Welcome to

Netværkssikkerhed
Jul med Kramshøj Hacking Seminar

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramshoej@Github

Formålet

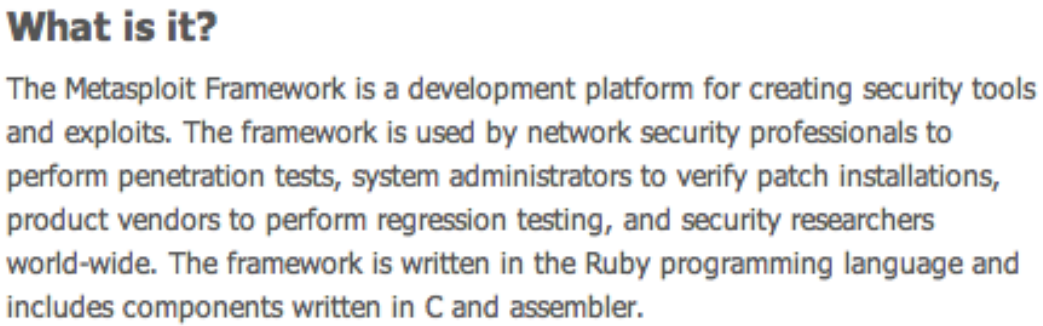
Don’t Panic!

pentest, hacking, historik og en hurtig gennemgang op til idag hvor vi har Metasploit og Armitage som state-of-the-art værktøjer

Vi bryder ind i computere og viser hvordan pentest værktøjer kan medvirke til både at spare tid og verificere opsætningen af netværksudstyr, som firewalls

Jeg bruger Kali 2.0 Linux hackerplatformen som eksempel

Metasploit and Armitage Still rocking the internet



Udviklingsværktøjerne til exploits er i dag meget raffinerede!

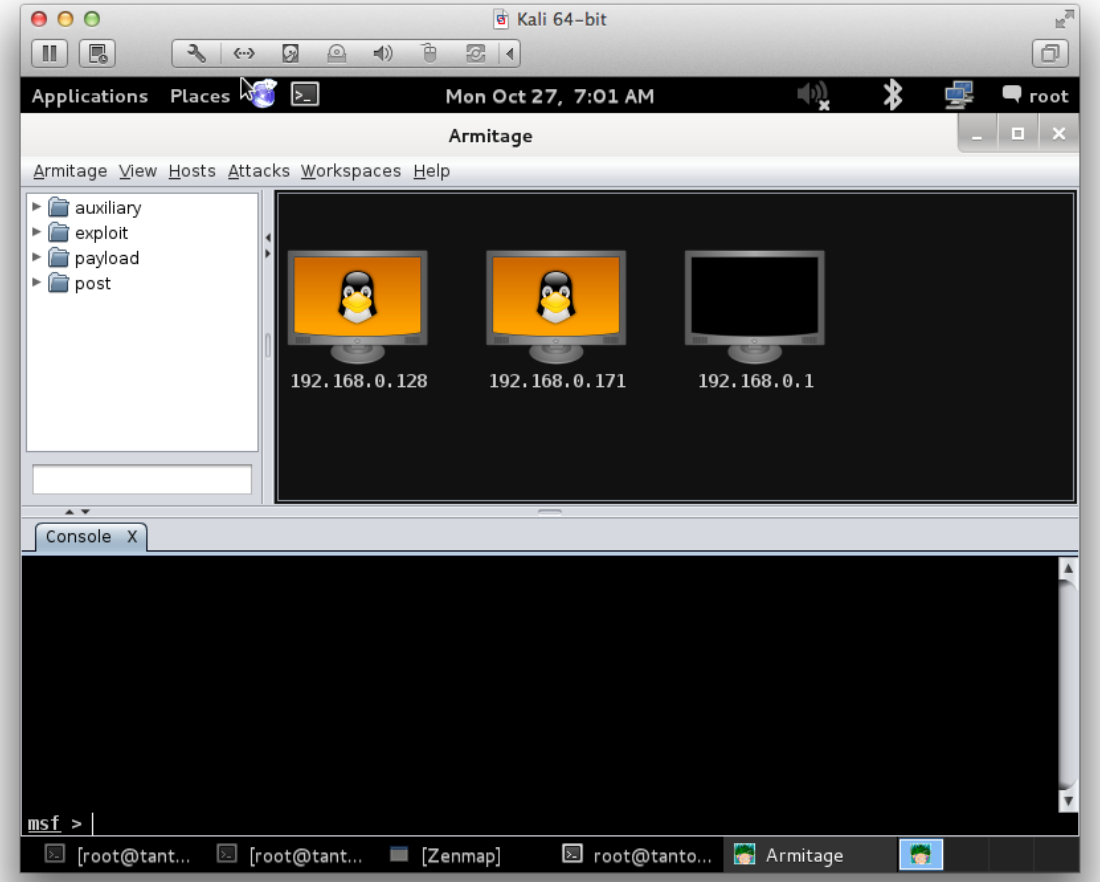
`http://www.metasploit.com/`

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

Demo: Metasploit Armitage



Agenda

Hvor kommer det fra! Fra SATAN til Armitage og åbne exploit databaser i dag

Kali introduktion

Portscanning med Nmap, IPv4 og IPv6

Script scanning med Nmap, eksempler som

```
nmap -p 443 --script ssl-heartbleed <target>
```

Hvordan sikrer vi os bedst!? Henriks bud på sikring af hjem og firma

Forventer løst format, afslappet, spørgsmål og afstikkere ☺

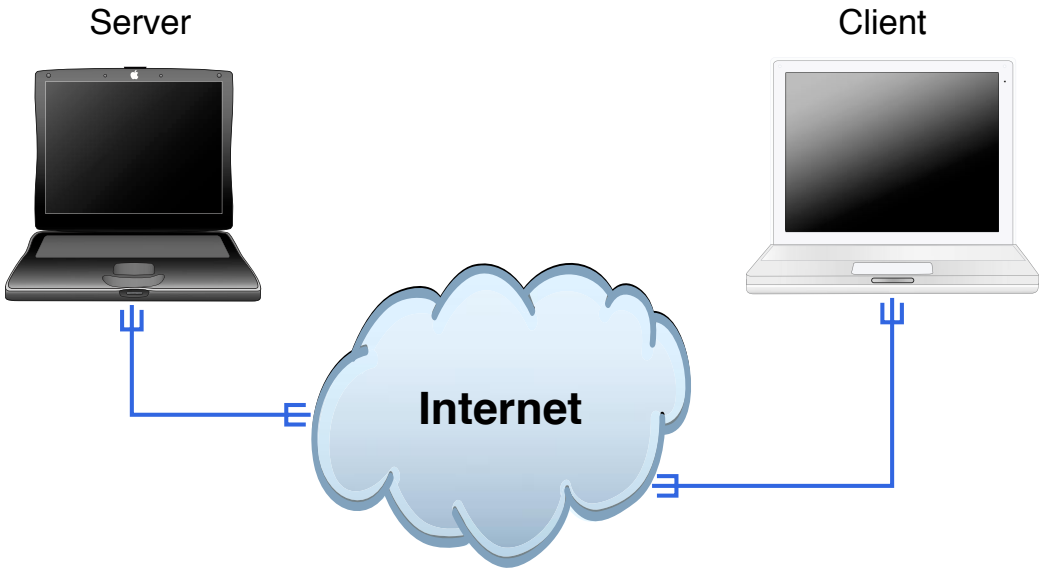
Aftale om test af netværk

Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man får konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde - eller fængselsstraf i alvorlige tilfælde
- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frit efter: `http://www.stophacking.dk` Det Kriminalpræventive Råd, siden er væk
- Frygten for terror har forstærket ovenstående - så lad være!

Internet idag



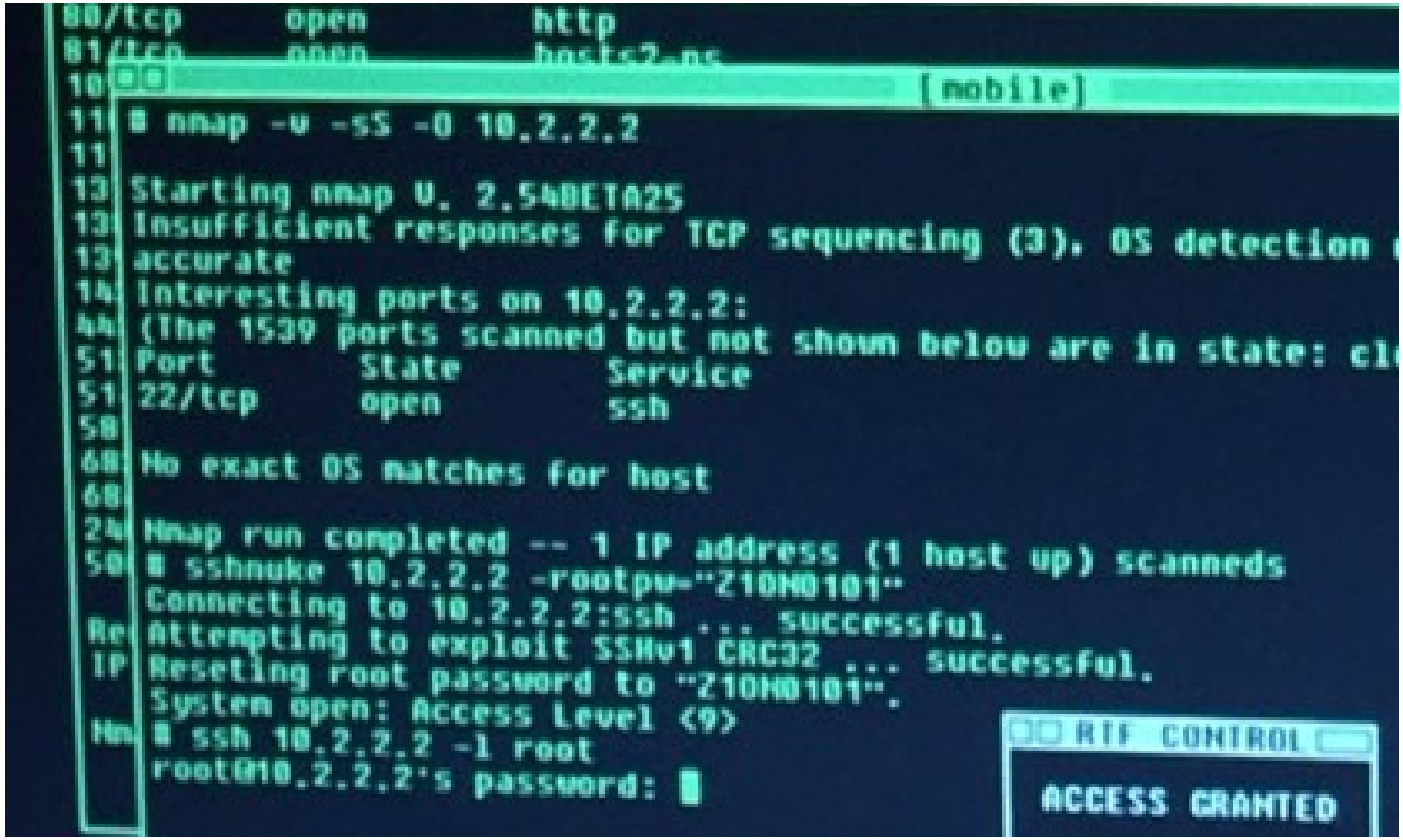
Klienter og servere

Rødder i akademiske miljøer

Protokoller hvor nogle er mere end 20 år gamle

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

Trinity breaking in



`http://nmap.org/movies.html`

Meget realistisk `http://www.youtube.com/watch?v=51lGCTgqE_w`

Hackerværktøjer

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

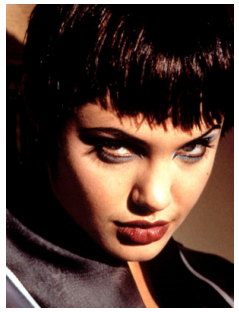
De udgav i 1995 så en softwarepakke med navnet SATAN *Security Administrator Tool for Analyzing Networks*

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`

Hackerværktøjer

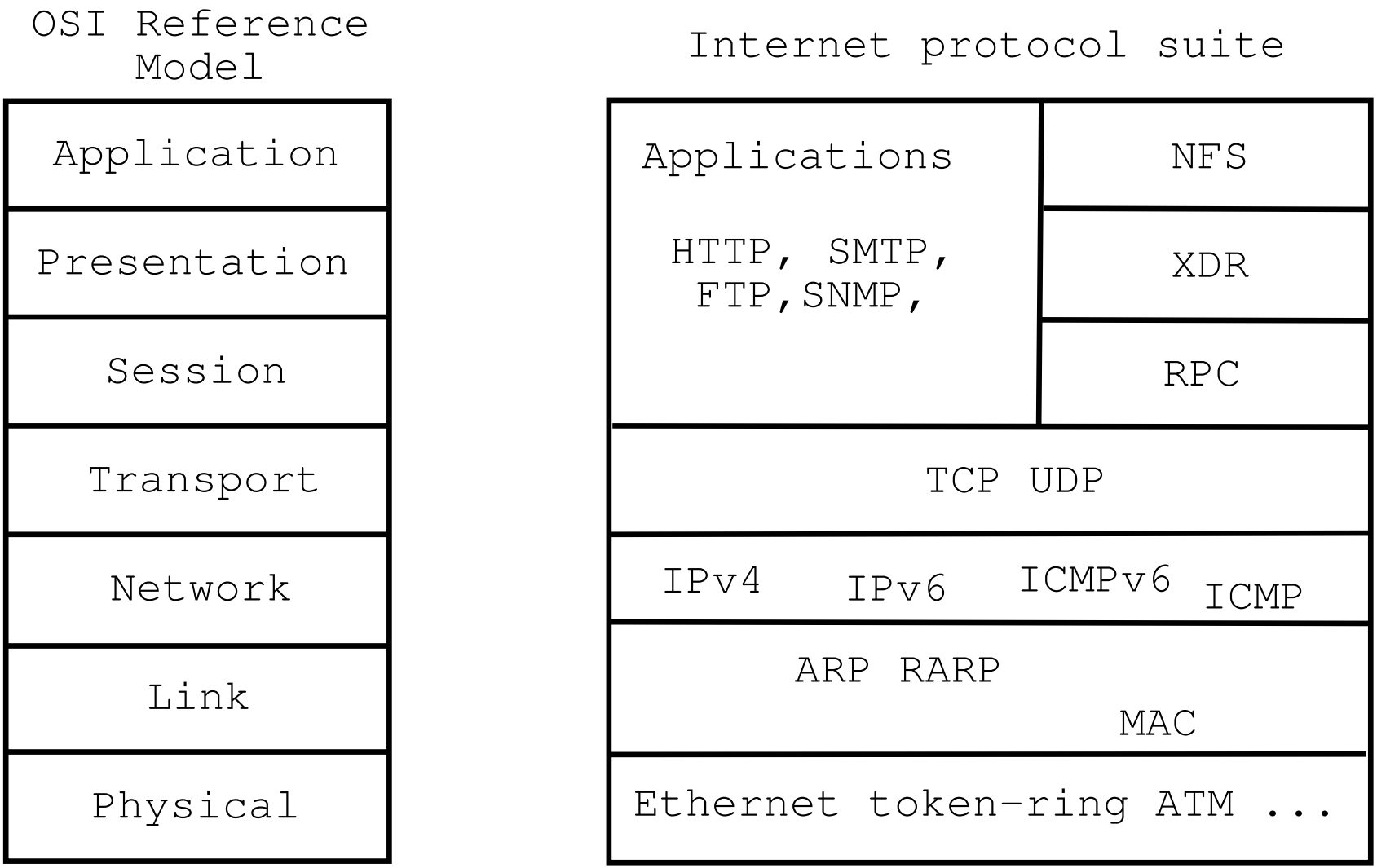


- Nmap, Nping - tester porte, godt til firewall admins `http://nmap.org`
- Metasploit Framework gratis på `http://www.metasploit.com/`
- Wireshark avanceret netværkssniffer - `http://http://www.wireshark.org/`
- Burpsuite `http://portswigger.net/burp/`
- OpenBSD operativsystem med fokus på sikkerhed `http://www.openbsd.org`

Kilde: billedet er Angelina Jolie fra Hackers 1995

Kræver en mere struktureret tilgang end de viser på film ☺

OSI og Internet modellerne



The Internet Worm 2. nov 1988

Udnyttede følgende sårbarheder

- buffer overflow i fingerd - VAX kode, Sendmail - DEBUG, Tillid mellem systemer: rsh, rexec, ...
- dårlige passwords

Avanceret + camouflage!

- Programnavnet sat til 'sh', Brugte fork() til at skifte PID jævnligt
- Fandt systemer i /etc/hosts.equiv, .rhosts, .forward, netstat ...
- Password cracking med intern liste med 432 ord og /usr/dict/words

Lavet af Robert T. Morris, Jr.

Medførte dannelsen af CERT, `http://www.cert.org`

1980'erne - det er vel fixet så?

2016 botnets Internet of things (IoT)

> This is bad news for cybersecurity as the IoT devices market heats up as people buy into the smart, automated systems. Gartner Inc. projects connected devices to rise to 6.4 billion worldwide in 2016 with almost 5.5 million devices being connected daily.

2016: Mirai Botnet Internet of things (IoT), 60 common factory default usernames and passwords
”Mirai was used in the DDoS attack on 20 September 2016 on the Krebs on Security site which reached 620 Gbps.”

2016: Currently, “Bashlight” is creating an army of a million IoT devices.
Eeen million enheder!

Sources: `https://en.wikipedia.org/wiki/Mirai_(malware)`

`http://heavy.com/tech/2016/10/mirai-iot-botnet-internet-of-things-ddos-attacks-internet-outage`

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 algoritm, 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 Cimpanu, Softpedia 15 September 2015

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

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-vulner`

`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-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`

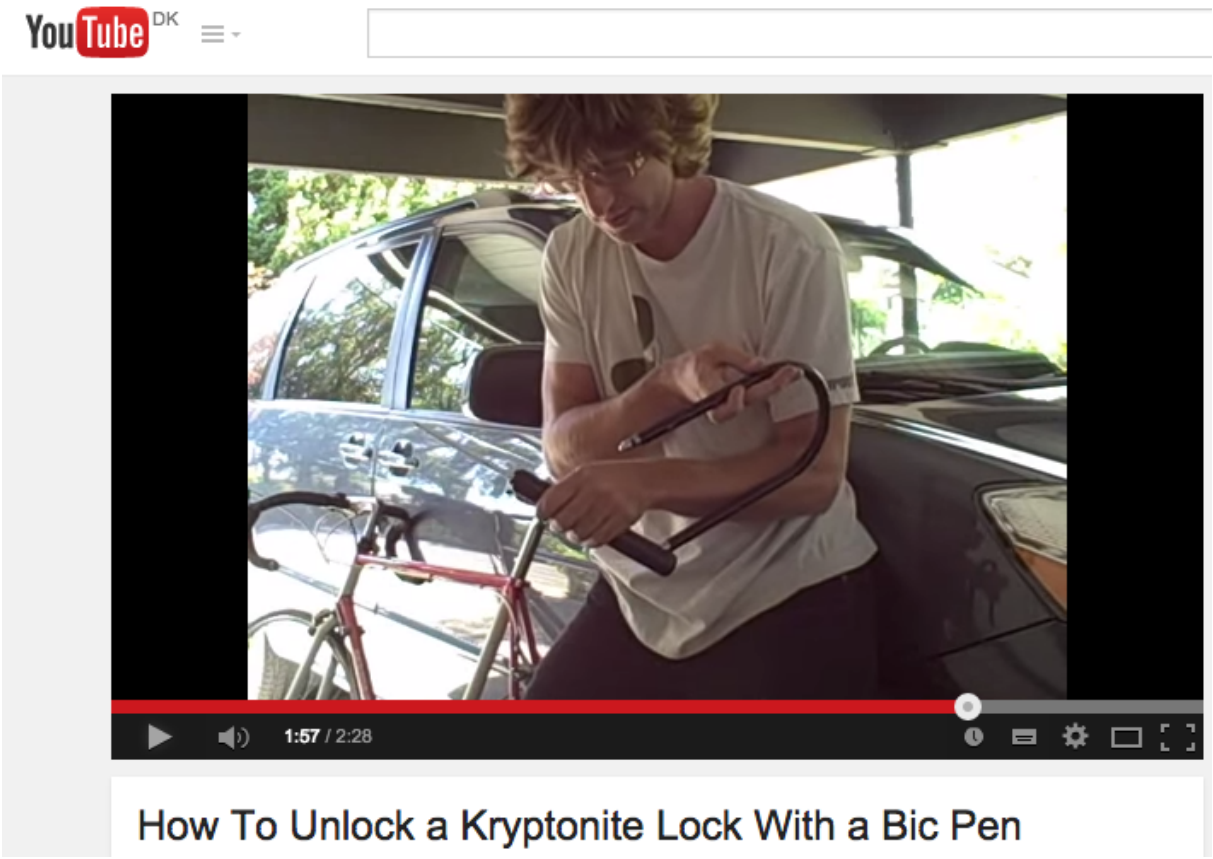
Sceneskift - Hacking er magi

Hacking ligner indimellem magi

Hacking er ikke 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`

Teknisk hvad er hacking

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

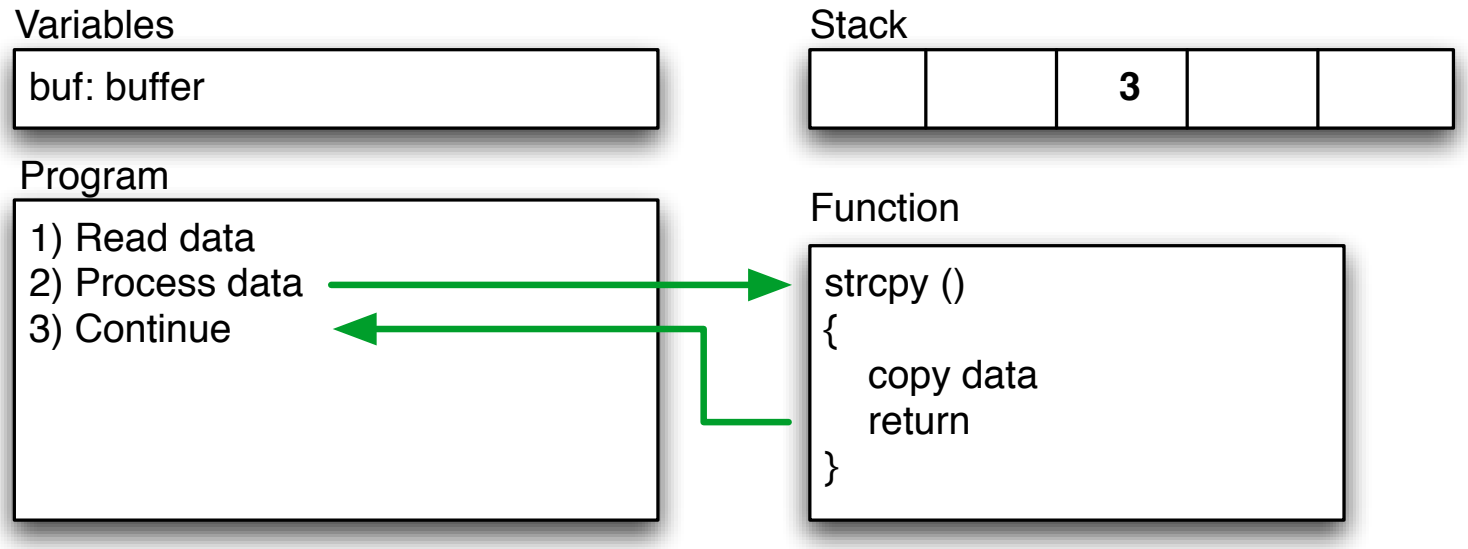
MAC filtrering

Buffer overflows et C problem

Et buffer overflow er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

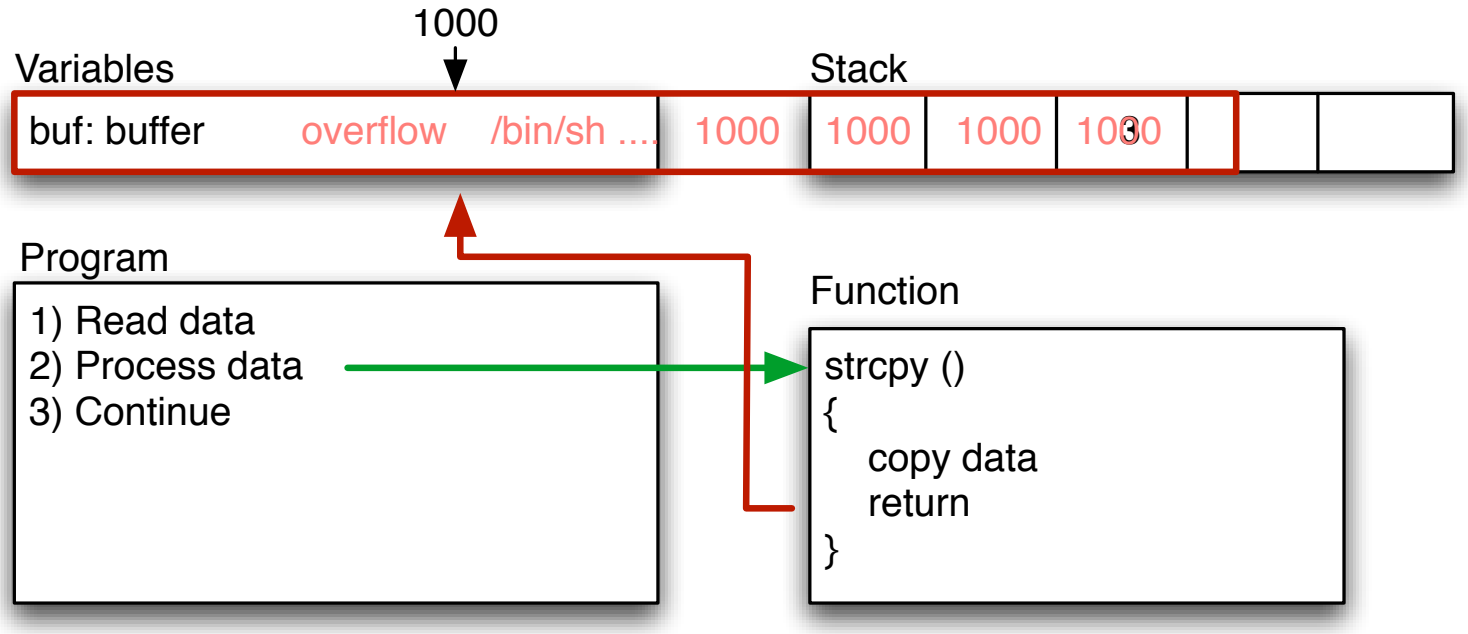
Stack protection er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

Buffer og stacks




```
main(int argc, char **argv)
{       char buf[200];
        strcpy(buf, argv[1]);
        printf("%s\n",buf);
}
```

Overflow – segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

Exploits – udnyttelse af sårbarheder

- Exploit/exploitprogram er udnytter en sårbarhed rettet mod et specifikt system.
- Kan være 5 linier eller flere sider ofte Perl, Python eller et C program

Eksempel demo i Perl, uddrag:

```
$buffer = "";
$null = "\x00";
$nop = "\x90";

$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0x01101d48; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
$address = pack('l', $the_shell_pointer);
$buffer .= $address;
exec "$program", "$buffer";
```

Hvordan finder man buffer overflow, og andre fejl

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review – automatisk eller manuelt

Fejl kan findes ved at prøve sig frem – fuzzing

Exploits virker typisk mod specifikke versioner af software

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

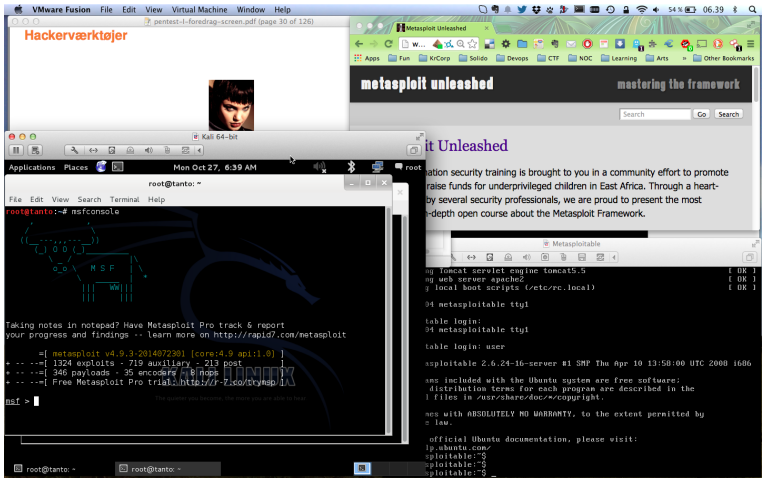
Udnyttelse/afprøvning: Metasploit, Nikto, exploit programs

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.

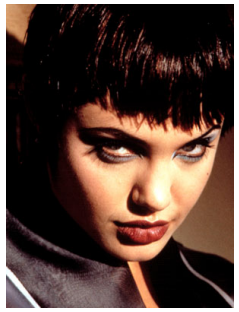
I skal jo også VISE andre at I gør noget ved sikkerheden.

Hackerlab opsætning



- Tænk som en hacker, rekognoscering, angreb, udnyt
- Hardware: en moderne laptop med CPU der kan bruge virtualiseting
  Husk at slå virtualisering til i BIOS
- Software: Windows, Mac, Linux og virtualiseringssoftware: VMware, Virtual box, vælg selv
- Hackersoftware: Kali Linux som en virtuel maskine
- 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/`
- Specialscannere, eksempelvis web sårbarhedsscanner – eksempelvis Burp, 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

Kali – `https://www.kali.org/` - den man bruger idag

Wireshark – `https://www.wireshark.org` avanceret netværkssniffer

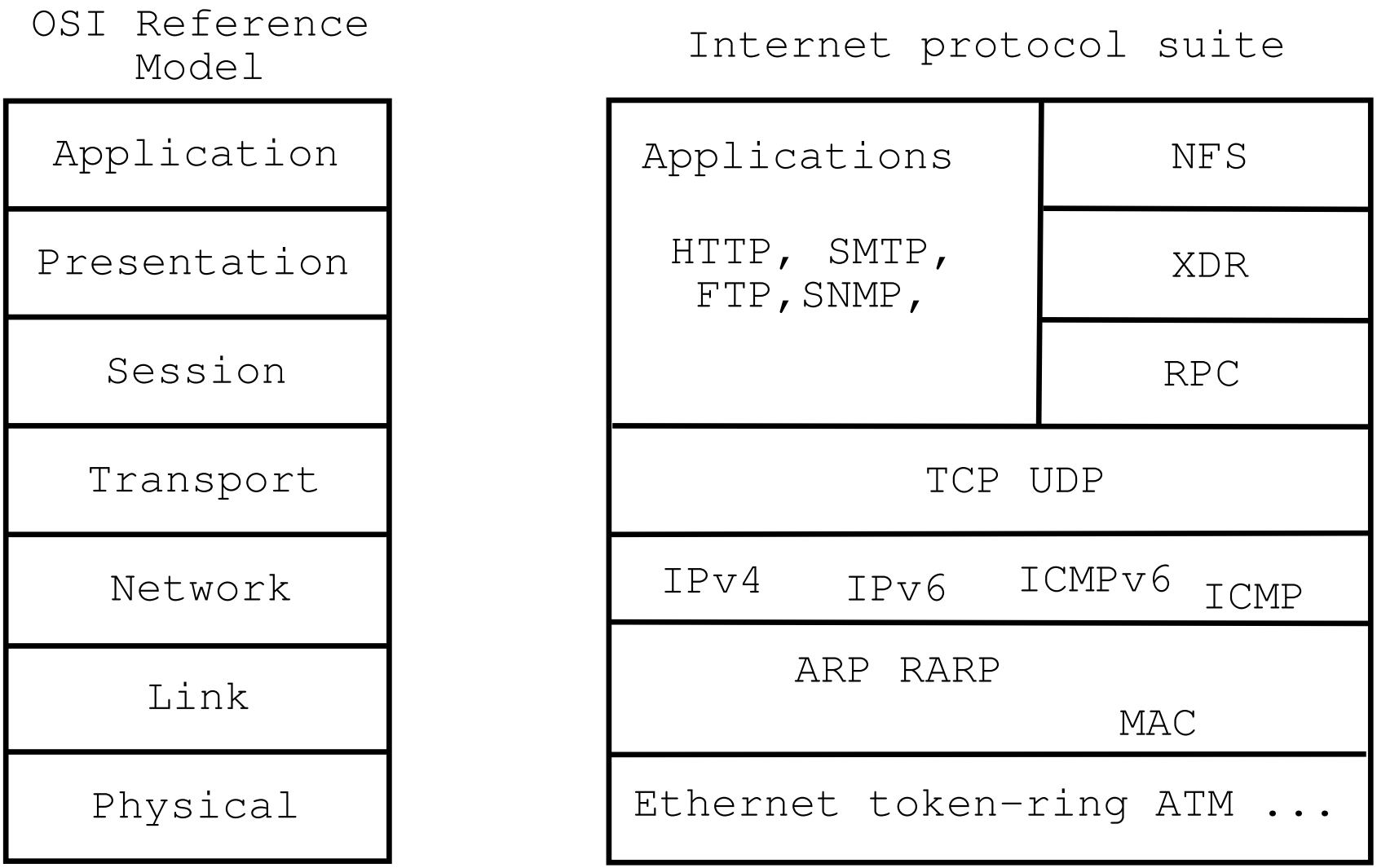
Meget nemt at starte med, og kommer nemt igang med mange tools

Brug hjemmesiderne for tools til tutorials og videoer

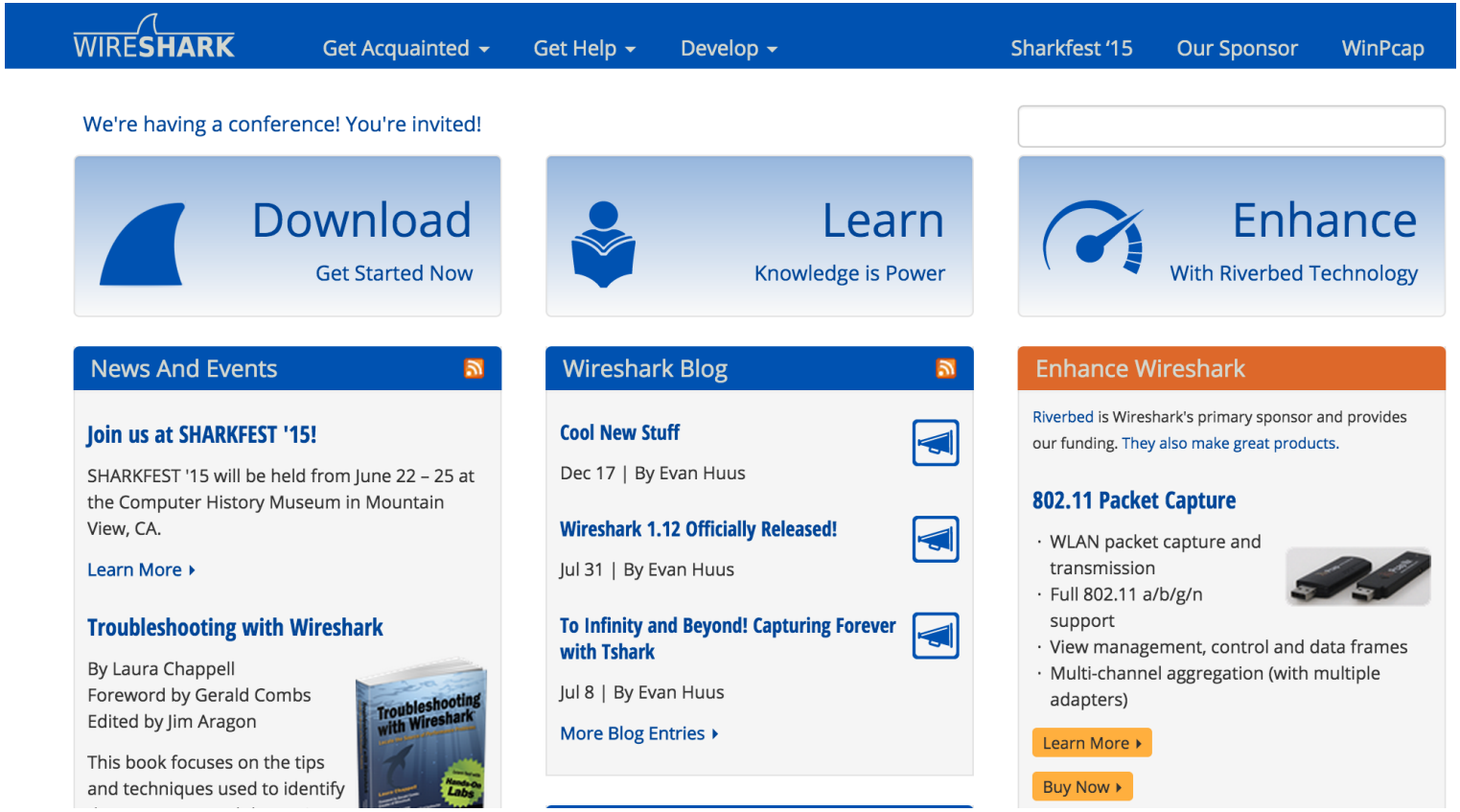
`youtube.com: kali hack > 200.000 hits`

Start evt med de mest populære fra `http://sectools.org/`

OSI og Internet modellerne



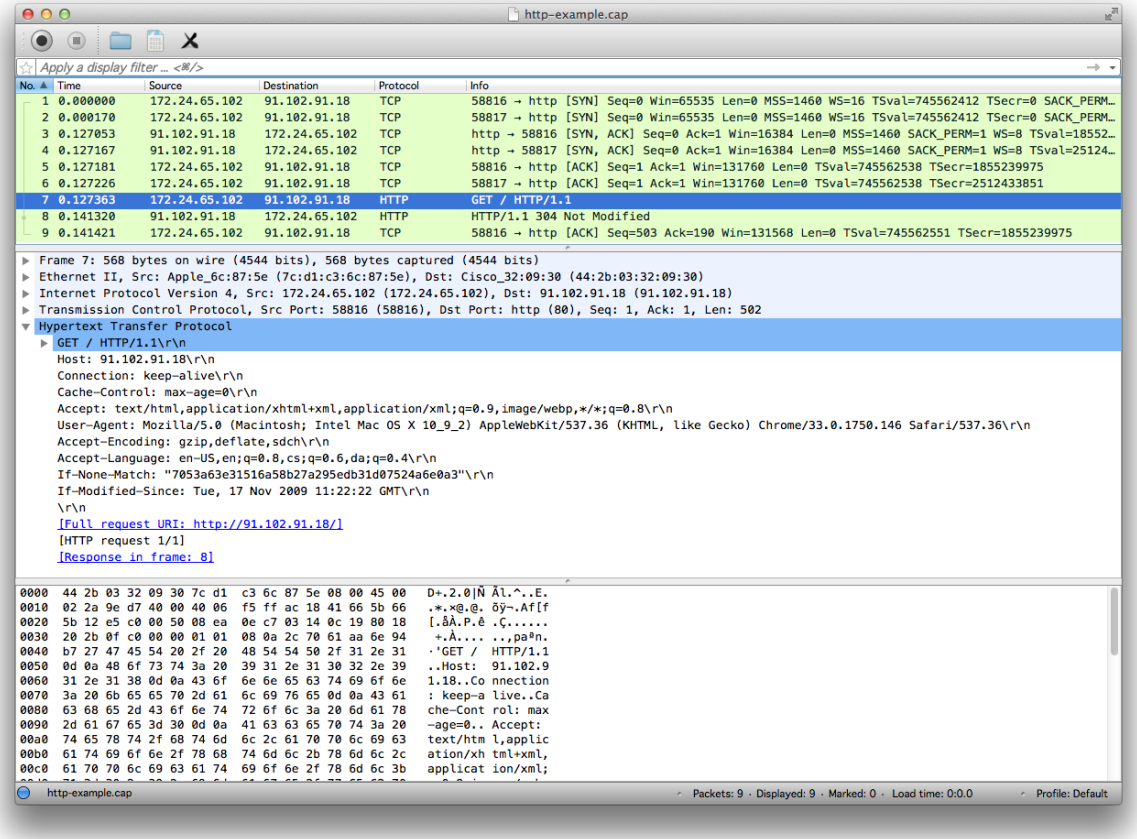
Wireshark - grafisk pakkesniffer



`http://www.wireshark.org`

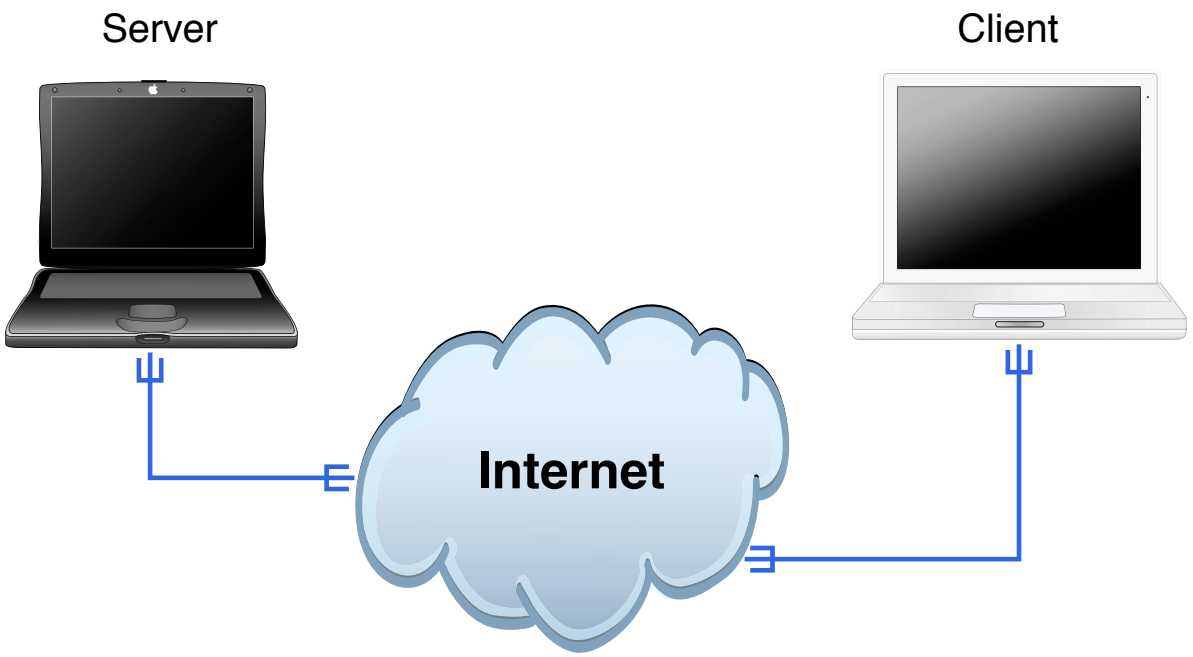
både til Windows og UNIX

Wireshark usage



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

Demo: Wireshark



Wireshark

The Exploit Database – dagens buffer overflow

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.

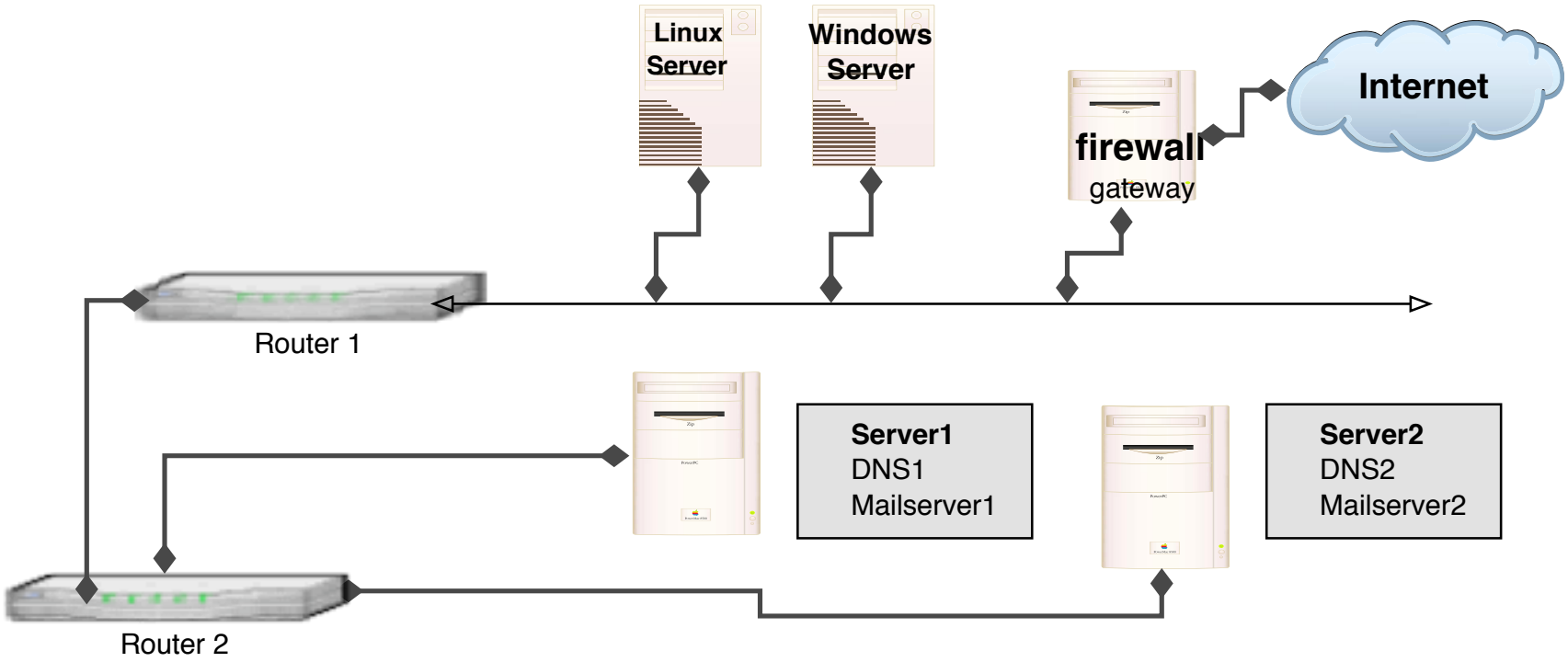
Source: `http://heartbleed.com/`

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_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..
```

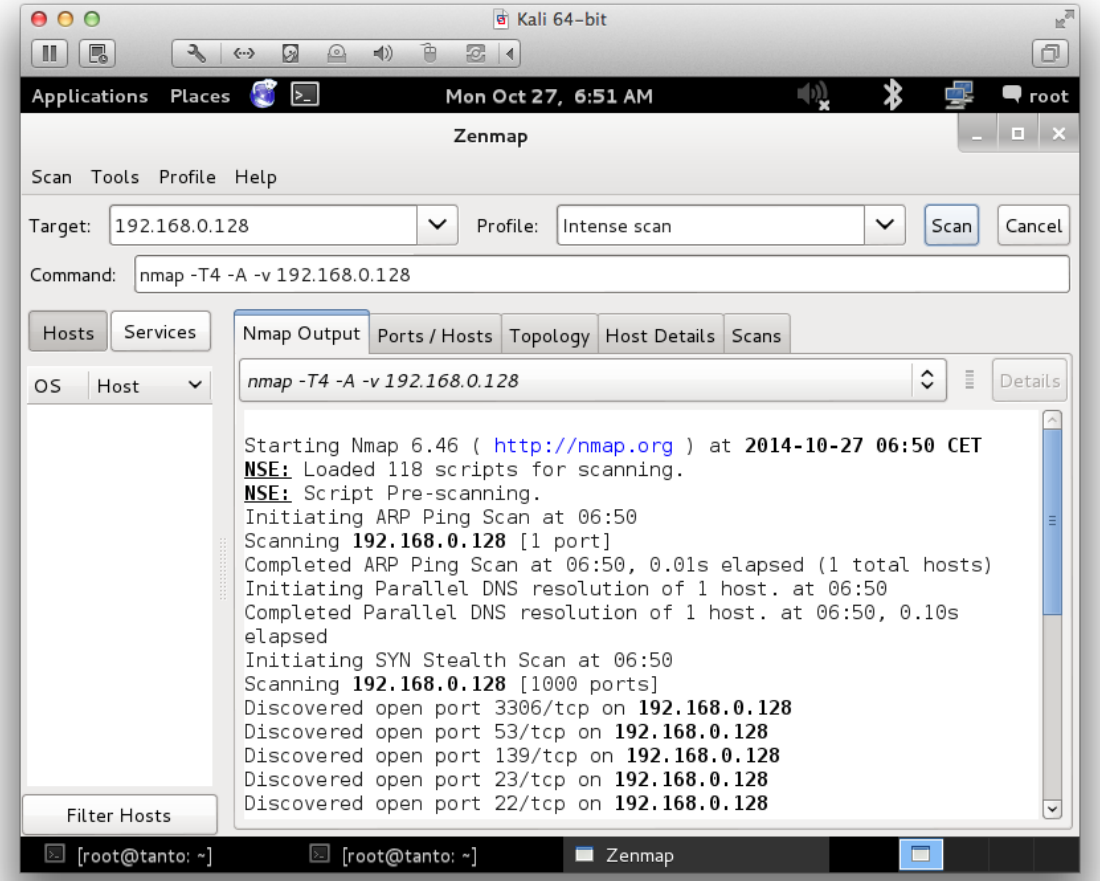
- Obtained using Heartbleed proof of concepts - Gave full credit card details
- ”can XXX be exploited- yes, clearly! PoCs ARE needed
  without PoCs even Akamai wouldn’t have repaired completely!
- `https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliar`
  `scanner/ssl/openssl_heartbleed.rb`

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

Hjemmearbejde: Kali øvelser

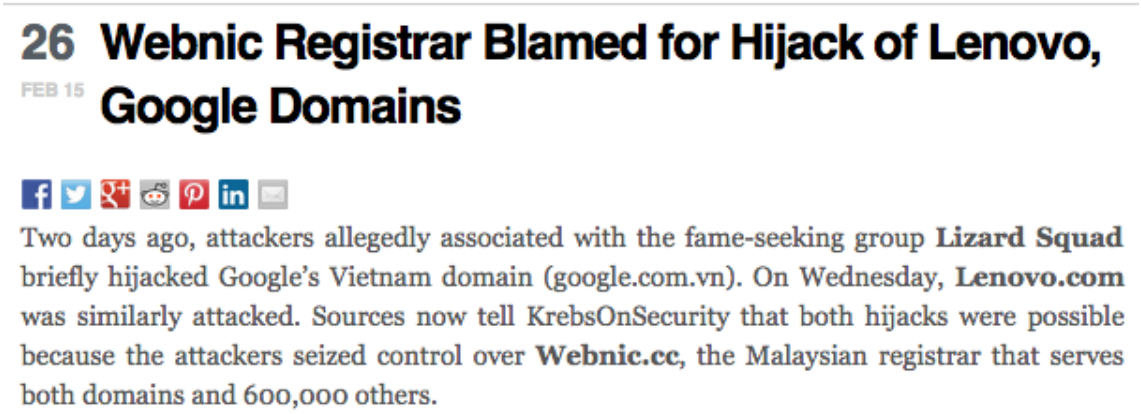
Prøv selv at gentage det jeg viste hjemme

- Wireshark
- Wireshark med FTP
- Nmap med Zenmap, script scan
- Armitage og Metasploit, husk `service postgresql start`
- WEP/WPA cracking

Beskyt dig selv, og dit netværk

Nu skifter vi over til at beskytte os selv!

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



26 FEB 15 **Webnic Registrar Blamed for Hijack of Lenovo, Google Domains**

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`

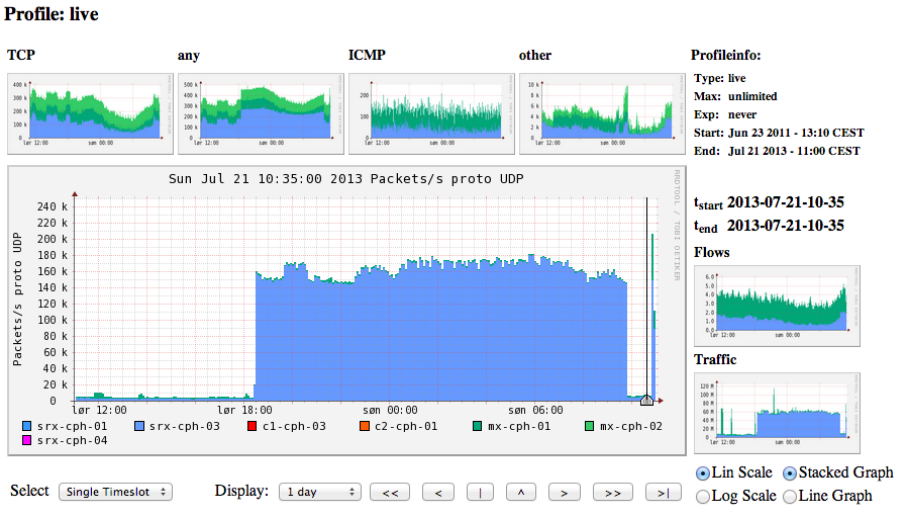
Kibana 4

Highly recommended for a lot of data visualisation

Non-programmers can create, save, and share dashboards

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

Brug hackerværktøjer!



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

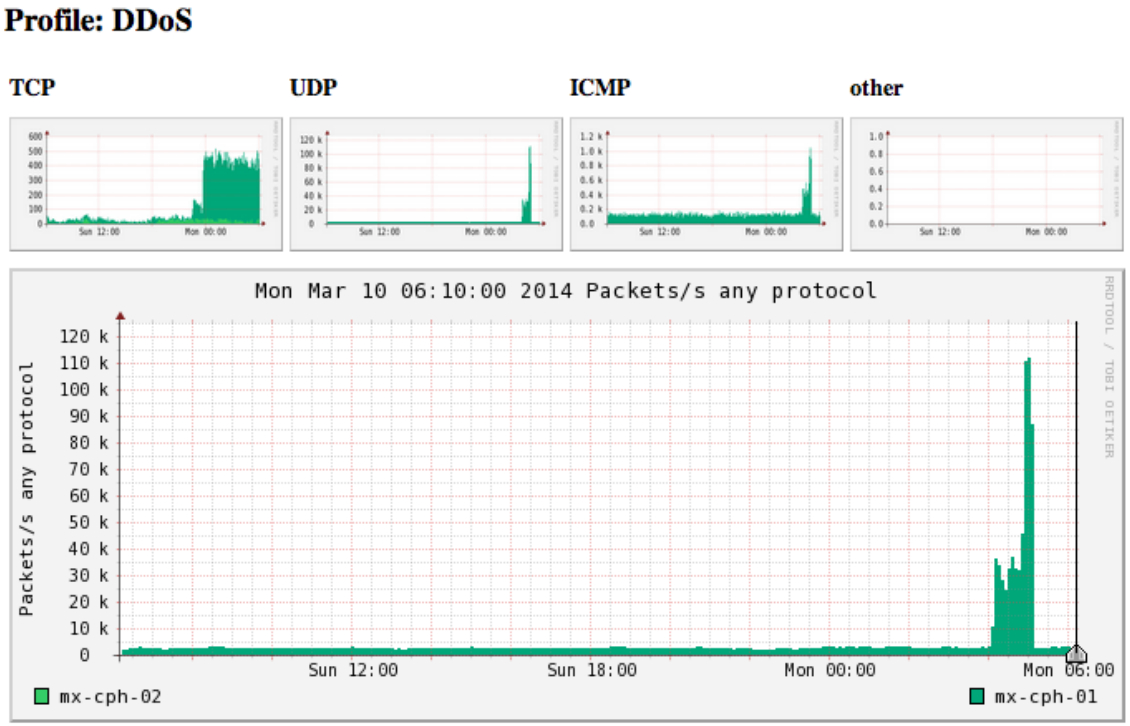
Hackerværktøjer – bruger I dem? – efter dette kursus gør I

Portscannere kan afsløre huller i forsvaret

I vil kunne finde mange potentielle problemer proaktivt ved regelmæssig brug

Værktøjerne er på Kali Linux allerede

Detecting DDoS example tool Nfsen

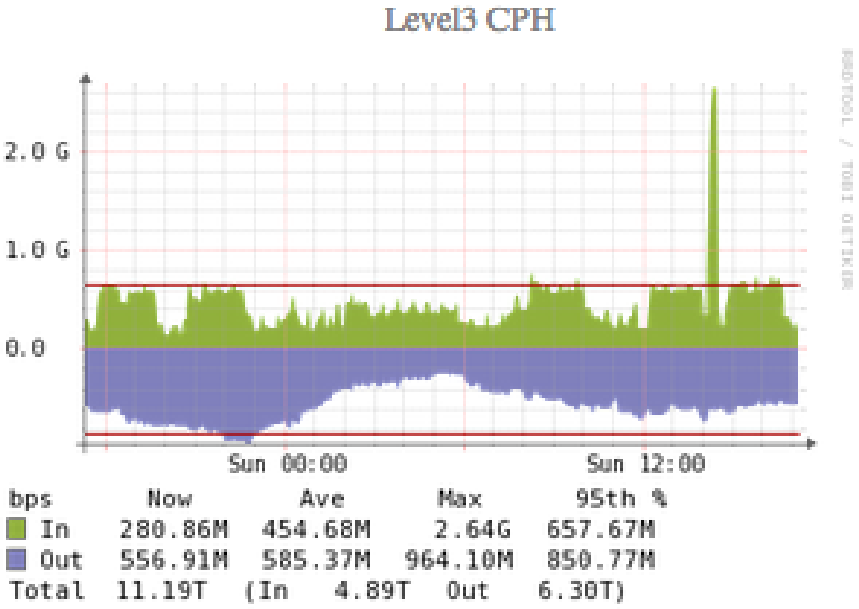


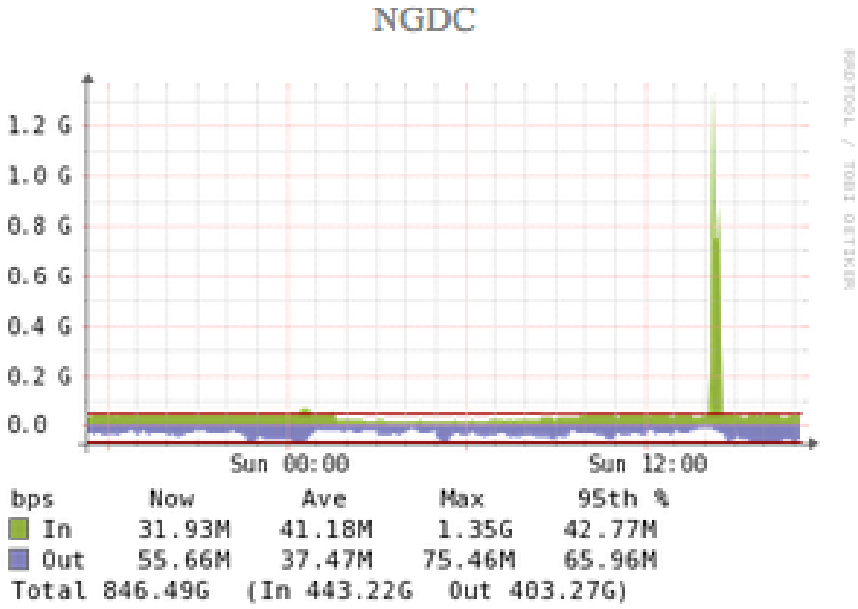
We created a DDoS profile with the common types.

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:%.lf
```

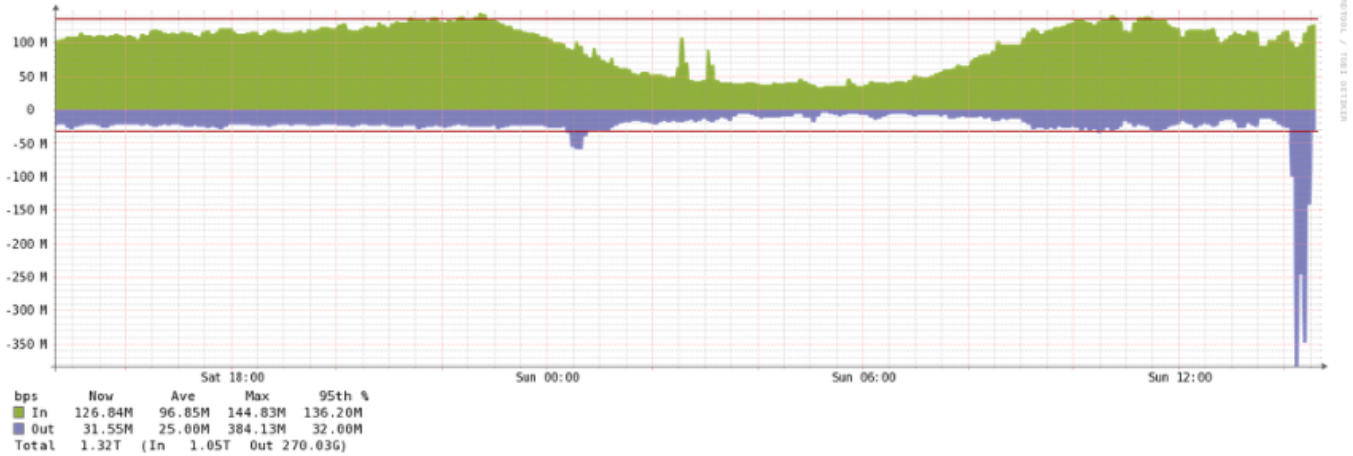
DDoS traffic before filtering





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

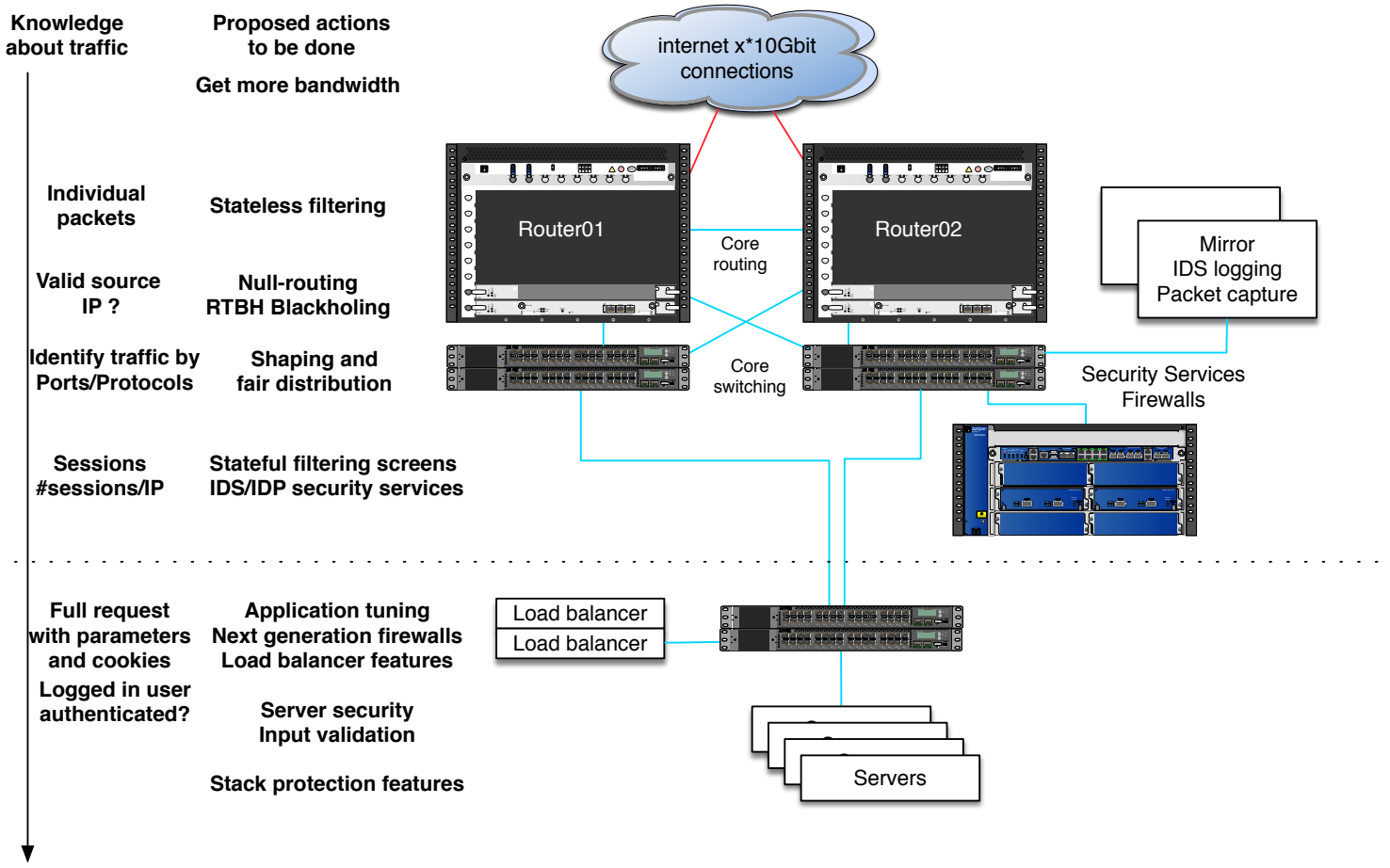
Problem: We receive unauthenticated chaotic traffic

Solution: Discard early, discard on edge, reduce noise

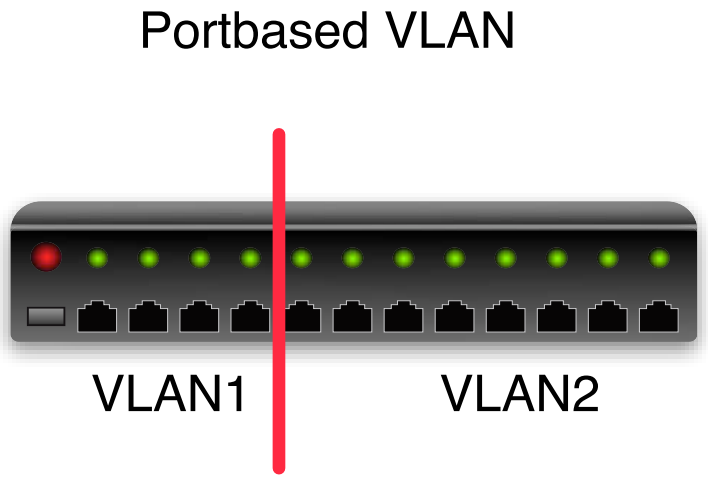
Only use CPU resources for potentially real traffic

Single firewall layer typically cannot cope!

Defense in depth - multiple layers of security



VLAN Virtual LAN



Nogle switche tillader at man opdeler portene

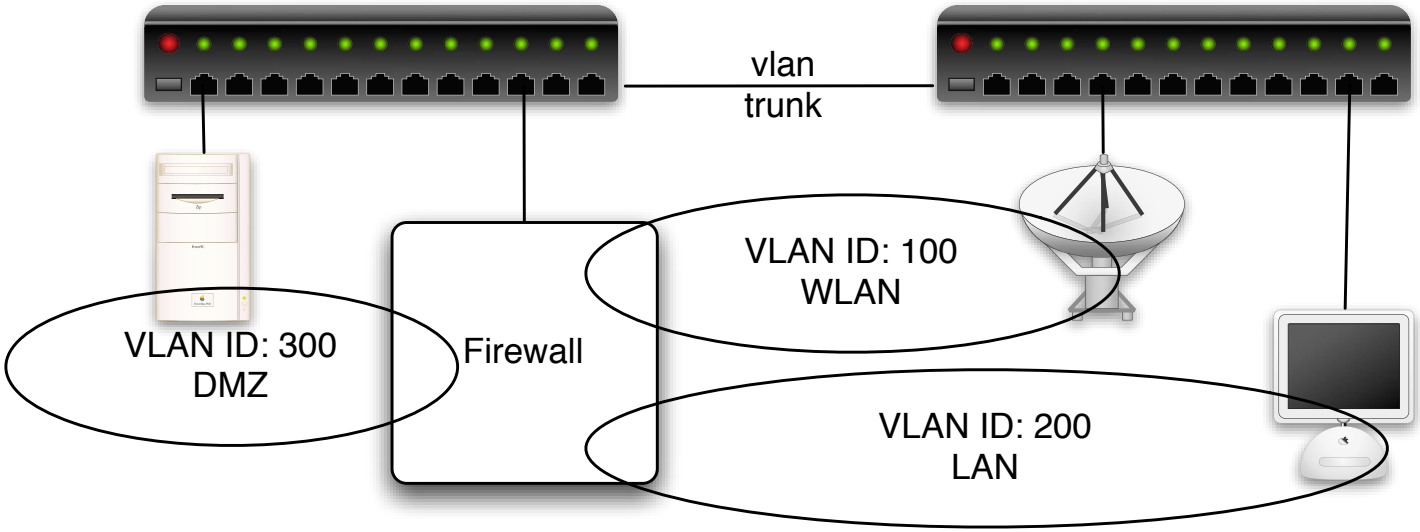
Denne opdeling kaldes VLAN og portbaseret er det mest simple

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 switche 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

Sample switch - less than 100 EUR ex VAT

JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots

TL-SG3210

- IP-MAC-Port-VID Binding, ACL, Port Security, DoS Defend, Storm control, DHCP Snooping, 802.1X Authentication and Radius provide you robust security strategies
- L2/L3/L4 QoS and IGMP snooping optimize voice and video application
- WEB/CLI managed modes, SNMP, RMON bring abundant management features

Understøtter VLANs 802.1q

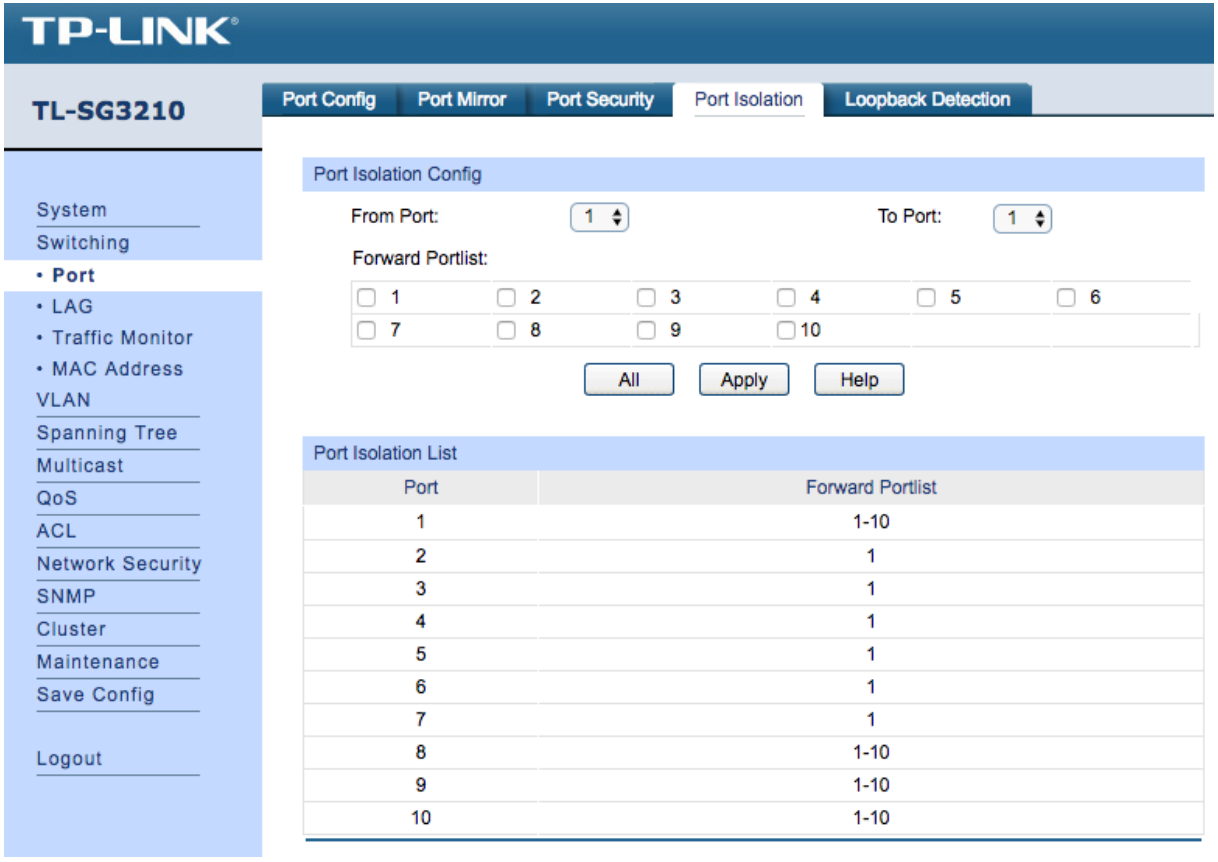
Port isolation, med forwarding list

IP ACLs!

SNMP, SSH

This is JUST AN EXAMPLE, research and select switches yourself

Port isolation



No subnetting, but individual ports cannot talk

Easier than subnetting and VLANs? Quick and dirty? ☺

VLANs i hjemmet

Jeg arbejder selv med en ide om at lave VLANs i hjemmet til diverse “funktioner”

media-vlan til chromecast og underholdning osv.

game-vlan til den ene teenagedreng

husets-vlan til automatisering, køleskabe osv.

lab-vlan1,2,3 - jeg laver altid diverse ting :-D

Guest-VLAN - gæsterne skal da isoleres

Hvilke mangler jeg?

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

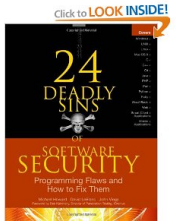
Example introductions:

- 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/`

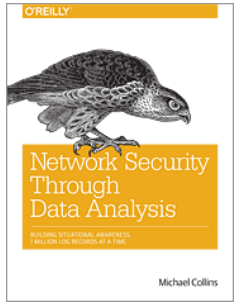
We are all Devops now, even security people!

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/`
Bornhack 2016 `https://www.instagram.com/bornhax/`
Reserver 22. - 29. August 2017! `https://bornhack.dk/`

Focus for the near future

- Walk through your infrastructure
  get a detailed view of data, flows, protocols, bandwidth, ports and services
- Automate pushing of 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 initate updates?

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