Laboration 2: Wireshark och omsändning

Introduktion

I Laboration 1 introducerades protokollanalysatorn Wireshark. I denna laboration utnyttjas Wireshark för att illustrera och exemplifiera fler fenomen och finesser i de olika lagren i TCP/IP-modellen.

Ethernet

Starta Wireshark och filtrera bort edp-protokollet.

Uppgift 1

Gör en infångning (Capture) av några hundra ramar. Skriv upp några source- och destination-adresser i Ethernetramarna. Är någon av dem din dators Ethernet-adress?

I Wireshark kan man bekvämt ta reda på tillverkaren av den utrustning som sänder eller tar emot nätverkstrafik. Genom att titta på de tre första av de sex bytes som utgör Ethernet-adressen för en enhet får man reda på detta. Denna översättning är redan gjord i Wireshark. T.ex. kan ett visst nätverkskort ha Ethernet-adressen

00:80:c8:7e:53:22

men i Wireshark visas denna Ethernet-adress även som

D-Link_7e:53:22

Översättningen är gjord genom att slå upp 00:80:c8 i en tabell över alla "vendor codes" (tillverkarkoder) som finns för Ethernet-adresser. Om man inte kör Wireshark men ändå vill ha reda på tillverkaren för en viss enhet kan man lätt hitta detta genom att söka just på "ethernet vendor codes". Detta kan vara bra om man inte känner igen viss trafik på ett nätverk och vill ta reda på vad det kan vara för något som anslutit sig.

Uppgift 2

Vem har tillverkat nätverkskortet på den dator du själv sitter vid?

Uppgift 3

Utnyttja Wiresharks statistikavdelning genom att köra Statistics-->Summary. Hur stor är den genomsnittliga ramstorleken?

TCP/IP

Starta ett termianlfönster på samma sätt som i föregående laboration. Ge kommandot ipconfig i kommandofönstret och notera din dators IP-adress. Ett standardprogram för att ta reda på IP-numret svarande mot en viss internetadress är ”nslookup”. Detta kommando finns både i Windows och i Linux.

Uppgift 4

Starta en ny Capture i Wireshark och använd sedan nslookup för att ta reda på IP-adressen till www.google.se. Stoppa därefter infångningen i Wireshark.

a) Leta upp alla paket med ”DNS” i protokollfältet. Vilket transportprotokoll och vilken serverport används?
b) Identifiera vilka av paketen som utgör svar. Kan man se i paketen vilken server som svarat?
c) Innehåller svaret mer än ett IP-nr?

Ett behändigt kommando att utnyttja är tracert i Windows(i Linux heter det traceroute). Detta används då man vill ta reda på vägen till en viss adress. För att t.ex. ta reda på alla hopp innan google kan man skriva ”tracert www.google.se” i ett kommandofönster.

Uppgift 5

Starta åter igen en ny Infångning i Wireshark och ge direkt därefter kommandot ovan för att få veta vilken rutt som gäller till www.google.se. Stoppa infångningen och identifiera de paket som härrör från traceroute-körningen.

a) Vilka protokoll återfinns i dessa paket?
b) Hur varierar TTL (Time to Live) dels i förfrågningarna och dels i svaren?
c) Hur gör tracert-kommandot för att hitta vägen till www.google.se?

För att titta lite på TCP och flödeshantering överförs en fil. Ett förslag är att leta upp någon fil någonstans under följande katalog

http://ftp.sunet.se/pub/network/monitoring/

Uppgift 6

Starta infångning och sätt igång nerladdning av en fil. Stoppa infångningen när filen överförts och använd filtrering så att bara de paket som gått till eller från din dator syns. Använd, liksom i laboration 1 filtret

(ip.addr == x.y.z.w) där x.y.z.w är din dators IP-adress.

a) Vilka transportprotokoll och portar används?
b) Vilka är de första sekvensnumren och acknumren i TCP-förbindelsen?
c) Hur är flaggorna (SYN, ACK, FIN) satta i början av TCP-förbindelsen?
d) I segmenten som skickas till servern finns ett speciellt nummer med ”Win=” före. Vad är det?

Omsändningar av paket

En fil ska skickas från A till B. Filen delas in i paket, varje paket innehåller d bitar data från filen och en header på h bitar vilket innebär att paketets totala längd är $d + h$. Risken att en bit blir fel är p. Om ett paket innehåller en eller felaktiga bitar så sänds det om av A. Låt oss kalla medelantalet gånger ett paket måste sändas om för N.

Programmet TestMean.java (som finns på hemsidan) mäter hur stort N är genom att göra ett antal statistiska experiment. Dock fattas en del kod i programmet.

Uppgift 8

Vilka värden på $d + h$ och p används av programmet?

Uppgift 8

Komplettera programmet så att du kan få fram medelantal gånger ett paket måste sändas om för de värden på $d + h$ och p som finns i programmet.

Uppgift 9

En fil på 20 000 bitar ska överföras. Den delas in i paket där varje paket förses med en header som är 160 bitar. Sannolikheten att det blir fel på en bit är $p = 0{,}001$. Värdet på d kan vara 100, 200, 400, 500, 1000 och 2000. Vilket av dessa värden på d gör att det totala antalet bitar som måste skickas från A till B är så litet som möjligt? Gör detta genom att bygga ut programmet från Uppgift 8.