International Journal of Pure and Applied Mathematics
Volume 117 No. 21 2017, 93-99
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Study of various attacks in Computer Networks and assessment methods

C.Lakshmi
Research Scholar
Sathyabama University, Chennai,Tamilnadu,India

P.Jesu Jayarin
Associate Professor
Jeppiaar Engineering College,Chennai,Tamilnadu,India

***Abstract*- Network security plays a vital role in monitoring and preventing unauthorized access/modification, denial of service(DOS) to a computer network and resources accessible through a network. Security management for networks is different for all kinds of situations. The network, transport and the user application layers of the ISO/OSI layers plays a key role. Some of the specific mechanisms used for security are VPN, Firewalls and IDS/IPS. Each of the security patterns has different architecture and mechanism. The security patterns are needed to secure the data transfer along with the security defenses at the OSI Layers. Although many security patterns and techniques have been proposed, it is still difficult to adapt security patterns to each type of threat. This paper analysis the various attacks in network security.**

Keywords-Firewall,VPN,IDS/IPS,Denial of service attacks.

I.INTRODUCTION

The operating system itself vulnerable to some attacks such as hacking of Bios Passwords, Login passwords, accessing the restricted drives etc., The network attacks such as password hacking ,Input validation attacks, Buffer overflow attacks, Privacy attacks, Denial of service(DOS) attacks, SQL injection attacks. Most of the attacks are deployed by using some malicious codes .The hackers uses some security information in malicious codes and send it to the end-user. The end-user accesses the particular code and gets hacked.

There are several filters and alerting systems are used to indicate the security issues in the network. In order to ensure the network security, the administrator installs, generally, filtering security components in strategic points. The network security is ensured by installing various security elements and positioning of these security element is also important. The abnormal traffic is a indication of network security.

In wireless networks the security components should be dynamic. But in core networks the various hardware and software security systems are installed, even though the attacker can easily hack secure system.

Viruses and worms are the main security threat in network. The worm is a program that replicates itself and virus is a bit of code that is executed as a part of the file. When the user installs the file the virus attack the system without the knowledge of the user.

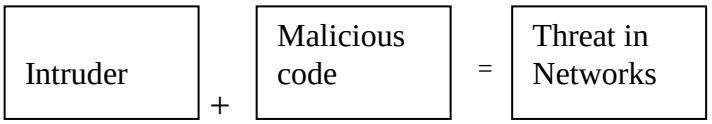

Figure 1:Network Threat

II.NETWORK HACKING

Telnet is the ultimate hacking tool that used to connect to remote computers and run command line programs. By using the IP address of the remote computer the connection with remote system has been made. Telnetting to 127.0.0.1 can be used to fool people into believing their system has been hacked.

A number of email borne viruses prevalent on the net are actually .hta applications containing malicious code. The HTA behaves like a normal .exe file, it can be executed anytime later. When running HTAs user should take some precautions as with any executable.

Input validation attacks spread in Internet because of poor authentication. Input validation attacks occurs because of poor programming practices. Sometimes the programmer bypass the security issues in the program All application that fail to validate the input received from either remote or local users are vulnerable to input validation attacks.

SQL injection attacks injected into the network by using SQL queries.SQL injection attacks is designed specially to steal or modify the content of the secure database.Uncovering illegitimate records, bypassing security features, carrying out malicious codes on the remote victim system-all possible for an attacker who located a vulnerable SQL server.

The following SQL injection attacks are used by the hackers.[9]

Tautology : The attacker inject the SQL query which is always true, the data are recovered from the database.

Syntax:
SELECT *FROM database WHERE querystring='education' or 1=1

Here the condition 1=1 is checked, it is always true, so the database returns all the record that matched the string education.

Logically incorrect query: An attacker deploy the wrong query to get the back end information of the database.

Stored Procedure : Malicious SQL injection queries which is injected on the network.

Piggy-Backed Queries: The queries are added into an original injected query

Union Query: UNION keyword is used to get the information by combining the injected query using authenticated query

A Distributed Denial of Service (DDoS) attack is a common threat used by the hackers in SDN network .This type of attack will occur at the network layer or the application layer of the systems that are connected to the network[7].Denial of Service(DOS) attacks are nothing but sending false request the server and reduces the server efficiency. The server is busy with false request and the true request cannot be served. Denial of service means denying valid Internet and network users from using the service of the target network or server. In TCP/IP instead of sending the single SYN packet to server for acknowledgement several SYN packets are sent to the server but all these SYN packets have bad source IP address. The target receives these SYN packets with bad IP addresses, it tries to respond to each one of them with a SYN ACK packet. The target system wait for the ACK message from bad IP address, it queues up all these request until it receives an ACK message.

Smurf Attack is a form of brute force DOS attack, in which a enormous amount of ping request are sent to a system .When the router gets a ping message, it will route it or return it back to the source, creates flooding in the network and increases the network traffic.

I.SECURITY MECHANISMS IMPLEMENTED IN NETWORK

Digital Immune system is implemented in network for constantly analyzing and monitoring the viruses and it should be continually update the digital immune software to protect the network from the threat.

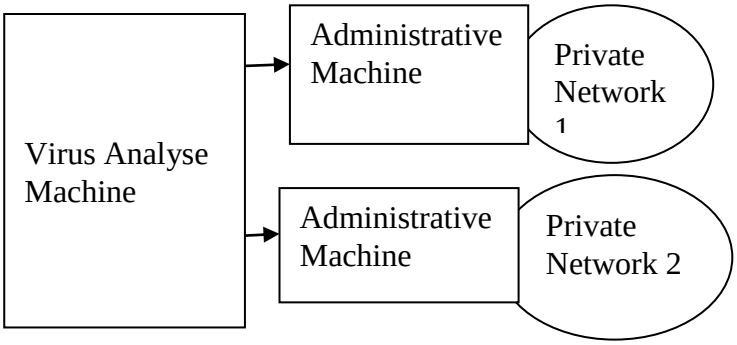

figure 2:Digital Immune System

A.Firewall

Firewall technology is used for network perimeter security. In packet firewall the predefined rules are created, the packets which matches with these rules are only allowed to enter in to the network and other packets are ignored. The packet firewall only checks the IP address of the source and destination, such firewalls can be fooled by IP spoofing. The attacker changes the IP address of the packet by using IP spoofing. Instead of checking the IP address of the packet alone the packet inspection firewalls verifies the content of the incoming packet instead of verifying the source and destination IP address. The firewall itself does not provide enough security. The attacker may gain the network access by using password cracking (brute force attack). A firewall in no way can prevent such occurrences.

One way to avoid IP spoofing is encrypting the Source IP address, but this is not applicable for large networks. Reference [11] the IP spoofing is eliminated by validating the source IP address. In this paper the author proposed hybrid mechanism such as the network has the own capability to verify the of IP addresses for all packets.

B.Intrusion Detection and Prevention system

The IDS is to detect future attacks .The IDS detect both misuse and anomaly penetration in network . The IDS detects the particular attacks that is stored in the database.

Network Intrusion Detection system(NIDS),deployed to detect security violations ,enhancing the security of modern computer networks. Intrusion Detection System used along with anti- virus software to improve intelligence of intrusion detection System.

In [2]a filter based feature secure algorithm is implemented in intrusion detection system. In this algorithm the some features are predetermined and the patterns are not having this features are eliminated. The better matching pattern are selected ,the overall accuracy achieved in this method is 95.75%.

Reference [1] proposes a method for testing and validating the models which are used in network intrusion detection. The simple network environment has intrusion model and the tools such as Nmap and other specialized tool. This model reduces the propagation of intrusions in the network.

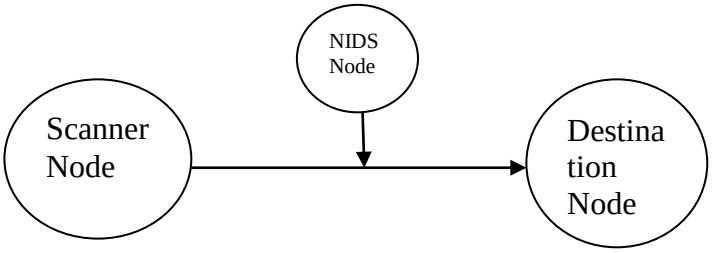

Figure 3: Simple test environment to test NIDS

C. Virtual Private Networks

VPN is secure connection between source and destination. The public networks are accessed in secure manner by using VPN .A virtual point-to-point link is created between the nodes to establish a secure connection. The wired network protected in both ways using VPN as well as Firewall. A dedicated link is created between source and destination to avoid the proxy interference. In contrast with firewall in VPN traffic is minimised.

Reference [3] has six different scenarios is simulated.The performance of VPN in wireless and Wired network is analyzed. In various mechanisms such as Point-to-Point Tunnelling Protocol (PPTP), Internet Protocol Security (IPSec) and Secure Socket Tunnelling Protocol (SSTP) are implemented to ensure the network security.

sIn[4] the various VPN protocols have been tested and evaluated on multiple operating systems with different algorithms and compared against each other

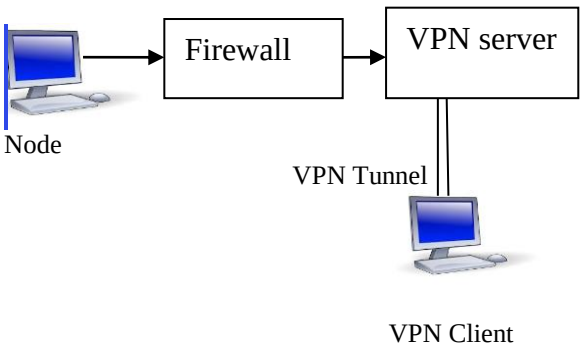

Figure 4: VPN Architecture

IV.SECURITY METHODS IMPLEMENTED IN NETWORK SECURITY

A. Neural Networks in Intrusion Detection System

In [6] the artificial neural network is implemented in computer network security . The artificial neural network is implemented in network security to improve security factor . In this paper the author proposes computer network security which is based on client server model. The behaviour of the node is determined from the input from the various input node. To solve the drawbacks of the artificial neural network the back propagation neural network is utilized[6].

In neural networks two methods are used. First method is supervised training and second method is unsupervised training. In case of supervised training method the system compares the output with predetermined and find the matches whereas in unsupervised training method the neural networks groups the patterns with most relevant features.

The neural network is implemented in network to detect external attacks in network perimeter. Neural network is also used to identify the inside threat also. The neural network used for anomaly detection in digital forensics.

The fitness value is computed from this equation

$$Fitness(j) = \sum_{j=0}^{n} (\mathrm{Av} - \mathrm{Ev})^{2} \text{----------(1)}$$

Fitness function calculates the best value of each chromosome. Better chromosomes are selected based on the fitness value. The chance is given to the he better chromosomes to reproduce themselves than those chromosomes that give low fitness value.

Benford's law is used to determine of number duplication in datasets and used to identify abnormal

occurrences. The data is collected to training and testing the neural network .The same dataset can be used for anomaly detection in computer networks

B.Pattern Matching Schemes used in Network Security

The pattern searching algorithm is used in Intrusion Detection Systems (IDS) to ensure the network security and eliminate the propagation of virus and malwares.

Reference [9] the pattern matching is implemented against SQL injection attack. SQL injection is used to hack the database. Pattern matching is used to identify element of a given pattern set which appears in the proposed traffic strings. [9]

In [7] Machine learning algorithms is deployed in IDS to detect DDoS attack in SDN. In this paper the various classifier algorithms such as access control algorithm ,Navie Bayes algorithm, KNN algorithm, K-Means classifier and K-medioids algorithm are used .Performance of various algorithm is analysed . Naive Bayes classifier is used to identify the incoming packets are normal or virus affected.

TABLE 1: Performance analyses of Various classifiers.

S.No	Classifier Name	Advantages
1	Naive bayes	Highest accuracy of 94%.For large dataset the pattern matching time is high
2	KNN	Detection rate is 90 percent
3	K-means	Less accuracy compare to Naive bayes and KNN. Even though the dataset increases the pattern matching time is less.
4	K-mediods .	Same accuracy as K-means but lesser than Naive bayes and KNN. Faster than Naive bayes and KNN

As far as accuracy is concerned in IDS the naive bayes is chosen even though it has more training time.

In [8] the complex pattern is decomposed to increase the matching speed. The matching speed is increased by 43%.It easy to check the small patterns in compared with large patterns. The hardware based system is proposed by the author to increase the throughput but the hardware is not modified based on the requirements.

A dot star is a common pattern in security. The regular expressions is.*A.*B{{1}.To combat this size increase, the Pattern is decomposed into .*A{{1a}}|.*B{{1}}.In this paper DFA (deterministic finite automata) used for pattern matching. The performance of DFA falls by 83% .

As is shown in Wikipedia,a deterministic finite automaton M is a 5-tuple, $(Q, \Sigma, \delta, q_0, F)$, consisting of

(i).a finite set of states (Q)

(ii).a finite set of input symbols called the alphabet (Σ)

(iii).a transition function ($\delta : Q \times \Sigma \rightarrow Q$)

(iv.)an initial or start state ($q_0 \in Q$)

(v).a set of accept states ($F \subseteq Q$)

To achieve the semi automation or automation in pattern matching DFA is implemented.

Reference [10] the Hybrid security architecture is deployed in network security. The meaning of ‘hybrid’ indicates the combination of security and networking and the combination of software and hardware. In hybrid security architecture the firewall and Intrusion detection system is combined together, virtual middle box is created. If software middle boxes are deployed the number of machines required is reduced to only 1.67%[10]

In [17] various pattern matching algorithms such as Brute force, RabinKarp, KMP and Boyer Moore are compared. The author conducted experiments on various algorithm and concluded that Boyer Moore and KMP algorithms are efficient compared to remaining algorithms. Boyer-Moore algorithm is efficient for large text and pattern. In KMP the searching time is reduced as compared to brute force algorithm. Rabin-Karp algorithm whose time complexity is not faster than naive search algorithm. Rabin-Karp algorithm is efficient by using a better hash function.

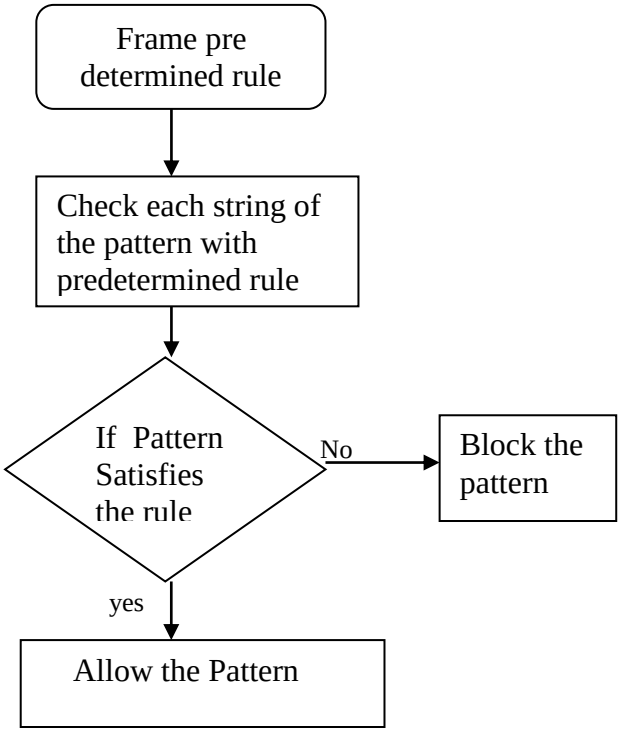

Figure 5:Pattern Matching Technology

In [18] the author proposes the innovative pattern matching algorithm, with reduced searching time. This algorithm is tested against Dos attack,Remote-2-local attack, user-to-root attack and Probe attack. This algorithm uses a DNA concept for pattern matching, since efficiency is improved and also exact pattern matching is achieved. All the datasets are converted into their respective DNA nucleotide sequence and testing dataset is converted into encoded nucleotide sequence. The encoded text string (network activity) is compared with encoded nucleotide sequence and the output is evaluated either it is a normal sequence or attack.

In [20],the authors proposed the Intrusion detection System based on the Genetic algorithm(GA).The fitness function is selected and genetic parameters are calculated. The goodness of each chromosome is calculated and the fitness function is calculated.

Several pattern matching algorithms are proposed and in some researches shows hybrid pattern matching schemes to increase accuracy and matching time.

V.CONCLUSION

In each of the network the source, destination and the perimeter have to be provided with different security mechanism. In every node host there has to be a Host Intrusion Prevention system (HIPS) and Host Intrusion Detection system (HIDS). In every network there has to be Network Intrusion Prevention system (NIPS) and Network Intrusion Detection system (NIDS). In every Perimeter of a network there has to be a firewall. This increases the configuration complexity. The above stated algorithms,Patterns and structures are implemented against particular attacks and each method has some disadvantages.

VI.FUTURE ENHANCEMENT

In order to overcome the difficulties faced in the current scenario, a hybrid security mechanism is need to be proposed .

REFERENCES

[1]. Marko MiUitla,Tomi Raty" Testing and Validating Activity Models for Network Intrusion Detection*"International Conference on Computer & Information Science (ICCIS)*,2012,_pp: 723 – 728.

[2]. Mohammed A. Ambusaidi ,Xiangjian,Priyadarsi Nanda and Zhiyuan Tan "Building an intrusion detection system using a filter-based feature selection algorithm" *IEEE Transactions On Computers*, Vol No:65, Issue:10,November 2014,_pp: 2986 – 2998.

.

[3]. Dr Y.P Kosta,Upena D Dalal and Rakesh Kumar Jha"Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)" *International Conference on Recent Trends in Information, Telecommunication and Computing*, 2010,pp: 281 - 283

[4]. Shaneel Narayan, Cameron J. Williams, Daniel K. Hart, Max W. Qualtrough "Network Performance Comparison of VPN Protocols on Wired and Wireless Networks". *International Conference on Computer Communication and Informatics (ICCCI -2015)*, Jan. 08 – 10, 2015,pp: 1 – 7.

[5]. Mandeep Pannu, Bob Gill, Robert Bird, Kai Yang, Ben Farrel "Exploring Proxy Detection Methodology" *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* ,2016,Pages: 1 - 6 .

[6]. Zhou Lianbing" Study on Applying the Neural Network in Computer Network Security Assessment" *Eighth International Conference on Measuring Technology and Mechatronics Automation*, 2016,_pp: 639 – 642.

[7]. Lohit Barki, Amrit Shidling, Nisharani Meti, Narayan D G and Mohammed Moin Mulla "Detection of Distributed Denial of Service Attacks in Software Defined Networks" *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sept. 21-24, 2016,pp: 680 – 689

[8]. Eric Norige, Alex Liu"A De-compositional Approach to Regular Expression Matching for Network Security *Applications" IEEE 36th International Conference on Distributed Computing Systems (ICDCS),2016*pp: 680 – 689.

[9]. MA Zhi-cheng,Zhang Lei ,YANG Ming-jie,Zheng Yi."Study on the pattern matching technology and its application in network security" *8th*

International Conference on Intelligent Computation Technology and Automation,2015,pp:888 - 891

[10]. Ho-Yu Lam, Song Zhao, Kang Xi, H. Jonathan Chao "Hybrid Security Architecture for Data Center Networks". *IEEE International Conference on Communications (ICC), 2012,* pp:2939 – 2944.

[11]. Guolong Chen, Guangwu Hu, Yong Jiang, Chaoqin Zhang "SAVSH: IP Source Address Validation for SDN Hybrid Networks" *IEEE Symposium on Computers and Communication (ISCC),2016*, pp: 409 – 414.

[12] Sreeja N. K., Sankar A., "Pattern Matching based Classification using Ant Colony Optimization based Feature Selection", *APPLIED SOFT COMPUTING, 2015, 31: 91-102.*

[13] Sun Li, Ren Pinyi, Du Qinghe, Wang Yichen, Gao Zhenzhen, "Security-Aware Relaying Scheme for Cooperative Networks With Untrusted Relay Nodes", *IEEE COMMUNICATIONS LETTERS, 2015,* 19(3): 463-466.

[14] Yavuz Canbay, Seref Sagiroglu "A Hybrid Method for Intrusion Detection" *IEEE 14th International Conference on Machine Learning and Applications*,2015,pp:156 – 161.

[15].Teleimersion" Research Journal of Pharmaceutical, Biological and Chemical Sciences on March – April 2016 issue.

[16].A Human Computer Interfacing Application ", International Journal of pharma and bio sciences

[17]. V. Gupta, M. Singh and V. K. Bhalla, "Pattern matching algorithms for intrusion detection and prevention system: A comparative analysis," *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, New Delhi, 2014, pp. 50-54.

[18]. N. Sheikh, K. Mustafi and I. Mukhopadhyay, "A unique approach to design an intrusion detection system using an innovative string searching algorithm and DNA sequence," *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, 2016, pp. 1-9.

[19]. M. Sadiq Ali Khan, "Rule based Network Intrusion Detection using Genetic Algorithm", International Journal of Computer applications (0975 – 8887), Volume 18– No.8, March 2011

[20]. G. P. Rout and S. N. Mohanty, "A Hybrid Approach for Network Intrusion Detection," *2015 Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, 2015, pp. 614-617.