

Welcome to

Tendenser i sikkerhed

Maj 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

Lots of documentation - examples only, not a recommendation

2012 Verizon Data Breach Investigations Report

2012 FireEye Advanced Threat Report - 2H 2012

2013 Trustwave Global Security Report

Worldwide Infrastructure Security Report 2012 Volume VIII, Arbor Networks

Alert Logic Releases 2013 State of Cloud Security Report

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

Secunia Vulnerability Review 2013


M-Trends 2013: Attack the Security Gap Mandiant

ACH is an eight-step procedure grounded in basic insights from cognitive psychology, decision analysis, and the scientific method. It is a surprisingly effective, proven process that helps analysts avoid common analytic pitfalls. Because of its thoroughness, it is particularly appropriate for controversial issues when analysts want to leave an audit trail to show what they considered and how they arrived at their judgment

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art11.html>
<http://jeffreycarr.blogspot.co.uk/2013/02/mandiant-apt1-report-has-critical.html>


- 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



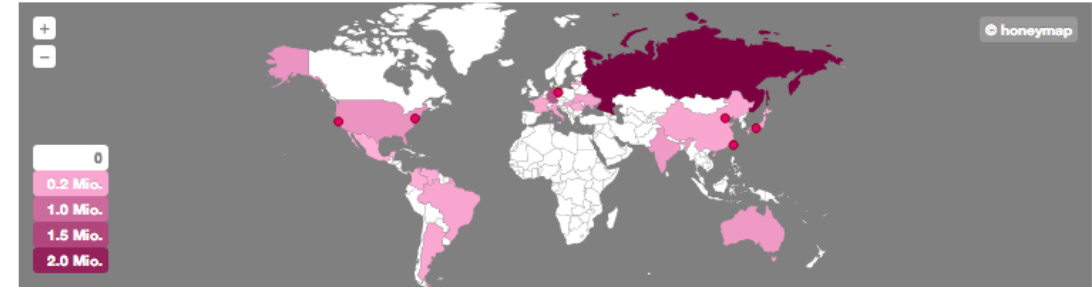
LIFE IS FOR SHARING.

OVERVIEWINFOIMPRINT



EnglishGerman

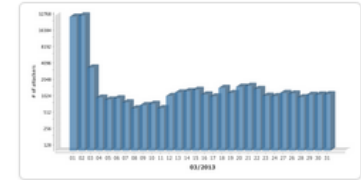
Overview of current cyber attacks (logged by 97 Sensors)



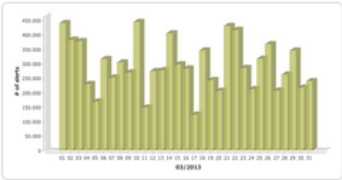
Live-Ticker

| Date | Source | Attack on | Parameter |
|---------------------|-----------|---------------|------------------------------------|
| 2013-04-09 09:29:38 | unbekannt | | Kippo.SSH_Connect.Fail |
| 2013-04-09 09:29:40 | unbekannt | | Kippo.SSH_Connect.Fail |
| 2013-04-09 09:29:40 | USA | Web site | /administra%20%3Cbr%20/%3E/&sa=U&a |
| 2013-04-09 09:29:40 | China | Console/Shell | Kippo.SSH_Connect.Fail |
| 2013-04-09 09:29:20 | unbekannt | | Kippo.SSH_Connect.Fail |

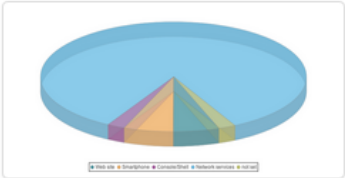
Overall sum of attackers per Day (Last Month)



Overall sum of attacks per Day (Last Month)



Distribution of Attack Targets (Last Month)



Top 15 of Source Countries (Last month)

| Source of Attack | Number of Attacks |
|-----------------------------------|-------------------|
| Russian Federation | 2,446,168 |
| Germany | 1,308,617 |
| Taiwan, Province of China | 536,034 |
| United States | 449,853 |
| Australia | 378,792 |
| India | 358,114 |
| Ukraine | 250,213 |
| Hungary | 237,607 |
| Brazil | 218,265 |
| China | 197,152 |
| Italy | 194,102 |
| France | 184,073 |
| Argentina | 182,166 |
| Japan | 151,861 |
| Venezuela, Bolivarian Republic of | 127,862 |

Top 5 of Attack Types (Last month)

| Description | Number of Attacks |
|----------------------------|-------------------|
| Attack on SMB protocol | 31,077,005 |
| Attack on Netbios protocol | 1,108,033 |
| Attack on Port 5353 | 921,115 |
| Attack on SSH protocol | 919,145 |
| Attack on Port 33434 | 687,446 |

<http://www.sicherheitstacho.eu/?lang=en>

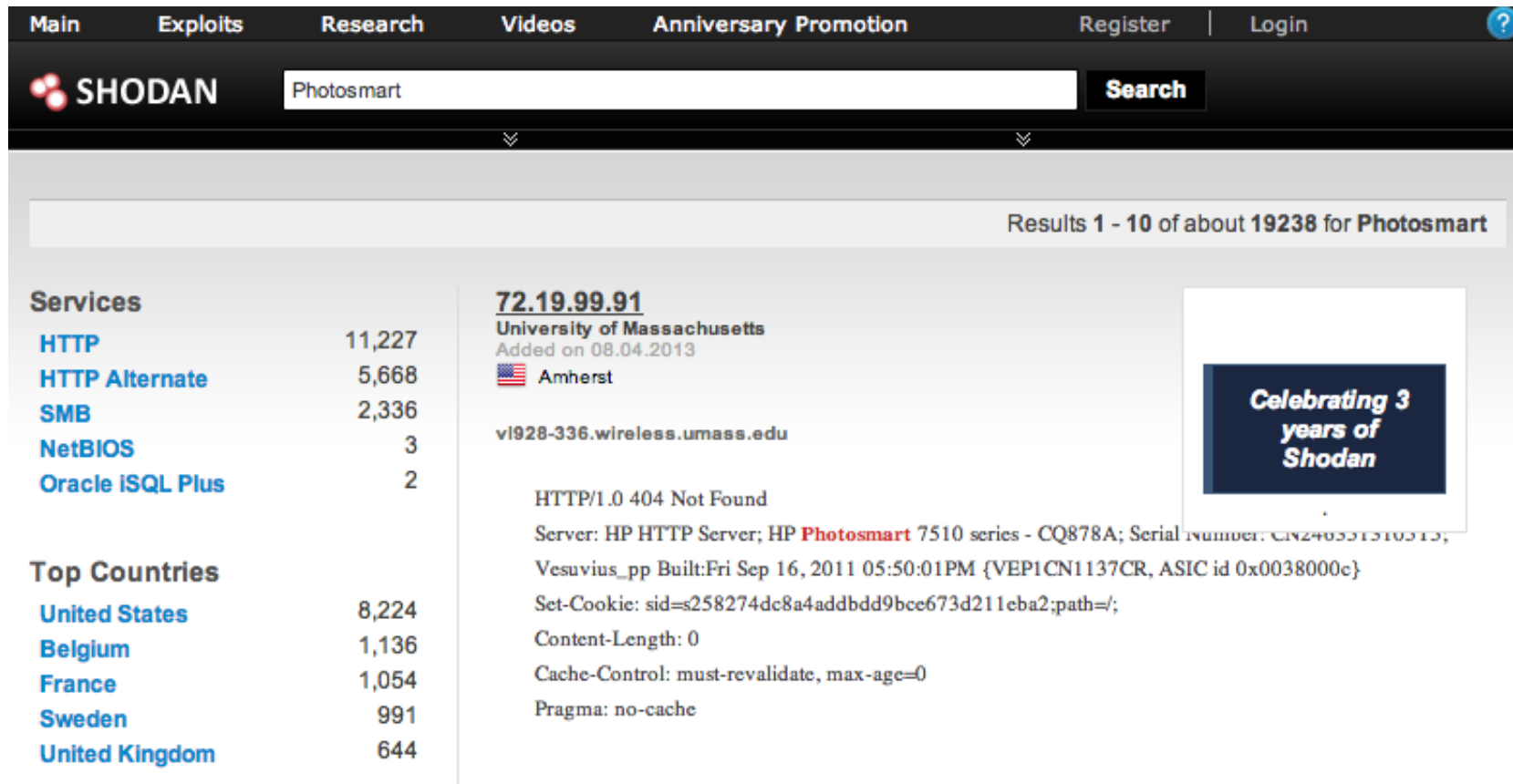
Internet Census 2012 Port scanning /0 using insecure embedded devices

Abstract While playing around with the Nmap Scripting Engine (NSE) we discovered an amazing number of open embedded devices on the Internet. Many of them are based on Linux and allow login to standard BusyBox with empty or default credentials. We used these devices to build a distributed port scanner to scan all IPv4 addresses. These scans include service probes for the most common ports, ICMP ping, reverse DNS and SYN scans. We analyzed some of the data to get an estimation of the IP address usage.

Additionally, with one hundred thousand devices scanning at ten probes per second we would have a distributed port scanner to port scan the entire IPv4 Internet within one hour.

Source: <http://internetcensus2012.bitbucket.org/paper.html>

http://www.theregister.co.uk/2013/03/19/carna_botnet_ipv4_internet_map/



The screenshot shows the Shodan search interface. At the top, there's a navigation bar with links: Main, Exploits, Research, Videos, Anniversary Promotion, Register, and Login. Below this is the Shodan logo and a search bar containing 'Photosmart' with a 'Search' button. The results section shows 'Results 1 - 10 of about 19238 for Photosmart'. On the left, there are two sidebars: 'Services' and 'Top Countries'. The 'Services' sidebar lists HTTP (11,227), HTTP Alternate (5,668), SMB (2,336), NetBIOS (3), and Oracle ISQL Plus (2). The 'Top Countries' sidebar lists United States (8,224), Belgium (1,136), France (1,054), Sweden (991), and United Kingdom (644). The main content area displays the first result for IP 72.19.99.91, identified as the University of Massachusetts Amherst, added on 08.04.2013. It shows the URL vi928-336.wireless.umass.edu and the HTTP response: HTTP/1.0 404 Not Found. The response headers include: Server: HP HTTP Server; HP Photosmart 7510 series - CQ878A; Serial number: CN248531310313; Vesuvius_pp Built: Fri Sep 16, 2011 05:50:01PM {VEP1CN1137CR, ASIC id 0x0038000c}; Set-Cookie: sid=s258274dc8a4addbdd9bce673d211eba2;path=/; Content-Length: 0; Cache-Control: must-revalidate, max-age=0; Pragma: no-cache. A small banner on the right says 'Celebrating 3 years of Shodan'.

| Services | Count |
|------------------|--------|
| HTTP | 11,227 |
| HTTP Alternate | 5,668 |
| SMB | 2,336 |
| NetBIOS | 3 |
| Oracle ISQL Plus | 2 |

| Top Countries | Count |
|----------------|-------|
| United States | 8,224 |
| Belgium | 1,136 |
| France | 1,054 |
| Sweden | 991 |
| United Kingdom | 644 |

72.19.99.91
University of Massachusetts
Added on 08.04.2013
Amherst
vi928-336.wireless.umass.edu

HTTP/1.0 404 Not Found
Server: HP HTTP Server; HP **Photosmart** 7510 series - CQ878A; Serial number: CN248531310313;
Vesuvius_pp Built: Fri Sep 16, 2011 05:50:01PM {VEP1CN1137CR, ASIC id 0x0038000c}
Set-Cookie: sid=s258274dc8a4addbdd9bce673d211eba2;path=/;
Content-Length: 0
Cache-Control: must-revalidate, max-age=0
Pragma: no-cache

Celebrating 3 years of Shodan

`http://www.shodanhq.com/search?q=Photosmart`

Title: Cisco's new password hashing scheme easily cracked

Description: In an astonishing decision that has left cryptographic experts scratching their heads, engineer's for Cisco's IOS operating system chose to switch to a **one-time SHA256 encoding - without salt** - for storing passwords on the device. This decision leaves password hashes vulnerable to high-speed cracking - modern graphics cards can compute over **2 billion SHA256 hashes in a second - and is actually considerably less secure than Cisco's previous implementation**. As users cannot downgrade their version of IOS without a complete reinstall, and no fix is yet available, security experts are urging users to avoid upgrades to IOS version 15 at this time.

Reference: via SANS @RISK newsletter

<http://arstechnica.com/security/2013/03/cisco-switches-to-weaker-h>

 **Poul-Henning Kamp** @bsdphk 19 Mar

As author of md5crypt(), my mind boggles at such incompetence:
arstechnica.com/security/2013/... Please do better than cisco:
password-hashing.net/index.html

 Hide summary  Reply  Retweet  Favorite  More

 **Ars Technica**

Cisco switches to weaker hashing scheme, passwords cracked wide open

By **Dan Goodin** @dangoodin001

Crypto technique requires little time and computing resources to crack.

[View on web](#)

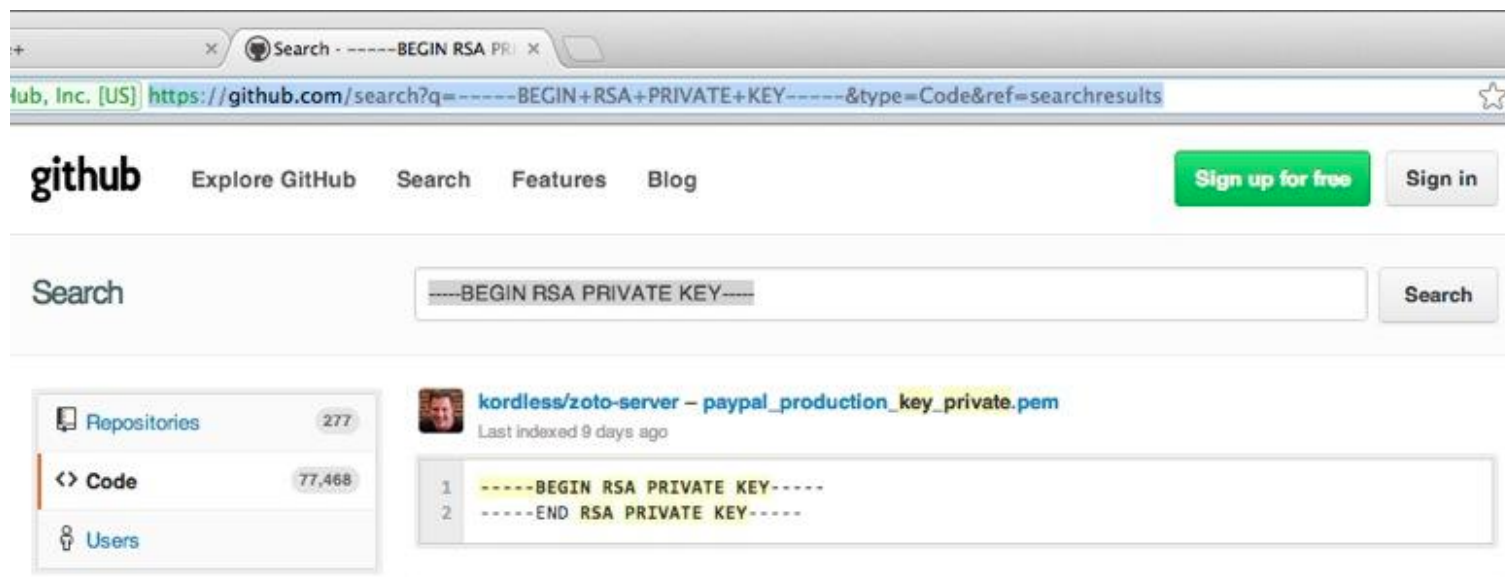
12 RETWEETS **3** FAVORITES



11:18 AM - 19 Mar 13 · Details [Flag media](#)

Poul-Henning Kamp @bsdphk er forfatter md5crypt som Cisco brugte
<http://phk.freebsd.dk/sagas/md5crypt.html>

January: Github Public passwords?



Sources:

<https://twitter.com/brianaker/status/294228373377515522>

<http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-de>

<http://www.leakedin.com/>

<http://www.offensive-security.com/community-projects/google-hacking-database/>

Security Notice: Service-wide Password Reset

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

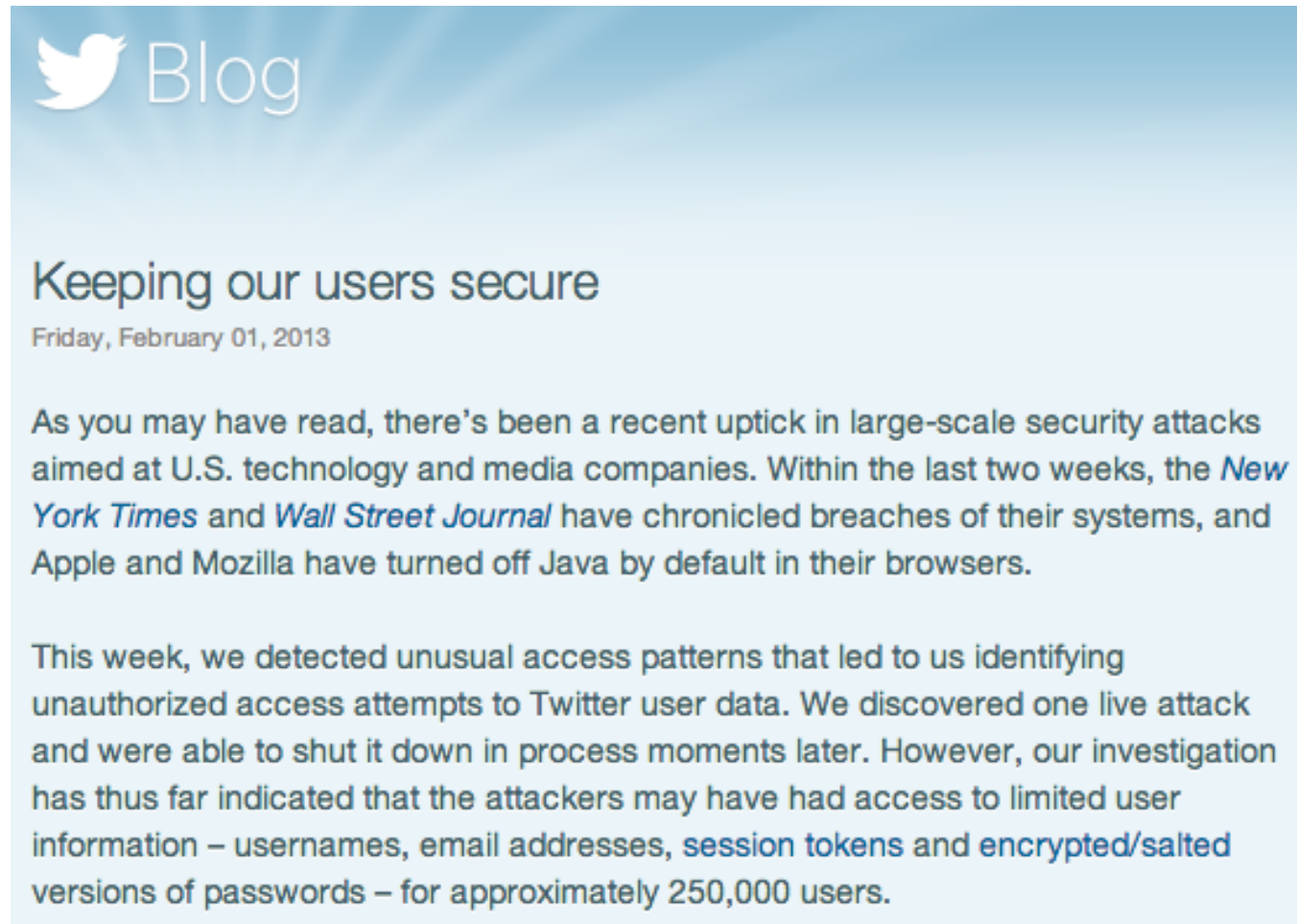
As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

In our security investigation, we have found no evidence that any of the content you store in Evernote was accessed, changed or lost. We also have no evidence that any payment information for Evernote Premium or Evernote Business customers was accessed.

The investigation has shown, however, that the individual(s) responsible were able to gain access to Evernote user information, which includes usernames, email addresses associated with Evernote accounts and encrypted passwords. Even though this information was accessed, the passwords stored by Evernote are protected by one-way encryption. (In technical terms, they are hashed and **salted**.)

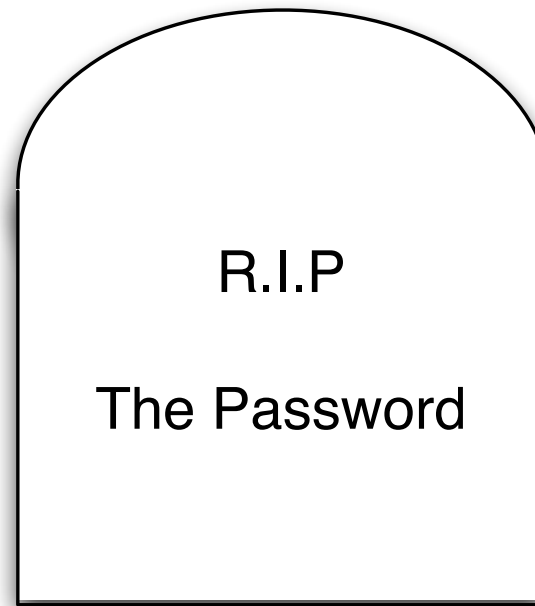
Sources:

http://evernote.com/corp/news/password_reset.php



Sources:

<http://blog.twitter.com/2013/02/keeping-our-users-secure.html>



Can we stop using passwords?

Muffett on Passwords has a long list of password related information, from the author of **crack** [http://en.wikipedia.org/wiki/Crack_\(password_software\)](http://en.wikipedia.org/wiki/Crack_(password_software))

<http://dropsafe.crypticide.com/muffett-passwords>

- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

Source:

<http://hashcat.net/wiki/>

<http://www.openwall.com/john/>

Fandt en god blog omkring password cracking eksempelvis omkring hvad der skal til for at bygge din egen GPU cracker

What hardware to choose when building a GPU based password cracker right now (Q1 2012)?

<http://champagneandsecurity.wordpress.com/category/password-cracking/>




Google looks to ditch passwords for good



"Google is currently running a pilot that uses a YubiKey cryptographic card developed by Yubico

The YubiKey NEO can be tapped on an NFC-enabled smartphone, which reads an encrypted one-time password emitted from the key fob."

Source: <http://www.zdnet.com/google-looks-to-ditch-passwords-for-good-with-nfc-based-replacement>

| | | | |
|---|--|--|---|
| Blocklists Safe DNSBLs for safe filters SBL Advisory XBL Advisory PBL Advisory DBL Advisory 禪 ZEN | Blocklist Removal Blocked? To check, get info and resolve listings go to ▶ Blocklist Removal Center Blocklist Use ▶ DNSBL Usage Terms ▶ How Blocklists Work  <p>The Industry's Most Accurate Realtime Spam Filter Data ▶ more info</p> | Documents ▶ Consumer Protection ▶ The Definition of "Spam" ▶ Email Marketing Guide Datafeed ▶ Datafeed service for ISPs and commercial users  <p>Spamhaus Datafeed 30-day Free Trial ▶ more info</p> | ROKSO ▶ Register of Known Spam Operations ▶ ROKSO Policy & FAQs ISP Area ▶ ISP Area ▶ ISP Abuse Desk FAQs  <p>TOP 10 World's Worst Spam Problem Networks ▶ charts</p> |
|---|--|--|---|

Source: <http://www.spamhaus.org/>

Title: Massive DDoS against Spamhaus reaches 300Gbps Description: Following a dispute between Dutch hosting provider Cyberbunker and anti-spam group Spamhaus, the latter suffered what initially began as a relatively small - 10 Gbps - DDoS, which escalated over the course of last week to a 300Gbps flood.

Source: <http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet>

CloudFlare CEO Matthew Prince said he was sure of the 300Gbps figure, pointing to an online comment from Richard Steenbergen, CTO of nLayer, one of the upstream network providers of CloudFlare. Although Steenbergen said the company saw a 300Gbps hit going after CloudFlare, which targeted "pieces" of the core network, it was nothing "record smashing" or "game changing"

Actual data proving a 300Gbps hit remains thin on the ground. Hammack said his firm had not seen anything above 160Gbps in a single DDoS, with 144 million packets sent per second, and he doesn't believe there has been one higher. He won't be convinced otherwise unless someone shows him proof one organisation's network took more traffic in an attack.

Source: Prolexic CEO: Biggest Cyber Attack Ever Was Built On Lies

<http://www.techweekeurope.co.uk/news/prolexic-ceo-scott-hammack-biggest-cyber-attack-lies-spam>

Så du skal *kun* beskytte dig mod 160Gbps 😊

We have talked about DNS for a long time:

- DNS: Domain Name System `www.domain.tld` → IP address like `10.1.2.2`
- DNSSEC read Michael W. Lucas, DNSSEC Mastery
- IPv6 DNS - configure IPv6 now please
- DNS TCP queries - reconfigure your firewall now please
- EDNS reply-size testing - check using tools from <https://www.dns-oarc.net/>



Sources: to many to mention, but read these

<http://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf>

<http://www.opine.me/cert-advisory-on-dns-amplification-offers-little-hope/>

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/>

Open Recursive Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks and pose a similar threat as those from Smurf attacks commonly seen in the late 1990's.

We have collected a list of 27,200,613 resolvers that respond to queries in some fashion. 25.2 million of these pose a significant threat (as of 07-APR-2013)

`http://openresolverproject.org/`


yeah yeah, and so f*cking what?

what about SNMP, syslog and other UDP services?

BIND Security Advisories

A Maliciously Crafted Regular Expression Can Cause Memory Exhaustion in named

A critical defect in BIND 9 allows an attacker to cause excessive memory consumption in named or other programs linked to libdns.

| | |
|---------------------------|---|
| CVE: | CVE-2013-2266  |
| Document Version: | 1.0 |
| Posting date: | 26 Mar 2013 |
| Program Impacted: | BIND |
| Versions affected: | "Unix" versions of 9.7.x, 9.8.0 -> 9.8.5b1, 9.9.0 -> 9.9.3b1. (Windows versions are not affected) |
| Severity: | Critical |
| Exploitable: | Remotely |

`https://www.isc.org/advisories/bind`

`https://www.isc.org/software/bind/security`

Remember if you run a public accessible server also to look at Response Rate Limiting patches `http://www.redbarn.org/dns/ratelimits`

BCP38 Network Ingress Filtering

Network Working Group
Request for Comments: 2827
Obsoletes: 2267
BCP: 38
Category: Best Current Practice

P. Ferguson
Cisco Systems, Inc.
D. Senie
Amaranth Networks Inc.
May 2000

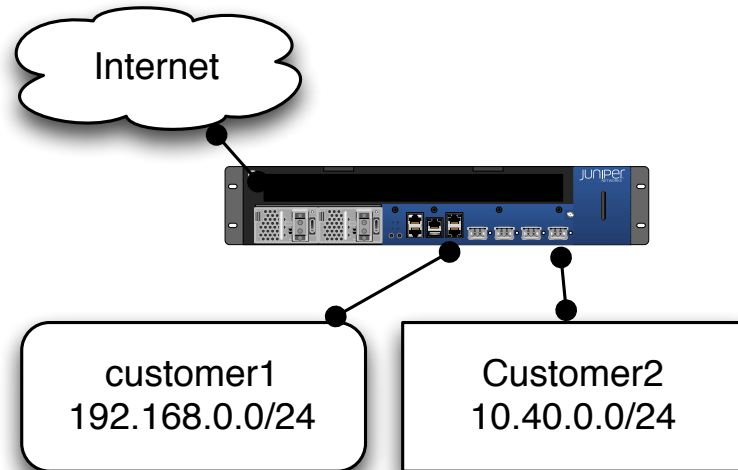
Network Ingress Filtering:
Defeating Denial of Service Attacks which employ
IP Source Address Spoofing

Note: you should try validating INCOMING traffic from customers, also note the date!

<http://tools.ietf.org/html/bcp38>

Reverse path forwarding (RPF) is a technique used in modern routers for the purposes of ensuring loop-free forwarding of multicast packets in multicast routing and to help prevent IP address spoofing in unicast routing.

Source: `http://en.wikipedia.org/wiki/Reverse_path_forwarding`

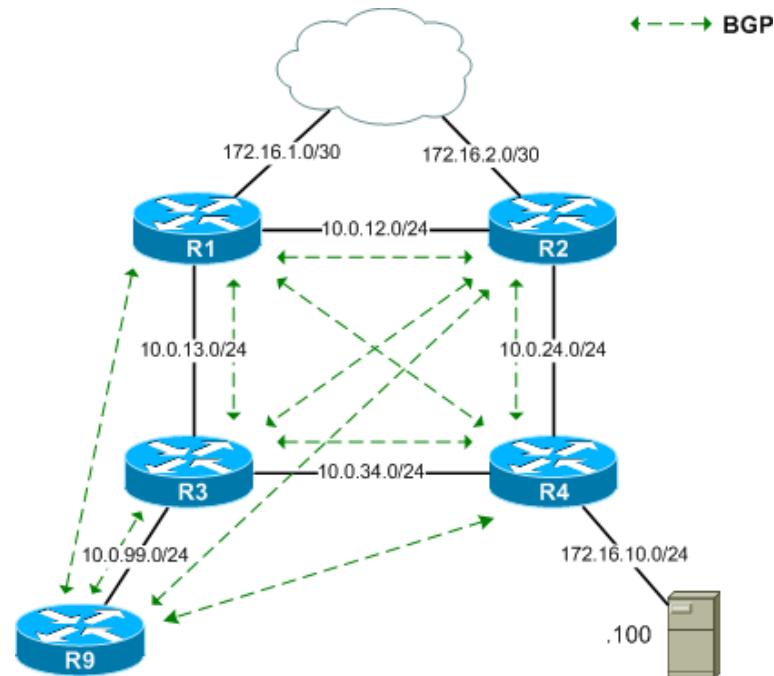


```
user@router# show interfaces
ge-0/0/0 {
  unit 2 {
    family inet {
      rpf-check fail-filter rpf-special-case-dhcp;
      address 192.168.0.254/24;
    }
  }
}
ge-0/0/1 {
  unit 2 {
    family inet {
      rpf-check fail-filter rpf-special-case-dhcp;
      address 10.40.0.254/24;
    }
  }
}
```

Configuring Unicast RPF Strict Mode

In strict mode, unicast RPF checks whether the incoming packet has a source address that matches a prefix in the routing table, **and whether the interface expects to receive a packet with this source address prefix.**

Remotely Triggered Black Hole Configurations



Picture from packetlife.net showing R9 as a standalone "management" router for route injection.

<http://packetlife.net/blog/2009/jul/6/remotely-triggered-black-hole-rtbh-routing/>

<https://ripe65.ripe.net/presentations/285-inex-ripe-routingwg-amsterdam-2012-09-27.pdf>

<https://www.inex.ie/rtbh>

```
hlk@katana:bgpq3-0.1.16$ ./bgpq3 -Jl larsen-data AS197495
policy-options {
  replace:
    prefix-list larsen-data {
      91.221.196.0/23;
      185.10.8.0/22;
    }
}
```

<http://snar.spb.ru/prog/bgpq3/>

```
+ route 173.X.X.X/32-DNS-DROP {  
+     match {  
+         destination 173.X.X.X/32;  
+         port 53;  
+         packet-length [ 99971 99985 ];  
+     }  
+     then discard;  
+ }
```

Resulted in router crashes - oooops

<http://blog.cloudflare.com/todays-outage-post-mortem-82515>

<http://www.slideshare.net/sfouant/an-introduction-to-bgp-flow-spec>

<https://code.google.com/p/exabgp/wiki/flowspec>

<http://www.slideshare.net/junipernetworks/flowspec-bay-area-juniper-user-group->

There were no known exploits at the time of release. ...

1. Persistent Denial of Service: an unauthenticated attacker may use this vulnerability to cause PostgreSQL error messages to be appended to targeted files in the PostgreSQL data directory on the server. ...
2. Configuration Setting Privilege Escalation: in the event that an attacker has a legitimate login on the database server, and the server is configured ...
3. Arbitrary Code Execution: if the attacker meets all of the qualifications under 2 above, and has the ability to save files to the filesystem as well (even to the tmp directory), then they can use the vulnerability to load and execute arbitrary C code. SELinux will prevent this specific type of exploit.

Sources:

<https://isc.sans.edu/diary/Postgresql+Patches+Critical+Vulnerability/15553>

<http://seclists.org/bugtraq/2013/Apr/26>

<http://www.postgresql.org/support/security/faq/2013-04-04/>

Java er et krav for at bruge NemID.

Brug gerne flere browsere, hvor kun een har Java slået til

PS Jeg kan godt lide Java og JVM, er bare træt af NemID

For mange opdateringer, jeg er træt ... af at skulle hjælpe folk med Java hele tiden.



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

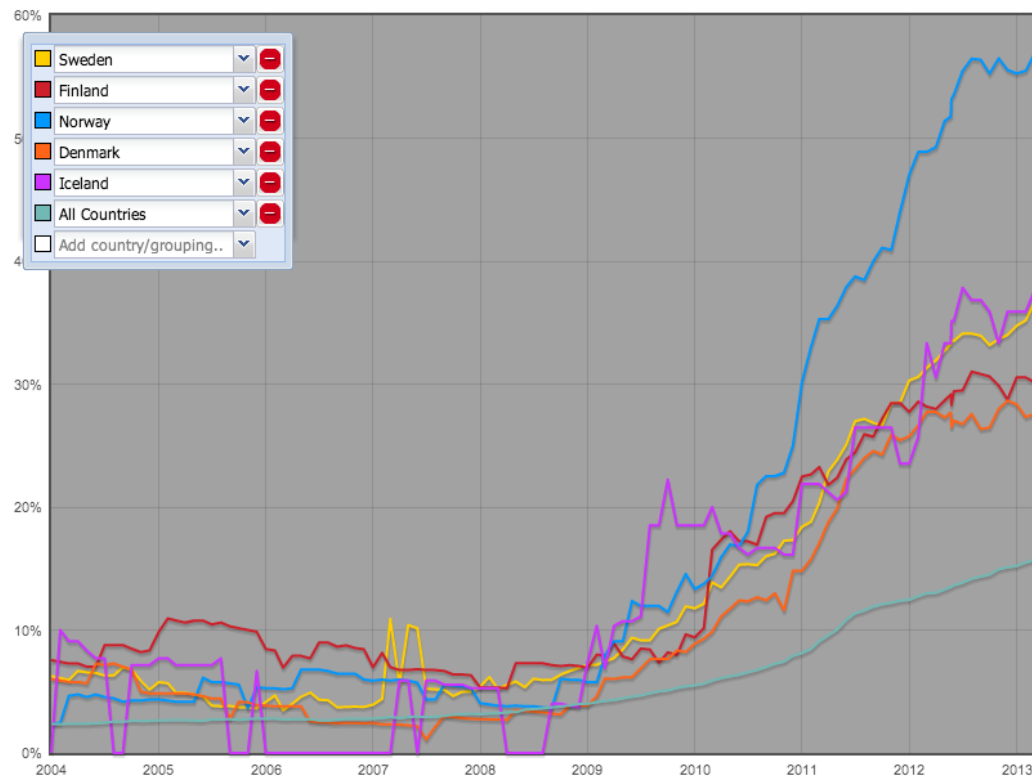
IPv6 in the Nordic region - 2013



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.kali.org/> <http://www.backtrack-linux.org>
- Suricata <http://www.openinfosecfoundation.org/>
- Nmap og Nping nmap.org
- Metasploit Framework <http://www.metasploit.com/>
- Parsing Windows Eventlogs in Powershell
- Security Onion, Bro Network Security Monitor
- Github is also a source of great scripts and input
- Qubes OS



The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - What's new ?

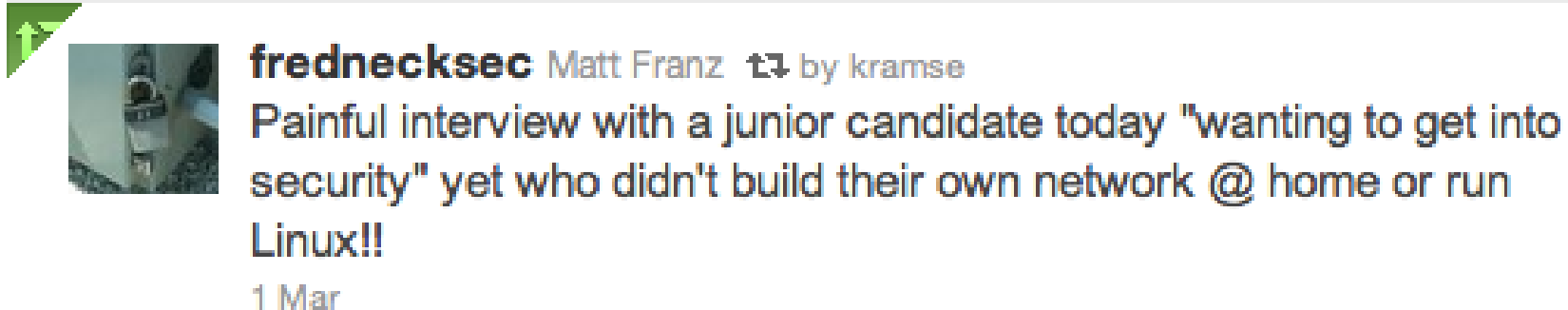
KALI LINUX
"the quieter you become, the more you are able to hear"

PENETRATION TESTING, REDEFINED.

A Project By Offensive Security

BackTrack <http://www.backtrack-linux.org>

Kali <http://www.kali.org/>



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>

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

<http://www.metasploit.com/>

Armitage GUI fast and easy hacking for Metasploit

<http://www.fastandeasyhacking.com/>

Metasploit Unleashed

http://www.offensive-security.com/metasploit-unleashed/Main_Page

Kilde:

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

[KB947226](#) helps to translate the EventIDs into readable information. Once we know which events are of interest, we can then extract them:

```
PS C:\TEMP> $seclog | ? { $_.eventid -match '5140' } | fl *
```

```
[...]
```

```
Message : A network share object was accessed.
```

```
Subject:
```

```
Security ID:      S-1-5-21-394181-2045529214-8259512215-1280
Account Name:     TRA29C
Account Domain:   AMER
Logon ID:         0x311a28b
```

```
Network Information:
```

```
Object Type:      File
Source Address:    10.11.192.16
Source Port:      6539
```

```
Share Information:
```

```
Share Name:       \\*\C$
Share Path:       \??\C:\
```

```
[...]
```

Source: via SANS Diary

<https://isc.sans.edu/diary/Parsing+Windows+Eventlogs+in+Powershell/15298>



`securityonion.blogspot.dk`



The Bro Network Security Monitor

Bro is a powerful network analysis framework that is much different from the typical IDS you may know.

While focusing on network security monitoring, Bro provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Bro has successfully bridged the traditional gap between academia and operations since its inception.

<http://www.bro.org/>

The key point that helped me understand was the explanation that Bro is a domain-specific language for networking applications and that Bro-IDS (<http://bro-ids.org/>) is an application written with Bro.

Why I think you should try Bro

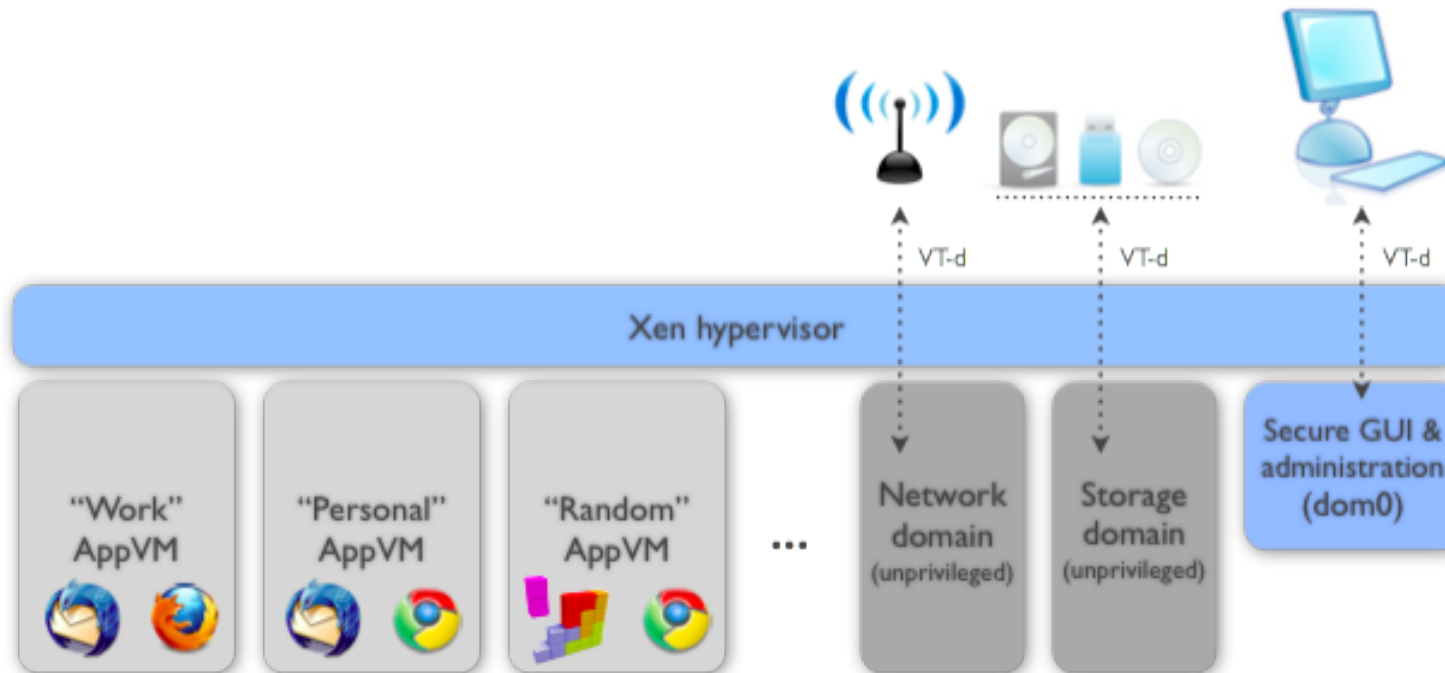
<https://isc.sans.edu/diary.html?storyid=15259>

```
global dns_A_reply_count=0;
global dns_AAAA_reply_count=0;
...
event dns_A_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
{
++dns_A_reply_count;
}

event dns_AAAA_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
{
++dns_AAAA_reply_count;
}
```

source: dns-fire-count.bro from

<https://github.com/LiamRandall/bro-scripts/tree/master/fire-scripts>



Qubes is an open source operating system designed to provide strong security for desktop computing. Qubes is based on Xen, X Window System, and Linux

Source: <http://www.qubes-os.org>

Sørg for at få overblik over infrastrukturen

- detaljeret information om data, protokoller, båndbredde, porte, services

Sørg for at have overblik over organisationen og leverandører

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

Kontrol med BYOD

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

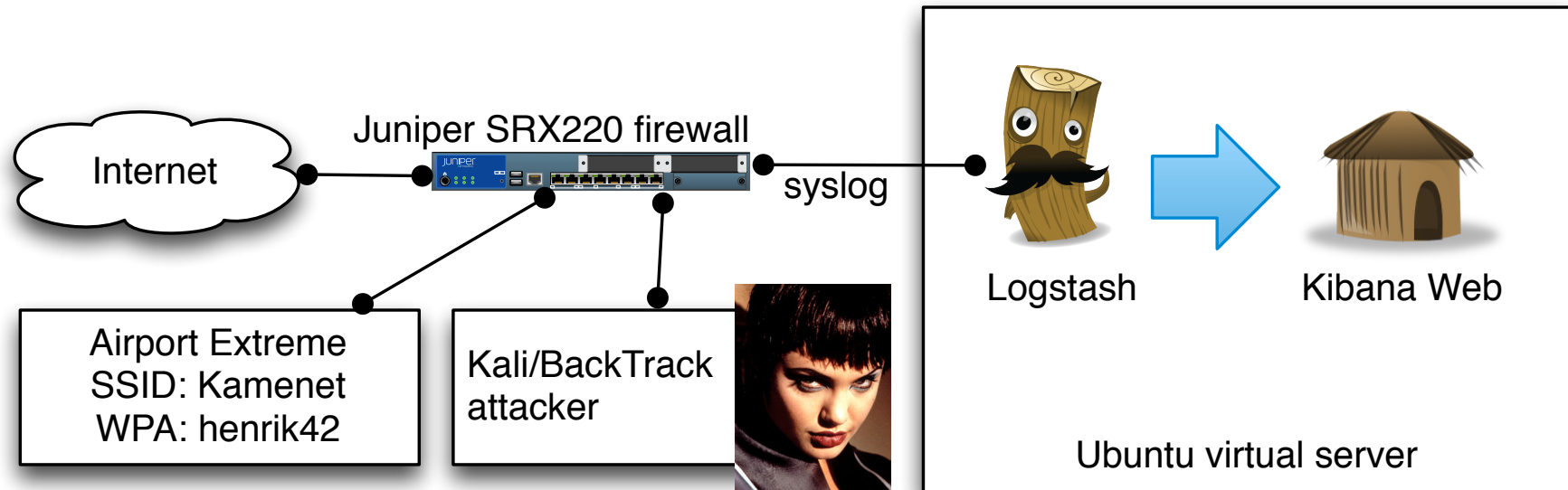
Afdække afhængigheder - hvem er din organisation afhængige af

Hjælpemidler

Configuration Management, Patch management og automatiseret sikkerhedstest

Start evt. med RANCID, NeXpose Community Edition og Metasploit fra BackTrack/Kali

Demo: Kibana og logstash



Source:

<http://logstash.net/> logstash is a tool for managing events and logs

<http://kibana.org/> Kibana is a highly scalable interface for Logstash and ElasticSearch that allows you to efficiently search, graph, analyze and otherwise make sense of a mountain of logs.

<http://www.kali.org/> the most advanced penetration testing distribution, ever.

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

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

høj oppetid, fordi internet teknologier er forretningskritiske

netværket er forretningskritisk nedetid == tab

Kunderne har ikke *nok* netværk til at have fuldtidsansatte

Hvad skal der til for at tilbyde Managed Security Services

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

Du kan også selv definere dine services

Kender I NIST special publications?

SP 800-119 Dec. 22, 2010 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/Bro

Conferences:

RIPE66 Dublin hardcore network people <https://ripe66.ripe.net/>

OHM2013 Observe Hack Make <http://ohm2013.org/>



Twitter has replaced RSS for me

Email lists are still a good source of data

Favourite Security Diary from Internet Storm Center

<http://isc.sans.edu/index.html>

<https://isc.sans.edu/diaryarchive.html?year=2013&month=4>

Hvad glemte jeg? Kom med dine favoritter 😊

evalg, DNS censur, NemID bashing, malware sucks, Android malware, iPhone malware?

Did you notice how a lot of the links in this presentation uses HTTPS - encrypted

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email