INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

EXPLORING VARIOUS ASPECTS OF NEWORK SECURITY

POONAM. A. MANJARE [1], PROF. R. R KEOLE [2],

1. PG Students H.V.P.M's college of Engg. & Tech., Amravati, India.
2. Faculty in H.V.P.M's college of Engg. & Tech., Amravati, India.

Accepted Date:
27/02/2013

Publish Date:
01/04/2013

Keywords

Network Security,
Vulnerabilities,
Threats, Firewalls,
Intrusion detection,
Secure E-mail

Corresponding Author
Ms. Poonam. A. Manjare

Abstract

The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. Threats can be seen as potential violations of security and exist because of vulnerabilities, i.e. weakness, in a system. When network and its components are structured, designed and architected well, the resulting system presents solid defenses and avoids potential single points of failure. The strongest network controls are solid authentication, access control, and encryption. But three controls are specific to networks, firewalls, intrusion detection systems and secure e-mail. Firewalls are just an updated form of reference monitor. Similarly, intrusion detection profits from more fundamental research into pattern matching and expert systems. And secure e-mail is really a carefully designed application of cryptography. These controls can be very effective in controlling our computing assets.

1. INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator [1]. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [2].

2. THREATS IN NETWORKS

2.1 Vulnerabilities:

Vulnerabilities are known security holes that exist in software. An example is a buffer overflow, which occurs when the developer of a software product expects a certain amount of data, for example 20 Bytes of information, to be sent at a particular point in the operation of a program, but fails to allow for an error condition where the user sends a great deal more data, or unexpected characters. Not all vulnerabilities are created equal- some will cause the program affected to crash or cause a reboot, or in the worst case, they can allow the attacker to gain root or administrative access to the affected system [2].

2.2 Threats or attacks

One useful way to categorize security threats or attacks is to look at the intent- a directed attack is one aimed at a single company- for example a company attempting to hack into a competitors network. A mass attack is usually a virus or worm, that is launched onto the internet, and that replicates itself to as many systems as possible, as quickly as possible. Attacks may come from outside of a company, or a company insider may carry them out. Threats aimed to compromise confidentiality, integrity, or availability, applied against data, software, and hardware by nature, accidents, no malicious humans, and malicious attackers.

3. NETWORK SECURITY CONTROL

The several strategies for addressing security concerns, such as encryption for confidentiality and integrity, reference monitors for access control, and overlapping controls for defense in depth. These strategies are also useful in protecting networks. There are particularly three important controls as firewalls, intrusion detection systems, and encrypted e-mail [3].

3.1 Firewall

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your internet access. A greater degree of protection is provided by a firewall router. A firewall is a device that protects one network from another while allowing communication between the two. When an incident is detected, the firewall can log details of the attempt, and it can optionally send e-mail to an administrator to report the incident. Using information from the log, the administrator can take action with the ISP of the hacker [4].

3.2 Intrusion detection system Intrusion detection system can be compared with a burglar alarm. For example, the lock system in a car protects the car from theft. But if somebody breaks the lock system and tries to steal the car, it is the burglar alarm that detects that the lock has been broken and alerts the owner by raising an alarm. The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the internet and the intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security**.** Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.

Components of Intrusion Detection System:

An intrusion detection system comprises of management console and sensors. Management console is the management and reporting console. Sensors are agents that monitor hosts or networks on a real time basis. An intrusion detection system has a database of attack signatures. If the sensors detect any malicious activity, it matches the malicious packet against the attack signature database. In case it finds a match, the sensor reports the malicious activity to the management console. The sensor can take different actions based on how they are configured. For example, the sensor can reset the TCP connection by sending a TCP FIN; modify the access control list on the gateway router or the firewall or send an email notification to the administrator for appropriate action.

Types of Intrusion Detection Systems:

There are broadly two types of Intrusion Detection systems. These are host based

Intrusion Detection System and network based Intrusion Detection System. A host based intrusion detection system has only host based sensors and a network based intrusion detection system has network-based sensor and network based IDS sensor has two interfaces. One of the interfaces is manageable. The IDS management console communicates with the sensor through the management interface. The other interface of the IDS is in promiscuous mode. This interface cannot be accessed over the network and is not manageable [6].

3.3 SECURE E-MAIL

Secure email is a safe, efficient alternative to regular email, fax and post. When you hit the send button on your secure email, the information contained in it is encrypted, so it can only be read by your intended recipient. By contrast, regular emails can be fairly easily intercepted and read by just about anyone. The Secure email service is an important part of the process of joining up the Criminal Justice System (CJS) in England and Wales. For the first time, it's made it possible for these key groups of people to send emails securely to each other. Secure email is already giving Criminal Justice Organizations and practitioners the confidence to send sensitive information via email. But you could be getting even more out of your secure email account by using it to send any confidential information related to your work [7].

Working of secure email:

Criminal Justice Organizations already have secure email systems (GSI, GSX and CJX) which are part of the Government Secure Community. They can send and receive sensitive information through these secure emil systems. Such organizations don't have to do anything to ensure that they are connected to the Secure email service, as this connects directly into - and is accredited by - the government secure Community. Criminal Justice Practitioners are not a part of this secure community; it falls to the Secure email service to provide the technology to encrypt the contents of an email when they send it. This encryption ensures that the email, if intercepted, will be unreadable. Once the email reaches its destination it will be decrypted so that the intended recipient can read it.

4. CONCLUSION

From the above paper we can conclude that it’s important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. It's important to get their feedback to understand what can be improved, and it's important to let them know why what have been done has been, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organization's exposure to them. Security is everybody’s business, and only with everyone’s cooperation, an intelligent policy, and consistent practices, it will be achievable.

5. REFERENCES

1. Jim Hietala"Network security" Sans track paper(2004)

2. Dr. Rahul Banerjee" An introduction to network security "self instructional material(SIM)module1(2006)

3. Network security white paper"digital malfunction and printing device"rich coporation(2007)

4. Juliegreen smith, uwenickline " Firewalls, Intrusion detection system and antivirus scanner" School of computer science and II NOTTIGHAM UNIVERSITY(2005)

5. SANS institude infosec reading room"intrusion detection system"(2011)

6. ntrusion Detection: Challenges and myths by Marcus J. Ranum http://secinf.net/info/ids/ids_mythe.html

7. Adam Shroll"An introduction to secure email"purdue university(2006)

8. Secure business communication with email encryption" water gaurd technology (2001)