IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Network Security, A Challenge

Harish Singh

Assistant Professor, Department of Computer Applications, Chandigarh Group of Colleges, Landran, Punjab, India

Abstract: The Internet is expanding with a tremendous speed so as its Security. Security is an important field that consists of the provisions made in underlying computer network infrastructure, policies adopted by the network administrator to protect the network, the network-accessible resources from unauthorized access and the effectiveness of these measures combined together. Personal, government, and business applications continue to multiply on the Internet and these work-based application and services can pose security risks to individuals and to information resources of companies and governments. Information is an asset that must be protected. Network security is more challenging than ever, as today's corporate networks become increasingly complex.

Keywords: Internet, Network Security, Firewall, Attacks, Threats, Phishing, DoS, Cookies.

I. INTRODUCTION

Network security is a challenge for network operators and internet service providers in order to prevent it from the attack of intruders. It deals with the requirements needed for a company, organization or the network administrator to help in protecting the network. Computers, networks, and the Internet affect our lives every day or we can say that we are so much dependent on them to make our life comfortable [2]. We all are connected to the internet without any boundary, so Network Security is essential in this environment because any organizational network is accessible from any computer in the world and, therefore, potential vulnerable to threats from individuals who do not require physical access to it.

Network Security can be referred as protecting websites domains from various forms of attack. If we have the knowledge of how various attacks are executed we can protect ourselves. Security means considering vulnerabilities, threats, attacks, countermeasures, and acceptable risks [1]. A Network were developed using different communicating devices .The Synchronous network consists of switches but do not require any security because switches do not buffer any data but a network consist of routers must be secure enough as information can be easily stolen by using malware like "Trojan Horse" [3].

Networks were developed so that we could share expensive computing resources. Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. The terms, information security and network security are most of the time used to represent the same meaning. Network security, though, is more specifically taken as the provision protection from outside intruders. When accessing information in an internetwork environment, secure areas must be created. The device that separates each of these areas is known as a firewall. A firewall usually separates a private network from a public network.

II. NEED FOR NETWORK SECURITY

Network security is the process through which we can protect the digital information. It is so crucial for all networks must be protected from threats and the risks so that a business can achieve its fullest potential. The objective of network security is:

A. To protect the confidentiality

The data must be accessed and read only by the authorized individuals or parties. It is the protection of the personal information. We can compare confidentiality with privacy. Data encryption, User Ids and passwords, biometric verifications are some of the methods through which confidentiality can be protected.

B. To maintain Integrity

It is the assurance of not only the information can be accessed or modifies by the authorized persons only but also the data must be accurate, consistent over its entire life cycle. Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous authentication practices. Cryptography plays a very major role in ensuring the data integrity. Hashing the data you receive and comparing it with the hash of original message is another method to ensure data integrity [4].

C. To Ensure Availability

Data must be available to the authorized persons at the right time. It can be ensured by rigorously maintaining all hardware, preparing hardware repairs immediately and maintaining a correctly functioning operating system environment. Regular backup must be taken, for information services that are highly critical, redundancy is appropriate method to ensure availability.

III. PROBLEMS IN NETWORK SECURITY

All network face one or more issues, it is the responsibility of the network administrator to keep the network secure for malicious software, worms, and threats and from other attacks. An attack is an information security threat through which the intruder attempt to obtain, alter, remove, implant or reveal confidential information without authorized access or permissions. Classes of attacks are [3], [5], and [8]:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

A. Passive Monitoring of Communications (Passive Attacks):
In this attack the disclosure of the confidential information or the files to an attacker without the consent of the authorized individual or an organization. The attacker monitors for the open ports or vulnerabilities to gain the information about the target without changing it on the target machine. There are two main types of passive attacks:

1) Release of Message Content: This is one of the easiest methods to grasp from its name and what it does it easily figured out also. In this type of attack it monitors the content of transmission either it is a telephonic conversation, an e-mail or a transferred file that contains the confidential information.
2) Traffic Analysis: This method also attack the confidentiality but it is little complicated than other methods. It is very subtle and hard to detect if we had a way to hide the information on a message and the hacker still viewed the hided information.

B. Active Attacks:
In this type of attack the hacker attempt to make changes to the data on the target machine. It can be said as the attacker can modify the stream of bits or creation of false stream of bits but the goal is same and much more of the passive attack and that is to steal the confidential information of the individual or organization and also do harm to the network or network services which they are providing. The active attacks are subdivided into different categories:

1) Replay Attack: It is a breach of security in which the hacker can store the information and then retransmit it with a trick to the receiver with some unauthorized operations such as false identification or a duplicate transaction. Replay attack is also known as a "man-in-the-middle attack," and It can be prevented by using strong digital signatures which include time stamps and inclusion of unique information that will be different from the previous transaction like a value of a constantly incremented sequence number.
2) Masquerade Attacks: The intruder pretends to be a particular user of the network system so that he can gain the access or some privileges that the user is authorized for. This attack is attempted through the use of stolen login Ids and passwords.
3) Modification of Messages: In this type of attack the intruder can use two different ways to modify the message either he will alter the packet header addresses to direct a message to a different destination or he will modify that data on the target machine so that an unauthorized effect can be produced. This is a very common type of attacks that is used.
4) Denial of Service (DoS): It is very hard to prevent the occurrence of DoS attacks because of all the vulnerabilities of software, hardware, and the network. Here users are deprived of access to the network or its resources. The entire network is disrupted by overloading the messages than it can handle to ruin its performance. DoS are the major threat to network security in today's scenario because they can be easily launched with some basic knowledge.
5) Distributed Denial of Service (DDoS): DDoS is a type of DoS attack where multiple compromised systems (Sometime called a botnet or zombie army), which are often infected with a Trojan horse, are used to target a single system causing a Denial of Service (DoS) attack.

C. Insider Attack:
These attacks involve someone who has authorized access to the network with either an account on the server or having a physical access to the network. He can intentionally or accidentally attack the network from some malicious or non-malicious ways. Malicious insiders intentionally eavesdrop, steal, or damage the information and they can use this information in a fraudulent manner. They can also deny access to other authorized users. In the same way attacks can be non-malicious while performing the tasks in an organization like carelessness, lack of knowledge, or intentional circumvention of security. Internal Intrusion Detection System (IDS) protect organizations against insider attacks.

D. Close-In Attack:
When an individual or a group is trying to attain close proximity to networks so that, they can modify, collect the information or deny the access to the information. Close physical proximity can be achieved through secret entry into the network or an open access [7]. One of the popular close-in attacks is social engineering, where the attacker compromises the network through social interaction through an e-mail or over the phone. The attacker will apply some tricks in the conversation so that the victim can reveal the secrets of the company and he attacker could gain unauthorized access to the network or to the system.

E. Phishing Attack:
It is also referred as brand spoofing or carding, the idea behind phishing is that the bait is thrown out with the hope that while most will ignore the bait, some will be tempted into biting. Phishing is a form of fraud in which the attacker tries to fetch the information such as login Ids, passwords, Credit card details etc by masquerading as a reputable entity or a person through e-mails, some communication channels or by creating fake websites which feels and look like authorized ones.

F. Exploit Attack:
In this type of attack on the computer system the attacker takes the advantage of a particular vulnerability that system offers to the intruders when the intruder knows about the security problem within an operating system or in a piece of software [9].

G. Password Attack:
Password attacks are the classic way to gain access to a computer system to find out the password and login Id. Their goals might differ, but they all tries to crack the passwords which are stored in a network account database or a password-protected file.

IV. CONCLUSION CATEGORIES OF NETWORK SECURITY THREATS

Network security threats are becoming increasingly sophisticated and dangerous because internet is an increasingly attractive hunting ground for hackers, criminals, activists and terrorists motivated to get noticed, make money, or even bring down corporations and governments through different threats of attacks. Network security threats can be categorized into four broad themes:

A. Unstructured Threats:
Unstructured threats mostly originate from inexperienced individuals using easily available hacking tools. These types of intruders are not most talented or experienced programmers or machine operators but they are those motivators who have ample of time to do something challenging. They are known as the script kiddies and pose a very serious threat to network security because many a time they cause a serious problem like a Trojan Horse or any other virus without known the consequences. Their skills can still do a lot of damage to a company.

B. Structured Threats:
Structured threats are imposed by individual or a group who are highly motivated and technically much strong than the script kiddies. They usually have knowledge of the network architecture, designs and their vulnerabilities. They know how they can penetrate and cause a problem to the network or the services they are providing. Occasionally, these intruders are hired by industries, some intelligence agency etc [6].

C. External Threats:
Threats originated from individuals or groups working outside of the organizations. They do not have authorized access to any of the computer systems or the network. They contact the organizations network from the internet or from the dial-up access servers.

D. Internal Threat:
A computer network or a server must be secure enough not only from the external threats but from the internal ones too. Internal threats originate from inside the organizations itself from a dissatisfied current or a former employee [6].

V. HOW NETWORK SECURITY CAN BREACHED

Connectivity of the internet has led to enormous social and economic benefits, but has also introduced numerous new challenges. Engineers and Specialist Officers with sophisticated skills are needed to prevent and defend against security breaching. A data breach is a security incident in which sensitive, protected or confidential data can be stolen, modified or damaged by any intruder. It can be done in any of the following methods:

A. Reconnaissance Attacks:
This attack is also known as information gathering. First of all, the intruder determine which IP addresses are alive and responsive just by giving a ping sweep, a technique that uses ICMP (Internet Control Message Protocol) echo and echo-reply to map a known network. After determining the IP Address the intruder determines which services or ports are active on that live IPs. From this information, the intruder can query the ports to determine which type of version of applications and operating systems are running on the target machine [5].

B. Access Attacks:
Access attacks can be used to gain unauthorized control of a system by installing software and hiding it so that it can be used latter on by the intruder. Access refers to the connection of a source machine with the destination one and both of the source and the destination machines can be in two different internetwork. Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.

C. DoS Attacks:
When the attacker corrupts the network system or services for the intended users by slowing it down to a specific point so that no authorized user can access the network resources or any of its services.

D. Web Cookies:
Although cookies do not carry viruses or any kind of malware cannot be installed on the host computer but cookies help the intruder to compile the records of browsing history of the individuals. Unencrypted cookies are the major network issue because they can breach the system using XSS (Cross Site Scripting) vulnerability and that is a major privacy concern. With “Open Cookies” the intruder could have access to any login data cookies (saved password sessions) on the network.

VI. TYPES OF NETWORK SECURITY

The different types of network security are as follows [3]:
A. Security by Obscurity:
Security by obscurity relies on the fact that a given vulnerability is hidden or secret as a security measure i.e. no one knows about the system that exists. Of course, if anyone or anything accidentally discovers the vulnerability, no real protection exists to prevent exploitation. The main problem with this type of security is that this is not a long term solution, once the system is detected no one can protect it and it will cause a lots of financial loss to the organization.

B. The Perimeter Defence (Firewalls):
To begin planning for perimeter-oriented network-defence strategy organizations securing network by putting it behind the firewall. Securing the company's network, it's best to start on the perimeter but one must know about its perimeter, it is basically where the system interfaces with the rest of the world. Security inside the deep of an organization by installing safeguards is good idea but the biggest bang for your security buck is by building up protection along the perimeter i.e. the network's boundary: the frontier where data flows in from (and out to) other networks, including the Internet. The security at the perimeter is done with the help of the firewall that act like

DOI 10.17148/IJARCCE.2016.5317

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

a checkpoint, allowing authorized data to enter unencumbered while blocking suspicious traffic.

C. Layered Security and Defence in the Depth: There is no doubt that layered security and defence in depth are two different concepts with a lot of overlap. To protect the information resources a layered security is extremely important. Defence in depth approach is applied to provide security at the maximum level i.e. it also deals with new conditions, new threats and flexible policies. It is a fundamental principle in the physical protection of the assets on an organization. Defence in depth strategies also include other security considerations than directly protective like monitoring, alerting, disaster recovery, forensic analysis.

D. Authentication:
The authentication procedure is further divided into three factor authentications. The advantage of using this three factor authentication method is that it makes sure that the person who is authenticating is the authenticated person. The disadvantage of this procedure is it takes time when a person forgot the first or second factor authentication.

1) One-factor authentication: Password i.e. "Something a user knows" is the most recognized type of one-factor authentication method. It is known to the user and he has to provide it for further authentication process.
2) Two-factor authentication**:** In addition to the first factor, the second factor is "something a user has." That can be a bio-metric impression, a signed digital certificate or a predetermined code through which user can prove his authorization.
3) Three-factor authentication**:** In addition to the previous two factors, the third factor is "something a user is." That can be about all bio-metric information of a user such as the user's voice, hand configuration, a fingerprint, a retina scan or similar.

VII. DEVELOPMENT IN NETWORK SECURITY

There are many dramatic changes in the technology of network security this is all because of new mobile operating systems, growing use of personal devices and many more reasons. Day to day enhancements both in technology and infrastructure make all these developments possible. There are more remote users, faster network connections, and extensive upgrades to mobile networks which are some of the reasons for network security [10].

A. Hardware Security Module (HSM):
HSM is a physical computing device and its core functionality is centred on encryption: the process by which sensitive data is rendered in a form that is not understandable to all except authorized ones. HSMs also offer a secure way to decrypt data to ensure message confidentiality and authenticity. These modules traditionally come in the form of plug-in card that attaches directly to a computer or network server. Functions of HSM are:

1) Onboard secure cryptographic key generations.
2) Use of cryptographic and sensitive data material.
3) Onboard secure cryptographic key storage and management.
4) Offloading application servers for complete asymmetric and symmetric cryptography.

B. Biometrics:
Biometrics use is obvious that is for secure workstation logons that is connected to a network. The primary advantage of this technology over others is that they really do what they should, i.e. they authenticate user by using human's physiological or behavioural characteristics to authenticate users. Biometric objects cannot be stolen as password, keys, and cards. Even the use of dead or artificial biometric characteristics should not let the attacker in. As we know nothing is perfect so biometric authentication methods also have their own shortcomings in terms of speed and accuracy [11].

C. Smart Cards:
It is an Integrated Circuit Card (ICC) of a pocket-sized that has embedded integrated circuits. They are made of plastics, generally polyvinyl chloride (PVC). Smart cards can provide personal identification, authentication, data storage, and application processing. Smart card can be stolen but there is a safety feature built into it. The authenticated uses have to enter a personal identification number (PIN) after using it. The PIN is verified from inside the smart card as it is never transmitted across the network, hence cannot be used if the smart card is stolen.

D. Intrusion Detection System (IDS):
An IDS is a listen only device or software application that monitors network or system activities for malicious activities. Intrusion prevention system (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them. IDS are placed out-of-band out he network infrastructure that is not a real-time communication path between the sender and the receiver of the information.

VIII. BIGGEST NETWORKS SECURITY CHALLENGES

Network systems are under attack from so many directions, with endpoints multiplying daily. Many network security technologies are still in their infancy and it is also known that the security and the network teams have historically not worked together closely [12].

A. Supporting Bring Your Own Device (BYOD):
A good number of enterprises now are supporting BYOD policy, it is a set of rules governing a corporate IT department's level of support for employee-owned PC's, smart phones and tablets. There are three critical components: a software application for managing the devices connecting to the network, a written policy outlining the responsibilities of both the employer and the user, and the agreement users must sign, acknowledging that they have read and understood the policy.

B. Automated Assessment and Response: Automation promises- the ability to respond to threats much quicker and possibly to greater effect. In this era everyone expects

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

high performance from their workplace networks but the technologies that make automation possible haven't succeed the trust level yet. Security automation technologies are not granular enough to be effective in scaling to such environments. Tools are required that can be more precise about the control.

C. Software-Defined Networking (SDN):
SDN is an approach to computer networking that allows network administrators to manage network services through abstraction of higher-level functionality. It has the potential to provide enterprises with the level of granular control they need in order to automate.

IX. CONCLUSION

Network security isn't something you either have or don't-it is a continual arms race against malicious hackers. Fortunately, as attacks become more sophisticated, so too does the technology and practices used to protect the network. One of the biggest security concerns today is the insider threat. Another major security concern is lack of consistency in enforcing "acceptable use" policy. Most of the policies are badly written, out of date and poorly communicated. Securing the network is just as important as securing the computers and encrypting the message. In current scenario there are number of ways, which guarantee for the safety and security of the network but it cannot be said they will everlasting. We have to perform regular network security testing.

REFERENCES

[1] Carle E. Landwehr, "Security Issues in Networks with Internet Access", Member, IEEE.
[2] Siddharth Ghansela, "Network Security: Attacks, Tools and Techniques", vol. 3, Issue 6, June 2013.
[3] Kartikey Agarwal, "Network Security: Attacks and Defence", vol. 1, Issue 3, August 2014.
[4] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
[5] http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html
[6] 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), Mouna Jouini
[7] Eric Cole, (2009), Network Security, Bible, 2nd Edition.
[8] Prakhar Golchha, "A Review on Network Security Threats and Solutions", 2347:3878, 2014.
[9] Inam Mohammad, "A Review of types of Security Attacks and Malicious Software in Network security", Vol. 4, Issue 5, May 2014.
[10] Bhavya Daya, "Network Security: History, Importance, and Future", University of Florida Department of Electrical and Computer Engineering.
[11] Vaclav Matyas, "Biometric Authentication-Security and Usability"
[12] https://powermore.dell.com/technology/network-security-three-biggest-challenges/