

MUUGLines

The Manitoba UNIX User Group Newsletter

June 2011

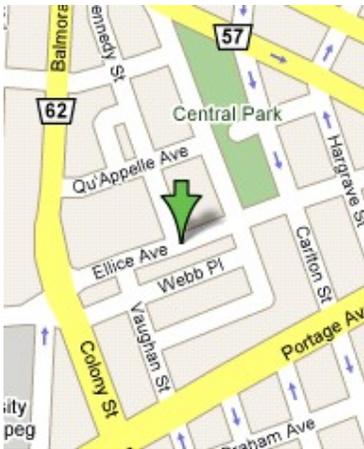
Volume 23 No. 10

Next Meeting: June 14th, 2011

Topic: Practical Security (Sean Cody)

For our last meeting of the season, Sean Cody will be speaking on Practical Security. The term “security” is thrown around quite readily and its meaning has been diluted to being a product adjective as opposed to a process or mind set. This presentation will go over the basic theory of computer security and will attempt to equip you with the knowledge to properly evaluate computer security, products and mitigation strategies.

Where to find the Meeting



Meetings are held at the IBM offices at 400 Ellice Ave. (between Edmonton and Kennedy Streets). 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 Meetings

September 13th, 2011

We'll start the 2011/2012 year with our first meeting on Tuesday, September 13th. Stay tuned (and make sure you're subscribed to one of the mailing lists) for details on that month's presentation.

Linux Kernel 3.0-RC1 Announced.

As originally noted in a posting by Linus (<http://lwn.net/Articles/445222/>) the Linux kernel branding is jumping a few points to 3.0.

No, marketing firms aren't searching for a new internet buzzword. The kernel major revision number is getting renumbered to 3. Linus explains the reasoning for the jump as “I can no longer [sic] comfortably count as high as 40.”

No big changes are actually expected. As usual, there will be some driver updates and random fixes. Code regarding VM's and VFS has been cleaned up some as well. Duplicate code and out-of-tree patches for ARM architecture has been improved somewhat, and will be ongoing.

The goal is to have a “nice stable 3.0” release instead of aiming for typical problems that plague a .0 release – sure and steady.

Red Hat Enterprise Linux 6.1 Released May 19

RHEL being a staple for Linux installation in the enterprise has shipped their next point release of the version 6 product line.

Updates listed:

- Additional configuration options for advanced storage configurations with improvements in FCoE, Datacenter Bridging and iSCSI offload, which allow networked storage to deliver the quality of service commonly associated with directly connected storage
- Enhancements in virtualization, file systems, scheduler, resource management and high availability
- New technologies that enable smoother enterprise deployments and tighter integration with heterogeneous systems
- A technology preview of Red Hat Enterprise Identity (IPA) services, based on the open source FreeIPA project
- Support for automatic failover for virtual machines and applications using the Red Hat High Availability Add-On
- Integrated developer tools that provide the ability to write, debug, profile and deploy applications without leaving the graphical environment
- Improvements to network traffic processing to leverage multi-processor servers that are getting increasingly common

For those not familiar with IPA, “Identity, Policy, and Audit” suite is similar to Novell’s Identity Manager and Microsoft’s Active Directory.

Gmail Gains Two Factor Authentication

A Gmail account can now use a new authentication scheme referred to as two-factor authentication. Basically two-factor authentication is composed of tokens matching something you know (account password), and something you have (such as a generated authentication code on a mobile device). Users can now have Gmail send them the authentication code via SMS or install an app on their Android, Blackberry, or iPhone to generate the code themselves.

You have the option of your machine remembering the verification code for 30 days. You can also set up one-time, application-specific passwords to sign in to your account from non-browser based applications

that are designed to only ask for a password.

If you feel comfortable with giving Google your cell phone number, you can turn on “2-step verification” in your Account Settings – click on your email address in the upper right when logged into Gmail.

Pcc 1.0 Has Been Released

“*pcc*” is a BSD licensed C-Compiler that has been gaining some popularity and attention in the past year. Not to be confused with the CLANG project. The recent work on *pcc* was funded by the BSD Fund and the focus was on optimizing the compiler (already noted for its performance) and having it be able to self host on and compile the kernels (and userland) of the BSD’s. This release can now build the userland and kernel of FreeBSD, NetBSD and OpenBSD base systems with the Linux kernel compatibility being targeted next.

pcc has been around since the 1970’s, but now has been released with AMD64 support and improved GCC compatibility, thanks to the BSD Fund and *pcc* maintainer Anders Magnusson. Future plans are noted:

With a little more help, pcc should run on the key mobile platforms we all carry today. Portability never goes out of style and pcc’s permissive licensing makes it attractive to the widest possible audience.”

Carriers and vendors are unlikely to support this, but persistent programmers and hobbyists seem to live by the motto “void your warranty.” We can count on seeing some interesting applications in the future!

OpenBSD 4.9 Released

With little fanfare, OpenBSD 4.9 was released on May 1st. The theme art of the release is modelled after the “Hitch Hiker’s Guide to the Galaxy.”



The highlights of the release include:

- NTFS (read-only) enabled by default in GENERIC kernel.
- vmt(4) driver enabled by default for VMWare tools support as a guest (this is a big deal for those wanting to utilize and manage OpenBSD VM hosts).
- Lots of usual work and improvements to the network stack and pf(4) firewall code.
- Re-audit and validation of the IPsec code (given the “scare” of a back-door which so far has proven to be FUD).
- Mandoc replacement for groff and friends finally considered stable and part of the release. For more information on this check out the BSDTalk podcast (#204) with the authors of this tool (<http://bsdtalk.blogspot.com/>).

OpenBSD’s IPsec Backdoor FUD Is Just That...

A huge bit of media hype surrounded an implication by one Gregory Perry that authors of part of the IPsec implementation for OpenBSD was subverted with back-door code sponsored by the FBI. While preposterous, Theo de Raadt made the accusation public and launched an effort to either validate or re-audit the code in question. The reputation of OpenBSD and its security & licensing morals are what blew this out of proportion, but since every accusation must at least be investigated, the media made a big deal out of what ended up being nothing.

Mikel King has assembled a bunch of articles, the original complaint and disclosure, as well as many other posts on this topic. The articles range from well-thought out to absolutely insane, but a good read nonetheless...

<http://bsdnews.net/index.php/2010/12/17/bsd-and-the-fbi-sponsored-ipsec-backdoor-yawn/>

Ubuntu 11.04 Natty Narwhal Exposed

There has been a ton of press on the radical changes Canonical is taking on the distribution of Ubuntu 11.04 (including an article in last month’s newsletter). The chief criticism is in the replacement of the GNOME desktop with Unity. Some people really like it and many “old-school” despise it, but you have to give a nod of respect to Canonical for trying something different.

If you are moving to this release there is a nice post by Manual Jose going over and linking to a bunch of useful tidbits on what has changed and how to make best use of the new features of this release.

You can check out his post at <http://www.techdrivein.com/2011/06/everything-you-need-to-know-about.html>.

Oracle to Hand Over OpenOffice.org to Apache Incubator

Ever since Oracle acquired Sun, there have been rumours and posturing over the future of OpenOffice.org. Like the botched handling of MySQL, the community of users was very wary of Oracle’s embarrassment of the popular product and many members of the community jumped ship and forked the project as Libre Office.

Since then, Oracle has proposed that the OpenOffice.org IP be “donated” to the Apache Foundation as part of its Apache Incubator project. Should this proceed, it would definitely solidify the licensing and availability of the product (using both LGPLv3+ and MPL licenses) and allow for continued OpenSource contributions while maintaining a commercial-friendly status.

Network World has posted a good summary article on this proceeding and announcement at: <http://www.networkworld.com/community/blog/oracle-proposes-openofficeorg-apache-incubato>.

A Simple Yet Effective “First Step” in Locking Down OpenSSH.

OpenSSH is the de-facto SSH implementation in use by almost every product offering an SSH implementation/feature. Over the past year, there have been increasingly aggressive attempts to brute force accounts on SSH daemons addressable over the internet. These attacks are generally referred to as “Hail Mary” brute-force attacks. There are many ways to reduce the effect or frequency of attacks, but a sure fire way to mitigate the attack is to turn off password authentication on the daemon on external/public interfaces and only allow key-based authentication. Doing this selectively isn’t obvious from the standard installation or sample configuration files, so Michael Lucas (of Absolute OpenBSD/FreeBSD fame) has written up a small article on how to do this, which you can get at <http://blather.michaelwlucas.com/archives/818>.

Another techniques is to packet filter “known miscreants” from even knocking on the port by blocking “known offenders” with the SSH blacklist provided by the folks at **OpenBL.org** (formerly **sshbl.org**). These folks host a number of SSH servers listening and detecting brute force attempts and puts them in a frequently updated list that can be injected into your packet filter (in a “black hole rule”) or by TCP wrappers via **host.deny** files. You can check them out at <http://www.openbl.org>.

Either technique by itself is great, but both together provide a very strong defence to this increasingly annoying attack vector.

“The Cloud” Isn’t Always Fluffy and White...

Just when you thought the DropBox debacle was simmering down, Colin Percival (of FreeBSD Security Officer & Tarsnap fame) took a deeper look at the Jungle Disk service’s code release. His conclusion is that the folks at Jungle Disk made the distinct decision to focus on ease of use rather than security. The key problem is in how Jungle Disk’s client encrypts their stream and completely avoids message authentication. It also has credential

management issues. All of these vulnerabilities would be entirely hidden from users, but thankfully there are studious folks out there like Mr. Percival who are auditing these services. If you want more detail about these issues, check out Colon’s blog post on the topic at: <http://www.daemonology.net/blog/2011-06-03-insecurity-in-the-jungle.html>

A Free BSD-Focused Magazine

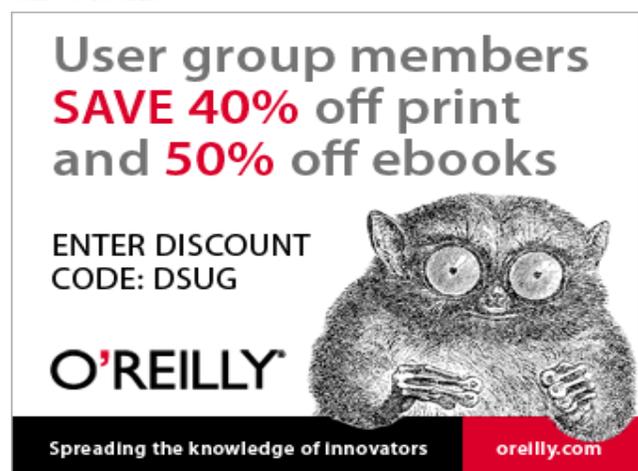
In the same vein as Linux Journal, there exists a nice BSD-focused magazine that just happens to be free! The articles are well written, come from BSD community members and covers all of the BSD’s (relative to article submissions). This month’s issue concentrates on NanoBSD and ALIX, though also has a nice article on OpenSSL.

Aside from an annoying “requires email address submission.” the magazine is free to download in PDF format. Check it out at <http://bsdmag.org>.

Inject Some Magic Into Your CLI

There are at least a few members in this group that delight in completing a crazy amount of work in a single command line. Many CLI tools are under-used and under-appreciated, but some of us go to ridiculous lengths to string along tools to do all kinds of repetitive tasks that make perl code look readable.

There is a really cool twitter feed which focuses on CLI tricks named **@climagic** (<http://twitter.com/climagic>) and while most of the tricks focus on Linux shells, there is a lot of good stuff to learn.



User group members
SAVE 40% off print
and **50%** off ebooks

ENTER DISCOUNT
CODE: DSUG

O'REILLY

Spreading the knowledge of Innovators oreilly.com

The advertisement features a woodcut-style illustration of a beaver wearing glasses and holding a pencil, positioned to the right of the text. The background is white with a black footer bar containing the O'Reilly logo and tagline.