Network Threats and Security Measures

ANJU DEVI

Department of Computer Science and IT

GNG College, Santpura, Yamuna Nagar

Email-Id:-anjucs16@gmail.com

Abstract: Network security has become crucial for securing receptive and confidential information of organization which is being shared and transferred across global networks. Various studies have explored different aspects of network security and have listed common threats that have been damaging the networks globally. The methodology adopted in this paper is a review of papers with keywords network threats and network security measures. The aim of this paper is to critically review the studies on networking security, categorizing various threats and measures that need to be implemented for protection. The paper also describes various concepts related to security including network security, cryptography and encryption.

Keywords: Network security, Information security, Cryptography, Network threats, Network security measures

Introduction

Recent advancements in the field of information and technology and competitiveness on real time data have led to an increase in the transmission of data and information globally. As a result the organizations have become more defenseless to network threats and attacks and are facing invasion in information security and computer networks as the sources of bypassing and breaking through security have increased. A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

The sensitive information being transmitted within the network can easily be accessed by an unauthorized user for malicious purposes. The organizations have been facing interruption, interception, modification and fabrication of their sensitive data from unauthorized sources which break into their security codes. As a result, the information security has become an extremely important aspect in ensuring safe and secured transmission of data through global networks.

Security

Security has been described as a secure environment which is free from danger pose. Data security has become of the major challenges in every field of life for business organizations including securing communication channel, encryption techniques and maintaining the databases. With recent advances in technology the networks are no longer safe from attackers and any unprotected system can easily be breach from unauthorized sources with an intention to steal information for wicked purposes. A successful organization needs to implement six kinds of layers of securities namely physical, personal, operational, communication, network and information.

Information System

Information system is a combination of hardware and software components which enable personnel working within as well as outside an organization to share and transfer data for useful purposes. With increased cybercrime and hacking, the organizational networks have come under great security threat. Therefore, knowledge, awareness and training is essential for securing the information.

Network Security

Network security is a fundamental component of information technology and can be categorize into different major areas including access control, authentication, non repudiation, confidentiality and integrity control. It is a concept of securing and protecting network and data transmission from unauthorized users who can use the information for spiteful purposes. It focuses on securing variety of networks including both public and private transactions and communications among businesses, government institutions and individuals.

Cryptography

Millions of peoples are used computer for many purposes such as: shopping, education, banking, in every field, it is used etc. Privacy is main issue in these applications, how are we need to make sure that an unauthorized person cannot read or modify the messages.

Cryptography is the art of coding the information in such a way that it becomes difficult for an unauthorized person to capture, disclose or transfer it. It is a science of writing secret code by constructing and managing protocol in order to block the adversaries. It is a vital component of computer and communication network and an emerging technology which protects the information from eavesdropping. The process of securing the information is known as encryption and a secret or disguised way of writing a code is known as a cipher. The encrypted information can be transferred back to its original form by an authorized user who has the cryptographic key. Different kinds of ciphers have been used for encryption namely traditional and modern symmetric key ciphers. Traditional ciphers include substitution and transposition ciphers and DES (Data Encryption Standard) and AES (Advanced Encryption Standard) come under the category of modern symmetric key ciphers

Encryption and Decryption

There are two types of encryptions: symmetric and asymmetric in nature. Symmetric encryptions also called the private symmetric key, use single key for encrypting as well as decrypting the code. On the other hand, Asymmetric encryptions work with two keys, public and private for encrypting and decrypting respectively.

Network Threats

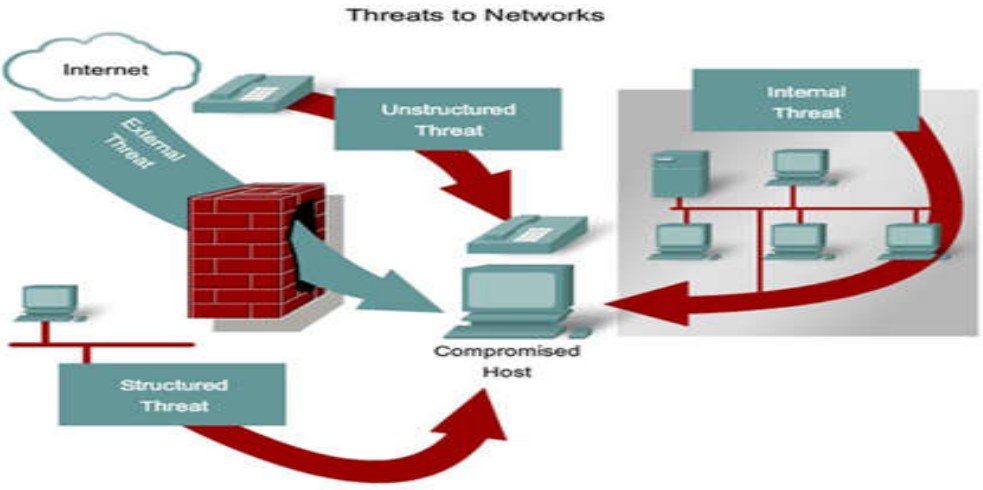
Businesses, government entities, and individuals alike all have to pay careful attention to dangers to their computers and networks. Network security threats are a growing problem for people and organizations the world over, and they only become worse and multiply with every passing day.

Network security is highly threatened by the presence of various threats and attacks that can lead to disclosure of sensitive and confidential information. The basic difference between a threat and an attack is that while threat is a presence of a constant danger to the integrity of information, an attack is an actual act of breaching the security of the network.

Types of Network Threats

There are following types of network threats which are described in details one by one:

1. Unstructured threats
2. Structured threats
3. Internal threats
4. External threats



Unstructured Threats

It consists of mostly inexperienced individuals using easily available hacking tools, such as scripts and password crackers. *Unstructured threats* often involve unfocused assaults on one or more network systems, often by individuals with limited or developing skills. The systems being attacked and infected are probably unknown to the perpetrator. These attacks are often the result of people with limited integrity and too much time on their hands. Malicious intent might or might not exist, but there is always indifference to the resulting damage caused to others.

The Internet has many sites where the curious can select program codes, such as a virus, worm, or Trojan horse, often with instructions that can be modified or redistributed as is. In all cases, these items are small programs written by a human being. They aren't alive and they can't evolve spontaneously from nothing. Some common terms to be aware of include the following:

(i)Virus :

A program capable of replicating with little or no user intervention, and the replicated programs also replicate. The virus requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator. In contrast, a computer worm is stand-alone programming that does not need to copy itself to a host program or require human interaction to spread. Viruses and worms may also be referred to as malware. A virus can be spread by opening an email attachment, clicking on an executable file, visiting an infected website or viewing an infected website advertisement. It can also be spread through infected removable storage devices, such USB drives. Many viruses also include avoidance capabilities that are designed to bypass modern antivirus and antimalware software and other security defenses.

(ii)Trojan Horse

A Trojan Horse proves to be malware which is not self replicating. Typically, such viruses are terribly cunning, in that they seem like they are performing a desirable task for the user. In reality though, they are making possible illegal access on to the user in question's computer system. The term itself comes from the Trojan Horse story in Homer's Illiad from Greek mythology.

These viruses are intended solely to permit the computer hacker the ability to remotely access the targeted computer. This is accomplished easily after such a Trojan horse is installed on the computer. Such operations which the cyber hacker is then able to engage on the machine are limited by the Trojan horse's design, as well as by user privileges on the computer in question. They include the following:

- Stealing of data, such as credit card data or passwords
- Utilization of the computer as a portion of a botnet attack, for creating Denial of service attacks
- Uploading or downloading of files
- Software installation
- Deletion or modification of files
- Wasting of computer storage and memory resources
- Viewing the screen of the user
- Causing the computer to crash

(iii)Worms

Computer worms are computer program malware which are self-replicating. They utilize a computer network in order to dispatch copies of themselves to other computers using the network. They are different from computer viruses in that they are not required to be attached to any existing programs. Worms practically always create some harm for a computer network, even if it is just in eating-up available bandwidth. This is different from viruses, which typically modify files or corrupt them entirely on the computer in question. Worms are far more harmful when they do more than simply replicate themselves onto other computers. In these cases, they may eliminate files on the host system, as with Explore Zipworms; execute a crypto-viral extortion attack, in which they encrypt various files on a computer; or even dispatch out documents using the email system. A common use for worms lies in their installing back doors on the harmed computer for the purpose of creating a zombie computer which the worm author then controls.

Structured Threats

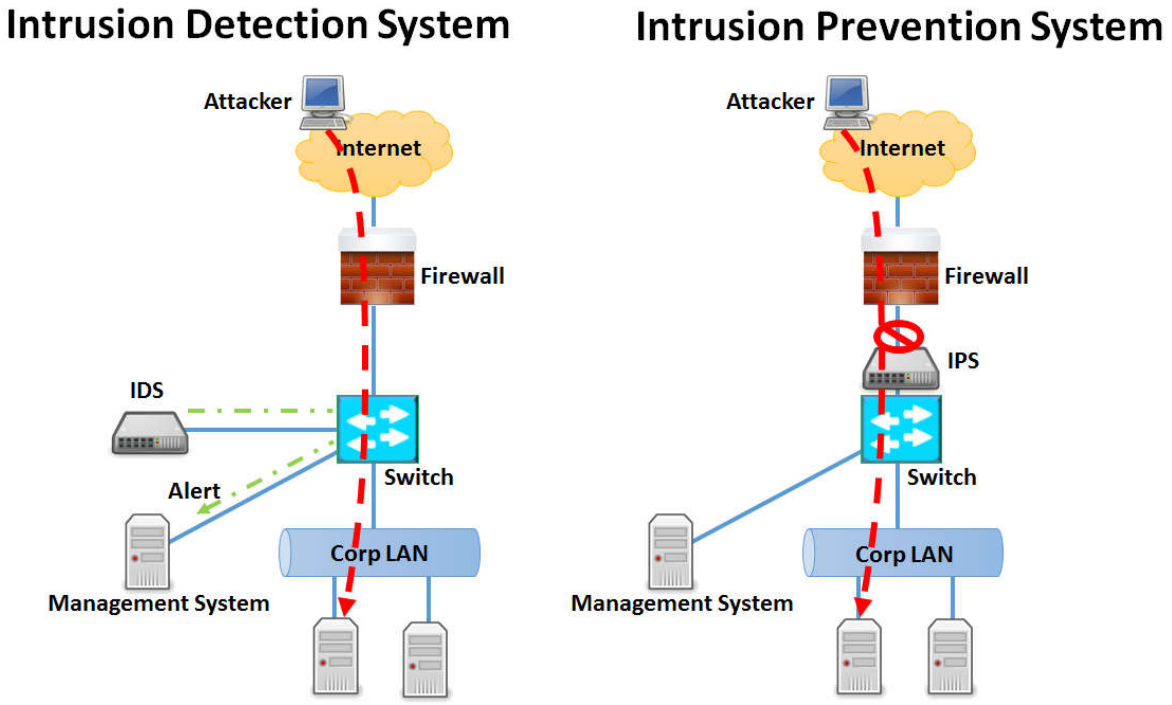
Structured threats are more focused by one or more individuals with higher-level skills actively working to compromise a system. The targeted system could have been detected through some random search process, or it might have been selected specifically. The attackers are typically knowledgeable about network designs, security, access procedures, and hacking tools, and they have the ability to create scripts or applications to further their objectives. These people know system vulnerabilities and use sophisticated hacking techniques to penetrate unsuspecting businesses. International terrorism and government-sponsored attacks on another country's computer infrastructure are becoming well documented. Systems of interest might include utilities, public safety, transportation systems, financial systems, or defense systems, which are all managed by large data systems, each with vulnerabilities.

Internal Threats

It occurs when someone has authorized access to the network with either an account or physical access. Many surveys and studies show that internal attacks can be significant in both the number and the size of any losses. If dishonest employees steal inventory or petty cash, or set up elaborate paper-invoicing schemes, why wouldn't they learn to use the computer systems to further their ambitions? With access to the right systems, a trusted employee can destroy an unsuspecting organization.

External Threats

It can arise from individuals or organizations working outside of a company who do not have authorized access to the computer systems or network. They work their way into a network mainly from the internet or dialup access servers. In trying to categorize a specific threat, the result could possibly be a combination of two or more threats. The attack might be structured from an external source, but a serious crime might have one or more compromised employees on the inside actively furthering the endeavor.



Intrusion Detection Systems (IDS)

There are many reasons to use intrusion detection system as a necessary part of the system to protect it. Many traditional systems and applications have been developed without security. Intrusion detection is a diagnostic procedure that attempts to identify unauthorized access to a network or the reduction of its performance. Intrusion detection system is divided into two main categories: host-based intrusion detection system (HIDS) and network-based intrusion detection system (NIDS). HIDS assesses the information content of operating systems, systems and software file and NIDS analyzes the information in network communications and evaluates the data packets that are exchanged over the network. The system matches the traffic with the attack pattern and if match is detected it gives the alarm to the administrator. However, the attacker may be clever enough to change the signature of the malicious traffic which the IDS fail to detect.

Intrusion prevention system (IPS)

IPS uses IDS algorithm for monitoring and allows network traffic to pass based on technical analysis. It usually works in different areas of the network and actively manages any suspicious activities that can bypass firewall. In fact, this system is a device or software that detects signs of intrusion to the network. This includes generating alarms and intrusion blocking. Generally, IPS is set into the network and monitors the information as they pass inside. An IPS has the ability to

do more than just warning or log its decision. In addition, the system has the ability to be programmed to react to what the diagnosis is. This feature makes the response much better than the IDS and IPS.

Security Measures

Firewalls

A firewall can be defined as a device which may be a computer or router acting between the internet and the organization network. Firewall lets only those packets to be transmitted through it into an organization's internal network which fulfils its perimeters configured by the firewall administrator to be a safe data packet and filters the other packets. Firewall acts at network, transport and application layers. Packet –filter firewall acts at network and transport layer and proxy firewall acts on the application layer. Firewall checks the traffic according to the specific rules it has been configured for but there may be chances when the attacker can portray the harmful data to have perimeters which firewall finds safe to be transmitted through it.

Antivirus Systems

These systems are used to detect and eradicate malware from our systems. The antivirus system should be kept updated with the latest updates so that it would be easy for it to scan the latest virus signatures. Sometimes an antivirus system is not able to detect the infected file if it is encrypted or zipped.

Intrusion detection systems

It is a network monitoring device or software application which keeps track of any malicious actions and policy desecrations and if found it immediately reports about the intrusion to the administrator. They are a set of programs which help detect intrusions and save the system from getting affected. There are two kinds of intrusion detection systems, namely Anomaly Intrusion Detection and Misuse Detection or Signature Based IDS. The Anomaly Intrusion Detection system includes neutral networks and prediction pattern generation, while the Misuse Detection or Signature Based IDS includes state transition tables, pattern matching, genetic algorithms, fuzzy logic, immune systems, and Bayesian method and decision tree. These systems may be Host –based IDS or Network –based IDS. The system matches the traffic with the attack pattern and if match is detected it gives the alarm to the administrator. However, the attacker may be clever enough to change the signature of the malicious traffic which the IDS fail to detect.

Conclusion

The importance of utilize the information in today's developed world will guide to protection threats. It can be said that the safety of computer network of organization, is important to create a viable advantage. Results from this study showed that threats and damage computer networks can be any event that could injure the data. Attacks common to computer networks, include denial of service attacks, eavesdrop, traffic analysis, handling of messages and data, e-mails containing viruses, network viruses, Web-based virus attacks on Web servers and RAID network users. To deal with these threats and vulnerability, there are various techniques that exist, including encryption technique where simple data is encrypted in text in such a way that it can be difficult to understand and interpret. This will reduce the possibility of network intrusion. On the other hand IDS and IPS techniques manage the swapping of information in the network and prevent unauthorized access. After the implementation of the planned techniques using internal and external penetration test can ensure security implementation. In this context, and based on the findings of this study to increase the security of computer networks.

References:

[1]http://www.google.com/network/intrusion detection/

[2]https://www.techopedia.com/definition/4030/network-based-intrusion-prevention-system-nips

[3]https://patents.google.com/patent/US6405318B1/en

[4]https://www.theamegroup.com/network-security-threats/

[5]https://patents.google.com/patent/US7603711B2

[6]http://www.wikipedia .com /network threats/

[7]https://patents.google.com/patent/US4622541A/en

[8]F. S. Roozbahani and R. Azad, “Security Solutions against Computer Networks Threats,” Int. J, pp. 2576–2581.

[9]P. Golchha, R. Deshmukh, and P. Lunia, “www.ijser.in A Review on Network Security Threats and Solutions,” Int. J. Sci. Eng. Res., vol. 3

[10]C. Manimegalai and A. Sumithra, “An Overview of Attacks in the Network Security System,” Int. J. Adv. Res. Comput. Sci. Softw. Eng.