Welcome to

Network Management

Communication and Network Security 2019

Henrik Lund Kramshøj hlk@zencurity.com

Slides are available as PDF, kramse@Github

7-Network-Management.tex in the repo security-courses

NTP Network Time Protocol

NTP opsætning

foregår typisk i `/etc/ntp.conf` eller `/etc/ntpd.conf`

det vigtigste er navnet på den server man vil bruge som tidskilde

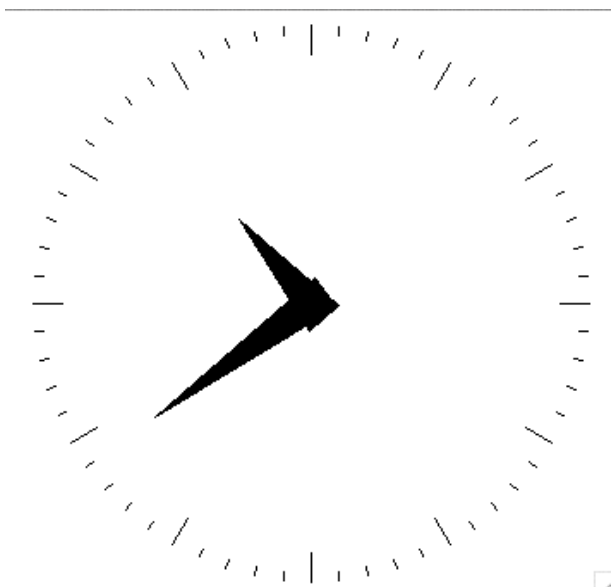
Brug enten en NTP server hos din udbyder eller en fra `http://www.pool.ntp.org/`

Eksempelvis:

```
server ntp.cybercity.dk

server 0.dk.pool.ntp.org
server 0.europe.pool.ntp.org
server 3.europe.pool.ntp.org
```

What time is it?



Hvad er klokken?

Hvad betydning har det for sikkerheden?

Brug NTP Network Time Protocol på produktionssystemer

What time is it? - spørg ICMP

ICMP timestamp option - request/reply

hvad er klokken på en server

Slayer icmpush - er installeret på server

viser tidstempel

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

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

Stop - NTP Konfigurationseksempler

Vi har en masse udstyr, de meste kan NTP, men hvordan

Vi gennemgår, eller I undersøger selv:

- Airport

- Switche (managed)
- Mac OS X
- OpenBSD - check `man rdate` og `man ntpd`

BIND DNS server

Berkeley Internet Name Daemon server

Mange bruger BIND fra Internet Systems Consortium - altså Open Source

konfigureres gennem `named.conf`

det anbefales at bruge BIND version 9

- *DNS and BIND*, Paul Albitz & Cricket Liu, O'Reilly, 4th edition Maj 2001
- *DNS and BIND cookbook*, Cricket Liu, O'Reilly, 4th edition Oktober 2002

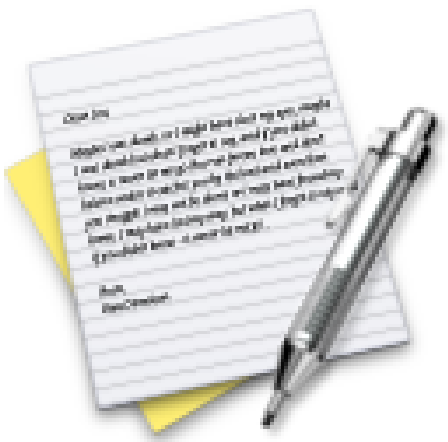
Kilde: `http://www.isc.org`

BIND konfiguration - et udgangspunkt

```
acl internals { 127.0.0.1; ::1; 10.0.0.0/24; };
options {
        // the random device depends on the OS !
        random-device "/dev/random"; directory "/namedb";
        port 53; version "Dont know"; allow-query { any; };
};
view "internal" {
   match-clients { internals; };
   recursion yes;
   zone "." {
       type hint;   file "root.cache"; };
   // localhost forward lookup
   zone "localhost." {
        type master; file "internal/db.localhost";   };
   // localhost reverse lookup from IPv4 address
   zone "0.0.127.in-addr.arpa" {
        type master; file "internal/db.127.0.0"; notify no;   };
```

```
...
}
```

Exercise

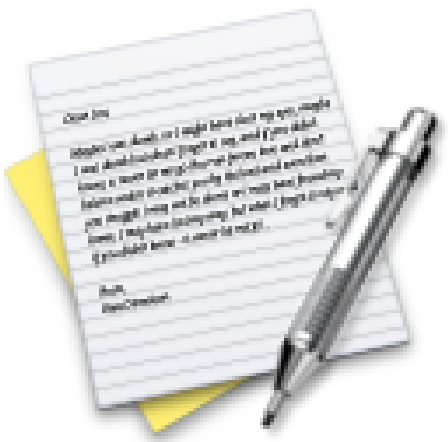


Now lets do the exercise

??

which is number **??** in the exercise PDF.

Exercise

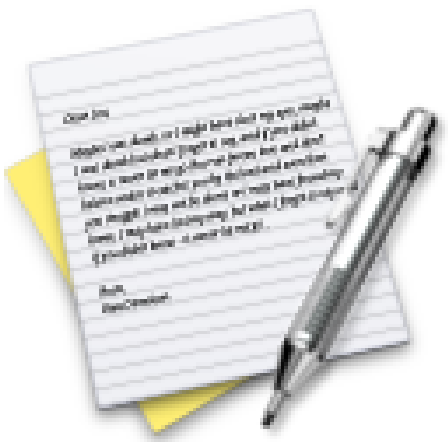


Now lets do the exercise

??

which is number **??** in the exercise PDF.

Exercise



Now lets do the exercise

??

which is number **??** in the exercise PDF.

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

DHCPD server

Dynamic Host Configuration Protocol Server

Mange bruger DHCPD fra Internet Systems Consortium
`http://www.isc.org` - altså Open Source

konfigureres gennem `dhcpd.conf` - næsten samme syntaks som BIND

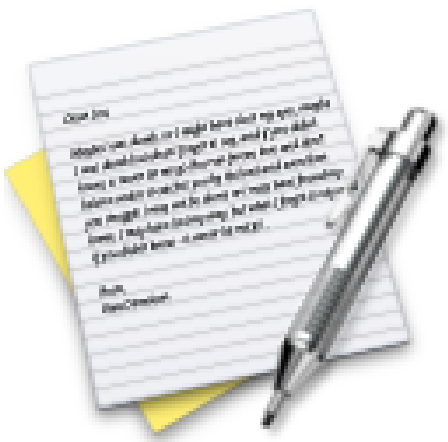
DHCP er en efterfølger til BOOTP protokollen

```
ddns-update-style ad-hoc;

shared-network LOCAL-NET {
    option  domain-name "security6.net";
    option  domain-name-servers 212.242.40.3, 212.242.40.51;
    subnet 10.0.42.0 netmask 255.255.255.0 {
            option routers 10.0.42.1;
            range 10.0.42.32 10.0.42.127;
```

```
    }
}
```

Exercise



Now lets do the exercise

??

which is number **??** in the exercise PDF.

Simple Network Management Protocol

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

hosts - skal slås til men følger som regel med

SNMP bruges til:

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

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

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

SNMP - *hacking*

Simple Network Management Protocol

sikkerheden afhænger alene af en Community string SNMPv2

typisk er den nem at gætte:

- public - default til at aflæse statistik
- private - default når man skal ændre på enheden, skrive
- cisco
- ...

Der findes lister og ordbøger på nettet over kendte default communities

Systemer med SNMP

kan være svært at finde ... det er UDP 161

Hvis man finder en så prøv at bruge **snmpwalk** programmet - det kan vise alle tilgængelige SNMP oplysninger fra den pågældende host

det kan være en af måderne at identificere uautoriserede WLAN Access Points på - sweep efter port 161/UDP

snmpwalk er et af de mest brugte programmer til at hente snmp oplysninger - i forbindelse med hackning og penetrationstest

snmpwalk

Typisk brug er:

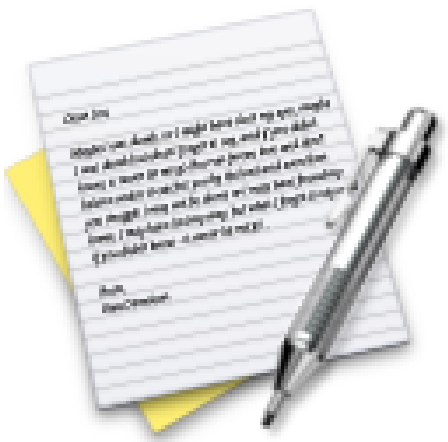
`snmpwalk -v 1 -c secret switch1`

`snmpwalk -v 2c -c secret switch1`

Eventuelt bruges `snmpget` og `snmpset`

Ovenstående er en del af Net-SNMP pakken, `http://net-snmp.sourceforge.net/`

Exercise



Now lets do the exercise

??

which is number **??** in the exercise PDF.

brute force

hvad betyder bruteforcing?
afprøvning af alle mulighederne

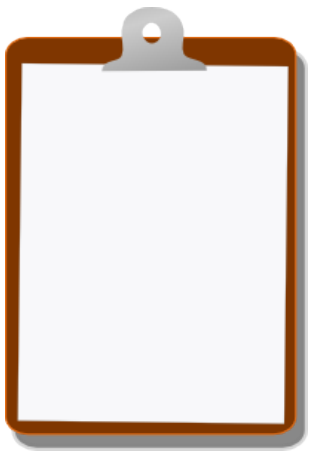
```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]
Options:
  -S        connect via SSL
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN  or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS   or -P FILE try password PASS, or load several passwords from FILE
  -e ns     additional checks, "n" for null password, "s" try login as pass
  -C FILE   colon seperated "login:pass" format, instead of -L/-P option
  -M FILE   file containing server list (parallizes attacks, see -T)
  -o FILE   write found login/password pairs to FILE instead of stdout
...
```

Eksempler på SNMP og management

Ofte foregår administration af netværksenheder via HTTP, Telnet eller SSH

- små dumme enheder er idag ofte web-enablet
- bedre enheder giver både HTTP og kommandolinieadgang
- de bedste giver mulighed for SSH, fremfor Telnet

For Next Time



- Think about the subjects from this time, write down questions
- Check the plan for chapters to read in the books
  Most days have about 100 pages or less, but one day has 4 chapters to read!
- Visit web sites and download papers if needed
- Retry the exercises to get more confident using the tools