Welcome to

11. System Security in Practice

KEA Kompetence Computer Systems Security 2019

Henrik Lund Kramshøj hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github

12-systems-security-in-practice.tex in the repo security-courses

Plan for today

Subjects

- Network security
- Infrastructure security
- Implement a small scale enterprise network

Exercises – System Security in Practice

Work on our model network, each team has a server and an attacker - reduce attack surface on the server by configuration

- Configure VLAN
- Configure SSH keys for more secure access
- Enable firewall

Reading Summary

Bishop chapters 28,29,30

Part VIII "Practicum"presents examples of how to apply the principles discussed throughout the book. It begins with networks and proceeds to systems, users, and programs. ... Part VIII tries to demonstrate that the material covered elsewhere can be, and should be, used in practice.

Chapter 28 Network Security

Chapter 29 System Security

Chapter 30 User Security

Network Security

- Goals of the Drib's security policy
- 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 the Drib 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 book.

Steps done by the book

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

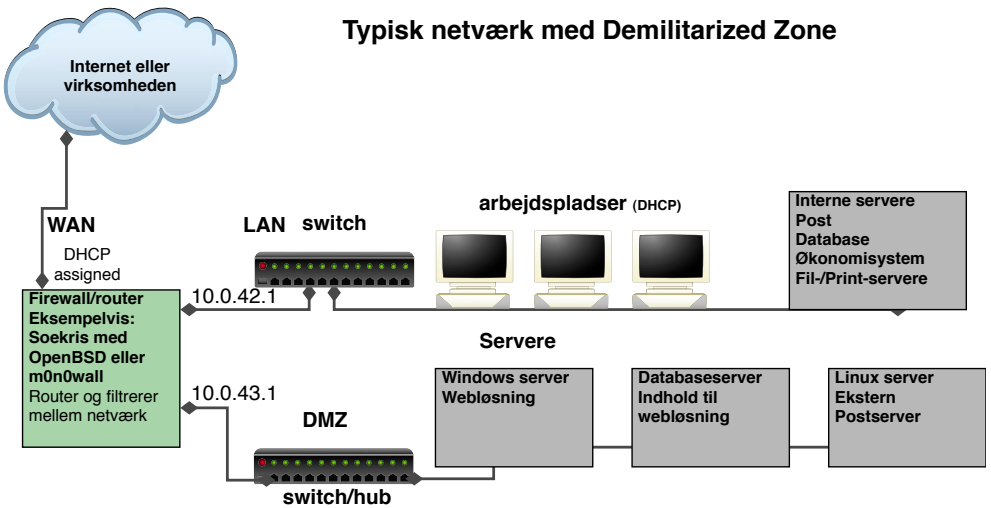
	Outsiders	Developers	Corporation Executives	Employees
Public data	Read	Read	Read	Read
Development data existing products		Read	Read	
Development data for future products		Read, Write	Read	
Corporate data			Read, Write	
Customer data	Write		Read	Read, Write

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.

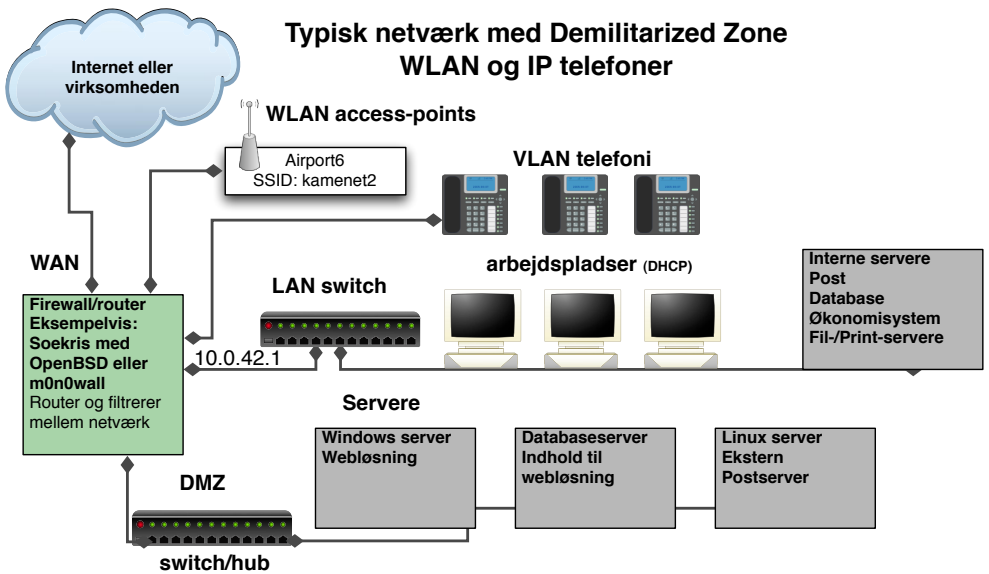
Network Organization – the DMZ



Definition 28-1 The *DMZ* is a portion of the network that separates a purely internal network from an external network.

The drawing in the book was how people did it before year 2000 ☺

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 serves - 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

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 2019

- 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 2019 præsentationen:

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

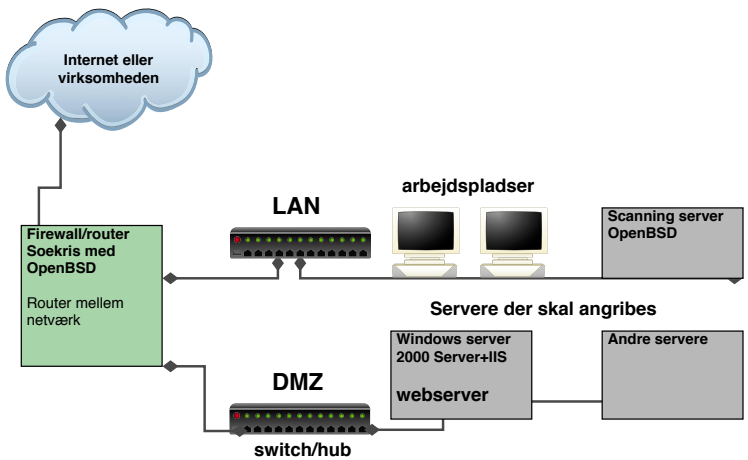
Design a robust network Isolation and segmentation

Hvad kan man gøre for at få bedre netværkssikkerhed?

- Bruge switche - der skal ARP spoofes og bedre performance
- Opdele med firewall til flere DMZ zoner for at holde udsatte 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.

Our Networks

We will now configure networks, using our sample switch TP-Link T1500G-10PS

Core network provides uplink through a switch / internet exchange

Each team will need:

- A switch TP-Link T1500G-10PS L2 features - default config
- USB Ethernet - or VLAN compatible virtualization network
- Ethernet cables

Network will provide:

- A shared switch TP-Link KramsIX for connecting teams
- Usual routed infrastructure - uplink to Internet
- Network services

Exercises – security in practice

Work on our model network, each team has a server and an attacker - reduce attack surface on the server by configuration.

- Configure VLAN on switch for the uplink
- Enable central logging
- Configure SSH keys for more secure access
- Enable firewall

Exercise switch config

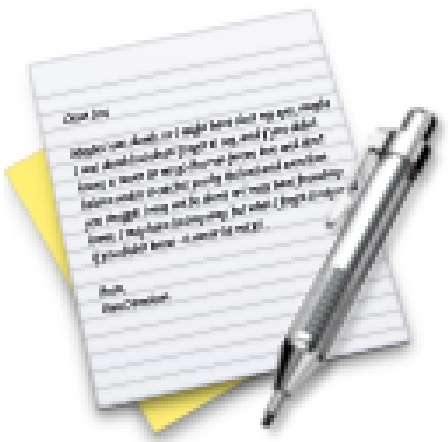
Each team will configure:

- Managed switch
- Configure uplink port to be a tagged VLAN trunk
- Configure port to connect to local Debian server, if tagged Debian must be configured with tag too! Access port is without tag.
- Insert USB into Debian server virtual machine

Use the guides from:

`https://www.tp-link.com/uk/support/download/t1500g-10ps/#Related-Documents`

Exercise

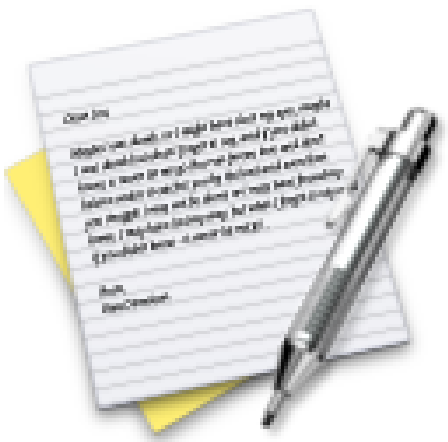


Now lets do the exercise

Switch configuration and uplink

which is number **26** in the exercise PDF.

Exercise

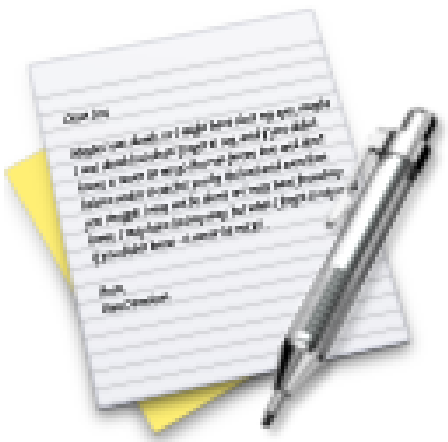


Now lets do the exercise

Centralized Logging

which is number 27 in the exercise PDF.

Exercise

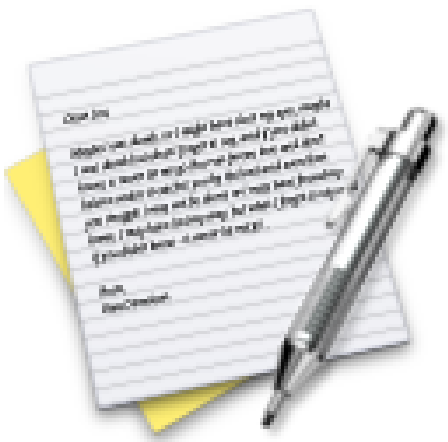


Now lets do the exercise

Configure SSH keys for more secure access

which is number **28** in the exercise PDF.

Exercise

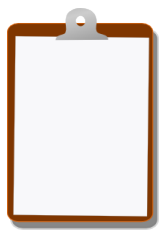


Now lets do the exercise

Enable firewall

which is number **29** 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
Most days have less than 100 pages, but some days may have more!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools