Velkommen til

Internet sikkerhedstendenser i 2009

Content Security Seminar

Henrik Lund Kramshj
hlk@security6.net

Slides er tilgngelige som PDF

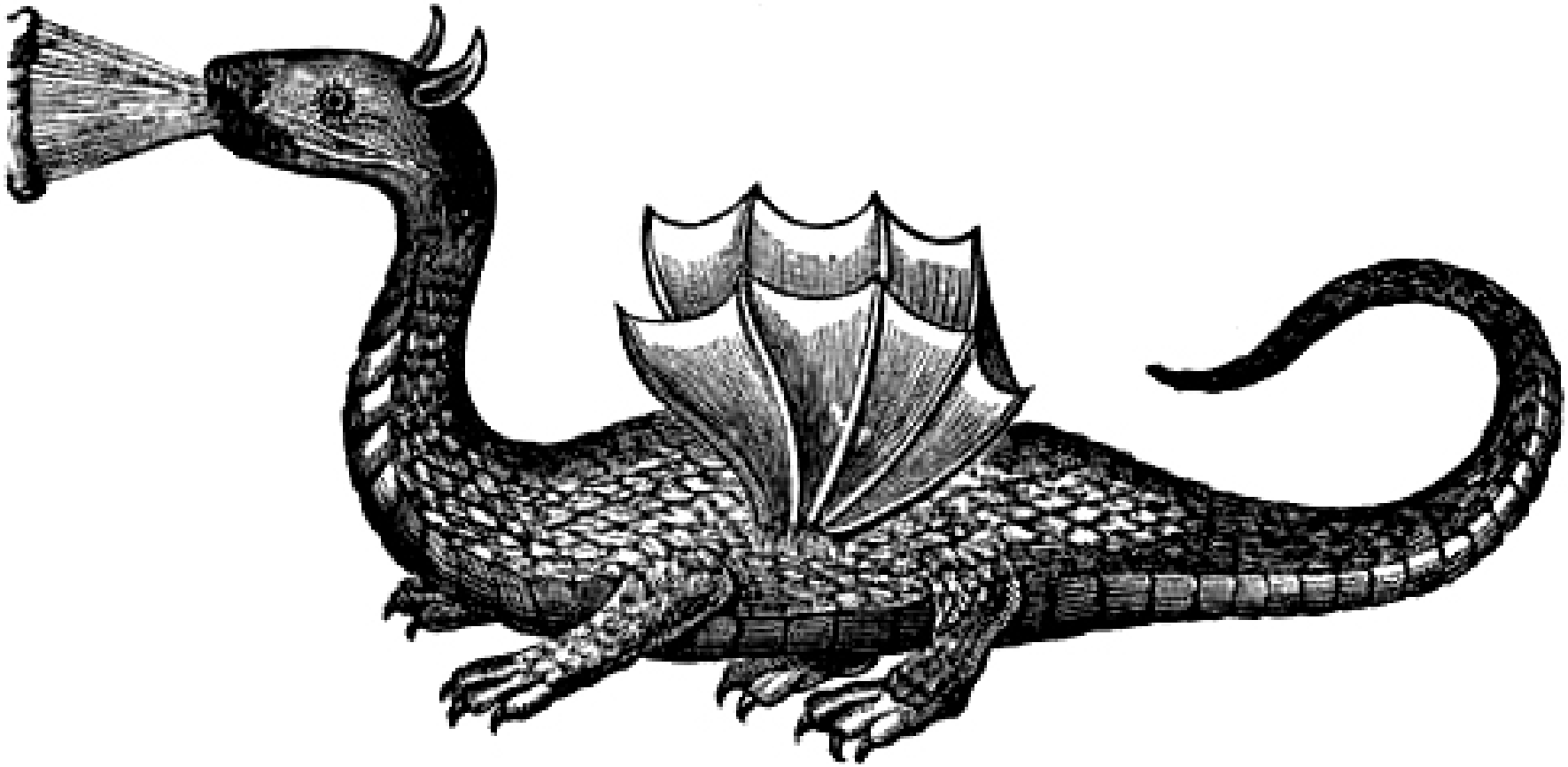
Forml

Give overblik over hvad internetsikkerhed betyder i r 2009

Hvad er almindeligt forekommende hndelser

Hvad kan vi forvente os af 2009

Internet - Here be dragons



Himlen falder ned

... igen

Rinse repeat

Kendte srbarheder udnyttes stadig

Kendte angrebsmetoder udvides - social engineering

Stadig misbrug af kreditkort, selv med Verified by VISA p plads osv.

Gider I hre de samme rd igen

2008 hvad skete der

Botnets fortstter med at vokse - millionvis af computere

Botnets bliver svrere at udrydde

Sikkerhed for botnets er blevet populrt

Botnets er blevet en hyldevare

Botnets er grundlaget for mange nye angreb

Moderne botnets

Botnets spreder sig ved at inficere s mange systemer som muligt

Botnets idag vokser gerne langsommere - ingen ny Code Red hastighedsrekord

Spreder sig via SMTP, HTTP, SMB, ... alle protokoller der kan overfre data

Bannerkampagner og 3. parts kilder til elementer p din side?!

Nr frst der er kommet malware p systemet udvides med moduler

Malware idag

Malware idag er sofistikeret

Modulrt opbygget

Benytter strk kryptering til at sikre administrationen af inficerede computere

Benytter seneste sikkerhedshuller - 0 days til at sprede sig

Benytter de seneste rootkit metoder til at holde sig skjult

Muterer efter alle kendte metoder for at undg opdagelse

Larmer mindre end tidligere

Botnets og malware slges med support

Malware programmrer har lrt kundepleje

”Kb denne version og f gratis opdateringer”

Lej vores botnet med 100.000 computere

milw0rm - dagens buffer overflow

http://milw0rm.com/

Metasploit

What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

Idag findes der samlinger af exploits som milw0rm

Udviklingsvrktjerne til exploits er idag meget raffinerede!

Exploits slges p bde bne og lukkede ”exploitbrser”

http://www.metasploit.com/

Spamming as a service

BBC programmet Click undersgte mulighederne for at kbe sig adgang til et botnet

Lejede 22.000 computere og afprvede skadevirkninger

Det virkede (desvrre) som forventet

Kilde: Marts 2009 BBC
http://news.bbc.co.uk/1/hi/programmes/click$_online/7932816.stm$

Hvad vil der ske p serverne i 2009

Problemerne med sikkerhed bliver ikke lst endeligt

Mange angreb vil fortstte - status quo

Organiseret kriminalitet vil fortstte med at udnytte mulighederne

Mlgruppen for angreb vokser - flere vil blive ramt

Serveroperativsystemerne er dog i mange tilflde mere resistente idag

Gode operativsystemer

Nyere versioner af Microsoft Windows, Mac OS X og Linux distributionerne inkluderer:

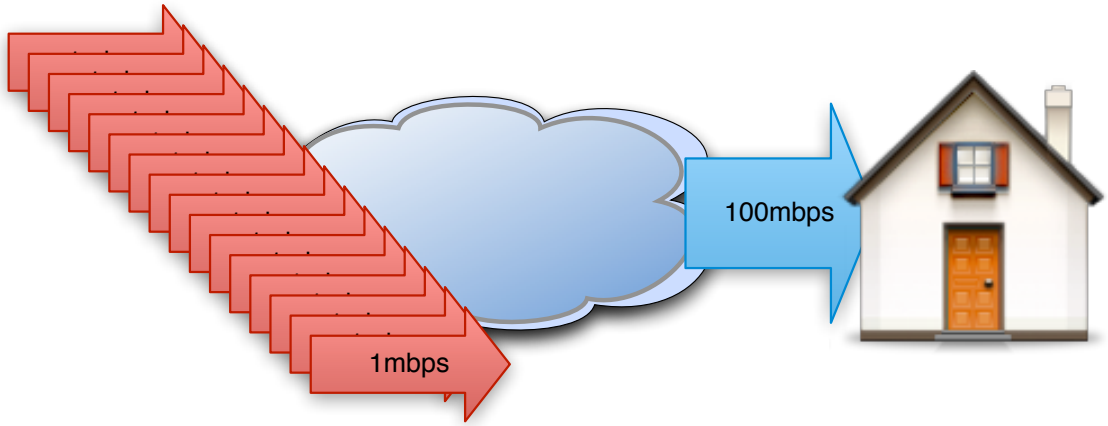
- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

Windows 2008 er klart at foretrkke fremfor Windows 2000 servere ;-)

OpenBSD er nok net lngst og et godt eksempel
http://www.openbsd.org/papers/

... og husk alle de sdvanlige rd, opdateringer, firewalls, backup, UPS osv.

Dr din infrastruktur i 2009



Selvom dine servere er iorden skal du vre klar til at modtage angreb

Hvor mange ressourcer bruger du p din infrastruktur

Kan du stadig supportere den og kre din forretning?

Hvad er *din* kerneforretning

Nyeste botnets

Det amerikanske sikkerhedsfirma Finjan har optrevlet et botnet med 1,9 millioner inficerede computere.

Finjan har offentliggjort fundet p RSA-konferencen og betegner botnettet som et af de strste, som er kontrolleret af en enkelt, kriminel bande, skriver CNet.

Botnettet har vret aktivt siden februar og hostes i Ukraine, hvorfra det styres af seks personer. Den kriminelle bande styrer de indlemmede Windows XP-maskiner til at kopiere filer, registrere tastetryk, sende spam og tage screenshots.

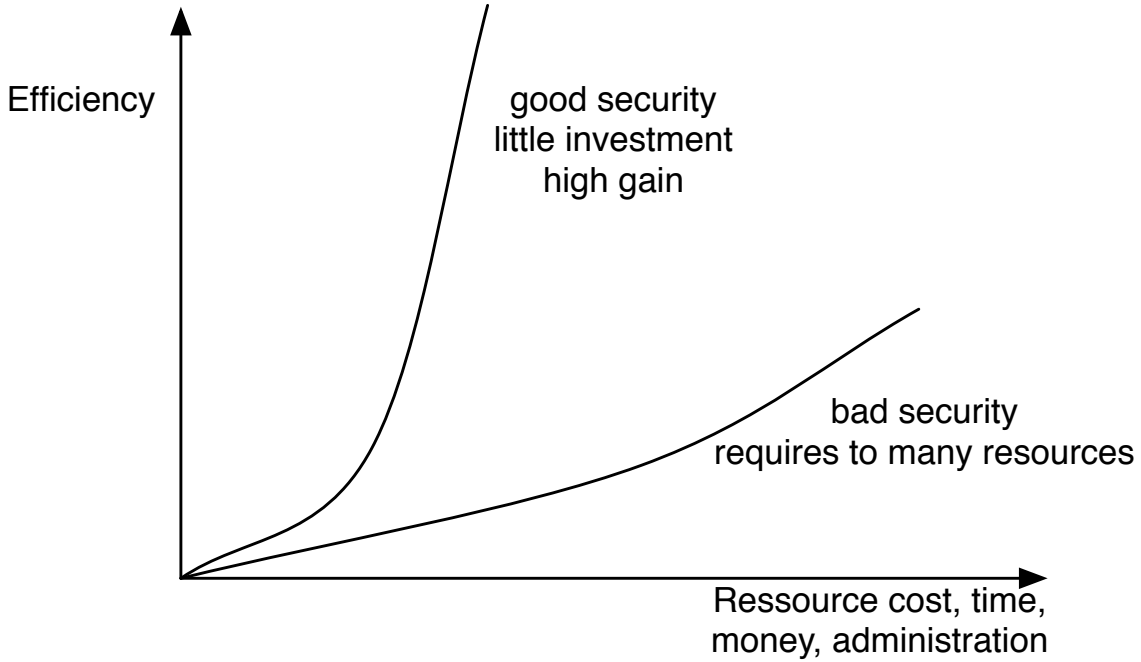
Iflge det engelske it-medie Computer Weekly har banden solgt kontrollen over de inficerede computere i bundter af 1.000 computere for omkring 250-600 kroner, og iflge CNet har banden kunnet tjene op til 1,1 millioner kroner om dagen ved at udleje zombierne til andre.

Hver uge har historier om botnets - denne artikel p version2.dk er fra 22. april

Kilde:

http://www.version2.dk/artikel/10679-sikkerhedsfirma-finder-botnet-med-19-mio-zombier

Gode sikkerhedsforanstaltninger



Du har begrnsede ressourcer - udnyt dem bedst muligt - det er din pligt

Din indsats skal st ml med effektiviteten

Hvad rammer dine brugere i 2009

Drive by hacking, flg et link til en server

- sekundet efter er din maskine inficeret - *booom*

Phishing - Receipt for Your Payment to mark561@bt....com

Mark Willson
145 Church Lane East
Aldershot, Hampshire, GU11 3ST
United Kingdom

Important Note: Mark Willson has provided an Unconfirmed Address. If you are planning on shipping items to Mark Willson, please check the Transaction Details page of this payment to find out whether you will be covered by the PayPal Seller Protection Policy.

Note:

If you haven't authorized this charge ,click the link below to cancel transaction

Cancel Transaction:

https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

*SSL connection:
PayPal automatically encrypts your confidential information in transit from your computer to ours using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available)
---

http://paypal-co.uk.dt6.pl/?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

Kan du selv genkende Phishing kan dine brugere

Fast flux

Tidligere var malware sites p f hackede servere

Idag er malware sites placeret p mange computere

Med lav DNS Time to Live (TTL) ”sikres oppetiden bedre”

Svrt at finde alle IP-adresserne og rapportere dem

Fast flux netvrk indgr idag i angreb mod danske firmaer

Know Your Enemy: Fast-Flux Service Networks
http://www.honeynet.org/book/export/html/130

Hvordan bliver dine brugere mere sikre

Lad vre med at bruge computere ☺

Lad vre med at bruge een computer til alt

Firmacomputeren er ikke en privat brbar, ls den - alle har rd til en privat netbook

Forskellige systemer til forskellige forml

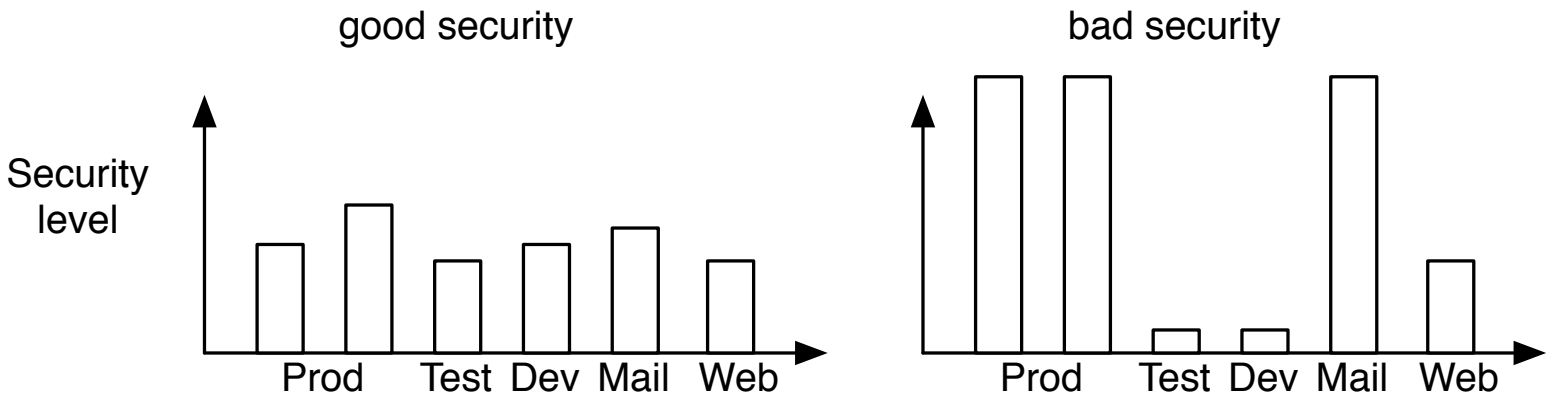
Brug en sikker konfiguration, minimumskonfiguration alle steder

Opstning af netvrk, hvordan? Security Configuration Guides + paranoia

- http://csrc.nist.gov/publications/PubsSPs.html
- http://www.nsa.gov/research/publications/index.shtml

- http://www.nsa.gov/ia/guidance/security$_{c}onfiguration_{g}uides/index.shtml$

Afbalanceret sikkerhed



Det er bedre at have et ensartet niveau

Hvor rammer angreb hvis du har Fort Knox et sted og kaos andre steder

Hackere vlger ikke med vilje den svreste vej ind

Forslag til aktiviteter

Accepter at der ikke findes 100% sikkerhed

Vlg dit sikkerhedsniveau

Vlg dine kampe med omhu
- lad andre kmpe mod spam hvis det ikke er din kerneforretning

For lidt samarbejde

Team up!

Snak med din sidemand/dame - I har sikkert mange af de samme udfordringer.

Husk flgende: Sikkerhed kommer fra langsigtede intiativer

Informationssikkerhed er en proces

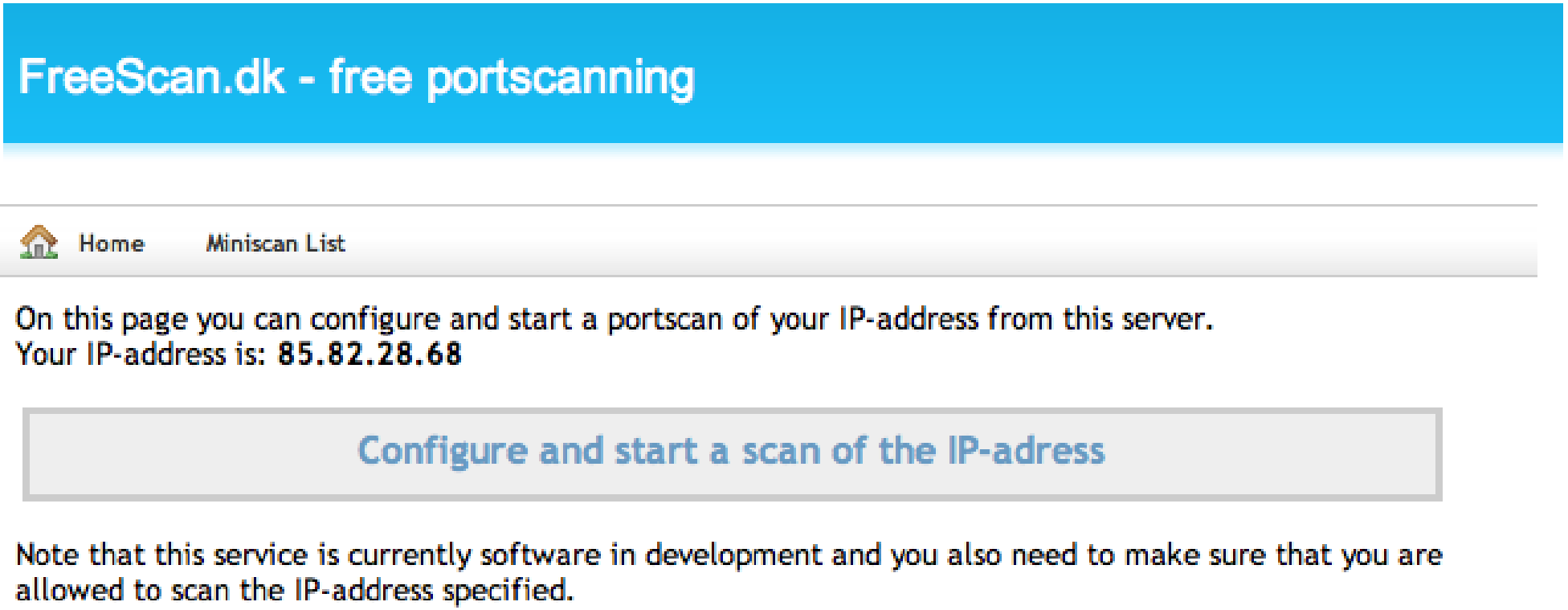
Sprgsml?

Henrik Lund Kramshj
hlk@security6.net

http://www.security6.net

I er altid velkomne til at sende sprgsml p e-mail

FreeScan.dk - gratis portscanning



http://www.freescan.dk

Reklamer: kursusafholdelse

Flgende kurser afholdes med mig som underviser

- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netvrk.
- Wireless teknologier og sikkerhed workshop - 2 dage
  En dag med fokus p netvrksdesign og fornuftig implementation af trdlse netvrk, samt integration med hjemmepc og wirksomhedsnetvrk.
- Hacker workshop 2 dage
  Workshop med detaljeret gennemgang af hackermetoderne angreb over netvrk, exploitprogrammer, portscanning, Nessus m.fl.
- TCP/IP workshop 2 dage
  Med fokus p almindelige protokoller i TCP/IP gennemgs grundlaget for internet gennem 5 dage med teori og opgaver p en skalmodel af internet
- Moderne Firewalls og Internetsikkerhed 2 dage
  Informere om trusler og aktivitet p Internet, samt give et bud p hvorledes en avanceret moderne firewall idag kunne konfigureres.

Se mere p http://www.security6.net/courses.html