INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ATTACK AND THEIR PROTECTION IN COMPUTER SECURITY

MR. NIKHIL E. KARALE, MISS. SNEHAL D. RAJGURE

M. E. (CSE), PRMITR, Badnera

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* In today's world, network Security is now very important issue. So because of that several of methods come in the existence to provide the security to the computer network. It is very important to know various techniques that emerge in world in order to be secure in computer networks. This paper gives the various attack and protection methods which are used to protect the network.

Keywords: Firewalls, Encryption, DOS attacks

Corresponding Author: MR. NIKHIL E. KARALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Nikhil E. Karale, IJPRET, 2016; Volume 4 (9): 697-704

PAPER-QR CODE

1. INTRODUCTION

Network security has a broad field which was developed in stages and as of today, it is still in emerging stage. Network security means protecting the servers or web domains from many forms of attack. Network security is very necessary in every field of today's world such as government, military and even in our daily life. If we know how the attack are coming to our computer then we are better able to survive from that forms of attacks. The structure of the network can be changed so that it can be prevent from the attack like firewall etc. If we want to know the current research about network then first we need to know the background of network. As well as some knowledge about internet working. The growth of Internet has widely spread in today's world. The internet is available everywhere in our home, in our working area, mobiles, cars everything is connected to the internet and if an unauthorized person is get entry to our network then it will obviously harm our information or confidential data.

Routers are the form of network which gives route data towards the destination. The Trojan horse is responsible to stolen the information from this router. Therefore, Network security is manly focused on the data that are used with the internet. Electronic mail is a maximum used service and it is also consist of some serious issues like SPAM are serious issue threat this only very less time and efforts to affect the thousands o0f email users by just providing fake advertisements or fake information.. A Network can contain many such vulnerabilities so that security is now became serious issues.

2. Need of Network Security

In earlier, hacker are programmer who can exploit the vulnerabilities just by knowing the computer communication across link. Now on internet there are so many tools are available so that anyone can became hacker, can gain the knowledge about hacking and hack our network. Because of this there is need established about the security to our computer network. One way to protect our network is to close our network for the outside users. A closed access provide access to only inside users, trust users. If outside users want the permission to access our network then it need permission to enter into network.

With the development of network, the threats are spreading with greater extent. Hackers have generate so many security holes so that they can easily get the unauthorized access. Thus it need to provide network security.

3. Types of Attack in Computer Network

3.1 Passive Attack

In the **passive attack, the attackers** look for the unencrypted traffic, monitor clear-text passwords and confidential information that can be used in other types of attacks. It mainly includes analysis of traffic, monitoring of unprotected sharing, decrypting weakly encrypted traffic and capturing authentication information. This might include passwords. Passive interception what actually type of passive attack enables adversaries to see coming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

3.2 Active Attack

In an **active attack,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

3.3 Distributed Attack

A **distributed attack** requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

3.4 Insider Attack

An **insider attack** involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task

3.5 Close-in Attack

A **close-in attack** involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both. One popular form of close in attack is **social engineering** in a social engineering attack, the attacker compromises the network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

a. Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or paypal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

4. Protection Against Network Attack

An inherent weakness in the system may it be by design, configuration or implementation which renders it to a threat. But most of the vulnerabilities are not because of faulty design but some may be caused due to disasters both natural and made, or some maybe cause by the by same persons trying to protect the system [2].Most of the Vulnerabilities caused due to poor design, poor implementation, poor management, physical vulnerabilities, hardware and software, interception of information and human vulnerabilities. Many of the network attacks can be easily prevented by the network admin monitoring his network closely and applying the entire latest patch available from the vendor to his software. However this cannot prevent most of the attacks, to prevent them, the network requires configurations such as:

4.1. Configuration Management

It is as important as having a descent firewall to protect the system. As soon as a network setup is completed all its default logins, Ids, address must be changed as soon as possible as all these information is available on the internet for anyone to view. Anyone can use the default login to

gain access to the network and it can put all the network at risk. The machines inside the network must be running the running up to date copies of O and all the patches especially the security patches must be installed as soon as they are available, configuration files must not have any known security holes, all the data is backed up in a secure manner, it allows us to deal with nine out of the ten topmost attacks. Several tools are also available which allows patches to deployed simultaneously and keep things tight.

4.2 Firewalls

It is the most widely sold and available network security tool available in the market. This is the wall which stands between the local network and the internet and filters the traffic ad prevents most of the network attacks. There are three different types of firewalls depending on filtering at the IP level, Packet level or at the TCP or application level [11]. Firewalls help preventing unauthorized network traffic through an unsecured network to a private network. They can notify the user when an untrusted application is requested access to the internet. They also create a log of all the connections made to the system. These log can be very harmful in case of any hacking attempts. Firewalls only works if they are correctly configured, if somebody makes a mistake while configuring the firewall, it may allow unauthorized to enter or leave the system. It takes certain knowledge and experience to correctly configure a firewall. If the firewall goes down one cannot connect to the network as in a case of DOS attack. Firewall also reduces the speed of network performance as it examines both incoming and outgoing traffic. Firewall does not manage any internal traffic where most of the attacks come from. Many companies are under false assumptions, that by just using a firewall they are safe, but the truth is they are not, firewall can be easily be circumvented. The best thing while configuring firewall is to deny anything that is not allowed [12].

4.3 Encryption

Using encryption methods one can prevent hacker listening onto the data because without the right key it will just be garbage to him. Different encryption method such as using HTTPS or SHTTP during the transmission of data between the client and user, will prevent Man in the middle attack (MIM), this will also prevent any sniffing of data and thus any eavesdropping. Using VPN will encrypt all the data going through the network, it will also improve the privacy of the user. Encryption also has downsides as all the encrypted mail and web pages are allowed through firewall they can also contain malware in them. Encrypting data takes processing power from the CPU. This in turn reduces the speed at which data can be send, the stronger the encryption the more time it takes [13].

4.4 Defense against DOS Attacks

To prevent DDoS attack many technologies have been developed such as intrusion detection systems (IDSs), firewalls, and enhanced routers. These things are used between the internet and servers. They monitor incoming connections as well as outgoing connections and automatically take steps to protect the network. They have traffic analysis, access control, redundancy built into them [15].IDSs are make a log of both the incoming and outgoing connections. These logs can then be compared to baseline traffic to detect potential Dos attacks. If there is unusually high traffic on the server it can also alert of a possible ongoing DOS attack such as TCP SYN flooding [14].Firewalls can also be used as defense against DOS attacks with the required configuration. Firewalls can be used to allow or deny certain packets, ports and IP addresses etc. Firewalls can also perform real time evaluation of the traffic and take the necessary steps to prevent the attack. Security measures can also be employed in routers which can create another defense line away from the target, so even if a DOS attack takes place it won't affect the internal network. Service providers can also increase the service quality of infrastructure. Whenever a server fails a backup server can take its place, this will make effect of DOS attack negligible.

4.5 Vulnerability Testing

To prevent any attacks on the network, one must find any open vulnerabilities in the network and close them, these may include open ports and also faulty and outdated software with known vulnerabilities, outdated firewall rules etc. There are different tools available which allows a user to test his own network security and also find vulnerabilities in a network [4]. One such method is using a port scanner which can be used to probe a server and find any open ports. This is used by many admins to verify policies of their servers and also can be used by attackers on a network to find exploits. Some of the tools which are available for free on the internet are Nmap, SuperScan. These tools can be downloaded by everyone and each comes with a detailed tutorial for using them [16].

5. CONCLUSION

As internet has become a huge part of our daily life, the need of network security has also increased exponentially from the last decade. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to defense secrets as a result there is huge need of network security. Billions of dollars of transactions happens every hour over the internet, this need to be protected at all costs. Even a

small unnoticed vulnerability in a network can have disastrous affect, if companies records are leaked, it can put the users data such as their banking details and credit card information at risk, numerous software's such as intrusion detection have been which prevents these attacks, but most of the time it's because of a human error that these attacks occur. Most of the attacks can be easily prevented, by following many simply methods as outlined in this paper.

6. REFERENCES

1. B. Daya, "Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013.
2. Li CHEN,Web Security : Theory And Applications,School of Software,Sun Yat-sen University, China.
3. J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.
4. A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.
5. S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009
6. M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.
7. R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.
8. Q. Gu, Peng Liu, "Denial of Service Attacks," Texas State University, San Marcos.
9. M. A. Shibli, "MagicNET: Human Immune System & Network Security," IJCSNS International Journal of Computer Science and Network Security,Vol. .9 No.1, January 2009.
10. M. Silva, "Virtual Forensics: Social Network Security Solutions," Proceedings of Student Research Day, CSIS, Pace University, 2009.
11. R. K. Khalil, "A Study of Network Security Systems," IJCSNS International Journal of Computer Science and Network Security, 2010.
12. S. Alabady, "Design and Implementation of a Network Security," Technology, Vol. 1, p. 11, 2009.
13. B. Preneel, "Cryptography for Network Security," Katholieke Universities Leuven and IBBT, 2009.
14. M. Kassim, "An Analysis on Bandwidth Utilization and Traffic Pattern," IACSIT Press, 2011.
15. M. Eian, "Fragility of the Robust Security Network: 80211," Norwegian University of Science and Technology, 2011.

16. D. Acemoglu, “Network Security And Contagion,” NATIONAL BUREAU OF ECONOMIC RESEARCH, 2013.
17. S. Shaji, “Anti Phishing Approach Using Visual Cryptography And Iris Recogn No. 3pp. 88-92, 2014.