International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 12 | Dec 2020 www.irjet.net p-ISSN: 2395-0072

The Advanced Study of Network Security and Threats

Ravindran R

Assistant Professor, Dept. of Computer Science and Engineering, Mount Zion college of Engineering, Kadammanitta, Kerala, India

---

Abstract- Security is a fundamental component in the computing and networking technology. The first and foremost thing of every network designing, planning, building, and operating a network is the importance of a strong security policy. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are different kinds of attack that can be when sent across the network. By knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide and all of these required different security mechanisms. In this paper, we are trying to study most different kinds of attacks along with various different kinds of security mechanism that can be applied according to the need and architecture of the network.

I. INTRODUCTION

Network Security management is different for all kinds of situations and is necessary as the growing use of internet. A home or small office may only require basic security while large businesses may require high- maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. New Threats Demand New Strategies as the network is the door to your organization for both legitimate users and would-be attackers.

For years, IT professionals have built barriers to prevent any unauthorized entry that could compromise the organization's network. And this network security is important for every network designing, planning, building, and operating that consist of strong security policies. The Network Security is constantly evolving, due to traffic growth, usage trends and the ever changing threat landscape.

When considering network security, it must be emphasized mainly that the whole network should be remain secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack, where the chances of threats are more penetrating. A possible hacker could target the communication channel, obtain the data, decrypt it and re- insert a false message. Hence, securing the network is just as important as securing the computers and encrypting the message which we want to be kept private. When developing a secure network, the following need to be considered

1. Accessibility – authorized users are provided the means to communicate to and from a particular network.

2. Confidentiality – Information in the network remains private, discloser should not be easily possible.

3. Authentication – Ensure the users of the network are, the user must be the person who they say they are.

4. Integrity – Ensure the message has not been modified in transit, the content must be same as they are sent.

5. Non-repudiation – Ensure the user does not refute that he used the network.

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack. The steps involved in understanding a secure network,. Typical security currently exists on the computers connected to the network. Security protocols sometimes usually appear as part of a single layer of the OSI network reference model. Current work is being performed in using a layered approach to secure network design. We have given the Trend micro security approach which is based on most then single layer of security. This security approach leads to an effective and efficient design which circumvents some of the common security problems. Computer technology is more and more ubiquitous and the penetration of computer in society is a welcome step towards modernization but society needs to be better equipped to grapple with challenges associated with technology. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered create difficulty for the security professionals in order to catch hackers.

II. TYPES OF ATTACKS

Networks are subject to attacks from malicious sources. And with the advent and increasing use of internet attach is most commonly growing on increasing. The main categories of Attacks can be from two categories: "Passive"

when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation. A system must be able to limit damage and recover rapidly when attacks occur. There are some more types of attack that are also essential to be considered:

A. Passive Attack A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. It includes traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

B. Active Attack In an active attack, the attacker tries to bypass or break into secured systems in the going on communication. 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. The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. 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.

C. 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.

D. Insider Attack According to a Cyber Security Watch survey insiders were found to be the cause in 21 percent of security breaches, and a further 21 percent may have been due to the actions of insiders. More than half of respondents to another recent survey said it's more difficult today to detect and prevent insider attacks than it was in 2011, and 53 percent were increasing their security budgets in response to insider threats, while a significant number of breaches are caused by malicious or disgruntled employees - or former employees - many are caused by well- meaning employees who are simply trying to do their job.

E. 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. 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.

F. Spyware attack A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. And this capture information is maliciously used as the legitimate user for that particular kind of work.

G. 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.

H. Hijack Attack In a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accidently.

I. Spoof Attack In the spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

J. Password Attack An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords [9]. A brute-force attack is when the attacker tries every possible combination of characters

K. Buffer Overflow A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

L. Exploit Attack In this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.

III. TECHNOLOGIES FOR PROVIDING SECURITY TO THE NETWORK

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defence and detection mechanisms were developed to deal with attacks mentioned earlier. Some of these mechanism along with advance concepts are mention in this section.

A. Cryptographic Systems Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

B. Firewall The firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defence mechanism against intruders to enter in the system. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. The most widely sold solution to the problems of Internet security is the firewall. This is a machine that stands between a local network and the Internet, and filters out traffic that might be harmful. The idea of a ―solution in a box‖ has great appeal to many organizations, and is now so widely accepted that it's seen as an essential part of corporate due diligence. Firewalls come in basically three flavours, depending on whether they filter at the IP packet level, at the TCP session level, or at the application level.

C. Driving Security to the Hardware Level To further optimize performance and increase security, Intel develop platforms also include several complementary security technologies built into multiple platform components, including the processor, chipset, and network interface controllers (NICs). These technologies provide low-level building blocks upon which a secure and high performing network infrastructure can be sustained. These technologies include Virtualization Technology, Trusted Execution Technology and Quick Assist Technology.

D. Intrusion Detection Systems An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. The typical antivirus software product is an example of an intrusion detection system. The systems used to detect bad things happening are referred to generically as intrusion detection systems. Intrusion detection in corporate and government networks is a fast-growing field of security research; this growth has been prompted by the realization that many systems make no effective use of log and audit data.

E. Anti - Malware Software and Scanners Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.

F. Secure Socket Layer (SSL) The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.

G. Dynamic Endpoint Modelling Observable's Security Solution, represents a profoundly new way to look at IT security. It models each device on your network, so you can understand normal behaviour and quickly take action when a device starts acting abnormally. There's no need to install agents on the devices, or attempt to use deep-packet inspection, giving you a powerful solution to overcome these new security challenges.

H. Mobile Biometrics Biometrics on mobile devices will play a bigger role in authenticating users to network services, one security executive predicted. Biometrics emerging on mobile endpoints, either as applications that gather users' behaviours or as dedicated features on mobile endpoints that scan personal features.

IV. CONCLUSION

Security is a very difficult and vital important topic. Everyone has a different idea regarding security' policies, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. 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 but Users who find security policies and systems too restrictive will find ways around them. There are different kinds of attacks on the security policies and also growing with the advancement and the growing use of internet. In this paper we are trying to study these different kinds of attacks that penetrates our system. As the threats are increasing, so for secure use of our systems and internet there are various different security policies are also developing.

REFERENCES

[1] Security Engineering, A Guide to building dependable distributed systems, Ross anderson

[2] A White Paper, ―Securing the Intelligent Network‖, powered by Intel corporation.

[3]Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.

[4] ―Network Security: History, Importance, and Future‖, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.

[5]TCP/IP Protocol Suit, Behrouz A Forouazan, Tata Mc Graw Hill Edition

[6]Cryptograbhy and Network c security, William stalling.