Open-Source tools: Incidence in the wireless security of the Technical University of Babahoyo

Herramientas de código abierto: Incidencia en la seguridad inalámbrica de la Universidad Técnica de Babahoyo

Joffre León-Acurio[1,*], Alfredo Vite[1,†], Carlos Sisa[1,‡], Luis Bastidas Zambrano[1,⊗], and Alex Santamaría Philco[2,θ]
[1]Universidad Técnica de Babahoyo, Ecuador
[2]Universidad Laica Eloy Alfaro de Manabí, Ecuador
{jleonv;avite;csisa;lbastidas}@utb.edu.ec;alex.santamaria@live.uleam.edu.ec

Received: August 15, 2017 — **Accepted:** September 15, 2017

How to cite: León-Acurio, J., Vite, A., Sisa, C., Bastidas Zambrano, L., & Santamaría Philco, A. (2018). Open-Source tools: Incidence in the wireless security of the Technical University of Babahoyo. *Journal of Science and Research: Revista Ciencia e Investigación, 3(CITT2017), 56-60.* https://doi.org/10.26910/issn.2528-8083vol3issCITT2017.2018pp56-60

***Abstract*—Computer security is a fundamental part of an organization, especially in Higher Education institutions, where there is very sensitive information, capable of being vulnerable by different methods of intrusion, the most common being free access through wireless points. The main objective of this research is to analyze the impact of the open source tools in charge of managing the security information of the wireless network, such as OSSIM, a set of active and passive components used to manage events that generate traffic within the network. net. This research exposes the use of free software as a viable option of low cost to solve the problems that afflict student staff, such as lack of access to academic services, problems of wireless interconnectivity, with the purpose to restore confidence in students in the Use of the services offered by the institution for research-related development, guaranteeing free and free access to the internet. The level of dissatisfaction on the part of the students confirms the problem presented at the Technical University of Babahoyo, thus confirming the positive influence of the Open-Source tools for the institution's wireless security.**

***Keywords*—Open-Source Tools, wireless security, higher education institution, free and free internet access.**

***Resumen*—La seguridad informática es una parte fundamental de una organización, especialmente en Higher Instituciones educativas, donde hay información muy sensible, capaz de ser vulnerables por diferentes métodos de intrusión, siendo el acceso libre más común a través de puntos inalámbricos. El objetivo principal de esta investigación es analizar el impacto de las herramientas de código abierto encargadas de administrar la información de seguridad de la red inalámbrica, como OSSIM, un conjunto de componentes activos y pasivos utilizados para administrar eventos que generan tráfico dentro de la red. red. Esta investigación expone el uso de software libre como una opción viable de bajo costo para resolver los problemas que afligen al estudiante personal, como la falta de acceso a servicios académicos, problemas de interconexión inalámbrica, con el propósito de restaurar la confianza en los estudiantes en el uso de los servicios. ofrecido por la institución para el desarrollo relacionado con la investigación, garantizando de forma gratuita y gratuita acceso a Internet. El nivel de insatisfacción por parte de los estudiantes confirma el problema presentado en la Universidad Técnica de Babahoyo, confirmando así la influencia positiva de las herramientas de código abierto para la seguridad inalámbrica de la institución.**

***Palabras Clave*—Herramientas de código abierto, seguridad inalámbrica, institución de educación superior, gratis y acceso gratuito a internet.**

INTRODUCTION

The technological progress is constant, the technologies and innovations are recurrent, during the last years the massive use of the wireless networks are populated, highlighting benefits of mobility where through a wireless device a user has the ability to elaborate their daily activities with Normality, taking the relevant security measures through the use of technological solutions such as perimeter security, unified wireless platforms, and access controls. The present investigation will have as an aim to analyze the incidence that could have the use of open source tools in the security of the wireless network of the Technical University of Babahoyo.

The access to the internet by the students of the different faculties, through the use of wireless access points placed in specific sectors within the institution, where the use of security protocols is not a sufficient mechanism that offers the protection of the information Of school administrators, teachers and students, and it is clear that there is no 100 % security within a network, so the systems department was forced to use a series of configurations that control access to

[*]Magister en Informática Empresarial.
[†]Ingeniero en Sistemas.
[‡]Ingeniero en Sistemas.
[⊗]Magister en Informática Empresarial.
[θ]Master Universitario en Ingenería de Software, Métodos Formales y Sistemas de Información.

Web sites, making it clear that having freedom of navigation to various inappropriate pages are exposed to the infection of advertisements, add-ons that are added to the browser due to the lack of knowledge of users, you do not get to have a control of The events and use that is given to the network. The purpose should be to use authentication and identification mechanisms, in addition to the control and management of network traffic, making it clear that the people benefiting from the services provided by the educational institution are direct students, thus excluding The misuse of unidentified users through the use of different high-gain devices will benefit from these services, so that adequate protection for the organization of the Technical University of Babahoyo would be manifested.

Security in information systems, represent the set of means and techniques implemented to ensure the integrity and not disseminate in an investible way the data that go through the information system, understanding as such the set of data and resources (Physical, logical and human) that allow to store and circulate the information it contains. It also represents the network of actors involved, who exchange data, access and use it.

Open-Source forms a large part of the Web 3.0 revolution as a fundamental factor in the collaboration of several people working to develop a usable tool, and even when it is finished, some of these same people or others can continue to improve In open-source development, encouraging collaborative development through the use of technologies that benefit the common good, to solve a problem (Tasner, 2011). ISO 27035 considers a security event to be an occurrence identified in the state of a system, service or network, indicating a possible violation of the security of the information, policy or failure of the controls, a previously unknown situation that may Be relevant to safety. The following is a series of examples related to safety events:

- Change security policies of a system.
- Failure to access a specific system.
- Creation of new users.
- Connections to a system.
- Password change notification of a user with administrator privileges.

The entity in charge of hosting security incidents is Ecuador's Computer Incident Response Center EcuCERT The Attorney General's Office in the first 5 months of 2016 recorded 530 computer crimes, in the provinces with the greatest impact Guayas 18 cases; Pichincha, 145; Manabí, 24; El Oro, 22; In the rest of provinces a smaller number was registered. The majority of complaints (368) correspond to the crime of "fraudulent appropriation by electronic means". A study by the National Police, Interpol, Ecuador's response center for Computer Incidents (Ecucert), supported by similar organizations in Latin America, indicates that 85 % of attacks on computer systems are caused by computer errors. Consumers, who do not take precautions when accessing social networks, using email, and using user and password.

TYPES OF INCIDENTS

- IP-PBX fraud: computer crime caused by people capable of making use of the local and cellular telephone service without self-restraint.
- Phishing: a technique used through social engineering for the purpose of obtaining credentials from users, with the use of fake web portals especially from banks.
- Open Proxy: used by spammers to send spam
- BotNet: is a kind of infection where the botnet creator has the ability to control infected computers remotely.
- Defacement: this attack consists of intrusion through various techniques, which mainly seek the vulnerabilities of the server or web system programming, usually the intrusion is done by injection SQL
- Fraud in social networks: this is the intrusion of applications in the mobile through advertisements which are responsible for receiving the user for its subsequent installation, this way is carried out theft of credentials and important data of the root user.

The percentage of attacks by connected users in Latin American countries is shown in Figure 1.

País	Porcentaje
Brasil	49,9%
Perú	41,9%
Bolivia	41,8%
Chile	40,0%
México	39,9%
Colombia	39,3%
Guatemala	37,5%
Ecuador	36,1%
Venezuela	36,0%
Uruguay	30,0%
Argentina	29,5%

Figure 1. Attack attempts by connected users in Latin America.
Source: (BBC, 2016).

OSSIM(Open Source Security Information Management) Open source distribution to build a security monitoring infrastructure that aims to provide a framework for centralizing, organizing and improving detection and visibility capabilities in monitoring security events within an institution (Figure 2). Advanced Network Threat Detector, developed using data shared by the Open Amenza Exchange (OTX) community, in addition to compliance with standards and basic reporting to support the information required by auditors and managers.

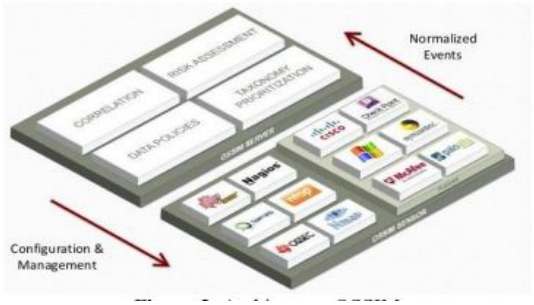

Figure 2. Architecture OSSIM.
Source: (Hargrave, 2013).

MONITORING TOOLS CONSOLA FORENSE Y MONITORES DE RED

Capacities

- Visibility dashboard
- Risk monitors and compartment for monitoring
- Prioritization
- Correlation
- Risk assessment

Kismet is a sniffer packet sniffer and intruder detector for 802.11 wireless networks its use is made through any wireless card that supports monitoring mode by exporting .log files are a great help as a source of information for OSSIM.

MikroTik HotSpot Provides authentication for users before accessing public networks, and has different methods of user authentication that uses the local client database on the router or a remote Radius server, restricting access to some web pages without authorization, Personalization of the portal when logging on where it is easy to display information about the institution, automatic and transparent change any IP address of a client to a valid address.

In RouterOS version 6.37.1.01 there are six different authentication methods which can be used one or more of them at the same time.

PAP HTTP: simple method that shows the HotSpot login page where it expects to obtain the information (username and password) to authenticate the user.

CHAP HTTP: Standard method that includes hash MD5 CHAP is used together with the user's password for the calculation of the string that will be sent to the HotSpot in order that the password is never sent in clear text over the network.

HTTPS: it's similar to the HTTP PAP method, but with the difference that it uses SSL protocol to encrypt the transmissions.

- HTTP cookie: after each successful login a cookie would be sent to the web browser and the same cookie would be added to the list of active HTTP cookies. The next time the user tries to connect, the web browser will attempt to connect, the web browser will send the saved HTTP cookie. This cookie is compared to that stored in the HotSpot gateway and only if the randomly generated source I source MAC address matches those stored in the gateway the user will register automatically.
- MAC address: attempts to authenticate clients as soon as they appear in the host list using the client's MAC address as the username.
- Trial: Users may be authorized to use the service free of charge for a period of time to be freely used with some limitations imposed by the provided user profile. In case the MAC address still has some unused test time, the login page will contain the test login link. The time is reset automatically so that anyone can use the MAC address for 30 minutes a day without having to register).

WLAN ARCHITECTURE

WLANs provide access to the network by means of a brocade signal through a radio frequency (RF) carrier. A station may

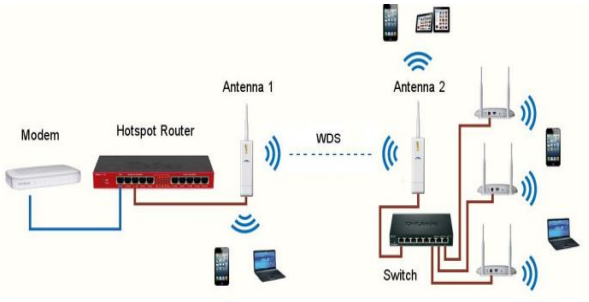

Figure 3. Hotspot router Mikrotik together with antennas connected WDS.

Source: (Mywifiservice, 2015).

be within a range of transmitters, which use a "service set identifier"(SSID). The station uses the SSID as a filter between received signals and locates the one it wants to listen to. Wireless networks have different modes of operation, among them are:

BSS (Basic Service Set): The BSS mode is the one that is normally used, this the mode is also called infrastructure mode. In this configuration a certain number of access points are connected to a wired network, each wireless network has its own the name which is the SSID of the network.

Wireless clients connect to this access points and the IEEE 802.11 standard defines the protocol used to make this connection. A wireless client can associate with a specific wireless network by specifying the SSID which can also be associated with any network that is available just by not specifying any SSID, its elements are:

The Access Point (AP). This works as a wireless hub of the WLAN network:

- All traffic passes through
- Extend a LAN
- Bridge between LAN and wireless stations
- It can serve as a repeater in the connectivity of the two WLAN roaming networks:
- Provides the possibility for a station to associate with other APs
- Web interface for your configuration
- Deploying several can cover a large area Stations:
- PCs, laptops, PDAs, etc.

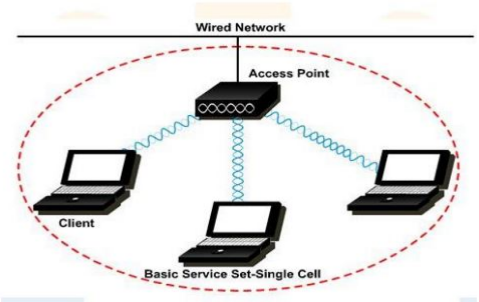

Figure 4. Illustration of a BS.

Source: http://es.scrib.com/doc/5703711/38/IBSS-Independent-BSS.

AD HOC PEER TO PEER

Also known as MANET "Mobile ad hoc networks". AD HOC comes from Latin and refers to something improvised, while in communications the purpose of ad hoc is to provide flexibility and autonomy by exploiting the principles of self-organization.

An ad hoc mobile network is a network formed without any central administration or there is no central node but consists of mobile nodes that use a wireless interface to send packets of data where all computers are under equal conditions.

Figure 5. Illustration of a connection AD HOC.
Source: http://www.eusso.com/Models/Wieless/UGL2454-01XR/UGL2454-01XR.

METHODOLOGY

The methodology used for the development of this research work is based on the documentary and bibliographic methodology, which facilitates to base the theoretical bases, according to an analysis and scientific foundation that frames the knowledge related to the problem, in addition to the references found In texts for the use of active and passive open source tools for the control of the access of the wireless security.

The paradigm applied to the development of the research is framed in a qualitative-quantitative structure, through the qualitative research modality will obtain references related to the problem about the control and security of the wireless network of the Technical University of Babahoyo. As for the quantitative research modality, it will be used to support the problems that cause users of the wireless network to be dissatisfied, through the results obtained from the surveys, carried out to the students of the campus of the Technical University of Babahoyo.

Within the techniques and instruments to be used to obtain information regarding the state of the wireless security of the Technical University of Babahoyo, the instrument to complement a certain technique is the application of a questionnaire of questions.

The population to be understood for the development of this research, will be made up to 6,698 students of the different faculties and extensions that count the Technical University of Babahoyo, through this number of population was carried out a sample that resulted in 377 in total to be surveyed.

RESULTS

According to the results related to the methodologies used during the development of the research, it is focused, in the execution of surveys to the students of the Technical University of Babahoyo, a person who directly intervene in the problem, through a questionnaire of Questions, which emphasizes the following question in question, which shows in real values the correspondent satisfaction with the internet service provided by the educational institution.

How do you consider the internet service in the last 6 months?.

Table 1. Resultados de encuesta

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Excelente	14	4 %
Muy buena	0	0 %
Buena	0	0 %
Regular	153	41 %
Mala	71	19 %
Muy mala	139	37 %
TOTAL	377	100 %

Source: Prepared by the authors.

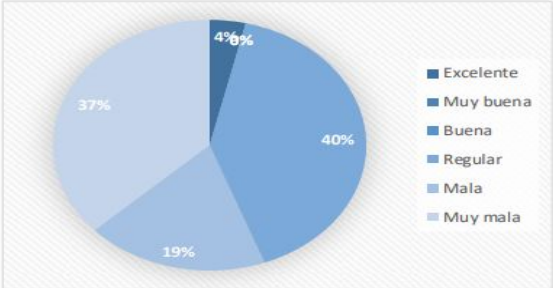

Figure 6. Description of results.
Source: Prepared by the authors.

ANALYSIS AND INTERPRETATION

Form students surveyed 4 % considered that the internet service during the last 6 months is excellent, 0 % very good, 0 % good, 41 % regular, 19 % bad and 37 % very poor. The students underscore the need to have a stable internet service for the accomplishment of their academic tasks and that in some way do not feel at ease at present.

STATISTICAL TEST APPLIED

The statistical test applied was Chi-square based on the execution of the in-slopes and tabulation of results, the degree of significance is detailed as follows corresponds to 95 % reliability where the value of chi-square is 11.07 and the result of the calculated chi is 42.38 much higher than the theoretical chi-square so the null hypothesis is rejected and the alternative hypothesis is accepted it is understood to the hypothesis proposed that the Open source tools affect the security in the wireless network of the Technical University of Babahoyo (See Table 2).

DISCUSSION

Through this research, the benefits of using open source tools as a solution to the insecurity of the wireless network within institutions of higher education, involving students and

Table 2. Chi-square test

FRECUENCIAS OBSERVADAS			TOTAL
CATEGORIA	PREGUNTA 2 Estudiantes	PREGUNTA 2 Docentes	
Excelente	14	2	16
Muy buena	0	1	1
Buena	0	5	5
Regular	153	22	175
Mala	71	10	81
Muy mala	139	15	154
TOTAL	377	55	432
	0.87	0.13	1

FRECUENCIA ESPERADAS			TOTAL
CATEGORIA	PREGUNTA	PREGUNTA	
Excelente	13,96	2,04	16,00
Muy buena	0,87	0,13	1,00
Buena	4,36	0,64	5,00
Regular	152,72	22,28	175,00
Mala	70,69	10,31	81,00
Muy mala	134,39	19,61	154,00
TOTAL	377,00	55,00	432,00

FRECUENCIAS OBSERVADAS			TOTAL
CATEGORIA	PREGUNTA	PREGUNTA	
Excelente	0,00	0,00	
Muy buena	0,87	5,98	
Buena	4,36	29,91	
Regular	0,00	0,00	
Mala	0,00	0,01	Chi
Muy mala	0,16	1,08	Cuadrado
TOTAL	5,40	36,99	42,38

Source: Prepared by the authors.

teachers are demonstrated, hoping that it will be possible to secure the use of instruments That provides the stability in the internet access in addition to the good use of the services offered by the UTB is used in a direct way with the students through the use of interconnection technology that establishes in a reliable, safe, timely and that guarantees in Mobility. The results obtained through the application of applied statistical techniques, instruments and tests have as a reference that the users' dissatisfaction is notorious according to the internet access service which has a direct impact on the development of their daily academic activities. The IT unit will take into account the implementation to improve and achieve an advanced level of security for the wireless internet.

CONCLUSIONS

- The students and teachers of the institution consider the use of the internet as a fundamental aspect for the elaboration of academic activities and search of information for the application of research projects benefiting the academic and technological advancement of students and teachers Of the different careers offered by the Technical University of Babahoyo.
- The use of academic platforms is of paramount importance to teachers and through them they can share information and evaluate students. Internet access is fundamental for its use, the comments of the students have a lot of emphases, in the nonfunctioning of the academic platforms and the constant attacks suffered by the main page of the U.T.B
- The control and management of the wireless network traffic through tools that are responsible for notifying security flaws and alerting the misuse and intrusion of users that are not related to the services offered by the Technical University of Babahoyo, would serve Of great help to strengthen security levels, offering in a timely, safe and accessible manner the benefits that should be offered within the campus of the educational institution for development and academic research.

BIBLIOGRAPHIC REFERENCES

BBC (2016). "12 ataques por segundo": cuáles son los países de América Latina más amenazados por "malware BBC Mundo.

Hargrave (2013). Solving the Open Source Security Puzzle.

Mywifiservice (2015). Building an HotSpot Wi-Fi network.

Tasner, M. S. (2011). *Marketing in the moment : the practical guide to using Web 3.0 marketing to reach your customers first*. FT Press.