FREE SECURITY SUITE 2

Easy, Intuitive and Complete Free Security Suite with Web Browser Integration

Javier Corral-García, Carlos-Jorge del Arco González
José Luis González-Sánchez and José Luis Redondo García
Department of Computing and Telematic System Engineering, University of Extremadura, Cáceres, Spain
javiercg@unex.es, cdelarco@alumnos.unex.es, jlgs@unex.es, jluisred@unex.es

Keywords: Free software, Security, Suite, Privacy, Network threats, Web browser extension.

Abstract: Nowadays there are many security suites to protect a system against threats from the network. However, users must purchase a license to use them. There is the possibility of installing some free-of-charge security tools (often Free Software tools), without license payments and avoiding illegal use of software. The disadvantages are that each tool focuses on monitoring only one security threat, leaving a loft of other aspects unprotected. Moreover, in most cases these tools run on command line, involving difficult configuration processes for non-expert users. We have developed a Free and easy to use suite that ensures the security of the systems in which it is installed, and designed for users who don't have enough time, nor high knowledge about computer security, to protect their systems against threats from the network adequately. In order to achieve our objectives, we made a thorough study of the latest free software tools, with the aim of choosing the best for our suite, developing several easy and intuitive graphical interfaces for the command line tools, even modifying the source code of one of them, and developing an extension to integrate FSS-2 in the Mozilla Firefox browser.

1 INTRODUCTION

System and network security are fundamental cornerstones that seek to ensure the protection of information. Unfortunately they are not easy goals to achieve (De-Silva et al., 2007). The Internet has grown dramatically and evolved significantly over the past 10 years (Arlitt & Williamson, 2007) and, as the level of trade and commerce conducted over it increases, so does the requirement that the Internet is reliable and secure. Unfortunately, the quantity and complexity of security threats to the Internet is also increasing (Sandford et al., 2006). The Free Security Suite 2 project, or FSS-2, appears with the need to offer users a complete easy and intuitive tool to protect their systems against increasing threats.

Nowadays there are many security suites to protect a system. However, users must purchase a license to use these Software products. This fact means that, generally, the user decides to leave their system unprotected or using this software illegally, facing the consequences accordingly. There is the possibility of installing some free-of-charge security tools in order to solve the problems of the user, without license payments and avoiding illegal use of software. The disadvantages are that each tool focuses on monitoring only one security threat, leaving a lot of other aspects unprotected, in most cases, involving difficult configuration processes and a complex interface for non-expert users.

Our previous version, Free Security Suite (Castuera et al., 2004), emerged to solve these problems, by offering a free security suite that integrated several easy and intuitive tools to control various security aspects at the same time. FSS became the only application with such features, and nowadays it still has this singularity, due to the non-existence of another Free Software security suite.

However, throughout these years, the application has become obsolete. For this reason we have developed FSS-2, a new version adapted to current needs. The philosophy is the same one but with an improved suite, returning to make a thorough study of the latest free software tools, with the aim of choosing the best for our suite, developing easy and intuitive graphical interfaces, also modifying the source code of one tool, and developing an extension to integrate FSS-2 in the *Mozilla Firefox* browser (Firefox, 2009), so that it can be used more comfortably.

2 PREVIOUS ANALYSIS

We proposed to develop Free and easy to use tool, that ensure the security of the systems in which it is installed, and directs towards users who don't have enough time, nor high knowledge about computer security, to adequately protect their systems. Thus, FSS-2 is a tool with easy use and configuration features, which controls the main aspects of security that concerns common users. We wanted to develop it as a Free Software tool, GPL licensed, among other reasons, so that its use would not involve any cost to any user. The source code is distributed with the tool and can be modified without restrictions, allowing anybody to improve its features or to adapt it to other specific requirements.

2.1 Tools Analysis

With the goal of making FSS-2 to strengthen the security of a system in as many aspects as possible, we previously performed a thorough analysis of the threats that presents nowadays a computer system, analyzing in depth the latest protection tools, in order to choose the most suitable to join FFS-2.

2.1.1 Anti-RootKit

FSS-2 includes *Tripwire* (2009), for to obtain and compare fingerprints of programs, and *Chkrootkit* (2009) and *Rkhunter* (2009), as a detection method if it is suspected that the rookit is already present in our system. These tools run on command line mode so we have developed an interface for each of them in order to make their use more intuitive to the user.

2.1.2 File Encryption

After analyzing many files encryption tools, we finally opted for *ScramDisk* (2009), which has an intuitive graphical interface that facilitates the task to the user.

2.1.3 e-Mail Encryption

GnuGP (2009) allows encrypt communications and data, with a key management system and access modules for all types of public key directories. It runs from the command line, so it was desirable to incorporate a graphical user manager to enable him to exploit all the opportunities offered by *GnuPG*. So, we were analyzed different possibilities, choosing *GPA* (2009) finally, due to its simplicity and its more intuitive use.

2.1.4 AntiPhising

Mozilla Firefox (Firefox, 2009) browser incorporates an antiphishing tool. It is GPL licensed, being chosen as the anti-phishing tool for FSS-2.

2.1.5 Firewall

We decided to include two tools: *Firestarter* (2009) is made for users who prefer an easy tool with good results; *GuardDog* is the option for users with higher knowledge and who wish to obtain a more advanced configuration from their firewall.

2.1.6 Antivirus

We have selected *ClamAV* (2009), a GPL licensed antivirus with support for Linux, simple updating method, and versions released often by their developers. *ClamAV* can be run on command line mode or on various graphical environments. In our suite, we have included the *KlamAV* environment (2009), which we considered it has the best features, providing exclusive options not included on others, and making habitual tasks such as updating of the Clam graphical environment easier.

2.1.7 Content Filter

FSS-2 includes the *Dansguardian* tool (2009), GPL licensed, after analyzing various content filtering tools. However, it runs on command line. So, we have developed a graphical interface that replaces command mode, developing modifications on the source code of the application, with the objective of improving it substantially.

2.1.8 Anti-Spam

Users are able to install *Thunderbird* (2009) with a Bayesian filter incorporated, and also the installation and configuration of the *CRM114* (2009) system to sort email messages using *Kmail* (2009) client. We have enabled an option in our application to access the *Evolution* (2009) mail client, because it presents an integrated anti-spam filter. *CRM114* was chosen because it has obtained the best results according to our preferences.

3 DEVELOPMENT

We developed graphical interfaces that allow users to configure and run the tools explained above. Besides this, we had to develop interfaces for

execute script files and operating system commands, to achieve applications that run specific command line orders.

Our suite can be easily installed and configured on any Linux system because our data model is based on a collection of text files.

In addition, we made a modification in the source code of the *Dansguardian* tool, in order to obtain a configuration based on user groups, so that each group can have a set of predefined filtering options, because its initial configuration was too complex.

3.1 Mozilla Firefox Extension

Although the application can be executed differently, we developed an extension to include FSS-2 as a tool in the *Mozilla Firefox* browser, so that it can be used more comfortably.

3.2 Installation Scripts

The installation was performed through automated scripts to avoid complex configurations task when the user begins to run the suite.

3.3 Implementation

FSS-2 applications may be used separately, independent of the suite. The implementation has been carried out using C++ programming language together with Shell Script language and operating system GNU/Linux commands. The tools used have been *Anjuta IDE* and *Glade* interface designer, in addition to some official libraries.

4 FSS-2

The access to the application is done through *Firefox* browser by opening the *Tools* menu and choosing the FSS-2 option. The main window shows eight tabs that allow access to the different tools, each one indicating its basic functionality.

4.1 Anti-rootkit

The *Anti-rookit* tab provides access to rootkit detection applications through the intuitive graphical user interfaces that we developed. We carry out several options for *Chkrootkit* for: to start the rootkits analysis, to access the latest analysis results, and to search for and install new updates automatically. *RKHunter* add another option, updating its database and saving the files analyzed as authentic. With *Tripwire* we allow users to verify the files integrity.

4.2 Antivirus

Using this tab, we include the *KlamAV* graphical interface in order to use the *ClamAV* antivirus. Thus, users can scan their systems (with the chance of scheduling this task), update antivirus, configure e-mails scanning, managing quarantine files, etc.

4.3 Antispam

The *Antispam* tab provides access to the email clients included with FSS-2, in addition to the *CRM114* tool that we integrated with *KMail*, due to the reasons set out in the tools analysis section, where we also explain the reasons for this choice.

4.4 File Encryption

FSS-2 allows the user to create encrypted disk partitions and volumes. Data is encrypted in a container, and when the user has access to this data, it is opened and automatically decrypted, through the *ScramDisk* tool.

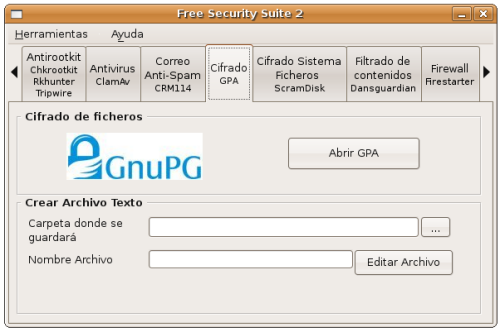

Figure 1: GPA encryption tab FSS-2.

4.5 e-Mail Encryption

We allow performing the encryption of text messages for later e-mail data transmission. The tool is used through *GPA* graphical environment, which that allows user to get all the *GnuPG* features in an easy and intuitive way. By means of the mentioned tools, it allows encryption, decryption, signature and document verification, besides import and export of public key.

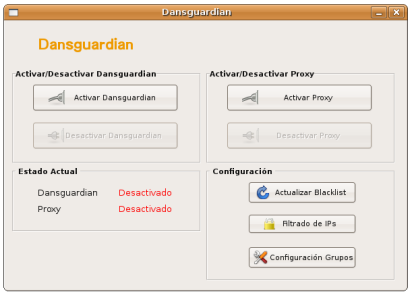

Figure 2: Dansguardian main window FSS-2.

4.6 Content Filter

Dansguardian, allows the control of Internet contents. We have developed a graphical environment for FSS-2 that allows users to use the tool in a comfortable and intuitive way. Also, we have realized a modification which consists on a configuration based on user groups, with the objective that each one can have a set of predefined filtering options, because its initial configuration seemed to be too complex to non-expert user.

4.7 Firewall

We had included two tools: *Firestarter*, for users who prefer an easy tool with good results, and *GuardDog* for users with higher knowledge and who wish to obtain a more advanced configuration.

4.8 Antiphising

The tool we offer is integrated into *Mozilla Firefox* web browser, however, FSS-2 incorporates a tab to enable/disable this protection in the browser.

4.9 General Preferences

Also, we have incorporated several options in order to automate various tasks, such as the execution of some tools or the whole suite at system start-up, or of different scheduled analysis.

5 CONCLUSIONS

We have developed an easy to use and Free tool that ensures the security of systems, and designed for users who don't have enough time, nor high knowledge about computer security, to protect their systems against threats in an easy and intuitive way.

Thus, FSS-2 is a tool with easy use and configuration features, which controls the main aspects of security that concerns common users. Besides, as free tool, the source code is distributed and can be modified without restrictions, allowing everybody to improve its features.

We made a thorough study of the latest free software tools, with the aim of choosing the best for our suite, developing easy and intuitive graphical interfaces for command line tools, even modifying the source code of one of them.

We performed the installation of FSS-2 through different automated scripts to avoid complex configurations task when user begins to run the suite, and although the application can be executed differently, we developed an extension to include FSS-2 as a tool in the *Mozilla Firefox* browser, so it can be used more comfortably.

REFERENCES

Arlitt, M., Williamson, C., 2007. The extensive challenges of Internet application measurement. In *IEEE Network*, 21 (3), pp. 41-46.

Castuera Toro, M., Carmona-Murillo, J.D., González-Sánchez, J.L., 2004. Free Security Suite: Sistema de navegación libre que aporta mecanismos de seguridad fácilmente configurables y portables. In *II Congreso del Observatorio para la Cibersociedad.* Barcelona, Spain, 2004, pp 1-16.

Chkrootkit. Accessed 2009, http://www.chkrootkit.org/

ClamAV. Accessed 2009, http://www.clamav.net/

CRM114. Accessed 2009, http://crm114.sourceforge.net/

Dansguardian. Accessed 2009, http://dansguardian.org/

De-Silva, M.S., Parish, D.J., Sandford, P., Sandford, J.M., 2007. Automated detection of emerging network security. In *ICN'07, Sixth International Conference on Networking, 2007.* IEEE, Martinique, 2007, pp 98-98.

Evolution. Acc. 2009, http://projects.gnome.org/evolution/

Firefox. Accessed 2009, http://www.mozilla.com/firefox/

Firestarter. Accessed 2009, http://www.fs-security.com/

GnuPG. Accessed 2009, http://www.gnupg.org/

GPA. Accessed 2009, http://www.gnupg.org/gpa.html

GuardDog. Accessed 2009, http://www.simonzone.com/software/guarddog/

KlamAV. Accessed 2009, http://klamav.sourceforge.net/

Kmail. Accessed 2009, http://kontact.kde.org/kmail/

Rkhunter. Accessed 2009, http://rkhunter.sourceforge.net/

Sandford, P.J., Parish, D.J., Sandford, J.M., 2006. Detecting security threats in the network core using data mining techniques. In *NOMS 2006, 10th IEEE/IFIP Network Operations and Management Symposium.* Vancouver, 2006, pp 1-4.

ScramDisk. Accessed 2009, http://sd4l.sourceforge.net/

Thunderbird. 2009, http://www.mozilla.com/thunderbird/

Tripwire. Accessed 2009, http://www.tripwire.com/