MUUGLines

The Manitoba UNIX User Group Newsletter

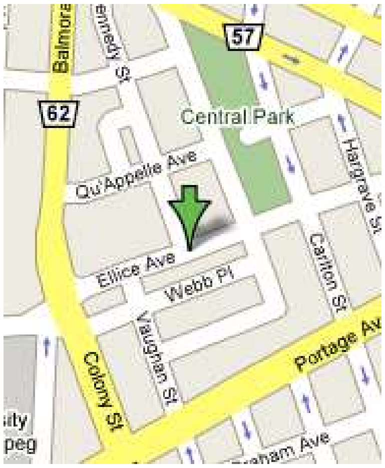
November 2009 Volume 22 No. 03

Next Meeting: November 10th, 2009

MediaWiki

MediaWiki is an open source wiki package, originally designed to implement **Wikipedia**. It is now used by several other projects of the non-profit Wikimedia Foundation and by many other sites. MediaWiki is written in PHP, and runs nicely in the typical LAMP stack. It is fairly easy to set up and most configuration can be done through a web browser.

In the collaborative spirit of MediaWiki, this presentation will be a joint effort between Kevin McGregor, Gilbert Detillieux and Michael Doob. Gilbert will focus on installing and configuring MediaWiki, Kevin will focus on using and managing it, and Michael will show a novel way he's using MediaWiki on a netbook to store and present class notes, complete with mathematical notation.



This month's RTFM topic, by Montana Quiring, will look at UNIX pipes.

Where to find the Meeting

Meetings are held at the IBM offices at 400 Ellice Ave. (between Edmonton and Kennedy). When you arrive, you will have to sign in at the reception desk. Please try to arrive by about 7:15pm, so the meeting can start promptly at 7:30pm.

Limited parking is available for free on the street, either on Ellice Ave. or on some of the intersecting streets. Indoor parking is also available nearby, at Portage Place, for $5.00 for the evening. Bicycle parking is available in a bike rack under video surveillance located behind the building on Webb Place.

Upcoming Meeting:

December 8th, 2009: SuseStudio

SuseStudio is an online virutal appliance builder based on OpenSUSE. John Lange will demo, from start to finish, the creation of a completely custom Linux distribution.

We Think Your Friends are Awesome!

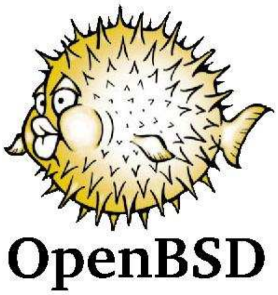
We Want To Meet Them!

Do you have a friend that is working on an interesting Linux/Unix project?

Why not ask them to present what they are doing at a future MUUG meeting?

Have them email **board@muug.mb.ca**

OpenBSD 4.6 Released



On October 18th the OpenBSD released version 4.6. This release brings a bunch of changes some new machine support for older SGI and MVME68k boards as well as a whole bunch of new drivers for all kinds of equipment (ethernet, wireless, SATA, video etc.). Also significant changes were made to PF which reduce parsing complexity and improve active-active pfsync setups. There are new tools as well such as a sendmail replacement via privilege-separated smptd and GNU screen replacement included in base (namely tmux).

For more information, take a look at the release article at **http://bit.ly/openbsd46**.

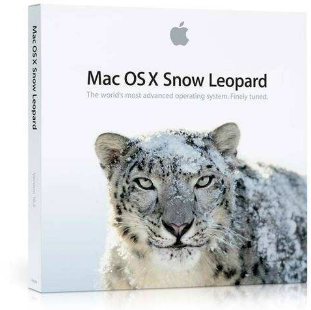
FreeBSD 8.0-RC2 Released

On its way to a stable tag (RELENG_8) the FreeBSD release team has put out RC2 on October 28th. The 8.0 release has focused on performance with improvements to the VFS layer, XEN dom-U, a new USB stack and a new version of the ULE scheduler. A neat feature of the updated schedule is that it makes it possible to eventually bind a Jail to a specific CPU as well as noticeable SMP performance gains. Packed with more feature additions than I can count the big guns of DTrace and ZFS in the kernel bring in the exciting technologies from Sun though DTrace is limited to the kernel tracing at them moment.

Google Android 2.0 Announced

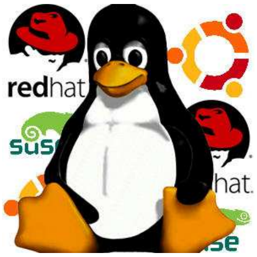
Continuing the OS updates this time Google drops its next major release of Android code named “eclair.” The first product to ship with this version will be the Motorola Droid. In its fast and furious attempts to out due the iPhone this release features built-in turn-by-turn navigation, “combined inbox” and MS exchange support,. As well many improvements to the camera application, the virtual keyboard and the built in browser now has full HTML5 support. You can find out more detailed platform information from the SDK highlights page at **http://bit.ly/4jMGKq**.

Apple Drops ZFS Support



On October 24th, MacOS Forge announced that the ZFS project has been discontinued and the corresponding source code repository and mailing lists were to be removed. ZFS was a highly anticipated new feature of OS X especially the snapshotting feature which was rumored to be the next upgrade to the Time Machine system backup feature. OS X Leopard already had ZFS read only support which fueled those rumors. Reasons for the discontinuation have not been made public but Sun’s Jeff Bonwick is on record stating that Apple and Sun were not able to reach a mutually agreeable licensing deal. While there won’t be official support for ZFS from Apple the MacFUSE project is working on implementing support for it though most of the revolutionary features would not be as usable.

Other OS Releases



As per distrowatch, the following projects have had releases in October:

- NexEnta 3.0 Alpha 1 on 20/14/2009
- CentOS 5.4 on 10/21/2009
- Ubuntu 9.10 on 10/29/2009
  - Leaf projects also released:
    - Xubundu
    - Mythbuntu
    - kubuntu

    - MythBuntu
    - UbuntuStudio
- Toorox 10.2009 on 10/29/2009
- OpenSUSE 11.2 RC2 on 10/30/2009

Sequoia Voting Systems to Publish Code

On October 27th Sequoia Voting Systems plan to publically release the source code for its new optical scan voting system. This new system is intended to be submitting for federal certification in the first quarter of next year. One of the most important factors in a voting system is the ability to audit and confirm results from peer review. Opening the source code for electronic voting systems allows for their eventual use in electronic voting systems but in this case even the public will be able to audit the system totally from collection and results.

A more detailed version of this story is in the Wired Threat Level blogs announcement (**http://bit.ly/190cnw**).

Microsoft to Open PST File Format.

On its Interoperability Blog (**http://bit.ly/2Ii4Cb**) Microsoft announced its intention on opening up the specifications for the PST file format used by its Outlook product. While it has previously been possible for access the contents of a PST via the MAPI interface, other mail clients (like Thunderbird or The Bat) were locked out of importing data stored in PST files. It isn't certain how open they are going to be but this definitely is a start.

Asterisk Bug Leads to Exploits Referred to as "Vishing"

Last September, tools were released to exploit a "low-level problem" in the Asterisk PBX system, allowing the user to attack Asterisk and, when successful, allowing hackers to use the system as they please. This lead to a rash of phishing attempts made via other people's PBX's which is being referred to as "vishing." A famous attack reported in October was apparently from a band of Romanian hackers who used the exploit to make telephone-based physicing calls to Liberty Bank customers in California.

This is shades of the Telco hacking that was common a few short decades ago. PBX hacking is by no means new but the use of PBX exploits to launch wide range "vishing" attempts is becoming "endemic" in the opinion of a larger article on this topic in The Standard (**http://bit.ly/3VXgWu**).

Finding IP Addresses for a Company

Occasionally a system administrator would get the request to block an online service or company at their firewall for many and varied reasons. One attempt is to block via URL but services such a Google's are tricky as they will frequently change the host names of their services and it is almost impossible keep up with the frequent change or track aggressive services. Blocking by IP is another attempt and even that is not fool-proof as IP space is still dynamic. Just doing a whois of google.com can be daunting but there is a way to automate it to generate lists of IP's.

All you really need is a single IP for a target network. In this case we'll try google via ARIN's database.

```
$ whois -a google.com
google.com QWEST-BUC-GOOGLE1 (NET-63-146-
123-0-1) 63.146.123.0 - 63.146.123.31
google.com QWEST-BUC-GOOGLE2 (NET-63-236-5-
128-1) 63.236.5.128 - 63.236.5.159
google.com QWEST-BUC-GOOGLE (NET-66-77-90-
48-1) 66.77.90.48 - 66.77.90.63
google.com QWEST-BUC-GOOGLE3 (NET-63-236-5-
224-1) 63.236.5.224 - 63.236.5.239
```

This gives us a start but not in a nice way so we can recurse on the net names and extract the CIDR's to feed into our firewall rules or other blocking tools.

This isn't very difficult and can be compressed into a bash script small enough to fit into a "tweet"!

```
for i in `whois -a $1|awk '{print $3}'|grep
NET|sed -e 's/[(]//;s/[)]//'`; do whois -a
$i|grep CIDR;sleep 5;done|awk '{print
$2}'|grep -v \:
```

where "$1" is a domain name, like google.com.

This still isn't a perfect approach or even a good one (we're only searching ARIN and Google has many netblocks around the world) but it can be useful in a pinch to buy you time to find something better. Another more crazy example is to watch a dump of a transparent bridge or squid cache and run the above against every request matching a particular domain over a period of time to get a large sampling of IP networks. The internet is a crazy and changing place but with a few simple tools you can take a bit more control over your network. Note you can do URL based filtering via OpenDNS though unless you trust OpenDNS and can live with the quirkiness of the service then the above option might be more palatable. Either way have fun and explore the whois database yourself to see what you can learn from a seemingly innocuous IP or hostname!

OpenDNS Announces New Services

OpenDNS

The OpenDNS service is an alternative to your ISP's default name servers and has offered many security and filtering features to homes and small businesses. On October 21st, the San Fransisco based company announced it was expending its support and features into the enterprice realm including new features such as MalWare blocking and block bypass to subscribing (as in not free) Enterprise customers. You can read more about this announcement from their press release at **http://bit.ly/3WGd0P**.

SFU No Longer Easy to Use or Find

As Adam mentioned in the last meeting's round table, Microsoft's Services For Unix is no longer easily obtained nor easy to install. For instance SFU is only permitted for use on Windows 7 Enterprise (with Windows 7 Pro being verboten). It is still available to run on the "Server" distributions however. NFSv4 is horribly broken on Windows 7, though Adam also mentioned to me that NFSv3 is purportedly faster than SMB to Samba on the same pair of hosts. More information on this can be found at **http://bit.ly/1x8DwG**.

Sending Us E-Mail?

Due to the amount of e-mail MUUG receives, we've set up an auto-reply to give you jaunty feedback, and redirect some of the e-mail to the appropriate places. Why not look at **http://www.muug.mb.ca/about.html#contacts** first?

Share Your Thoughts

E-mail us with your comments on the newsletter, whether it's criticisms or commendations, and continue to send in articles or ideas for the same. Specifically, what sort of material you would rather see: Announcements, technical articles, new products, or…?

What Do You Think?

If you have a How-To or other idea, and aren't ready to give a presentation at MUUG, an article is a great alternative! If you can write better than the editor, that's terrific; if you can't, submit it anyway and we'll get it into shape for publication. We know that many of you have some great ideas and lots of knowledge. Why not share? Send Mail to: **editor@muug.mb.ca**.