International Journal of scientific research and management
(IJSRM) ||Volume||2||Issue||4||Pages||742-748||2013||
Website: www.ijsrm.in ISSN (e): 2321-3418

Network Security Issues and Tools for Testing Security in Computer Network.

[1]Rachit Gupta, [2]ShwetanakSaurabh, [3]Neeraj Kumar
Dronacharya Group of Institution
rachitsden@gmail.com
krshwetanksaurabh009@gmail.com
raja.sam729@gmail.com

Abstract
This research paper tries to put forward a solution for improving the security of network. This study mainly focuses on information security standards, based on the ISO 27000 series.
Further, the thesis implements the 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.

1 Introduction
An increasing number of users, in addition to businesses in private network, demand access to Internet services such as the World Wide Web (WWW), electronic mail, Telnet, file transfer Protocol (FTP) and so on. Security is of indispensable concern when an organization connects its private network to the Internet.
There will be upward apprehension about the network security of the organization for system administrators in the case of revealing private data and network infrastructure to the crackers and intruders in particular when those data should be transferred via network.
Every organization has to define a security policy to display the level of protection which they need to avoid unauthorized access to the resources of their internal network, and to defend against the unauthorized export of private information. Even when connection to the internet is not established, it would be crucial to set up an internal security policy to control user access to part of the network and protect sensitive or classified information. Information is considered as being an asset; it is vital to be accurately protected like other important business assets. This is particularly essential in the increasing business environments which are connected to each other as an effect of this growing interconnectivity.
Information is in numerous forms. It can be printed or written on paper, stored by specific electronic devices , shown on films, transferred via ordinary post or by electronic means or it can even be found in conversation. Whatever forms the information takes, or by which it is shared or stored, it should always be thoroughly protected. In order to guarantee business permanence, minimize business risk, and maximize return on finances and opportunities, the security of the information and organization should be completely assured.Information security is obtained by implementing a proper group of controls, including policies, processes, routines, organizational structures and software or hardware functions, which should be established, implemented, monitored, reviewed, and improved where required to guarantee the presence of particular security and business objectives.

2 Information Security Standards
2.1 Introduction
Nowadays, 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

table2.1.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. [8]

Confidentiality	Guarantee that access to information is properly authorized.
Integrity	Safeguarding the correctness and unity of informational and processing methods.
Availability	Guarantee that authorized users have access to information when they need it

Table 2-1

To manage information security and achieve the three major concepts of security in organization, one solution is to implement ISMS (Information Security Management System) and use the ISO (International Organization for Standardization) standards as a guide to increase effectiveness of ISMS; [2] For example, to recognize information security risks in the organization, the organization may need to do a risk assessment. The best way to correctly evaluate the information is to think about Network Security Issues, Tools for official requirements, in addition, to decide what its own requirements are to develop or improve your own information security program. BS17799 simply tries to help those who want to improve their information security requirement for overall safety.

From another point of view, because the information has value and is therefore an asset, it needs to be protected just like any other assets. Information should be protected just like the Infrastructure that supports this information, including all the networks, systems and functions that enable an organization to control and manage its information assets. BS7799 explains the ways to protect organization's information assets. [1]

2.2 History of ISO Information Security Standards

The U.K Department of Trade and Industry (DTI) arranged a working group to work on codes for high-quality security practice, and the user version of this was published in 1989.

This standard was basically a list of security controls in which the practices were considerably suitable, normal, and as well as appropriate to the technology and environment of that era. The DTI code of practice for users was published as a British Standard (BS) instruction and, afterwards, was released as a BS with the name; BS 7799:1995 Part 1.Part 1 contains a list of controls of best practices for information security. [1]

A further part of the standard was introduced as BS 7799:1998, Part 2. The purpose was to provide a tool to assess and monitor Part 1, and to suggest a benchmark for certification. Following as the result of revision, Part 1 was published as BS 7799:1999, Part 1, was considered as an international standard (ISO), and published as ISO 17799:2000. Revision of Part 2 was published as BS 7799:2002, Part 2. The standard ISO 17799 was once more edited and published as ISO 17799: 2005, then there was a name change, to ISO 27002:2005. In July 2007, BS 7799, Part 2 was submitted as an international standard and was released as ISO 27001:2005.

2.3 International Security Management Standards

Table 2-2 presents a list, and short explanation of some security standards that are, or will be, published in the ISO 27000 series. Anything marked "pending" is theoretical at the time of the writing of this paper

ISO/IEC	standard description
27001	information security management system requirements (specification)
27002	code of practice for information security management
27003	(Pending) implementation guidance.
27004	(Pending) metric and measurement.
27005	(Pending) risk management.

Table 2-2 (Taken from [2])

Organizations having been certified aligned with BS 7799, Part 2, should renovate their certification with the latest ISO 27001 standard. ISO 27002 is the new name for ISO 17799,ISO/IEC 27003 covers implementation guidance, and is based on BS 7799, Part 2; the date of publication of this standard is pending (at the time of writing this report).[4]

In BS 7799, Part 2 (and ISO 27001), the PDCA model (plan, do, check, act – is a scientific method to continuous improvement) is also covered and is used not only to enforce information security standards, but is generally used to enforce other management standards, including ISO 9001 and ISO 14001. ISO 27004 will focus on how to employ metric to measure the performance and efficiency of ISMS operations; once more, the publishing date is pending (at the time of writing this report). [2] ISO 27005 will probably include risk management and will be similar to BS 7799, Part 3, which is about instruction for information security management. Additional organized standards at this time in the ISO 27000 series are ISO 27006, which is probably, contains the instruction for the

certification or registration routine, and the ISO 27007 instruction for auditing information
security management system. [1]

The standards are updated at least every two years in order to: [3]

- Provide a solution to the need of international organizations
- Develop best practices for information security
- Indicate to the lately deliberation in information security
- Stay aligned with other information security-related standards, such as ISO 27002(17799), COBIT v4.1 and PCI/DSS .
- Include information on the latest 'hot topics'.

2.4 The Necessity of Information Security

Information is now accepted as being a critical asset for most of the organizations and businesses in the world. The purpose of information security is the protection of organizational assets (in other words, information) from exposure by unauthorized or accidental modification, and guarantees that the information is ready for use when needed. Conventionally, organizational asset space mostly consists of physical assets, like equipment and buildings, and negotiable ones, like stocks,bonds, currency or gold.Thus, to remain viable, the organization must take information security seriously and implement effective ISMS, using a disciplined approach for instance, ISO standards, as a guideline. ISO 27001 is designed to support this mission. It is easy to understand the results for an organization if its information is lost, damaged, corrupted, burnt, flooded, maliciously destroyed or abused. [3]

3 Security Models

3.1 Introduction

As mentioned before, computer security rests on confidentiality, integrity, and availability. Security policy recognizes the threats and clarifies the requirements to provide a secure system. Security method detects and prevents attacks and enables recovery as well.

A security policy is a set of rules and practices prescribing how important information is managed, protected, and distributed, and also expresses the precise security level by defining which security methods are to be performed. [7]

This is an important part that has a major role in defining the design of the system. The security policy is a base for the specifications of a system and provides the baseline for evaluating a system. A system provides trust by executing the security policy and also deals with the relationship between subjects and objects. [8]

The policy must point out which subjects can access different objects, and what actions are acceptable and unacceptable. To provide a level of trust which is acceptable, a system must be on the architectural foundation that provides the ability to protect itself from unreliable processes, intentional or unplanned compromises, and attacks toward different layers of the system. A majority of the trust rating needs a specific subset of subjects and objects, explicit domains, and the separation of resources so the activities performed on them can be verified and their access can be controlled. [7]

A trust of the system is defined by a set of criteria. When a system is checked against this set of criteria, a rating is assigned to the system and is used by customers, vendors and the computing society. These criteria verify whether the security policy is being supported or implemented
accurately. [8]

3.2 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 policymakers 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. [9] Hence, a policy is what encloses security goals like "each subject must be authorized to access each object". The security model takes the necessity and provides the essential mathematical formulas, relationships, and structure which should be followed to perform this goal. Specifications are developed from here for different operating systems (UNIX, Windows, or Macintosh), and single vendors can decide how to implement mechanisms that cover these necessary specifications.

As a basic example, if a security policy conveys that subjects to access objects need to be authorized, the security model would suggest the mathematical relationships and formulas describing how x can access y just through outlined specific methods.

Specifications are then developed to provide a link to what is in a computing environment and how it maps to components and mechanisms that are to be coded and developed. The developers then write the program code to create the mechanisms that provide a method for a system to use access control lists and give administrators some levels of control.

This mechanism provides a GUI representation for the network administrator, like check boxes, to choose what subjects can access what objects, and the possibility to put this configurationwithin the operating system. This elementary example is useful in presenting the relationship

between the security policy and the security model; in reality, security models can be very complex. [6]

Some security models implement rules to guarantee confidentiality, such as the Bell-LaPadula model, while others implement rules to guarantee integrity, such as the Biba model. The above mentioned formal security models are used to offer high guarantees of security. Informal models, such as Clark-Wilson, are used more as a framework to describe how security policies have to be stated and executed.

A security policy indicates main goals with no idea of how they would be performed. A model is a framework that provides form to the policy and tries to find solutions for security problems for particular situations. Several security models have been developed to enforce security policies. in other words, the security policy provides then conceptual goals, and the security model provides necessary things which should be done to accomplish these goals.

4 Tools for Assessing the Security of the Network

4.1 Introduction

The network monitoring tools gather necessary information about all the computers and networks by testing the specific network services, such as finger, NFD, HTTP, FTP, SMTP and other services.

The information which is gathered shows the existence of different information services,

including possible security vulnerabilities. These security vulnerabilities typically appear due to improperly setup or configured network

services or equipment, the presence of notorious bugs in system utilities or weak policy implementation or design.There are several network assessment and monitoring tools around to assess the security of the network but, according to the survey released by insecure company in 2006-7, which asked 3243 hackers to name their favourites tools, the favourite vulnerability scanner tools are: 1-Nessus, 2-GFI LANGuard, and 3-Retina. We use Nessus and GFI LANGuard in the lab to find out the security vulnerabilities which exist on the simulated network and understand how they work.

4.2 Nessus

Nessus is a powerful and simple to use free remote network security scanner. Nessus offers an environment to audit a given network remotely, and discover if there is some vulnerability inside the network which hackers can use to get into it, or mistreat it in some way. Because every computer has thousands of communication paths, which are called ports, some services may listen to them for related communication packets. Nessus first recognizes what service is running on the ports by testing each port then, by testing the service, it tries to discover if there is vulnerability in that service which can be used by a hacker. Nessus does not notice that a specific service is always running on a specific port. This feature is completely different compared to the other security scanners and it means that, for example, if a mail server is running on port 1111 for the security consideration, it will discover it and test if

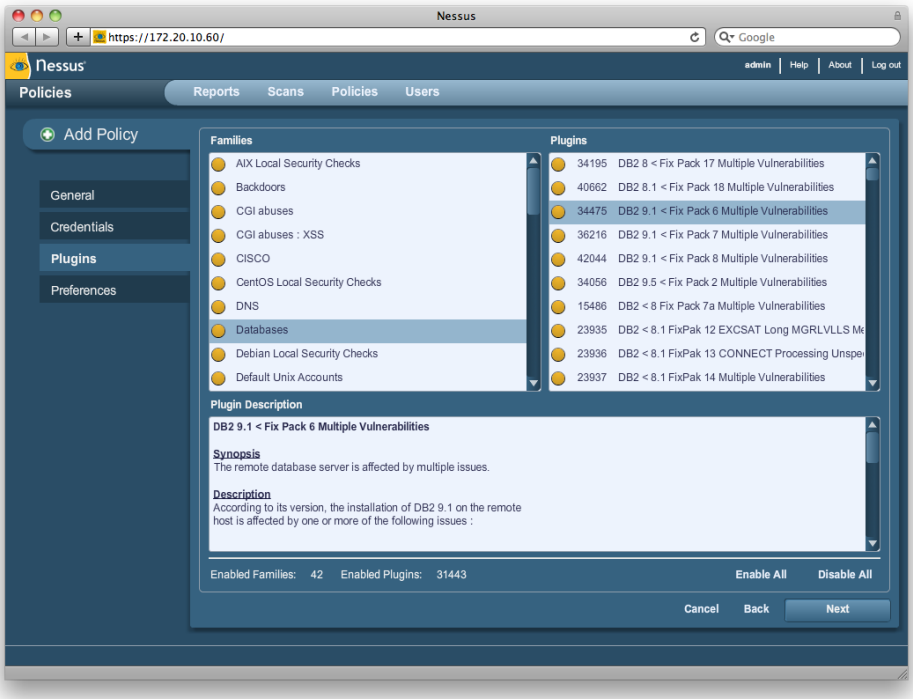

Fig 4.1 The main page of Nessus Client software

it is secure.

Another important feature this software has is that Nessus does not recognize that a particular service has vulnerability because of the version of that remote service; this means that it will actually try to exploit the vulnerability of the service.

Another powerful feature of the Nessus is that, by default, it can do more than 7000 security vulnerability tests, which are separated into 23 different categories, such as: different backdoors, CGI vulnerabilities, CISCO, DoS(denial of service), finger misuse, firewalls, FTP, earn root privilege remotely, Netware. By providing a scripting language, the administrator can write their own script to test a particular system; this feature makes the Nessus very extensible. In addition, it must be mentioned that Nessus is a remote scanner, so it is not required to be installed on a computer to test it. This means that it can be installed on only one computer and test the all the computers on the network.

Nessus consists of two major parts: a server and a client. The role of server part is to run all the scans and the role of the client part is to controlthe scans and observe reports. The structure of the Nessus, which is based on client-server architecture, provides capability for the server, which acts as scanner, and the client, which acts as graphical user interface (GUI), to distribute inseveral configurations. This allows the use of one server by several clients, reducing management costs.

4.3 GFI LANguard

The GFI LANguard is a vulnerability scanner for the network which offers a centralized environment for the IT administrators of the organizations to discover and solve security vulnerabilities by scanning computers on the network.

This software is produced in two versions: one as a licensed product and the other as a free version. The free version of this software has all available features but a maximum of 5 IP addresses can be scanned. However, the licensed product can be used for larger networks with numerous IP addresses.

This is a powerful tool for scanning and auditing all the computer ports for the existence of known vulnerabilities and also for the security of the network.

One of the important features which makes this software more powerful is that it offers central patch management abilities, which provide a central environment for downloading and distribution of patches to systems which are recognized to have vulnerabilities. This means that this software has the ability to perform like both a patch manager and vulnerability scanner. It has also some strong features, such as gathering all the network's important information, like network devices and identification of the device type, such aswired, wireless or virtual.

It recognizes wide range of vulnerabilities for different network services and open shares on the computers and lists the all users who have access to these shares and permissions these users have.The above mentioned feature provides the ability for this software to act as a networ

Audit ause 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 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. More specifically, after implementing and enforcing the security policy inside of the network (as a part of information security), by using the network monitoring tools, an administrator of the network can more precisely evaluate the situation of the network security and make correct decisions to improve the level of the security inside the network against the malicious hacker who tries to gain access to any computer which is connected to the network.

To gain such a level of security, each organization needs to have setup a working group of experts to identify, design and implement the security policies; to evaluate the security level of the organization from time to time; to prepare the management report and to offer solutions for the vulnerabilities which are probably present inside the network. Currently, this way is going to be established as a development solution to improve the security of the information inside all organizations around the world.

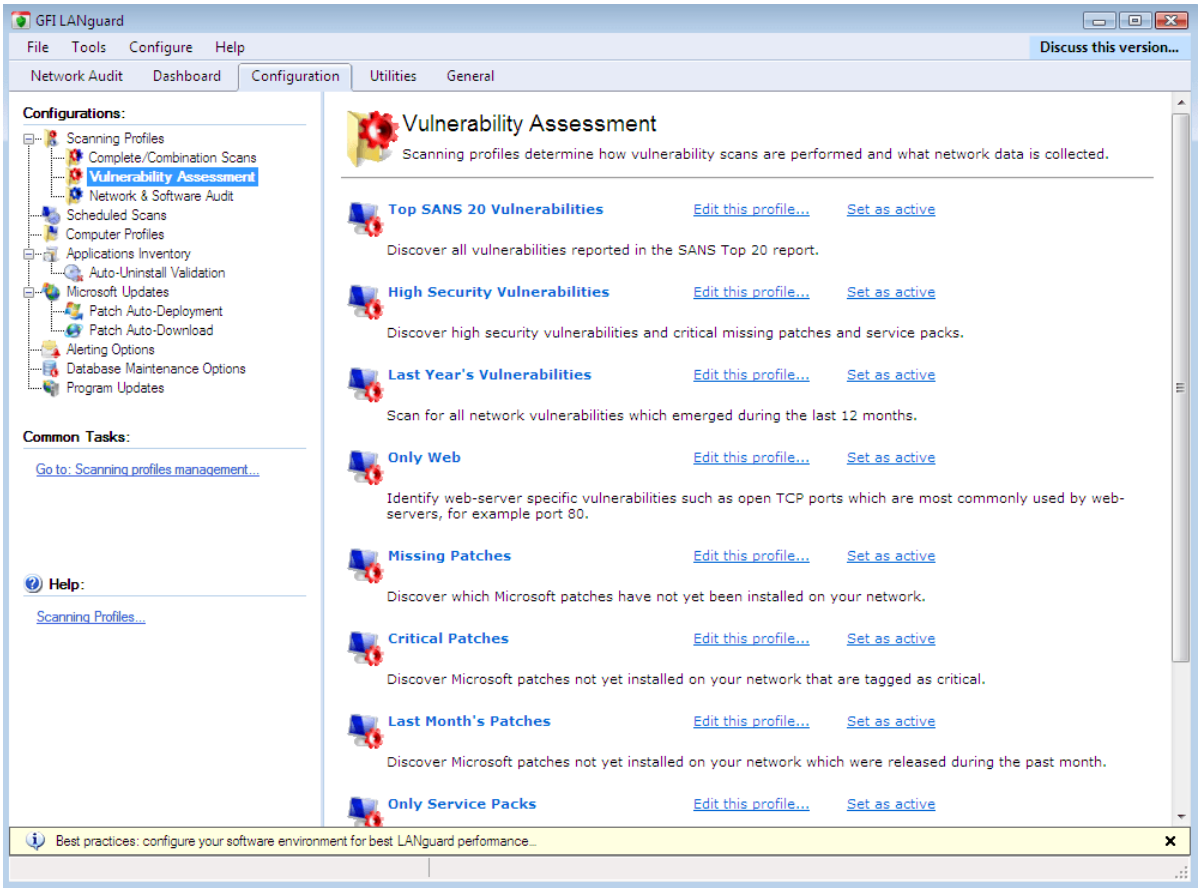

Fig 4.2 Main page of GFLAN guard

6 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] Sigurjon Thor Arnason and Keith D. Willett, "How to Achieve 27001 Certification", Published by CRC Press, 2007

[3] The standard of good practice available at: https://www.isfsecuritystandard.com

[4] IT management – BS 7799 available at: http://www.tech-faq.com/bs7799.shtml

[5] Introduction to ISO 27001 available at: http://www.isoqar.ir/html/iso_27001.html

[6] Ed Tittel, James Michael Stewart, Mike Chapple, "CISSP:Certified Information System
Security Professional", 2nd edition, SybexInc, 2003

[7] Michael E. Whitman and Herbert J. Mattord, "Principle of Information Security", 2nd

edition, Thomson Course Technology, 2005

[8] Matt Bishop, "Introduction to Computer Security", Addison-Wesley, 2005

[9] Dieter Gollmann, "Computer Security", Wiley, 1999

[10] Joshua Backfield, John Bambenek, "Network Security Model", SANS Institute, 2008