Welcome to

Penetration testing I
Introduktion til hacking og pentest metoder

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramshoej@Github

Try searching for pentest-I-foredrag.tex in the repo

Formålet i dag

Don’t Panic!

Introducere begrebet penetration testing og basale penetrationstestmetoder

Introducere basale værktøjer indenfor genren af hackerværktøjer

Give indblik i processen omkring sikkerhedstest

Skabe en grundig forståelse for hackerværktøjer samt penetrationstest metoder

Vise et hackerlab og kravene til de følgende workshops

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`

Brug hackerværktøjer!

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

Portscannere kan afsløre huller i forsvaret

Webtestværktøjer som crawler igennem et website og finder alle forms kan hjælpe

I vil kunne finde mange potentielle problemer proaktivt ved regelmæssig brug af disse værktøjer – også potentielle driftsproblemer

Husk dog penetrationstest er ikke en sølvkugle

Honeypots kan måske være med til at afsløre angreb og kompromitterede systemer hurtigere

Hacker – cracker

Det korte svar – drop diskussionen

Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig – og i dag har det begge betydninger.

I dag 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

Aftale om test af netværk

Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.

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
- Frygten for terror har forstærket ovenstående – så lad være!

ISC2 code of ethics

Code of Ethics Preamble:

- The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principles.
- Advance and protect the profession.

Hvis man vil CISSP certificeres skal man overholde ovenstående.
`https://www.isc2.org/ethics/default.aspx`

Er sikkerhedstest interessant?

Sikkerhedsproblemer i netværk er mange

Pentest kan være et krav fra eksterne – eksempelvis VISA PCI krav

- Chefen: skal vi ikke have en sikkerhedstest udført?
- IT-chefen: hmm, det kan vi da godt
- IT-medarbejderen: *gisp* – jeg ved sikkerheden halter flere steder!
- Husk at det ikke er jeres systemer – tag ikke kritik personligt, men som hjælp til at forbedre

Mange opdager fordelene efter et pentest projekt, prøv det!

Introduktion – begreber og teknologierne

Sikkerhedstest / penetrationstest
Afprøvning af sikkerhedsforanstaltninger og evaluering af sikkerhedsniveau ved hjælp af IT systemer og *hackerværktøjer*

Kaldes tillige sårbarhedstest, sårbarhedsanalyse m.v.

Ekstern – udføres fra internet, typisk over WAN

Intern, inside, on-site – udføres hos kunden, typisk over LAN og bag firewall

`https://www.google.com/search?q=sikkerhedstest`

Blackbox, greybox og whitebox

Forudsætninger og forudgående kendskab til miljøet

Afhængig af de informationer der er tilgængelige om opbygningen af det scannede netværk forud for NetSikkerhedsanalysen taler man om henholdsvis White, Grey og Black Box testning.

- Black Box testen involverer en sikkerhedstestning af et netværk uden nogen form for insider viden om systemet udover den IP-adresse, der ønskes testet. Dette svarer til den situation en fjendtlig hacker vil stå i og giver derfor det mest realistiske billede af netværkets sårbarhed overfor angreb udefra. Men er dårlig ressourceudnyttelse.
- I den anden ende af skalaen har vi White Box testen. I dette tilfælde har sikkerhedsspecialisten både før og under testen fuld adgang til alle informationer om det scannede netværk. Analysen vil derfor kunne afsløre sårbarheder, der ikke umiddelbart er synlige for en almindelig angriber. En White Box test er typisk mere omfattende end en Black Box test og forudsætter en højere grad af deltagelse fra kundens side, men giver en meget detaljeret og tilbundsgående undersøgelse.
- En Grey Box test er som navnet siger et kompromis mellem en White Box og en Black Box test. Typisk vil sikkerhedsspecialisten udover en IP-adresse være i besiddelse af de mest grundlæggende systemoplysninger: Hvilken type af server der er tale om (mail-, webserver eller andet), operativsystemet og eventuelt om der er opstillet en firewall foran serveren.

Fordele ved at få udført planlagt sikkerhedstest

Formålet med en sikkerhedstest er at nedbringe risici for systemerne og sikre organisationen mod uventede tab af data, tab af omdømme, forøgede omkostninger.

Målgrupper:

- IT-afdeling og teknisk personale
- Ledelse, koncernledelse
- Eksterne revisorer, VISA PCI, offentligheden

Afleveringer:

- Rapport med tekniske anbefalinger og opsummering/checklister
- Executive summary

Formålet er ikke at udpege en syndebuk eller identificere dårlige medarbejdere!

Persongalleri, Godkendelse og tilladelse

Sikkerhedskonsulent – den konsulent der kommer ud til kunden

Inden en test kan udføres skal der indhentes tilladelser fra:

- Systemejer – den ansvarlige for et bestemt system
- Netværksejer – den ansvarlige for netværk hos kunden
- Driftorganisation – dem der driver systemerne
- Sikkerhedsansvarlig – den ansvarlige for sikkerheden hos kunden
- Kontaktperson udpeges – kundens ansatte som kan hjælpe med praktiske spørgsmål og skabe kontakt til de rette personer i kundens organisation

Planlægning af sikkerhedstest

Sårbarhedsanalysens omfang aftales på forhånd

- Scope – hvad skal testes
- Hvornår skal testes – indenfor et aftalt tidsrum, wall clock time
- Hvor testes fra – logfilerne vil afsløre IP-adresser
- Kan overskrides delvist – eksempelvis ved port 80 scan på samme subnet eller tilsvarende
- Skal der forsøges ude af drift angreb – DoS
- Se endvidere slide om Rules of engagement senere

Sårbarhedsanalysen omfatter (targets):

- 192.168.1.1 – firewall/router
- 192.168.1.2 – mailserver
- 192.168.1.3 – webserver
- Testen udføres i tidsrummet mandag 1. til fredag 5.
- Testere udfører *angreb* fra 192.0.2.0/28

Før konsulenten ankommer – forberedelse

Testplan med oversigt over targets og IP-adresser

Netværkstegninger og anden information som er aftalt oplyst

Hvor skal sikkerhedskonsulenten placeres ved insidetest – ikke i serverrum, tak :-)

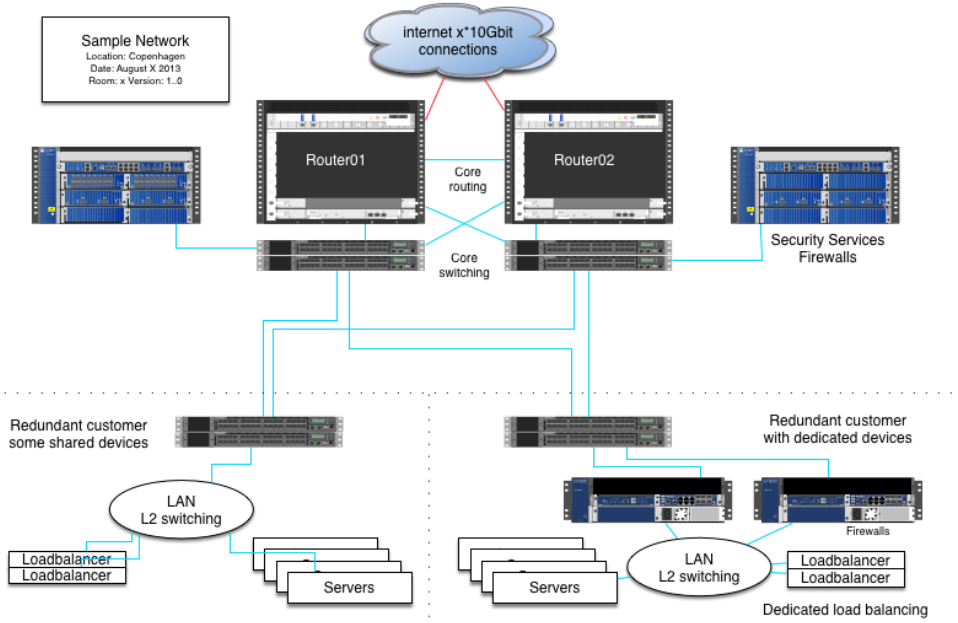
Kabling af netværksstik

Gæstekort – til test over flere dage

Kantine, toiletter osv.

Betragt det som en ny kollega – med tidsbegrænset kontrakt

Udvælgelse af systemer til test



Typiske interessante mål og årsager

- Routere på netværksvejen til kritiske systemer og netværk - tilgængelighed
- Firewall – begrænses trafikken tilstrækkeligt
- Mailservere – tillades relaying udefra
- Webservere – kan der afvikles kode på systemet, downloades data

Scannerudstyr på insidetest

Scannersystemer, hardware og software kræver en del ekspertice og opsætning. Det er tidskrævende at foretage denne opsætning og konsulenten har på forhånd udvalgt og konfigureret udstyr til testen. Det skal derfor accepteres at konsulenten tilslutter eget udstyr til de pågældende netværk og dette sker naturligvis under strenge krav til konsulentens udstyr.

Det er ikke en mulighed at bruge kundens udstyr!

Testens udførelse

Testen udføres ved samarbejde mellem konsulent og virksomhed

Først og fremmest skal testen startes

- Når konsulenten ankommer kontaktes kontaktpersonen
- Konsulenten vises til rette og pakker ud/stiller op
- Såfremt det ønskes inspiceres og godkendes udstyret
- Konsulenten tilslutter sig netværket og test er officielt igang
- Konsulenten verificerer adgangen til netværk og melder klar, begynder test

... tiden går ... testen udføres ...

Kontaktpersonen er hele tiden til rådighed på mobiltelefon

Testen afsluttes og der pakkes ned i modsat rækkefølge

Afbrydelse af testen – kompromitterede maskiner

Der kan være årsager der medfører at testen skal indstilles

Sikkerhedskonsulenten afbryder testen

- Det anses for uforsvarligt at fortsætte, der er fundet kompromitterede systemer eller beviser der kan ødelægges
- Netværket er dårligt, mulighederne for udførelse er forringet

Kunden ønsker at afbryde testen

- Der opleves for store problemer under udførelsen
- Systemnedbrud på forretningskritiske systemer
- Andre kriser der gør det valgte tidspunkt uegnet

NB: Eksempler! – man afbryder altid når kunden ønsker det!

Oprydning efter testen

Sikkerhedskonsulenten er ansvarlig for:

- Fjerne data fra systemerne
- Fjerne brugerkonti, få fjernet brugeroplysninger og loginmuligheder
- Fjerne software som ikke skal benyttes mere

Driftsorganisationen er ansvarlig for:

- Undersøgelse af systemerne
- Eventuel genstart af systemer, der kan være nedsat effektivitet
- Fjerne patchkabler for stik der er kablet speciet til konsulenten

Afrapportering – resultater

Hvad indeholder en sikkerhedstest rapport:

- Titel, indholdsfortegnelse, firmanavne – ca. 15-30 sider for 5 hosts
- Fortrolighedserklæring – det er fortrolige oplysninger
- Executive summary – ofte i større virksomheder
- Information om den udførte scanning
- Omfang/scope
- Gennemgang af targets – detaljeret information og med anbefalinger
- Konklusion – ofte mere teknisk
- Bilag – detaljerede oplysninger og oversigter, checklister

Det er organisationen der selv vælger hvilke anbefalinger der følges

Rules of engagement – regler og etik for sikkerhedstest

- NB: Stor forskel på Danmark og udlandet!
- Sikkerhedskonsulenten må ikke give anledning til nye sårbarheder som følge af testen
- Sikkerhedskonsulenten må ikke installere ny software på systemer uden forudgående aftale
- Sikkerhedskonsulenten efterlader ikke usikre systemadministratorkonti eller tilsvarende efter testen
- Sikkerhedskonsulenten tager altid kontakt til kunden ved høj-risiko sårbarheder
- Er man hyret til netværkssikkerhed kan man godt *snuse* lidt rundt om systemerne under test – der kan være et sårbart testsystem lige ved siden af
- Min holdning er at ved opdagelse af åbenlyse sikkerhedsrisici dokumenteres disse i rapporten, uanset scope for opgaven ellers

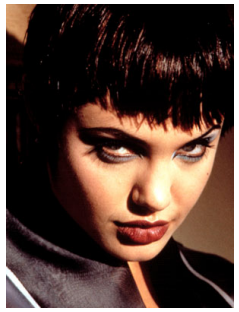
Det er en balancegang

Konsulentens udstyr – vil du være sikkerhedskonsulent

Laptops, gerne flere, men én er nok til at lære!

- Sikkerhedskonsulenterne bruger typisk Open Source værktøjer på Linux og enkelte systemer med Windows – jeg bruger helst Windows 7 i dag
- Netværkserfaring *TCP/IP protocol suite* – TCP, UDP, ICMP osv. i detaljer
- Programmmeringserfaring er en fordel
- Linux/Unix kendskab er ofte en **nødvendighed**
  - fordi de nyeste værktøjer er skrevet til Unix i form af Linux og BSD
- *A Hands-On Introduction to Hacking by Georgia Weidman*, June 2014
  `http://www.nostarch.com/pentesting`
- Metasploit Unleashed – gratis kursus i Metasploit
  `https://www.offensive-security.com/metasploit-unleashed/`

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 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

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

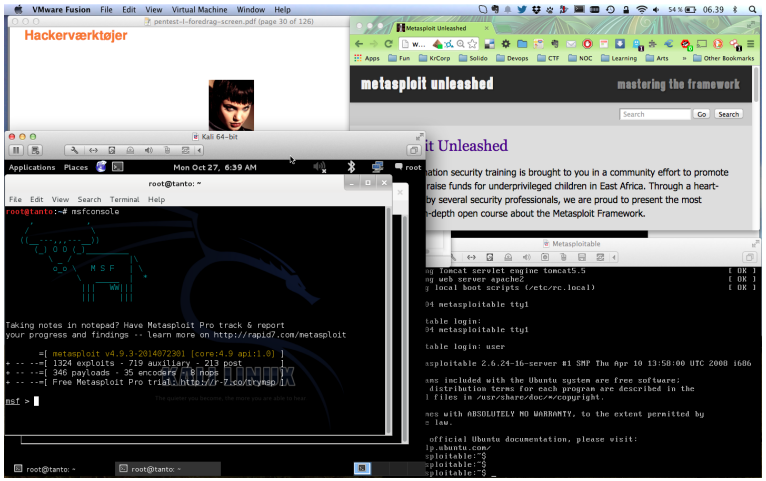
Udnyttelse/afprøvning: Metasploit, Nikto, exploit programs

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.

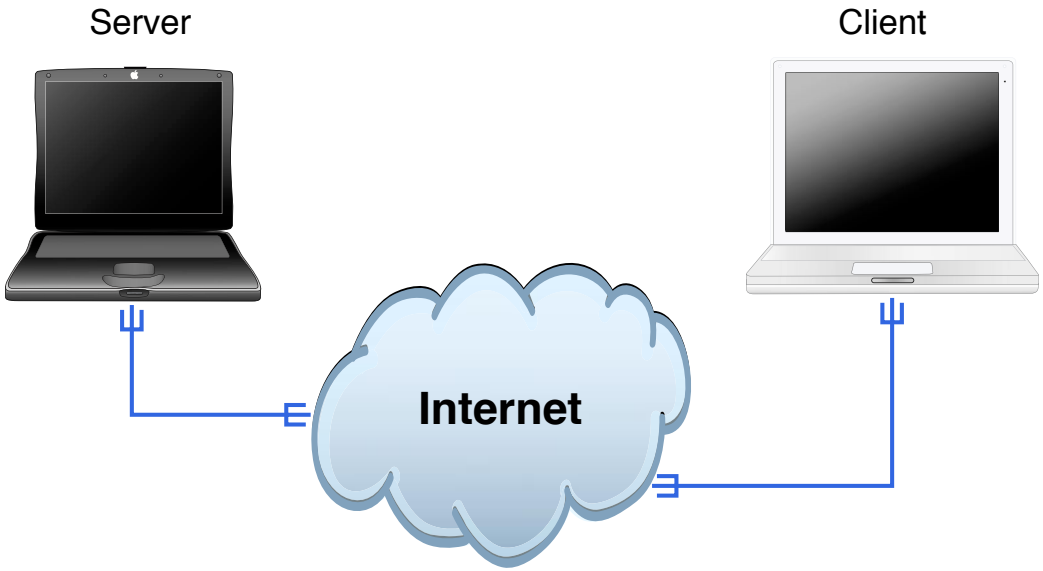
Hackerlab opsætning



- 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, ...

Teknisk hvad er hacking

Internet i dag



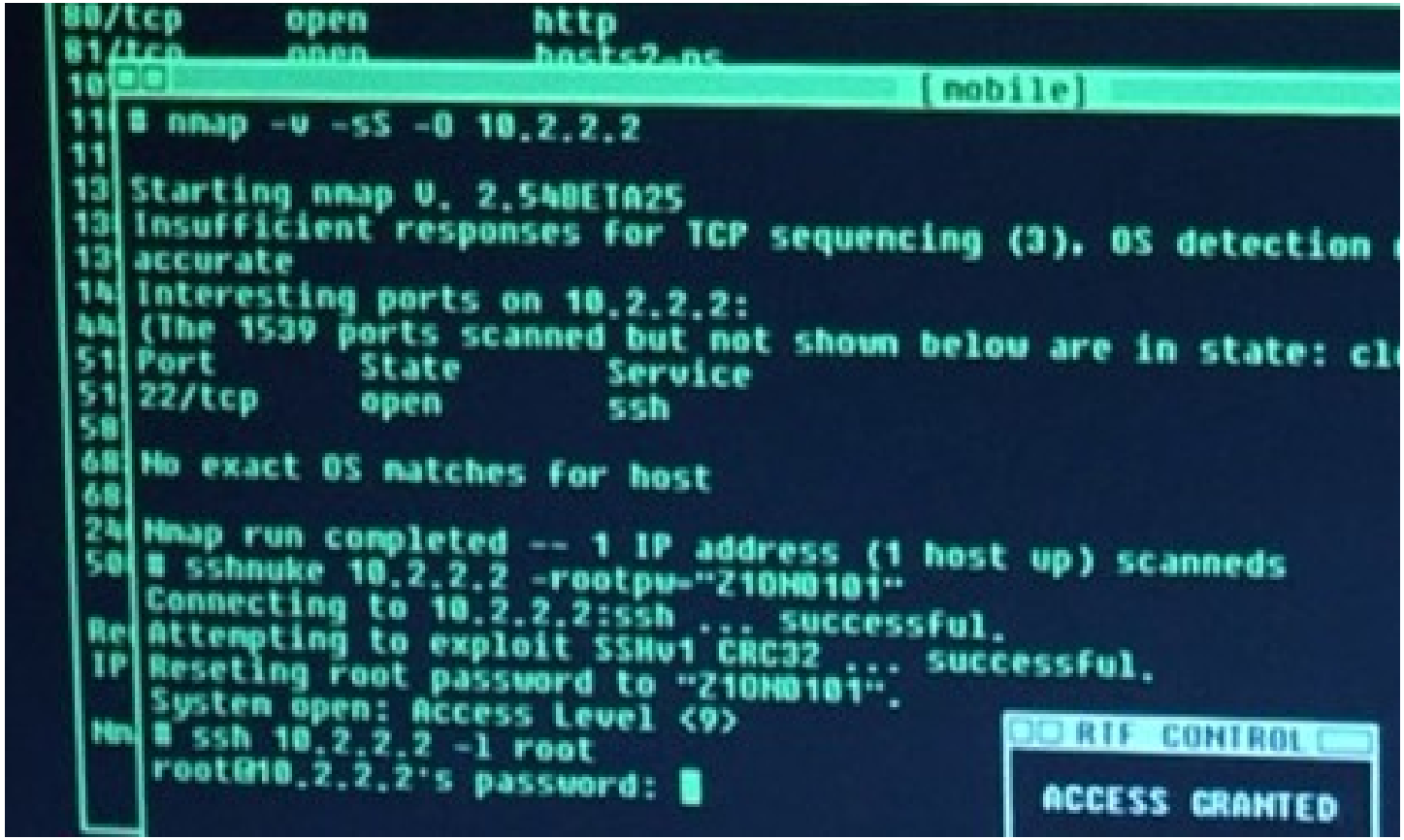
Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

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

Trinity breaking in



Meget realistisk - sådan foregår det næsten:

`https://nmap.org/movies/`

`https://youtu.be/51lGCTgqE_w`

Hacking er magi

Hacking ligner indimellem magi

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

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

og man kan aflæse de godkendte når de er aktive på netværket

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

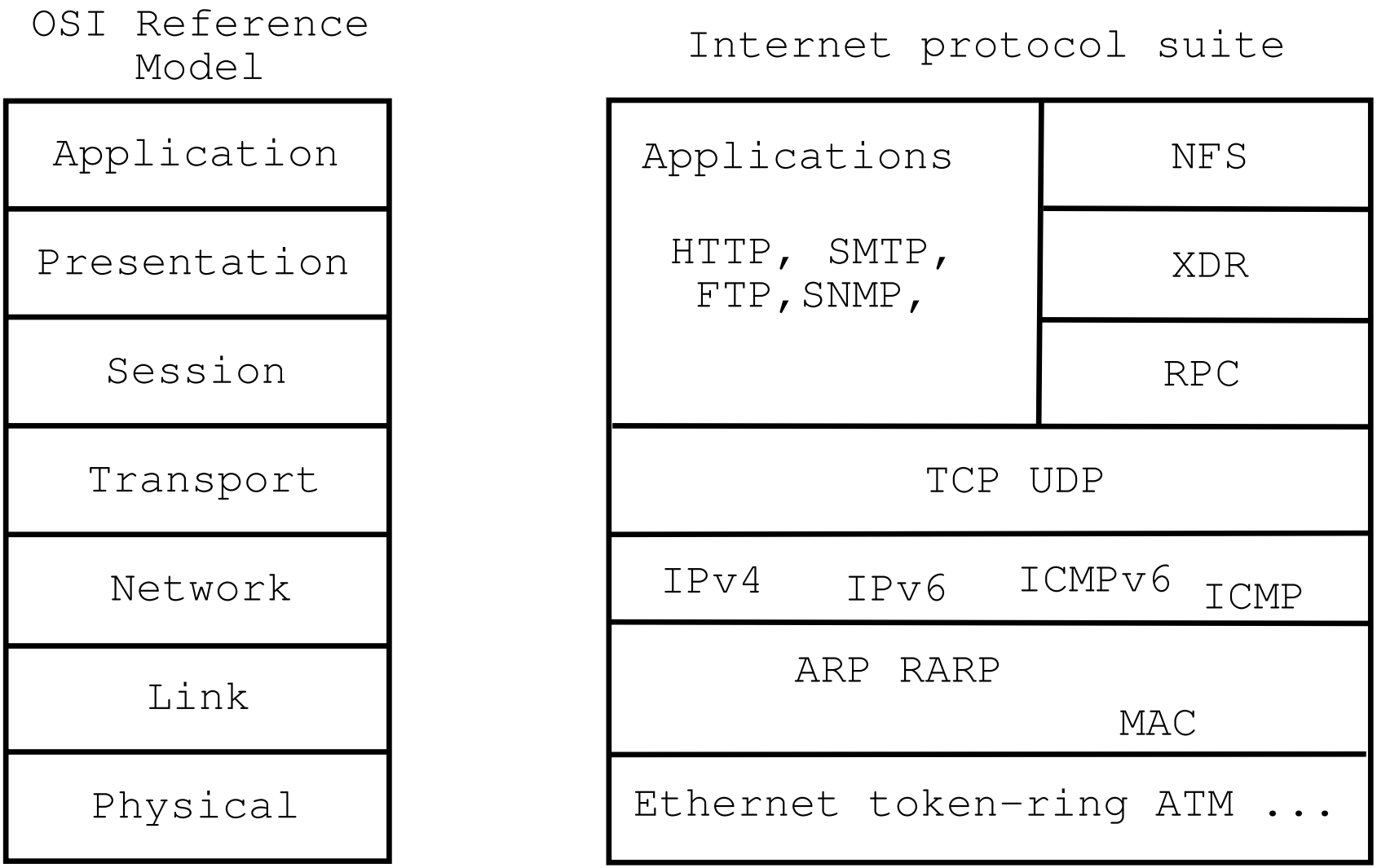
Løsninger?

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

MAC filtrering

OSI og Internet modellerne



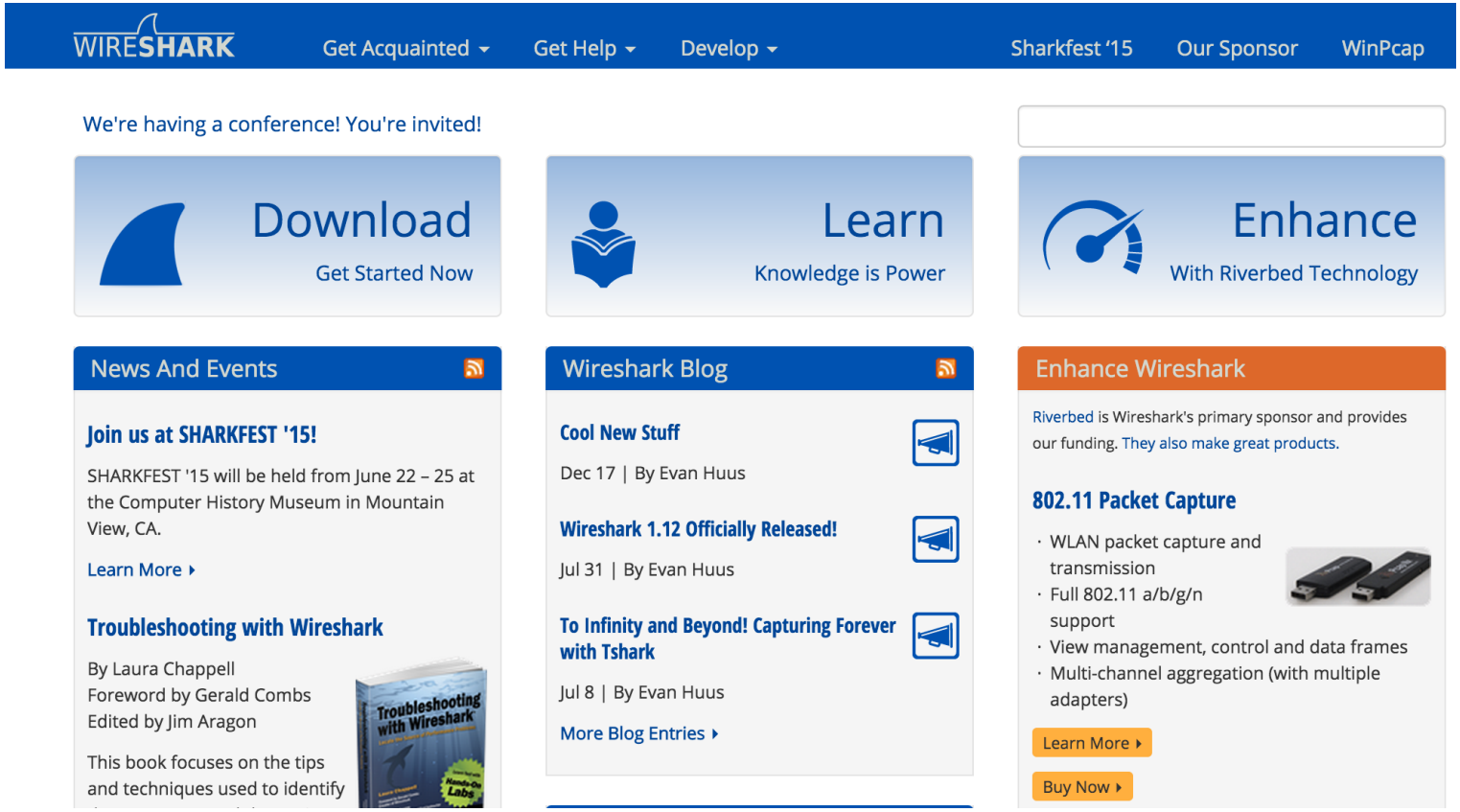
Kali Linux the new backtrack

BackTrack – `http://www.backtrack-linux.org`

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

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

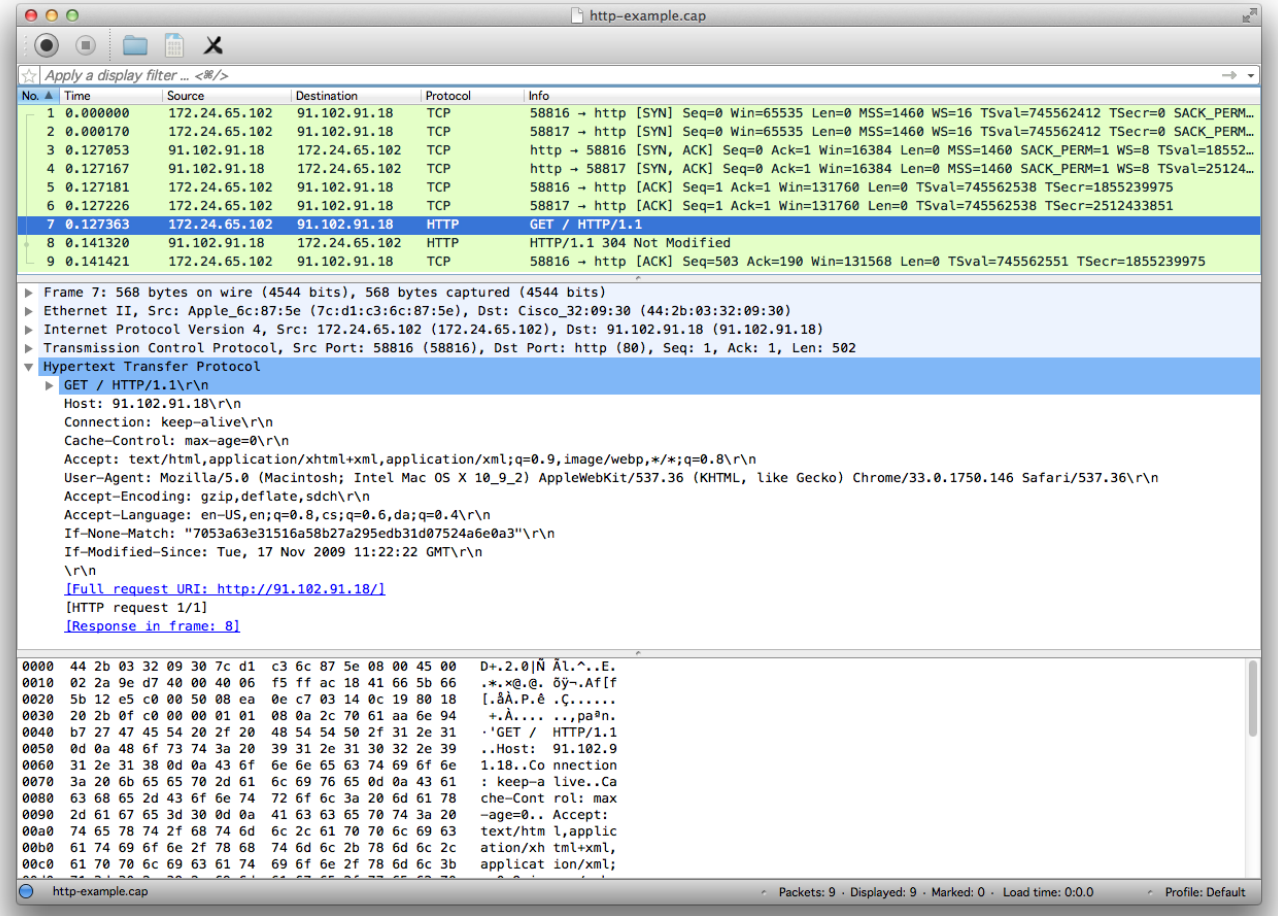
Wireshark – grafisk pakkesniffer



https://www.wireshark.org

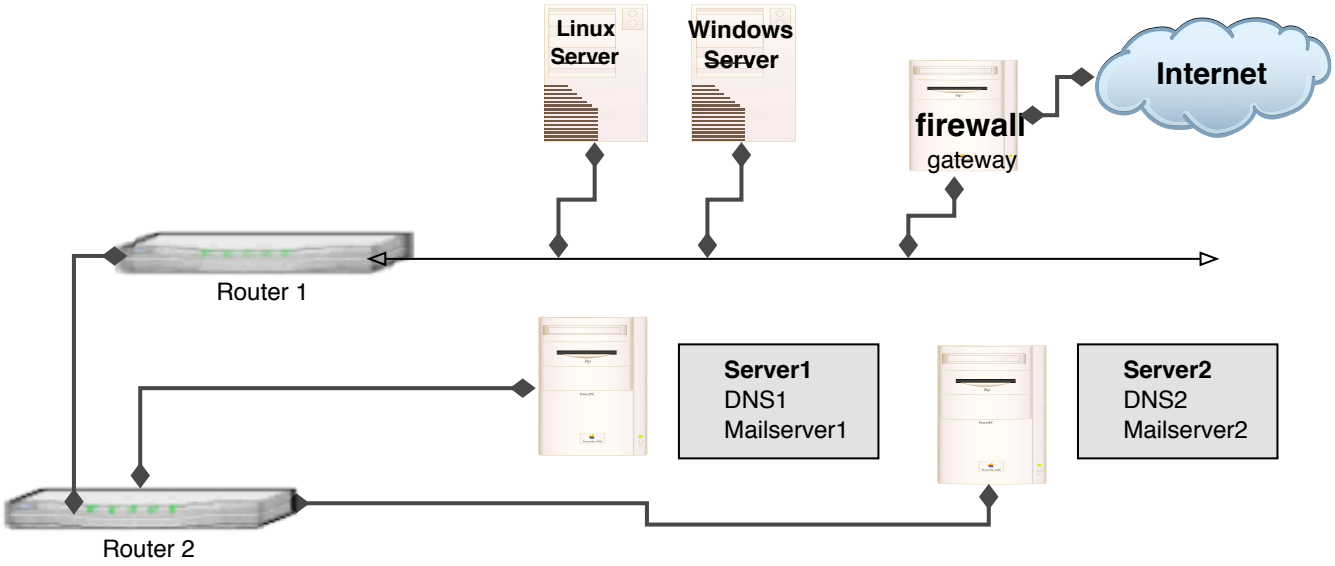
Både til Windows og Unix

Brug af Wireshark



Læg mærke til filtermulighederne

Network mapping



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

Levetiden (TTL) for en pakke tælles ned på hver router, sættes denne lavt opnår man at pakken *timer ud* – besked fra hver router på vejen

Default Unix er UDP pakker, Windows tracert ICMP pakker

traceroute – med UDP

```
 #  tcpdump -i en0 host 10.20.20.129 or host 10.0.0.11
tcpdump: listening on en0
23:23:30.426342 10.0.0.200.33849 > router.33435: udp 12  [ttl 1]
23:23:30.426742 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.436069 10.0.0.200.33849 > router.33436: udp 12  [ttl 1]
23:23:30.436357 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.437117 10.0.0.200.33849 > router.33437: udp 12  [ttl 1]
23:23:30.437383 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.437574 10.0.0.200.33849 > router.33438: udp 12
23:23:30.438946 router > 10.0.0.200: icmp: router  udp port 33438 unreachable
23:23:30.451319 10.0.0.200.33849 > router.33439: udp 12
23:23:30.452569 router > 10.0.0.200: icmp: router  udp port 33439 unreachable
23:23:30.452813 10.0.0.200.33849 > router.33440: udp 12
23:23:30.454023 router > 10.0.0.200: icmp: router  udp port 33440 unreachable
23:23:31.379102 10.0.0.200.49214 > safri.domain:  6646+ PTR?
200.0.0.10.in-addr.arpa. (41)
23:23:31.380410 safri.domain > 10.0.0.200.49214:  6646 NXDomain* 0/1/0 (93)
14 packets received by filter
0 packets dropped by kernel
```

Basal Portscanning

Hvad er portscanning

Afprøvning af alle porte fra 0/1 og op til 65535

Målet er at identificere åbne porte – sårbare services

Typisk TCP og UDP scanning

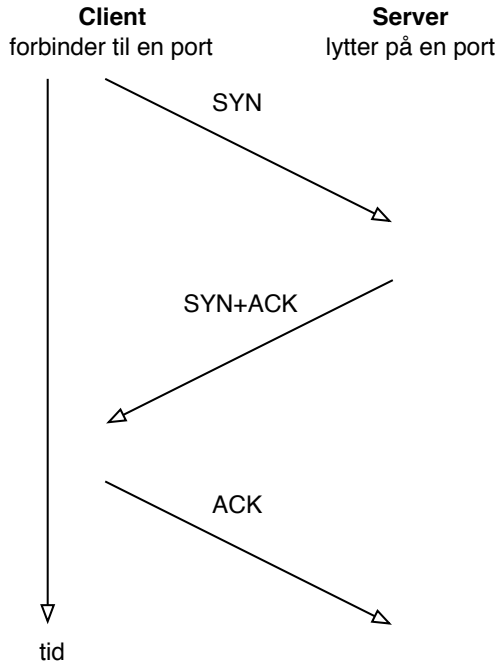
TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere, skal svare SYN

UDP applikationer svarer forskelligt – hvis overhovedet
Svarer på rigtige forespørgsler, uden firewall svares ICMP på lukkede porte

Brug GUI programmet Zenmap mens i lærer Nmap at kende

TCP three-way handshake



- **TCP SYN half-open** scans
- Tidligere loggede systemer kun når der var etableret en fuld TCP forbindelse – dette kan/kunne udnyttes til *stealth*-scans
- Hvis en maskine modtager mange SYN pakker kan dette fylde tabellen over connections op – og derved afholde nye forbindelser fra at blive oprette – **SYN-flooding**

Ping og port sweep

Scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

- konfigurer en maskine med to IP-adresser som ikke er i brug
- hvis der kommer trafik til den ene eller anden er det portscan
- hvis der kommer trafik til begge IP-adresser er der nok foretaget et sweep – bedre hvis de to adresser ligger et stykke fra hinanden

Pro tip: Hvis du leder efter et Netværks IDS, så kig på Suricata `suricata-ids.org`

Nmap port sweep efter webservere

```
root@cornerstone:~#  nmap -p80,443 172.29.0.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:31 CET
Nmap scan report for 172.29.0.1
Host is up (0.00016s latency).
PORT    STATE    SERVICE
80/tcp  open     http
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00012s latency).
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:46:22:FB (VMware)
```

Nmap port sweep efter SNMP port 161/UDP

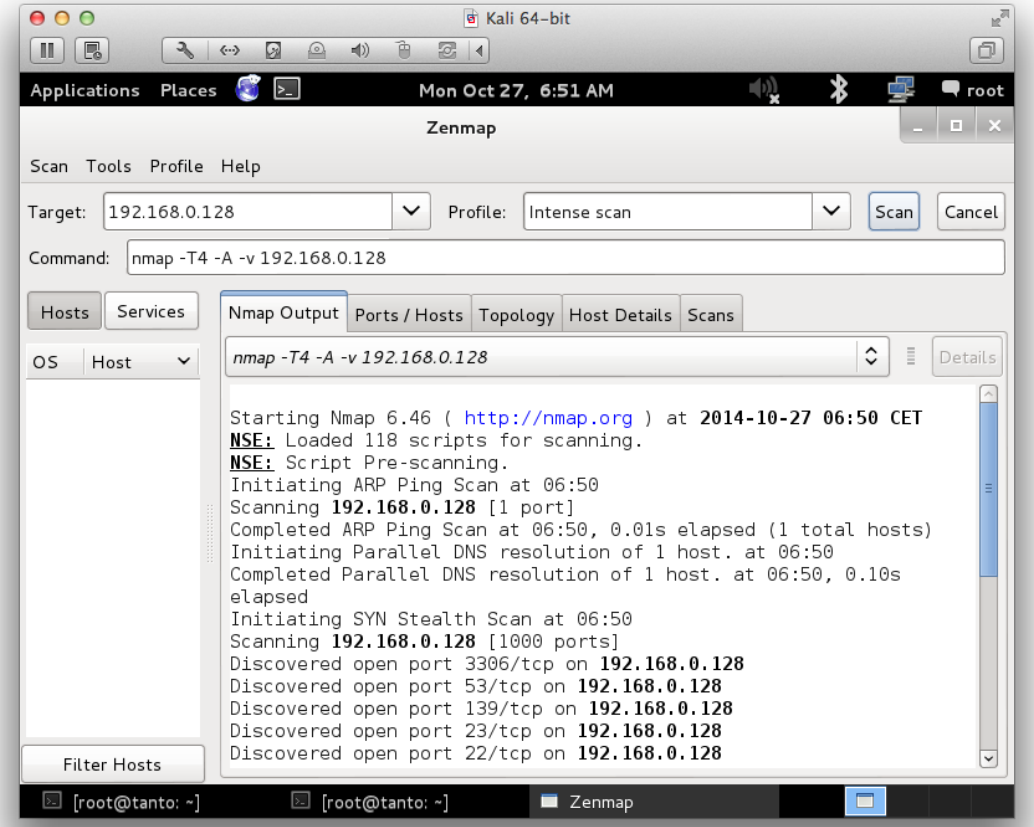
```
root@cornerstone:~# nmap -sU -p 161 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:30 CET
Nmap scan report for 172.29.0.1
Host is up (0.00015s latency).
PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00011s latency).
PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 00:0C:29:46:22:FB (VMware)
...
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.18 seconds
```

Nmap Advanced OS detection

```
root@cornerstone:~# nmap -A -p80,443 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:37 CET
Nmap scan report for 172.29.0.1
Host is up (0.00027s latency).
PORT    STATE    SERVICE VERSION
80/tcp  open     http    Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: media device|general purpose|phone
Running: Apple iOS 6.X|4.X|5.X, Apple Mac OS X 10.7.X|10.9.X|10.8.X
OS details: Apple iOS 6.1.3, Apple Mac OS X 10.7.0 (Lion) - 10.9.2 (Mavericks)
or iOS 4.1 - 7.1 (Darwin 10.0.0 - 14.0.0), Apple Mac OS X 10.8 - 10.8.3 (Mountain Lion)
or iOS 5.1.1 - 6.1.5 (Darwin 12.0.0 - 13.0.0)
OS and Service detection performed.
Please report any incorrect results at http://nmap.org/submit/
```

- Lavniveau måde at identificere operativsystemer på, prøv også `nmap -A`
- Send pakker med *anderledes* indhold, observer svar
- En tidlig og detaljeret reference: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin, 2001

Portscan med Zenmap GUI



Zenmap følger med i pakken når man henter Nmap `https://nmap.org`

Erfaringer hidtil

Mange oplysninger

Kan man stykke oplysningerne sammen kan man sige en hel del om netværket

En skabelon til registrering af maskiner er god

- Svarer på ICMP: □ echo, □ mask, □ time
- Svarer på traceroute: □ ICMP, □ UDP
- Åbne porte TCP og UDP:
- Operativsystem:
- ... (banner information m.v.)

Mange små pakker kan oversvømme store forbindelser og give problemer for netværk

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 is yet another bug in SSL products

What versions of the OpenSSL are affected?
Status of different versions:

* OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
* OpenSSL 1.0.1g is NOT vulnerable
* OpenSSL 1.0.0 branch is NOT vulnerable
* OpenSSL 0.9.8 branch is NOT vulnerable

Bug was introduced to OpenSSL in December 2011 and has been out in the wild since OpenSSL release 1.0.1 on 14th of March 2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.

It's just a bug - but a serious one

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.

Proof of concept programs exist - god or bad?

Some of the tools released shortly after Heartbleed announcement

- `https://github.com/FiloSottile/Heartbleed` tool i Go
  site `http://filippo.io/Heartbleed/`
- `https://github.com/titanous/heartbleeder` tool i Go
- `https://gist.github.com/takeshixx/10107280` test tool med STARTTLS support
- `http://possible.lv/tools/hb/` test site
- `https://twitter.com/richinseattle/status/453717235379355649` Practical Heartbleed attack against session keys links til, `https://www.mattslifebytes.com/?p=533` og "Fully automated here "
  `https://www.michael-p-davis.com/using-heartbleed-for-hijacking-user-sessio`
- Metasploit er også opdateret på master repo
  `https://twitter.com/firefart/status/453758091658792960`
  `https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliar`
  `scanner/ssl/openssl_heartbleed.rb`

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

Compare SSL

```
/* Read type and payload length first */
  if (1 + 2 + 16 > s->s3->rrec.length)
      return 0; /* silently discard */
  hbtype = *p++;
  n2s(p, payload);
  if (1 + 2 + payload + 16 > s->s3->rrec.length)
      return 0; /* silently discard per RFC 6520 sec. 4 */
  pl = p;
```

Ditch OpenSSL - write our own?

SSL implementations compared - above code from OpenSSL copied from this:
`http://tstarling.com/blog/2014/04/ssl-implementations-compared/`

LibreSSL announced, OpenBSD people
`http://www.libressl.org/` and `http://opensslrampage.org/`

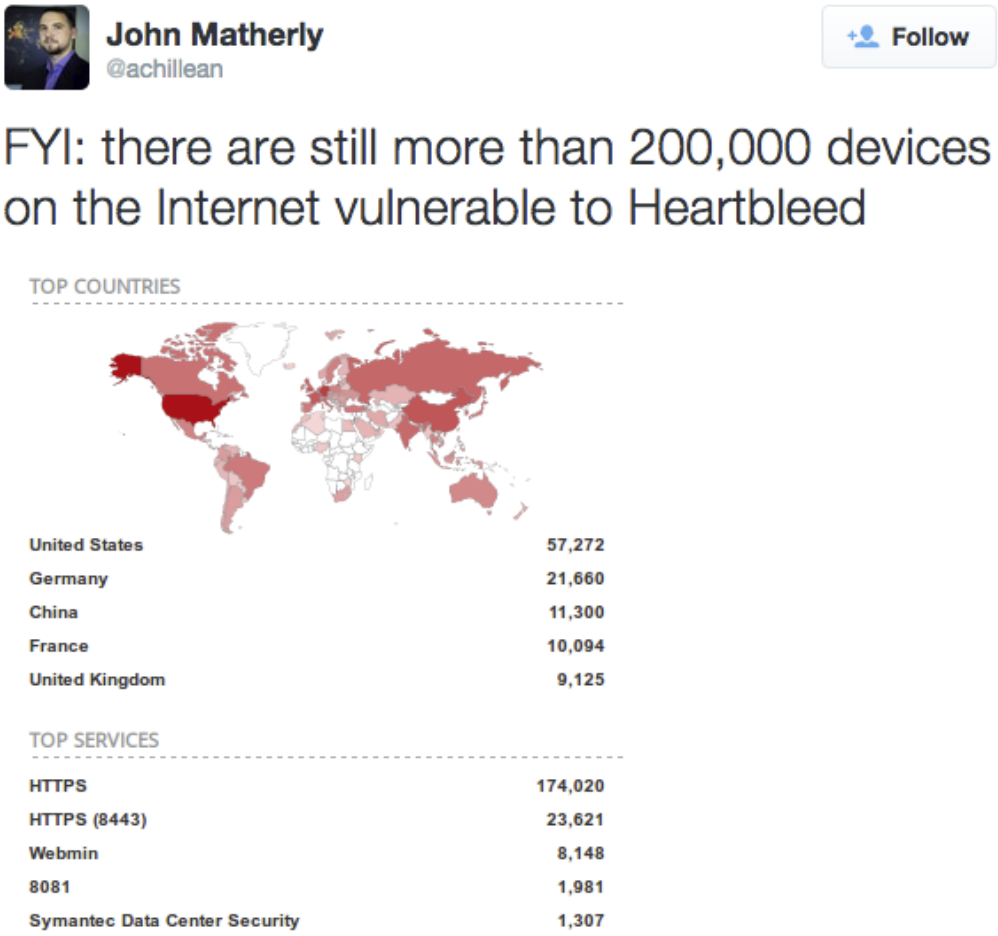
Key points after heartbleed

Source: picture source

`https://www.duosecurity.com/blog/heartbleed-defense-in-depth-part-2`

- Writing SSL software and other secure crypto software is hard
- Configuring SSL is hard
  check you own site `https://www.ssllabs.com/ssltest/`
- SSL is hard, finding bugs ”all the time”`http://armoredbarista.blogspot.dk/2013/01/a-brief-chronology-of-ssltls-attacks.html`
- Rekeying is hard - slow, error prone, manual proces - Automate!
- Proof of concept programs exist - god or bad?

September 2015: Heartbleed vulnerable servers



John Matherly
@achillean

Follow

FYI: there are still more than 200,000 devices on the Internet vulnerable to Heartbleed

TOP COUNTRIES

United States	57,272
Germany	21,660
China	11,300
France	10,094
United Kingdom	9,125

TOP SERVICES

HTTPS	174,020
HTTPS (8443)	23,621
Webmin	8,148
8081	1,981
Symantec Data Center Security	1,307

Source: Data from Shodan and Shodan Founder John Matherly

2016: Heartbleed vulnerable servers

Source: Data from Shodan and Shodan Founder John Matherly

`https://www.shodan.io/report/89bnfUyJ`

Simple Network Management Protocol

SNMP er en protokol der supporteres af de fleste professionelle netværksenheder, såsom switche, routere

hosts – skal slås til men følger som regel med

SNMP bruges til:

- *network management*
- statistik
- rapportering af fejl – SNMP traps

Sikkerheden baseres på community strings der sendes som klartekst ...

Det er nemmere at brute-force en community string end en brugerid/kodeord kombination

Brute force

Hvad betyder bruteforcing?
afprøvning af alle mulighederne

```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]

Options:
  -S         connect via SSL
  -s PORT    if the service is on a different default port, define it here
  -l LOGIN   or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS    or -P FILE try password PASS, or load several passwords from FILE
  -e ns      additional checks, "n" for null password, "s" try login as pass
  -C FILE    colon seperated "login:pass" format, instead of -L/-P option
  -M FILE    file containing server list (parallizes attacks, see -T)
  -o FILE    write found login/password pairs to FILE instead of stdout
...
```

John the Ripper

> John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

Unix passwords kan knækkes med alec Muffets kendte Crack program eller eksempelvis John the Ripper `http://www.openwall.com/john/`

Jeg bruger selv John the Ripper

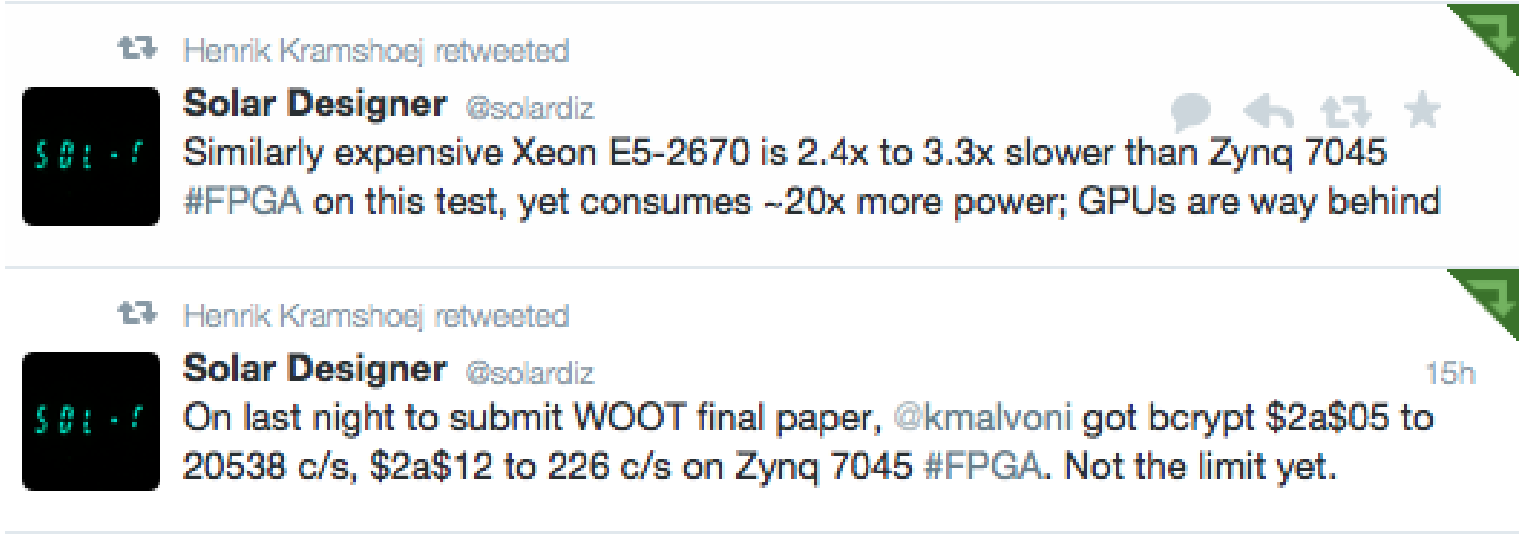
Cracking passwords

- 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:

`https://hashcat.net/wiki/`
`http://www.openwall.com/john/`

Parallella John



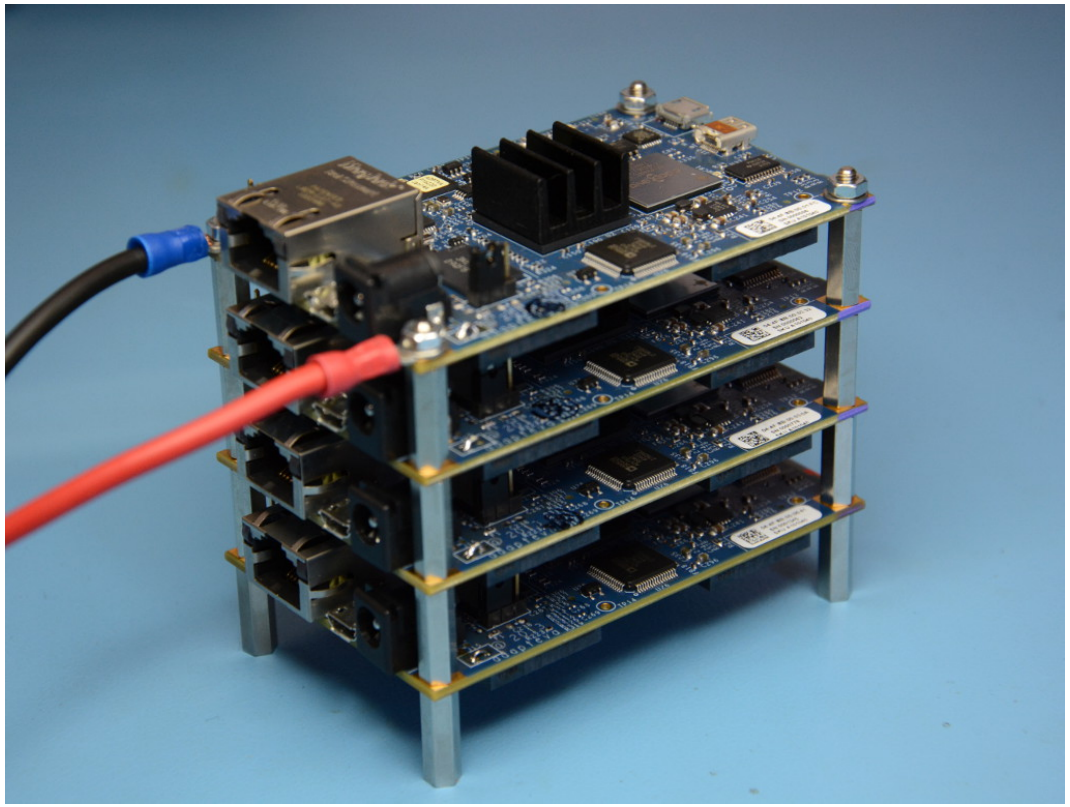
`https://twitter.com/solardiz/status/492037995080712192`

FPGA hacking er populært

Dog mange forskellige hardware systemer/modeller

Ringere support for algoritmer

Stacking Parallella boards



FPGA og ASICS må vi forvente at eksempelvis NSA bruger

`https://www.parallella.org/`

`https://en.wikipedia.org/wiki/Application-specific_integrated_circuit`

Getting to your data: Google for it

Google as a hacker tool? oprindeligt beskrevet af Johnny Long

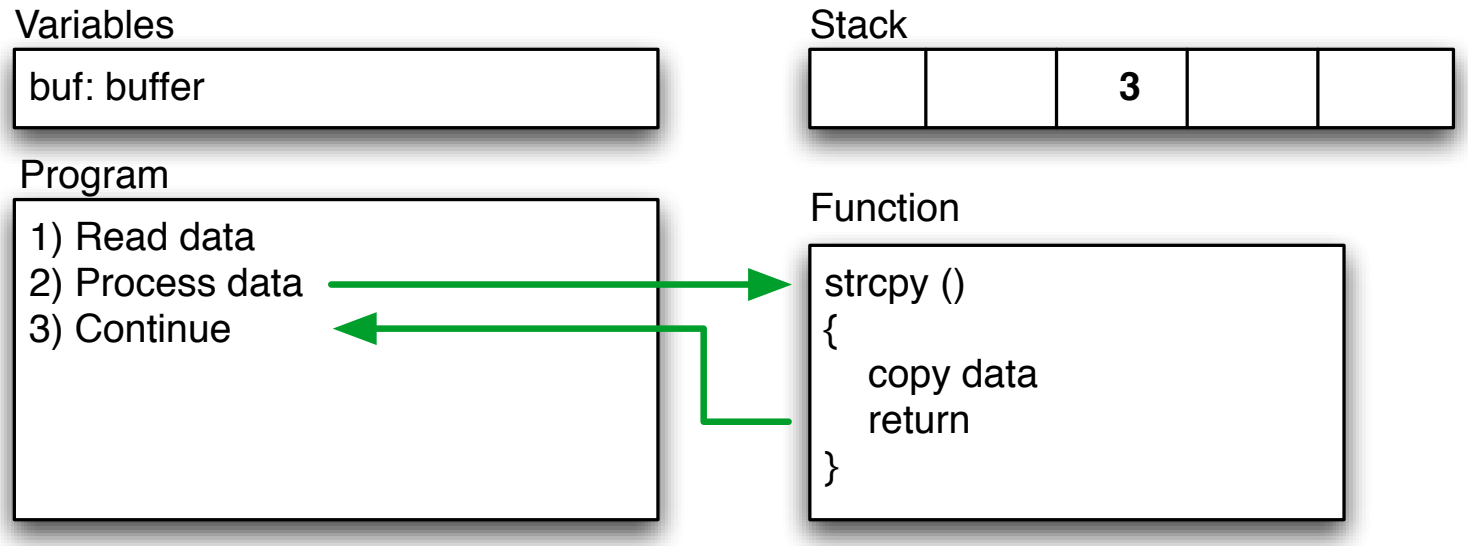
Concept named googledorks when google indexes information not supposed to be public `http://www.exploit-db.com/google-dorks/`

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.

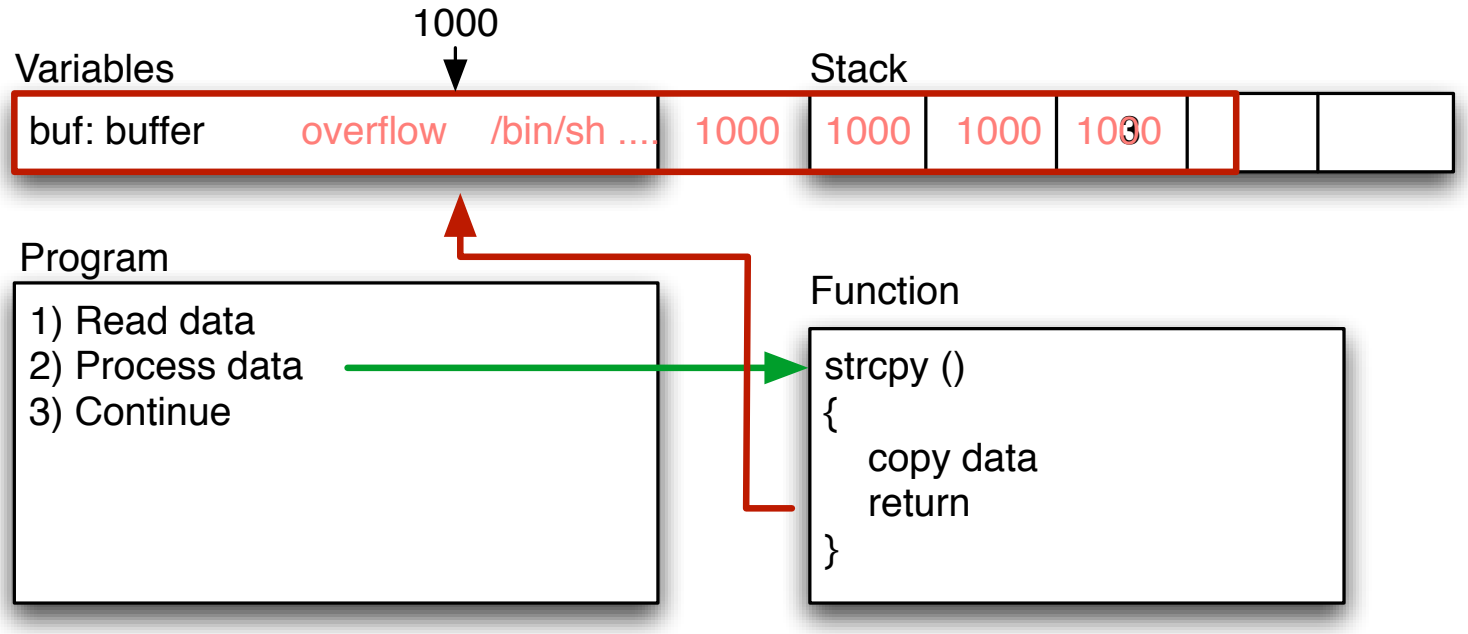
Buffer og stacks




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

PS Simplificeret gennemgang

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

Privilegier least privilege

Hvorfor afvikle applikationer med administrationsrettigheder - hvis der kun skal læses fra eksempelvis en database?

Least privilege betyder at man afvikler kode med det mest restriktive sæt af privileger – kun lige nok til at opgaven kan udføres

Dette praktiseres sjældent i webløsninger i Danmark

Privilegier privilege escalation

Privilege escalation er når man på en eller anden vis opnår højere privileger på et system, eksempelvis som følge af fejl i programmer der afvikles med højere privilegier. Derfor HTTPD servere på Unix afvikles som nobody – ingen specielle rettigheder.

En angriber der kan afvikle vilkårlige kommandoer kan ofte finde en sårbarhed som kan udnyttes lokalt – få rettigheder = lille skade

Eksempel: man finder exploit som giver kommandolinieadgang til et system som almindelig bruger

Ved at bruge en local exploit, Linuxkernen kan man måske forårsage fejl og opnå root, GNU Screen med SUID bit eksempelvis

Local vs. remote exploits

Local vs. remote angiver om et exploit er rettet mod en sårbarhed lokalt på maskinen, eksempelvis opnå højere privilegier, eller beregnet til at udnytter sårbarheder over netværk

Remote root exploit - den type man frygter mest, idet det er et exploit program der når det afvikles giver angriberen fuld kontrol, root user er administrator på Unix, over netværket.

Zero-day exploits dem som ikke offentliggøres – dem som hackere holder for sig selv. Dag 0 henviser til at ingen kender til dem før de offentliggøres og ofte er der umiddelbart ingen rettelser til de sårbarheder

Demo: Insecure programming buffer overflows 101

NB: udelades måske hvis vi mangler tid

Forslag til fremgangsmåde:

- Prøv at skrive dette program ind som `demo.c`
- Dernæst oversættes med kommandoen: `gcc -o demo demo.c`
- start programmet med kommandoen `./demo test` eller andre input

Hjælp:

```
main(int argc, char **argv)
{       char buf[10];
        strcpy(buf, argv[1]);
        printf("%s\n",buf);
}
the_shell()
{  system("/bin/sh");  }
```

GDB GNU Debugger

GNU compileren og debuggeren fungerer ok, men check andre!

Prøv `gdb ./demo` og kør derefter programmet fra *gdb prompten* med `run 1234`

Når I således ved hvor lang strengen skal være kan I fortsætte med `nm` kommandoen – til at finde adressen på `the_shell`
Skriv `nm demo | grep shell`

Kunsten er således at generere en streng der er præcist så lang at man får lagt denne adresse ind på det *rigtige sted*.

Perl kan erstatte AAAAA således `` `perl -e "print 'A'x10"` ``

Debugging af C med GDB

Vi laver sammen en session med GDB

Afprøvning med diverse input

- `./demo langstrengsomgiverproblemerforprogrammethvorformon`
- `gdb demo` efterfulgt af run med parametre
  `run AAAAAAAAAAAAAAAAAAAAAAAAAAAA`

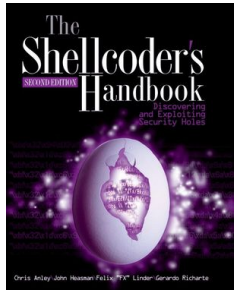
Hjælp:
Kompiler programmet og kald det fra kommandolinien med `./demo 123456...7689` indtil det dør ... derefter prøver I det samme i GDB

Hvad sker der? Avancerede brugere kan ændre `strcpy` til `strncpy`

GDB output

```
hlk@bigfoot:demo$ gdb demo
GNU gdb 5.3-20030128 (Apple version gdb-330.1) (Fri Jul 16 21:42:28 GMT 2004)
Copyright 2003 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "powerpc-apple-darwin".
Reading symbols for shared libraries .. done
(gdb) run AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Starting program: /Volumes/userdata/projects/security/exploit/demo/demo AAAAAAA
Reading symbols for shared libraries . done
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Program received signal EXC_BAD_ACCESS, Could not access memory.
0x41414140 in ?? ()
(gdb)
```

Buffer overflows



Hvis man vil lære at lave buffer overflows og exploit programmer er følgende dokumenter et godt sted at starte

Smashing The Stack For Fun And Profit Aleph One

Writing Buffer Overflow Exploits with Perl – anno 2000

Følgende bog kan ligeledes anbefales: *The Shellcoder's Handbook : Discovering and Exploiting Security Holes* af Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan ”noir”Eren, Neel Mehta, Riley Hassell, John Wiley & Sons, 2004

NB: Bogen er avanceret og således IKKE for begyndere!

Forudsætninger

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Som forsvarer: Kan du bryde kæden af forudsætninger har du vundet!

Eksempler på forudsætninger:

Computeren skal være tændt, Funktionen der misbruges skal være slået til, Executable stack, Executable heap, Fejl i programmet

alle programmer har fejl

Gode operativsystemer

Nyere versioner af Microsoft Windows, Mac OS X og Linux distributionerne inkluderer:

- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.
- ... en masse mere

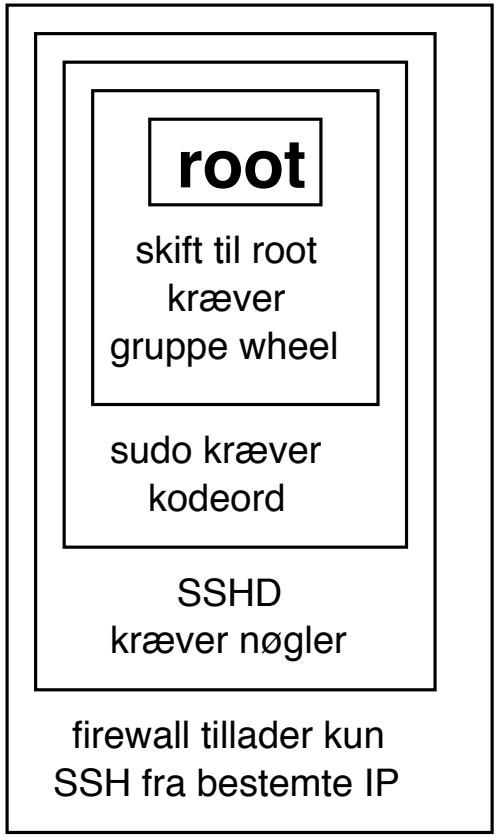
Vælg derfor hellere:

- Windows 7/8/10, fremfor Windows XP
- Mac OS X 10.11 fremfor 10.8
- Linux sikkerhedsopdateringer, sig ja når de kommer

Det samme gælder for serveroperativsystemer

NB: Meget få indlejrede systemer har beskyttelse! Internet of Thrash

Defense in depth - multiple layers of security



Forsvar dig selv med flere lag af sikkerhed!

Undgå standard indstillinger

Når vi scanner efter services går det nemt med at finde dem

Giv jer selv mere tid til at omkonfigurere og opdatere ved at undgå standardindstillinger

Tiden der går fra en sårbarhed annonceres på internet til den bliver udnyttet er meget kort i dag! Timer!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist – inden ormene kommer

NB: Ingen garanti – og det hjælper sjældent mod en dedikeret angriber

Dårlige passwords og konfigurationsfejl – ofte overset

Client side hacking: Java, Flash, PDF

Drive-by download

From Wikipedia, the free encyclopedia

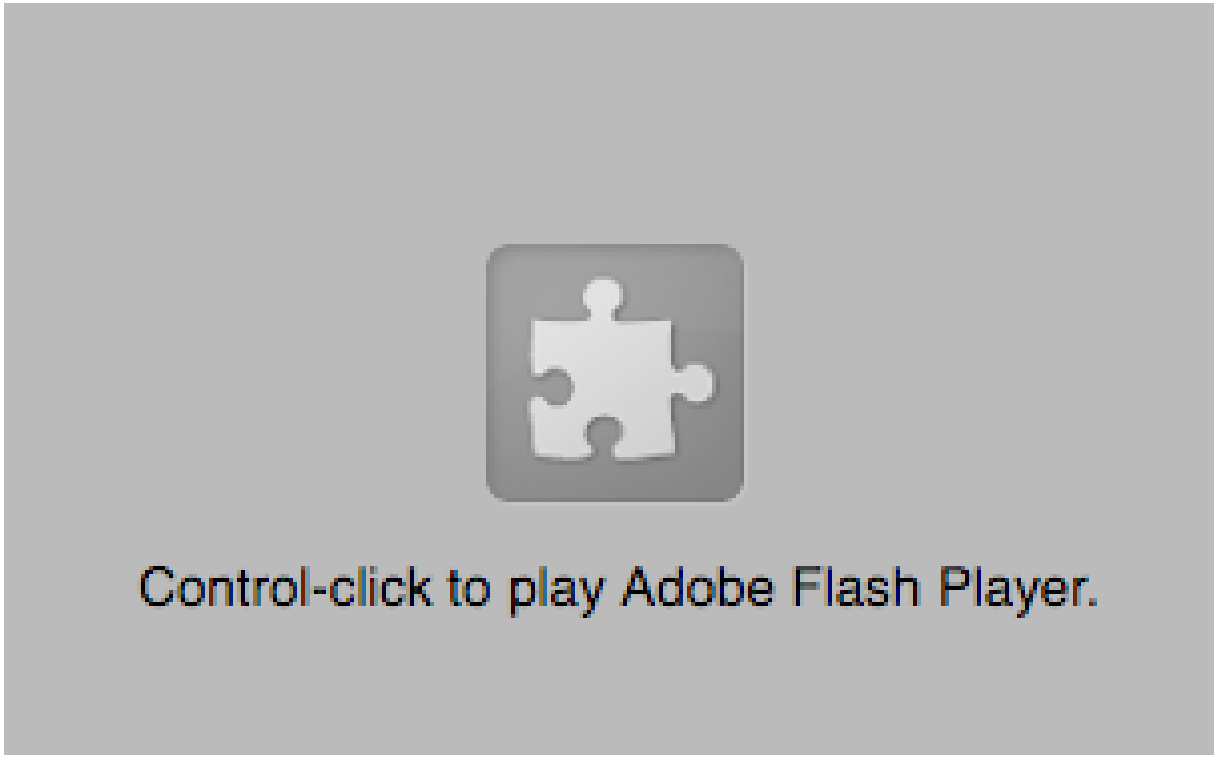
Drive-by download means three things, each concerning the unintended download of computer software from the Internet:

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet). This is usually caused by poor security design[*clarification needed*]. The user should not be frequently asked to accept security-critical decisions, often with very limited knowledge and within limited time.
2. Any download that happens without a person's knowledge.
3. Download of spyware, a computer virus or any kind of malware that happens without a person's knowledge.

Kan vi undvære Java, Flash og PDF?

Kilde: `https://en.wikipedia.org/wiki/Drive-by_download`

Flash blockers



Slå Flash fra

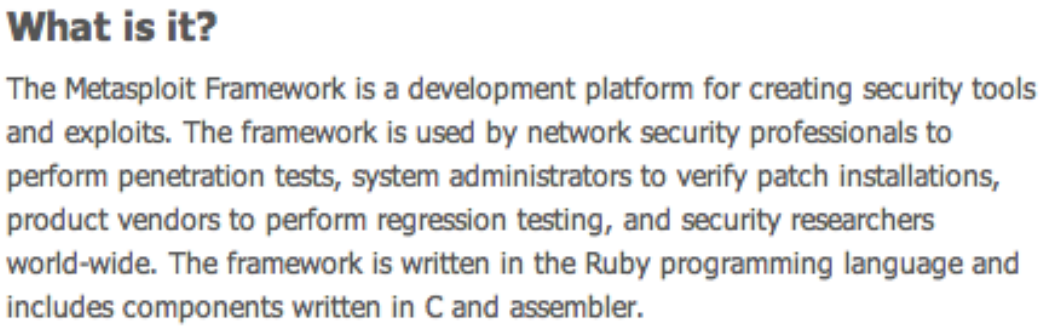
Afinstaller Flash

Brug kun indbyggede i eksempelvis Chrome - som opdateres løbende med browser

The Exploit Database – dagens buffer overflow

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

Metasploit and Armitage Still rocking the internet



Udviklingsværktøjerne til exploits er i dag meget raffinerede!

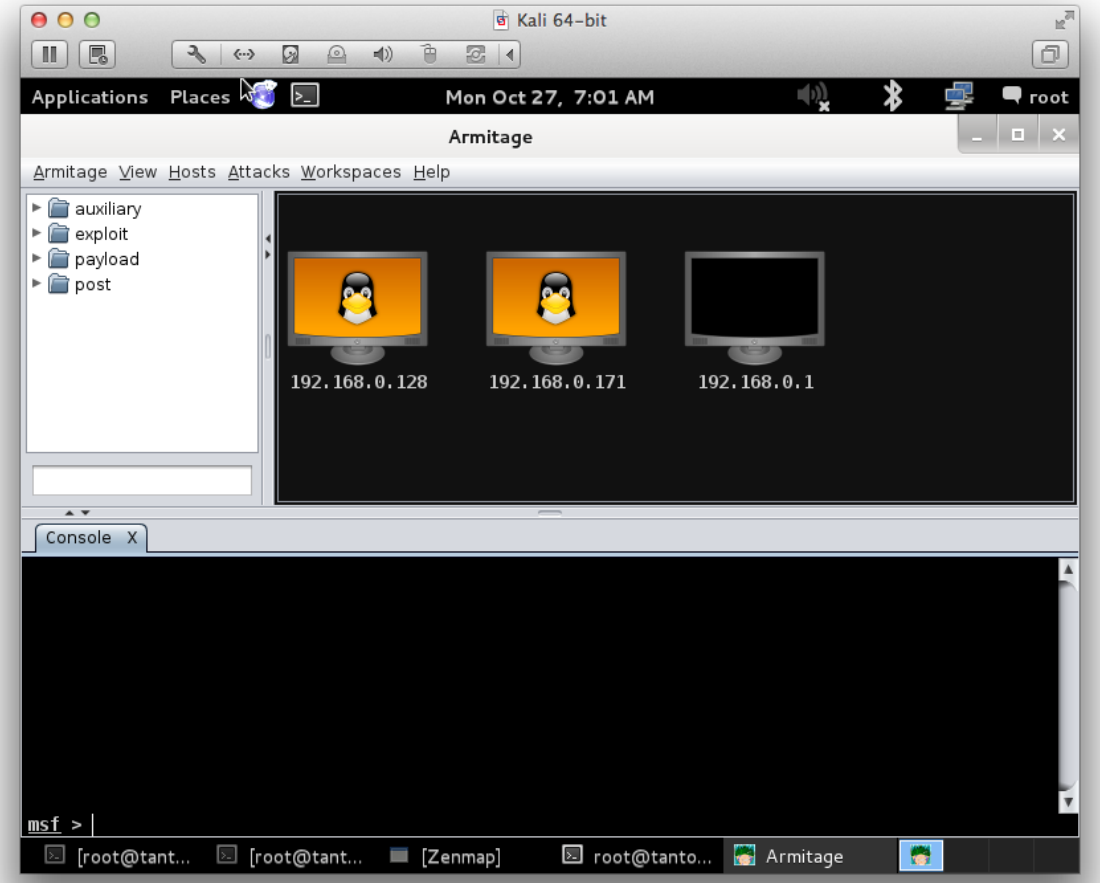
`http://www.metasploit.com/`

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 - ældre bog, kan undværes

Demo: Metasploit Armitage



CTF

Flere år har der været afholdt PROSA-CTF konkurrence

Sjovt og lærerigt - en mulighed for at afprøve sine hackerskillz

Omkring 100 personer på måske 15 hold over hele Danmark

God øvelse til angreb OG forsvar

Billede fra: `http://prosa-ctf.the-playground.dk/`

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

Use Github! Der er så mange biblioteker og programmer, noget eksisterende løser måske dit problem 90

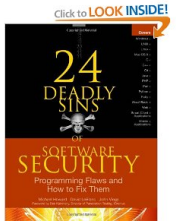
Example introductions:

- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide

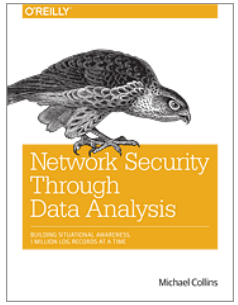
We are all Devops now, even security people!

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.



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