Introductie

Wie zijn wij?

- Rens Sikma
- Thomas Brasser

Wat doet AT Computing?

- Linux en Open-Source opleider sinds 1985
- Consultancy en Detachering
- Sinds 3 jaar onderdeel van de Vijfhart Groep

  www.atcomputing.nl

Je vind de opdrachten en bestanden op:
https://github.com/atcomputing/itvitae

Introductie

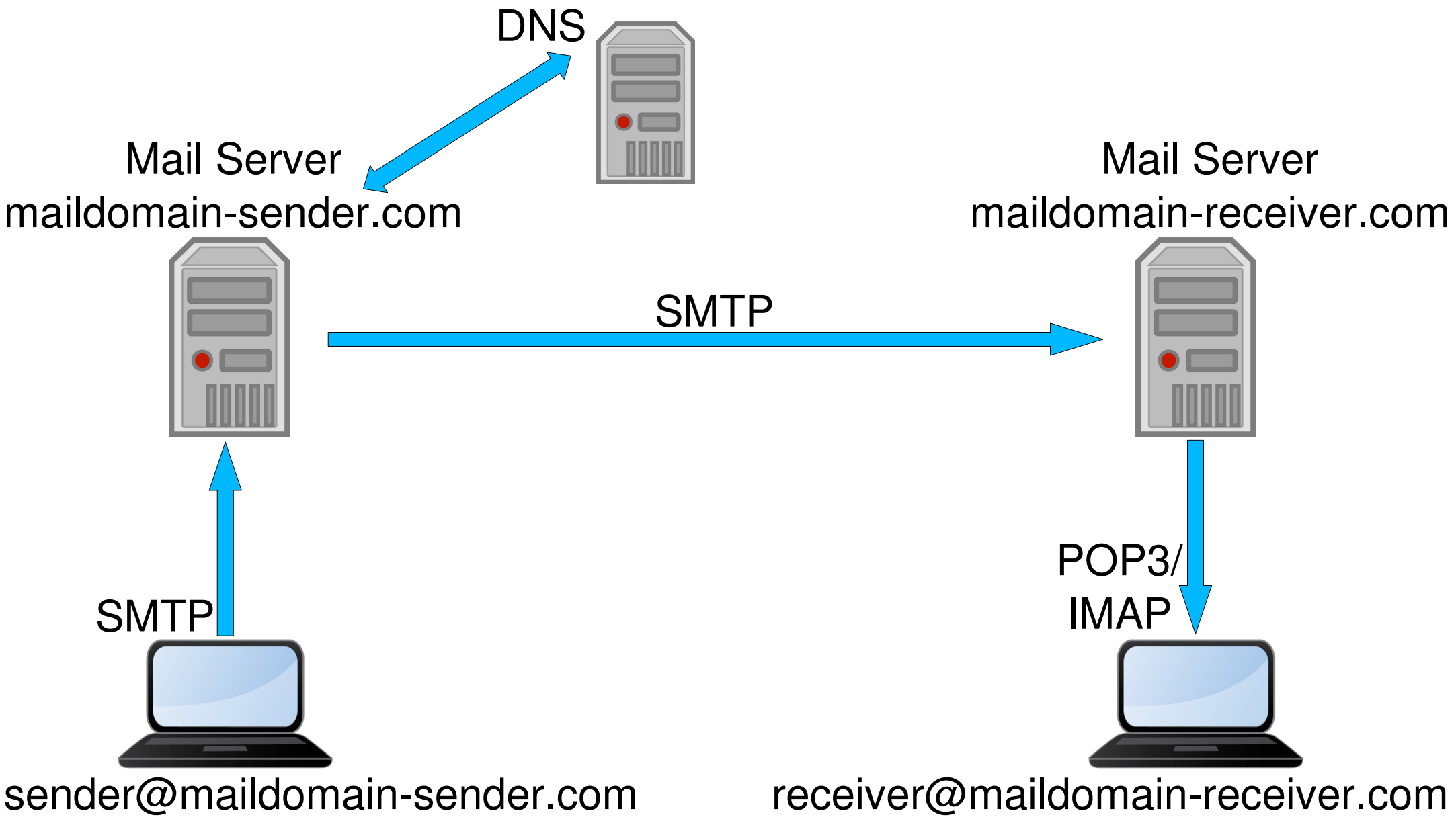
Onderwerpen / Planning

- Ochtenddeel
  - Email – Algemeen
  - Authenticatie
  - DNS
    - Opdracht 1
- Lunch
- Middagdeel
  - TCPDump
  - Email – SMTP
    - Opdracht 2
  - Netcat
    - Opdracht 3
  - Email – Spoofing
    - Eindopdracht

Email – Algemeen

- hoe oud is email?
- weinig ontwikkelingen protocol
- nieuwe features zijn optioneel en worden niet overal gebruikt

Email – Architectuur

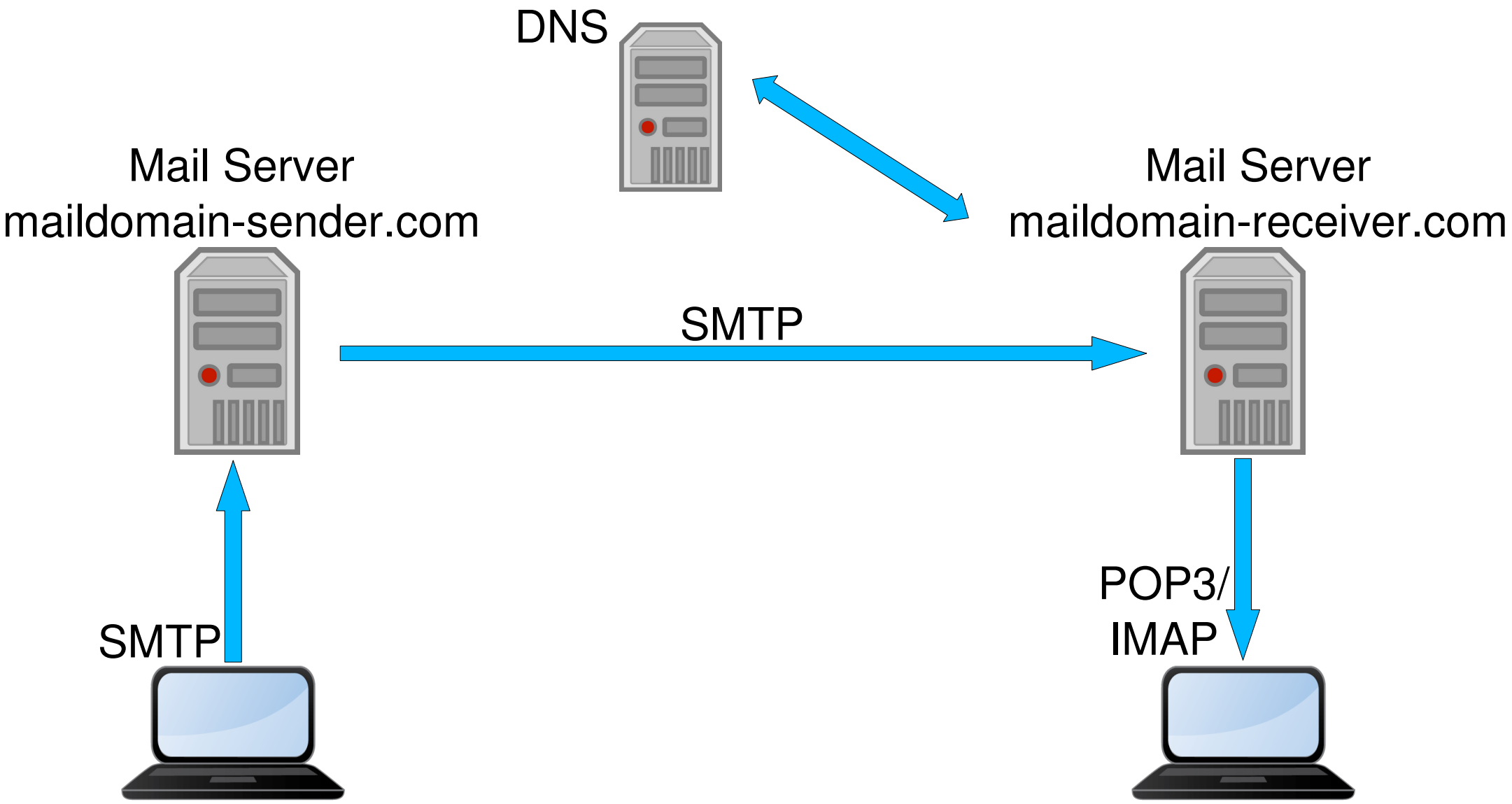


DNS – Domain Name System

- hierarchisch systeem

- A/AAA/CNAME records verwijzen web adressen naar webservers
- MX records verwijzen emailadressen naar mailservers
- TXT records bieden ruimte aan SPF en andere beveiligingsmaatregelen

Email – SPF


DNS
Mail Server
maildomain-sender.com
Mail Server
maildomain-receiver.com
SMTP
SMTP
POP3/
IMAP
sender@maildomain-sender.com
receiver@maildomain-receiver.com

DIG – DNS Tool

DNS Record lookup: commando **dig**

- vraag MX records op

```
$ dig outlook.com mx
....
;; ANSWER SECTION:
outlook.com.        299  IN   MX   5 outlook-com.olc.protection.outlook.com.
...
```

- vraag TXT records op

```
$ dig outlook.com txt
....
;; ANSWER SECTION:
outlook.com.        64   IN   TXT  "v=spf1 include:spf-a.outlook.com include:spf-b.outlook.com
ip4:157.55.9.128/25 include:spf.protection.outlook.com include:spf-a.hotmail.com include:_spf-ssg-
b.microsoft.com include:_spf-ssg-c.microsoft.com ~all"
outlook.com.        64   IN   TXT  "google-site-verification=0iLWhIMhXEkeWwWfFU4ursTn-_OvoOjaA0Lr7Pg1sEM"
outlook.com.        64   IN   TXT  "google-site-verification=DC2uC-T8kD33lINhNzfo0bNBrw-vrCXs5BPF5BXY56g"
....
```

Linux Netwerk Debug Tools

- welke programma's luisteren op een netwerk poort?

  ss (netstat, lsof)
- kan ik een tcp/http connectie maken?

  netcat (telnet,curl, openssl,curl,nmap)
- komen mijn pakketten aan / wat wordt er verzonden en ontvangen.

  tcpdump (wireshark, tcpflow, ngrep, ...)

TCPDump

waarom tcpdump: staat vaak geïnstalleerd, geen gui nodig

```
$ man tcpdump
# tcpdump -i eth0 -nn -A not port 22
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:11:15.045833 IP 192.168.30.25.42034 > 173.194.69.139.80: Flags [S], .... , length 0
E..<.A@.@..k......E..2.P.............m............4........
12:11:15.062346 IP 173.194.69.139.80 > 192.168.30.25.42034: Flags [S.], seq 1586098358, ack
2293432598, win 62392, options [mss 1430,sackOK,TS val 3516341257 ecr 2803022644,nop,wscale 8],
length 0
E..<`(..j.....E......P.2^.............................4....
12:11:15.062412 IP 192.168.30.25.42034 > 173.194.69.139.80: Flags [.], ack 1, win 502, options
[nop,nop,TS val 2803022661 ecr 3516341257], length 0
E..4.B@.@..r......E..2.P....^........1........E...
12:11:15.062502 IP 192.168.30.25.42034 > 173.194.69.139.80: Flags [P.], seq 1:75, ack 1, win 502,
options [nop,nop,TS val 2803022661 ecr 3516341257], length 74: HTTP: GET / HTTP/1.1
E..~.C@.@..'......E..2.P....^..................E... GET / HTTP/1.1
Host: google.com
User-Agent: curl/7.68.0
Accept: */*
```

Email – SMTP

```
S: 220 smtp.example.com ESMTP Postfix
C: EHLO relay.example.com
S: 250 smtp.example.com, I am glad to meet you
C: MAIL FROM:<bob@example.com>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.com>
C: To: Alice Example <alice@example.com>
C:
C: Je bericht.
C: .
S: 250 Ok: queued as 12345
C: QUIT
```

Netcat

Cat voor netwerken

- testen of er een (tcp/udp) connectie gemaakt kan worden:

```
$ echo test | ncat -v host 8000
```

```
$ ncat -lv 8000
test
```

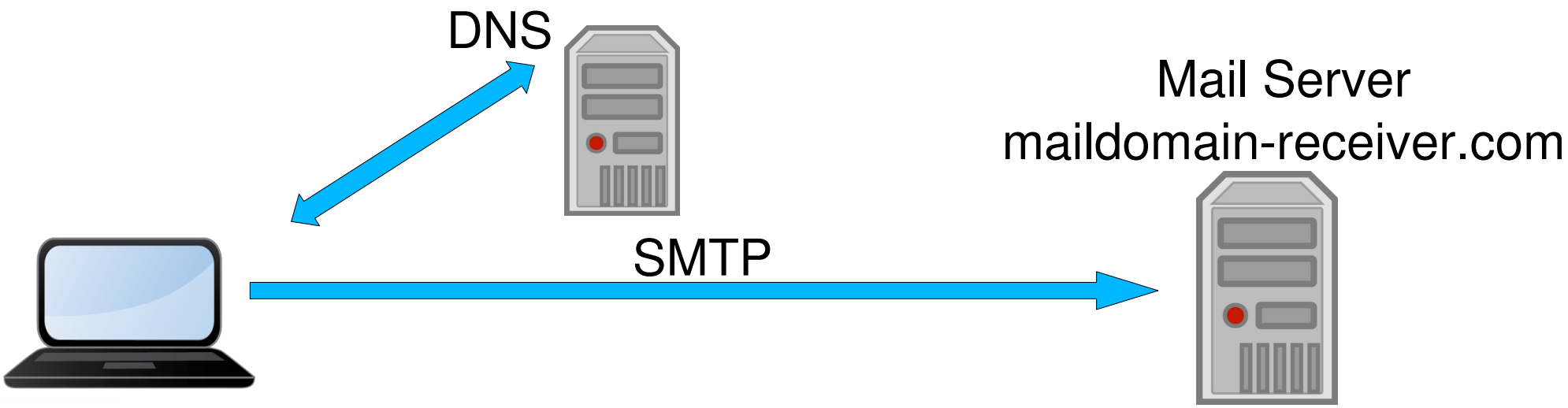
- handmatig (tcp/udp) connecties maken:

```
$ ncat -Cv www.google.com 80 << EOF
GET /index.html HTTP\1.0
Host: www.google.com

EOF
```

- meerdere implementaties in omloop; GNU, BSD (nc), Nmap (ncat)

Email – Spoofing



Email Spoofing: spamming, (spear) phishing, Testing.

- vind adres ontvangende mail server,
  via MX record
- kies as wie je de mail wil spoofen.
  controleer of het geen streng spf record heeft
- Praat smtp met de server,
  en spoof evelop sender, From, To

Einde

“Zoek de wachtwoorden” puzzel:
https://www.atcomputing.nl/puzzelen-maar/