IPv6 Security Workshop

øvelseshæfte

Henrik Lund Kramshøj

hlk@solido.net

15. marts 2012

Indhold

Forord

Dette kursusmateriale er beregnet til brug på kurset *IPv6 Security 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@solidonetworks.com, 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.

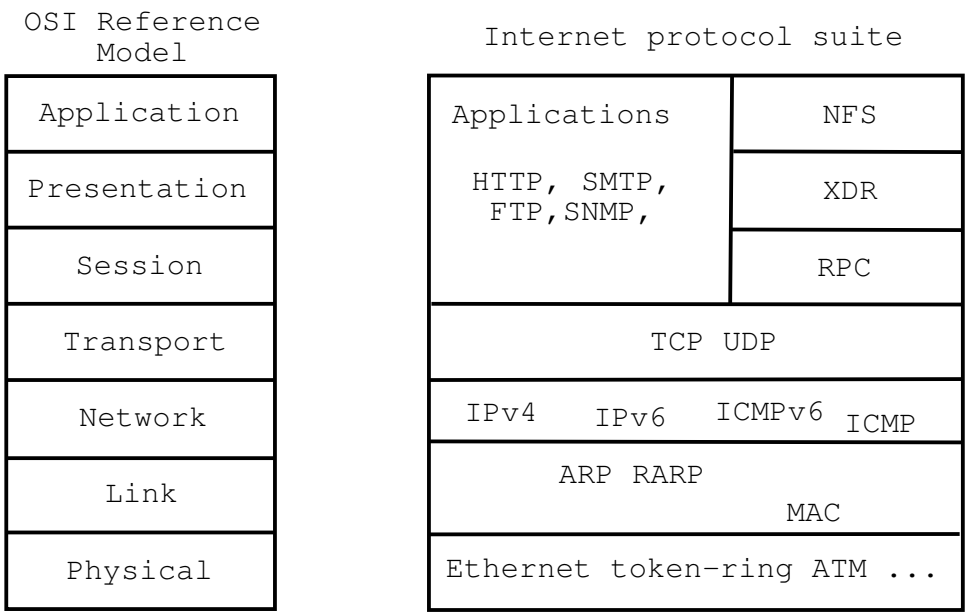
OSI reference model

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 RFC0791 altså er en standard og den erstatter RFC0760.

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.

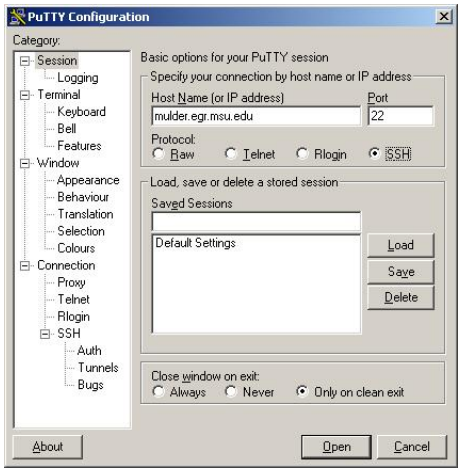
Indholdet i øvelserne

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

Hjælp:
Putty er en terminal emulator og erstatter telnet programmet i Windows. Det er ofte den foretrukne brugergrænseflade 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 kursus20 - allesammen med kodeord *kursus*.

Forslag til løsning:
Start Putty eller Boot på 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: . . . -

Øvelse 4

Netværksinformation: ifconfig/ipconfig

Opgave:
Brug ifconfig på Unix eller ipconfig på Windows 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 og Luffe 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 5

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 6

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 7

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.

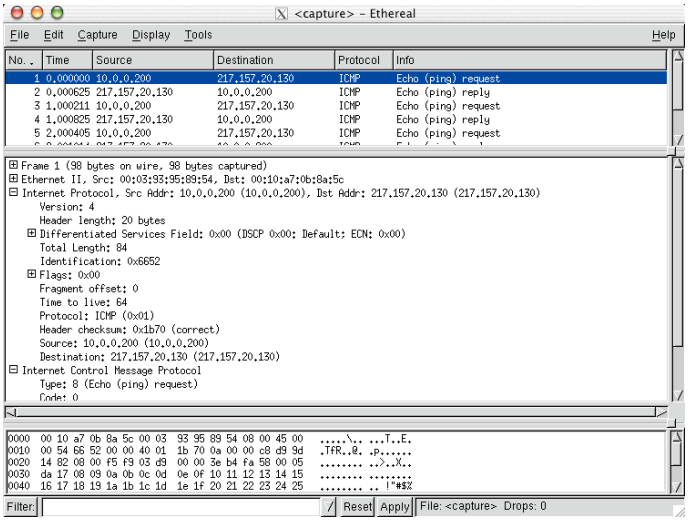
Ekstra: Hvad er forskellen på (skal udføres på OpenBSD/Unix)

- **traceroute6** og **traceroute6 -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 8

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?

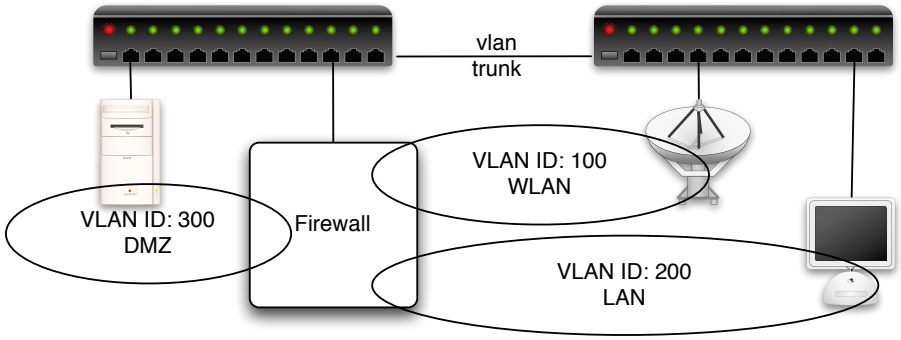
Husk også at sniffe en TCP session og sammensæt alle pakkerne med TCP Follow Stream funktionaliteten.

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

Specielt med IPv6 vil man se ICMPv6 Router Advertisement og Neighbor Discovery Protocol ICMPv6 pakker.

Øvelse 9

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:

- Dell 3448 switch
- Linksys WRV-200 switch, access point og router
- Juniper SRX210 firewall og router
- 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 10

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 11

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 12

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 13

Test din forbindelse test-ipv6.com

Opgave:
Besøg hjemmesiden http://www.test-ipv6.com

Formål:
Undersøg om din forbindelse er klar til IPv6.

Forslag til fremgangsmåde:

Hjælp:

Forslag til løsning:

Diskussion:

Øvelse 14

Test din forbindelse for DNS problemer

Opgave:
Besøg hjemmesiden http://labs.ripe.net/content/testing-your-resolver-dns-reply-size-issues og kør testprogrammet.

Formål:
Undersøg om din forbindelse er klar til DNS med større pakker.

Forslag til fremgangsmåde:

Hjælp:

Forslag til løsning:

Diskussion:

Øvelse 15

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 din PC 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.

Der findes et GUI til programmet kaldet jperf.

Øvelse 16

THC IPv6 attack toolkit

Opgave:
Hent THC-IPV6 fra hjemmesiden: http://thc.org/thc-ipv6/

Formål:
Se eksempel på angrebsværktøjer rettet specifikt mod IPv6

Forslag til fremgangsmåde:
Læs på hjemmesiden, hent seneste version, udpak programmet - prøv det evt. af på BackTrack Linux

Hjælp:

Diskussion:
Er det rimeligt at den slags frit kan downloades?

