

Welcome to

Hacking today

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

<http://www.solidonetworks.com>



Don't Panic!

Skabe forståelse for hackerværktøjer samt penetrationstest metoder

webbaserede angreb

netværkssikkerhed

lidt kryptografi

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 ligner indimellem magi



Hacking kræver blot lidt ninja-træning

Movie:Kryptonite lock - old



Just search for: kryptonite lock bic pen

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

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

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

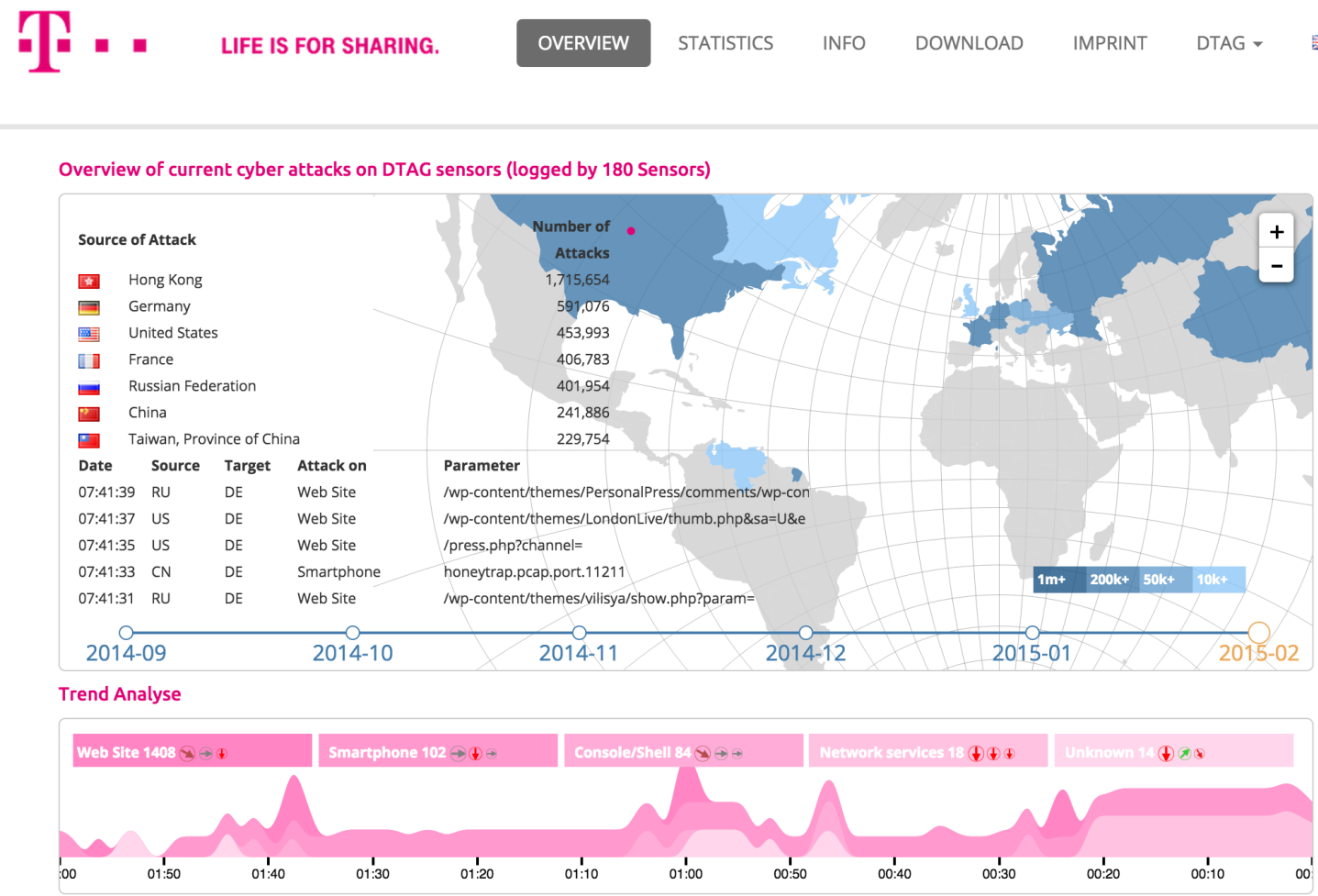
Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger? ■

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere





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

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/>

```
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 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/>

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/>
- Burp is a highly recommended commercial Web proxy EUR 275/user/year 2.000DKK
http://portswigger.net/burp/help/suite_gettingstarted.html

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 ...	


[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

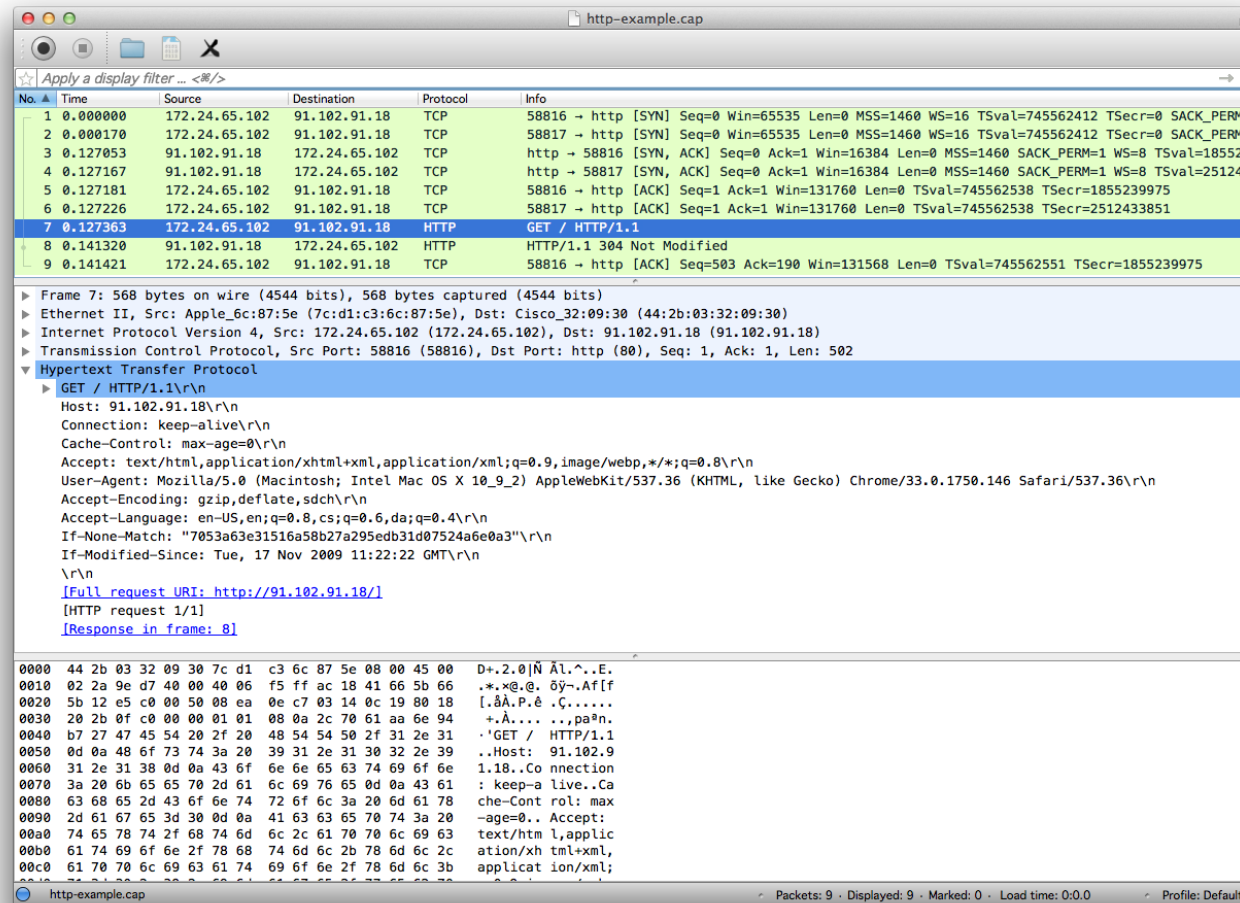
- WLAN packet capture and transmission
- Full 802.11 a/b/g/n support
- View management, control and data frames
- Multi-channel aggregation (with multiple adapters)



[Learn More ▶](#)

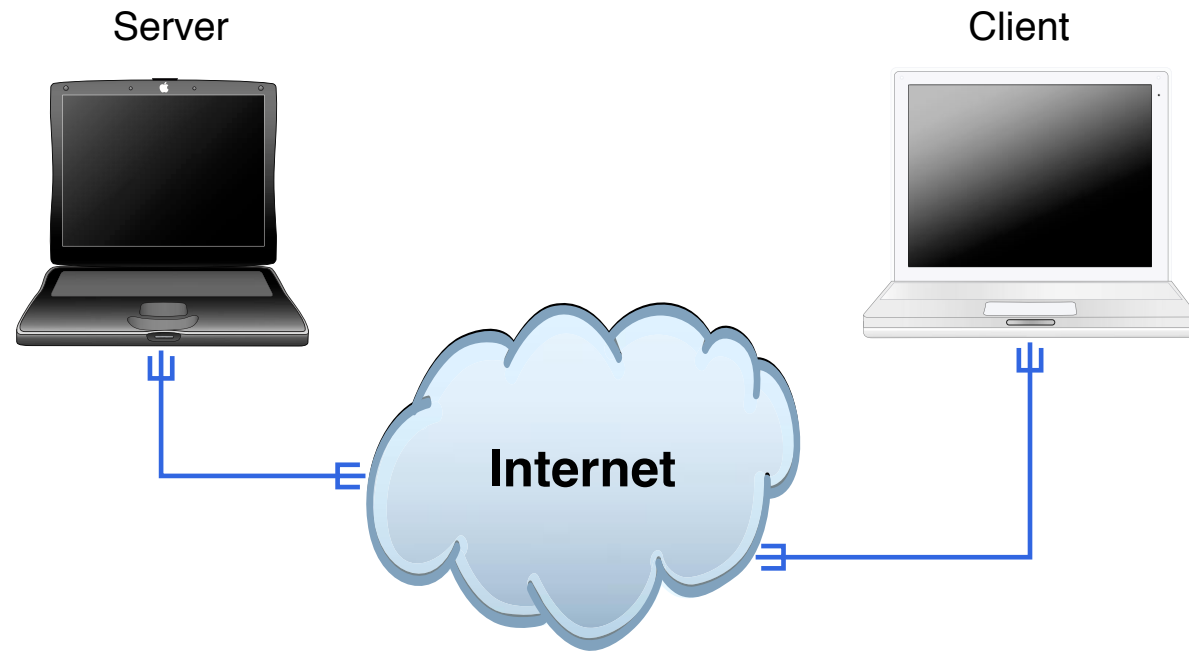
[Buy Now ▶](#)

`http://www.wireshark.org`
både til Windows og UNIX

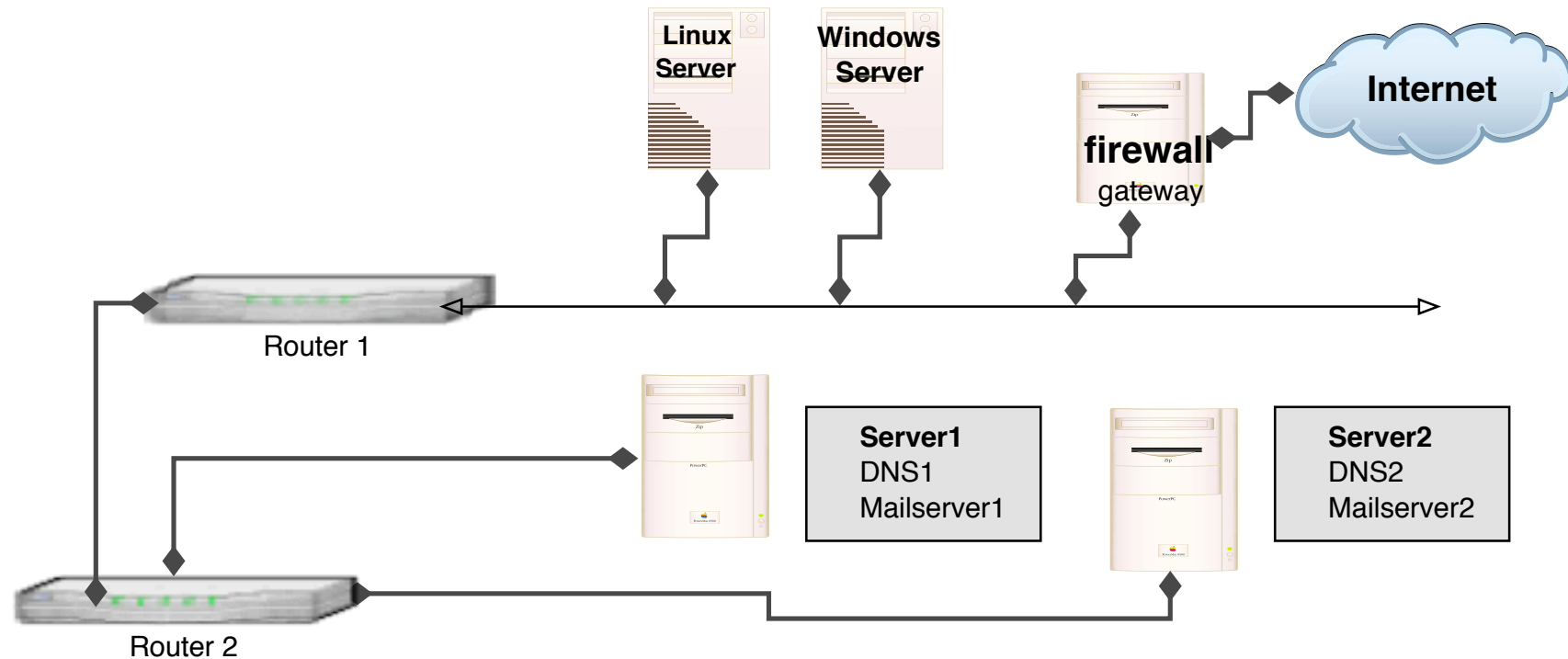


Wireshark: Filters, hexdump, protocol dissection, overview, coloring, advanced features

Demo: Wireshark

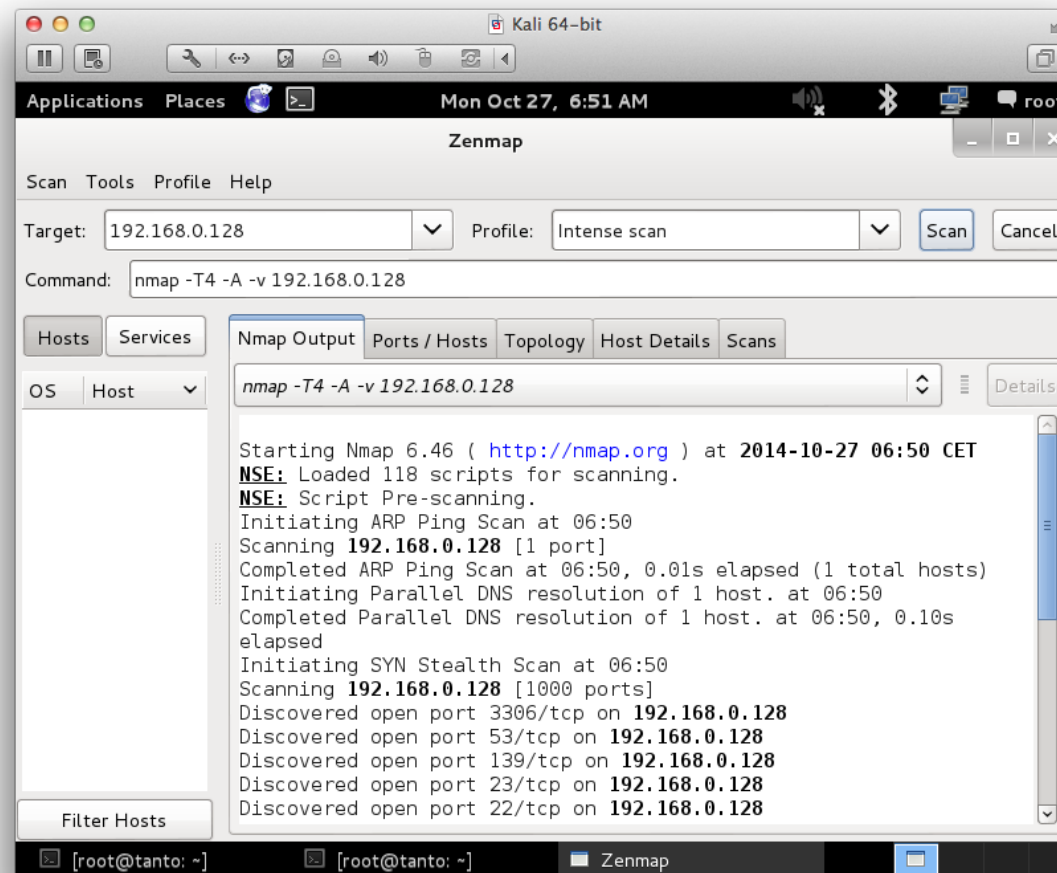


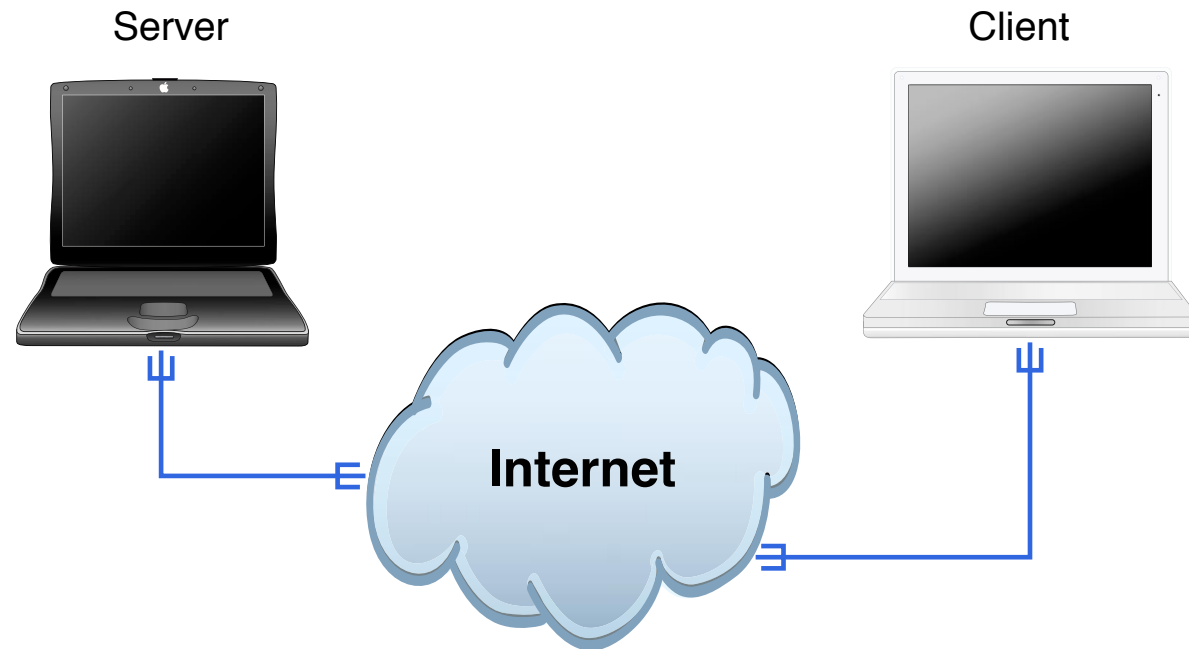
Wireshark



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

Portscan med Zenmap GUI





Armitage og Metasploit

”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

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";
```

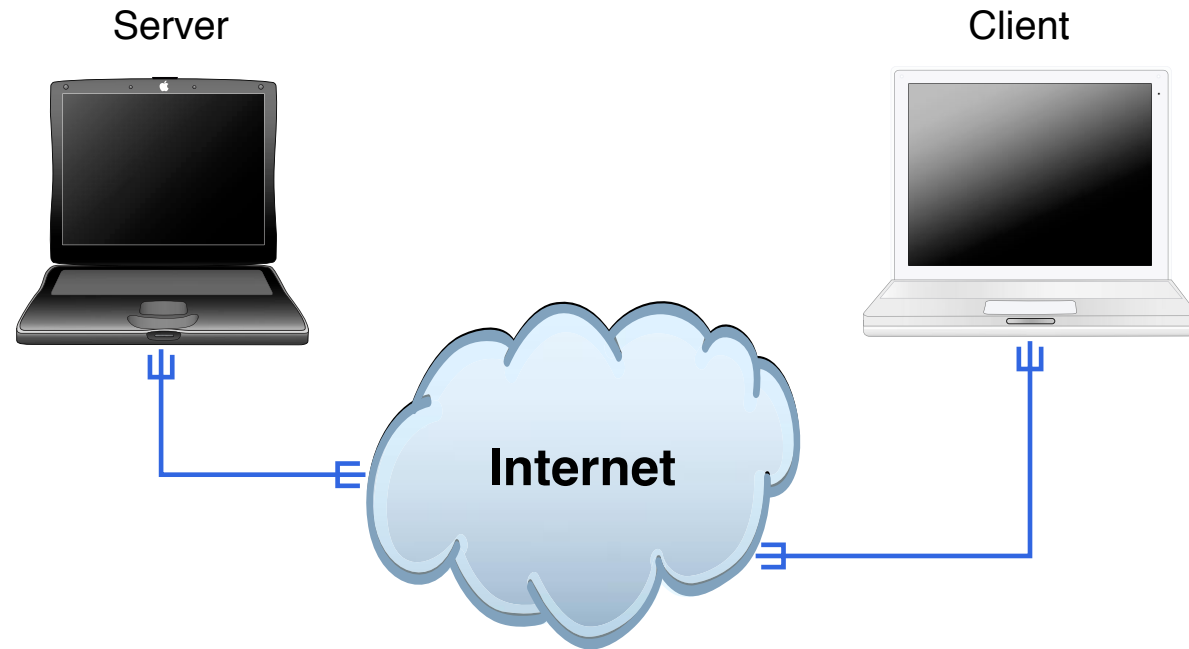
Listing 2.6: SSL settings for nginx
[configuration/Webservers/nginx/default]

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/>

Demo: Webhacking WebGoat



Webhacking WebGoat

February and March 2015, Security Onion updates



Security Onion 12.04.5.1 ISO image now available, plus Suricata IDS engine 2.0.7

Learn NSM with Security Onion today - its free

Source:

<http://blog.securityonion.net/>



Highly recommended for a lot of data visualisation

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

- 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?

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email