Welcome to

Email Security - domains, clients and servers

2020

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

email-security-2020.tex in the repo security-courses

Goal for today

This presentation will be focused on email security overall - from domains to clients to servers. The presentation will include a lot of acronyms and some technical details, the goal though is to get an overview of available technologies and their benefits.

- Plan:
- Approx 4h, with breaks
- Inspiration for solving the tasks, prioritizing the tasks
- I dont have tailer made solutions or easy answers for your organisation

Todays Agenda - approximate time plan

- 17:00 - 18:15 Part I: Client Security and Email Threats
- 30min Break - eat, drink and socialize
- 18:45 - 19:30 Part II: Basic Email Services
- 15min break
- 19:45 - 20:15 Part III: Testing Email Services
- 15min break
- 20:30 - 21:00 Part IV: Strategy for Your Email Security

Please help me keep the time, thank you ☺

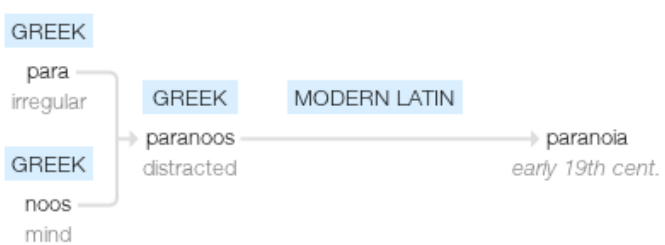
Paranoia defined

par·a·noi·a
/ˌparəˈnoiə/

noun
noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.
   synonyms: persecution complex, delusions, obsession, psychosis More
- suspicion and mistrust of people or their actions without evidence or justification.
  "the global paranoia about hackers and viruses"

Origin



More

Source: google paranoia definition

Hackers don’t give a shit

Your system is only for testing, development, ...

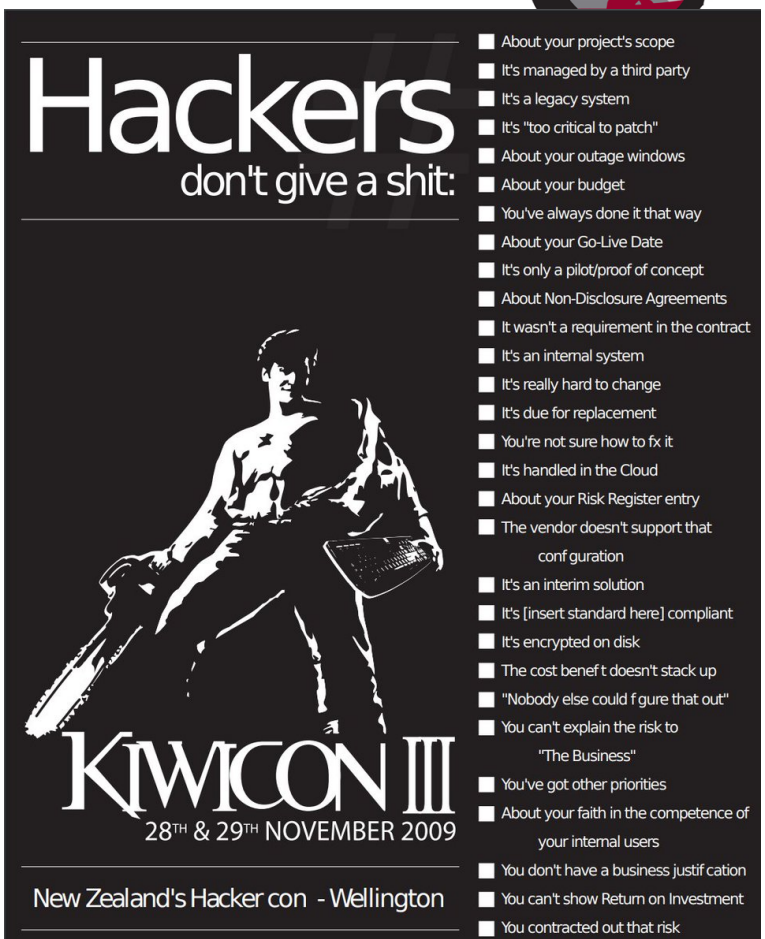
Your network is a research network, under construction, being phased out, ...

Try something new, go to your management

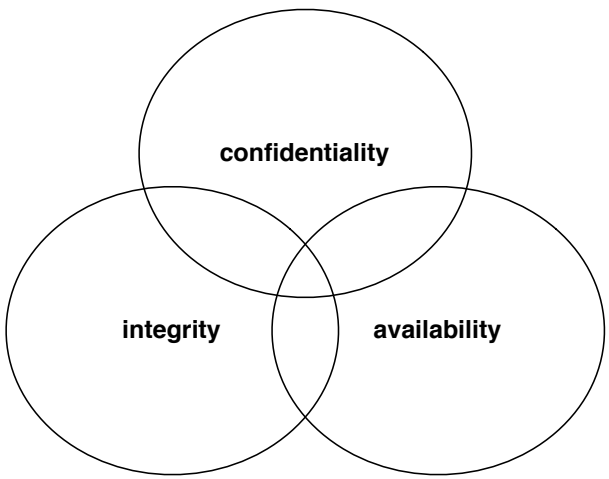
Bring all the exceptions, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

Ask for permission to go full monty on your security

Think like attackers - don’t hold back



Confidentiality Integrity Availability



We want to protect something

Confidentiality - data is kept confidential, secrets are secrets

Integrity - data is not subjected to unauthorized changes

Availability - data and systems are available for authorized users when they need it

Overlapping Security Incidents

New data breaches nearly every week, these from danish news site `version2.dk`

Problem, we need to receive data from others

Data from others may contain malware

Have a job posting, yes
- then HR will be expecting CVs sent as .doc and .pdf files

Part I: Client Security and Email Threats

We will discuss client features which are considered dangerous, loading images automatically etc. and how to improve your client security by using only specific protocols with encryption.

Attacking 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

Attacking Email

- 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

The Internet Worm 2. nov 1988

Exploited the following vulnerabilities

- buffer overflow in fingerd - VAX code
- Sendmail - DEBUG functionality
- Trust between systems: rsh, rexec, ...
- Bad passwords

Contained camouflage!

- Program name set to 'sh'
- Used fork() to switch PID regularly
- Password cracking using intern list of 432 words and /usr/dict/words
- Found systems to infect in /etc/hosts.equiv, .rhosts, .forward, netstat ...

Made byRobert T. Morris, Jr.

Computer Viruses

Definition 23-4 A *computer virus* is a program that inserts (a possibly transformed version of) itself into one or more files and then performs some (possibly null) action.

Would spread through floppy disks and boot sector

Today more virus are spread through network shares, networked file systems

- Boot sector virus - when booting a PC infects
- A executable - exe files, similar types on PC platform .scr screensavers, .vbs visual basic scripts etc. Linux shell archives shar files.
- Data - macro virus, found in Microsoft Office formats .doc etc.

Polymorphic virus change their fingerprint/code during execution/infection

Definition from *Computer Security: Art and Science*, 2nd ed, Matt Bishop, 2019

Computer worms

Definition 23-14 A *computer worm* is a program that copies itself from one computer to another.

Definition from *Computer Security: Art and Science*, 2nd ed, Matt Bishop, 2019

Computer worms has existed since research began mid-1970s

Morris Worm from November 2, 1988 was a famous example

ILOVEYOU worm from May 2000 written in Visual Basic was another

Virus, trojan or worm?

Unless you work specifically in the computer virus industry, call it all malware

Trojan horses

Definition 23-1 *Malicious logic*, more commonly called *malware*, is a set of instructions that cause a site's security policy to be violated.

Definition 23-2 A *Trojan horse* is a program with an overt (documented or known) purpose and a covert (undocumented or unexpected) purpose.

Definitions from *Computer Security: Art and Science*, 2nd ed, Matt Bishop, 2019

Book also mentions the Ken Thompson example with login program and compiler
Insert Login backdoor, by inserting backdoor to notice when compiling compiler ☺

Lots of free applications on Android have been trojans, for example stealing data

The history lesson `https://en.wikipedia.org/wiki/Trojan_Horse`
`https://en.wikipedia.org/wiki/Trojan_horse_(computing)`

Ransomware

Defition 23-21 *Ransomware* is malware that inhibits the use of resources until a ransom usually monetary, is paid.

Definition from *Computer Security: Art and Science*, 2nd ed, Matt Bishop, 2019

Book also mentions 1989 example, PC CYBORG targetting PC/DOS computers

Uses cryptography to render data unreadable

Has become a huge problem for enterprises during the last 5-10 years

Often uses crypto-currencies today, like BitCoin (BTC) for payment

Often contains errors so decryption is impossible, or possible without payment!

Phishing and spear phishing

Definition 23-22 *Phishing* is the act of impersonating a legitimate entity, typically a website associated with a business, in order to obtain information such as passwords, credit card numbers, and other private information without authorization

Example creating a fake bank website and make customers try to login

Definition 23-23 *Spearphishing* is a phishing attack tailored for a particular victim.

Definitions from *Computer Security: Art and Science*, 2nd ed, Matt Bishop, 2019

Spear phishing – targeted attacks

Spearphishing - targeted attacks directed at specific individuals or companies

- Use 0-day vulnerabilities only in a few places
- Create backdoors and mangle them until not recognized by Anti-virus software
- Research and send to those most likely to activate program, open file, visit page
- Stuxnet is an example of a targeted attack using multiple 0-day vulns

A lot of threats are delivered through email or links sent via email

also, we haven't solved email security problems in +30 years, and probably never will

Malware defenses

Theorem 23.2 It is undecidable whether an arbitrary program contains a malicious logic.

Scanning defenses,

- Check disk and memory for known bad malware signatures
- Check for changes - integrity protection

Behavioural - what does a malware do, that normal programs dont

Static analysis - what does a program normally do, what actions does malware do

Containment - change the environment to be more restricted

Theorem from *Computer Security: Art and Science*, 2nd ed, Matt Bishop, 2019

I dont trust or use anti-virus programs, fight me

Vulnerabilities in popular mail programs

- They load pictures from the internet, enables tracking bugs
  Disable as many features as possible, use a firewall
- Show HTML, run JavaScript, run in browsers often - XSS Cross-site scripting
  Decide if you trust browser or email client
- Send headers with their specific version, enabling better buffer overflow attacks
  Disable in mail client, and update often
  All software has vulnerabilities
- Reveal IP - by connecting to server directly over internet
  Only countermeasure might be to use VPN or Tor unless you run your own mail server
- Allow cleartext authentication and sending, enabling snooping
  Check your settings for using encrypting protocols TLS/STARTTLS
- Also marks emails with sending date and time
  How paranoid are you? Cases in Denmark regarding Snowden plane was *interesting*

Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) is a communication protocol for electronic mail transmission. As an Internet standard, SMTP was first defined in 1982 by RFC 821, and updated in 2008 by RFC 5321 to Extended SMTP additions, which is the protocol variety in widespread use today. Mail servers and other message transfer agents use SMTP to send and receive mail messages.

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

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

Internet Message Access Protocol (IMAP)

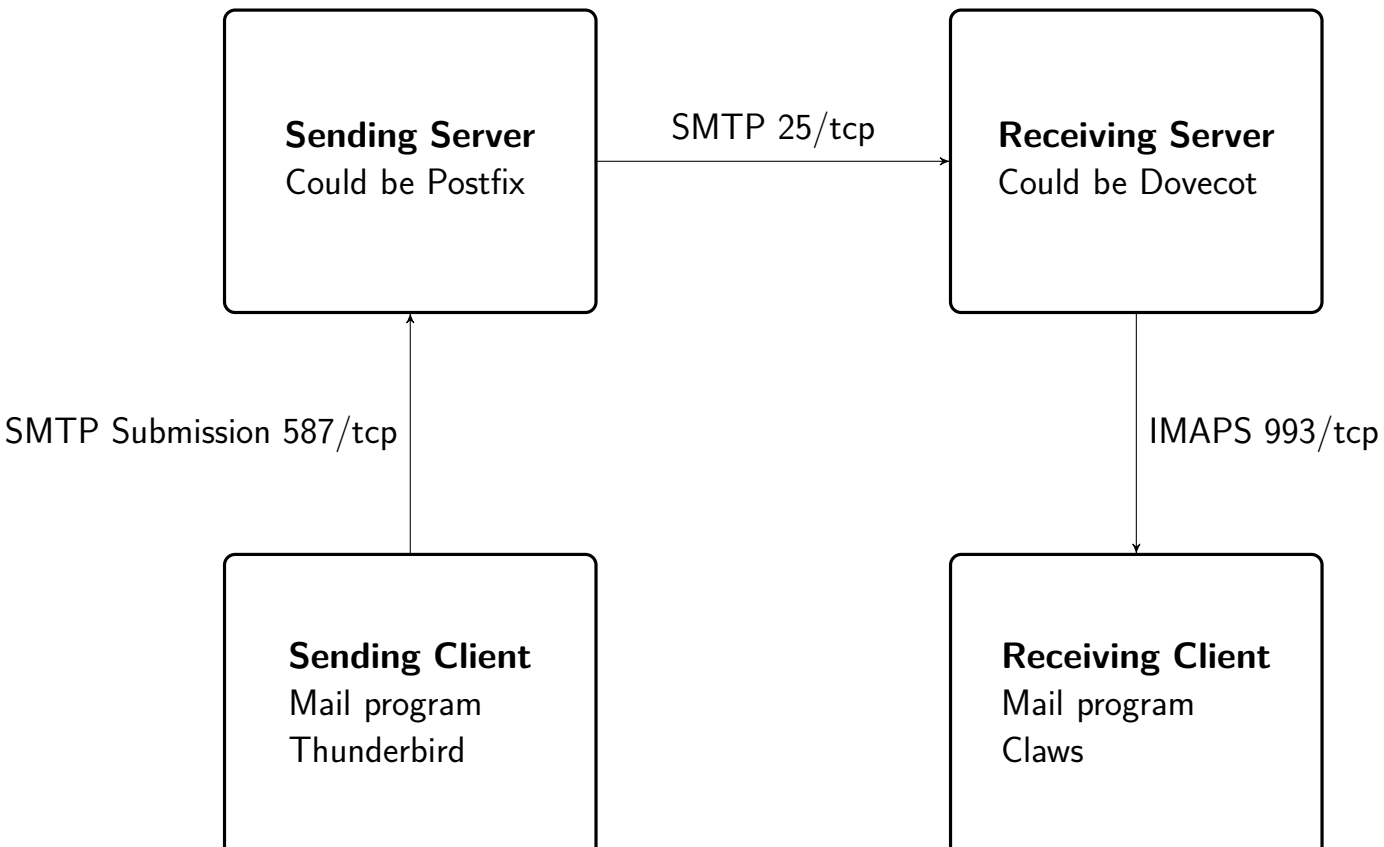
In computing, the Internet Message Access Protocol (IMAP) is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection.[1] IMAP is defined by RFC 3501.

IMAP was designed with the goal of permitting complete management of an email box by multiple email clients, therefore clients generally leave messages on the server until the user explicitly deletes them. An IMAP server typically listens on port number 143. IMAP over SSL (IMAPS) is assigned the port number 993.

Virtually all modern e-mail clients and servers support IMAP, which along with the earlier POP3 (Post Office Protocol) are the two most prevalent standard protocols for email retrieval.[2] Many webmail service providers such as Gmail, Outlook.com and Yahoo! Mail also provide support for both IMAP and POP3.

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

Example of SMTP and IMAP

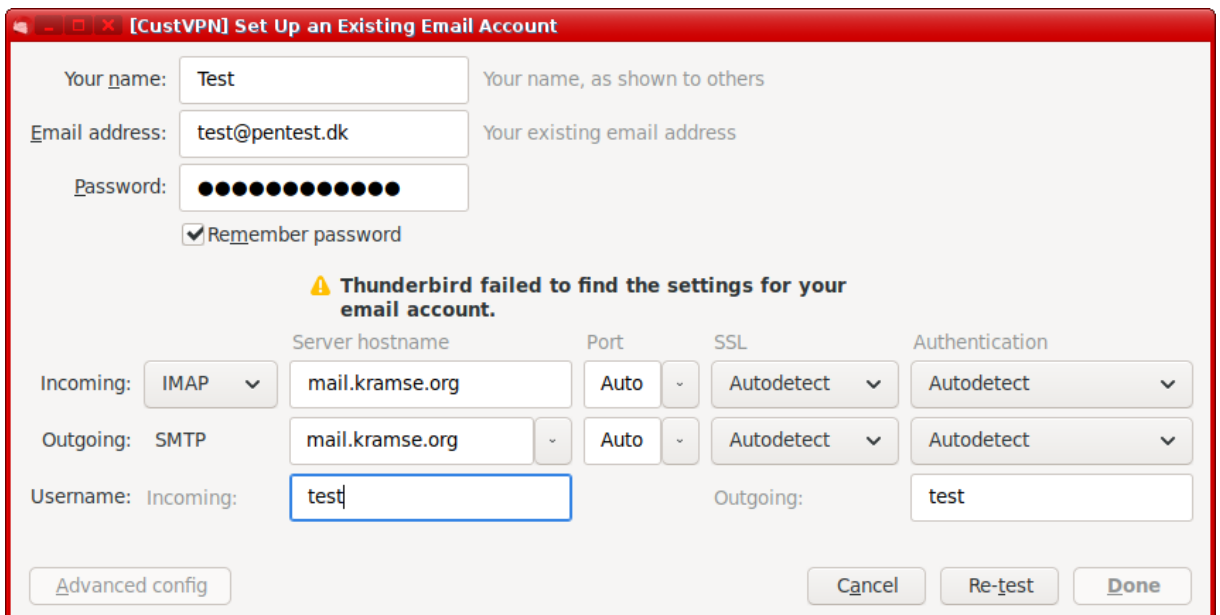


Securing Your Email Client

- Security settings
- Use TLS for SMTP
- Use TLS for IMAPS
- Disable loading of remote content, images, HTML parts, content, bugs, tracking
- Disable sending version strings
- Add plugins you need, but only those!

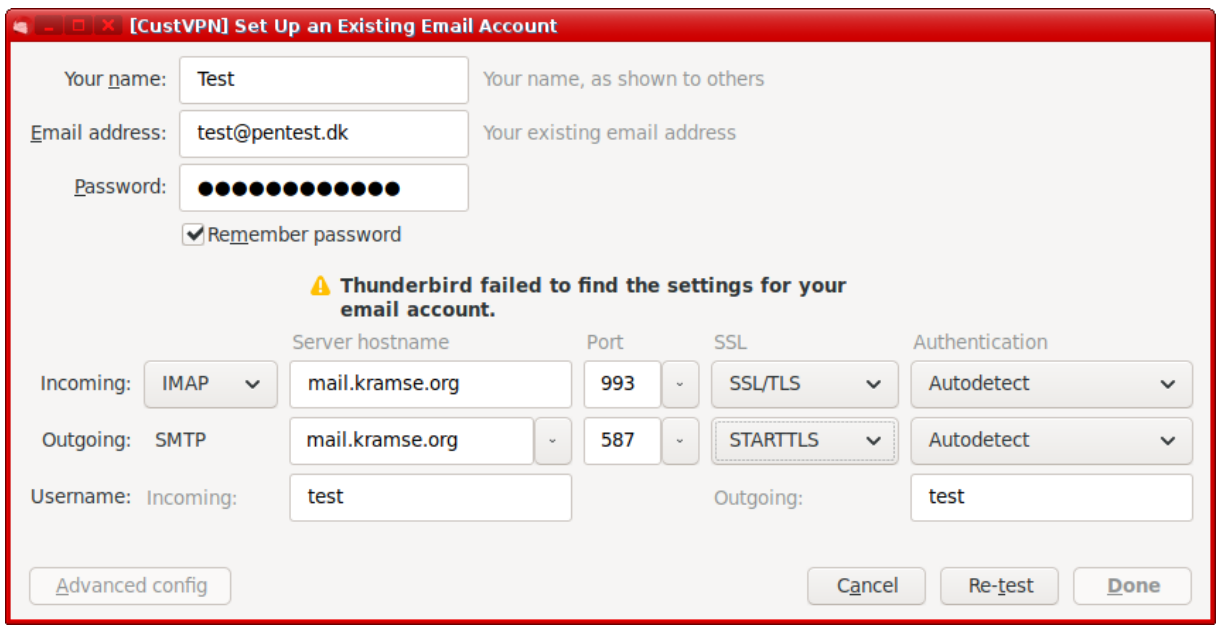
Thunderbird mentioned as being one of the most popular email clients

Thunderbird Default Port Settings



By default Thunderbird will try to probe settings, which is fine

Thunderbird Chosen Port Settings



I prefer to fix the ports to my known ports. Here running on default ports 993/tcp and 587/tcp

Inside an email – headers

```
Return-Path: <hkj@zencurity.com>
X-Original-To: test@pentest.dk
Delivered-To: test@kramse.org
Received: from localhost (unknown [94.18.243.144])
(using  TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
(No client certificate requested)
by mail.kramse.org ( Postfix) with ESMTPSA id 95958393EF
for <test@pentest.dk>; Tue, 10 Mar 2020 15:05:05 +0100 (CET)
Date: Tue, 10 Mar 2020 15:05:03 +0100
From: Henrik Kramselund Jereminsen <hkj@zencurity.com>
To: test@pentest.dk
Subject: Claws to Thunderbird
Message-ID: <20200310150503.7432a7a1@zencurity.com>
Organization: Zencurity Aps
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

--=20
Mvh/Best regards

Henrik
```

Thunderbird Default header User-Agent

```
To: hlk@kramse.org
From: Test <test@pentest.dk>
Subject: test headers
Message-ID: <25d9b367-872e-2858-b1ad-5c19a418bc54@pentest.dk>
Date: Tue, 10 Mar 2020 15:11:02 +0100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
 Thunderbird/68.5.0
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 7bit
Content-Language: en-US

Almost empty email
```

So an attacker can now wait for a vulnerability in this *specific version* and *specific operating system* – Linux

CVE Details – All software has errors!

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2004	13		4	2							1				
2005	13	2	4	3	1					3	1				
2006	65	24	37	13	9		6			6	2	3			
2007	16	8	10	6	6		1								
2008	50	20	20	7	6		7	3		11	4				
2009	39	23	19	1	20		3			3	2				1
2010	61	23	40	18	19		5			5	6	2			6
2011	68	39	44	12	29		1	1	1	11	8	3			
2012	148	68	99	26	58		18			11	9	3	1		
2013	113	55	83	32	39		7			8	5	7	1		1
2014	64	31	37	14	16		3			9	10	1			
2015	30	12	15	9	9					4	3	1	2		
2016	13	12	9	7	4						2	1			
2018	175	1	1	48	25		2			10	15		1		
2019	53		1	12	6		2			2	4		1		
Total	921	318	423	210	247		55	4	1	83	72	21	6		8
% Of All		34.5	45.9	22.8	26.8	0.0	6.0	0.4	0.1	9.0	7.8	2.3	0.7	0.0	

Source: `https://www.cvedetails.com/product/3678/Mozilla-Thunderbird.html?vendor_id=452`

Thunderbird Settings:

> Email messages can contain remote content such as images or stylesheets. To protect your privacy, Thunderbird does not load remote content automatically, but instead shows a notification bar to indicate that it blocked remote content.

- Privacy and security settings

  `https://support.mozilla.org/da/products/thunderbird/privacy-and-security-settings`

  `https://support.mozilla.org/en-US/products/thunderbird/privacy-and-security-settings`
- Previously you could override the User-Agent setting, setting it empty:
  Does not work anymore `https://bugzilla.mozilla.org/show_bug.cgi?id=1114475`
- GPG and Enigmail for OpenPGP suppoprt - encrypted email
  `https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages`

Claws Security Settings

In my mail application there are other settings you can play with:

- ✔ Render HTML messages as text
- ✔ Use secure file deletion if possible
- ✔ Never send Return Receipts

  When you receive a message that requests a Return Receipt a notification area is shown just above the message view. You can either use the 'Send receipt' button, or ignore the request - no receipts are sent automatically.
- ☐ Automatically display attached images
- ☐ Display images inline
- ☐ Add user agent header – don't

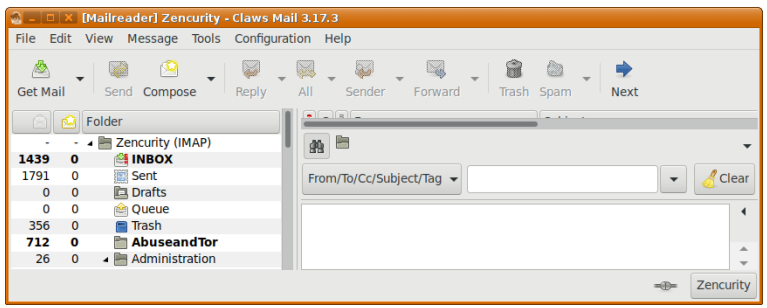
BTW my mail client is not perfect either:

`https://www.cvedetails.com/vulnerability-list/vendor_id-12415/Claws-mail.html`

Other Email Clients

- Security settings Gmail
- Good thing – Scan your email for suspicious pictures, ask before loading
- Bad thing for privacy – they scan your email for commercial gain

Advanced: Run your mail client in a VM



I run my email client in a VM, which can only connect to my mail server and my printer

```
[hlk@dom0 ~]$ qvm-firewall Mailreader
NO  ACTION  HOST             PROTOCOL  PORT(S)  SPECIAL TARGET  ICMP TYPE  EXPIRE  COMMENT
0   accept  91.102.91.22/32  tcp       993      -               -          -       -
1   accept  91.102.91.22/32  tcp       587      -               -          -       -
2   accept  10.0.42.13/32    tcp       515      -               -          -       -
3   drop    -                -         -        -               -          -       -
[hlk@dom0 ~]$
```

Part II: Basic Email Services

We will talk about domains and the current internet standards and recommendations for setting DNS records and features to optimise the reception of email securely - using encryption and certificates. Also which DNS records and features will prevent your domains from being abused for sending fake emails such as phishing with you as the sender.

Servers will be discussed as examples of email architectures. Common blueprints for email will be discussed including which components are to be used for getting insights into your email security - reporting functions. Example open source software will be shown.

Email Software

My recommendations are:

- Sending mail with SMTP using Postfix
- Receiving mail with IMAP using Dovecot

I would NOT use these:

- Exim - multiple Remote Code Execution in 2019, fatal security vulns `https://www.exim.org/static/doc/security/`
- OpenSMTPD has had some really strange vulnerabilities recently `https://www.opensmtpd.org/security.html`
- Dont use Sendmail - old and horrible

Many more exist: `https://en.wikipedia.org/wiki/Comparison_of_mail_servers`

Postfix

Postfix is a free and open-source mail transfer agent (MTA) that routes and delivers electronic mail.

It is released under the IBM Public License 1.0 which is a free software license. Alternatively, starting with version 3.2.5, it is available under the Eclipse Public License 2.0 at the user's option.[2]

Originally written in 1997 by Wietse Venema at the IBM Thomas J. Watson Research Center in New York, and first released in December 1998[3], Postfix continues as of 2020 to be actively developed by its creator and other contributors.

Source: `https://en.wikipedia.org/wiki/Postfix_(software)`

Home page: `http://www.postfix.org/`

Dovecot

Dovecot is an open-source IMAP and POP3 server for Unix-like operating systems, written primarily with security in mind.[3] Timo Sirainen originated Dovecot and first released it in July 2002. Dovecot developers primarily aim to produce a lightweight, fast and easy-to-set-up open-source email server.

The primary purpose of Dovecot is to act as mail storage server. Mail is delivered to the server using some mail delivery agent (MDA) and stored for later access with an email client (mail user agent, or MUA).

Source: `https://en.wikipedia.org/wiki/Dovecot_(software)`

Dovecot is an open source IMAP and POP3 email server for Linux/UNIX-like systems, written with security primarily in mind. Dovecot is an excellent choice for both small and large installations. It's fast, simple to set up, requires no special administration and it uses very little memory.

Home page: `https://www.dovecot.org/`

Advanced: Removed headers – client IP

Postfix

`Postfix` has a `cleanup(8)` service which takes care of a lot of stuff like address rewriting and content inspection before placing the email on the queue. The content inspection features include `header_checks` which uses a `regexp:` lookup table to inspect mail headers and act on them. This means I can define a new `cleanup(8)` service for my clients which can remove the headers matching some regular expression.

Lookup Table

My `regexp:` lookup table looks like this:

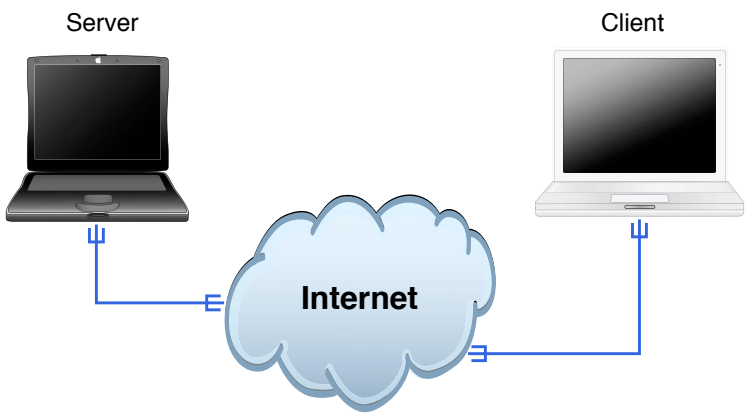
```
# Remove Received: header showing clients ip for authenticated locally submitted email
/^Received:.* with ESMTPSA id/ IGNORE

# Remove X-Originating-IP
/^X-Originating-IP:/ IGNORE

# Remove X-Mailer and User-Agent
/^X-Mailer:/ IGNORE
/^User-Agent:/ IGNORE
```

https://blog.tyk.nu/blog/postfix-and-privacy/ Thank you Thomas

Internet i dag



Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

Meget lidt kryptering, mest på http til brug ved e-handel

Data found in Network traffic

Many older internet protocols are cleartext - no encryption

Lets take an example, DNS

Domain Name System DNS breadcrumbs

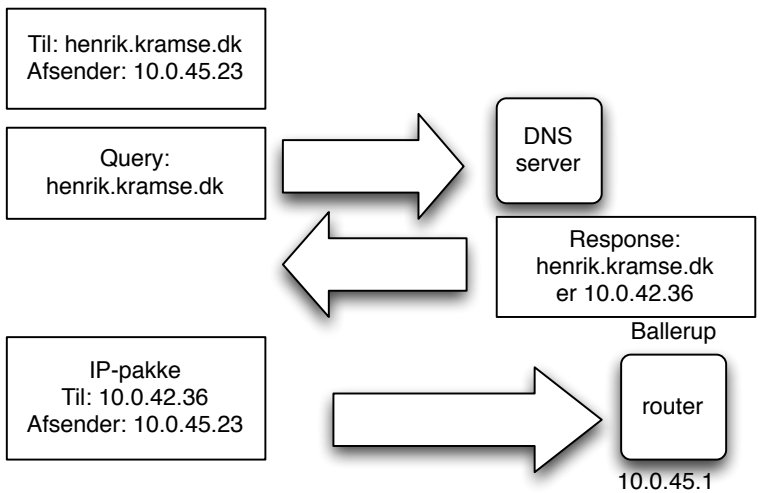
- Your company domain, mail servers
- Emails being sent are essentially post cards

Advice show your users, ask them to participate in a experiment

Sniffing a wireless network is easy

Maybe use VPN more - or always!

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 more than just web site name lookup

DNS is based on resource records of types:

- A-record is an address
- Quad-A AAAA-records are IP version 6 addresses
- Authoritative name servers are listed in NS-records
- Email exchangers are put into MX-records
- Multiple others: md , mf , cname , soa , mb , mg , mr , null , wks , ptr , hinfo , minfo , mx ....
- Previously there was SRV server records and types being added, but today a lot of functionality is put into TXT records – a text string with information

```
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 Example

```
user@Projects:images$ host -t ns zencurity.com
zencurity.com name server ns1.gratisdns.dk.
zencurity.com name server ns2.gratisdns.dk.
zencurity.com name server ns3.gratisdns.dk.
zencurity.com name server ns4.gratisdns.dk.
zencurity.com name server ns5.gratisdns.dk.
user@Projects:images$ host -t mx zencurity.com
zencurity.com mail is handled by 10 mail.kramse.org.
```

So this domain is found at the GratisDNS system and uses a single mail server record.

By default all of this happens without encryption and no integrity protection!

Note: I use mostly `host` while DNS admins typically use `dig`

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`

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

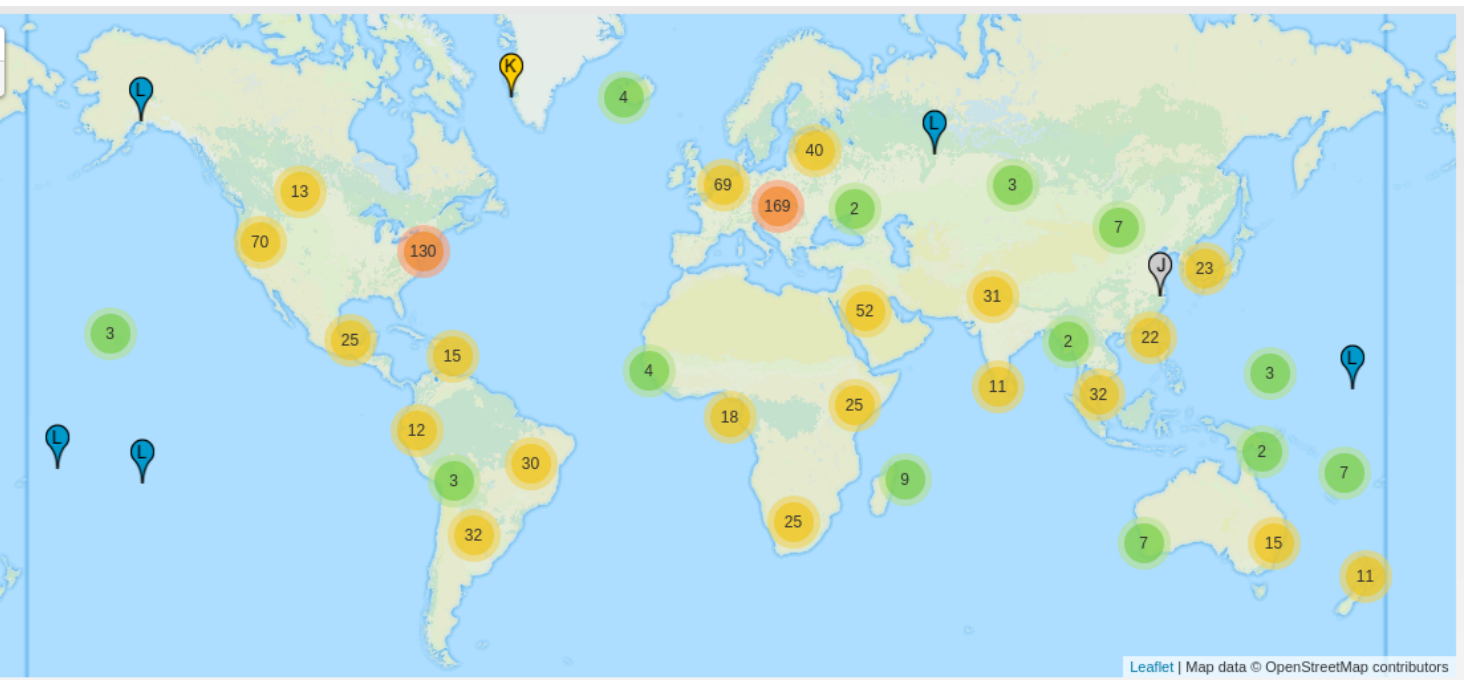
typisk indhold er domænenavn og IP-adresser for navneservere

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/

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.

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/`

Crypto slides here!

Imagine a long presentation inserted here showing:

- HTTPS and Transport Layer Security (TLS)
  `https://en.wikipedia.org/wiki/Transport_Layer_Security`
- Elliptic Curve Encryption
  `https://en.wikipedia.org/wiki/Elliptic-curve_cryptography`
- Diffie-Hellman
  `https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange`

SSL og TLS

- Originally from Netscape Communications Inc.
- Secure Sockets Layer SSL was adopted by IETF and generalized into Transport Layer Security TLS
- RFC-2246 The TLS Protocol Version 1.0 fra Januar 1999
- Recommend *Serious Cryptography A Practical Introduction to Modern Encryption* by Jean-Philippe Aumasson November 2017, 312 pp. ISBN-13: 978-1-59327-826-7
- Stanford Dan Boneh is writing a crypto book `https://crypto.stanford.edu/~dabo/cryptobook/`

Fokus: Encryption and TLS settings

- Check your TLS settings multiple times a year
- Easy for web servers Qualys sslscan
- Almost as easy with a command line tool

SMTP TLS

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

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) cryptographic authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

Source:

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

DNSSEC in Denmark

DNSSEC - also for .dk

Using the root DNSSEC and .dk – you can add your own certificates!

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

DNSSEC is something you should enable ASAP where possible

DNSSEC and DANE

"Objective:

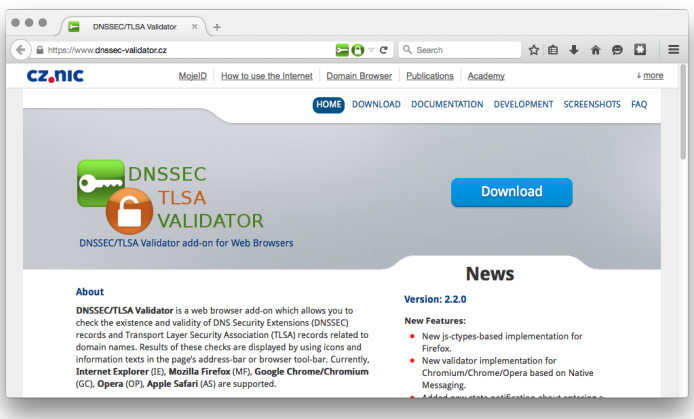
Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name."

DNS-based Authentication of Named Entities (DANE)

DANE protocol (RFC 6698)

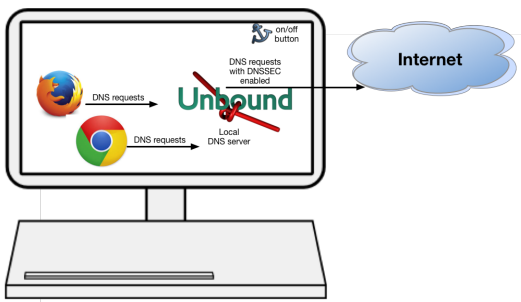
`https://en.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities`

TLSA Records



"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."

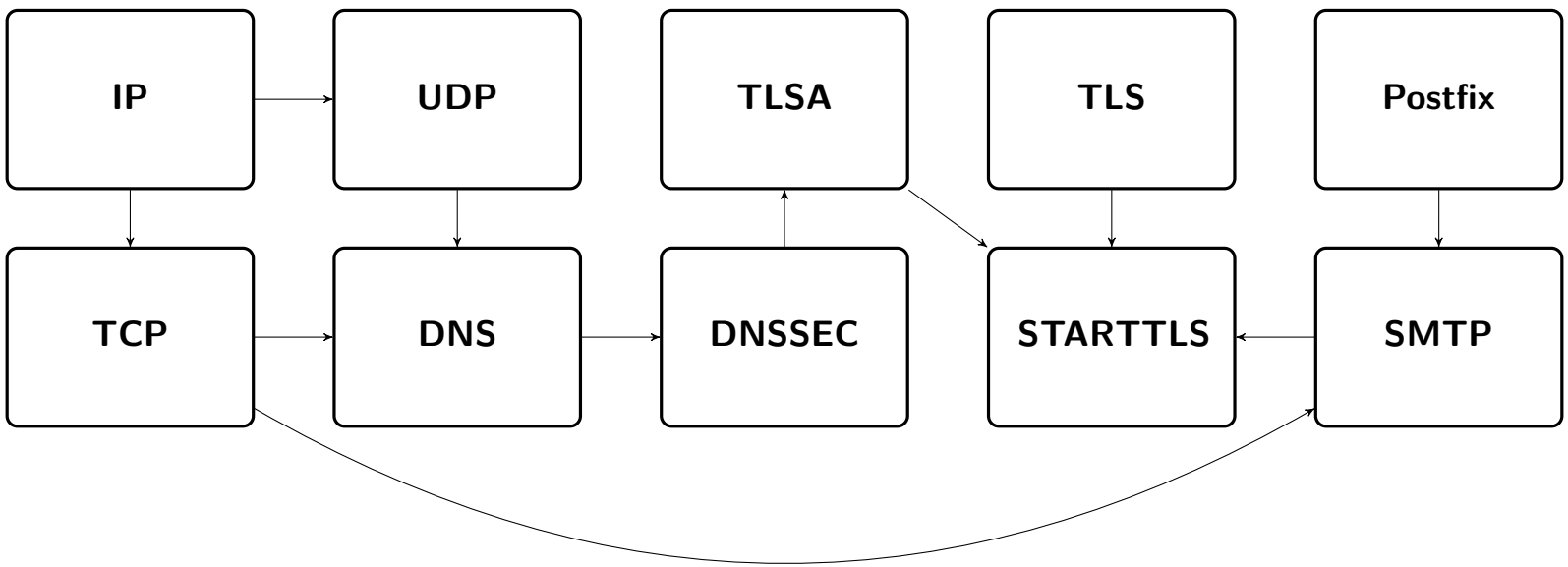
DNSSEC trigger



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/`

Puzzle with SMTP



Quite a lot of pieces, but it works

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:

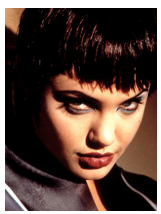
Specification for DNS over Transport Layer Security (TLS) (DoT), RFC 7858 MAY 2016
`https://en.wikipedia.org/wiki/DNS_over_TLS`

DNS Queries over HTTPS (DoH) RFC 8484

How to cofigure DoT `https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients`

Part III: Testing email services

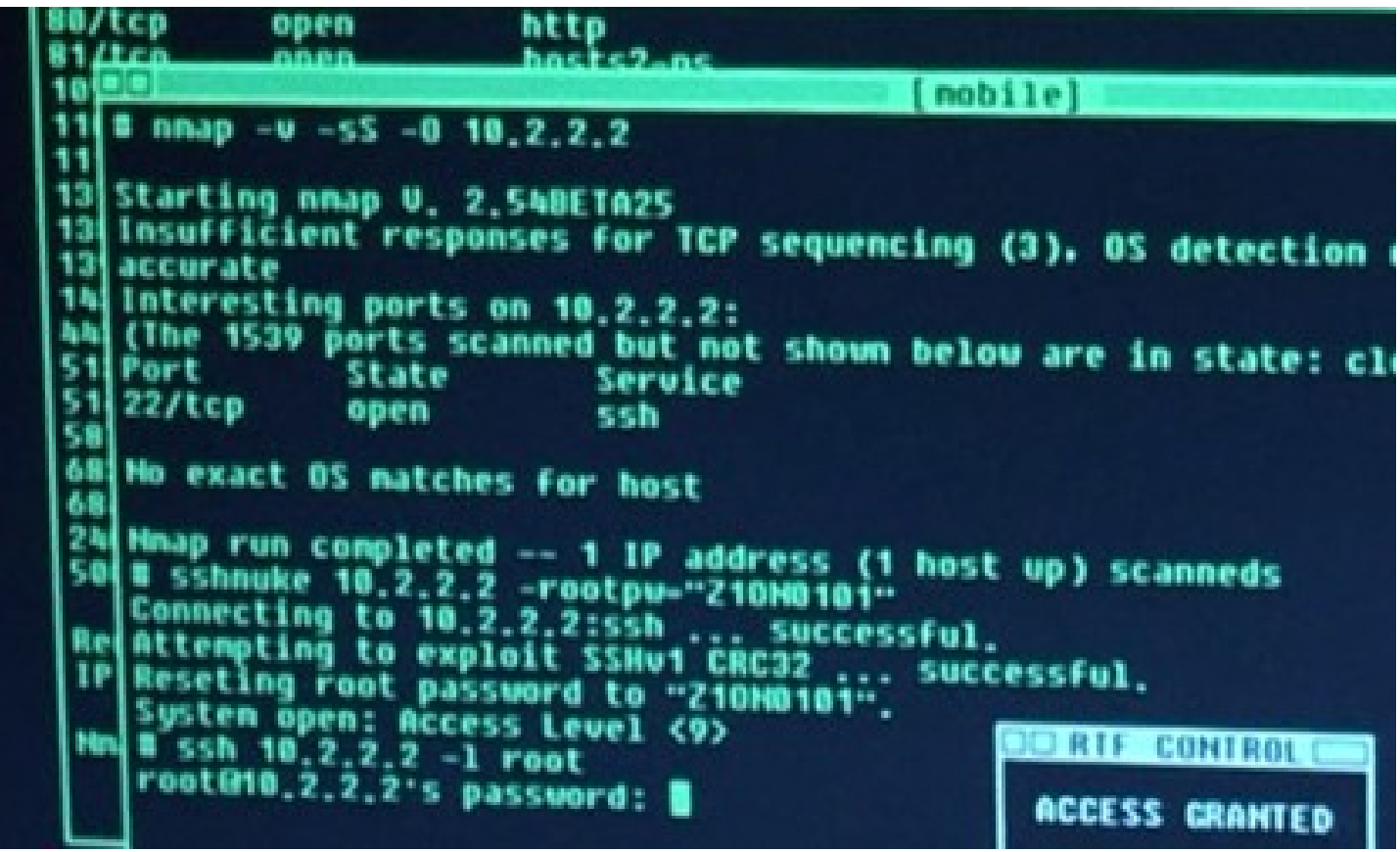
Hackertools are for everyone!



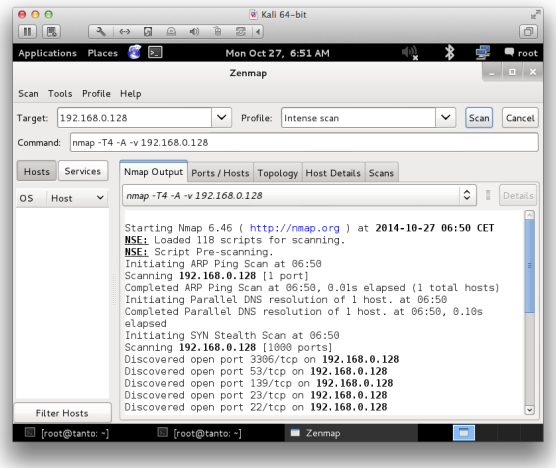
- Hackers work all the time to break stuff, Use hackertools:
- Nmap, Nping `http://nmap.org`
- Wireshark - `http://www.wireshark.org/`
- Aircrack-ng `http://www.aircrack-ng.org/`
- Kali Linux `http://www.kali.org`

Most popular hacker tools `http://sectools.org/`

Nmap the world



Really do Nmap your world



- Nmap is a port scanner, but does more
- Finding your own infrastructure available from the guest network?
- See your printers having all the protocols enabled AND a wireless?

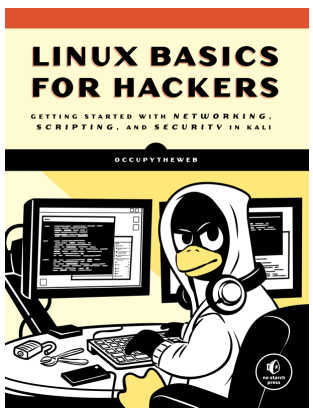
Generic Encryption settings sslscan

- Easy to use tool `sslscan www.domain.tld`
- Check TLS/SSL on Web Servers
- Check TLS/SSL on other services – Mail servers

Hacking is not magic

- Hacking only requires some ninja training
- We have been doing this since 1995 when SATAN was released
- Listen, Plan, Act, Do hacking

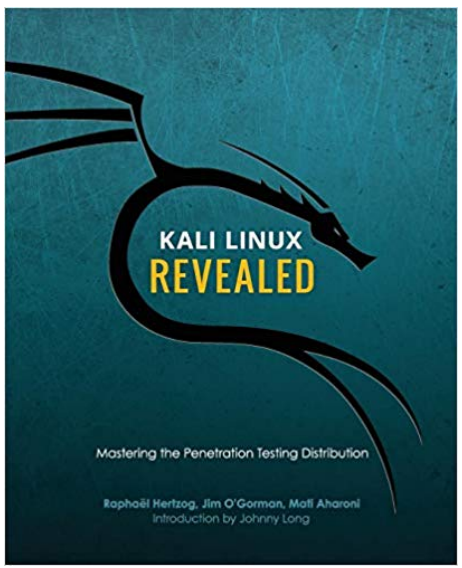
Book: Linux Basics for Hackers (LBfH)



Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali by OccupyTheWeb December 2018, 248 pp. ISBN-13: 9781593278557

`https://nostarch.com/linuxbasicsforhackers`

Book: Kali Linux Revealed (KLR)



Kali Linux Revealed Mastering the Penetration Testing Distribution

`https://www.kali.org/download-kali-linux-revealed-book/`
explains how to install Kali Linux

Nmap efter SSL og TLS

Example Usage

```
nmap -sV -sC <target>
```

Script Output

```
443/tcp open   https   syn-ack
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

Nu vi har lært Kali og Nmap at kende

- Find nemt alle ssl version 2 og 3
  `nmap --script ssl-enum-ciphers`
- Brug ssllabs https://www.ssllabs.com/

sslscan

```
root@kali:~# sslscan --ssl2 web.kramse.dk
Version: 1.10.5-static
OpenSSL 1.0.2e-dev xx XXX xxxx

Testing SSL server web.kramse.dk on port 443
...
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.kramse.dk
Altnames: DNS:*.kramse.dk, DNS:kramse.dk
Issuer:   AlphaSSL CA - SHA256 - G2
```

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

SSLscan can check your own sites, while Qualys SSLLabs only can test from hostname

sslscan STARTTLS

```
$ sslscan --starttls-smtp mail.kramse.org
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 P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 2048 bits
...
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 2048 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256         DHE 2048 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA            DHE 2048 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-CAMELLIA128-SHA256    DHE 2048 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-CAMELLIA128-SHA       DHE 2048 bits
```

Hardenize - web sites with testing

Multiple sites provide testing of domains and configurations

- `https://internet.nl/` – recommended for mail settings
- `https://dmarcian.com/` – recommended for mail settings
- `https://www.hardenize.com/`
- `https://www.ssllabs.com/` – recommended for web sites

Part IV: Strategy for Your Email Security

The goal for this presentation is for participants to get an overview of current email security, to allow them to evaluate their own posture - and plan a strategy to improve email security, both personally and professionally.

Make sure everyone attending know about methods to restrict sending of false emails, how to secure this using DNSSEC, SPF, DMARC - DNS based updates to your email domain security

Building Secure Infrastructures

A real-life setup of an email infrastructure from scratch can be daunting!

You need:

- Policies
- Procedures
- Incident Response

Running systems which require

- Configurations
- Settings
- Supporting infrastructure – networks
- Supporting infrastructure – logging, dash boarding, monitoring

Building something *secure* is **hard work!**

Email and Web Browser Protections

CIS controls 7-16 are Foundational

CIS Control 7:
Email and Web Browser Protections
Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Use centralized proxies, with filtering settings?

Automated browser updates

Source: Center for Internet Security CIS Controls 7.1 CIS-Controls-Version-7-1.pdf

Email security – Goals

- SPF Sender Policy Framework

  `https://en.wikipedia.org/wiki/Sender_Policy_Framework`
- DKIM DomainKeys Identified Mail

  `https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail`
- DMARC Domain-based Message Authentication, Reporting and Conformance

  `https://en.wikipedia.org/wiki/DMARC`
- Use them all

A huge part of email security is ensuring our domains are not abused in spoofing attacks, and spam

Sender Policy Framework (SPF)

```
$ host -t TXT zencurity.com
zencurity.com descriptive text "v=spf1 a mx mx:kramse.dk -all"
```

Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of the email.[1] SPF alone, though, is limited only to detect a forged sender claimed in the envelope of the email which is used when the mail gets bounced.[1] **Only in combination with DMARC can it be used to detect the forging of the visible sender in emails** (email spoofing[2]), a technique often used in phishing and email spam.

SPF allows the receiving mail server to check during mail delivery that a mail claiming to come from a specific domain is submitted by an IP address authorized by that domain's administrators.[3] The list of authorized sending hosts and IP addresses for a domain is published in the DNS records for that domain.

Source:

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

DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain.[1] It achieves this by affixing a digital signature, linked to a domain name, to each outgoing email message. The recipient system can verify this by looking up the sender's public key published in the DNS. A valid signature also guarantees that some parts of the email (possibly including attachments) have not been modified since the signature was affixed.[2] Usually, DKIM signatures are not visible to end-users, and are affixed or verified by the infrastructure rather than the message's authors and recipients.

Source:

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

Domain-based Message Authentication (DMARC)

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing emails, email scams and other cyber threat activities.

Once the DMARC DNS entry is published, any receiving email server can authenticate the incoming email based on the instructions published by the domain owner within the DNS entry. If the email passes the authentication it will be delivered and can be trusted. If the email fails the check, depending on the instructions held within the DMARC record the email could be delivered, quarantined or rejected.

DMARC extends two existing mechanisms, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).

DMARC Domain-based Message Authentication, Reporting and Conformance Source:

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

DMARC for non-sending Domains

If you have domains that *never send email* then add the following SPF and DMARC to avoid misuse.

from my own DSN template for *parked domains*:

```
gdns.template    v=spf1 -all      43200
_dmarc.gdns.template    v=DMARC1; p=reject;      43200
```

Get Started and Get Resources

Suggested method:
Use services on the internet, such as `https://internet.nl/` and `https://dmarcian.com/` to see current status for your domains.

Hints:
I suggest the following strategy when you implement these methods, if you dare do it right now. If you make a plan.

Basic mail security

1. Implement DNSSEC - turn it on, most likely easy
2. Configure Sender Policy Framework, perhaps only `~all` tilde means soft fail
3. Configure DomainKeys Identified Mail
4. Configure receiving email address for DMARC
5. Configure Domain-based Message Authentication - reject none

Advanced mail security

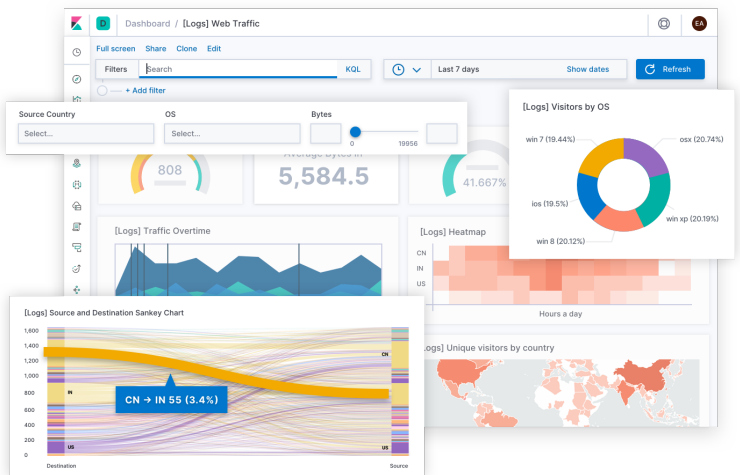
1. Create real certificates for TLS and DANE, I use Lets Encrypt
2. Publish them ☺

Take domain(s) of your choice and make a table:

Domain ✉	DNS NS 2+	DNSSEC	SPF	DKIM	DMARC	DANE
zencurity.com	✔	✔	✔		✔	

Discussion:
You need to research before making changes to important domains.

Graphs and Dashboards!



Screenshot from `https://www.elastic.co/kibana`

Suggested method:

Visit the web page for *Getting started with the Elastic Stack* :

`https://www.elastic.co/guide/en/elastic-stack-get-started/current/get-started-elastic-stack.html`

Email tools are abundant

Spend some time trying different tools for DMARC reporting. A month or a week, depending on the domain and your users. Github alone has 100s of projects concerned with parsing, reporting and working with DMARC.

Then after some time has passed, and you have reviewed reporting from DMARC, turn it on for real:

1. Configure SPF to disallow with hard fail use `-all` minus
2. Configure DMARC with reject - reject emails not following policy

- Before implementing security, monitor your services
- DMARC Analysis and reporting tools
- SMTP TLS Reporting

Next steps

Future mail standards - young and not widely used:

- MTA Strict Transport Security (MTA-STS)
  `https://www.rfc-editor.org/rfc/rfc8461.txt`
- SMTP TLS Reporting
  `https://www.rfc-editor.org/info/rfc8460`
- OpenARC The Authenticated Received Chain (ARC) Protocol, JULY 2019 RFC 8617
  `https://www.rfc-editor.org/info/rfc8617`

Some input from Sidsel, thank you, and more information at:

`https://www.version2.dk/blog/fremtidens-mailstandarder-dane-mta-sts-tls-reporting-openarc-1082819`

I only support TLS encrypted email since august 2019, and have few problems

`https://www.version2.dk/blog/skal-starttls-vaere-krav-foelsomme-email-1088758`

Checking for new standards

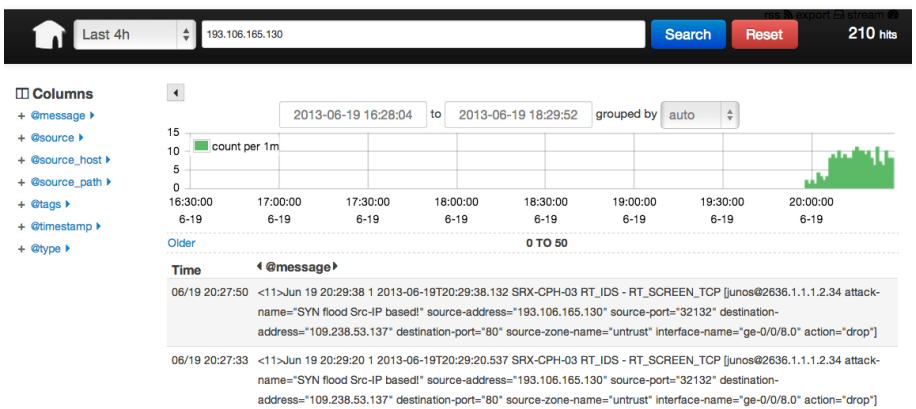
Update (23 April 2019): Gmail has become the first major email provider to support MTA-STS and TLSRPT, making it easier to justify deploying these new standards. More information is available in their blog post.

Update (26 Sep 2018): MTA-STS has been officially published as RFC 8461.

MTA-STS (full name SMTP Mail Transfer Agent Strict Transport Security) is a new standard that aims to improve the security of SMTP by enabling domain names to opt into strict transport layer security mode that requires authentication (valid public certificates) and encryption (TLS). In this blog post we discuss why MTA-STS exists and how it's used, as well as announce full support for its most recent draft in Hardenize.

Source: `https://www.hardenize.com/blog/mta-sts`

Advanced Network tools - examples



- Net: Zeek `https://www.zeek.org/` Suricata `http://suricata-ids.org`
- DNS: DSC and PacketQ `https://github.com/dotse/packetq/wiki`
  Storing query logs, old school or needed?
- Syslog: Elasticsearch, Logstash, and Kibana, called ELK stack or Elastic stack
- Use these to see inside systems using DNS and SMTP for unauthorized traffic

Questions?

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

You are always welcome to send me questions later via email

Email: hlk@zencurity.dk Mobile: +45 2026 6000