

Anbefalet software

Nedenstående er en liste over software som jeg klart kan anbefale med nogle få kommentarer - du er velkommen til at sende mig yderligere spørgsmål omkring mine erfaringer med nedenstående.

Jeg bruger udelukkende UNIX operativsystemer til arbejde og forretningskritiske opgaver og nedenstående liste er derfor primært Open Source og UNIX relateret. Jeg kan dog til nød afvikle Windows software såfremt jeg bliver tvunget til dette af samarbejdspartnere eller der ikke er et alternativ til det pågældende software på UNIX - se eksempelvis ISS System Scanner
Formålet med denne side er at give andre mulighed for at opdage god software

Software er forsøgt inddelt i passende områder

Operativsystemer

Jeg bruger Mac OS X på alle arbejdsstationer og OpenBSD på alle servere og infrastruktureheder som DNS, firewall, postservere. Dvs alle steder hvor det er mig der bestemmer.

- Mac OS X et brugervenligt UNIX operativsystem med det hele <http://www.apple.com/macosx>
- OpenBSD et multiplatform UNIX operativsystem med ekstrem fokus på sikkerhed <http://www.openbsd.org>

Derudover bruger jeg og har mange gode erfaringer med:

- NetBSD et multiplatform UNIX operativsystem <http://www.netbsd.org>.
NetBSD er meget portabelt!
- FreeBSD et yderst brugervenligt og fleksibelt UNIX operativsystem med super dokumentation <http://www.freebsd.org>.

Jeg har også brugt Linux i mange år og det kan klart anbefales, hvis man kan leve med det kludetæppe af software som det indimellem er ;-). De distributioner af Linux som jeg har brugt "for nyligt"/bruger for tiden er:

- Auditor Security Collection som er en boot-cd med Linux og mange sikkerhedsprogrammer. Denne CD bruger jeg på alle mine kurser <http://www.remote-exploit.org/index.php/Auditor>
- BackTrack er projektet som er kommet ud af kombinationen af Auditor og Whax - jeg har ikke haft tid til at afprøve denne <http://www.remote-exploit.org/index.php/BackTrack>
- Se mere på <http://www.remote-exploit.org>

Infrastruktur software

Der skal bruges en masse software for at understøtte brugen af computere udover operativsystemet. Her er en liste over det software som jeg har valgt - selvom der i mange tilfælde ikke er meget at overveje.

Navne og adresser

Disse funktioner følger med i OpenBSD men refereres her fordi softwaren jo skal konfigureres.

- ISC BIND version 9 er den software som langt de fleste bruger som navneserver på internet. BIND har en god konfigurationsfil og er velbeskrevet. Manualen følger med software i Docbook format <http://www.isc.org/>
- ISC DHCPD er den DHCP serversoftware som mange bruger DHCPD har en god konfigurationsfil og er velbeskrevet. <http://www.isc.org/>
- rtadvd er funktionen til at uddele prefixes til IPv6 ved at udsende *router advertisement packets*

Logging og dataopsamling

Det er vigtigt at kunne fejlfinde og det kræver at man opsamler information om systemerne.

- syslogd følger med alle UNIX systemer og er de facto standarden for UNIX logging. Denne funktionalitet er så udbredt at man på næsten alle netværksenheder kan få logging sendt til en syslogd centralt. Jeg kan anbefale Tina Bird som underviser indenfor logging infrastrukturer og det website som hun har været med til at opbygge <http://www.loganalysis.org>
- Snort intrusion detection systemet er alle tiders system til at få information om netværk - og lære om angreb. NB: det kan kræve mange ressourcer at understøtte et IDS system! Jeg anbefaler at man er yderst kritisk med hvilke signaturer man inkluderer i sin konfiguration - for at undgå en flodbølge af information. <http://www.snort.org>
- OpenNTPD er software til at sikre ensartet tid henover netværket - yderst vigtigt for at kunne sammenholde information mellem systemer. OpenNTPD er udviklet af OpenBSD projektet og følger derfor med i OpenBSD. <http://www.openntpd.org>

Firewalls

Default Publication

Jeg bruger primært OpenBSD Packet Filter, som forkortes til OpenBSD PF eller bare PF. Denne moderne og velfungerende firewall implementation har vundet indpas flere steder og følger idag med i OpenBSD, FreeBSD og NetBSD.

<http://www.openbsd.org/faq/pf/index.html>

Hvis man ikke har lyst til at bruge OpenBSD PF anbefaler jeg at man bruger m0n0wall som er en firewall bygget på FreeBSD som har en enkel og simpel brugergrænseflade gennem en webbrowser med en masse god funktionalitet. <http://www.m0n0.ch/wall/> Jeg anbefaler IKKE Linux som firewall! Linux firewall implementationen har et håbløst konfigurationsinterface. Designerne af kommandoerne til at indsætte reglerne har valgt at gøre det på en tåbelig måde, der gør det umuligt at læse og overskue firewall scripts. Ved at bruge options fremfor at definere en passende syntaks gøres det umuligt at læse. (måske ikke umuligt men sværere, og det har man ikke brug for i en firewall konfigurationsfil!)
Eksempel:

```
iptables -I INPUT -i $LAN_IFACE -p udp --dport 67:68 --sport 67:68 -j ACCEPT
```

og fordi det er options til en kommando kan samme så hvis man har lyst skrives:

```
iptables -p udp --dport 67:68 --sport 67:68 -j ACCEPT -i $LAN_IFACE -I INPUT
```

Til forskel har FreeBSD IPFW som ligeledes benytter en kommando til at indsætte regler valgt at definere syntaksen og derfor rækkefølgen - hvilket gør brugen af options med ----- overflødigt.

Eksempel svarende til ovenstående i IPFW format:

```
$fwcmd add allow udp from any 67,68 to any 67,68 via $oif
```

- det læses nemmere efter min mening!

Det skal afslutningsvis siges at man ofte kan konfigurere Linux firewall gennem en bedre brugergrænseflade indbygget i eksempelvis Red Hat Linux distributionerne og at det performer fint når det er konfigureret. Det er *ok* - men heller ikke bedre. <http://www.netfilter.org/>

Applikationssoftware

Jeg bruger en del software som jeg vil betegne som værende forretningskritisk for mig og min virksomhed. Denne software er i stort omfang open source og det er vigtigt for mig ikke at skulle afsætte mange tusind kroner for hvert enkelt system som jeg vil arbejde på.

De mest forretningskritiske applikationer på arbejdsstationer er nok:

- LaTeX som jeg bruger til alle præsentationer og alt mit kursusmateriale. LaTeX gør det muligt nemt at lave PDF udgaver af materiale og inkludere konfigurationsfiler og andet direkte.
- Versionsstyring som bruges til alle LaTeX filerne, jeg bruger CVS og SVN
- Adobe Acrobat Reader eller Mac OS X Preview til visning af præsentationer
- Grafiske biblioteker som benyttes af

Det anbefales at melde sig ind i Dansk TeX-brugergruppe (DK-TUG) <http://www.tug.dk> man modtager derefter CD/DVD med TeX-Live <http://www.tug.org/texlive/>.

Applikationsservere til web

Jeg er ret vild med JAVA og da jeg skulle vælge et CMS til at erstatte flade HTML filer med server side includes fandt jeg efter en del overvejelser frem til Apache Lenya.

Jeg ved ikke rigtigt om man kan anbefale Apache Lenya - for det er indimellem lidt svært at forstå hvordan det virker og hvor man skal tilpasse det.

Det gode ved Lenya er:

- Det er en del af miljøet omkring Apache Software Foundation og derved opnås en vis sikkerhed for at projektet drives efter nogle gode regler
- Det kører i en Tomcat som efter min mening er en sikker og nem måde at afvikle websystemer
- Tomcat og Lenya integrerer godt med Apache HTTP server
- Lenya kan eksportere hele websitet til flade filer, hvis man ønsker dette
- Lenya virker med Firefox som platform for et antal editorer til websiderne
- Det er nemt at vedligeholde flere websites i den samme Lenya
- Det er ikke PHP
- Den laver websider som overholder standarderne
- Udseendet af websider styres udelukkende med CSS
- Systemet er baseret på Cocoon som gør det simpelt at lave PDF fra XML på websystemet
- Det bruger XML filer som er til at forstå - der er altså en exit-mulighed fra værktøjet. Vigtigt!

Apache Software Foundation projekterne findes nemt gennem websiden <http://www.apache.org>