Welcome to

Penetration testing I basale pentest metoder

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Agenda

SOLIDO NETWORKS

Idag er en introduktion og forberedelse til workshops:

14. januar pentest-II Web hacking
`http://www.hk.dk/Aktuelt/Kalender/D2259208266`

21. januar pentest-III Wireless 802.11 hacking
`http://www.hk.dk/Aktuelt/Kalender/D2259208268`

29. januar pentest-IV Cryptography og Cracking
`http://www.hk.dk/Aktuelt/Kalender/D2259208269`

Hvis man vil på workshops og udføre angreb er det et krav at medbringe laptop med **virtualisering og Kali Linux installeret - FØR workshop**

Brug vejledningen *Kali Linux Hard Disk Install* fra `http://docs.kali.org/`
og eksempelvis Virtual box `https://www.virtualbox.org/`

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Formålet idag

Don’t Panic!

Introducere begrebet penetration testting 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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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`

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Efter SATAN

SOLIDO NETWORKS

SATAN og ideerne med automatiseret scanning efter sårbarheder blev siden ført videre i programmer som Saint, SARA

idag findes mange hackerværktøjer og automatiserede scannere

- Oprindeligt var det Unix scripts og tiger tools i 1990'erne
- idag har vi større pakker som Fyodor Nmap og Metasploit idag med god dokumentation

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Hacker - cracker

SOLIDO NETWORKS

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Definition af hacking, oprindeligt

Eric Raymond, der vedligeholder en ordbog over computer-slang (The Jargon File) har blandt andet følgende forklaringer på ordet hacker:

- En person, der nyder at undersøge detaljer i programmerbare systemer og hvordan man udvider deres anvendelsesmuligheder i modsætning til de fleste brugere, der bare lærer det mest nødvendige
- En som programmerer lidenskabligt (eller enddog fanatisk) eller en der foretrækker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofter arbejder med eller på det; som i "en Unixhacker".

Kilde: Peter Makholm, `http://hacking.dk`

Benyttes stadig i visse sammenhænge se `http://labitat.dk`

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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!

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

ISC2 code of ethics

Code of Ethics Preamble:

- Safety of the commonwealth, duty to our principals, 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 commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

The following additional guidance is given regarding pursuit of these goals.

https://www.isc2.org/ethics/default.aspx

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Er sikkerhedstest interessant?

Sikkerhedsproblemer i netværk er mange

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Pentest in the news

version2

IT-NYHEDER | BLOGS | IT-JOB | IT-FIRMAER | WHITEPAPERS

EMNER *Hacking, It-sikkerhed*

Se kommentarer (7)

Hackerkursus satte Dong på sporet af sårbare servere

En uges kursus i at tænke som en hacker gav flere aha-oplevelser for sikkerhedskonsulent hos Dong Energy. For eksempel fandt han efterfølgende server-software, der kørte med standard-password.

Af Jesper Kildebogaard Mandag, 19. marts 2012 - 6:59

Det kræver kun én lille sprække i forsvarsværkerne, før en hacker kan snige sig ind. Men hvordan opdager man som sikkerhedsansvarlig sprækken før hackeren?

Hos energikoncernen Dong Energy har et af svarene været at lære at tænke som hackerne. Og det gør det muligt at se på systemerne med helt andre øjne, fortæller en af de Dong-folk, der har været på hackerkursus.

»Kurset var et wakeup-call om, hvor nemt det er for hackere, som går systematisk til værks, og som ved, hvad de gør,« siger Keld Hjortskov, der er sikkerhedskonsulent hos Dong.

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

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Blackbox, greybox og whitebox

SOLIDO NETWORKS

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.

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Fordele ved at få udført planlagt sikkerhedstest

SOLIDO NETWORKS

Formålet med en sikkerhedstest er at nedbringe risici for systemerne og sikre organisationen mod uventede tab af data, tab af omdømme, forøgede omkostninger. Formålet er ikke at udpege en syndebuk eller identificere dårlige medarbejdere.

Giver gavnlig information

undgår nedbrud på uheldige tidspunkter

Målgrupper:

- IT-afdeling og teknisk personale
- Ledelse, koncernledelse

Afleveringer:

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Værktøjer

Alle bruger nogenlunde de samme værktøjer

- Portscanner - Fydor Nmap
- Generel sårbarhedsscanner - OpenVAS/Nessus, Metasploit
- Specialscannere, eksempelvis web sårbarhedsscanner - eksempelvis Nikto, Skipfish
- Specielle scannere - wifi Aircrack-ng, m.fl.
- ...
- Rapportværktøj - manuel eller automatisk, helst så automatiseret som muligt
- Meget ofte er sikkerhedstest automatiseret på de indledende skridt og manuel derefter

og scripting, powershell, unix shell, perl, python, ruby, ...

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Persongalleri

- Sikkerhedskonsulent - den konsulent der kommer ud til kunden
- Kontaktperson - kundens ansatte som kan hjælpe med praktiske spørgsmål og skabe kontakt til de rette personer i kundens organisation
- 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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Planlægning af sikkerhedstest

SOLIDO NETWORKS

Sårbarhedsanalysens omfang

- Scope - hvad skal testes
- Hvornår skal testes - indenfor et aftalt tidsrum
- Hvor testes fra - logfilerne vil afsløre IP-adresser
- Skal være aftalt på forhånd
- 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. fra 91.102.91.16/28

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Før konsulenten ankommer - forberedelse

Testplan med oversigt over targets og IP-adresser

Netværkstegninger og anden information som er aftalt oplyst

Hvor skal sikkerhedskonsulenten placeres på insidetest - ikke i serverrum tak :-)

Kabling af netværksstik

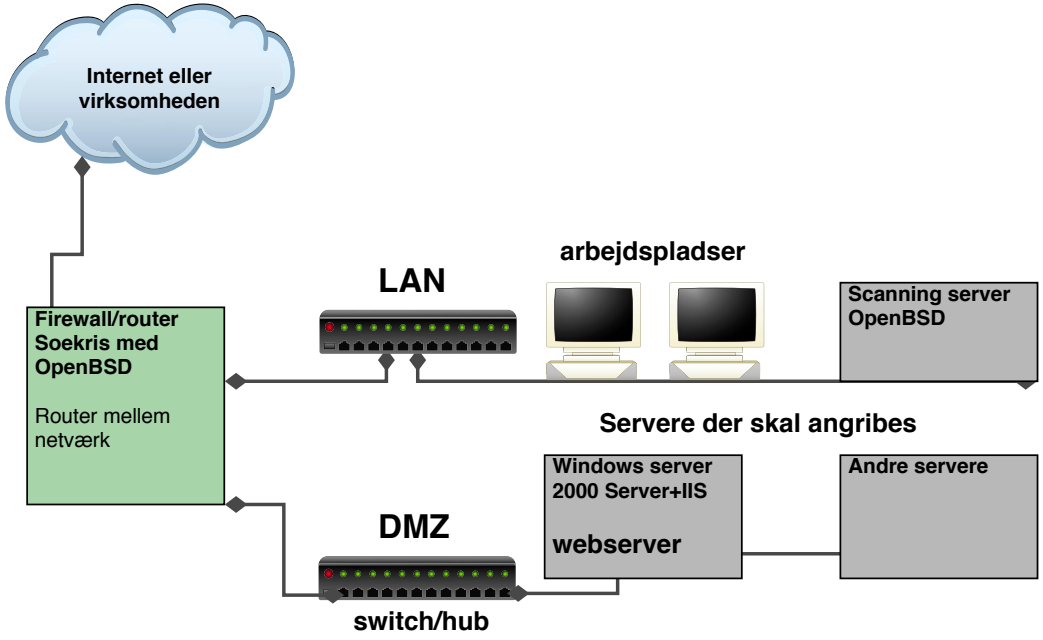
Gæstekort - til test over flere dage

kantine, toiletter osv.

Betragt det som en ny kollega - med tidsbegrænset kontrakt

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Godkendelse og tilladelse

Udførelse af test kan have negativ indflydelse på driften

Inden en test kan udføres skal der indhentes tilladelser fra:

- systemejere
- netværksejer
- driftorganisationer

At belyse problemerne er formålet
- at få dem belyst indenfor et aftalt tidsrum er en fordel!

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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!

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Afbrydelse af testen - kompromitterede maskiner

SOLIDO NETWORKS

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!

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Oprydning efter testen

SOLIDO NETWORKS

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Rules of engagement - regler og etik for sikkerhedstest

SOLIDO NETWORKS

- 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
- Solido vil ved opdagelse af åbenlyse sikkerhedsrisici dokumentere disse i rapporten, uanset scope for opgaven ellers

Det er en balancegang

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Bøger og resourcer

SOLIDO NETWORKS

Konsulentens udstyr - vil du være sikkerhedskonsulent

Sikkerhedskonsulenterne bruger typisk Open Source værktøjer på Linux og enkelte systemer med Windows - jeg bruger helst Windows 7 idag

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

- *A Hands-On Introduction to Hacking by Georgia Weidman*, June 2014
  `http://www.nostarch.com/pentesting`
- *Metasploit The Penetration Tester's Guide* by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni
  `http://nostarch.com/metasploit`
- Metasploit Unleashed - gratis kursus i Metasploit
  `http://www.offensive-security.com/metasploit-unleashed/`

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Forudsætninger

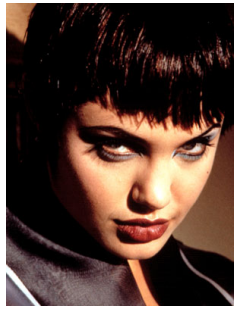
Teknisk foredrag og fuldt udbytte kræver at deltagerne har mindst 2 års praktisk erfaring som teknikker og/eller systemadministrator

Til penetrationstest og det meste Internet-sikkerhedsarbejde er der følgende forudsætninger

- Netværkserfaring
- TCP/IP principper - ofte 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
- Alle øvelser kan udføres fra en Windows PC eller Mac
- Øvelserne foregår via virtualiserede systemer

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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/`
- Skipfish `http://code.google.com/p/skipfish/`
- OpenBSD operativsystem med fokus på sikkerhed `http://www.openbsd.org`

Kilde: Angelina Jolie fra Hackers 1995

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

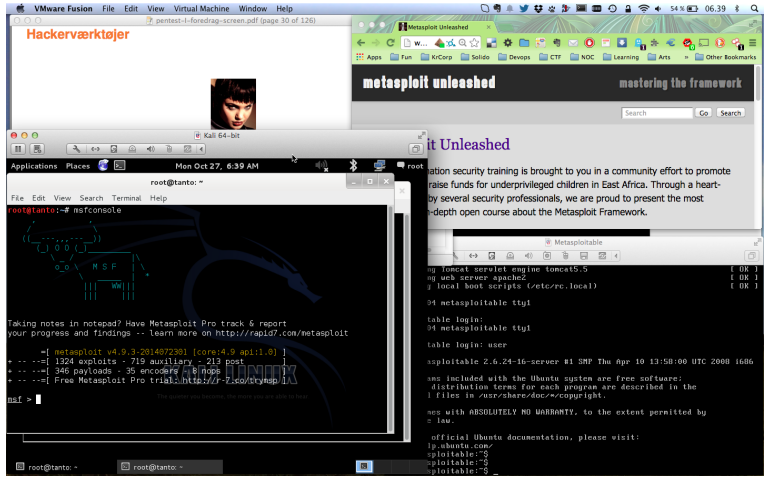
Oprydning/hærdning vises måske ikke, men I bør i praksis:

- 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.

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Hackerlab opsætning



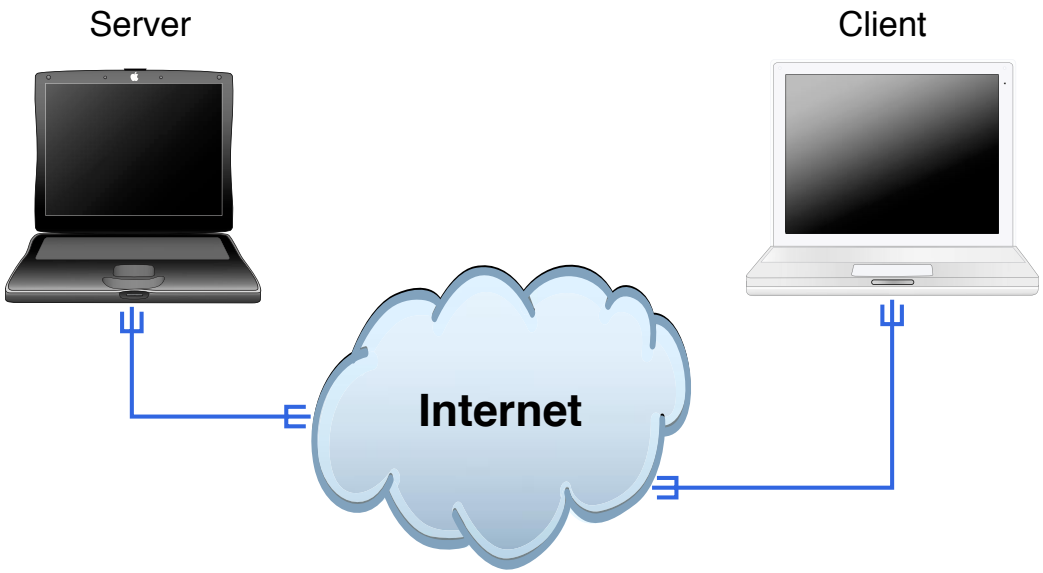
- Hardware: en moderne laptop med CPU der kan bruge virtualiseting
  Husk at slå virtualisering til i BIOS
- Software: dit favoritoperativsystem, Windows, Mac, Linux
- Virtualiseringssoftware: VMware, Virtual box, vælg selv
- Hackersoftware: Kali Linux som en virtuel maskine
- Soft targets: Metasploitable, Windows 2000, Windows Xp, ...

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Teknisk hvad er hacking

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Internet idag



Klienter og servere

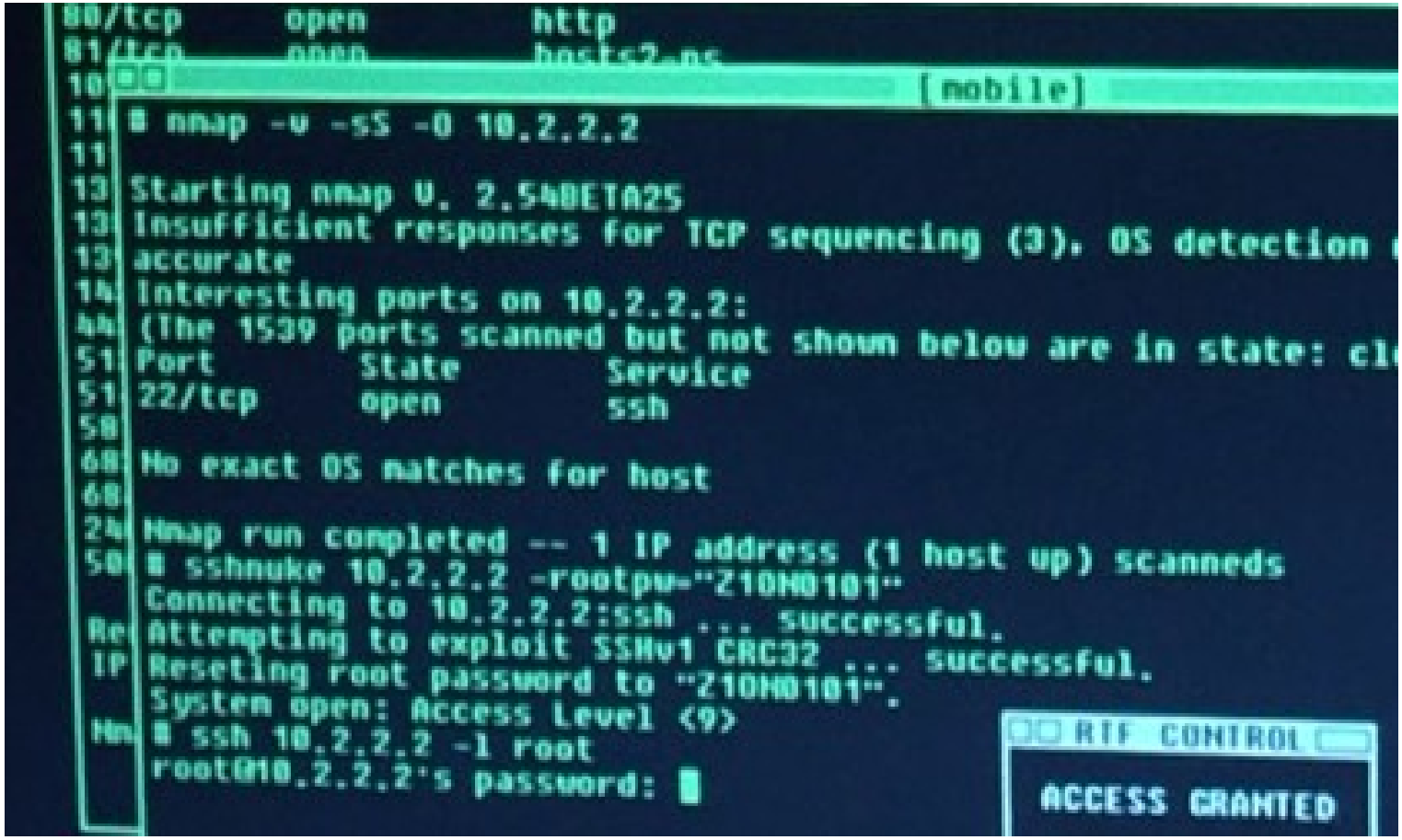
Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Trinity breaking in



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

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

Hacking er magi

Hacking ligner indimellem magi

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

MAC filtrering

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Getting to your data: Google for it

Google as a hacker tools?

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

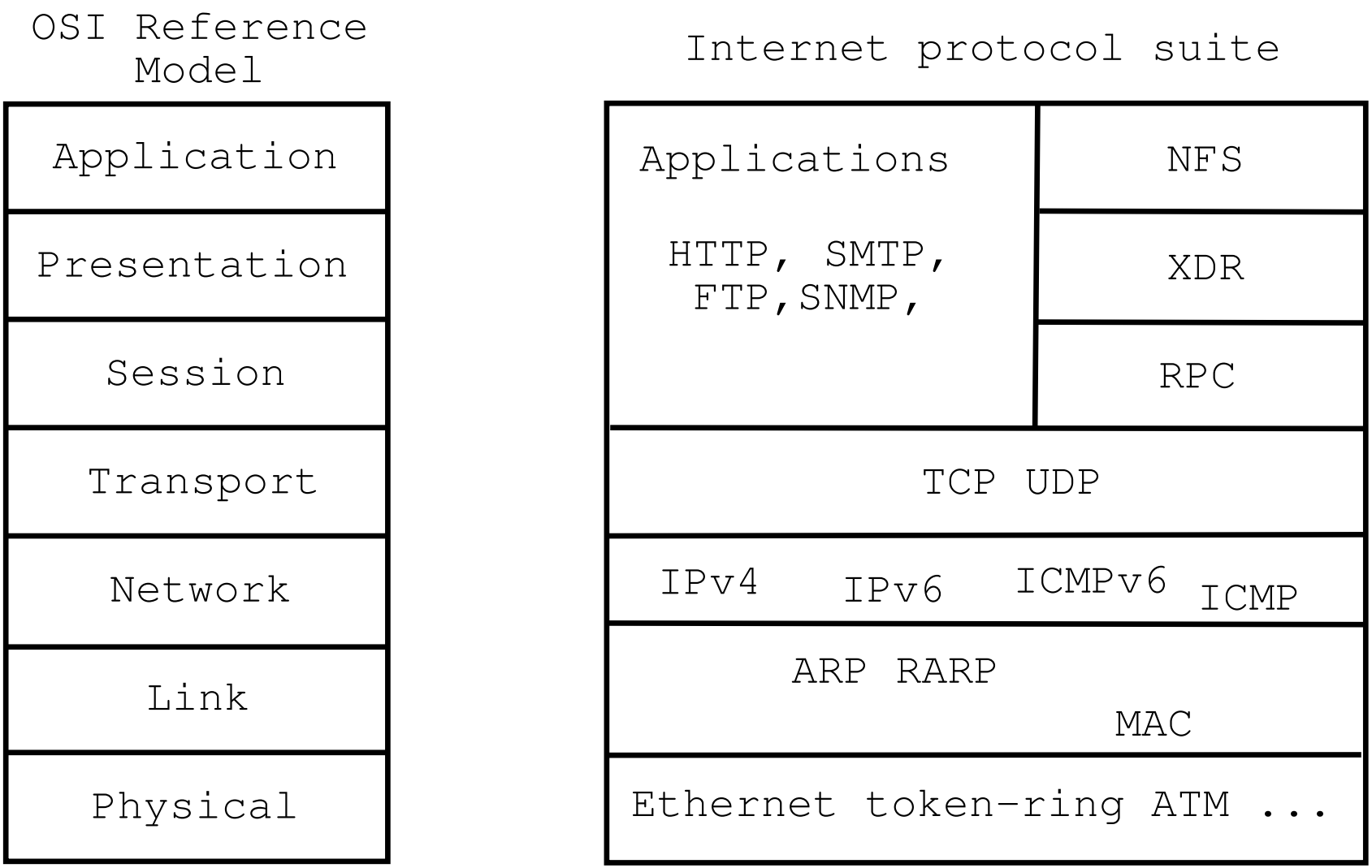
Heartbleed hacking

```
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.

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

OSI og Internet modellerne



© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

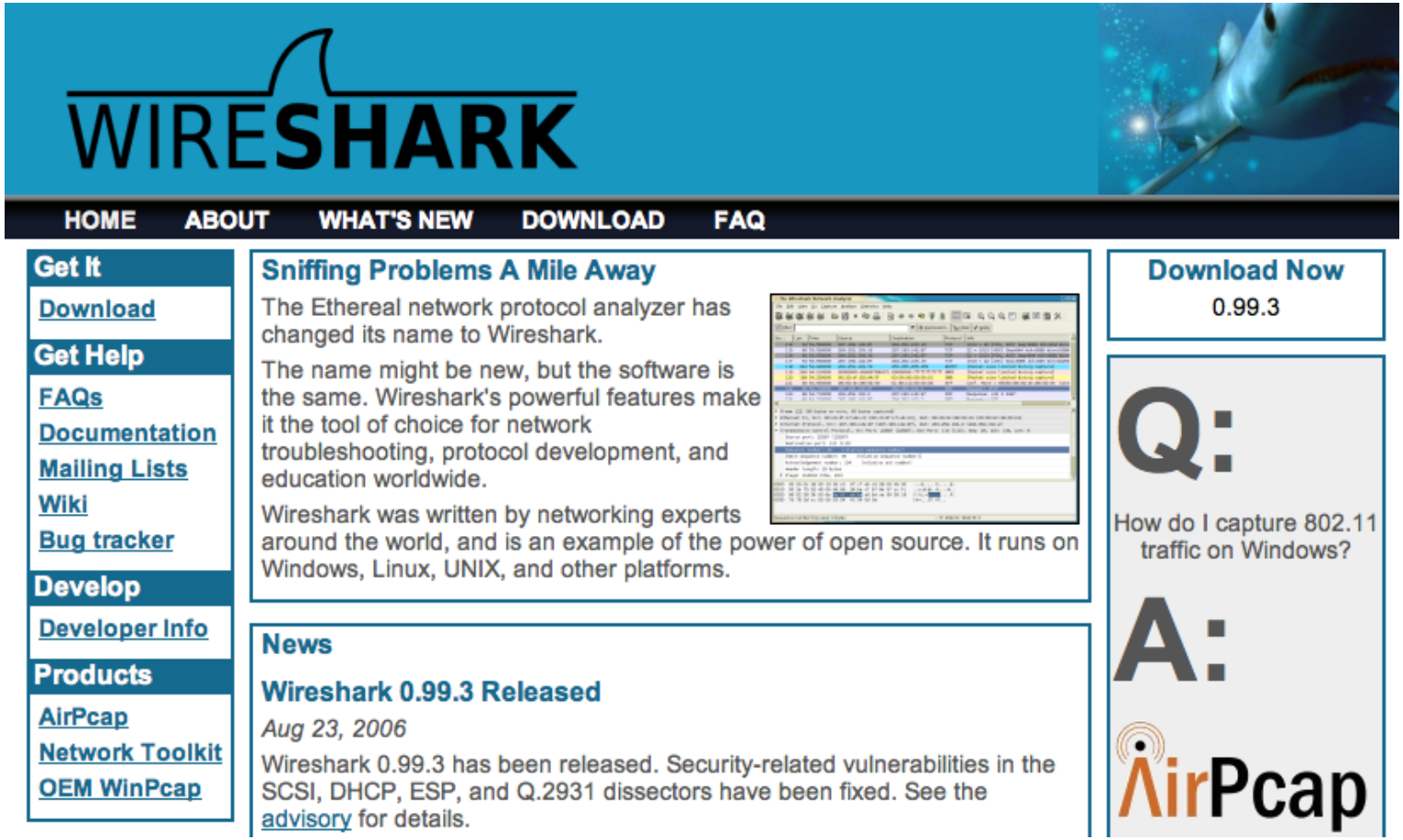
Kali Linux the new backtrack

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

Kali `http://www.kali.org/`

Wireshark - `http://www.wireshark.org` avanceret netværkssniffer

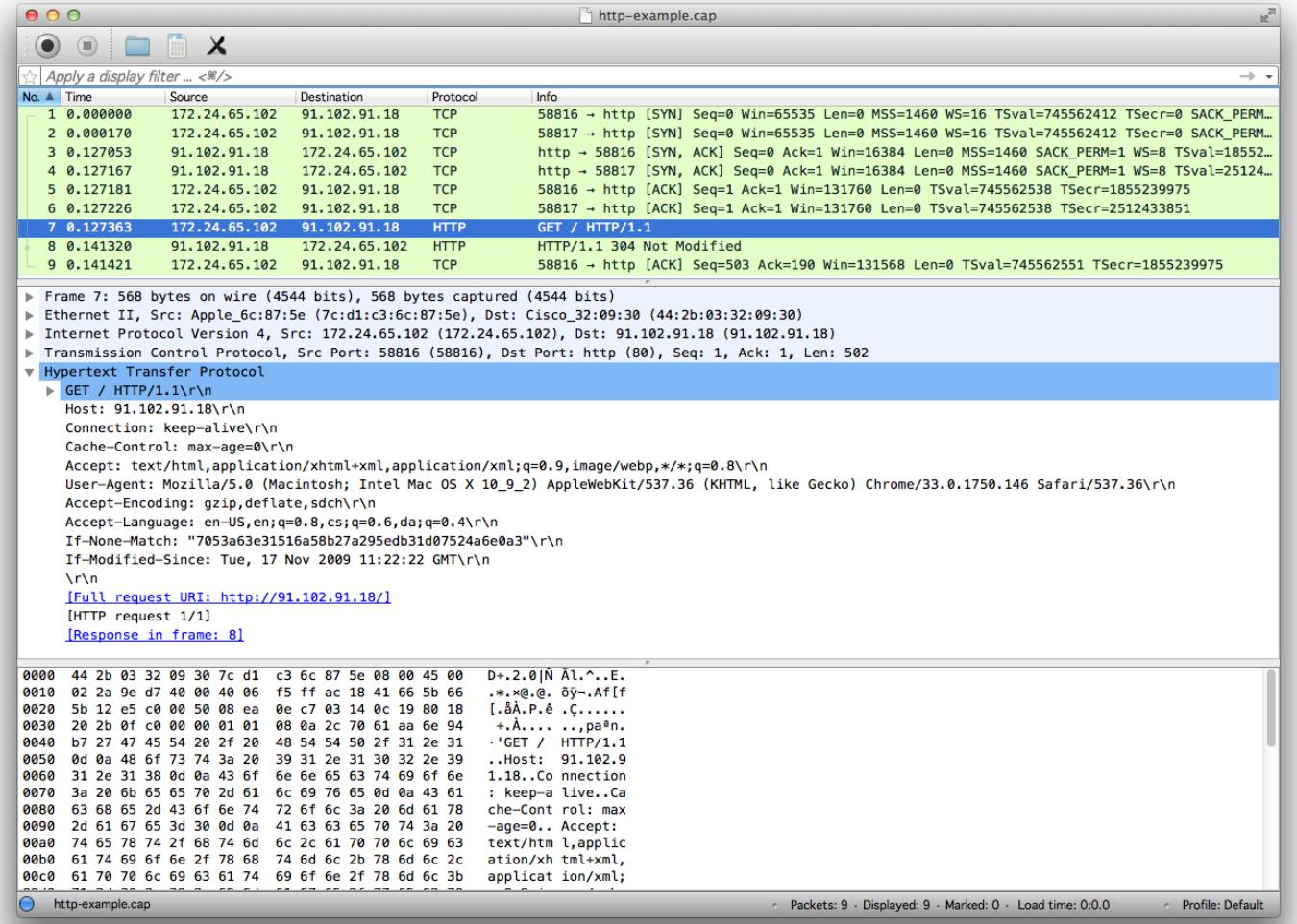
Wireshark - grafisk pakkesniffer



`http://www.wireshark.org`

både til Windows og Unix

Brug af Wireshark



Læg mærke til filtermulighederne

traceroute

traceroute programmet virker ved hjælp af TTL

levetiden for en pakke tælles ned i hver router på vejen og ved at sætte denne lavt opnår man at pakken *timer ud* - besked fra hver router på vejen

default er UDP pakker

```
  traceroute 10.20.20.129
traceroute to 10.20.20.129 (10.20.20.129)

, 30 hops max, 40 byte packets
 1  safri (10.0.0.11)  3.577 ms  0.565 ms  0.323 ms
 2  router (10.20.20.129)  1.481 ms  1.374 ms  1.261 ms
```

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

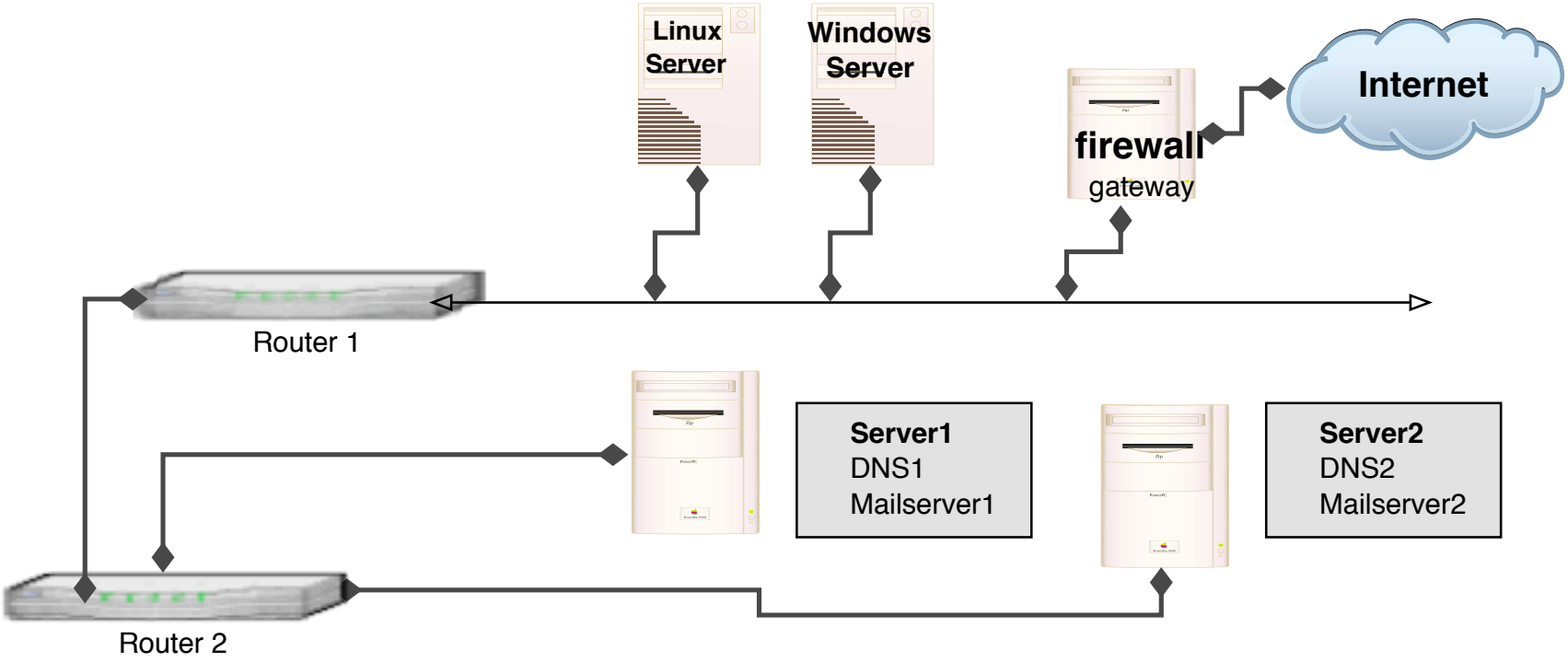
traceroute - med UDP

```
 #  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
```

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

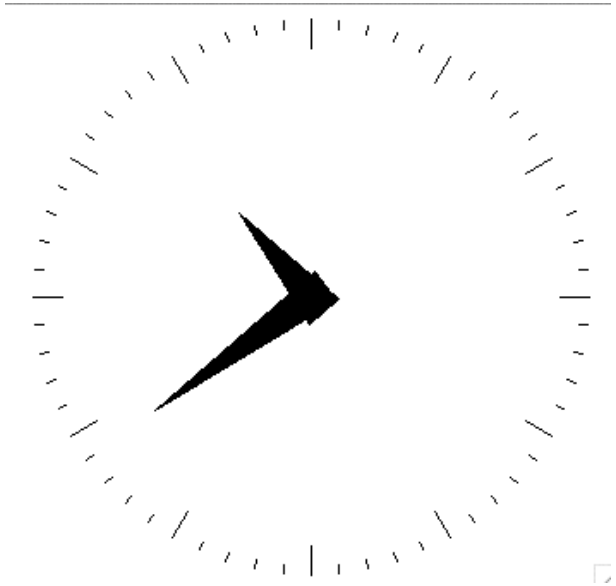
Network mapping



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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

What time is it?



Hvad er klokken?

Hvad betydning har det for sikkerheden?

Brug NTP Network Time Protocol på produktionssystemer

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

What time is it? - spørg ICMP

ICMP timestamp option - request/reply

hvad er klokken på en server

Slayer icmpush - gammelt program

viser tidstempel

```
#  icmpush -v -tstamp 10.0.0.12
ICMP Timestamp Request packet sent to 10.0.0.12 (10.0.0.12)

Receiving ICMP replies ...
fischer          -> 21:27:17
icmpush: Program finished OK
```

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Informationsindsamling

Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet

passiv kunne være at lytte med på trafik eller søge i databaser på Internet

aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

whois systemet

IP adresserne administreres i dagligdagen af et antal Internet registries, hvor de største er:

- RIPE (Réseaux IP Européens) `http://ripe.net`
- ARIN American Registry for Internet Numbers `http://www.arin.net`
- Asia Pacific Network Information Center `http://www.apnic.net`
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands `http://www.lacnic.net`
- AfriNIC African Internet Numbers Registry `http://www.afrinic.net`

disse fem kaldes for Regional Internet Registries (RIRs) i modsætning til Local Internet Registries (LIRs) og National Internet Registry (NIR)

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

DNS systemet

navneopslag på Internet

tidligere brugte man en **hosts** fil
hosts filer bruges stadig lokalt til serveren - IP-adresser

UNIX: /etc/hosts

Windows `c:\windows\system32\drivers\etc\hosts`

skrives i database filer, zone filer

```
[hlk@bigfoot ~]$ host www.solidonetworks.com
www.solidonetworks.com has address 91.102.95.20
www.solidonetworks.com has IPv6 address 2a02:9d0:10::9
```

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Mere end navneopslag

SOLIDO NETWORKS

består af resource records med en type:

- adresser A-records
- IPv6 adresser AAAA-records
- autoritative navneservere NS-records
- post, mail-exchanger MX-records
- flere andre: md , mf , cname , soa , mb , mg , mr , null , wks , ptr , hinfo , minfo , mx ....

```
   IN        MX        10        mail.solido.net.
   IN        MX        20        mail2.solido.net.
www       IN        A         91.102.95.20
www       IN        AAAA      2a02:9d0:10::9
```

Små DNS tools bind-version - Shell script

```
#! /bin/sh
# Try to get version info from BIND server
PROGRAM=`basename $0`
. `dirname $0`/functions.sh
if [ $# -ne 1 ]; then
   echo "get name server version, need a target! "
   echo "Usage: $0 target"
   echo "example $0 10.1.2.3"
   exit 0
fi
TARGET=$1
# using dig
start_time
dig @$1 version.bind chaos txt
echo Authors BIND er i versionerne 9.1 og 9.2 - måske ...
dig @$1 authors.bind chaos txt
stop_time
```

http://www.kramse.dk/files/tools/dns/bind-version

Små DNS tools dns-timecheck - Perl script

```
#!/usr/bin/perl
# modified from original by Henrik Kramshøj, hlk@kramse.dk
# 2004-08-19
#
# Original from: http://www.rfc.se/fpdns/timecheck.html
use Net::DNS;

my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers($ARGV[0]);

my $query = Net::DNS::Packet->new;
$query->sign_tsig("n","test");

my $response = $resolver->send($query);
foreach my $rr ($response->additional)
  print "localtime vs nameserver $ARGV[0] time difference: ";
  print$rr->time_signed - time() if $rr->type eq "TSIG";
```

http://www.kramse.dk/files/tools/dns/dns-timecheck

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Intrusion Detection Systems - IDS

angrebsværktøjerne efterlader spor

hostbased IDS - kører lokalt på et system og forsøger at detektere om der er en angriber inde

network based IDS - NIDS - bruger netværket

Automatiserer netværksovervågning:

- bestemte pakker kan opfattes som en signatur
- analyse af netværkstrafik - FØR angreb
- analyse af netværk under angreb - sender en alarm

`http://www.suricata-ids.org` - det kan anbefales at se på Suricata

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

TCP sequence number prediction

tidligere baserede man ofte login og adgange på de IP adresser som folk kom fra

det er ikke pålideligt at tro på address based authentication

TCP sequence number kan måske gættes

Mest kendt er nok Shimomura der blev hacket på den måde, måske af Kevin D Mitnick eller en kompagnon

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

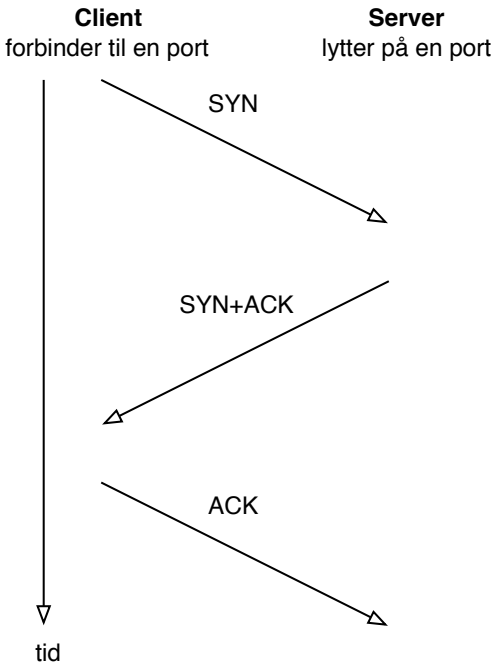
TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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**

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

nmap port sweep efter port 80/TCP

Port 80 TCP er webservere

```
 #  nmap  -p 80 192.168.20.130/28

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (10.20.20.129):
Port        State        Service
80/tcp      filtered     http

Interesting ports on www.kramse.dk (192.168.20.131):
Port        State        Service
80/tcp      open         http

Interesting ports on  (192.168.20.139):
Port        State        Service
80/tcp      open         http
```

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

nmap port sweep efter port 161/UDP

Port 161 UDP er SNMP

```
 #  nmap -sU -p 161 192.168.20.130/28

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (10.20.20.129):
Port        State        Service
161/udp     open         snmp

The 1 scanned port on mail.kramse.dk (192.168.20.130) is: closed

Interesting ports on www.kramse.dk (192.168.20.131):
Port        State        Service
161/udp     open         snmp

The 1 scanned port on  (192.168.20.132) is: closed
```

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

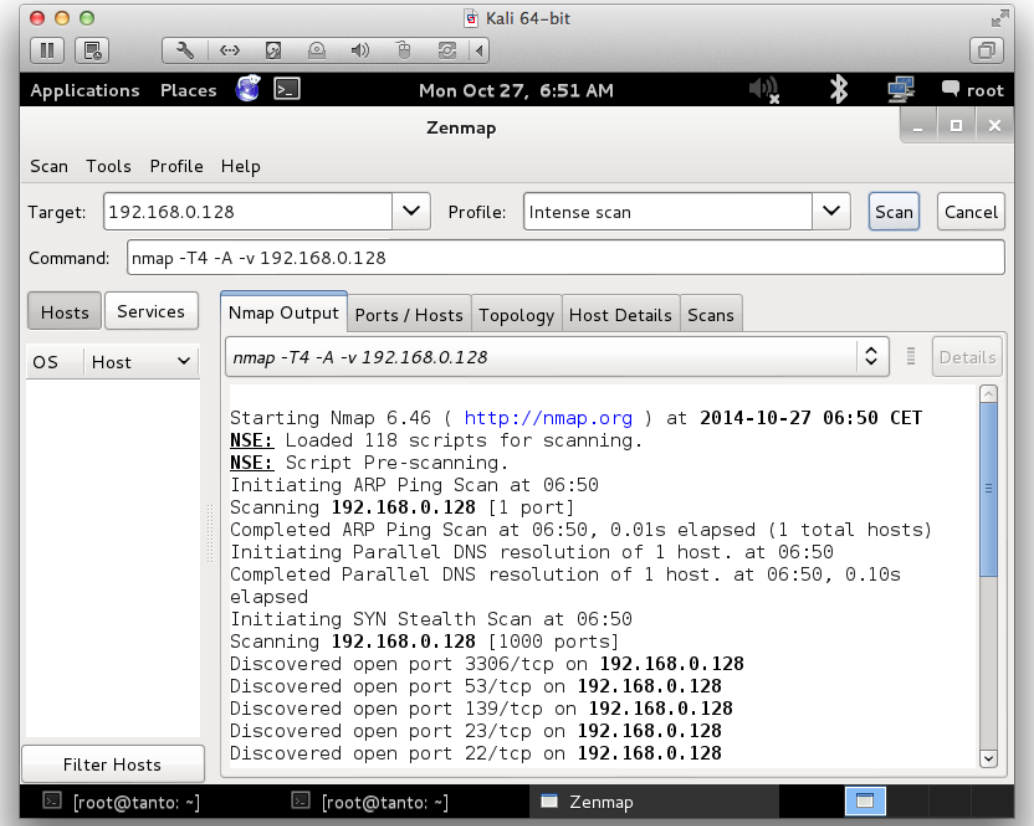
OS detection

```
# nmap -O ip.adresse.slet.tet scan af en gateway
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-03 11:31 CET
Interesting ports on gw-int.solido.net (ip.adresse.slet.tet):
(The 1653 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1080/tcp open  socks
5000/tcp open  UPnP
Device type: general purpose
Running: FreeBSD 4.X
OS details: FreeBSD 4.8-STABLE
Uptime 21.178 days (since Wed Nov 12 07:14:49 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 7.540 seconds
```

- lavniveau måde at identificere operativsystemer på, prøv også `nmap -A`
- send pakker med *anderledes* indhold
- Reference: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin
  `http://www.sys-security.com/html/projects/icmp.html`

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Portscan med Zenmap GUI



Zenmap følger med i pakken når man henter Nmap `http://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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Hvad er værdien af pentest?

hvor og hvordan kan I bruge penetrationstest

hvis man vil have et andet indblik i netværket, TCP, UDP, ICMP, portscannning og samle puslespil udfra få informationer

Netværksadministratorer kan bruge pentesting til at sikre egne netværk ved brug af samme teknikker som hackere

IT-/sikkerheds-chef vurdere og evaluere tilbud og løsninger for sikkerheden. Er den påtænkte løsning fornuftig?

Man står med en server der er kompromitteret - hvordan skete det? - hvordan forhindrer vi det en anden gang.

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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
...
```

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

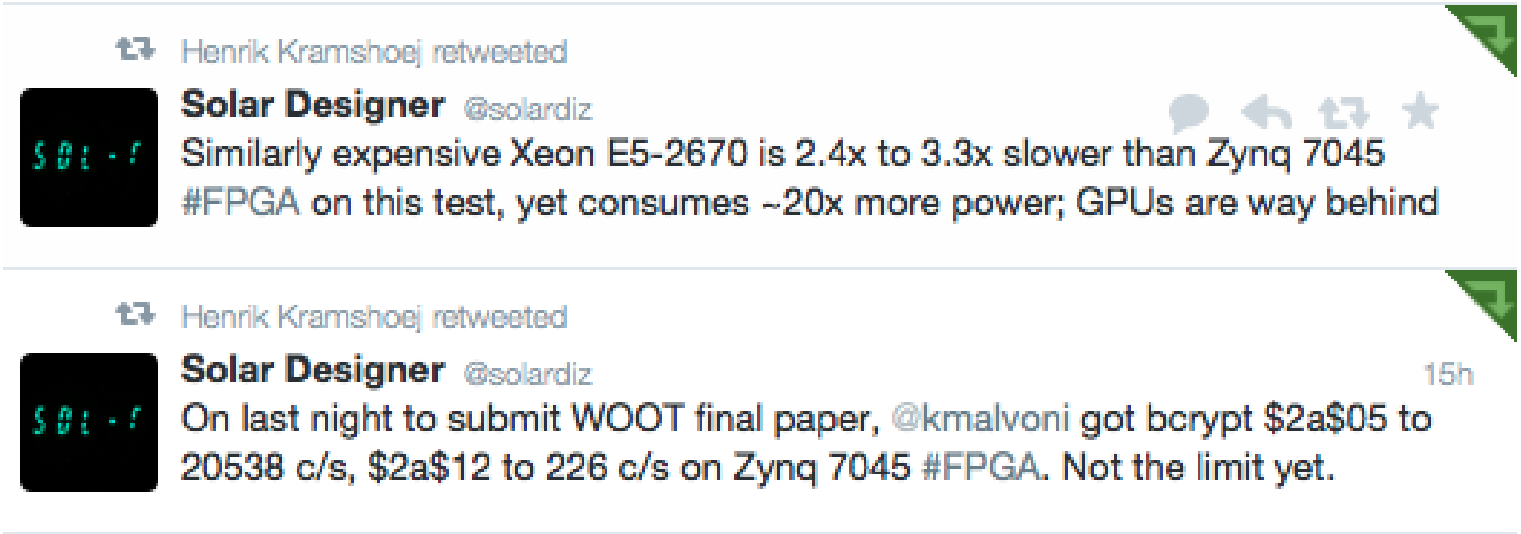
Cracking passwords

- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Parallella John

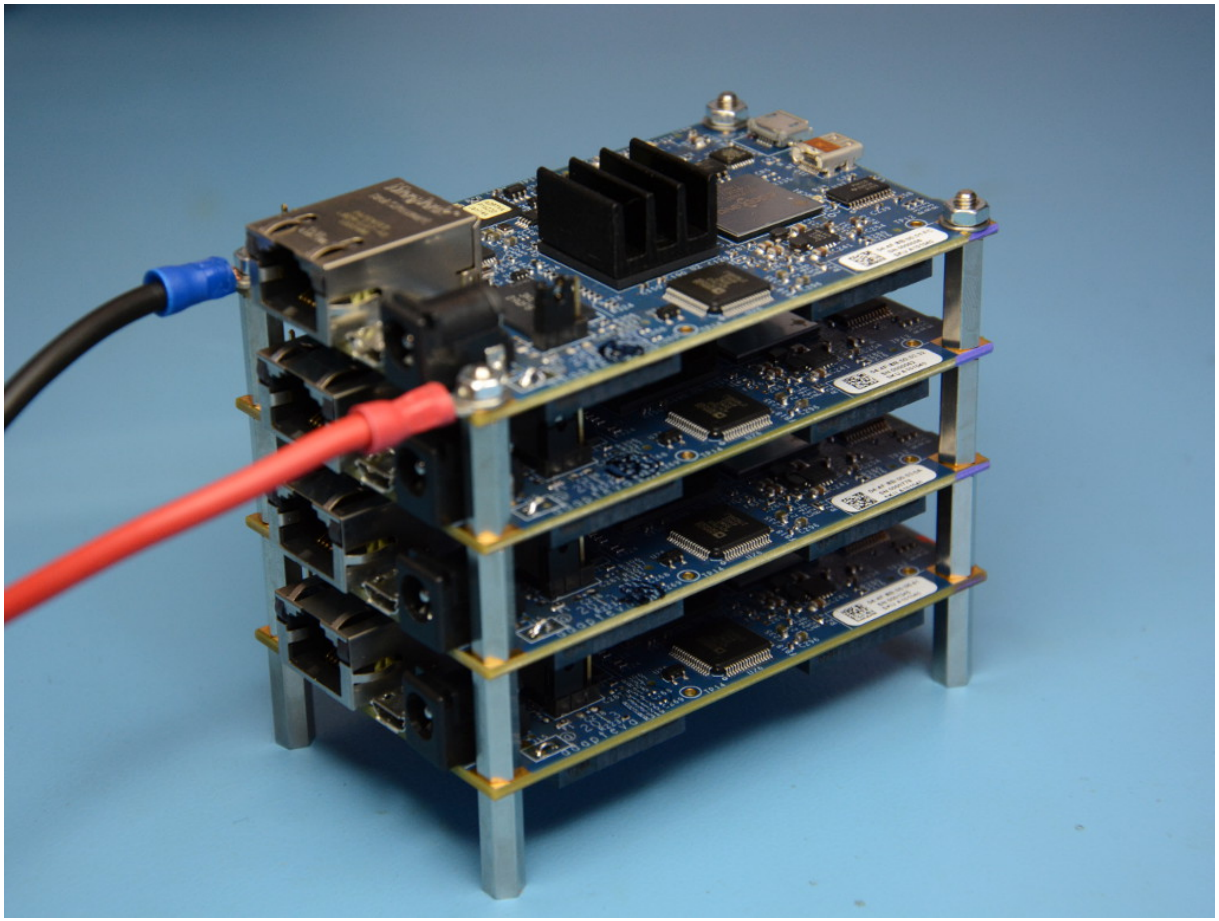


`https://twitter.com/solardiz/status/492037995080712192`

Warning: FPGA hacking - not finished part of presentation ☺

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Stacking Parallella boards



http://www.parallella.org/power-supply/

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

buffer overflows et C problem

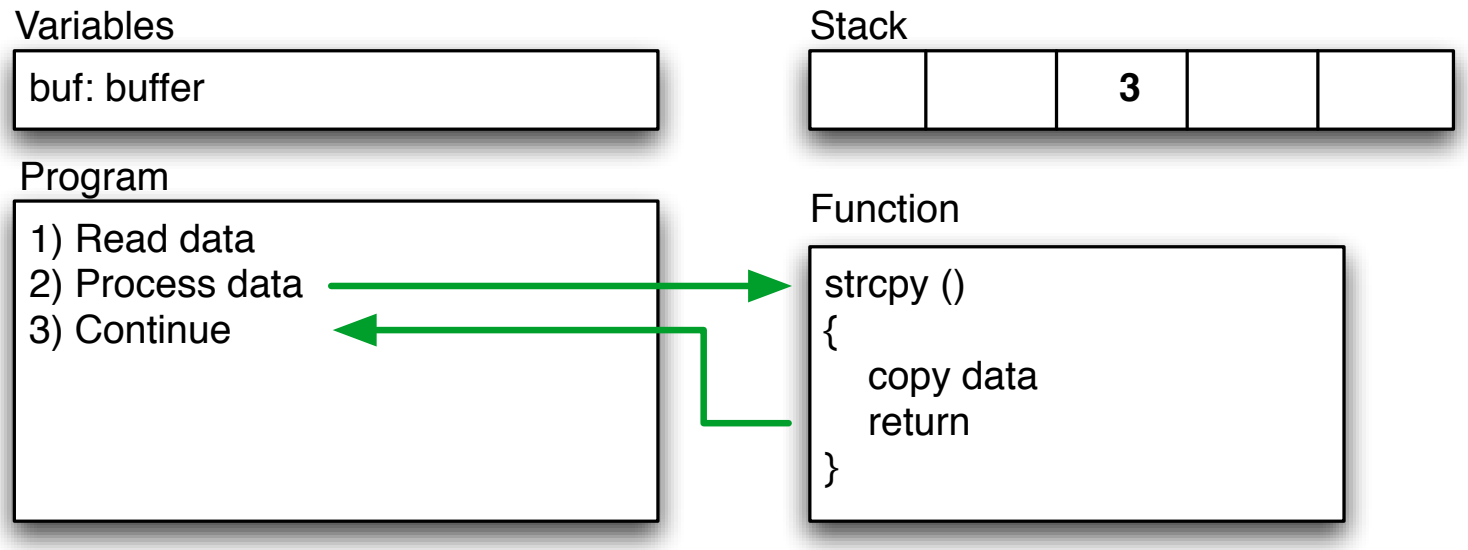
SOLIDO NETWORKS

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.

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

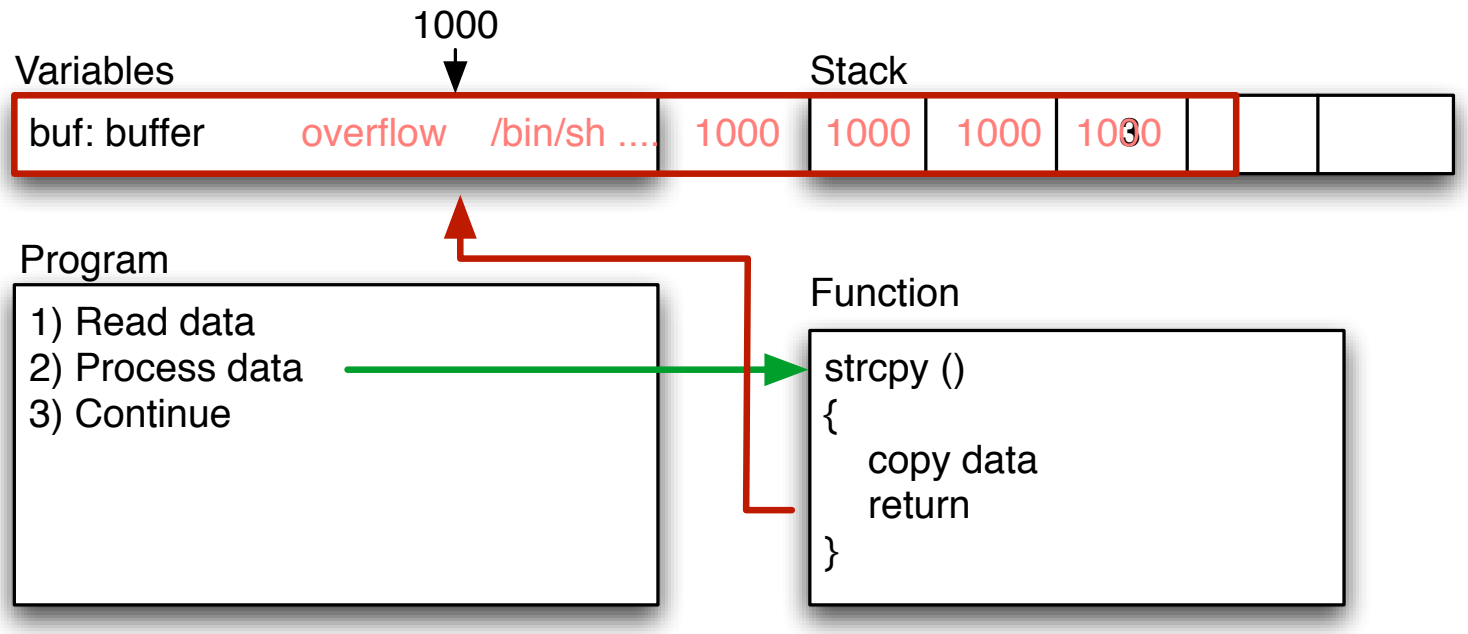
Buffer og stacks




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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Exploits - udnyttelse af sårbarheder

exploit/exploitprogram er

- udnytter eller demonstrerer en sårbarhed
- rettet mod et specifikt system.
- kan være 5 linier eller flere sider
- Meget ofte Perl eller et C program

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Exploits

```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
$address = pack('l', $the_shell_pointer);
$buffer .= $address;
exec "$program", "$buffer";
```

Demo exploit in Perl

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Sårbarheder - CVE

Common Vulnerabilities and Exposures (CVE) er:

- klassifikation
- unik navngivning af sårbarheder.

Sårbarheder tildeles

- initielt oprettes med status CANDIDATE

CVE vedligeholdes af MITRE - som er en not-for-profit organisation skabt til forskning og udvikling i USA. National Vulnerability Database er en af mulighederne for at søge i CVE.

Kilde: `http://cve.mitre.org/` og `http://nvd.nist.gov`

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Sårbarheder - OSVDB

Læg mærke til at der er forskel på antallet af sårbarheder - nogle databaser opretter enkeltvis mens andre slår dem sammen

Demo sårbarhederne idag tæller eksempelvis i OSVDB 1 sårbarhed for hvert sårbart script

Kilde: `http://www.osvdb.org`

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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 ikke i webløsninger i Danmark - eller meget få steder

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

konfigurationsfejl - ofte overset

Forkert brug af programmer er ofte overset

- opfyldes forudsætningerne
- er programmet egnet til dette miljø
- er man udannet/erfaren i dette produkt

Kunne I finde på at kopiere cmd.exe til /scripts kataloget på en IIS?

Det har jeg engang været ude for at en kunde havde gjort!

hvis I under test af en server opdager at denne har /scripts/cmd1.exe eller ”FTP-scripts” til at hente værktøjer ... så er den pågældende server formentlig kompromitteret

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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 bugtraq til den bliver udnyttet er meget kort idag!

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Demo: Insecure programming buffer overflows 101

Opgave: Lav et C program og oversæt det

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");  }
```

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

GDB GNU Debugger

GNU compileren og debuggeren fungerer godt!

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"` ``

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Debugging af C med GDB

SOLIDO NETWORKS

Vi laver sammen en session med GDB

Afprøvning med diverse input

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

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`

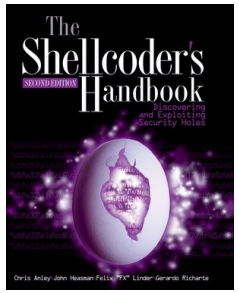
© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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!

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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

Kan du bryde kæden af forudsætninger har du vundet!

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Eksempler på forudsætninger

SOLIDO NETWORKS

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

Executable heap

Fejl i programmet

alle programmer har fejl

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Stack protection

Stack protection er mere almindeligt
- med i OpenBSD current fra 2. dec 2002

Buffer overflows er almindeligt kendte

- Selv OpenSSH har haft buffer overflows
- Stack protection prøver at modvirke/fjerne muligheden for buffer overflows. arbitrary code execution bliver til ude af drift for berørte services

Propolice
`http://www.openbsd.org`
`http://www.trl.ibm.com/projects/security/ssp/`

StackGuard
`http://www.immunix.org/stackguard.html`

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

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.

Vælg derfor hellere:

- Windows 7, end Windows Xp
- Mac OS X 10.7 fremfor 10.6
- Linux sikkerhedsopdateringer, sig ja når de kommer

Det samme gælder for serveroperativsystemer

NB: meget få embedded systemer har beskyttelse!

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Client side: Flash, PDF, Facebook

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 Flash og PDF?

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Flash blockers

Safari `http://clicktoflash.com/`

Firefox Extension Flashblock

Chrome extension called FlashBlock

Internet Explorer 8: IE has the Flash block functionality built-in so you don't need to install any additional plugins to be able to block flash on IE 8.

FlashBlock for Opera 9 - bruger nogen Opera mere?

FlashBlockere til iPad? iPhone? Android? - hvorfor er det ikke default?

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

milw0rm - dagens buffer overflow

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]

MILW0RM

[highlighted]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2009-03-05	Winamp <= 5.541 Skin Universal Buffer Overflow Exploit	3128	R		D	SkD
2009-02-26	Coppermine Photo Gallery <= 1.4.20 (BBCode IMG) Privilege Escalation	7338	R		D	StAkeR
2009-02-25	Apple MACOS X xnu <= 1228.x Local Kernel Memory Disclosure Exploit	4111	R		D	mu-b
2009-02-23	Adobe Acrobat Reader JBIG2 Local Buffer Overflow PoC #2 0day	17652	R		D	Guido Landi
2009-02-23	MLdonkey <= 2.9.7 HTTP DOUBLE SLASH Arbitrary File Disclosure Vuln	4225	R		D	Michael Peselnik
2009-02-23	Multiple PDF Readers JBIG2 Local Buffer Overflow PoC	7781	R		D	webDEVIL

[remote]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2009-03-05	SupportSoft DNA Editor Module (dnaedit.dll) Code Execution Exploit	1093	R		D	X Nine:Situations:Group
2009-03-04	Easy File Sharing Web Server 4.8 File Disclosure Vulnerability	1424	R		D	Stack
2009-03-04	EFS Easy Chat Server Authentication Request Buffer Overflow Exploit (pl)	969	R		D	Dr4sH
2009-03-04	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast)	3965	R		D	Ahmed Obied
2009-03-03	EFS Easy Chat Server (XSRF) Change Admin Pass Vulnerability	1215	R		D	Stack
2009-03-03	Imera ImeraIEPlugin ActiveX Control Remote Code Execution Exploit	1020	R		D	Elazar

[local]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2009-03-05	Media Commands (m3u File) Universal SEH Overwrite Exploit	669	R		D	His0k4
2009-03-05	Media Commands .m3l File Local Buffer Overflow Exploit	621	R		D	Stack

`http://milw0rm.com/` - men ingen opdateringer

The Exploit Database - dagens buffer overflow

EXPLOIT Database

Currently Archiving 10343 Exploits

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

The Exploit Database

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

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

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

Remote Exploits

Date	D	A	V	Description	Plat.	Author
2010-01-27	D	A	✔	CamShot v1.2 SEH Overwrite Exploit	windows	tecnik
2010-01-25	D	-	✔	AOL 9.5 Phobos.Playlist 'Import()' Buffer Overflow Exploit (Meta)	windows	Trancer
2010-01-22	D	A	✔	IntelliTamper 2.07/2.08 (SEH) Remote Buffer Overflow	windows	loneferret
2010-01-21	D	-	✔	EFS Easy Chat server Universal BOF-SEH (Meta)	windows	FB1H2S
2010-01-20	D	-	✔	AOL 9.5 ActiveX 0day Exploit (heap spray)	windows	Dz_attacker
2010-01-19	D	-	✔	Pidgin MSN <= 2.6.4 File Download Vulnerability	multiple	Mathieu GASPARD
2010-01-18	D	A	✔	Exploit EFS Software Easy Chat Server v2.2	windows	John Babio

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

Metasploit

SOLIDO NETWORKS

What is it?

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

Idag findes der samlinger af exploits som milw0rm

Udviklingsværktøjerne til exploits er idag meget raffinerede!

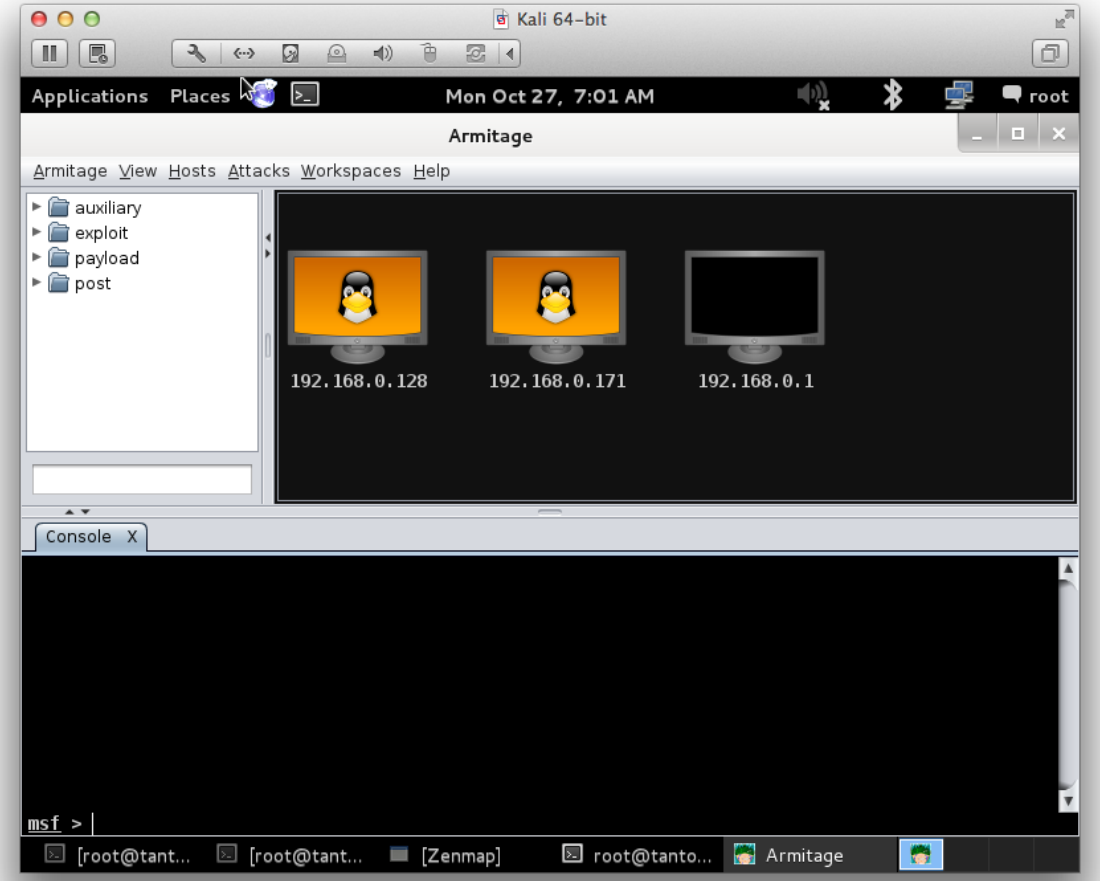
`http://www.metasploit.com/`

`http://www.fastandeasyhacking.com/` Armitage GUI til Metasploit

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

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Demo: Metasploit Armitage



CTF

Næsten hvert år afholdes en dansk CTF konkurrence

I år bliver det fredag den 28. november 2014 til lørdag

Capture the Flag er en mulighed for at afprøve sine hackerskillz

Distribueret CTF med hold Sjovt og lærerigt

Kilde: `http://prosa-ctf.the-playground.dk/`
Get ready! Lær debuggere, perl, java at kende, start på at hacke

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Questions?

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

You are always welcome to send me questions later via email

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj

Reklamer: kursusafholdelse

SOLIDO NETWORKS

Følgende kurser afholdes med mig som underviser

- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 1-2 dage
  En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og wirksomhedsnetværk.
- Hacker workshop 2 dage
  Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, Nessus m.fl.
- Forensics workshop 2 dage
  Med fokus på tilgængelige open source værktøjer gennemgås metoder og praksis af undersøgelse af diskimages og spor på computer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage
  Informere om trusler og aktivitet på Internet, samt give et bud på hvorledes en avanceret moderne firewall idag kunne konfigureres.

© license CC BY 3.0. 2015 Solido Networks, Henrik Lund Kramshøj