BSD-DK Nyhedsbrev 009

December 2007

INDHOLD

1. INTRODUKTION

Af: Søren Hansen

Velkommen til denne niende udgave af BSD-DKs nyhedsbrev. I sidste nyhedsbrev lagde vi op til, at frekvensen af nyhedsbrevet skulle være omkring 1 hver anden måned. I den periode, der er gået har der været afholdt julefrokost og et enkelt foredrag i BSD-regi. Begge dele var samtidig store succeser indholdsmæssigt, men desværre uden specielt mange deltagere. Hvorfor er det, at der er dette misforhold?

I dette nyhedsbrev vil vi som noget nyt introducere et afsnit for de enkelte BSD-distrubutioner, og hvad der i øjeblikket er »hot« indenfor dem. Derudover har Henrik Kramshøj skrevet et indlæg om Prelude-IDS – helt sikkert noget jeg personligt skal have kastet mig over, og som jeg da også vil foreslå taget op til næste Happy-Hacking arrangement.

God læselyst!

2. ÅRETS JULEFROKOST!

Af: Peter Larsen, formand for BSD-DK

Årets Julefrokost blev indtaget på Café Høegs / www.hoegs.dk på Enghavevej.

Ialt 10 fremmødte blev det til, og med masser af god øl (vi drak alt Hoegaarden der var i huset) til rådighed og med en flaske snaps på bordet blev der voldsomt hygget igennem og fortalt mange sjove og spændende historier.

Maden bestod af:

Forret: Røde, marrineret og karrysild med diverse tilbehør (og kapers) til.
Hovedret: En platte med fiskefilet, flæskesteg, mørbradbøf, to slags ost og kiks samt tilbehør.
Dessert: Ris a la mande med lun kirsebær sauce.

Vi gik derefter ombord i de mange drinks, der var at vælge imellem.

http://surl.dk/3ci/
(mand og blomst)

Nooooogle (pege) gik måske mere til den end andre..

Hyggeligt var det, og den sidste flok gik hjem et godt stykke over midnat.

Næste hyggemøde?
Næste hyggemøde er pt. ikke planlagt, men jeg vil tro at når vi er trillet hen over julen og har fået fyrret krudt af til nytår.. og hovedpinen er væk igen. Så har jeg nok fundet et sted hvor vi skal nyde en burger/god mad og en øl i 2. / 3. uge i januar. Hold øje med kalenderen!

3. HOT I BSD DISTROERNE

Følger du med i udviklingen i alle BSD-distributionerne? De fleste af os holder os nok til til lige at følge med i den distribution, som vi selv bruger, for det kan hurtigt blive en uoverkommelig opgave, at følge med i alle mailinglister, hvis du gerne vil bruge tilværelsen på andet.

Derfor indskrænker de fleste sig til at følge med i netop det, der er umiddelbart relevant for dem. Nemlig det de selv bruger. Men derfor kan udviklingen i de andre distributioner da alligevel godt være interessant. Hvad foregår der egentlig af spændende udvikling ovre i de andre BSD-distributioner, som du ikke lige selv bruger?

For at svare på dette spørgsmål vil vi i nyhedsbrevet fremover prøve at få samlet op på, hvad der i øjeblikket er hot i de enkelte distributioner. Det bliver en meget kort gennemgang, hvor nogle rutinerede brugere af de enkelte systemer har sagt ja til at være redaktører for hver deres OS og at lave en kort appetikvækker for den nuværende udvikling indenfor netop deres område.

Tre personer har sagt ja til denne opgave, og det drejer sig om Søren Strårup, som skriver om FreeBSD, Anders Mundt Due, der skriver om NetBSD og Thomas Alexander Frederiksen, der skriver om OpenBSD.

3.1 NetBSD

Af: Anders Mundt Due

Midt i November var NetBSD 4.0 RC4 klar, og man kan jo kun håbe at vi efterhånden nærmer os en endelig release af 4.0.

http://mail-index.netbsd.org/netbsd-announce/2007/11/09/0001.html

Som kan hentes fra: ftp://ftp.netbsd.org/pub/NetBSD/NetBSD-4.0_RC4

Automated Testing Framework er på vej ind i NetBSD source træet og antages at være klar til når 5.0 engang kommer på gaden.

http://www.netbsd.org/~jmmv/atf/

Det nye NetBSD Core Team bestående af 5 medlemmer er sammensat og etableret.

http://mail-index.netbsd.org/netbsd-announce/2007/11/21/0000.html

3.2 OpenBSD
Af: Thomas Alexander Frederiksen

1. November (lidt tidligere for de der havde købt CD'erne) kom seneste OpenBSD release, som altid til tiden. OpenBSD 4.2 byder på en række små-forbedringer over hele linien, som det jo er typisk for den type release-cycle der bruges af projektet. Enkelte af dem fortjener dog nærmere omtale:

FFS2-support er kommet med, der mangler dog endnu lidt arbejde før alle dele af systemet er klar til filsystemer over 2TB - ligesom der endnu mangler snapshot- og background fsck-support. De sidste ting der mangler for at komme over 2TB burde dog være på plads når 4.3 kommer 1. Maj 2008.

PF har også, til dels sammen med netværksstakken, fået en større overhaling. Til og med 4.1 brugte PF mbuf tags, men der er nu skiftet fra en packet header mbuf + mbuf tag til styring af hvad der sker med pakker, til at det gøres direkte i en packet header mbuf. Det sparer et par malloc-kald per pakke, og forbedrer performance dramatisk under de fleste forhold. Der er også optimeret på en lang række andre områder, og samlet set har det øget performance under det simplest tænkelige regelsæt (bridging + pass all) ganske meget - fra 29 Mbit/s til 58 Mbit/s på en Soekris 4801.

På hoststated-siden er der også sket meget nyt. Der er kommet layer 7-support, med HTTP SSL-terminering, generisk SSL-terminering, HTTP header-manipulation og meget, meget mere. Graceful reloading er kommet til i layer 3-delen, og kan forventes at være klar i layer 7-delen inden 4.3.

Den sidste større klump af ændringer der er værd at tage med er på wireless-siden, hvor det på det nærmeste har regnet med bugfixes, små-ændringer og clean-ups. Det store hop der mangler er WPA-support, noget der dog tilsyneladende afventer at en eller flere udviklere har tid og lyst til at tage det store ryk.

Ellers er alt vist business as usual i OpenBSD-land.

3.3 FreeBSD
Af: Søren Strårup

FreeBSD 7.0-R forberedelserne er sat igang. Noget af det, der er ændret i HEAD på sidste, er at SCHED_ULE er blevet til den scheduler man bruger hvis man bruger en GENERIC kerne, dette er dog kun sandt for i386 og amd64. Som følge deraf er man nødsaget til at skifte til ADAPTIVE_GIANT (I mit tilfælde kunne jeg dog ikke bruge det da em(4) driveren fik boksen til at panic'e).

FreeBSD på andet end de "almidelige" desktop/server arkitekture er ved at skride fremad. Der er folk/grupper som arbejder på PowerPC, MIPS og ARM arkitekturer. P.T. arbejder jeg selv, når tiden tillader det, på AT91RM9200. Det er jo ved at være en »gammel« udgave. En af de ting, som jeg ser, at er godt for f.eks ARM processorer, er, at der er så mange leverandører om udbudet så priserne er »ok«. Hastigheden er dog stadig et problem.

En form for wearleveling er også efterlyst. Der er noget som hedder geom_nand, men der er ikke noget officielt om det. Et ønske kunne godt være noget bistand til hvordan f.eks. kunne bruge geom laget til at lave noget FS uafhængit wearleveling.

Vil lige afslutte med min famøse sætning:
»If a program is not working right, then send a patch«

4. FOREDRAG OM CRUISECONTROL

Af: Peter Larsen, formand for BSD-DK

I vores store eftersøgning efter menngsfyldte foredrag til vores videnshugrende medlemmer af BSD-DK, er vi faldet over Hack Kampbjørn's interessante viden om CruiseControl.

CruiseControl er kort fortalt et testing suite af e.g. java/c#/perl/php/ruby osv. kode. Man sætter en række test cases op, og ud fra det får man en rapport og interessante informationer tilbage.

Vi havde en interessant generalprøve på fordraget d. 12. november hvor undertegnet, Flemming Jacobsen, Henrik Kramshøj og ganske få andre var tilstede. Måske var foredraget for sent annonceret.

Vi mente dog, at fordraget godt kunne tåle en gentagelse, da vi hurtigt fandt ud af at ALLE (selv enkeltmandsvirksomhederne) ville kunne bruge CruiseControl til at kvalitetssikre og gennemføre ordentlig testing af al slags kode, og dermed forhøje kvalitetsoplevelsen for deres kunder.

Jeg vil derfor opfordre til at alle møder op til Hack's gentagelse af fordraget d. 14 januar, og hvis vi bliver over 20 tilhører, så har jeg hørt at formanden giver en øl på vej hjem!

5. PRELUDE-IDS PÅ BSD

Af: Henrik Kramshøj

Siden september har jeg benyttet et IDS system kaldet Prelude-IDS, eller mere præcist har jeg benyttet et antal programmer som er bundet sammen af Prelude-IDS hybrid IDS framework.

Grunden til at jeg stødte på Prelude-IDS er, at der var en annoncering af ports til OpenBSD med delene til frameworket. Ved et besøg på hjemmesiden fandt jeg ligeledes ud af at Prelude-IDS findes både i pakkesystemerne til NetBSD og FreeBSD - så hvad er mere passende end at omtale dette i nyhedsbrevet.

Prelude-IDS er som sagt et framework, og det lyder jo som en masse lim, men ikke noget at binde sammen. Men det er der. Selve Prelude-IDS projektet indeholder mange værktøjer. Hertil kommer det kommercielle firma der laver Prelude-IDS tilpasning og sælger nogle kommercielle moduler.

Hvad får man så med Prelude-IDS?

Man får et par centrale moduler, blandt andet en manager der kræver en database. Jeg valgte som sædvanligt Postgresql, men MySQL er også understøttet. Dernæst skal man bruge en frontend, hvor det naturlige valg er Prewikka som er med fra projektet, med nogle kommercielle udvidelser til salg.

Når man således har en manager kan man tilmelde et antal sensorer, og nu bliver det sjovt. Den sensor man først bør kaste sig over er Prelude-LML som er Prelude Log Monitoring Lackey, altså en hjælper til at læse logs. Lakajen er din hjælper der forstår PCRE og med nogle
simple udtryk kan uddrage information fra dine logfiler – hvadenten det så er logfiler fra Sendmal, Postfix, sudo, SSH eller lignende.

Der medfølger en del eksempler og det er nemt at tilføje nye. Til sammenligning er det en forbedret udgave af Swatch der også kan bruges med syslog generelt.

Ved at smide lakajen på alle dine servere kan du nu nemt centralt se alle logins med ssh og sudo, både fejlslagne og successfulde logins.

Det næste man så bør se på er PFlogger, for PF er jo verdens bedste firewall og med PFlogger sensor smider man nemt log til Prelude. Faktisk er det så nemt at man blot skal registrere sin sensor i prelude manager og derefter starte PFlogger. Når det er gjort vil man få en event i sin database for hver linie i pf.conf der har keyword log med. Så nemt kan det laves!

Til gengæld finder man ud af hvor mange maskiner ude på internet der er inficeret med virus/orme, så en hurtig forbedring er at ændre pf.conf i stil med:

```
scrub in
block in log

# clean stuff from log
block in quick from any to 224.0.0.0/8
block in quick proto {udp tcp} from any to any port { 67 68 135 137 138 139
445 1433 1434 }
block in quick from <foes>
block in quick from <spammers>
block in quick from <blogspammers>
```

Bemærk at man derved undgår events og logs for ting som er ligegyldige.

Når dette første setup er kørende skal man huske at køre Postgresql vacuum på sin database jævnligt og nyde det gode overblik i Prewikka :-)

Der findes et antal andre sensorer som plugger direkte ind i frameworket og listen vokser hele tiden. Af de mere interessante for mig er: Snort - Open Source NIDS har direkte understøttelse for Prelude PAM - Pluggable Authentication Modules Samhain - file integrity / intrusion detection system

Til sidst skal måske også nævnes at Prelude-IDS benytter et standard databaseformat kaldet IDMEF som gør at andre værktøjer nemt burde kunne genbruge data.

Opsummeret er der følgende fordele ved Prelude:

- ikke PHP
- nemt at installere, centrale server 2 timer, sensor 1 time
- nemt af konfigurere, centrale server 1 time, sensorer 1-uendeligt
- overblik centralt
- aktiv udvikling
- understøttelse for avanceret funktionalitet
- prewikka er nem at forstå for de fleste.

Eneste anke med Prelude-IDS er nok licensen som er GNU General Public License version 2, men bare det ikke er GPLv3 så går det nok :-)

Så hvis du vil have overblik over dit netværk mht. logins, angreb, logfilerne så er Prelude værd at se på.

Links:

- http://www.prelude-ids.org/ Open Source Prelude-IDS
- http://www.prelude-ids.com/ PreludeIDS Technologies
- https://trac.prelude-ids.org/wiki/Prewikka
- Et blog indlæg med enkelte billeder: http://blog.kramse.dk/blojsom/blog/default/2007/09/05/Prelude-IDS-overblik-over-sikkerheden

6. KOMMENDE BSD-DK ARRANGEMENTER
Udover hyggemøder i uge 2/3 samt i uge 7, som der endnu ikke er sat præcis dato på, er følgende arrangementer planlagt til den første del af 2008. Følg med på announce-listen for annoncering af tid og sted for enkelte arrangementer.

- **Mandag den 14. januar** Foredrag om CruiseControl v/Hack Kampbjørn
- **Onsdag den 30. januar** Happy Hacking
- **Fredag den 8. februar** Foredrag om Open Source som nyskabelse v/Gregers Petersen
- **Onsdag den 27. februar** Happy Hacking
- **Fredag den 7. marts** Foredrag om ARM9 og FreeBSD v/Søren Strårup
- **Lørdag den 22. marts** BSD-DKs fødselsdag
- **Onsdag den 26. marts** Happy Hacking

Husk at du også kan se BSD-DKs kalender på foreningens hjemmeside, samt at du kan subscribe på kalenderen i iCalendar format.

7. NETIKETTE PÅ BSD-DK MAILINGLISTERNE
Fra http://www.bsd-dk.dk/netikette.shtml

Før du søger hjælp på mailinglisterne, er der nogle ting som du kan gøre for at få bedre hjælp:

- **Lad være med at stille de samme spørgsmål**
  Søg i mailarkivet for at se om der er andre der har haft et tilsvarende problem. Så slipper folk på listen for at svare på de samme spørgsmål om og om igen.
  Kig i mail arkivet.
- **Tal pænt.**
  Folk på listen får ikke penge for at løse dine problemer, de gør det af egen fri vilje. Hvis du udviser almindelig høflighed kommer du langt! Dette gælder i lige så høj grad de "garvede" på listen! Det at du har en masse erfaring giver dig ikke ret til at skræmme vores nytilkommere væk! Husk at du selv var grøn engang. Vejled de nye i at blive gode mailinglist medlemmer i en god tone.
- **Vær præcis**
  For at undgå at bruge flere mails på at afdække trivielle detaljer bør du inkludere dem allerede i den første. Eksempler kan være versionsnummer på den pågældene applikation eller på operativsystemet, stinavne og environment variable hvis det er relevant. Forklar proceduren du gjorde da du opdagede problemet og/eller hvordan man kan reproducere det. Inkluder den eksakte ordlyd af fejlbeskeden (Brug klip & klistre hvis det lader sig gøre). Disse informationer kan hjælpe andre når de skal søge efter et tilsvarende problem.
- **Prøv først selv.**
  Listens imødekommenhed øges dramatisk hvis det kan ses at du faktisk har prøvet at løse problemet inden du sendte det til listen. Beskriv hvad du selv har gjort for at løse problemet. Hvis du sidder fast, så prøv at læse de relevante manual sider eller søg information på steder som Google - det afslører måske den detalje der sætter dig i stand til at løse problemet selv. Udover fornøjelse og selvrespekt, er det processen ved at løse problemer, som virkelig sætter skub i det at lære nye ting.
- **Giv tjenesten tilbage ;).**
  Hvis du har lidt tid og løsningen til et problem som du har set på listen, så overvej venligst at skrive en mail til listen. Den information du ligger inde med kan være uvurderlig for personen som søger hjælp og den er med til at gøre mailinglisten et værdifuldt sted at søge hjælp.

8. NÆSTE NYHEDSBREV

Næste nummer af nyhedsbrevet vil udkomme i begyndelsen af februar. Jeg skal derfor opfordre alle, der har noget på sinde, at informere os i god tid, og indlevere deres indlæg inden den 1. februar. Indlæg kan indsendes til bestyr (hos) bsd-dk.dk