Welcome to

11. DNS and Email Security

Communication and Network Security 2020

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

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

Goals for today

Todays goals:

- Talk about DNS and email standards
- We already discussed DNSSEC
- Try running DNS servers!

Trying to make today less heavy with information.

Plan for today

Subjects
- DNS introduction
- SMTP introduction
- SMTP TLS
- SPF, DKIM, DMARC
- DNSSEC - DNS integrity
- DNS over TLS vs DNS over HTTPS - DNS encryption
  Exercises

Exercises
- Check some examples like how danish banks are using DMARC, and how your own companies can start using it
- SSLscan with SMTP TLS
- Run a DNS server Unbound

Reading Summary

Re-read PPA DNS pages 173-183

`https://en.wikipedia.org/wiki/Sender_Policy_Framework`

`https://en.wikipedia.org/wiki/DMARC`

`https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail`

ANSM chapter 14,15 - 66 pages

Fokus 2020: DNS og email

- Vi er afhængige af email, modtagelse og afsendelse
- Når vi modtager skal det helst gå hurtigt
- Når vi sender skal vi ikke ende i spam mappen
- Phishing, hvem kan sende *fra vores domæne*

Various key attack types, clients and employees

- Phishing - sending fake emails, to collect credentials
- Spear phishing - targetted attacks
- Person in the middle - sniffing and changing data in transit
- Drive-by attacks - web pages infected with malware, often ad servers
- Malware transferred via USB or email
- Credential Stuffing, Password related, like re-use of password, see slide about being pwned

If we all wait a bit, and not click links immediately

Hackers try to create "urgency", click this or loose money

Well-known port numbers

IANA vedligeholder en liste over magiske konstanter i IP

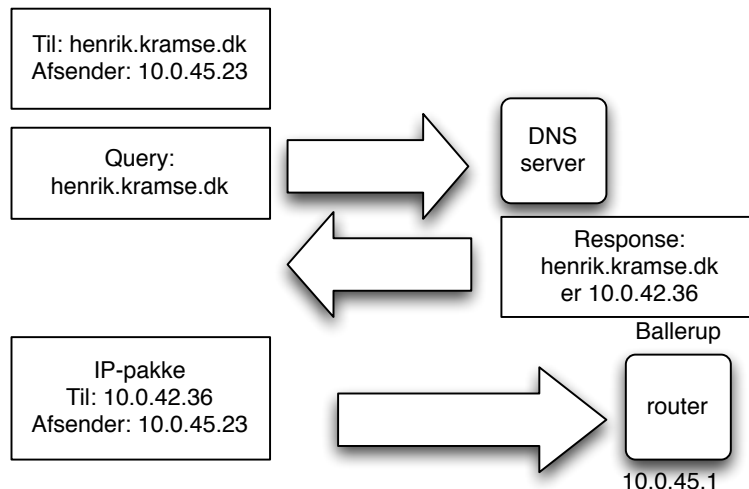De har lister med hvilke protokoller har hvilke protokol ID m.v.

En liste af interesse er port numre, hvor et par eksempler er:

- Port 25 SMTP Simple Mail Transfer Protocol
- Port 53 DNS Domain Name System
- Port 80 HTTP Hyper Text Transfer Protocol over TLS/SSL
- Port 443 HTTP over TLS/SSL

Se flere på `http://www.iana.org`

Domain Name System

Gennem DHCP får man typisk også information om DNS servere

En DNS server kan slå navne, domæner og adresser op

Foregår via query og response med datatyper kaldet resource records

DNS er en distribueret database, så opslag kan resultere i flere opslag

DNS systemet

navneopslag på Internet

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.zencurity.com har adressen 185.129.60.130

skrives i database filer, zone filer

```
ns1     IN      A       185.129.60.130
        IN      AAAA    2a06:d380:0:3065::53
www     IN      A       185.129.60.130
        IN      AAAA    2a06:d380:0:3065::80
```

DNS er 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.zencurity.dk.
IN      MX      20      mail2.zencurity.dk.
```

Basal DNS opsætning

```
domain zencurity.net
nameserver 91.239.100.100
nameserver 2001:67c:28a4::
nameserver 89.233.43.71
nameserver 2a01:3a0:53:53::
```

`/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

De viste servere er fra censurfridns.dk og kan benyttes frit

DNS root servere

As of 2019-01-29, the root server system consists of 933 instances operated by the 12 independent root server operators.

http://root-servers.org/

DK-hostmaster

bestyrer .dk TLD - top level domain

man registrerer ikke .dk-domæner hos DK-hostmaster, men hos en registrator

Et domæne bør have flere navneservere og flere postservere

autoritativ navneserver - ved autoritativt om IP-adresse for maskine.domæne.dk findes

ikke-autoritativ - har på vegne af en klient slået en adresse op

Det anbefales at overveje en service som `http://www.gratisdns.dk` der har flere navneservere distribueret over stor geografisk afstand

www.zencurity.com

hlk@zencurity.com

DNS AAAA record tilføjes

```
www     IN A    91.102.91.17
        IN AAAA 2001:16d8:ff00:12f::2


mail.zencurity.com has address 91.102.91.22
mail.zencurity.com has IPv6 address 2a02:9d0:3000:1::216
```

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

- Biblen omkring DNS og BIND er:
  DNS and BIND, Paul Albitz & Cricket Liu, O'Reilly, 5th edition Maj 2006

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;    };
...
}
```

BIND is still used a lot, but I recommend Unbound for recursive servers, and outsourcing authoritative DNS

Unbound and NSD

Unbound is a validating, recursive, caching DNS resolver. It is designed to be fast and lean and incorporates modern features based on open standards.

To help increase online privacy, Unbound supports DNS-over-TLS which allows clients to encrypt their communication. In addition, it supports various modern standards that limit the amount of data exchanged with authoritative servers.

```
https://www.nlnetlabs.nl/projects/unbound/about/
```

My preferred local DNS server. We will now stop and look at this configuration file and function.

Also check out uncensored DNS and his DNS over TLS setup!

Even has pinning information available:

```
https://blog.censurfridns.dk/blog/32-dns-over-tls-pinning-information-for-unicastcensurfridnsdk/
```

Exercise

Now lets do the exercise

Test a DNS server 30min

which is number **58** 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
- http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

e-mail servere

Example software Sendmail og Postfix

- Sendmail - den ældste
- Postfix en modulært og sikkerhedsmæssigt god e-mail server
  er ligeledes nem at konfigurere

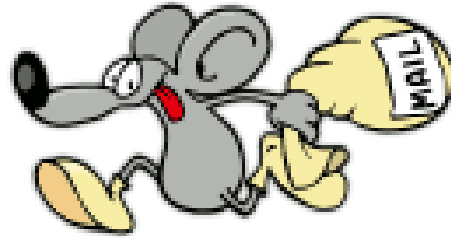Dertil kommer diverse andre mailservere:

Microsoft Exchange på Windows servere

Related software Roundcube, Dovecot IMAP server, Thunderbird, etc.

also need anti-spam solutions

I use Spamhaus lists, `https://www.spamhaus.org/`

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
```

Skal ikke tillade relaying

Idag benyttes ofte en stjålet brugerkonto med brugernavn og kodeord til at sende spam.

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

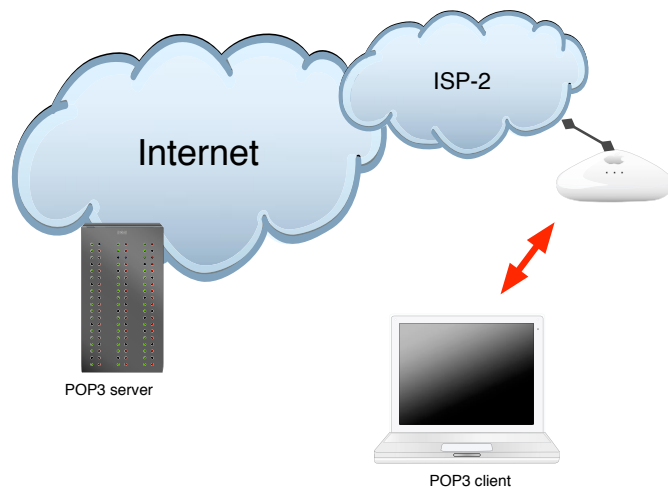IMAP er bedst hvis du vil tilgå din post fra flere systemer

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

POP3 server

ISP

Internet

POP3 client
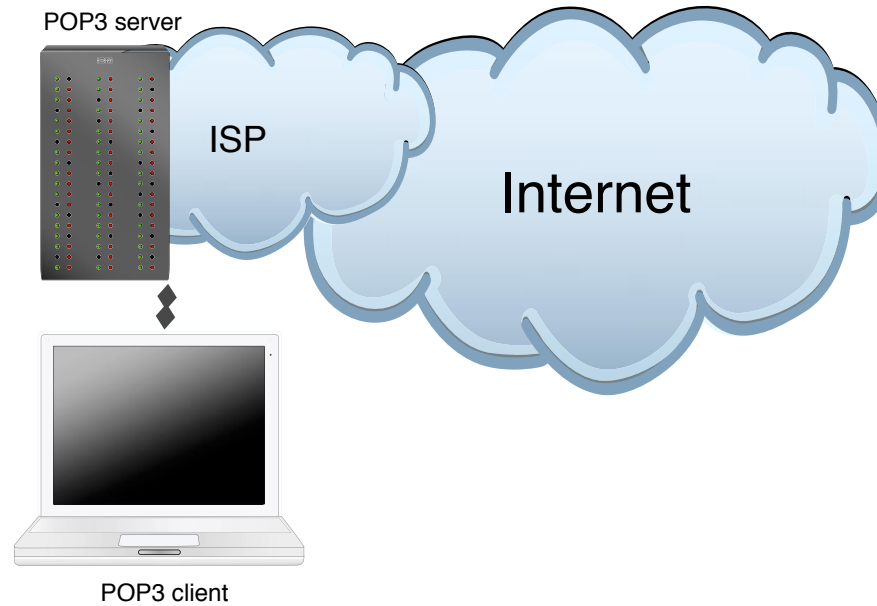
Man har tillid til sin ISP - der administrerer såvel net som server

POP3 i Danmark - trådløst

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

Deler man et netværksmedium med andre?

Brug de rigtige protokoller! IMAPS SMTPTLS

The STARTTLS command for IMAP and POP3 is defined in RFC 2595, for SMTP in RFC 3207, for XMPP in RFC 6120 and for NNTP in RFC 4642. For IRC, the IRCv3 Working Group has defined the STARTTLS extension. FTP uses the command "AUTH TLS"defined in RFC 4217 and LDAP defines a protocol extension OID in RFC 2830. HTTP uses upgrade header.

SMTP was extended with support for Transport Layer Security TLS

Also called **Opportunistic TLS**, where the quote is also from:

`https://en.wikipedia.org/wiki/Opportunistic_TLS`

DNSSEC DNS integrity
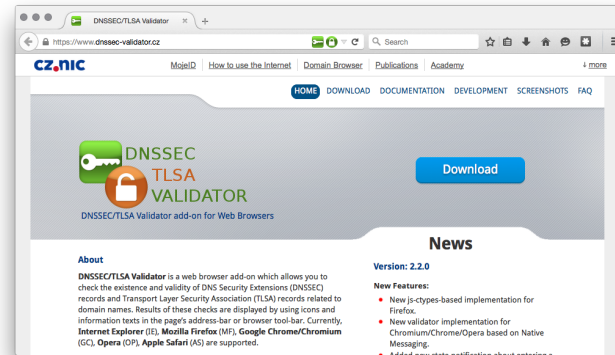
"TLSA records store hashes of remote server TLS/SSL certificates. The authenticity of a TLS/SSL certificate for a domain name is verified by DANE protocol (RFC 6698). DNSSEC and TLSA validation results are displayer by using several icons."

DNSSEC is something you should enable ASAP where possible

DNSSEC

DNSSEC nøgle(r)				(Bruger-id: DKHM1-DK)
Domænenavn ▾	Nøgle-ID	Algoritme	Hashingalgoritme	Hash
☐ net.dk	9880	RSASHA256	SHA-1	🔑
☐ net.dk	9880	RSASHA256	SHA-256	🔑

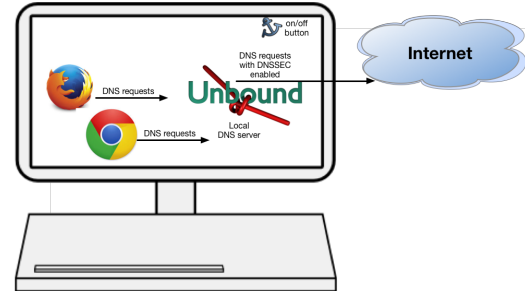Slet nøgle | Opret nøgle

Tilbage til Selvbetjeningens forside

DNSSEC - nu ogs<E5> i Danmark

Du kan sikre dit domæne med DNSSEC - wooohooo!

Det betyder en tillid til DNS som muliggør alskens services.

Kilde:

https://www.dk-hostmaster.dk/english/tech-notes/dnssec/

DNSSEC trigger

Der findes mange DNSSEC programmer, blandt andet DNSSEC-trigger som er en navneserver til din lokale PC

- DNSSEC Validator for firefox
  `https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/`
- OARC tools `https://www.dns-oarc.net/oarc/services/odvr`
- `http://www.nlnetlabs.nl/projects/dnssec-trigger/`

DNSSEC and DANE

"Objective:

Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name."

DNS-based Authentication of Named Entities (dane)

SPF, DKIM, DMARC

- SPF Sender Policy Framework - which IPs can send for my domain

  `https://en.wikipedia.org/wiki/Sender_Policy_Framework`

- DKIM DomainKeys Identified Mail - when sending we use these keys

  `https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail`

- DMARC Domain-based Message Authentication, Reporting and Conformance

  `https://en.wikipedia.org/wiki/DMARC`

  Who tried sending spam which does not match our SPF and DKIM, tell us!

- DANE DNS-based Authentication of Named Entities

  `https://en.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities`

  Put everything in DNS and secure it with DNSSEC

- Brug allesammen, check efter ændringer!

Email security 2020- Goals

DNS problems

The Domain Name System (DNS) [32][33] provides for a distributed database mapping host names to IP addresses. An intruder who interferes with the proper operation of the DNS can mount a variety of attacks, including denial of service and password collection. There are a number of vulnerabilities.

We have a lot of the same problems in DNS today

Plus some more caused by middle-boxes, NAT, DNS size, DNS inspection

- DNS must allow both UDP and TCP port 53
- Your DNS servers must have updated software, see DNS flag day
  https://dnsflagday.net/ after which kludges will be REMOVED!
- DNS is unencrypted

DNS attacks, Your registrar

26 **Webnic Registrar Blamed for Hijack of Lenovo,**
FEB 15 **Google Domains**

Two days ago, attackers allegedly associated with the fame-seeking group **Lizard Squad**
briefly hijacked Google's Vietnam domain (google.com.vn). On Wednesday, **Lenovo.com**
was similarly attacked. Sources now tell KrebsOnSecurity that both hijacks were possible
because the attackers seized control over **Webnic.cc**, the Malaysian registrar that serves
both domains and 600,000 others.

DNS insecurity has huge impact on your security!

Most are denial of service, by may create Mitm or confidentiality concerns

Select DNS providers with care

Sources:

https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/

http://www.version2.dk/artikel/google-og-lenovo-defaced-som-foelge-af-overset-sikkerhedsproblemstilling-91295

DNS over TLS vs DNS over HTTPS - DNS encryption

- Protocols exist that encrypt DNS data, like dnscrypt which is not RFC standard `https://dnscrypt.info/` `https://en.wikipedia.org/wiki/DNSCrypt`
- Today we have competing standards:
- *Specification for DNS over Transport Layer Security (TLS)* (DoT), RFC 7858 MAY 2016 `https://en.wikipedia.org/wiki/DNS_over_TLS`
- *DNS Queries over HTTPS (DoH)* RFC 8484
- How to cofigure DoT `https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients`

sslscan - can do STARTTLS with SMTP too

```
$ sslscan --starttls-smtp mail.kramse.org
Connected to 91.102.91.22
Testing SSL server mail.kramse.org on port 25 using SNI name mail.kramse.org
...
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 2048 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  DHE-RSA-CHACHA20-POLY1305     DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA256    DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA       DHE 2048 bits
...
Subject:  mail.kramse.org
Altnames: DNS:mail.kramse.org
Issuer:   Let's Encrypt Authority X3
Not valid before: Mar 24 15:05:20 2020 GMT
Not valid after:  Jun 22 15:05:20 2020 GMT
```

Source: Originally sslscan from http://www.titania.co.uk but use the version on Kali

For Next Time

Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools