Welcome to

12. Building Robust Networks

Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.com

Slides are available as PDF, kramse@Github

12-Building-Robust-Networks.tex in the repo security-courses

Plan for today

Subjects

- Design a robust network
- Isolation and segmentation
- Routing Security
- Switch and access security, port security
- Wireless security
- Using reputation lists

Exercises We will design and build a sample network together

- Configure port security
- VLANs, Routing and RPF
- Wifi, WPA and guest network
- Monitoring - setup LibreNMS
- IDS with Bro and Suricata

Reading Summary

- Read
- https://nsrc.org/workshops/2018/myren-nsrc-cndo/networking/cndo/en/presentations/Campus_Security_Overview.pdf
- https://nsrc.org/workshops/2018/tenet-nsrc-cndo/networking/cndo/en/presentations/Campus_Operations_BCP.pdf
- Download, but dont read it all

  https://nsrc.org/workshops/2015/apricot2015/raw-attachment/wiki/Track1Agenda/01-ISP-Network-Design.pdf

Produktionsmodning af miljøer

Tænk på det miljø som servere og services skal udsættes for

Sørg for hærdning

BIND sikring

Nedenstående kan bruges mod andre typer servere!

Sikringsforanstaltninger:

- Opdateret software - ingen kendte sikkerhedshuller eller sårbarheder
- fjern **single points of failure** - er man afhængig af en ressource skal man ofte have en backup mulighed, redundant strøm eller lignende
- adskilte servere - interne og eksterne til forskellige formål
  Eksempelvis den interne postserver hvor alle e-mail opbevares og en DMZ-postserver hvor ekstern post opbevares kortvarigt
- lav filtre på netværket, eller på data - firewalls og proxy funktioner
- begræns adgangen til at læse information
- begræns adgangen til at skrive information - dynamic updates på BIND, men samme princip til webløsninger og opdatering af databaser
- **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 - Windows, UNIX, BIND, Oracle, ...

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

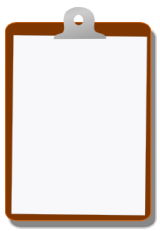
Fundamentet skal være iorden

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

- redundans
- opdateret
- dokumenteret
- nem at vedligeholde

Husk tilgængelighed er også en sikkerhedsparameter

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 about 100 pages or less, but one day has 4 chapters to read!

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools