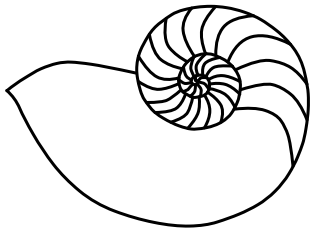
Vol. 15 No. 7 March 2003
$2.50



MUUGlines

The Manitoba UNIX User Group Newsletter

March 11, 2003: Wiki and TWiki

Wiki (http://www.wiki.org/wiki.cgi?WhatIsWiki) is a piece of server software that allows users to freely create and edit Web page content using any Web browser. Wiki supports hyperlinks and has a simple text syntax for creating new pages and crosslinks between internal pages on the fly.

Bill Reid will present a Wiki implementation called TWiki (http://www.twiki.org/), a flexible, powerful, and easy to use Web-based collaboration platform. Use TWiki to run a project development space, a document management system, a knowledge base, or any other groupware tool, on an intranet or on the Internet. Web content can be created collaboratively by using just a browser. Developers can create new web applications based on a Plugin API.

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, and then wait for someone to take you (in groups) to the meeting room. Please try to arrive by about 7:15 PM, so the meeting can start promptly at 7:30 PM. Don't be late, or you may not get in.

Limited parking is available for free on the street, or in a lot across Ellice from IBM, for $1.00 for the evening. Indoor parking is also available nearby, at Portage Place, for $2.00 for the evening.

Linux Server Hacks

Industrial-Strength Tips & Tools from Linux Experts

Once relegated to a lonely back room, the Linux server has earned its place in the enterprise. No longer an eccentric whim, it is now a high performance system for routing large amounts of information through a network connection. The job of the Linux system administrator is to pull all the power and performance out of it that's possible, while not getting lost in the details of administrative tasks. For help with this task, there's basic documentation online, but there is much beyond the basics that a competent system administrator needs to know. The best source for this type of knowledge is from people who have hands-on, real-world experience—people who have worked through the same challenges and found efficient solutions. This is the kind of "know-how" that can be found in "Linux Server Hacks" by Rob Flickenger (O'Reilly, US $24.95).

"Linux Server Hacks" is a collection of industrial-strength, real-world, tested solutions to practical problems. The book contains one hundred independent but related tips, tools, and scripts that solve common but frequently difficult administrative tasks. Some of the hacks are subtle, many of them are non-obvious, and all of them demonstrate the power and flexibility of a Linux system. The book offers hacks devoted to tuning the Linux kernel to make one's system run more efficiently, as well as using CVS or RCS to track the revision to system files.

There are hacks covering alternate ways of doing backups, using the system monitoring tools to track system performance, and a variety of secure networking solutions. "Linux Server Hacks" also includes tips on managing large-scale web installations running Apache, MySQL, and other open source tools that are typically part of a Linux system. Every hack can be read in just a few minutes, but will save hours of searching for the right answer.

"This book is for administrators who use Linux every day, and want to use their systems more effectively," explains Flickenger. "While it contains one hundred directly applicable hacks that solve common but frequently difficult tasks, 'Linux Server Hacks' is also intended to convey a particular methodology to be used when solving technical problems. When properly applied, Linux becomes a powerful and expressive medium in which to create elegant solutions to common problems, all while being educational and even entertaining along the way. This methodology is the hacker's attitude, and is the spirit which drives Linux as a living, evolving solution to technical problems."

Written by experts for intelligent, advanced users, O'Reilly's new Hacks Series have begun to reclaim the term "hacking" for the good guys. In recent years the term "hacker" has come to be associated with those nefarious black hats who break into other people's computers to snoop, steal information, or disrupt Internet traffic. But the term originally had a much more benign meaning, and you'll still hear it used this way whenever developers get together. O'Reilly's new Hacks Series is written in the spirit of true hackers—the people who drive innovation.

On Choosing OpenBSD For A Firewall

Brandon Newport, Appalachian Web Solutions

My partner and I decided to evaluate different firewalls before actually putting anything into production. I have worked as a network and infrastructure security consultant for almost 10 years and have experience with various firewalls like Cisco PIX, CheckPoint Firewall-1, Gauntlet, and Raptor among a few lesser known firewalls. My partner has been a network, systems, and security administrator for 6 years and has worked with Linux, FreeBSD, Solaris, AIX and Windows Operating Systems as well as the firewalls CheckPoint Firewall-1 and Cisco PIX. We both knew that the firewall should be integrated into the system and if it was to be on an operating system, that operating system must be secure and have a good track record for security.

Our requirements were simple, we wanted a industry proven, stable, reliable, and most importantly secure firewall that was relatively easy to manage. We did not feel all these things were asking too much, so we also added speed. The firewall must be stateful, be able to watch for IP Options, Fragmented packets, and other strange anomalies such as port scans, etc. Both of us being comfortable with command line, we did not have a need for the firewall to have a graphical user interface (GUI).

We ruled windows out quickly with all the security issues released, which seems like a daily event. AIX, HP-UX, and Solaris were out of the question because the cost justification did not allow for such expensive platforms (especially being this hosting company was funded by us with no venture capitalist money). While CheckPoint does run on Linux we quickly ruled it out not only based on price but the number of vulnerabilities it has had in the past few years was among the highest of all the firewalls. It seemed as if it was between PIX and Linux running IPTABLES (we eliminated IPCHAINS because it is not stateful), we are familiar with the PIX interface and its strengths and weaknesses. We had someone willing to donate a PIX to us for our hosting company, and we did test it. The cost of maintenance and support was costly and we felt the cost justification for a commercial package was not feasible compared to the level of security that can be reached with an Open Source firewall. The technical merit of using a Cisco PIX was also greatly reduced when attempting to group similar objects. Cisco introduced grouped object into the 6.2.2 code for the PIX. The addition of objects into the groups is extremely antiquated compared to other firewalls that allow you to create group objects fairly easily. One who is familiar with writing basic shell scripts would have no problem creating objects (or variables) in Open Source based firewalls. PDM can be installed onto the PIX which add additional management capabilities via a web browser (and eases the pain of creating groups); however, we did not want to add any additional services to the firewall unless absolutely needed.

While we started looking into IPTABLES, I had used OpenBSD for a couple other projects and discussed with my partner the possibility of trying OpenBSD running PF as the firewall in comparison to Linux running IPTABLES. Both being security minded, a quick evaluation of the facts pointed out that OpenBSD has only had one exploit in over 7 years—very impressive by itself, but that was not quite enough to move that direction. Researching both OSes for quite sometime specifically with security in mind, everything pointed to OpenBSD. Several excerpts from "Building Linux and OpenBSD Firewalls" (Chapter 4) explain why OpenBSD is actually a better firewall than Linux, while the book may be a little dated on the versions of OSes and also limits its Linux distribution to only RedHat it does explain the fundamental reasons for choosing OpenBSD over Linux which is what we were looking for. A well written article at http://www.benzedrine.cx/pf-paper.html by Daniel Hartmeier explains that IPTABLES does not perform sequence number analysis. The sequence

number analysis gives a little added security by reducing the amount of information an attacker knows about the systems. The fact that OpenSSH, OpenSSL and PF were all written by OpenBSD people, also assisted in the decision, but actually testing the firewall proving that it was more than capable of handling loads and still maintaining its composure was what changed our minds.

We implemented OpenBSD 3.1 into our environment and have never thought twice about it. We obviously had to patch a security hole (OpenSSH) and watch for any new vulnerabilities like any good administrator. The upgrade was done using CVS and there were no problems with the update.

While most hosting companies do not implement firewalls and only lock the systems down at the OS layer (or they should if they don't), we did feel like this offers enough protection for our customers. We believe in best practices for security, which is to provide security in layers, the firewall being the first layer for our environment, second being the OS layer of each system, and third being the application level.

[For example configurations and other detail, see http://www.deadly.org/article.php3?sid=20030301141353 –Ed.]

The Desktop Linux Consortium

Responding to the overwhelming interest in Desktop Linux, representatives from key firms and organizations announced the formation of the Desktop Linux Consortium (www.desktoplinux consortium.org), or DLC. The vendor-neutral association will promote interests and raise awareness of the emerging role and benefits offered by GNU/Linux on the desktop. Consortium members comprise both commercial companies and open source organizations that are developing and shaping the technology that will speed the adoption rate of Linux to the desktop.

Formation committee members represent community leaders and firms that are central to Desktop Linux-related technologies. Companies and organizations announcing support for today's announcement include ArkLinux, CodeWeavers, Debian, DesktopLinux.com, KDE, Linux Professional Institute (LPI), Lycoris, The Linux Terminal Server Project (LTSP), MandrakeSoft, NeTraverse, OpenOffice.org, Questnet (Support4Linux.com), Samba.org, theKompany, SuSE, TransGaming Technologies, TrustCommerce, Xandros, and Ximian.

Additional companies will be announced shortly. Membership is open to those companies pioneering Linux and related technologies for desktop computing. Bruce Perens, long time Linux developer and well known open source community leader said, "The Desktop Linux Consortium will assure that there is fairness in all Desktop Linux-related issues and events. All vendors will be fully represented and the open source ethos will be respected."

Linus Torvalds, creator of Linux, said "We already have all of the tools, in Open Source software, necessary for 80 percent of office workers in the world: an office suite including spreadsheet, word processor, and presentation program; a web browser, graphical desktop with file manager, and tools for communications, scheduling, and personal information management. The Linux desktop is inevitable!"

Targeting the needs of corporate, institutional, and home users, the DLC will help shape the future of Linux on the desktop. Open standards, lower licensing fees, proven and reliable technologies, along with a vast worldwide developer base underscore GNU/Linux as the ideal software platform for end-user computing. Group initiatives will include trade shows, conferences, and participation in Consortium-sponsored public relations activities and programs.

Broad corporate participation in the DLC organizational meeting underscores the exploding interest in Desktop Linux. The DLC will serve to facilitate development of common messages on using Linux in personal desktop computing, in governmental systems and in schools to name just a few of the fast-emerging growth areas worldwide.

The Desktop Linux Consortium will be incorporated as a non-profit trade association. Membership is open to companies and open source organizations throughout the world who offer products that support Desktop Linux. Consortium provisions will allow both commercial and non-commercial projects to work side by side in delivering joint messages and programs that promote the adoption of Linux on the desktop.

The ultimate beneficiary of the Consortium is the computing public, which will be assured a vibrant, open, stable alternative to closed propri-

etary systems and applications, interoperability, and an end to ever-escalating licensing fees.

An Epiphany

In the beginning, there was Mosaic. Mosaic begat Netscape, which in turn eventually begat Mozilla. Mozilla was intended to be a smaller, faster version of Netscape, the code to which was said to be very bloated and convoluted. In time, Mozilla, while definitely smaller and faster than Netscape, also began to be perceived as 'bloated'.

Some folks felt something had to be done, and thus Mozilla begat Galeon, which was supposed to be a lean version of Mozilla without all the extras that caused much bloat. In time, certain members of the Galeon project splintered off to go in their own direction: Epiphany (http://epiphany.mozdev.org/). What follows is their own description of their goals.

Epiphany is a GNOME web browser based on the mozilla rendering engine. The name meaning: "An intuitive grasp of reality through something (as an event) usually simple and striking"

Manifesto

A web browser is more than an application, it is a way of thinking, it is a way of seeing the world. Epiphany's principles are simplicity and standards compliance.

Simplicity: While Mozilla has an excellent rendering engine, its default XUL-based interface is considered to be overcrowded and bloated. Furthermore, on slower processors even trivial tasks such as pulling down a menu is less than responsive.

Epiphany aims to utilize the simplest interface possible for a browser. Keep in mind that simple does not necessarily mean less powerful. We believe the commonly used browsers of today are too big, buggy, and bloated. Epiphany addresses simplicity with a small browser designed for the web — not mail, newsgroups, file management, instant messenging or coffee making. The UNIX philosophy is to design small tools that do one thing, and do it well.

Epiphany also address simplicity with modularity to make a light and powerful application. If something can be implemented using external applications or components, we use it rather than wasting resources in the web browser. Integration will be achieved with CORBA, Bonobo, and the ever popular command line. Mail will be handled with your favorite e-mail application (Evolution, pine, mutt, balsa, pronto, whatever).

Standards compliance: The introduction of non-standard features in browsers could make it difficult or impossible to use alternative products like Epiphany if developers embrace them. Alternative (standards complying) browsers could not be able to fully access web sites making use of these features. The success of non-standard features can ultimately lead to forcing one browser, on one platform to dominate the market. Standards compliance ensures the freedom of choice. Epiphany aims to achieve this.

User Interface Guidelines

HIG compliance Epiphany is going to follow version 1.0 of the gnome user guidelines. Unless there are very serious reasons to make an exception not following it will be considered a bug. "I follow the HIG only when I like it" is not a legitimate approach. Any areas where we diverge from the HIG will communicated to the HIG team for future consideration.

Gnome integration Epiphany's main goal is to be integrated with the gnome desktop. We don't aim to make Epiphany usable outside Gnome. If someone will like to, it's just a plus. For example: Making people happy that don't have control center installed is not a good reason to have mime configuration in Epiphany itself.

Simple design Feature bloat and user interface clutter is evil :)

Preferences We will follow the new Gnome policy about preferences. Havoc Pennington already explained it a lot better than we could.

User target We target non-technical users by design. This happens to be 90% of the user population. (Technical details should not exposed in the interface.) We target web users, we don't directly target web developers. A few geek-oriented features can be kept as long as they are non-obtrusive.

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?