IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

A Network Security Review

Pratik G. Dhange, Ashwini A. Patil, Gaurav V. Barde, Dhanshree S.Joshi
Department of Computer Engineering, Late G. N. Sapkal College of Engineering, Nashik, India

Abstract: *The introduction of the Worldwide Organizations worldwide have benefited from the Web and the rise of e-commerce applications and social networks. generate a lot of data every day. The most important factor in guaranteeing secure online information transfer is data security. Network professionals are becoming more and more interested in computer network security as businesses spend more time and money securing their sensitive data. The importance of network security challenges is also growing as society transitions to the digital information era. Any network, whether it is for a school, college, university, the government, or the military, must prioritise network security. With the development of networking technology, protecting the network from knowledgeable hackers and attackers has become a very difficult task. Saving your network is a major concern. Therefore, it is crucial to comprehend the various risks that might affect any network, as well as the origins of those threats and the solutions to them, which are discussed below.*

Keywords: Introduction, Needs of Network Security, CIA Triad, Problems, Countermeasures, Conclusion.

I. INTRODUCTION

The internet is becoming more and more popular; if a stranger is able to access it, he or she can quickly ruin our life in addition to spying on us. Network security is a concept used to safeguard wireless networks and data transmission. A network security system often uses layers of security and has many different parts, such as hardware, appliances, networking monitoring and security software. Each element contributes to the overall security of the computer network. Data security can be achieved via a method known as cryptography. Thus, it may be said that A developing technology that is crucial for network security is cryptography. The measures and regulations a network administrator adopt to prevent and keep track of unauthorised access, misuse, modification, and denial of a computer network and network-accessible resources are known as network security.

The science of writing in secret code is known as cryptography. Modern cryptography is primarily concerned with building and analysing protocols that thwart adversaries; it also addresses other areas of information security like data secrecy, data integrity, authentication, and non-repudiation. Among the uses for cryptography are electronic commerce, computer passwords, and ATM cards. The growth of the World Wide Web led to the widespread usage of cryptography in business and e-commerce applications.

II. NEEDS OF NETWORK SECURITY

In the past, hackers were knowledgeable programmers who were familiar with computer systems and their weaknesses. Anyone today can become a hacker by obtaining some open-source attack tools from the internet.

Three primary goals underpin network security:

1. **Availability:** Data must always be made available to authorised users as needed. It is the server's responsibility to maintain its data using specific tools and approaches so that end users can access it. Data can be made accessible by routine backup and redundancy procedures. The process of granting authorised users access to private material is known as confidentiality.
2. **Confidentiality:** For instance, when conducting bank transactions, only you and the approved user of the bank should save your record; everyone else should not. Failure to do so resulted in data theft and leakage.
3. **Data Integrity:** If data hasn't been changed or updated, data integrity is maintained. For instance, when a user requests to visit a website and a malicious attacker sends them to another website, or when the price of an e-commerce site is changed.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

Figure 1

III. PROBLEMS

Given how frequently people access and transfer information via the internet. It comes with a number of hazards, and the network administrator is responsible for shielding the websites' data from these nefarious intruders.

Attacks fall into two categories:
a)Active Attacks
b)Passive Attacks

1. Passive Attacks:

Figure 2: Passive Attacks

Attacks of this nature also involve communication observation or monitoring. A passive assault does not deplete system resources; instead, it tries to gather or use information from the system. The adversary wants to obtain the information being transferred.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

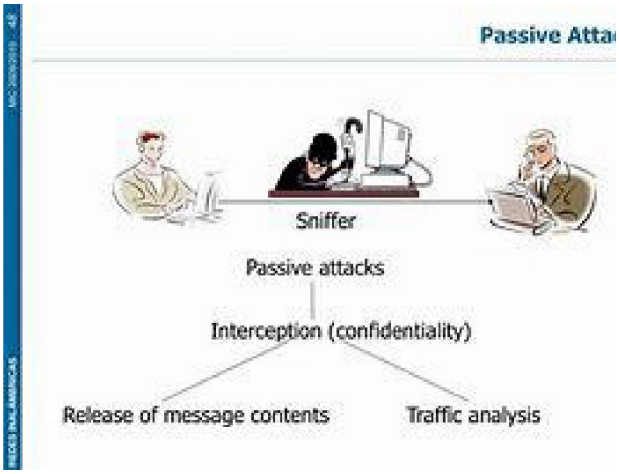

Figure 3: Types Of passive Attacks

Varieties of passive assaults:

- Traffic analysis: The message traffic appears to be sent and received normally, neither the sender nor the recipient is aware that anyone else has read their communications or seen their traffic.
- Release of Message Contents: Read the message's contents from the sender to the recipient.

2. Active Attacks:

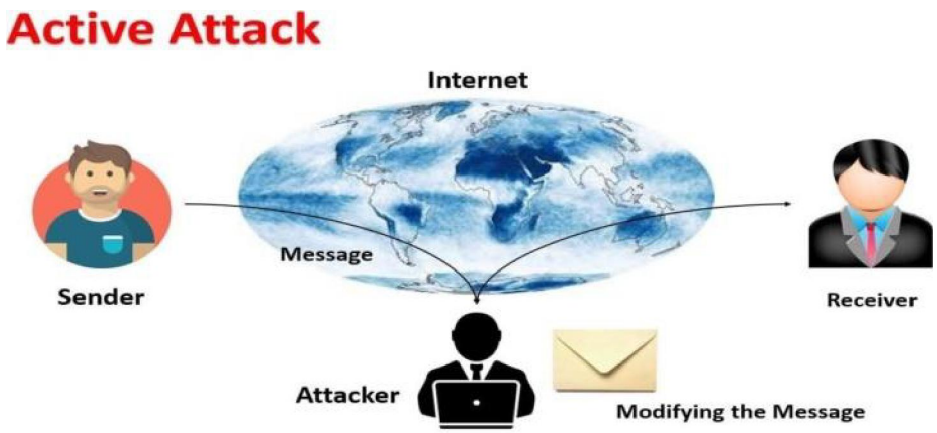

Figure 4:Active Attacks

An active assault tries to change system resources or interfere with their functionality. It requires changing the data stream in some way or making a bogus stream.

Active attack types include the following:

- **Modification of Messages:** A section of a genuine communication is changed, or messages are delayed or rearranged.
- **Denial of Service:** A party has the option to block all messages going to a specific location.
- **Replay:** This technique entails passively capturing a data unit and retransmitting it to create an unauthorized effect.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

IV. COUNTERMEASURES

To stop security-related dangers, network service providers now have a difficult responsibility to complete: network security. Today, we rely entirely on networks or are surrounded by the internet to make our daily tasks easier. However, this presents a problem for businesses because any remote computer that isn't authorised to access those resources can access the information on their network. If there is an attack, we have a countermeasure for it. For instance, if someone is attempting to locate a passage through the network, we must take some kind of action.

1. **Access Management:**It is a technique for safeguarding the network by giving authorised users permission to access it. This will secure the network by preventing any authorised attacks on it. Certain policies that are outlined in information security management are used in this procedure. This procedure was included to protect the private data being exchanged across the network.

2. **Wireless Security:** Utilising the wireless network, Wireless Security guards against computer intrusion and unauthorised access. The two most popular wireless security protocols are WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) Compared to WPA, WEP is less secure since its password is more easily crackable with certain software tools. Wireless communication has some security concerns. Ad hoc networks, unconventional networks, network injection, and caffe latte attacks are all methods that a bad person can use to attack a network. Static IP addresses, encryption, 802.11 security, SSID concealment, and other security measures are only a few examples.

3. **Firewall:** The topic of firewall has already covered. It controls network traffic and serves as a safety precaution for network communication:

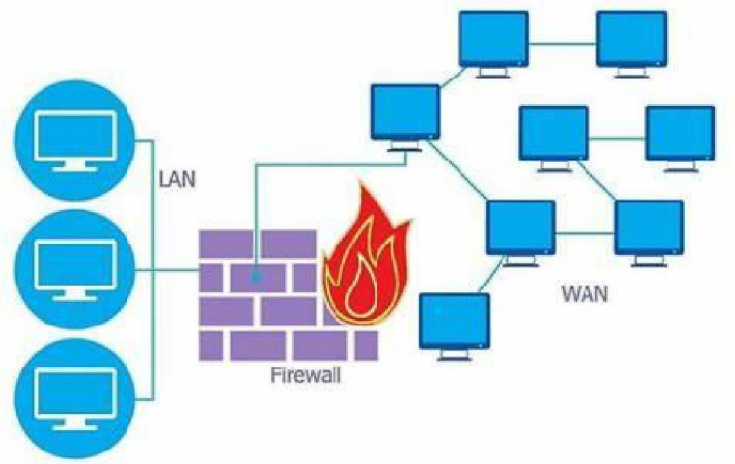

Figure 5: Firewall

4. **Endpoint Security:**Another strategy for network security that secures distant networks is endpoint security. Devices in this adhere to a set of security criteria. It controls how the user accesses the company network. The operating system, an antivirus programme, and a VPN (Virtual Private Network) are the three major elements of this sort of protection. This security management approach uses a client-server architecture. Another concept applied here is "Software as a Service."

5. **Honeypot:**Another security measure for network security is the honeypot. It recognises, prevents, and mitigates the usage of information systems without authorization. It consists of data that is isolated and tracked but seems to be a component of the website. Production honeypots and research honeypots are the two categories into which honeypots are divided. Research honeypots gather data about the black hat communities attempting to attack the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

network, whereas production honeypots are simple to operate and simply take limited data. Honeypots can be categorised as pure honeypots, low-interaction honeypots, or high-interaction honeypots based on their design.

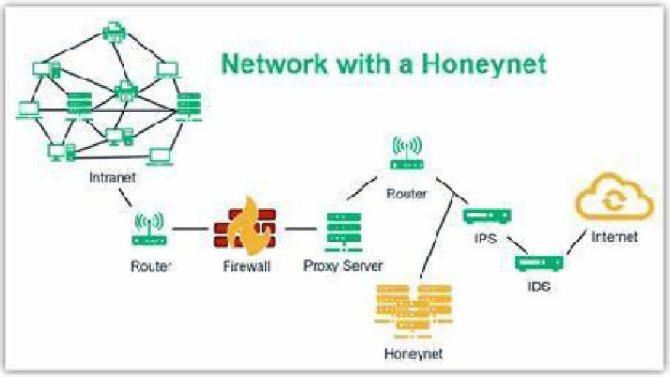

Figure 6: Honeypot

6. **Hole Punching:** It is a method of computer networking that creates a direct link between the two parties by means of network address translation (NAT). In this case, one party or both parties may be protected by a firewall. Each client establishes a connection with a third-party server that is free to temporarily store both internal and external address and port information in order to punch a hole. The information from each client is transmitted to the other through a server, and a direct connection is made utilising that information. As a result, packets are sent from one side to the other.
7. **Malware Detection:** A malware is a piece of software code created specifically to harm a computer network. Malware code can take the shape of spyware, Trojan horses, worms, viruses, or other threats. Finding and eradicating all malicious code from the network is the goal of malware detection. Malware in the network can be found using antivirus software, firewalls, and other similar techniques.
8. **Information Security:** is the term for a collection of tactics used to thwart threats to both digital and non-digital information. It is a fascinating topic for network security as well. The tactics used are centred on the CIA's enlarged objectives of confidentiality, integrity, and availability. These goals ensure that the information can only be accessed by authorised individuals.

V. CONCLUSION

As the internet grows in popularity, network security is a crucial area that is receiving more attention expands. The internet protocol and security risks were examined to identify the required security technology. Although several widely used pieces of hardware are used, security technology is primarily software-based. The state of network security is not particularly outstanding right now. Initially, it was believed that new security techniques—hardware and softwarewould be actively developed due to the importance of the network security area. It was unexpected to see that the majority of development was occurring in the same technologies that are already in use. Internet users may benefit greatly from the new internet protocol IPv6's inherent security.

Despite significant security concerns, the IPv6 internet protocol appears to. It was unexpected to see that the majority of development was occurring in the same technology currently in use. Internet users may benefit greatly from the new internet protocol IPv6's inherent security. Despite certain security concerns, the IPv6 internet protocol appears to be immune to many of the current common attacks. In the near future, IPv6 and security solutions like firewalls, intrusion detection, and authentication procedures will work well together to protect intellectual property. Unstructured threats, structured threats, external threats, and internal threats are the four main dangers to network security.

REFERENCES

[1] R. Khan, "Network Threats, Attacks and Security Measures: a Review," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 8, pp. 116–120, 2017.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, June 2023

[2] A. Funmilola and A. Oluwafemi, “Review of Computer Network Security System,” Netw. Complex Syst., vol. 5, no. 5, pp. 40–47, 2015.
[3] 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 Al Salqan, Y.Y., "Future trends in Internet security," Distributed Computing Systems, 1997.
[4] Shyam Nandan Kumar, “Technique for Security of Multimedia using Neural Network,” Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014.
[5] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317-323.
[6] Carle E. Landwehr, “Security Issues in Networks with Internet Access”, Member, IEEE.
[7] http://whatis.techtarget.com/definition/Conf identiality-integrityand-availability-CIA
[8] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.
[9] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. “A. Handbook of Applied Cryptography”. ISBN 0-8493-8523-7.