NETWORK SECURITY ESSENTIALS: UNDERSTANDING ITS KEY ATTACKS AND POTENTIAL SECURITY MECHANISM

Vikay Kumar Sharma[1], Sanju Saini[2], Vikram Prajapat [3]
[1]Assistant professor,[2,3]Research scholar
[1,2,3]Department of computer science
Arya College of Engineering, Jaipur, Rajasthan

Abstract- In computing and networking technology, security is a crucial element. The importance of a strong security policy should be the first and foremost consideration for any network being designed, planned, built, and operated. Users of personal computers, businesses, and the military now place a higher priority on network security. Security has grown to be a major concern since the internet's inception. Numerous security threats were made possible by the structure of the internet itself. Due to the ease with which intellectual property can be obtained via the internet, network security is becoming increasingly crucial. There are numerous attack types that can be transmitted over a network. Knowing the attack strategies enables the development of the right security. In order to protect themselves from the internet, many businesses use 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, Trend Micro internet security.

1. Introduction

Network Security management is different for all kinds of situations and is necessary as the growing use of internet. While large businesses may need high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming, a home or small office may only need basic security. [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.
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 remaining 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 developing a secure network, the following need to be considered:

- Accessibility – authorized users are provided the means to communicate to and from a particular network.
- Confidentiality – Information in the network remains private, discloser should not be easily possible.
- Authentication – Ensure the users of the network are, the user must be the person who they say they are.
- Integrity – Ensure the message has not been modified in transit, the content must be same as they are sent.
- Non□repudiation – Ensure the user does not refute that he used the network.

2. **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:

1. 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.
2. 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 attacker's monitors, listens to and modifies the data stream in the communication channel are known as active attack.

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.
4. 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. BYOD programs and file sharing and collaboration services like Drop box 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.

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. 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.
6. 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.

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.

1. 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.
2. 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

3. 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.
4. 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.

3. 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 mechanisms along with advance concepts are mention in this section.

1. 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.
2. 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.
3. Driving Security to the Hardware Level- To further optimize performance and increase security, Intel develops 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.
4. Intrusion Detection Systems- An additional defense mechanism that aids in preventing computer intrusions is an intrusion detection system (IDS). IDS systems are hardware and software tools that can be used to find an attack. IDS tools are used to keep an eye on connections and check for active attacks. Others attempt to stop the attack, while some IDS systems simply monitor and alert of an attack. An example of an intrusion detection system is the typical antivirus software package. Intrusion detection systems are a general term for the devices that are used to spot bad things before they happen. The realization that many systems do not effectively use log and audit data has sparked a rapid growth in the field of intrusion detection in corporate and governmental networks.
5. 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. Secure Socket Layer (SSL). 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.

6. 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. 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.

4. **Some Advance Network Security Policies**

1. 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.
2. Zero-Trust Segmentation Adoption-This model was initially developed by John Kundera 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). 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.
3. 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.

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 made up of a global network of threat intelligence technologies and sensors that provide thorough protection against all types of threats, including data loss and malicious files, spam, phishing, and web threats. The Smart Protection Network lessens reliance on conventional security measures by integrating in-the-cloud reputation and patent-pending correlation technologies.

5. CONCLUSION

A very challenging and crucially important subject is security. Everyone has a different understanding of security procedures and acceptable levels of risk. Establishing what security means in relation to your current needs and usage is essential to creating a secure network. Once that has been established, the entire network's activity can be assessed in light of that policy. Users who find security policies and systems to be too restrictive will find ways around them, so it's important to build systems and networks so that the user is not constantly reminded of the security system around him.

There are different kinds of attacks on the security policies and also growing with the advancement and the growing use of internet. In this essay, we're attempting to investigate the various attacks that can infiltrate our system. As the threats grow, so do the security policies that are being developed to ensure the safe use of our systems and the internet. In this paper, we discuss a few security measures that a large number of users can take advantage of as well as some modern advancements that are appropriate for the more intrusive environments of today, such as the security features of Trend Micro and the use of big data for security. Security is everyone's concern, and it can only be achieved with everyone working together, a wise policy, and consistent practices.

REFERENCES

1. Stallings, W. (2020). Network security essentials: Applications and standards (6th ed.). Pearson.

2. Bishop, M. (2018). Computer security: Art and science (2nd ed.). Addison-Wesley.

3. Kizza, J. M. (2020). Guide to computer network security (5th ed.). Springer.

4. Schneier, B. (2015). Applied cryptography: Protocols, algorithms, and source code in C (20th anniversary ed.). Wiley.

5. Whitman, M. E., & Mattord, H. J. (2019). Principles of information security (6th ed.). Cengage Learning.

6. Kaufman, C., Perlman, R., & Speciner, M. (2021). Network security: Private communication in a public world (3rd ed.). Pearson.

7. Amoroso, E. (2012). Cyber attacks: Protecting national infrastructure. Elsevier.

8. Grimes, R. A. (2017). Hacking the hacker: Learn from the experts who take down hackers. Wiley.

9. Andress, J. (2021). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice (3rd ed.). Syngress.

10. Shoniregun, C. A., & Crosier, B. (2008). Cybersecurity for critical infrastructures. Springer.

11. Northcutt, S., & Novak, J. (2002). Network intrusion detection (3rd ed.). New Riders.

12. Vacca, J. R. (2014). Computer and information security handbook (2nd ed.). Elsevier.