

Velkommen til

Best practice sikkerhed for UNIX systemer

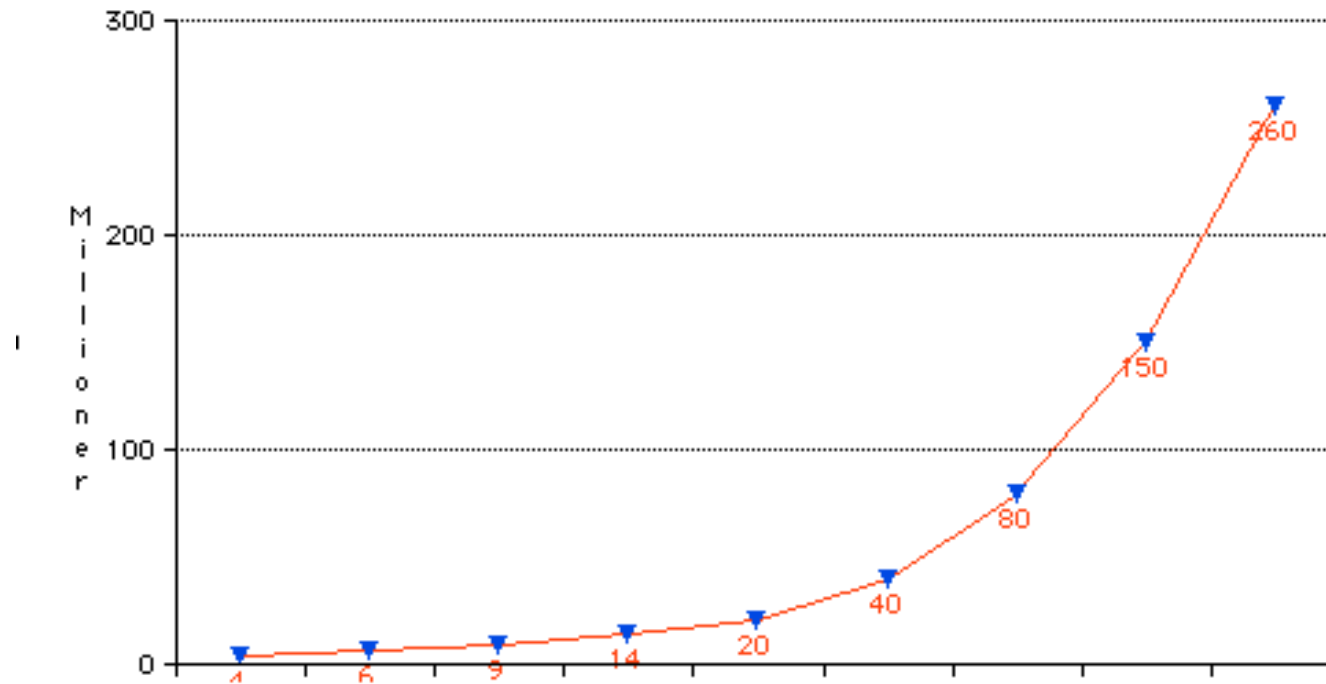
anno 2005

Henrik Lund Kramshøj
hk@security6.net

<http://www.security6.net>



Årsregnskabet fremlægges - omsætningen stiger



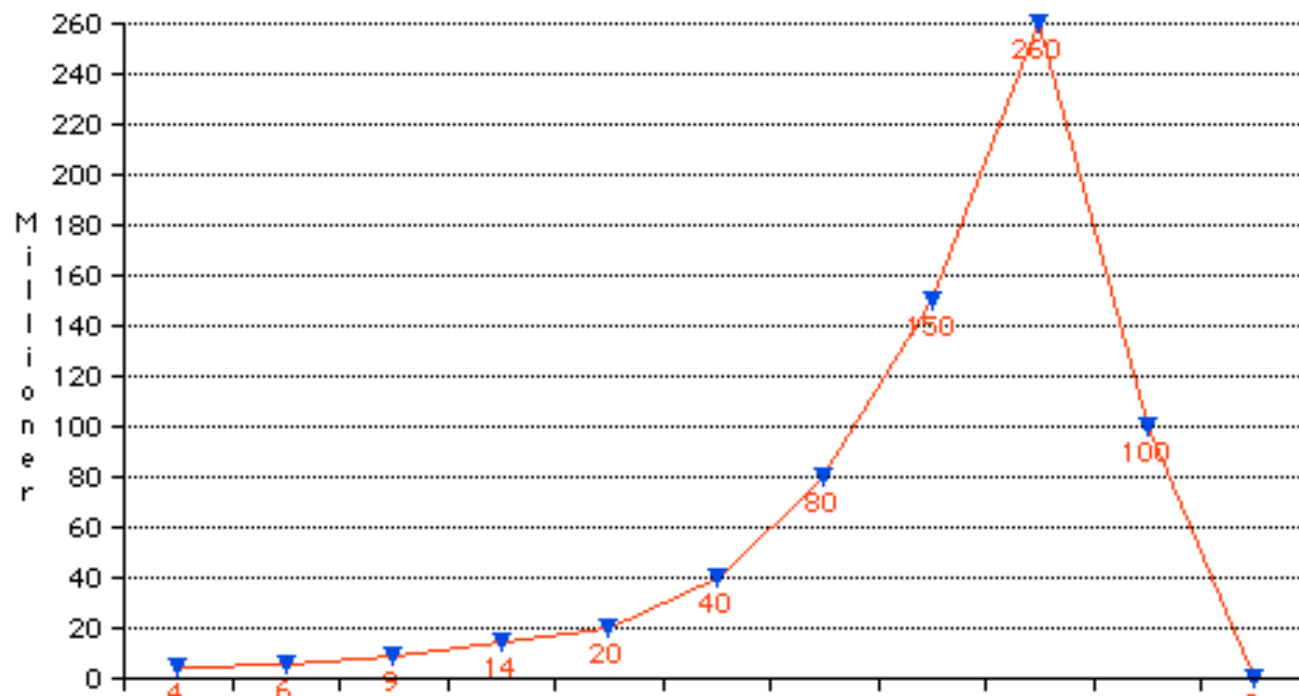
Velkommen til fremlæggelse af årsregnskabet for Opensourceforum DK Vi har haft en perfekt markedspenetrering og vores shoutability har været i top.

Vores produkter opfylder alle WAF specifikationer og købes af alle

hehe vi bliver rige når vi laver børsintroduktionen den 1. august!

Når facaden krakelerer

Den 5. marts falder bomben mens alle systemadministratorer fjoller rundt på en konference - hackerangreb lammer hele infrastrukturen i en uge, alle data mistes



Hvor er omsætningen? Hvor er firmaet på vej hen?

Hvorfor gik det galt for firmaet?

Sikkerheden var for dårlig

firmaet led måske et knæk på troværdigheden
de mistede muligheden for at leverere, fakturere
de kunne ikke føre lovpligtigt regnskab

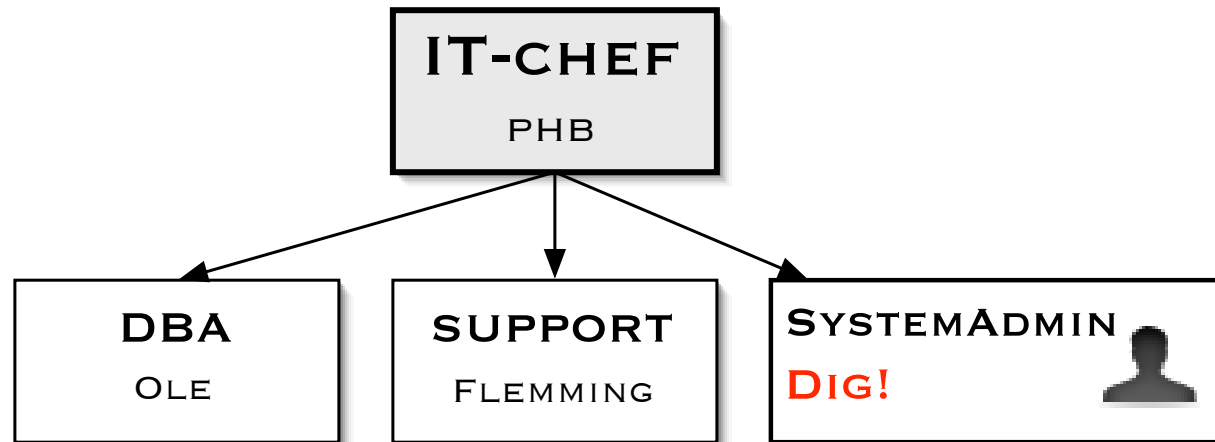


man kan sige de mistede muligheden for at eksistere

Du er i farezonen!

OPENSOURCEFORUM DK

IT AFDELINGEN



En interessant og usikker maskine med adgangsveje fra Internet vil formentlig blive hacket

Er det dit ansvar? bliver det dit ansvar?

Effekten af et hackerangreb

Ordredatabasen forsvinder

Alle kundeoplysninger og kreditkortnumre mistes

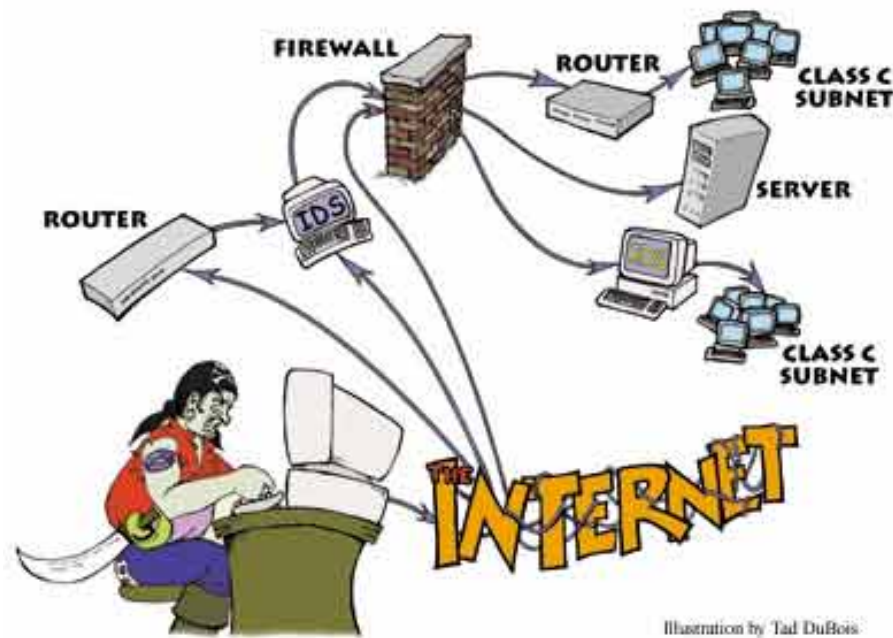
Regnskabet forsvinder - hvad skal der betales af moms?



Du er FYRET!!!!

Sådan kan det gå!

Er UNIX sikkerhed interessant?



UNIX er grand old man i Internet

Mange UNIX services findes idag på andre platforme

UNIX har fået en renæssance med Linux, Mac OS X og BSD

ALLE kommercielle UNIX varianter leveres i en usikker konfiguration

Formål



At introducere UNIX best-practice sikkerhed

Kendskab til basale hjælpemidler

Minimering af risici i UNIX miljøer - hvordan kommer I igang

Der vises **ikke** ekstremer indenfor sikkerhed og beskyttelse af UNIX

Sikkerhed koster ikke altid noget - hverken penge eller funktionalitet

Best current practice

Hvad er best current practice

- Overholdelse af god forretningskik
- Forventede minimumskrav
- Bedre end gennemsnittet
- Internet RFC Best Current Practice subseries
<http://www.rfc-editor.org/categories/rfc-best.html>
- CERT/CC guidelines
http://www.cert.org/tech_tips
- *Quick Guide til optimering af efterforskningsmuligheder*, Tom Engly Henriksen, kriminalassistent, Rigspolitiet i samarbejde med Dansk IT

Best Current Practice er noget man BØR GØRE!

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

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 daemongen - telnetd må og skal dø!

FTP daemongen - ftpd må og skal dø!

POP3 daemongen port 110 må og skal dø!

IMAPD daemongen port 143 må og skal dø!

væk med alle de ukrypterede forbindelser!

Hvordan stopper man telnetd

inetd en super server

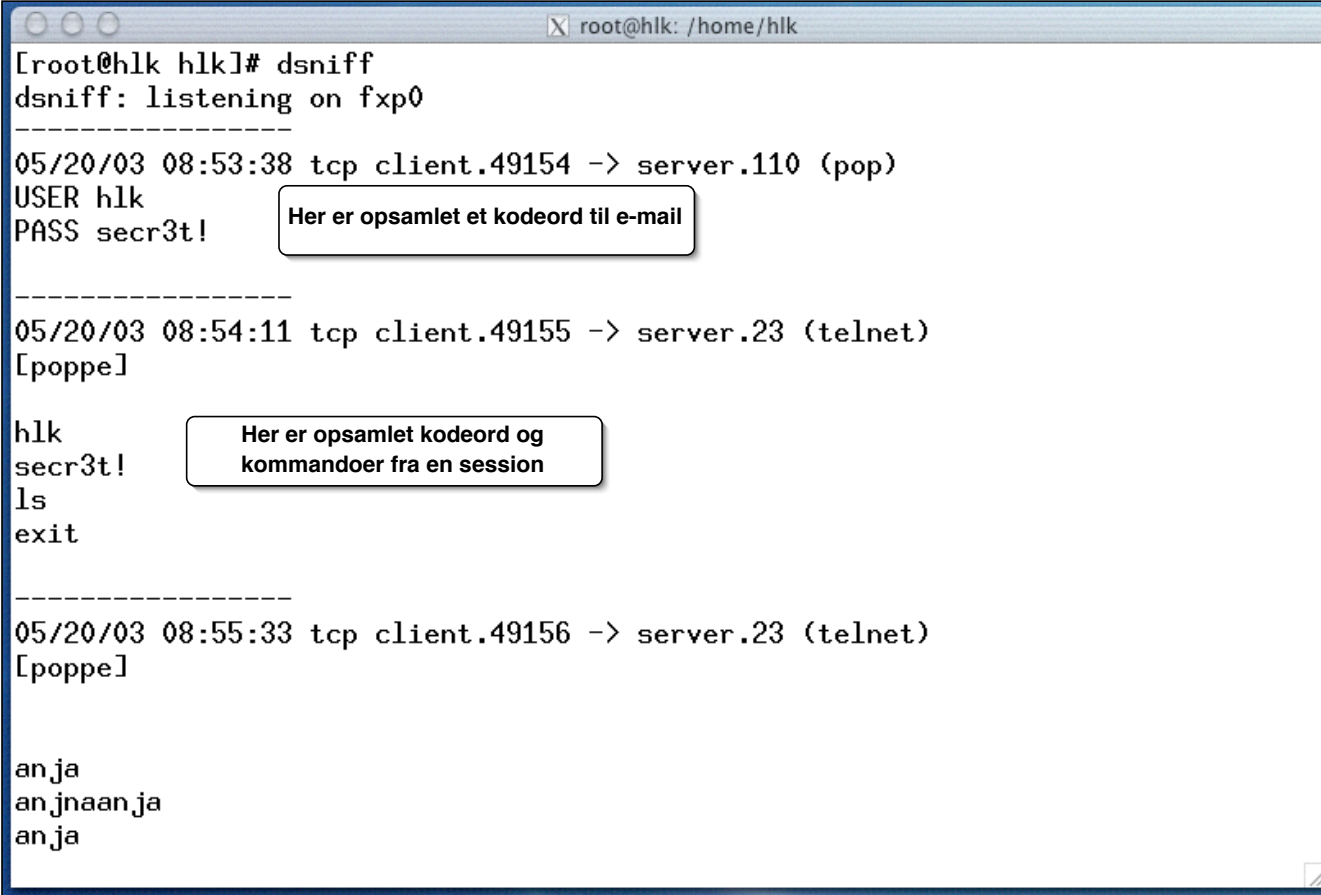
inetd har mange funktioner

inetd er ofte overflødig idag - stop den!

hvorfor er følgende services default i inetd.conf på systemer?

```
finger stream tcp      nowait  nobody  /usr/libexec/tcpd  fingerd -s
ftp      stream tcp      nowait  root    /usr/libexec/tcpd  ftpd -l
login   stream tcp      nowait  root    /usr/libexec/tcpd  rlogind
nntp    stream tcp      nowait  usenet  /usr/libexec/tcpd  nntpd
ntalk   dgram  udp      wait    root    /usr/libexec/tcpd  ntalkd
shell   stream tcp      nowait  root    /usr/libexec/tcpd  rshd
telnet  stream tcp      nowait  root    /usr/libexec/tcpd  telnetd
uucpd   stream tcp      nowait  root    /usr/libexec/tcpd  uucpd
comsat  dgram  udp      wait    root    /usr/libexec/tcpd  comsat
tftp    dgram  udp      wait    nobody   /usr/libexec/tcpd  tftpd /tftpboot
```

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!
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]
hlk
secr3t!
ls
exit
-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]
an ja
an jnaan ja
an ja
```

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

Secure Shell - SSH og SCP i OpenSSH



SSH afløser en række protokoller som er usikre:

- Telnet til terminal adgang
- r* programmerne, rsh, rcp, rlogin, ...
- FTP med brugernavn/passord

SSH - de nye kommandoer er

kommandoerne er:

- ssh - Secure Shell
- scp - Secure Copy
- sftp - secure FTP
- Login kan foretages på forskellige måder:

```
ssh kursus1@server
```

```
ssh -l kursus1 server
```
- Secure copy scp kan bruges direkte fra kommandolinien:

```
scp /tmp/filnavn server:relativsti
```

```
scp /tmp/filnavn server:/fuld/sti/til/placering
```

Husk: SSH er både navnet på protokollerne - version 1 og 2 samt programmet `ssh` til at logge ind på andre systemer

SSH tillader også port-forward, tunnel til usikre protokoller, eksempelvis X protokollen til UNIX grafiske vinduer

NB: Man bør idag bruge SSH protokol version 2!

SSH nøgler

Mange bruger ofte login med password via SSH, hvilket er en stor fejl

Man letter sin dagligdag med SSH nøgler og SSH agenter der kan holde nøglen

- først skal der genereres et nøglepar **id_dsa og id_dsa.pub** - `ssh-keygen -t dsa`
- Den offentlige del, filen `id_dsa.pub`, kopieres til serveren
- Der logges ind på serveren
- Der udføres følgende kommandoer:

```
cd skift til dit hjemmekatalog  
mkdir .ssh lav et katalog til ssh-nøgler  
cat id_dsa.pub >> .ssh/authorized_keys kopierer nøglen  
chmod -R go-rwx .ssh skift rettigheder på nøglen
```

SSHD konfiguration

Forslag til indholdet i `sshd_config`

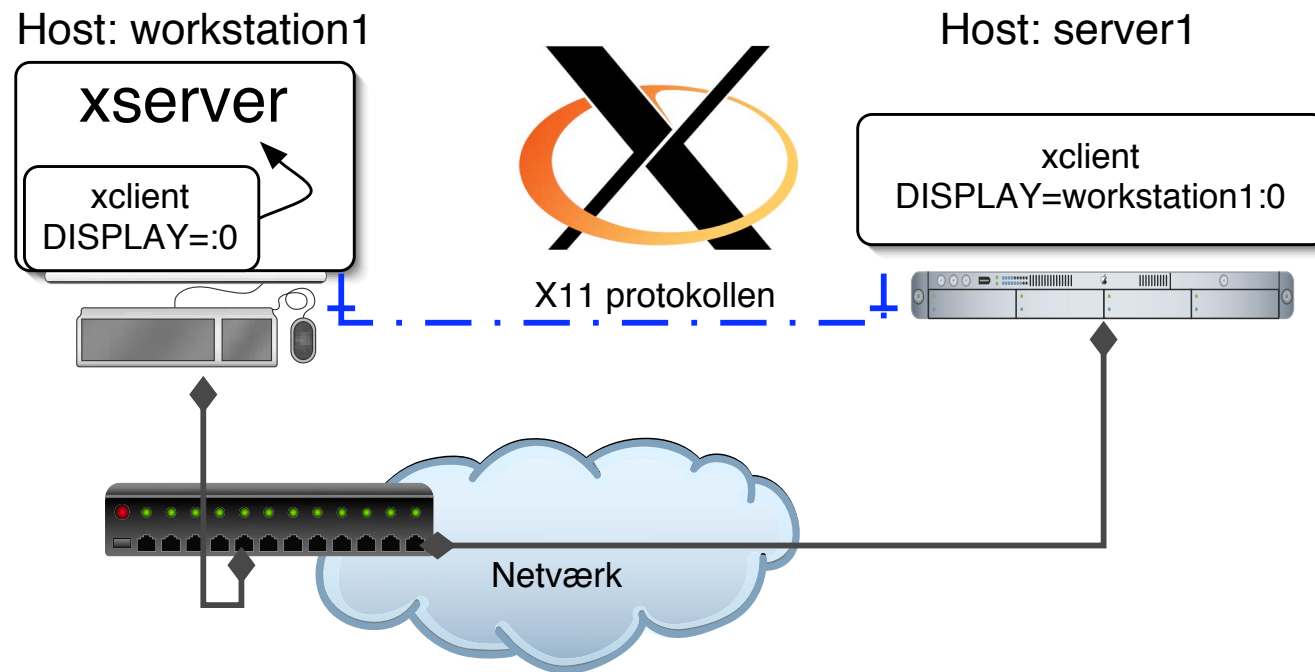
filen findes typisk under `/etc/ssh`

Husk at læse i manualen til `sshd` og `sshd_config` hvis du er i tvivl

Kommentarer i kursiv

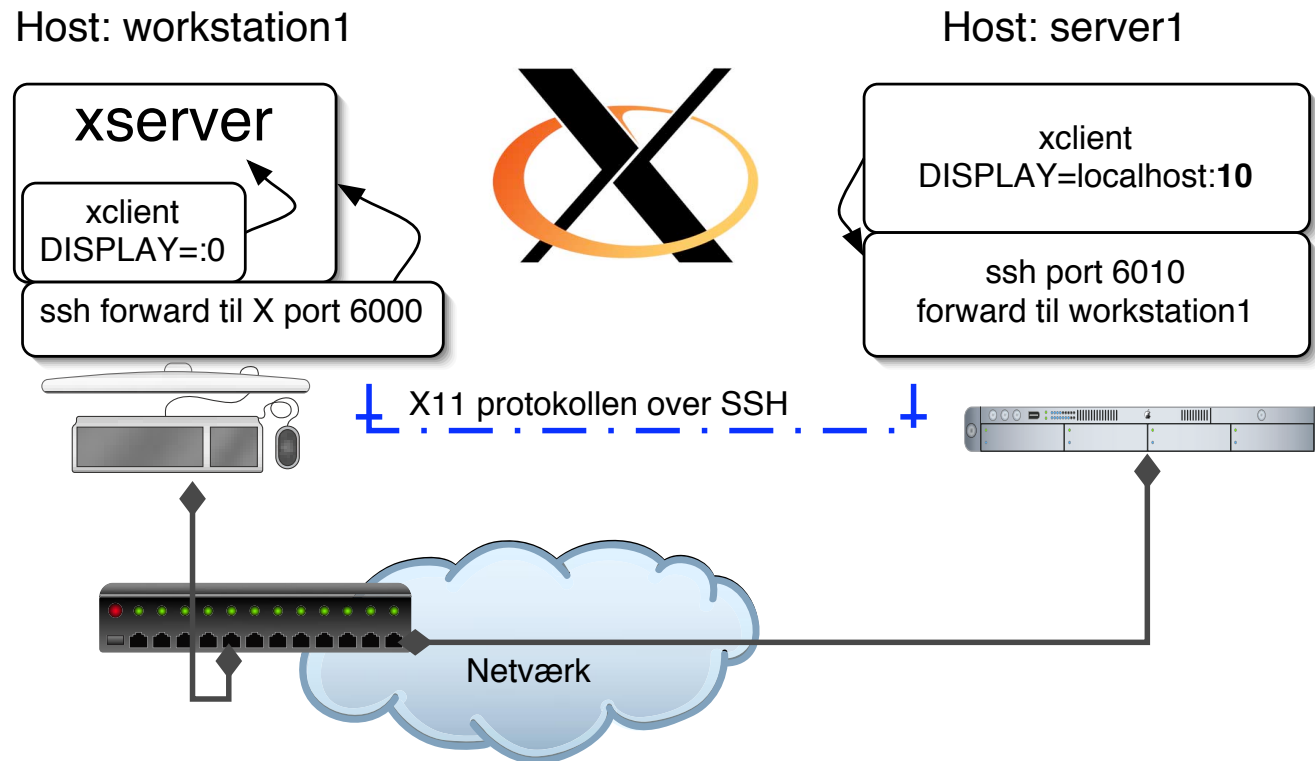
```
#Port 22
Port 13578      hvorfor bruge den samme port som alle andre?
#Protocol 2,1
Protocol 2      alle gode klienter forstår version 2
....
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no ingen kodeord tillades, kun nøgler
```

X11 klienter og servere



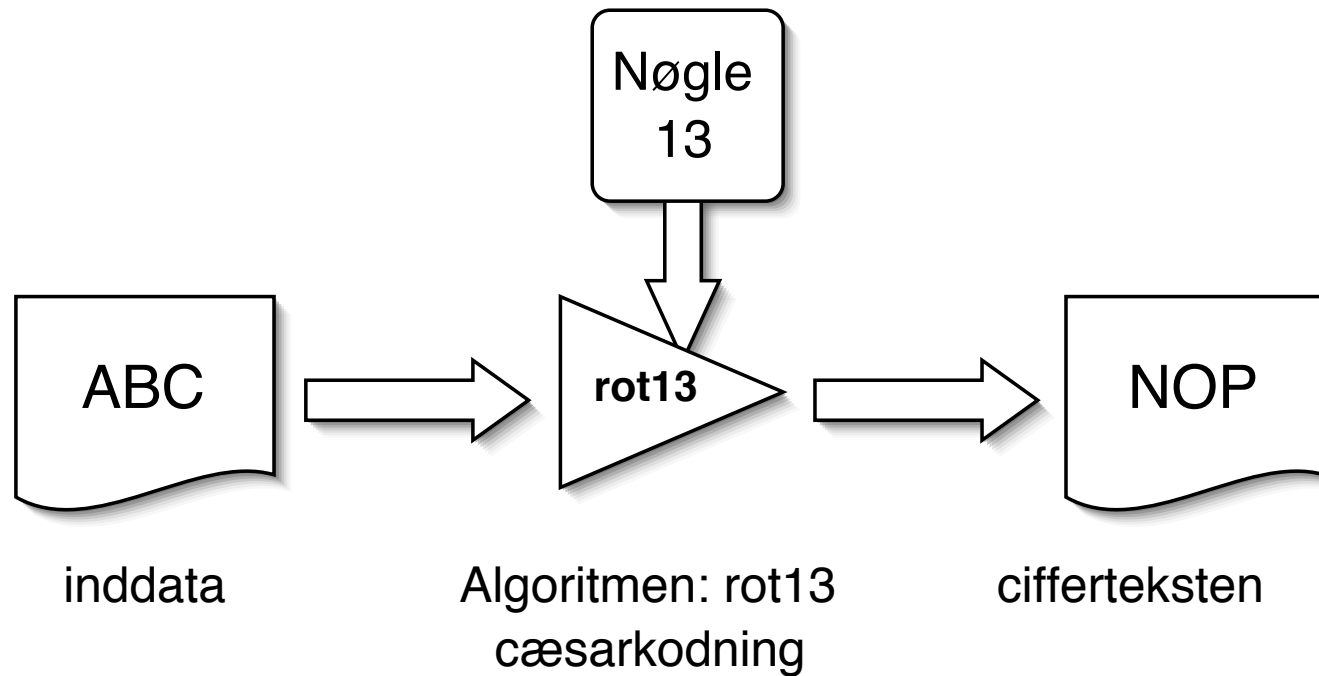
- Man logger ind på en server over netværk
- Der sættes en variabel der fortæller hvor vinduer skal tegnes `$DISPLAY`
- Applikationen afvikles på en maskine, al grafik vises på en anden

SSH X forwarding



- X11 protokollen er ikke sikker!
- Hvis man bruger SSH kan der automatisk sættes en variabel: typisk DISPLAY=hostname:10
- Derved sendes X11 protokollen gennem en lokal portforwarding til X serveren

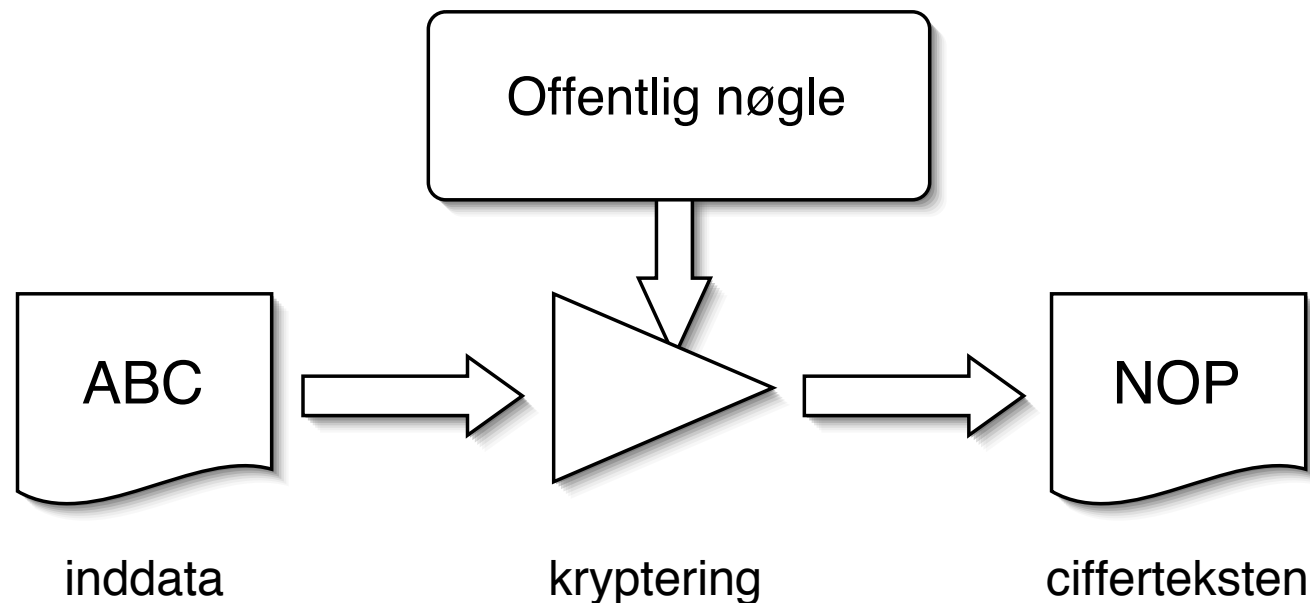
Kryptografi



Kryptografi er læren om, hvordan man kan kryptere data

Kryptografi benytter algoritmer som sammen med nøgler giver en ciffertekst - der kun kan læses ved hjælp af den tilhørende nøgle

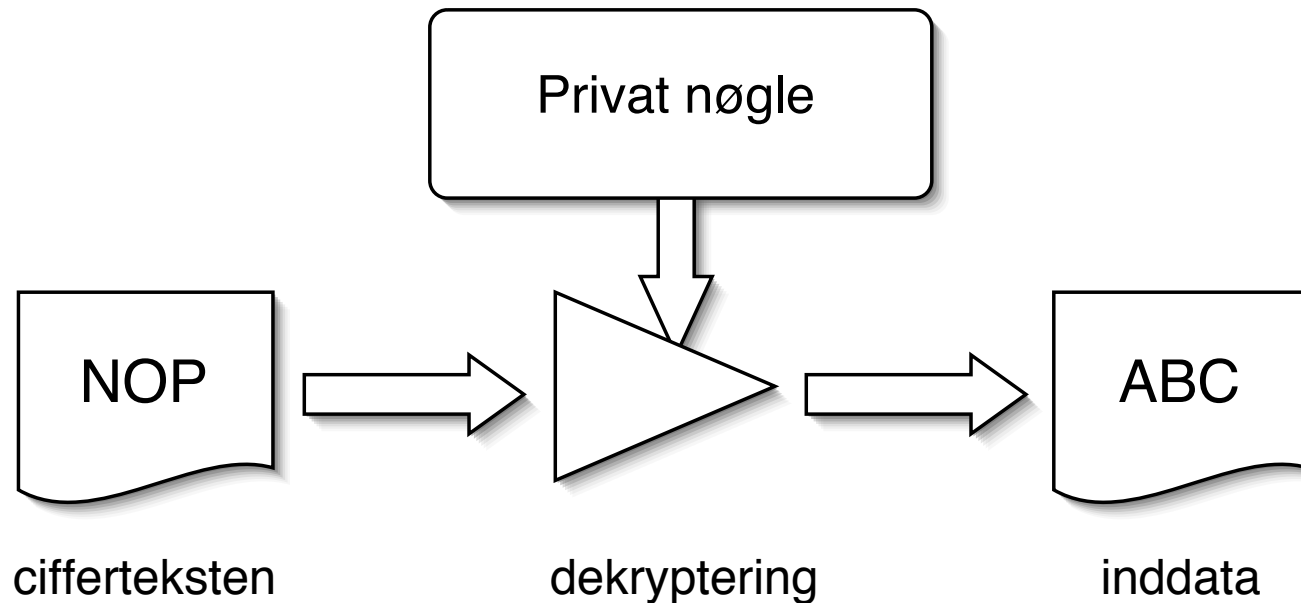
Public key kryptografi - 1



privat-nøgle kryptografi (eksempelvis AES) benyttes den samme nøgle til kryptering og dekryptering

offentlig-nøgle kryptografi (eksempelvis RSA) benytter to separate nøgler til kryptering og dekryptering

Public key kryptografi - 2



offentlig-nøgle kryptografi (eksempelvis RSA) bruger den private nøgle til at dekryptere

man kan ligeledes bruge offentlig-nøgle kryptografi til at signere dokumenter - som så verificeres med den offentlige nøgle

Kryptografiske principper

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et succesfuldt angreb på en krypto-algoritme er enhver genvej som kræver mindre arbejde end en gennemgang af alle nøglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgås nøje!

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid

<http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

DES, Triple DES og AES

AES

Advanced Encryption Standard

DES kryptering baseret på den IBM udviklede Lucifer algoritme har været benyttet gennem mange år.

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

Kilde: <http://csrc.nist.gov/encryption/aes/>

<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>

Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

e-mail og forbindelser

Kryptering af e-mail

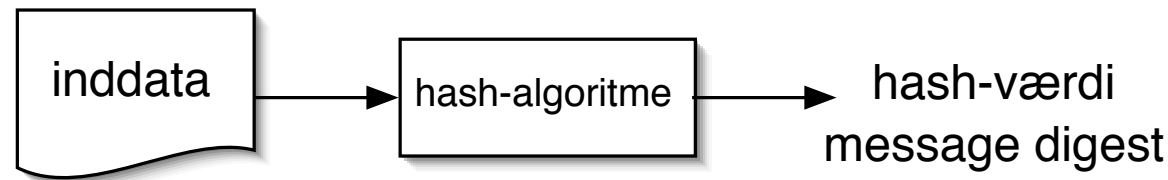
- Pretty Good Privacy - Phil Zimmermann
- PGP = mail sikkerhed

Kryptering af sessioner SSL/TLS

- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

Sender I kreditkortnummeret til en webserver der kører uden https?

MD5 message digest funktion



HASH algoritmer giver en unik værdi baseret på input

værdien ændres radikalt selv ved små ændringer i input

MD5 er blandt andet beskrevet i RFC-1321: The MD5 Message-Digest Algorithm

Både MD5 og SHA-1 undersøges nøje og der er fundet kollisioner som kan påvirke vores brug i fremtiden - *stay tuned*

Mission 2: Lær at genkende angreb

Alle IP adresser modtager en konstant strøm af portscan og angreb

Hjæææælp jeg bliver pinget!

Nu bliver jeg traceroutet!!!! ■

Alle aktive hackerværktøjer efterlader et spor - en angrebssignatur

Brug Ethereal til at lære dit netværk at kende!

Overvej at lave statistik med Intrusion Detection Systemer (IDS)

Hvordan ved du om et angreb er alvorligt?

■ Sørg for kun at gå i panik når det er nødvendigt!

IDS og Honeypots - ressourcekrævende?

The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks

"There are 69 separate departments at Georgia Tech with between 30,000-35,000 networked computers installed on campus." ... "In the six months that we have been running the Georgia Tech Honeynet **we have detected 16 compromised Georgia Tech systems on networks** other than our Honeynet. These compromises include automated worm type exploits as well as individual systems that have been targeted and compromised by hackers."

Honeypots og IDS systemer kan være ressourcekrævende, men måske en kombination kan være mere effektiv i visse tilfælde?

Kilde:

<http://www.tracking-hackers.com/papers/gatech-honeynet.pdf>

whois systemet

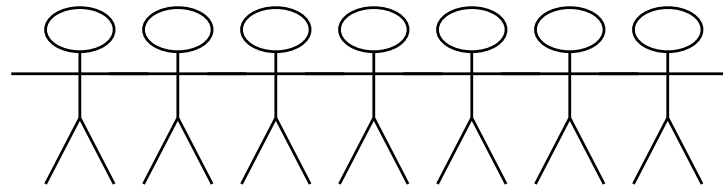
IP adresserne administreres i dagligdagen af et antal Internet registries, hvor de største er:

- RIPE (Réseaux IP Européens) <http://ripe.net>
- ARIN American Registry for Internet Numbers <http://www.arin.net>
- Asia Pacific Network Information Center <http://www.apnic.net>
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands <http://www.lacnic.net>

Man slår den ansvarlige abuse-adresse op med whois

Man skriver dernæst til `abuse@isp...`

Mission 3: Lær at samarbejde med andre



Et værn mod trusler

Du skal snakke høfligt til dine kolleger i andre firmaer

Du skal rapportere hvis du har kendskab til problemer hos andre

■ Hvordan ved modtageren at du er seriøs? PGP!

Hvordan ved du om hackeren lytter med?

■ Det ved du ikke

Case: en falsk paypal side - phishing

Jeg modtog mail om at jeg skulle gå til en *paypal URL*

Jeg sendte mail: February 21, 2005 7:56:36 AM CET

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hi Abuse

Please investigate the server:

<http://613.733.608.990/.cgi-bin/webscr/paypal/login.html>

Received in a piece of spam/phishing mail today

Thanks

Henrik

-----BEGIN PGP SIGNATURE-----

...

Case: en falsk paypal side - svar fra Hetzner

Min mail sendt: February 21, 2005 7:56:36 AM CET

Modtog midlertidigt e-mail svar: February 21, 2005 7:58:58 AM CET

Modtog endelig e-mail: February 21, 2005 9:37:06 AM CET

Hello Henrik,

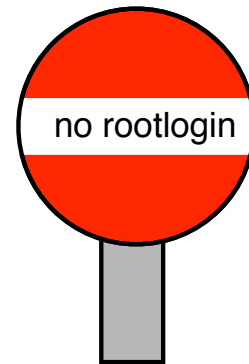
the site is offline now.

best regards

Stephan Konvickova

Hetzner Online AG

Mission 4: Lav et sæt regler for din virksomhed



Du må ikke benytte samme kodeord på private og virksomhedskonti

Du må ikke dele kodeord med de andre medarbejdere

Du må ikke efterstræbe root kodeordet på servere

Du må ikke foretage direkte login som root

■ Du bør overveje sudo eller tilsvarende

■ Man kan med sudo lave servere UDEN root kodeord!

SUDO konfiguration

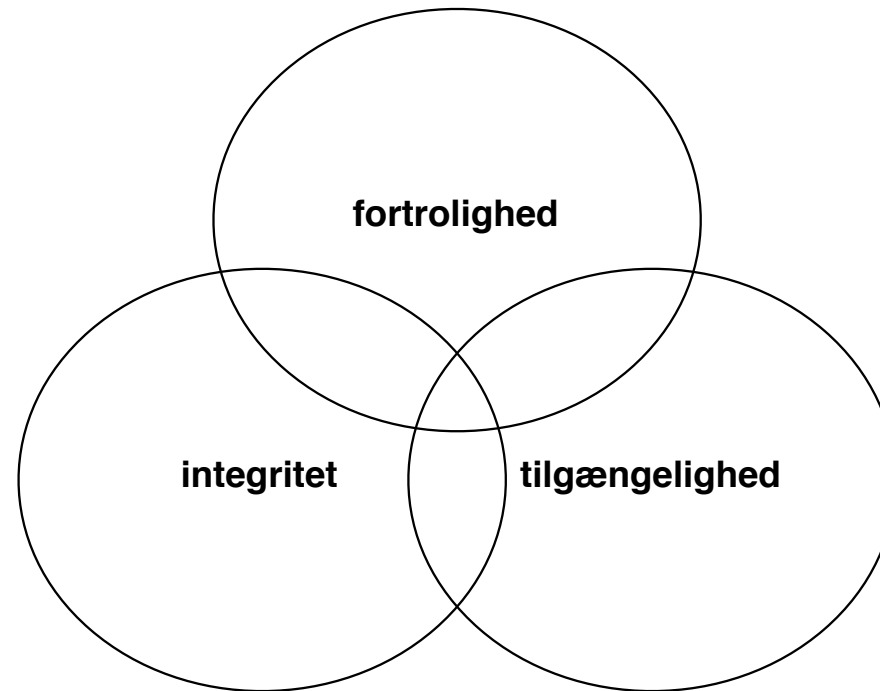
Eksempler fra manualsiden til sudoers skrives i filen `/etc/sudoers`:

```
# User alias specification
User_Alias      FULLTIMERS = millert, mikef, dowdy
# Runas alias specification
Runas_Alias     OP = root, operator
Runas_Alias     DB = oracle, sybase
# Cmnd alias specification
Cmnd_Alias      HALT = /usr/sbin/halt, /usr/sbin/fasthalt
Cmnd_Alias      REBOOT = /usr/sbin/reboot, /usr/sbin/fastboot
...

root            ALL = (ALL) ALL
%wheel          ALL = (ALL) ALL
FULLTIMERS     ALL = NOPASSWD: ALL
operator        ALL = HALT, REBOOT, /usr/oper/bin/
```

Husk ejerskab på scripts der udføres med SUDO!

Confidentiality Integrity Availability



fortrolighed/hemmeligholdelse - data holdes hemmelige

integritet - data er i god stand

tilgængelighed - data kan nås når man har brug for dem

teknologi eksempler

Der findes mange sikkerhedsprodukter

- firewalls
- anti-virus
- adgangskontrolsystemer
- fysiske låse
- ...

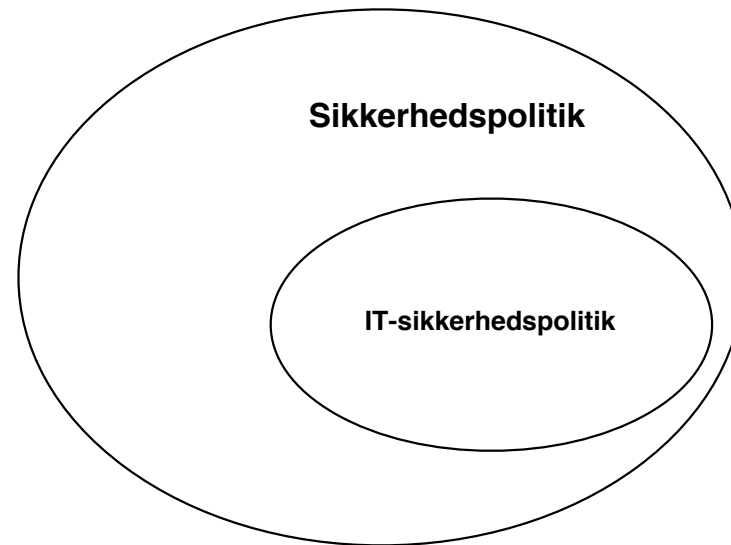
Men hvordan skal det hele bruges?

Tænk langsigtet!

god sikkerhed kommer fra langsigtede initiativer

Brug sikkerhedsprincipperne til at afgøre hvad der er vigtigst for jer

Definition: sikkerhedspolitik



Definition: Et sæt regler for virksomheden

Definition: it-sikkerhedspolitik
en politik der er begrænset til IT-områderne i virksomheden

- kan være en del af CYA strategi, cover your assets ;-)

Software og e-mail politik

Manglende e-mail politik: brevhemmelighed er beskrevet i straffeloven, og e-mail er omfattet! Uberettiget firing kan ligeledes være dyrt for virksomheden

Besøg fra Antipiratgruppen - kan resultere i dummebøder eller firing

Brug af Internet - er der båndbredde til at arbejde, hvis alle sidder og ser Tour de France på Internet?

Der skal være et sæt regler - så medarbejdere ved hvad der forventes af dem

Der skal ofte udføres en risikoanalyse for at sikre at alle områder dækkes med sikkerhedspolitikken

Mission 5: Lær at konfigurere din firewall

Du bør bruge firewalls

Du bør ikke bruge firewalls - som eneste sikkerhedsforanstaltning

En firewall er noget som **blokerer** trafik på Internet

■ En firewall er noget som **tillader** trafik på Internet

firewalls

Basalt set et netværksfilter - det yderste fæstningsværk

Indeholder typisk:

- Grafisk brugergrænseflade til konfiguration - er det en fordel?
- TCP/IP filtermuligheder - pakkernes afsender, modtager, retning ind/ud, porte, protokol, ...
- kun IPv4 for de kommercielle firewalls
- både IPv4 og IPv6 for Open Source firewalls: IPF, OpenBSD PF, Linux firewalls, ...
- foruddefinerede regler/eksempler - er det godt hvis det er nemt at tilføje/åbne en usikker protokol?
- typisk NAT funktionalitet indbygget
- typisk mulighed for nogle serverfunktioner: kan agere DHCP-server, DNS caching server og lignende

En router med Access Control Lists - ACL kaldes ofte netværksfilter, mens en dedikeret maskine kaldes firewall - funktionen er reelt den samme - der filtreres trafik

firewall regelsæt eksempel

```
# hosts
router="217.157.20.129"
webserver="217.157.20.131"
# Networks
homenet=" 192.168.1.0/24, 1.2.3.4/24 "
wlan="10.0.42.0/24"
wireless=wi0

# things not used
spoofed=" 127.0.0.0/8, 172.16.0.0/12, 10.0.0.0/16, 255.255.255.255/32 "
```

block in all # default block anything

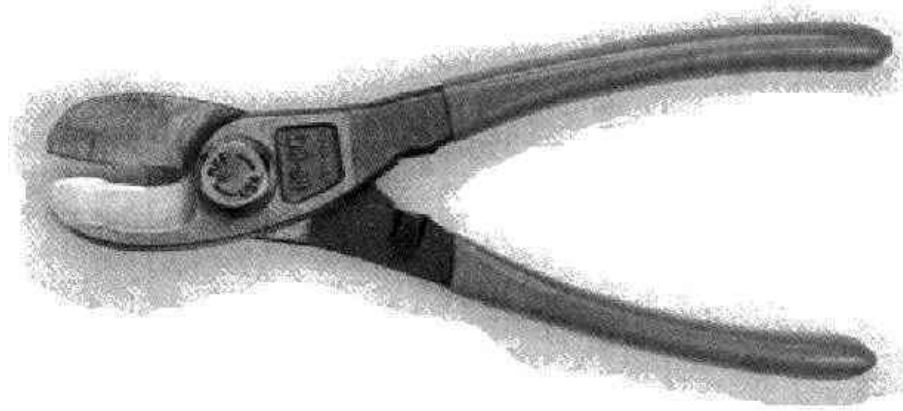
```
# loopback and other interface rules
pass out quick on lo0 all
pass in quick on lo0 all

# egress and ingress filtering - disallow spoofing, and drop spoofed
block in quick from $spoofed to any
block out quick from any to $spoofed

pass in on $wireless proto tcp from $wlan to any port = 22
pass in on $wireless proto tcp from $homenet to any port = 22
pass in on $wireless proto tcp from any to $webserver port = 80

pass out quick proto tcp from $homenet to any flags S/S keep state
pass out quick proto udp from $homenet to any keep state
pass out quick proto icmp from $homenet to any keep state
```

netdesign - med firewalls



Kilde: Marcus Ranum The ULTIMATELY Secure Firewall

Hvor skal en firewall placeres for at gøre størst nytte?

Hvad er forudsætningen for at en firewall virker?

At der er konfigureret et sæt fornuftige regler!

Hvor kommer reglerne fra? Sikkerhedspolitikken!

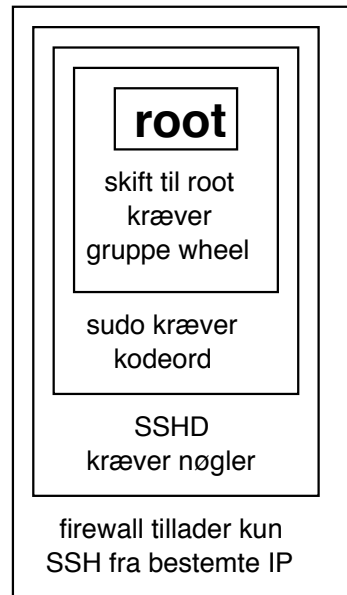
Mission 6: Lær at hærde dine systemer

Du bør hærde dit operativsystem

Du bør hærde dine applikationer

Du bør bruge buffer overflow beskyttelse

Flere lag af sikringsforanstaltninger



Ved at bruge flere sikkerhedsforanstaltninger kan man tåle enkelte nedbrud

Firewalls and Internet Security, William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Addison-Wesley, 2nd edition, 2003

Sørg altid for at have flere lag af sikkerhed!

hærdning af UNIX

start med at installere det mest nødvendige, reinstaller eventuelt maskinen

gennemgå systemerne kritisk

stop alle services som ikke skal bruges

slå alt til som skal bruges - logning eksempelvis

begræns adgangen til dem som skal bruges: eksempelvis tillad kun adgang til SSHD fra bestemte IP-adresser

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

Drop legacy kompatibilitet

Udryd gamle usikre

- protokoller - som SSH version 1
- programmer telnet, FTP, R* - password i klartekst
- undgå usikre NFS konfigurationer - root adgang m.v.

VÆK med dem!

Det handler om sikkerhed, det der ikke er aktivt kan ikke misbruges

Fundamentet skal være i orden

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

- redundans
- opdateret
- dokumenteret
- nem at vedligeholde

Husk tilgængelighed er også en sikkerhedsparameter

OSI og Internet modellerne

OSI Reference Model

Application
Presentation
Session
Transport
Network
Link
Physical

Internet protocol suite

Applications HTTP, SMTP, FTP, SNMP,	NFS
	XDR
	RPC
TCP UDP	
IPv4 IPv6 ICMPv6 ICMP	
ARP RARP MAC	
Ethernet token-ring ATM ...	

konfigurationsfejl - ofte overset

Forkert brug af programmer er ofte overset

- opfyldes forudsætningerne
- er programmet egnet til dette miljø
- er man udannet/erfaren i dette produkt

Hvad tror I der sker hvis en kommandofortolker som cmd.exe kopieres til webserverens programkatalog - /scripts på en IIS?

Det gør webfolk indimellem ...

buffer overflows et C problem

C programmeringssproget har dog også ulemper!

Det er svært at lave det rigtigt, man kan nemt glemme at frigive hukommelse og der er pointere som kan pege til forkerte adresser

Et buffer overflow er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

Stack protection er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken mod returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

Hvad kan man gøre - privilegier!

Hvorfor afvikle med administrationsrettigheder - hvis der kun skal læses fra en database?

least privilege betyder at man afvikler kode med det mest restriktive sæt af privileger - kun lige nok til at opgaven kan udføres .

privilege escalation er når man på en eller anden vis opnår højere privileger på et system, eksempelvis som følge af fejl i programmer der afvikles med højere privilegier. Derfor HTTPD servere på UNIX afvikles som nobody - ingen specielle rettigheder.

få rettigheder = lille skade

Secure Programming

DESCRIPTION

The `strcpy()` and `strncpy()` functions copy the string `src` to `dst` (including the terminating `'\0'` character).

`strncpy()` copies not more than `len` characters into `dst`, appending `'\0'` characters if `src` is less than `len` characters long, and not terminating `dst` if the length of `src` is greater than or equal to `len`.

Brug de rigtige funktioner!

undgå de farlige funktioner!

eksempelvis:

- `strcpy` er farlig - den kopierer til den møder en null-byte
- `strncpy` er i orden, den kopierer maksimalt /empty-bytes

secure programming burde være kendt - men nye programmører laver samme fejl :(

Stackguard

StackGuard detects and defeats stack smashing attacks by protecting the return address on the stack from being altered. StackGuard places a "canary" word next to the return address when a function is called. If the canary word has been altered when the function returns, then a stack smashing attack has been attempted, and the program responds by emitting an intruder alert into syslog, and then halts.

StackGuard <http://www.immunix.org/stackguard.html>

ved at placere en tilfældig værdi - og efterfølgende kigge på denne kan man opdage et buffer overflow og stoppe programmet

den tilfældige værdi kaldes for en canary - lidt i stil med minearbejderes kanariefugl som kunne advare om iltmangel

Advarsel: Stackprotection er ikke fejlfrit!

Selvom stackprotection med Stackguard og Propolice lyder som en 100% sikker løsning er der muligheder for at omgå det!

Det er et våbenkapløb

Men udviklerne finder også på nye måder at beskytte:

- non-executable heap
- non-executable stack
- Writable xor eXecute - enten kan man skrive til en side i hukommelsen, ELLER udføre programmer fra den side
- privilege separation - store programmer opdeles i en *kritisk del* og en ikke-kritisk del - som så kan udføres med lavere privileger. Eksempelvis SSHD

Mange af disse funktioner indbygges i UNIX systemer idag!

Mission 7: Lær at dokumentere dine systemer

Du bør beskrive dine forudsætninger for driften

Du bør dokumentere opsætningen

Du bør foretage revision af dokumentationen jævnligt

Du bør etablere change management - eksempelvis CVS til konfigurationsfiler

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 ved store opgraderinger

Burde være god systemadministrator praksis

Mission 8: Lær at overvåge dine systemer

Du bør overveje en centraliseret logningsstruktur hvis du har flere servere

Du bør altid bruge Network Time Protokol NTP til at synkronisere tiden

Du bør bruge integritetscheckere som tripwire, mtree, tcbck(AIX) eller AIDE

UNIX syslog

syslog er system loggen på UNIX og den er effektiv

- man kan definere hvad man vil se og hvor man vil have det dirigeret hen
- man kan samle det i en fil eller opdele alt efter programmer og andre kriterier
- man kan ligeledes bruge named pipes - dvs filer i filsystemet som tunneller fra chroot'ed services til syslog i det centrale system!
- man kan nemt sende data til andre systemer

Hvis man vil lave en centraliseret løsning er følgende link vigtigt:

<http://loganalysis.org>

swatch

Er et simpelt program til at analysere logs og handle ud fra indholdet

swatch kan eksempelvis:


- sende mail
- udføre et program, en handling
- give besked på skærmen eller lignende

swatch er baseret på en simpel configurationsfil

Webserver logs

I logfilerne kan man se hacker angreb - som referencer til filer der ikke eksisterer - 404 not found:

Statistics of: www.kramse.dk
Last Update: 09 Jun 2003 - 12:52
Reported period: Jun 2003 OK



[Close window](#)

```

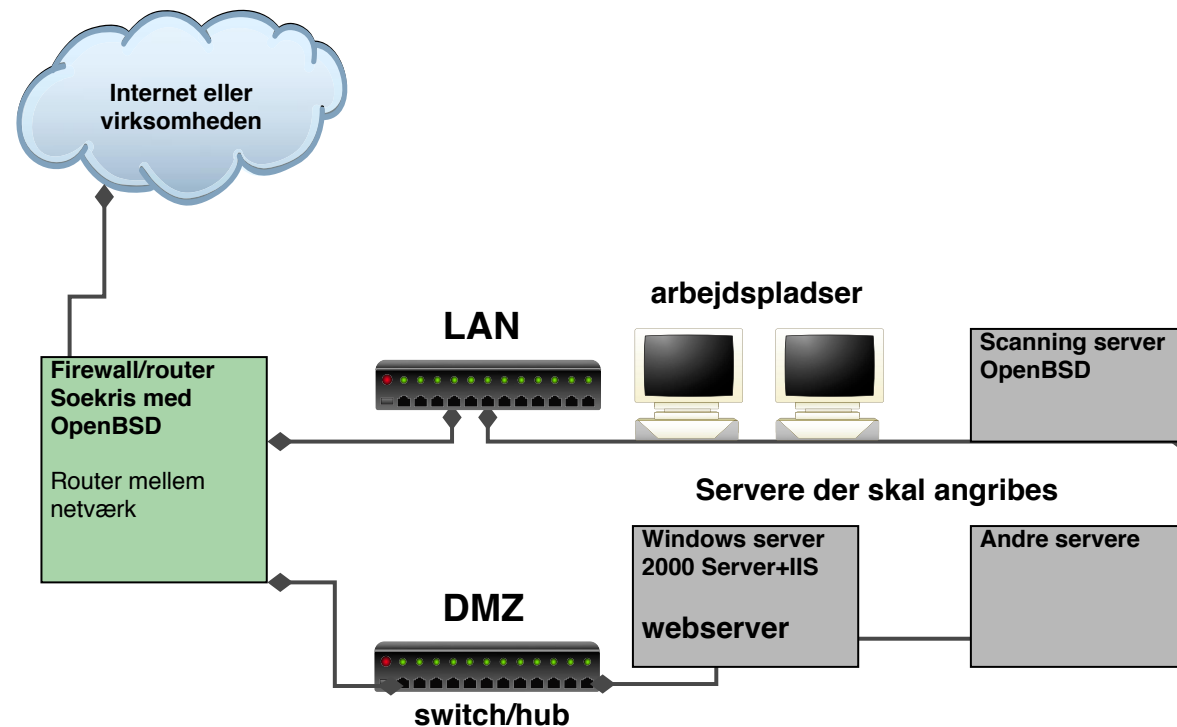
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
/_vti_bin/..%255c../%255c../%255c../winnt/system32/cmd.exe?/c+dir
/scripts/root.exe?/c+dir
/d/winnt/system32/cmd.exe?/c+dir
/c/winnt/system32/cmd.exe?/c+dir
/scripts/..%255c../winnt/system32/cmd.exe?/c+dir
/MSADC/root.exe?/c+dir
/_mem_bin/..%255c../%255c../%255c../winnt/system32/cmd.exe?/c+dir
/scripts/..%252f../winnt/system32/cmd.exe?/c+dir
/scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
/scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
/msadc/..%255c../%255c../%255c/..%c1%1c../%c1%1c../%c1%1c../winnt/system32/cmd.exe?/c+dir
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
/pics/LoginTiffs
  
```

integritetscheckere - når det går galt

integritetscheckere - hjælper med til at opdage problemer
er baseret på en signatur af filerne - hvordan de skal se ud
typisk informeres man hvis en af følgende hændelser sker:

- Hvis ejerskabet ændres
- Hvis rettighederne ændres
- Hvis filen ændres - størrelse/indhold - check foretages med hash algoritmer som MD5

Mission 9: Lær at isolere problemerne



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

chroot og jails

chroot står for change root, og betyder at processen som kalder chroot systemkaldet udskifter sin *filesystemsrod*-/ med et andet katalog på systemet

oprindeligt blev denne funktion lavet til at teste nye UNIX releases uden at overskrive det oprindelige miljø man havde på systemet

men det kan bruges til at give mere sikkerhed

en daemon eller service der kører chroot'ed er sværere at udnytte - simpelthen fordi den kun har adgang til en lille del af systemet

FreeBSD har en endnu mere avanceret version af chroot som giver endnu mere kontrol over det miljø som programmerne ser

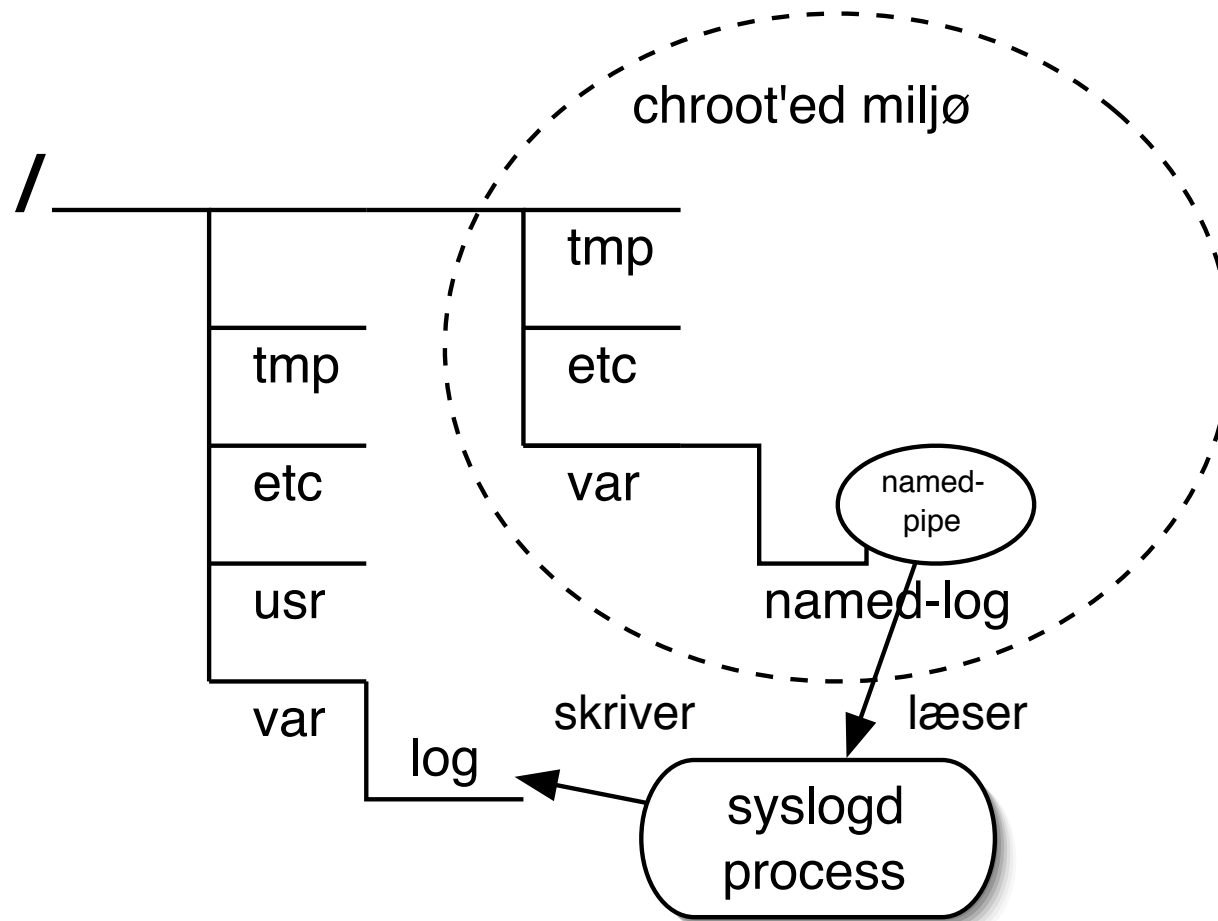
Solaris 10 har fået *jails på steroider*

brug af chroot

De services man typisk vil chroot'e er BIND, Apache og andre udsatte services

Der findes heldigvis udførlige beskrivelser af hvordan man chroot'er de mest almindelige services

chroot konceptet



named pipes og chroot giver mulighed for logging udenfor chroot

Når det går galt

Vi håndterer selv hændelsen

Vi installerer de seneste patches og en firewall det er *godt nok(tm)*



Er det best current practice?



Nej, det er en begynderfejl, **ad-hoc oprydning giver ikke tryghed**

Kend dine begrænsninger!

Kend best practice for oprydning!

Brug eksempelvis CERT guidelines

Hvad koster dårlig sikkerhed?

Regningen for håndtering af en sikkerhedshændelse med hjælp udefra

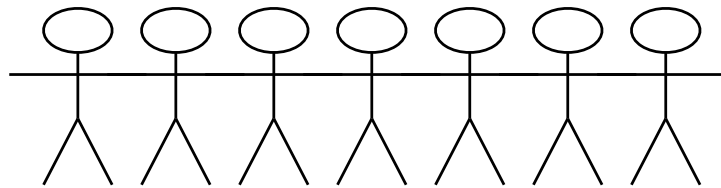
Konsulentbistand 20 timer med weekendtillæg a 2.500, ialt eks moms kr. 50.000

Arbejdstid for egne medarbejdere

Mistede ordrer - risiko er også risiko for at gå glip af noget gunstigt

En banal hændelse koster mindst kr. 50.000!

Opsummering



Et værn mod trusler

Husk følgende:

- UNIX og Linux er blot eksempler - Apache HTTPD kører fint på Windows
- DNS er grundlaget for Internet - og sikkerheden er dårlig generelt!
- Procedurerne og vedligeholdelse er essentiel for alle operativsystemer!
- Man *skal hærde* operativsystemer *før* man sætter dem på Internet
- Husk: IT-sikkerhed er ikke kun netværkssikkerhed og serversikkerhed!

Sikkerhed kommer fra langsigtede initiativer

Spørgsmål?

Henrik Lund Kramshøj
hk@security6.net

<http://www.security6.net>

I er altid velkomne til at sende spørgsmål på e-mail

PS Jeg kan anbefale det sidste nummer af Usenix ;Login: februar 2005 bladet er spækket med artikler om UNIX sikkerhed!

Hacker - cracker

Det korte svar - drop diskussionen

Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig - og idag har det begge betydninger.

Idag er en hacker stadig en der bryder ind i systemer!

ref. Spafford, Cheswick, Garfinkel, Stoll, ... - alle kendte navne indenfor sikkerhed

Hvis man vil vide mere kan man starte med:

- *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Clifford Stoll
- *Hackers: Heroes of the Computer Revolution*, Steven Levy
- *Practical Unix and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz

Aftale om test af netværk

Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man får konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde - eller fængselsstraf i alvorlige tilfælde
- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frit efter: <http://www.stophacking.dk> lavet af Det Kriminalpræventive Råd
- Frygten for terror har forstærket ovenstående - så lad være!

Anbefalinger til jer

Oversigt over anbefalinger

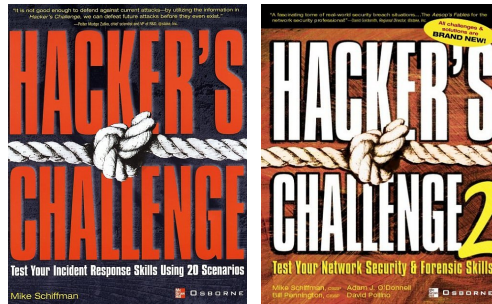
Følg med! - læs websites, bøger, artikler, mailinglister, ...

Vurder altid sikkerhed - skal integreres i processer

Hændeshåndtering - du vil komme ud for sikkerhedshændelser

Lav en sikkerhedspolitik - herunder software og e-mail politik

Hackers Challenge



Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

Hacker's Challenge II : Test Your Network Security and Forensics Skills af Mike Schiffman McGraw-Hill Osborne Media, 2003 ISBN: 0072226307

Bogen indeholder scenarier i første halvdel, og løsninger i anden halvdel - med fokus på relevante logfiler og sårbarheder

CISSP fra ISC2

(ISC)²SM

(CISSP)[®]

(SSCP)^{CM}

Approved marks of the International Information Systems Security Certification Consortium, Inc.

Primære website: <http://www.isc2.org>

Vigtigt link <http://www.cccure.org/>

Den kræver mindst 3 års erfaring indenfor et relevant fagområde

Multiple choice 6 timer 250 spørgsmål - kan tages i Danmark

GIAC GSEC krav



Security Essentials - basal sikkerhed

Krav om en *Practical assignment* - mindst 8 sider, 15 sider i gennemsnit

multiple choice eksamen

Primære website: <http://www.giac.org>

Reading room: <http://www.sans.org/rr/>

Der findes en god oversigt i filen *GIAC Certification: Objectives and Curriculum* http://www.giac.org/GIAC_Cert_Brief.pdf

Referencer

Papers - der findes MANGE dokumenter på Internet

- CERT/CC <http://www.cert.org>
- AusCERT Computer Emergency Response Team for Australia
<http://www.auscert.org.au/>
- <http://www.securityfocus.com>
- CERIAS hotlist http://www.cerias.purdue.edu/tools_and_resources/hotlist/
- Dansk site holder jævnligt møder <http://www.sikkerhedsforum.dk>

Honeypots og sårbare systemer

- <http://www.project.honeynet.org> - diverse honeynet projekter information om pakker og IP netværk

Husk også at mange forlag tillader at man henter et kapitel som PDF!

Referencer: bøger

- *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Ed Skoudis, Prentice Hall PTR, 1st edition July 2001
- *CISSP All-in-One Exam Guide*, Shon Harris, McGraw-Hill Osborne Media, 2nd edition, June 17 2003
- *Practical UNIX and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz, 3rd Edition, O'Reilly February 2003
- *Network Security Assessment: Know Your Network*, Chris McNab, O'Reilly March 2004
- *Secure Coding: Principles & Practices*, Mark G. Graff, Kenneth R. van Wyk, O'Reilly June 2003
- *Firewalls and Internet Security*, William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Addison-Wesley, 2nd edition, 2003
- *Building Firewalls with OpenBSD and PF*, Jacek Artymiak, 2nd edition 2003
- bøger om TCP/IP - Alle bøger af Richard W Steven kan anbefales!
- Reference books for the CISSP CBK domains - en liste der vedligeholdes af Rob Slade
<http://victoria.tc.ca/int-grps/books/techrev/mnbksccd.htm>

Hackerværktøjer

- nmap - <http://www.insecure.org> portscanner
- Nessus - <http://www.nessus.org> automatiseret testværktøj
- l0phtcrack - <http://www.atstake.com/research/lc/> - The Password Auditing and Recovery Application, kig også på Cain og Abel fra <http://oxid.it> hvis det skal være gratis
- Ethereal - <http://www.ethereal.com> avanceret netværkssniffer
- OpenBSD - <http://www.openbsd.org> operativsystem med fokus på sikkerhed
- <http://www.isecom.org/> - Open Source Security Testing Methodology Manual - gennemgang af elementer der bør indgå i en struktureret test
- Putty - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> terminal emulator med indbygget SSH



<http://www.remote-exploit.org/?page=auditor> - Auditor security collection - en boot CD med hackerværktøjer

Hvordan bruges hackerværktøjerne

Tænk som en hacker

Rekognoscering

- ping sweep
- portscan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

Udnyttelse/afprøvning: Nessus, whisker, exploit programs

Oprydning

- Lav en rapport
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

I skal jo også VISE andre at I gør noget ved sikkerheden.

Reklamer: kursusafholdelse

Security6.net afholder følgende kurser med mig som underviser

- IPv6 workshop - 1 dag
Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk. Internetprotokollerne har eksisteret i omkring 20 år, og der er kommet en ny version kaldet version 6 af disse - IPv6.
- Wireless teknologier og sikkerhed workshop - 2 dage
En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk og integration med eksempelvis hjemmepc og virksomhedens netværk
- Hacker workshop 2 dage
Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, Nessus m.fl.
- Forensics workshop 2 dage
Med fokus på tilgængelige open source værktøjer gennemgås metoder og praksis af undersøgelse af diskimages og spor på computer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage
Informere om trusler og aktivitet på Internet, samt give et bud på hvorledes en avanceret moderne firewall idag kunne konfigureres.

Security6.net holder i 2005 kurser i eget navn og med rabat!

Foreninger



Sikkerhedsforum DK - dansk forening for sikkerhed

<http://www.sikkerhedsforum.dk>

BSD-DK - dansk forening for BSD'erne, <http://www.bsd-dk.dk>

SSLUG, Skåne Sjælland Linux User Group

<http://www.sslug.dk>

DKUUG, Dansk UNIX User Group, <http://www.dkuug.dk> - giver god rabat på bøger gennem <http://www.polyteknisk.dk>, typisk 15-20%

Soekris bestilling i Danmark



- Soekris 4501-30 + case..... 1300,- Soekris 4801-50 + case..... 1750,-
- Strømforsyning 1.5A (lille).... 130,- Strømforsyning 3A (stor)..... 170,-
- vpn1411 miniPCI..... 550,- 4801 Harddisk mount kit 2.5"..... 70,-
- Alle priser er circapriser og ekskl. moms. kontakt Catpipe for nøjagtige oplysninger!
<http://www.catpipe.net>