Welcome to

12. System Security in Practice

KEA Kompetence Computer Systems Security 2021

Henrik Kramselund Jereminsen hkj@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
- Talk about centralized logging
- Configure SSH keys for more secure access

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

Note: Matt Bishop refers to older tools, which I cannot recommend. TCP wrappers, Apache web server, r-protocols rlogin etc. Dont use those – we have better and more modern alternatives!

Goals for today:

Todays goals:

- 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 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

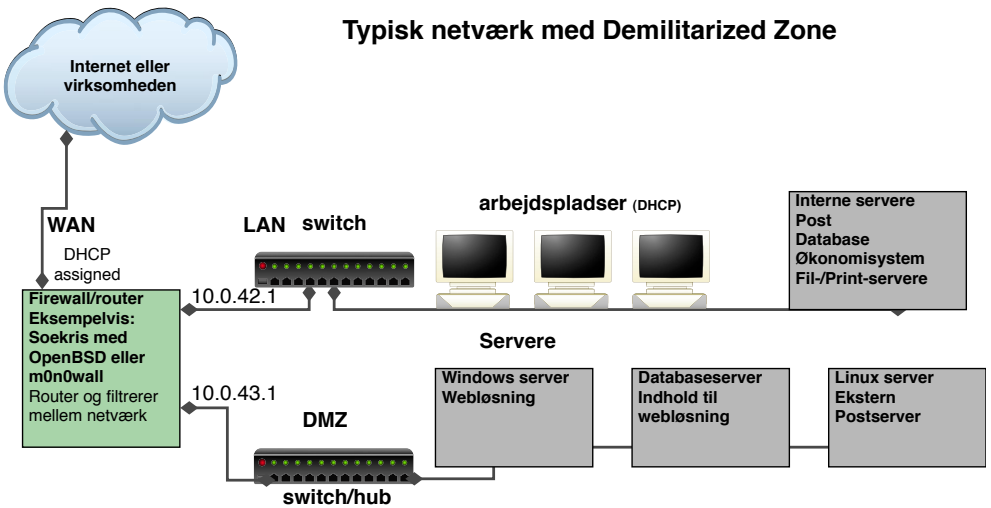
	Outsiders	Developers	Corporation Executives	Employees
Public data	Read	Read	Read	Read
Development data existing products		Read	Read	
Development data for future products		Read, Write	Read	
Corporate data			Read, Write	
Customer data	Write		Read	Read, Write

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.

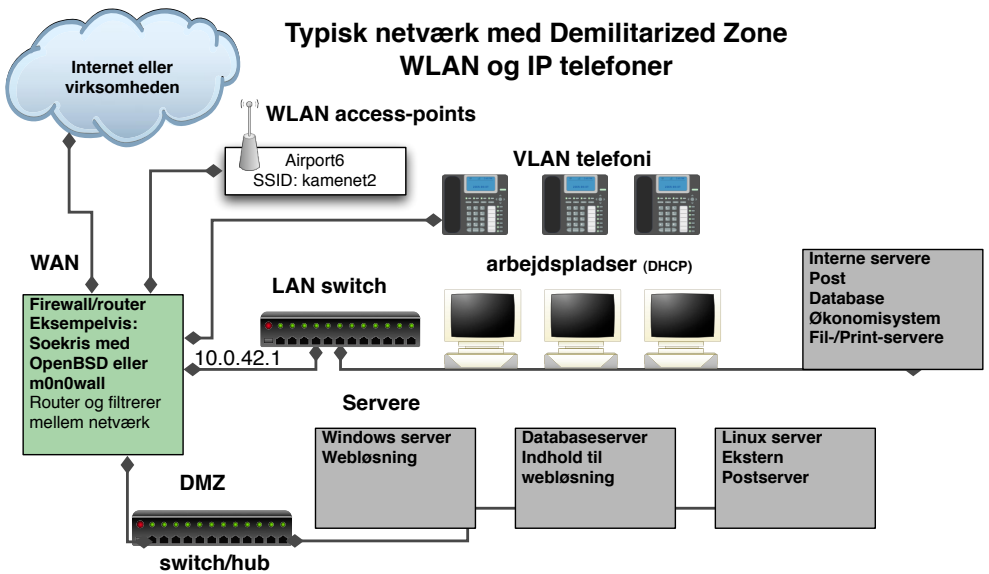
Network Organization – the DMZ



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

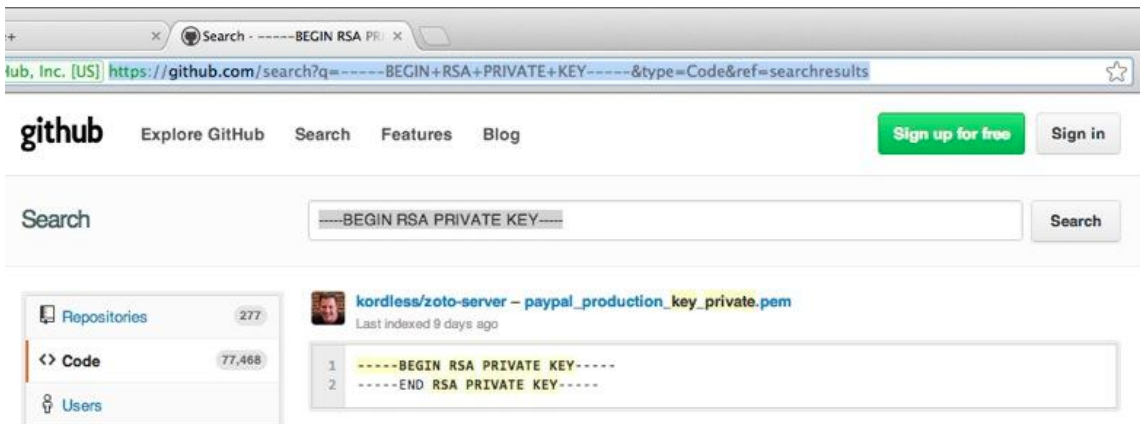
User Security

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?



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

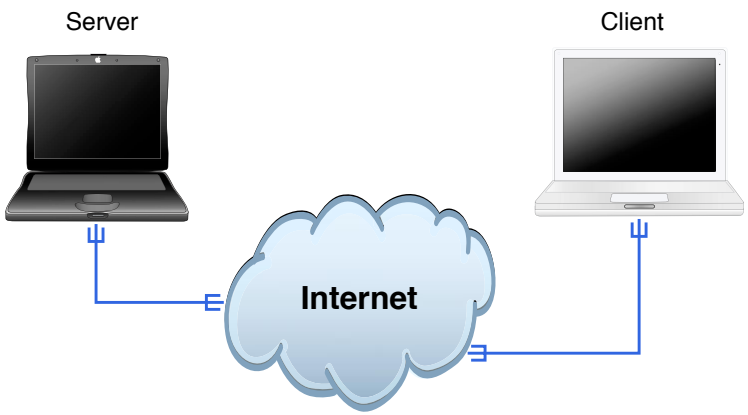
brute force

hvad betyder bruteforcing?
afprøvning af alle mulighederne

```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]

Options:
  -S        connect via SSL
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN  or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS   or -P FILE try password PASS, or load several passwords from FILE
  -e ns     additional checks, "n" for null password, "s" try login as pass
  -C FILE   colon seperated "login:pass" format, instead of -L/-P option
  -M FILE   file containing server list (parallizes attacks, see -T)
  -o FILE   write found login/password pairs to FILE instead of stdout
...
```

Demo: snmpwalk og Hydra



snmpwalk og Hydra

Vi laver sammen noget SNMP scanning og bruteforcing

Are passwords dead?

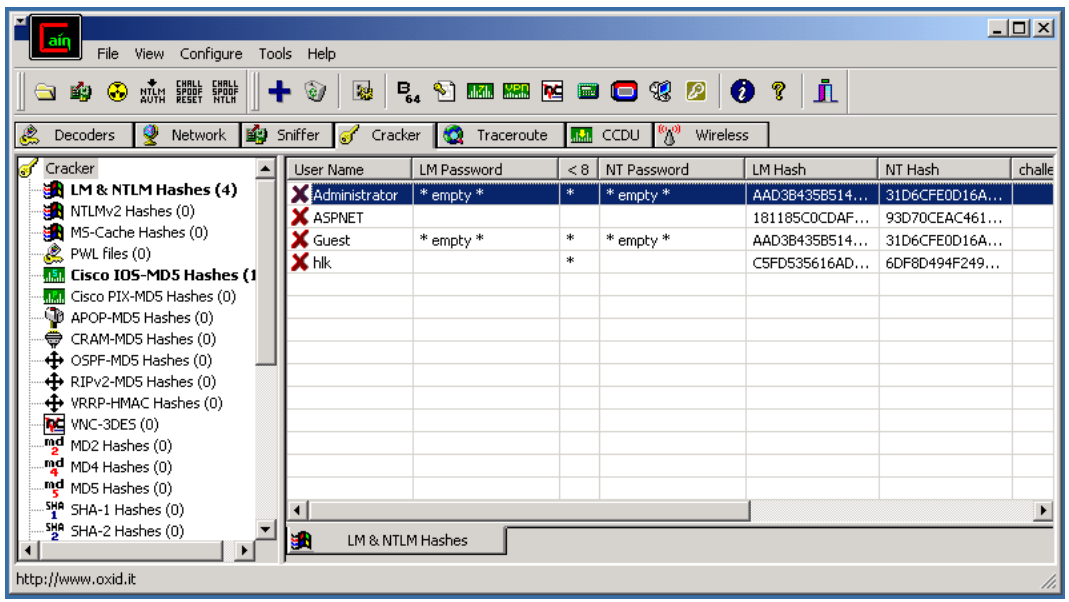
Can we stop using passwords?

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://dropsafe.crypticide.com/muffett-passwords`

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

Cain og Abel



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.

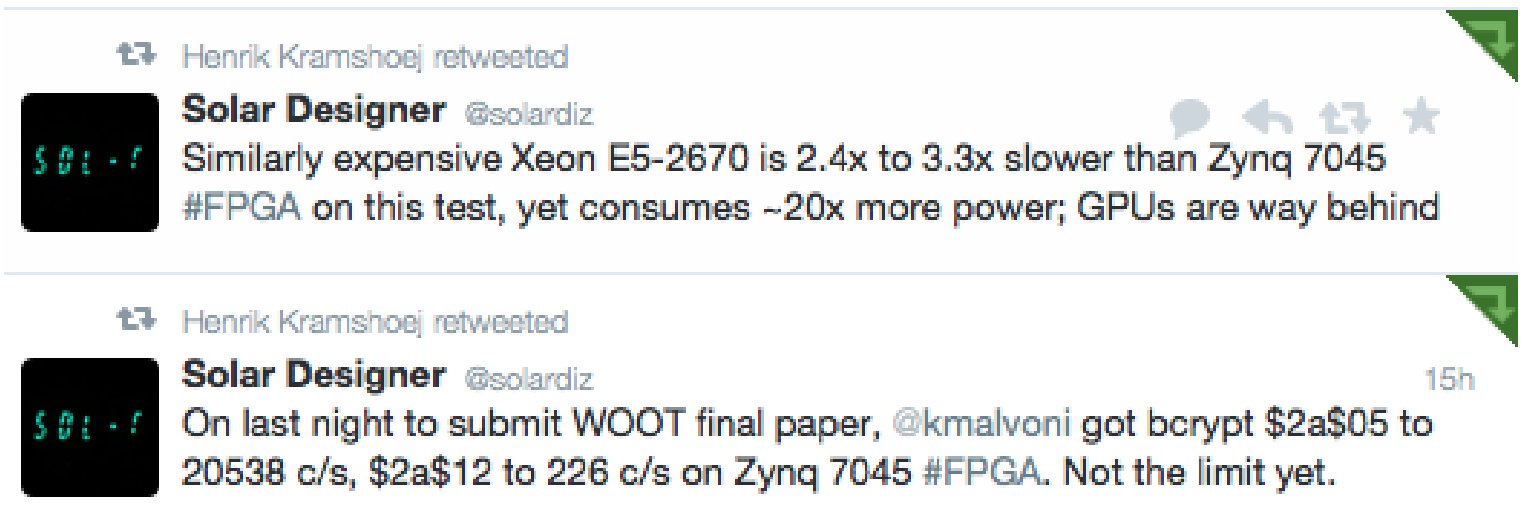
UNIX passwords kan knækkes med alec Muffets kendte Crack program eller eksempelvis John The Ripper `http://www.openwall.com/john/`

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/`

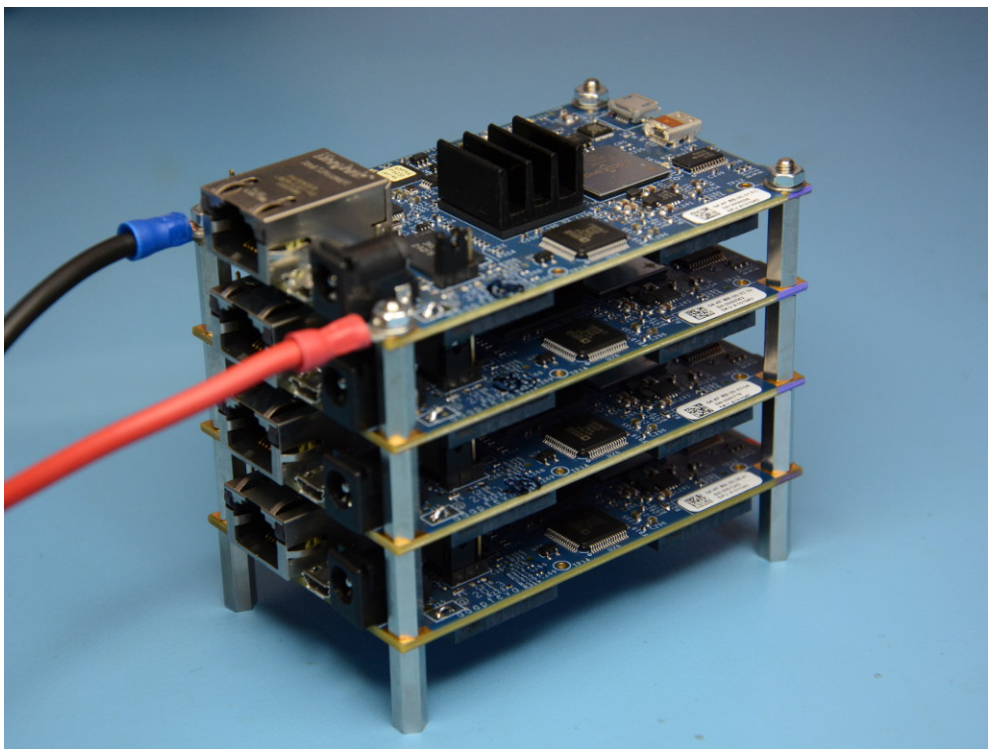
Parallella John



`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.parallella.org/power-supply/

Passwords vælges ikke tilfældigt

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 2021

- 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`

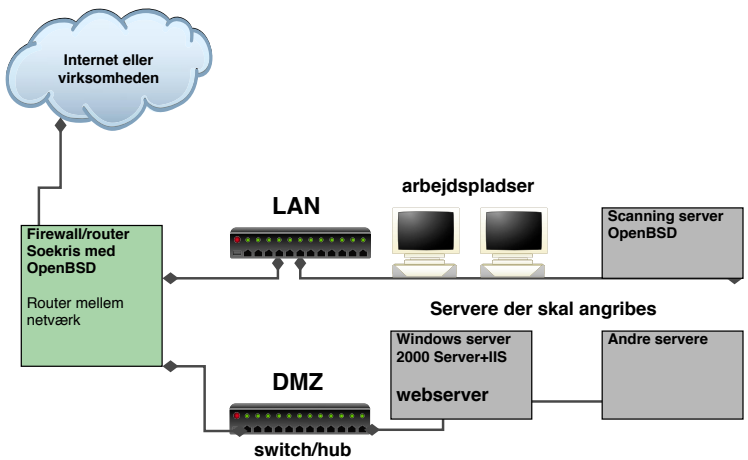
Design a robust network Isolation and segmentation

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

Exercise switch config

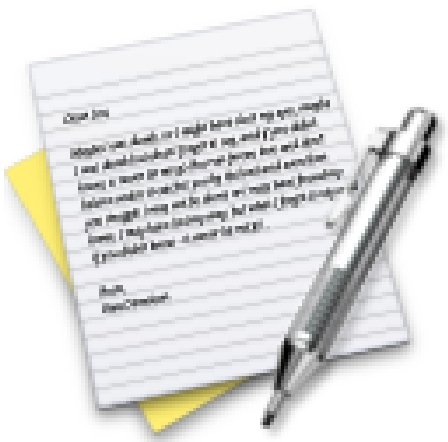
Each team will configure:

- 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

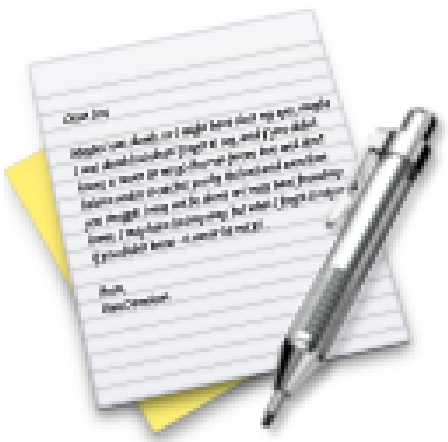


Now lets do the exercise

Bonus: Switch configuration and uplink

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

Exercise

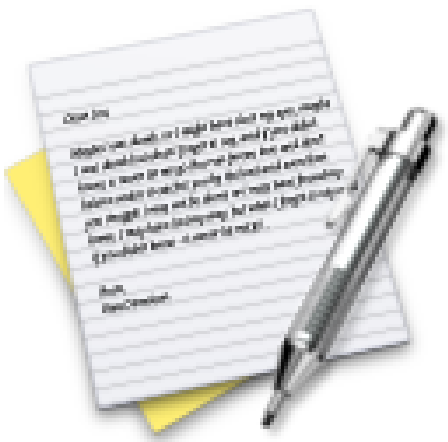


Now lets do the exercise

Centralized Logging

which is number **37** in the exercise PDF.

Exercise

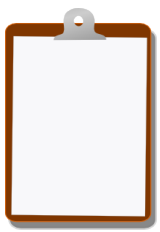


Now lets do the exercise

Configure SSH keys for more secure access

which is number **38** 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