UNIVERSIDAD TÉCNICA DEL NORTE

FACULTY OF ENGINEERING IN APPLIED SCIENCES

CAREER IN ELECTRONIC ENGINEERING AND COMMUNICATION NETWORKS

ETHICAL HACKING TO DETECT FLAWS AT INFORMATION SECURITY THE INTRANET OF PROVINCIAL GOVERNMENT OF IMBABURA AND IMPLEMENT AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS), BASED ON NORM ISO/IEC 27001:2005

PROJECT PRIOR TO THE AWARD OF THE TITLE OF ENGINEER IN ELECTRONICS AND COMMUNICATION NETWORKS

AUTHOR: BRAULIO FERNANDO ORTIZ BELTRÁN

DIRECTOR: MSC. EDGAR MAYA

IBARRA – ECUADOR

JANUARY 2015

Ethical Hacking to detect flaws at information security the intranet of Provincial Government of Imbabura and implement an information security management system (ISMS), based on norm ISO/IEC 27001:2005

Ortiz, Fernando
Universidad Técnica del Norte
Ibarra-Ecuador
f_ortiz_b@hotmail.com

Summary— The project consist to identify the assets of most important information Provincial Government of Imbabura, namely devices that are part of the intranet of the institution directly related to the transportation, storage or modification of information whose evaluation is to conduct a risk analysis and then detect server failures the Provincial Government of Imbabura using techniques of Ethical Hacking from a perspective of black box, as is the total ignorance of the characteristics of the servers.

With the results of the three analyzes proceed to use the norm ISO/IEC 27001:2005 to design the System Management Information Security (ISMS) by analyzing the selection the controls of the most suitable as a measure for the treatment of risks; finally preparing the documents that are part of the ISMS such as policy information security, procedures, regulations and safety standards.

Keywords— System Management Information Security, Ethical Hacking, ISO/IEC 27001:2005.

I. INTRODUCTION

At present the institutions regardless of their size provide much of its attention to economic activities in which they perform, but forget the issue of information security, namely the information is considered a valuable asset for any institution especially when critical data is processed, if it is obtained by malicious users can cause great economic, social, political damage among others, thus securing devices and information should be a primary task.

The implementation of the System Management Information Security (ISMS) requires compliance with three initial requirements requested by the ISO / IEC 27001: 2005 which are:

- Information assets.
- Identification of vulnerabilities.
- Risk analysis.

The present ISO standard undetermined how to perform these tasks so these aspects left to the evaluator, however for this project Magerit Methodology (Methodology for Analysis and Risk Management Information Systems) is used to perform the first two requirements.

The information assets the Network Provincial Government of Imbabura (GPI) immersed the project are:

1. Document management server - Quipux
2. Email server - Zimbra
3. Web server
4. Proxy server
5. IP telephony server - Elastix
6. Land management server - Gis
7. Financial Accounting Server – Olympo
8. Customer service
9. Blade server
10. Core switch
11. Access switch
12. Firewall
13. Packet Shaper
14. Router CNT
15. Desktops
16. structured cabling
17. Backbon
18. Air conditioning system
19. UPS[1]
20. Electric power system
21. Access Control
22. Security Cameras
23. Environmental monitoring system

[1] UPS: Uninterruptible power supply.

24. Fire protection system
25. IP Phone
26. Internet

Corresponding to the identification of vulnerabilities or ethical hacking process is developed from the perspective of black box or black-box, namely the attacker or assessor unknown of the technical characteristics of the servers, so you need to use specialized software on the topic. For the present project was used an operating system based on Debian Linux which is Kali because it has preinstalled specialized tools used for such tasks among which the following were used:

- Nmap (Port scanner and services)
- Metasploit (Framework of explotation)
- Sqlmap (SQL[2] injection tool database).
- Nessus (Vulnerabilidades scanner)
- Armitage (Framework dof metasploit)
- Ping (sending packages ICMP)
- Client software applications

II. DESIGN ISMS

The design begins of the risk analysis which specifies the threats are exposed each information asset, for it evaluates threats Magerit grouped into five categories:

- Natural Disasters.
- Industrial disasters.
- Errors and unintentional failures.
- Attacks intentioned.

Each threat information asset is assigned a rating based on several proposed by the Magerit methodology among those appearing typing asset criteria, dependence between assets and self-assessment and cumulative properties of information as they are the confidentiality, integrity and availability.

Risk treatment specifies the selected controls from Annex A of ISO/IEC 27001:2005 that will be implemented in the ISMS of the institution. The controls are selected by analyzing the results of the risk analysis report and the reports of vulnerabilities in servers namely for each threat and/or vulnerability select one or more controls that allow accept the risk, evade, transfer or mitigate.

III. IMPLEMENTATION

The implementation of ISMS is the development of the documents required by the ISO/IEC 27001:2005 which follow a hierarchical level as follows.

- Policy Information Security
- Regulations and procedures for information security.
- Standards.
- Security Logs

A. Policy Information Security

The politics of information security is the most important document of the institution sets the general guidelines, needs and requirements for information security as measures taken to keep safe the information and assets they processed, transported or stored for ensure business activities of the institution.

B. Regulations.

The safety regulations implementing one or several related controls focusing on an area of security defining the conditions and assets to protect under specific scenarios or previously defined policy information security situations. The regulations developed in the implementation of the ISMS of GPI are listed in Table 1:

C. Procedures

Are the actions or activities undertaken describing the procedure to execute, related to information security and officials responsible for monitoring, updating and compliance. The procedures developed in the ISMS are listed in Table 1.

D. Standards

Determine the necessary actions to complete the process of a specific procedure to be considered as

[2] SQL: Lenguaje de consulta estructurado de acceso a la base de datos.

standard or common to all users of a service, in this ISMS project has developed two standards listed in Table 1.

E. Assigning responsibilities.

The following table summarizes the regulations, procedures and standards developed as part of the implementation of the Management System of Information Security and the respective allocation for each agency of the Department of Computer GPI.

TABLE I
ASSIGNMENT OF DOCUMENTS ISMS A SUB-DIRECTIONS OF DEPARTMENT OF COMPUTING

DOCUMENTS THE ISMS	**DEPENDENCES GPI THE DEPARTMENT OF COMPUTING**		
NORM	**Services Management**	**Infrastructure Management**	**Project Management**
Norm of agreements with third parties		✓	
Norm of administration of security incident of the information	✓	✓	
Norm of administration of network security		✓	
Norm of good practice of information security	✓		
Norm of access control	✓	✓	
Norm of change control|		✓	✓
Norm of business continuity management		✓	✓
Norm of maintenance of equipment and installations		✓	
Norm of protection against malicious software		✓	
Norm of security requirements of information for new installations and acquisition of software	✓	✓	✓
Norm of roles and responsibilities of information security	✓	✓	✓
Norm of segregation of duties	✓	✓	
Norm of information security for human resource management	✓	✓	
Norm of information security	✓	✓	✓
Norm of licensed software	✓		✓
Norm of electrical supply		✓	
Norm of internet use	✓	✓	
PROCEDURES			
Procedures of contact with interest groups concerning information security	✓		✓
Procedures of arrangement of storage media and computer equipment	✓	✓	
Procedures of generation and storage of backups		✓	
Procedures of protection and review of audit records		✓	
Procedures of physical and environmental security of the data center		✓	
Procedures for the creation, modification y elimination of user access systems		✓	
Procedures for identification and classification of information assets	✓	✓	
STANDARDS			

Standard passwords for users and administrators	✓	✓	✓
Standard Asset Tagging information	✓	✓	

IV. RESULTS

One of the most important procedures of the project is to identify vulnerabilities GPI servers through an approach Ethical Hacking by exploitation techniques, access to both services and confidential information.

The following table summarizes the types of vulnerabilities detected on the servers of the Provincial Government of Imbabura, marked the affected servers with the respective vulnerability.

TABLE II

COMMON VULNERABILITY OF SERVERS GPI.

	SERVER						
VULNERABILIT	1	2	3	4	5	6	7
XSS-Cross site Scripting		x	x	x	x		x
Access to database		x	x	x			
SQL Injection			x		x		
Disclosure	x	x	x	x	x	x	
Error in PHP	x						
Access control		x	x	x			x
Transmission unencrypted credentials		x	x	x	x		x

The ISO/IEC 27001:2005 requires the completion of the project, drafting the final document "Statement of Applicability" which sets the controls implemented with the respective documents ISMS developed, and the controls not implemented justify their exclusion.

V. CONCLUSIONS

The process of Ethical Hacking revealed major flaws in servers Provincial Government of Imbabura, not only errors by administrators or developers, also by the users because more than 60% use the username email as password. The vulnerabilities are due in great part to the obsolescence of computer applications.

The recognition of the characteristics of the servers as ports and versions of the services had no major impediments by the mechanisms of perimeter protection such as firewall, router or switch or the servers themselves, no clutch exists controls block from inside the network, namely it was left uncovered attacks from anywhere on the internet, and this point was evident in the ease of exploitation of vulnerabilities reported by each server.

The security policy of information is the most important document in which decisions and actions are based to take on security issues, no internal regulations or procedure is on the policy and any violation thereof shall be punished according internal regulation.

Los funcionarios debe respetar sus roles, responsabilidades y privilegios de acceso hacia los sistemas de información y no intentar sobrepasar los límites de acceso asignados o poner en peligro la integridad de la información o los equipos con acciones ilegales o negligentes.

VI. RECOMMENDATIONS

Proper selection of security controls depends directly on the correct risk analysis of information assets and identification of all mild or severe vulnerabilities of assets, because these results lead the development of the rest of the project until the implementation of the ISMS.

The ISO/IEC 27001:2005 clearly states realize periodic monitoring of the functioning of the measures taken for the security of information, and update or make changes based on experience or failures encountered until the review.

It is advisable to train and practice the actions to take in case of any contingency arise from staff support, so act upon each will know the responsibilities assigned and processes that have to intervene to manage security incidents information.

The protection of information should be commitment of all staff of the Provincial

Government of Imbabura, each employee must be aware about the potential damage if security gets information to commit acts maliciously endangered own benefit or neglect. Motivate staff to take the initiative and capacitase on security of information or ask any questions or need clarification knowledge.

Until the moment, the Provincial Government of Imbabura has not suffered any serious security incident information assets, but the vulnerabilities exist and is the rate of time until some malicious attacker assault on the technological infrastructure of the institution, yet it is also imperative implementing a security operations center (SOC) to provide, monitor and control the network security and Internet.

VII. REFERENCES

[1] Ali, S., & Heriyanto, T. (2011). BackTrack 4: Assuring Security by Penetration Testing. Birmingham: Packt Publishing Ltd.

[2] Calles García, J. A., & González Pérez, P. (2011). La Biblia del Footprinting. Obtenido de Flu Project: Flu Project.com

[3] Graves, K. (2010). CEH: Certified Ethical Hacker Study Guide. Indianapolis: Wiley.

[4] ISO, & 27001, I. (2005). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.

[5] López Neira, A., & Ruiz Spoh, J. (2012). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/sgsi.html#section2a

[6] Nieves, R. (2010). Teoría del Delito y Práctica Penal – Reflexiones dogmáticas y mirada crítica. Santo Domingo, D.N.: Editora Centenario, S. A.

[7] The hacker news. (2012). CVE-2012-2122 : Serious Mysql Authentication Bypass Vulnerability. Obtenido de http://thehackernews.com/2012/06/cve-2012-2122-serious-mysql.html?m=1

Ortiz B., Autor

He was born on February 25, 1988, in Ibarra - Ecuador. He obtained his bachelor's title in specialization Physical Mathematical Sciences at the National "Teodoro Gomez de la Torre" College.

He completed his studies at the Technical University Northern University in the Engineering in Electronics and Communication Networks. He has worked as Integral technician at the National Telecommunications Corporation (CNT) from July 2011 to September 2013.

Maya E., Director

Edgar Alberto Maya Olalla was born on April 22, 1980, He obtained the title of Engineer in Computer Systems at the Technical University of the North (2006), He has Higher Certified Investigation (2009) and the title of Master in Communication Networks (2014).

He obtained certifications as instructor CISCO-UTN Academy in the four levels of CCNA and IT Essentials CISCO Academy ESPOL Guayaquil.

He has participated in various seminars, workshops and specialized courses with 1146 hours of professional academic training and investigation projects.

He currently serves as a professor of the School of Engineering in Electronics and Communication Networks FICA at the Technical University of North and as instructor-UTN CISCO Academy.