

Welcome to

Tendenser i sikkerhed

April 2013

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

<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 2013

En potpourri af sikkerhedsemner - inspiration

Feedback og kommentarer modtages, dialog 😊



Kl 17-21 med pauser

Mindre foredrag mere snak

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

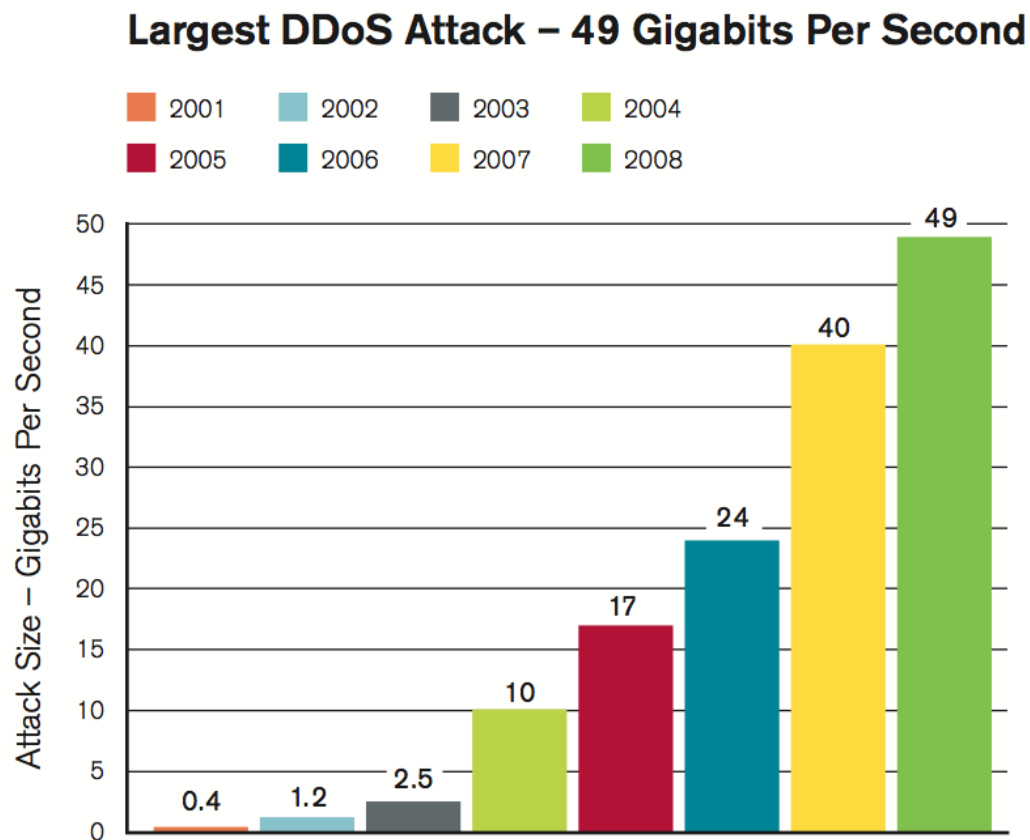


Figure 1: Largest DDoS Attack – 49 Gigabits Per Second

Source: Arbor Networks, Inc.

Kilde: <http://www.arbornetworks.com/report> 2009 rapporten

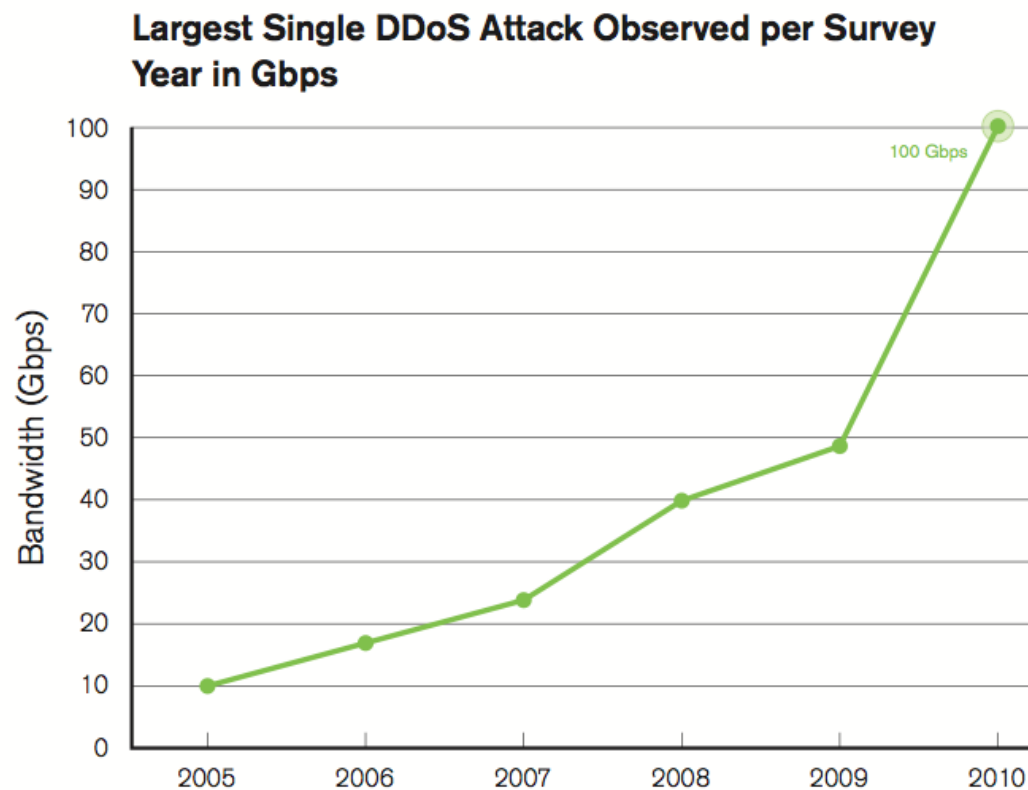


Figure 1

Source: Arbor Networks, Inc.

Kilde: <http://www.arbornetworks.com/report> 2010 rapporten

Lots of documentation

2012 Verizon Data Breach Investigations Report

2013 Trustwave Global Security Report



2013 State of Software Security Report The Intractable Problem of Insecure Software,
Veracode April 2013

- 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 - 2011 slide repeated here without changes

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 - woohooo!

Det betyder en tillid til DNS som muliggør alskens services.

Kilde:

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

cloudflare 300Gbit DDoS?



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?



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



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

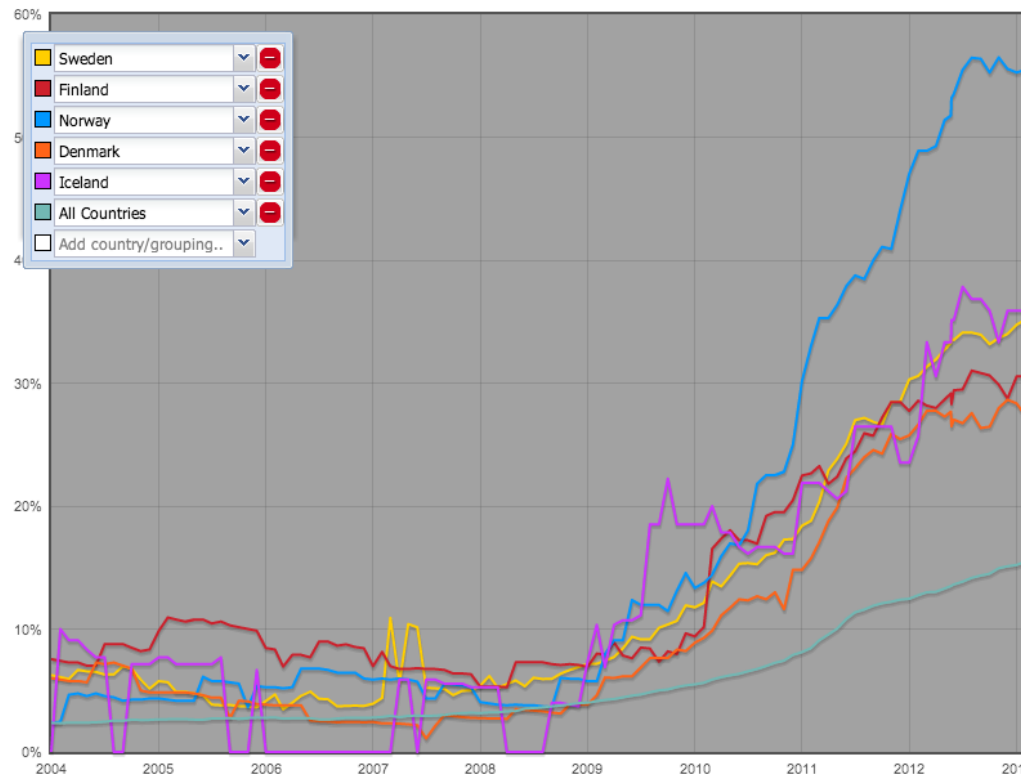
IPv6 in the Nordic region - 2013



IPv6 Enabled Networks

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

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



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

<https://www.ripe.net/membership/indices/DK.html>

Software and tool releases:

- BackTrack Kali <http://www.backtrack-linux.org>
- Suricata <http://www.openinfosecfoundation.org/>
- Nmap og Nping nmap.org
- Metasploit Framework <http://www.metasploit.com/>
- Github is also a source of great scripts and input

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
```

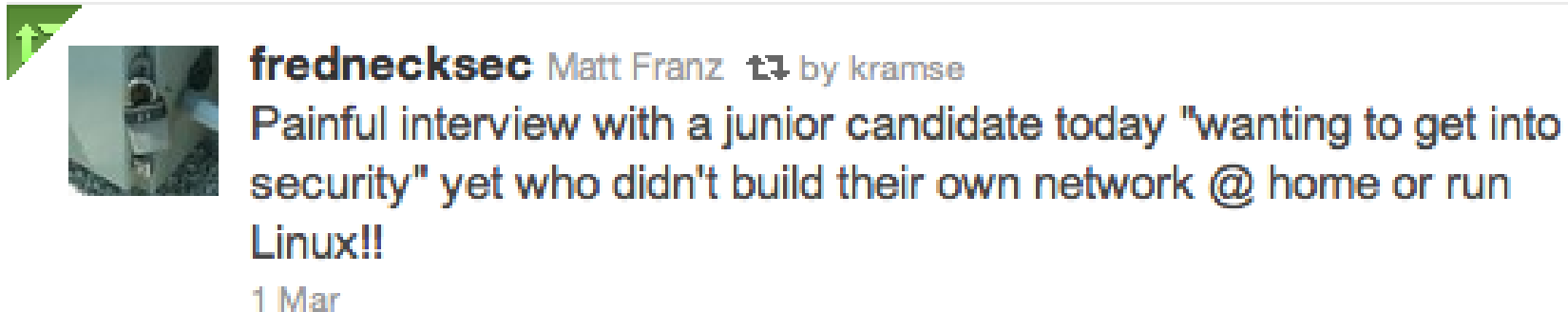
<http://nmap.org>

Still rocking the internet

Armitage GUI fast and easy hacking for Metasploit <http://www.fastandeasyhacking.com/>

Kilde:

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



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=dFU1AQZB9Ng>

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.

Sørg for at få overblik over infrastrukturen

Sørg for at have overblik over organisationen og leverandører

Put evt. kritiske tlfnr ind i mobilen - NOC og support hos dine ISP'er

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

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

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

Kunderne vil have høj opetid, 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

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.

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?

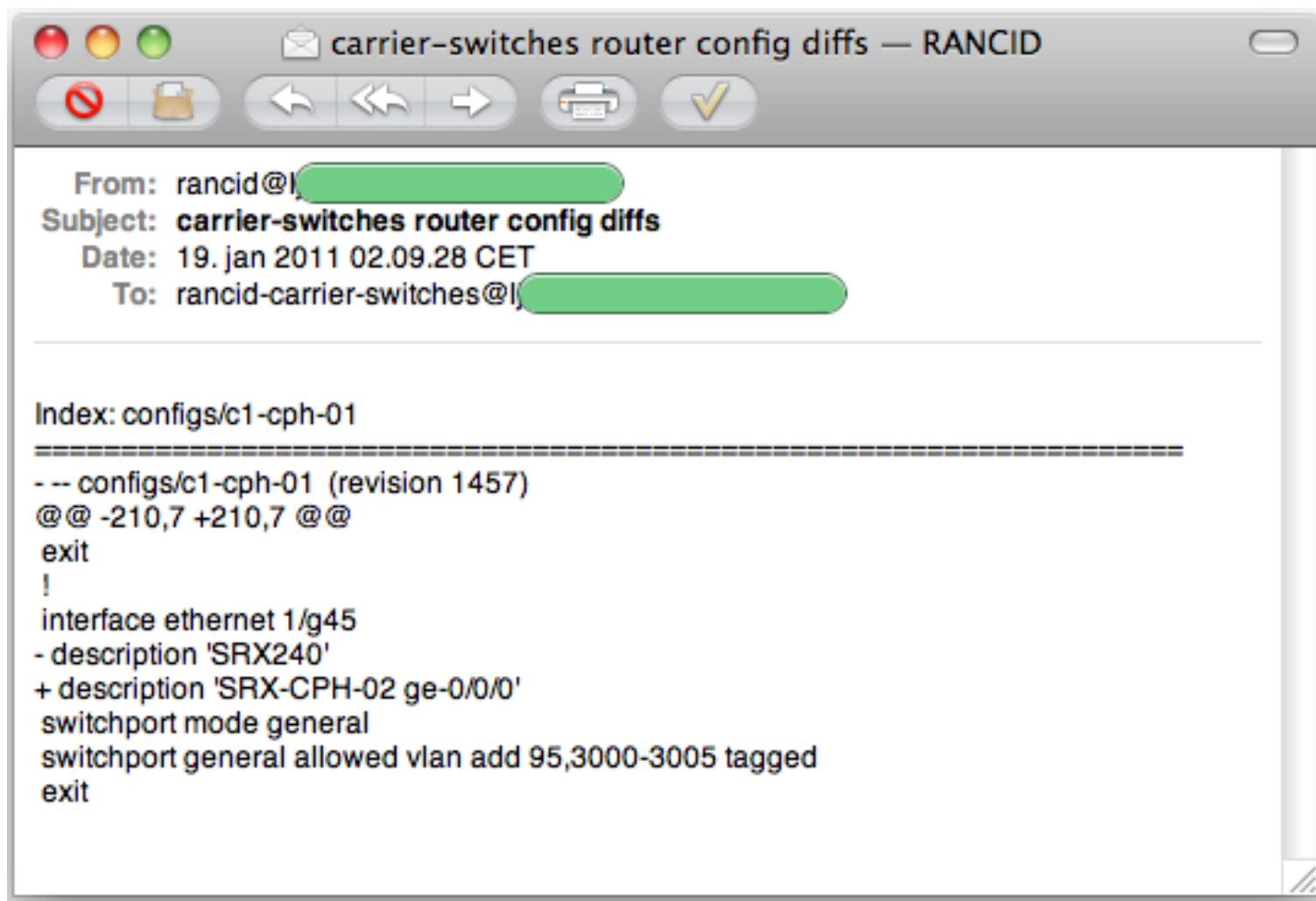
Ansvar - SLA dækker jo opetid, hvad med brud på sikkerheden

Virtualisering af sikkerhed

```
[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



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

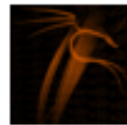
<http://csrc.nist.gov/publications/PubsSPs.html>

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

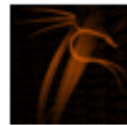
Mere IPv6:

Automatic BGP blackhole routing, perhaps based on input from Suricata

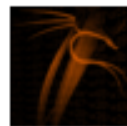
Conferences RIPE66 Dublin hardcore network people, OHM2013 Observe Hack Make



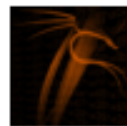
exploitdb [webapps] – BPAffiliate Affiliate Tracking
Authentication Bypass Vulnerability: <http://bit.ly/9LOC3K>
about 5 hours ago via twitterfeed



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

Twitter has replaced RSS for me

Email lists are still a good source of data

Hvad glemte jeg? Kom med dine favoritter 😊

Henrik Lund Kramshøj, internet samurai
`hlk@solido.net`

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email