Netværkssikkerhed i firmanetværk

øvelseshæfte

Henrik Lund Kramshøj

hlk@solido.net

5. oktober 2012

Indhold

Forord

Dette kursusmateriale er beregnet til brug på kurset *Netværkssikkerhed i firmanetværk workshop*. Materialet er lavet af Henrik Lund Kramshøj, http://www.solidonetworks.com
Materialet skal opfattes som beskrivelse af netværkssetup og applikationer til kurser og workshops med behov for praktiske øvelser.
Til workshoppen hører desuden en præsentation som udleveres og der henvises til et antal dokumenter som kan hjælpe under øvelserne.

God fornøjelse

Oversigt

Materialet er inddelt i et antal områder som er beregnet til at give valgfrihed i opsætningen af miljøet.

Formålet med kurserne at ofte at give kursusdeltagerne et indblik i hvordan emnet i praksis ser ud og opfører sig. De foreslåede konfigurationer ligger derfor tæt op ad virkelige konfigurationer, men kan samtidig passes ind i et eksisterende kursusnetværk.

Forudsætninger

Dette materiale forudsætter at deltageren har kendskab til TCP/IP på brugerniveau. Det betyder at begreber som www.solidonetworks.com, hlk@solido.net, IP-adresse og DHCP ikke bør være helt ukendte.

Værktøjer

Materialet er beregnet på at kunne udføres i et almindeligt kursuslokale med netværksopkoblede pc'er.

De praktiske øvelser benytter i vid udstrækning Open Source og kan derfor afvikles på blandt andet følgende platforme:

- Unix - herunder Linux, OpenBSD, NetBSD, FreeBSD og Mac OS X
- Microsoft Windows 2000 og XP - primært som klientoperativsystem
- Kravene til kursisternes arbejdspladser er generelt en browser og SSH adgang
- På visse kurser udleveres en Linux boot CD som kan benyttes til at skifte kursusisternes arbejdsplads til at køre Linux

Udover de programmer der gennemgås er der følgende programmer som kan være til stor nytte:

- http://www.openbsd.org - OpenBSD - en moderne Unix med fokus på sikkerhed
- http://www.openssh.com - OpenSSH - Secure Shell værktøjer både server og klientprogrammer. Giver sikkerhed mod aflytning

Introduktion til netværk

TCP/IP - Internet protokollerne

Det er vigtigt at have viden om IP for at kunne implementere sikre infrastrukturer da man ellers vil have svært ved at vælge mellem de mange muligheder for implementation.

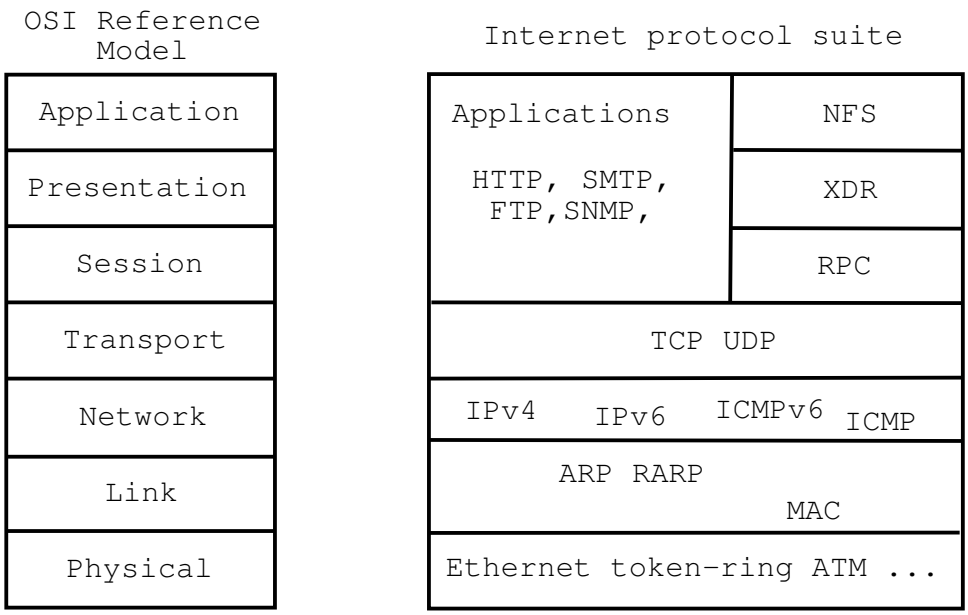
OSI reference model

En af de mest benyttede modeller til beskrivelse af netværk er OSI reference modellen som gennemgås i alle datakommunikationsbøger.

Denne model beskriver hvorledes man kan opdele funktionerne i netværk i lag som så kan implementeres uafhængigt og derfor kan udskiftes nemmere - eksempelvis når der kommer nye transmissionsteknologier på de lavere niveauer.

På billedet ses en oversigt over OSI referencemodellen, også kaldet 7-lags modellen. OSI modellen sammenlignes med internetmodellen, som ligeledes er lagdelt.

Fordelen ved at opdele i flere lag er at man kan løse problemerne uafhængigt og får frihed til at udskifte dele. Eksempelvis er de nederste fysiske lag med tiden blevet hurtigere ved skift fra 10Mbit Ethernet baseret på coax-kabler, henover 100Mbit Ethernet på twisted-pair kabler til idag hvor Gigabit er udbredt.



Figur 1: OSI og Internetmodellerne

Standarder og RFC'er

De dokumenter som beskriver internet-standarderne udgives i en række Request for Comments (RFC'er) som kan hentes via ftp://ftp.ietf.org/rfc. Når en standard eller et dokument i denne serie opdateres sker det ved genudgivelse

under et nyt nr - og derved bevares de gamle versioner af alle dokumenterne. For at lette navigeringen i disse dokumenter udgives et index-dokument som blandt andet beskriver om et dokument er erstattet med en ny version. I serien er også oversigter over opdelinger indenfor RFC'erne: eksempelvis standarder (STD), For Your Information (FYI) og Best Current Practice (BCP).

Et eksempel fra index filen er IP specifikationen (version 4):
0791 Internet Protocol. J. Postel. Sep-01-1981. (Format: TXT=97779 bytes) (Obsoletes RFC0760) (Updated by RFC1349) (Also STD0005) (Status: STANDARD)

Det betyder at RFC-0791 altså er en standard og den erstatter RFC-0760.

Hvis man så kigger på den tilsvarende information for et *forældet* dokument ser det således ud:
760 DoD standard Internet Protocol. J. Postel. Jan-01-1980. (Format: TXT=81507 bytes) (Obsoletes IEN 123) (Obsoleted by RFC0791) (Updated by RFC0777) (Status: UNKNOWN)

Hardware og netværk til øvelserne

I dette afsnit beskrives de krav der stilles til miljøet hvor de beskrevne øvelser kan udføres.

Forudsætningerne for øvelserne er et lokale med et antal PC'er med Microsoft Windows klienter og netværksadgang.

En del af øvelserne udføres med Unix, specifikt med OpenBSD, dette valg er udfra en betragtning om at det er meget stabilt og understøtter de funktioner godt som beskrives i kurset.

OpenBSD er et moderne operativsystem som er frit tilgængeligt og fordi det er Open Source tillader det at man kan undersøge og tilpasse systemet. Man kan endda benytte BSD systemerne kommercielt - hvis man ønsker det.

Hvis der er mulighed for det kan man installere en anden Unix variant, ellers skal der som minimum være adgang til en maskine som flere brugere deler:

- Et flerbruger Unix system som eksempelvis kan være OpenBSD
- et udvalg af editorer - så folk føler sig hjemme, EMACS, VI, JOVE, Nedit ... I de grafiske brugergrænseflader findes flere lettilgængelige editorer, der som Nedit fungerer med en File -¿ Save menu.
- OpenSSH - mulighed for både login og filoverførsel på sikker vis.
- webserver med de filer der skal bruges
- hubs, switches, netkort - alt efter hvor komplekst et setup der vil arbejdes med

Et antal windows programmer stilles til rådighed via webserveren:

- putty - SSH adgang fra Windows
- winscp - nem adgang til filoverførsel via SSH indeholder tillige editor
- wireshark - open source pakkesniffer

Formålet med kurset er blandt andet at forstå hvad der sker i netværk og derfor introduceres emnerne ved hjælp af konfigurationsfiler og lavniveau beskrivelse af emnet.

Konfigurationsfilerne er ofte mere kompakte og tydelige end tilsvarende screen-dumps fra GUI programmer.

Tilsvarende implementerer GUI programmerne ikke altid alle dele af de underliggende lag - og er derfor ikke komplette. Eksempelvis indeholder firewall funktionen på Mac OS X ingen information om TCP og UDP eller forskellen på disse.

Alle filer er tilgængelige både på den lokale server i kursuslokalet og via Internet. På kurset gives anvisninger til adgangen.

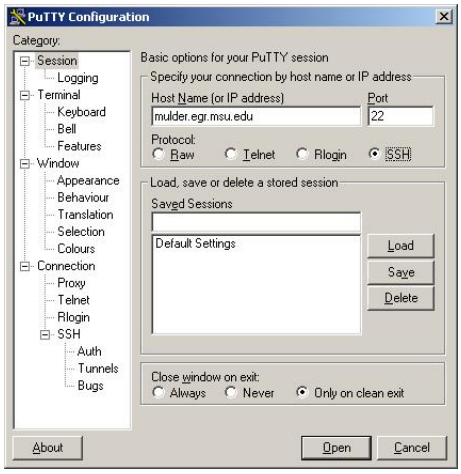
Indholdet i øvelserne

De fleste af øvelserne har følgende indhold:

- **Opgave:** Hvad går øvelsen ud på
- **Formål:** Hvad forventes det at man lærer ved at løse opgaven
- **Forslag til fremgangsmåde:** er en hjælp til at komme igang
- **Hjælp:** et eller flere tips eller beskrivelser af hvordan man kan løse opgaven
- **Forslag til løsning:** en mulig løsning til opgaven
- **Diskussion:** er oplæg til diskussion efter løsning af opgaven. Der er mulighed for at sammenligne og diskutere de valgte løsninger.

Øvelse 1

Putty installation - Secure Shell login



Opgave:
Installer Putty lokalt på Windows maskinen

Formål:
Installere et SSH program således at man kan tilgå servere og systemer senere i kurset.

Forslag til fremgangsmåde:
Hent og installer programmet, hent fra webserveren eller
http://www.chiark.greenend.org.uk/šgtatham/putty/download.html

Hjælp:
Putty er en terminal emulator og erstatter telnet programmet i Windows. Det er ofte den foretrukne bruger-grænseflade for Unix brugere og hackere. Husk at putty skal have at vide at det er SSH protokollen og ikke Telnet

Hvis der skal ændres på profiler kan Putty godt drille lidt, husk altid at trykke `Save` i profilvinduet - så indstillingerne du har valgt gemmes til næste gang

Forslag til løsning:
Hvis man kender SSH i forvejen anbefales det at man ser på brug af public key autentifikation herunder nøglegenerering og installation.

Diskussion:
SSH protokollen tillader både login og filoverførsel - secure copy

Man BØR bruge SSH protokol version 2!

NB: benyt gerne chancen til at skrive IP-adresser ind i hosts filen lokalt på din maskine.

Eksempel:

```
10.0.45.36     fiona
```

Det gør det nemmere senere at skrive `ping fiona` for at se om der er forbindelse til serveren.

Øvelse 2

WinSCP installation - Secure Copy

Opgave:
Installer WinSCP lokalt på Windows maskinen

Formål:
Installere et GUI program så man kan undersøge serversystemerne senere, eksempelvis læse konfigurationsfiler. Sekundært afprøve SSH protokollen til filoverførsel - se at det er nemt.

Forslag til fremgangsmåde:
Hent og installer programmet, hent winscp fra webserveren eller fra
http://winscp.sourceforge.net

Installer programmet som beskrevet

Hjælp:
WinSCP kan være en stor hjælp når I skal arbejde med filer på Unix systemet - I kan ofte slippe for Unix editorerne VI og EMACS

Diskussion:
Kan WinSCP bruges generelt til opdatering af websites? hvad kræver det? kan brugerne finde ud af det?

WinSCP indeholder også en editor, så vi slipper for Unix VI editor ;-)

Øvelse 3

Login på Unix systemerne

Opgave:
Brug jeres arbejdsplads til at logge ind på serverne

Det kræves at der er installeret SSH program, eksempelvis Putty fra øvelse 1.

Formål:
Få adgang til Fiona server således at man kan udføre opgaverne fra denne server senere i kurset

Forslag til fremgangsmåde:
Brug SSH til at logge ind på Fiona eller en anden host i netværket

Hjælp:
Der skal bruges enten Putty på Windows eller ssh programmet på Unix/boot CD

Med Unix/boot CD og OpenSSH kan logges ind således:
`ssh brugernavn@server -p port` dvs på fiona:
`ssh kursus1@fiona -p 22`

NB: fiona er ikke med i DNS, så brug IP-adressen!

På kursusservere er brugernavne: kursus1, kursus2, kursus3, op til kursus10 - allesammen med kodeord *kursus*.

Forslag til løsning:
Start Putty/Boot på CD'en

Diskussion:
Kan boot CD'en bruges til andre formål?

Hvad indeholder CD'en?

Hostoplysninger:

- I bedes registrere IP-adresserne for maskinerne
- Filer til installation - installationsprogrammer:
  http:// . . . /public/windows/
- IP: . . . - Din egen arbejdsstation - Windows
- IP: . . . - Fiona OpenBSD scanserver, nmap mv.
- IP: . . . -
- Til mange opgaver er det nødvendigt med superbruger privilegier - root
- Skift til root med kommandoen: `sudo -s` - hvorefter jeres prompt ændres til en have låge #

Øvelse 4

Føling med Unix

Opgave:
Brug manualsiderne til at besvare følgende spørgsmål:

- Hvad er `cal`? Hvad skete der i september 1752?
- Hvad er `date`?
- Hvad gør `clear`?
- Hvad gør `echo`?

Formål:
Prøve et par kommandoer for at blive fortrolig med Unix - det gør ikke ondt :-)

Forslag til fremgangsmåde:
Log ind på systemet og udfør opgaven fra kommandolinien.

Du kan enten skrive `man cal`, `man date`, `man clear`, `man echo` eller måske blot prøve at skrive kommandoerne

```
$ date
...
$ cal
...
$ cal 2007
...
$ cal 1752
... osv. - output er skjult med vilje i ovenstående :-)
```

Hjælp:
I denne opgave er det ligegyldigt hvilken server der vælges. Manualsystemet bruger ofte programmet `less` til at vise manualsiderne - dette program bruger / til at søge med. Tryk / og skriv et søgeord og tryk enter.

Du kan søge baglæns med spørgsmålstegnet.

Forslag til løsning:
Skriv `man cal` og søg efter 1752 med /

Diskussion:
Søgning med / og ? er ofte benyttet i Unix programmer, eksempelvis manualsystemet.

Øvelse 5

Unix - adgang til root

Opgave:
Hvad er forskellen mellem switch user `su -` og superuser do `sudo -` ?

Formål:
Lære at kunne skifte til root, således at man kan udføre eksempelvis portscan med Nmap effektivt

Forslag til fremgangsmåde:
Brug manualsiderne til at besvare følgende spørgsmål:

- Hvad er forskellen på `su -` og `sudo -s`?
- Kan su konfigures til ikke at kræve kodeord? kan sudo?
- Hvilket kodeord skal man bruge til de to kommandoer?

Hjælp:
Switch user er den gamle og kendte kommando til at skifte til en anden bruger, hvis man kender pågældende brugers kodeord.

Superuser do er en mere moderne måde at skifte bruger, eller udføre administrationskommandoer på Unix. SUDO tillader at man bruger sit eget kodeord, kodeord for brugeren man vil skifte til eller man kan konfigurere den til ikke at kræve kodeord.

Su giver altid fuld adgang og man skal give root kodeord til alle.

Sudo giver fintmasket adgang til at udføre enkelte kommandoer. Eksempelvis vil en webadministrator kunne få lov til at genstarte Apache, men ellers ikke andet som root.

Diskussion:
Sudo benyttes næsten alle steder og betragtes som de facto standarden. Nogle steder og på egne servere/workstations benyttes den ofte uden password - er det fornuftigt?

Vi skal bruge root adgang til at læse konfigurationsfiler til services og genstarte services. Pas på når I kører som root, log evt. ind som kursusbruger altid og skift kun til root med `sudo kommando` - så går det ikke helt galt :-)

Eksempel kommando med sudo:

```
hlk@bigfoot:hlk$ sudo apachectl configtest
Syntax OK
hlk@bigfoot:hlk$ sudo apachectl restart
hlk@bigfoot:hlk$
```

(Bemærk også at Unix ikke fortæller ret meget når ting går godt)

Øvelse 6

Unix boot CD

Opgave:
Boot en PC med en Unix boot CD

Formål:
Prøve en værktøjskasse med netværksværktøjer.

Forslag til fremgangsmåde:
Brug den udleverede CD i en PC, eller vi gør det fælles

Hjælp:
Der findes et stort antal boot CD'er baseret på Linux til forskellige formål. Nogle af de mest kendte indenfor sikkerhed er:

- BackTrack Linux - en større samling af sikkerhedsbærktøjer til penetrationstest
- Damn Vulnerable Linux, en usikker Linux distribution, hvor man kan lære om sikkerhedsproblemer i software

Diskussion:
Til mange af CD'erne er der nogle boot koder som indimellem er nødvendige - typisk for at vælge opløsning for det grafiske miljø. Hvis CD'en ikke virker i en bestemt maskine kan det være nødvendigt at prøve i en mere standard maskine.

Typisk er det fordi producenterne af trådløse netkort og grafikkort ikke vil oplyse specifikationerne og instruktionerne til at programmere enheden.

Specielt hvis man ønsker at bruge trådløse værktøjer fra BackTrack CD'en kan det være en fordel at indkøbe specielle netkort. Kort baseret på Atheros chipset plejer at virke fint.

Øvelse 7

Netværksinformation: ifconfig/ipconfig

Opgave:
Brug ifconfig/ipconfig til at indsamle information

Formål:
Lære at læse output fra netværkskonfiguration - specielt skal man kunne genkende netværksmasker og checke om de er sat rigtigt.

Forslag til fremgangsmåde:
Udfør kommandoen `ifconfig -a` på Unix systemerne og se information om netværkskort.

Tilsvarende udføres kommandoen `ipconfig /all` på Windows og se information om netværkskort.

Hjælp:
Hvad er forskellen på
`ifconfig -a` og `ifconfig vr0` (Linux: `ifconfig eth0`)

Diskussion:
Udover ifconfig og netstat der altid findes på Unix kan det være en fordel at installere list open files kommandoen, `lsof`. Med denne kommando kan man se hvilke programmer der benytter hvilke filer, herunder netværksforbindelser.

Bemærk: på Linux kaldes netværkskort for eth0, eth1, ... mens OpenBSD bruger interfacenavne svarende til den driver/hardware som benyttes nfe0, vr0, em0 osv. Mac OS X og AIX bruger en0, en1, ...

Vores systemer Fiona, Luffe og Biance benytter allesammen VIA Rhine kort. Soekris 4801 systemer benytter sis driver, så netkort hedder sis0, sis1 og sis2

Timon benytter Intel gigabit netkort som kaldes em0, Atheros baserede netkort til 802.11b/g kaldes typisk for ath0, ath1 osv.

AIX og Mac OS X kalder netkortene for en0, en1 - Mac OS X gør det endda for wireless kort.

Windows kalder kommandoen ifconfig for `ipconfig` eller `ipv6` hvis det er information omkring IPv6.

Forvirret? :-)

Brug altid først `ifconfig -a` evt. `ifconfig -a | more`

Øvelse 8

Netværksinformation: netstat

Opgave:
Brug netstat til at indsamle information

Formål:
Netstat er et af de primære værktøjer til at undersøge routingtabeller og det er nødvendigt at kende routing for at kunne bruge mere avancerede features som VLANs

Forslag til fremgangsmåde:
Udfør kommandoerne `netstat` på systemerne og se information om netværkskort, lyttende serverprogrammer og igangværende forbindelser.

Hjælp:
Hvad er forskellen på
`netstat -an` og `netstat -a`

Netstat har mange options, men den mest benyttede er:
`netstat -an` evt. kombineret med grep
`netstat -an | grep -i listen`

Netstat kan også vise memoryforbrug og interfacestatistik med -m og -i options.

Routingtabellen vises med `netstat -rn` evt. `netstat -rn -f inet` eller `netstat -rn -f inet6`

Diskussion:
Udover ifconfig og netstat der altid findes på Unix kan det være en fordel at installere list open files kommandoen, `lsof`. Med denne kommando kan man se hvilke programmer der benytter hvilke filer, herunder netværksforbindelser.

Øvelse 9

ping og traceroute

Opgave:
Lær at bruge ping og traceroute programmerne

Formål:
Disse programmer er vores primære diagnosticeringsprogrammer for netværk og det er obligatorisk at kende dem.

Forslag til fremgangsmåde:
Brug `ping` og `traceroute` til at teste netværksforbindelsen - kan udføres fra både windows og Unix.

Husk at traceroute hedder `tracert` på windows.

Er der forbindelse til alle servere på oversigtstegningen?

Hjælp:
ICMP er Internet Control Message Protocol det bruges typisk til at rapportere om fejl, host unreachable og lignende.

Ping programmet benytter ICMP ECHO request og forventer ICMP ECHO reply. Traceroute programmet sender ICMP eller UDP og forventer ICMP svar tilbage for at kunne mappe et netværk.

Ekstra: Hvad er forskellen på (skal udføres på OpenBSD/Unix)

- **traceroute** og **traceroute -I**
- NB: traceroute med -I findes kun på Unix - traceroute med ICMP pakker
- Der er mange der ikke blokerer for ICMP traceroute

Øvelse 10

ping6 og traceroute6

Opgave:
Lær at bruge ping og traceroute programmerne - men med IPv6

Formål:
Disse programmer er vores primære diagnosticeringsprogrammer for netværk og det er obligatorisk at kende dem.

Forslag til fremgangsmåde:
Brug `ping6` og `traceroute6` til at teste netværksforbindelsen - kan udføres fra både windows og Unix.

Husk at traceroute hedder `tracert6` på windows.

Er der forbindelse til alle servere på oversigtstegningen?

Hjælp:
ICMP er Internet Control Message Protocol det bruges typisk til at rapportere om fejl, host unreachable og lignende. IPv6 har tilsvarende ICMPv6 med samme funktioner - men har overtaget ARP funktionen.

Ping programmet benytter ICMP ECHO request og forventer ICMP ECHO reply. Traceroute programmet sender ICMP eller UDP og forventer ICMP svar tilbage for at kunne mappe et netværk.

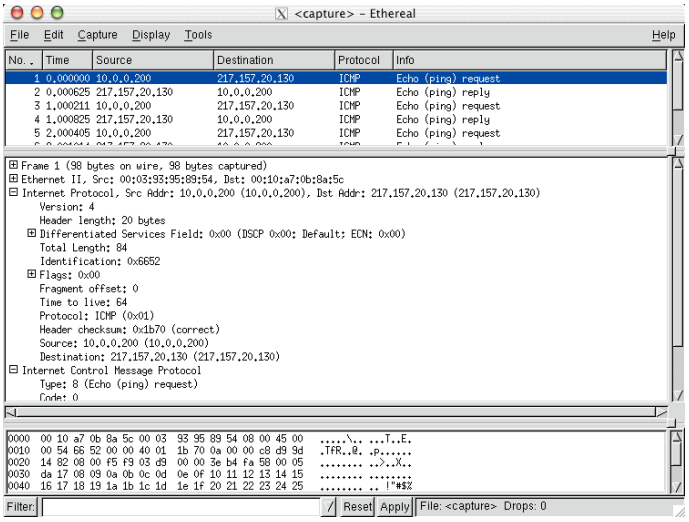
Ekstra: Hvad er forskellen på (skal udføres på OpenBSD/Unix)

- **traceroute** og **traceroute -I**
- NB: traceroute med -I findes kun på Unix - traceroute med ICMP pakker
- Der er mange der ikke blokerer for ICMP traceroute

Det er ikke altid at IPv4 og IPv6 routes går gennem de samme routere! Det er med vilje lavet simpelt i vores setup.

Øvelse 11

Wireshark netværksniffer



Opgave:
Prøv en Wireshark sniffer på din maskine!

Brug lidt tid på at lære den at kende.

Formål:
Lære at bruge en sniffer til enkle undersøgelser, så man senere kan lære mere om netværk.

Forslag til fremgangsmåde:
Find Wireshark og installer denne, hent fra den lokale webserver eller http://www.wireshark.org

Hjælp:
Find ud af hvordan det er understøttet i dit favorit operativsystem ved at bruge eksempelvis http://www.google.com

Forslag til løsning:
Windows - hvis du er på Windows skal der installeres WinPCAP - packet capture - biblioteket. Dette bibliotek følger med Wireshark i installationsfilen.

Unix - de fleste Unix varianter har installationspakker til Wireshark og TCPdump

Prøv efter installationen at kigge på den normale trafik på nettet, eller generer selv trafik med ping og traceroute (windows: tracert) programmer - når dette er gjort virker snifferen

Diskussion:
Kender du forskel på ICMP, TCP og UDP?

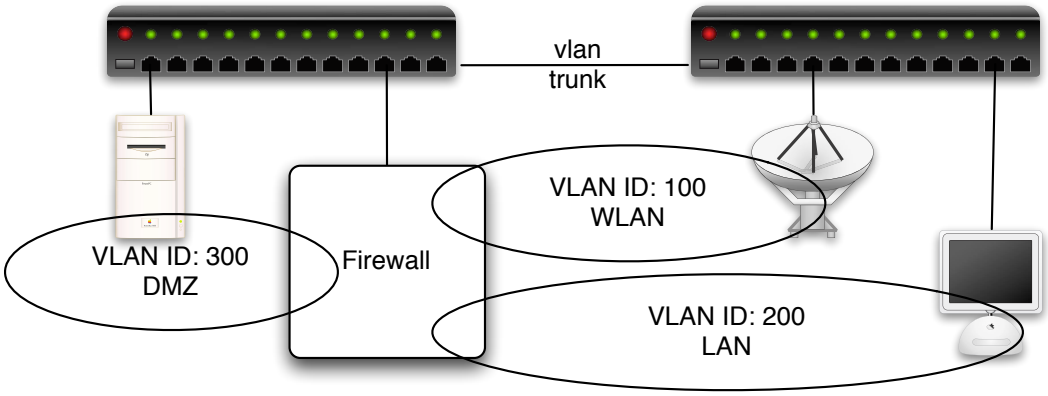
Hvilke protokoller bruger kryptering?

Husk også at sniffe en TCP session og sammensæt alle pakkerne med TCP Follow Stream funktionaliteten.

Wireshark er en efterfølger til Ethereal, navneskiftet skyldes et jobskifte hvor ejeren af Ethereal domænet ikke ville give det med programmøren.

Øvelse 12

VLAN 802.1q



Opgave:
Se VLAN konfiguration i webinterface

Formål:
Se et par eksempler på hvordan 802.1q kan være implementeret. Der er stor forskel på brugervenligheden.

Forslag til fremgangsmåde:
Login på de tilgængelige enheder som har 802.1q

Der er følgende enheder:

- Managed switch
- OpenBSD, hvis man kender OpenBSD i forvejen - se man `hostname.if` ;-)

NB: ikke alle enheder tillader flere samtidige logins, specielt firmware i små enheder gør ikke

Hjælp:
Mange moderne managed switche har mulighed for VLAN efter 802.1q standarden.

Diskussion:
Er det for besværligt?

Husk at hvis man opdeler i VLAN kan maskinerne ikke se hinanden, og der skal routes ligesom hvis det var fysiske interfaces!

Øvelse 13

DNS og navneopslag

Opgave:
Prøv forskellige programmer til at spørge en service

Formål:
Lære om DNS records og hvordan man kan slå dem op programmatisk

Forslag til fremgangsmåde:

- nslookup - findes både på Unix og Windows
- Prøv nslookup -q=txt -class=CHAOS version.bind. 0
- dig - syntaks @server domain query-type query-class
- host - syntaks host [-l] [-v] [-w] [-r] [-d] [-t querytype] [-a] host [server]
- prøv **host -a security6.net**
  host -a www.security6.net - hvad er forskellen

Hjælp:
Host programmet er med som standard på OpenBSD - så brug Fiona eller Luffe

På Unix Boot CD og MS Windows platformen findes mange GUI programmer til det samme.

Diskussion:
Hvad er en zonetransfer? det er alle de records der er defineret for et domæne

Hvad er forward og reverse lookup? forward er fra hostnavn til IP adresse, mens reverse er fra IP adresse til hostnavn

Øvelse 14

DNS og navneopslag - IPv6

Opgave:
Prøv host programmet til at spørge efter Quad-A (AAAA) records.

Formål:
Lære om IPv6 specifikke DNS records og hvordan man kan slå dem op programmatisk

Forslag til fremgangsmåde:

- host - syntaks host [-l] [-v] [-w] [-r] [-d] [-t querytype] [-a] host [server]
- prøv **host -t A security6.net**
  host -t AAAA security6.net - hvad er forskellen

Hjælp:
Host programmet er med som standard på OpenBSD - så brug Fiona eller Luffe

På Unix Boot CD og MS Windows platformen findes mange GUI programmer til det samme.

Diskussion:
DNS har mange recordtyper og AAAA er blot endnu en. Typisk vil programmer der har IPv6 funktionalitet forsøge at slå både AAAA records og A records op - og forsøge at forbinde til AAAA først.

Øvelse 15

Opslag i whois databaser

Opgave:
Lær at bruge whois

Formål:
Lære whois at kende - eksempelvis kunne slå abuse adresser op

Forslag til fremgangsmåde:

- Login på UNIX server - læs manualen til programmet whois eller brug webinterface på http://www.ripe.net

Hjælp:
Whois databaserne er fordelt på ARIN, RIPE, LACNIC og APNIC.

Kommandoen `whois -r 90.184.69.97` vil på en OpenBSD give svaret på et opslag i RIPE databasen efter IP adresse 90.184.69.97

Diskussion:
I skal lære at spørge efter IP adresser og spore oprindelsen - find eksempelvis brugeren af IP-adressen 217.157.20.129

Øvelse 16

Ekstraopgave: ICMP tool icmpush

Opgave:
Lær at bruge icmpush programmet

Formål:
Se et eksempel på et kommandolinieværktøj der kan sende valgfrie data til netværket - uden programmering

Forslag til fremgangsmåde:
Login på Unix server - læs manualen til programmet

Hjælp:
ICMP er Internet Control Message Protocol det bruges typisk til at rapportere om fejl, host unreachable og lignende.

Ping programmet benytter ICMP ECHO request og forventer ICMP ECHO reply. Traceroute programmet sender ICMP eller UDP og forventer ICMP svar tilbage for at kunne mappe et netværk.

Diskussion:
I skal lære at spørge efter mindst echo, time og netmask med icmpush

Øvelse 17

Netværksinformation: sysctl

Opgave:
Brug sysctl kommandoen til at indsamle information

Formål:
Se eksempler på parametre der kan tunes på en TCP/IP implementation

Forslag til fremgangsmåde:
Udfør kommandoen `sysctl -a | grep net` på systemerne og se information om IP-stakken på systemet.

Hjælp:

Sysctl giver adgang til mange informationer:
`net.inet.ip.forwarding`
`net.inet6.ip6.forwarding`

Netstat kan også vise memoryforbrug og interfacestatistik med -m og -i options.

Diskussion:
Udover ifconfig og netstat der altid findes på Unix kan det være en fordel at installere list open files kommandoen, `lsof`. Med denne kommando kan man se hvilke programmer der benytter hvilke filer, herunder netværksforbindelser.

Øvelse 18

Performance tool - iperf

Opgave:
Lær at bruge iperf programmet

Formål:
Få et indblik i hvordan man med enkle testprogrammer kan få målbare data fra netværksperformance

Forslag til fremgangsmåde:
Login på Unix server start en iperf server og tilsvarende start en iperf client på en anden maskine i netværket.

Brug eksempelvis fiona som client og bianca som server.

Hjælp:
Iperf er et lille nemt program som blot skal startes som server på en maskine og derefter kaldes som klient på et andet. Så måler den som default et kort stykke tid og præsenterer resultatet.

Diskussion:
Til rigtige performancemålinger er det uhensigtsmæssigt at netværket benyttes til anden traffik under målingerne, medmindre man ønsker at måle nu og her.

Øvelse 19

Afprøv Apache Benchmark programmet

Opgave:
Afprøv ApacheBench programmet

Formål:
Få et indblik i hvordan man med enkle testprogrammer kan få målbare data fra webservere

Forslag til fremgangsmåde:
Prøv at køre med 100 eller 1000 forespørgsler på en fil/url

Hjælp:
Prøv `ab -n 100 http://www.pentest.dk/`

Diskussion:
Hvornår vil det være relevant at bruge ApacheBench?

Øvelse 20

SNMP walk

Opgave:
Log ind på et OpenBSD Unix system og se på `snmpwalk`

Formål:
Se eksempel på data fra netværksenheder

Forslag til fremgangsmåde:
SNMP walk betyder at man går igennem alle SNMP oplysningerne fra et system.

Hjælp:
```
snmpwalk -v 2c -c public 10.0.45.2
```

Public er default på meget udstyr og findes stadig mange steder i produktion.

Private er et andet kendt community name og gav tidligere lov til at ændre indstillingerne på enheder.

Diskussion:

Øvelse 21

Logning med syslogd og syslog.conf

Opgave:
log ind på et OpenBSD Unix system og se på `syslog.conf`

Formål:
Se mulighederne for at samle eller sortere logbeskeder med en standardfunktionalitet

Forslag til fremgangsmåde:

- Hvor ligger den? - i hvilket katalog?
- Hvordan kan man sende loggen videre til en anden maskine?
- Hvilken protocol og port bruger syslog - hvis I skal tillade det gennem en firewall?

Hjælp:
Indholdet af filen kan ses nedenfor:

```
*.err;kern.debug;auth.notice;authpriv.none;mail.crit    /dev/console
*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none /var/log/messages
kern.debug;user.info;syslog.info                        /var/log/messages
auth.info                                               /var/log/authlog
authpriv.debug                                          /var/log/secure
...
# Uncomment to log to a central host named "loghost".
#*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none        @loghost
#kern.debug,user.info,syslog.info                               @loghost
#auth.info,authpriv.debug,daemon.info                           @loghost
```

Diskussion:
Se også http://www.loganalysis.org/

Syslog er standard logging format/protokol for netværksenheder, ikke bare Unix

Øvelse 22

BIND version

Opgave:
Find version på BIND software på Unix

Formål:
Se et eksempel på et lille script

Forslag til fremgangsmåde:
Brug en af følgende kommandoer til at finde version på BIND på navneserveren:

```
nslookup -q=txt -class=CHAOS version.bind. 0 server

dig @server version.bind chaos txt
```

Hjælp:

Diskussion:
BIND softwaren er ofte udsat for angreb

BIND og navnesystemet er kritisk for mange funktioner som web og mail

Et mere komplet script kunne være:

```
#! /bin/sh
# Try to get version info from BIND server, several ways to do this:
# nslookup -q=txt -class=CHAOS version.bind. 0
# dig @$* version.bind chaos txt

PROGRAM=`basename $0`
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
dig @$1 hostname.bind chaos txt
dig @$1 ID.SERVER chaos txt
dig @$1 version.bind chaos txt
echo Authors BIND er i versionerne 9.1 og 9.2 - m<E5>ske ...
dig @$1 authors.bind chaos txt
```


Øvelse 23

AirPort Extreme

Opgave:
Konfiguration af Apple AirPort Extreme

Formål:
Prøve et administrativt interface til et access point, sekundært se de mange muligheder som repræsenterer avancerede netværksenheder

Forslag til fremgangsmåde:
Hent AirPort konfigurationsprogrammet til Windows og brug denne til at konfigurere Apple AirPort

Hjælp:
Manualen til udstyret forefindes i PDF format

Forslag til løsning:
Sæt det trådløse udstyr i et isoleret netværk når det skal konfigureres

Diskussion:
Hvad er de mange Ethernet stik til?

Sørg for at undersøge alle mulighederne i konfigurationen

Prøv evt. også at se på Linksys udstyret WAP54 og WRV-200

Øvelse 24

Wardriving på Windows - inSSIDer

Opgave:
Installer inSSIDer på en Windows laptop - og lav wardriving

Kræver I har et netkort der er understøttet

Formål:
Se hvor nemt det er at wardrive

Forslag til fremgangsmåde:
Med inSSIDer(windows), Kismet(unix) og andre kan man scanne efter trådløse netværk med almindeligt trådløst udstyr

Hjælp:

Forslag til løsning:
Hent programmet fra internet eller fra den lokale webserver http://www.metageek.net/products/inssider

Diskussion:
Er det lovligt?

Hvorfor er der så mange åbne netværk?

Øvelse 25

Wardriving på Unix - Kismet

Opgave:
Afprøv Kismet laptoppen - og lav wardriving

Kræver I har et netkort der er understøttet af Boot CD/Linux

Formål:
Se hvor nemt det er at wardrive

Forslag til fremgangsmåde:
I skal blot se hvorledes wardriving tager sig ud på Unix - kende programmerne

Hjælp:

Forslag til løsning:
I skal være velkomne til at undersøge hvordan Kismet installeres

Diskussion:
Der findes "stumbler" programmer til de mest benyttede platforme, men hvilke kort understøttes!

Det kan ofte være en god ide at undersøge om det kort man vil købe kan bruges til at wardrive - idet wardriving er vigtigt internt i virksomhederne for at finde uautoriserede (engelsk: rogue) access points.

Øvelse 26

Ekstraopgave: Airodump-ng lavniveau sniffer

Opgave:
Afprøv airodump-ng hvis I har lyst og har et netkort

Kræver I har et netkort der er understøttet af Boot CD/Linux

Formål:
Se hvor nemt det er at sniffe på trådløse netværk, hvis man har det rigtige værktøj

Forslag til fremgangsmåde:
Start kortet i monitormode med `airmon-ng start` derefter `airodump-ng kort` eksempelvis `airmon-ng start ath0` og `airodump-ng ath1`

Hjælp:

Forslag til løsning:

Diskussion:
Der findes en masse howto dokumenter og vejledninger, se http://www.aircrack-ng

Øvelse 27

RADIUS client

Opgave:

Formål:
Prøve at bruge et RADIUS testprogram fra Fiona serveren - den har både RADIUS server og client

Forslag til fremgangsmåde:
Undersøg med vores systemer og kommandoen radclient. Der er defineret en enkelt "user"i `/etc/raddb/users` med teksten:

```
"kursus1"       Cleartext-Password := "kursus"
                Reply-Message = "Hello, %User-Name"
```

Dette bør ved brug af kommandoerne nedenfor give resultat.

```
echo "User-Name = kursus1" | radclient 127.0.0.1:1812 auth testing123
```

```
echo "User-Name=kursus1,Cleartext-Password=kursus " | radclient 127.0.0.1:1812 auth testing123
```

Output skulle ligne:

```
Received response ID 102, code 3, length = 36
        Reply-Message = "Hello, kursus1"
```

Hjælp:
Husk secret vores er testing123 som er default mange steder! (bør selvfølgelig ændres)

Se også: http://wiki.freeradius.org/Radclient

Diskussion:
RADIUS er OK - men mange loginmetoder og protokoller er ikke!

RADIUS sikrer at man kan snakke sammen, men hvis man bruger cleartext passwords giver det naturligvis ringe sikkerhed.

Et godt råd er at sikre:

- Hvem må tale med RADIUS serveren, IP-adresser
- Hvem kender hemmeligheden, secret
- Brug TLS/SSL osv.
- Lad være med at bruge PAP med cleartext password, lad være med at bruge PPTP osv.

Øvelse 28

LDAP client

Opgave:
Brug et LDAP klientprogram til at slå op i LDAP

Formål:
Prøve at bruge et LDAP testprogram

Forslag til fremgangsmåde:
Undersøg med `ldapsearch` vores systemer.

```
ldapsearch -h 10.0.45.12 -x -b 'dc=darky,dc=kramse,dc=dk' '(uid=root)'

ldapsearch -h 10.0.45.12 -x -b 'dc=darky,dc=kramse,dc=dk' '(uid=*)'
```

(husk den rigtige IP-adresse på serveren)

Hjælp:
I kan også prøve JXplorer som er et JAVA GUI program til LDAP

Det skal udfyldes med følgende oplysninger: Host: 10.0.45.12 Port: 389
Protocol LDAP v3
BaseDN: dc=darky,dc=kramse,dc=dk
User DN: uid=diradmin,cn=users,dc=darky,dc=kramse,dc=dk
Password: henrik42

http://www.jxplorer.org/

Diskussion:
Hvad er bind?

Hvad med LDAP kan det bruge SSL?

Øvelse 29

Ekstraopgave: Firewallkonfiguration

Opgave:
Konfiguration af en firewall - se eksempler, fællesopgave

Formål:
Lær at genkende forskellige regelsæt og firewallimplementationer

Forslag til fremgangsmåde:

- Hvordan enabler man firewall?
- Hvordan åbner man for noget i vores firewall?
- Tilføj en regel for at tillade adgang til noget mere på vores systemer

På OpenBSD kan man se om firewall er enablet med kommandoen `pfctl`. Prøv følgende kommandoer på eksempelvis Luffe

- `sudo pfctl -s all | more`
- `sudo pfctl -s rules | more`
- `sudo pfctl -s nat | more`
- `sudo pfctl -s states | more`
- `sudo pfctl -s info | more`
  ...

Hjælp:
Vi gennemgår sammen ændringen på de forskellige firewalls vi har til rådighed!

Diskussion:
Sørg for at Henrik viser flere firewalls!

Der er GUI på Mac OS X, Windows, Linux og også til OpenBSD PF pfw

Øvelse 30

Ekstraopgave: Find maskiner

Opgave:
Log på Unix og brug nmap til at søge efter maskiner på lokalnetværket som ping sweep eller port sweep

Formål:
Afprøv portscanning så I senere kan finde maskiner og services

Forslag til fremgangsmåde:
Lav forskellige typer scan og inddel resultaterne efter:

- aktive systemer
- åbne porte/services

Hjælp:
Prøv med Nmap sweep:

```
nmap -sP 10.0.45.*
nmap -p 80 10.0.45.*
```

Prøv også gerne de andre netværk, .46 .53 osv.

Diskussion: Er det noget som foregår på Internet? Ja, konstant

Øvelse 31

Ekstraopgave: nmap portscanning

Opgave:
Brug nmap til at finde åbne porte på netværket

Formål:
Afprøv portscanning så I senere kan teste maskiner og services

Forslag til fremgangsmåde:
Brug `nmap -p 1-1024 server` til at scanne de første 1024 TCP porte på en server Brug `nmap -sU` til at scanne efter UDP porte og `-P0` option til at undgå at sende ping først

Hjælp:
Eksempel: `nmap -P0 -sU -p1-1024 server` UDP portscanning af port 1-1024 uden ping først

Diskussion:
TCP og UDP portscanning er meget forskelligt. TCP er forbindelsesorienteret og har session setup i form af en three-way handshake som gør at en client først sender TCP-SYN, server svarer med TCP-SYN+ACK og derefter etableres forbindelsen endeligt med TCP-ACK fra klienten. UDP er forbindelsesløs kommunikation og der er ingen session setup - derfor er UDP scanning mere upålideligt.

Bilag A

Hostoplysninger

- I bedes registrere IP-adresserne for maskinerne
- Filer til installation - installationsprogrammer:
  http:// . . . /public/windows/ - webserver med diverse tools
- IP: . . . - Fiona
- Fiona maskinen benyttes med SSH
- Kursus login brugernavne: kursus1, kursus2, ... kursus10 kodeord: `kursus` - uanset brugernavn
- Skift til root med: `sudo -s`

Vores maskiner

- IP: . . . -
- IP: . . . -
- IP: . . . -
- IP: . . . - OpenBSD Fiona server
- IP: . . . - Din egen arbejdsstation - Windows/Linux

