Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.728 – 735

RESEARCH ARTICLE

The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms

Monali S. Gaigole
Student of Master of Engineering in (CSE)
Dr. Saw. Kamaltai Gawai College of Engineering and Technology
Amravati, India
monaligaigolecmps@gmail.com

Prof. M. A. Kalyankar
Assistant professor in the Department of (CSE)
Dr. Saw. Kamaltai Gawai College of Engineering and Technology
Amravati, India
meghalikalyankar.kgiet@gmail.com

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.

Keywords: Network Security, attacks, hackers, Cloud-environment security, zero-trust model (ZTM), Trend Micro internet security.

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 [1]. 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 [3]. For example, the widespread adoption of cloud computing, social networking and bring-your-own-device (BYOD) programs are introducing new challenges and threats to an already complex network.

According to the UK Government, Information security is: "the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so" (Source: UK Online for Business). Information systems need to be secure if they are to be reliable. Since many businesses are critically reliant on their information systems for key business processes (e.g. websites, production scheduling, transaction processing), security can be seen to be a very important area for management to get right.
The vast topic of network security is analyzed by researching the following:

- History of security in networks
- Internet architecture and vulnerable security aspects of the Internet
- Types of internet attacks and security methods
- Security for networks with internet access
- Current development in network security hardware and software

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]:
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.

As an example, Figure 1 [2] shows a typical security implementation designed to protect and connect multiple parts of a corporate network. This is the most common design as according to the area of the network.

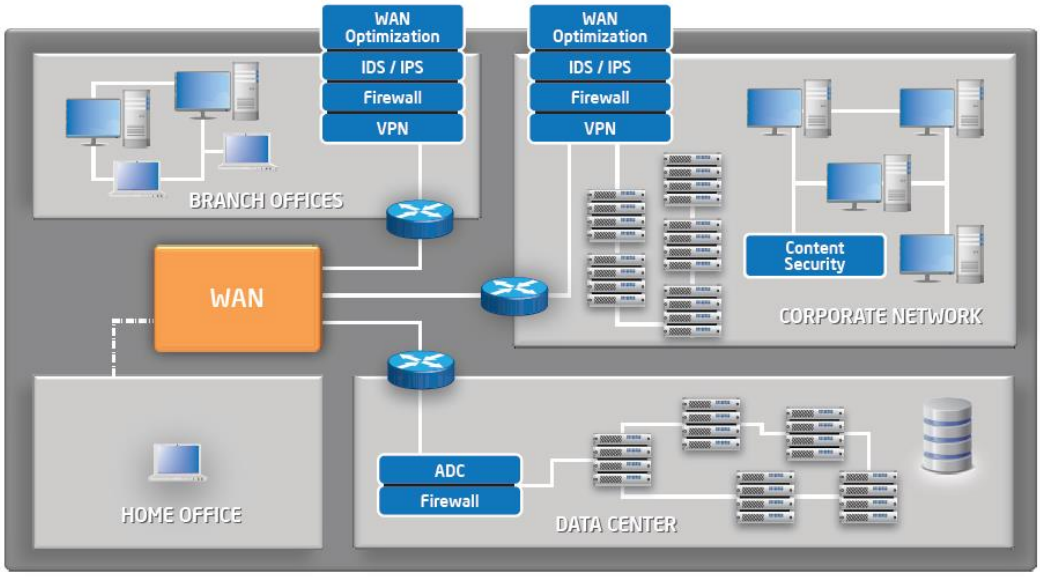

Figure1. Security present in the different kinds of the Network.

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 [1]. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor. 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. The difficulties of staying up to date with security issues within the realm of IT education are due to the lack of current information. The recent research is focused on bringing quality security training combined with rapidly changing technology [4]. Online networking security is to provide a solid understanding of the main issues related to security in modern networked computer systems [5]. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures.

In this paper, we are briefly elaborating the concept of Network Security, how it can be done in the past. And with the advent and increasing use of internet how security threats are penetrating to our devices is also studied. We have mention most of all types of attack that are mostly happened on the any network including home, office and organizations. In the last section, we are studying various security mechanisms that are important to keep our network secure. In this section we are covering most of the modern concept that are suitable for providing security, needed for today's hacking and possible attacks.

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 [6]. 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 [7]. 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. BYOD programs and file sharing and collaboration services like Dropbox mean that it will be harder than ever to keep corporate data under corporate control in the face of these well-meaning but irresponsible employees.

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 defense 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 defense. 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 defense 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 [9]. 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 flavors, 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 Modeling

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 behavior 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' behaviors or as dedicated features on mobile endpoints that scan personal features. For example, the iPhone 5s finger scan, will emerge in 2014, if these features are open and extensible, it could lead to real innovation in ensuring the identities of remote users.

IV. SOME ADVANCE NETWORK SECURITY POLICIES

A. Making Security in Clouds Environment

Analysts project that IT spending will increase slightly from 2013. This increase in investment is largely attributed to cloud computing [10]. Over half of IT organizations plan to increase their spending on cloud computing to improve flexible and efficient use of their IT resources. Intel Trusted Execution Technology (Intel TXT) is specifically designed to harden platforms against hypervisor, firmware, BIOS, and system level attacks in virtual and cloud environments. It does so by providing a mechanism that enforces integrity checks on these pieces of software at launch time. This ensures the software has not been altered from its known state. This TXT also provides the platform level trust information that higher level security applications require to enforce role-based security policies. Intel TXT enforces control through measurement, memory locking and sealing secrets.

B. Zero-Trust Segmentation Adoption

This model was initially developed by John Kindervag of Forrester Research and popularized as a necessary evolution of traditional overlay security models. One alternative that is a strong candidate to improve the security situation is the zero-trust model (ZTM). This aggressive approach to network security monitors every piece of data possible, under the assumption that every file is a potential threat [11]. It requires that all resources be accessed in a secure manner, that access control be on a need-to-know basis and strictly enforced. The systems verify and never trust; that all traffic be inspected, logged, and reviewed and that systems be designed from the inside out instead of the outside in. It simplifies how information security is conceptualized by assuming there are no longer "trusted" interfaces, applications, traffic, networks or users. It takes the old model "trust but verify" and inverts it, because recent breaches have proved that when an organization trusts, it doesn't verify.

C. Trend Micro Threat Management Services

Because conventional security solutions no longer adequately protect against the evolving set of multilayered threats, users need a new approach. Trend Micro delivers that approach with the Trend Micro Smart Protection Network [12]. The Smart Protection Network infrastructure provides innovative, real-time protection from the cloud, blocking threats before they reach a user's PC or a company's network. Leveraged across Trend Micro's solutions and services, the Smart Protection Network combines unique Internet-based, or "in-the-cloud," technologies with lighter-weight clients. By checking URLs, emails, and files against continuously updated and correlated threat databases in the cloud, customers always have immediate access to the latest protection wherever they connect—from home, within the company network, or on the go.

Trend Micro's Threat Management Services provides a comprehensive view of the activities occurring in the network. The solution evaluation offers a unique network security assessment that provides organizations with tangible details on the value of adding an over watch security layer for a current defense-in-depth strategy [13]. The over watch security layer can uncover when a breach has occurred and, more importantly, immediately take action to intercept it and remediate it to ensure that it doesn't happen again. Threat Management Services offers an approach to network security that assesses risk and provides insight on potential gaps within the current security environment.

The Smart Protection Network is composed of a global network of threat intelligence technologies and sensors that deliver comprehensive protection against all types of threats— malicious files, spam, phishing, web threats, denial of service attacks, web vulnerabilities, and even data loss. By incorporating in-the-cloud reputation and patent-pending correlation technologies, the Smart Protection Network reduces reliance on conventional pattern file downloads and eliminates the delays commonly associated with desktop updates. Businesses benefit from increased network bandwidth, reduced processing power, and associated cost savings.

D. Advanced Threat Protection with Big Data

Big Data makes big sense for security as it involves using specialized technologies and techniques to collect, coordinate, store, and analyze truly massive amounts of related and perhaps even disparate data to uncover insights and patterns that would otherwise remain obscured. Leveraging Big Data for information security purposes not only makes sense but is necessary [14]. Big Data analytics can be leveraged to improve information security and situational awareness. For example, Big Data analytics can be employed to analyze financial transactions, log files, and network traffic to identify anomalies and suspicious activities, and to correlate multiple sources of information into a coherent view.

Data-driven information security dates back to bank fraud detection and anomaly-based intrusion detection systems. Fraud detection is one of the most visible uses for Big Data analytics. Credit card companies have conducted fraud detection for decades. However, the custom-built infrastructure to mine Big Data for fraud detection was not economical to adapt for other fraud detection uses. Off-the-shelf Big Data tools and techniques are now bringing attention to analytics for fraud detection in healthcare, insurance, and other fields.

V. 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. In this paper we have mention some of the security policies that can be used mostly by number of users and some new advance qualities that fits to the todays more penetrating environments like Trend micro security mechanism, use of big data qualities in providing security, etc. Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will it be achievable.

REFERENCES

[1] Predictions and Trends for Information, Computer and Network Security [Online] available: http://www.sans.edu/research/security-laboratory/article/2140

[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] Ateeq Ahmad, "Type of Security Threats and its Prevention**",** Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.

[6] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257

[7] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", *(IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.*

[8] Network Security Types of attacks [Online] available: http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html.

[9] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, vol., no., pp.77-82, 13-15 May 2008.

[10] Securing the Intelligent Network [Online] available: http://www.trendmicro.co.in/cloud-content/us/pdfs/security-intelligence/white-papers/wp_idc_network-overwatch-layer_threat-mngmt.pdf

[11] Network security needs big data [Online] available: http://www.computerworld.com/article/2851517/network-security-needs-big-data.html.

[12]Trend Micro™ Smart Protection Network™ Security Made Smarter [Online] available: http://la.trendmicro.com/media/wp/smart-protection-network-whitepaper-en.pdf.

[13] Charles J. Kolodgy Christian A. Christiansen, "Network Security Over watch Layer: Smarter Protection for the Enterprise", Sponsored by: Trend Micro, November 2009.

[14] CLOUD SECURITY ALLIANCE Big Data Analytics for Security Intelligence [Online] available: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf

