Welcome to

Running a Modern Network

Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.com

Slides are available as PDF, kramse@Github

13-Running-a-Modern-Network.tex in the repo security-courses

Infrastrukturer i praksis

Vi vil nu gennemgå netværksdesign med udgangspunkt i vores setup

Vores setup indeholder:

- Routere
- Firewall
- Wireless
- DMZ
- DHCPD, BIND, BGPD, OSPFD, ...

Den kunne udvides med flere andre teknologier vi har til rådighed:

- VLAN inkl VLAN trunking/distribution
- WPA Enterprise

Hvad taler for og imod - de næste slides gennemgår nogle standardsetups

En slags Patterns for networking

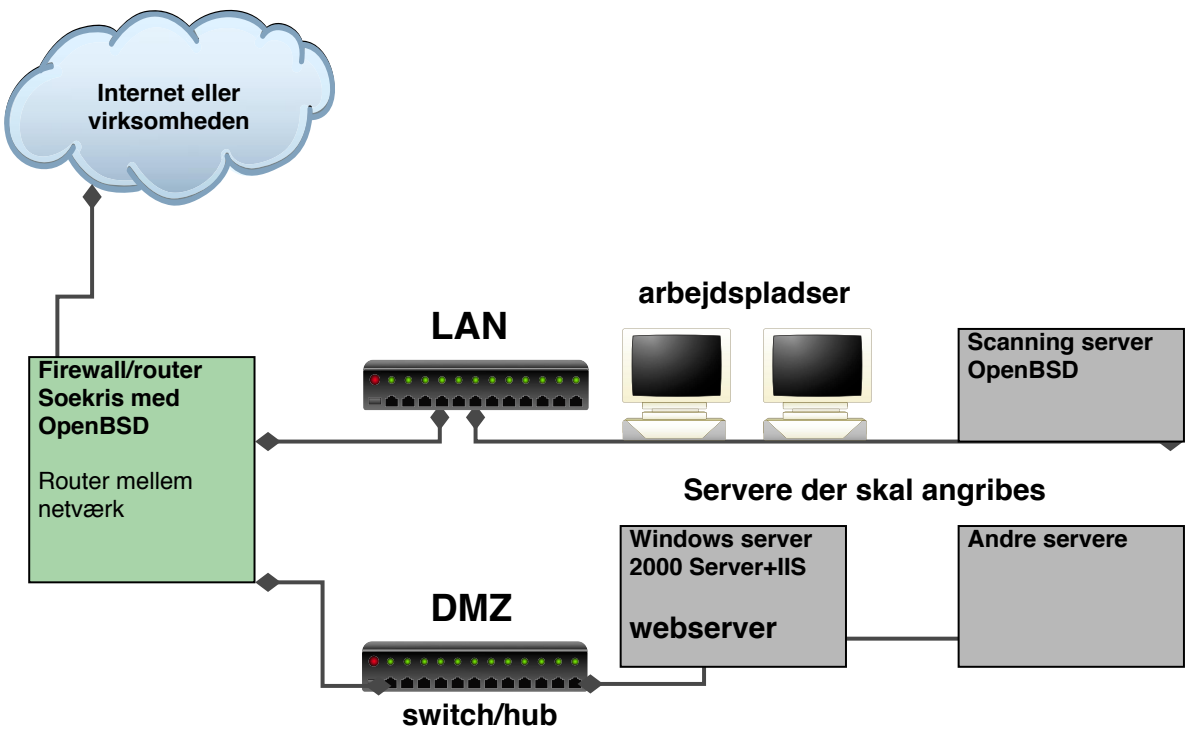
Netværksdesign og sikkerhed

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

basalt netværk



Du bør opdele dit netværk i segmenter efter traffik

Du bør altid holde interne og eksterne systemer adskilt!

Du bør isolere farlige services i jails og chroots

Intrusion Detection Systems - IDS

angrebsværktøjerne efterlader spor

hostbased IDS - kører lokalt på et system og forsøger at detektere om der er en angriber inde

network based IDS - NIDS - bruger netværket

Automatiserer netværksovervågning:

- bestemte pakker kan opfattes som en signatur
- analyse af netværkstrafik - FØR angreb
- analyse af netværk under angreb - sender en alarm

`http://www.snort.org` - det kan anbefales at se på Snort

snort

Snort er Open Source og derfor godt til undervisning

man kan se det som et antivirus system til netværket

forsøger at detektere *angreb*, *skadelig* og *forkert* traffik

pakker der minder om eksempelvis:

- nmap portscan
- nmap OS detection - med underlige pakker
- fragmenter der overlapper
- shellcode der sendes til systemer som BIND

Snort regler

```
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ICMP Address Mask
Reply"; icode:0; itype:18; classtype:misc-activity; sid:386; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Address Mask
Reply undefined code"; icode:>0; itype:18; classtype:misc-activity;
sid:387; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Address Mask
Request"; icode:0; itype:17; classtype:misc-activity; sid:388; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Address Mask
Request undefined code"; icode:>0; itype:17; classtype:misc-activity;
sid:389; rev:7;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Alternate
Host Address"; icode:0; itype:6; classtype:misc-activity; sid:390; rev:5;)
```

- sid - snort rules id - identificerer en signatur
- reference - hvor kommer reglen fra
- icode - ICMP code

- itype - ICMP type
- ... se mere i snort manualen

Ulemper ved IDS

snort er baseret på signaturer

mange falske alarmer - tuning og vedligehold

hvordan sikrer man sig at man har opdaterede signaturer for angreb som går verden rundt på et døgn

Planlægning af IDS miljøer

Før installationen

- Hvad er formålet - reaktion eller "statistik"
- Hvor skal der måles - hele netværket eller specifikke dele
- Hvad skal måles og hvilke operativsystemer og servere/services

Implementationen

- Er infrastrukturen iorden som den er
- Er der gode målepunkter - monitorporte
- Et målepunkt eller flere
- Hvormeget trafik skal måles

Selve idriftsættelsen

- Ændringer af infrastrukturen
- Installation af udstyret
- Test af udstyret udenfor drift

- Installation i driftsmiljøet
- Test af udstyret i driftsmiljøet

Opsætning og konfiguration af IDS miljøer

Vælg en simpel installation til at starte med!

Undgå for alt i verden for meget information

- Start med en enkelt sensor
- Byg en server med database og "brugerværktøjer"
- Start med at overvåge dele af nettet
- Brug et specifikt regelsæt i starten - eksempelvis kun Windows eller kun UNIX
- Lav nogle simple rapporter til at starte med

Gør netværket mere sikkert før du lytter på hele netværket

Brug tcpdump/Ethereal til at se på trafik, lær IP pakker at kende

Brug Snort til at evaluere

- husk at man kan starte med Snort og senere skifte til andre produkter
- Erfaring tæller, Snort tillader at man ser de fine detaljer - motoren

Vedligehold og overvågning af IDS miljøer

Uden vedligehold er IDS værdiløst - lad hellere være!

- Vedligehold af software på operativsystemet
- Vedligehold af IDS softwaren
- Vedligehold af regelsæt

Overvågning - kører IDS systemet, databaser og sensorer

Statistik og brug af IDS systemet

- Vedligehold af rapporter - hvad er vi interesseret i
- Automatisk rapportgenerering - daglig rapport, rapport pr måned
- Specielle hændelser - hvad skete der onsdag mellem 11-12

Et IDS kan også blot være en ARPwatch

ARPwatch advarer hvis nogen tager adressen fra default gateway

Honeypots

Man kan udover IDS installere en honeypot

En honeypot består typisk af:

- Et eller flere sårbare systemer
- Et eller flere systemer der logger traffik til og fra honeypot systemerne

Meningen med en honeypot er at den bliver angrebet og brudt ind i

Hvad muligheder har man

- Ændre miljø
- forbedre systemerne
- undgå standardindstillinger
- vær opdateret på sikkerhedsområdet
- have retningslinier - ens sikkerhedsniveau
- drop kompatibilitet med usikre systemer

- en god infrastruktur
- brug kryptografi
- brug standardbiblioteker
- test af systemer

Ændre miljø

Ændre arkitektur sw/hw/netværkstopologi

- blokere porte således at en webserver IKKE kan connecte tilbage til hackeren!
- blokere de services der IKKE skal tilgås udefra
- skifte programmeringssprog

Husk altid at hackeren også kan gå ind ad hovedøren

eksempelvis SAP Internet gateway, hvor man kunne lægge det bagvedliggende system ned med loginrequests

Forbedre systemerne

Operativsystemet

- non-executable stack
- non-executable heap

Applikationsservere

- filtrering af "dårlige"requests e-Eye sikret IIS
- mere "sikker"default opsætning

Jeg tror vi vil se flere implementere den slags løsninger

Eksempelvis:

- Microsoft IIS web server version 6 er mere sikker i default opsætningen
- Apache HTTPD web server version 2 er mere modulær og nemmere at bygge sikkert

Undgå standard indstillinger

Giv jer selv mere tid til at patche og opdatere

Tiden der går fra en sårbarhed annonceres på bugtraq til den bliver udnyttet er meget kort idag!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist - inden ormene kommer

NB: ingen garanti

Pattern: erstat Telnet med SSH

Telnet er død!

Brug altid Secure Shell fremfor Telnet

Opgrader firmware til en der kan SSH, eller køb bedre udstyr næste gang

Selv mine små billige Linksys switche forstår SSH!

Pattern: erstat FTP med HTTP

Hvis der kun skal distribueres filer kan man ofte benytte HTTP istedet for FTP

Hvis der skal overføres med password er SCP/SFTP fra Secure Shell at foretrække

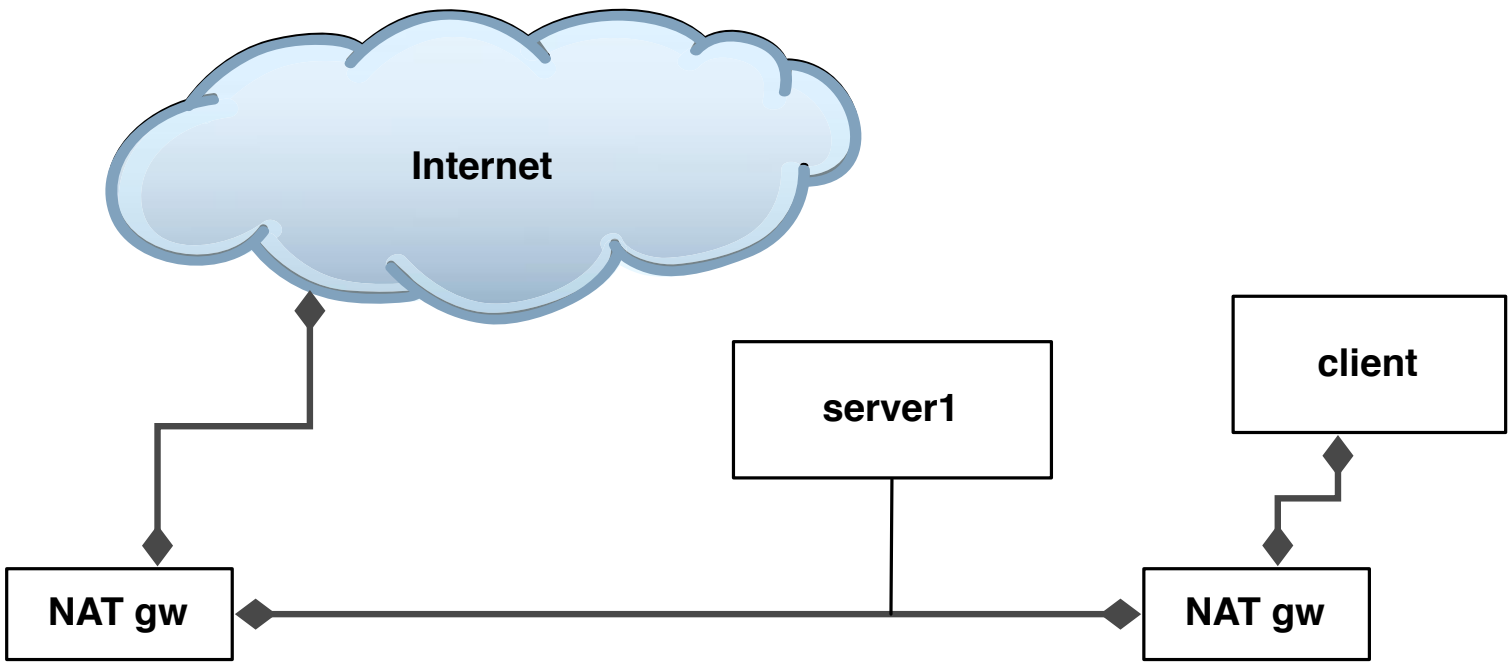
Anti-patterns

Nu præsenteres et antal setups, som ikke anbefales

Faktisk vil jeg advare mod at bruge dem

Husk følgende slides er min mening

Anti-pattern dobbelt NAT i eget netværk



Det er nødvendigt med NAT for at oversætte traffik der sendes videre ud på internet.

Der er ingen som helst grund til at benytte NAT indenfor eget netværk!

Anti-pattern blokering af ALT ICMP

```
ipfw add allow icmp from any to any icmptypes 3,4,11,12
```

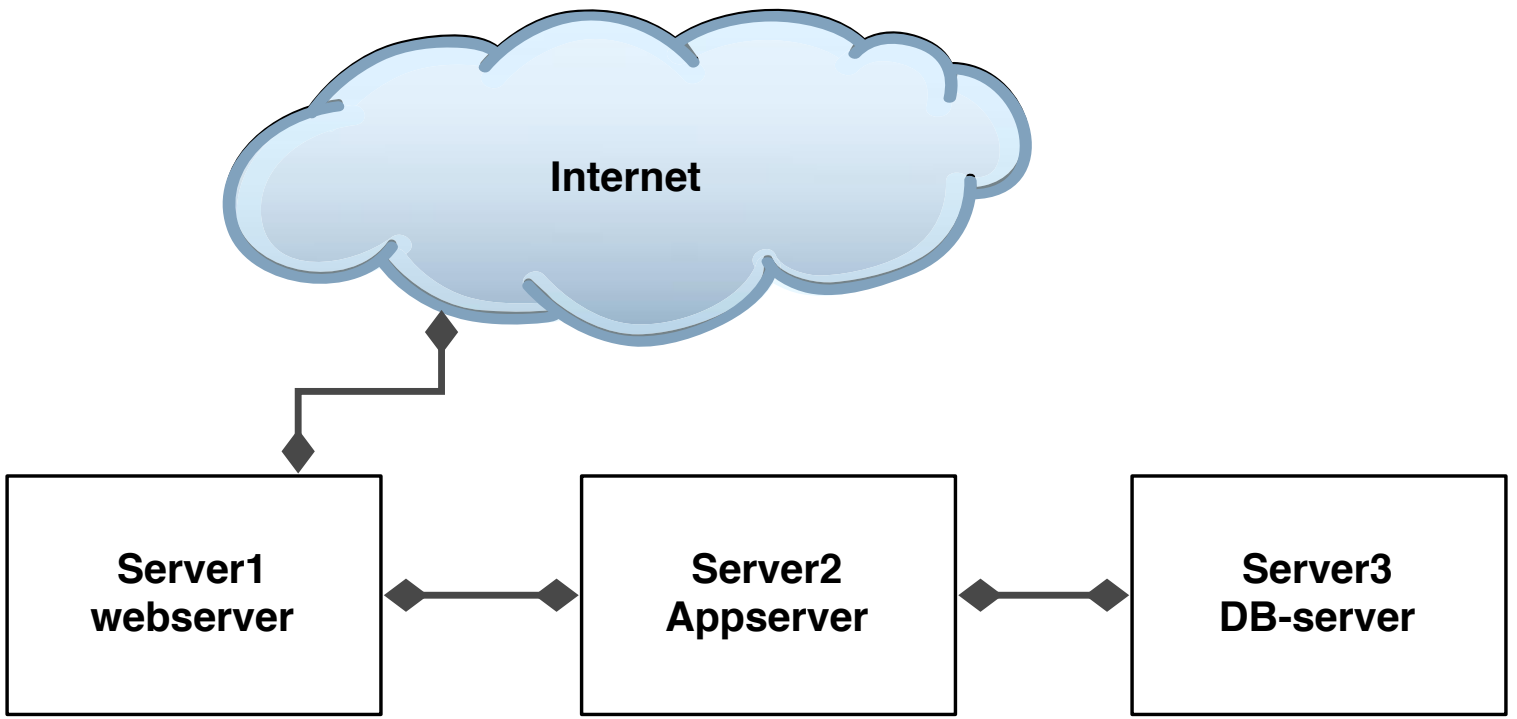
Lad være med at blokere for alt ICMP, så ødelægger du funktionaliteten i dit net

Anti-pattern blokering af DNS opslag på TCP

Det bliver (er) nødvendigt med DNS opslag over TCP på grund af store svar. Det betyder at firewalls skal tillade DNS opslag via TCP

Guide:
Brug en caching nameserver, således at det kun er den som kan lave DNS opslag ud i verden

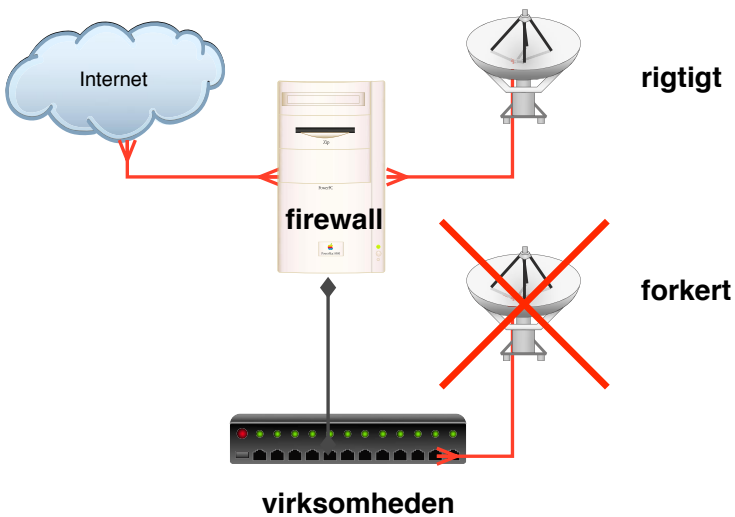
Anti-pattern daisy-chain



Daisy-chain af servere, erstat med firewall, switch og VLAN

Det giver et væld af problemer med overvågning, administration, backup og opdatering

Anti-pattern WLAN forbundet direkte til LAN



WLAN AP'er forbundet direkte til LAN giver risiko for at sikkerheden brydes, fordi AP falder tilbage på den usikre standardkonfiguration

Ved at sætte WLAN direkte på LAN risikerer man at eksterne får direkte adgang

Kan selvfølgelig gå an i et privat hjem

Det forværres jo flere AP'er man har, har du 100 skal du være sikker på allesammen er sikre!

At være på internet

RFC-2142 Mailbox Names for Common Services, Roles and Functions

Du BØR konfigurere dit domæne til at modtage post for følgende adresser:

- postmaster@domæne.dk
- abuse@domæne.dk
- webmaster@domæne.dk, evt. www@domæne.dk

Du gør det nemmere at rapportere problemer med dit netværk og services

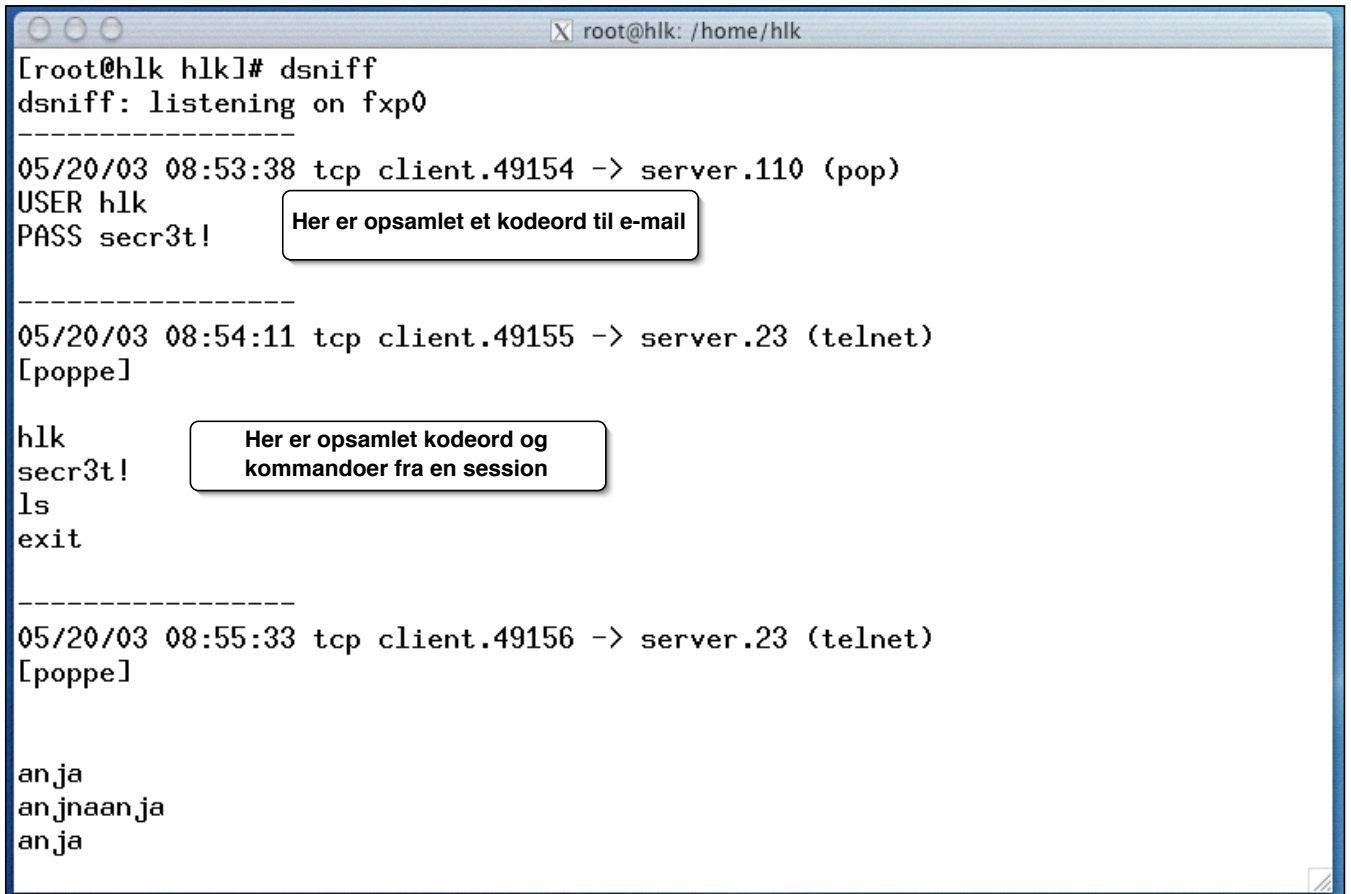
E-mail best current practice

MAILBOX	AREA	USAGE
ABUSE	Customer Relations	Inappropriate public behaviour
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries
...		
MAILBOX	SERVICE	SPECIFICATIONS
POSTMASTER	SMTP	[RFC821], [RFC822]
HOSTMASTER	DNS	[RFC1033-RFC1035]
USENET	NNTP	[RFC977]
NEWS	NNTP	Synonym for USENET
WEBMASTER	HTTP	[RFC 2068]
WWW	HTTP	Synonym for WEBMASTER
UUCP	UUCP	[RFC976]

FTP FTP [RFC959]

Kilde: RFC-2142 Mailbox Names for Common Services, Roles and Functions. D. Crocker. May 1997

Brug krypterede forbindelser


root@hlk: /home/hlk
[root@hlk hlk]# dsniff
dsniff: listening on fxp0

05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER hlk
PASS secr3t!
Her er opsamlet et kodeord til e-mail

05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]
hlk
secr3t!
ls
exit
Her er opsamlet kodeord og kommandoer fra en session

05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]
anja
anjnaanja
anja

Især på utroværdige netværk kan det give problemer at benytte sårbare protokoller

Mission 1: Kommunikere sikkert

Du må ikke bruge ukrypterede forbindelser til at administrere UNIX

Du må ikke sende kodeord i ukrypterede e-mail beskeder

Telnet daemonen - telnetd må og skal dø!
FTP daemonen - ftpd må og skal dø!
POP3 daemonen port 110 må og skal dø!
IMAPD daemonen port 143 må og skal dø!

væk med alle de ukrypterede forbindelser!

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

individuel autentificering!

ssh root@server1

Mange UNIX systemer administreres fejlagtigt ved brug af root-login

Undgå direkte root-login

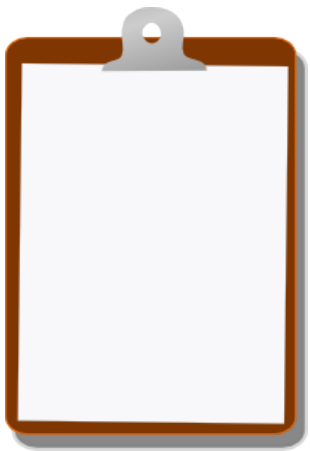
Insister på `sudo` eller `su`

Hvorfor?

- Sporbarheden mistes hvis brugere logger direkte ind som root
- Hvis et kodeord til root gættes er der direkte adgang til alt!

Jump Host

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