Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

An Analysis of Network Protection with Its Infiltration Attacks and Potential Defense Mechanisms

Mr. Arifuddin Syed[1], Dr. M. A. Kalyankar[2]

[1]Research Scholar, Rayalaseema University, Kurnool – 518007, Andhra Pradesh, India.
[2]Associate Professor, Rayalaseema University, Kurnool – 518007, Andhra Pradesh, India.

Abstract

Cyberattacks are becoming more frequent and sophisticated in the current digital era, network security has become a major problem. A thorough examination of network security systems is provided in this study, with an emphasis on frequent infiltration attacks and the defense strategies used to thwart them. In order to obtain unauthorized access, interfere with operations, or jeopardize data integrity, infiltration assaults—which include malware injection, phishing, man-in-the-middle attacks, and denial-of-service (DoS) attacks—take advantage of flaws in network infrastructures. In addition to evaluating current security solutions like firewalls, intrusion detection and prevention systems (IDPS), encryption methods, and multi-layered defense strategies, the study investigates different kinds of attack vectors and categorizes them according to their threat levels. The report also outlines the latest developments, difficulties, and opportunities in protecting networks from ever changing cyberthreats. The results are intended to give researchers, IT specialists, and enterprises looking to improve their cybersecurity frameworks some useful information.

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

INTRODUCTION

As internet usage increases, network security management is required in a variety of scenarios. While a house or small office would just need basic protection, major enterprises might need sophisticated hardware and high-maintenance software to fend off spam and hacking assaults. Since the network serves as the entryway to your company for both authorized users and malicious actors, new threats necessitate new approaches.

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.

"The practice of ensuring that information is only read, heard, changed, broadcast, and otherwise used by people who have the right to do so" is what the UK government defines as information security (Source: UK Online for Business). For information systems to be dependable, they must be secure. Security can be viewed as a crucial issue for management to get right because many firms depend heavily on their information systems for essential company operations (such as websites, production scheduling, and transaction processing).The following topics are investigated in order to assess the broad subject of network security:

- The history of network security
- The architecture of the Internet and its weak points
- Security for networks with internet connectivity;
- Types of online assaults and security techniques;
- Current advancements in network security software and hardware

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.

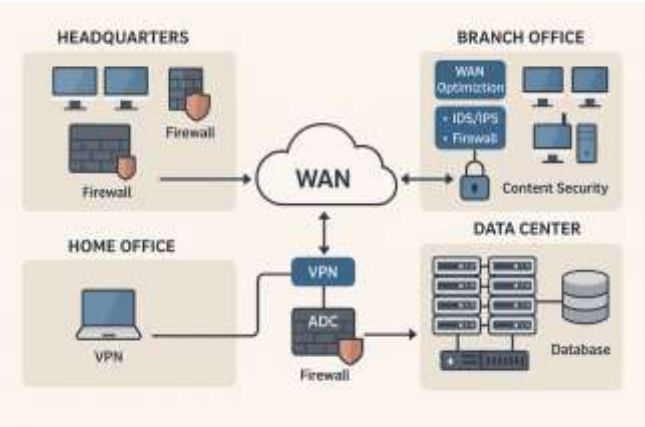

Figure1. Security present in the different kinds of the Network.

Understanding security concerns, possible attackers, the required level of protection, and the elements that make a network susceptible to attack helps create an efficient network security plan [1]. This study project follows the procedures necessary to comprehend the structure of a secure network, whether it be the internet or anything else. There is now standard security on the networked computers. In the OSI network reference model, security protocols often appear as a single layer. Currently, a layered approach to secure network design is being used. The Trend micro security strategy, which is based on a single layer of security, is what we have provided.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.

TYPES OF ATTACKS

Malicious actors can launch attacks on networks. Additionally, the use of the internet is generally growing as a result of its introduction. Attacks fall into two basic categories: "Passive" attacks, in which a network intruder intercepts data as it passes through the network, and "Active" attacks, in which the intruder issues commands to interfere with the network's regular operations [6]. When attacks happen, a system needs to be able to quickly recover and limit damage. Other attack kinds that must also be taken into account are as follows:

A. Passive Assault

In order to find sensitive data and clear-text passwords that can be utilized in other kinds of attacks, a passive attack watches unencrypted traffic. Passive attacks occur when unauthorized intruders listen in on and observe the communication channel. Traffic analysis, unprotected communication monitoring, decrypting poorly encrypted traffic, and password and authentication information capture are all included. Adversaries are able to predict future activities through passive interception of network processes. Information or data files are revealed to an attacker using passive attacks without the user's knowledge or agreement.

A. 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.

B. 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.

C. 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.

D. An attack by spyware

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.

E.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.

F. 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.

G. 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.

H. 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

I. 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.

III. TECHNOLOGIES TO GIVE THE NETWORK SECURITY

As long as information can be accessed and shared over the Internet, internet risks will remain a significant problem in the worldwide community. To counter the aforementioned attacks, various defensive and detection systems were created. This section describes a few of these mechanisms as well as advanced notions.

A. Systems of cryptology

Nowadays, cryptography is a practical and popular technology in security engineering. It entailed converting information into incomprehensible data using codes and ciphers.

A. 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.

B. 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.

C. 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.

D. *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.

E. 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.

F. 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.

SOME ADVANCE NETWORK SECURITY POLICIES

A. Establishing Security in a Cloud Setting

According to analysts, IT expenditures would marginally rise from 2013. Cloud computing is largely responsible for this rise in investment [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.

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.

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. **"Network Security Essentials: Applications and Standards"**
   Author: William Stallings
   - A foundational book covering key concepts of network security, cryptography, and threat defense.
2. **"Computer Security: Principles and Practice"**
   Authors: William Stallings and Lawrie Brown
   - In-depth coverage of system security, threats, and practical mitigation techniques.
3. **"Cryptography and Network Security: Principles and Practice"**
   Author: William Stallings
   - A classic text on cryptographic techniques and how they apply to network protection.
4. **"Network Security: Private Communication in a Public World"**
   Authors: Charlie Kaufman, Radia Perlman, Mike Speciner
   - Detailed insight into secure network communication, authentication, and attack resistance.
5. **"Cybersecurity and Cyberwar: What Everyone Needs to Know"**
   Authors: P.W. Singer and Allan Friedman
   - Offers context and explanation of cybersecurity challenges, threats, and policies.
6. **"The Web Application Hacker's Handbook"**
   Authors: Dafydd Stuttard and Marcus Pinto
   - Practical exploration of web-based attack techniques and how to defend against them.
7. **"Hacking: The Art of Exploitation"**
   Author: Jon Erickson
   - Covers low-level network and software vulnerabilities with a focus on how attacks are performed.
8. **"The Hacker Playbook 3: Practical Guide To Penetration Testing"**
   Author: Peter Kim
   - A hands-on guide to modern hacking methods, attack simulations, and testing defenses.
9. **"Security+ Guide to Network Security Fundamentals"**
   Author: Mark Ciampa
   - Aligned with CompTIA certification, this book provides beginner-to-intermediate level coverage of network security concepts.
10. **"Network Security and Cryptography"**
    Author: Bernard Menezes
    - Focuses on the integration of cryptographic tools with network protection principles.
11. **"Zero Trust Networks: Building Secure Systems in Untrusted Networks"**
    Authors: Evan Gilman and Doug Barth
    - A must-read on implementing the Zero Trust Model (ZTM) in modern networks.
12. **"Cloud Security and Privacy"**
    Authors: Tim Mather, Subra Kumaraswamy, Shahed Latif