Logning (snifning) af mail, http, IM mv.

Hvordan du enkelt og effektiv logger mail, http sider mv. med en sniffer. I artiklen tages der udgangspunkt i et windows program ved navn Netloggerse.

Skrevet den **03. Feb 2009** af **caspers** I kategorien **Netværk / Monitorering** | ★☆☆☆☆

Monitorering af lokalnettet eller internet forbindelsen

Der mange rigtig gode grunde til at se lidt på den net trafik der passerer forbi på lokalnettet og ikke mindst den trafik der går til og fra internettet.

Bare for lige at nævne et par enkelte gode grunde:
Logning af uvedkommende tilgang til lokalnettet.
Finde virus eller andre netforbrugene uønskede programmer
Se trafik fordeling mellem lokal maskiner på eget net
Logge mail, IM og http trafik I firmaer hvor man har den IT politik
Lave statistik over netbrug lokalt eller f.eks. af egen webserver
Identificerer eventuelle problemer på lokalnettet

Der er naturlig rigtig mange gode grunde til at sniffe nettrafik, ud over dem der mener det er vigtig at overvåge konen/manden eller børnene.

En forudsætning for at sniffe netværkstrafik er at den maskine der sniffer kan "se" trafikken, med "se" mener jeg at trafikken fra de maskiner hvis trafik der skal overvåges kommer til netkortet på sniffer maskinen. For at kunne sniffe den relevante trafik, skal sniffer maskinen placeres på en hub sammen med f.eks. den eksterne forbindelse til internettet.

Der efterhånden mange værktøjer til at monitorere nettrafik, specielt til Linux hvor mit erfarings felt er størst. Men de fleste er enten meget lowlevel eller meget dedikerede til en bestemt brug, så jeg har valgt at beskrive et program der både kan analyserer lowlevel trafik, og kan bringe det op på et meget forædlet data niveau. Programmet hedder Netlogger SE og er en software version af et hardware produkt der er anvendt af efterretningsvæsen og portaler rundt i verden.

Først sørger du for at din maskine kan se den trafik du vil logge. Hvis ikke du har en hub, kan du evt. placere to netkort i din maskine, og lade alt trafik passere gennem den, eller hvis din switch har en monitor port eller en span port så kan du sætte den til at monitorere alt ind og udgående trafik på den port hvori din forbindelse til internettet sidder.

Hent programmet hos download.com eller direkte hos producenten Unispeed:
http//:www.unispeed.com/netloggerse.html
Under installationen skal man hente en 30dages prøve licens, og så er vi i gang.

Programmet installerer sig som en service, det vil sige, når først det er konfigureret kan man lade den logge og analysere trafikken i baggrunden, der udover er der en bruger grænseflade der giver dig mulighed for at bygge en konfiguration op. I modsætning til f.eks. Etherreal skal man fortælle hvad man gerne vil se før data dumper ind på skærmen, tilgængæld for man præcis de data man skal bruge.

Bruger grænsefladen er beregnet til at styre mange services på forskellige maskiner, men her skal vi bare åbne den allerede konfigurerede lokale service. Når den er åbnet kan de enkelte konfigurations dele

trækkes ind på "skærmen". Træk først "Collect Packets" ind, og vælg hvilket netkort den skal sniffe på, den vil så sætte det netkort i promiscous mode, hvilket vil sige at alt netkortet "ser" bliver sendt videre til sniffer programmet. Det valgte netkort kan også være et WIFI netkort, og i det tilfælde er det naturligvis langt lettetre at placere sig et sted hvor man ser alt trafikken. Husk at trykke på værktøjets signallys for at sætte det i gang.

Med højre musetast og datasamples kan man se om der er noget trafik på nettet. Nu kan man så begynde at sætte alle de forskellige trafik analyse værktøjer ind, og sætte dem sammen næsten vilkårligt, og det kan være ret sjovt, specielt hvis der er lidt kød på den trafik man ser på.

Som man kan se er der mange protokoller man kan vælge at "extracte" her under SMTP, POP3, HTTP og messenger. "Extract" er det de kalder det når pakkerne bliver samlet og f.eks. en email samt evt. vedhæftede filer bliver uddraget. Det er værktøjer som dette politiet bruger på netovervågnings opgaver.

træk f.eks. "Extract SMTP" ind, og dobbelt klik på den og marker at du vil have "body" med)selve mailen og ikke kun informationer om til/fra og emne. Nu skal de så forbindes, så programmet ved at det er den trafik der kommer ud af "Collect Packets" der skal ind i "Extract SMTP", det gøres ved at trække pilen fra det ene værktøj over på pilen det andet. Nu vil du kunne se eksempler på mails der bliver fanget af din computer, på samme som før, men denne gang naturligvis højre musse tast på "Extract SMTP". For at beskrive hvor de fangede mails skal gemmes, placerer du en "Log to File", og under på den under properties skal du skrive et filnavn. Når du har trykket alle signallysene grønne loger du alle de mail der kommer forbi.

Du kan også logge nettrafikken Rå, og kigge på den senere, eller lave komplicerede analyser af f.eks. web trafik og gemme det direkte i en database, men det må du selv prøve. Selv funktioner der ikke lige er tilgængelige kan man ved at skrive en stump Python script i et dertil indrettet værktøj. Et eks. kunne være "Send mig en mail, og log alt trafik hvis ordet Frihed optræder i en mail eller et html dokument"

Hvis du har en Linux maskine enten som router eller bare på lokalnettet kan du fra den logge trafik til senere analyse sådan her:

```
tcpdump -s 1600 -w logfilnavn.pcap
```

hvis du bruger en Windows maskine som router, installer da servicen på den, og brugergænsefladen på din egen maskine.

Kommentar af henrik22 d. 03. Nov 2006 | 1

Kommentar af riversen d. 29. Jul 2008 | 2

Det virker ikke til du aner hvad du skriver om. Snifning bruges normalt kun i fejlfindingssituationer. Til generel overvågning af netværkets tilstand, uønskede gæster, internettrafik o.l. bruger man normalt snmp, ips, ids etc. Med snifning opsnapper du kun trafik der kommer forbi din pc, hvilket der ikke vil være noget af i et switchet netværk udover broadcasts og pakker til pc'en selv.

Kommentar af human d. 04. Nov 2005 | 3

I dit link mangler du //. Desuden hedder det unispeed, ikke uinspeed som der også står. Ret den her artikel, den er nærmest ulæselig.

Kommentar af therichman d. 04. Nov 2005 | 4

En ganske interresant artikel, og jeg vil da straks afprøve det.
Hvad jeg mangler i din artikel er en mulighed for at sikre sig imod sniffing, altså programmer, firewall eller hvad ved jeg.
Forresten, så ret lige dine stavefejl... specielt den her: "forskællige" :p

Kommentar af over-load d. 09. Nov 2005 | 5

Som sagt før, giver din manglende gennemlæsning af din artikel den en form for uproffesionalisme, men stoffet er som sådan ganske udemærket!