Welcome to

Hacking today

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

`http://www.solidonetworks.com`

Formålet med foredraget

Don’t Panic!

Skabe forståelse for hackerværktøjer samt penetrationstest metoder

Hacker - cracker

Det korte svar - drop diskussionen

Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig - og idag har det begge betydninger.

Idag er en hacker stadig en der bryder ind i systemer!

ref. Spafford, Cheswick, Garfinkel, Stoll, ... - alle kendte navne indenfor sikkerhed

Hvis man vil vide mere kan man starte med:

- *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Clifford Stoll
- *Hackers: Heroes of the Computer Revolution*, Steven Levy
- *Practical Unix and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz

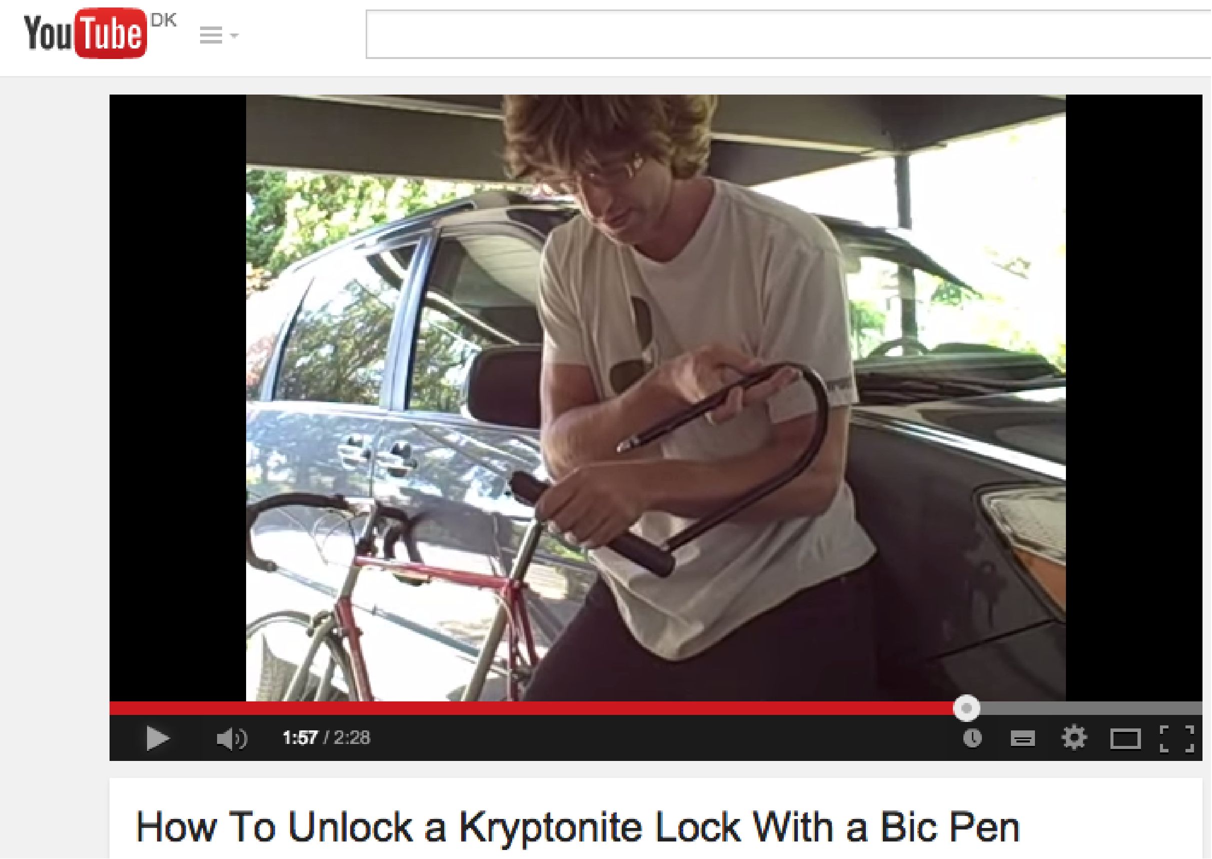
Hacking er magi

Hacking ligner indimellem magi

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

Movie:Kryptonite lock - old



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

Myten om MAC filtrering

Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing - producenterne sætter store mærkater på æskerne

Manglende indsigt - forbrugerne kender reelt ikke koncepterne

Hvad *er* en MAC adresse egentlig

Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

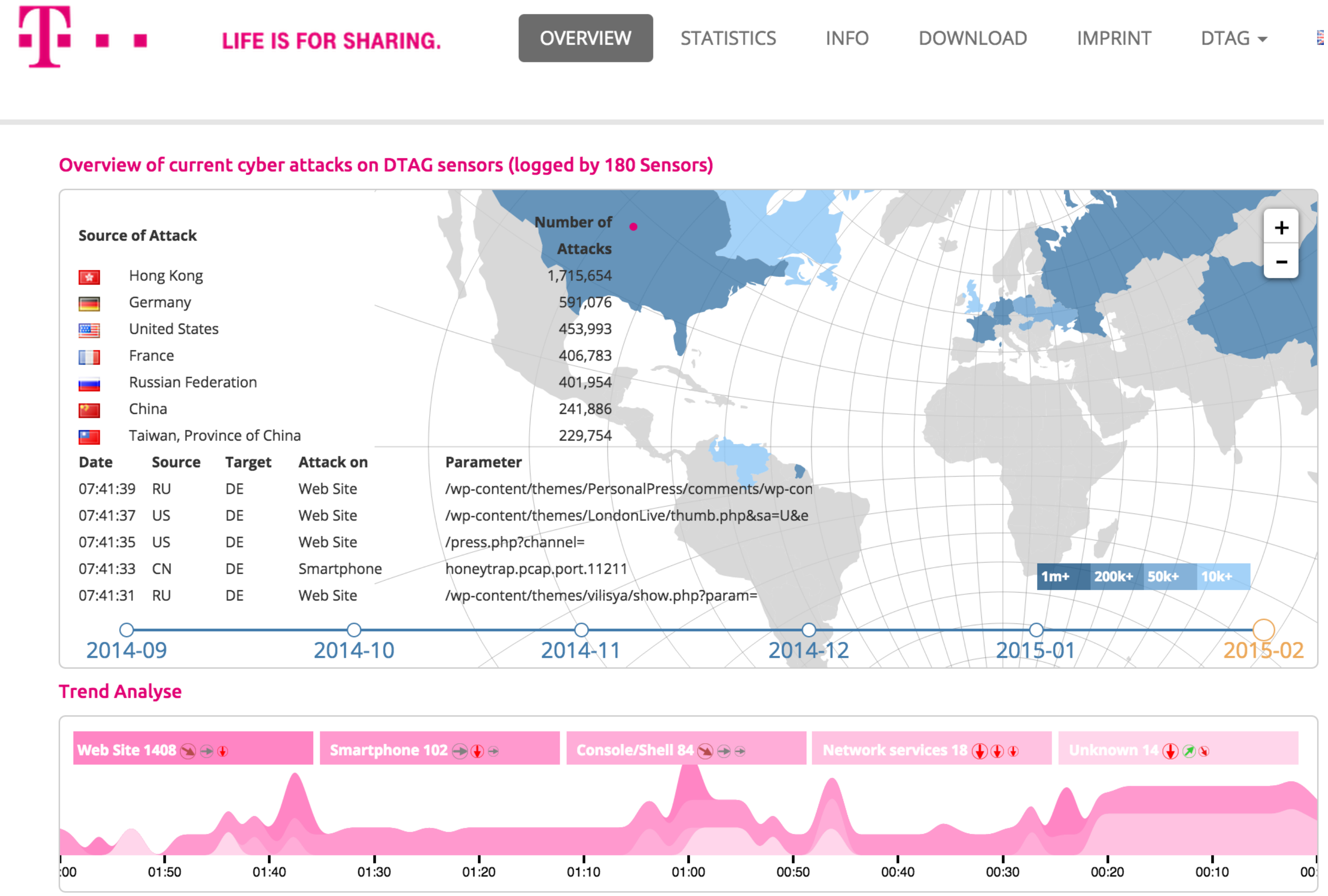
Løsninger?

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

MAC filtrering

Attack overview



Overview of current cyber attacks on DTAG sensors (logged by 180 Sensors)

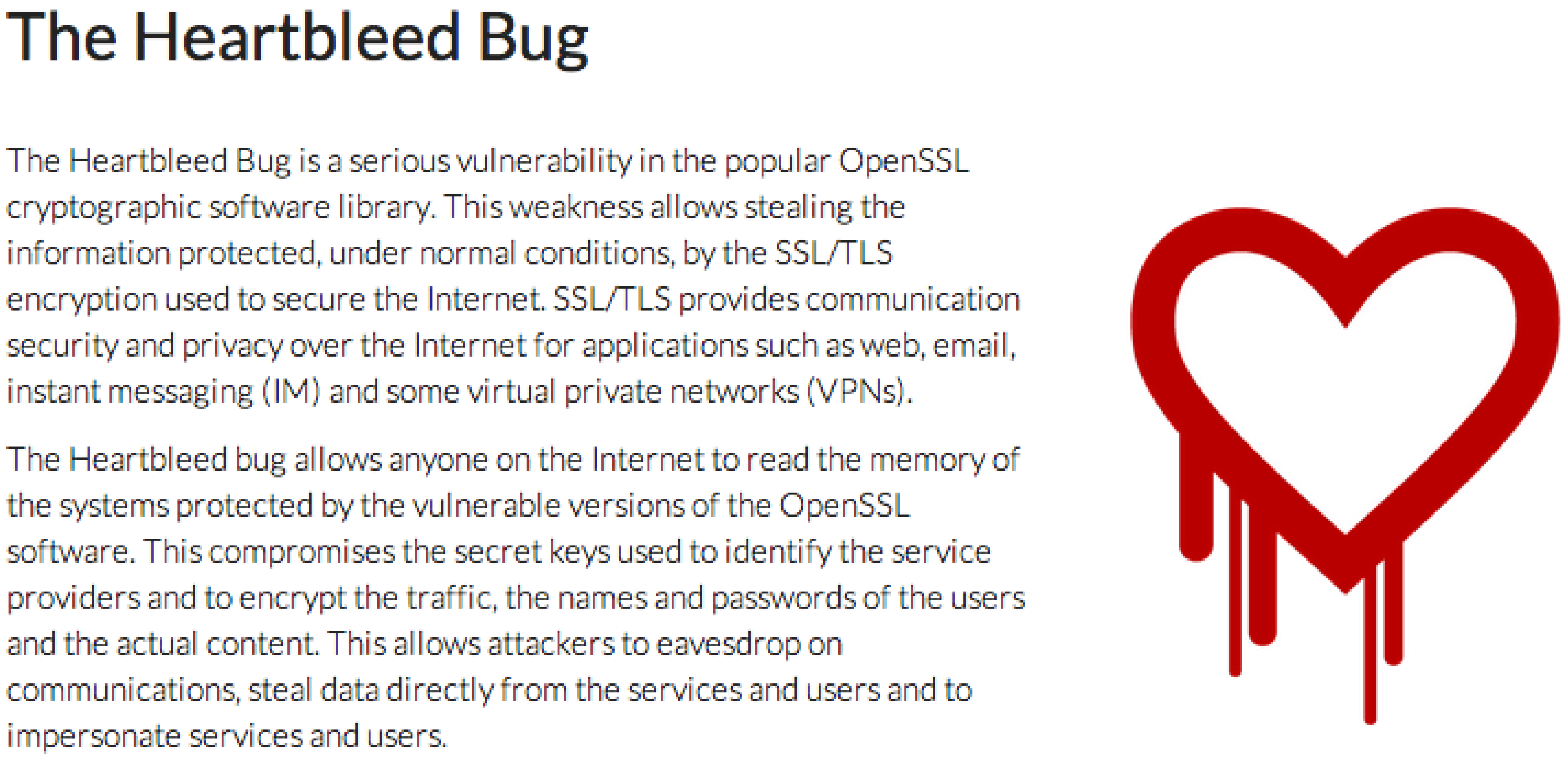
Source of Attack	Number of Attacks
Hong Kong	1,715,654
Germany	591,076
United States	453,993
France	406,783
Russian Federation	401,954
China	241,886
Taiwan, Province of China	229,754

Date	Source	Target	Attack on	Parameter
07:41:39	RU	DE	Web Site	/wp-content/themes/PersonalPress/comments/wp-con
07:41:37	US	DE	Web Site	/wp-content/themes/LondonLive/thumb.php&sa=U&e
07:41:35	US	DE	Web Site	/press.php?channel=
07:41:33	CN	DE	Smartphone	honeytrap.pcap.port.11211
07:41:31	RU	DE	Web Site	/wp-content/themes/vilisya/show.php?param=

Trend Analyse

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

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.

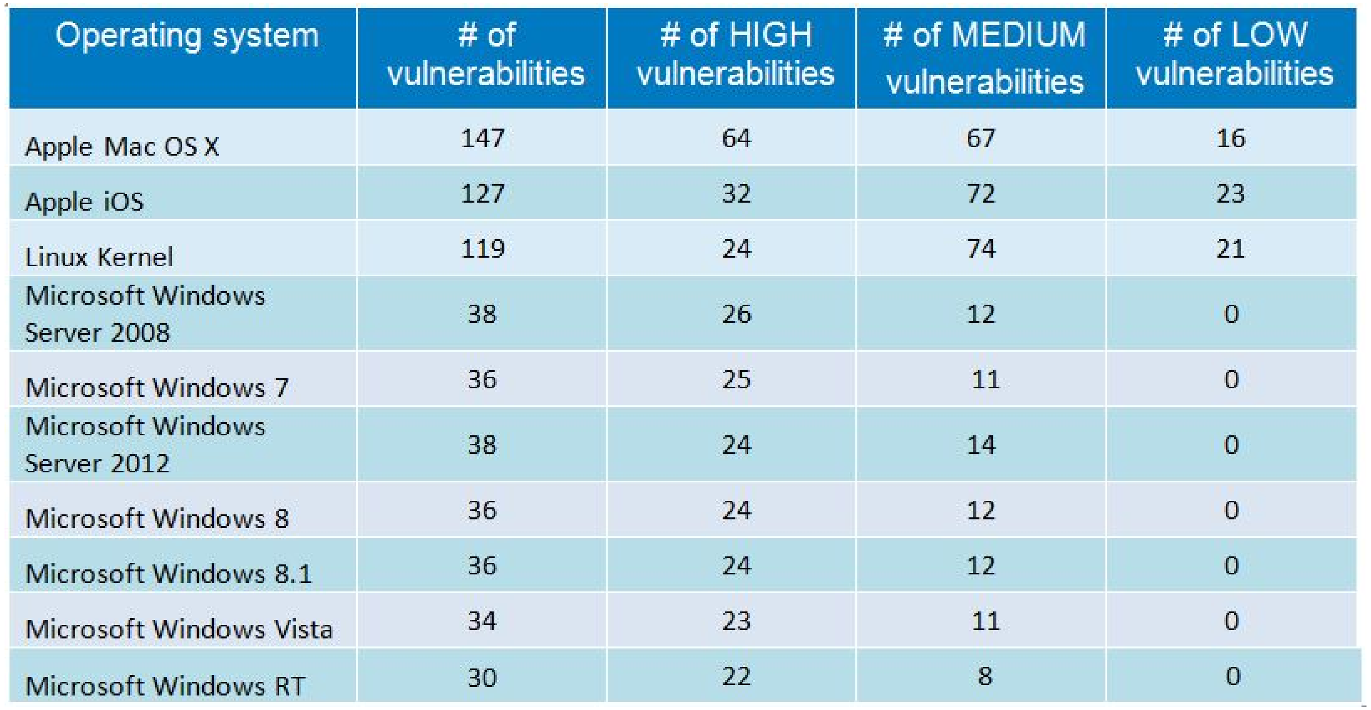
Source: `http://heartbleed.com/`

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_ins
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 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 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!
- The internet was ALMOST fooled into thinking getting private keys from Heartbleed was not possible - scary indeed.

Most vulnerable operating systems in 2014



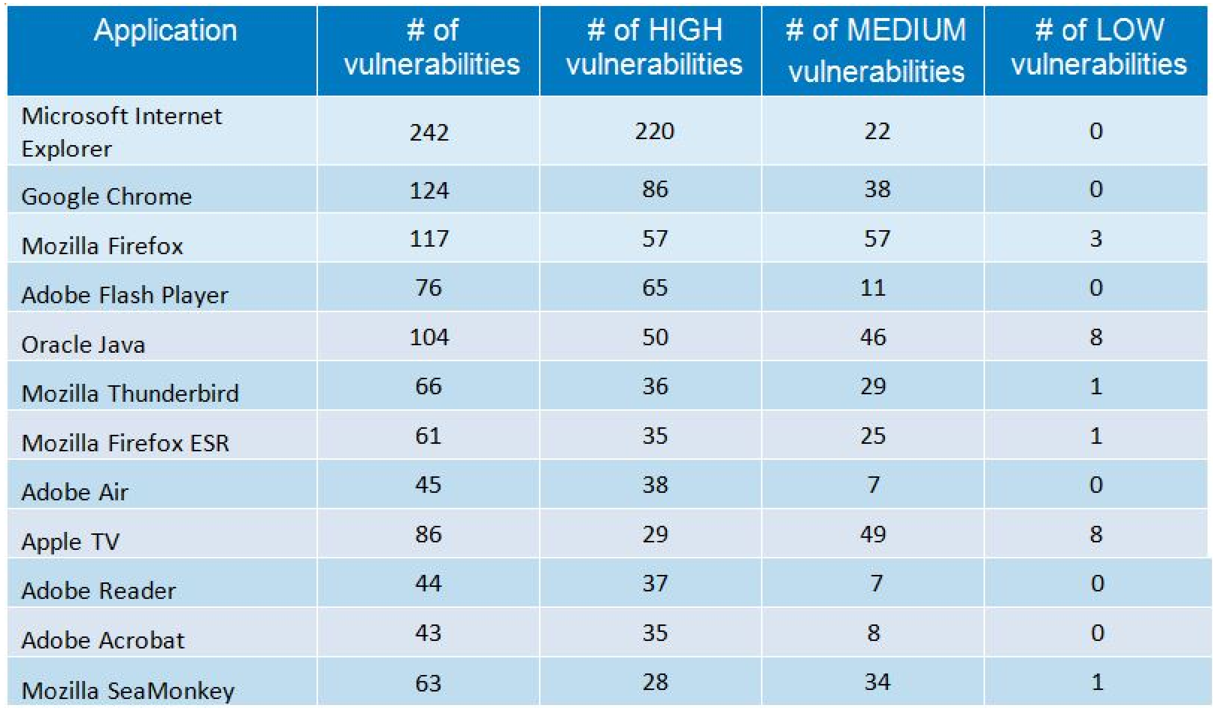
Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	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:

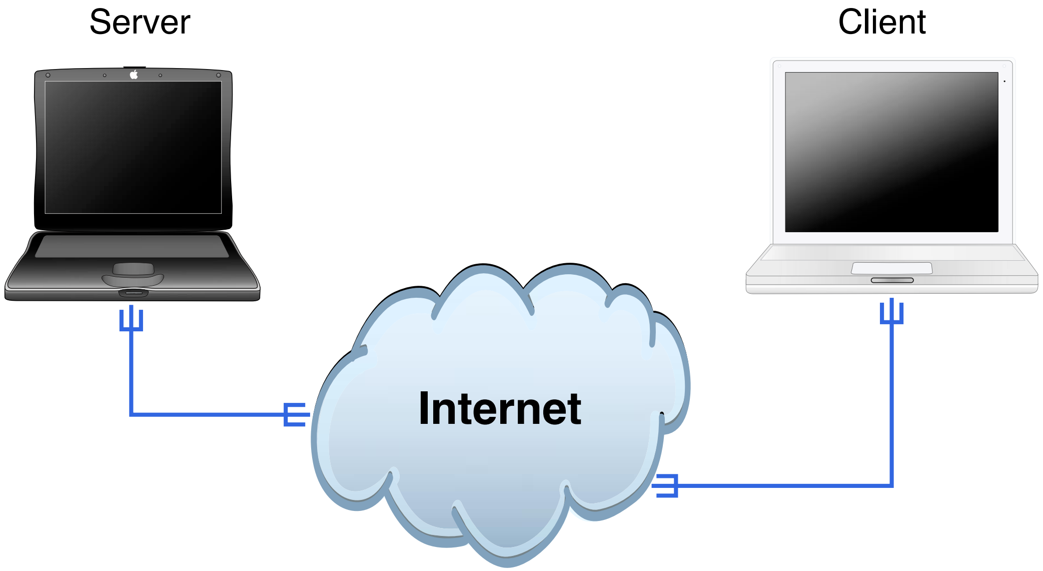
`http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/`

Hackerværktøjer

Der benyttes en del værktøjer:

- Nmap - `http://www.insecure.org` portscanner
- Wireshark - `http://http://www.wireshark.org/` avanceret netværkssniffer
- OpenBSD - `http://www.openbsd.org` operativsystem med fokus på sikkerhed
- Kali Linux `http://www.kali.org/`

Internet idag



Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

Meget lidt kryptering, mest på http til brug ved e-handel

Internet er åbne standarder!

We reject kings, presidents, and voting.
We believe in rough consensus and running code.
– The IETF credo Dave Clark, 1992.

Request for comments - RFC - er en serie af dokumenter

RFC, BCP, FYI, informational
de første stammer tilbage fra 1969

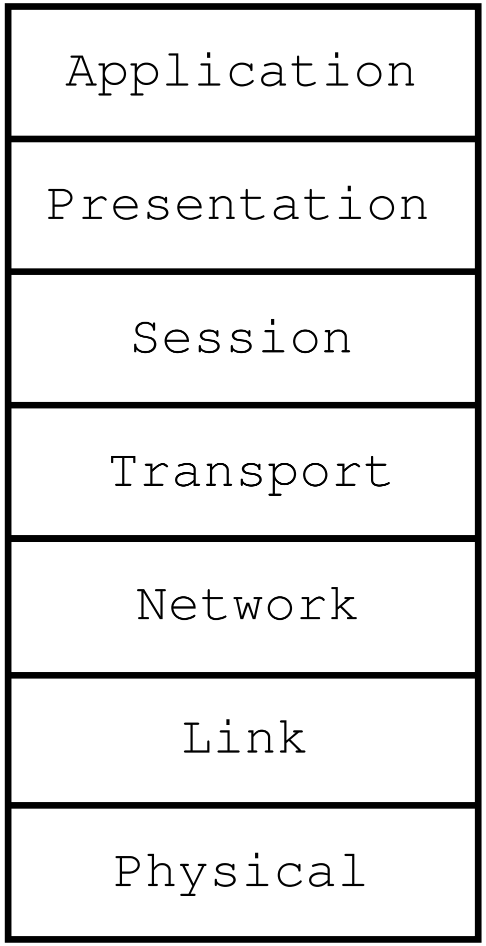
ændres ikke, men får status Obsoleted når der udkommer en nyere version af en standard

Standards track:
Proposed Standard → Draft Standard → Standard

åbne standarder = åbenhed, ikke garanti for sikkerhed

OSI og Internet modellerne

OSI Reference Model



Application

Presentation

Session

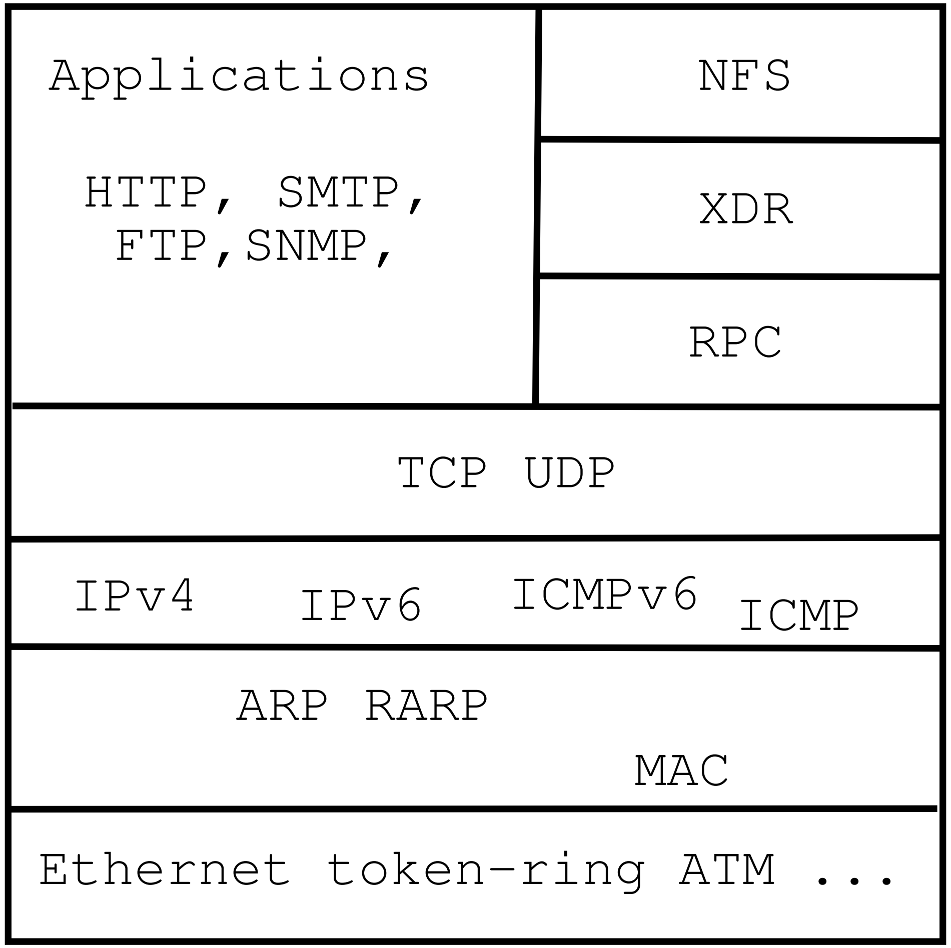
Transport

Network

Link

Physical

Internet protocol suite



Applications

HTTP, SMTP, FTP, SNMP,

NFS

XDR

RPC

TCP UDP

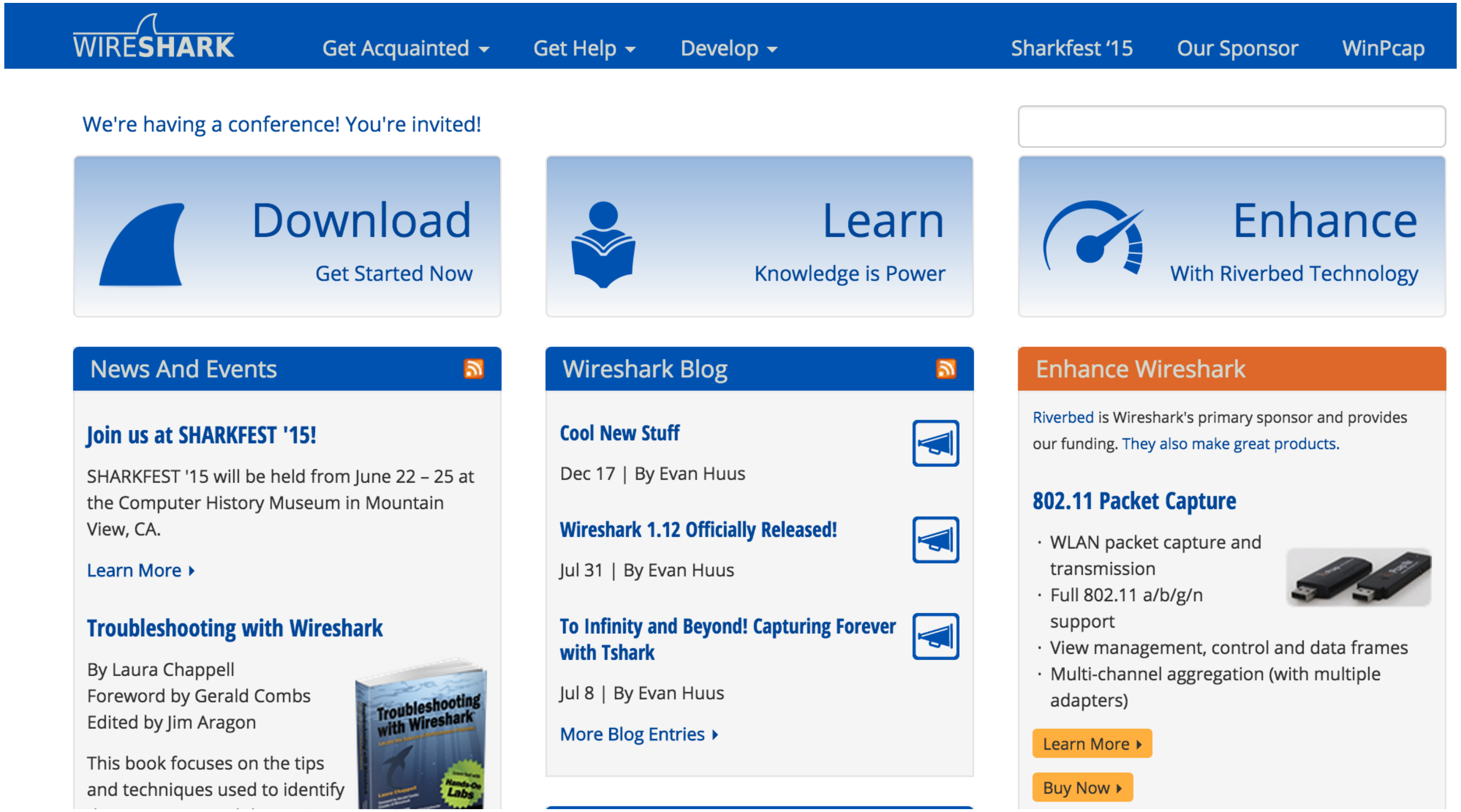
IPv4 IPv6 ICMPv6 ICMP

ARP RARP

MAC

Ethernet token-ring ATM ...

Wireshark - grafisk pakkesniffer



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

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)

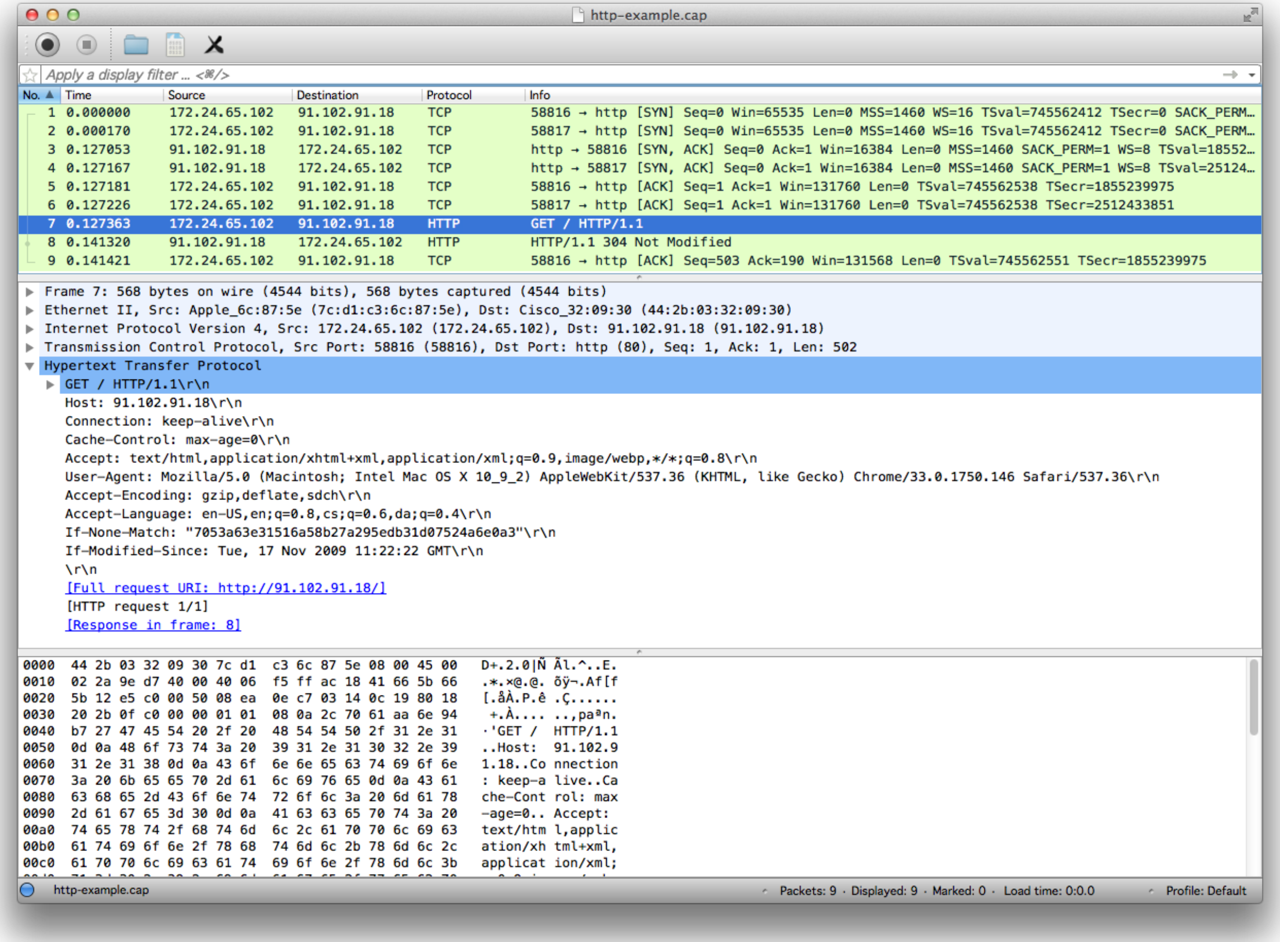
Learn More ▸

Buy Now ▸

`http://www.wireshark.org`

både til Windows og UNIX

Wireshark usage



```
No. ▲ Time      Source         Destination    Protocol  Info
  1 0.000000    172.24.65.102  91.102.91.18   TCP       58816 → http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=745562412 TSecr=0 SACK_PERM…
  2 0.000170    172.24.65.102  91.102.91.18   TCP       58817 → http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=745562412 TSecr=0 SACK_PERM…
  3 0.127053    91.102.91.18   172.24.65.102  TCP       http → 58816 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TSval=18552…
  4 0.127167    91.102.91.18   172.24.65.102  TCP       http → 58817 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TSval=25124…
  5 0.127181    172.24.65.102  91.102.91.18   TCP       58816 → http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=745562538 TSecr=1855239975
  6 0.127226    172.24.65.102  91.102.91.18   TCP       58817 → http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=745562538 TSecr=2512433851
  7 0.127363    172.24.65.102  91.102.91.18   HTTP      GET / HTTP/1.1
  8 0.141320    91.102.91.18   172.24.65.102  HTTP      HTTP/1.1 304 Not Modified
  9 0.141421    172.24.65.102  91.102.91.18   TCP       58816 → http [ACK] Seq=503 Ack=190 Win=131568 Len=0 TSval=745562551 TSecr=1855239975
```

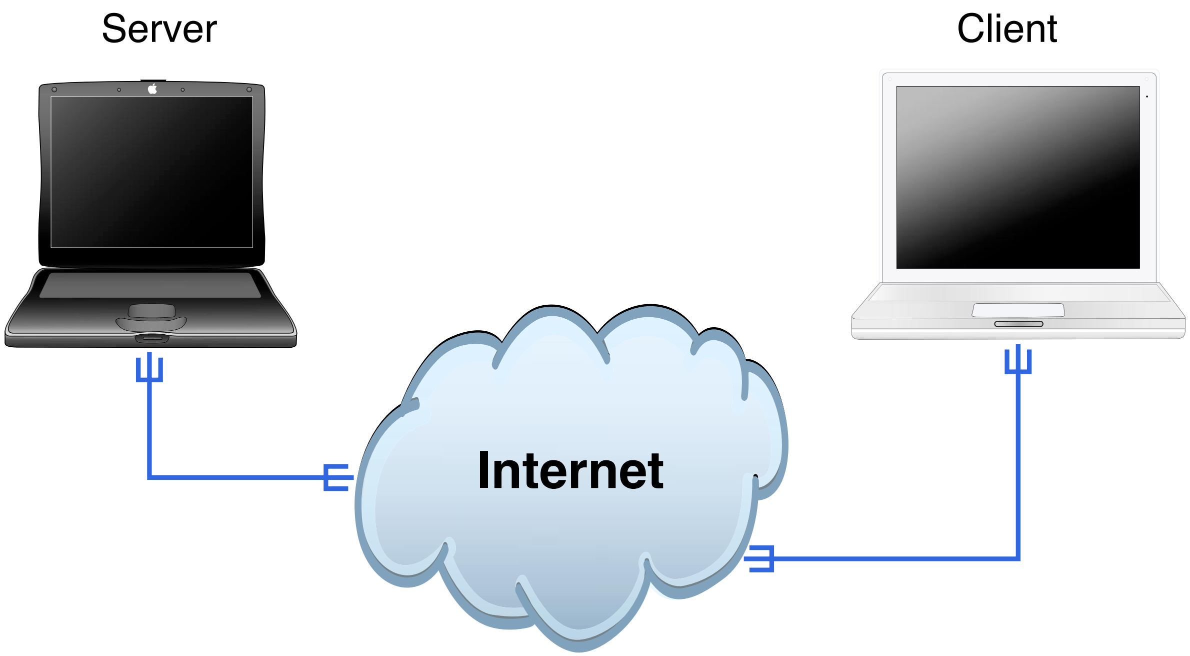
```
▶ Frame 7: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits)
▶ Ethernet II, Src: Apple_6c:87:5e (7c:d1:c3:6c:87:5e), Dst: Cisco_32:09:30 (44:2b:03:32:09:30)
▶ Internet Protocol Version 4, Src: 172.24.65.102 (172.24.65.102), Dst: 91.102.91.18 (91.102.91.18)
▶ Transmission Control Protocol, Src Port: 58816 (58816), Dst Port: http (80), Seq: 1, Ack: 1, Len: 502
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: 91.102.91.18\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    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\r\n
    Accept-Encoding: gzip,deflate,sdch\r\n
    Accept-Language: en-US,en;q=0.8,cs;q=0.6,da;q=0.4\r\n
    If-None-Match: "7053a63e31516a58b27a295edb31d07524a6e0a3"\r\n
    If-Modified-Since: Tue, 17 Nov 2009 11:22:22 GMT\r\n
    \r\n
    [Full request URI: http://91.102.91.18/]
    [HTTP request 1/1]
    [Response in frame: 8]
```

```
0000  44 2b 03 32 09 30 7c d1  c3 6c 87 5e 08 00 45 00   D+.2.0|Ñ Ãl.^..E.
0010  02 2a 9e d7 40 00 40 06  f5 ff ac 18 41 66 5b 66   .*.×@.@. õÿ¬.Af[f
0020  5b 12 e5 c0 00 50 08 ea  0e c7 03 14 0c 19 80 18   [.åÀ.P.ê .Ç......
0030  20 2b 0f c0 00 00 01 01  08 0a 2c 70 61 aa 6e 94    +.À.... ..,paªn.
0040  b7 27 47 45 54 20 2f 20  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 2e 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  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 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 70 6c 69 63   text/htm l,applic
00b0  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
00c0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
```

```
http-example.cap          Packets: 9 · Displayed: 9 · Marked: 0 · Load time: 0:0.0          Profile: Default
```

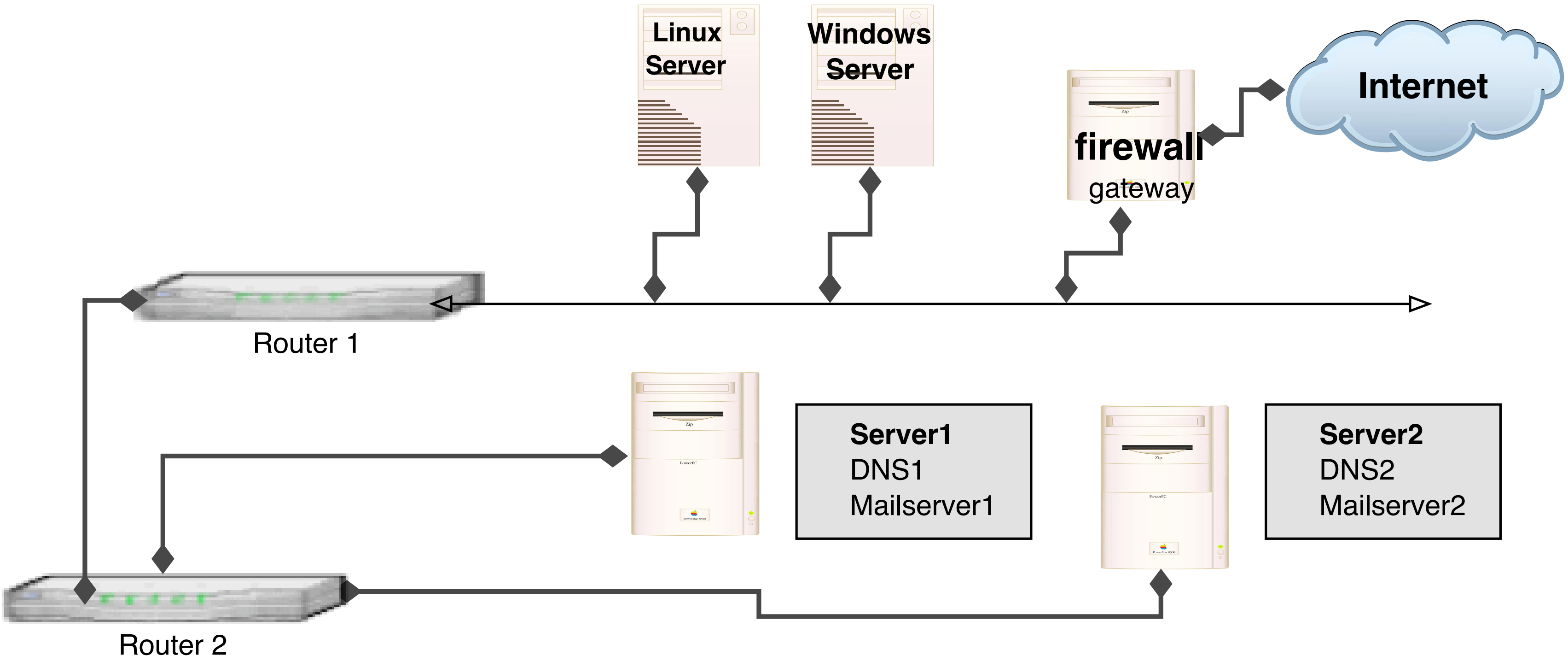
Wireshark: Filters, hexdump, protocol dissection, overview, coloring, advanced features

Demo: Wireshark



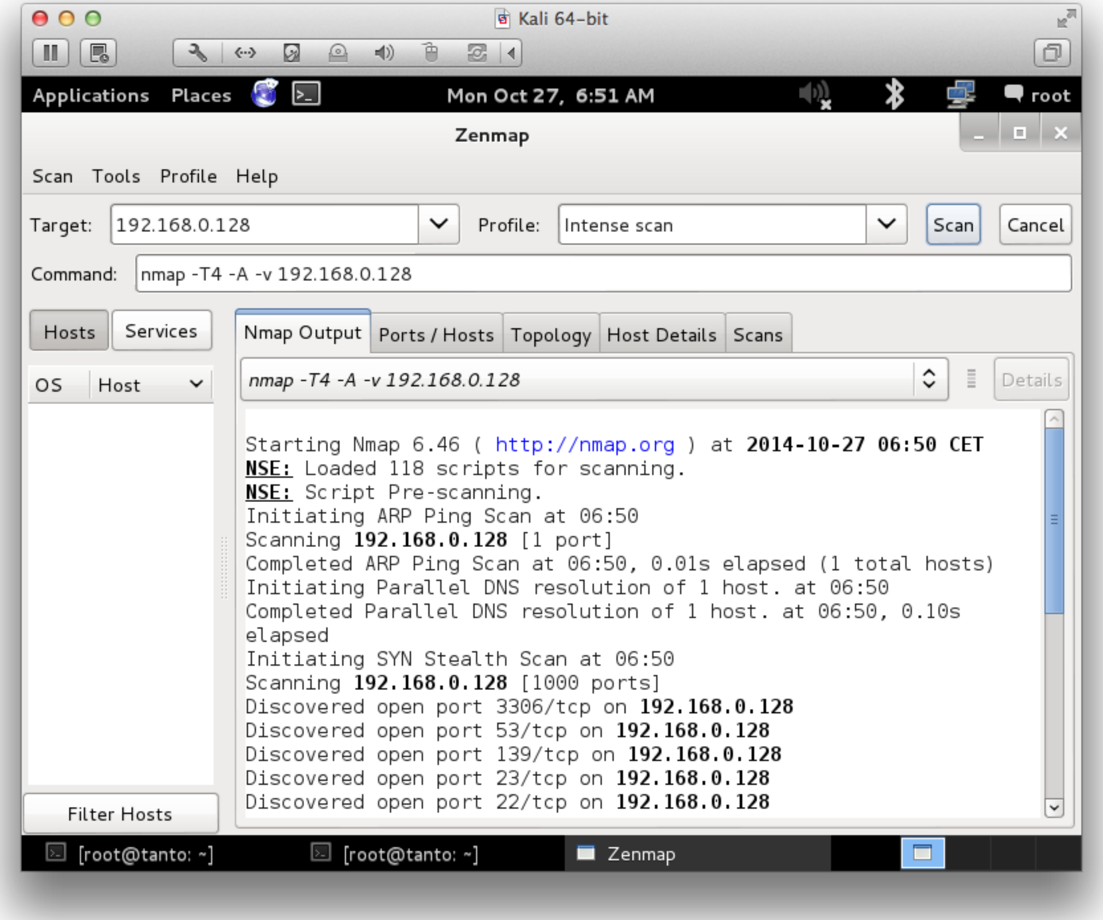
Wireshark

Network mapping



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

Portscan med Zenmap GUI



Target: 192.168.0.128

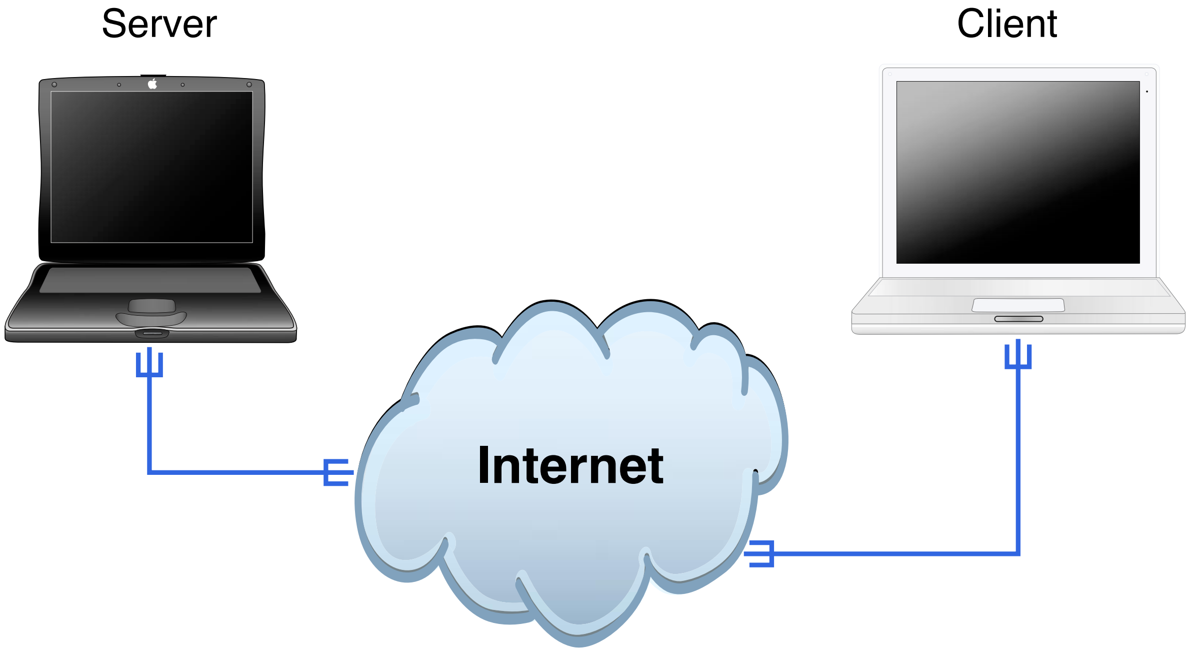
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.128

```
nmap -T4 -A -v 192.168.0.128

Starting Nmap 6.46 ( http://nmap.org ) at 2014-10-27 06:50 CET
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 06:50
Scanning 192.168.0.128 [1 port]
Completed ARP Ping Scan at 06:50, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:50
Completed Parallel DNS resolution of 1 host. at 06:50, 0.10s
elapsed
Initiating SYN Stealth Scan at 06:50
Scanning 192.168.0.128 [1000 ports]
Discovered open port 3306/tcp on 192.168.0.128
Discovered open port 53/tcp on 192.168.0.128
Discovered open port 139/tcp on 192.168.0.128
Discovered open port 23/tcp on 192.168.0.128
Discovered open port 22/tcp on 192.168.0.128
```

Demo: Armitage og Metasploit



Armitage og Metasploit

FREAK March 2015

> ”A group of cryptographers at INRIA, Microsoft Research and IMDEA have discovered some serious vulnerabilities in OpenSSL (e.g., Android) clients and Apple TLS/SSL clients (e.g., Safari) that allow a ’man in the middle attacker’ to downgrade connections from ’strong’ RSA to ’export-grade’ RSA. These attacks are real and exploitable against a shocking number of websites – including government websites. Patch soon and be careful.”

Source: Matthew Green, cryptographer and research professor at Johns Hopkins Univ

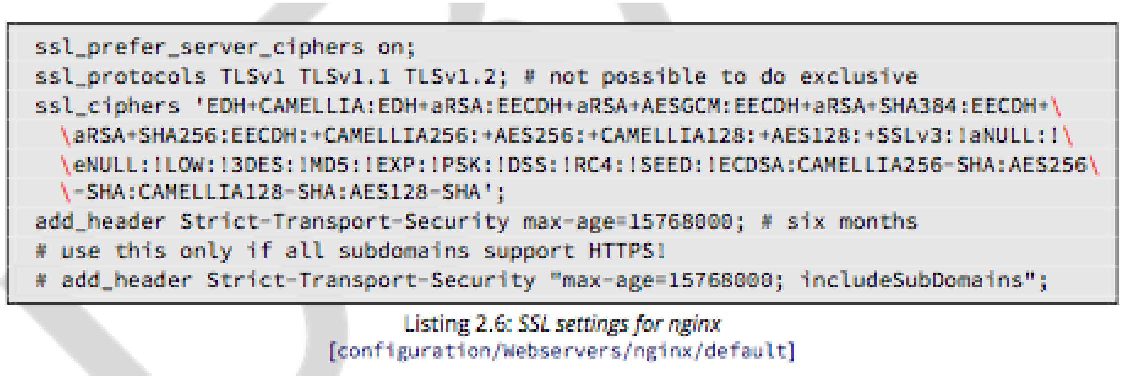
`http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html` `https://www.smacktls.com/` `https://freakattack.com/`

OpenSSL, LibreSSL, Apple SSL flaw exit exit exit!, Android SSL, certs certs!!!111, SSLv3, Heartbleed, MS TLS

PS From now on its TLS! Not SSL anymore, any SSLv2, SSLv3 is old and vulnerable

Bettercrypto.org pretty good advise

SSL settings for nginx



```
ssl_prefer_server_ciphers on;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # not possible to do exclusive
ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+\
  \aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!\
  \eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256\
  \-SHA:CAMELLIA128-SHA:AES128-SHA';
add_header Strict-Transport-Security max-age=15768000; # six months
# use this only if all subdomains support HTTPS!
# add_header Strict-Transport-Security "max-age=15768000; includeSubDomains";
```

Listing 2.6: *SSL settings for nginx*
[configuration/Webservers/nginx/default]

Overview

> ”This whitepaper arose out of the need for system administrators to have an updated, solid, well researched and thought-through guide for configuring SSL, PGP, SSH and other cryptographic tools in the post-Snowden age. ... This guide is specifically written for these system administrators.”

https://bettercrypto.org/

Overview of malware bypass today

Quote: The primary malware installation, sometimes referred as an infection, can be achieved using several attack vectors. The goal is always to run malicious code. Some of the most common attack vectors are:

- 1. Browser-based social engineering: where a user is tricked into clicking on a legitimate-looking URL which in turn triggers code execution using browser or browser-plugin vulnerabilities in Java and Flash. More advanced attacks can hide in legitimate traffic without requiring any user-interaction. These are commonly referred to as drive-by downloads.
- 2. Email-based social engineering and spear phishing: where a user receives an email that contains a hidden or visible binary, which executes when the user clicks on it.
- 3. Credential theft: when guessed or stolen credentials are used to access a remote machine and execute (malicious) code, such as installing a backdoor.

Source: Great summary article by Alon Nafta, senior security engineer at SentinelOne
How Malware Bypasses Our Most Advanced Security Measures, february 2015

`http://www.darkreading.com/perimeter/how-malware-bypasses-our-most-advanced-security-measures/a/d-id/1318974?_mc=RSS_DR_EDT`

Overview of malware bypass today, continued

Evasion techniques To evade detection, during and after installation, malware uses five primary techniques.

1. Wrapping. This process attaches the malicious payload (the installer or the malware itself) to a legitimate file. ... IceFog is a well-known malware commonly wrapped with a legitimate-looking CleanMyMac application and used to target OS X users. On the Windows platform, OnionDuke has been used with legitimate Adobe installers shared over Tor networks to infect machines.

2. Obfuscation. This involves modifying high level or binary code it in a way that does not affect its functionality, but completely changes its binary signature. ... Malware authors have adopted the technique to bypass antivirus engines and impair manual security research. ...

Source: How Malware Bypasses Our Most Advanced Security Measures

`http://www.darkreading.com/perimeter/how-malware-bypasses-our-most-advanced-security-measures/a/d-id/1318974?_mc=RSS_DR_EDT`

Overview of malware bypass today, continued

3. Packers. These software tools are used to compress and encode binary files, which is another form of obfuscation.... These techniques are extremely effective at circumventing static signature engines.

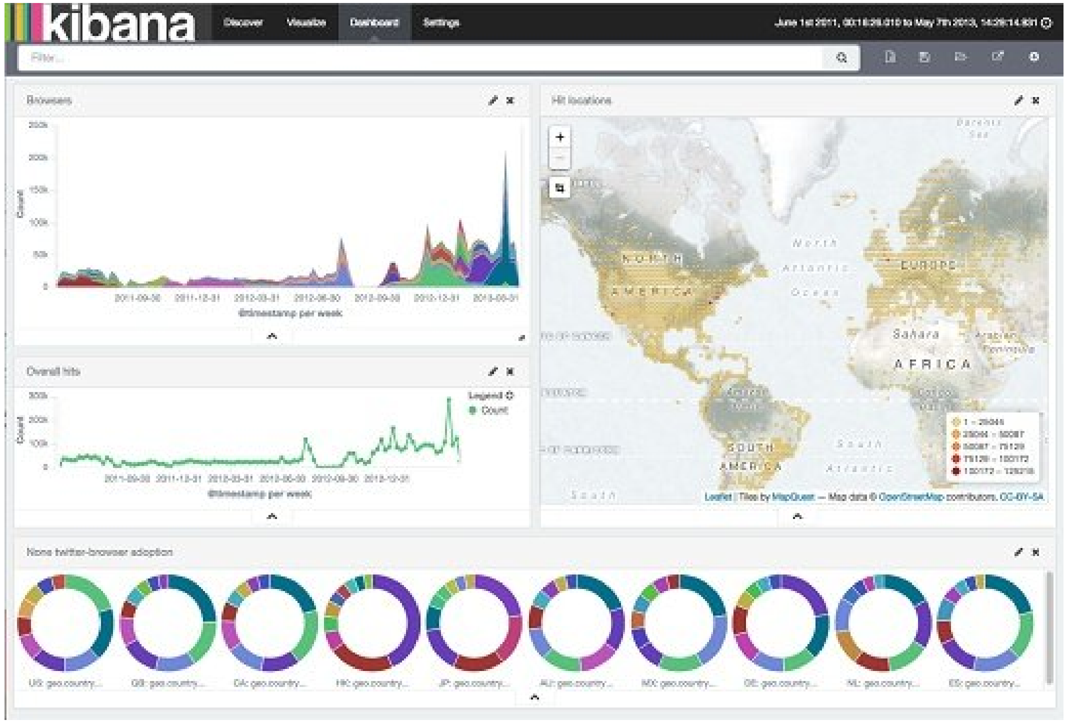
4. Anti-debugging. Like obfuscation, anti-bugging was originally created by software developers to protect commercial code from reverse-engineering. Anti-debugging can prevent a binary from being analyzed in an emulated environments such as virtual machines, security sandbox, and others. ...

5. Targeting. This technique is implemented when malware is designed to attack a specific type of system (e.g. Windows XP SP 3), application (e.g. Internet Explorer 10) and/or configuration (e.g. detecting a machine not running VMWare tools, which is often a telltale sign for usage of virtualization). ...

Source: How Malware Bypasses Our Most Advanced Security Measures

`http://www.darkreading.com/perimeter/how-malware-bypasses-our-most-advanced-security-measures/a/d-id/1318974?_mc=RSS_DR_EDT`

Kibana 4 february 2015



Highly recommended for a lot of data visualisation

Source: `https://www.elastic.co/products/kibana`

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?

Future actions- spring and summer 2014

- Document your processes, systems, applications, databases, backup and restore procedures
  Finish before summer - so you can have vacation, will be needed!
- Share information within your organisation, and outside
  Make friends!
- Crypto Parties - get them started, keep them going!
- Conferences: DKNOG, TheCamp this summer, RIPE in May, CCC Summercamp

Questions?

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email