MUUGLines

The Manitoba UNIX User Group Newsletter

April 2008 Volume 20 No. 8

Next Meeting: April 8th, 2008

Demonstration of the OLPC XO Computer

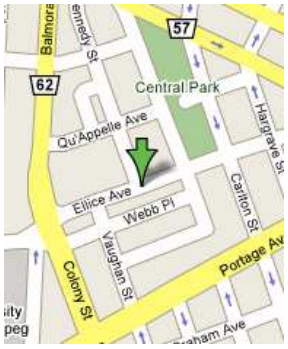
There will be a demonstration of the One Laptop Per Child (OLPC) computer at this month's meeting. This laptop is meant to be a low-cost, perhaps $100, computer to be used by students in third-world countries. It is being developed by an organization headed by Nicholas Negroponte (from MIT) and, in his words, "It's an education project, not a laptop project."

Several members of MUUG bought laptops under the G1G1 (Give One, Get One) program, and this will allow us to demonstrate them at the meeting. If you happen to have one of these laptops, please bring it along and we'll set up a meshnet.

Here is a brief description of the laptop: it is really small (25cm by 23cm by 3 cm) with a high-impact plastic case and a membrane-covered keyboard. It looks like it came from Toys-R-Us! The release catches for opening the display are actually two antennae that allow wireless access. The display itself is surrounded by two speakers, two microphones, a camera, as well as power, battery and activity buttons. On the edges of the display are three usb ports, audio in and headphone jacks. There is also provision to install extra memory using an SD card.

There is a variety of software that comes with the laptop. It includes a web browser (which also reads PDF's), a python interpreter, and programs for creating audio and video files. It also has journaling software that is user-accessible. This acts like a history that allows the user to jump back to a previous session. There is an installed window manager (called *sugar*) that is really different from what we are used to on a Linux machine. In addition and not surprisingly, the laptop comes with yum; there is a huge repository of files that may be transferred to this laptop.

Where to find the Meeting



Meetings are held at the IBM offices at 400 Ellice Avenue between Edmonton and Kennedy (see map). When you arrive, you will have to sign in at the reception desk, and then wait for someone to take you (in groups) to the meeting room. Please try to arrive by about 7:15pm, so the meeting can start promptly at 7:30pm. Don't be late, or you may not get in – but don't come too early either, since security may not be there to let you in before 7:15 or so. Clearly, the suggestion is: Punctuality is appreciated. *Non-members are welcome, but may be required to show photo ID at the security desk.*

Limited parking is available for free on the street, either on Ellice Avenue or on some of the intersecting streets. Indoor parking is also available nearby, at Portage Place, for $3.00 for the evening. Bicycle parking is available in a bike rack under video surveillance located behind the building on Webb Place.

Upcoming Meetings:

May 13th, 2008: TBA

Future meeting topics are subject to change. Please check the MUUG web site for the most up-to-date details.

MUUG Meetings on Google Calendar

MUUG meetings are now listed on Google Calendar! If you're using Google Calendar, you can have these events added to your own calendar. Here's how:

- Log into your Google Calendar/Gmail account
- In a new tab (or window), go to this URL: **http://www.google.com/calendar/gallery**
- Search for the word: **MUUG**
- It should be the first one on the list, so just click the "**Add to Calendar**" button.

These calendar events are maintained and updated by Montana Quiring.

Blocking SSH Probes With Iptables

By Gilbert Detillieux

If you run a UNIX or Linux system that's accessible via SSH on the Internet, one of the recent annoyances you've most likely faced is the swarms of script kiddies using brute-force probing on your SSH port. Even if you don't have to worry about your SSH daemon being vulnerable, or about having accounts with weak passwords, just having to deal with the extra traffic and the clutter in your log files is annoying enough that you'll probably want a solution of some kind.

Some have suggested configurations that limit unsuccessful logins on a particular account before disabling it, but this does little to guard against this sort of probing, and may only result in legitimate accounts being disabled needlessly. Others have suggested installing add-on daemons, such as `sshguard` (**sshguard.sourceforge.net**), to watch the logs, and then dynamically block offending IP addresses.

For Linux users, `iptables` provides a much simpler and almost maintenance-free solution. Simply put the following in your list of `iptables` commands, before any commands that would accept connections on port 22 (SSH):

```
iptables -A INPUT -m state --state NEW -p tcp
  --dport 22 -m recent --name sshprobe --set
iptables -A INPUT -m state --state NEW -p tcp
  --dport 22 -m recent --name sshprobe --rcheck
  --seconds 60 --hitcount 8 -j DROP
```

The first command tags new SSH connections, and the next one will drop connection request if more than 8 of them happen within a rolling 60-second window. (Feel free to adjust the duration or hit count.) If you want to log some of the probe attempts (but not all, since this would generate a lot of the log file clutter we're looking to avoid), you can add commands such as the following, after the previous two:

```
iptables -A INPUT -m state --state NEW -p tcp
  --dport 22 -m recent --name sshprobe --rcheck
  --seconds 60 --hitcount 4 -j LOG --log-prefix
  SSH-REJECT:
iptables -A INPUT -m state --state NEW -p tcp
  --dport 22 -m recent --name sshprobe --rcheck
  --seconds 60 --hitcount 4 -j REJECT
  --reject-with tcp-reset
```

The first command logs connection request if more than 4 of them happen within a rolling 60-second window. (But less than 8, in which case the earlier filter rule will drop the packets.) The last command then rejects the packet with a TCP reset, so the client will know that the connection was refused. (This may be useful as you're testing this out, in case legitimate connections are affected.)

After putting in this sort of filtering, you'll probably want to thoroughly test out your normal use of SSH, to be sure you're not preventing legitimate clients from connecting. Check your logs for rejected connections too, and adjust duration and hit counts if needed. You may also want a filtering rule, before all of the above, to accept SSH connections without restriction from particular, trusted addresses. This

would be useful, for example, if you allow non-interactive, password-less SSH connections (using key exchange) from particular clients, since such connections might occur at a fast enough rate to trigger filtering otherwise.

If you're running a Red Hat or Fedora Linux system, you can put the above lines in the configuration file `/etc/sysconfig/iptables`, without the `iptables` command name, and adjusting the `INPUT` queue name accordingly. (Place them just before the line accepting connections on TCP port 22.) The lines would look something like this:

```
-A RH-Firewall-1-INPUT -m state --state NEW -p
  tcp --dport 22 -m recent --name sshprobe --set
-A RH-Firewall-1-INPUT -m state --state NEW -p
  tcp --dport 22 -m recent --name sshprobe
  --rcheck --seconds 60 --hitcount 8 -j DROP
-A RH-Firewall-1-INPUT -m state --state NEW -p
  tcp --dport 22 -m recent --name sshprobe
  --rcheck --seconds 60 --hitcount 4 -j LOG
  --log-prefix SSH-REJECT:
-A RH-Firewall-1-INPUT -m state --state NEW -p
  tcp --dport 22 -m recent --name sshprobe
  --rcheck --seconds 60 --hitcount 4 -j REJECT
  --reject-with tcp-reset
-A RH-Firewall-1-INPUT -m state --state NEW -m
  tcp -p tcp --dport 22 -j ACCEPT
```

The idea for this came from the following web site: **http://www.teaparty.net/technotes/ssh-rate-limiting.html**. You could also find many similar variations on this theme by searching online for the keywords `iptables`, `recent`, `hitcount`, and `ssh`.

Xen and the Art of Virtual Machine Maintenance

By Montana Quiring

I finally got the nerve up to take another crack at creating some Xen virtual machines. My previous attempt was fraught with all kinds of problems until I eventually ran out of time. This time around I had my share of problems but I am able to give you a Xen tutorial of sorts that someone new to Xen should be able to follow and get up and running in less than one day.

The OS I'm working with is CentOS 5.1. Why not Ubuntu, or Debian, or distro X? I dunno. I guess it drew the short stick. I'm running it on a fairly old x86 machine (1.6Ghz with 1 GB of RAM) that doesn't appear to support hardware virtualization. This tutorial will give you 10 easy steps to help you create a CentOS virtual machine on a CentOS install.

Step 1: Do an install of CentOS 5.1 with at least the Virtualization and Gnome categories checked (Troy, you can install KDE) and then update it so that its packages are current.

Step 2: Patch the "Virtual Machine Manager" so that you have the option to use "Shared physical device" in Step 8. See this URL:

http://bugs.centos.org/view.php?id=2516

NOTE: If you need them, instructions on how to apply it are at the bottom of the web page.

Step 3: Run the "Virtual Machine Manager" under Applications -> System Tools

Step 4: Click the "New" button on the bottom of the window and off we go into the wizard....

Step 5: Work your way through the wizard till you get to the virtualization type page. This tutorial only talks about para-virtualization, but feel free to try "Fully Virtualized" if the option is there and you are feeling adventurous.

Step 6: Now it should ask you for some install media. Enter the following into the "Install Media Field":

http://centos.arcticnetwork.ca/5.1/os/i386/

NOTE: You may want to use a different URL if you are running a 64-bit machine or you prefer a different source.

Step 7: For storage space, I chose a "Simple File", cuz I like simple... and I like the simplicity of backing up a single file. Make sure "Allocate entire virtual

disk now?" is checked off and set the size to give you room to breathe down the road.

Step 8: Now comes the networking. If this is a laptop that you connect to multiple networks, you will probably want "Virtual network". If it's a box that stays put and has a static IP, you can choose "Shared physical device".

Step 9: I'm sure you're planning for your virtual CentOS to have swap space, but make sure to give it enough RAM to function at a decent speed, but not so much that your host OS will grind to a halt.

Step 10: Install CentOS 5.1 in your new virtual machine

That's it. Did you have so much fun that you want to do it again? Go to Step 3!

Want to make a virtual LAMP server? Look here:

http://howtoforge.com/centos-5.1-server-lamp-email-dns-ftp-ispconfig

Happy Xening !

Recent Linux Releases

Waiting eagerly for the Fedora 9 release? Well, you won't have to wait much longer, as the target release date is April 29th, according to the schedule at **fedoraproject.org**. Can't wait until then to try out its new features, such as KDE 4.0.2 (as featured at our February meeting), Gnome 2.22 and Firefox 3 Beta? The Fedora 9 Beta just came out on March 25th.

If Ubuntu is more your style, the beta of 8.04 "Hardy Heron" was just released. The official release is due for around April 24th. Or if the Novell-Microsoft deal hasn't soured your opinion of SUSE, you might want to look at the openSUSE 11.0 Alpha 3 release, also just recently announced.

Looking for something with a smaller footprint? You might want to look at NimbleX 2008 RC, a Slackware-based mini distribution, or PUD GNU/Linux, an Ubuntu-based mini-distro with Xfce.

If you're looking for something smaller still (think Linux on a stick, as discussed at the December meeting), consider Damn Small Linux 4.3 RC1, which has just been released, or Puppy Linux (featured in the April *Linux Journal*), although it hasn't been updated since version 3.01 in October 2007.

Information on all of the above Linux distributions, and more, can be found at **distrowatch.com**.

Sending Us E-Mail?

Due to the amount of e-mail MUUG receives, we've set up an auto-reply to give you immediate 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…?

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**.

Horner's Five-Thumb Postulate:
Experience varies directly with equipment ruined.
(From the "fortune" file)