

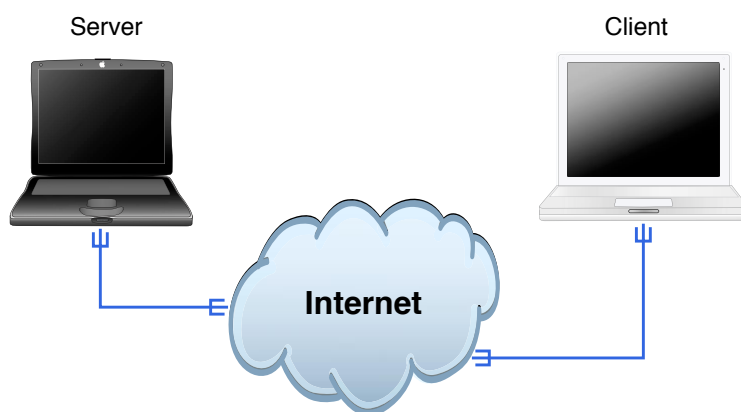
Hackerworkshop

øvelseshæfte

Henrik Lund Kramshøj

hlk@security6.net

28. september 2008



Indhold

1	Putty installation - Secure Shell login	6
2	WinSCP installation - Secure Copy	8
3	Login på UNIX systemerne	9
4	Føling med UNIX	10
5	UNIX - adgang til root	11
6	UNIX boot CD	13
7	Wireshark installation	14
8	Opsamling af trafik	16
9	ping og traceroute	17
10	ICMP tool - icmpush	18
11	Opslag i whois databaser	19
12	DNS og navneopslag	20
13	Lær at bruge host programmet	21
14	Afprøv bind-version programmet	22
15	Afprøv dns-timecheck programmet	23
16	Kig på arpspoof og dsniff	24
17	Find maskiner	25
18	Foretag nmap TCP portscanning	26
19	Foretag nmap servicescanning	27
20	Foretag nmap OS detection	28
21	Foretag mini-pentest med cd-rom	29
22	Find systemer med SNMP	30
23	Afprøv Hydra bruteforce	31
24	RPC info	32

25	Netcat til scripting	33
26	OpenSSL forbindelser	34
27	Nessus scanning	35
28	AirPort Extreme	36
29	Wardriving på Windows - netstumbler	37
30	Wardriving på UNIX - Kismet	38
31	Aircrack-ng	39
A	Hostoplysninger	40

Forord

Dette kursusmateriale er beregnet til brug på kurset *hackerworkshop workshop*. Materialet er lavet af Henrik Lund Kramshøj, <http://www.security6.net>

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 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 er ofte at give kursisdeltagerne et indblik i hvordan emnerne 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.security6.net, hlk@security6.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 kursusternes 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.

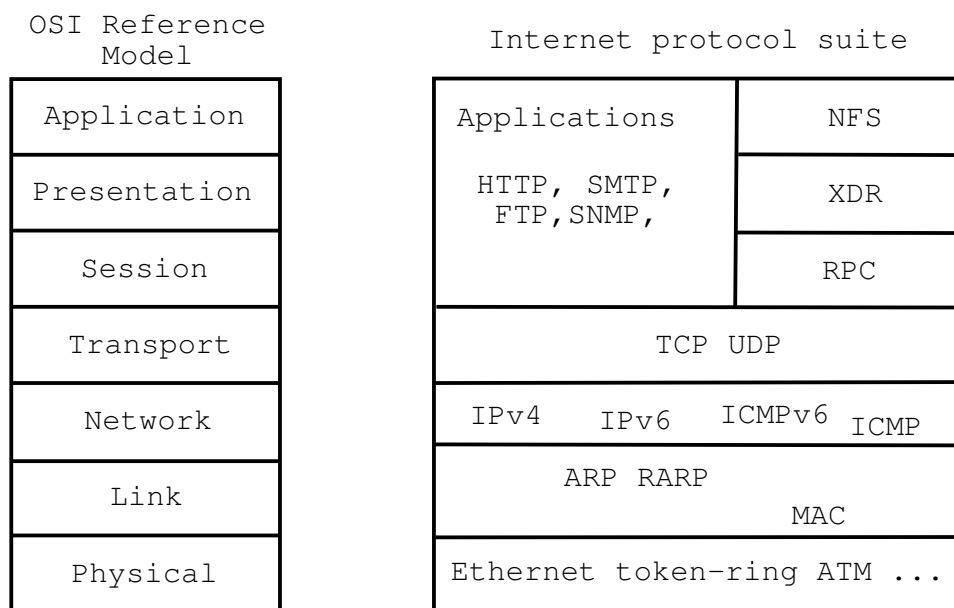
OSI reference model

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 [?] altså er en standard og den erstatter [?].

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)

Adressestruktur

Der anvendes et privat adresserum som angivet i RFC-1918

- 10.0.45.0 - svarende til en C-klasse med ca. 250 brugbare adresser

Det angivne netværk forbindes til virksomhedens gennem en NAT gateway som således maskerer at der er et netværk bagved.

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.

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, ...
- 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
- ethereal - 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.

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

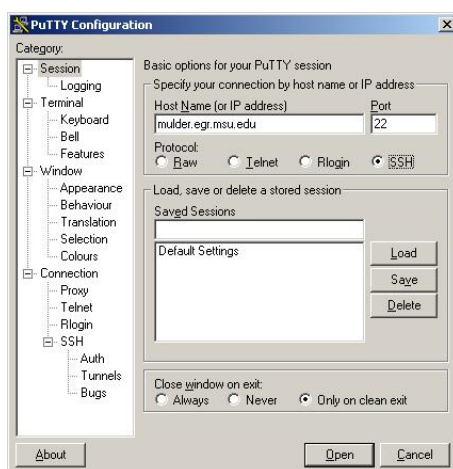
Indholdet i øvelserne

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:** er 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 jeres arbejdsstation

Øvelse:

Installer Putty lokalt på Windows maskinen

Forslag til fremgangsmåde:

Hent og installer programmet, hent fra webserveren eller

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

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.

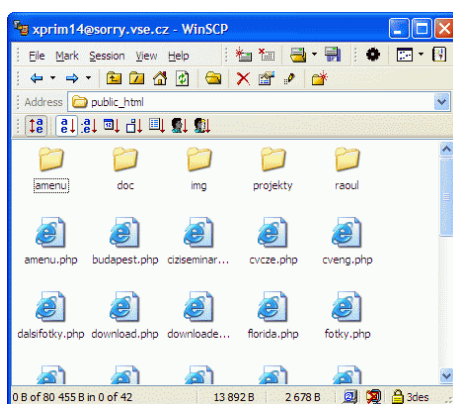
Eksempel:

```
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

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

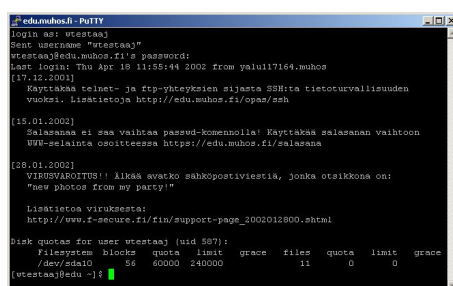
Diskussion:

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



```
eduuhos.fi - PuTTY
login as: wtestaa
Sent username "wtestaa"
wtestaa@edu.muhos.fi's password:
Last login: Thu Apr 18 11:55:44 2002 from yalul17169.muhos
[17.12.2001]
  Käyttäkää telnet- ja ftp-yhteyksien sijasta SSH:tä tietoturvallisuuden
  vuoksi. Lisätietoja http://edu.muhos.fi/opas/ssh

[15.01.2002]
  Salasanat ei saa vaihtaa passwd-komenolla! Käyttäkää salasanan vaihtoon
  WWW-selainta osoitteessa https://edu.muhos.fi/salasana

[18.01.2002]
  VIRUSVAROITUS!! Älkää avakko sähköpostiviestiä, jonka otsikkona on:
  "new photos from my party!"

  Lisätietoja viruksesta:
  http://www.f-secure.fi/fi/support-page_2002012800.shtml

Disk quotas for user wtestaa (uid 507):
   Filesystem blocks quota limit grace files quota limit grace
   /dev/sda10    56 60000 240000    11    0    0
[wtestaa@edu ~]$
```

Opgave:

Brug jeres arbejdsplads til at logge ind på serverne

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

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?

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`?

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. Manuals systemet 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 manuals systemet.

Øvelse 5

UNIX - adgang til root

Opgave:

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

Forslag til fremgangsmåde:

Brug manualsiderne til at besvare følgende spørgsmål:

- Hvad er forskellen på `su -` og `sudo -s`?
- Kan `su` konfigureres 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

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 er:

- Knoppix som er beregnet til almindeligt arbejde, surfing på net, Open Office skrivearbejde, E-mail med videre
- Auditor Security Collection, nu BackTrack - en større samling af sikkerhedsværktøjer til penetrationstest
- Damn Vulnerable Linux, en usikker Linux distribution, hvor man kan lære om sikkerhedsproblemer i software

Diskussion:

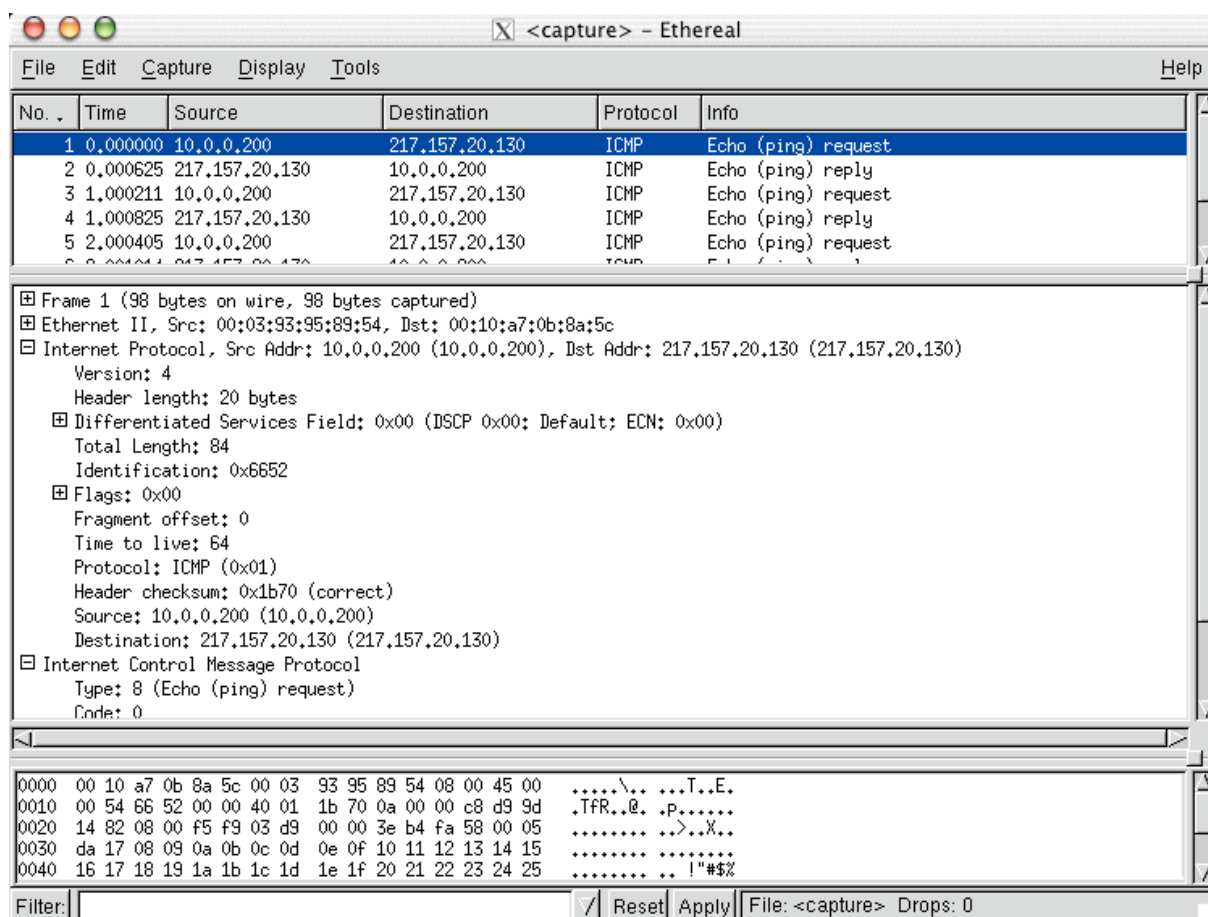
Til mange af CD'erne er der nogle boot koder som indimellem er nødvendige - typisk for at vælge opløsning for det grafiske miljø. Hvis CD'en ikke virker i en bestemt maskine kan det være nødvendigt at prøve i en mere standard maskine.

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

Wireshark installation



Opgave:

Installer Wireshark lokalt på Windows maskinen

Forslag til fremgangsmåde:

hent Wireshark programmet fra webserveren eller <http://www.wireshark.org>

WinPcap kan hentes alene fra <http://www.winpcap.org/>

NB: idag indeholder Wireshark installprogrammet til WinPcap

Hjælp:

PCAP er et packet capture bibliotek som er nødvendigt for at lytte i promiscuous mode

Diskussion:

Wireshark er blot et af mange programmer til analyse af netværkstrafik

Øvelse 8

Opsamling af trafik

Opgave:

Lær at kigge på netværkstrafik - opsnap ICMP echo pakker, fra ping programmet

Forslag til fremgangsmåde:

start pakkesniffer

brug menuen Capture - Start, sæt evt. filter på her og start så ping af default gateway. Undersøg derefter pakkerne

Hjælp:

De forskellige vinduer indeholder oversigt over pakkerne, pakken der er valgt - hvor der kan peges på header information, dekoder pakkerne

Den nederste del indeholder pakkens data i rå format hexadecimalt og som ascii tekst

Diskussion:

Øvelse 9

ping og traceroute

Opgave:

Lær at bruge ping og traceroute programmerne

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

ICMP tool - icmpush

Opgave:

Lær at bruge icmpush programmet

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 11

Opslag i whois databaser

Opgave:

Lær at bruge whois

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 12

DNS og navneopslag

Opgave:

Prøv forskellige programmer til at spørge en service

Forslag til fremgangsmåde:

- nslookup - findes både på UNIX og Windows
- Prøv nslookup -q=txt -class=CHAOS version.bind. 0
- Prøv kommandoen dig: **dig @n1.gratisdns.dk www.kramse.dk A**
- prøv kommandoen: **host -a security6.net**
host -a www.security6.net - hvad er forskellen
- host - syntaks host [-l] [-v] [-w] [-r] [-d] [-t querytype] [-a] host [server]

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 13

Lær at bruge host programmet

Opgave:

Brug host programmet til at finde den autoritative navneserver for et domæne

Forslag til fremgangsmåde:

Login på UNIX server - kørs programmet med en DNS server som I kender eller den autoritative for security6.net domænet

Hjælp:

```
$ host -t ns security6.net
security6.net name server ns1.security6.net.
security6.net name server ns6.gandi.net.
$ host -t ns security6.net 217.157.20.131
...
```

Diskussion:

Øvelse 14

Afprøv bind-version programmet

Opgave:

Lær at bruge et shell script på UNIX

Hint: #! i starten angiver at det er program og med x-bitten sat virker scripts som alle andre programmer

Forslag til fremgangsmåde:

Login på UNIX server - kørs programmet med en DNS server som I kender eller den autoritative for security6.net domænet

Hjælp:

UNIX shell scripting findes i flere varianter. O'Reilly bogen *Classic shellscripting* anbefales

Diskussion:

Øvelse 15

Afprøv dns-timecheck programmet

Opgave:

Lær at bruge et Perl program

Hint: #! i starten angiver at det er program og med x-bitten sat virker scripts som alle andre programmer

Forslag til fremgangsmåde:

Login på UNIX server - kørs programmet med en DNS server som I kender eller den autoritative for .se TLD

Hjælp:

Perl kan være svært at gå til - der findes dog gode tutorials og O'Reilly bøgerne kan varmt anbefales

Diskussion:

Hvad er fordele og ulemper ved Perl programmet i forhold til shell-scriptet

Øvelse 16

Kig på arpspoof og dsniff

Opgave:

Læs om arpspoof og dsniff - prøv dem gerne

Forslag til fremgangsmåde:

Log på UNIX systemet - skriv **man arpspoof** og **man dsniff**

Hjælp:

Hvad kræver programmerne som input?

ARP spoof lyver om relationen mellem hardware adresser og IP adresser til de systemer der skal overvåges. Dsniff afkoder trafikken som er dirigeret til systemet.

Diskussion:

Hvilke muligheder er der med disse programmer?

Bemærk at det kan genere netværket hvis man stopper sin arpspoofing uden at fortælle de andre maskiner den rigtige MAC adresse!

Øvelse 17

Find maskiner

Opgave:

Log på UNIX og brug nmap til at søge efter maskiner på lokalnetværket

Forslag til fremgangsmåde:

Lav forskellige typer scan og inddel resultaterne efter:

- aktive systemer
- åbne porte/services

Hjælp:

Prøv med Nmap port sweep

Diskussion: Er det noget som foregår på Internet?

Øvelse 18

Foretag nmap TCP portscanning

Opgave:

Brug nmap til at finde åbne porte på netværket

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.

Øvelse 19

Foretag nmap servicescanning

Opgave:

Brug nmap service detection til at finde ud af hvilke services der gemmes sig bagved de åbne porte på netværket

Forslag til fremgangsmåde:

Brug `nmap -A` option til at slå service detection til

Hjælp:

Kig på manual siden til nmap

Diskussion:

Hvordan finder man ud af hvilken protokol der ligger bagved en port?

Øvelse 20

Foretag nmap OS detection

Opgave:

Brug nmap OS detection til at finde operativsystemerne på netværket

Forslag til fremgangsmåde:

Find listen med aktive systemer fra tidligere (eller lav sweeps) kig på manualsiderne **man nmap** udfør OS detection på de fundne maskiner

Hjælp:

Brug `nmap -O` option til at slå OS detection til

Nmap portscanneren kan sende specielle pakker og dermed udlede hvilket operativsystem der gemmer sig - udfra de svar der kommer retur

Diskussion:

Nmap OS detection er ikke altid lige præcis - det hjælper hvis der angives både en åben og en lukket port - hvorfor? og **man xprobe**

Øvelse 21

Foretag mini-pentest med cd-rom

Opgave:

Brug den udleverede cd-rom til at foretage en mini-pentest med portscanning fra et tilfældigt system

Forslag til fremgangsmåde:

boot cd-rom, indlæs driver til netkortet, start DHCP klient, foretag portscanning med nmap

Hjælp:

Mange bootbare cd-rom distributioner er baseret på Linux og der kan indlæses moduler til kernen - og dermed er de fleste hardware enheder på almindelige pc-systemer dækket ind.

Diskussion:

Cd-rom kan også bruges til computer forensics - hvis man står med en kompromitteret server.

Øvelse 22

Find systemer med SNMP

Opgave:

Find SNMP systemer

Forslag til fremgangsmåde:

Log på UNIX og brug nmap til at finde systemer med SNMP - kan være svært ... det er UDP 161

Hjælp:

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

- Prøv først **snmpwalk -v 2c -c public 10.0.43.12**
bør give en masse information om den pågældende netværksenhed

Diskussion:

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

Øvelse 23

Afprøv Hydra bruteforce

Opgave:

Afprøv bruteforceprogrammet hydra/Xhydra

Forslag til fremgangsmåde:

Log på UNIX server eller brug CD'en

Lav en kort liste med passwords og brug hydra til at bruteforce systemer

Hjælp:

Prøv først almindeligt login - så I kan forvisse jer om at servicen findes og et login virker

lav derefter en liste med passwords der indeholder det rigtige

Diskussion:

Der er mange options, men hydra er ikke så slem endda - den grafiske brugergrænseflade hjælper også

Øvelse 24

RPC info

Opgave:

Find RPC services på UNIX

Forslag til fremgangsmåde:

```
rpcinfo -p 10.0.43.11
```

Hjælp:

RPC info programmet kontakter portmapper programmet på den pågældende server og får en liste over de tilgængelige services

Diskussion:

Bør denne funktion være tilgængelig på produktionsudstyr?

Hvad er ulempen ved services der ikke ligger på faste porte? (hint: tænk firewalls)

Prøv det tilsvarende nbtstat mod Windows maskiner

Øvelse 25

Netcat til scripting

Opgave:

Lær at bruge netcat til scripting: `./head.sh www.pentest.dk 80`

Forslag til fremgangsmåde:

Login på UNIX server - læs manualen til nc programmet. Lav dernæst et program head.sh:

```
#!/bin/sh
# get HEAD from Webserver
cat | nc $1 $2 << EOF
HEAD / HTTP/1.0

EOF
```

Hjælp:

Netcat programmet sender vilkårlige data videre ud på nettet.

Øvelse 26

OpenSSL forbindelser

Opgave: Lær at bruge openssl til scripting af forbindelser til SSL/TLS

Forslag til fremgangsmåde:

Login på UNIX server - læs manualen til openssl programmet - se især på `s_client` delen. Lav dernæst et program `headssl.sh` med følgende indhold:

```
#!/bin/sh
# get HEAD from Webserver SSL port
openssl s_client -host $1 -port $2 << EOF
HEAD / HTTP/1.0

EOF
```

Udfør programmet med: `./headssl.sh server 443`

Hjælp: Openssl programmet kan fungere som en wrapper til forbindelser til webservere og andre protokoller som benytter SSL/TLS

Diskussion:

Secure Sockets Layer SSL er idag blevet adopteret af IETF og kaldes derfor også for Transport Layer Security TLS - se RFC-2246. TLS er baseret på SSL Version 3.0

Øvelse 27

Nessus scanning

Opgave:

Brug Nessus til at lave en test af lokalnettet

Forslag til fremgangsmåde:

Start en Nessus klient og start en scanning ved brug af UNIX serveren - som har en Nessus server installeret

Hjælp:

Der findes en Windows klient til Nessus - men serveren afvikles altid på UNIX

Diskussion:

Nessus servere kan installeres bredt i et større netværk og kan derved understøtte distribueret scanning.

Øvelse 28

AirPort Extreme

Opgave:

Konfiguration af Apple AirPort Extreme

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 to LAN stik til? - begge er jo Ethernet?

Sørg for at undersøge alle mulighederne i konfigurationen

Øvelse 29

Wardriving på Windows - netstumbler

Opgave:

Installer netstumbler på en Windows laptop - og lav wardriving

Kræver I har et netkort der er understøttet

Forslag til fremgangsmåde:

Med netstumbler(windows), Kismet(unix) og iStumbler kan man scanne efter trådløse netværk med almindeligt trådløst udstyr

Hjælp:

Forslag til løsning:

Diskussion:

Er det lovligt?

Hvorfor er der så mange åbne netværk?

Øvelse 30

Wardriving på UNIX - Kismet

Opgave:

Afprøv Kismet laptoppen - og lav wardriving

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

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 31

Aircrack-ng

Opgave:

Afprøv Aircrack-ng til at knække kryptering

Forudsætter I har et netkort der er understøttet af Boot CD/Linux som kan gå i monitor-mode

Forslag til fremgangsmåde:

I skal blot se hvorledes aircrack tager sig ud på UNIX - kende programmerne

Hjælp:

Forslag til løsning:

I skal være velkomne til at undersøge hvordan aircrack-ng installeres, men ellers afvikles det fra Boot CD'en

Diskussion:

Der findes "stumbler" programmer til de mest benyttede platforme, som inkluderer samme funktionalitet som aircrack.

Der findes en masse hjælpe på hjemmesiden for aircrack-ng:

<http://www.aircrack-ng.org/>

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 til **port 22781!**
- Kursus login brugernavne: kursus1, kursus2, ... kursus10 kodeord: `kursus` - uanset brugernavn
- Skift til root med: `sudo -s`

Vores maskiner

- IP: . . . -
- IP: . . . -
- IP: . . . - OpenBSD
- IP: . . . - OpenBSD scanserver
- IP: . . . - Din egen arbejdsstation - Windows/Linux