



Welcome to

It-sikkerhedsupdate

2020

Henrik Kramselund Jereminsen hkj@zecurity.com @kramse  

Slides are available as PDF, kramse@Github
`it-sikkerhedsupdate-2020-short.tex` in the repo `security-courses`

slides are available on Github

Goal for today



FreeFoto.com

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 2h including break
- Inspiration for solving the tasks, prioritizing the tasks
- I dont have tailor made solutions or easy answers for your organisation
- Less presentation, more dialog

Happy New Year



- Same problems
- Repeat last year?
- ... or try something new!
- 2020 was a nightmare of break-ins and data leaks
- GDPR is here and the snow ball is rolling



Try not to panic, but there are lots of threats

Paranoia defined



par·a·noi·a

/parə'noiə/ ◄)

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

GREEK

MODERN LATIN

noos

mind

paranoos
distracted

early 19th cent.

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

Hackers don't give a shit:

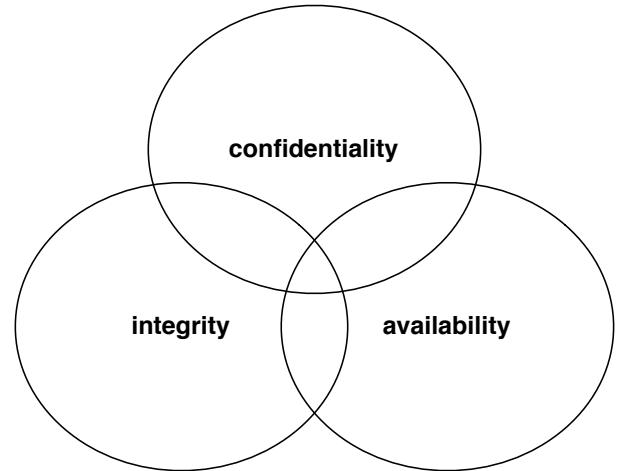


KIWICON III
28TH & 29TH NOVEMBER 2009

New Zealand's Hacker con - Wellington

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fix it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that configuration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benefit doesn't stack up
- "Nobody else could figure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justification
- You can't show Return on Investment
- You contracted out that risk

Confidentiality Integrity Availability



We want to protect something

Confidentiality - data is kept a secret

Integrity - data is not subjected to unauthorized changes

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

Security engineering 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

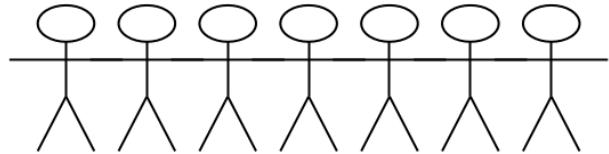
Focus 2020



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

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

Focus 2020: 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

Centraliseret brugerstyring



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



The 50 Most Used Passwords

- | | | | | |
|--------------|--------------|----------------|--------------|-------------|
| 1. 123456 | 11. 123123 | 21. mustang | 31. 7777777 | 41. harley |
| 2. password | 12. baseball | 22. 666666 | 32. f*cky*u | 42. zxcvbnm |
| 3. 12345678 | 13. abc123 | 23. qwertyuiop | 33. qazwsx | 43. asdfgh |
| 4. qwerty | 14. football | 24. 123321 | 34. jordan | 44. buster |
| 5. 123456789 | 15. monkey | 25. 1234...890 | 35. jennifer | 45. andrew |
| 6. 12345 | 16. letmein | 26. p*s*y | 36. 123qwe | 46. batman |
| 7. 1234 | 17. shadow | 27. superman | 37. 121212 | 47. soccer |
| 8. 111111 | 18. master | 28. 270 | 38. killer | 48. tigger |
| 9. 1234567 | 19. 696969 | 29. 654321 | 39. trustno1 | 49. charlie |
| 10. dragon | 20. michael | 30. 1qaz2wsx | 40. hunter | 50. robert |

Source: <https://wpengine.com/unmasked/>

Your data has already have been owned by criminals



A screenshot of a web browser displaying the Have I Been Pwned? website at <https://haveibeenpwned.com>. The page has a teal header with the site's logo and navigation links. Below the header is a large white button containing the text ':--have i been pwned?'. Underneath the button, a sub-header reads 'Check if you have an account that has been compromised in a data breach'. A search input field contains the email address 'hlk@kramse.org'. To the right of the input field is a dark blue button labeled 'pwned?'. Below the search area, a large red banner displays the message 'Oh no — pwned!' in white. Underneath the banner, smaller text states 'Pwned on 7 breached sites and found no pastes (subscribe to search sensitive breaches)'.

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

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

Check your 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/>

Focus 2020: 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

Hvad er 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

The screenshot shows the RackTables web interface. At the top, it displays "RackTables" and "Hello, RackTables Administrator. This is RackTables 0.17.0. Click here to logout". Below this is a search bar labeled "Search". The main area contains seven categories with corresponding icons:

- Rackspace**: Represented by a rack unit icon.
- Objects**: Represented by a server tower icon.
- IPv4 space**: Represented by a stack of IP address blocks icon.
- Files**: Represented by a folder icon.
- Configuration**: Represented by two wrenches icon.
- Reports**: Represented by a line graph icon.
- IPv4 SLB**: Represented by a stack of server icons.

- Der findes mange systemer
- 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



Flere detaljer i gigantisk hotel-hack: 5,25 mio. ukrypterede pasnumre taget
Jakob Møllerhøj | Sikkerhed | 07. jan 2019

7,6 millioner spillerkonti løkket fra populært onlinespil
Niels Møller Kjemstrup | Sikkerhed | 07. jan 2019

Største løk i tysk historie: Politikeres og kunstneres data smidt på nettet
Morten Egedal | Sikkerhed | 04. jan 2019

Gentleman-aftale mellem politiske partier skal danne mur mod dataløk, hacking og fake news
Louise Holst Andersen | Sikkerhed | 04. jan 2019

Boligfond beklager løk af følsomme persondata: En menneskelig fejl
Sikkerhed | 28. dec 2018

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

Focus 2020: 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, må der downloades data til offline
- Er laptops sikre, og hvad betyder det?

Are your data secure - data at rest



*...et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercit...
commodo consequat. Duis aute irure dolor in reprehenderit in voluptate veli...
ob ea soluad incor... quae egen ium im... end. Officia deserunt mollit a...orum Et
harumd dereud fac... er expedit distinct. Gothica quam nunc putamus parum...
litterarum formas humanitatis per seacula quarta; modo typi... is videntur ... clari fiant
sollemnes in futurum; litterarum f... humanitatis per seacu... cima et quinta decima, modo typi
qui nu... tur parur... llemnes in futuru... rit ! Nam liber te conscient to factor
tum p... ioque civi... eque pecun moc... honor et imper r... et,
conse... ng elit, sec... ut dolore magna aliquam is nostrud exercitation... lo
conse... e in voluptate ve... esse cillum dolore eu fugiat nulla pariatur. At vver e... am
dignissum qui blandit est praesent.*

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!

2018 attack



Drive	1	2	3	4	5	6	7	8	9	Impact
Crucial MX100 (all form factors)	X	X	X							X Compromised
Crucial MX200 (all form factors)	X	X	X							X Compromised
Crucial MX300 (all form factors)	✓	✓	✓		X	✓	✓	✓	✓	X Compromised
Samsung 840 EVO (SATA)	X	✓	✓		✓	✓	✓	X	✓	~ Depends
Samsung 850 EVO (SATA)	X	✓	✓		✓	✓	✓	✓	✓	~ Depends
Samsung T3 (USB)				X						X Compromised
Samsung T5 (USB)				X						X 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 - 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 2020: Penetration testing



A screenshot of the Burp Suite interface. The top navigation bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', and 'Help'. Below this is a main toolbar with tabs for 'Dashboard', 'Target' (which is selected and highlighted in blue), 'Proxy', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Project options', and 'User options'. Underneath the main toolbar is a secondary toolbar with 'Intercept' (selected and highlighted in blue), 'HTTP history', 'WebSockets history', and 'Options'. At the bottom of the interface are buttons for 'Forward', 'Drop', 'Intercept is on' (which is highlighted in red), and 'Action'. Finally, at the very bottom are 'Raw' and 'Hex' tabs.

- 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
- Try scanning everything, start in a small corner, expand
- Scan all your 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 which flaws available

Check *Security Assessment of Cisco ACI*

<https://www.ernw.de/en/whitepapers/issue-68.html>

Hackertools are for everyone!

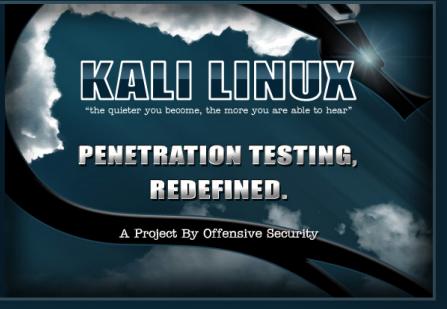


- Hackers work all the time to break stuff, Use hackertools:
- Nmap, Nping <http://nmap.org>
- Wireshark - <http://www.wireshark.org/>
- Aircrack-ng <http://www.aircrack-ng.org/>
- Metasploit Framework <http://www.metasploit.com/>
- Burpsuite <http://portswigger.net/burp/>
- Kali Linux <http://www.kali.org>

Most popular hacker tools <http://sectools.org/>

The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new?](#)



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

Kali 64-bit

Mon Oct 27, 6:51 AM

Zenmap

Scan Tools Profile Help

Target: 192.168.0.128 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.0.128

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

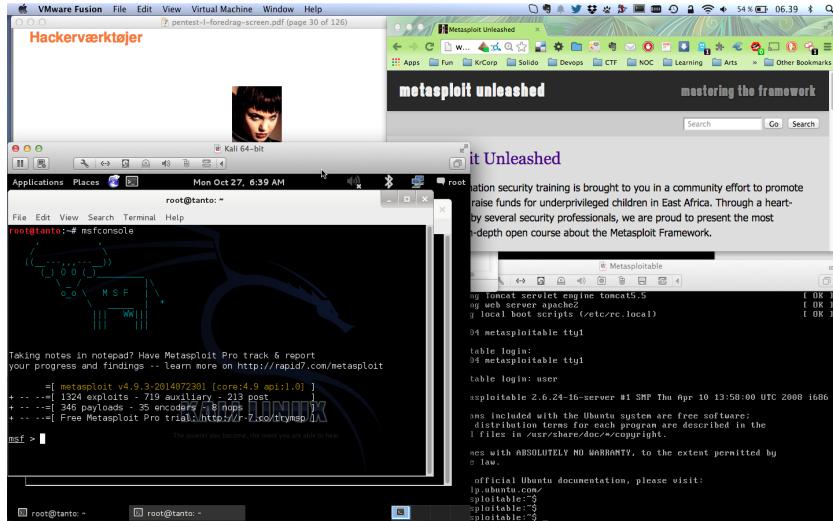
nmap -T4 -A -v 192.168.0.128

Starting Nmap 6.46 (<http://nmap.org>) at 2014-10-27 06:50 CET
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 06:50
Scanning 192.168.0.128 [1 port]
Completed ARP Ping Scan at 06:50, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 06:50
Completed Parallel DNS resolution of 1 host at 06:50, 0.10s elapsed
Initiating SYN Stealth Scan at 06:50
Scanning 192.168.0.128 [1000 ports]
Discovered open port 3306/tcp on 192.168.0.128
Discovered open port 53/tcp on 192.168.0.128
Discovered open port 139/tcp on 192.168.0.128
Discovered open port 23/tcp on 192.168.0.128
Discovered open port 22/tcp on 192.168.0.128

Filter Hosts

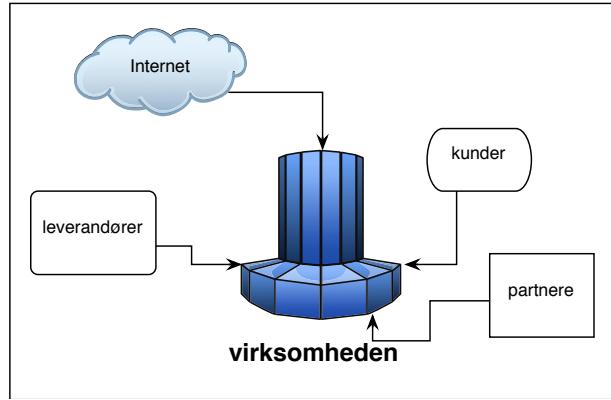
[root@tanto: ~] [root@tanto: ~] Zenmap [root@tanto: ~]

Hackerlab setup



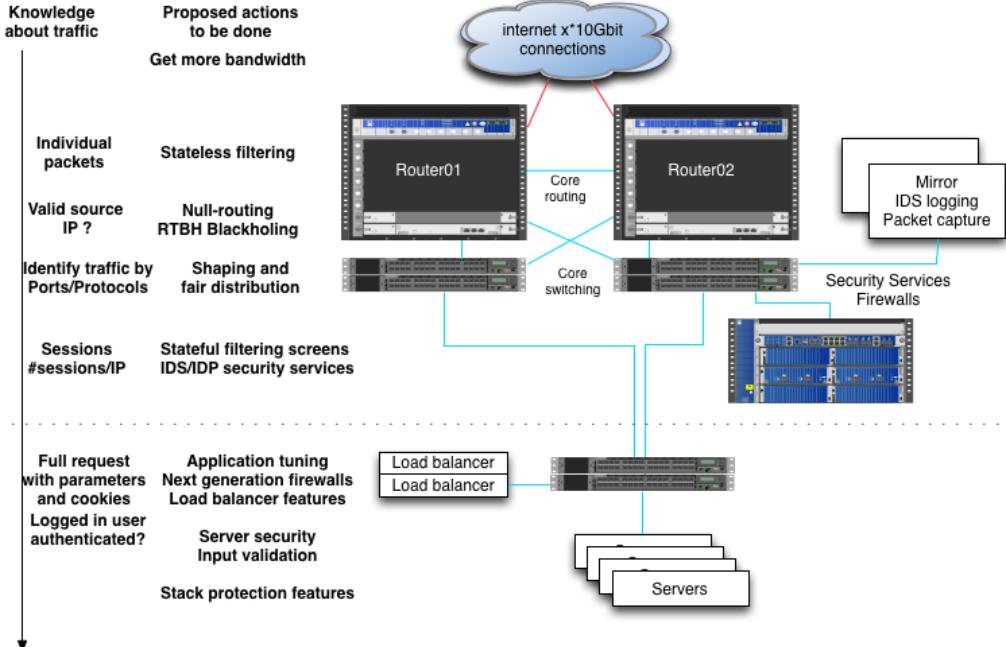
- Create hacker labs, encourage hacker labs!
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine <https://www.kali.org/>

Focus 2020: 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?
- Segmentering af netværk er en solid sikkerhedsforanstaltning

Big firewalls



Big firewalls are not a single device

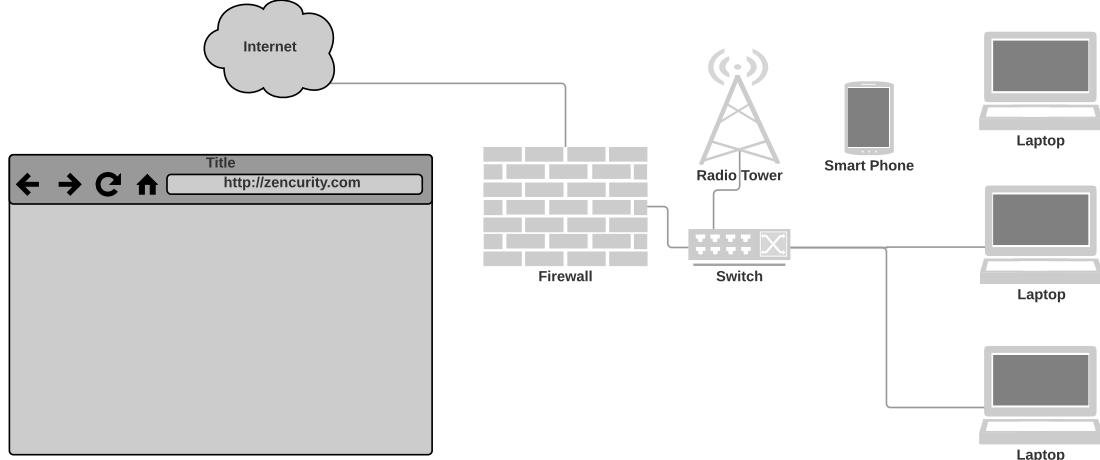
PS also check for updates to your network devices, at least once a year 😊

Focus 2020: 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: 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/> - kræver hostnavn og til HTTPS
- sslscan kommandoen kan checke alle jeres TLS sites, også på IP

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:

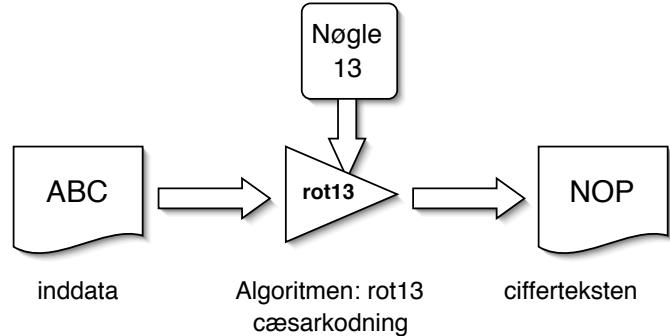
```
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048
```

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

SSLscan can by IP and also SMTP STARTTLS and others

<https://sikkerpånettet.dk/>

VPN indstillinger



PPTP, fjern, kill on sight

Check hvert år:

- Certifikater/nøgler - ligesom TLS lange og rulles indimellem
- Algoritmer DES/3DES, SHA1, MD5 bye bye, husk både encryption og auth
- DH-Group - mindst +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
- Check både client VPN og site-2-site

Focus 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

DNSSEC get started now



The screenshot shows a web browser window with the URL <https://www.dnssec-validator.cz>. The page is titled "DNSSEC/TLSA Validator". It features a logo for "DNSSEC" with a green key icon and "TLSA" with an orange padlock icon. Below the logo, it says "DNSSEC/TLSA Validator add-on for Web Browsers". A prominent blue "Download" button is centered. To the right, there's a "News" section with a "Version: 2.2.0" heading and a list of "New Features" including support for Firefox, Chromium/Chrome/Opera, and Native Messaging. The top navigation bar includes links for "MojID", "How to use the Internet", "Domain Browser", "Publications", "Academy", "HOME", "DOWNLOAD", "DOCUMENTATION", "DEVELOPMENT", "SCREENSHOTS", and "FAQ". The "cz.nic" logo is at the top left.

"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 displayed 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 2020 - 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>
- DNSSEC Domain Name System Security Extensions
https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- 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 2020: 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 tools - examples



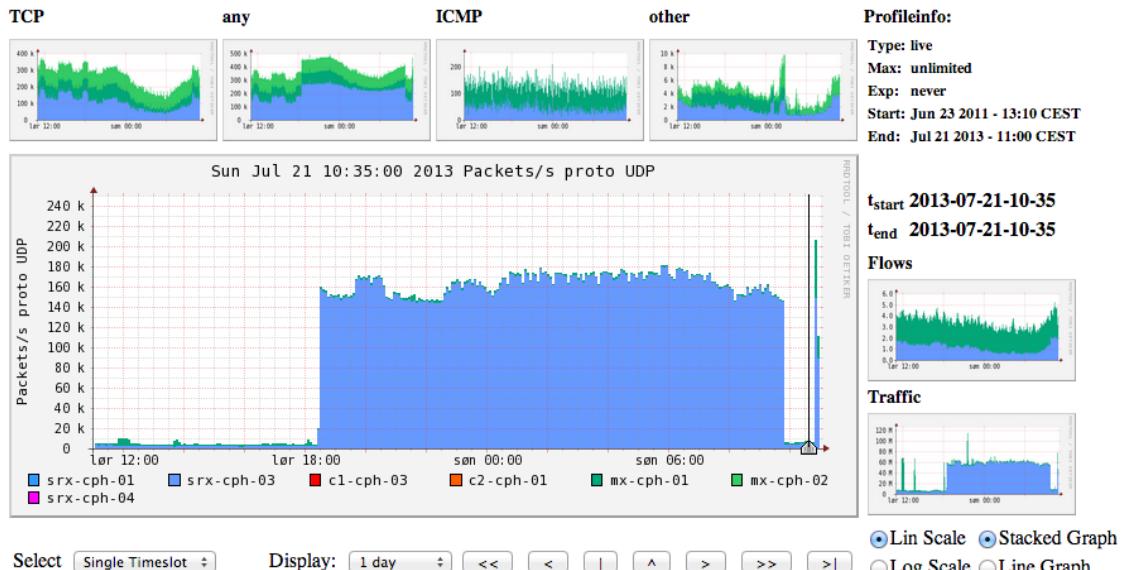
- Net + SSL/TLS: Zeek <http://www.bro-ids.org>
Suricata <http://suricata-ids.org>
- DNS query logs, keep it for at least a week?
 - with DSC and PacketQ <https://github.com/DNS-OARC/PacketQ>
- Log with Elasticsearch?

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

Network visibility: Netflow with NFSen



Profile: live



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



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>

Suricata with Dashboards



Picture from Twitter

<https://twitter.com/nullthreat/status/445969209840128000>

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

Reklame: SIEM og log-analyse (5 ECTS)



Teaching dates: **26/11 2020**, 1/12 2020, 3/12 2020, 8/12 2020, 10/12 2020,
15/12 2020, 17/12 2020 Exam: Date 7/1 2021

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

https://kompetence.kea.dk/kurser-fag/siem-og-loganalyse?kust_id=5154

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

Focus 2020: 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

Flere detaljer i gigantisk hotel-hack: 5,25 mio. ukrypterede pasnumre taget

Jakob Møllerhøj | Sikkerhed | 07. jan 2019

3

7,6 millioner spillerkonti løkket fra populært onlinespil

Niels Møller Kjemstrup | Sikkerhed | 07. jan 2019

2

Største løk i tysk historie: Politikeres og kunstneres data smidt på nettet

Morten Egedal | Sikkerhed | 04. jan 2019

2

Gentleman-aftale mellem politiske partier skal danne mur mod dataløk, hacking og fake news

Louise Holst Andersen | Sikkerhed | 04. jan 2019

12

Boligfond beklager løk af følsomme persondata: En menneskelig fejl

Sikkerhed | 28. dec 2018

6



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/2020/01/21/attackers-used-a-linkedin-job-ad-and-skype-call-to-breach-banks-defences/>

Øv krisesituationer



- Lav rollespil
- Lav tabletop exercises

Spørgsmål og mere debat



"On the Internet, nobody knows you're a dog."

Henrik Kramselund Jereminsen hkj@zecurity.com @kramse  