

Welcome to

# Basic hacking - black/white hat

Henrik Lund Kramshøj, internet samurai  
hlk@solido.net

<http://www.solidonetworks.com>



## Don't Panic!

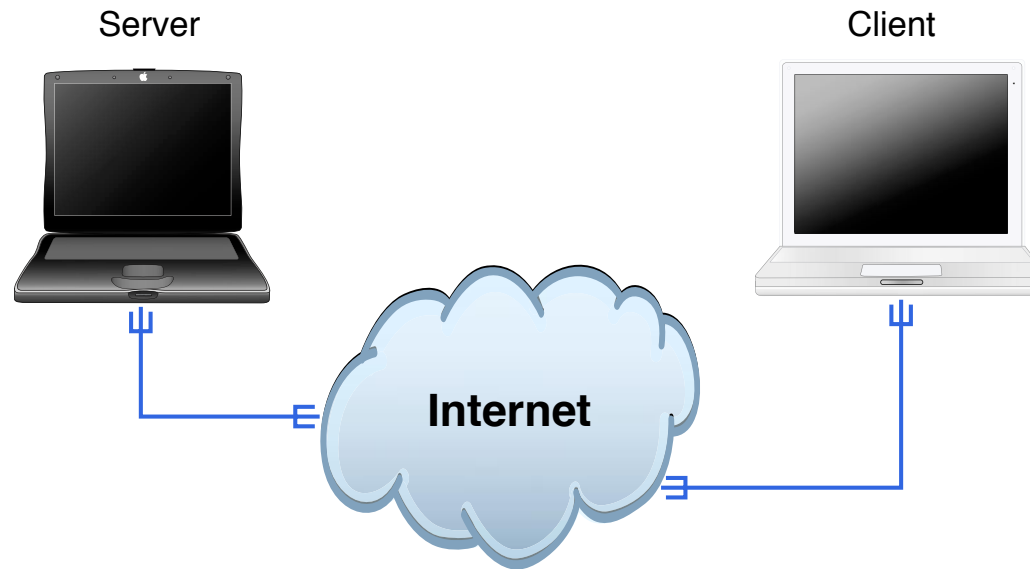
Skabe en forståelse for hackerværktøjer samt penetrationstest metoder

Design af netværk til minimering af risici.

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

Hacking kan betyde:

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




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



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

```
80/tcp    open      http
81/tcp    open      hosts2.nc
10.0.0.1  [nobile]
11 # nmap -v -sS -O 10.2.2.2
11
13 Starting nmap V. 2.540E1A25
13 Insufficient responses for TCP sequencing (3). OS detection
13 accurate
14 Interesting ports on 10.2.2.2:
44 (The 1539 ports scanned but not shown below are in state: closed)
51 Port      State      Service
51 22/tcp    open      ssh
58
68 No exact OS matches for host
68
24 Nmap run completed -- 1 IP address (1 host up) scanned
50 # sshnuke 10.2.2.2 -rootpw-"210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "210N0101".
System open: Access Level (9)
H # ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

<http://nmap.org/movies.html>

Meget realistisk [http://www.youtube.com/watch?v=51lGCTgqE\\_w](http://www.youtube.com/watch?v=51lGCTgqE_w)



Hacking ligner indimellem magi



Hacking kræver blot lidt ninja-træning



*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>

Alle bruger nogenlunde de samme værktøjer

- Portscanner - Fyodor 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, ...

## 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/>

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
- Programmeringserfaring 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



- 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

Tænk som en hacker

## Rekognoscering

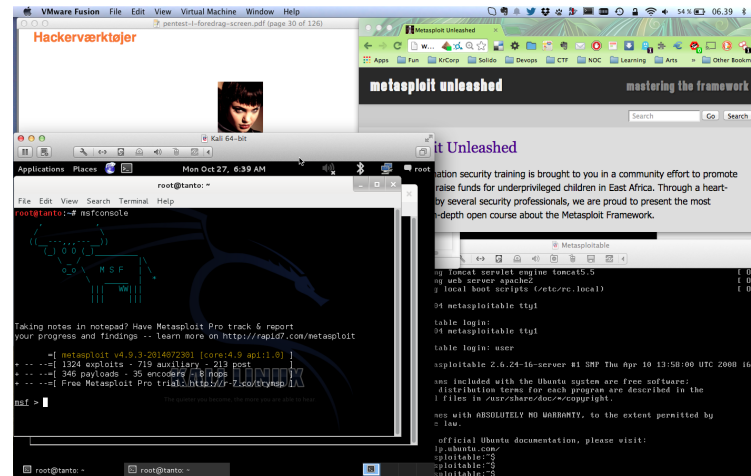
- ping sweep, port scan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

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.



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

OSI Reference  
Model

Application
Presentation
Session
Transport
Network
Link
Physical

Internet protocol suite

Applications  HTTP, SMTP, FTP, SNMP,	NFS
	XDR
	RPC
TCP UDP	
IPv4	IPv6 ICMPv6 ICMP
ARP RARP	
MAC	
Ethernet token-ring ATM ...	



## Udnyttede følgende sårbarheder


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

## Avanceret + camouflage!

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

Lavet af Robert T. Morris, Jr.

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



The screenshot shows the Wireshark website homepage. At the top is a blue banner with the Wireshark logo (a shark fin) and the word "WIRESHARK" in large, bold, black letters. To the right of the logo is a small image of a shark swimming underwater. Below the banner is a navigation bar with links: HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. The main content area is divided into several sections. On the left is a sidebar with links under the heading "Get It" (Download), "Get Help" (FAQs, Documentation, Mailing Lists, Wiki, Bug tracker), "Develop" (Developer Info), and "Products" (AirPcap, Network Toolkit, OEM WinPcap). The central part of the page features a section titled "Sniffing Problems A Mile Away" with a sub-header "The Ethernet network protocol analyzer has changed its name to Wireshark." and a paragraph explaining the name change and the software's features. To the right of this text is a small screenshot of the Wireshark interface showing a packet capture. Below this is a "News" section titled "Wireshark 0.99.3 Released" dated "Aug 23, 2006", with a paragraph about security-related vulnerabilities being fixed. On the right side of the page is a "Download Now" section showing the version "0.99.3". Below this is a Q&A section with a question "How do I capture 802.11 traffic on Windows?" and an answer "A:" followed by the AirPcap logo.

## WIRESHARK

HOME ABOUT WHAT'S NEW DOWNLOAD FAQ

### Get It

[Download](#)

### Get Help

[FAQs](#)  
[Documentation](#)  
[Mailing Lists](#)  
[Wiki](#)  
[Bug tracker](#)

### Develop

[Developer Info](#)

### Products

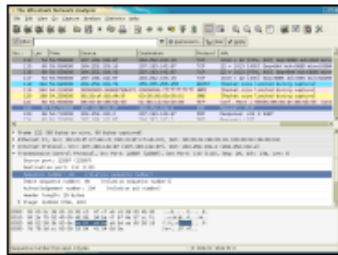
[AirPcap](#)  
[Network Toolkit](#)  
[OEM WinPcap](#)

### Sniffing Problems A Mile Away

The Ethernet network protocol analyzer has changed its name to Wireshark.

The name might be new, but the software is the same. Wireshark's powerful features make it the tool of choice for network troubleshooting, protocol development, and education worldwide.

Wireshark was written by networking experts around the world, and is an example of the power of open source. It runs on Windows, Linux, UNIX, and other platforms.




### Download Now

0.99.3

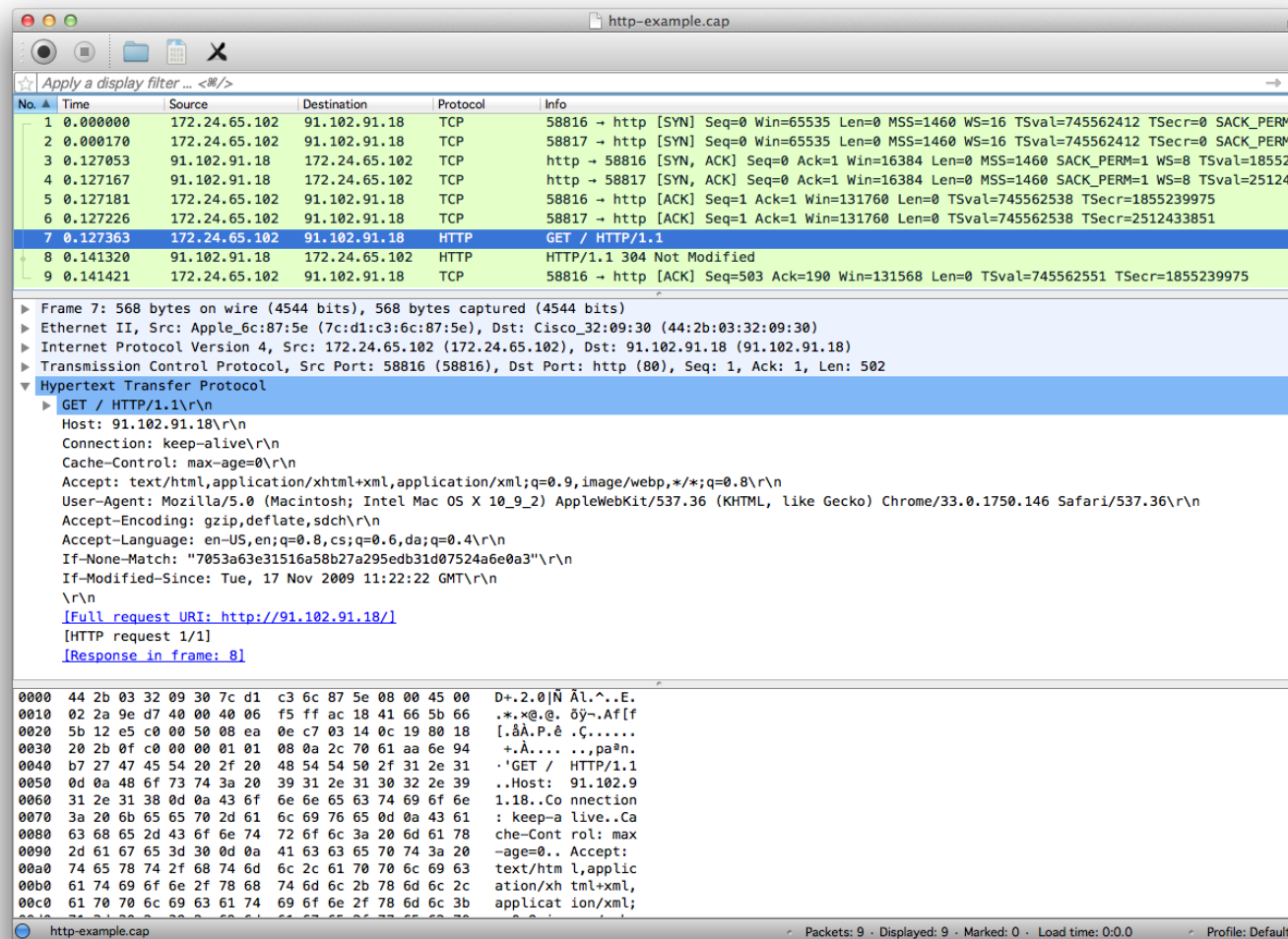
### Q:

How do I capture 802.11 traffic on Windows?

### A:



<http://www.wireshark.org>  
både til Windows og Unix



Læg mærke til filtermulighederne

traceroute programmet virker ved hjælp af TTL

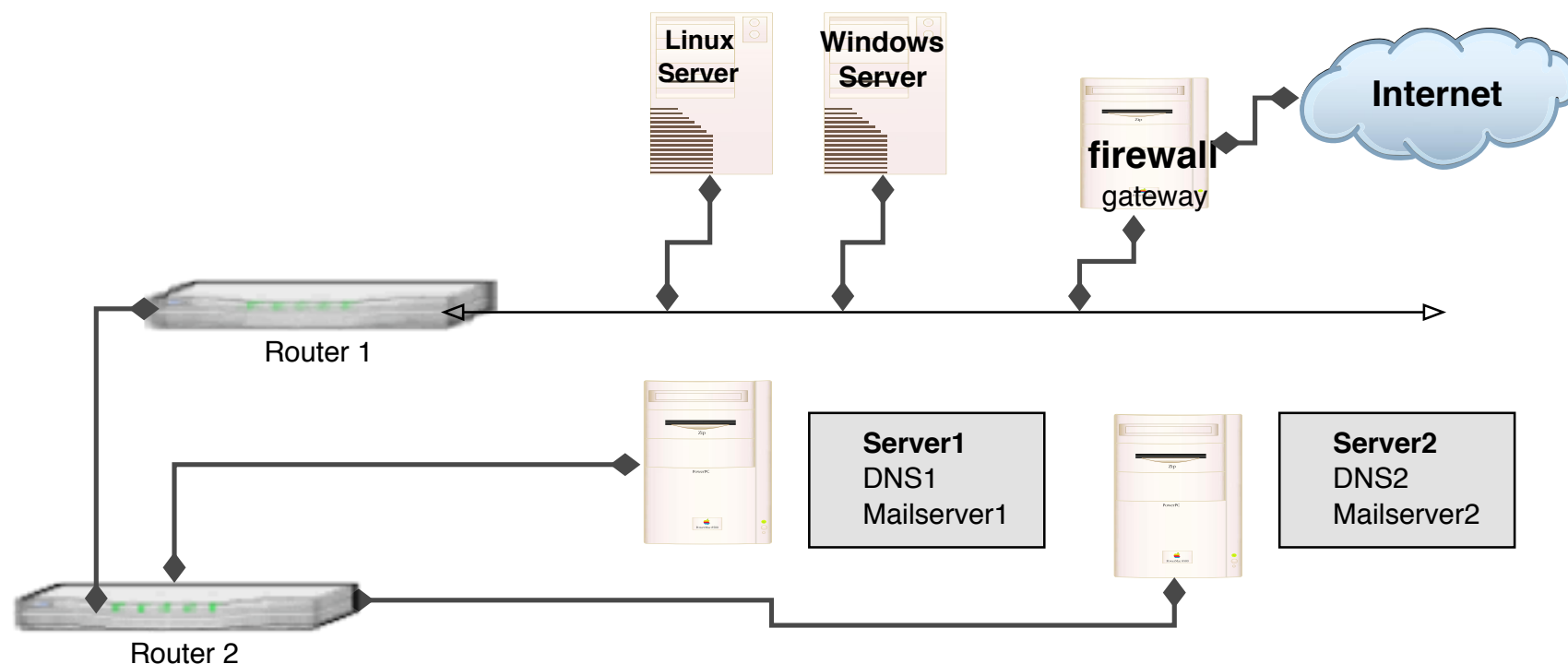
levetiden for en pakke tælles ned i hver router på vejen og ved at sætte denne lavt opnår man at pakken *timer ud* - besked fra hver router på vejen

default er UDP pakker, men på UNIX systemer er der ofte mulighed for at bruge ICMP

```
$ traceroute 91.102.91.18
```

```
traceroute to 91.102.91.18 (91.102.91.18), 64 hops max
```

```
 1  192.168.1.1 (192.168.1.1)  4.212 ms  6.932 ms  3.345 ms
 2  89.150.142.1 (89.150.142.1)  33.975 ms  24.961 ms  26.780 ms
 3  ge0-0-0.dex1.vby.dk.ip.fullrate.dk (90.185.4.17)  25.698 ms  41.764 ms  30.
 4  te5-1.cosw1.hoer.dk.ip.fullrate.dk (90.185.7.77)  25.540 ms  30.221 ms  33.
 5  te6-1.alb2nxc7.dk.ip.tdc.net (87.54.42.85)  27.565 ms  42.934 ms  25.277 ms
 6  so-4-0-0.ar1.cph1.gblx.net (64.208.110.21)  31.336 ms  28.399 ms  25.565 ms
 7  ge1-2-10g.ar3.cph1.gblx.net (67.17.105.246)  43.153 ms  33.472 ms  27.527 m
 8  64.211.195.226 (64.211.195.226)  26.504 ms  36.456 ms  26.321 ms
 9  91.102.91.18 (91.102.91.18)  32.093 ms  29.654 ms  29.368 ms
```



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

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 netværkspakker og portscanne

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)

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`

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	zfront01.solido.net.
	IN	MX	20	zfront02.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;

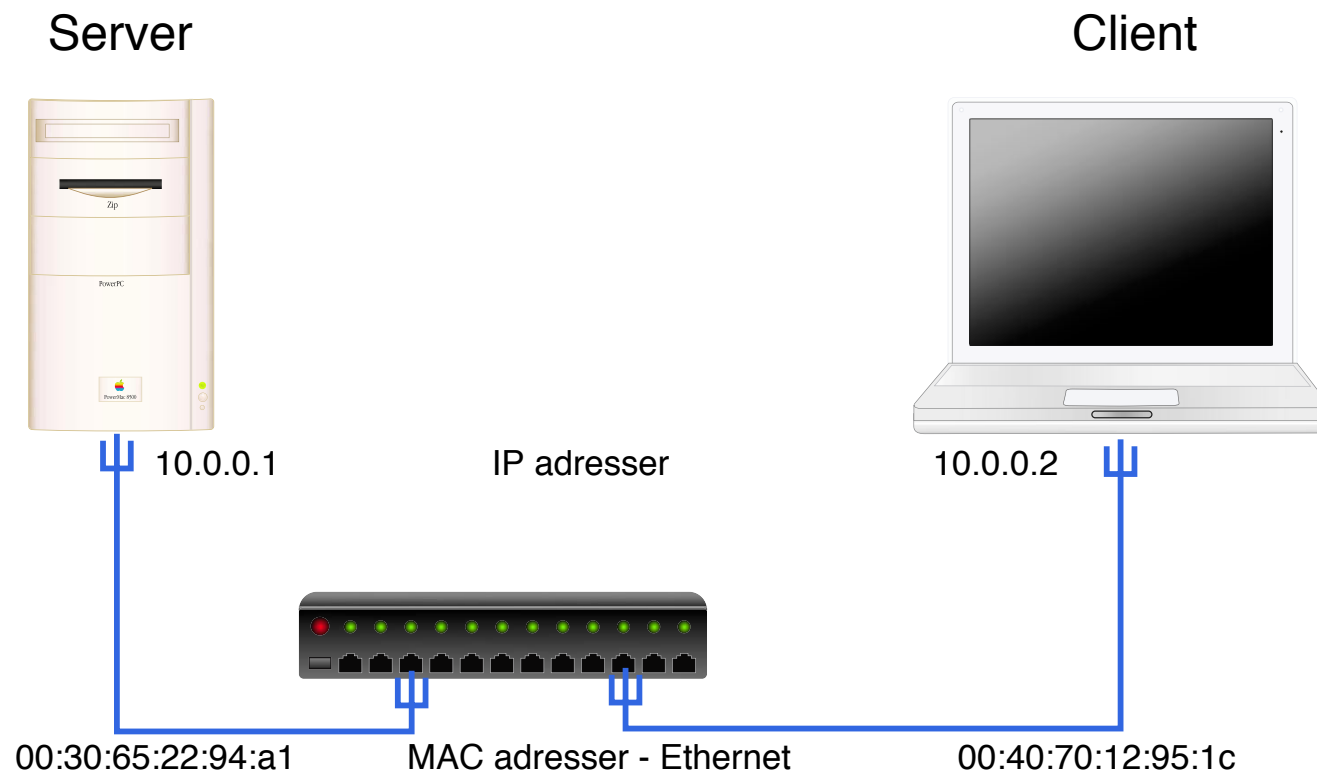
my $resolver = Net::DNS::Resolver->new;
$resolver->nameservers($ARGV[0]);

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>

# Hvordan virker ARP?



**ping 10.0.0.2** udført på server medfører

ARP Address Resolution Protocol request/reply:

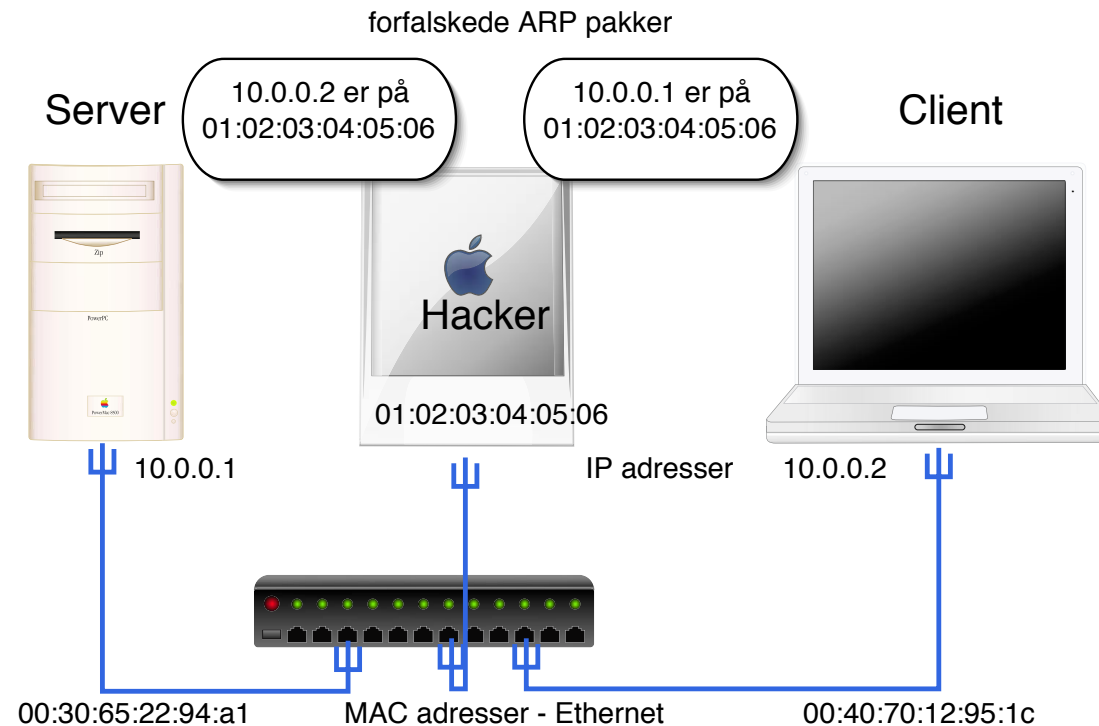
- ARP request i broadcast - Who has 10.0.0.2 Tell 10.0.0.1
- ARP reply (fra 10.0.0.2) 10.0.0.2 is at 00:40:70:12:95:1c

IP ICMP request/reply:

- Echo (ping) request fra 10.0.0.1 til 10.0.0.2
- Echo (ping) reply fra 10.0.0.2 til 10.0.0.1
- ...

ARP udføres altid på Ethernet før der kan sendes IP trafik  
(kan være RARP til udstyr der henter en adresse ved boot)

# Hvordan virker ARP spoofing?



Hackeren sender forfalskede ARP pakker til de to parter

De sender derefter pakkerne ud på Ethernet med hackerens MAC adresse som modtager - han får alle pakkerne

en sniffer til mange usikre protokoller

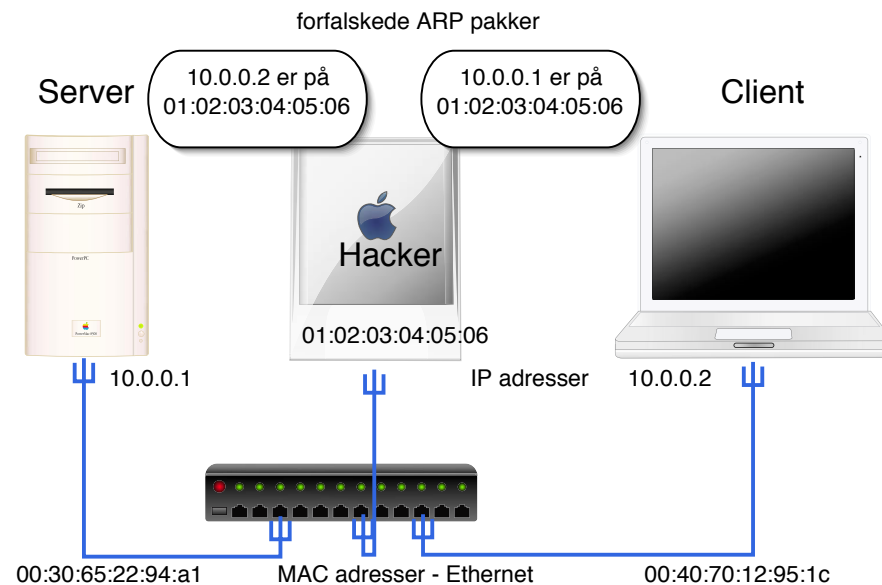
inkluderer **arpspoof**

Lavet af Dug Song, [dugsong@monkey.org](mailto:dugsong@monkey.org)

dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL\*Net, Sybase and Microsoft SQL protocols.

Der er visse forudsætninger der skal være opfyldt

- Man skal have trafikken
- Det kan gøres gennem arp spoofing eller ved at hacke ind i et system/router på netværksvejen



Hvad kan man gøre?

låse MAC adresser til porte på switche

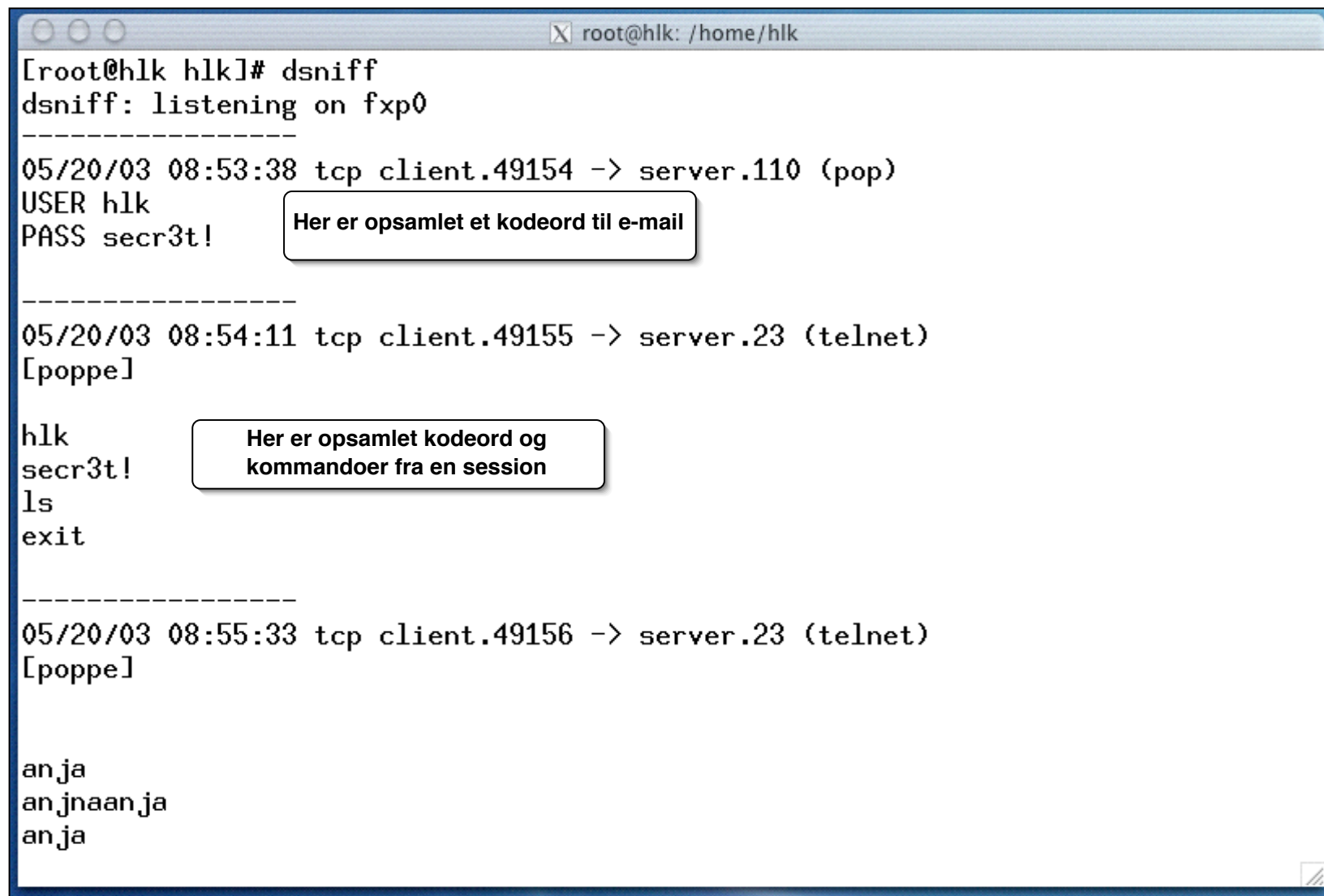
låse MAC adresser til bestemte IP adresser

Efterfølgende administration!

**arpwatch er et godt bud** - overvåger ARP

bruge protokoller som ikke er sårbare overfor opsamling

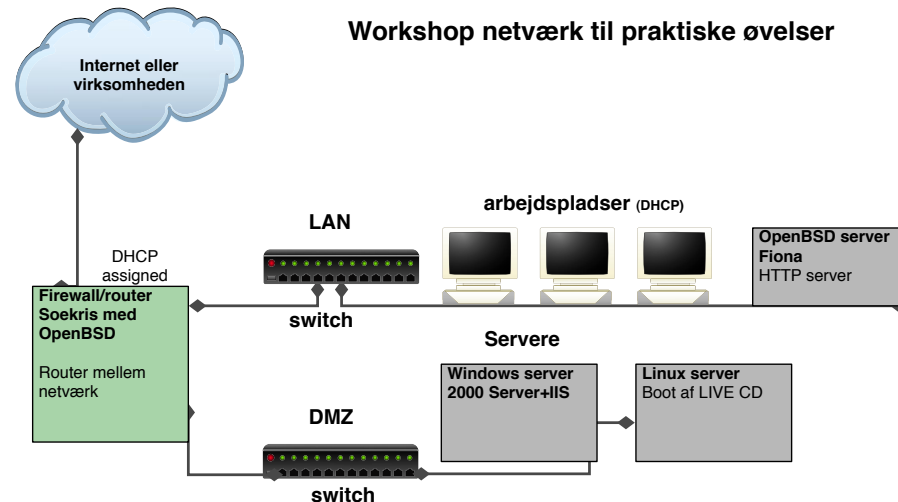




```
root@h1k: /home/h1k
[root@h1k h1k]# dsniff
dsniff: listening on fxp0
-----
05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER h1k
PASS secr3t!
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]
h1k
secr3t!
ls
exit
-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]
an ja
an jna an ja
an ja
```

Her er opsamlet et kodeord til e-mail

Her er opsamlet kodeord og kommandoer fra en session



Hvad kan man gøre for at få bedre netværkssikkerhed?

- bruge switche - der skal ARP spoofes og bedre performance
- opdele med firewall til flere DMZ zoner for at holde udsatte servere adskilt fra hinanden, det interne netværk og Internet
- overvåge, læse logs og reagere på hændelser

Hvad er portscanning

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

målet er at identificere åbne porte - sårbare services

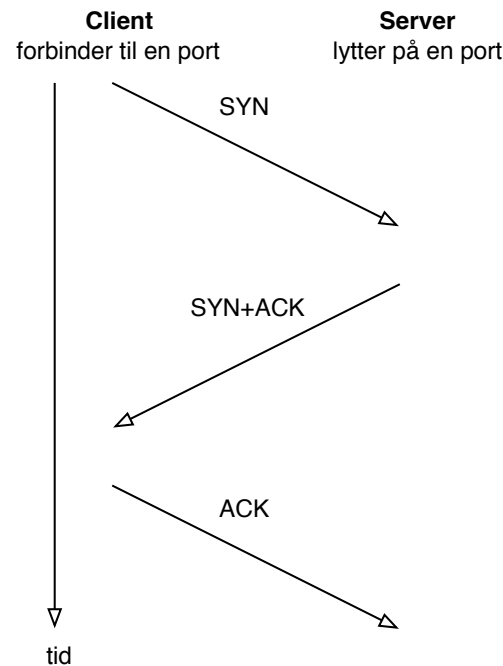
typisk TCP og UDP scanning

TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

# 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**

scanninger på tværs af netværk kaldes for sweeps

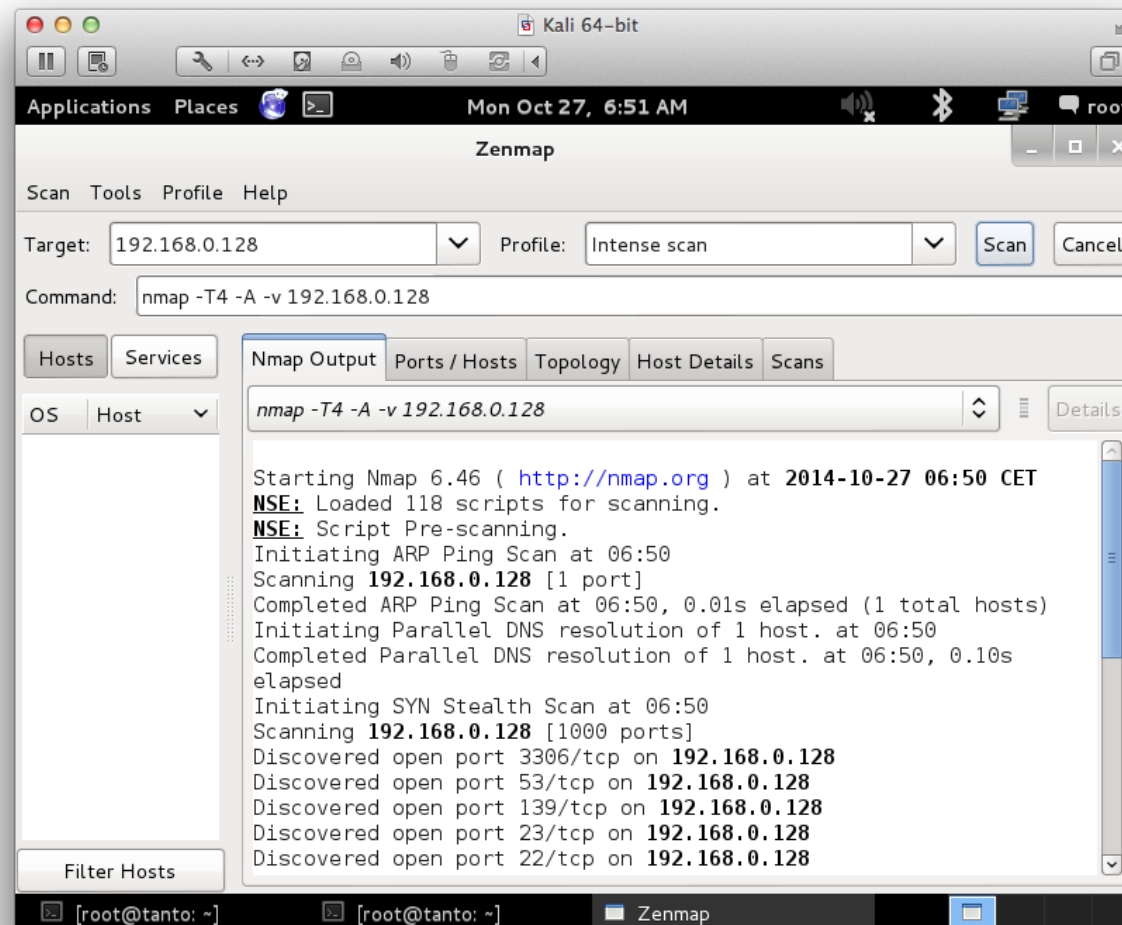
Scan et netværk efter aktive systemer med PING

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

# Portscan med Zenmap GUI



Zenmap følger med i pakken når man henter Nmap <http://nmap.org>



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



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?

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, AAAAAAAAAA

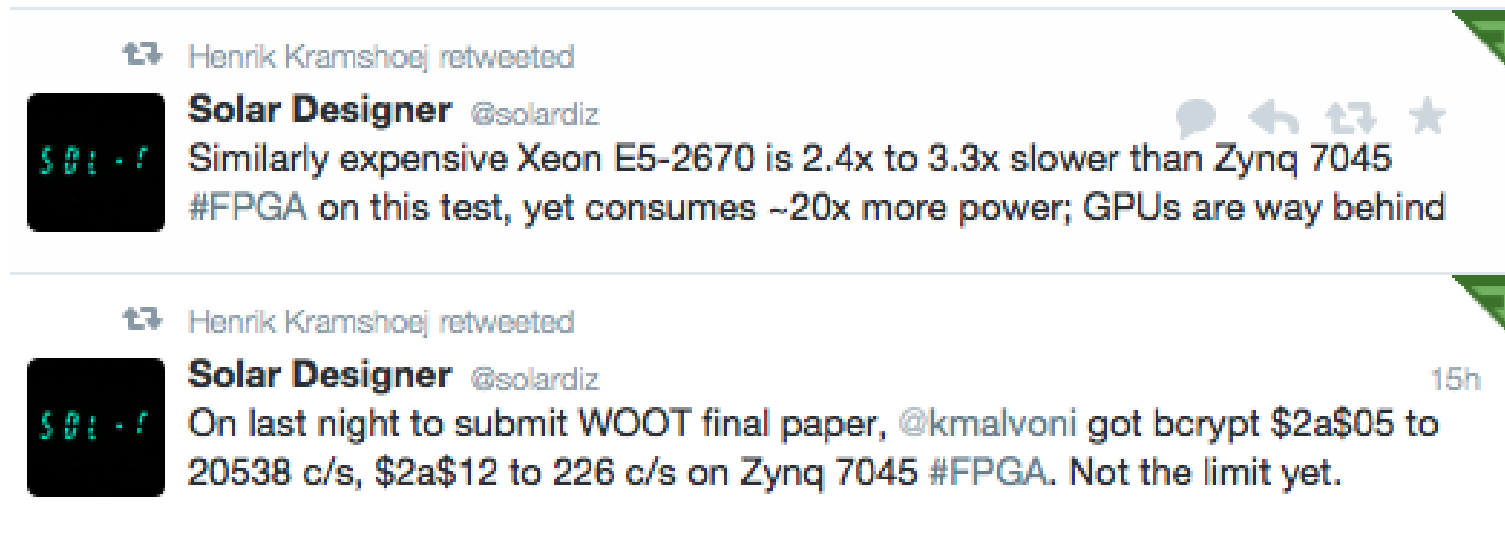
<http://masterzorag.blogspot.com/>

- 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/>

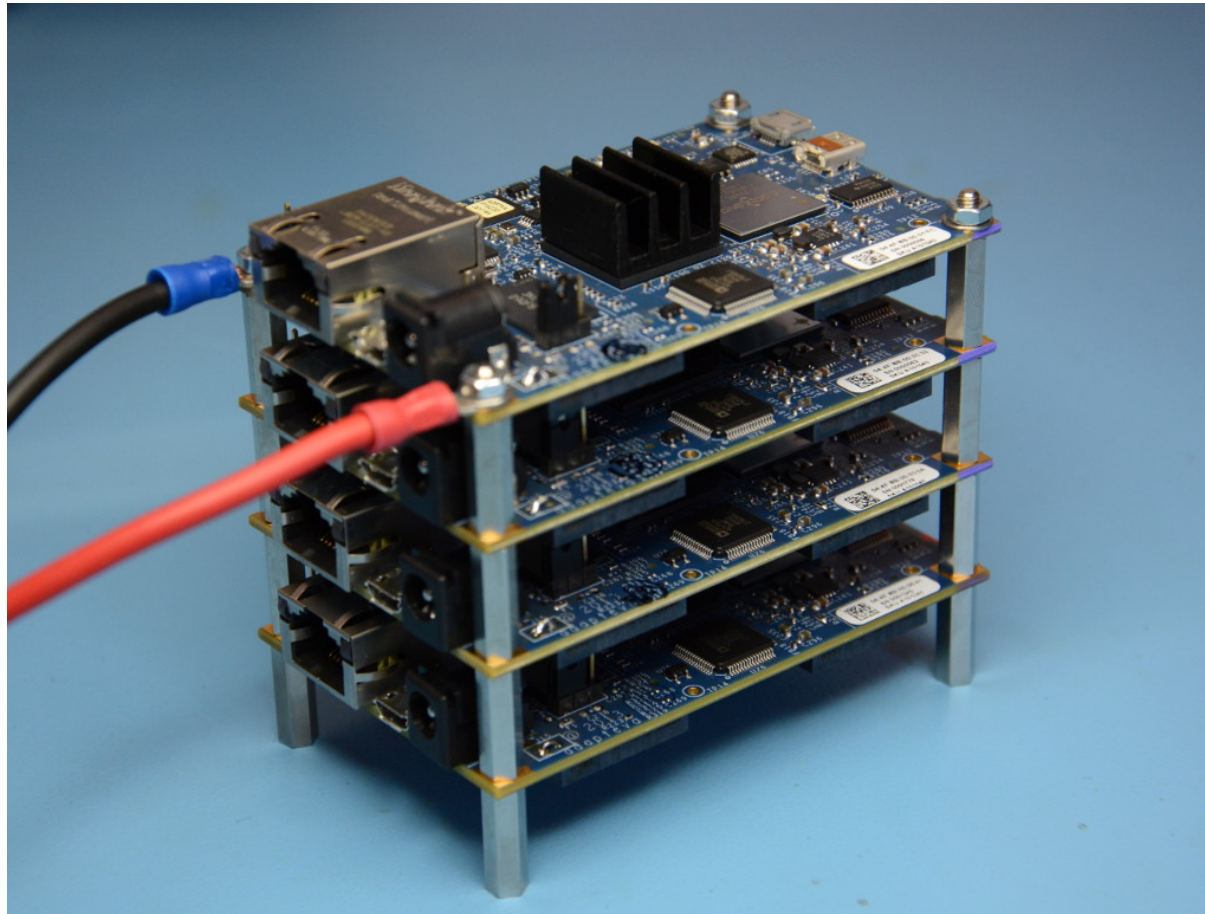
<http://www.openwall.com/john/>



<https://twitter.com/solardiz/status/492037995080712192>

Warning: FPGA hacking - not finished part of presentation ☺

# Stacking Parallella boards

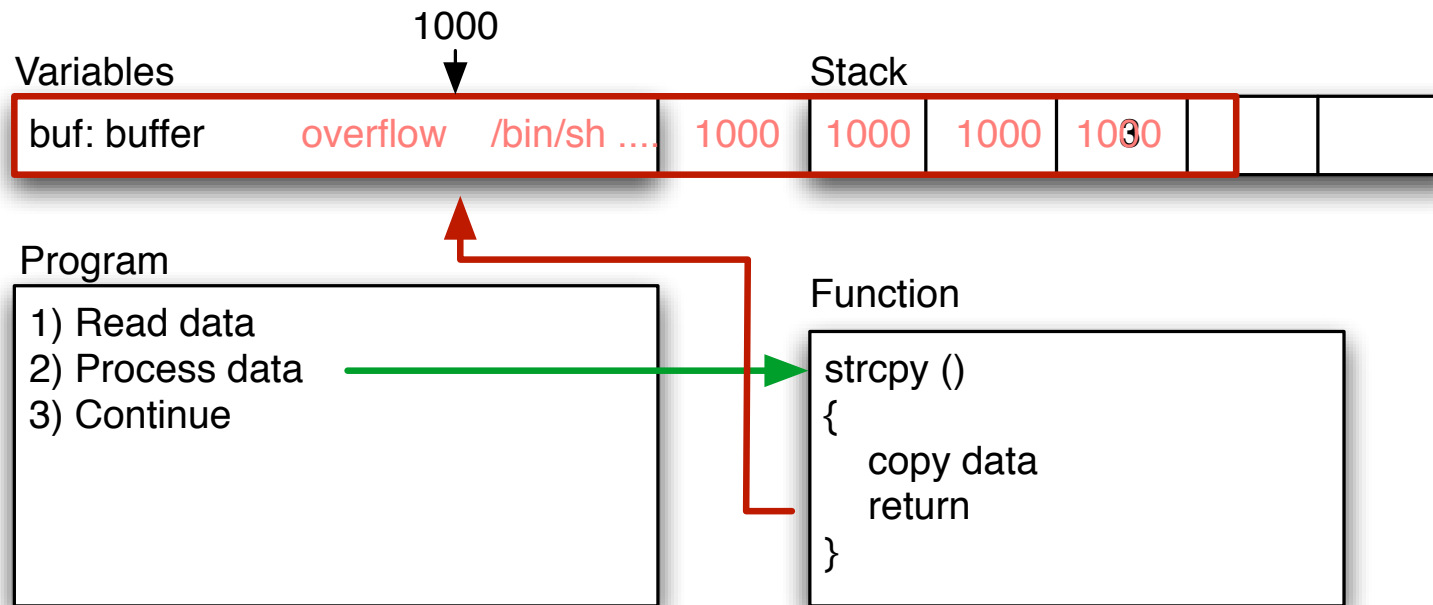


<http://www.parallella.org/power-supply/>

# Real life bruteforce? Found in on real server

```
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
```

# Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

**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.



## Variables

buf: buffer

## Program

- 1) Read data
- 2) Process data
- 3) Continue

## Stack

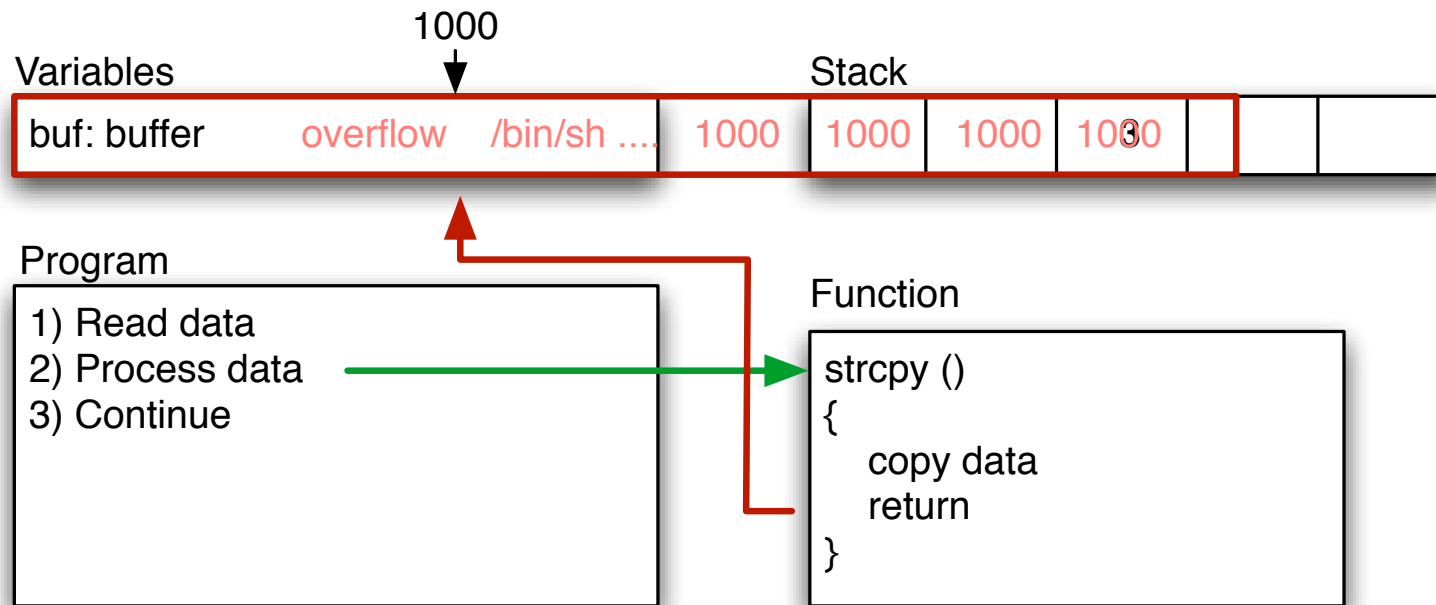


## Function

```
strcpy ()  
{  
    copy data  
    return  
}
```

```
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

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

```
$buffer = "";  
$null = "\x00";  
$nop = "\x90";  
$nopsiz = 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 += $nopsiz) {  
    $buffer .= $nop;  
}  
$address = pack('l', $the_shell_pointer);  
$buffer .= $address;  
exec "$program", "$buffer";
```

Demo exploit in Perl

Vi laver sammen en session med GDB

Afprøvning med diverse input

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

## 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`

```
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 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Starting program: /Volumes/userdata/projects/security/exploit/demo/demo AAAAAAA
Reading symbols for shared libraries . done
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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

# 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

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



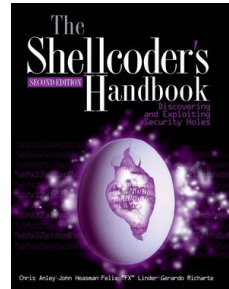
**privilege escalation** er når man på en eller anden vis opnår højere privileger på et system, eksempelvis som følge af fejl i programmer der afvikles med højere privilegier. Derfor HTTPD servere på UNIX afvikles som nobody - ingen specielle rettigheder.

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

**local vs. remote** 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



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

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

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>



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.
- ... og hackere forsøger hele tiden at omgå det.

OpenBSD er nok nået længst og et godt eksempel

<http://www.openbsd.org/papers/>

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

Senere i 1995 udgav de så en softwarepakke med navnet SATAN *Security Administrator Tool for Analyzing Networks* Pakken vagte en del furore, idet man jo gav alle på internet mulighed for at hacke

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.

SATAN og ideerne med automatiseret scanning efter sårbarheder blev siden ført videre i programmer som Saint, SARA og idag findes mange hackerværktøjer og automatiserede scannere:

- Nessus, ISS scanner, Fyodor Nmap, Typhoon, ORAScan

**Kilde:** [http://www.porcupine.org/satan/demo/docs/admin\\_guide\\_to\\_crack.html](http://www.porcupine.org/satan/demo/docs/admin_guide_to_crack.html)

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



The screenshot shows the homepage of the Exploit Database. At the top, the word "EXPLOIT" is displayed in large, stylized letters, with "Database" written below it in a smaller font. To the right, it says "Currently Archiving 10343 Exploits". Below the header is a navigation bar with links: [ home ] [ news ] [ remote ] [ local ] [ web ] [ dos ] [ shellcode ] [ papers ] [ search ] [ D ] [ submit ] [ rss ]. The main content area features the title "The Exploit Database" followed by a description: "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." Below this, there are two lines of text: "We are running a general cleanup on the DB and have changed our submission policy - please **check it out** before submitting exploits to us." and "Due to recent DOS attacks, our application downloads are now captcha protected." The section "Remote Exploits" is highlighted with a large quote icon. Below it is a table listing recent 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	✓	IntelliTammer 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 Oday 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/>



```
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 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.

## 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 exploit-db og Metasploit

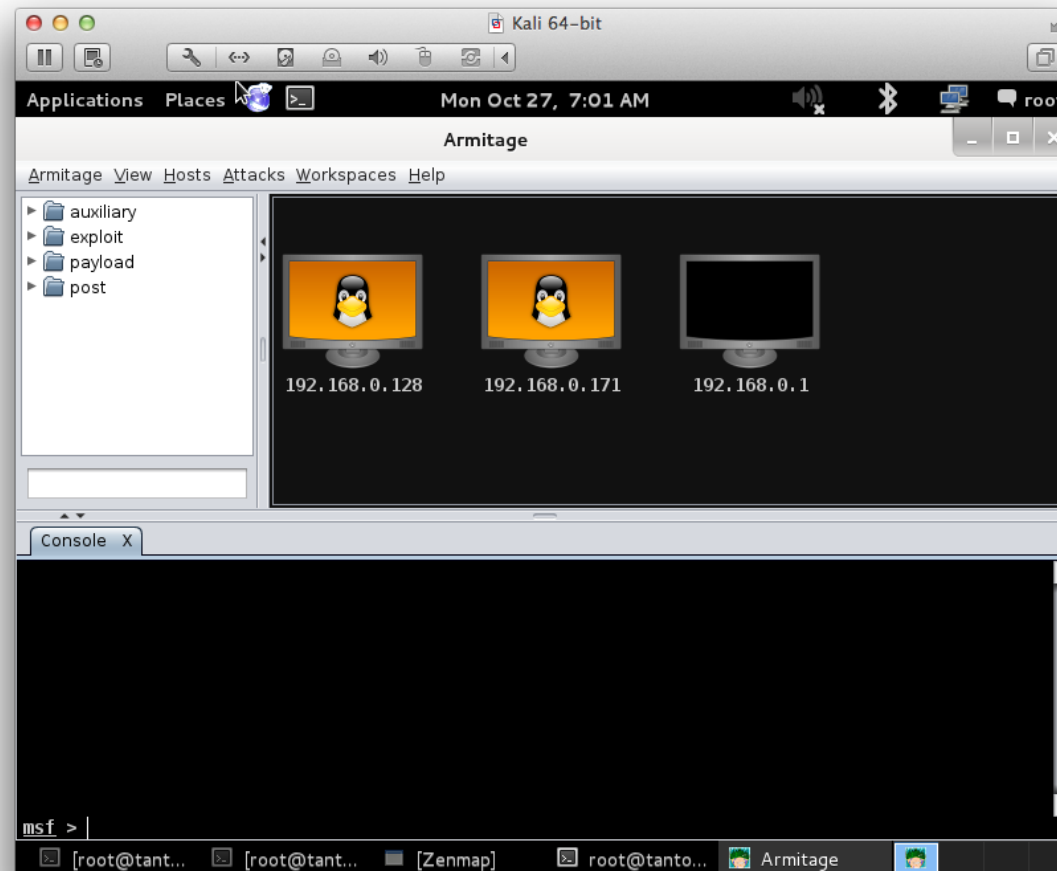
Udviklingsværktøjerne til exploits er idag meget raffinerede!

<http://www.metasploit.com/>

<http://www.fastandeasyhacking.com/> Armitage GUI til Metasploit

<http://www.offensive-security.com/metasploit-unleashed/>

# Demo: Metasploit Armitage





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

Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
- God sikkerhed kommer fra langsigtede initiativer
- Hvad er informationssikkerhed?
- Data på elektronisk form
- Data på fysisk form
- Social engineering er måske overset - *The Art of Deception: Controlling the Human Element of Security* af Kevin D. Mitnick, William L. Simon, Steve Wozniak

Computer Forensics er reaktion på en hændelse

## Informationssikkerhed er en proces

Henrik Lund Kramshøj, internet samurai  
`hlk@solido.net`

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email

(ISC)<sup>2</sup><sup>SM</sup>

(CISSP)<sup>®</sup>

(SSCP)<sup>CM</sup>

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

## 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



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 lidenskabeligt (eller enddog fanatisk) eller en der foretrækker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofte arbejder med eller på det; som i "en Unixhacker".

Kilde: Peter Makholm, <http://hacking.dk>

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