Network Security Issues in Computer Network

Himanshu Trivedi[1], Manoj Mali [2]
[1]*M. Tech Scholar, Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India.*
[2] *Assistant Professor, Shri U.S.B. College of Engineering and Management, Abu Road, Mount Abu, Rajasthan, India.*

***Abstract*-This Paper tries to a solution for improving the security of network. This study mainly focuses on information security standards, based on the ISO 27000 series. Further, the paper suggested solution inside a simulated network and monitors and evaluates it by using the network vulnerability scanner.**

With regard to the suggested solution, it is necessary to discuss the concepts of information security standards, and different security models and observe the advantages and limitations of them. Therefore, this research includes the definition of information security standards and the advantages and limitations of security models.

I. INTRODUCTION

Now a days, a huge range of security threats, from equipment malfunction to human errors, fraud, theft, damage, in so many countries, threaten organizations so that the need to protect information arises.

Information security indicates the need for protecting information from unauthorized access, use, exposure, interruption and alteration. The word "standard" is used inside the context of information security policies to distinguish between policies, standards and procedures.

To make the environment of an organization secure, all three levels of documentation should be preserved. The foremost goal of all information security standards is to focus on three main principles to guarantee information security, which are integrity, confidentiality and availability.

Integrity refers to the need to protect the unity and accuracy of the information as well as the methods used to process it. Confidentially refers to the guarantee that the information can only be accesses by the persons who have been permitted to utilize the information and all associated resources when needed. Availability refers to the guarantee that authorized users have access to information whenever they need it.

II. SECURITY MODELS

Security model is a main concept in design and analysis of secure systems since it unifies the security policy that should be imposed in the system. A model is a symbolic demonstration of a policy by which the requirements of the policy makers would be mapped into a group of rules that should be followed by a computer system.

It is a conceptual term that represents the whole objectives and goals of a system which must be met and performed to be acknowledged as secure and acceptable. There are many complex steps during the system's design and development to make conceptual security policy feasible in the system.

A security model indicates the conceptual goals to implement the security policy in an information system by indicating necessary precise data structures and methods of performance.

A security model is generally represented in analytical and mathematics facts, which are then mapped to system situations and, as a result, program developers will develop it through programming code.

III. IMPLEMENTATION

We have carried out a simulation on the available equipment where we used the network, as shown in figure below. We have carried out the entire process of improving the security of network by using ISO 27001 standards and evaluating the result by using network vulnerability scanner tools.

To reach the above aim, we devised a scenario which simulates a real network by using twodesktop computers, a router and a switch, and also using GFI LANguard software to evaluate the security of the network both before, and after, implementation of the security solution inside the network.

IV.CONCLUSION

Today, whereas organizations are faced with a large range of security threats, from equipment malfunction to human errors, fraud, theft, damage, in so many countries and, according to the fact that information can exist in many forms, the protection of information from a such threats in order to ensure business continuity is a necessity for the management of the organization.

Because of the importance of the security policy to guarantee a secure system, some research organizations have been trying to find new security models which cover all the essential concepts of computer security.

It is a fact that, currently (at the time of this report), there is no specific model for network security. In 2008, Joshua Backfield and John Bambenek (from SANS Institute), by publishing a paper, have defined a possible network security model as a framework which will allows general network security to be implemented and maintained by any size of company.

The proposed network security model (NSM) is a seven layer model based on the Open Systems Interconnection Model (OSI), which has been used to teach networking and troubleshooting networking for the past 25 years.

It should be mentioned that the implementation of the information security is not a one-time process; it is a routine which needs to be performed continuously.

This process can be achieved by identifying the objectives and goals of the information security in the organization, and by defining an efficiency security policy which covers these objectives and preparing checklists for all the information assets, based on the ISO standard series in order to implement the security policy.

REFERENCES

[1] ISO/IEC 17799:2005 – Code of practice for information security management available at:
http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm
[2] Matt Bishop, “Introduction to Computer Security”, Addison-Wesley, 2005
[3] Dieter Gollmann, “Computer Security”, Wiley, 1999
[4] Joshua Backfield, John Bambenek, “Network Security Model”, SANS Institute, 2008