Windows vs. Linux: A Comparative Study

One of the many rows of Linux servers at Google's server farm

Presented by:

Joe Cabrera

Technical Writing – N4

Spring 2009

Linux vs. Windows: A comparative study

For:

Dr. Jackie Domingue
Technical Writing Instructor
Blinn College
Bryan, TX

Presented by:

Joe Cabrera
Technical Writing – N4
14 April 2009

27 April 2009

4302 College Main Apt. 377
Bryan, TX 77801

Dr. Jackie Domingue
Technical Writing Instructor
Blinn College
1234 Villa Maria
Bryan, TX 77840

Dear Dr. Domingue:

This is my comparative of study of Linux and Windows on server. The goal of this proposal is to persuade the reader to use Linux on servers that they are administrating. It is written in somewhat technical language yet, it is my desire to greatly simplify and explain the language to non-technical readers. This comparative guide strives to explain the differences to a non-technical user. In addition to providing an in-depth overview of the major system difference, this guide also discusses specific instances when one operating system would be more appropriate for certain tasks.

This guide is directed to any system or website administrator that needs a stable and reliable operating system to run on their server. I recommend Linux for any business, governmental, or educational institution that needs a quality server. It is important to have secure operating system for your server, since your server will only be as secure as the operating system it is running on. After using Linux on my home computer and work server I have come to the conclusion that Linux is the best operating system to be used on server platform and even on the desktop computer of a very computer savvy enthusiast. I used the work server for many tasks including running a Web server and Mail server. I have also been highly involved in the Texas A&M Linux and Unix Group (TAMULUG). All of these applications stem from my interest in computers and electronics that I have had from an early age. With this said I have use have used Windows and MAC OS and can even vaguely remember using DOS in the years before Windows became quite popular.

I have completed this comparison with the aid of several print and electronic resources. I have also drawn on my personal experience and knowledge to further advocate my position. While I realize I may be speaking to an audience that is largely comfortable with Windows, my goal is to help administrators everywhere embrace the need for the Linux operating system.

Sincerely,

Joe Cabrera

Informational Abstract

Linux vs. Windows: A comparative study

This proposal is directly towards business, governmental, or educational institution that needs to implement a quality server. While this topic includes highly technical language, it is the goal of this report to convey the necessary material in a form that is easy to understand for the more non-technical readers. The report contains a glossary of terms that is designed to explain some terms that the average computer user would mostly likely not be familiar with. Several graphics are included throughout the study to provide information and aid the reader in understanding some of the harder concepts.

This report examines Windows and Linux side by side on the following criteria: Cost, Security, Configurability, and User-friendliness. This report will also examine specific instances when each operating system might be the more suitable choice for the task at hand. After reading this proposal, I hope that the readers will have gained a more informed knowledge of the differences between both operating systems as they relate to a server platform.

Table of Contents

Page

Figures

Glossary

UNIX - first truly portable computer operating system designed at AT&T Bell Labs by Dennis Ritche and Ken Thompson in 1969. Linux shares many similar characteristics with UNIX and both are “nix” systems

Server - in the strictest sense is a computer that accepts requests from clients. In the context of this document a Web server accepts HTTP requests from clients.

C language - low-level multipurpose computer programming language developed in 1972 by Dennis Ritche while he was working at AT&T Bell Labs. It was originally used to develop the UNIX operating system.

DoS - Denial-of-Service attack. Attack that attempts to make a computer resource unavailable to users with legitimate access.

GUI - Graphical User Interface. Used to describe the graphical interface the user uses to interact with the computer. It usually offers icons and visual items are opposed to a text-based interface which usually only handles and returns text input.

RPC - Remote Procedure Call. This call allows a computer program to run in another address space, commonly another computer on the same network. This allows programs to be remotely executed without the programmer specifically stating who will call it.

SQL - Structured Query Language. It is a database computer language that aids in the revival and management of data stored in large databases. It was first developed in the 1970s by Andrew Richardson of IBM.

MySQL - An open source Database Management System that is written in C and is cross platform. It is used by many as a free and open source alternative to SQL

IP address - Internet Protocol address. Logical address used by computer and other similar devices for identification on a computer network. The current and most widely used Internet Protocol Version 4 (IPv4) uses 32-bit numbers.

Port - In the case of computer network, a port is program specific software device that allows the program to receive and send network communications at one central point. Most applications or services have a specific port that they will listen and transmit on.

Protocol - a standard set of rules used for data transmission, error detecting, and signaling on a specific communication channel.

Active Directory – database system created for Windows to provide several network services including LDAP services, Kerberos-based authentication, and the DNS naming system

Domain Controller – On a Windows based server system, it is a server that responds to security authentication request including those used by the LDAP database.

Introduction

Linux and Windows are two operating systems that are constantly competing from control of the computer market. Both operating systems have shown considerable growth in the server world. Microsoft released its first server OS in 1993 under the name Windows NT, just about the time that the Linux OS began surfacing on the internet. Since then Windows servers and Linux servers began growing by leaps and bounds. Many servers that were run by UNIX began converting to Linux, a trend that would continue into the early twenty-first century. Windows NT use began growing largely due to the fact that NT introduced the first 32-bit implementation of the Windows API. An API includes the protocol, routines, and libraries needed for application building. By 2000, Windows and Linux each controlled roughly half of the overall server market. The Linux side contained such as NetWare, BSD, and Debian-based Linux. However by 2008, Windows controlled 38.8 percent of the overall server market share compared to Linux's 12.7 percent. However this data is based on total revenue of both servers and most Linux server software distributions are free and sales are rarely documented. As of 2009, five of the top ten most reliable servers ran Linux, three ran FreeBSD, and only two ran Windows. Some examples include Google, Yahoo, YouTube, and Facebook and key governmental agencies such as the US Army. Linux is by far the choice of operating system for many major websites. One of the few major website I could find that ran Windows was by no surprise windows.com. In many peoples' minds Linux is the only opinion for quality web servers, but for others nothing is easier than the "point and click" allure of Windows. Ever since 1993, Linux and Windows have both attempted to gain control of the server market. There are many advantages and disadvantages to both operating systems in the server world.

Server Market Share

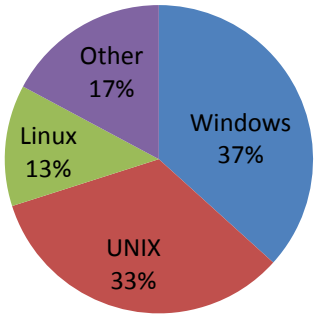


Figure. 1 Pie Chart

The purpose of my report is to examine the key differences between Linux and Windows and how these differences can affect the potential use of each server. There are several key areas in which I would like to compare Linux and Windows. These areas are cost, security, configurability, and user friendliness. In will also examine particular instance were each operating system would be more suited for specific tasks. My audience is any computer administrator that needs to implement a quality and reliable server.

Cost

The newest version of Windows server software, Windows Server 2008 Standard, retails in the United States at $999 and includes five Client Access Licenses (CALs). A Client Access License is a type of software license that allows client computers to connect to Microsoft server software. Windows Server 2008 and 2003 require one CAL form each concurrent connection. To illustrate this, take for example that a business network has computers that are used by 10 people. However of this computer network there are never more than five people using the server software at one time. Then the business would only need five CALs. CALs can be use by either users or devices; devices could include kiosks or shared computer systems. While this option may be affordable for small businesses with limited technical

support, but it would become quite expensive for many large businesses and corporations. Windows also markets their more extensive Windows Server 2008 Enterprise edition to larger businesses in need of server software with larger scalability. The Enterprise edition also includes 25 CALs and is priced at $3,999, but also can handle more application demands than the Standard edition can.

Linux on the other hand is completely free. It is licensed under the GNU General Public License which allows for the free distribution of the Linux source code. Anyone can modify the code to suit their specific needs as long as the code is never sold for a price. However it is also important to note that many companies provide subscription-based support for Linux at a nominal fee. Red Hat, of the many companies that provide Linux support, offers Red Hat Enterprise Linux with a basic support subscription for $349 which includes Web support, 2 business day response, and unlimited incidents. The hidden cost in Linux lies in its support and maintenance. In an Analyst report by Hewitt Consulting, it is stated that "Over time, it is generally agreed that Linux talent supply will increase" and due to this "not only will Linux talent hiring be challenging, but Linux costs will rise." It is no surprise to note that this report was commissioned by Windows and is prominently displayed on their site comparing Linux servers to Windows servers. Windows also emphasizes that Windows Server reduces the Total Cost of Ownership (TOC). However once a Linux server is properly installed and tailored to your needs, it is significantly more cost efficient to maintain in the long run. The chief technology architect at Merrill Lynch & Co. is quoted in ComputerWorld for stating that "the cost of running Linux is typically a tenth of the cost of Unix and Microsoft alternatives" (Greene). The head technician at oil company Amerada Hess manages 400 Linux servers by himself.

Security

Windows servers are based off the Windows kernel and are thus susceptible to many of the same security threats as any normal Windows operating system. To understand this it is important to

user stand some of the history of Windows. Windows was originally designed to be a single user operating system and when it was first released had no networking capabilities. Prior to the release of Windows NT, Windows only offered one category of users that could do anything. Prior to Windows Vista, the first user account created during the Windows setup process is automatically a member of the administrator group. Most users never changed to an account with fewer rights, thus giving malicious programs full access to the system. It was not until Windows Vista that Microsoft finally addresses this issue and created User Access Control (UAC). In Vista all logged in sessions including administrator users run with standard user privileges and actions that require administrator status to operate must use UAC. UAC picked up on the principle of least user access that UNIX has used since it was first created. The principle of least user access allows every module (user, process, or program) to only access resources that are necessary for its legitimate purposes. UAC assigns tokens to each user that logs on, but only assigns administrators tokens to members of the Administrator group. In the second half of 2005 alone there were 11,000 malware programs discovered for Windows. Windows has also become susceptible to botnets. Botnets are a network of infected computers that are controlled by malicious persons and have commonly been used to stage massive DoS attacks. Microsoft claims that its Windows Server 2008, just like did with Windows Server 2003, is secure by design. Windows Server 2008 included many features for hardening all of its services including the use of Active Directory to authenticate users. Windows's closed source approach only allows Microsoft employed programmers to fix bugs. Microsoft continues to claim that closed source offers a faster and more effective response to security issues or bugs. However major fixes and patches are only released once a month after extensive programming and testing. It is common for specific bugs and security issues to go unpatched for several months.

There are many flaws in the Microsoft design that make it more vulnerable to security attacks. Many people falsely believe that Windows is the primary target of security problems and viruses simply because it has the largest market share. However this reasoning is strongly defeated when "According to

the September 2004 Netcraft web site surveys, 68% of all websites run the Apache web server. Only 21% of web sites run Microsoft IIS." Using this logic one would concluded that Apache web server is more susceptible to attack, however this is not the case. The massive Code Red Worm that was released in 2001 targeted Microsoft's IIS web server and defaced many servers worldwide. While both IIS and Apache are equally vulnerable to attack, it is important to understand that your web server is only as secure as the platform that is running. If an attacker can gain administrative privileges on an OS, it is relativity easy to take control of the web server it is running. With Windows's many underlying security flaws it is thus plain to see why IIS web servers are usually compromised with greater success.

The Linux model for security traces its roots back directly to UNIX, which was the first multi-tasking and platform portable computer operating system. Here it is important to understand the history of the UNIX operating system to fully see the reason why UNIX and therefore Linux are very secure. When UNIX was created computers were only available in large institutions such as universities and key government research facilities. It was too expensive to maintain a personal computer and many of the early computers took up entire rooms and contained as much processing power as our modern day calculators. Most computers during this age contained vacuum tubes and data was stored on punch cards. Thus Ken Thompson and Dennis Ritch, creators of UNIX and the C language, developed the idea of time sharing and used it for their first operating system, UNIX. UNIX was created to harness the new found computational powers of the world first computers and divide its processing power equally between users. With the development of the modem it also allowed users to for the first time in history to remote connect to computers and access these resources from a home terminal. UNIX from the beginning separated administrator privileges from those of the normal user, something that Windows did not implement until they realized that people would actually be using their operating system for more than one user. The UNIX operating system also utilized the first encryption methods to be used on computers and developed a system that allowed computers to secure communicate with each. Since the

first computers networks linked these large computers together, it was necessary to ensure security across the network and ensure that data packets got to their intended destinations. The Linux operating system has inherited all of its security measures and design from UNIX and has even in many cases added to it.

The UNIX operating system divides control between normal users and a one superuser, known as root. All users by default when they login onto the system begin as normal users and then can become the superuser if they know the correct password. This prevents a novice user from accidently making a system-wide change that could bring the system to a grinding halt. It also protects a normal user from making any destructive changes to the system that could jeopardize the use by other users on the system. In the UNIX system, every file and process belongs to a specific user and a specific group. Every file has specific permissions for the owner, group, and others that include read, write, and execute access. The root user can execute any file with execute permission and read, write, and modify any file on the filesystem. This model ensures that only the correct people have access to files and commands. Since major system changes can only be accomplished as superuser, it makes it very hard for anyone to cause destruction to a system without sufficient privileges. While it is still possible for an attacker to exploit a kernel security hole, with thousands of people worldwide contributing to the code it is possible to fix a security hole in a matter of usually hours. On the other hand, it might take several months to fix a security hole in Windows. With the case of the Code Red worm that attacked IIS, Microsoft released a fix to patch the hole, but many server operators were slow to patch the system and thus the next wave, Code Red II was also very successfully. Microsoft's own servers were not immediately updated and thus Microsoft once again fell to the next round of the attack. Thus represents a case were the system administrators did not act quickly to patch the system when holes were known to exist and fix even existed.

The modular design of the UNIX operating system makes it greatly more stable than Windows. UNIX is a text based system that does not require an additional GUI to function and thus will not fail if your computer has a bad graphics driver. Even though many Linux distributions included a GUI, Linux can always drop down a text-based system if the GUI fails for some reason. While Windows requires reboots after system, driver, and sometimes occasional program updates, Linux only needs to be restarted for kernel updates. Using a special system utility it is even possible to load a new kernel and execute it without a hardware reset. Linux relies on no specific web browser or email program and thus a flaw in a particular web browser will not cause damage to the entire system. While the kernel supports many modular drivers, the kernel for the most part is monolithic where services are tied closely together (Petreley). However, Linux runs under the view that "Whenever a task can be done outside the kernel, it must be done outside the kernel" (Petreley). This is in strongly contrast to Windows that forces graphic drivers to run in the kernel and thus one bad graphic driver can bring Windows to a screeching halt.

Linux also does not rely on the RPC model, which commands another program to do something that can be run from a remote machine (Petreley). On a Linux system it is possible to disable all RPC related services and still maintain system functionality. MySQL for example is by default setup to not listen to the network, whereas SQL always listen. Most Linux applications skirt around this need for RPCs by responding to Linux's built in loopback method that allows applications to only respond to the local machine.

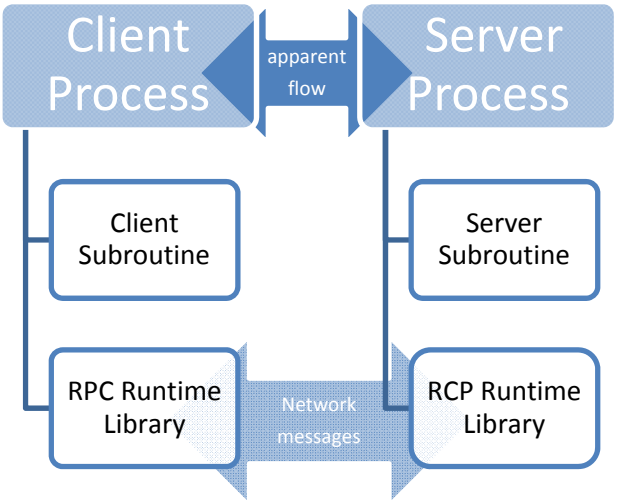


Figure. 2

Linux servers are designed be a headless system that can be controlled remotely. Most Linux servers consist of just the computer tower that has power and an internet connection. This greatly cuts down the number of problems and susceptibilities of a locally administered server such as Windows Server. Security holes on the remote system will not affect the server you are administering.

Configurability

Windows systems are limited by the need to have a graphic face to properly maintain and configure the server. Instead of being able to easily add new security features and elements, Windows monolithic design makes it difficult to successfully add a new security module to the existing system without having to do a major system overhaul. All the security features that come with the release of a particular Windows Server software release are the only features that will be available to the system administrator. It terms of user authentication, Windows has Active directory and it is used to force users and client to prove their identity to the server. While Linux based authentication allows for authentication from Windows based clients, Active Directory on the other hand will only authenticate Windows based clients. Custom packet filtering is not something that is native to Windows and thus a Windows server that wants to implement custom packet filtering may need to turn to an IPSec implementation to serve their needs. Windows Server 2003 featured a very basic packet filter that would only block specific incoming packets based on source IP address and destination port. Windows Server 2008 expanded this to filter both incoming and outbound packets based on protocol, source IP address, destination IP address, source port, and destination port. However while Windows Server 2008 did finally introduce this feature, it is important that packet filtering not something that is native or even consistent in Windows.

Linux is designed to be tailored to the specific needs of the user. Since Linux is open source software anyone can download it, customize it and then recompile it to fit their specific needs. Also since Linux is not limited by the reliance on a graphical interface, the users can usually highly customize

programs to do exactly what they need them to do and if they want more control, they can even delve into shell scripting to automate and further customize specific tasks. Due to Linux's modular design it does not always have to rely on specific proprietary software to accomplish tasks. The Samba project has introduced a way for Linux servers to authenticate windows machines and has even developed a way to emulate Active Directory on a Linux machine. This makes it possible for a Linux server to be deployed on a network that serves both Linux and Windows machines. Rather than use a "firewall" program, the Netfilter program developed for Linux allows you to setup individuals rule chains that can control the filtering of incoming, outbound, and forwarding packets. These chain rules can filter packets based on protocol, source address, source port, destination port, interface, state, type-of-service (TOS), and even user on outbound packets (Hunt, 264). Since many Linux machines serve as common gateways, firewalls, and access points in is imperative that Netfilter allow users to configure rules for forwarding packets.

Chain INPUT (policy ACCEPT)									
Packets	Bytes	Target	Protocol	Opt	In	Out	Source	Destination	State
0	0	Accept	All	--	lo	any	anywhere	anywhere	
0	0	Accept	All	--	any	any	anywhere	anywhere	Established,Related
0	0	Accept	TCP	--	any	any	anywhere	anywhere	TCP dport: ssh
0	0	Accept	TCP	--	any	any	anywhere	anywhere	TCP dport: www
0	0	Drop	All	--	any	any	anywhere	anywhere	
Chain OUTPUT (policy ACCEPT)									
0	0	Accept	All	--	any	any	anywhere	anywhere	

Figure. 3

Linux machines can be tweaked to meet the specific needs of each and every user. While it might take more time to configure and customize Linux to your needs the almost endless numbers of ways you can tailor Linux greatly outnumber the amount of time taken.

User-friendliness

When it comes to user friendliness no other operating system comes closer than Windows. With its easy "point and click" atmosphere and beautiful GUI what more could you ask for. While Windows Server is not as secure as Linux right out of the box, it is definitely easier to setup and install out of the box. It is possible to setup, install, and configure Windows Server 2008 within a few hours. Most of the functionality of Windows Server can be discovered by simple "point and click trial and error" and the Windows help included in Windows Server does a good job of answering most trivial questions that the new server administrator would have. Every available customizable option in Windows Server is right at your fingertips. While Windows server is very user friendly it also means that practically and person with average computers could setup a Windows server and thus they tend to be less secure, less maintained, and offer fewer services in comparison to Linux servers. On the other if you want a server that you will not have to hire a computer professional to manage or buy a manual to learn Linux than Windows Server might be your best bet.

Linux on the other hand might seem a bit more daunting to average computer user and sometimes even computer administrators. While many Linux distributions these days come with a GUI either Gnome or KDE, an effective Linux server is best run using no GUI at all and simply relying on text-based commands. This places the user in a position that requires him to learn how to navigate and configure a Linux machine entirely using text-based commands. Linux includes a built in manual commonly known as the man pages to aid a user in understand all of the different opinion each program or command offers. This manual is quite extensive in provided not only shell commands but even commands for installed software and programming languages such as C. It can be expected that most

Linux novices will require significant documentation and practice to successfully navigate on a Linux machine. This knowledge can be gained from online communities of Linux users, website, and books. Linux in many senses can be considered very user friendly to someone who is well experienced in Linux. It has also been that noted that usually Linux servers are more secure, better maintained, and offer more service than servers running Windows, simply because it takes a person that has above average computer skills to understand the Linux operating system in the first place.

Case Studies

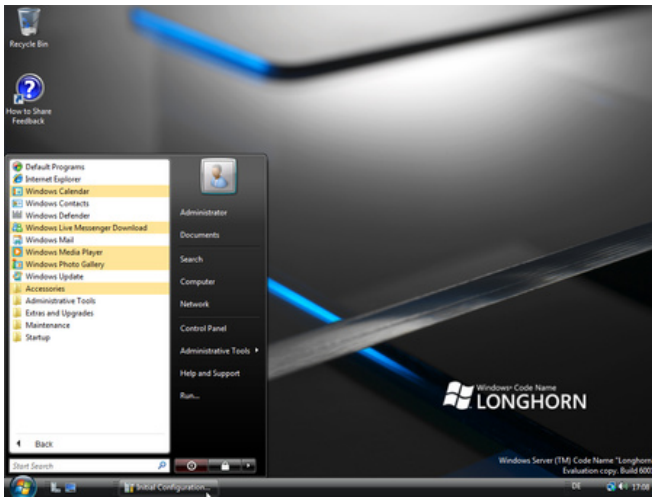
In addition to understanding the basic differences between Linux and Windows, it is also important to understand when it might be more appropriate to use Linux or Windows on a server. One of the great projects developed for Linux is the Samba project which makes it possible for Linux servers to talk to windows computers. It is even possible to use a Linux server to manage the Windows machines on your network, as a domain controller. One of the problems at most people run into when using Linux to control a Windows is when it comes to using Active Directory. While it is possible to skirt around some of the services that Active Directory provides, when you need to authenticate one-way trusts with clients on the network, Windows Server is the most appropriate choice. However, currently the beta version of Samba 4 includes an Active Directory compatible server. Any proprietary software that exclusively uses Windows Server would also be a situation when Windows Server needs to be used.

Linux servers are usefully for pretty much any other server application that you can think of. While the Apache Web Server is available for Windows, it runs in more secure environment when it runs in Linux. Linux can also be used for network authentication such as Kerberos and LDAP directory services. A Linux server can also be configured to securely run the DNS service and a DHCP server to allocate IP address dynamically. Since the Linux operating system offers greater security than Windows, it would be better to use Linux than Windows to manage a firewall separating your organization's

private network from the public Internet. If you need to manage a large database, MySQL is the perfect choice for this operation. These are just a sampling of the many uses for Linux in the server realm.

Conclusion

Linux and Windows will both continue to complete from control of the server market. After comparing the key areas of both operating system that are most important to the operation of a good server, Linux is the choice if you are looking for a server that will be secure, cost efficient, stable and will allow for maximum configurability. Windows leads the way in the realm of user-friendless and would be most appropriate for a server that is easy to manage and will not perform critical functions. Overall Linux offers more features and a more secure environment that are essential for a successfully server.



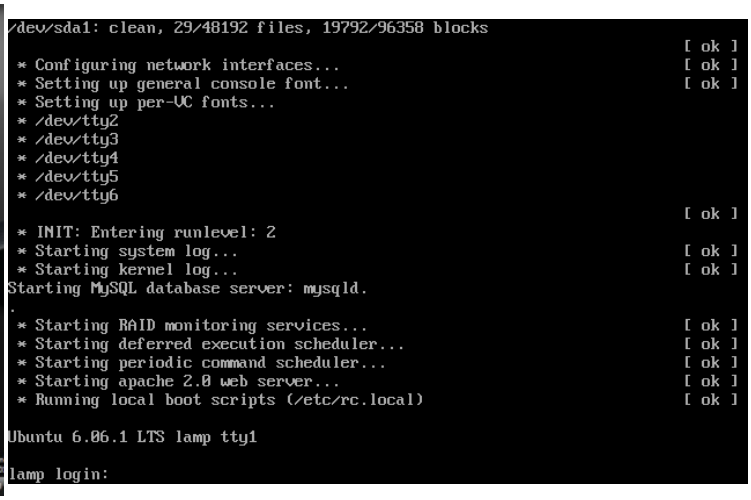


Figure. 4

Bibliography

Arora, Pooja. "MS Windows Talent Edge." Windows Server Compare. Apr 2008. Hewitt Associates. 11 Mar 2009 <http://download.microsoft.com/download/e/d/d/edd40b84-7889-4b7f-9eee-d9d690751db2/MS%20Windows%20Talent%20Edge.pdf>.

Greene, Jay. "Pecked by Penguins ." Business Week 3 Mar 2003: 1-2. 11 Mar 2009 <http://www.businessweek.com/magazine/content/03_09/b3822610_tc102.htm>.

Hunt, Craig. Linux Network Servers. Alameda, CA: Sybex, 1999.

Hunt, Craig. Linux Security. Alameda, CA: Sybex, 2001.

Mearian, Lucas. "Wall St. Leans Toward Linux." Computer World 21 Oct 2002: 1-2. 11 Mar 2009 <http://www.computerworld.com/softwaretopics/os/linux/story/0,10801,75271,00.html>.

Petreley, Nicholas. "Security Report: Windows vs Linux." The Register 22 Oct 2004: 1-24. 11 Mar 2009 <http://www.theregister.co.uk/2004/10/22/security_report_windows_vs_linux/>.