

DESIGN OF THE SECURITY MODEL OF DEFENSE IN DEPTH, IN THE USER LEVELS, INTERNAL NETWORK AND PERIMETER NETWORK BASED ON THE ISO/IEC (March 2015)

Author: A. Zura
Director: MSc. Maya E.

Summary - GAD Municipal of Otavalo provides various telecommunications services for the benefit of the population, for it has a network of distributed data in internal network, wireless links and access to ICT's in both urban and rural; which is why it is important that your infrastructure deliver high availability and quality of service, supporting large amounts of traffic, in addition to possessing scalability, flexibility and security.

This work raises a design of multi-tier security model, known as defense in depth; the same which will be applied at three levels; at the user level is developed a Manual of rules and procedures of information security on the basis of the ISO IEC 27002, which socialized in conjunction with the network administrator to users; in the level of internal network design is a hierarchical model based on the study by layers; and in the perimeter network through tools-based intrusion detection engines Suricata under a unified platform called SELKS.

In addition using a referential budget it was demonstrated that it is possible to migrate a proprietary solution to a solution under free software; enabling you to minimize costs and make better use of resources.

I. INTRODUCTION

En the present public institutions tend to provide various telecommunication services for the benefit of the population. The GAD Municipal of Otavalo is no exception, as it has a network of distributed data in internal network, wireless links and access to ICT's in both urban and rural. To achieve this objective, in recent years have improved their infrastructure.

Year after year has increased the users of the network of the GAD Municipal of Otavalo, causing difficulty in managing the network because it has not been taken the considerations of segmentation in the same, causing drop in the links. But the increasing numbers of users not only brings problems of administration, but also problems in information security, in spite of the fact that this topic has been taken into account and that has not presented any kind of threat or active attack , has been taken as a security mechanism, the acquisition of two firewalls UTM Sophos, which have been configured with minimum security policies based on the restriction of web pages for the intranet, policies that are not sufficient to prevent attacks of access, of modification, as well as denial of service attacks, among others; making the network even vulnerable

both internally and externally.

Because of these drawbacks, it will be necessary to implement mechanisms to counteract these vulnerabilities, taking into account that the level of security not only should be considered internally but outside of it, in the network must be segmented by applying controls access lists toward the VLANs, deploy the security model based on the "Defense in Depth" in the user levels, internal network and perimeter network; and consider new security policies that will help to prevent attacks by detecting to time and giving a timely response to prevent further damage.

II. ANALYSIS OF THE CURRENT STATUS OF THE DATA NETWORK

There are several methodologies for the analysis of the level of information security within an organization. In this case study was chosen the methodology of OSSTMM¹ of the Open Methodology of testing of security) due to the features and benefits that this methodology offers.

AND sta methodology covers the entire operational safety, and engage in the different areas or channels as described by the manual, and it can be seen in Table I :

¹ one of the most complete professional standards and used in Security Audits to analyze the security of the systems. Describes in great detail, the phases that should be performed for the execution of the audit. (Alvarado (Manual

Table I

SCOPE OF OSSTMM			
Physical Security to		Security of spectrum ^{to}	
		Security of Communications ^{to}	
Human ^b	Physical ^b	Communications Wireless ^b	Telecommunications (b) Data Networks ^b
Understands the human element of the communication.	Includes the element of tangible security.	Includes all electronic communications, signals, and fumes that are produced in the (EM).	Includes all the telecommunications networks, digital or analog. Includes all the electronic systems and data networks.

Note: The table was adapted from (Herzog, OSSTMM 3.0)
 Classes : are defined as areas of study, research or operation.

^B channels: are the specific means of interaction with the assets .

A. HUMAN CHANNEL

The safety assessment on the human channel, was focused on the level of access and trust that this factor provides the security of the information. To realize this is evidence of direct observation and social engineering, with what we were able to obtain valuable information that compormete information security.

The results obtained are muetsran in Fig.1, the same that reflect chord to the parameters of the methodology that safety is quite low, taking into account that this evaluates the various policies and procedures implemented by the administration.

The controls being security mechanisms put in place to protect the operations, it should be emphasized that it was a high priority in regard to the compensation of personnel, but not as well in other cont which roles are completely null as the subjugation and continuity.

The limitations are weighted individually, but these are directly related to some controls and operational safety, it is as well that due to development and has limitations are void as in the non-repudiation; and almost nil in regard to confidentiality, privacy, integrity and alarm.

The safety assessment on the physical channel, was focused on the level of access to the room of equipment, the availability of devices, and especially to the response to contingencies of the same.

The results obtained are muetsran in Fig 2., the same as reflected in keeping with the parameters of the methodology that lto operational security is relatively high, taking into account that this evaluates the various policies and procedures implemented by the administration. This reflects the priority it has been given to the physical security.

The controls being security mechanisms put in place to protect the operations, it should be emphasized that according to test made, unfortunately do not have implemented controls respective to the physical security, this being a white computer for the attackers.

The limitations are weighted individually, but these are directly related to some controls and operational safety, is so because the values in operational safety are relatively high, these values predominate to the calculation of the limitations is also relatively high. And so is of great concern because it is a limitation of very high vulnerability in relation to other values.

Human Security Testing			
OSSTMM version 3.0			
Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.			
OPSEC			
Visibility	1		
Access	3		
Trust	2		
Total (Porosity)	6		
CONTROLS			
Class A		Missing	
Authentication	3	3	
Indemnification	6	0	
Resilience	1	5	
Subjugation	0	6	
Continuity	0	6	
Total Class A	10	20	
Class B		Missing	
Non-Repudiation	0	6	
Confidentiality	1	5	
Privacy	1	5	
Integrity	1	5	
Alarm	1	5	
Total Class B	4	26	
All Controls Total	14	46	
Whole Coverage	23.33%	76.67%	
LIMITATIONS		Item Value	Total Value
Vulnerabilities	2	8.666667	17.333333
Weaknesses	1	4.333333	4.333333
Concerns	4	5.333333	21.333333
Exposures	1	1.677778	1.677778
Anomalies	0	1.422222	0.000000
Total # Limitations	8	44.6778	83.57
Actual Security: 83,6299 ravs			

Fig. 1 Result of the calculation of the RAVs in human channel
 Source: OSSTMM Calculator

B. PHYSICAL CHANNEL

Physical Security Testing			
OSSTMM version 3.0			
Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.			
OPSEC	Visibility	8	
	Access	4	
	Trust	9	
	Total (Porosity)	21	
ISECOM			
	OPSEC		11,038515
	True Controls		4,482838
CONTROLS			
Class A			
	Authentication	1	20
	Indemnification	8	13
	Resilience	0	21
	Subjugation	0	21
	Continuity	1	20
	Total Class A	10	95
Class B			
	Non-Repudiation	0	21
	Confidentiality	0	21
	Privacy	1	20
	Integrity	2	19
	Alarm	0	21
	Total Class B	3	102
	All Controls Total	13	197
	Whole Coverage	6.19%	93.81%
True Missing			
	True Coverage A		9.52%
	True Coverage B		2.86%
	Total True Coverage		6.19%
OSSTMM			
	Limitations		17,846690
	Security Δ		-24.40
	True Protection		75.40
LIMITATIONS			
	Vulnerabilities	10	10,380952
	Weaknesses	5	5,523810
	Concerns	4	5,857143
	Exposures	8	1,440816
	Anomalies	1	1,306803
	Total # Limitations	28	167,6905
Actual Security: 76,2728 ravs			
OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM			

Fig. 2. Result of the calculation of RAVs in the physical channel.
Source: OSSTMM Calculator

C. TELECOMMUNICATIONS CHANNEL

The safety assessment on the channel of telecommunications, was made a map of communication protocols with the help of the software NetScan, to which it was a port scan, shaming the level of access to the applications.

The results obtained are muetsran in Fig.3, the same that reflect chord to the parameters of the methodology that I to operational security is high, mainly in the aspect of Trust, in which it has been considered all the ports that are open, analyzing the because of its state. This reflects the importance that is given to the security of telecommunications.

The controls being security mechanisms put in place to protect the operations, it should be emphasized that according to the test, you have solely controls of compensation, authentication and privacy; meanwhile the other controls are zero; thus leaving a gap for the insecurity of the information.

The limitations are weighted individually, but these are directly related to some controls and operational safety, is so because the values in operational safety are relatively high, these values predominate to the calculation of the limitations is also relatively high. It is as well that highlight limitations such as the vulnerabilities, exploits and exhibits the same that reflect an administration not suitable that exposes them to the network to certain threats to information security.

Telecommunications Security Testing			
OSSTMM version 3.0			
Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.			
OPSEC	Visibility	3	
	Access	4	
	Trust	21	
	Total (Porosity)	28	
ISECOM			
	OPSEC		11,883968
	True Controls		5,402289
CONTROLS			
Class A			
	Authentication	5	23
	Indemnification	7	21
	Resilience	0	28
	Subjugation	0	28
	Continuity	0	28
	Total Class A	12	128
Class B			
	Non-Repudiation	0	28
	Confidentiality	0	28
	Privacy	8	20
	Integrity	0	28
	Alarm	1	27
	Total Class B	9	131
	All Controls Total	21	259
	Whole Coverage	7.50%	92.50%
True Missing			
	True Coverage A		8.57%
	True Coverage B		6.43%
	Total True Coverage		7.50%
OSSTMM			
	Limitations		15,579924
	Security Δ		-22.06
	True Protection		77.94
LIMITATIONS			
	Vulnerabilities	5	10,250000
	Weaknesses	5	5,571429
	Concerns	1	5,678571
	Exposures	6	0,624107
	Anomalies	0	1,086607
	Total # Limitations	17	88,5304
Actual Security: 78,3062 ravs			
OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM			

Fig. 3. Result of the calculation of the RAVs in telecommunications channel.
Source: OSSTMM Calculator

D. CHANNEL DATA NETWORKS.

The safety assessment on the channel of data networks, was performed with the use of network sniffing to identify the protocols that emanate from response of the network services or requests in its case. For example, Netbios, ARP, SAP, NFS, BGP, OSPF, MPLS, RIPv2, etc.

The results obtained are muetsran in Fig.4, the same that reflect chord to the parameters of the methodology that safety is too high, mainly in the aspect of trust in which has been used methodologies of sniffing of network to identify the protocols that emanate from response of the network services or requests in its case.

The controls being security mechanisms put in place to protect the operations, it should be emphasized that according to test made, ay null values in controls such as subjugation, non-repudiation, confidentiality and integrity; thus leaving a gap for the insecurity of the information.

The limitations are weighted individually, but these are directly related to some controls and operational safety, it is so because the values in operational safety are very high, these values predominate to the calculation of the limitations is also relatively high. It is as well that highlight limitations such as the vulnerabilities and exposures that reflect the same administration that does not adequately exposed to the network

to certain threats to information security.

RED DE DATOS			
OSSTMM version 3.0			
Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.			
OPSEC			
Visibility	17		
Access	14		
Trust	67		
Total (Porosity)	98		
CONTROLS			
Class A		Missing	
Authentication	5	93	
Indemnification	6	92	
Resilience	3	95	
Subjugation	0	98	
Continuity	4	94	
Total Class A	18	472	
Class B		Missing	
Non-Repudiation	0	98	
Confidentiality	0	98	
Privacy	8	90	
Integrity	0	98	
Alarm	1	97	
Total Class B	9	481	
All Controls Total	27	953	
Whole Coverage	2.76%	97.24%	
True Missing			
LIMITATIONS		Item Value	Total Value
Vulnerabilities	20	10,724490	214,489796
Weaknesses	9	5,814327	52,346939
Concerns	0	5,908163	0,000000
Exposures	17	0,603530	10,260006
Anomalies	0	0,960756	0,000000
Total # Limitations	46		277,0967
Actual Security: 71,2849 ravs			

Fig. 4. Result of the calculation of RAVs in the channel data networks.
Source: OSSTMM Calculator

III. DESIGN OF THE MODEL OF SECURITY DEFENSE IN DEPTH

Within the design of the model of security defense in depth, it raises security policies and standards set out in ISO/IEC 27002, the design of the segmentation of the network, in the same way the designs of the IDS/IPS, firewalls according to the results obtained in the lifting of prior information.

A. DESIGN OF THE MODEL OF DEFENSE AT THE USER LEVEL.

The education the user through rules and procedures is the basis of security in the first level of Defense in Depth model; that is why, in this section we will develop a practical guide for the development of safety standards in the GADMO, to create confidence in the activities of this entity. (NTE INEN-ISO/IEC 27002, 2009).

Thanks to the results obtained in the analysis of risks previously made with the methodology OSTMM, may be "determine the action of proper management and priorities for the management of the risks of information security, as well as for implementing the controls selected for protection against these risks". (NTE INEN-ISO/IEC 27002, 2009)

On the basis of these results has been proposed to create a safety guide; the same which aims to maintain and improve the management of information security in the organization, as well as to gain a greater awareness in the staff of the GADMO the good use of the information, and "compliance with legal requirements, statutes, regulations and contractual that must meet the institution, its trading partners, contractors and service providers, as well as their socio-cultural environment." (NTE INEN-ISO/IEC 27002, 2009).

The manual is structured on the basis of the following domains that were taken from reference to the Standard NTE INEN-ISO/IEC 27002:2009:

1. Security Policy
2. Organization of information security.
3. Asset Management
4. Security of human resources
5. Physical Security and the environment
6. Communications Management and Operations
7. Access Control
8. Acquisition, development and maintenance of information systems
9. Management of the incidents of the security of the information
10. Management of the business continuity
11. Compliance

B. DESIGN OF THE MODEL OF DEFENSE PERIMETER IN THE LEVEL.

For the model of the diene of defense in depth in the edge level describes the features and functions of Suricata software, which was chosen for the design of the IDS/IPS on free software, also describes the process for their preparation, defining the configuration parameters required for its correct operation. Additionally, it describes the Firewall features both physical and logical of the GADMO, as well as your configuration. Finally I will describe the applications of the server farm, and the proposal for setting up a DMZ, which might help to minimize the security risks in the institution.

1) IDS/IPS

For the choice of a system of intrusion detection/prevention was conducted after a comparison between different solutions, whether they own or under free software, the same as detailed in Table II.

Table II

COMPARISON OF THE DIFFERENT FREE SOFTWARE AND COMMERCIAL IDS/IPS.				
SYSTEMS OF DETECTION AND PREVENTION OF intruders				
	BRO	SNORT	BUSINESS SOLUTIONS	SURICATA
Multi-Hilos	Not	Not	Not	If
Support for IPv6	If	If	Cisco, IBM, Stonesoft	If
IP Reputation	Somet hing	Not	Cisco	If
Automatic detection of protocols	If	Not	Not	If
With GPU Acceleration	Not	Not	Not	If
Global Variables/Flowbits	If	Not	Not	If
Advanced analysis of HTTP	If	Not	Not	If
HTTP Access Logging	If	Not	Not	If
SMB Access Logging	If	Not	Not	If
Anomaly Detection.	Not	Not	If	Not
High Availability	Not	Not	If	Not
Administration GUI	Not	Not	If	Not
Free	If	If	Not	If

On the basis of the comparison of the different solutions, the choice of software to be used in the system of intrusion detection/prevention is Suricata.²

Once you've chosen and configured the software, the next step is the physical location of the same within the data network; the same which will be made between the firewall and the internal network, with this location you can get certain benefits, such as:

- Allows you to monitor intrusions that can traverse the firewall.
- You can detect attacks against servers.
- Allows you to identify attacks and scans more communes.

As all intrusion detection system, there are also certain disadvantages, the same that are presented below.

- Does not allow to identify attacks that use encryption methods
- Depending on the amount of traffic the IDS-IPS, may or may not parse it all. This will depend on the design of the system.

In the Fig.5 presents a graphical representation of the location of the intrusion detection/prevention.

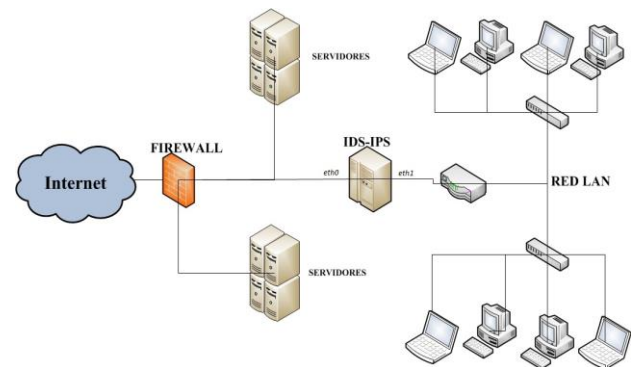


Fig.5. Location of the IDS-IPS in your network.

Fuente: Developed by Andrea Zura


2) FIREWALL

The GADMO account currently (January 2015) with two firewall, BY ASTARO Gateway 320; the same that are configured in such a way that protects the farm of external attacks .

The firewall has certain technical features that are presented in Table 2.

² Suricata is a engine IPS/IDS under open source license GPLv2and developed by the community of OISF (Open Information Security Foundation), is relatively new but with very good features the most important being your architecture Multi-threads, it is also totally compatible with the Snort rules and Emerging Threads. (Alfon, 2011).

Table III

TECHNICAL INFORMATION OF THE FIREWALL UTM Sophos		
Figure	Capacity	Hardware Specifications:
<p>By Astaro Security Gateway 320</p> 	<p>Performance of the firewall: 3.4 Gbit/s performance of the VPN: 700 Mbit/s performance of the IPS: 1300 Mbit/s performance of the UTM: 165 Mbit/s emails per hour: 600.000 Users: Unrestricted concurrent connections: 600.000 in quarantine Storage: 60 GB storage of records/reports: 80 GB.</p>	<p>Hard drive: 160 GB Ethernet ports: 8 USB Ports: 4 COM Ports: 1 (RJ-45) VGA ports: 1 (rear) LCD screen: 1</p>

In addition there were certain basic configurations in the software, such as enable the SSH access which allows the administrator access remotely and securely, in situations in which cannot be solved problems by means of the WebAdmin; also to activate the automatic sending of backups, allowing you to obtain these always to hand, so that the administrator can use when you need it; it should be stressed that these take up very little space and are saved in either the server or in our e-mail, among others.

3) DEMILITARIZED ZONE (DMZ)

To perform the design of the DMZ must have knowledge of all the services that provides the GADMO, on which platforms are installed, both at the level of hardware and software. In addition the server farm is protected by two

firewalls, but in a distribution not recommended due to the fact that there could be intrusion attempts.

Taking clear the three main elements that are part of the perimeter network, shown in Fig.6, the proposed design for the data network of the GADMO, detailing each of these parties.

It is noted that in the demilitarized zone are the services of e-mail and web server; the same that are protected by the first firewall, continually following the following firewall, additionally you have the IDS-IPS in the location already explained before the same that will allow you to keep the security of the LAN.

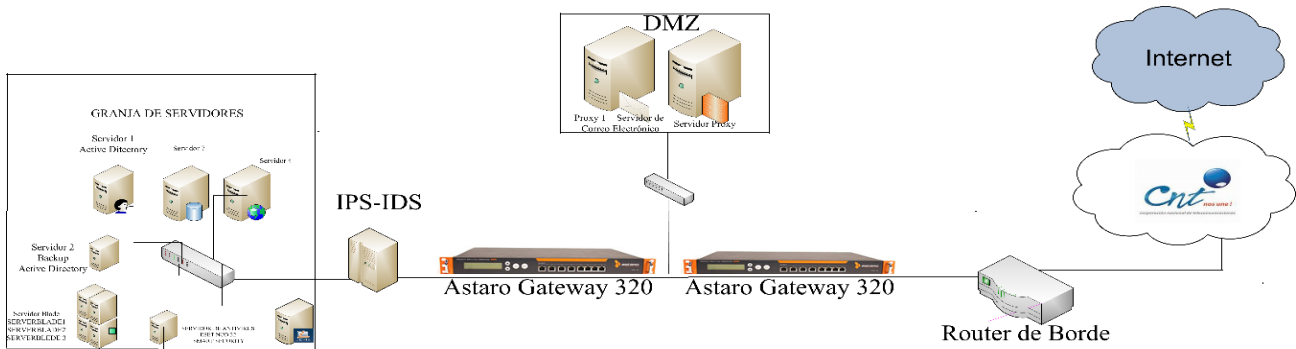


Fig.6. Design of perimeter network
 Source: Prepared by Andrea Z ura

C. DESIGN OF THE MODEL FOR DEFENSE IN THE LEVEL OF INTERNAL NETWORK

Considering the infrastructure and current requirements of the data network of the GADMO, proposes a hierarchical model and the logical segmentation of the network. Thus providing a solution that will improve the performance and services.

1. DESIGN OF THE NETWORK MODEL

The hierarchical model of network has several advantages that will allow the data network of the GADMO more secure, scalable, redundant, flexible and efficient.

This model is based on the design and structuring by separate layers that meets specific functions. The separation of the different existing functions in a network makes the design of the network become modular, this facilitates the scalability and performance. The hierarchical model of typical design is separated into three layers: access layer, Layer and layer core distribution. (CISCO), the same that is presented in Fig 7.

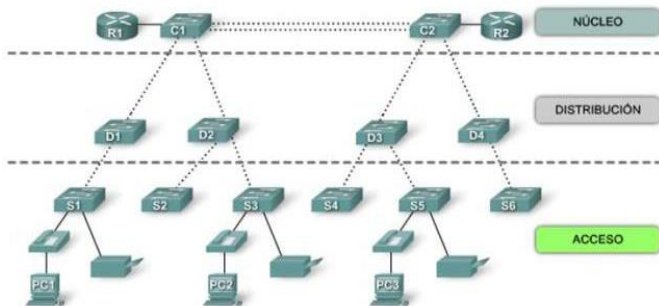


Figure 7. Hierarchical Network Model
Source: Extracted Image of (Cisco)

Based on this model will be described the characteristics of the switches with the GADMO; on the basis of their characteristics will be classified in the various layers of the hierarchical model.

1) Access layer switches

Access layer switches make it easy to connect the devices end-node to the network. For this reason, they need support features such as port security, VLAN, Fast Ethernet/Gigabit Ethernet, PoE and added links. Port security allows the switch decides how many and which specific devices will allow you to connect to the switch. Port security is applied in the access layer. In consequence, is an important first line of defense for a network.

According to the features needed for the access switches, is presented in Table IV a summary of the elect with their respective features.

Table IV
FEATURES ACCESS LAYER SWITCHES

Speed				
		MCS ^{to} :48Gbps		
		MCT ^b :35.5 Mbps		
		MCS: 13.6 Gbps		
		MCT: 10.1 Mbps		
		MCS: 104 Gbps		
		MCT: 74 Mbps		
3COM 2226 SFP PLUS 24P	10/100	MCS: 8.8 Gbps	✓	✓
		MCS: 48 Gbps		
		MCT: 35.5 Mbps		
		MCS: 13.6 Gbps		
		MCT: 10.1 Mbps		
		MCS: 56 Gbps		
		MCT:41.7 Mbps		
3COM 4500G 24P	10/100	MCS: 8.8 Gbps	✓	✓
3Com 4900 12P	10/100/1000		✓	✓
3Com 4210 18P	10/100		✓	✓
3COM 2952		MCS: 104 Gbps.		
48P		MCT: 74 Mpps;		

To be the access layer a direct link with the end-user, this integrates to end all the equipment, such as, computers, cameras, IP phones, scanner, printers, copiers, etc. ; which allows the administrator to control all the computers that connect to the network. This has logically considered segmenting the network. Is presented in Fig 8.

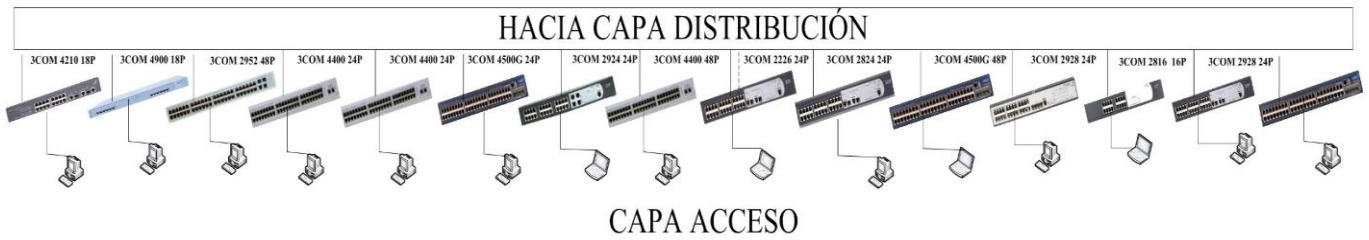


Fig.8. Access layer switches
Source: Prepared by Andrea Zura

In the study of the current situation it was determined that the users are grouped together according to the role that they play and chord to the resources they consume.

Before you perform the segmentation that there are several things to consider:

- You must assign each user a IP address, the same that must not be modified without authorization; to control this; to associate the MAC address of each computer , with the assigned IP address, so that if the two do not match, the user will not be able to access the network.
- You must have an updated record of the changes made the network infrastructure.
- Segmentation and IP Addressing

The segmentation of a network allows you to significantly improve the security, because administrators can configure segments in such a way that transmit and receive packets only from your subnet, ensuring that unauthorized packets are not sent within or outside the segment.

To perform the segmentation has been considered the grouping that is maintained in the GADMO, grouping by the different directions, coordination and/or chiefdoms, functions performed by each user and the resources they use and need to use

The distribution of VLAN you can differentiate the following:

- VSERV: VLAN of servers and computers; the same that has been designed for IP addressing of the servers and equipment of the active coordination of ICT's.
- VADMIN: management VLAN; the same that has been designed for IP addressing of the administrators of the network, i.e. the technicians and engineers of the coordination of ICT's.
- VTECN: VLAN of technicians and collaborators; the same that has been designed for IP addressing of the staff of all the addresses that require the use public

web pages, web pages informative and/or commercial e-mail and for your work.

- VASIST: VLAN of attendees; the same that has been designed for IP addressing of the wizards and/or secretaries who only need the email for your work.
- VDIREC: VLAN directors; the same that has been designed for IP addressing of the directors and/or coordinators, who will have priority access to all services.

Such distribution is shown in table V.

Table V

EXTRACT OF THE SCATTERS OF VLANS ON THE DATA NETWORK OF THE GADMO			
Unit	#VLAN	VLAN Name	
Switches and Routers	VLAN 2	Native VLAN	
Servers	VLAN	VSERV	
Development Unit			
Networks Unit			
Maintenance Unit			
Director	VLAN 4	VDAP	
Sewerage Technical			
Technical Marketing			
Laboratory Technicians			
Wizards	VLAN 6	VAAP	
Mayor	VLAN 7	VALCAL	
Internal Audit			
Legal Advice			
General Secretariat			
Audit			
Wizards	VLAN 9	VAALCAL	
Director	VLAN 10	VDAVAL	
Urban Appraisals			
Rural Appraisals			
Wizards	VLAN 12	VAVAL	

2) *Distribution layer switches*

The switches of distribution layer collected data from all the access layer switches and send them to the core layer switches, also provide functions of routing between VLANS.

Among the characteristics that must withstand the distribution layer switches are the send rate high, Gigabit ports

Ethernet/ 10Gigabit Ethernet, redundant components, policies of security/access control lists, adding links and quality of service. (Cisco)

According to the features needed for the access switches, is presented in Table VI a summary of the elect with their respective features:

Table VI.

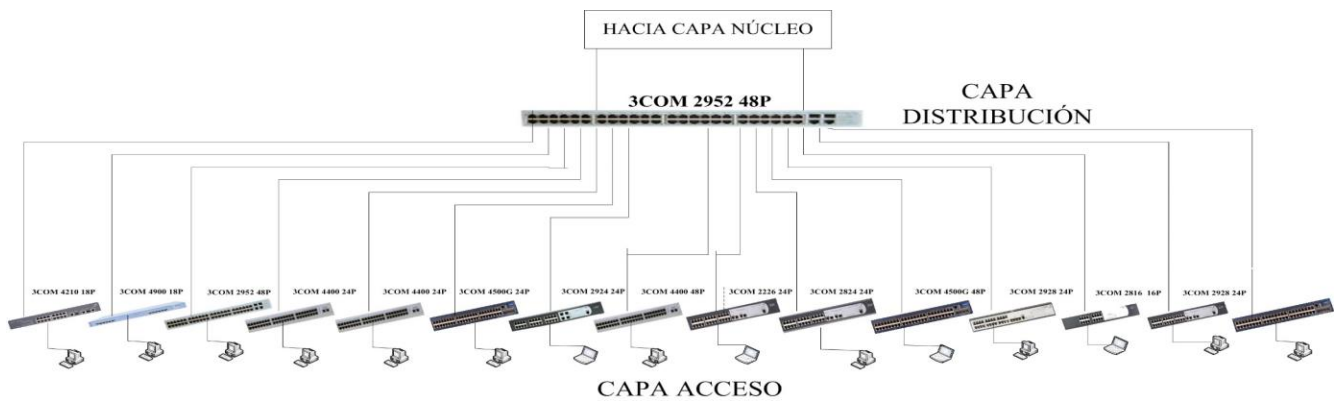
SWITCH 2952 SFP PLUS 48P	
Features	Description
Performance	48 10BASE-T/ 100BASE-X/ 1000BASE-T 4 Gigabit SFP ports Maximum switching capacity: 104 Gbps. Maximum transmission capacity 74 Mpps;
Layer 2 Switching	VLANs based on IEEE 802.1Q protocol Spanning Tree Protocol (STP) IEEE 802.1D Rapid Spanning Tree Protocol (RSTP) IEEE 802.1w
Layer 3 Switching	Static routes: 32 VLANs Virtual Interface: 8
Traffic prioritization	Class of Service/Quality of Service (CoS/QoS) IEEE 802.1p in output
Security	Filters ACLs based on IP addressing and MAC to filter the network traffic and to improve the control of the network. ACLs based on time, allow greater flexibility with access to the management network.

- Design Considerations

The distribution layer adds the data received from the access layer switches before being transmitted to the core layer for routing to their final destination. (Cisco)

The 3Com switches 2952 SFP PLUS 48P will manage the links of connection with all connections to the servers, connections in the internal network as well as the management of inter VLANs on the network of GADMO. Additionally these computers will be configured as backup thus ensuring the availability of the network. This topology is shown in the fittings,

Fig.9.



Fittings, Fig.9. Distribution layer switches.
Source: Prepared by Andrea Zura

3) Core layer switches.

The core layer of a hierarchical topology is a high-speed backbone network and requires switches that can handle very high rates of forwarding. The forwarding rate required depends largely on the number of devices that participate in the network. Therefore a switch layer core must support layer

3, its ports must be Gigabit Ethernet/10 Gigabit Ethernet, have redundant components, link aggregation and support quality of service. (Cisco).

In keeping with the features needed for the access switches, is presented in Table VII a summary of the switch chosen with their respective features.

Table VII

3COM SWITCH 5500 SFP 24P	
Features	Description
Performance	24-Port 10/100/1000 Mbps 4Ports 1000 Mbps SFP Maximum switching capacity: 184 Gbps. Maximum capacity of 136.9 Mbps transmission;
Layer 2 Switching	VLANs based on IEEE 802.1Q protocol Spanning Tree Protocol (STP) IEEE 802.1D Rapid Spanning Tree Protocol (RSTP) IEEE 802.1w
Layer 3 Switching	Hardware-based routing Static Routes: 100 Virtual Interfaces IP: 64 RIP (protocol for routing information), v1 and v2 Open Shortest Path First (OSPF)
Traffic prioritization	Class of Service/Quality of Service (CoS/QoS) IEEE 802.1p in output
Security	The access control lists based on the time

• Design Considerations

The core layer is essential to the interconnectivity between the devices of the distribution layer, therefore, it is important that the core is highly available, and redundant. In addition you can connect to the Internet resources. (Cisco)

In addition could be demonstrated that the current topology of the data network of the GADMO has switches in cascade configuration by the need to serve the majority of users, however, this reduces the performance of the network.

The data network of the GADMO, account with equipment COM, brand owner with XRN technology, the same that allows you to improve the operation of the network, through the administration of the different switches as a single unit. Is muetsra in Fig.10.

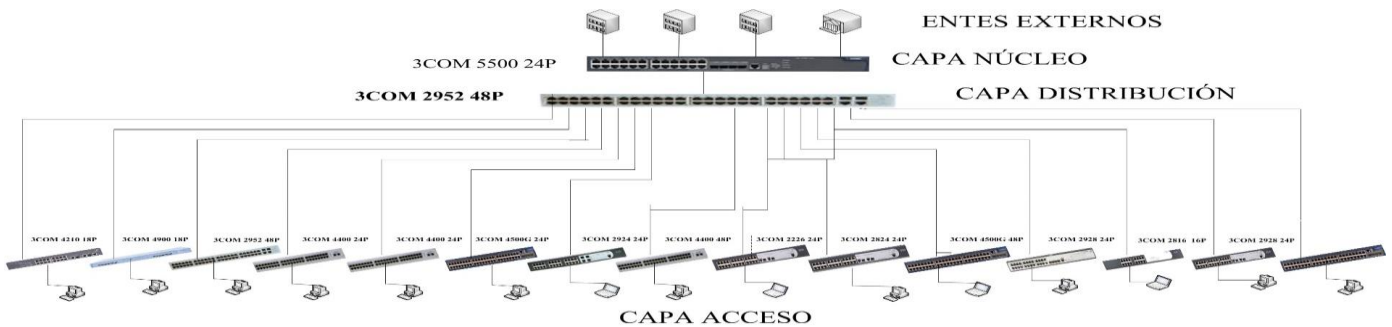


Fig.10.Switch layer Core
Source: Prepared by Andrea Zura

D. OPERATIONAL TESTS.

The functional tests will be carried out using the methods of hacking Ethics; the same as that by (Silver) consists in the simulation of possible scenarios where attacks are reproduced in a controlled manner, as well as activities of cyber criminals, this form of act has its justification in the idea that: "to catch an intruder, you must first think like intruder"

1) Detection of vulnerabilities

The attacker in general, look for vulnerabilities in the system that can take advantage of to transform them in attacks or threats. These vulnerabilities can be Queries to databases, consultations of headers of mails, port scanning, http requests, search for data within files, among others (Tori).

Given this, there will be a port scan through the tool Nmap, whose objective is the identification of open ports, which are waiting for new connections, allowed or not.

It should be noted that all the tests are based on the White Box Test method; that according to (Tori): this is a check that is carried out by a pentester that has all the information about the system.

a) Attacks or intrusions by layers

The objectives of the ethical hacking according to (Silver) are:

- Assess vulnerabilities through the identification of weaknesses caused by a bad configuration of the applications.
- Analyze and categorize the exploitable weaknesses, based on the potential impact and the possibility that the threat will become a reality.
- Provide recommendations based on the priorities of the organization to minimize and eliminate the vulnerabilities and thus reduce the risk of occurrence of an adverse event.

Based on these objectives the tests were conducted in the different layers of the OSI model, and taking as reference the Fig.11

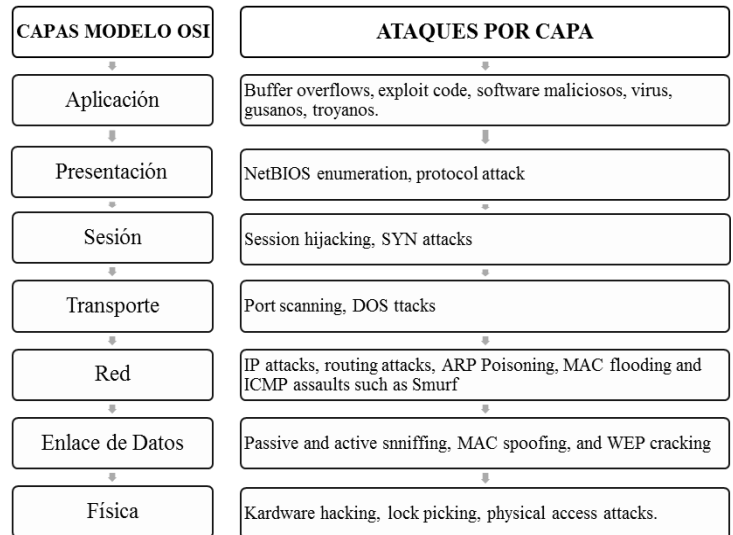


Fig. 11. Attacks for each layer of the OSI model.
Source: Extracted from (Cabrera, 2012)

1. Data Link Layer .

ARP spoofing was the chosen technique to perform the ethical hacking in this layer; this technique according to (Thomas Demuth) is a technique where the attacker deliberately transmits an ARP packet false.

- Mitigation.

In the same directory as the rules of suricata, find the file scirius.rules; in which i could combat this attack; by activating the alert on that protocol.

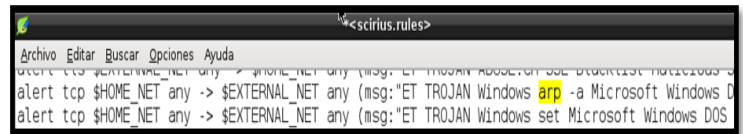


Fig. 12 Attack Mitigation Arp Spoofing
Source: Extracted from SELKS

The IDS-IPS, displays alerts due to this attack of Spoffing ARP. In the screen are displayed all the MAC addresses that are making demands on the network; and in keeping with the number of times that each MAC address click a request you will see a summary of alerts for that event, in which indicated between the most important parameters the source IP address and destination. Shown in Fig 12.

Field	Action	Value
@timestamp	Q	2015-02-04T05:48:58.943Z
@version	Q	1
_id	Q	BByTFosFTgubmAWY__7#Q
_index	Q	logstash-2015.02.04
_type	Q	SELKS
dest_ip	Q	192.168.4.1
dest_port	Q	443
event_type	Q	tls
flow_id	Q	35998032
host	Q	SELKS
in_iface	Q	eth1
path	Q	/var/log/suricata/eve.json
proto	Q	TCP
src_ip	Q	192.168.4.11
src_port	Q	5135
timestamp	Q	2015-02-04T00:48:58.943158
tls.fingerprint	Q	a2:13:46:5c:0a:d3:e7:3f:3a:c3:7f:0a:d6:57:b8:5e:57:1d:6a:90
tls.issuerdn	Q	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
tls.subject	Q	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
tls.version	Q	TLS 1.2
type	Q	SELKS

Fig. Detail of 13 alerts produced
Source: Extracted from SELKS

II. Network Layer

In this layer you can perform different types of attacks the same based its objective to stifle the normal access to the services and resources of an organization for an indefinite period of time.

- ICMP Flood

Saturates the a team with requests for ICMP Echo Request so that it cannot respond to actual requests.

- Mitigation

In the same directory as the rules of suricata, find the file scirius.rules; in which i could combat this attack; by activating the alert on that protocol.

```

*scirius.rules>
Archivo Editar Buscar Opciones Ayuda
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET WEB SERVER PHP Attack Tool Morfeus F Sca
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WEB SERVER PHP Attack Tool Morfeus F Sca
alert icmp any any -> any any (msg:"SURICATA ICMPv4 invalid checksum"; icmpv4-csum:invalid; sid
    
```

Fig. ICMP attack 14 Flood Mitigation

The result shown by Suricata, it can be seen in different ways; one of them is through a statistical chart which shows all the alerts raised on the network.

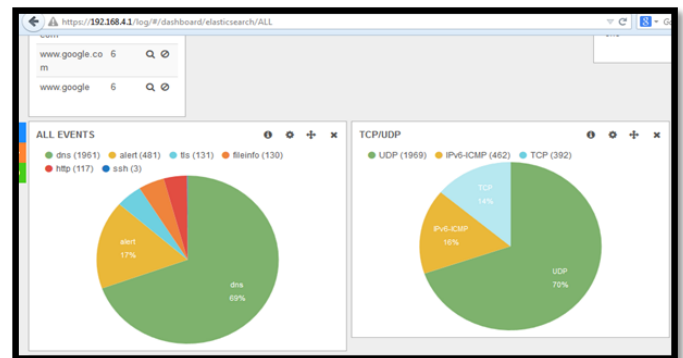


Fig. 15 Statistical result of Suricata

III. Transport Layer

In this layer there are different types of attacks, in which is the Scan³, a technique that allows you to collect meaningful information when pointing a scan to the hosts of the objective or in processing the information that provides this as a result. (Tori).

- Port Scanning

Discover what ports are open or closed, filtered, in addition to finding out what type and version of application is running on these ports and services. On the basis of these preliminary

³ is a technique that consists in analysing the tracks it leaves an operating system on your network connections. It is based on the response times for the different packages, to establish a connection in the TCP/IP protocol, used by different operating systems. <http://urlmin.com/4qp95>

concepts; conducted a port scan, using the tool nmap. Shown in Figure 17.

- Mitigation

In the same directory as the rules of suricata, find the file scirius.rules; in which i could combat this attack; by activating the alert on that protocol.

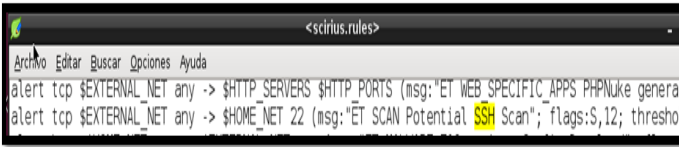


Fig. 16 Attack mitigation for port scanning
Source: Extracted from SELKS

The result in Suricata is:

Field	Action	Value
@timestamp	Q O III	2015-01-28T13:27:02.287Z
@version	Q O III	1
_id	Q O III	eViqKdPNQz2FuzkCOYr0KQ
_index	Q O III	logstash-2015.01.28
_type	Q O III	SELKS
dest_ip	Q O III	192.168.4.1
dest_port	Q O III	22
event_type	Q O III	ssh
flow_id	Q O III	52660336
host	Q O III	SELKS
in_iface	Q O III	eth1
path	Q O III	/var/log/suricata/eve.json
proto	Q O III	TCP
src_ip	Q O III	192.168.4.11
src_port	Q O III	1325
ssh.client.proto_version	Q O III	2.0
ssh.client.software_version	Q O III	PuTTY_Release_0.60

Fig 17. Result of alerts by port scanning
Source: Extracted from SELKS

Highlighting information provided by the alert; such as the IP address from where the request was made, the service or protocol; the exact date and time; as well as the software and version used to perform the intrusion.

IV. Session Layer

In this layer you can do different attacks such as TCP SYN scan, a technique that sends a package SYN. If the answer is a SYN/ACK, the port is open, while if is a RST, is closed.

- Mitigation

In the same directory as the rules of suricata, find the file stream-events.rules; in which i could combat this attack; by activating the alert on that protocol.

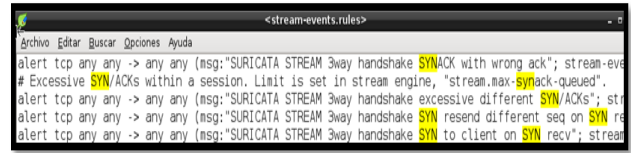


Fig. 18 Mitigation scan TCP SYN attack
Source: Extracted from SELKS

The result of Suricata is presented in a summary indicating the source IP address of the intrusion the type of intrusion, the hour in which succinct; among others.



Fig. 19 Result of intrusion alert to TCP-SYN
Source: Extracted from SELKS

V. . Application Layer

In this layer you can carry out attacks by downloading applications of questionable provenance.

- Mitigation

In the same directory as the rules of suricata, find the file files.rules; in which i could combat this attack; by activating the alert in the attack.

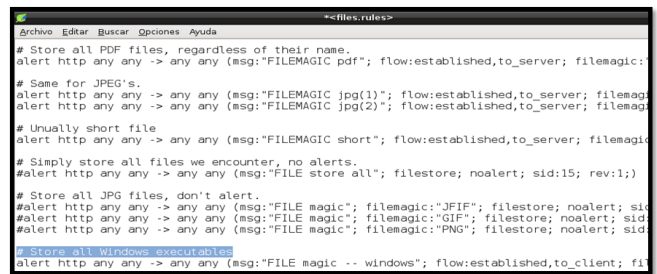


Fig.20 Mitigation attacks of dubious downloads of files
Source: Extracted from SELKS

It is so that the software shows a statistical chart of downloads

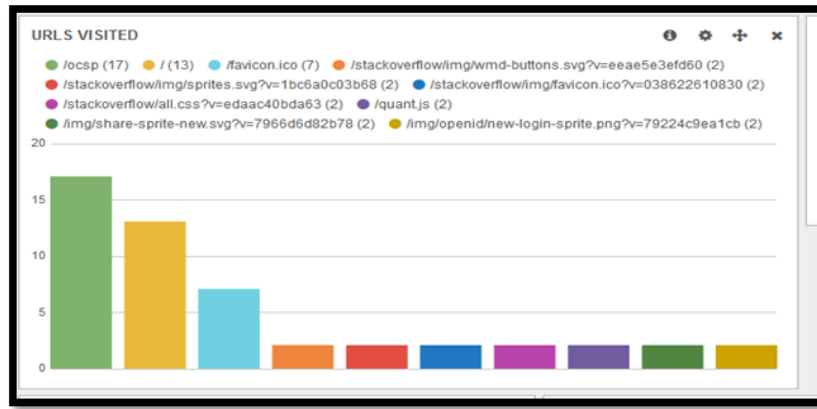


Fig 20 stat plot of downloads
Source: Extracted from SELKS

E. Referential BUDGET

There will be a referential budget taking into account a comparison of have a licensed solution and a solution in free software, in the installation of an IDS/IPS.

It should be emphasized that the budget analysis referential has as main objective provide a measure of the budget invested in the realization of a project.

1) Calculation

Before starting with the calculation of the budget, it is necessary to clarify that for the design of the model presented in this project; in the internal network is made with the switching equipment in the existing GADMO; in the perimeter network in the same way. In the latter, we have implemented a system of intrusion detection/prevention in free software, on the basis of this will be the reference budget.

For the migration of a system or software program Owner (not free) to free software (SL) the following procedure is used to calculate the Total Cost of the Solution (CTS). This method should be applied to both Proprietary Software as Free Software. If the cost of the latter is smaller than the name of the owner should be performing the migration. (National Secretariat of Public Administration, 2014)

In addition, the web portal (National Secretariat of Public Administration, 2014), stresses that as prerequisites to the migration of a trading system to a system under free software is necessary to have the following considerations:

- Take the minimum capabilities and functional techniques required by the organization and users.
- Maintain or increase the productivity of the organization and users.
- Be compatible or integratable in platforms of existing hardware and software.

Table VIII

AN INVESTIGATION METHOD A BUDGET		
Total Cost of the Solution	UTM Sophos	SURICATA
CP	4,285.00	0.40
CI	0	0
CADH	2,875.00	479
CADS	13,000.00	0
CM	0	0
CMH	1,750.00	180.00
CASS	1,465.00	0.40
CRH	1.5	1.50
CT	0	5000
CU	0	0

It should be emphasized that the calculations were performed on the basis of the following calculations.

- Total Cost of the Solution (CTS)

For the calculation of the total cost of the Solution (CTS) according to (National Secretariat of Public Administration, 2014) is considered 3 components:

$$CTS = CTI + CTA + CTC$$

Equation 1 Total Cost of Solution

Source: Recovered from (National Secretariat of Public Administration, 2014)

Where:

- CTI: Total Cost of Implementation
- CTA: Total Administrative Cost
- TAGS: Total Cost of Training

- a. Total cost of implementation (CTI)

It is the total cost of items and activities necessary to operate the solution. It includes equipment acquisition, licensing, and human resource for timely deployment. The CTI is calculated as follows:

$$CTI = CP + CI + CADH + CADS + CM$$

Equation 2 2 Total Cost of Implementation

Source: Recovered from (National Secretariat of Public Administration, 2014)

Where:

- CP: Cost of the licenses of the software architecture considering
- CI: Costs of installation, configuration and customization (if any)
- AHRC: additional costs of hardware and infrastructure
- CADS: additional costs of software
- CM: Costs of data migration and integration

- b. Total Administrative Cost (CTA)

Is the total annual average cost of items and activities necessary to ensure the availability, capacity and continuity of the implemented solution. Includes the total cost of the average annual human resource employee in these activities. The CTA is calculated as follows:

$$CTA = CMH + CASS + CRH$$

Equation 3 3 Total Administrative Cost

Source: Recovered from (National Secretariat of Public Administration, 2014)

Where:

- CMH: Costs of upgrade and maintenance of the hardware and infrastructure
- CASS: Costs of upgrade and support of the software
- CRH: Costs of Human Resources
- c. Total Cost of training (CTC)

Is the average annual cost for the ongoing training of staff (technical and users) in the operation and use of the solution.

$$CTC = CT + CU$$

Equation 4 Total Cost of Training

Where:

CT = hourly cost technical training * technical * number of number of hours * number years of operation of the solution

CU = hourly cost user training * number of users * hours * number years of operation of the solution.

RESULT

If the cost of free software is less than the owner should be performing the migration.

Then:

$$\text{If } CTS_{Propietario} = \$ 23,376.50$$

$$\text{AND } CTS_{Libre} = \$ 5661.30$$

$$\text{Is met: } CTS_{Libre} < CTS_{Propietario}$$

YOU MUST PERFORM THE MIGRATION.

F. CONCLUSIONS

There was a security design, using a multilayer model called "Defense in Depth" in the data network of the GAD Municipal of Otavalo, applying new security policies on the basis of the ISO/IEC 27002, so that internal and external attacks can be detected and avoided in due course.

ISO/IEC 27002, was the main basis for the realization of the design, because it lays down certain guidelines and goals that allow you to identify clearly the risks that can be exposed the Organization, and as a result, it could create a Handbook of rules and procedures of information security; in addition to create access policies in the perimeter network and internal network.

The lifting of information is executed with OSSTM 3.0 ; a methodology of penetration testing that allows you to perform a risk analysis in the channels, human, physical, telecommunications and data networking, obtaining results that helped to develop a manual of rules and procedures on the basis of the normo ISO/IEC 27002, the same that is compatible with the methodology mentioned above.

The study of the current situation, in terms of the network infrastructure allowed us to identify the features and benefits of all the equipment; on this basis, we used the infrastructure in a new topology that will help to improve the service and the improvement of the administration.

The benefit of having two firewalls, data network infrastructure helps combat the hotbeds of insecurity; always and when these are placed in such a way that will utilize all of the features that these computers offer.

A hierarchical network model used to perform the design of internal network, allows you to optimize the use of network resources; thanks to the implementation of a network topology based on layers are obtained features of scalability, flexibility, and above all safety.

Tests were carried out attack simulation based on the objectives of ethical hacking; in the different layers of the OSI model, with what we could not verify the proper functioning of the IDS-IPS and its system of alerts.

After performing the referential budget, and to establish the differences between having a solution and a solution licensed under free software, it was concluded that the total cost solution under free software is less than the licensed solution.

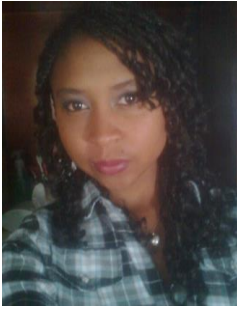
REFERENCES

- [1]Alfon. (22 February 2011). Networking and Security . Obtained from <http://seguridadyredes.wordpress.com/2011/02/22/ids-ips-suricata-entendiendo-y-configurando-suricata-parte-i/>
- [2]Alvarado, M. S. (n.d.). OSSTMM 3. Analysis and Design of Information Systems , 2.
- [3]Bertolín, J. A. (2008). Information Security . Spain: Auditorium.
- [4]Cabrera, E. C. (2012). Methodologies and frameworks for work in information security. Common attacks in layer 3 A. Pereira .
- [5]CISCO. (n.d.). CCNA 3.

- [6] Academic networking. (n.d.). CCNA Exploration 4.0 . In switching and wireless LAN.
- [7] Estrada, A. C. (2011). *Security levels by Spain: DarFE*.
- [8] February, B. M. (2011). *ANALYSIS OF TRAFFIC WITH Wireshark, Spain*.
- [9] Gómez, D. G. (July 2003). Intrusion Detection Systems.
- [10] Guiovanni, A. (n.d.). *GUIOOS' Blog* . Obtained from <https://guiooos.wordpress.com>
- [11] Hernandez Sampieri, R. , Fernández Collado, C. , & Baptista Lucio, P. (Mexico). *Methodology of the Ivestigacion*. MCGRAW-hill.
- [12] Herzog, P. (n.d.). *OSSTMM 2.1* .
- [13] Herzog, P. (n.d.). *OSSTMM 3.0* .
- [14] Lopez, P. A. (n.d.). *Security Informatics*. Editex.
- [15] Martínez, C. G. (2010). Model for Defense in Depth.
- [16] Mathon, P. (2002). *ISA Server 2000 Firewall and Proxy, Barcelona* : EMI.
- [17] Microsoft. (2004). Guide antivirus defense in depth.
- [1 8] NTE INEN-ISO/IEC 27002. (2009). *Information Technology - Security techniques - Codifo of Practice for Information Security Management, Quito* .
- [19]Silver, A. R. (n.d.). *Ethical hacking*.
- [20] National Secretariat of Public Administration. (January 22 2014). *Government Elecctronico* . obtained from <http://www1.gobiernoelectronico.gob.ec>
- [21] Stuart "Andy" Tanenbaum, A. (2003). *Computer Networks, Mexico* : Pearson.
- [22] Thomas Demuth, A. L. (n.d.). *ARP spoofing and poisoning, TRICKS OF TRAFFIC*.
- [23] Tori, C. (n.d.). Ethical hacking Rosario .
- [24] Toth, J. , & Sznec, G. (2014). Implementation of the NIST SP800-30 guide through the use of OSSTMM. Neuquén.

Biografías

Zura Ch. Andrea Y. Born in Ibarra, Ecuador on 10 May 1990. Her primary studies conducted in the Educational Unit Sacred Heart of Jesus.; in 2007 he obtained his bachelor Computing technical specialization in the College National Ibarra; in the same year, joined as a student of pre-degree at the Technical University of the North in the career of Electronic Engineering and communication networks.



Performed their internships in the company FIX WIRELESS in the technical department, performing duties of technical study prior installation of service, technical support on site and via telephone, and internet service installation in the north of the country; in the Government decentralized autonomous Municipal of Otavalo performed the tasks of installing network points, technical support,

equipment configuration L2 and L3, lifting information, monitoring and inventory IP.

Currently working as Site Engennier in the Project of MODERNIZATION 2G CLEAR in the city of Quito.



Maya O. Edgar TO . Ibarra was born in Imbabura province on April 22, 1980. Engineer in Computing Systems, Technical University of Norte-Ecuador in 2006. He is currently teaching for a career in Engineering in Electronics and communication networks in the Technical University of the North, Ibarra, Ecuador. Master's degree in Communication Networks, Pontifical Catholic University of Ecuador, Quito - Ecuador.