TECH-CHRONICLE
AN INTERNATIONAL E-JOURNAL ON
EMERGING TRENDS IN SCIENCE, TECHNOLOGY AND MANAGEMENT

Cyber security and Networking

[1]Miss. Amita S. Chouhan
Tulsiramji Gaikwad-Patil College Of Engineering and Technology Nagpur, India
Contact No:9168285943
Email: amitachouhan15@gmail.com

Abstract: Cyber security is the body of technologies, processes and practices design to protect networks, computers, programs and data from attack, damage or unauthorized access.
In computing context the term security implies cyber security.
This paper is about simulations of attacks, defenses, and consequences in complex cyber systems such as computer networks. Network security is a complex and challenging problem. The area of network defense mechanism design is receiving immense attention from the research community for more than two decades. However, the network security problem is far from completely solved. Researchers have been address the network security issues. We begin by discussing limitations on simulation that are relatively unique to information protection, how simulation works. Next we show results of individual simulations and runs of a few thousand simulations that characterize small portions of the design space for attacks alone and then attacks in the presence of defenses.
In this paper we show how to protect the system from the cyber attack with the help of simulation and also protect the network. The key concept is to deal with cyber attack that is the main part of cyber security as we mention above the security in terms of computer is a cyber security.

In terms of security we have to provide some strong security to our computer system so that the attacker cannot crack it easily. The security involves protecting information and system from major cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage.

Keyword: - Cyber security, simulation attacks, cyber threats, security attacks.

I. INTRODUCTION

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs

and data from attack, damage or unauthorized access. In a computing context, the term security implies cyber security
Cyber security involves protecting information and systems from major cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage. In their most disruptive form, cyber threats take aim at secret, political, military, or infrastructural assets of a nation, or its people. Cyber security is therefore a critical part of any governments' security strategy.

I. RELATED WORK

Cyber criminals target financial institutions, businesses of all sizes, government agencies and military organizations

across the globe. They have the power to inflict significant damage through interruption of service, intellectual property theft, network viruses, data mining, financial theft and theft of sensitive customer data. Cyber security specialists identify and resolve these highly complex issues to keep information secure, allowing business to continue as normal. Cyber security specialists are responsible for keeping cyber crime at bay by using their proficiency in analysis, forensics and reverse engineering to monitor and diagnose malware events and vulnerability issues. They then make recommendations for solutions, including hardware and software programs that can help mitigate risk. These professionals typically design firewalls, monitor use of data files, and regulate access to safeguard information and protect the network. Staying up-to-date on current virus

reports and protecting networks from these viruses is a major aspect of a cyber security specialist's job duties. They often train users, promote security awareness, develop policies and procedures, and provide updates and reports to management and executive staff.

II. Elements

Ensuring cyber security requires coordinated efforts throughout an information system. Elements of cyber security include:

A. Tools supporting security management and development:

The cyber security management process is a known "system" of interrelated elements that act in concert with one another to achieve the over-arching goal of the system itself --to protect the confidentiality, integrity and availability of information and represents knowledge of many of these system elements. While not all of the elements of the map will be discussed in this paper, primary attention is given to policy and technology. Driven by policy, the cyber security management process applies technology and requires effective planning in order to achieve the goal.

B. Computer network security:

The field Network and internet security consist of measure to deter, prevent, and correct security violation that involve the transmission of information. That is board statement that covers a host of possibilities. To give you feel for your area covered in this topic. In the network security the main term is to provide the security to the computer network when it is communicating with other computer or the other system
So the network security provides a protection to the data in a network against un authorize access and hackers.

C. Cyber-attack detection:

In this element we can show the how to detect the cyber attack. The cyber attack are very harmful for the system some time it damage or destroy the system.
Cyber attacks crime and cyber attacks terror increase exponentially. To save innocent people life we suggest to set ethical rules for virtual world according to real life. Furthermore new security actions are required to protect private life in virtual world. This paper introduces a survey of cyber attacks detection. Cyber attacks are actions that attempt to bypass security mechanisms of computer systems. Cyber attack detection has been defined as "the problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges. We add to this definition the identification of attempts to use a computer system without authorization or to abuse existing privileges.

Cyber Attack Types

a. Denial of Service Attacks
b. Attacks Detection Strategies
c. Analysis Approach

D. Cryptographic Solution

A cryptography is the process of encryption and decryption in cryptography we can use two algorithm first is encryption and the second is for decryption. The encryption is the process in which the plain text is converted into cipher text. And the decryption is the process in which cipher text is converted into plain text.Encryption and decryption process provide the security to the data which is send to one place to another place or one system to another system.
This is the standard.The many schemes use for encryption constitute the area of study known as cryptography. Such system is known as cryptographic system or cipher.
Cryptanalysis is what the layperson calls "breaking the code". The area of cryptography and cryptanalysis is together call cryptology.

E. Network Security:

Network security is a process of taking physical and software preventative measures to protect the under laying networking infrastructure from unauthorized access, misuse, Malfunction modification, destruction or improper discloser, thereby creating a secure platform for computers, users and programs to perform.Security management for network is different for all kinds of situation A. home or small office may only require basic security while large businesses may require high maintenance and advance software and hardware to prevent malicious attack from hacking and spamming.

Types of Attack in network security:
Attack can be from two categories "passive" when a network intruder intercepts data travelling through the network and active in which an intruder initiate command to disrupt the networks normal operation.

III. Classification of Cyber Attacks

The attacker will expect the process to be harmonized in order to infect the system. Synchronization of the steps involved to steal the information leads them to achieve what they expect. The hackers will get their result in time, in step and in their line. An organized form of the methods will be used by the attacker or hacker lead to infect the system very easily. The usage of logically organized methods leads them to get more efficient results. The attacks are regimented with perfect sequence and in such a way that the resulting damage is severe enough to compromise the working of the organization.

Reconnaissance Attacks Type of attack which involves unauthorized detection system mapping and services to steal data

Access Attacks An attack where intruder gains access to a device to which he has no right for access.

Denial of Service Intrusion into a system by disabling the network with the intent to deny service to authorized users Denial of service (DOS) is class of attack where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine.

Cyber crime The use of computers and the internet to exploit users for materialistic gain

Cyber espionage The act of using the internet to spy on others for gaining benefit.

IV. Advantages of Cyber Security:

a. Improved security of cyber space.
b. Increase in cyber defense.
c. Increase in cyber speed.
d. Allow more option to save data.
e. Better response time to national crisis.

VI. Disadvantage of Cyber Security:

a. Improved hacker speed and ability
b. Interconnected to computers
c. Improved viruses, malware and worms
d. Increase in cyber warfare possibly
e. More anonymity between hackers.

VII. Conclusion:

This paper introduced and discussed different cyber attack detection strategies. We have carried out comparison and analysis between different cyber attacks strategies. Cyber attack techniques have been improved dramatically over time, especially in the past few years. Developing new cyber attack detection schemes is necessary because cyber attackers develop their strategies continuously too. Information fusion from multiple sources required intelligence techniques to characteristic the cyber attackers. It seems that traditional cyber attacks detection schemes may prevent cyber attackers temporary and partial. To overcome the lack of traditional cyber attacks detection schemes we propose new scheme for real-time and short-term response to actual attacks

Reference:

I. M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification", International Journal of Network Security, vol. 15, no. 6, **(2013)**, pp. 391-397.
II. S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", IJCSNS International of Computer Science and Network Security, vol. 9, no. 5, **(2009)** May, pp. 1-10.
III. M. E. Kuhl, J. Kistner, K. Costantini and M. Sudit, "Cyber Attack Modeling And Simulation For Network Security Analysis", Proceedings of the 2007 Winter Simulation Conference, pp. 1180-1188.
IV. C. S. Dangi, R. Gupta and G. S. Chandel, "Cyber Security Approach in Web Application using SVM", International Journal of Computer Application, vol. 57, no. 20, **(2012)**, pp. 30-34.
V. Forsythe, C., Silva, A., Stevens-Adams, S., & Bradshaw, J. (2013). Human dimension in cyber operations: Research and development priorities. In Foundations of Augmented Cognition (pp. 418-422). Springer Berlin Heidelberg.