ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (335-340), Month: April - June 2015, Available at: www.researchpublish.com

Scope of Enhanced Network Security

BODLA. SHESHANAG

Abstract: **In the contemporary world every organization is in need of using the secure network. The threats are increasing rapidly. The reliability on wired or wireless networks is getting reduced. Industries are in need of security to fulfill their requirements efficiently. Defence also needs authenticated security since the intruders may steal the important information which is essential for the country. WI-FI devices and networks are most common in providing resources wirelessly. These WI-FI networks and devices are easily vulnerable to hackers. I would like to propose some scenarios so that a secured network can be launched in the organizations.**

Keywords: **WI-FI devices, Network Security.**

I. INTRODUCTION

The definition of Network Security is explained as providing the security to the networks from the third party applications in order to save the personalized data. There are various policies adopted by the network administrator depending on the attacks. Network security limitations are explained as below.

1) SECURITY ATTACKS:

Security attacks are differentiated in to two types they are:

-->Active attacks and

-->passive attacks

Active attacks:

In this type of attack the attacker blocks the stream of data in both or single directions. The properties or characteristics of Active attacks are

-->Interruption:

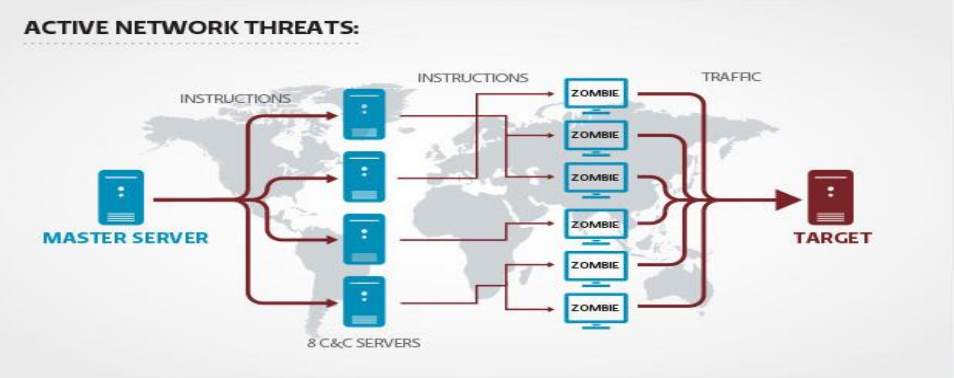
The information or data which is stored is lost.

-->Fabrication:

In this fabrication some extra data is added to the already stored data and it is very artfully done such that it is very hard to differentiate.

-->Modification:

Modification as the name itself specifies the definition that the type of attacks modifies the data so that they may perform the extra operation.



PASSIVE ATTACKS:

In the passive attacks the third party doesn't involve in any alteration of data. But the third party person can read all the data in the system. These type of attacks are very hard to find out because there are no alterations made by the un authorized persons. The characteristics of Passive attacks are

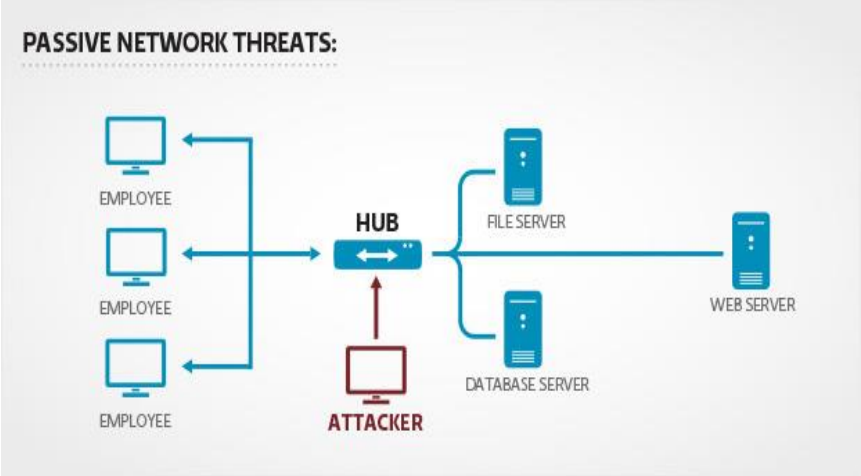
-->It is also called as tapping

-->Very hard to find out because no alterations are made.

Passive attacks are classified in to various types they are:

-->Traffic analysis and

-->Interception.



II. MEASURES NEED TO TAKE FOR THE SECURE NETWORK

->Establish a strong security firewall so that unauthorized people are not allowed.

->Assign a very strong password and try to change it more often.

->If you are using a wireless networks try to assign a sturdy password.

->Use a durable anti-virus for securing the system and data.

Some tools used for better network security:

->VMware
->Helix
->True Crypt
->Argus
->IDA pro
->X-scan
->Wikto
->BASE

III. DIFFERENT SECURITY METHODS FOR NETWORK SECURITY

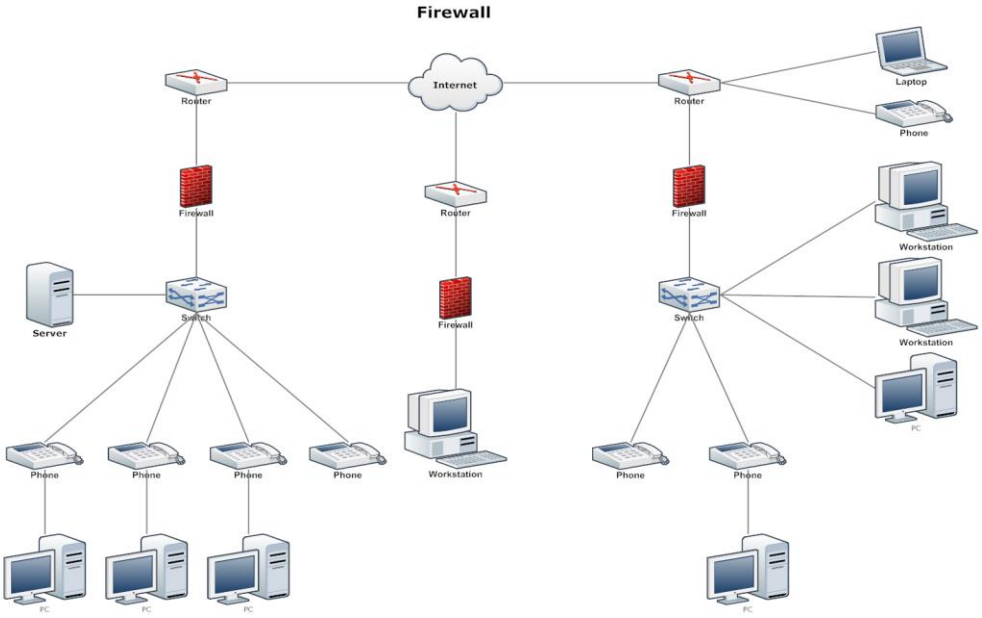
There are various security methods among them some strong methods are:

-->Firewalls:

The firewalls are nothing but it forms barrier between two networks.

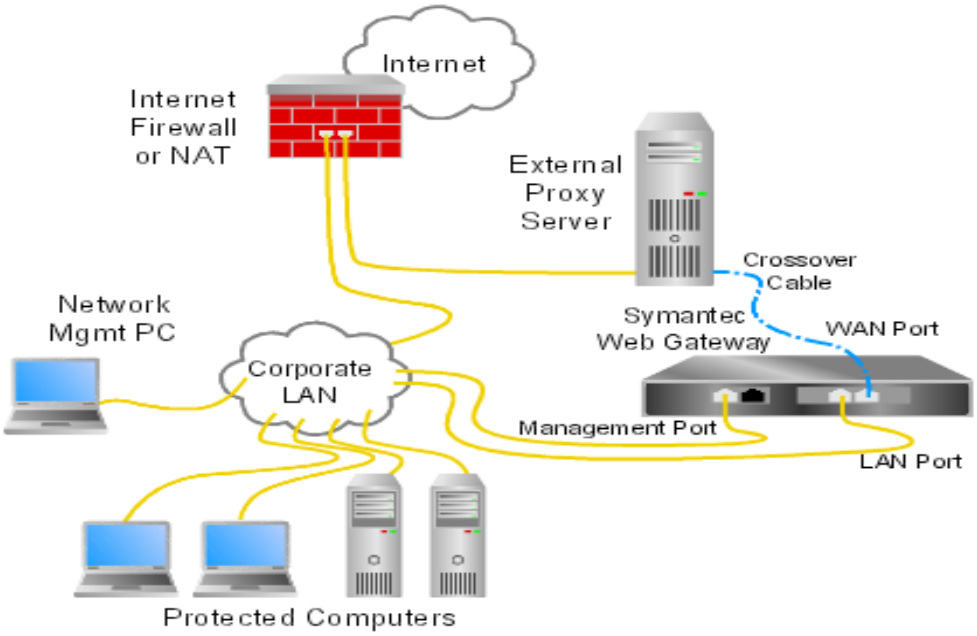
Firewalls are classified into different types they are:

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (335-340), Month: April - June 2015, Available at: www.researchpublish.com



-->Proxy gateways:

These act as a proxy server. This is also called as Application gateways because this program runs at the application layer of the referencing models like OSI/ISO. This gateways are most strong and secure because it does not allow any thing by default.



->PACKET FILTERING:

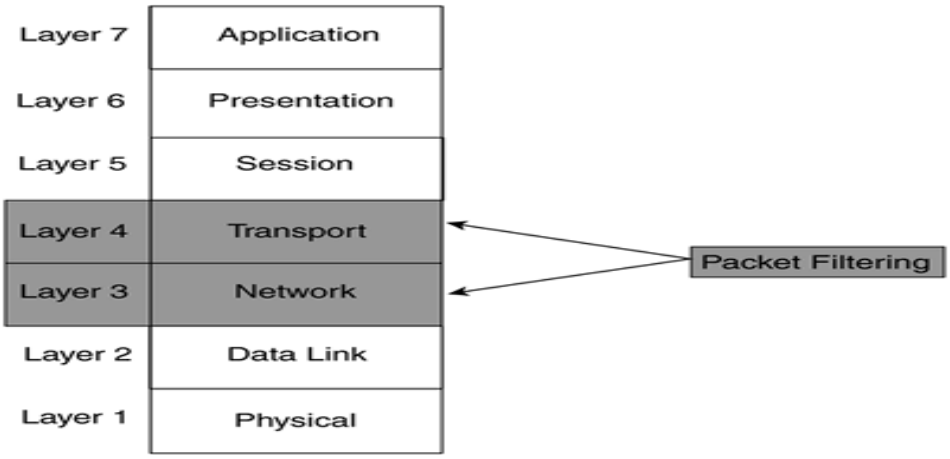
In this Packet Filtering the Access Control Lists are kept turned on for the routers. The access Control Lists provides which type of permission is given to the public to access the internal network. This packet filtering is done at lower OSI.ISO layer so it is less complicated than the application gateways or proxy gateways.

Characteristics of Packet Filtering:

1) Less complicated.

2) More faster.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (335-340), Month: April - June 2015, Available at: www.researchpublish.com



IV. SECURITY CHALLENGES

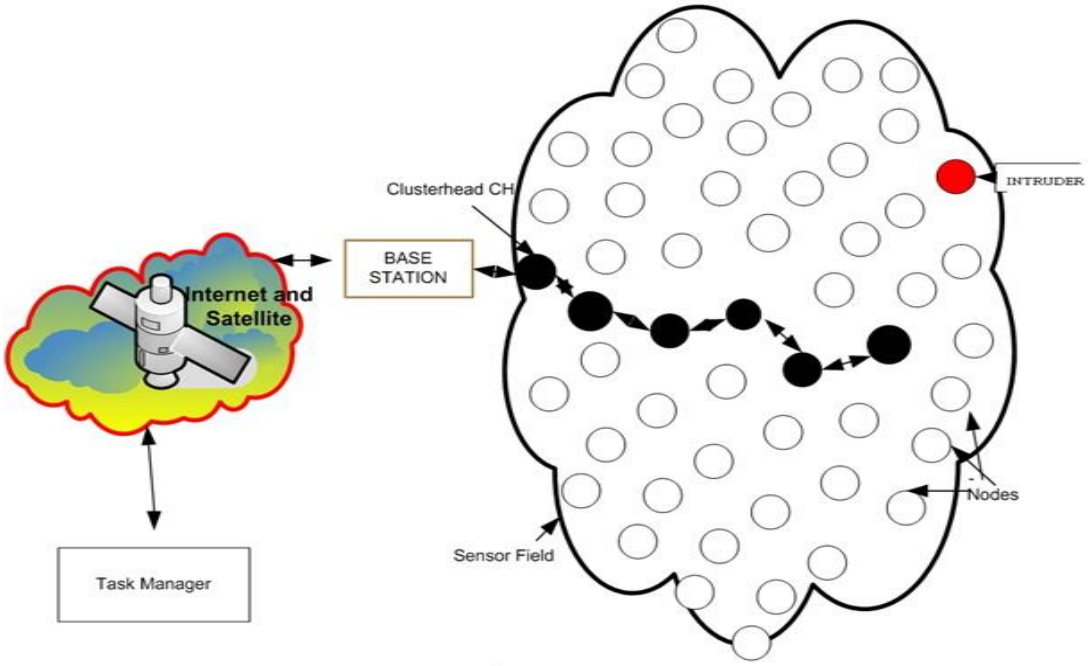
There are various security challenges they are described below:

->Every organization will be having some security procedures and implementation techniques but mostly they are not implementing them exactly. So, now a day's making sure that the network is secured or not is a big issue for the organization.

->The concept of implementing the security became a big challenge. The IT Managers must also concentrate on the security issues not only on the administration of technology.

->The organizations should also upgrade their infrastructure as per today's challenges and issues.

->Securing the point products is the biggest issue for the organizations wile implementing the security.



V. RESPONSIBILITIES OF ORGANIZATION'S

There are many responsibilities for an organization to provide the security some of them are:

->The security procedures must change depending on the requirements and the user need to feel comfortable and flexible with the security provided.

->As nowadays many organizations are developing rapidly so, the old organizations need to compete with the developing organizations in all the possibilities like what level of applications and size.

->The organizations must keep changing the process of providing security based on the changing of requirements because different platform of technology needs different types of security.

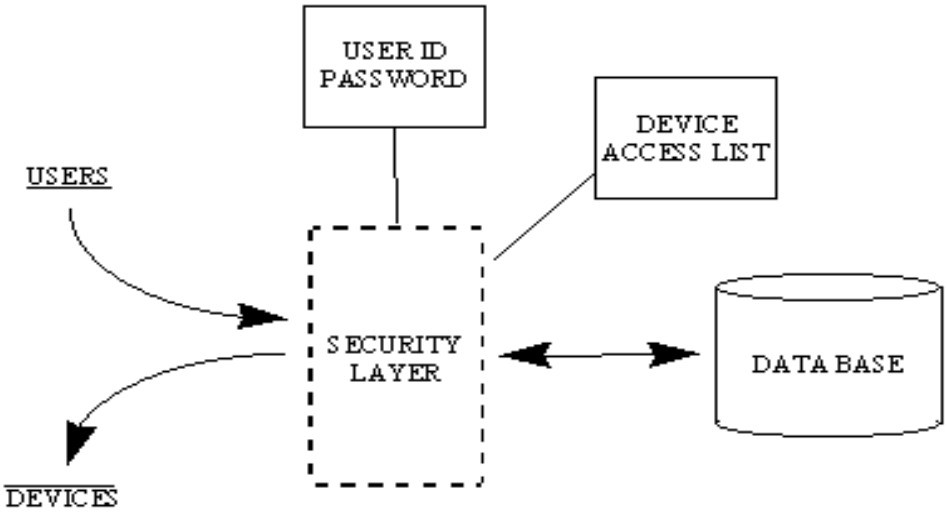
->Web-enabled technology is most frequently affected/attacked so, organizations must enable web-security services in order to access secure web applications.

->The procedure of providing the security must be easy to understand and to deploy.

VI. EXAMPLE

In this example I would like to show you that how data in an organization is gathered by the user from the data storage disks in a secured manner

EXAMPLE:



The explanation of the above example is that in an organization the information is gathered by the user like firstly the user sign 'sin in to his account by providing his ID and pass code then the process of the verification will be running internally and then authenticated by using the process of digital signature then the permission is granted to the user to access and gathering the information in the data storage. This is the security mechanism applied in the organizations.

VII. EMERGING DEVELOPMENT WORK FOR FUTURE

As the threats, malfunctioning and attacks are rapidly growing with the developing networks and also the intensity of damage is also increasing. So, organization must need to know the types of malfunctioning, threats and attacks which are forthcoming in the future so that they can get ready to face any type of issues and challenges in the future.

In the present era the system tools are WEB-BASED but previously systems tools are used to be Command Line Interfaces.

VIII. CONCLUSION

In today's contemporary world as the number of networks are developing in the same ratio the attacks are also developing. Different people have different perspectives in providing the security but the main motto of every person is to provide the good and strong security measures for the network which consists of information. Basically the organization need to understand the purpose of security and then implement the security for the networks. And there may be various levels of the organizations. The security should be provided in such a way that the user must feel comfortable for using it user must not feel that they are restricted in using or accessing the data. At the same time the network should be secured.

In the above discussion I mentioned all the necessary details and information about how to setup a SECURED NETWORK.

REFERENCES

[1] A beginner's guide to network security, CISCO Systems, found at http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf, 2001

[2] http://www.researchgate.net/publication/221635407_Challenges_for_Enhanced_Network_Self-Manageability_in_the_Scope_of_Future_Internet_Development.

[3] http://www.cs.colorado.edu/~rhan/EBSS_tech_report_CU_CS_951_03.pdf

[4] Farrow, R., Network Security Tools, found at http://sageweb.sage.org/pubs/whitepapers/farrow.pdf

[5] Flauzac, O.; Nolot, F.; Rabat, C.; Steffenel, L.-A., "Grid of Security: A New Approach of the Network Security", In Proc. of Int. Conf. on Network and System Security, 2009. NSS '09, pp. 67-72, 2009.

[6] http://www.academia.edu/8221162/ENHANCED_NETWORK_SECURITY_SYSTEM_USING_FIREWALLS

[7] Murray, P., Network Security, found at http://www.pandc.org/peter/presentations/ohio-tech-2004/Ohio-tech-security-handout. pdf.