

Welcome to

# Tendenser i sikkerhed

November 2010

Henrik Lund Kramshøj  
hlk@solidonetworks.com

<http://www.solidonetworks.com>

Slides are available as PDF

Give en update på udviklingen indenfor internetsikkerhed og sikkerhedstrusler

Give input til hvad I skal fokusere på

Jeg vil forsøge at gennemgå ting fra 2010

En potpourri af sikkerhedsemner - inspiration

Feedback og kommentarer modtages



KI 17-21

Mindre foredrag mere snak

Mindre enetale, mere foredrag 2.0 med socialt medie, informationsdeling og interaktion

Chelmsford, Mass., January 19, 2010 - Botnet-driven distributed denial of service (D-DoS) attacks focused on services and applications are the number one operational security problem facing the service provider community

## Attacks Shift to the Cloud

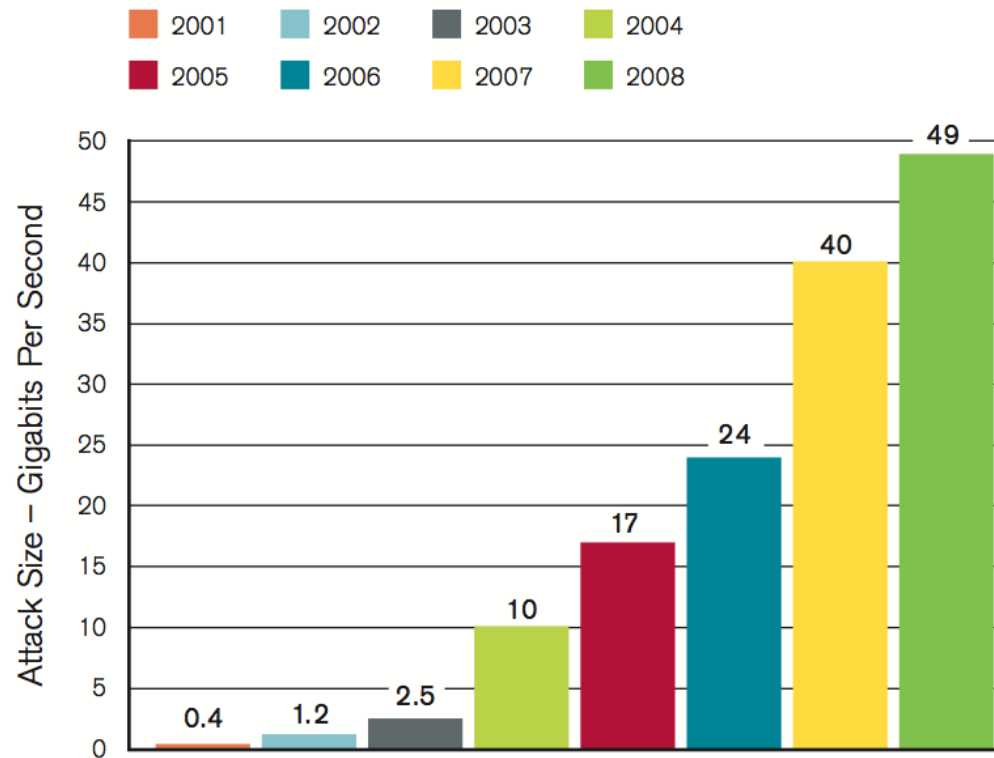
Nearly 35% of respondents believe that more sophisticated service and application attacks represent the largest operational threat over the next 12 months, displacing large scale botnet-enabled attacks, which came in second this year at 21%.

... near doubling in peak distributed denial of service (DDoS) attack rates year-over-year, with peak attack rates growing from 400 Mbps to more than 40 Gbps since 2001.

This year, providers reported a peak sustained attack rate of 49 Gbps, a 22% growth over last year's peak of a 40 Gbps attack, which shows the attack scale growth has slowed in the past 12 months.

Kilde: <http://www.arbornetworks.com/report>

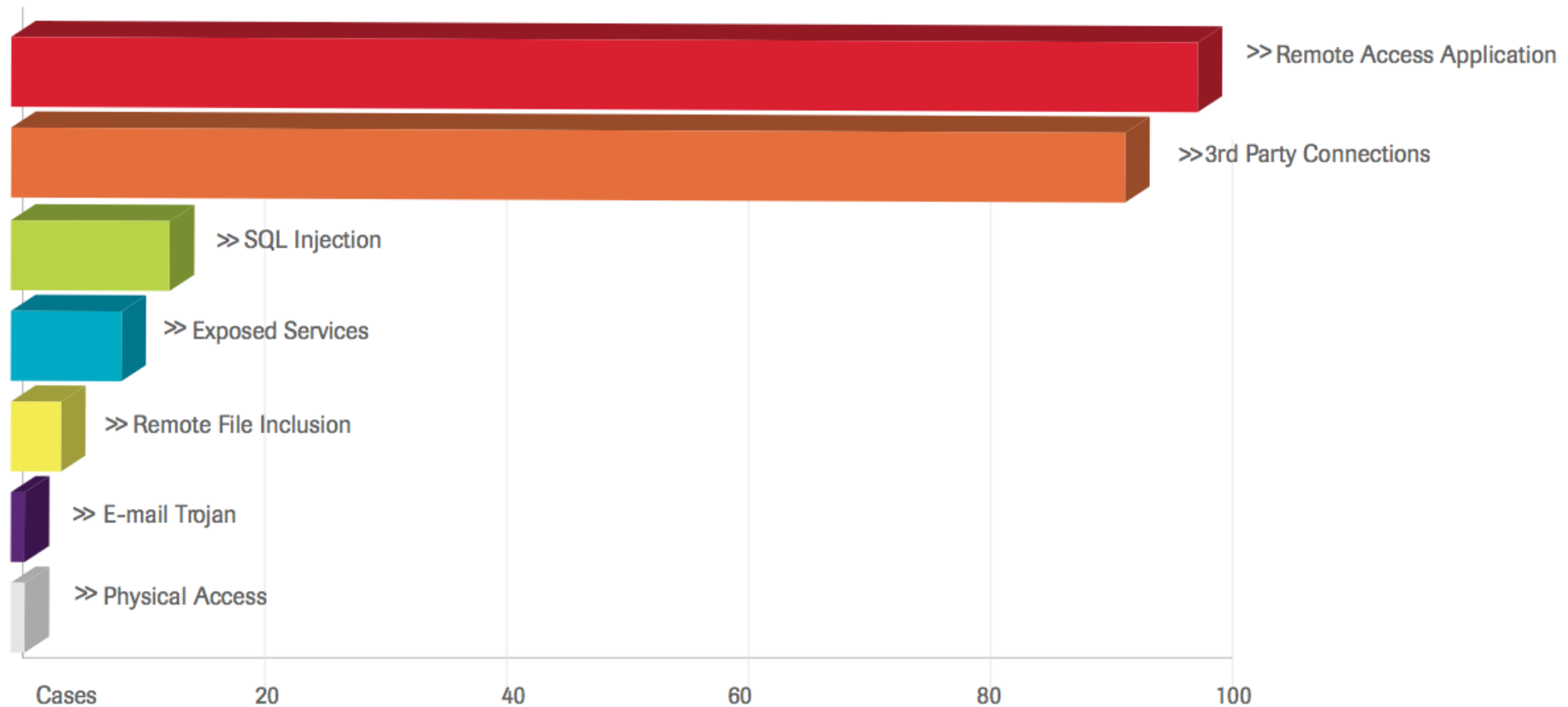
## Largest DDoS Attack – 49 Gigabits Per Second



**Figure 1:** Largest DDoS Attack – 49 Gigabits Per Second

Source: Arbor Networks, Inc.

Se også <http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/ddos-basics.pdf>



Initial Entry: The method utilized by the attacker to gain unauthorized access to a system.

Kilde: <https://www.trustwave.com/>

- Remote Access Application: A remote access application is any application used to administer a system remotely. While GUI-based remote access solutions are popular today, command-line remote applications, such as telnet, are still in use today. ... The level of attack difficulty is intermediate, but can be trivial when passwords are blank or left as the default value.
- Third Party Connectivity: This could include any telecommunications line connecting two or more physically dispersed networks, such as multiprotocol label switching (MPLS), asynchronous transfer mode (ATM), and frame relay, a data transmission technique. This easy-to-use method could leave the entire network accessible via the connections, and therefore open to compromise.
- SQL Injection: Gaining mass popularity with the explosion of Web-based, database-driven applications, SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. This method of attack has existed since 1998; on Christmas Day, a security researcher known as rfp detailed the attack in an article called "NT Web Technology Vulnerabilities" published in Phrack magazine, issue 54.

Rapporten kan varmt anbefales - men der er skræmmende mange gamle sårbarheder!

Kilde: <https://www.trustwave.com/>

The Phrack Staff is proud to announce that p67 will be released on November 17.  
( Current issue : #66 — Release date : 11/06/2009 )



Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. ... This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface.

State-of-the-art kompleks trussel

Jeg er ikke ekspert på Stuxnet

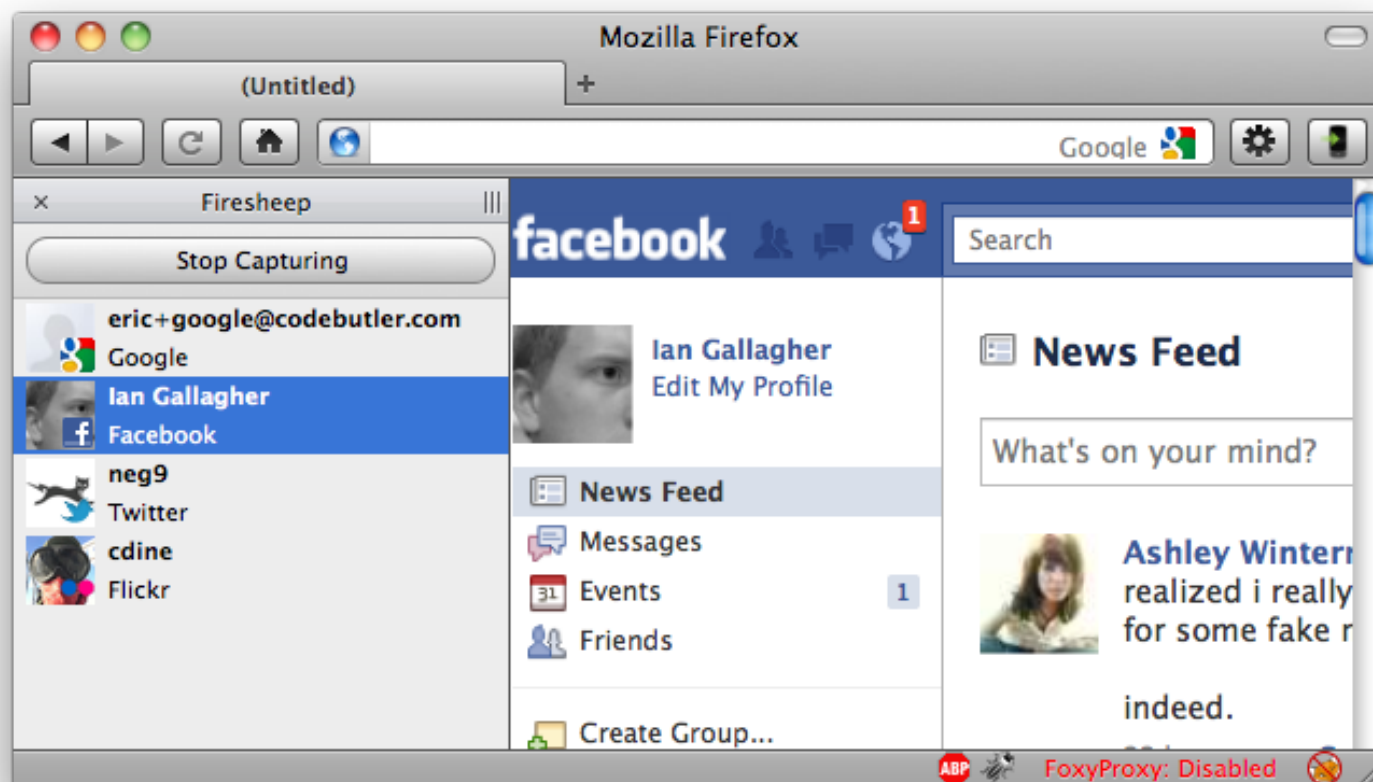
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)

<http://www.symantec.com/connect/blogs/stuxnet-breakthrough>

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution. Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732)
- Spreads in a LAN through a vulnerability in the Windows Print Spooler. Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073)
- Spreads through SMB by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874).
- Copies and executes itself on remote computers through network shares.
- Copies and executes itself on remote computers running a WinCC database server.
- Copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded.
- Updates itself through a peer-to-peer mechanism within a LAN.

- Exploits a total of four unpatched Microsoft vulnerabilities, two of which are previously mentioned vulnerabilities for self-replication and the other two are escalation of privilege vulnerabilities that have yet to be disclosed.
- Contacts a command and control server that allows the hacker to download and execute code, including up- dated versions.
- Contains a Windows rootkit that hide its binaries.
- Attempts to bypass security products.
- Fingerprints a specific industrial control system and modifies code on the Siemens PLCs to potentially sabo- tage the system.
- Hides modified code on PLCs, essentially a rootkit for PLCs.

Kilde: Symantec



Alt bliver nemmere, eksempelvis Firesheep add-on til Firefox  
<http://codebutler.github.com/firesheep/>

## Description

PDF Dissector is a GUI-based PDF malware analysis tool that was specifically built to assist PDF malware analysts.

To achieve this, PDF Dissector bundles everything malware analysts need for PDF malware analysis into a single tool. PDF Dissector has a PDF file format parser that was specifically built to detect malicious PDF files. It provides ways to quickly search through the elements of PDF files. It has a built-in JavaScript interpreter to execute malicious scripts and it has an Adobe Reader emulator to make sure that all features of malicious scripts are correctly executed.

The plugin architecture of PDF Dissector makes it possible to customize and automate PDF Dissector with plugins and scripts written in Java, Python, or Ruby.

Flash og PDF har (igen) haft ekstremt mange problemer i 2010, resulterer i kommercielle tools til analyse - 250EUR single user license!

PDF Dissector is a GUI-based PDF malware analysis tool that was specifically built to assist PDF malware analysts.

Kan vi undvære Flash og PDF?

Kilde: internet og <http://www.zynamics.com/dissector.html>

<http://blog.didierstevens.com/2010/09/26/free-malicious-pdf-analysis-e-book/>

Nogle ting bliver også sværere - buffer overflow protection

Teknologier som Address Space Layout Randomization ASLR

[http://en.wikipedia.org/wiki/Address\\_space\\_layout\\_randomization](http://en.wikipedia.org/wiki/Address_space_layout_randomization)

No eXecute NX-bit, dele af memory kan ikke afvikles som kode

Data Execution Prevention DEP

[http://en.wikipedia.org/wiki/Data\\_Execution\\_Prevention](http://en.wikipedia.org/wiki/Data_Execution_Prevention)

Modsvar: Return-oriented programming (ROP) is one of the buzzing advanced exploitation techniques these days to bypass NX, ASLR - byg exploits med stumper af eksisterende kode og stakken

Kilder: diverse præsentationer fra BlackHat

<http://www.blackhat.com/html/bh-us-10/bh-us-10-archives.html>

<https://media.blackhat.com/bh-us-10/presentations/Zovi/BlackHat-USA-2010-DaiZovi-Return-Oriented.pdf>

Det bliver også sværere at analysere exploits, kræver ofte *memory forensics*  
eksempelvis <http://blog.mandiant.com/archives/1459>

Andre exploits kræver at man afvikler dem i virtuelle systemer for at kunne analysere dem

Hvad betyder cloud security?

Er data mere eller mindre sikre i skyen? Gælder det for alle?

Serverroom flooding <http://www.youtube.com/watch?v=t0gBReKskXQ>

Der er også sikkerhedsprodukter i skyen, log analyse, virusscan



Udfordringer:

10G Ethernet kommer, men hvad med IDS og IPS

10 Gbit Hardware Packet Filtering Using Commodity Network Adapters

[http://www.ntop.org/TNAPI\\_HwFiltering.html](http://www.ntop.org/TNAPI_HwFiltering.html) 8.000kr

Suricata, kan udnytte GPU - kom hurtigt igang

<http://openinfosecfoundation.org/index.php/download-suricata>

Napatech specialadaptere, kan sprede belastningen på flere CPU'er

<http://www.napatech.com/> - NB: dyrt 30kkr:-)



Problem: er IPv6 allerede indenfor murene?

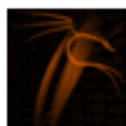
IPv6 catch up - feature parity, men er det nødvendigt?

NDPmon ligesom arpswatch?

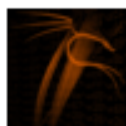
Hvad skal med i switche, a la DHCP snooping

**Kilder:** <http://ndpmon.sourceforge.net/>

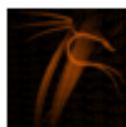
[http://en.wikipedia.org/wiki/DHCP\\_snooping](http://en.wikipedia.org/wiki/DHCP_snooping)



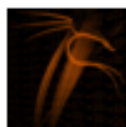
**exploitdb** [webapps] – BPAffiliate Affiliate Tracking  
Authentication Bypass Vulnerability: <http://bit.ly/9LOC3K>  
about 5 hours ago via twitterfeed



**exploitdb** [webapps] – BPDIRECTORY Business Directory  
Authentication Bypass Vulnerability: <http://bit.ly/c4TeLz>  
about 5 hours ago via twitterfeed



**exploitdb** [webapps] – BPCONFERENCEREPORTING Web Reporting  
Authentication Bypass Vulnerability: <http://bit.ly/cM61AK>  
about 5 hours ago via twitterfeed



**exploitdb** [webapps] – BPREALESTATE Real Estate  
Authentication Bypass Vulnerability: <http://bit.ly/bYx2aY>  
about 5 hours ago via twitterfeed



**sans\_isc** [Diary] Mac OS X Server v10.6.5 (10H575) Security  
Update: <http://support.apple.com/kb/HT4452>, (Tue, Nov  
16th): .... <http://bit.ly/azBrso>  
about 7 hours ago via twitterfeed

Nye kilder til information:

har twitter afløst RSS? NB: favoritsite <http://isc.sans.edu/index.html>

## Software releases:

- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Metasploit Express \$3.000 list price, Metasploit Pro \$15.000 list price!  
eller Metasploit Framework gratis på <http://www.metasploit.com/>
- Java GUI til Metasploit <http://pauldotcom.com/2010/07/metasploit-new-gui.html>
- Skipfish <http://code.google.com/p/skipfish/>
- BackTrack 4 R1 <http://www.backtrack-linux.org>
- Wireshark <http://www.wireshark.org/download.html>
- BlindElephant <http://blindelephant.sourceforge.net/>

NU snakker vi kode ... og høj kvalitet er mere sikker.

Hudson Extensible continuous integration server <http://hudson-ci.org/>

Sonar <http://www.sonarsource.org/>

Yasca can scan source code written in Java, C/C++, HTML, JavaScript, ASP, ColdFusion, PHP, COBOL, .NET, and other languages. Yasca can integrate easily with other tools

<http://www.scovetta.com/yasca.html>

**Automatisk analyse af software**

[http://samate.nist.gov/index.php/Source\\_Code\\_Security\\_Analyzers.html](http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html)

NB: du skal stadig tænke dig om :-)

Web applikationer er specielt udsatte

Glem ikke OWASP, der findes efterhånden vejledninger til alle sprog, eksempelvis:

Ruby On Rails Security Guide



<http://guides.rubyonrails.org/security.html>

men hvad med XML web services?

<http://questions.securitytube.net/questions/203/xml-web-services-penetration-testing>

DNSSEC nøgle(r)

( Bruger-id: DKHM1-DK )

Domænenavn ▾	Nøgle-ID	Algoritme	Hashingalgoritme	Hash
<input type="checkbox"/> net.dk	9880	RSASHA256	SHA-1	
<input type="checkbox"/> net.dk	9880	RSASHA256	SHA-256	

Slet nøgle

Opret nøgle

Tilbage til Selvbetjeningens forside

## DNSSEC - nu også i Danmark

Du kan sikre dit domæne med DNSSEC - wooohooo!

Det betyder en tillid til DNS som muliggør alskens spændende services, alle burde gøre det nu!

Kilde:

<https://www.dk-hostmaster.dk/english/tech-notes/dnssec/>

```
$ dig @ns1.gratisdns.dk +multi +dnssec hacking.dk
```

```
...
```

```
;; ANSWER SECTION:
```

```
hacking.dk.      1200  IN  A  109.74.200.101
```

```
hacking.dk.      1200  IN  RRSIG A 5 2 1200 20101213020721 (
                20101113020721 33825 hacking.dk.
                v/PaOCAQERqiAtTQ9D+GDxYkYgUp4jHaF53lfn6EfSJQ
                yZeJrmOHze89mildl1/KWacG/HmqEbnEcBrm/QT5w== )
```

Har du gjort det for dine domæner? Peter Makholm har gjort det for sit `hacking.dk`

Kilde:

<http://www.version2.dk/artikel/9921-kom-lad-os-lege-med-dnssec>



```
options
    recursion yes;
    dnssec-enable yes;
    dnssec-validation yes;
    allow-query 192.168.0.0/16; ;
;

// Find trust-anchor with the commando:
// dig +short @k.root-servers.net. dnskey . | grep ^257
managed-keys
    . initial-key 257 3 8 "=="[base64tekst]=="";
;
```

eller brug <http://censurfridns.dk/>

**Kilde:** <https://www.dk-hostmaster.dk/english/tech-notes/dnssec/>

The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere?

The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere?

Google kan:

<http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html>

Men alt for få gør det

Hvilke versioner af SSL/TLS?

Secure Sockets Layer - Transport Layer Security

SSL Survey HTTP Rating Guide version 1.0 (5 July 2010) Copyright © 2010 Qualys  
SSL Labs ([www.ssllabs.com](http://www.ssllabs.com))

<https://media.blackhat.com/bh-us-10/whitepapers/Ristic/BlackHat-USA-2010-Ristic-Qualys-SSL-Survey.pdf>

Hvilke versioner af SSL/TLS?

Secure Sockets Layer - Transport Layer Security

SSL Survey HTTP Rating Guide version 1.0 (5 July 2010) Copyright © 2010 Qualys  
SSL Labs ([www.ssllabs.com](http://www.ssllabs.com))

<https://media.blackhat.com/bh-us-10/whitepapers/Ristic/BlackHat-USA-2010-Ristic-Qualys-SSL-Survey.pdf>

Næste spørgsmål er så hvilke rod-certifikater man stoler på ...

Vi ser en trend mod GPU baserede hackerværktøjer og folk bygger små clustersystemer

Nu kan man dog også købe GPU i Amazon EC2

Så kunne man vel leje sådan en og finde et hackerværktøj, men er det ikke svært?

<http://stacksmashing.net/2010/11/15/cracking-in-the-cloud-amazons->

Hmmm, jeg har vist en WPA capture som jeg gerne ville knække ...

Hvad skal I bruge tiden på i juleferien

Gode gamle kvaliteter som tcpdump og Wireshark, går aldrig af mode:

[http://acs.lbl.gov/~jason/tcpdump\\_advanced\\_filters.txt](http://acs.lbl.gov/~jason/tcpdump_advanced_filters.txt)

Fjern allerede nu de ting som du ved er dårlige, du ved dem fra 2006 ...

Jeg har selv hjulpet en kunde med at gøre to Windows 2000 servere overflødige i år.

Tutorials <http://www.backtrack-linux.org/tutorials/>

Det vigtige her er at forstå at mange kan lære hacking - og mange gør!

Hvad skal I bruge tiden på at planlægge og teste

Patch management og automatiseret sikkerhedstest

Start evt. med NeXpose Community Edition og Metasploit fra BackTrack

Opdater IT-sikkerhedspolitikken hvert år - det er snart nytår :-)

Gå SANS Internet Storm Center Cyber Security Awareness month posts igennem

<http://isc.sans.edu/diaryarchive.html?year=2010&month=10>

Gør dig selv overflødig, du skal ikke være en flaskehals



Kender I NIST special publications?

SP 800-125 July 7, 2010 DRAFT Guide to Security for Full Virtualization Technologies

SP 800-119 Feb. 22, 2010 DRAFT Guidelines for the Secure Deployment of IPv6

SP 800-118 Apr. 21, 2009 DRAFT Guide to Enterprise Password Management

SP 800-97 Feb 2007 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

SP 800-58 Jan 2005 Security Considerations for Voice Over IP Systems

SP 800-54 Jul 2007 Border Gateway Protocol Security

SP 800-41 Rev. 1 Sept. 2009 Guidelines on Firewalls and Firewall Policy

M.fl.

<http://csrc.nist.gov/publications/PubsSPs.html>

Næste CitySec-aften er onsdag d. 1. december kl 19 på Plenum, ved Sankt Hans Torv (der hvor vi har været de sidste par gange).

Næste OWASP-møde afholdes TORSDAG d. 9. kl 17 hos PwC, Strandvejen 44, Hellerup og vil være en helaftensworkshop i fuzzing afholdt af Knud Erik Højgaard fra nSense.

<http://www.owasp.org/index.php/Denmark>



PROSA afholdt fredag 17. september - til lørdag 18. september Capture the Flag

Distribueret CTF med 6 hold og arrangørerne i Aalborg

Sjovt og lærerigt - gentages helt sikkert

Kilde: <http://prosa-ctf.the-playground.dk/>

Man snakker meget om: Internet of Things

Diverse nye enheder som Smartphones, iPads - de er ikke automatisk mere sikre som standard

Nogle tendenser:

- Fortsat konvergens i netværk - flere services lægges sammen på færre "ledninger" eksempelvis IP telefoni sammen med data eller administrative netværk til styring af virtualisering
- Always ON - men hvorfra?
- Højt teknisk niveau i information omkring hacking - sofistikerede angreb
- Gamle troværdige algoritmer og produkter rystes jævnlgt af hidtil ukendte sårbarheder
- Gamle kendte sårbarheder virker stadig - IE6 skal dø, men findes stadig MANGE steder
- Virksomheder har budget til informationssikkerhed - brug det!
- Voice over IP - er udbredt, men ofte er sikkerheden glemt. Brug VLANs!

Det er nu 100% nødvendigt at du kender VLAN terminologier og kan konfigurere det på switche - grundet VoIP, sikkerhed, management m.v.

A VLAN has the same attributes as a physical LAN

Private VLAN hvor enkelte porte ikke kan snakke sammen, men godt kan sende til en firewall/router subnets

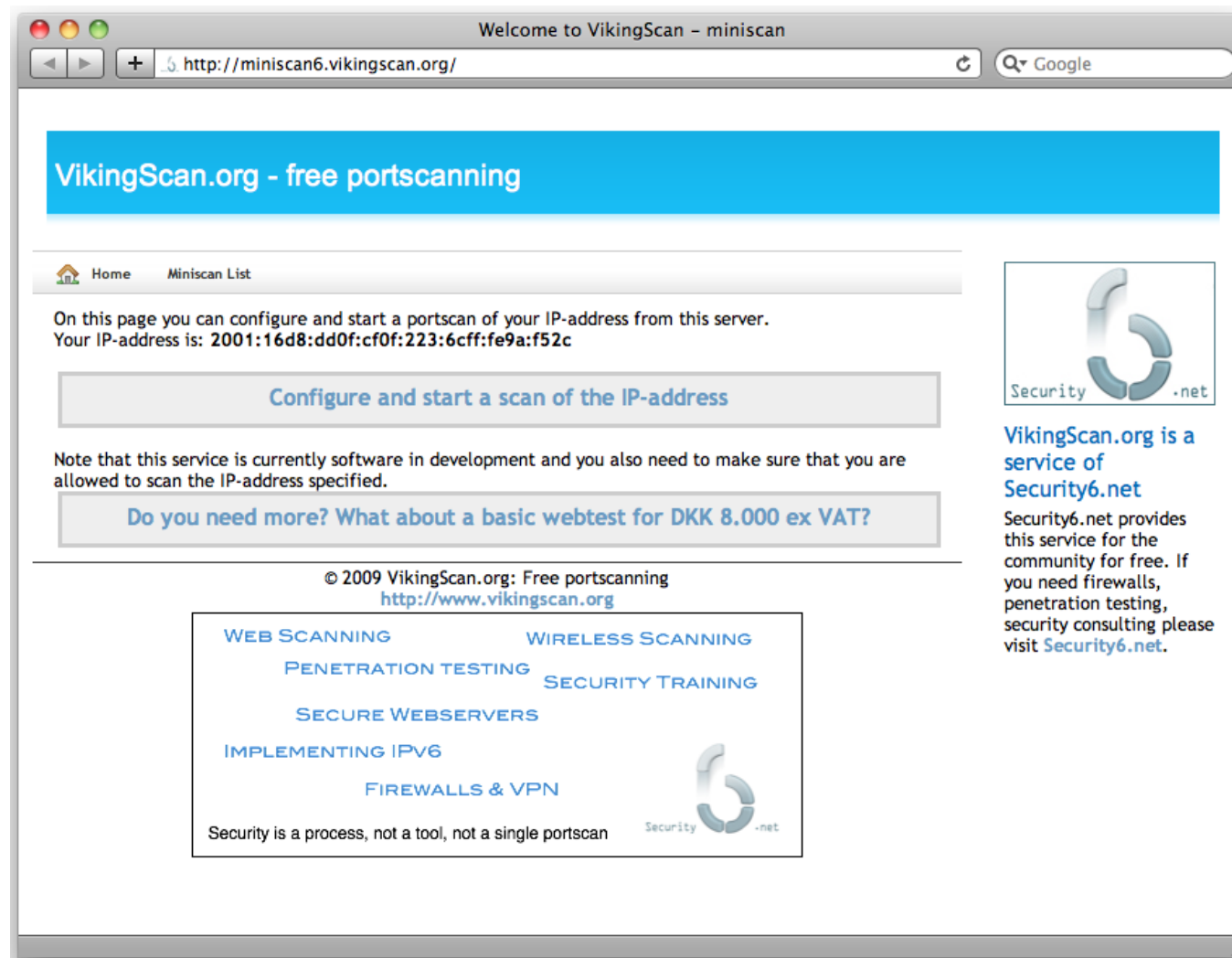
**Kilde:** [http://en.wikipedia.org/wiki/Virtual\\_LAN](http://en.wikipedia.org/wiki/Virtual_LAN)  
[http://en.wikipedia.org/wiki/IEEE\\_802.1Q](http://en.wikipedia.org/wiki/IEEE_802.1Q)  
[http://en.wikipedia.org/wiki/Private\\_VLAN](http://en.wikipedia.org/wiki/Private_VLAN)

Hvad glemte jeg? Kom med dine favoritter :-)

Henrik Lund Kramshøj  
hlk@solidonetworks.com

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email







- Henrik Lund Kramshøj, freelance IT-security consultant
- Email: [hlik@solidonetworks.com](mailto:hlik@solidonetworks.com)      Mobile: +45 2026 6000
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- CISSP and CEH certified
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks Aps