MODERN NETWORK SECURITY: ISSUES AND CHALLENGES

Minal Kunal Thakur

University of Mumbai Institute of Distance & Open Learning (IDOL),

Information Technology, University of Mumbai

Abstract:

Secure Network has now become a need of any organization. The security threats are increasing day by day and making high speed wired/wireless network and internet services, insecure and unreliable. Now – a - days security measures work more importantly towards fulfilling the cutting edge demands of today's growing industries. The need is also induced in to the areas like defense, where secure and authenticated access of resources are the key issues related to information security. In this paper Author has described the important measures and parameters regarding large industry/organizational requirements for establishing a secure network. Wi-Fi networks are very common in providing wireless network access to different resources and connecting various devices wirelessly. There are need of different requirements to handle Wi-Fi threats and network hacking attempts. This paper explores important security measures related to different network scenarios, so that a fully secured network environment could be established in an organization. Author also has discussed a case study to illustrate the minimal set of measures required for establishing network security in any organization.

Keywords:

Cryptography; Security Attacks; Security Measures; Security Tools; WAN; Security Factors; Firewalls; Gateways; Intrusion Detection.

INTRODUCTION:

Network security can be defined as protection of networks and their services from unauthorized alteration, destruction, or disclosure, and provision of assurance that the network performs in critical situations and have no

harmful effects for neither user nor for employee [6].

It also includes provisions made in an underlying computer

network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access. Network security design constraints can be summarized

under the following,

A. Security Attacks:

Security attacks can be classified under the following categories:

Passive Attacks

This type of attacks includes attempts to break the system by using observed data. One of the examples of the passive attack [8,11] is plain text attacks, where both plain text and cipher text are already known to the attacker.

The attributes of passive attacks are as follows:

- **Interception**: attacks confidentiality such as eavesdropping, “man-in-the-middle” attacks.
- **Traffic Analysis**: attacks confidentiality, or anonymity. It can include trace back on a network, CRT radiation.

Active Attacks

This type of attack requires the attacker to send data to one or both of the parties, or block the data stream in one

or both directions. [8, 11] The attributes of active attacks are as follows,

- **Interruption**: attacks availability such as denial-of-service attacks.
- **Modification:** attacks integrity.
- **Fabrication:** attacks authenticity.

B. Network Security Measures:

Following measures are to be taken to secure the network:

- A strong firewall and proxy to be used to keep unwanted people out.
- A strong Antivirus software package and Internet Security Software package should be installed.
- For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
- When using a wireless connection, use a robust password.
- Employees should be cautious about physical security.
- Prepare a network analyzer or network monitor and use it when needed.
- Implementation of physical security measures like closed circuit television for entry areas and restricted zones.
- Security barriers to restrict the organization's perimeter.
- Fire asphyxiators can be used for fire-sensitive areas like server rooms and security rooms.

C. Network Security Tools:

Following tools are used to secure the network:

- N-map Security Scanner is a free and open-source utility for network exploration or security auditing.
- Nessus is the best free network vulnerability scanner available.
- Wire shark or Ethereal is an open-source network protocol analyzer for UNIX and Windows.
- Snort is light-weight network intrusion detection and prevention system excels at traffic analysis and packet

logging on IP networks.

- Net Cat is a simple utility that reads and writes data across TCP or UDP network connections.
- Kismet is a powerful wireless sniffer.

SECURITY METHODS:

a. Cryptography

- The most widely used tool for securing information and services.
- Cryptography relies on ciphers, which is nothing but mathematical functions used for encryption and decryption of a message.

b. Firewalls

A firewall is simply a group of components that collectively form a barrier between two networks. There are three basic types of firewalls:

I) Application Gateways:

This is the first firewall and is sometimes also known as proxy gateways as shown in figure 1. These are made up of bastion hosts so they do act as a proxy server. This software runs at the Application Layer of the ISO/OSI Reference Model. Clients behind the firewall must be categorized & prioritized in order to avail the Internet services. This is been the most secure, because it doesn't allow anything to pass by default, but it also need to have the programs written and turned on in order to start the traffic passing.

II) Packet Filtering:

Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent through it. ACL's is a method to define what sorts of access is allowed for the outside world to have to access internal network, and vice versa. This is less complex than an application gateway, because the feature of access control is performed at a lower

ISO/OSI layer. Due to low complexity and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins. Working at a lower level, supporting new applications either comes automatically, or is a simple matter of allowing a specific packet type to pass through the gateway. There are problems with this method; thought TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, use layers of packet filters are must in order to localize the traffic

III) Hybrid Systems:

In an attempt to combine the security feature of the application layer gateways with the flexibility and speed of packet filtering, some developers have created systems that use the principles of both. In some of these systems,

new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed. Uses of packet filtering and application layer proxies are the other possible ways. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network.

SECURITY MANAGEMENT ISSUES:

- Ensuring the security strength of the organization is a big challenge nowadays. Organizations have some pre-defined security policies and procedures but they are not implementing it accordingly. Through the use of technology, we should impose these policies on people and process.
- Building and affirming high-quality resources for deployment and efficient management of network security infrastructure.
- Adopting technologies that are easy and cost effective to deploy and manage day-to–day network security operations and troubleshoots in the long run.
- Ensuring a fully secure networking environment without degradation in the performance of business applications.
- On a day-to-day basis, enterprises face the challenge of having to scale up their infrastructure to a rapidly increasing user group, both from within and outside of the organizations. At the same time, they also have to ensure that performance is not compromised.
- Organizations sometimes have to deal with a number of point products in the network. Securing all of them totally while ensuring seamless functionality is one of the biggest challenges they face while planning and implementing a security blueprint.
- The implementation and conceptualization of security blueprint is a challenge. Security is a combination of people, processes, and technology; while IT managers are traditionally tuned to address only the technology controls. Network Security cuts across all functions and hence initiative and understanding at

the top level is essential. Security is also crucial at the grassroots level and to ensure this, employee awareness is a big concern. Being update about the various options and the fragmented market is a challenge for all IT managers. In the security space, the operational phase assumes a bigger importance. Compliance also plays an active role in security; hence the business development team, finance, and the CEO's office have to matrix with IT to deliver a blueprint.

FUTURE WORK:

Malicious code and other attacks are increasing in intensity and the damage that they cause. With little time to react, organizations have to become more proactive in their security stance. Reactive security will no longer work. Therefore, organizations need to better understand what the future trends, risks, and threats are so that they can be better prepared to make their organizations as secure as possible.

Generally, the network security system tools in the past were command line interface (CLI) based. It's only in these last few years that more and more computer and network administration task is done remotely through a web-based tool. Network system tools are very important no matter whether they are GUI or CUI, in today's heavily inter-connected era.

CONCLUSION:

Security has become important issue for large computing organizations [6]. There are different definitions and ideas for the security and risk measures from the perspective of different persons. The security measures should be designed and provided, first a company should know its need of security on the different levels of the organization and then it should be implemented for different levels. Security policies should be designed first before its implementation in such a way, so that future alteration and adoption can be acceptable and easily manageable.

The security system must be tight but must be flexible for the end-user to make him comfortable, he should not feel that security system is moving around him. Users who find security policies and systems too restrictive will find ways around them. Author have shown the minimum set of requirements parameters to establish a secure network environment for any organization with the help of case study of a software development firm. Security policies should not be fixed

rather than it should be flexible enough to fulfil the need of an organization as well as it should be capable enough to tackle future security threats while at the same time easily manageable and adoptable.

ACKNOWLEDGMENT:

The author is very thankful to Babu Banarsi das National Institute of Technology and Management, Lucknow, India, for providing excellent computation facilities in the College campus. Author also pays her regards to her Director of College, Department HOD and colleagues for giving their moral support and help in this research work.

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] Al-Akhras, M.A., “Wireless Network Security Implementation in Universities” In Proc. of Information and Communication Technologies, 2006. ICTTA '06., Vol. 2, pp. 3192 – 3197, 2006.

[3] Brenton, C. and Hunt, C. (2002): Mastering Network Security, Second Edition, Wiley

[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.