International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Network Security Issues and Protection Against Attacks

Sanchita Kuldeep Jedhe, Nikita Joshi, Aparna Mote
Department of Computer Engineering, Zeal College of Engineering & Research, Pune, Maharashtra, India

Article Info
Volume 9, Issue 2
Page Number : 432-436

Publication Issue :
March-April-2022

Article History
Accepted : 15 March 2022
Published: 30 March 2022

ABSTRACT

Network Security Secure Network has now become a need of any organization. The security threats are increasing day by day and making high speed wired/wireless network and internet services, insecure and unreliable. The need is also induced in to the areas like defence, where secure and authenticated access of resources are the key issues related to information security. The security measures should be designed and provided, first a company should know its need of security on the different levels of the organization and then it should be
implemented for different levels. Security policies should be designed first before its implementation in such a way, so that future
alteration and adoption can be acceptable and easily manageable.

Keyword: - Network security, Concept and Specification, benefits of network security

I. INTRODUCTION

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become “wired”, an increasing number of people need to understand the basics of security in a networked world.
network security is the role of the global network today a brief overview of various attacks on the network. A network attack is an attempt to gain unauthorized access to an organization’s network, with the objective of stealing data or perform other malicious activity.

1.1 Basics Network Security

Network security is vital to maintaining the integrity of your data and the privacy of your organization and employees. It encompasses everything from the most basic practices, such creating strong passwords and fully logging out of community computers, to the most complex, high-level processes that keep networks, devices and their users safe. More and more sensitive information is
stored online and in these various devices, and if an unauthorized user gains access to that data, it could lead to disastrous results.

1.1.1 Importance of Network Security

Network security is the key to keeping that sensitive information safe, and as more private data is stored and shared on vulnerable devices, network security will only grow in importance and necessity.

- While each and every member of your organization can take strides to help keep things

secure, network security has become more complex in recent years. Adequately protecting networks and their connected devices requires comprehensive network training, a thorough understanding of how networks actually work and the skills to put that knowledge into practice. It's crucial for networks to be thoroughly and properly set up, secured and monitored to fully preserve privacy.

- Network security is a smaller subset that falls under the larger umbrella of cybersecurity, and it refers to the practice of preventing unauthorized users from accessing computer networks and their associated devices. It involves physically protecting network servers and devices from external threats, as well as taking steps to secure the digital network. In an age of increasingly sophisticated and frequent counter-attacks, network security matters more now than ever before.

1.2 Network Attacks Methods

Eavesdropping – Interception of communications by an unauthorized party Data Modification –Data altering, reading from unauthorized party Identity Spoofing (IP Address Spoofing) – IP address to be falsely assumed— identity spoofing and the attacker can modify, reroute, or delete your data Password-Based Attacks – By gaining your access rights to a computer and network resources are determined by who you are, that is, your user name and your password Denial-of-Service Attack(DOS) – Prevents normal use of your computer or network by valid users, and it could be used for sending invalid data to application, to flood the computer, block traffic, etc. a simple network attack example to understand the difference between active and passive attack.

1.3 Security Attacks

- Passive Attacks This type of attacks includes attempts to break the system by using observed data. One of the example of the passive attack is plain text attacks, where both plain text and cipher text are already known to the attacker.
- Active Attacks This type of attack requires the attacker to send data to one or both of the parties, or block the data stream in one or both directions

1.4 Need for Network Security

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies. The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks.

1.5 Network Security Tools

- N-map Security Scanner is a free and open source utility for network exploration or security auditing.
- ssus is the best free network vulnerability scanner available.
- Wire shark or Ethereal is an open source network protocol analyser for UNIX and Windows.
- Snort is light-weight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks.
- Net Cat is a simple utility that reads and writes data across TCP or UDP network connections.
- Kismet is a powerful wireless sniffer

1.6 Types of Network Security Protections

Firewall Network Segmentation Access Control Remote Access VPN Zero Trust Network Access (ZTNA) Email Security Data Loss Prevention (DLP) Intrusion Prevention Systems (IPS) Sandboxing

1.6.1 Authentication

One-factor authentication – this is "something a user knows." The most recognized type of one factor authentication method is the password. Two-factor authentication – in addition to the first factor, the second factor is "something a user has." Three-factor authentication – in addition to the previous two factors, the third factor is "something a user is."

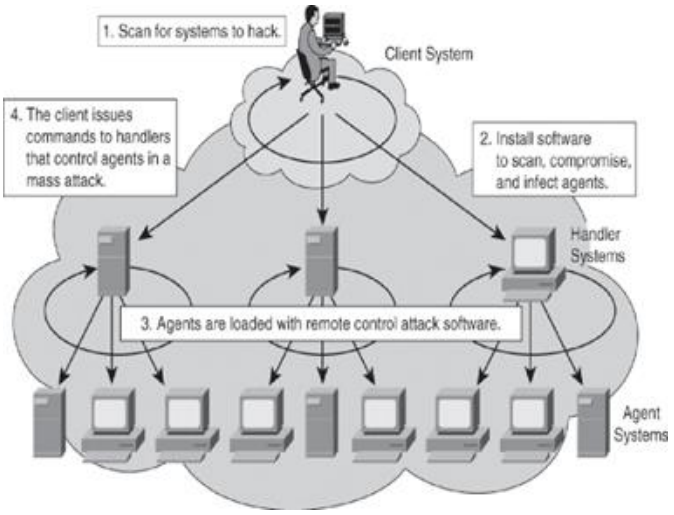
The main objective of authentication is to allow authorized users to access the computer and to deny access to the unauthorized users. Operating Systems generally identifies/authenticates users using following 3 ways: Passwords, Physical identification, and Biometrics. These are explained as following below.

1) Passwords: Passwords verification is the most popular and commonly used authentication technique. A password is a secret text that is supposed to be known only to a user.
2) Physical Identification: This technique include machine readable badges(symbols), card or smart cards. In some companies, badges are required for employees to gain access to the organization's gate. In many system, identification is combined with the use of password i.e the user must insert the card and then supply his /her password. This kind of authentication is commonly used with ATM.
3) Biometrics: This method of authentication is based on the unique biological characteristics of each user such as finger prints, voice or face recognition, signatures and eyes. Biometric devices often consist of – A scanner or other devices to gather the necessary data about user. Software to convert the data into a form that can be compared and stored. A database that stores information for all authorized users.

II. CONCEPT AND SPECIFICATION

Network security starts with authentication, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users.[3] Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS)[4] help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wire shark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account.



III. BENEFITS OF NETWORK SECURITY

- Secure and reliable networks protect not just organizational interests and operations, but also any client or customer who exchanges information with the organization, in addition to

the general public. And if information protection isn't cause enough to invest in network security, consider the cost: according to SolarWinds MSP, the global cost of dealing with damage caused by cybercrime is estimated to reach 6 trillion by 2021, with the average cause of a cyber attack to tiling upwards of 1 million. If this isn't motivation enough, here's a reminder of the top benefits your company stands to gain from improved network security.

1. Builds trust Security for large systems translates to security for everyone. Network security boosts client and consumer confidence, and it protects your business from the reputational and legal fallout of a security breach.
2. Mitigates risk The right network security solution will help your business stay compliant with business and government regulations, and it will minimize the business and financial impact of a breach if it does occur.
3. Protects proprietary information Your clients and customers rely on you to protect their sensitive information. Your business relies on that same protection, too. Network security ensures the protection of information and data shared across the network.
4. Enables a more modern workplace From allowing employees to work securely from any location using VPN to encouraging collaboration with secure network access, network security provides options to enable the future of work.

IV. CONCLUSION

network security is an important field that is increasingly gaining attention as the Internet usage increases. The security threats and Internet protocols were analysed to determine the necessary security technology. However, the current development in network security is not very impressive and significant.

V. FUTURE WORK

The scope of network security consist of two main sub-scopes: users awareness: If you a very sophisticated security system but your employee's are not aware of security risks that might occur because of an action they might do and compromise the whole system. security levels: Includes S/W and H/W security from securing the operating system on each machine alone up to securing the whole network traffic inside and outside the network

VI. APPLICATIONS

Below are the applications of Network Security:

1. Defence Pro: It is a mitigation device that protects the infrastructure against network and application downtime.
2. Defence Flow: Network-wide, multivendor attacks can be detected and mitigated by using Defence Flow.
3. App Wall: To ensure the fast, reliable and secure delivery of critical applications, we use App Wall.
4. Emergency Response Team: Emergency Response Team is used by the companies facing denial of service attacks as it provides twenty-four cross seven security services.
5. Inflight: Inflight is a monitoring application using which all the user transactions are captured from inflight network traffic and real-time intelligence is delivered for business applications.
6. Cloud WAF Service: Web application security is provided by the application and it protects from the evolving threats.
7. Cloud DDOS Protection Service: Enterprise-grade DDOS protection in the cloud is provided by cloud DDOS protection service.
8. Cloud Malware Protection Service: Unknown malware is detected based on their unique behaviour patterns by using patented algorithms on the data collected from a community of two million users and this collected data is analysed to

provide a defence to the organizations against the malware by cloud malware protection service.

VII. REFERENCES

[1]. Jangid, J., & Malhotra, S. (2022). Optimizing software upgrades in optical transport networks: Challenges and best practices. Nanotechnology Perceptions, 18(2), 194–206. https://nano-ntp.com/index.php/nano/article/view/5169

[2].http://www.studymafia.org

[3]. http://www.wikipedia.com