Laboration- Wireshark

I denna laboration ska ni lära er att använda programmet ***Wireshark*** för att fånga och analysera nätverkstrafik på paketnivå. Att kunna fånga och analysera nätverkstrafik är en viktig del i felsökningsarbetet men även nyttigt för att öka förståelsen för hur data skickas i ett nätverk och för att få en inblick i vad som händer på nätverket och kanske upptäcka avvikelser och felaktigheter (oönskad trafik).

Det finns flera gratisprogram för detta som går under benämningen ***packet sniffers***. Det mest kända är kanske ***Wireshark***. Microsoft har också ett gratisprogram som heter ***Network Monitor***.

Antal: Enskilt

Material: Till denna laboration krävs endast en dator med Internetuppkoppling samt programmet *Wireshark* som går att ladda hem gratis från http://wireshark.org

Tips: Titta på genomgångarna om Wireshark som återfinns på hemsidan http://itlararen.se/videos.html#video4. Mer hjälp finns även i dokumentationen på Wiresharks hemsida.

Utförande: Alla uppgifter och allt ni gör skall dokumenteras, gärna med skärmdumpar.

1. Installera Wireshark
2. Fånga en normal hämtning av en webbsida och dokumentera förloppet. Det är din egen trafik som du ska fånga. Välj lämpligt nätverkskort och starta inhämtningen av paket samtidigt som ni besöker en webbplats (som inte ligger i webbläsarens cache-minne). Lämpligt att fånga ca 10-30 sekunders trafik.
3. Hur upprättas en förbindelse?

4. Vilka protokoll används för att överföra hemsidan (från start till slut)?

5. Vad innebär ***promiscuous-mode***?

6. Filtrera innehållet genom att applicera ett *display filter* som enbart visar UDP-trafik. Hur åstadkommer man detta?

7. Hur skapar man ett filter som enbart visar TCP-trafik från ett visst IP-nummer (t.ex. 192.168.0.1)?

8. **OBS inte säkert att denna uppgift går att göra beroende på lokala förutsättningar -** Prova att fånga trafik till och från en annan host på det lokala nätverket. Antigen trådlöst via monitor mode, eller fysiskt med hjälp av en hub eller genom att konfigurera en switch med spanning port.

Detta skall du kunna efter genomförd labb:

- ✓ Hämta och installera programmet Wireshark
- ✓ Fånga nätverkstrafik
- ✓ Filtrera och analysera nätverkstrafik