MUUGLines

The Manitoba UNIX User Group Newsletter

Volume 26 No. 7, March 2014

Editor: Trevor Cordes

Next Meeting: March 11th, 2014

RTFM and presentation:

FreeNAS enables users to build network-attached-storage (NAS) on nearly any hardware platform. The FreeNAS project and software were founded in 2005 on the principle that network storage be made available to the world at no cost and unencumbered by license restrictions.

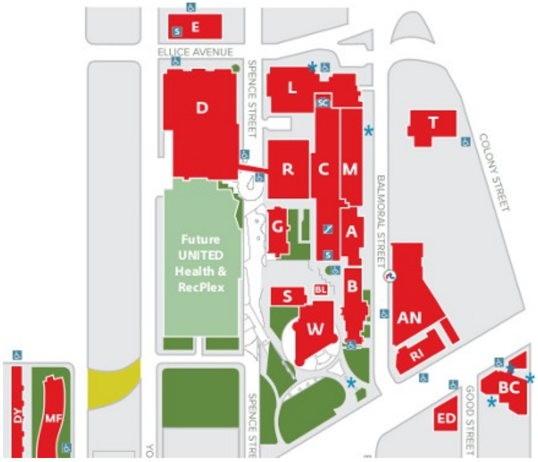
FreeNAS provides a solid service platform based on FreeBSD and includes such features as replication, data protection, backups, encryption, snapshots, file sharing and a plug-in architecture.

Kevin McGregor will present an overview of these features and his experiences with implementing some of them.

For this month's RTFM topic, Adam Thompson will talk about quoting special characters in shell input.

Where to Find the Meeting

University of Winnipeg Lockhart Hall (marked "L" on the map), on the south-east corner of Spence and Ellice. Parking is available on the surrounding streets. Meetings are normally in room 1L08, but occasionally are relocated to nearby rooms. If there is a change, it should be conveyed via a sign on the door to 1L08.



MUUG Mugs!

Back by popular demand! MUUG now has new coffee mugs, laser-etched with our age old, lovable logo for sale for $15 cash. There are a limited number available, so get yours at the next meeting!

A Decade Of Fedora

fedora 20

The latest Fedora is out! Fedora 20, was released on the occasion of Fedora's 10th anniversary. It was in 2003 that Fedora Core 1 was released to fill the void left by the withdrawal of RedHat's Free-As-In-Beer products.

Sadistic Trolls

A recent Canadian study has found validity in what we all have heretofore suspected: those pesky trolls common to website comment forums actually are, in many cases, sadistic psychopaths.

Trolls are people who purposely post inflammatory comments, usually with abysmal signal-to-noise ratios, that go against the predominant views of a site.

The study found that "people who like to troll are also likely to show signs" of "sadism, psychopathy, and Machiavellianism".

http://tinyurl.com/nskk3a4

http://tinyurl.com/pe4kqe5 (requires paid access)

Linksys Routers Wormed

Several of the Linksys router models sold in the last five years or so are vulnerable to a worm dubbed "The Moon". The models affected are all in the E-series. The venerable and popular WRT-series does not appear to be vulnerable.

The worm exploits an open administration port 8080 to obtain details of the router and then sends a crafted request that launches a shell script that downloads the remainder of the worm. The flaw in the router that makes this possible is that it does not check the validity of the passed-in admin password: it accepts any random string.

To be protected, you should update your firmware if possible and/or disable remote management and reboot the router.

http://tinyurl.com/lxuxzgn

Video Of The Month

Is Facebook defrauding paying customers? An interesting amateur investigative report with over 1.5M views offers a look at the practice of "paying for likes", whether via shady third parties or, surprisingly, Facebook itself.

Never heard of "click farms", or perhaps as we should now call them: "like farms"? Watch the video and decide for yourself if all is not kosher at Facebook, especially before you spend your business dollars on a service which may harm, not help, your bottom line.

http://tinyurl.com/p7vaesp

Systemd Story Of The Month

For Fedora and ArchLinux (and soon to be foisted upon RHEL and CentOS, amongst other) users, systemd, the init/upstart successor, now does Yet Another Weird Thing I'm Not Sure Is Good (YAWTINSIG): by default it transparently gives each daemon its own private /tmp space.

This author has not been able to figure out by what mechanism it achieves this, especially the transparent-to-the-daemon aspect. It is clear that it is creating per-daemon subdirectories in /tmp and then somehow changing the daemon's idea of where /tmp is.

On the one hand, this is a great idea as it effectively eliminates the age-old temp file race condition exploit that still occurs to this very day. Lazy programmers often create temp files with fixed names. A malicious local user could utilize this flaw to create a bogus symlink of the same name, leading to all sorts of possible mischief.

On the other hand, it makes it difficult or impossible to have two daemons "meet up" for IPC (i.e. with named pipes) where the fifo file resides on /tmp. It also makes it difficult for someone debugging to find debug files they may normally write out to /tmp: one must first figure out which randomly-named subdirectory contains that daemon's /tmp.

Supposedly there exists an option (PrivateTmp=false) you can place in a systemd .service file that disables this behaviour, but this author has found that feature to currently be broken.

Fedora 20 Oddities

The latest Fedora marks a first in the RedHat bloodline: by default no MTA is installed. Up to this point, sendmail has been installed by every RedHat/Fedora installer as the default MTA. Of course, it will still be installable as an extra package.

The decision to exclude an MTA is "in the interests of paring down services that are generally not used on desktop systems". Though one will wonder how the myriad of daemons and command line programs that expect /bin/sendmail and /bin/mail to do something will behave when they don't exist or don't have any MTA to talk to.

Perhaps more surprisingly, Fedora 20 also excludes *syslog by default. Instead, systemd's "journal" takes over logging duties. YAWTINSIG. You can still easily install rsyslog to achieve the old behaviour.

Acoustic Vulnerabilities

Ever had a modern computer open and noticed that you can hear different high-pitched sounds depending on what tasks the computer is performing? It turns out those sounds may be leaking your privacy and security.

Researchers have discovered a way to capture RSA keys (even 4k ones) used by GnuPG from laptops using nothing more than a microphone placed within four meters, or even a mobile phone adjacently placed. It takes about an hour of audio capture, but considering the ease of which one can get a phone or mic. within the required distance, one should not discount this new snooping method.

GnuPG itself closed this particular hole by adding "RSA blinding" during decryption in the 1.4.16 version. How other programs will be affected or react remains to be seen.

http://tinyurl.com/7xl79ck

M-DISC: The Unknown Media

Take a close look at your DVD-RW drive. One of the logos you will may notice is a little *M@DISC*. This little-known product is *Millenial Disc*, a write-once technology supporting DVD and Blu-ray formats.

The raison d'etre of M-DISC is longevity. Whereas cheap optical media is reputed to last around 5 years, and better media 10-15 years, M-DISC is designed to last 1000 years.

It achieves this by using a "single inorganic recording layer" as opposed to a separate dye and reflective layer. It also uses a higher-powered laser.

Recorded discs are readable on standard, non-M-DISC drives. Blanks are substantially more expensive than normal: currently at around $65 CAD per 10-pack.

Sharing screen Screen

Did you know you could share a terminal screen with another user, even over the network? Perhaps you want to work on a problem with a friend over the phone. Achieving this is super easy. First, make sure both people are logged into the computer to be used (i.e. with ssh) as the same user. In many cases, for admin tasks where both users are trusted, this could be root. Otherwise, a third, shared account could be added to the system. Make sure *screen* is installed; use your favourite package manager.

You run:

```
screen -S foo
```

where **foo** is any identifier you choose to name this session.

The other user runs:

```
screen -x foo
```

using the same identifier you chose in the previous step.

Both users now see the same terminal session. Both users can type. Somehow screen reconciles any differences in terminal column/row sizing and things "just work".

The icing on the cake is that venerable screen has been able to do this for decades! GUI? We don't need no stinking GUI (to paraphrase the popular cinema quote).

Email Password? No Way!

A rant by Trevor Cordes

You probably have noticed the odd and disconcerting request some websites and apps have made for your email address and password. Distressingly, this is becoming more common, and numerous massive sites such as Facebook, LinkedIn, Google, Yelp, etc, are doing it. Even more distressingly, not many people are noticing or ranting about it, not even the Usual Suspects such as the EFF.

What I'm talking about specifically is unrelated third-party sites asking for the keys to your email account. For example, Yelp asking for the credentials to your Gmail account. They do this ostensibly to find out who your contacts are, and what things you like, so they can auto-populate your friend lists and such.

These sites have no business accessing your email account, let alone even asking. I have no idea when this practice became acceptable, nay standard, as part of every big site's normal registration procedure. I find it disturbing that its prevalence is growing. I find it disquieting that such companies make it **appear** completely innocuous, risk-free, mandatory and beneficial. Doubtless many billions of non-savvy users have been duped into complying.

Old hands likely instantly recognized the danger of such practices and no doubt declined. For those yet convinced, consider these points, as highlighted by kindred spirit Jeff Atwood:

1. Such credentials are the "de-facto master password for your online identity". For instance,

almost every site allows you to reset your password via an email sent to your email account. If a third-party has access to it, theoretically it could gain unauthorized access to nearly any website you visit.

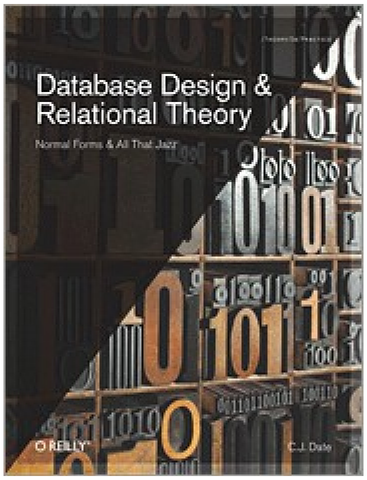
2. Your emails are a “treasure trove” of personal information, identifying your interests, hobbies, habits, etc. If you value privacy in any way, shape or form, you would think twice before fulfilling these dataminers’ wildest dreams. And, is the NSA listening?
3. How do you “know they’re not going to store [your] email password, perhaps insecurely, in a place some disgruntled programmer or hacker can eventually get to it”? Given how companies leak credit card data to hackers by the millions on a regular basis, do you really trust them to safeguard your password?

Think twice before you acquiesce to these email credential requests. Educate your less-savvy friends of this clear and present danger. Make a stink about it to the companies who continue this abhorrent practice.

http://tinyurl.com/mz8r6wr

Book Review: Database Design and Relational Theory by C.J. Date (O’Reilly)

by Trevor Cordes



As a person who uses, administers and programs databases every day, I eagerly anticipated *Database Design and Relational Theory*. Having also taken Database Theory in university, and therefore having a priori exposure to normal forms, I thought this book would be a breeze.

While billed as a book to “bridge the gap” between theory and practice, I found it heavily geared towards the theorist, or at least the academic. In fact, it is far denser than any database textbook I had previously been exposed to at the university level. As such, it is definitely aimed at those at the advanced/expert edge of database use. With frequent identification of axioms and proofs, one may be forgiven for thinking they were reading a math text.

Though not explicitly stated in the book, I would strongly recommend brushing up on database theory with other, intermediate-level books prior to tackling this one. In particular, it would be useful to read C.J. Date’s other books, which he frequently references and draws concepts and acronyms from. In fact, he admits in several places that terminology, etc, is not standardized across the field and literature, and so several quirks are unique to him. For example, I found this book lacking any firm definition of FD and JD’s and how one would go about identifying them. These two concepts are critical to the entire book and as such should warrant a brief refresher.

The chapters are well organized, roughly counting through the 5 + BC normal forms. The examples are illustrative of the concepts and are generally followable, even for the database layman. Each chapter is followed by many challenging exercises and answers are provided at the back.

For what I do in my daily database life, this book was of limited use, as by the end I had discovered two things: one, I generally had already been using the “best” normal form for the job by virtue of experience and common sense; and two, I had only achieved a moderate grasp of the concepts presented in the book even after an above-average duration devoted to each page.

If I could influence one thing regarding future edition changes, I would recommend adding a chapter on applying the theory to the real world. Alternatively, each chapter could include a similar addition to illustrate the concept just introduced.

I would recommend this book only to very advanced users, students, and readers who have already mastered the concepts found in simpler books.

Thank you to O’Reilly Media for their kind donation of this book to MUUG. It was given away as a door prize at our January meeting.