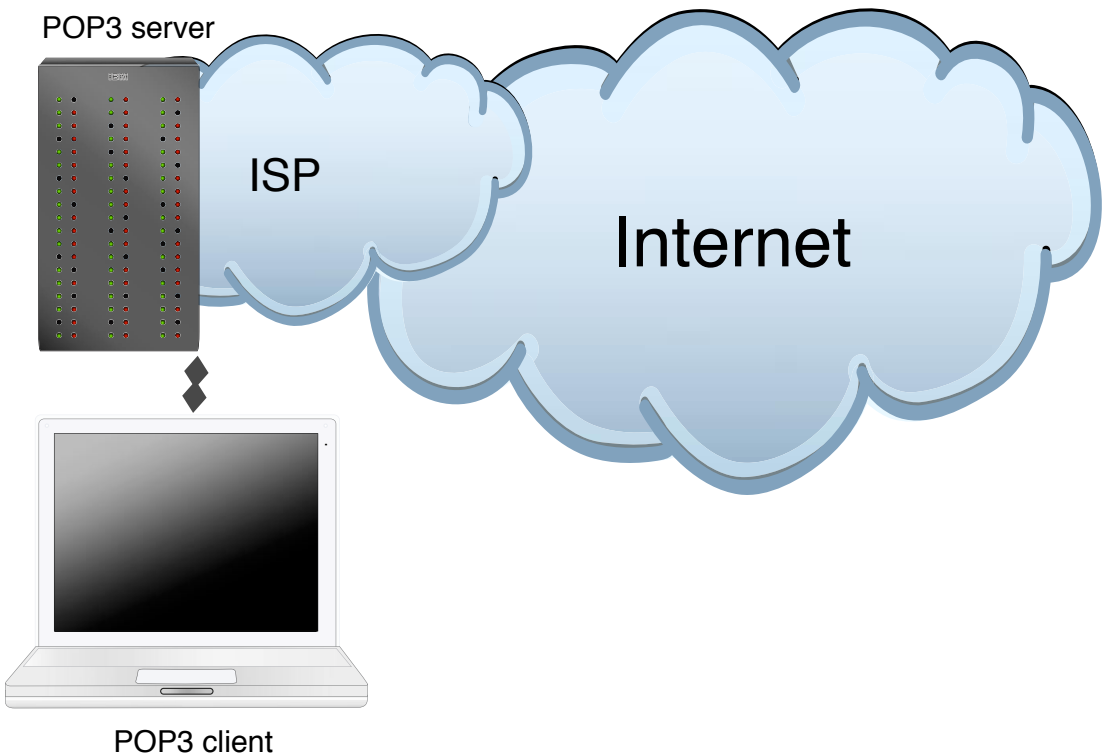
Forskellen mellem de to er at man typisk med POP3 henter posten, hvor man med IMAP lader den ligge på serveren

POP3 er bedst hvis kun en klient skal hente

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

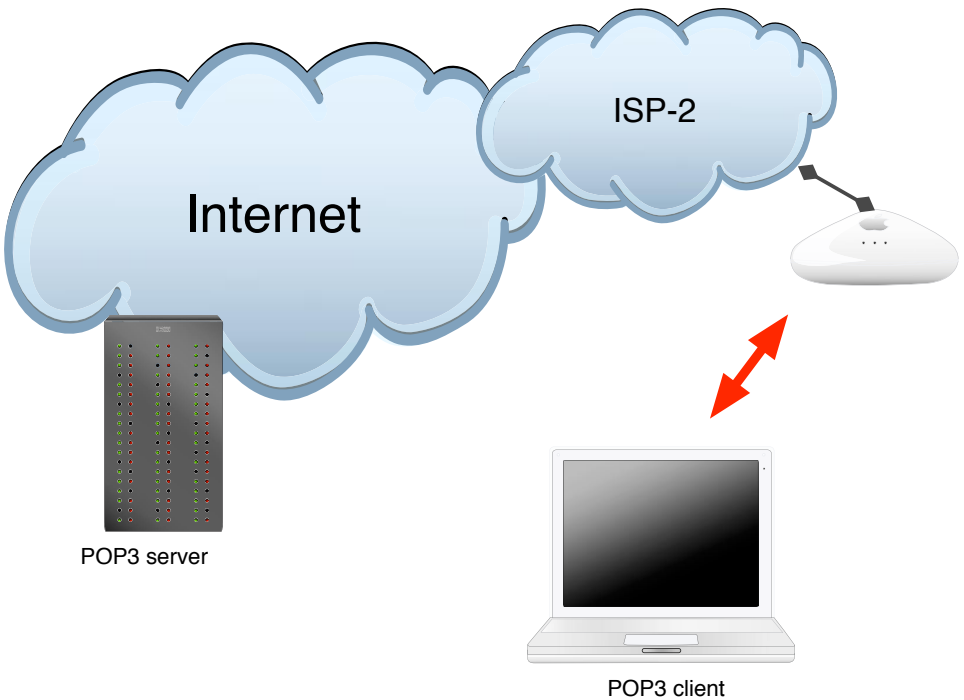
Jeg bruger selv IMAPS, IMAP over SSL kryptering - idet kodeord ellers sendes i klartekst

POP3 i Danmark



Man har tillid til sin ISP - der administrerer såvel net som server

POP3 i Danmark - trådløst



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

Deler man et netværksmedium med andre?

Brug de rigtige protokoller!