David Lambert

Professor Randolph Langley

CNT4603

18 July 2012

Final Paper / Securing Your Linux Box

This paper consists of two parts. In the first part, I will talk about the fruits harvested from the Computer and System Administration class I recently finished taking at Florida State University. After that task is conquered, I will focus on a system administration topic of my choosing: “Securing Your Linux Box”.

Unlike some classes I have taken at FSU, this is fortunately one that I can honestly say I have walked away with additional knowledge I did not possess prior to attending. I started out knowing a good deal about how to navigate a Unix system, and basics of networking, servers, and the like, but I definitely cannot say I didn’t learn anything new. The hands-on approach of the assignments in the computer lab were an extremely effective way to grasp understanding of topics.

It was very fascinating to understand concepts that I always wondered about - like how to set up a DNS server, for instance. My understanding of how a client computer connects to a DNS server to fetch an IP equivalent of a domain address already existed, but up until this class, I had simply used a “hosts” file copied to each PC on my home network in order to accomplish this. Attempts in the past at setting up a DNS server were too daunting. I understood the concept but now I understand the implementation. Now I have my home file server set up to act as a simple DNS server as well. Not that I have more than a partial handful of computers in my household, but

now I can "*ssh daveserv*" instead of "*ssh 192.168.1.x*". This and the many other topics learned through the assignments I can tell will help immensely when I get out into the "real world" of computer and network administration.

Aside from the assignments, the lectures absolutely helped a great deal as well. It was evident that the lectures facilitated absorption of the potentially bland-natured material, but the way the topics were translated to the students seemed to make it plenty bearable. I can at least speak for myself when I say that sometimes I would hurry home after class to research a topic that was discussed during lecture.

There are much too many rewards benefited from this class for me to list in the confines of this paper, but I do want to mention a few. To start, I was introduced to the Linux distribution that I am currently using to this day: Linux Mint. I had previously used Ubuntu at home but Linux Mint Debian Edition seems much peppier and less bloated than Ubuntu. The crisp, clean appearance of Mint absolutely doesn't hurt at all, too (especially when compared to Gnome 3 and Unity). If not for Professor Langley's discussion of this distro in class, I possibly would still not know about it. Other knowledge gained from this class include a great deal of how the inner-workings of a *nix system operate, many tips and tricks, how to correctly configure *iptables*, and I even was prompted to learn to use *emacs* after it being demonstrated in just about every lecture.

One final thing worth mentioning that I took away from the class was the recommended reading in the Linux Administration Handbook (by Nemeth, et al). In fact, I ended up reading the whole book, as it was very easy to digest, albeit thorough. It was probably one of the best-written computers books I have read to date.

And now the remainder of this paper will be about securing a typical Linux box. Since I am still a student in the learning stage of computer security, the information in this section of the paper is by no means an all-inclusive guide, but should at least be a source of inspiration for blossoming system administrators to get moving in the right direction in terms of securing their herd.

I think the best way to begin securing your Linux box would be to select an already-fairly-secure distribution. With most distros stemming from roots of either Debian, Red Hat, or Slackware[1], there are in fact hundreds of distros to choose from. As of the writing of this essay, DistroWatch.com lists 321 different “flavors” of Linux[2]. While the nature of most modern incarnations of Linux is to be more secure than alternative breeds of operating systems (e.g., Microsoft Windows), simply having “Linux” in the title does not specifically imply that every Linux distro is the wisest choice for someone concerned about security. Ubuntu Linux, the second-most popular distribution[2], is a good place to start. But although it is one of the most easy-to-use distros, security is simply not their top priority[3]. While it would most likely settle just fine for the average end user, it’s probably not the best pick for a system administrator, let alone a server.

For a secure-from-the-start distro, you might want to consider looking at CentOS. Originally based on Red Hat Enterprise Linux, one of CentOS’s largest defining points in terms of security is its default inclusion of “SELinux”. SELinux is a subsystem of Linux that allows the ability to secure a system based on predetermined policy, even imposing upon the root user’s abilities on a system. While SELinux is generally available to add to any flavor of Linux, it is convenient that it is already on your system if you are running a

distro such as CentOS or Red Hat.

Since I've mentioned SELinux, it'd probably be a good idea to explain it a little more. If you don't like Red Hat-based distributions, you can usually add SELinux to your Debian or Slackware-based distro fairly easily. If you're interested in a secure system, installing SELinux should be a requisite. It basically works by restricting programs and data to delegated users and processes, by use of a centralized policy. It's actually a lot like an internal firewall for your operating system. The administrator of the SELinux policy can determine which users and programs can have access to various resources such as files, devices, networks, and inter-process communication[4].

A good way to think about security is to visualize it in layers. The more layers you have, the harder it is for a potential hacker to get through them all. In that respect, you should by no means stop at your distro, or even at SELinux, if you want a secure system. One area that can often be easily overlooked is physical security of your system. Gaining physical access to a target computer, even for a short amount of time, could be extremely helpful to any would-be hackers to your system.

A good place to start physically securing your system is with passwords. Having a secure password can easily be classified as your first line of defense against potential attacks[5]. If someone else knows your password, there's not much else in the way of them accessing your private data and running malicious programs under your username. What do I mean by a secure password? In the most generic terms, it is one that is easy for you to remember, but difficult for others to guess or crack (to determine forcefully, usually using algorithms and programs).

There are many ways one could attempt to snatch your password. Some of the most common[6] include programs that simply try a slew of guesses at what your password might be based on information found about you (it's all too common for people to choose passwords based on more readily available information about the themselves than they think, e.g., their middle name or phone number), programs that try every word in the dictionary against your password, brute-force attacks (programs that run algorithms against your password to test literally millions of possible combinations of letters, numbers, and symbols), phishing (fake e-mails asking a user for their password, which appear to be legitimately from a system administrator), and even social engineering (from asking a user for their password while impersonating a system administrator to simply looking over someone's shoulder while they type in a password).

Some examples of poor choices[5,6] (easily-crackable or easily-guessable) for passwords include: information accessible about yourself (family member names, birth dates, etc.), dictionary words, passwords with repeating characters (e.g., 111222), and passwords with sequential characters (e.g., 12345 or ABCDE). But there are some ways to make your passwords more secure. These include, but are not limited to[5,6]: using at least eight characters (less than eight characters take considerably less time for a computer to crack), using symbols and numbers in addition to letters (again, this takes more time to crack), and changing your passwords often (increasing the chance that by the time someone illegitimately determines your password, you've already changed it to something else).

Another area of opportunity in physical security which sadly gets all too often overlooked, would be to develop a habit of simply locking your screen while you're away

from your computer, even if you plan on returning within a short amount of time. This may seem like it would be standard procedure but I unfortunately personally witnessed several peers in my system administration class carelessly leaving their machine unlocked while they stepped out of the room for several minutes, even after Professor Langley specifically cautioned against doing so. Most distributions (and most operating systems in general) allow some sort of method to quickly lock your screen or terminal, requiring your password to unlock it when you return. A simple instance of one leaving their screen unlocked while they use the restroom could be more than sufficient time for someone to run some sort of malicious script on your machine, possibly enabling them remote access to your machine for later intrusion.

Another great way to add a layer of security to your system is to make sure you have an enabled and properly-configured firewall. This is especially so if your computer is connected to a public network such as the Internet, as opposed to being isolated on a private one. Note that I specifically mentioned to make sure that your system's firewall is enabled - unfortunately, while most Linux distros do include a firewall program, it is often not enabled by default.

If your computer is not connected to a network, a firewall won't really do you much good. But the purpose of a firewall when you're connected to a network is to help control which network traffic is allowed and which is prohibited from making its way in and out of your system. Different services used on networks usually agree to communicate to each other on specific "ports". For example, web pages you read in a web browser are usually served to you through port 80. It is common to have this port open on your system if you are serving web pages, but it's a good idea to use your

firewall to keep most other ports closed unless you specifically need to open them. Having a firewall is very important as rudimentary protection against network-based malicious attacks - it essentially reduces the number of “doors” a hacker could go through to access your system.

If your network is behind a modern network router, the router is most likely acting as a firewall already. Therefore, it’s not quite as important to set up firewall software on every individual computer on your network unless you’re worried about attacks originating from within your network (this is more likely in larger corporations where it’s not very feasible to physically account for each system at all times). If your router does have a firewall built-in, it is still worth checking to make sure it is configured to your needs.

One final topic I will talk about in this paper is keeping your system up to date. That pesky little reminder on your computer’s desktop to update your system is more than just an annoyance. Associated with most major Linux distributions are teams of security personnel who continuously update programs in order to fix security vulnerabilities[7]. Theoretically, every time a security “hole” is found in a piece of software, these security people fix it and release a new version of the program. If you’re still using an old version of the program, it makes you more susceptible to an attack or intrusion. Information on the particular program’s compromise is generally publicly available on the Internet, so it’s definitely in your best interest to stay up to date to avoid any negative impact.

It would be conceivable that I could go on writing about computer security until I’ve exhausted all hard drive space on my computer, so I will limit my discussion to the

preceding pages. It should at least give you an idea of some places you could start to make your system and your network more secure.

If after you've implemented all of the above recommendations you're still looking for more ways to secure your system, there is an abundance of information available on the Internet; Google is your friend.

Works Cited

1. Lundqvist, Andreas. “GNU/Linux Distribution Timeline 12.02”. *Futurist.se.* 20 Feb 2012. Web. 21 Jul 2012. <http://futurist.se/gldt/>.
2. “DistroWatch Page Hit Rating”. *Distrowatch.com.* 21 Jul 2012. Web. 21 Jul 2012. <http://distrowatch.com/dwres.php?resource=popularity>.
3. “Why Use Ubuntu.” *Ubuntu.* Canonical Ltd., n.d. Web. 22 Jul 2012. <http://www.ubuntu.com/ubuntu/why-use-ubuntu>.
4. “FAQ”. *SELinux Wiki*. n.p. 16 Oct 2009. Web. 22 Jul 2012. <http://selinuxproject.org/page/FAQ>.
5. “The Importance of a Secure Password”. *Campus Connection*. University of Wisconsin-La Crosse. 13 Oct 2011. Web. 23 Jul 2012. <http://news.uwlax.edu/the-importance-of-a-secure-password/>.
6. “The Importance of Strong Passwords”. *Security Awareness.* University of Texas at Austin. 05 Oct 2010. Web. 24 Jul 2012. <http://www.utexas.edu/its/secure/articles/importance_strong_passwords.php>.
7. Sharma, Mayank. “How to Secure Your Linux System”. *TechRadar Computing.* Future US Inc., 04 Jan 2011. Web. 24 Jul 2012. <http://www.techradar.com/news/software/operating-systems/how-to-secure-your-linux-system-915651>