International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 7 ǁ July 2022 ǁ PP. 567-570

Tittle - A Review Paper on different types of attacks in network Security

[1] Sayali.Shinde , [2] B.Mandre , [3] Pankaj.Pardeshi

Sayali.N.Shinde Student of 3rd year btech, Department of Computer Engineering college of ssvps engineering and technology in dhule
Assistant professor , b.R.Mandre ,Department of Computer engineering college of ssvps engineering and technology , Dhule
Assistant Professor , Pankaj.Pardeshi , Department of mechanical engineering college D.Y.Patil engineering and technology , Pimpri
Corresponding Author - Sayali.Nishikant.Shinde

ABSTRACT
In today's world of technology and communication, this knowledge and practice is invaluable. Ordinances, confidential information, files and other confidential information can be compromised if not stored. Like your IT company, all companies should remain the same. With the advancement of new technologies and the security of communications, octaves do not fall. They use specialized installation tools and focus on the weaknesses of most companies. Communication security is important because the military, government, finance, health care, and businesses collect unprecedented data. An important part of this information may be confidential whether financial statements, intellectual property,

Date of Submission: 05-07-2022 Date of acceptance: 19-07-2022

I. INTRODUCTION

A good approach to network security involves a wide range of security features including a secure network, computer, software, or information. Within societies, processes, people, and resources it is necessary to find other ways to find real security in the face of network attacks.

People

Consumers should respect and obey basic security ethics information such as choosing strong passwords, alerting email resources, and storing data. Learn more about basic internet security values.

Process

The government needs to have a blueprint for how they deal with popular cyber-attempts and attacks. Some respectful lines can follow you. It explores how you can identify conflicts, protect organizations, alert and respond to threats, and improve on successful events.

Technology

Technology is needed to provide individuals and organizations the security tools needed to protect against network attacks. Three key elements must be considered: endpoint such as computer, manual and direct device; process; in the cloud. Disposable technologies to protect these devices include state-of-the-art firewalls, DNS crawling, malware protection, anti-virus tools, and email detection.

Definition

It can be defined as a mechanism for reducing security risks to protect against damage, business loss or financial loss to the entire organization. The issue of network security clearly needs to be a safe haven that we recommend that employees who are frequently connected to the internet or network can contact. There are many obstacles and throws to overcome. The most important truth in keeping information is that it is not a one-time process but a continuous process. The owner of the organization must keep the items fresh in the capacity to minimize the risk.

How does network security make working so easy?

There is no doubt work a lot easier, ensuring that limited capital is available in any network. An advertisement or a company can seem like a huge loss if you are not honest about the security of their online presence. In today's interconnected world, everyone is being helped by progressive cyber defense programs. On a separate level, lead to the theft of vital data, similar family photos, from identity theft to attempted extortion. Everyone relies on dangerous structures, such as influential factories, sick businesses and monetary services. The security of these and other societies is essential for us to have confidence in our civilization. On the one hand, the remuneration of the work of cyber threat investigators, similar to ’250-person risk investigators, who discover new and evolving fears and network attack policies. They explore new sensitivities, teach the community about the state of and strengthen open source tools. Their work makes the internet harmless to everyone.

1.Types of Network Attacks
1.1.Denial of Services Attack –
A denial-of-service attack is a type of attack that may take advantage of a problem identified in the use of a particular application or system, or may attack features or vulnerabilities in certain services.
With this attack, the attacker tries to deny access to users the ability to submit information on the computer orthe network itself.
The purpose of this attack may be simply to block access to the program's use, or the attacker may be used in connection with his actions to gain unauthorized access to a computer or network.

1.2.Active and Passive Attack –
Active attack : In an active attack, the content of the original message is somewhat enhanced. These attacks cannot be easily prevented.

- Interruption – I when an unauthorized user pretends to be another user.
- Modification – it contains replay attack and Alteration .A user captures a sequence of event and re-send it. Alteration involves some modification changes to the original message.

Passive Attack- This is a passive attack, in which the attacker intends to receive information on the go. In a random attack, the attack does not involve any changes to the content of the original message. So it is difficult to detect an attack on the skin.

- Release of message content - means a confidential message should be accessed by authorized user otherwise a message is released against our wishes
- Traffic analysis – is a passive attacker may try to find out similarities between encodes message for some clues regarding communication and this analysis is known as traffic analysis.

1.3. Man in the Middle –

- A man-in-the-middle attack, generally occurs when attackers are able to place themselves in the middle of two other hosts that are communicating in order to view and/or modify the traffic
- This will do by making sure that all communication going to or from the target host is routed through the attacker’s host.
- Then the attacker can be able to observe all traffic before transmitting it and can actually modify or block traffic. To the target host, communication is occurring normally, since all expected replies are received
- If the communication is encrypted then the amount of information that can be obtained in a man-in-the-middle attack.

1.4. Replay –

- A replay attack is an where the attacker captures a portion of a communication between two parties and transmits is after some time.
- Example, an attacker might replay a series of commands and codes used in a financial transaction in order to cause the transaction to be conducted multiple times.
- Normally replay attacks are associated with attempts to avoid authentication mechanism, like as the capturing and reuse of a certificate or ticket.
- The best way to prevent replay attacks is with encryption, cryptographic authentication, and time stamps.

1.5. Phishing –
Phishing involves server-like fake messages that look like emails from trusted sources. The goal is to carefully analyze data that is similar to your credit card details as well as login details. It is the most common type of network attack. You can help with manual security by learning or creating a solution to scan your email

II. Goals of Network Security ?

The ultimate goal of network security is to protect against actual theft or co-managed data. To achieve this, we focus on 3 important network security goals.

1. Defensive the Privacy of Information
2. Conserving the Integrity of Information
3. Controlling the Obtainability of information only to approved users

These triple objectives reflect the Confidentiality, Integrity, and Access (CIA) that underpin overall security planning. This CIA triple model is a security model designed to guide data security strategies within a community or organization. This model is also referred to as an alternative to the triple AIC (Accessibility, Integrity, and Confidentiality) to avoid errors in the CIA. Trinity Essentials reflects the three most important principles of safety. CIA standards are used by many businesses and corporations when making requests, records, or accessing new information. For a complete database, this will result in PAs. Looking at expectations can be wrong, as they are safety nets that work together. CIA Triad is the ultimate collective standard for measuring, selecting, and installing appropriate security tapes to protect against threats.

2.1. Confidentiality –

We ensure that your complex numbers will be accessible to authorized employees and will not reveal information to anonymous users. If the key is private and not shared, there will be a tendency to interfere with privacy. M.

MethodstoSafeguardConfidentiality

- Data encryption
- Two or Multifactor verification
- Confirming Biometrics

2.2. Integrity –

Make sure all your data is accurate; reliable and should not be changed in performance from one fact to another.

Method for ensuring integrity

- No law can delete records, which violates privacy. Therefore, there will be
- Manage user communications.
- Should have important information to return to soon.
- Translator members should stay close to check the record to see who changed it

2.3. Availability

Each time an operator requests some statistics from a resource, a combat notification, such as a denial of service (Do), is not notified. Evidence must be available. For example, a website is in the hands of an attacker, making it difficult to access.

Here are few steps to maintain these goals

1. Classify assets according to their status and priority. The most important things are always kept safe.
2. The threat is captured.
3. Determine the safety system for each track
4. Investigate any incidents involving damage to the remaining and moving data.
5. Frequent repairs and responses to any related problems.
6. Develop a risk management strategy based on previous research.

III. Advantages

Includes many extras. As they say, it saves your connection or your system, and we all know that keeping things better. Some of the benefits are described below. Public Security: A security agreement is the protection of an organization's communications from external attacks. Of course, the public will adhere to the best practices and will protect their valuable information.

3.1 * Hardware protection - the most sensitive data such as student data, patient data and exchange data must be protected by unauthorized access to prevent it. That's what we can get from network storage.

3.2 * Prevention of intrusion helps us to stop the process after being taken by someone who is not allowed to touch us. Data is stored under reliable security and can be accessed by authorized users.

3.3 * Communication security provides protection against information theft, protects the workplace from theft, reduces PC usage, and secretly informs people employees, give reliable advice, and it is difficult for you to use non -employees.

3.4 * This is the only way to protect your computer from worms, viruses and other unwanted programs. The system protects against hacker attacks, removes and / or blocks from existing networks, limits access to relevant networks, removes other programs or organizations that may interact, and makes it more difficult to protect information.

3.5* Network Security provides greater network security, greater network access, faster data recovery and enterprise data protection. It protects itself, contacts and letters, and fights hackers and information theft.

3.5 * Provides protection against unauthorized access to data because attackers cannot interfere with the network by setting security measures.Provides a hacking system. Keep records. This can be achieved by adhering to safety rules and regulations.

IV. Disadvantages

Properly set up firewalls can be a challenge, well-designed firewalls can prevent operators from doing anything online before a firewall is properly connected, you need to update keep up with the latest software to remember security now, and network security can be costly. ordinary workers. In addition, network security requires the loss of a significant number of users. It is difficult to establish firewall rules properly. Plan security for weeks or too many hours. Ordinary things are expensive. Your service provider may not be able to access the various network components with incorrect firewall instructions.

V. Conclusion

The next generation of cybersecurity will be remembered as it is today: difficult to define and delimit, as digital technology connects people across all aspects of politics, race, family and party. We built this plan with the idea of "work" and the idea of "security" becoming "network security" in the first half of 2010. This event is not far off, but different. in three cases. This is not the point of our research; which one is the most difficult. We believe that the addition of cybersecurity solutions is not far away (if not really today), so that they can better understand the "critical issues" of the Internet age. This places him at the top of the list of challenges to meet and almost always seeks to influence climate change, rather than worry about jobs.