



Welcome to

Hacking Seminar

Henrik Lund Kramshøj hlk@zecurity.dk

Slides are available as PDF, kramshoej@Github



Don't Panic!

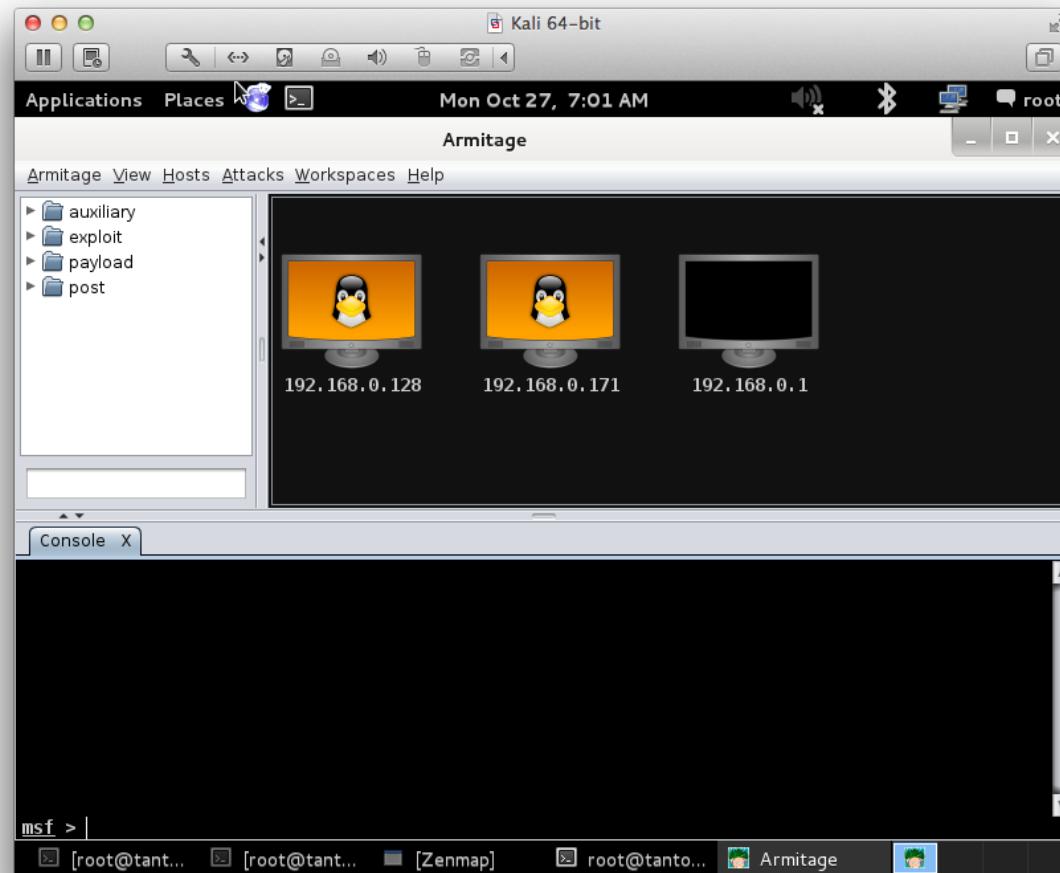
Hvad er truslerne, hvad er nogle trends indenfor sikkerhed

Hvordan foregår hacking

Hvad kan vi gøre for at dæmme op for truslerne

Jeg bruger Kali 2.0 Linux hackerplatformen som eksempel

Demo: Metasploit Armitage





Metasploit and Armitage Still rocking the internet

What is it?

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

Udviklingsværktøjerne til exploits er i dag meget raffinerede!

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

Armitage GUI fast and easy hacking for Metasploit

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

Kursus Metasploit Unleashed

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

Bog: Metasploit: The Penetration Tester's Guide, No Starch Press

ISBN-10: 159327288X

Hackerværktøjer



Improving the Security of Your Site by Breaking Into it af Dan Farmer og Wietse Venema i 1993

De udgav i 1995 så en softwarepakke med navnet SATAN *Security Administrator Tool for Analyzing Networks*

De forårsagede en del panik og furore, alle kan hacke, verden bryder sammen

We realize that SATAN is a two-edged sword – like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Kilde: <http://www.fish2.com/security/admin-guide-to-cracking.html>

Security Breaches: Ashley Madison



When hackers swiped an estimated 36 million accounts associated with Ashley-Madison.com, a site which helps married people cheat on their partners, there was a rush to find out what had been stolen.

- Ashley Madison, inkl password hacking
- Popular passwords 123456, ,password ,12345 ,qwerty ,12345678,football
- Also hacking kills? Suicides and family break-ups?
- accidental outing of gays/ Gay persecution, death?

Source:

<http://www.zdnet.com/article/these-are-the-worst-passwords-from-the-ashley-madison-hack/>

Security Breaches: Top 20 Ashley Madison Passwords



Previously thought to be impossible thanks to the slow pace and high stress it puts on a computer's CPU, the CynoSure Prime group managed to crack over 11 million passwords from the total of 36 million, mainly due to a programming error in how the passwords were hashed.

- Main passwords hashed with slow (good) bcrypt algorithm, but hackers found tokens hashed with MD5
<http://cynosureprime.blogspot.dk/2015/09/how-we-cracked-millions-of-ashley.html>
- Also check out Twitter Mark Burnett @m8urnett and his 10 million password dump
<http://wpengine.com/unmasked/>
- Systems exist which can try 135 billion MD5 hashes PER SECOND with 8 GPUs

Source: Catalin Ciampanu, Softpedia 15 September 2015

<http://news.softpedia.com/news/top-20-ashely-madison-passwords-491799.shtml>

Ransomware web ransomware



Tre Randomware familier rammer Danmark Ransomware, som rammer Danmark er groft fordelt i tre malware familier: Cryptowall, CTB-Locker og FileCoder. De spredes via to centrale metoder: spamkampagner med vedhæftede filer og ved brug af "drive-by"angreb.

Source: <https://www.csis.dk/da/csis/news/4676/>

Andre kilder:

The World Is Now Richer with 21 Million New Types of Malware, 230,000 Each Day

<http://news.softpedia.com/news/the-world-is-now-richer-with-21-million-new-types-of-malware-230-000-each-day-4915.shtml>



Most vulnerable operating systems in 2014

| Operating system | # of vulnerabilities | # of HIGH vulnerabilities | # of MEDIUM vulnerabilities | # of LOW vulnerabilities |
|-------------------------------|----------------------|---------------------------|-----------------------------|--------------------------|
| Apple Mac OS X | 147 | 64 | 67 | 16 |
| Apple iOS | 127 | 32 | 72 | 23 |
| Linux Kernel | 119 | 24 | 74 | 21 |
| Microsoft Windows Server 2008 | 38 | 26 | 12 | 0 |
| Microsoft Windows 7 | 36 | 25 | 11 | 0 |
| Microsoft Windows Server 2012 | 38 | 24 | 14 | 0 |
| Microsoft Windows 8 | 36 | 24 | 12 | 0 |
| Microsoft Windows 8.1 | 36 | 24 | 12 | 0 |
| Microsoft Windows Vista | 34 | 23 | 11 | 0 |
| Microsoft Windows RT | 30 | 22 | 8 | 0 |

An average of 19 vulnerabilities per day were reported in 2014, according to the data from the National Vulnerability Database (NVD).

Source:

<http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/>



Most vulnerable applications in 2014

| Application | # of vulnerabilities | # of HIGH vulnerabilities | # of MEDIUM vulnerabilities | # of LOW vulnerabilities |
|-----------------------------|----------------------|---------------------------|-----------------------------|--------------------------|
| Microsoft Internet Explorer | 242 | 220 | 22 | 0 |
| Google Chrome | 124 | 86 | 38 | 0 |
| Mozilla Firefox | 117 | 57 | 57 | 3 |
| Adobe Flash Player | 76 | 65 | 11 | 0 |
| Oracle Java | 104 | 50 | 46 | 8 |
| Mozilla Thunderbird | 66 | 36 | 29 | 1 |
| Mozilla Firefox ESR | 61 | 35 | 25 | 1 |
| Adobe Air | 45 | 38 | 7 | 0 |
| Apple TV | 86 | 29 | 49 | 8 |
| Adobe Reader | 44 | 37 | 7 | 0 |
| Adobe Acrobat | 43 | 35 | 8 | 0 |
| Mozilla SeaMonkey | 63 | 28 | 34 | 1 |

Not surprisingly at all, web browsers continue to have the most security vulnerabilities because they are a popular gateway to access a server and to spread malware on the clients.

Source:

<http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/>



Release of vuln information without patch

Google project Zero

Follow a "90-day disclosure deadline statement... which in this instance has passed."

Released Zero-day information about Microsoft and Apple OS X vulnerabilities

MS patched some in *first Patch Tuesday of 2015, which came out on Jan. 13.*

Sources:

<http://googleonlinesecurity.blogspot.fr/2014/07/announcing-project-zero.html>

<http://searchsecurity.techtarget.com/news/2240238448/Googles-Project-Zero-reveals-another-Windows-zero-day-vulnerability>

<http://www.engadget.com/2015/01/02/google-posts-unpatched-microsoft-bug/>

<http://www.eweek.com/security/google-project-zero-continues-its-microsoft-zero-day-assault.html>

[http://www.zdnet.com/article/googles-project-zero-reveals-three-apple-os-xzero-day-vulnerabilities/](http://www.zdnet.com/article/googles-project-zero-reveals-three-apple-os-x-zero-day-vulnerabilities/)

Trend with more vulnerabilities per day, and
even big vendors cannot react quickly enough



Samba remote code execution

```
=====
== Subject:      Unexpected code execution in smbd.
==
== CVE ID#:     CVE-2015-0240
==
== Versions:    Samba 3.5.0 to 4.2.0rc4
==
== Summary:     Unauthenticated code execution attack on
== smbd file services.
==
```

=====

Great, even our old tools still has multiple bugs

Source:

<https://www.samba.org/samba/security/CVE-2015-0240>

DNS attacks, February 2015 - ongoing for +10 years!



26 Webnic Registrar Blamed for Hijack of Lenovo, Google Domains

FEB 15



Two days ago, attackers allegedly associated with the fame-seeking group **Lizard Squad** briefly hijacked Google's Vietnam domain (google.com.vn). On Wednesday, **Lenovo.com** was similarly attacked. Sources now tell KrebsOnSecurity that both hijacks were possible because the attackers seized control over **Webnic.cc**, the Malaysian registrar that serves both domains and 600,000 others.

DNS insecurity has huge impact on your security!

Most are denial of service, by may create Mitm or confidentiality concerns

Select DNS providers with care

Sources:

<https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/>

<http://www.version2.dk/artikel/google-og-lenovo-defaced-som-foelge-af-overset-sikkerhedsproblemstilling-91295>



Example, Using tools similar to PacketQ

Using PacketQ

Let's have a practical look at how PacketQ works by trying to figure out what kind of DNS ANY queries are being sent towards our name-server.

DNS ANY traffic is currently commonly abused for DNS amplification attacks (See Blog post "[DDoS-Angriffe durch Reflektierende DNS-Amplifikation vermeiden](#)" in German). The first thing I want to know is what are the IP addresses of the victims of this potential DNS amplification attack:

```
packetq -t -s "select src_addr,count(*) as count from dns where qtype=255 group  
by src_addr order by count desc limit 3" lolo.20130118.070000.000179  
"src_addr" , "count"  
"216.245.221.243" , 933825  
"85.126.233.70" , 16802  
"80.74.130.55" , 91
```

Are you using your brain and existing tools? Building own specialised tools?
Discussion: bridging the gaps between Devops and Security? Good thing, easy?

<http://securityblog.switch.ch/2013/01/22/using-packetq/>

<http://jpmens.net/2013/05/27/server-agnostic-logging-of-dns-queries-responses/>



Storing query logs, old school or needed?

- [policy/protocols/ssl/expiring-certs.bro](#)
- [policy/protocols/ssl/extract-certs-pem.bro](#)
- [policy/protocols/ssl/heartbleed.bro](#)
- [policy/protocols/ssl/known-certs.bro](#)
- [policy/protocols/ssl/log-hostcerts-only.bro](#)
- [policy/protocols/ssl/validate-certs.bro](#)
- [policy/protocols/ssl/validate-ocsp.bro](#)
- [policy/protocols/ssl/weak-keys.bro](#)

Looking at DNS PacketQ it was an Older link, but thinking the time is now for doing:

- DNS query logs, keep it for at least a week? - with DSC and PacketQ

- SSL/TLS full logs over sessions, certs, keys - with Bro/Suricata

<https://www.bro.org/sphinx-git/script-reference/scripts.html>

- Log and search with Elasticsearch?

<https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html>

- Even netflow session logging, full 1:1 - NFSen, Suricata Flow mode?



February 2015: Finding infected sources

"We were contacted by a client to help with their incident response in tracking down an infection on a clients machine with the new CTB-Locker ransomware (Curve-Tor-Bitcoin Locker) aka Critroni which had no signatures available at the time of infection for this variant.

LANGuardian includes a file share activity monitoring module which provided a very detailed forensic analysis of the ransomware and the paths it had taken in order to encrypt the clients system and also the fileserver in which it was connected to, the initial infection came from the opening of an attachment in an e-mail."

It has become critical to identify vulnerable or infected ASAP!

Source: <https://www.netfort.com/support-team-stories-detecting-the-source-of-ransomware/>

Dont forget Suricata <http://suricata-ids.org/> **and Security Onion**
<https://github.com/Security-Onion-Solutions/security-onion/wiki/Installation>

Kibana 4



Highly recommended for a lot of data visualisation

Non-programmers can create, save, and share dashboards

Source: <https://www.elastic.co/products/kibana>

DDoS in 2015



Survey Peak Attack Size Year Over Year

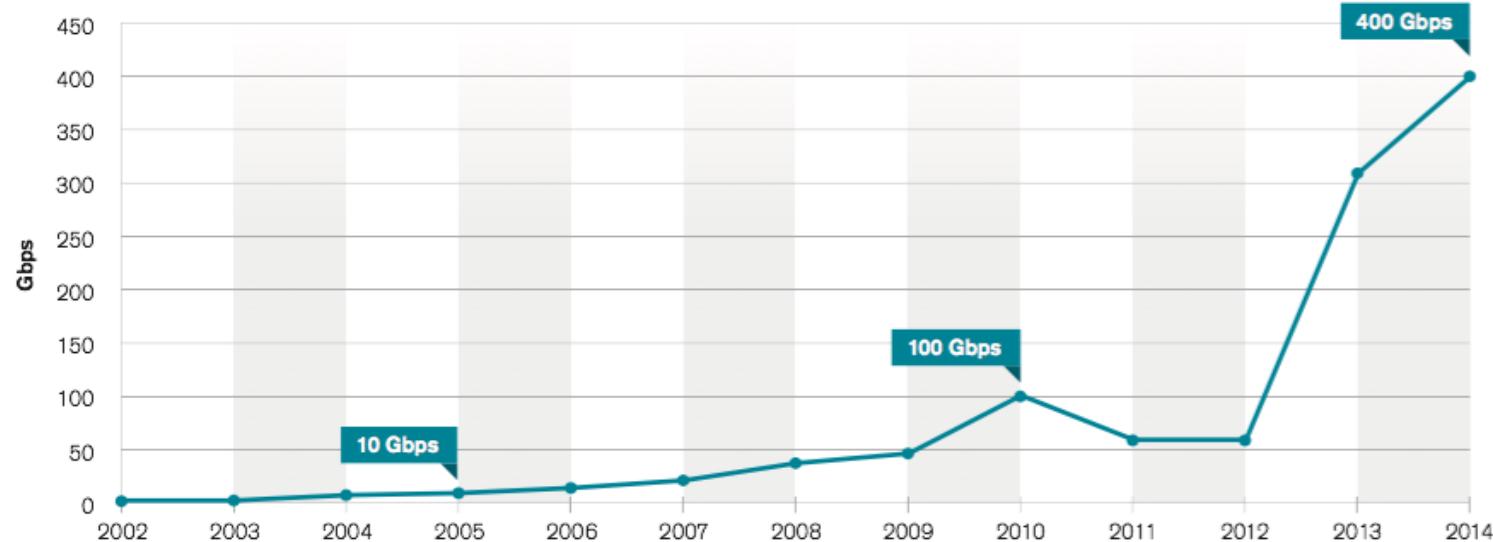


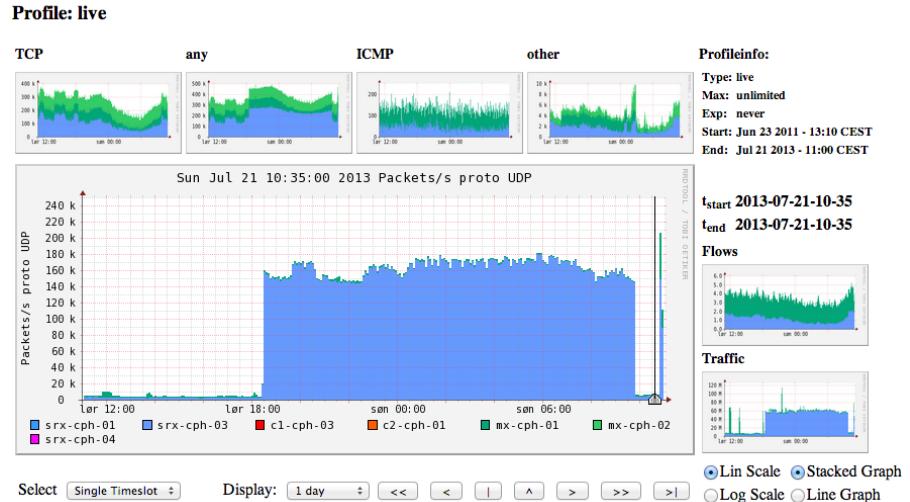
Figure 12 Source: Arbor Networks, Inc.

Expect amplification attacks and 3-digit attacks for some years

Source:

Arbor Networks: Worldwide Infrastructure Security Report, Volume X January 2015

Brug hackerværktøjer!



An extra 100k packets per second from this netflow source (source is a router)

Hackerværktøjer – bruger I dem? – efter dette kursus gør I

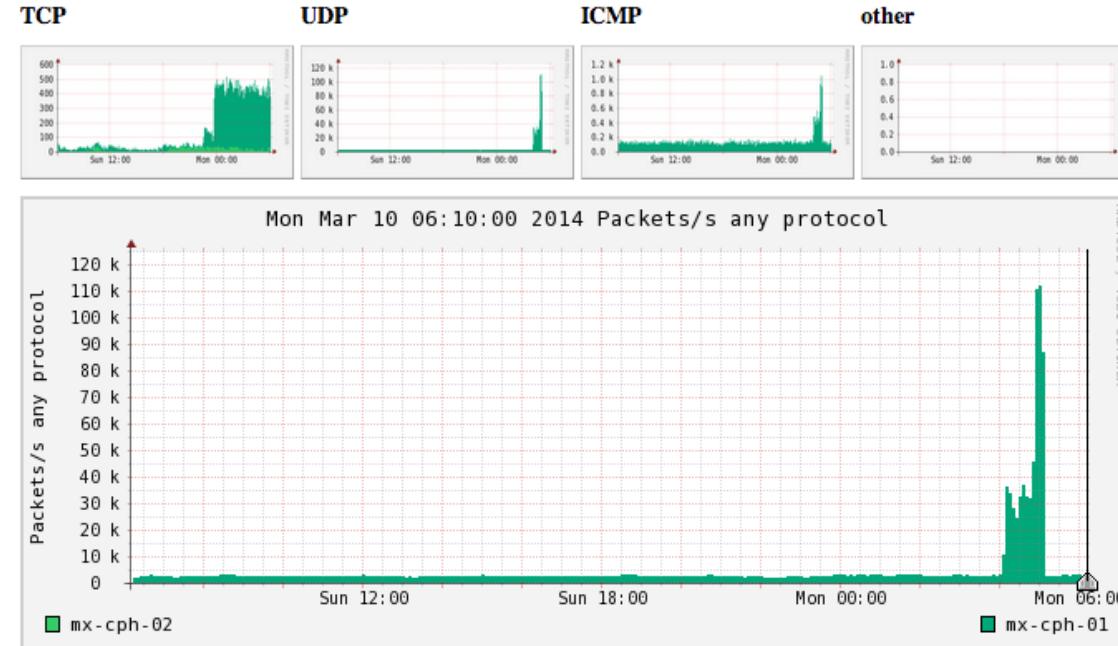
Portscannere kan afsløre huller i forsvaret

I vil kunne finde mange potentielle problemer proaktivt ved regelmæssig brug

Detecting DDoS example tool Nfsen



Profile: DDoS

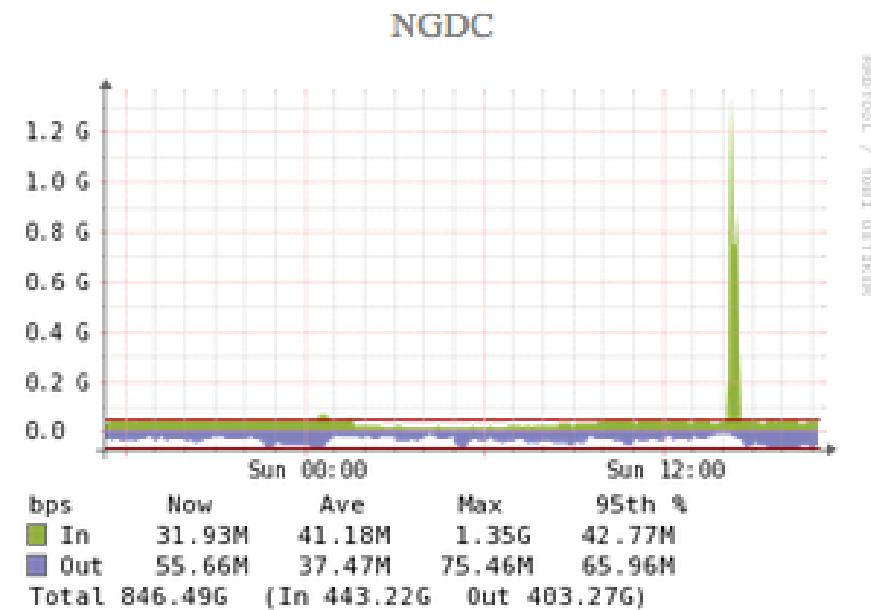
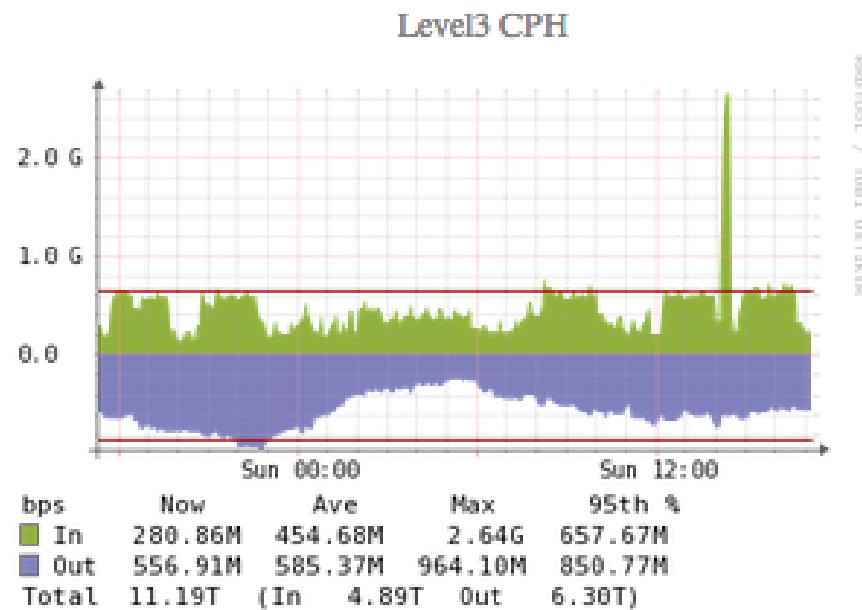


We created a DDoS profile with the common types.

We can ask RRDtools about max, average etc.

```
rrdtool graph x -s -24h DEF:v=DDoS/mx-cph-01.rrd:packets:MAX  
VDEF:vm=v,MAXIMUM PRINT:vm:%.1f
```

DDoS traffic before filtering



Only two links shown, at least 3Gbit incoming for this single IP



DDoS traffic after filtering



Link toward server (next level firewall actually) about 350Mbit outgoing

Problem: We receive unauthenticated chaotic traffic

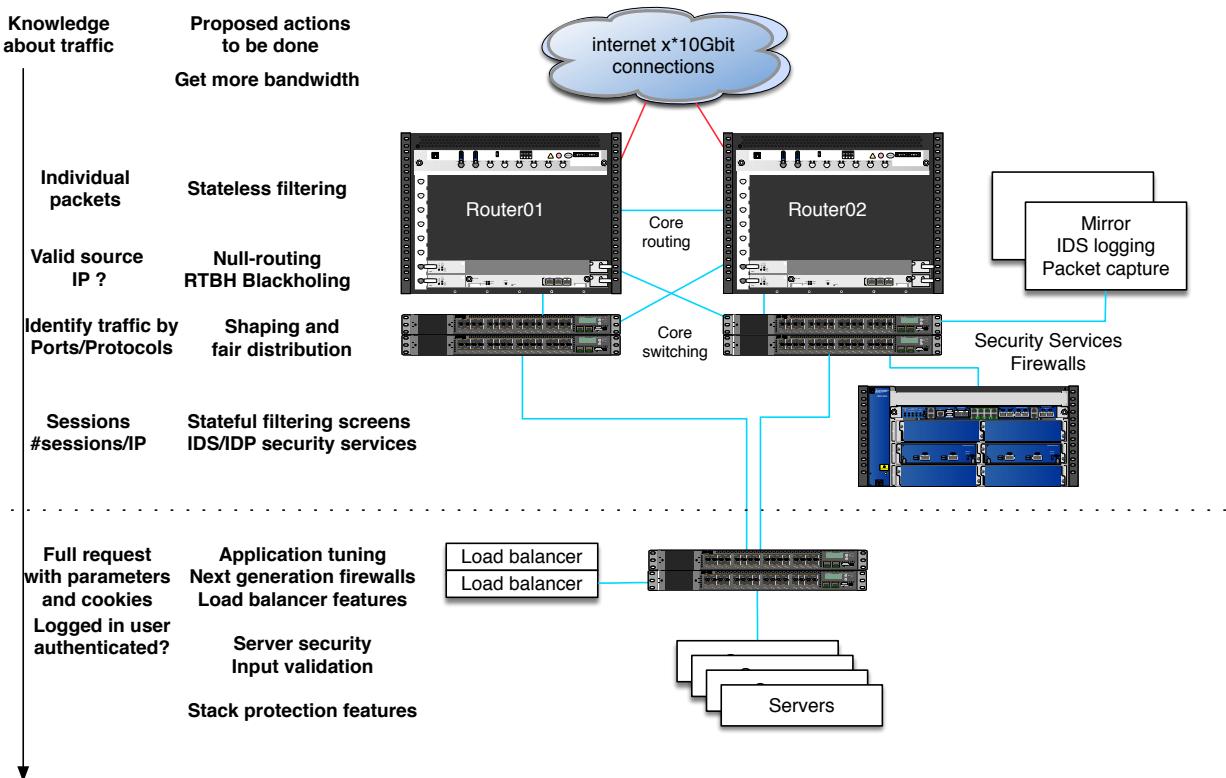
Solution: Discard early, discard on edge, reduce noise

Only use CPU resources for potentially real traffic

Single firewall layer typically cannot cope!



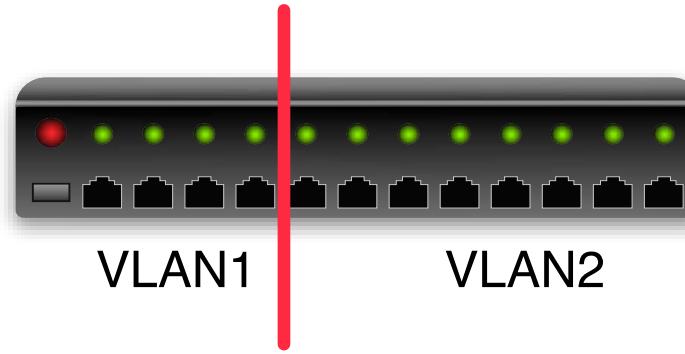
Defense in depth - multiple layers of security



VLAN Virtual LAN



Portbased VLAN



Nogle switcher tillader at man opdeler portene

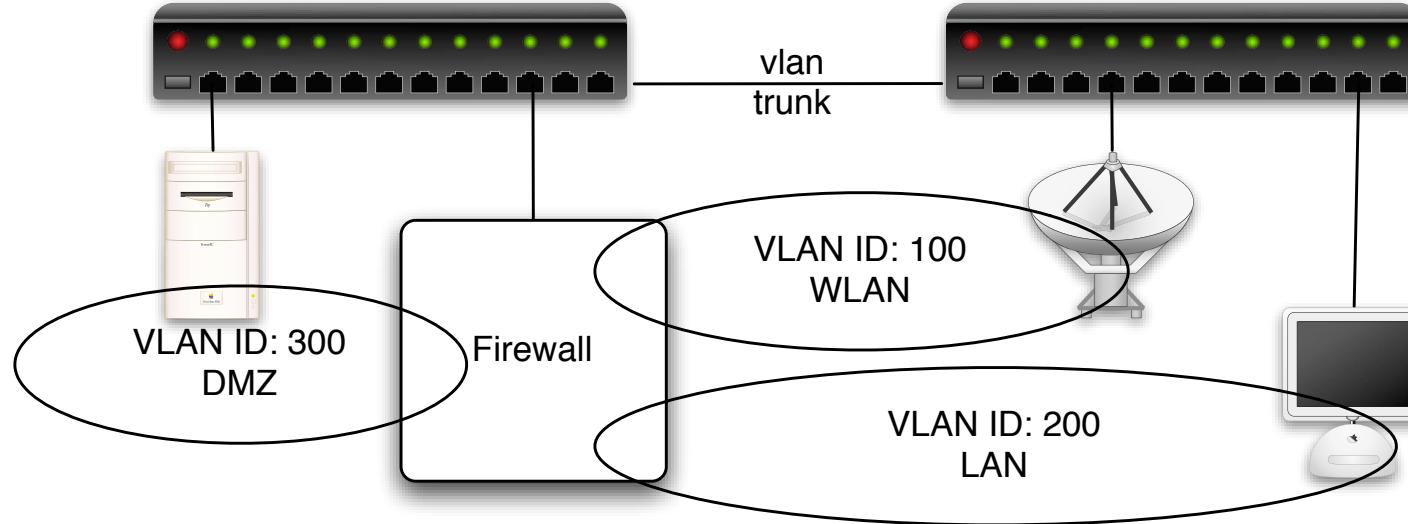
Denne opdeling kaldes VLAN og portbaseret er det mest simple

Port 1-4 er et LAN

De resterende er et andet LAN

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

IEEE 802.1q



Nogle switcher tillader konfiguration med 802.1q VLAN tagging på Ethernet niveau

Data skal omkring en firewall eller en router for at krydse fra VLAN1 til VLAN2

VLAN trunking giver mulighed for at dele VLANs ud på flere switches

Der findes administrativ værktøjer der letter dette arbejde:

Prøv evt. openNAC, FreeNAC, Cisco VMPS

Focus for the near future



- Walk through your infrastructure
get a detailed view of data, flows, protocols, bandwidth, ports and services
- Create a list of critical phone numbers and contacts, enter it in your phone
- Automate updates for both clients and servers, goal update everything in hours
- Learn to run Nmap and Metasploit scripts - identify vulnerable servers

consider the fact we have multiple overlapping critical security incidents now!

How many incidents can your organisation handle in parallel?

Can multiple people in your organisation initiate updates?

Sceneskift - Hacking er magi



Hacking ligner indimellem magi

Hacking er ikke magi



Hacking kræver blot lidt ninja-træning



Movie:Kryptonite lock - old

YouTube DK ▾



1:57 / 2:28

How To Unlock a Kryptonite Lock With a Bic Pen

Just search for: kryptonite lock bic pen

<https://www.youtube.com/watch?v=LahDQ2ZQ3e0>



Hacking eksempel - det er ikke magi

MAC filtrering på trådløse netværk

Alle netkort har en MAC adresse - BRÆNDT ind i kortet fra fabrikken

Mange trådløse Access Points kan filtrere MAC adresser

Kun kort som er på listen over godkendte adresser tillades adgang til netværket ■

Det virker dog ikke ☺

De fleste netkort tillader at man overskriver denne adresse midlertidigt

Derudover har der ofte været fejl i implementeringen af MAC filtrering

MAC filtrering





Hvad skal der ske?

Tænk som en hacker

Rekognoscering

- ping sweep, port scan
- OS detection – TCP/IP eller banner grab
- Servicescan – rpcinfo, netbios, ...
- telnet/netcat interaktion med services

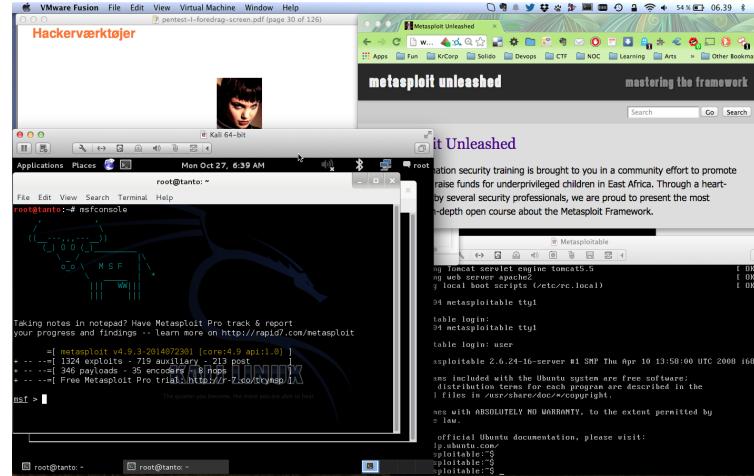
Udnyttelse/afprøvning: Metasploit, Nikto, exploit programs

Oprydning/hærdning vises måske ikke, men I bør i praksis:

- Lav en rapport
- Ændre, forbedre og hærde systemer
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

I skal jo også VISE andre at I gør noget ved sikkerheden.

Hackerlab opsætning



- Hardware: en moderne laptop med CPU der kan bruge virtualisering
Husk at slå virtualisering til i BIOS
- Software: dit favoritoperativsystem, Windows, Mac, Linux
- Virtualiseringssoftware: VMware, Virtual box, vælg selv
- Hackersoftware: Kali som Virtual Machine <https://www.kali.org/>
- Soft targets: Metasploitable, Windows 2000, Windows XP, ...



Hackerværktøjer



- Alle bruger nogenlunde de samme værktøjer, se også <http://www.sectools.org/>
- Portscanner Nmap, Nping – tester porte, godt til firewall admins <https://nmap.org>
- Generel sårbarhedsscanner Metasploit Framework [https://www.metasploit.com/](https://www.metasploit.com)
- Specialscannere, eksempelvis web sårbarhedsscanner – eksempelvis Nikto, Skipfish
- Specielle scannere – wifi Aircrack-ng, web Burpsuite <http://portswigger.net/burp/>
- Wireshark avanceret netværkssniffer – <https://www.wireshark.org/>
- og scripting, PowerShell, Unix shell, Perl, Python, Ruby, ...

Billedet: Angelina Jolie fra Hackers 1995

Kali Linux the new backtrack



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 ?](#)

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

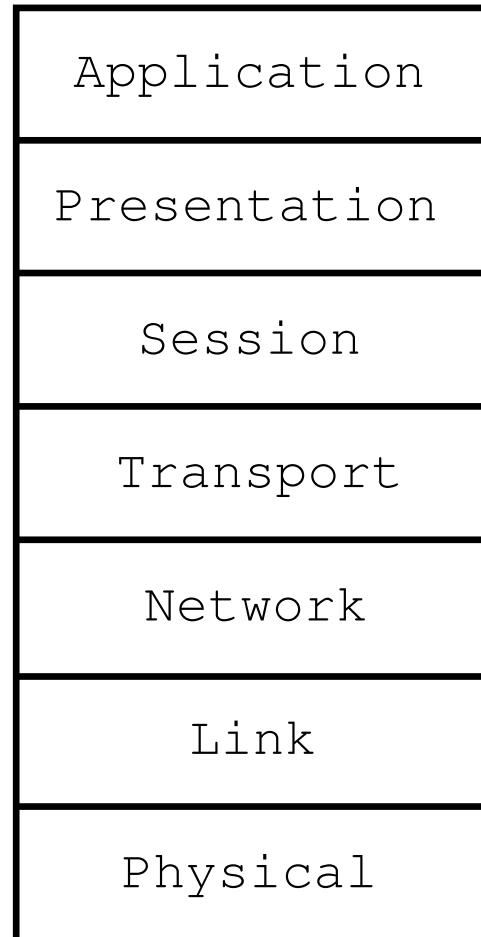
Kali – <https://www.kali.org/> version 2.0 netop udkommet!

Wireshark – <https://www.wireshark.org> avanceret netværkssniffer

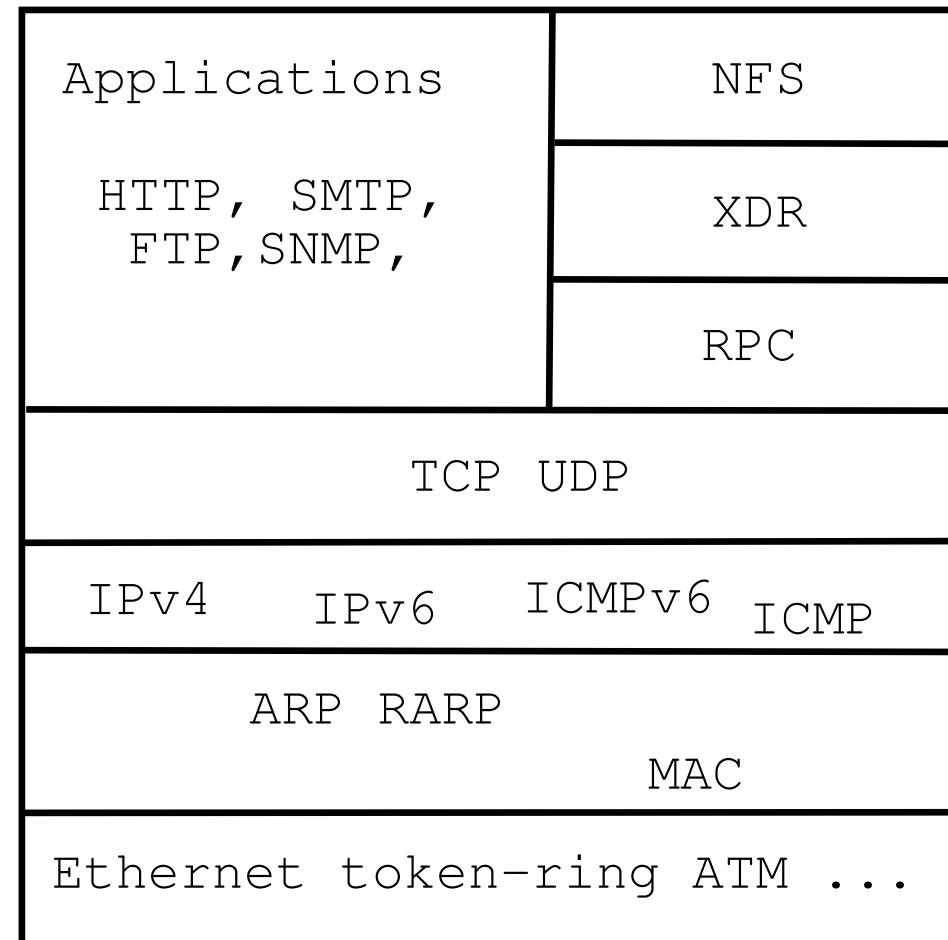
OSI og Internet modellerne



OSI Reference
Model



Internet protocol suite



Wireshark - grafisk pakkesniffer



WIRESHARK

Get Acquainted ▾ Get Help ▾ Develop ▾

Sharkfest '15 Our Sponsor WinPcap

We're having a conference! You're invited!

Download
Get Started Now

Learn
Knowledge is Power

Enhance
With Riverbed Technology

News And Events

Join us at SHARKFEST '15!
SHARKFEST '15 will be held from June 22 – 25 at the Computer History Museum in Mountain View, CA.
[Learn More ▶](#)

Troubleshooting with Wireshark
By Laura Chappell
Foreword by Gerald Combs
Edited by Jim Aragon
This book focuses on the tips and techniques used to identify

Wireshark Blog

Cool New Stuff
Dec 17 | By Evan Huus

Wireshark 1.12 Officially Released!
Jul 31 | By Evan Huus

To Infinity and Beyond! Capturing Forever with Tshark
Jul 8 | By Evan Huus

[More Blog Entries ▶](#)

Enhance Wireshark

Riverbed is Wireshark's primary sponsor and provides our funding. [They also make great products.](#)

802.11 Packet Capture

- WLAN packet capture and transmission
- Full 802.11 a/b/g/n support
- View management, control and data frames
- Multi-channel aggregation (with multiple adapters)

[Learn More ▶](#)

[Buy Now ▶](#)

<http://www.wireshark.org>

både til Windows og UNIX

Wireshark usage



The screenshot shows a Wireshark window with the following details:

- Packets:** 9
- Displayed:** 9
- Marked:** 0
- Load time:** 0:0:0
- Profile:** Default

Protocol Column Headers: No, Time, Source, Destination, Protocol, Info

Selected Packet (Frame 7):

```
GET / HTTP/1.1
Host: 91.102.91.18
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.146 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8,cs;q=0.6,da;q=0.4
If-None-Match: "7053a63e31516a58b27a295edb31d07524a6e0a3"
If-Modified-Since: Tue, 17 Nov 2009 11:22:22 GMT
\

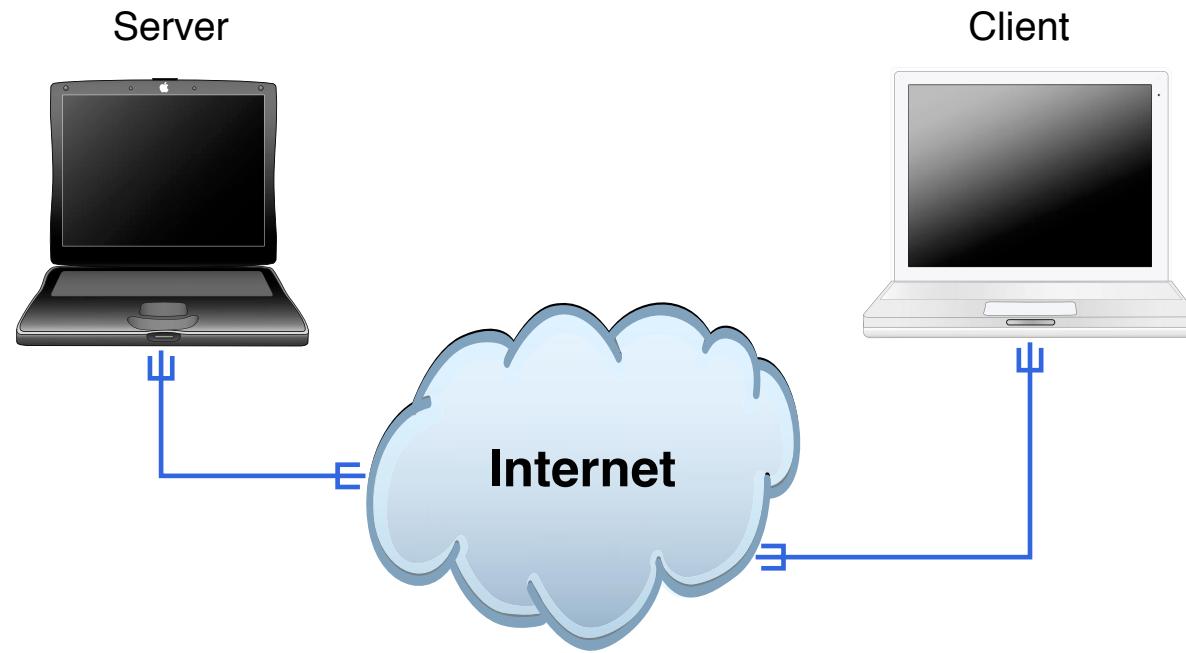
[Full request URI: http://91.102.91.18/]
[HTTP request 1/1]
[Response in frame: 8]
```

Hex and ASCII Data:

```
0000  44 2a 03 32 09 30 7c d1 c3 6c 87 5e 08 00 45 00 D+2.0[N Ál.^..E.
0010  02 2a 9e d7 40 00 40 06 f5 ff ac 18 41 66 5b 66 .*.x@.öý-.Aff
0020  5b 12 e5 c0 00 50 08 ea 0e c7 03 14 0c 19 08 18 [,.åP.é .ç.....
0030  28 2b 0f c0 00 00 01 01 08 0a 2c 79 61 aa 6e 94 +.Ä.... .,paøn.
0040  b7 27 47 45 54 20 2f 48 54 54 50 2f 31 2e 31 .'GET / HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20 39 31 2e 31 30 32 2e 39 ..Host: 91.102.9
0060  31 2a 31 38 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 1.18..Co nnection
0070  3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 : keep-a live.Ca
0080  62 68 65 2d 43 6f 6e 74 72 6f 6c 3a 29 6d 61 78 che-Cont rol: max
0090  2d 61 67 65 3d 30 0d 0a 41 63 63 65 70 74 3a 20 -age=0.. Accept:
00a0  74 65 78 74 2f 68 74 6d 6c 2c 61 70 6c 69 63 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
00b0  61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c
00c0  61 70 78 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b application/x-javascript
```

Wireshark: Filters, hexdump, protocol dissection, overview, coloring, advanced features

Demo: Wireshark



Wireshark

The Exploit Database – dagens buffer overflow



EXPL0IT
D a t a b a s e

Currently Archiving
10343
Exploits

[home] [news] [remote] [local] [web] [dos] [shellcode] [papers] [search] [D] [submit]
[rss]

The Exploit Database

The ultimate archive of exploits and vulnerable software - A great resource for vulnerability researchers and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

We are running a general cleanup on the DB and have changed our submission policy - please [check it out](#) before submitting exploits to us.

Due to recent DOS attacks, our application downloads are now captcha protected.

Remote Exploits

| Date | D | A | V | Description | Plat. | Author |
|------------|---|---|---|---|----------|-----------------|
| 2010-01-27 | D | A | ✓ | CamShot v1.2 SEH Overwrite Exploit | windows | technik |
| 2010-01-25 | D | - | ✓ | AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta) | windows | Trancer |
| 2010-01-22 | D | A | ✓ | IntelliTamper 2.07/2.08 (SEH) Remote Buffer Overflow | windows | loneferret |
| 2010-01-21 | D | - | ✓ | EFS Easy Chat server Universal BOF-SEH (Meta) | windows | FB1H2S |
| 2010-01-20 | D | - | ✓ | AOL 9.5 ActiveX Oday Exploit (heap spray) | windows | Dz_attacker |
| 2010-01-19 | D | - | ✓ | Pidgin MSN <= 2.6.4 File Download Vulnerability | multiple | Mathieu GASPARD |
| 2010-01-18 | D | A | ✓ | Exploit EFS Software Easy Chat Server v2.2 | windows | John Babio |

<http://www.exploit-db.com/>

Heartbleed CVE-2014-0160



The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.



Source: <http://heartbleed.com/>

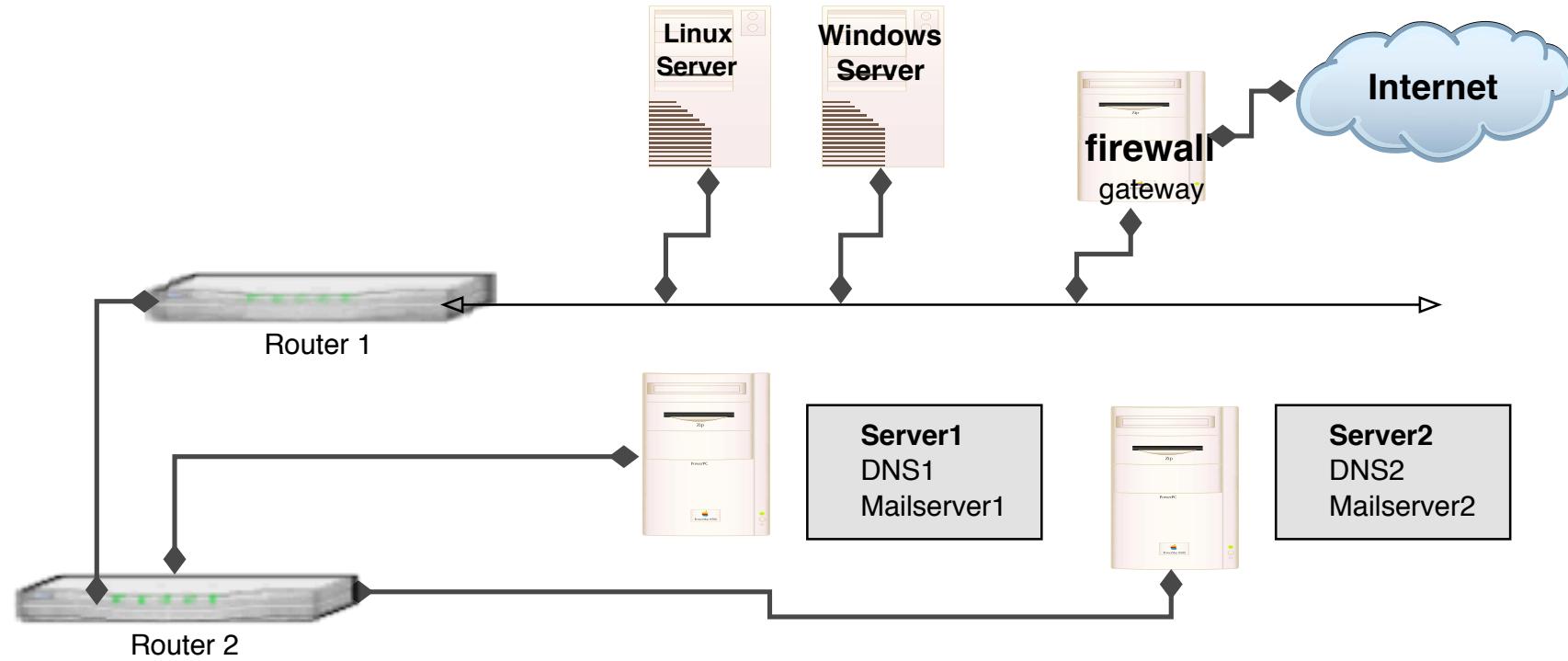


Heartbleed hacking

```
06b0: 2D 63 61 63 68 65 0D 0A 43 61 63 68 65 2D 43 6F -cache..Cache-Co
06c0: 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D ntrol: no-cache.
06d0: 0A 0D 0A 61 63 74 69 6F 6E 3D 67 63 5F 69 6E 73 ...action=gc_in
06e0: 65 72 74 5F 6F 72 64 65 72 26 62 69 6C 6C 6E 6F ert_order&billno
06f0: 3D 50 5A 4B 31 31 30 31 26 70 61 79 6D 65 6E 74 =PZK1101&payment
0700: 5F 69 64 3D 31 26 63 61 72 64 5F 6E 75 6D 62 65 _id=1& card'numbe
0710: XX r=4060xxxx413xxx
0720: 39 36 26 63 61 72 64 5F 65 78 70 5F 6D 6F 6E 74 96&card'exp'mont
0730: 68 3D 30 32 26 63 61 72 64 5F 65 78 70 5F 79 65 h=02&card'exp'ye
0740: 61 72 3D 31 37 26 63 61 72 64 5F 63 76 6E 3D 31 ar=17&card'cvn=1
0750: 30 39 F8 6C 1B E5 72 CA 61 4D 06 4E B3 54 BC DA 09.l...r.aM.N.T..
```

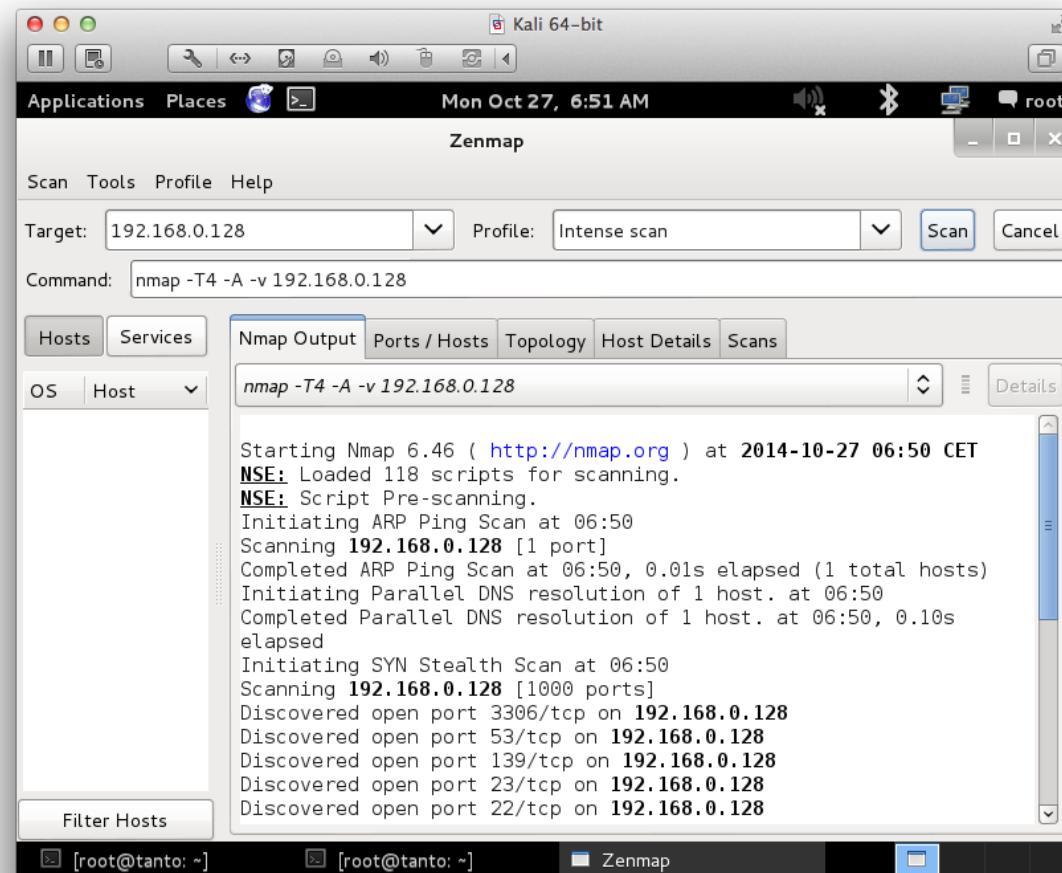
- Obtained using Heartbleed proof of concepts - Gave full credit card details
- "can XXX be exploited- yes, clearly! PoCs ARE needed without PoCs even Akamai wouldn't have repaired completely!
- https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/ssl/openssl_heartbleed.rb

Network mapping



Ved brug af traceroute og tilsvarende programmer kan man ofte udlede topologien i det netværk man undersøger

Portscan med Zenmap GUI





Scan for Heartbleed and SSLv2/SSLv3

Example Usage

```
nmap -sV -sC <target>
```

Script Output

```
443/tcp open  https  syn-ack
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
```

```
nmap -p 443 --script ssl-heartbleed <target>
https://nmap.org/nsedoc/scripts/ssl-heartbleed.html
```

```
masscan 0.0.0.0/0 -p0-65535 --heartbleed
https://github.com/robertdavidgraham/masscan
```

Almost every new vulnerability will have Nmap recipe

Cracking 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/>

Parallella John



Henrik Kramshøj retweeted

Solar Designer @solardiz

Similarly expensive Xeon E5-2670 is 2.4x to 3.3x slower than Zynq 7045 #FPGA on this test, yet consumes ~20x more power; GPUs are way behind

Henrik Kramshøj retweeted

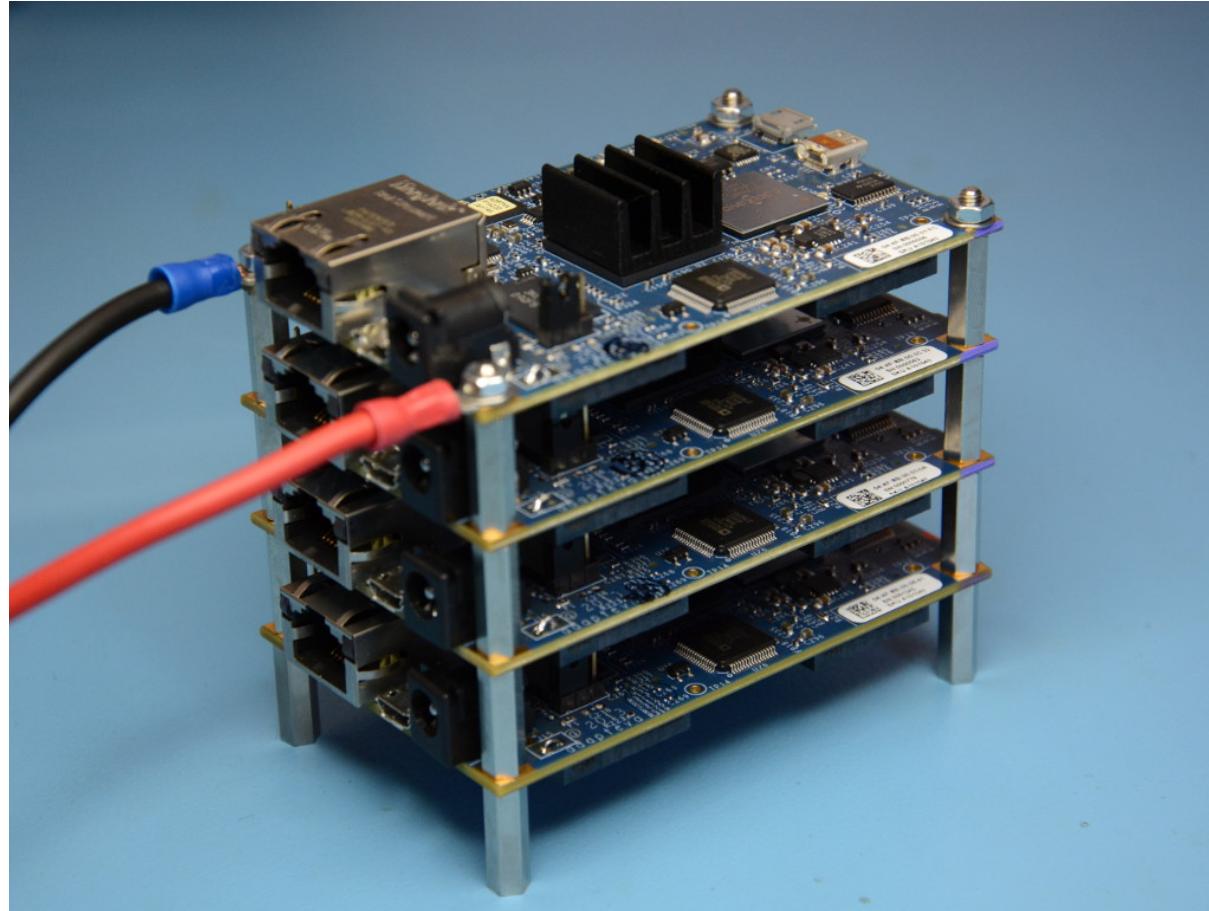
Solar Designer @solardiz

On last night to submit WOOT final paper, @kmalvoni got bcrypt \$2a\$05 to 20538 c/s, \$2a\$12 to 226 c/s on Zynq 7045 #FPGA. Not the limit yet.

<https://twitter.com/solardiz/status/492037995080712192>

Warning: FPGA hacking - not finished part of presentation

Stacking Parallelia boards



<http://www.parallelia.org/power-supply/>

Kali øvelser



Vi kan ikke nå alverden men prøv selv at gentage det jeg viste hjemme

- Wireshark
- Wireshark med FTP
- Nmap med Zenmap
- Armitage og Metasploit, husk service postgresql start

Security devops



We need devops skillz in security

automate, security is also big data

integrate tools, transfer, sort, search, pattern matching, statistics, ...

tools, languages, databases, protocols, data formats

Example introductions:

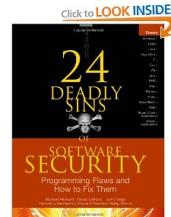
- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide
<http://www.elasticsearch.org/guide/en/elasticsearch/guide/current/index.html>
- <http://www.elasticsearch.org/overview/kibana/>
- <http://www.elasticsearch.org/overview/logstash/>

We are all Devops now, even security people!

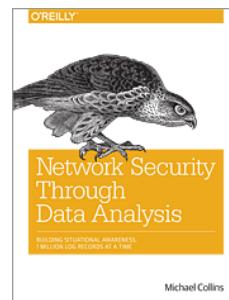


Recommended Books: Get Started

24 Deadly Sins of Software Security Michael Howard, David LeBlanc, John Viega 2. udgave, første hed 19 Deadly Sins



Network Security Through Data Analysis: Building Situational Awareness
By Michael Collins, O'Reilly Media, February 2014 Pages: 348 Low page count, but high value! Recommended.



Join Camps



Chaos Communication Camp 2015 It was Awesome!

Source Wikipedia and <https://www.flickr.com/photos/schwarzbrot/20447504269/>

Questions?



Henrik Lund Kramshøj hlk@zencurity.dk

Need DDoS testing or pentest, ask me!

You are always welcome to send me questions later via email

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