Secure your Ubuntu

"The only security that a man can have in this world is a reserve of knowledge, experience and ability"

Henry Ford

Security is one of, if not the most debated topic with people using computers. Losing data be it personal photos, bank statements or work related documents is every users worst nightmare. This article is dedicated in enlightening and empowering you to enhance your experience on this wonderful operating system. Security I have tried to give at least one example of the solution wherever possible.

Is Linux really a Secure System?

This is one of the biggest questions that a new Linux user is confronted with after switching over from another operating system. A lot of comparisons can be raised between different operating systems explaining their loopholes. However, there is no operating system in the world that will be completely invulnerable to security issues, and there never will be.

But unlike other systems, Ubuntu comes as close as possible to provide you with a protected platform for doing your work. Each process running on the Linux system has its own private memory pages and cannot access the memory pages being used by another process. The kernel maintains its own memory areas. For security purposes, no processes can access memory used by the kernel processes. Also, each individual user on the system has a private memory area used for handling any applications the user starts. This method of isolation prevents unauthorized entry of various malicious software into Ubuntu.

Install minimum packages

It is a good idea to remove packages that you do not use regularly. Even after uninstalling some programs, their dependencies may still exist. Such dependencies should be removed using a program like the *Computer* Janitor available under *System –> Administration* in Ubuntu. It will not only enhance your security but also improve performance. The Figure 1 shows the various dependencies that still existed even after removing the programs using a package manager.

Also, it is advised to install software only from trusted sources. This is because security vulnerabilities are not induced only from malicious software installed on the system. They might even exist in current supported packages residing within Ubuntu reposito-

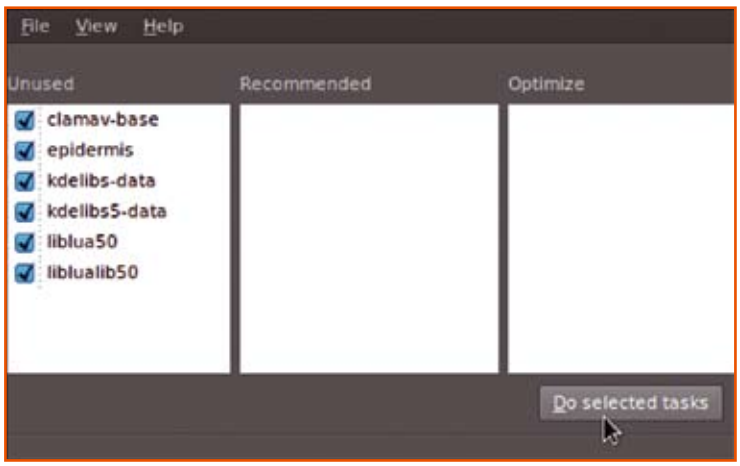

Figure 1. *Computer Janitor in Ubuntu*

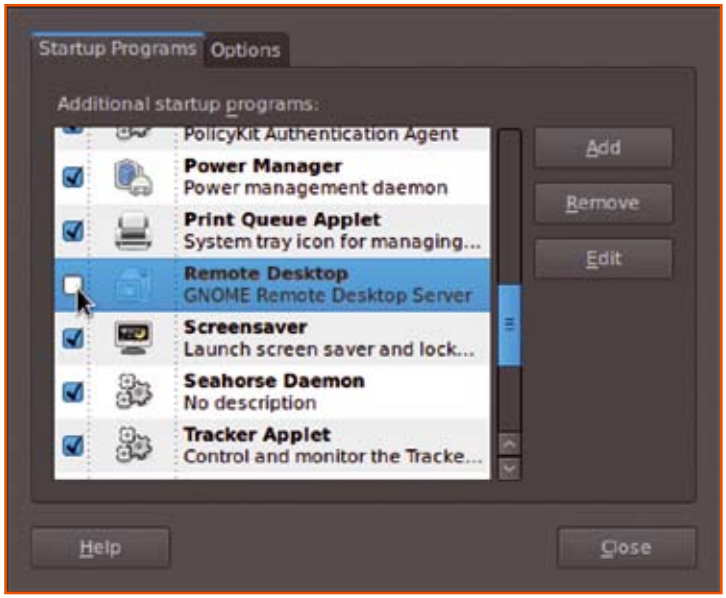

Figure 2. *Disable Unused Startup Services*

Figure 3. *Provide your password for administrative tasks*

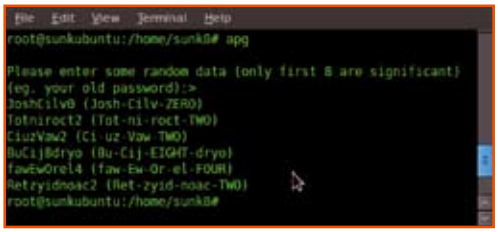

Figure 4. *Example of APG in Terminal*

ries. A regularly updated list can be viewed at the *Ubuntu Security Notices* page available at *http://www.ubuntu.com/usn*

It is a good practice to visit this page before installing a new program on Ubuntu to be informed about its security vulnerabilities.

Disable Unused Services

It is important to disable the services that you do not plan to use for some time. These services can be found at the *System –> Preferences –> Startup Applications* menu.

For example, you may turn off the Remote Desktop service (see Figure 2) if you do not wish to use it. These changes will not only enhance your security but also speed up your boot process.

Administrative Privileges

There are certain applications that require special privileges. When you try to open such a program, a pop up window similar to the one shown in the Figure 3 may appear. When some malware wants to gain access to your computer, it requires this password.

When confronted by such a window think carefully before providing the password. The details menu will give you more information about the process that is trying to gain access.

The window should launch only when you have asked a certain application to do something which requires administrative privileges. These applications have the potential to cause major changes in the system.

A similar case may arise while trying to run a command in the terminal. Here you may be asked either to provide a password directly or use `sudo` at the beginning of the command.

If you're unsure about the application, simply hit [*Cancel*] or press the [*Esc*] key.

Strong Passwords

This is a practice that should be followed by a user whether you are setting a password for your work email account or just a social networking site.

There are various elements that a password should contain for it to be called strong. A very good method of creating a strong password is by using an Automated Password Generator. The pack-

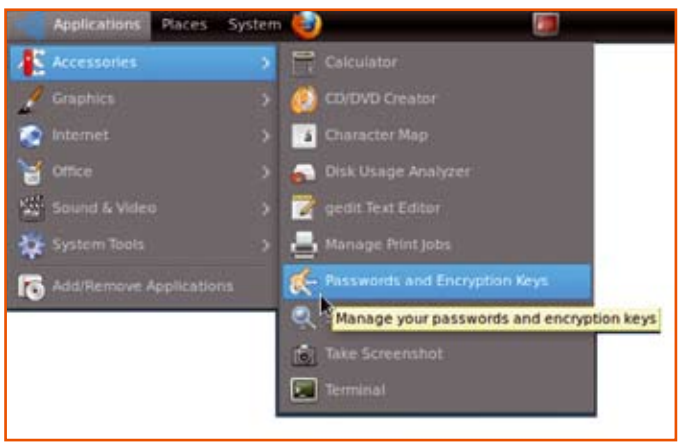

Figure 5. *Open Seahorse via menu*

Figure 6. *Creating a PGP Key*

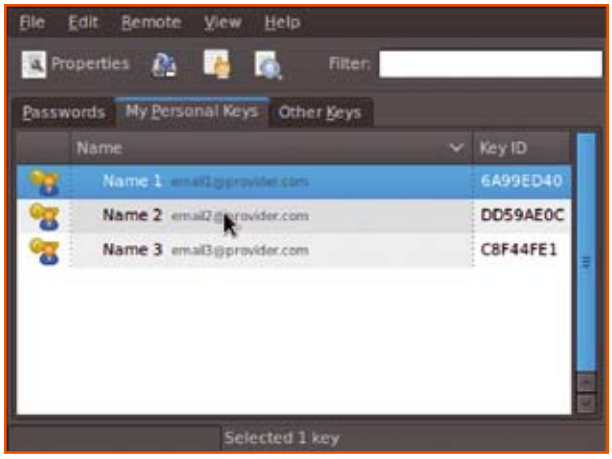

Figure 7. *Your PGP Keys*

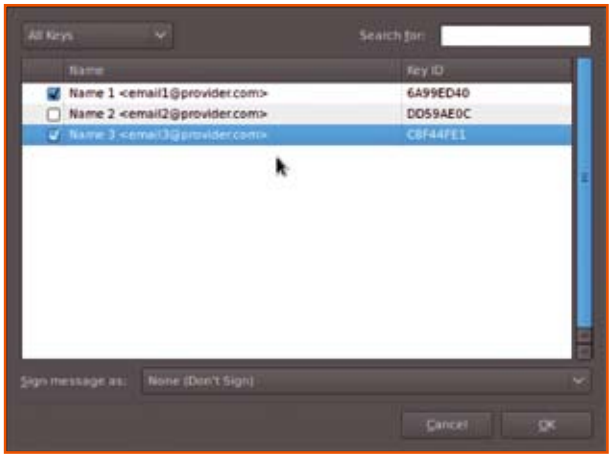

Figure 8. *Choose Recipients*

age *apg* in the Ubuntu repositories is a very useful tool to creating passwords that are very difficult to crack.

The Figure 4 shows an example of the `apg` command generating six strong passwords automatically. Also these passwords are easy to remember when associated with their pronunciations as shown in the parentheses beside them.

Encrypting your files and folders

There may be times when you want to keep your information hidden from other people having access to your computer. Or to ensure that important information is not divulged when an unauthorized person obtains your data. At such times, just making your files/folders hidden or changing their permissions is not enough. Here, it is better to make use of encryption.

Encryption simply means encoding information in such a way that it will be accessible only to the persons authorized to view it. There are many popular ways of encrypting files and folders in Ubuntu. As an example, I have explained encryption on a Ubuntu Desktop with PGP keys using Seahorse.

The package *Seahorse* is a front-end for the *Gnu Privacy Guard* program that integrates into the Gnome Desktop. This package is provided in the Ubuntu 10.04 System by default. For Kubuntu, you can make use of the *KGPG* package which is available by default. These programs allow us to create a variety of keys that can be used to encrypt information.

Note: For this method to run we will need to install the package *seahorse-plugins* which is not provided by default. Install this package using the *Synaptic Package Manager* or the following command in the Terminal:

```
$ sudo apt-get install ↵
  seahorse-plugins
```

Creating a PGP Key

Choose *Passwords and Encryption Keys* from the *Applications –> Accessories* menu as shown in theFigure 5.

The *Passwords and Encryption Keys* window will come up. Choose *File –> New...* or press [*Ctrl*] + [*N*]. You will be confronted with the pop-up window.

Note: If you already have a key, the same can be imported into Seahorse. To do this choose *File –> Import...* and specify the location of the key. It is a good practice to keep backup of keys on your computer remote servers. A key can be exported using the *File –> Export...* command.

Here choose *PGP Key* as shown in the Figure 6 and click on continue.

A simple setup will guide you through this creation process. You will be asked information like your full name and email address. You will also be asked to *enter* and *confirm* a passphrase for the new PGP key. This is the cipher/password that is essential to lock and unlock information using this key. Be sure to remember it or your data could be lost forever.

You can view the created PGP keys in the *My Personal Keys* Tab as shown in the Figure 7.

These keys only exist on your computer at the moment. You can synchronize these keys with remote servers. To do this in Seahorse choose *Remote –> Sync and Publish Keys...* from the menu.

Encrypting your information

Now go to the files and folders that you wish to encrypt. Select the files/folders, right-click and choose *Encrypt...* from the menu. A *Choose Recipients* window (see Figure 8) will open where you are required to specify the key that you want to associate with these set of files and folders.

In case there are multiple files or folders another window will pop up as shown in the Figure 9.

If you have selected the option of encrypting by packing together in a package, a compression package of the specific extension will be produced. Or else, you will see files with the extension *pgp* which are the files encrypted using this key.

Decrypting your information

To open encrypted packages or pgp files, simply double-click them. The packages will open via your default compression application where you

will be asked the passphrase. In case of pgp files, you will be first asked to enter a new name to save the file. Then you will be required to enter the key's passphrase. The decrypted file will then be created in the specified folder.

Security Updates

Developers of Ubuntu OS often come up with various security patches and updates that can be easily integrated into your existing system. Ubuntu 10.04 is tagged as a Long-Term-Support (LTS) release. For LTS releases, Ubuntu provides security and patch updates for up to 3 years.

Hence, it is advisable to keep your system up-to-date by downloading and installing the latest updates. This can be easily done under Ubuntu using the Update Manager. To start the program choose *System –> Administration –> Update Manager*.

You may also want Ubuntu to install security updates automatically. This is also possible through the Update Manager. To do so open the Update Manager and click on the *Settings...* button present in the bottom. The window as shown in Figure 10 will pop up.

The drop-down menu under *Automatic Updates* allows you to choose the frequency of installation. Click on the radio button saying *Install security updates without confirmation* to install security updates automatically.

Social Engineering

Notorious people seeking information have started the use of techniques of manipulating people instead of technical hacking tools as was popular earlier. Hence, this aspect also requires a mention in this article.

Hackers and such other elements are constantly trying to illegally gain information from various computers be it from a Government institution or your grandma's laptop. The risk multiplies even more if you are using your Personal Computer to view mails or download from unknown sites over the Internet.

And there is only one solution to it: Be Smart. Don't trust anyone over the Internet. Never ever divulge any information over the Internet unless you are sure that it cannot be misused.

Strengthen your Web Browser

Of the many web browsers available in the Ubuntu Family repositories, Mozilla Firefox is the most popular cross-platform browser. Also, it allows a user the functionality of installing various addons to enhance its productivity and security.

Note: The https protocol suggests a secure site compared to the standard http protocol. Use it whenever a site supports it to keep your information safe when on-line.

We can further strengthen the forces by installing various addons that promote security over the Internet. I will mention only a few

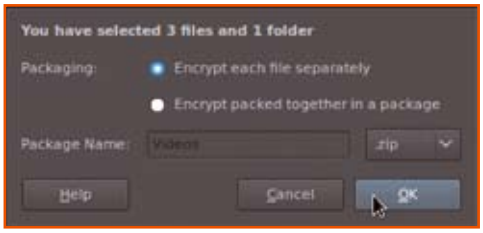

Figure 9. *Pack Multiple Files / Folders*

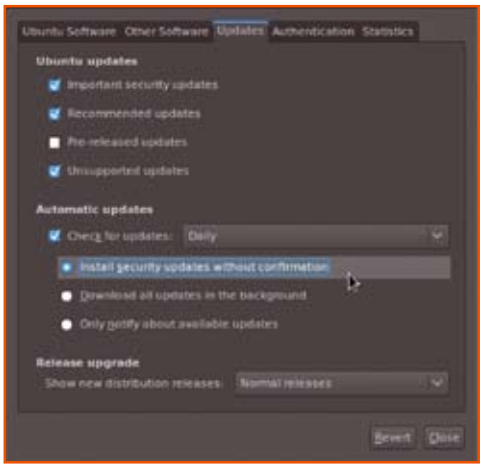

Figure 10. *Automatic Security Updates*

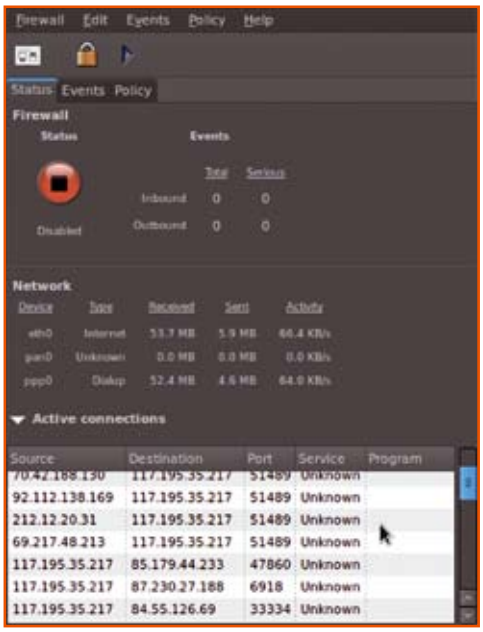

Figure 11. *Firestarter for Ubuntu*

Table 1. *Various addons that promote security over the Internet*

Addon	Description
Adblock Plus	This is a beautiful addon that lets you block specific pieces of javascript.
NoScript	This addon allows active content to run only from those sites that you trust, and thus protects you against XSS and Clickjacking attacks.
WOT	This addon gives you extra information about the site that you are currently at. They have a scorecard for rating every site. You can also upload your data and further improve their database.
Xmarks Sync, Weave Browser Sync	These are recommended addons that allow you to store and synchronize your passwords and bookmarks.

addons that you can install in Mozilla Firefox to make your browsing experience secure and pleasant (see Table 1).

The Firefox preferences window can be opened via *Edit –> Preferences*. It has two tabs *Privacy* and *Security* which offer many self-explanatory options.

Firewall

Ubuntu by default has a very secure built-in kernel firewall called *iptabled*. There are various open-source applications available in the Ubuntu repositories which allow you to configure this firewall. *Firestarter* is a one nice tool that allows you to create rules for various inbound and outbound connections on Ubuntu. The Figure 11 shows the status of a certain computer connected to the Internet.

For Kubuntu, you may want to use another tool called *Guarddog*. Other available open-source applications include *gui-ufw*, *Firewall Builder* and *KmyFirewall*.

Anti-virus

One does not really need an anti-virus on Linux. This is because malicious software affecting Windows Systems do not affect Linux. This is true even if you have an emulator like WINE installed. This is because, when trying to make any changes to the system, you will always be prompted for a password.

However, some users prefer to dual-boot the two operating systems. In this case, malicious software that might get downloaded in Ubuntu will affect their Windows system. For such cases, there is a very smart free open-source anti-virus program available right in the Ubuntu repositories. For GNOME desktop it is called *ClamAV* while on KDE it is referred to as *KlamAV*.

The Figure 12 shows *ClamAV* while scanning the user's home directory. One can also scan a specific file or directory present on the disk. You also have an option to move certain files to quarantine if you feel that they are infected.

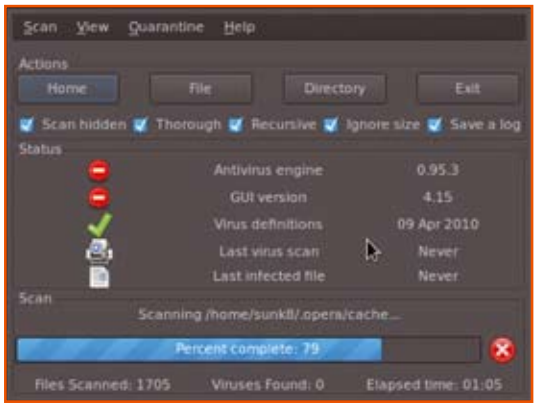

Figure 12. *Scan /home using ClamAV*

KlamAV is just the KDE front-end to ClamAV. The Figure 13 shows KlamAV scanning the user's windows directory which is on the different partition. KlamAV lets the user configure advanced options like updates, quarantine area and e-mail protection. It also has an inbuilt *Virus Browser* that gives you information about all the malware listed in the anti-virus database. And the *Events* tab that keeps a history log of the anti-virus.

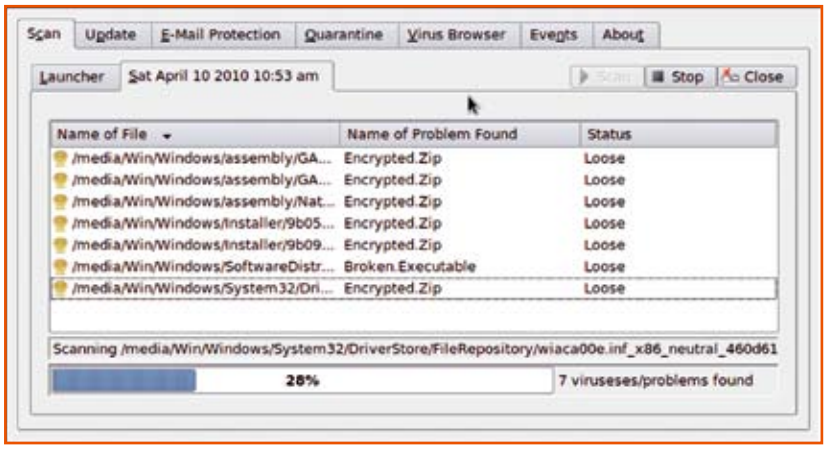

Figure 13. *Scan Windows Directory using KlamAV*

Third-Party Security Applications

As we have seen earlier, an anti-virus or firewall may prove useful on Ubuntu. Besides free and open-source software, there are also commercial versions offered by various companies. Other available Linux anti-virus suites include *Avast, AVG, Avira, Bitdefender, Eset, F-secure, F-prot Kaspersky, McAfee, Panda Security, Sophos, Symantec* and *Trend Micro*. Other firewall applications include *AppArmor, Gufw, Modsecurity, Systrace* and *Zorp*.

Conclusion

Security is one of the most debated topics on Ubuntu. Often it is said that lack of popularity has kept Linux from been targeted by unethical programmers. However, this is not true. The more you use it, the more you'll find that Linux is very robust compared to other operating systems.

References

- *http://sites.google.com/site/easylinuxtipsproject/security*
- *https://help.ubuntu.com/community/Security*
- *https://help.ubuntu.com/community/StrongPasswords*
- *https://help.ubuntu.com/community/GnuPrivacyGuardHowto*
- *https://wiki.ubuntu.com/Testing/Applications/Seahorse*
- *http://en.wikipedia.org/wiki/Social_engineering_(security)*
- *http://en.wikipedia.org/wiki/Linux_malware*
- *https://help.ubuntu.com/community/Antivirus*
- *https://help.ubuntu.com/community/Firewall*