Security in Operating System: Windows and Linux Ubuntu

Seguridad en Sistemas Operativos: Windows y Linux Ubuntu

Segurança em Sistemas Operacionais: Windows e Linux Ubuntu

Helena Clara Isabel Alemán Novoa

M.Sc Seguridad Informática Universidad Internacional de la Rioja UNIR

Fundación Universitaria Juan de Castellanos, Grupo de Investigación CIyT

haleman@jdc.edu.co

José Custodio Najar

M.Sc Seguridad Informática Universidad Internacional de la Rioja UNIR

Fundación Universitaria Juan de Castellanos, Grupo de Investigación CIyT

jnajar@jdc.edu.co

 ***Abstract* — The OS of any computer device is the base software where the resources within a system are managed, and it depends on its correct configuration and operation to provide security to the software itself. This paper describes some security tools for Windows and Ubuntu OS, in order to inform users about new possibilities to protect information from any threat, avoiding being exposed to vulnerabilities and security breaches, which can be prevented if the security mechanisms available to each of these operating systems are known and applied.**

 ***Keywords— Operating Systems, Security, Ubuntu, Windows.***

 ***Resumen—* El sistema operativo de cualquier equipo de cómputo es el software base desde donde se administran los recursos adheridos a un sistema, y depende de su correcta configuración y operación proveer seguridad a los mismos. En el presente documento se describen algunas herramientas de seguridad de los sistemas operativos Windows y Ubuntu, con el fin de dar a conocer a los usuarios nuevas posibilidades para resguardar la información de cualquier amenaza, evitando estar expuesto a vulnerabilidades y brechas de seguridad, que se pueden prevenir si se conocen y aplican los mecanismos de seguridad con que cuentan cada uno de estos sistemas operativos.**

 ***Palabras Clave***— ***Sistemas Operativos, Seguridad****,* ***Ubuntu, Windows.***

 ***Resumo—* O sistema operacional de qualquer equipamento de computador é o software básico a partir do qual os recursos conectados a um sistema são gerenciados e depende de sua configuração e operação corretas para fornecer segurança a eles. Este documento descreve algumas ferramentas de segurança dos sistemas operacionais Windows e Ubuntu, a fim de informar os usuários sobre novas possibilidades de proteger informações de qualquer ameaça, evitando serem expostos a vulnerabilidades e brechas de segurança, que podem impedir se os mecanismos de segurança disponíveis para cada desses sistemas operacionais são conhecidos e aplicados.**

 ***Palavras-chave***— ***Palavras-chave Sistemas operacionais, Windows, Ubuntu, Segurança.***

1. **INTRODUCTION**

N

owadays, in the technological market we can find different OS, which make up a set of basic software, designed to perform tasks on a computer and, simultaneously, work as an intermediary in order to link the user with the computer. In the technological era, there are some operating systems more important, with greater trajectory and recognition than others, being one of the most important factors that leads to defining that one operating system has more recognition than others and the security that come along and is offered to the different users, which allows it to protect it from threats, vulnerabilities, damages or risks that may arise in the different areas of performance.

 The operating systems have countless security mechanisms that are incorporated into it, which applied and managed correctly, provide security and minimize the risk of computer attacks, such as: physical attacks, password stealing, viruses, worms and Trojans, among others. However, these tools are unknown to the user or are not used correctly, opening security gaps that compromise the availability, confidentiality and integrity of the information.

 For this reason, in the following words some security mechanisms of the most used OS, Windows and Linux Ubuntu, which allow the protection of information, resources and services administered directly from the base operating system, are described.

1. **DEVELOPMENT OF THE TOPIC**

 An operating system is a program that works as an intermediary between the user and the hardware of a computer system (Candela, Ruben Garcia, Quesada, Santana, & Santos, 2007), its functions are the easiness to use the device, the efficiency so that the resources of a computer system take advantage of a better way, and the capacity of evolution. This one allows the OS to be built in a way that allows effective development, verification and the introduction of new functions in the system, providing independence between resources and services (Stallings, 1997).

 Regarding security, it has been a concern in the development of operating systems, having special relevance the incorporation of new tools to counteract threats, such as: attacks by intruders, viruses, malware, Denial-of-service attacks (DoS attacks), hardware failures, social engineering, among others (Romero López, 2018).

 Among the most known and used operating systems worldwide, is Windows, a graphical platform through which the entire system is manipulated and the application programs are executed in a more user-friendly way (Hernández, 2006). This one was developed by Microsoft Corporation, and is equipped with a graphical user interface based on the prototype of windows. A window represents a task executed or running. On the other hand, we have Linux operating system, it is a free software OS (it is not owned by any person or company); therefore, it is not necessary to buy a license to install it and use it on a computer. It is a multitasking, multi-user system, compatible with UNIX, and provides a command interface and a graphical interface. The Linux operating system was developed by Linus Torvalds, and is based on the Minix system, which is based on the Unix system. Torvalds was adding tools and utilities, making it operational (Rouse, 2017).

 In the area of computer security, it is important to have clear concepts related to security and protection. Security is the absence of a risk, applying this definition to the corresponding topic, reference is made to the risk of unauthorized access, manipulation of information, manipulation of settings, among others; likewise, protection refers to the different mechanisms used by the OS to take care of information, processes, users, etc., being the main objective to control the access to resources and the usability of them by different users (Seguridad y Protección de los sistemas operativos, 2012), it is so, from this point of view, an operating system is safe if it is well managed and configured (Reyes Muñoz, 2018).

 Some of the vulnerabilities in operating systems are determined by the degree of usability of the same, inevitably, all operating systems contain vulnerabilities and exposures that can be the target of hackers and virus; however, Windows vulnerabilities receive the greatest publicity, due to the number of computers that are managed under this operating system (Securelist, s.f.). In turn, the most used version of the Linux operating system is Ubuntu, which also for its domestic use stands out for having a large percentage of vulnerabilities, such as CVE-2016-5195, CVE-2016-7910, CVE-2016-7911, CVE-2016-7912, CVE-2016-7916 (Velasco, 2017), among others, more than 14 according to the security bulletin published by the Canonical organization in 2016 where some patch recommendations were made to overcome them.

 The following are some security mechanisms incorporated in the Windows and Linux Ubuntu OS, which will provide protection to the computer systems (software, hardware, users and resources) managed by these operating systems.

* 1. **SECURITY MECHANISMS WINDOWS OS**

 Since its inception in 1981, with the version of Windows 1.0, Microsoft bet for launching the Windows operating system to the market. (Hannifin, Alpern, & Alpern, 2010), determining its own course as one of the greatest lines of OS that evolve constantly due to their continuous versions that take part in the world market; talking about security, in its latest version, Windows 10 there are several improvements, one of them is Parental Control, whose functionality is to control and limit by the parents the use that children can give to a portable device, as well as controlling the access to unsuitable Internet content for children (Deidev, 2015). This mechanism allows assigning a Windows account to each child at home and start Windows with his/her own account, where to each account a PIN is assigned that the adult can control. Also, it can be managed from a web page, allowing access from any mobile device and even outside home (Pascual, 2017).

 The secure boot of UEFI in Windows 10, helps to prevent malware from embedding itself in the hardware or starting before the operating system, and preserves the integrity of the other components of the OS. UEFI is an interface that is located between the operating system and the firmware platform, this interface holds a data table that contains information related to the platform, likewise with the startup and the services that start with the OS. One of the features of UEFI and security that is related to the latest Microsoft OS is the system called Secure Boot. This system ensures that only authorized operating systems can boot into the computer. Secure Boot works by reading a cryptographic signature that is in the bootloader of the OS, verifying that this signature is among the authorized keys and previously saved in the UEFI firmware (Aveldaño, 2015).

 Another important feature of the Windows operating system in security, is the information encryption tools, since it is important to take into account any problem of theft or loss of the computer system, for this reason BitLocker is mentioned, it is defined as a feature of security available in the Professional and Enterprise versions of Windows 10, which "encrypts" or "encodes" the data of a computer system to deal with threats such as data theft or compromise the data in case of loss, theft of the computer system or extraction of inappropriate devices (Juan, 2014). BitLocker in Windows 10, offers comprehensive security to the OS protecting from "attacks without connection", which are those that come after by disabling or avoiding the installed operating system, or by physically removing the hard drive to attack the data independently (Bejarano, 2015).

 This security mechanism can be applied in the different storage units of the computer system, internal or external, requiring to access the encrypted information, the access keys registered at the beginning of the process of activation of the same. To activate this encryption tool, you can click on Windows Start, select Control Panel, click on Security, and then on BitLocker Drive Encryption, there you can select the unit you want to encrypt. (Microsoft).

 Another of the security tools incorporated in the Windows operating system is AppLocker, which enhances the functions of application control and the functionality of software restriction policies. This contains new functions and extensions that let to create rules to allow or deny applications to run based on unique file identities, as well as specify what users or groups can run those applications (Microsoft). This tool has taken on greater importance due to its new features in order to provide greater protection and security to the user, allowing the user to restrict through policies the installation of applications in Windows environments.

 It is said that through the configuration of AppLocker different benefits can be obtained, such as: assigning rules to a security group or to a particular user, creating exceptions to the rules, for example, it is possible to create a rule or policies that allow to execute all processes except the remote desktop (mstsc), likewise, it can implement the audit mode, which allows to see the impact of the rule before it is actually implemented. Define rules based on file attributes, import and export rules, have control over applications with extensions .exe, .com. Scripts, DLL files, Windows Installer files and others (Microsoft). AppLocker helps to reduce the administrative burden by preventing users from installing unauthorized or unwanted applications, and then preventing them from presenting system failures (Solvetic Seguridad , 2016).

 Microsoft SmartScreen is an identification system incorporated in Windows 10, which simultaneously, allows to combat phishing, whose scenario is usually associated with the ability to duplicate a web page to make the visitor believe that it is on the original website and not in the fake site, in order to steal confidential information such as user names, passwords, account numbers, among others (Borghello, 2011). The function of this tool is to block the pages that identifies as phishing or malware, acting as a filter, likewise, it uses a dynamic list of phishing and malicious software sites, sending verification notifications and compares downloaded files from the internet and if they correspond to malicious files or software and then it blocks them for security (Microsoft, 2017).

 The Windows hello tool reinforces security for access to the system, allowing entry by PIN, image or fingerprint as a password, also allows access through facial recognition or the iris of the eye, being a useful tool not only to give access to the system but also to access Internet services, and other applications (Microsoft, 2017), getting to leave behind passwords, which are very easy to decipher or to be violated (Microsoft, 2015). Similarly, Microsoft Azure Active Directory is found, which is a comprehensive solution to manage access and identities in the cloud (Marqueting), these are security solutions provided by Windows 10 in terms of identity protection in the OS.

 In the version of the operating system Windows 10, it also includes the antivirus and antimalware software of Microsoft Windows Defender, being this even more effective, by exchanging data using P2P techniques among the almost one billion Windows users, to react in question of milliseconds to possible waves of attacks and malware infections (González, 2016). In this way, it detects new threats and protects against advanced malware (Valle, 2015).

* 1. **SECURITY MECHANISMS OS UBUNTU**

 The Ubuntu operating system (OS) is a GNU / Linux distribution that is easy to use and oriented to both the desktop user and the server. It is maintained by a community of developers that receive support from Canonical enterprise, which sells services related to distribution. (Sanjuán Martínez). Among the most important security mechanisms to activate from the OS, the Iptables firewall stands out, which decided whether a data packet has access, is modified, converted or discarded. Firewalls can be used in any network and work as Internet protection in companies, however, they can also have a dual function: control external accesses inward and also internal accesses outward (Altadill Izura). Just like all OS, the firewall is essential to increase the security of computer systems networks. In the Ubuntu operating system is not the exception, in spite of not being perceived by the users due to the fact that it does not have a graphical interface, its activation mode and configuration are made by means of commands in the console (Sano, Okamoto, & Winarno, 2016).

 Another security mechanism used by Ubuntu and the most important are the so-called Access Control Lists (ACL), which have a functional level that goes hand in hand with the chmod command, and are used to grant permissions and privileges to each of the users and groups to access the files contained in the OS. (Molina, 2010). The ACLs provide customizable security levels, combined with the management of users and groups, according to the scenario presented (Guan & Uhrig, 2013), determining access permissions, traffic filtering and network flow control (Listas de Control de acceso ACL). In addition, Ubuntu users take the security measure of encrypting the disk partitions, meaning the stored data is protected with a password and the more "strong" it is, the harder it will be to break the encryption. To facilitate this task, it is best to use a password manager, this in order to protect the information, before the loss or theft of the computer system, since this information will not be available to anyone, encrypt the disk has an important advantage and is to have greater security, but at the same time it is important to note that it has some disadvantages such as: affects the performance of the computer, although in the user experience is imperceptible; if the password is lost, access and data are lost (Muy Linux, 2014). This disk encryption is usually done during the installation of the operating system and previously making the necessary partitions to the same.

 In the Ubuntu OS there is a variety of features that contribute to maintaining security, PAM (Pluggable Authentication Modules) is one of them, and it works as a flexible mechanism for centralized user authentication. It allows modeling customized security policies depending on the service for different users (Nexolinux, 2013). PAM describes how to develop programs independently of identity verification. For this, these programs use modules that are responsible for the execution request. For example, an authentication policy can authorize a user to execute a command locally, but not remotely (Guillen, 2011).

With this valuable tool available in Unix operating systems, the system administrator can apply security policies, focused on restricting user access, which access to users can be prevented where they cannot access the system outside the hours established by the administrator, for this, PAM has a pam\_time module together with the cron utility. To activate this, the command line is usually used: /etc/pam.d/common-account:account required pam\_time..so (Chamillard, 2011).

Finally, there is the application proxy, it is an application software responsible for eliminating connections to services such as FTP or Telnet, and only allow the use of services where they find a proxy; for example, if the gateway has a proxy only for HTTP and FTP connections, the rest of the services will not be available to the user (Sarubbi, 2008). One of the main functions of a proxy server is to act as a web content cache (http). This improves the performance of a network consuming fewer resources, because in front of a new order of a site that has already been made, instead of generating traffic to the internet, the site whose content is stored on the server is delivered. (Ryte Wiki, s.f.).

 In the Ubuntu OS you can use the SQUID proxy server, freely distributed software to perform the task of a proxy server with very professional features that has the advantages of saving traffic, speed of response time, user demand, filtering of contents, content modification, among others (Scribd). It usually comes along with the most common distributions, although it can also be obtained from its official site (<http://www.squid-cache.org/>). Previous versions are not recommended to 2.4, since they present security flaws, currently the stable version is 2.6 STABLE. SQUID can work as an Intermediate Server (Proxy) and Network content cache for HTTP, FTP, GOPHER and WAIS protocols, SSL Proxy, transparent cache, DNS query cache and many more such as domain filtering and access control by IP and per user. It provides powerful options to have complete control over the sites that are visited, as well as to filter, allow or block the access of certain computers, IPs, domains, etc. (López, 2006). Some of the disadvantages of the proxy, is that you must configure the applications one by one so they can access the Internet through the proxy, for example: web browser, FTP client, mail client, etc.; if it happens to some kind of failure in the proxy, the system will be without an internet connection, so a network administrator is required to look over and perform a permanent maintenance to the proxy (Scribd).

 Snort is an administrative tool considered as an IDS or Intrusion Detection System, in charge of monitoring the events that occur in a computer system in search of intrusion attempts (Mira Alfaro). Snort implements an attack detection and port scanning engine, which allows registering, alerting and responding to any previously defined anomaly such as patterns that correspond to attacks, sweeps, attempts to exploit some vulnerability, protocol analysis, etc. All of this, the tool executes it in real time (Alfon, 2003). In order to use this tool, it will be necessary to carry out its respective installation and configuration; this configuration will depend on the system that will be monitored (Acosta & Rodríguez, 2008).

 Another security tool that can be activated in Ubuntu is SElinux (Security Enhanced Linux), improved security in Linux, which is already included in the Linux kernel to configure access control policies. SELinux allows three basic modes of operation: restrictive, permissive and disabled (debian, s.f.). It is important to highlight that, when you deactivate this security option, the security mechanisms of the system are removed, it is only recommended to disable it in a strictly necessary case or to search for the most appropriate configuration.

 As for Ubuntu's encryption tools, it is already found by default in version 9.10 the encryption of the root directory, with this option also appears the possibility of encrypting the swap partition, since in many cases it is used to store personal data temporarily. The disadvantage of activating the encryption of the root directory is that the option to hibernate the computer system will be lost, since the encryption method with the swap partition is incompatible at this moment with this mode (Bitel, 2009). Also, among the different options to protect a removable memory through encryption, there are tools for Ubuntu with graphical environment such as Gnome Encfs Manager or Crypt Folder-Indicator, but it can also resort to the one that comes integrated by default in the system, allowing to carry always the encrypted information, so that when entering the memory in the computer asks for the password to decrypt the content (Atareao, 2015).

 Ubuntu, as well as the other versions of Linux, despite being a secure system, has its free ClamAV antivirus for Unix / Linux systems, which provides support for compressed files such as RAR, Zip, Gzip and Bzip 2, among others. It detects more than 320,000 viruses, worms, Trojans, including Microsoft Office macro virus (Guerrero Clavo, Monteza León, Quintana Jaramillo, Sánchez Tejada, & Vásquez Villalobos, 2009).

 For the configuration of secure passwords in the Ubuntu and Debian versions of Linux, the libpam\_cracklib library can be used, which will verify that the new password to be entered is not part of a dictionary. This library also verifies that the new password is not equal to a previously used one, or if it has been reused by changing only one character, likewise, it checks if the password is too short or little complex and also ensures that it does not have a single character entered several times consecutively, etc. (De Luz, 2016).

 However, there are also other tools for managing passwords securely such as KeePass, placing all passwords in a database blocked simultaneously with a master key or a key file, thus protecting all passwords, the base of data is also encrypted with encryption algorithms such as AES and Twofish, the application will record dates of creation, modification, access and expiration of each password (Security in-a-box, 2016).

1. **CONCLUSION**

 During the this study, some security mechanisms of the Windows and Ubuntu operating systems could be established; however, it will depend on its correct configuration and use to reinforce the security of all the resources that are managed from them. Likewise, it can be evidenced that in spite of having different security tools incorporated into each OS, mostly, security depends on the user since this is the one who finally decides what to do and what not to do, where to access or not, and to whom give the permissions and privileges of the system, without neglecting, that no matter how careful you are you can always be exposed to vulnerabilities or threats that arise in the systems, such as possible virus attacks, information theft, malware, among others, it should be noted that Linux operating systems, in this case the Ubuntu version, has an advantage in terms of security, because its use is not very frequent and many users do not know how it works, while the Windows operating system is one of the most used and also the security of this will depend on the activation of the functionalities incorporated in it.

**REFERENCES**

Acosta, A., & Rodríguez, L. (2008). Snort como herramienta administrativa. *Inventum*(5), 74-78.

Alfon. (2003, Agosto 19). *Maestros del Web.* Retrieved from http://www.maestrosdelweb.com/snort/

Altadill Izura, P. X. (n.d.). *IPTABLES: manual práctico.*

Atareao. (2015, Mayo 8). *El Atareao.* Retrieved from https://www.atareao.es/software/seguridad/proteger-tus-unidades-usb-mediante-cifrado-en-ubuntu/

Aveldaño, C. (2015, 12 01). *Sidertia*. Retrieved from https://www.sidertia.com/Home/Community/Blog/2015/12/01/Windows-10-II-UEFI-y-TPM-arranque-eficaz-y-seguro

Bejarano, L. (2015, Diciembre 15). *Muy Computer Pro.* Retrieved from http://muycomputerpro.com/movilidad-profesional/2015/12/15/bitlocker-windows-10/

Bitel, J. (2009). *ubuntu guia.* Retrieved from http://www.ubuntu-guia.com/2009/10/encriptacion-de-unidades-para-ubuntu.html

Borghello, C. (2011). *Segu.Info.* Retrieved from https://www.segu-info.com.ar/malware/phishing.htm

Candela, S., Ruben Garcia, C., Quesada, A., Santana, F. J., & Santos, J. M. (2007). *Fundamentos de sistemas operativos.* Madrid: Magallanes.

Chamillard, G. (2011). *UBUNTU: Administración de un sistema Linux.* Barcelona: Editions ENI. Retrieved from https://books.google.com.co/books?id=XzQazm9tLXEC&pg=PA336&lpg=PA336&dq=mecanismos+de+seguridad+en+ubuntu&source=bl&ots=2El33qmHoo&sig=0bk5uqGn89Z-nfzGvIfTmKZaog8&hl=es&sa=X&ved=0ahUKEwjW-e2B5JjUAhXHOCYKHaaVCyQ4ChDoAQgzMAQ#v=onepage&q=mecanismos%20de%20se

De Luz, S. (2016, Septiembre 13). *Redes Zone.* Retrieved from https://www.redeszone.net/2016/09/13/configura-la-politica-contrasenas-debian-ubuntu-proteger-mas-equipo/

*debian*. (n.d.). Retrieved from https://debian-handbook.info/browse/es-ES/stable/sect.selinux.html

Deidev, G. (2015, 08 25). *SecureKids*. Retrieved from https://securekids.es/que-es-el-control-parental-y-para-que-sirve/

González, C. (2016, Septiembre 4). *ADSL Zone.* Retrieved from https://www.adslzone.net/2016/09/04/necesario-instalar-antivirus-windows-10/

Guan, E., & Uhrig, M. N. (2013). *Lista de control de acceso.* Oro Verde: Free Software Foundation.

Guerrero Clavo, J., Monteza León, A., Quintana Jaramillo, S., Sánchez Tejada, M., & Vásquez Villalobos, J. (2009). *Linux.* Chiclayo.

Guillen, A. (2011, Julio 7). *make install.es.* Retrieved Mayo 15, 2018, from http://www.makeinstall.es/2011/07/que-es-pluggable-authentication-modules.html

Hannifin, D., Alpern, N. J., & Alpern, J. (2010). Chapter 10 - Securing Windows Server 2008 R2. In *Microsoft Windows Server 2008 R2* (pp. 461-532). doi:https://doi.org/10.1016/B978-1-59749-578-3.00010-4

Hernández. (2006). *Sistema operativo Windows: presente y futuro.* EL Cid Editor.

Juan. (2014, Septiembre 3). *Muy Computer Pro.* Retrieved from https://www.muycomputerpro.com/movilidad-profesional/2014/09/03/seguridad-informatica-en-movilidad/

Listas de Control de acceso ACL. (n.d.).

López, E. (2006). *Servidor Proxy SQUID.*

Marqueting. (n.d.). *apen .* Retrieved from https://apen.es/2017/02/16/windows-10-es-el-sistema-operativo-de-microsoft-mas-seguro/

Microsoft. (2015, Marzo 17). *Microsoft Blogs.* Retrieved from https://blogs.windows.com/latam/2015/03/17/windows-10-mas-personal-y-mas-seguro-con-windows-hello/#3rRlOpWY1FOjV2WA.97

Microsoft. (2017, Noviembre 30). *Support Microsoft.* Retrieved from https://support.microsoft.com/es-ec/help/17215/windows-10-what-is-hello

Microsoft. (2017, Noviembre 3). *Support Microsoft.* Retrieved from https://support.microsoft.com/es-co/help/17443/windows-internet-explorer-smartscreen-filter-faq

Microsoft. (n.d.). *Microsoft MSDN Library.* Retrieved from https://msdn.microsoft.com/es-es/library/hh831440(v=ws.11).aspx

Microsoft. (n.d.). *TechNet Microsoft.* Retrieved from https://technet.microsoft.com/es-es/library/cc664686.aspx#mainSection

Microsoft. (n.d.). *TechNet Microsoft.* Retrieved from https://technet.microsoft.com/es-es/library/mt431866(v=vs.85).aspx

Mira Alfaro, E. J. (n.d.). *Implantación de un sistema de detección de intrusos en la Universidad de Valencia.* Valencia.

Molina, D. (2010, Julio 12). *Ubuntu a fondo.* Retrieved Junio 2, 2018, from http://dmolinap.blogspot.com/2010/07/seguridad-en-ubuntu-ii-usuarios-y.html

Muy Linux. (2014, Julio 23). *MuyLinux.* Retrieved from https://www.muylinux.com/2014/07/23/cifrado-disco-ubuntu/

Nexolinux. (2013, Marzo 7). *Nexolinux.* Retrieved Junio 1, 2018, from http://www.nexolinux.com/autenticacion-pam-en-linux-elevando-la-seguridad/

Pascual, J. A. (2017, Junio 4). *Computer Hoy.* Retrieved from https://computerhoy.com/paso-a-paso/software/como-activar-configurar-control-parental-windows-10-62596

Reyes Muñoz, D. (2018, Febrero 23). *AntiFraude.* Retrieved from http://www.antifraude.org/2018/02/cual-es-el-sistema-operativo-mas-seguro/

Romero López, G. (2018). Servidores seguros: Seguridad en sistemas operativos.

Rouse, M. (2017, Enero). *SearchDataCenter en Español*. Retrieved Abril 2017, from http://searchdatacenter.techtarget.com/es/definicion/Sistema-operativo-Linux

*Ryte Wiki*. (n.d.). Retrieved from https://es.ryte.com/wiki/Servidor\_Proxy

Sanjuán Martínez, O. (n.d.). *Guía Practica 1: Introducción y manejo del sistema operativo.* Retrieved from https://564376d2-a-62cb3a1a-s-sites.googlegroups.com/site/informaticabiologia/practicas/GUIAPRACTICA1.pdf?attachauth=ANoY7cr1C0uEOFZbUy8vE76CUjeYeZI36sHKpIqWEM34wbvCrWHQfPtcPGBs0uR8EUQqg2T2OGzCNdnoDd\_WG7fbzXYtxvHWpHoPEr-CHvaM5EO9ODkibhupK9fDt94ZB6PKsuKfgq

Sano, F., Okamoto, T., & Winarno, I. (2016). *Science Direct.* Retrieved Junio 1, 2018, from www.sciencedirect.com/science/article/pii/S1877050916320208

Sarubbi, J. P. (2008). *Seguridad informática: Técnicas de defensa comunes bajo variantes del sistema operativo Unix.* Buenos Aires. Retrieved from https://books.google.com.co/books?id=o3war7zF-g8C&printsec=frontcover&hl=es&source=gbs\_ge\_summary\_r&cad=0#v=onepage&q&f=false

*Scribd.* (n.d.). Retrieved from https://es.scribd.com/document/218846535/Proxy

*Scribd.* (n.d.). Retrieved from https://es.scribd.com/document/225148190/Ventajas-y-Desventajas-de-Un-Servidor-Proxy

*Securelist*. (n.d.). Retrieved Mayo 23, 2018, from https://securelist.lat/threats/ejemplos-de-vulnerabilidades/

*Security in-a-box.* (2016, Agosto 10). Retrieved from https://securityinabox.org/es/guide/keepassx/linux/

*Seguridad y Protección de los sistemas operativos.* (2012, Noviembre 5). Retrieved Abril 28, 2018, from http://blog.utp.edu.co/seguridadso/

Solvetic Seguridad . (2016, Julio 11). *Solvetic*. Retrieved from https://www.solvetic.com/tutoriales/article/2819-bloquear-uso-de-aplicaciones-windows-10/

Stallings, W. (1997). *Operating Systems. Second Edition.* Upper Saddle River, NJ: Prentice Hall.

Valle, M. (2015, Julio 29). *Globb Security.* Retrieved from https://globbsecurity.com/seguridad-windows-10-35385/

Velasco, R. (2017, Abril 18). *Redes Zone.* Retrieved Mayo 23, 2018, from https://www.redeszone.net/2017/04/18/solucionadas-14-vulnerabilidades-ubuntu-16-04-lts/