Laboration 1: Protokollanalysator

Introduktion

Målet med denna laboration är att få en inblick i hur trafiken på ett nätverk kan analyseras. Detta görs med programmet Wirehsark. Det är en fri programvara som är populär att använda för nätverksanalys. På http://www.wireshark.org/ finns programmet och dess dokumentation.

Laborationen kommer att genomföras på befintligt nät, det vill säga vi bygger inte upp något eget lokalt nät avskilt från Internet. Detta innebär att en hel del trafik kommer att synas på nätet

Oftast är inställningen i Wireshark att infångningen visas i realtid (efter hand som paket fångas upp). Då syns ett antal färgade rader där varje rad svarar mot ett infångat paket. I kolumnen ”Protocol” visas då ett av protokollen som är aktivt för varje paket, oftast det protokoll som ligger högst i TCP/IP-stacken.

Genomförande

Starta Wireshark.

Vänta ungefär 20 sekunder eller tills antalet ramar är tillräckligt stort (åtminstone 100) och avbryt därefter infångningen av ramar. Titta också på en webbsida under infångningen. I det övre fönstret listas alla fångade ramar. I det mellersta fönstret syns detaljerad strukturinformation om markerad ram och i det nedersta fönstret syns ytterligare detaljerad information om ramen i form av rådata uttryckt både i ASCII-form och i hexadecimal form.

I mittenfönstret syns tre olika sorters adresser. Dels finns där 48-bitars (6 oktetter) Ethernet-adresser. Varje nätverkskort har en unik Ethernet-adress. Den andra typen av adress är 32-bitars (4 oktetter) IP-nummer vilka också måste vara unika för varje nätverksenhet. Skillnaden är att Ethernet-adresserna bara syns "lokalt" medan IP-numren ska kunna adresseras över flera hopp.

Den sista sortens adress består av enbart ett decimalt tal och benämns port. På den ena av de två datorer som kommunicerar med varandra talar portnumret om vilken typ av tillämpning som används. Denna dator fungerar som server. Den andra datorn är klient och frågar efter en viss tjänst på servern. Det andra portnumret (hos klienten) är ganska slumpmässigt och avslöjar inte vilken typ av förbindelse det är frågan om.

Ibland kan något protokoll "skräpa ner" så mycket att det blir svårt att hitta de paket man egentligen är intresserad av. Man kan då utnyttja "Filter"-rutan. Om till exempel protokollet EDP ger väldigt många ramar kan man filtrera bort alla sådana genom att skriva "not edp" i filterrutan och sen klicka på knappen "Apply". För att ta bort filtret klickar man bara på "Clear".

Uppgift 1: Leta upp någon ram som har TCP angivet som protokoll. Markera motsvarande rad i det översta fönstret och titta på strukturinformationen i mittfönstret. Vilka tre nivåer (lager) från TCP/IP-modellen kan man se här?

Uppgift 2: Titta på den rad i mittfönstret som börjar med "Ethernet II". Vad är det för nummer som har sex stycken hexadecimala tal separerade med kolon?

Uppgift 3: På raden under syns två olika nummer sammansatta av vardera fyra decimala tal separerade av punkter. Vad är det för nummer?

Uppgift 4: Försök att hitta någon ram som har något portnummer och tag med portnumrets hjälp reda på vilken typ av förbindelse det är frågan om. Det portnummer som finns på server-sidan avslöjar nämligen vilken typ av service det är frågan om. T.ex. motsvarar port 80 att servern är en HTTP-server (webserver).

Ping-kommandot

Kommandot ping är användbart då man vill se om det går att få kontakt med en viss dator på Internet. Ping använder ett protokoll som heter ICMP, ”Intenet Control Message Protocol”.

Starta en ny infångning i Wireshark. Klicka på alternativet "Continue without Saving" eftersom vi inte bryr oss om att spara den första körningen. Kör därefter programmet ping i ett terminalfönster och pinga på någon adress (till exempel www.svt.se eller www.swedbank.se) eller något IP-nr. Låt ping göra några försök och stoppa sedan med Ctrl-C. Stoppa därefter infångningen och försök hitta de ramar som svarar mot ping-kommandot. Detta kan vara lite svårt men underlättas av att man först klickar på kolumnrubriken "Protocol". Då sorteras alla protokollnamnen i bokstavsordning och alla ICMP är samlade på ett ställe. Det är ganska troligt att inte så många andra ICMP-ramar hinner slinka mellan våra ping-ramar så nu återfinns dessa prydligt i en följd efter varandra parvis med förfrågan (request) och svar (reply). I det mittersta fönstret finns strukturinformation om ramen.

Uppgift 5: Vilka lager i TCP/IP-modellen finns med? I vilket lager finns Ethernet-adresserna?

Uppgift 6: Källa och destination framgår av mittfönstrets data. Avgör dessa både för Ethernet-adresserna och för IP-numren.

Webtrafik

För att titta på vad som skickas när man surfar på webben startar vi en webläsare och strax därefter en ny Capture i Wireshark. Surfa sen till www.google.se och gör en sökning på något (varför inte "Wireshark"). Efter det bör Wireshark ha fått tillräckligt många ramar för att det ska vara lönt att undersöka dem. Stoppa infångningen och leta upp en ram där HTTP står angivet som protokoll.

Uppgift 7: Identifiera vilka TCP/IP-lager som finns representerade i den valda ramen.

Nu är vi mest intresserade av vår egen trafik så det skulle vara bra om det gick att filtrera bort allaramar som inte är "våra" dvs de som inte innehåller vår IP-adress varken som källa eller som destination. Detta är lätt att göra i Wireshark: I raden under ikonmenyn finns en rad som börjar med en ruta som det står "Filter:" i. Skriv i det efterföljande fältet in följande

```
ip.addr == w.x.y.z
```

där naturligtvis w, x, y och z ska ersättas med ditt eget IP-nummer. IP-numret kan man få reda på genom kommandot ifconfig i ett terminalfönster.Skriv in ditt IP-nummer i fältet och klicka på

knappen "Apply". Helt plötsligt reduceras antalet ramar väsentligt. Precis i början syns ett par ramar där protokollet heter DNS.

Uppgift 8: Markera den första av de två DNS-ramarna. Ange vilka protokoll som används i de 4 lagren som syns i ramen.

Uppgift 9: Försök hitta den ram där google-sökkommandot finns och expandera den sista raden i mittfönstret. Vilket protokoll står angivet på denna rad och vilken information visas på "underrubrikerna" till denna rad?

Uppgift 10: Högerklicka på ramens rad i det översta fönstret och välj alternativet "Follow TCP Stream". Vad inträffar då?

Med denna teknik kan man rekonstruera delar av filer som överförs.