Welcome to

12. Building Robust Networks

Communication and Network Security 2024

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

Slides are available as PDF, kramse@Codeberg

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

Plan for today

Subjects

- Design a robust network
- Isolation and segmentation
- Switch and access security, port security

Exercises We will discuss network design and how to build a sample network together

- VLANs, Routing and RPF
- Wifi, WPA and guest network
- Monitoring - setup LibreNMS
- IDS with Zeek and Suricata - if we have time
- Configure port security - if we have time

Discuss what a real robust network should be, and why are most networks NOT configured with *Best Current Practice*.

Reading Summary

- Read: ANSM chapter 5,6 - 50 pages,
- 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 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 2024

- 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:

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

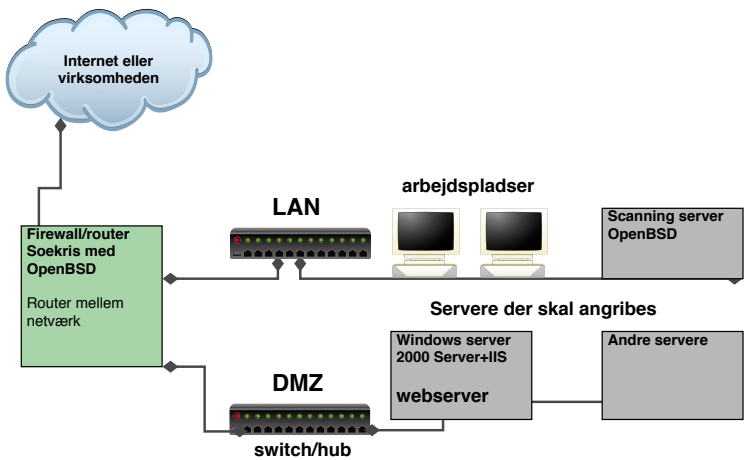
Design a robust network Isolation and segmentation

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
- An access point UniFi UAP Pro - preconfigured
- USB Ethernet - or VLAN compatible virtualization network
- Ethernet cables

Exercise in networking VLANs, Routing and RPF

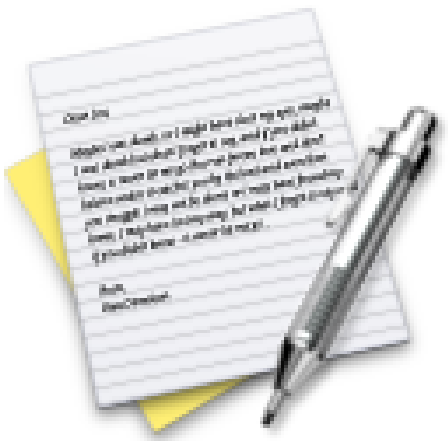
Each team will configure:

- Debian VM router-on-a-stick - L3 forwarding https://en.wikipedia.org/wiki/One-armed_router
- Recommended to serve DHCP service, and possibly NTP etc.
- Configure Monitoring and LibreNMS - optional
- Connect your IDS - optional, Configure port security - optional
- Reconfigure Wireless AP for multiple SSIDs / VLANs - optional
- Reconfigure uplink from static routing to BGP - optional

Use the guides from:

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

Exercise



Now lets do the exercise

ℹ VLANs and Routing 60min

which is number **68** in the exercise PDF.

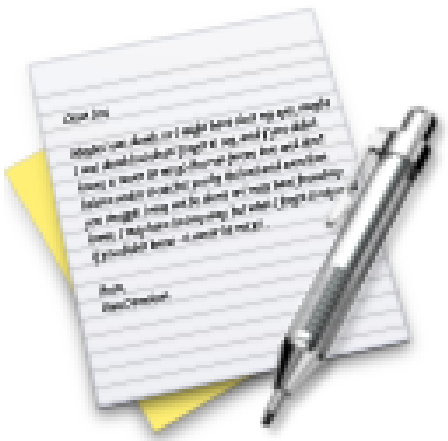
Exercise

Now lets do the exercise

Monitoring - setup LibreNMS 60 min

which is number **69** in the exercise PDF.

Exercise



Now lets do the exercise

ℹ Real IDS with Zeek and Suricata 30min

which is number **70** in the exercise PDF.

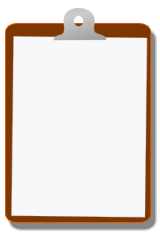
Exercise

Now lets do the exercise

Configure port security 30min

which is number **71** 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