



Welcome to

12. System Security in Practice

KEA Kompetence Computer Systems Security 2025

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg
12-systems-security-in-practice.tex in the repo security-courses

Goals



- Various tips and tricks for real environments
- Return to email security – uses many parts of system security
- Start checking your own environments with knowledge from this course

Photo by Thomas Galler on Unsplash

Plan



Subjects

- Infrastructure security
- Email security as an example

Exercises – System Security in Practice

- Talk more about centralized logging
- Configure SSH keys for more secure access
- Talk about email security – modern standards and all that

Reading Summary



DSH chapter 23: The Extra Mile

After reading this book, you should be ready to provide the sound building blocks of an information security program. You should also be fully equipped to handle the common insecure practices that we've seen in so many environments. But the learning doesn't stop here! Here in the extra mile we'll give you some additional tidbits of information and some great resources for you to go check out that will make your defenses that much stronger.

Source: *Defensive Security Handbook: Best Practices for Securing Infrastructure*, Lee Brotherston, Amanda Berlin
ISBN: 978-1-491-96038-7

- Email servers and DNS servers – let's check these for your organizations

Goals for today:



- System security in a larger context
- Talk about infrastructure security as a whole – a holistic view
- Try using our knowledge in a made up setting

Network Security



- Goals of security policies
- Data related to company plans is to be kept secret. In particular sensitive corporate data. available only to those who need to know.
- When a customer provides data to a company as part of a purchase, the data and all information about the customer, are to be available only to those who fill the order. Company analysts may obtain statistics about a number of orders for planning purposes.
- Releasing sensitive data requires the consent of the company's officials and lawyers.

Shortened a bit from the Bishop book.

System security in practice



Describe the organization - three main internal organizations: CSG, DG, CG

Define data classes:

- Public data,
- Development data for existing products
- Development data for future products
- Corporate data
- Customer data

User classes: Outsiders, Developers, Corporation executives, Employees

Rules for data and user access to data



The classes of users, data and their allowed accesses

The classes of users, data and their allowed accesses

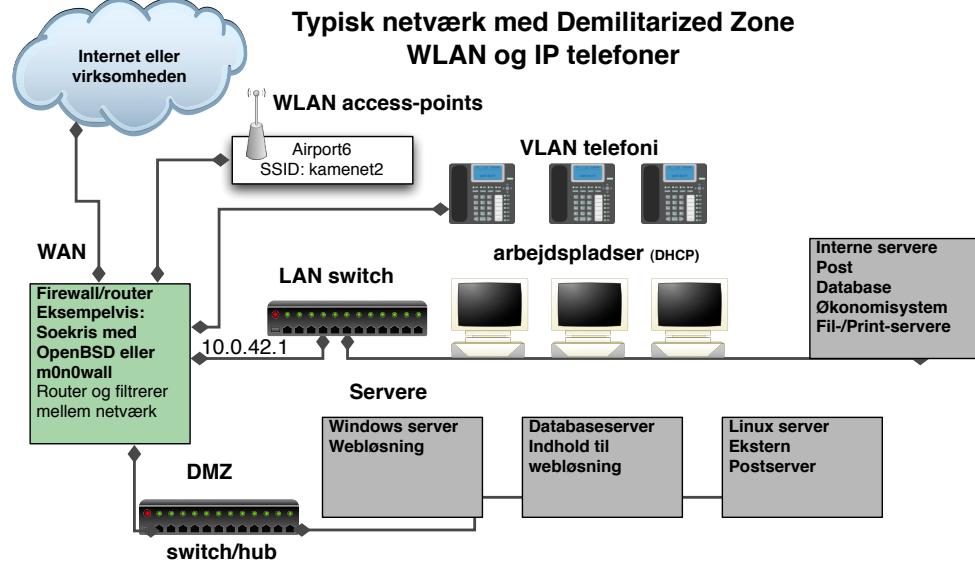
	Outsiders	Developers	Corporation Executives	Employees
Public data	Read	Read	Read	Read
Development data existing products		Read	Read	
Development data for future products		Read, Write	Read	
Corporate data			Read, Write	
Customer data	Write		Read	Read, Write

This is an access control matrix combining elements of confidentiality and integrity, compare to our models from earlier chapters.

Book defines transformation rules how specific classes of people can move data from one class to another.

Corporate officers want the systems to be available for 99% of the time, leaving the last 1% for planned maintenance and unexpected downtimes.

Network separation



Often even more DMZ like networks needed: guests, partners, support from vendors, Voice over IP systems etc.

BTW NAT is NOT a security feature

Network Servers



Mail servers , local mailserver gets internet mail through 3rd party - does filtering, anti-spam etc.
OR outsourced email at some vendor

Web servers - most companies with basic web pages outsource these to some hosting company

Companies which provide service over internet has a whole infrastructure separated from their local network, most likely at hosting provider or cloud provider

DMZ DNS server, split DNS etc. Dont run authoritative DNS yourself, not worth the time. Do run local resolvers for your clients. DNS resolver can also be configured with block lists, blocked Top-level Domains etc.

DMZ log server - do run log servers, or at least local forwarding proxies that can collect data even when network is down and forward

Above is how I see this most often – in Denmark at least

User Security



User accounts and named users are required for good security

Less shared user accounts, more accountability

System accounts are needed though

January 2013: Github Public passwords?



The screenshot shows a web browser window with the GitHub homepage. The address bar displays the URL <https://github.com/search?q=-----BEGIN+RSA+PRIVATE+KEY-----&type=Code&ref=searchresults>. The GitHub logo is at the top left, followed by navigation links: Explore GitHub, Search, Features, Blog, Sign up for free, and Sign in. Below the header is a search bar with the placeholder text "Search" and a search button. On the left, there's a sidebar with three categories: Repositories (277), Code (77,468, which is highlighted in orange), and Users. The main content area shows a search result for a file named "paypal_production_key_private.pem" located in the repository "kordless/zoto-server". The file content is partially visible, showing the beginning of an RSA private key.

Sources:

<https://twitter.com/brianaker/status/294228373377515522>

<http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-details/>

<http://www.leakedin.com/>

<http://www.offensive-security.com/community-projects/google-hacking-database/>

Use different passwords for different sites, yes - every site!

Simple Network Management Protocol



SNMP er en protokol der supporteres af de fleste professionelle netværksenheder, såsom switche, routere

hosts - skal slås til men følger som regel med

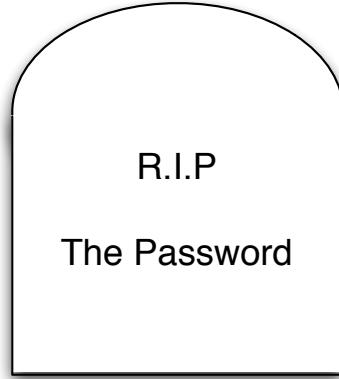
SNMP bruges til:

- *network management*
- statistik
- rapportering af fejl - SNMP traps

sikkerheden baseres på community strings der sendes som klartekst ...

det er nemmere at brute-force en community string end en brugerid/kodeord kombination

Are passwords dead?



Can we stop using passwords?

Alec Muffett on Passwords has a long list of password related information, from the author of crack [http://en.wikipedia.org/wiki/Crack_\(password_software\)](http://en.wikipedia.org/wiki/Crack_(password_software))

<http://dropsafe.crypticide.com/muffett-passwords>

https://en.wikipedia.org/wiki/Alec_Muffett

Cain og Abel



The screenshot shows the Cain and Abel interface. On the left, a tree view under the 'Cracker' tab lists various hash types: LM & NTLM Hashes (4), NTLMv2 Hashes (0), MS-Cache Hashes (0), PWL files (0), Cisco IOS-MD5 Hashes (1), Cisco PIX-MD5 Hashes (0), APOP-MD5 Hashes (0), CRAM-MD5 Hashes (0), OSPF-MD5 Hashes (0), RIPv2-MD5 Hashes (0), VRRP-HMAC Hashes (0), VNC-3DES (0), MD2 Hashes (0), MD4 Hashes (0), MD5 Hashes (0), SHA-1 Hashes (0), and SHA-2 Hashes (0). On the right, a table displays cracked user accounts:

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	chall
Administrator	* empty *	*	* empty *	AAD3B435B514...	31D6CFE0D16A...	
ASPNET				181185C0DCAF...	93D70CEAC461...	
Guest	* empty *	*	* empty *	AAD3B435B514...	31D6CFE0D16A...	
hlk		*		C5FD535616AD...	6DF8D494F249...	

Cain og Abel *anbefales til demoer* <http://www.oxid.it>

Bruger selv John the Ripper eller Hashcat hvis jeg skal lave brute forcing

John the ripper



John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

UNIX passwords kan knækkes med alec Muffets kendte Crack program eller eksempelvis John The Ripper <http://www.openwall.com/john/>

Cracking passwords



- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

Source:

<http://hashcat.net/wiki/>

<http://www.openwall.com/john/>

Parallella John



Henrik Kramshoer retweeted

Solar Designer @solardiz

\$ 0 t + 7

Similarly expensive Xeon E5-2670 is 2.4x to 3.3x slower than Zynq 7045
#FPGA on this test, yet consumes ~20x more power; GPUs are way behind



Henrik Kramshoer retweeted

Solar Designer @solardiz

\$ 0 t + 7

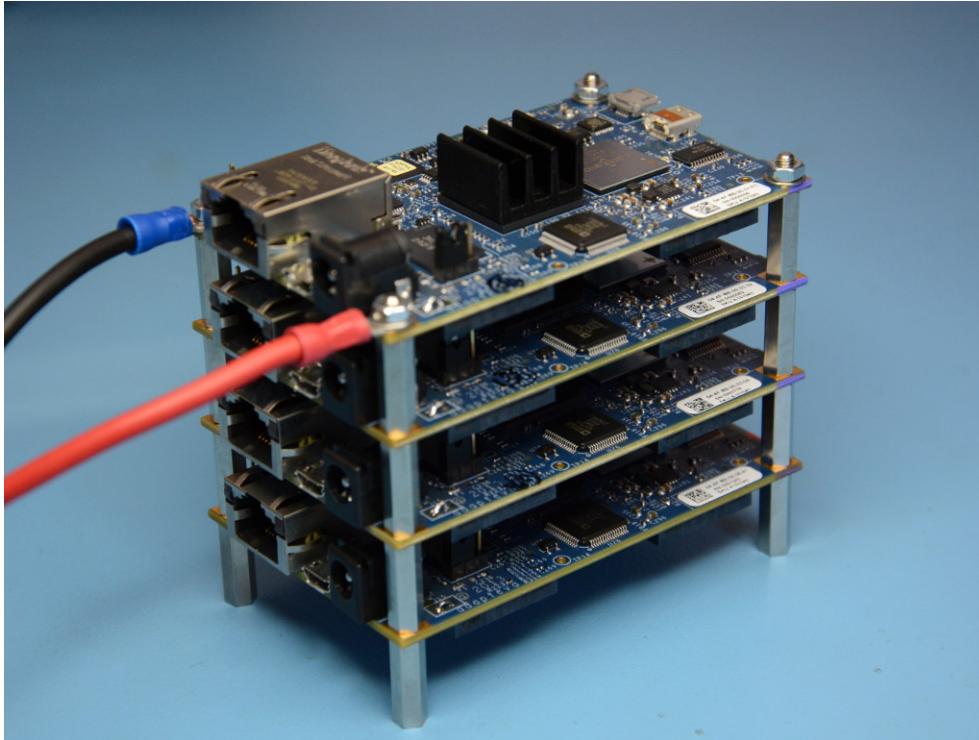
On last night to submit WOOT final paper, @kmalvoni got bcrypt \$2a\$05 to
20538 c/s, \$2a\$12 to 226 c/s on Zynq 7045 #FPGA. Not the limit yet.

15h

<https://twitter.com/solardiz/status/492037995080712192>

Expect specialized hardware to be used by NSA, GCHQ, and perhaps even organised crime

Stacking Parallella boards



<http://www.parallel.org/power-supply/>

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/>

Pass the hash



Lots of tools in pentesting pass the hash, reuse existing credentials and tokens *Still Passing the Hash 15 Years Later*
<http://passing-the-hash.blogspot.dk/2013/04/pth-toolkit-for-kali-interim-status.html>

If a domain is built using only modern Windows OSs and COTS products (which know how to operate within these new constraints), and configured correctly with no shortcuts taken, then these protections represent a big step forward.

Source:

<http://www.harmj0y.net/blog/penetesting/pass-the-hash-is-dead-long-live-pass-the-hash/> <https://samsclass.info/lulz/pth-8.1.htm>

Produktionsmodning af miljøer



Tænk på det miljø som servere og services skal udsættes for

Sørg for hærdning og tænk generel sikring:

- Opdateret software - ingen kendte sikkerhedshuller eller sårbarheder
- Fjern **single points of failure** - redundant strøm, ekstra enheder, to DNS servere fremfor en
- Adskilte servere - interne og eksterne til forskellige formål
 - Eksempelvis den interne postserver hvor alle e-mail opbevares og en DMZ-postserver til ekstern post
- Lav filtre på netværket, eller på data - firewalls og proxy funktioner
- Begræns adgangen til at læse information
- Begræns adgangen til at skrive information - eksempelvis databaser
- Brug **least privileges** - sørg for at programmer og brugere kun har de nødvendige rettigheder til at kunne udføre opgaver
- Følg med på områderne der har relevans for virksomheden og *jeres* installation

Meld jer på security mailinglister for de produkter I benytter, også open source

Change management



Er der tilstrækkeligt med fokus på software i produktion

Kan en vilkårlig server nemt reetableres

Foretages rettelser direkte på produktionssystemer

Er der fall-back plan

Burde være god systemadministrator praksis

Fundamentet skal være iorden



Sørg for at den infrastruktur som I bygger på er sikker:

- redundans
- opdateret
- dokumenteret
- nem at vedligeholde

Husk tilgængelighed er også en sikkerhedsparameter

Fokus 2025



- Brugerstyring
- Asset management
- Laptop sikkerhed
- VPN alle steder
- Penetration testing
- Firewalls og segmentering
- TLS og VPN indstillinger
- DNS og email
- Syslog og monitorering
- Incident Response og reaktion

Check eventuelt IT sikkerhedsupdate præsentationen – samme råd siden 2019:

<https://github.com/kramse/security-courses/tree/master/presentations/misc/it-sikkerhedsupdate-2019>

Design a robust network Isolation and segmentation

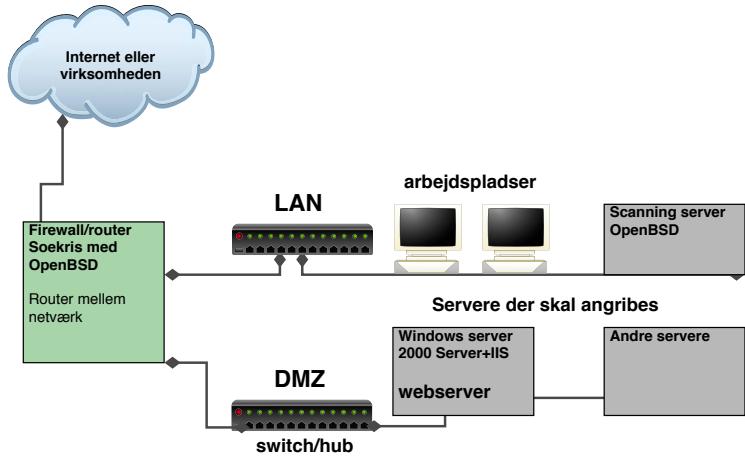


Hvad kan man gøre for at få bedre netværkssikkerhed?

- Bruge switcher - der skal ARP spoofes og bedre performance
- Opdele med firewall til flere DMZ zoner for at holde utsatte servere adskilt fra hinanden, det interne netværk og Internet
- Overvåge, læse logs og reagere på hændelser

Husk du skal også kunne opdatere dine servere

Basic Network Security Pattern Isolate in VLANs



Du bør opdele dit netværk i segmenter efter trafik

Du bør altid holde interne og eksterne systemer adskilt!

Du bør isolere farlige services i jails og chroots

Brug port security til at sikre basale services DHCP, Spanning Tree osv.

Exercise

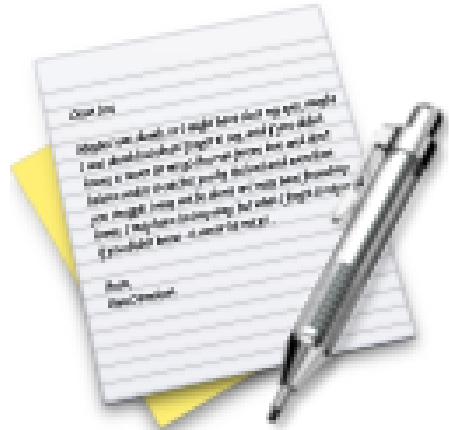


Now lets do the exercise

i Configure SSH keys for more secure access 30min

which is number **22** in the exercise PDF.

Exercise



Now lets do the exercise

⚠ Email Security – up to 45min

which is number **36** in the exercise PDF.

Exercise



Now lets do the exercise

⚠ SSL/TLS scanners 15min

which is number **27** in the exercise PDF.

Exercise



Now lets do the exercise

⚠ DNSSEC KeyTrap 20min

which is number **41** in the exercise PDF.

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools