Velkommen til

Tendenser i sikkerhed

March 2011

Henrik Lund Kramshøj
hlk@solidonetworks.com

`http://www.solidonetworks.com`

Slides are available as PDF

Formål

Give en update på udviklingen indenfor internetsikkerhed og sikkerhedstrusler

Give input til hvad I skal fokusere på

Jeg vil forsøge at gennemgå ting fra 2011

En potpourri af sikkerhedsemner - inspiration

Feedback og kommentarer modtages, dialog ☺

Planen idag

Kl 17-21

Mindre foredrag mere snak

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

DDoS udviklingen, januar 2010 rapporten

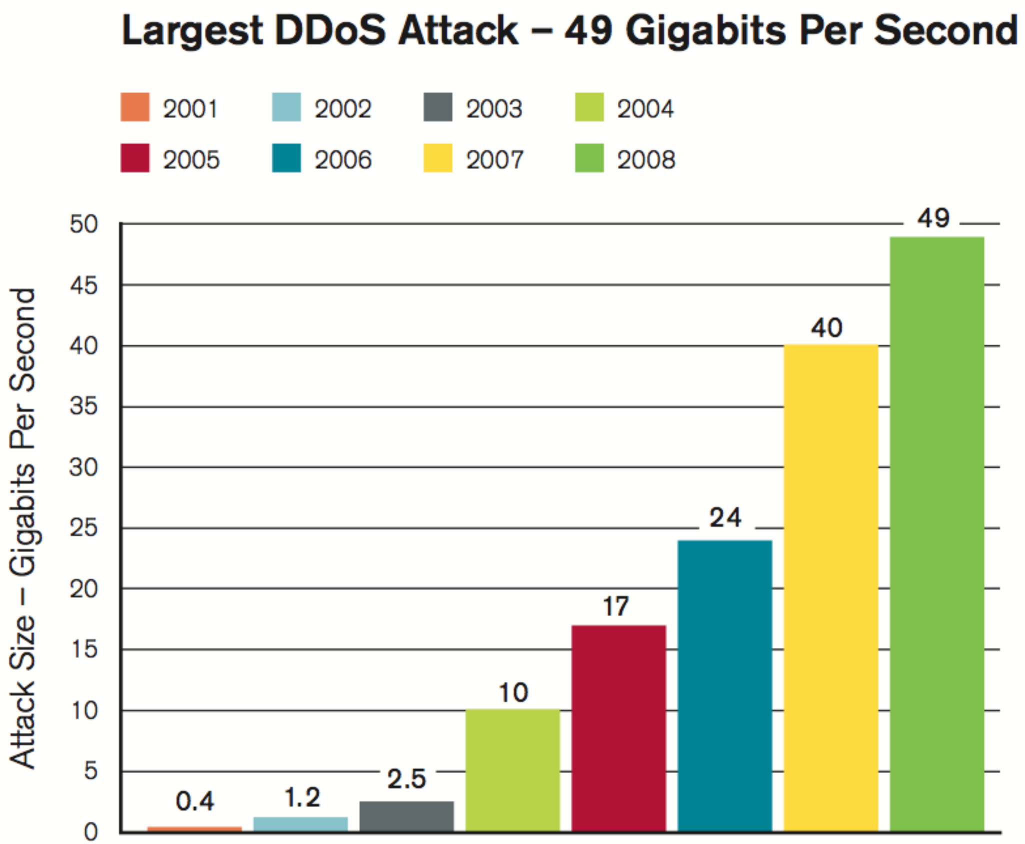


***Figure 1:** Largest DDoS Attack – 49 Gigabits Per Second*

Source: Arbor Networks, Inc.

Kilde: `http://www.arbornetworks.com/report` 2009 rapporten

DDoS udviklingen, februar 2011

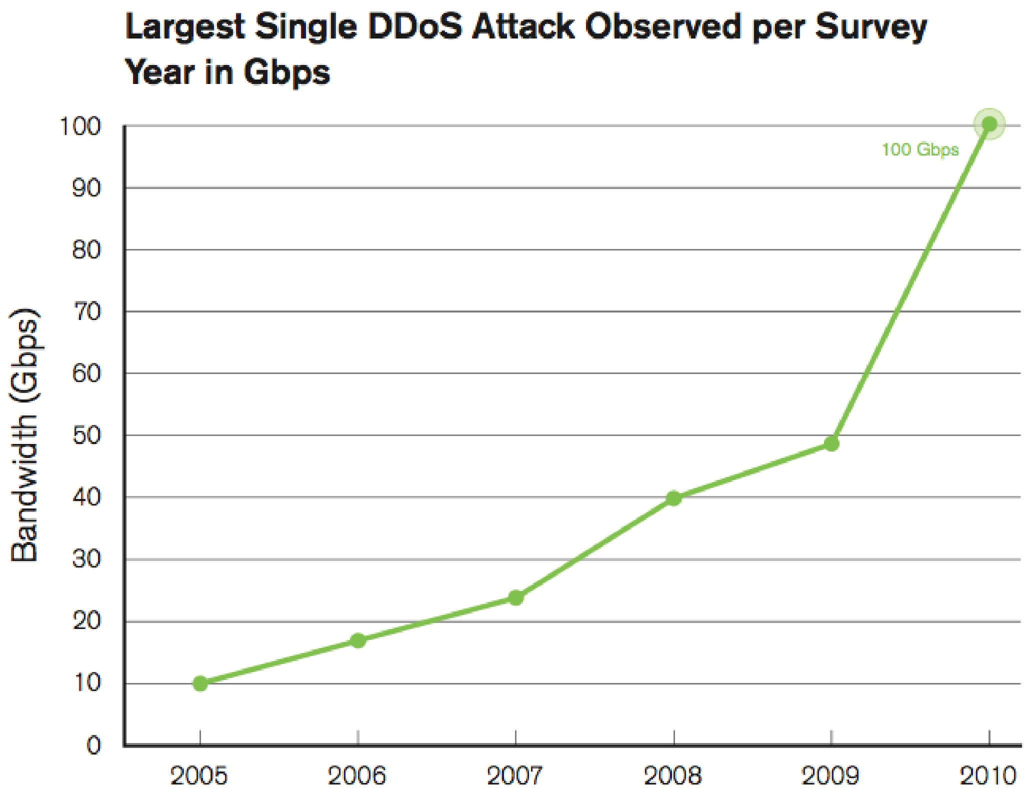


Figure 1

Source: Arbor Networks, Inc.

Kilde: `http://www.arbornetworks.com/report` 2010 rapporten

Worldwide Infrastructure Security Report, 2010 Report

Key finding:
Application-Layer DDoS Attacks Are Increasing in Sophistication and Operational Impact
IDC and mobile/fixed wireless operators in particular are reporting significant outages, increased OPEX, customer churn and revenue loss due to application-layer DDoS attacks. These attacks are targeting both their customers and their own ancillary supporting services, such as DNS, Web portals, etc.
...
Conclusions
We further note that the fastest-growing category of ISPs-mobile and fixed wireless broadband operators-are also the least-prepared organizations in terms of network visibility, network control, and overall ability to successfully defend themselves and their customers against attack. These operators are balancing an overwhelming array of threats with conflicting budget pressures and business objectives.

Mere komplekse trusler, betyder det flere firewall?

Key findings

- Application-Layer DDoS Attacks Are Increasing in Sophistication and Operational Impact
- Mobile/Fixed Wireless Operators Are Facing Serious Challenges to Maintaining Availability in the Face of Attacks
- Firewalls and IPS Devices Are Falling Short on DDoS Protection
- DNS Has Broadly Emerged as an Attack Target and Enabler
- Lack of Visibility into and Control over IPv6 Traffic Is a Significant Challenge
- Chronic Underfunding of Operational Security Teams
- Operators Continue to Express Low Confidence in the Efficacy of Law Enforcement
- Operators Have Little Confidence in Government Efforts to Protect Critical Infrastructure

Kilde: `http://www.arbornetworks.com/report` februar 2011

Fremtiden - er success en risiko

The Mobile Network in 2010 and 2011
Global mobile data traffic grew 2.6-fold in 2010, nearly tripling for the third year in a row. The 2010 mobile data traffic growth rate was higher than anticipated. Last year's forecast projected that the growth rate would be 149 percent. This year's estimate is that global mobile data traffic grew 159 percent in 2010.
...
Last year's mobile data traffic was three times the size of the entire global Internet in 2000. Global mobile data traffic in 2010 (237 petabytes per month) was over three times greater than the total global Internet traffic in 2000 (75 petabytes per month).
...
There will be 788 million mobile-only Internet users by 2015. The mobile-only Internet population will grow 56-fold from 14 million at the end of 2010 to 788 million by the end of 2015.

Kilde: *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010 - 2015*

HBGary - Anatomy of a Data Breach

> HBGary's website has been defaced and its CEO Aaron Barr has had his social media accounts hijacked and his personal information leaked online - all in retribution for his claims that he had infiltrated Anonymous, the loosely-affiliated collective of hacktivists.
>
> HBGary founder Greg Hoglund has told Krebs on Security that Anonymous ”didn't just pick on any company, but we try to protect the US government from hackers. They couldn't have chosen a worse company to pick on.”For its part, Anonymous contends that HBGary couldn't have picked a worse group to pick on.

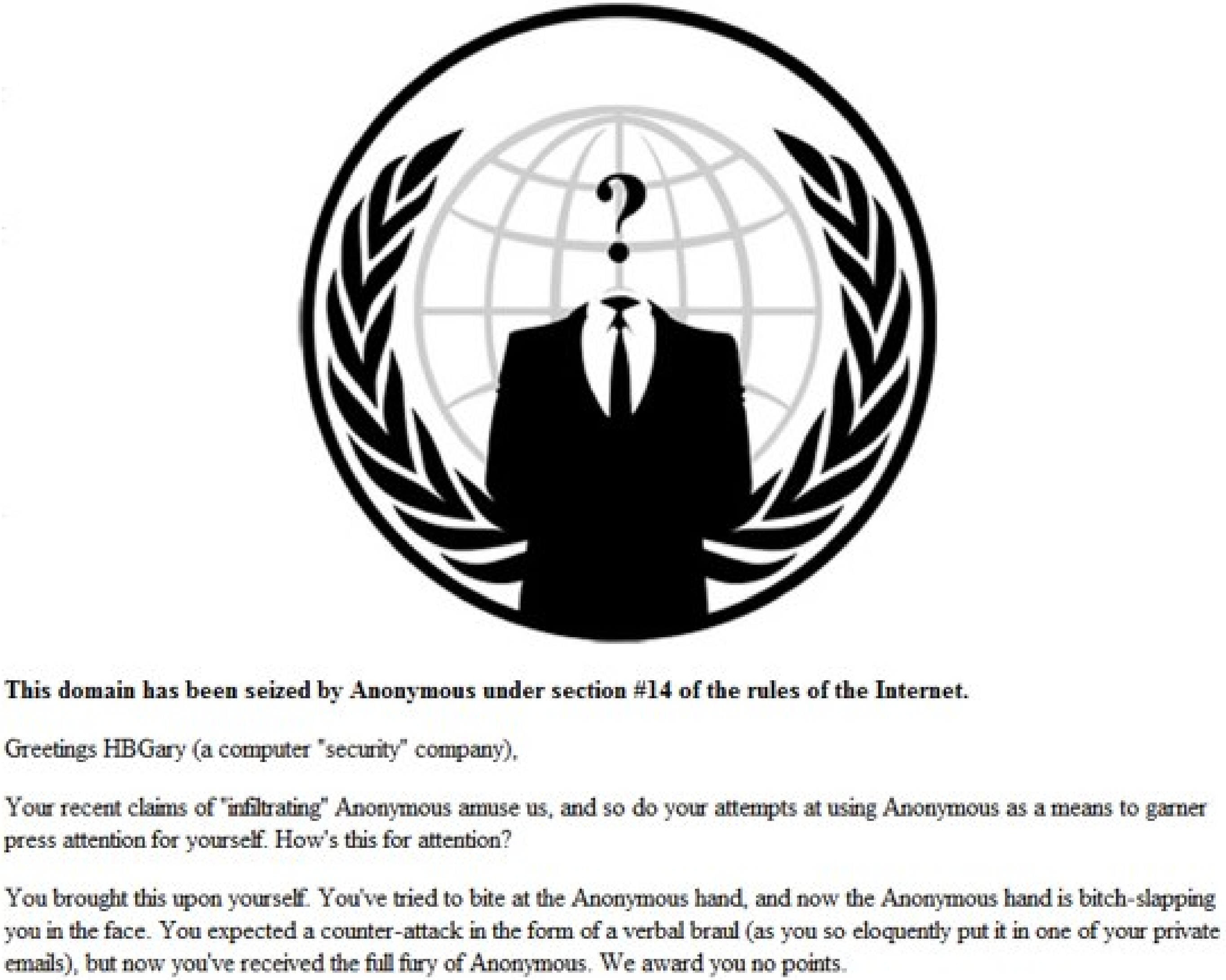
Emails kan hentes/læses på nettet

Social enginering og adgang via firewall

Kilder: mange nyhedssites på internet

`http://www.readwriteweb.com/archives/anonymous_hacks_security_company_hbgary_dumps_5000.php`

Defacement



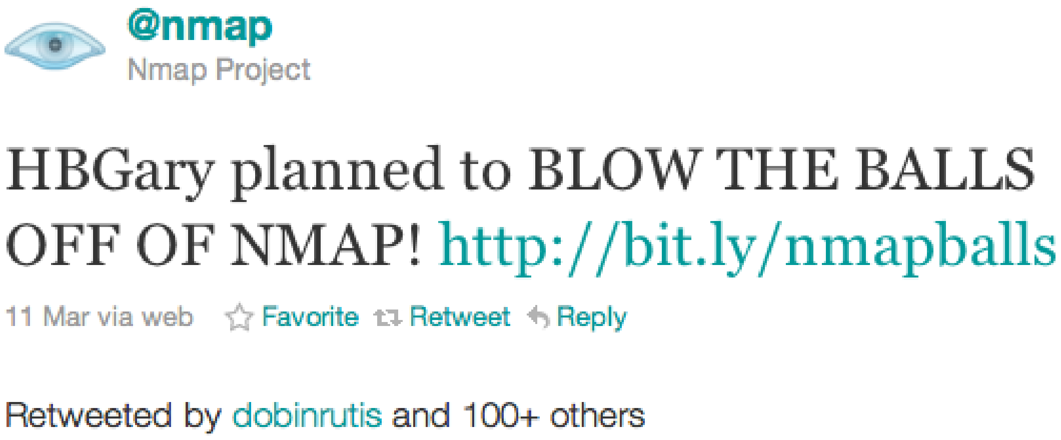
This domain has been seized by Anonymous under section #14 of the rules of the Internet.

Greetings HBGary (a computer "security" company),

Your recent claims of "infiltrating" Anonymous amuse us, and so do your attempts at using Anonymous as a means to garner press attention for yourself. How's this for attention?

You brought this upon yourself. You've tried to bite at the Anonymous hand, and now the Anonymous hand is bitch-slapping you in the face. You expected a counter-attack in the form of a verbal braul (as you so eloquently put it in one of your private emails), but now you've received the full fury of Anonymous. We award you no points.

HBGary - Nmap balls



@nmap
Nmap Project

HBGary planned to BLOW THE BALLS OFF OF NMAP! http://bit.ly/nmapballs

11 Mar via web

Retweeted by dobinrutis and 100+ others

`http://hbgary.anonleaks.ch/greg_hbgary_com/13401.html`

Kilder: Nmap tweet og mailinglist

Hacking rammer alle

Der er mange pointer at lære fra HBGary

Social Engineering rockz! Uddannelse!

Alle er et mål, evt. som springbrædt ind til andre

Anonymous er en flok forkælede møgunger? helte? egoer? løst knyttet gruppe, tæt knyttet gruppe?

Hacktivism er okay, bare det rammer Scientology?

... flere pointer?

Hacking er ikke cool og koster mange resourcer!

RSA - Anatomy of a Data Breach - 1

Open Letter to RSA Customers
Arthur W. Coviello, Jr.
Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Note: det er ikke RSA **algoritmen** men firmaet **RSA**

Kilder:
`http://www.rsa.com/node.aspx?id=3872`

RSA - Anatomy of a Data Breach - 2

> Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.

Aka SQL injections?

Kilder:

`http://www.rsa.com/node.aspx?id=3872`

RSA - Anatomy of a Data Breach - outcome

> We have no evidence that customer security related to other RSA products has been similarly impacted. We are also confident that no other EMC products were impacted by this attack. It is important to note that we do not believe that either customer or employee personally identifiable information was compromised as a result of this incident.

Kan vi stole på vores SecureID tokens nu?
- og hvad med NemID?

Kilder:

`http://www.rsa.com/node.aspx?id=3872`

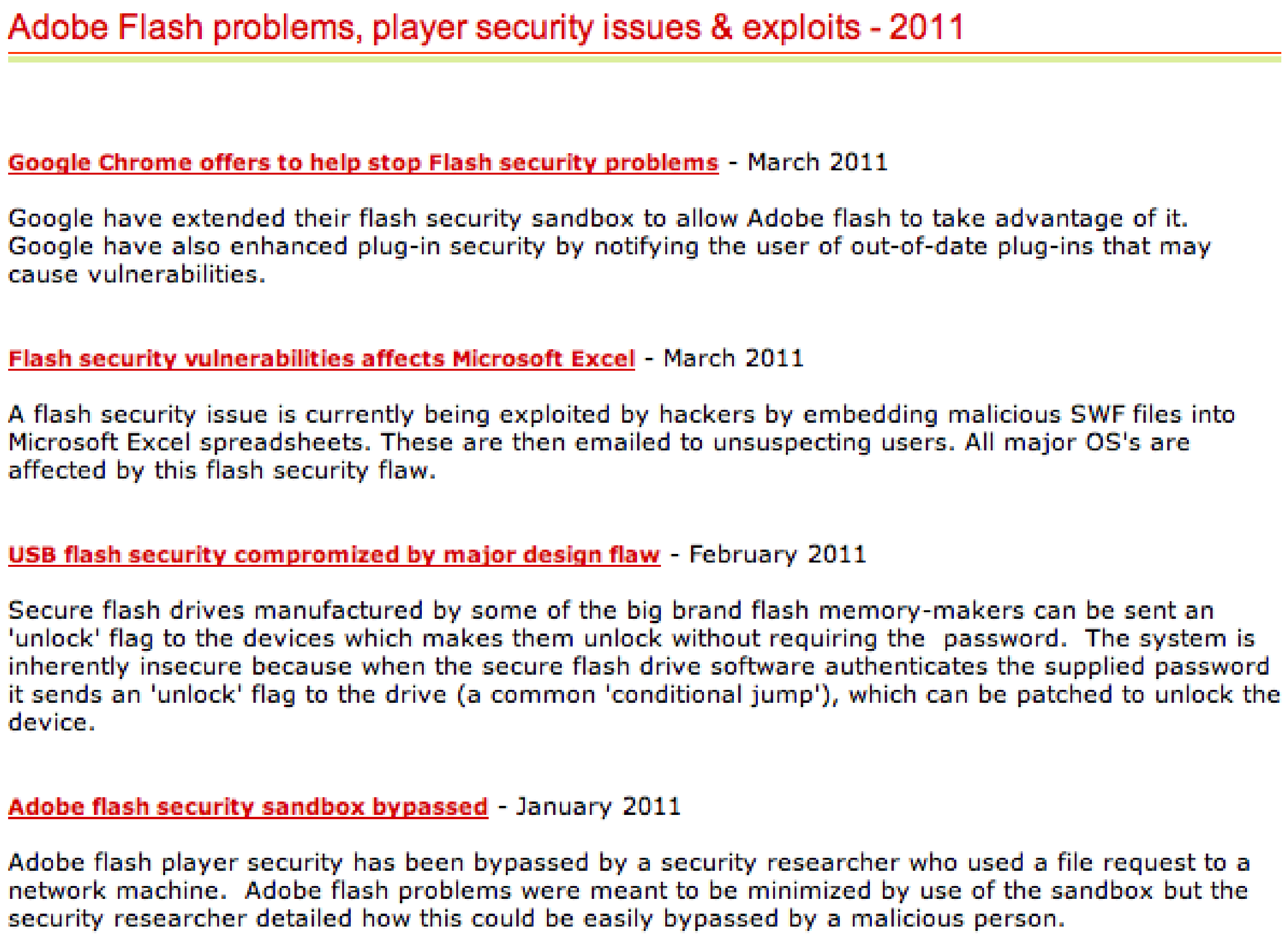
`http://www.schneier.com/blog/archives/2011/03/rsa_security_in.html`

`http://computersweden.idg.se/2.2683/1.374749/rsa-hacket-hotar-25-000-foretag`

`http://securosis.com/blog/rsa-breached-secureid-affected`

`http://www.cs.columbia.edu/~smb/blog//2011-03/2011-03-18.html`

Flashback



Adobe Flash problems, player security issues & exploits - 2011

Google Chrome offers to help stop Flash security problems - March 2011

Google have extended their flash security sandbox to allow Adobe flash to take advantage of it. Google have also enhanced plug-in security by notifying the user of out-of-date plug-ins that may cause vulnerabilities.

Flash security vulnerabilities affects Microsoft Excel - March 2011

A flash security issue is currently being exploited by hackers by embedding malicious SWF files into Microsoft Excel spreadsheets. These are then emailed to unsuspecting users. All major OS's are affected by this flash security flaw.

USB flash security compromized by major design flaw - February 2011

Secure flash drives manufactured by some of the big brand flash memory-makers can be sent an 'unlock' flag to the devices which makes them unlock without requiring the password. The system is inherently insecure because when the secure flash drive software authenticates the supplied password it sends an 'unlock' flag to the drive (a common 'conditional jump'), which can be patched to unlock the device.

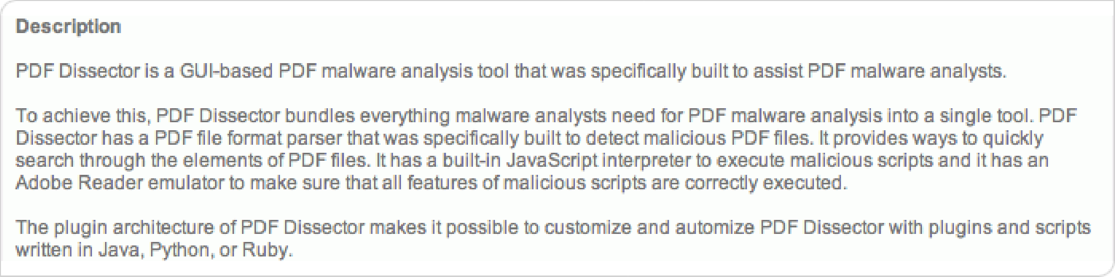
Adobe flash security sandbox bypassed - January 2011

Adobe flash player security has been bypassed by a security researcher who used a file request to a network machine. Adobe flash problems were meant to be minimized by use of the sandbox but the security researcher detailed how this could be easily bypassed by a malicious person.

Kilde: `http://www.locklizard.com/adobe-flash-security.htm`

Client side: Flash, PDF, Facebook

Gentagelse fra sidst



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 automize 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/`

Flash blockers

Safari `http://clicktoflash.com/`

Firefox Extension Flashblock

Chrome extension called FlashBlock

Internet Explorer 8: IE has the Flash block functionality built-in so you don’t need to install any additional plugins to be able to block flash on IE 8.

FlashBlock for Opera 9 - bruger nogen Opera mere?

FlashBlockere til iPad? iPhone? Android? - hvorfor er det ikke default?

IPv6 is coming, fortsat fra sidst

An important consideration is that IPv6 is quite likely to be already running on the enterprise network, whether that implementation was planned or not. Some important characteristics of IPv6 include:

- IPv6 has a mechanism to automatically assign addresses so that end systems can easily establish communications.
- IPv6 has several mechanisms available to ease the integration of the protocol into the network.
- Automatic tunneling mechanisms can take advantage of the underlying IPv4 network and connect it to the IPv6 Internet.

Kilde:

`http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-629391.html`

Implications

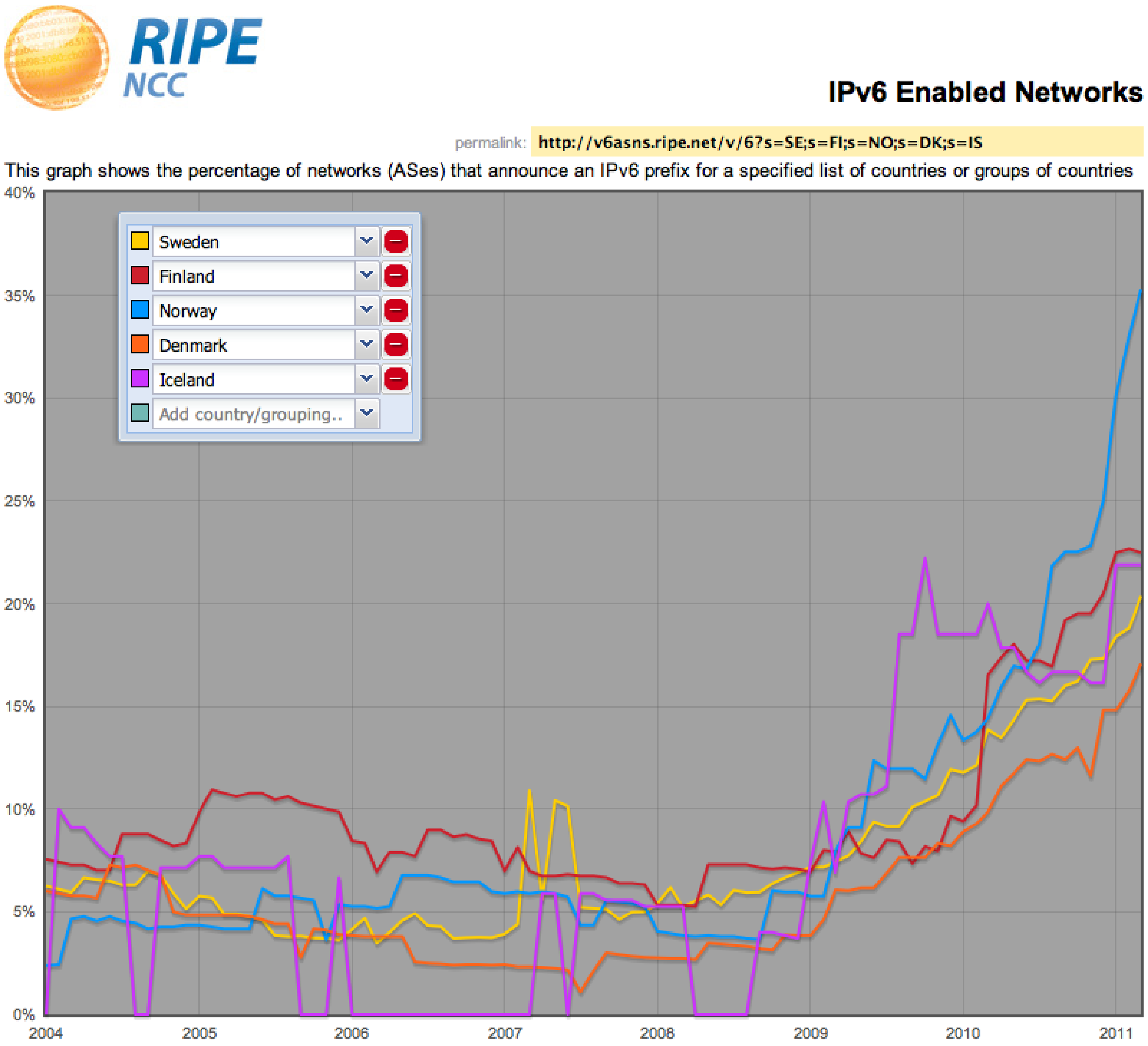
For an IPv4 enterprise network, the existence of an IPv6 overlay network has several of implications:

- The IPv4 firewalls can be bypassed by the IPv6 traffic, and leave the security door wide open.
- Intrusion detection mechanisms not expecting IPv6 traffic may be confused and allow intrusion
- In some cases (for example, with the IPv6 transition technology known as 6to4), an internal PC can communicate directly with another internal PC and evade all intrusion protection and detection systems (IPS/IDS). Botnet command and control channels are known to use these kind of tunnels.

Kilde:

`http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-629391.html`

IPv6 i Norden



IPv6 Enabled Networks

permalink: http://v6asns.ripe.net/v/6?s=SE;s=FI;s=NO;s=DK;s=IS

This graph shows the percentage of networks (ASes) that announce an IPv6 prefix for a specified list of countries or groups of countries

- 🟨 Sweden
- 🟥 Finland
- 🟦 Norway
- 🟧 Denmark
- 🟪 Iceland
- Add country/grouping..

Hackersoftware og andre tools

Software and tool releases:

- Nmap 5.50: Now with Gopher protocol support! Januar 2011`nmap.org`
- Metasploit Framework 3.6 gratis på `http://www.metasploit.com/`
- BackTrack 5 til Maj?`http://www.backtrack-linux.org`
- Suricata 1.1 beta 1, December 2010 `http://www.openinfosecfoundation.org/`
- `https://github.com/chrislee35/team-cymru` queries Team Cymru's ASN, Malware, and FullBogon services
- `https://www.c0decafe.de/loki.html` new Loki - ikke alt er layer 7

Nmap 5.50

> I'm so excited about NSE that I made it the topic of my presentation with David Fifield last summer at Defcon and the Black Hat Briefings. You can watch the video at http://nmap.org/presentations/.
>
> Since Nmap 5.21, we've more then doubled the number of NSE scripts to 177 and NSE libraries jumped from 30 to 54. They're all detailed at http://nmap.org/nsedoc/.
>
> Meanwhile, we added 636 OS fingerprints and 1,037 version detection signatures to Nmap since 5.21, bringing the totals to 2,982 and 7,319, respectively. No other tool comes close.

Kilde: Januar 2011 `http://nmap.org`

Nping check TCP socket connection

```
hlk@pumba:nmap-5.51$ nping -6  www.solidonetworks.com

Starting Nping 0.5.51 ( http://nmap.org/nping ) at 2011-03-04 10:18 CET
SENT (0.0061s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (0.0224s) Handshake with 2a02:9d0:10::9:80 completed
SENT (1.0213s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (1.0376s) Handshake with 2a02:9d0:10::9:80 completed
SENT (2.0313s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (2.0476s) Handshake with 2a02:9d0:10::9:80 completed
SENT (3.0413s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (3.0576s) Handshake with 2a02:9d0:10::9:80 completed
SENT (4.0513s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (4.0678s) Handshake with 2a02:9d0:10::9:80 completed

Max rtt: 16.402ms | Min rtt: 16.249ms | Avg rtt: 16.318ms
TCP connection attempts: 5 | Successful connections: 5 | Failed: 0 (0.00%)
Tx time: 4.04653s | Tx bytes/s: 98.85 | Tx pkts/s: 1.24
Rx time: 4.06292s | Rx bytes/s: 49.23 | Rx pkts/s: 1.23
Nping done: 1 IP address pinged in 4.07 seconds
```

Metasploit 3.6

2011-03-07: Metasploit 3.6.0 Released! We are excited to announce that version 3.6.0 of Metasploit Pro, Metasploit now ships with 648 exploit modules, 342 auxiliary modules, and 23 post modules.

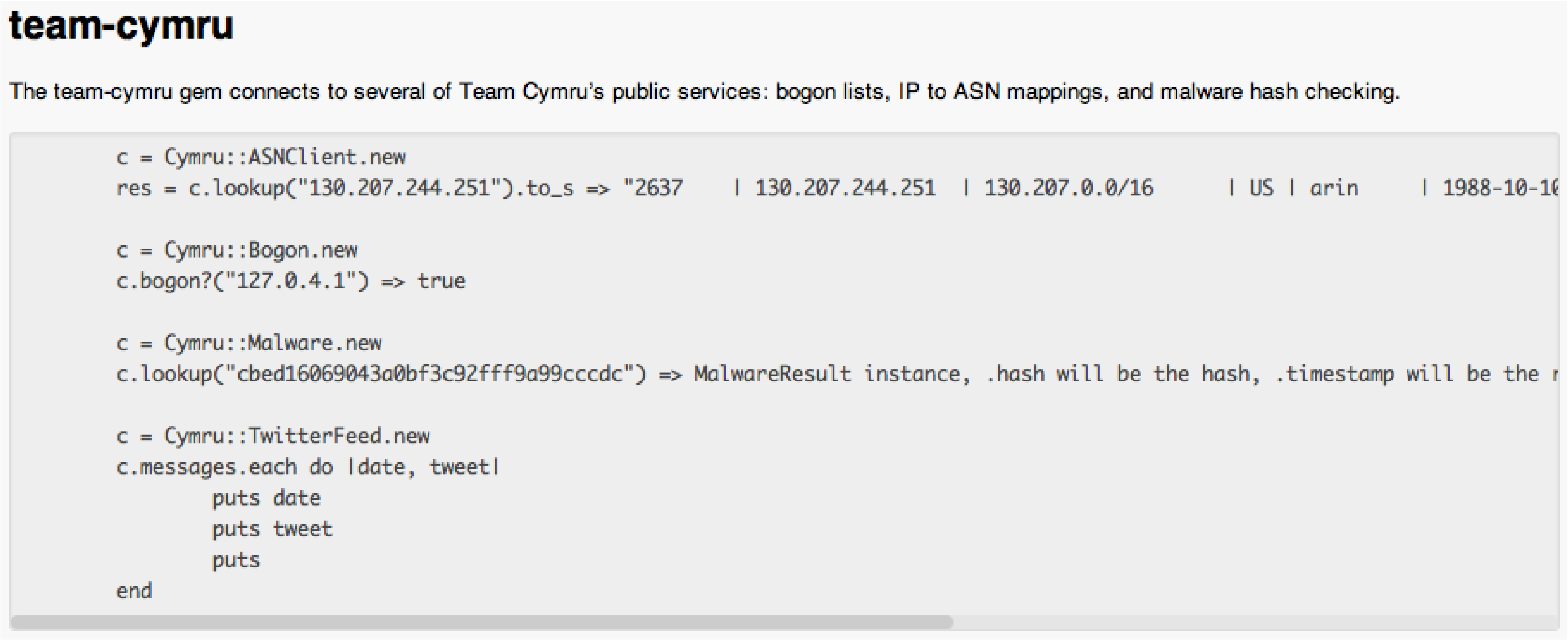
8 new exploits and 12 auxiliary modules have been added since the last point release.

Husk også Armitage GUI til Metasploit `http://www.fastandeasyhacking.com/`

Kilde:

`http://www.metasploit.com/redmine/projects/framework/wiki/Release_Notes_360`

Team Cymru



team-cymru

The team-cymru gem connects to several of Team Cymru's public services: bogon lists, IP to ASN mappings, and malware hash checking.

```
        c = Cymru::ASNClient.new
        res = c.lookup("130.207.244.251").to_s => "2637     | 130.207.244.251  | 130.207.0.0/16       | US | arin      | 1988-10-1

        c = Cymru::Bogon.new
        c.bogon?("127.0.4.1") => true

        c = Cymru::Malware.new
        c.lookup("cbed16069043a0bf3c92fff9a99cccdc") => MalwareResult instance, .hash will be the hash, .timestamp will be the

        c = Cymru::TwitterFeed.new
        c.messages.each do |date, tweet|
                puts date
                puts tweet
                puts
        end
```

Kilde: `https://github.com/chrislee35/team-cymru`

New Loki - ikke alt er layer 7

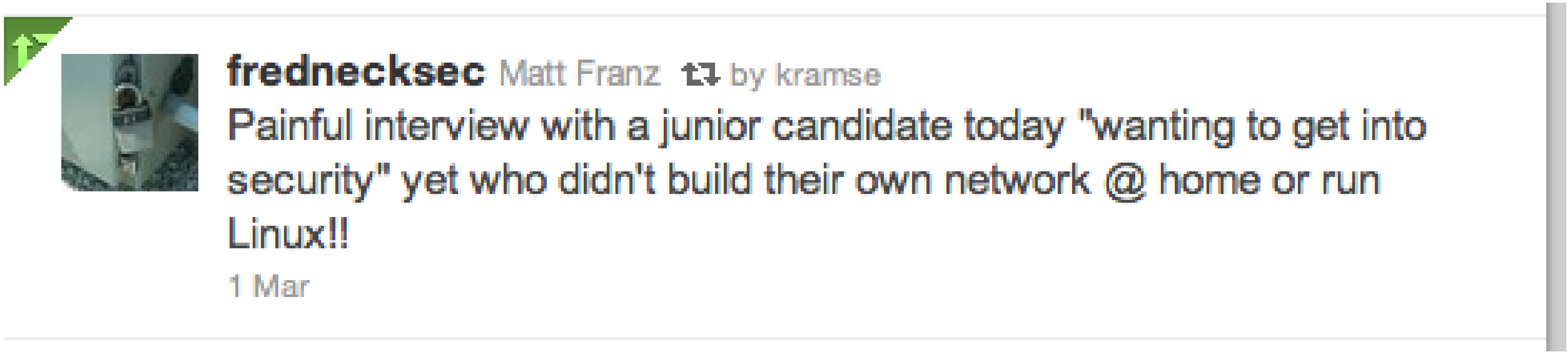
> At the beginning LOKI was made to combine some stand-alone **command line tools**, like the `bgp_cli`, the `ospf_cli` or the `ldp_cli` and to give them a **user friendly, graphical interface**. In the meantime LOKI is more than just the combination of the single tools, it gave its modules the opportunity to base upon each other (like **combining ARP-spoofing from the ARP module with some man-in-the-middle actions, rewriting MPLS-labels for example)** and even inter operate with each other. (Fremhævning: HLK)

`https://www.c0decafe.de/loki.html` Loki

`http://www.packetstan.com/2011/02/running-loki-on-backtrack-4-r2.html`

”Yersinia is a network tool designed to take advantage of some weakeness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.”`http://www.yersinia.net/`

it’s a Unix system, I know this



fredneckse Matt Franz ⇄ by kramse
Painful interview with a junior candidate today "wanting to get into security" yet who didn't build their own network @ home or run Linux!!
1 Mar

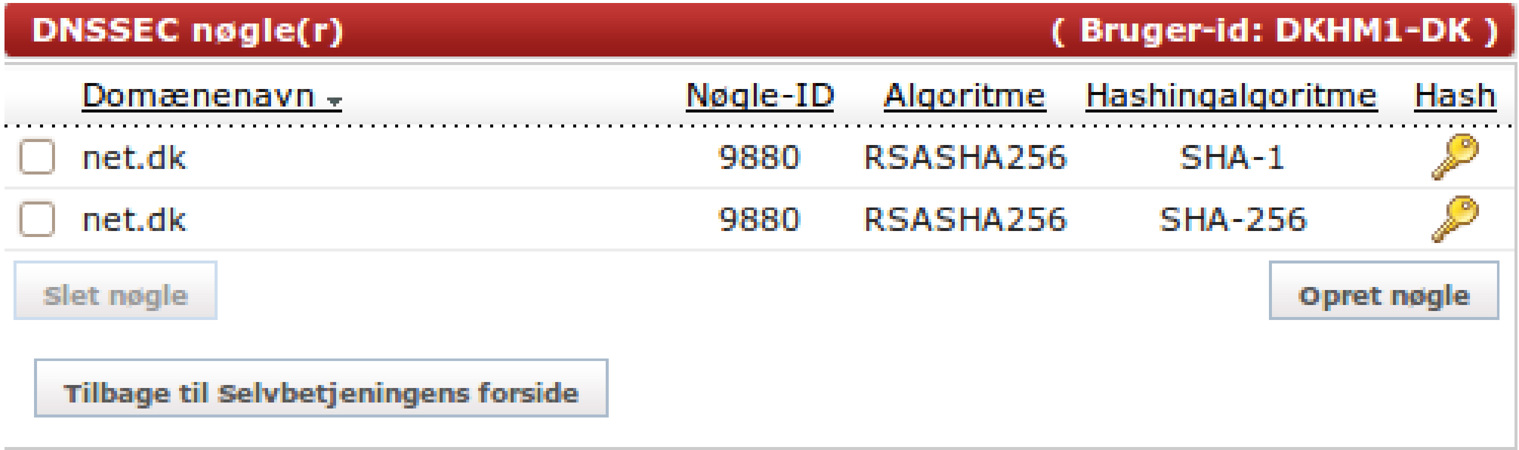
Skal du igang med sikkerhed?

Installer et netværk, evt. bare en VMware, Virtualbox, Parallels, Xen, GNS3, ...

Brug BackTrack, se evt. youtube videoer om programmerne

Quote fra Jurassic Park `http://www.youtube.com/watch?v=dFUlAQZB9Ng`

DNSSEC



DNSSEC nøgle(r) (Bruger-id: DKHM1-DK)

	Domænenavn	Nøgle-ID	Algoritme	Hashingalgoritme	Hash
□	net.dk	9880	RSASHA256	SHA-1	🔑
□	net.dk	9880	RSASHA256	SHA-256	🔑

DNSSEC - nu også i Danmark

Du kan sikre dit domæne med DNSSEC - wooohooo!

Det betyder en tillid til DNS som muliggør alskens services.

Kilde:
`https://www.dk-hostmaster.dk/english/tech-notes/dnssec/`

SSL

> 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

▮

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

Internet sniffing by government

Ægypten, Sudan, Tunesien, ...

Den der kontrollerer ISPerne kontrollerer trafikken

Facebook revolutionerne

Blokering er umulig, men det forsøges

Spredning af falsk information

Kilde: `http://irevolution.net/2011/02/10/facebook-for-repressive-reg`

Fokus i nærmeste fremtid

Fjern allerede nu de ting som du ved er dårlige, du ved dem fra 2010 ...
Jeg arbejder stadig på at få kunderoutere over på SSH som management

Sørg for at indsamle config fra enheder, hvis nu en switch stack skulle crashe ...

Sørg for at have adgang til de rigtige ressourcer hos dine leverandører og partnere

Kommuniker sikkert - brug HTTPS til alt
- der findes flere gode add-ons/extensions som tvinger SSL

Fokus på længere sigt

Hvad skal I bruge tiden på - planlægge fremtiden

Har du beredskab til sommeren, se på ressourcer - er der fyret medarbejdere

Kast ansvar fra dig? Har du reelt ressourcer til at udføre arbejdet forsvarligt

Afdække afhængigheder - hvem er din organisation afhængige af - CSC vs PROSA?!

Configuration Management, Patch management og automatiseret sikkerhedstest
Start evt. med RANCID, NeXpose Community Edition og Metasploit fra BackTrack

Managed security giver mening!

Trenden går mod komplekse infrastrukturer, mere af den og højere krav

Kunderne vil have høj oppetid, fordi internet teknologier er forretningskritiske

Kunder der ikke betragter netværket som forretningskritisk lider tab

Kunderne har ikke *nok* netværk til at have fuldtidsansatte

Hvad skal der til for at tilbyde Managed Security Services

Typiske Managed Security Services

> In computing, managed security services (MSS) are network security services that have been outsourced to a service provider.

Kilde: `http://en.wikipedia.org/wiki/Managed_security_service`

Opgaver som tidligere blev håndteret in-house, eller ignoreret:

Event opsamling og analyse, Email scanning, Anti-virus og spam,

Firewall opsætning, drift og konfiguration

Audit af netværk løbende, som en service - aktive pentest, paper review

Netværksopsætning internt, STP, RSTP, stacks, LACP, LLDP, ...

Netværksopsætning eksternt, BGP, LC-SC, single-mode, mono-mode, multi-mode, link-net, PI, PA, RIPE

Angreb DoS, DDoS m.v.

Udfordringerne i MSS

Definition af nye produkter - hvad får kunden

Kommunikation, både ved ændringer, problemer, opfølgning

Det er en omstilling for os at definere produkterne, men sundt

Kunderne er ikke vant til at overlade så meget til os

Hvem har reelt kontrollen? kan man out-source sikkerhed?

Ansvar - SLA dækker jo oppetid, hvad med brud på sikkerheden

Virtualisering af sikkerhed

Penetration testing execution standard

Following are the main sections defined by the standard as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Konkurrent til ISECOM Open Source Security Testing Methodology Manual?

Kilde: `http://www.pentest-standard.org/index.php/Main_Page`

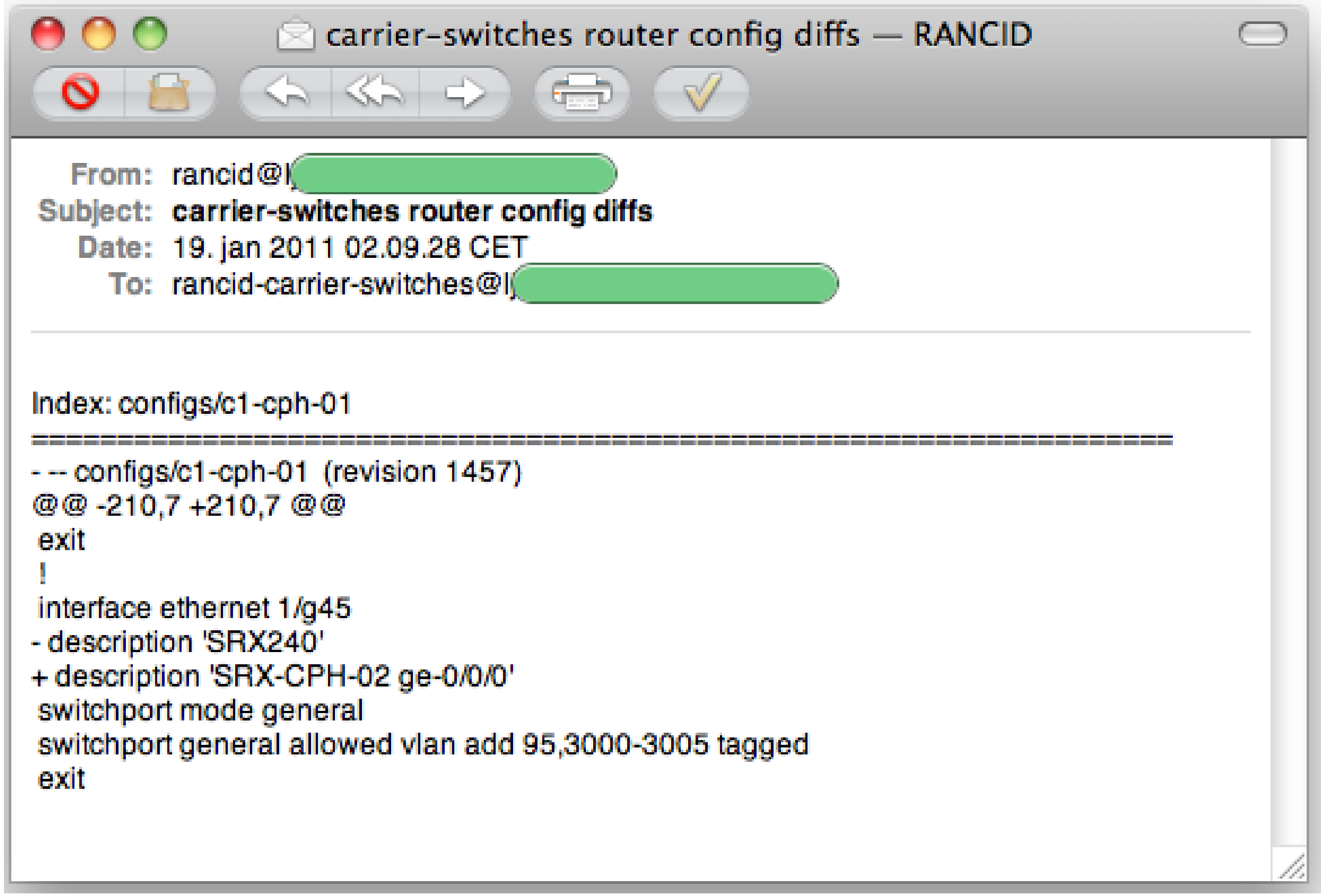
RANCID - Really Awesome New Cisco config Differ

```
[rancid@ljh routers]$ cat router.db
mx-lux-01:juniper:up
mx-lux-02:juniper:up
...
[rancid@ljh routers]$ crontab -l
# run config differ hourly
07 0-23/2 * * * /usr/local/rancid/bin/rancid-run
# clean out config differ logs
50 23 * * * /usr/bin/find /usr/local/rancid/var/logs -type f -mtime +2 -exec rm {}
```

RANCID will then fetch configurations, and more, and put it into version control SVN/CVS

Changes are emailed to an email alias

RANCID output



From: rancid@[redacted]
Subject: **carrier-switches router config diffs**
Date: 19. jan 2011 02.09.28 CET
To: rancid-carrier-switches@[redacted]

```
Index: configs/c1-cph-01
===================================================================
- -- configs/c1-cph-01  (revision 1457)
@@ -210,7 +210,7 @@
 exit
 !
 interface ethernet 1/g45
- description 'SRX240'
+ description 'SRX-CPH-02 ge-0/0/0'
 switchport mode general
 switchport general allowed vlan add 95,3000-3005 tagged
 exit
```

NIST Special Publication 800 series

Kender I NIST special publications?

SP 800-119 Feb. 22, 2010 DRAFT Guidelines for the Secure Deployment of IPv6
God fordi den forklarer hvad IPv6 er

SP 800-58 Jan 2005 Security Considerations for Voice Over IP Systems
Giver næsten et design der kan bruges direkte, giver svar på spørgsmål du selv har glemt at stille

`http://csrc.nist.gov/publications/PubsSPs.html`

PROSA CTF

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/`

Get ready! Lær debuggere, perl, java at kende, start på at hacke

Open Mike night ...

Hvad glemte jeg? Kom med dine favoritter ☺

Questions?

Henrik Lund Kramshøj
hlk@solidonetworks.com

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email

Husk at sige DK-NOG

Min nærmeste fremtid - resten af 2011

Nyt firma, konsolidering

Flere DNS, Luxembourg, flere kunder Luxembourg

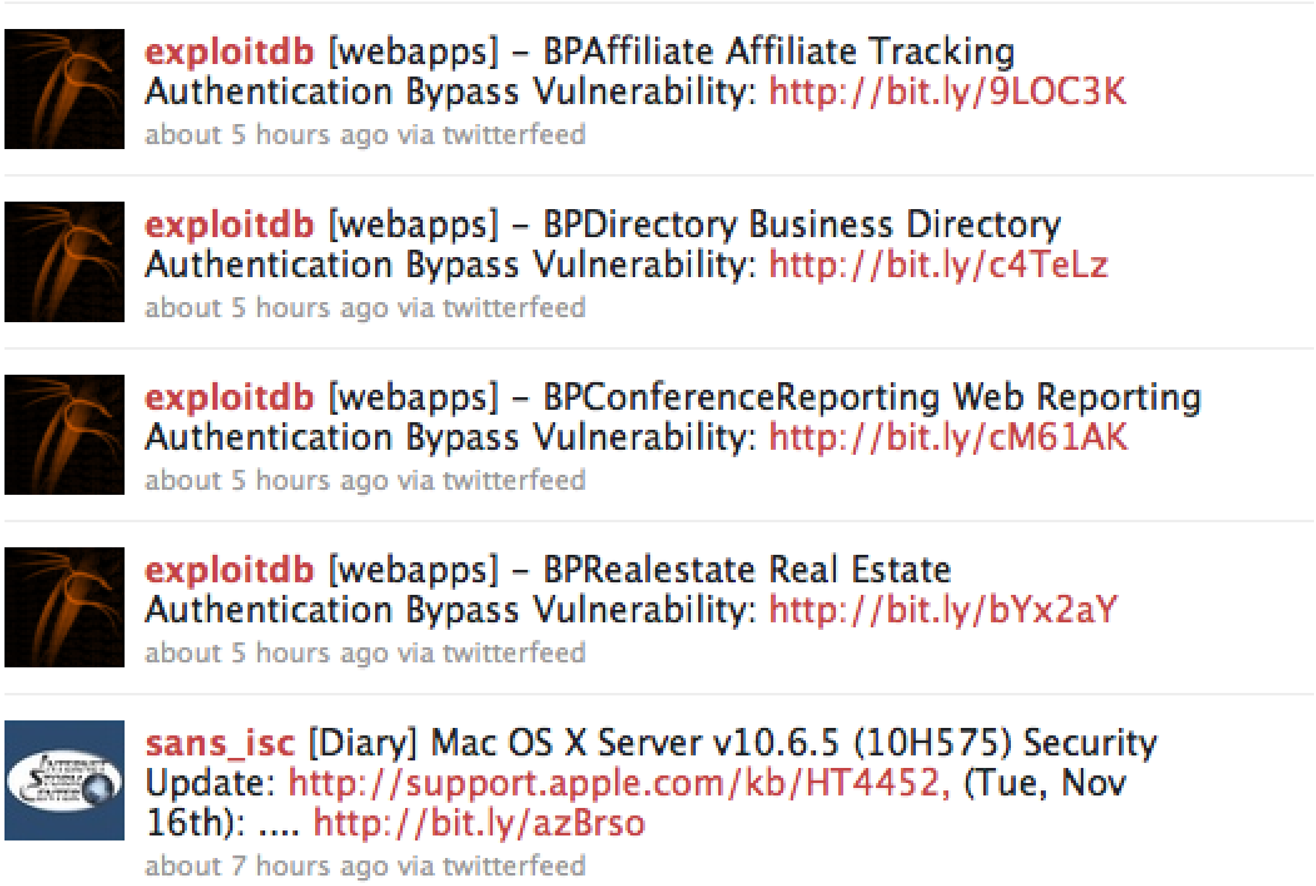
DNS TCP queries, IPv6 DNS, DNS reply-size testing

DNSSEC

IPv6, APNIC løber tør i år.

Bogon filter updates, BGP IPv6 filters, update

informationskilder



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

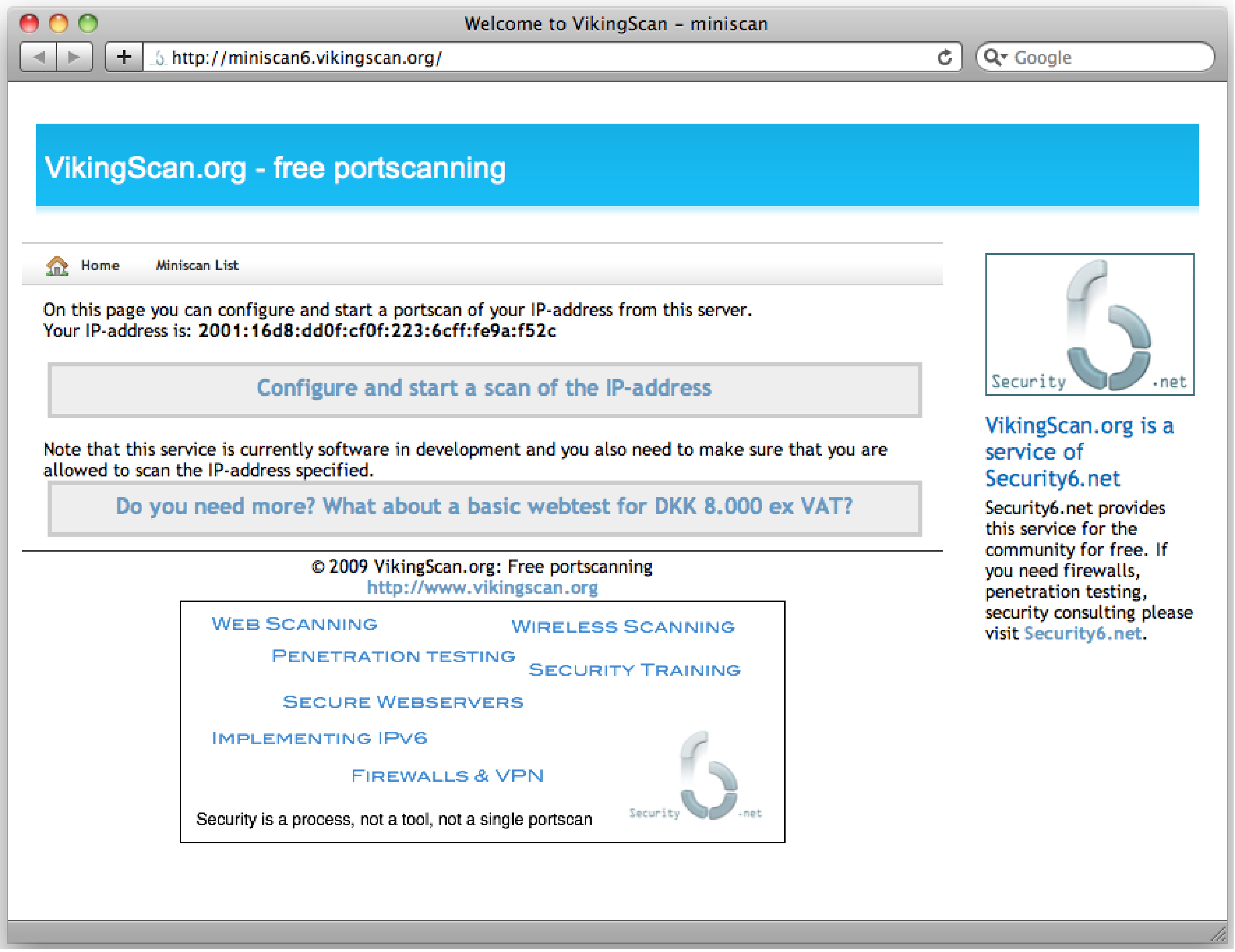
exploitdb [webapps] – BPRealestate Real Estate Authentication Bypass Vulnerability: http://bit.ly/bYx2aY
about 5 hours ago via twitterfeed

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`

VikingScan.org - free portscanning



Welcome to VikingScan – miniscan
http://miniscan6.vikingscan.org/
Google

VikingScan.org - free portscanning

On this page you can configure and start a portscan of your IP-address from this server.
Your IP-address is: **2001:16d8:dd0f:cf0f:223:6cff:fe9a:f52c**

Configure and start a scan of the IP-address

Note that this service is currently software in development and you also need to make sure that you are allowed to scan the IP-address specified.

Do you need more? What about a basic webtest for DKK 8.000 ex VAT?

© 2009 VikingScan.org: Free portscanning
http://www.vikingscan.org

Security is a process, not a tool, not a single portscan

VikingScan.org is a service of Security6.net

Security6.net provides this service for the community for free. If you need firewalls, penetration testing, security consulting please visit Security6.net.

Kontaktinformation og profil

- Henrik Lund Kramshøj, IT-sikkerhed og internet samurai
- Email: hlk@solido.net Mobil: +45 2026 6000
- Cand.scient fra Datalogisk Institut ved Københavns Universitet, DIKU
- CISSP og CEH certificeret
- 2003 - 2010 Selvstændig sikkerhedskonsulent
- 2010 Stifter og partner i Solido Networks ApS

Reklamer: kursusafholdelse

Følgende kurser afholdes med mig som underviser

- IPv6 workshop - 2 dage
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 1-2 dage
  En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og wirksomhedsnetværk.
- Hacker workshop 2 dage
  Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, OpenVAS 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.

Se mere på `http://www.solidonetworks.com`