Welcome to

It-sikkerhedsupdate

2021

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

it-sikkerhedsupdate.tex in the repo security-courses

slides are available on Github

Goal for today

What are the things on the table for a responsible it-security strategy. Which subjects are most important, and what are the threats, if you dont get started immediately with the top 10 priorities.

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

Every Year

- Same problems last year? Same problems EVERY year
- 2020 was a nightmare of break-ins and data leaks
- Data leaks, GDPR, ransomware, ...

Try not to panic, but there are lots of threats

Are we loosing the battle?

Har du haft snakken med din CISO?

IT-sikkerhed:
Vi vil gerne bede om 10 millioner til IT-sikkerhed i budget næste år
CTO/CIO/CISO:
Umuligt
IT-sikkerhed:
OK, fair nok. Så skal vi bare bede om **100 millioner til Ransomware**, tak.
Husk også at uddanne CFO i bitcoin transaktioner.

- Er ovenstående urealistisk?

Demant 2019

- For året 2019 rapporterede vi et tab i omsætning på **575 millioner kroner**. Det i sig selv er alvorligt. Hvad angår vores opmærksomhed på it-sikkerhedsområdet, har it-hændelsen været med til at understrege nødvendigheden af, at tage dette felt seriøst. Angreb mod it-infrastruktur er uden tvivl en af de største trusler mod en virksomhed, og det kan gå galt, hvis man ikke er i stand til at lukke ned for skaden og bruge sin back-up.

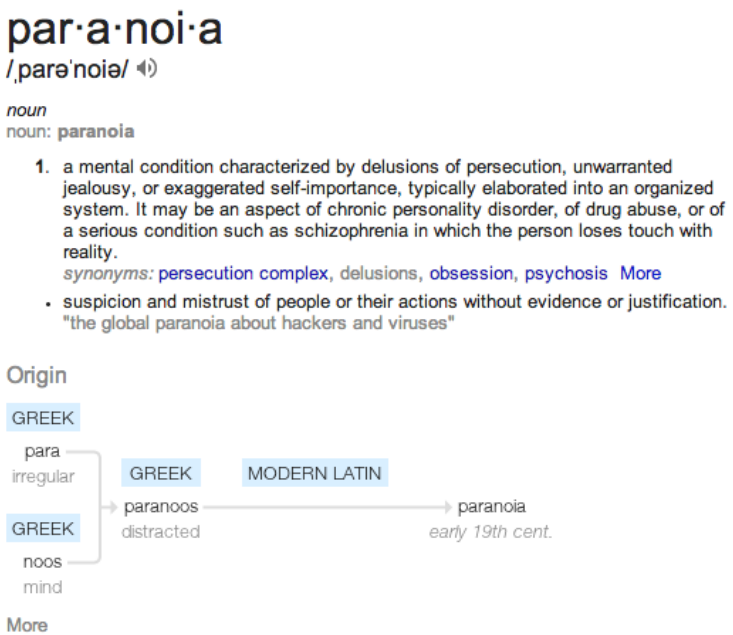
...

- På det konkrete plan har vi fået et mantra der lyder **'Active Directory is king, and backup is Queen'**. Men mere overordnet har vi også lært at Focus skal helt op på øverste niveau i virksomheden, at man skal skaffe høj faglig indsigt i sikkerhed og trusler, og at det er et arbejde, der skal være under konstant observation og udvikling.

Kilde: `https://dit.dk/Nyheder/2021/Demant`

- Vi taler altså om tab i størrelsesorden tre-cifrede millionbeløb!

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

GREEK
para
irregular
GREEK
noos
mind
GREEK
paranoos
distracted
MODERN LATIN
paranoia
early 19th cent.

More

Source: google paranoia definition

Use appropriate paranoia, and yes, hot pink red blinking is an appropriate threat level

Hackers don’t give a shit

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

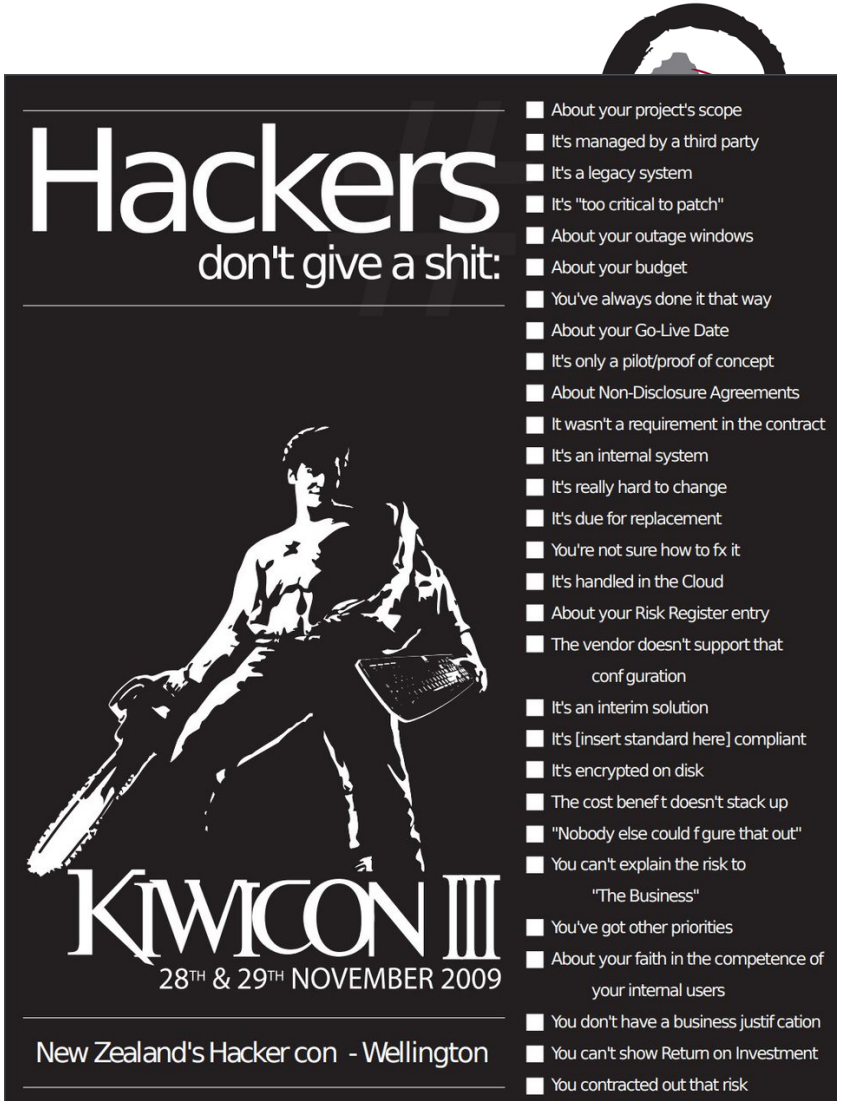
Your network is a research network, under construction, being phased out, ...

Try something new, go to your management

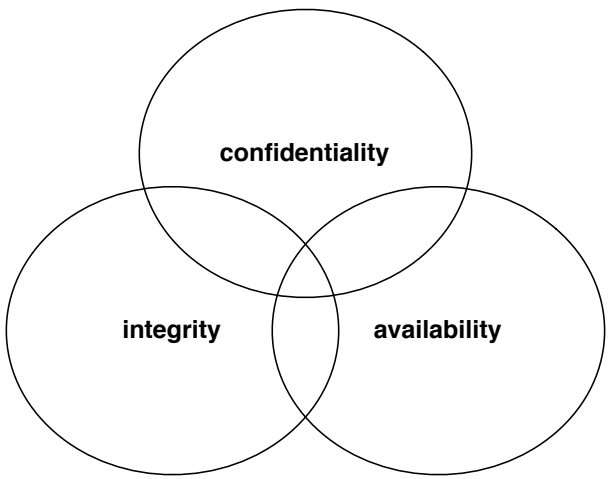
Bring all the exceptions, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

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 kept secret

Integrity - no unauthorized changes to data

Availability - data and systems are available to authorized uses when they need them

Security engineering as a job role

On any given day, you may be challenged to:

- Create new ways to solve existing production security issues
- Configure and install firewalls and intrusion detection systems
- Perform vulnerability testing, risk analyses and security assessments
- Develop automation scripts to handle and track incidents
- Investigate intrusion incidents, conduct forensic investigations and incident responses
- Collaborate with colleagues on authentication, authorization and encryption solutions
- Evaluate new technologies and processes that enhance security capabilities
- Test security solutions using industry standard analysis criteria
- Deliver technical reports and formal papers on test findings
- Respond to information security issues during each stage of a project's lifecycle
- Supervise changes in software, hardware, facilities, telecommunications and user needs
- Define, implement and maintain corporate security policies
- Analyze and advise on new security technologies and program conformance
- Recommend modifications in legal, technical and regulatory areas that affect IT security

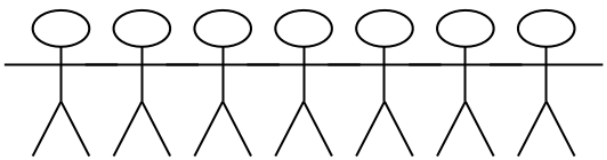
Source: https://www.cyberdegrees.org/jobs/security-engineer/
also https://en.wikipedia.org/wiki/Security_engineering

Focus on the basics

- User management - including administrative users
- Asset management
- Laptop security
- Penetration testing
- Firewalls and segmentation
- VPN everywhere
- TLS and VPN settings, encryption
- DNS and email security
- Syslog and monitorering
- Incident Response and response

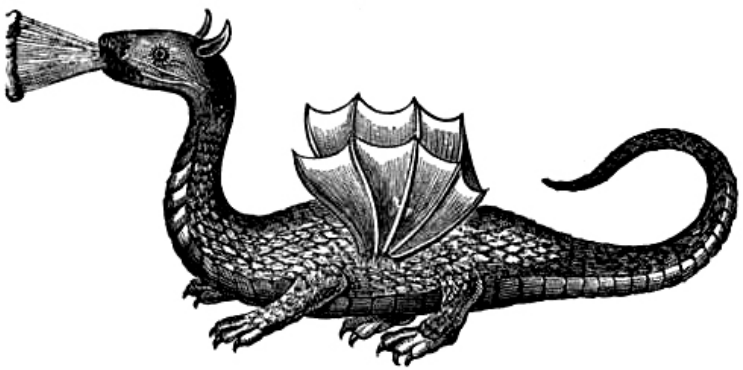
I hope you have a team, otherwise choose a few at a time

Focus: User management



- Relevant for alle organisationer
- Er måden vi sikrer godkendte brugere kan udføre opgaver
- Kodeord bruges til at forhindre uautoriseret adgang
- Har I styr på brugerid?
- Hvor er brugere oprettet?
- Hvor hurtigt kan I fjerne "een bruger"eller "deaktivere en bruger"alle steder!
- Er det et kludetæppe - ja, mange steder er det

Local administrator?



- Findes der systemer som er helt åbne, med lokal administrator
- Er det stadig nødvendigt

Centralized User management

Active Directory, mange danske virksomheder bruger det

LDAP central brugerstyring

... men brug det endnu mere

- Konfigurer applikationer til central styring
- Fjern applikationer som ikke tillader central styring
- Overvågning på fejlslagne logins, og godkendte logins

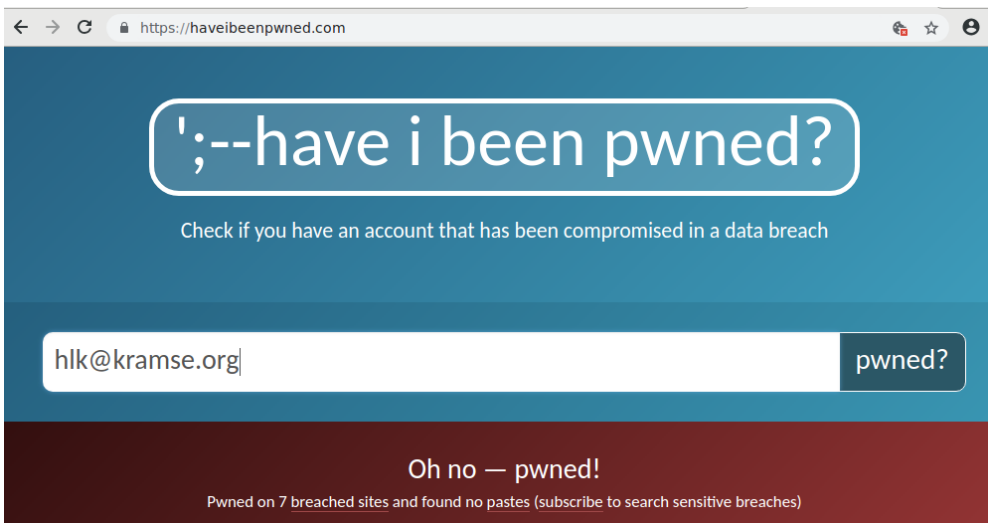
Generelt minimer brugere andre steder end i den centrale database

Hvad med ILO, DRAC, temperaturovervågning - en fælles password database, med begrænset adgang, måske?

Passwords vælges ikke tilfældigt

Source: `https://wpengine.com/unmasked/`

Your data has already have been owned by criminals



Your data is already being sold, and resold on the Internet

Stop reusing passwords, use a password safe to generate and remember

Check you own email addresses on `https://haveibeenpwned.com/`

They have an API you can integrate to

Brug mere sikre passwords

> Pwned Passwords overview
> Pwned Passwords are more than half a billion passwords which have previously been exposed in data breaches. The service is detailed in the launch blog post then further expanded on with the release of version 2. The entire data set is both downloadable and searchable online via the Pwned Passwords page.

I kan forhindre brugere i at vælge passwords der ALLEREDE er lækket

I kan bruge deres API eller download

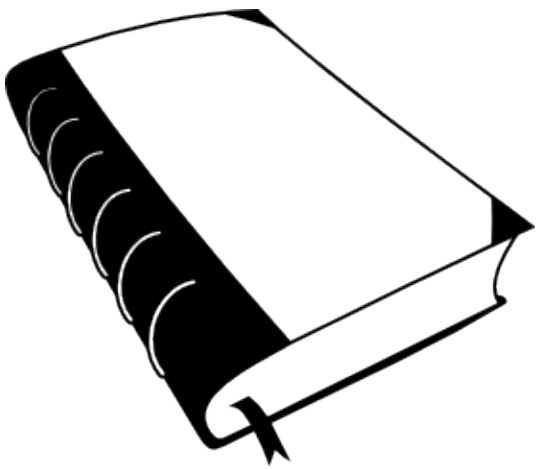
`https://www.troyhunt.com/introducing-306-million-freely-downloadable-pwned-passwords/`

Opbevaring af passwords

"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

- Use password managers! Available as cloud connected, local only, teams based
- You will have to investigate which one to choose, but find one!

Focus: Asset management



Free graphics by Lumen Design Studio

- Specielt relevant for mellemstore til store organisationer
- Hvilke assets har vi?
- Hvordan sikrer vi at vi ikke mister værdierne

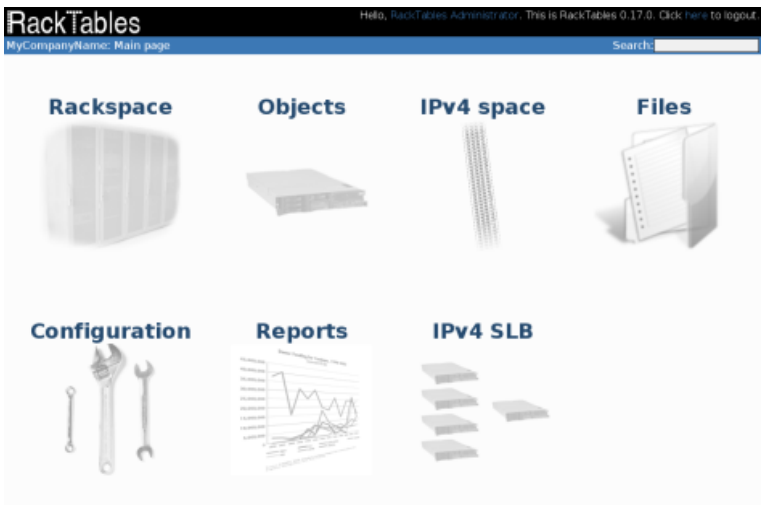
What is asset management

> CIS Control 1:
> Inventory and Control of Hardware Assets Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Source: `https://www.cisecurity.org/`

- Hardware - både indkøbte, opkoblede, udlånte, stjålne ...
- Software - licenser, indkøb, brug, opgraderingspriser
- Virtuelle arkiver - eksempelvis forretningskritiske data
- ...

Hardware asset management

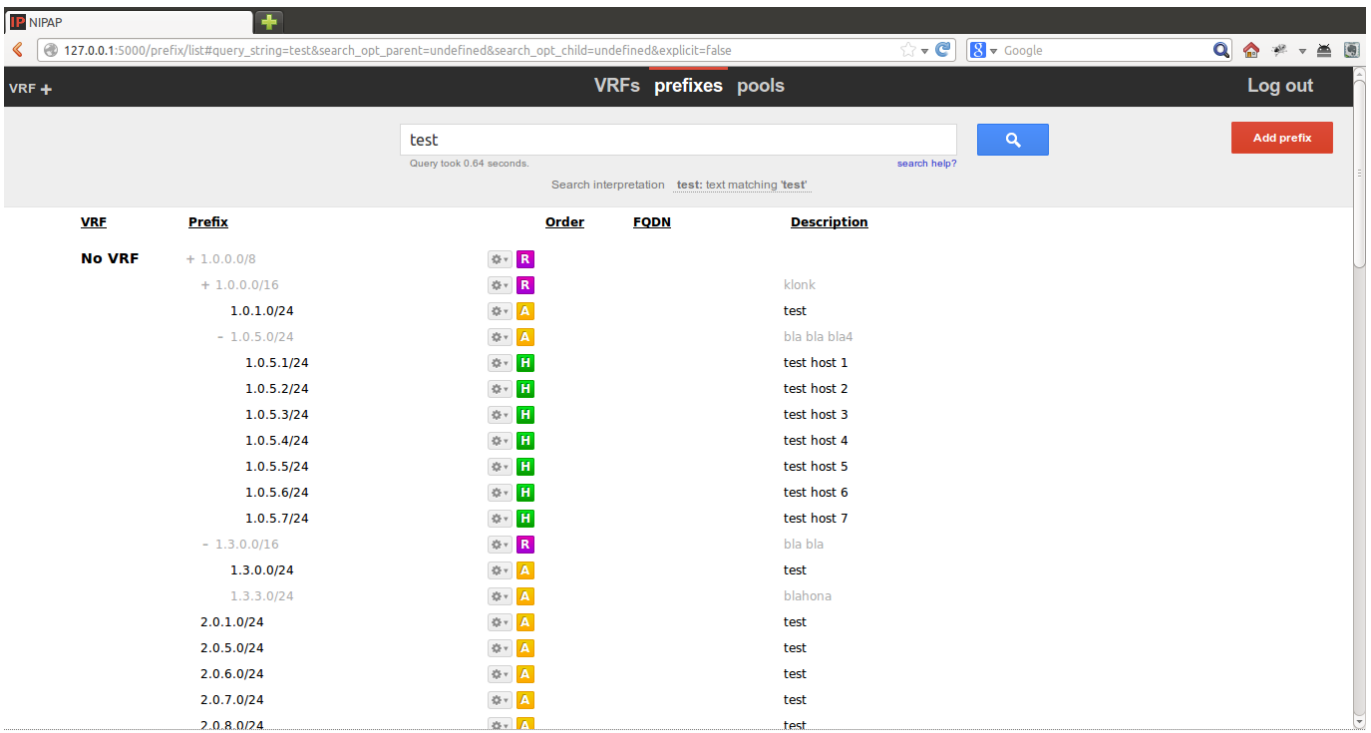


- Der findes mange systermer
- Det anbefales at bruge specialiserede systemer, a la RackTables:
  Have a list of all devices you've got, Have a list of all racks and enclosures, Mount the devices into the racks, Maintain physical ports of the devices and links between them

Software asset management - virtuelle arkiver

- Software - licenser, indkøb, brug, opgraderingspriser
- Virtuelle maskiner - er en server et asset, eller er det data?
- IP adresser
- Data arkiver - GDPR

IP Address Management IPAM



- Anbefaler Nipap `http://spritelink.github.io/NIPAP/`

Har du styr på afhængighederne

.

- Skal det være helt flot så få også styr på dependencies
- Er jeres produktion afhængig af andres moduler, biblioteker osv.
- Tænk tilbage til Heartbleed, gik flere år før de sidste opdateringer kom
- Container scannere, hvilke sårbarheder er der under jeres applikationer
- Nyt ord supply-chain attacks: Solarwinds sagen

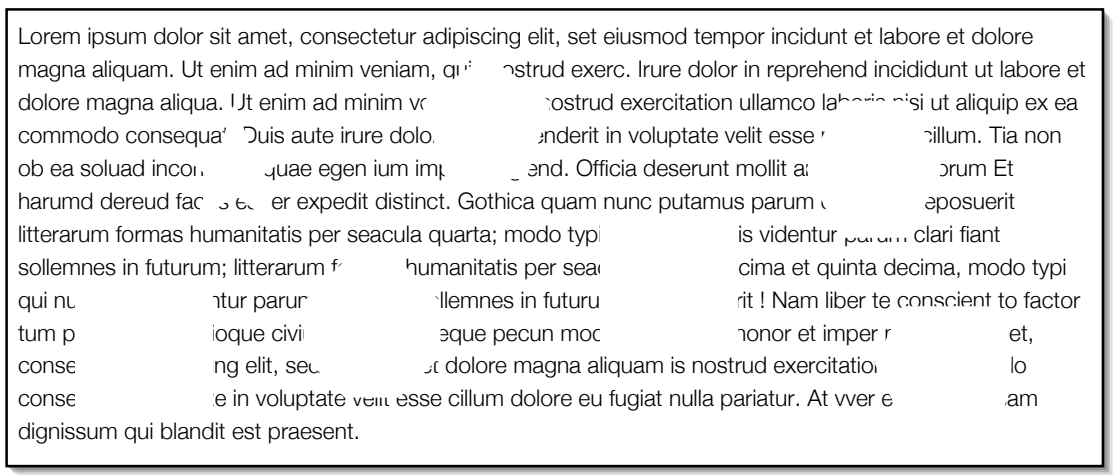
Focus: Laptop sikkerhed

- Relevant for alle
- Hvordan sikrer vi at vi ikke mister værdierne, hardware og data typisk

Secure Laptops

- Laptops (og mobile enheder)
- Hvad kendetegner en laptop?
- Hardware naturligvis, en Macbook koster officielt mere end en brugt mellemklassebil
- - og husk brugen af laptops
- Er laptops sikre, og hvad betyder det?

Are your data secure - data at rest



Stolen laptop, tablet, phone - can anybody read your data?

Do you trust ”remote wipe”

How do you in fact wipe data securely off devices, and SSDs?

Encrypt disk and storage devices before using them in the first place!

Circumvent security - single user mode boot

Unix systems often allows boot into singleuser mode
press command-s when booting Mac OS X

Laptops can often be booted using PXE network or CD boot

Mac computers can become a Firewire disk
hold t when booting - firewire target mode

Unrestricted access to un-encrypted data

Moving hard drive to another computer is also easy

Physical access is often - **game over**

Encrypting hard disk

Becoming available in the most popular client operating systems

- Microsoft Windows Bitlocker
- Apple Mac OS X - FileVault
- FreeBSD GEOM og GBDE - encryption framework
- Linux LUKS distributions like Ubuntu ask to encrypt home dir during installation
- Some vendors have BIOS passwords, or disk passwords

Attacks on disk encryption

Firewire, DMA & Windows, Winlockpwn via FireWire
Hit by a Bus: Physical Access Attacks with Firewire Ruxcon 2006

Removing memory from live system - data is not immediately lost, and can be read under some circumstances
Lest We Remember: Cold Boot Attacks on Encryption Keys
`http://citp.princeton.edu/memory/`

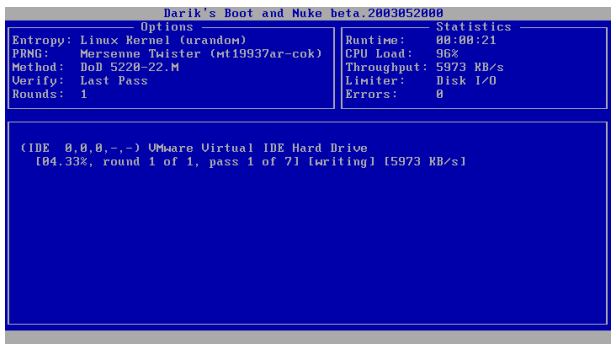
This is very CSI or Hollywoord like - but a real threat

VileFault decrypts encrypted Mac OS X disk image files
`https://code.google.com/p/vilefault/`

FileVault Drive Encryption (FVDE) (or FileVault2) encrypted volumes
`https://code.google.com/p/libfvde/`

So perhaps use both hard drive encryption AND turn off computer after use?

… and deleting data



Getting rid of data from old devices is a pain

Some tools will not overwrite data, leaving it vulnerable to recovery

Even secure erase programs might not work on SSD - due to reallocation of blocks

I have used Darik's Boot and Nuke ("DBAN") `http://www.dban.org/`

2018 attack

Drive	1	2	3	4	5	6	7	8	9	Impact
Crucial MX100 (all form factors)	✗	✗	✗							✗ Compromised
Crucial MX200 (all form factors)	✗	✗	✗							✗ Compromised
Crucial MX300 (all form factors)	✓	✓	✓		✗	✓	✓	✓	✓	✗ Compromised
Samsung 840 EVO (SATA)	✗	✓	✓		✓	✓	✓	✗	✓	∼ Depends
Samsung 850 EVO (SATA)	✗	✓	✓		✓	✓	✓	✓	✓	∼ Depends
Samsung T3 (USB)				✗						✗ Compromised
Samsung T5 (USB)				✗						✗ Compromised

[1] Cryptographic binding in ATA Security (High mode)
[2] Cryptographic binding in ATA Security (Max mode)
[3] Cryptographic binding in TCG Opal
[4] Cryptographic binding in proprietary standard
[5] No single key for entire disk
[6] Randomized DEK on sanitize
[7] Sufficient random entropy
[8] No wear leveling related issues
[9] No DEVSLP related issues

self-encrypting deception: weakness in the encryption of solid state drives (SSDs)
`https://www.ru.nl/publish/pages/909282/draft-paper.pdf`

Recommendations - Comply Everywhere, Act Anywhere

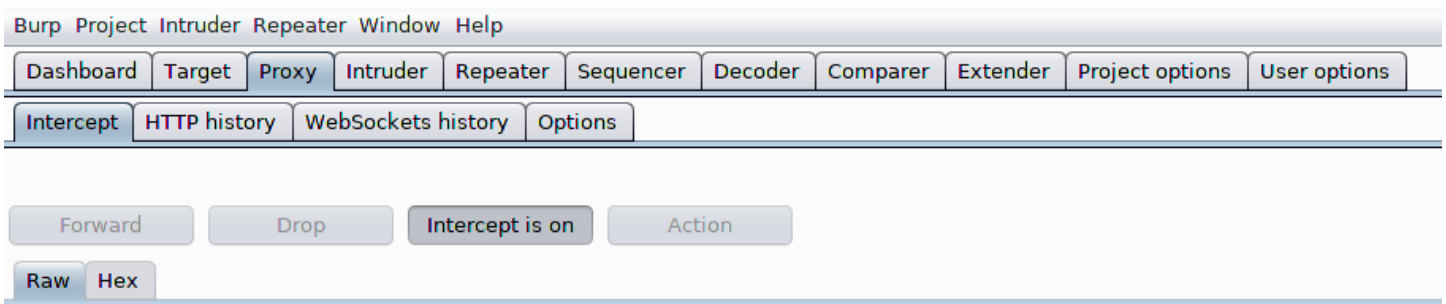
Laptop storage must be encrypted

Firewall must be enabled

Next suggestion:

- Try sniffing data from a laptop, setup Access Point/Monitor port
- Portscan your laptop networks - use Nmap
- Write an email to everyone in your organisation:
  "Hi All, we need to identify laptops without full disk encryption
  - come see us, we have christmas cookies left, Best regards IT"

Focus: Penetration testing



- Relevant hvis du driver et netværk, specielt hvis det er forbundet til internet eller stort
- Du bliver hele tiden testet - internet-tinnitus
- Penetration testing
- Kontrol af sikkerheden med aktive værktøjer
- Brug Nmap pakken til at checke åbne porte
- Køb Burp Suite hvis du har et web site du tjener penge på

Start Attacking from the Inside

- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?
  Having a large open network may cost you **1.9 billion DKK - ref Maersk case**
- Try scanning everything, start in a small corner, expand
- Scan all you danish segments, one by one, then the nordic, then the world
- Yes, things may break - FINE, BREAKING is GOOD

Better to break while we are ready to un-break

How to break stuff

Think like an attacker, and begin at the bottom.

I sit here, but where am I connected:

```
reading from file cisco-lldp-1.cap, link-type EN10MB (Ethernet)
16:39:43.468745 LLDP, length 328
        Chassis ID TLV (1), length 7
          Subtype MAC address (4): 70:ff:1a:01:03:02 (oui Unknown)
        Port ID TLV (2), length 8
          Subtype Local (7): Eth1/47
        Port Description TLV (4), length 12: Ethernet1/47
        System Description TLV (6), length 158
          Cisco Nexus Operating System (NX-OS) Software 14.0(2c) TAC support: http://www.cisco.com/tac Copyright (c) 2002-
2020, Cisco Systems, Inc. All rights reserved.
```

I love LLDP, but it does reveal software version, so be careful

Check *Security Assessment of Cisco ACI* – 6 CVEs in one product, from a few weeks of testing
`https://www.ernw.de/en/whitepapers/issue-68.html`

Hackertools are for everyone!

Hackers work all the time to break stuff

Blue teams can use hackertools, and become more effecient:

- Nmap, Nping `http://nmap.org`
- Wireshark - `http://www.wireshark.org/`
- Aircrack-ng `http://www.aircrack-ng.org/`
- Metasploit Framework `http://www.metasploit.com/`
- Burpsuite `http://portswigger.net/burp/`
- Kali Linux `http://www.kali.org`

Most popular hacker tools `https://tools.kali.org/` and `http://sectools.org/`

Aktiv testing What happens now?

Think like a hacker

Recon phase – gather information reconnaissance

- Traceroute, Whois, DNS lookups
- Ping sweep, port scan
- OS detection – TCP/IP and banner grabbing
- Service scan – rpcinfo, netbios, ...
- telnet/netcat interact with services

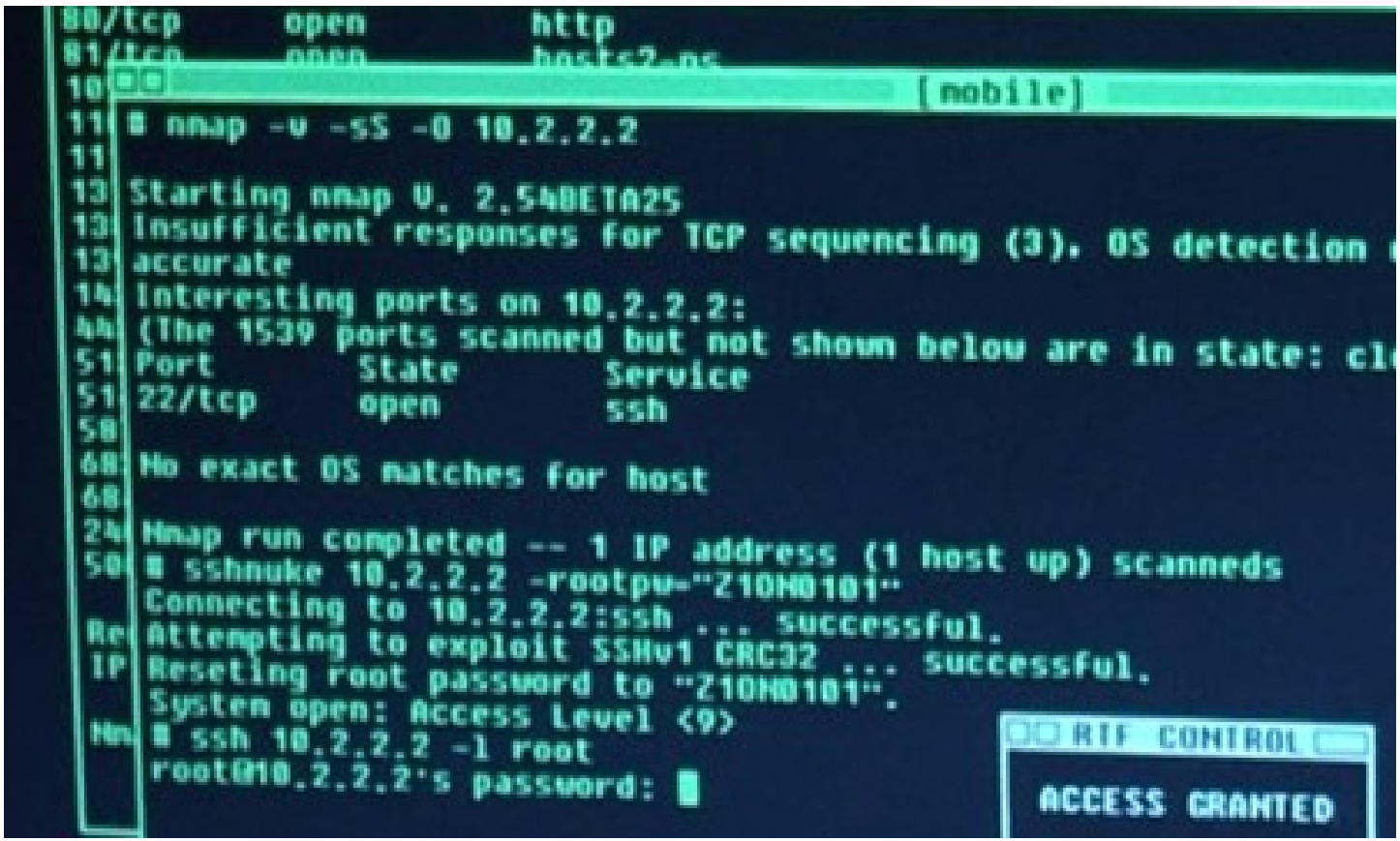
Kali Linux the pentest toolbox

Kali `http://www.kali.org/`

100.000s of videos on youtube alone, searching for kali and $TOOL

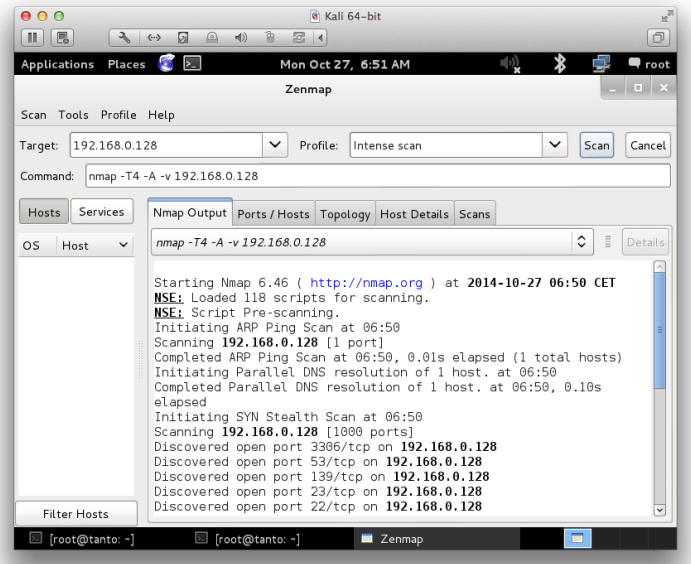
Also versions for Raspberry Pi, mobile and other small computers

Nmap the world

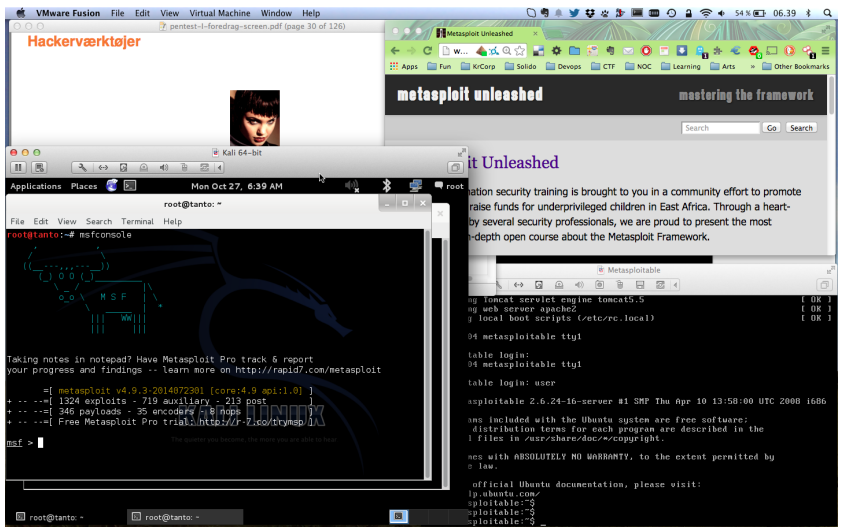


Really do Nmap your world

- 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?
- Includes scripting, and a lot of useful scripts by default
- Often when a new vuln is published, there will be a test script for Nmap



Hackerlab setup



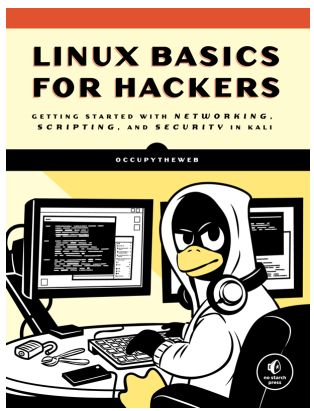
- Create hacker labs, encourage hacker labs!
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine `https://www.kali.org/`

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 (LBhf)

`https://nostarch.com/linuxbasicsforhackers`

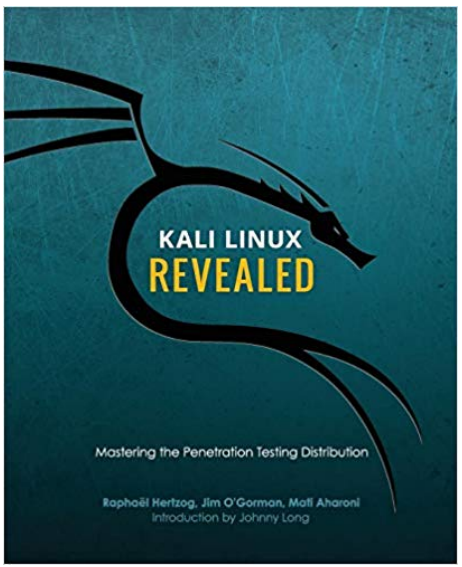


Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali by OccupyTheWeb December 2018, 248 pp. ISBN-13: 9781593278557

Note: this book is about using Unix (Linux) but teaches this using Kali Linux

Running hacker tools comes after you can make directories and find your way around it

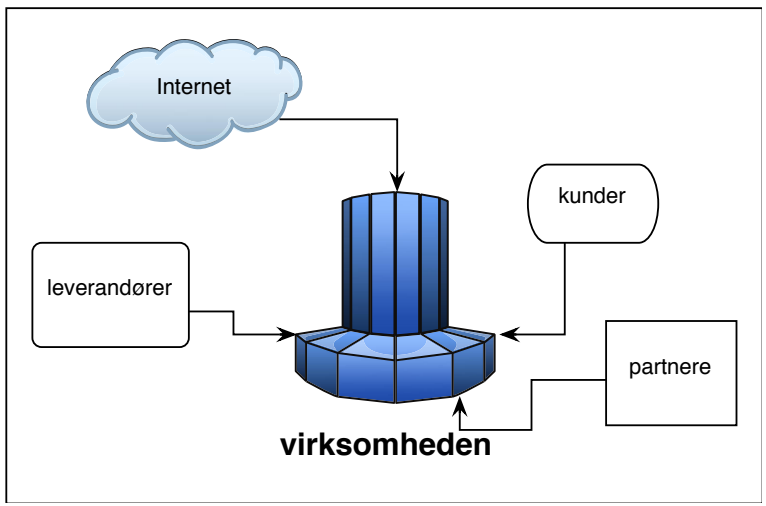
Book: Kali Linux Revealed (KLR)



Kali Linux Revealed Mastering the Penetration Testing Distribution

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

Focus: Firewalls og segmentering

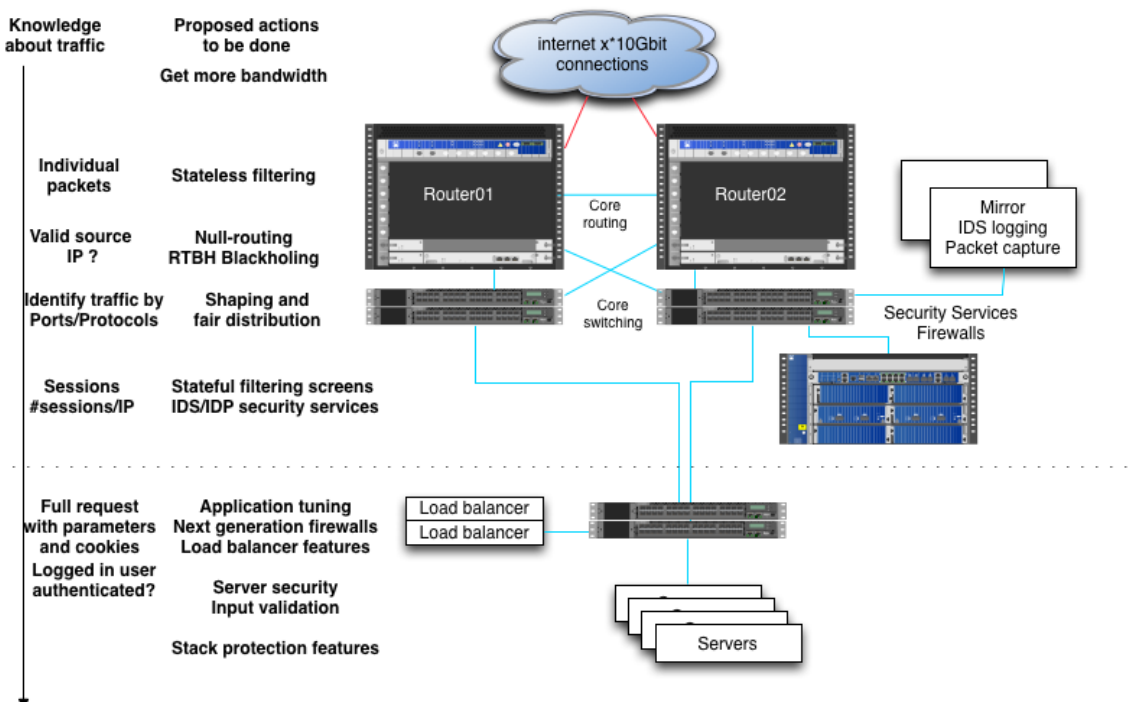


- Hvis du har et netværk, så bør du have en firewall
- En firewall tillader autoriseret trafik og blokerer resten
- Hvornår har du sidst set din løsning efter?
- Hvor lang tid tager det at se en 5.000 linier Cisco ASA config igennem?

Imagine Attacks from the Inside

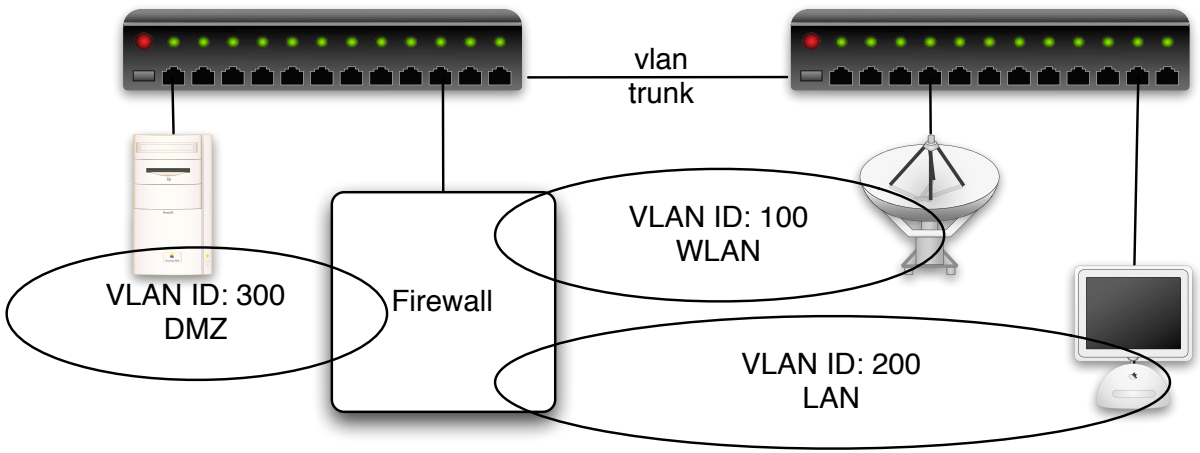
- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?
  NotPetya cost Maersk about 1.9 billion DKK
- entry thought to be via software update of M.E.Doc [uk] an Ukrainian tax preparation program
- Attackers are very creative and have a large attack surface to most companies

Big firewalls



Big firewalls are not a single device

IEEE 802.1q VLANs

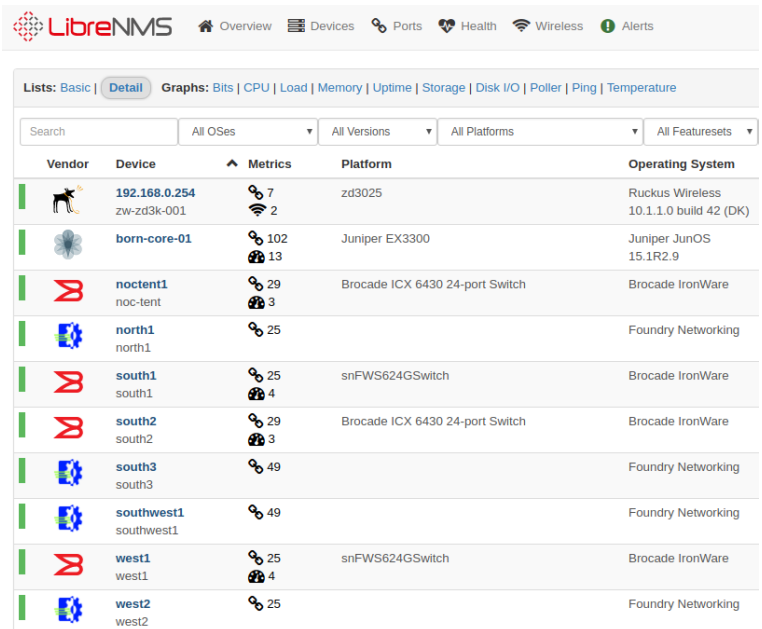


Med 802.1q tillades VLAN tagging på Ethernet niveau

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

VLAN trunking giver mulighed for at dele VLANs ud på flere switches

Netværk generelt

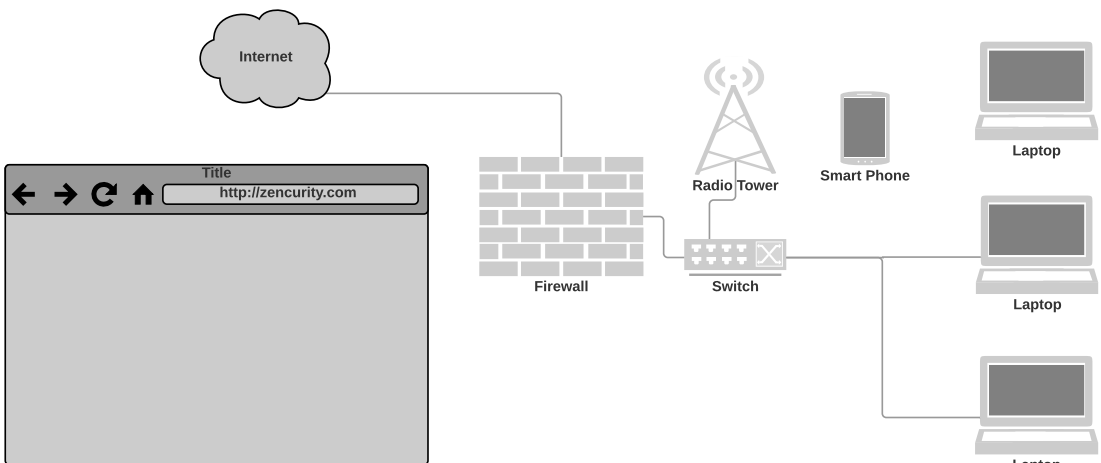


- Måske også på tide lige at se om der er opdateringer til switche
- Jeg anbefaler LibreNMS `https://www.librenms.org/`

Focus: VPN alle steder

- VPN er relevant for alle der har data af værdi
- Sikrer data der flyttes
- Virtual Private Network dækker over klienter der kobler op, og site-2-site

Your Privacy



- Your data travels far
- Often crossing borders, virtually and literally

Maybe use VPN more - or always!

Focus 2020: SSL og TLS

Oprindeligt Secure Sockets Layer (SSL) udviklet af Netscape Communications Inc.

Adopteret af IETF og kaldes Transport Layer Security (TLS)

RFC-3207 SMTP STARTTLS

A Graduate Course in Applied Cryptography, Dan Boneh and Victor Shoup
`https://toc.cryptobook.us/`

Serious Cryptography: a practical introduction to modern cryptography, Jean-Philippe Aumasson. 1st ed. (2017). No Starch Press. ISBN: 9781593278267.

TLS og VPN indstillinger

```
  # Input from https://github.com/tykling/ansible-roles/blob/master/nginx_server/templates/tls.conf.j2#L6
  ssl_protocols                   TLSv1.2 TLSv1.3;
  ssl_ciphers                     ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES256-SHA;
  ssl_prefer_server_ciphers       on;
  ssl_session_cache               shared:SSL:10m;     ssl_session_tickets       off;   ssl_session_timeout    4h;
  ssl_stapling                    on;                 ssl_stapling_verify       on;
  resolver                        105.238.53.1;
  ssl_ecdh_curve secp384r1;                           ssl_dhparam /etc/nginx/dh4096.pem;
  add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
  add_header Referrer-Policy "no-referrer";  add_header X-Content-Type-Options "nosniff";
  add_header X-Frame-Options "DENY";  add_header X-XSS-Protection "1; mode=block";
  add_header Content-Security-Policy "default-src 'self'; script-src 'self; img-src 'self'; object-src 'none'; font-
src 'self'; frame-ancestors 'none' https:";
```

- De fleste har https nu, men er det konfigureret optimalt
- Anbefaler at alle indstillingerne gennemgås regelmæssigt!
- Lav et dokument med de indstillinger I bruger i jeres organisation

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

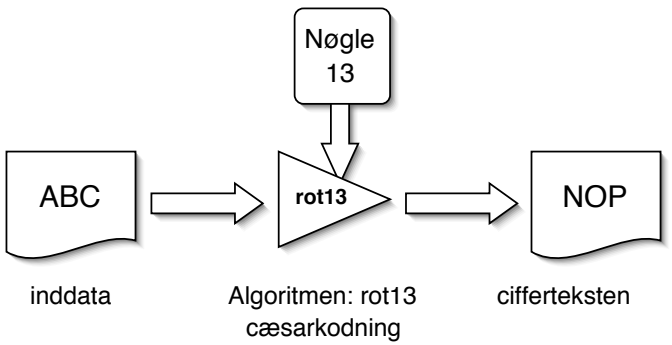
TLS Best Current Practice guidelines

Current recommendations are to phase out Transport Layer Security (TLS) version 1.0 and TLS version 1.1, and all previous versions of Secure Sockets Layer (SSL). DHE is Diffie-Hellman key exchange and should be updated to always use more than 1024 bit for example 2048 or 4096 bits.

- Best current practice can be found in documents like:

`https://english.ncsc.nl/binaries/ncsc-en/documents/publications/2021/january/19/it-security-guidelines-for-transport-layer-security-1/IT+Security+Guidelines+for+Transport+Layer+Security+v2.1.pdf`

VPN indstillinger



PPTP og 3DES, fjern, kill on sight

Check hvert år:

- Certifikater/nøgler - ligesom TLS lange og rulles indimellem
- Algoritmer DES/3DES bye bye, husk både encryption og auth algoritmer
- DH-Group - +15 tak
- Check både client VPN og site-2-site

Anbefalinger til VPN

Use the following guidelines when configuring Internet Key Exchange (IKE) in VPN technologies:
Avoid IKE Groups 1, 2, and 5.
Use IKE Group 15 or 16 and employ 3072-bit and 4096-bit DH, respectively.
When possible, use IKE Group 19 or 20. They are the 256-bit and
384-bit ECDH groups, respectively.
Use AES for encryption.

Paper:
`https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html`

- Certifikater/nøgler - ligesom TLS lange og rulles indimellem
- Algoritmer DES/3DES bye bye, husk både encryption og auth algoritmer
- DH-Group - +15 tak
- Check både client VPN og site-2-site

Focus: 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

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 ....

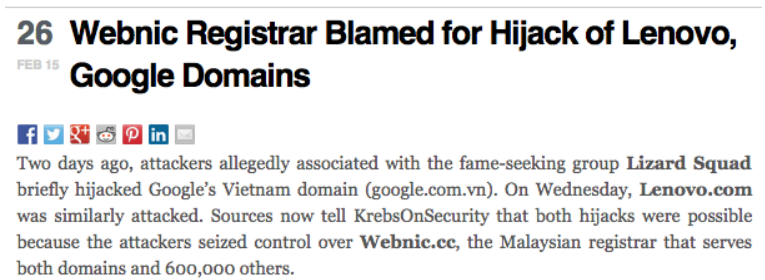
```
IN      MX      10      mail.zencurity.dk.
IN      MX      20      mail2.zencurity.dk.
```

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

DNS attacks, Your registrar



26 Webnic Registrar Blamed for Hijack of Lenovo, Google Domains

FEB 15

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

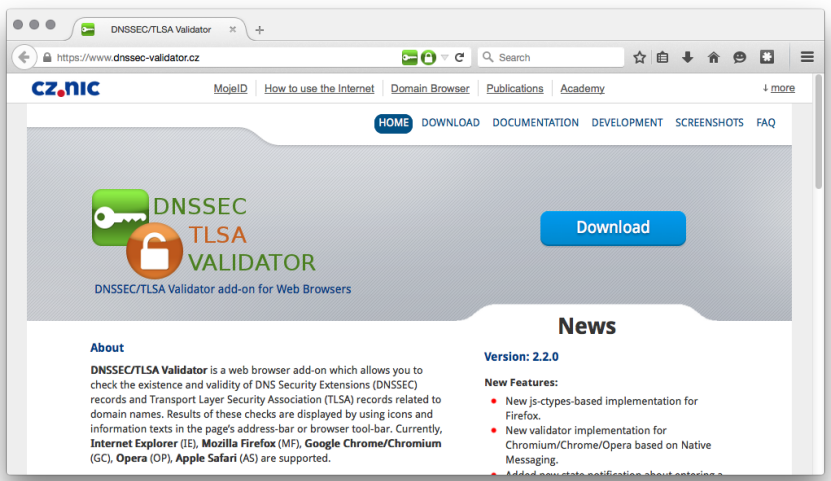
Select DNS providers with care

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`

DNSSEC get started now



"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 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)

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`
- DANE DNS-based Authentication of Named Entities

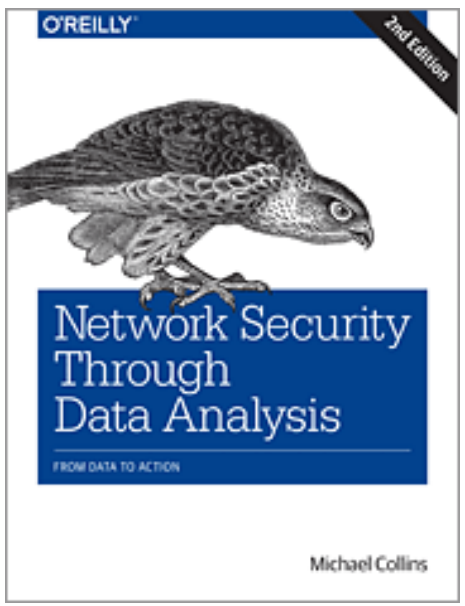
  `https://en.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities`
- Brug allesammen, check efter ændringer!

Jeg er glad for at teste med `https://dmarcian.com/`

Focus: Syslog og monitorering

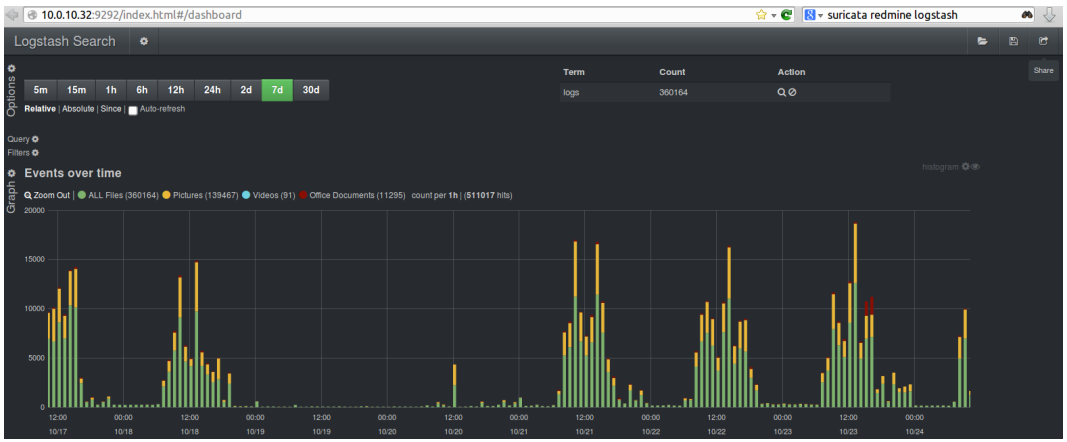
- Vi har allesammen security incidents
- Vi skal kunne efterforske, derfor er et niveau af syslog vigtigt
- Også i dagligdagen til at sikre at systemerne kører optimalt

Network Security Through Data Analysis



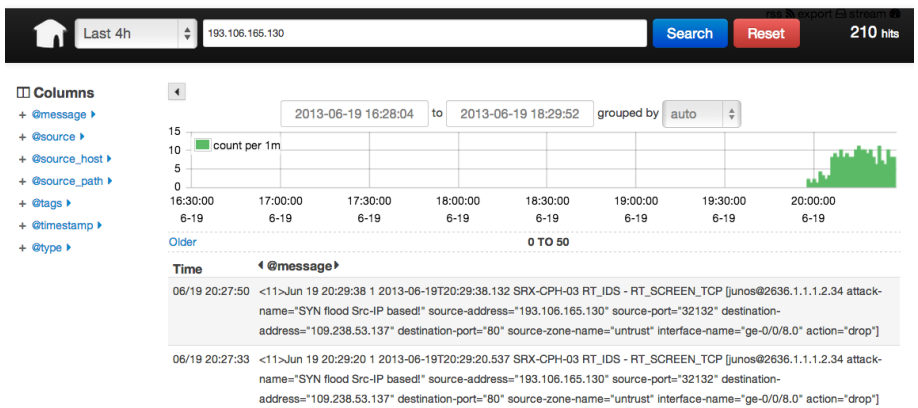
- Low page count, but high value! Recommended.
- *Network Security through Data Analysis*, 2nd edition By Michael S Collins Publisher: O'Reilly Media 06-10-2017, 428 Pages

Graphs and Dashboards!



- Screenshot from Peter Manev, OISF
- Shown are Suricata IDS alerts processed by Logstash and Kibana

Network tools - examples



- Net: Zeek `http://www.zeek.org` Suricata `http://suricata-ids.org`
- DNS: DSC and PacketQ `https://github.com/dotse/packetq/wiki`
- Syslog: Elasticsearch, Logstash, and Kibana, called ELK stack or Elastic stack

Indicators of Compromise and Signatures

An IOC is any piece of information that can be used to objectively describe a network intrusion, expressed in a platform-independent manner. This could include a simple indicator such as the IP address of a command and control (C2) server or a complex set of behaviors that indicate that a mail server is being used as a malicious SMTP relay.

When an IOC is taken and used in a platform-specific language or format, such as a Snort Rule or a Bro-formatted file, it becomes part of a signature. A signature can contain one or more IOCs.

Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders

Storing query logs, old school or needed?

- policy/protocols/ssl/expiring-certs.bro
- policy/protocols/ssl/extract-certs-pem.bro
- policy/protocols/ssl/heartbleed.bro
- policy/protocols/ssl/known-certs.bro
- policy/protocols/ssl/log-hostcerts-only.bro
- policy/protocols/ssl/validate-certs.bro
- policy/protocols/ssl/validate-ocsp.bro
- policy/protocols/ssl/weak-keys.bro

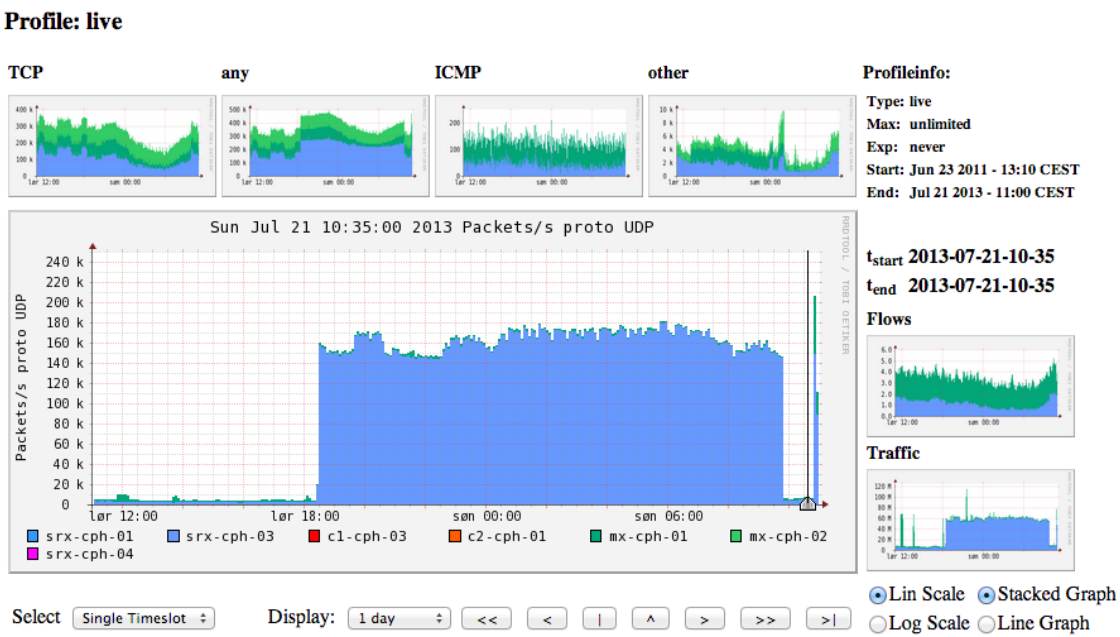
- DNS query logs, keep it for at least a week?
  - with DSC and PacketQ `https://github.com/DNS-OARC/PacketQ`
- SSL/TLS log with Bro/Suricata

  `https://www.bro.org/sphinx-git/script-reference/scripts.html`
- Log with Elasticsearch?

  `https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html`

Uetisk? eller smart hvis man vil spore hvor malware kom ind

Network visibility: Netflow with NFSen



An extra 100k packets per second from this netflow source (source is a router)

Also look into Elastiflow! `https://github.com/robcowart/elastiflow`

How to get started

How to get started searching for security events?

Collect basic data from your devices and networks

- Netflow data from routers
- Session data from firewalls
- Logging from applications: email, web, proxy systems

Centralize!

Process data

- Top 10: interesting due to high frequency, occurs often, brute-force attacks
- *ignore*
- Bottom 10: least-frequent messages are interesting

Case: Maltrail

Maltrail is a malicious traffic detection system, utilizing publicly available (black)lists containing malicious and/or generally suspicious trails, along with static trails compiled from various AV reports and custom user defined lists, where trail can be anything from domain name (e.g. `zvpprsensinaix.com` for Banjori malware), URL (e.g. `http://109.162.38.120/harsh02.exe` for known malicious executable), IP address (e.g. `185.130.5.231` for known attacker) or HTTP User-Agent header value (e.g. `sqlmap` for automatic SQL injection and database takeover tool). Also, it uses (optional) advanced heuristic mechanisms that can help in discovery of unknown threats (e.g. new malware).

`https://github.com/stamparm/maltrail`

Next steps for monitoring

In our network we are always improving things:

Suricata IDS `http://www.openinfosecfoundation.org/`
More graphs, with **automatic identification** of IPs under attack
Identification of **short sessions without data** - spoofed addresses
Alerting from **existing** devices
Dashboards with key measurements

Conclusion: Combine tools!

Logstash pipeline

```
input { stdin { } }
output {
  elasticsearch { host => localhost }
  stdout { codec => rubydebug }
}
```

- Logstash receives via **input**
- Processes with **filters** - grok
- Forward events with **output**
- Today many tools can produce JSON with fields already
- Elastic also have defined: Elastic Common Schema (ECS)
  `https://www.elastic.co/guide/en/ecs/current/index.html`

Logstash as SNMPtrap and syslog server

```
input {
  snmptrap {
    host => "0.0.0.0"
    type => "snmptrap"
    port => 1062
    community => "xxxxx"
  }
  tcp {
    port => 5000
    type => syslog
  }
  udp {
    port => 5000
    type => syslog
  }
}
```

- We run logstash on port 5000 - but use IPtables port forwarding

Maybe you have a device sending SNMP traps right now ...

Reklame: KEA Kompetence SIEM og log-analyse (5 ECTS)

Primary literature:

- Data-Driven Security: Analysis, Visualization and Dashboards Jay Jacobs, Bob Rudis ISBN: 978-1-118-79372-5 February 2014 https://datadrivensecurity.info/
- Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan by Jeff Bollinger, Brandon Enright, and Matthew Valites
- Intelligence-Driven Incident Response ISBN: 9781491934944 Scott Roberts
- Security Operations Center Building, Operating, and Maintaining your SOC ISBN: 9780134052014 Joseph Muniz

Materiale er på min github @kramse

Lektionsplan:

`https://zencurity.gitbook.io/kea-it-sikkerhed/siem-and-log-analysis/lektionsplan`

Focus: Incident Response og reaktion

- Fortsat fra logningen ... hvad så nu!
- Hvis du har en sikkerhedshændelse skal den håndteres
- jo hurtigere og mere effektivt det håndteres jo bedre

Lifeguard training photo by Margarida CSilva on Unsplash

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 files

or the other way

Attackers used a LinkedIn job ad and Skype call to breach bank's defences

The attack

One of these is the Chilean news site's claim that the attack started with a LinkedIn advert offering a developer role to which a Redbanc employee replied.

The attackers set up a Skype call to conduct an interview during which the individual was tricked into downloading a file called ApplicationPDF.exe, sent via a weblink, which subsequently infected the employee's computer.

`https://nakedsecurity.sophos.com/2019/01/21/attackers-used-a-linkedin-job-ad-and-skype-call-to-breach-banks-defences/`

Øv krisesituationer

- Lav rollespil
- Lav tabletop exercises

Spørgsmål og mere debat

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse