Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Intrusion Detection System (A Layered Based Approach for Finding Attacks)

Kiran Dhangar
M.Tech Scholar,CSE Dept.
Indore, India.

Prof. Deepak Kulhare
Faculty CSE Dept.
CIIT Indore, India.

Arif Khan
Faculty CSE Dept
CIIT Indore, India.

Abstract ***This paper titled "Intrusion Detection System A Layered Based Approach for Finding Attacks" is an OSI layered based network intrusion detection system (IDS) proposed. Here we are concentrating and analyzing OSI layers based attack finding technique. Moreover the proposed IDS approve the effectiveness of the proposed system, and presented results shows advantages of host based as well as network based security. The proposed model of IDSs offers several advantages over alternative systems. First of all it provided layers wise (Application, transport and Network) attack find capability that mean all the attack will be capture according to their layers in network based module, it supported high availability and scalability, and most important thing it produced good results in terms of normal and abnormal behaviors of captured packet. The proposed model includes integration of individual components to produced batter results. In addition it provide host based intrusion detection functionality, in which two type of attribute find in security event log file one is login-logoff time and another is unauthorized accessing of the host.***

Keywords— IDS, Protocols, Network, Security, TCP, Attacks

I. INTRODUCTION

Nowadays the number of computer networks keeps growing in parallel with transactions, especially on the Internet while streaming, video conferencing, chatting, searching, etc. These various types of transactions introduce many intrusions and anomalies into the network. A Network attack or security or security incident is defined as a threat as shown in figure 1, intrusion, and denial of service or other attack on a network infrastructure that will analyze our network and gain information to eventually cause our network to crash or to become corrupted. In many cases, the attacker might not only be interested in exploiting software applications, but also try to obtain unauthorized access to network devices. Unmonitored network devices are the main source of information leakage in organizations. Network traffic is often seen to display sudden deviations from normal behavior. Some of these aberrations are caused by malicious network attacks such as Denial-Of-Service or viruses, whereas others are the result of equipment failures and accidental outages [10]. Many methods have been developed by organizations and play very important roles to secure network infrastructure and communications via the Internet such as through the use of firewalls, anti-virus software packages and intrusion detection systems. Current firewalls cannot defend against every category of intrusion, whereby some intrusions take advantages of computer system vulnerabilities [11]. An intrusion detection system (IDS) provides around-the-clock network observation and is an additional wall to secure the network. The intrusion detection system is a process of determining an intrusion into a system through the observation of available information concerning the state of the system, monitoring user activities and reporting to a management station. Intrusion detection refers to the detection of cruel activity (break-ins, penetrations, and other forms of computer abuse) in a computer-related system [12]. Therefore, the ID techniques are classified into host-based and network-based depending on the type and source of information used to identify security breaches [13, 14] depending on the method of intrusion detection. One definition from the study that an intrusion is any activity that moves a system from a safe state to an unsafe state, but this does little to clarify the situation. Another definition declares, in essence, that an intrusion is anything that violates the policy of the site under consideration, but this also does little to address the issues at hand. Here defining each word of intrusion detection (ID) **Intrusion:** The act of wrongfully entering upon, seizing, or taking possession of the property of another.

- **Detection**: The act of discovering or determining the existence, presence, or fact of.
- **Intrusion Detection**: The act of discovering or determining the existence, presence, or fact of the wrongfully entering upon, seizing, or taking possession of the property of another.

The concept of security and the word intrusion detection system might be intimidating and complicated. The objective of the paper is to develop a tool that mediates the user and the operations to achieve security goals. A platform independent tool with user-friendly graphical user interface, using already existing techniques and concept for intrusion detection system will be resulting product. People need to use the intrusion detection system in order to identified attacks in host based system and network based system. The operations include bunch of rules to identify the attacks of foreigners to reach and read personal files that is located in personal computer or the owner would like to send somewhere. Computers connected directly to the Internet are subject to relentless probing and attack. While protective measures such as safe

configuration, up-to-date patching, and firewalls are all prudent steps they are difficult to maintain and cannot guarantee that all vulnerabilities are shielded. IDS provides defense in depth by detecting and logging hostile activities. An IDS system acts as "eyes" that watch for intrusions when other protective measures fail. The primary objective of the proposed work is to propose a new "**Intrusion Detection System**" (IDS) concept which is including both type (host and network) functionality, without explaining the fixed intrusion detection system used in that concept. In this we have more concentrated on the layered wise attack .The proposed IDS affects the performance of execution and security analysis. Each issue will be investigating in detail in the
Proposed work. The proposed concept does rely on specific HIDS. Rest of the paper is organized are as follow: Section II presents proposed work where we have discussed proposed work in the field of IDS. Section III is presets results analysis and finally section IV present conclusion.

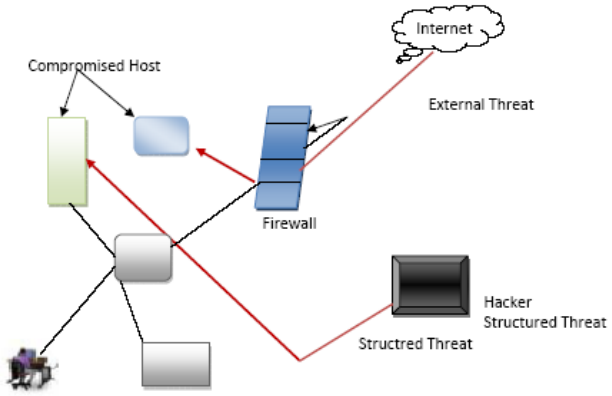


Figure 1: Security Threats

II. PROPOSED WORK

Proposed intrusion detection system monitors individual systems upon the network. In this case, the sensor of the IDS is located inside of the particular host to monitor system-level behavior. This type of intrusion detection is especially useful for monitoring potentially dangerous user activity within the network. It's clear that there are two types of host-based intrusion detection software: host wrappers (or personal firewalls) and agent-based software. Here describes the host wrappers as tools that can be configured to look at all network packets, connection attempts, or login attempts to the monitored machine. The agent-based software has the same abilities as the host wrappers, but can also detect changes in system files and changes in user privileges. A report by Network Associates makes a good argument for host-based intrusion detection, stating, and any masking techniques such as insertion, padding, fragmentation, or out-of-sequence delivery, which would evade a network-based IDS can be easily caught by a host-based IDS." Additionally, host-based IDSs can be quite effective in switched environments, whereas network-based IDS systems are less effective in that environment. A switch tends to isolate communications on the network, making it difficult for network-based IDS to monitor all traffic. However, if the systems on the switched network have host-based IDSs installed, potential attacks may be thwarted.
Figure 2 is showing the proposed system architecture which is the combination of host based and network based intrusion detection system, and known as "Proposed Intrusion Detection System (PIDS)". In this figure particular IDS model capture packets and call to detector agent where detector agent pass capture packets to rule matching process

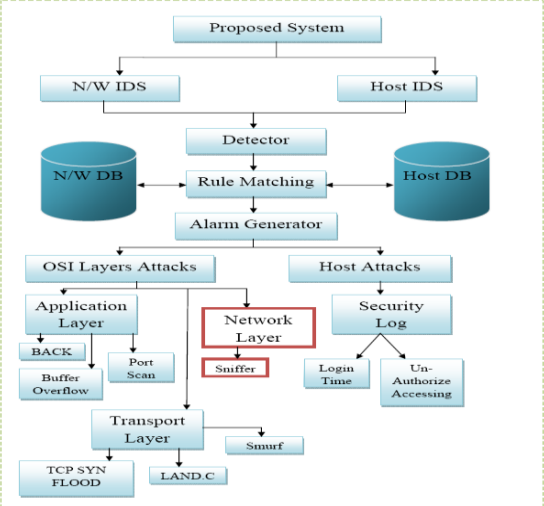


Figure 2: Architecture of the proposed system

2.1 Proposed NIDS

Where rule matching process check attacks criteria from the database, where we have already defend and stored rule to find attack. After completing this process alarm will activate if any type of attack find in the captured packet otherwise it will be deactivate and this processes will continue till on the proposed system. In network based module we have concentrate on layers wise attack finding mechanism, that mean which layers in the OSI model are producing what type of attack. All **the details of layer attacks are shown in next part. At the time of TCP packets header extracting proposed system checks the arriving IP header. From IP header it selects only TCP protocol. Figure 7 is showing block diagram of proposed "**Network Intrusion Detection System (NIDS)"**. In NIDS we are finding layer attack or abnormality in the captured pactes which is follows: in application layer attack we are finding 'Back", "Buffer overflow" and "Port Scan". In Transport layer we are finding "TCP SYN FLOAD Attack" "Land" and "Smurf". Finally network layer attack are future work of this research. The Proposed IDS system is provide additional functionality of** "Host Intrusion Detections System (HIDS)" which is shown on figure 8. **In this we are finding one type of attack by analyzing the security event log file which is stored in local system. From security event log file we have finding two types of attacks which is follows: "Un-authorize accessing" and Login failed". The proposed NIDS find six different conditions for attacks first it monitor and catch packets which is traveling over public network like internet, after catching packets, TCP header is extracted and analyzed its attribute. If RST flag find in its attribute then it will treat as an abnormal packet and will go to the alarm generator to**

note that this is infected packets and it should be treat as an attack type. Another condition is for Back/land type attack this type attack is belongs to DOS attack (Shown in figure 3) category this will be work on both layer application as well as transport layers also.

Basically "Back" attack find on application layers and "Land" attack find on transport layers. The condition for this type of attack is to analyze number of packet which is arriving from same host with in a time. In this we have set time limit to capture such type of packets and the time limit is 3 second time and 15 packets. If the same host are sending 15 or more then 15 packets in 3 second then that host is the intruder which is generating reported fake address then it will also treat as an attack type. Another condition of application layer attack is the buffer overflow which is belongs to U2R attack is unauthorized access from a remote machine which is also shown in figure 4. For this attack we have set window buffer size and check overflow condition if overflow is occurring by the capture packets that mean such type of attack can be activate another definition of this attack capturing packet are lager then the predefined window buffer size then that packet will treat as an attack type.

Another application layer attack is the port scan. A Port Scan is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines Connected to a network run many services that use TCP or UDP ports. A port scan

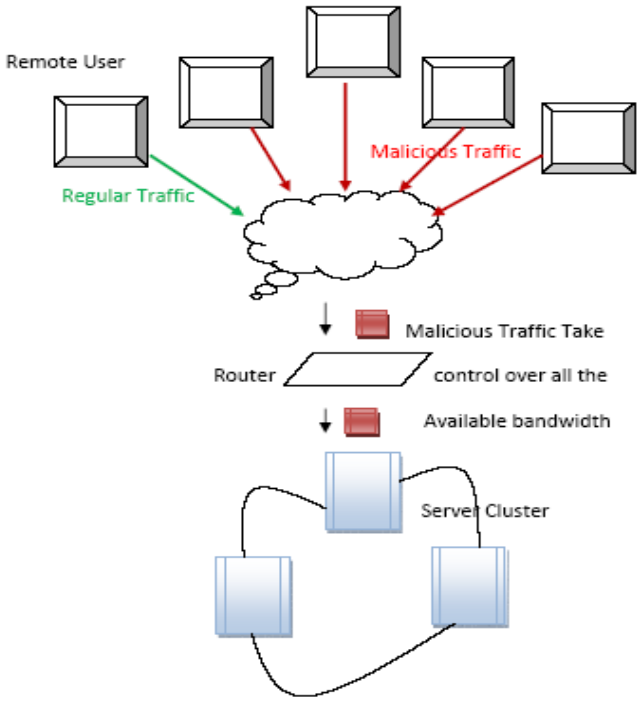


Figure 3: DOS Attack

helps the attacker find which ports are available. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness.At transport layer we have check TCPSYNFLOOD attack shown in figure 5 condition in this we check the threshold value of the arriving packets if the threshold value of the arriving packet are less then predefined threshold value then the packet is normal otherwise packet as infected packets and it will treat as an attacks type.

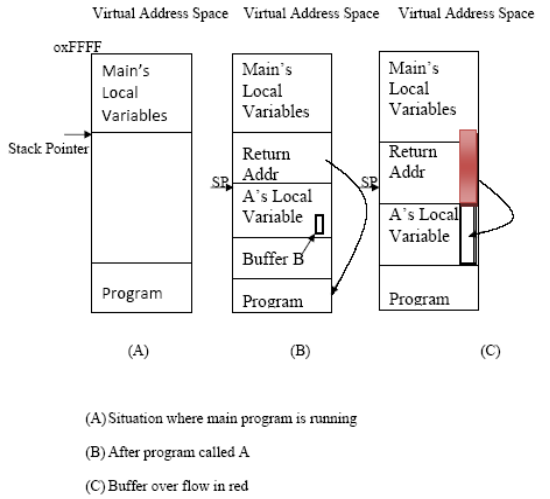


Figure 4: Buffer Overflow attack

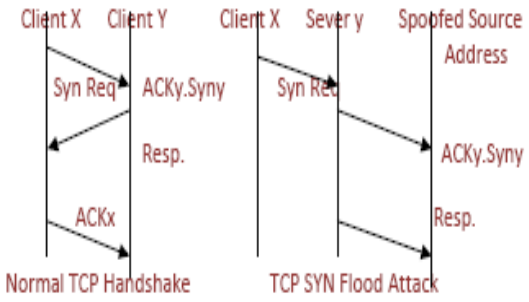


Figure 5: TCPSYNFLOOD Attack

Another transport layer attack where attackers can also consume bandwidth by directing unnecessary traffic to the victim's network. A classic example of this type of attack is the smurf attack. There are two major components in a smurf attack:

- The use of bogus Internet Control Message Protocol (ICMP) echo request packets
- The routing of packets to IP broadcast addresses

Normally, ICMP handles errors and barters control messages. For example, the popular tool called ping uses ICMP. It is used to verify that a specific system on the network is responding. It does this by sending an ICMP echo request packet to such a system. Consequently, it expects the system to return an ICMP echo reply packet. In smurf attacks, ICMP echo request packets are sent to IP broadcast addresses of remote subnets to degrade network performance. Figure 6 illustrates the essentials of smurf attacks. In smurf attacks, usually there is an attacker, an intermediary, and a victim (in this case, a web server). If the network is 192.168.1.0 with a 24-bit subnet mask of 255.255.255.0, the broadcast address will be 192.168.1.255. If the ICMP traffic is sent to the broadcast address, all the systems or nodes on the network will receive the ICMP echo request packets and, consequently, send ICMP echo reply packets in return. Additionally, the intermediary can also become the victim, because it receives an ICMP echo request packet sent to the IP broadcast address of its network. Attackers make this technique successful by using spoofed packets. By doing this, the victim responds with ICMP echo reply packets that consume available bandwidth.

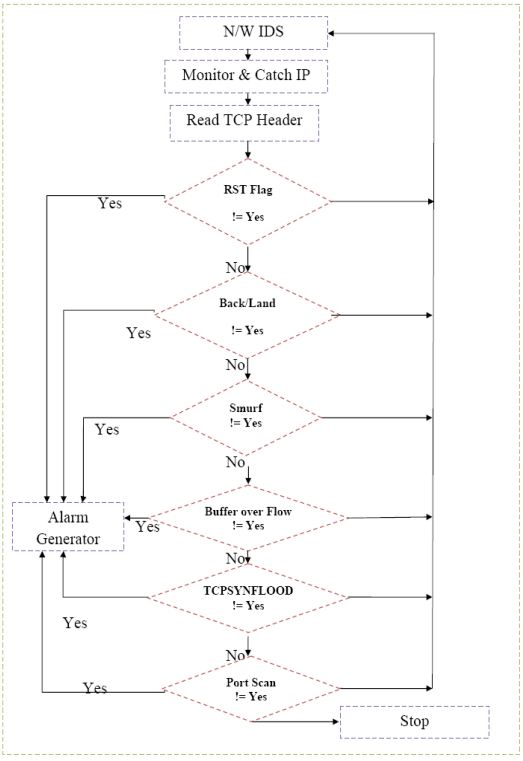


Figure 6: Smurf Attack Example

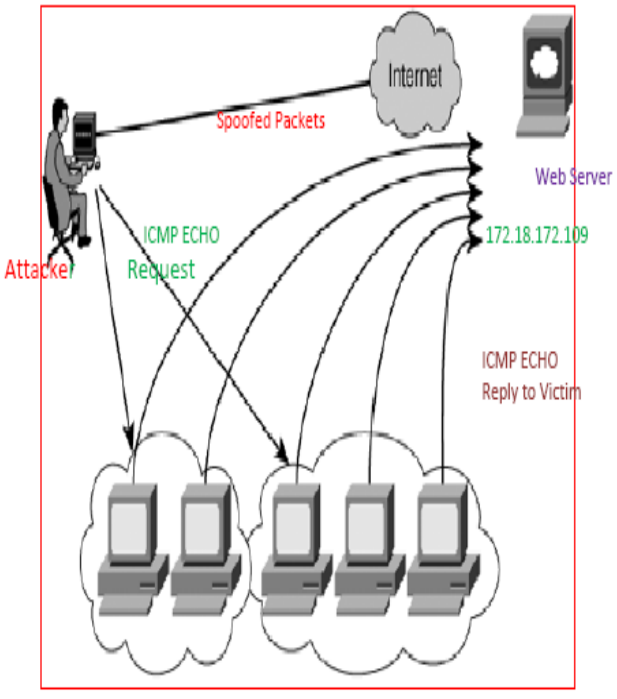


Figure 7: Block Diagram of Proposed NIDS

Figure 8 is showing the block diagram proposed "**Host Based Intrusion Detections System (HIDS)**". In this system we have concentrating only for security log file where security log analyzer will detect attack which is related with system security. As we know that in this log file there are so many values to analyze security of the system but we have concentrate only two value which is already define above.

2.2 Proposed HIDS

Proposed HIDS call security analyzer to check or find attack in local host then it will detect security attack in security event log file. After completing this it will produce results. If any illegal activity find in this log file like un-authorize accessing or login failed then it will go to alarm system for information that this system is suffering from attack.

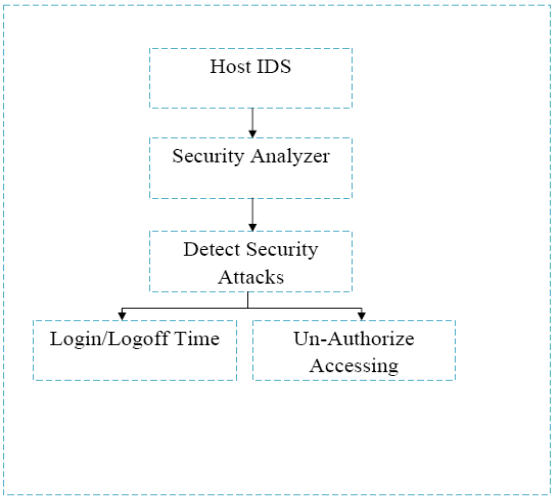


Figure 8: Block Diagram of Proposed HIDS

III. RESULT ANALYSIS

This paper focused on OSI layers attack in NIDS as well as security event log file analyzing attack in HIDS. To detect various type of N/W attacks we have set some parameter like window buffer size for U2R, 5 IP address from same source in 1 second that means face address for DOS, TCP header flag are set RST then abnormal and to detect SYN attack we are using the threshold time interval value of Δ T which will be vary from small to large. So we set Δ T =15 sec, 25 sec and 35 sec and T=1000 millisecond by default. Default value will be use in the absence of actual threshold value. In the host based IDS we have set password to the tested system and defined working time. And we are login with wrong user name and password and also login in wrong time period to capture host based attack. For experiment, proposed system used desktop machine. Configuration of that machine is Intel Pentium ® Dual Core CPU E6700 @ 3.20 GHz 3.19 GHz, 1.93 GB of Ram and Window-XP SP-X (1, 2, and 3). Table 1 is showing abnormal packets which is capturing by the proposed N/W IDS. Table 2 is showing application layer attack. Table 3 is showing transport layer attack for Land and Smurf attacks. Table 4 is also showing transport layer attacks but it is for SYN FLOOD attack. And finally Table 5 is showing security log attack in Host IDS. Proposed system run number of time and results are shown in tables 1 -5 and corresponding Graph 1-5.

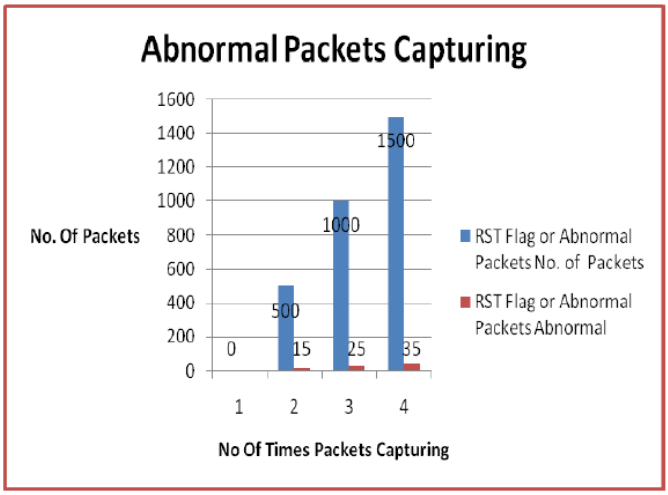
IV. FIGURES/CAPTIONS

Table 1: **RST Flag or Abnormal Packets**

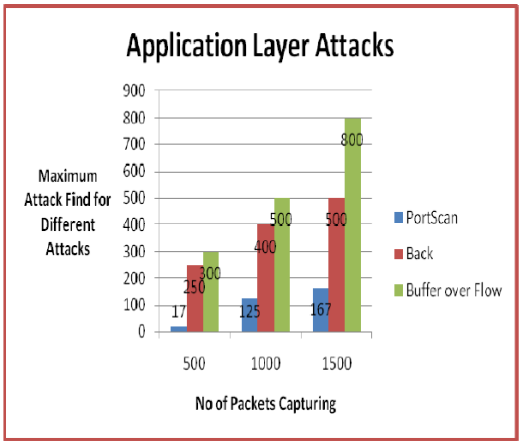
No. of Packets	Abnormal
Presented Results for Attack are in approx	
500	15
1000	25
1500	35

Table 2: Application Layer Attacks

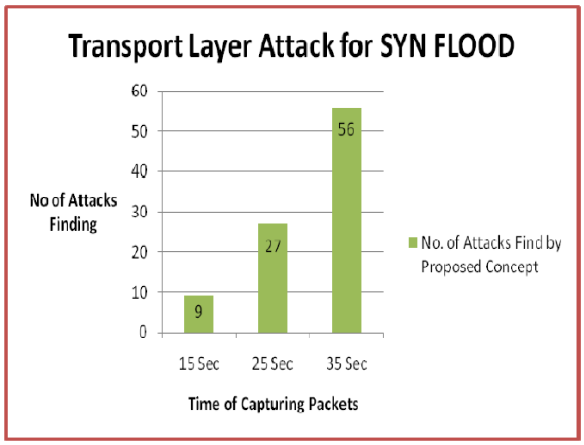
No. of Packets	Port Scan	Back	Buffer over Flow
Presented Results for Attack are in approx			
500	17	250	300
1000	125	400	500
1500	167	500	800



Graph 1: Abnormal Packets



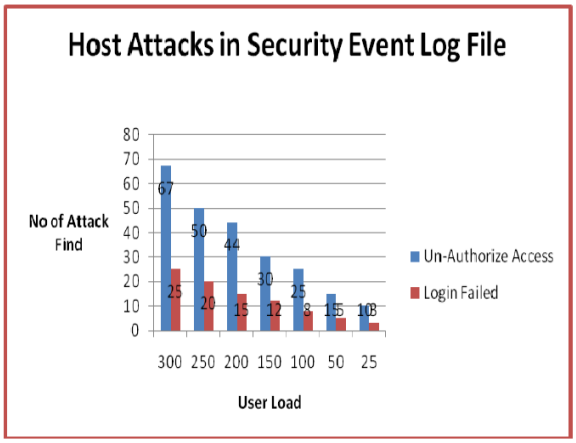
Graph 2: Application Layer Attacks



Graph 3: Transport Layer Attacks for Land and Smurf

Table 5: Host Attack		
Total Events	**Un-Authorize Access**	**Login Failed**
300	67	25
250	50	20
200	44	15
150	30	12
100	25	8
50	15	5
25	10	3

Graph 4: Transport Layer Attacks for SYN FLOOD



Graph 5: Host Attacks

V. CONCLUSION

In this paper, we proposed an IDS system to detect various types of layers attacks like application layer, transport layer and Abnormal packets in N/W IDS and additionally in Host IDS UN-authorize accessing and login/logout failed. The proposed system is providing both type of functionality in one system which is improving overall efficiency of the existing IDS. In future we will we work on network layers protocol and try to find attack on network layers that mean in this layers what type of attack will perform and how we can protect from or prevent them.

References

[1] *Jeevaa Katiravan, C. Chellappan and J. Gincy Rejula Detecting the Source of TCP SYN Flood Attack using IP Trace Back European Journal of Scientific Research ISSN 1450-216X Vol.71 No.1 (2012), pp. 78-84*

[2] *V. Jyothsna, V. V. Rama Prasad and K. Munivara Prasad "A Review of Anomaly based Intrusion Detection Systems" International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, August 2011*

[3] *Asmaa Shaker Ashoor and Prof. Sharad Gore "Importance of Intrusion Detection System (IDS)" International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011 ISSN 2229-5518*

[4] *Firkhan Ali Bin Hamid Ali and Yee Yong Len "Development of Host Based Intrusion Detection System for Log Files" IEEE symposium on business, engineering and industrial application(ISBEIA) langkawi, malaysia 2011*

[5] *Chung-Ming Ou and C.R. Ou "Immunity-inspired Host-based Intrusion Detection Systems" 2011 Fifth IEEE International Conference on Genetic and Evolutionary Computing.*

[6] *Ferdous A. Barbhuiya, Santosh Biswas, Neminath Hubballi and Sukumar Nandi "A Host Based DES Approach for Detecting ARP Spoofing" IEEE Conferences 2011*

[7] *Bin Zeng, Lu Yao, ZhiChen Chen "A Network Intrusion Detection System with the Snooping Agents" IEEE International Conference on Computer Application and System Modeling (ICCASM 2010) 2010.*

[8] *LIN Ying, ZHANG Yan and OU Yang-Jia " The Design and Implementation of Host-based Intrusion Detection System" Third IEEE International Symposium on Intelligent Information Technology and Security Informatics 2010*

[9] *Anuradha and Anita Singhrova A Host Based Intrusion Detection System for DDoS Attack in WLAN IEEE International Conference on Computer & Communication Technology (ICCCT)-2011*

[10] *Chundong Wang, Quancai Deng, Qing Chang,Hua Zhang and Huaibin Wang " A New Intrusion Detection System Based on Protocol Acknowledgement" IEEE 2010*

115] Jin-Tae Oh , Sang-Kil Park, Jong-Soo Jang and Yong-Hee Jeon "Detection of DDoS and IDS Evasion Attacks in a High-Speed Networks Environment" published in IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.6, June 2007

[12] Vera Marinova-Boncheva "A Short Survey of Intrusion Detection Systems" 2007

[13] Moad Alhamaty , Ali Yazdian and Fathi Al-qadasi "Intrusion Detection System Based On The Integrity of TCP Packet" published in World Academy of Science, Engineering and Technology 11 2007

[14] T. S. Sobh "Wired and wireless intrusion detection system Classifications, good characteristics and state-of-the-art", Computer Standards & Interfaces 28, pp. 670-694, Science Direct, 2006.

[15] A. Lakhina, M. Crovella, & C. Diot, Mining Anomalies Using Traffic Feature Distributions. In proce. SIGCOM, Philadelphia,PA. 2005

[16] C. Lui, T. Fu Chung, & T. Ch eung. Agent-based Network Intrusion System Using Data Mining Appr roaches. In Proceedings of the 3rd IEEE International Conference on Information Technology and Applications, Vol.1, pp131-136. 2005.

[17] Moad Alhamaty , Ali Yazdian and Fathi Al-qadasi "Intrusion Detection System Based On The Integrity of TCP Packet" published in World Academy of Science, Engineering and Technology 11 2005.

[18] Douglas J. Brown, Bill Suckow, and Tianqiu Wang "A Survey of Intrusion Detection Systems" 2004

[19] Tatsuya Baba and Shigeyuki Matsuda "A Proposal of Protocol and Policy-Based Intrusion Detection System" published in Systemic, Cybernetics and Informatics volume 2 - Number 3 2004

[20] Douglas J. Brown, Bill Suckow, and Tianqiu Wang "A Survey of Intrusion Detection Systems" 2004

[21] Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", on September 11, 2003.

[22] SANS Institute Staff, Intrusion Detection and Vulnerability Testing Tools: What Works? 101 Security Solutions E-Alert Newsletters. 2001.

[23] Paul Innella Tetrad, "The Evolution of Intrusion Detection Systems", Digital Integrity,LLC on November 16, 2001.

[24] N o r t h c u t t, S. Network Intrusion Detection: An Analyst's Handbook. New Riders, Indianapolis, 1999.

[25] B a c e, R. An Introduction to Intrusion Detection and Assessment: For System and Network Security Management, ICSA White Paper, 1998.

[26] P u k e t z a, N., M. C h u n g, R. O l s s o n, B. M u k h e r j e e. A Software Platform for Testing Intrusion Detection Systems. – IEEE Software, September/October, 1997.

[27] Heberlein, L. etal. "A Network Security Monitor." Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, May 1990, pp. 296-303.

{28] D. E. Denning, "An intrusion-detection model." IEEE Transactions on Software Engineering, Vol. SE-13(No. 2):222-232, Feb. 1987.

[29] Anderson, James P., "Computer Security Threat Monitoring and Surveillance",Fort Washington, Pa., 1980.

[30] http://www.whitehelm.com/intru-det.html

[31] http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

