Research Journal of Recent Sciences _____ ISSN 2277-2502
Vol. **3(4),** 88-94, April **(2014)** *Res.J.Recent Sci.*

Characterizing Strengths of Snort-based IDPS

Ghilman Ahmed, Mehdi Hussain and M.N.A. Khan
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, PAKISTAN

Available online at: www.isca.in, www.isca.me
Received 27th July 2013, revised 1st October 2013, accepted 23rd November 2013

Abstract

The Internet has revolutionized computer networks and the last decade witnessed tremendous expansion in its usage. It provides remarkable opportunities and growth potential for all types of organizations, academia and businesses. Network security is vital for any organization connected to the Internet. Foolproof network security is a key challenge which can be addressed by hardening the network against threats e.g., hackers, malwares, botnets, data thieves etc. Firewalls, antivirus and intrusion detection systems are used to protect the network. Firewall can control network traffic but sole dependence on this type of security measure is not enough. Attackers use open ports such as web server (http) port 80 and POP server port 110 to infiltrate networks. Intrusion detection system (IDS) minimizes security gaps and strengthens security of a network by analyzing the network packets for sifting malicious packets. Snort is renowned as a leader in IDS technology. Snort uses both misuse-based and anomaly-based techniques for capturing malevolent packets. Addition of prevention support in IDS is a step forward as it can help block malicious packets. Real time detection with prevention by Intrusion Detection and Prevention Systems (IDPS) has taken the security of a network to an advanced level by hardening the network against mischievous activities. The objective of this paper is to review the contemporary literature and to provide a critical evaluation of various techniques of intrusion detection and prevention systems. We analyze and identify the strengths and limitations of various techniques used in Snort-based IDPS systems. This paper also highlights the usefulness of IDPS in network security environment.

Keywords: Snort, IDS, IDPS, misuse detection, anomaly detection, intrusion prevention system.

Introduction

Computer networks are backbone of enterprises in the 21st century. Because of financial constraints, corporate and public service activities have shifted much of their services and business activity on the Internet. Common populace has increased its dependence on information technology in their daily work. Organization network systems communicate with other networks through Internet for mutual benefits and sharing of services. These intranets connect together for providing services to users around the world. Financial groups, banks, public service organizations and private business enterprises now communicate with masses worldwide through Internet. This web of resources is helping people in their endeavors to promote businesses. Multi-dimensional Internet opportunities and benefits are the pros of this technology. The security of web is pivotal for World Wide Web and different threat forms and their solutions are suggested by Santosh[1]. Another new technology emerged in networks is based on wireless communication. Like wired connections wireless networks can use a novel technique proposed by Shivlal[2] for performance enhancement and to secure the wireless network communication. The cons are that Internet is full of savvy users, script kiddies and professionally organized hacking groups. These nefarious users are more than willing to act aggressively to steal or destroy data of others either for fun or financial gains. To make network secure from threats, multiple strategies have emerged such as firewall, antivirus, and intrusion detection and prevention systems. An IDS uses signature-based approach to target already known attack signatures, and anomaly-based technique to identify new unknown attacks. Snort IDS is an intrusion detection system which uses signature-based method to detect intrusions.

Firewall allows only for the desired IP addresses and ports to pass traffic through it, but it cannot sense whether the traffic is normal or nefarious one. Therefore, firewall has certain obvious benefits, but it lacks ability to detect attacks. Intrusion detection system on the other hand detects threats and attacks by monitoring the network traffic. When an intrusion activity occurs in a network, an alert is generated by IDS which prompts the network administrator for instigating and action to block or mitigate the attack. Yadav et al.[3] proposed a spiral process model for requirements relating to systems and software. The proposed model enhances the reuse of information through repository, hardens the information security[3]. "Routing protocols in Mobile Ad Hoc Networks" suggested by Baba[4] highlights the importance of Manets and their applications. By using IDS in Manets can overcome the inbuilt limitation in Manets relating to security issues. There are many new techniques and mediums are used to establish communication between hosts. One of the medium come up is in the form of Bluetooth. Arnab et al.[5] proposed one such technique which provides communication application using bluetooth medium.

All the new innovative and emerging communicating mediums are required to be checked for a possible intruding users and malicious software's, which are helpful in intrusive activities. History of intrusion events has proved that only detection is not enough to block the intruders from attacking the networks. Therefore, intrusion detection and prevention system came into existence. IDPS not only report attack events to the administrator but also block them instantly.

The purpose of this paper is to review the literature and provide critical evaluation of IDPS solutions based on snort IDS. Rest of this paper is organized as follows:- Section II provides an elaborated discussion on security threats, their remedies and solutions. Different IDS and their types are also described in this section. Section III presents literature review of from the contemporary literature. Section IV provides critical analysis of different snort based IDS techniques. Finally, Section V summarizes conclusion and future work.

Security Paradigm

This section describes several security paradigms components used to secure networks.

Security Threats to the Networks: Nowadays, numerous security challenges are faced by networks. These are in the form of hackers, malicious viruses, malware, botnets, denial of service attacks, data thefts, insider attacks etc. A remedy to the above mentioned security problems is to harden the network with security enhancing tools and policies. Firewalls and intrusion detection systems are helpful in mitigating security threats if not completely capable of eradicating them.

Firewall: Firewall operates on the gateways to protect the network from outside threats. It analyzes network packets according to the rules defined by the administrator to allow or deny network traffic. Firewalls can allow or block traffic on the basis of IP addresses, host addresses and port numbers. However, firewall cannot analyze the network packets on the basis of signatures. It cannot detect malwares and viruses coming in from the known ports like port 80 and 110. Therefore we need a system which can analyze network traffic to detect malicious activity.

IDS: Intrusion is an act of entering into a network or system forcibly with malicious intent i.e., either to steal information or damage the system. Intrusion detection system sits on the gateways or on the host machines with promiscuous mode to monitor the network traffic. If any malicious traffic is identified, an alert is generated by the IDS, informing responsible person to take action. There are two basic types of IDS, signature-based and anomaly based.

Signature based IDS detects malicious network packets on the basis of known list of attack signatures. This known list is already saved into a database for latter comparison in real time mode. Signature based approach is very effective against known signatures of attacks but lacks in detecting new (or unknown) attacks.

Anomaly based IDS approach uses system profile to detect any anomaly in the data packets. Initially, system is trained with a normal expected traffic and a profile is built with normal system behavior. The trained profile is later on used to detect anomalous activities. Though anomaly detection technique has a high false positive rate, but it is more effective against unknown attacks.

Hybrid based approach combines both the signature-based and anomaly-based techniques to block the malicious network packets. Hybrid approach augments the strengths of both the techniques to overcome their particular drawbacks.

IDPS: An IDS detects attack packets and generates alerts accordingly. It cannot act on its own to block the attacker. Intrusion detection and prevention systems overcome the limitation of IDS by not just detecting the attack, but also inhibiting it from thrusting into the network or system. IDPS works as network based IDS (NIDPS) and host based IDS (HIDPS).

Network intrusion detection and prevention system operates in a network environment to detect and prevent malicious intruders from attacking the network. NIDPS normally works on gateways or at a point where NIDPS can monitor incoming and outgoing network traffic. Malicious network packets are blocked using signature based and anomaly based methods. NIDPS targets the outsider attacks to block them.

Host based IDS performs its operation of detection and prevention for a single host. HIDPS detects abnormal activity in a host by monitoring the logs. Kernel logs and application logs are helpful in determining the attack. Normal attack scenarios can be user rights escalation, unauthorized access to resources and any suspicious activity which does not correspond to normal system operation. HIDPS also keeps a check on the insider attacks happening in a host.

Literature Review

The purpose of this literature review is to highlight the significance of IDPS using snort. In this section, we analyze and identify the strengths and limitations of snort based IDPS using various methods such as signature-based and anomaly-based approaches. We also outline ideas how these different IDPS systems can be further improved.

"Bsnort" proposed by Padmashani et al.[6] is an improved version of snort IDPS which focuses the in-built shortcomings of snort. Proposed approach fills gaps in snort with better algorithm for misuse and anomaly detection. Main improvement is throughput increase and performance enhancement. It minimizes the false alarms rate along with search and match process of packet

strings. The system limitation is that it targets only Transmission Control Protocol (TCP). System needs to counter other protocols e.g., UDP, ICMP, etc. In this system, attack detection is serialized by first matching threat signatures in misuse detection phase. In case of failure in first phase, packets are directed towards anomaly detection module. However, this approach is slow and inefficient. Packets can be fed to both modules simultaneously. This duo processing of packets will be faster, smoother and more effective.

An incident handling and response system which is a customized intrusion detection and prevention solution is suggested by Kalbande et al.[7] The customization is done by combining Snort IDPS with multiple tools namely Tcpdump, Nmap, Tripwire, Clamwin antivirus and Sleuth kit. Numbers of bash shell scripts are included to enhance the functioning and effectiveness of the proposed system. The system strength is that it can be custom made to different threat scenarios. Mixing the tools aggregate the strengths of the response system, making harder for the attacker to break in and do damage to network and system resources. There are some drawbacks in the system as a lot of testing and tweaking is required to be done with different tools configurations. Another problem lies in its customization, because there is no standard configuration of the system is defined. The system can be standardized with particular tools with easy to understand interface for error logging, event correlation and system integration[7].

Saleh et al.[8] proposed a system which used signature based approach to detect attacks, with packet filtering firewall to prevent them. Proposed system used Snort Network Intrusion Detection System (NIDS) which generates alerts when attacks are detected, and transfers those alerts as policy rules in the form of Extensible Markup Language (XML) schema from NIDS to firewall. Firewall uses the XML schema for the creation of incoming and outgoing network traffic rules. Authors suggested that proposed technique will be most effective if servers are positioned in Demilitarized Zone (DMZ). Advantage of this proposed system is that it works best against attacks whose signatures are already known, but lacks ability to detect novel attacks. Known attacks can be blocked instantly as soon as they are detected. Expert administrator is required to analyze the alerts produced by the NIDS. System is expensive because it is much dependent on hardware. The system required a reconfiguration of hardware for XML schema. The proprietary companies can add this support to their products. Technique is also vulnerable to high rate of false positives and false negatives. System can be improved with some modifications for novel attack detection[8].

An approach suggested by alshubhi et al [9] for intrusion detection and prevention system is based on the idea of combining Snort IDS for misuse signature detection and lightweight "FireCollaborator" as anomaly detector. Main theme of the proposed technique is to strike a balance between attack detection rate and good performance. This approach uses extensive information, which is gathered from different data sources to handle multiple threat occurrences. However, proposed idea bears a caveat that it becomes inefficient while synthesizing lot of information from different sources. Human intervention is required to understand the latest collected information about threats and to preempt attacks according to the gathered information. External firecollaborator resources on the premises of an ISP form a ring of anomaly detectors. It catches any anomalous traffic coming into the network. These external anomaly catchers interact with internal network. An in-house solution can be built to end the dependence on outside help, along with automatic response system to avert human dependence. Firecollaborator technique can be applied on a system which is proposed by saleh et al[8], to overcome the deficiency present in the system while detecting novel attacks.

"Traceback-based bloom filter" is suggested by Tang et al.[10] which is capable to protect the network and systems from SYN flooding attacks. SYN flooding attack is a type of DDoS attack which paralyzes the system to respond to requests due to overwhelming the system with fake illegitimate requests. Servers offering any services are the main targets. Authors proposed a bloomfilter to record the traffic statistics. Traffic statistics recorded during TCP session include IP-Time-To-Live (IP-TTL) of SYN packets. The system learning is done in normal traffic mode so that training data will be saved in Bloomfilter for later comparisons. In an event of attack, traffic statistics are matched against standard recorded traffic data. Ill matched packets are dropped during comparisons. The proposed technique uses four Bloom filters for TCP packet data recording and comparisons. The network portion under attack is separated from other traffic to minimize the false positive rate. The proposed approach has limited scope as it addresses only Synchronize and Acknowledgement (SYN-ACK) schemes for attack detection. The suggested idea can be broadened to handle other types of threat scenarios with improved better detection schemes, i.e., FIN, RST, UDP DoS, U2R, R2L etc.

Jianrong[11] suggested a technique of intrusion prevention system by researching the kernel codes of snort and netfilter. The proposed approach of IPS is based on three phases: intrusion detection modal, policy control modal and a firewall. Intrusion detection modal analyze the network packets for a possible attack. In case of an attack, intrusion detection modal generates an alert. Policy control modal has three functions: intrusion detection, policy control and actions manage. To reduce the false positive rate, intrusion control pops an alert if an attack occurs for some specific number of times. Policy control creates a firewall rule for the alert. Action manage process insert the rule into the firewall. The proposed system enhances snort capability to detect more attack packets. However, rules should be created carefully as otherwise a miscalculated rule would degrade performance of the system.

The system proposed by Tuteja and Shanker[12] observed deficiencies in earlier approaches by figuring out the threat

signatures by just analyzing the incoming traffic in a network. The authors suggested an optimization solution for snort based IDPS, which enhances the effectiveness of the IDPS system. If outgoing traffic is also observed along with the incoming traffic, then it acts as a hint about malicious traffic. In such scenario, the proposed system will increase capturing ability of snort IDPS manifolds. The proposed system produces optimum results. The main limitation faced by the system lies in large traffic volume observation. This slows down the system. For better judgments on the network traffic to make right decision, human involvement is required. System can be improved by fine tuning so that fewer alerts are generated. Automating the system with dynamic rule creation and deletion can help further improve the system.

Hou et al[13] observed an obvious limitation in Snort IDPS when it handles an address resolution protocol (ARP) spoofing attack. The authors proposed an ARP detection module plug-in for the pre-processor portion of snort IDPS. Static binding of IP addresses and MAC addresses of network hosts are done in a configuration file to rectify the ARP spoofing problem. The suggested system works only with static entries of IP and MAC addresses. Proposed technique can be further improved with support of dynamic entries of IP and MAC addresses.

Lee and Chiang[14] observed that servers and clients are infected by different malware botnets. These botnets establish connection with their master server over the Internet. The suggested technique detect rogue botnets and block them communicating with external malicious controllers. Botnets use Internet Relay Chat (IRC) protocol for communication. Suggested technique is implemented through code support written in Hypertext Preprocessor (PHP). The code recognizes harmful bots among the legitimate ones. The idea proposed used snort IDS and net filter firewall on Linux operating system. Snort IDS capture packets and logs the information about malicious packets. Abnormality is detected on the basis of multiple malicious bots trying to communicate outside the network or sending response to their master controllers. System analyzes payload of the packets to distinguish the malicious bots. However the system proposed requires specific administrator commands to take action of blocking the malicious bots in the form of firewall rules . The system can be improved with having an automatic firewall rule generation mechanism.

Patil and Mishram[15] proposed a denial of service DoS attack prevention system. The proposed technique uses the flow-based data packets analysis for detecting DoS attacks. There are two units in snort pre-processing engine: protocol based analysis and flow based analysis. In flow based technique, a specific protocol related flow is determined such as protocol name, traffic direction etc. Network traffic is stored and analyzed using statistical and probabilistic theory for setting thresholds to detect DoS attacks. This approach spares the intrusion detection system from processing large amount of data. The system lacks in handling the scenario where attacker uses single packet or some specific number of SYN packets to attack the network. The proposed system can be improved to look for the maliciousness in the network packets by checking protocol headers and content area.

Peng et al.[16] proposed a distinct architecture of design and implementation of network instruction detection system based on snort IDS and network probe tool “Ntop”. Proposed system has three parts: data acquisition module, data processing module and control center. Network traffic data is collected through data acquisition model. Preprocessing and data analysis is performed in data processing module. Data processing also stores alerts in a database and transfers them to the control center. Control center handles input and output command and displays the information on a console. Proposed system performs well in detecting network threats. Suggested system suffers from high failure rate and distorting rate. Future improvement direction will be to minimize the distorting and failure rate.

A cost effective solution is proposed by Naveed et al.[17] which incorporates snort IDS and a router to provide intrusion detection and prevention services to an organization. The proposed system is not only economical, but also is efficient. Snort IDS is coupled with MySQL support to log the alerts generated by snort IDS. Optimized packet capturing rules are applied to generate alerts. Router is connected through telnet to add ACL rules based on snort IDS logs, because snort logs represent potential threat events. The main advantage of the proposed system lies in its effectiveness with ease of implementation. But this system cannot handle the situation in which dynamic IP addresses are used. There is a possibility of wrongly detecting a legitimate host as a threat. In that case, a rule could be added to the router, as otherwise this would cause denial of service situation. Miscalculated rules will need to be removed manually or wait for the system to delete it later. The suggested system can be enhanced through blocking the hardware addresses and malicious packets rather than blocking the IP addresses.

Patil et al.[18] proposed an intrusion prevention system to stop the denial of service attacks. Different DoS attacks are targeted to be stopped by the proposed system like flooding attack, flooding with IP spoofing attack to hide their identity and ping of death. Proposed system developed packet sniffer using ipcap library on java virtual machine (JVM) for platform independence. Libpcap on Linux and winpcap on Windows platform are required to run jpcap. Promiscuous mode is enabled for packet sniffing. Packet sniffer sniffs packets at entry point of the network. Packets entering in the network are scanned to check for attack packets. Alerts are only logged if continuous stream of SYN, ACK, RST and FIN flags is observed for any destination. Based on alerts, rules are created in firewall to block the malicious packets. Proposed system has ability to detect and block different denial of service attacks effectively. The proposed system main disadvantage is its poor accuracy. If some legitimate traffic is detected as a threat, than it means a service is denied.

To enhance efficiency of the snort IDS, Li and Liu[19] used support vector machines (SVM) to intelligently classify the network traffic as legitimate or malicious one. Using support vector machines with snort IDS, system is trained with learning sample data. Based on sample data features, output is produced which is converted into firewall rules to block attack traffic. This proposed system is able to minimize miss rate and error rate of network traffic detection. Using this system in in-line mode can be risky because the system uses only anomaly based approach, anomaly based IDS usually have high false alarm rate. Suggested system can be improved by adding misuse detection module.

Sandip et al.[20] proposed architecture based on hybrid intrusion detection model. The proposed model unites the strengths of misuse and anomaly based technique. The proposed technique uses conditional random fields to enhance the attack detection accuracy of snort IDS. An encrusted layered framework is used for signature based approach to label the network signatures. In anomaly case, volatile data of a system is used to make a profile of a system. Conditional random field is used to detect anomaly in network traffic data. The suggested system needs improvement in anomaly portion to minimize false alarm rate. Active protection should be introduced in the system with a firewall support to block attack packets.

Critical Analysis

In this section we provide a critical review of different approaches in tabulated form.

Table-1
Critical review of IDPS and NIDS techniques

Ref	System/ Type/ Method	Solution	Signature		Anomaly		Strength	Weakness	Suggestive Improvements
			Detection	Prevention	Detection	Prevention			
6.	Hybrid Network IDPS	Performance enhancement through Bsnort Framework.	Yes	Yes	Yes	Yes	Increased throughput. Minimum memory usage. Lesser computation time.	Serialized packet processing in misuse and anomaly phases. Increase packets latency.	Parallel processing of packets can be employed.
7.	Signature based Adaptive IDPS	Set of tools like Sleuth Kit, Snort IDS, Tripwire, Clamwin etc.	Yes	Yes	No	No	Customizable as per user preferences. Improved protection. Provides detailed damage assessment.	Requires lot of testing and tweaking. Only administrator can operate it.	Standard features of different tools should be integrated into one package.
8.	Signature Based IDPS	Integration of Snort IDS and firewall. Data can be exported in XML Form.	Yes	Yes	No	No	Instant action on known attacks. XML integration is platform independent.	Lacks novel attack detection. Only experts can analyze alerts.	Support of anomaly detection would be an added feature.
9.	Hybrid Network IDPS	Snort IDS + FireCollaborator	Yes	Yes	Yes	Yes	Enhanced detection rate. Draws balance between detection rate and traffic flow.	Dependency on external resources. Trained human resource is required to analyze information. Extensive information collection and processing.	Technique could be formulated to work with internal resources.
10.	Anomaly based NIDS	BloomFilter to record stats.	No	No	Yes	Yes	SYN/ACK attack precision and holdback rate is 98%. Low false positive rate.	Limited to only SYN Flooding attack.	Broadened to counter other attacks, .like Smurf and fraggle,U2R, R2L.
11.	Signature based NIDS	Kernel codes of Snort IDS and firewall (Netfilter).	Yes	Yes	No	No	Increased rate of packet analysis. Enhanced performance.	Lack of behavioral anomaly detection. Rule checking is required to minimize false alarm.	Rules can further be fine tuned for getting better results.
12.	Signature based NIDS	Snort IDS with supplementary rule creation.	Yes	Yes	No	No	More secured. Analyzes input and output of the network. Avoids DOS attacks of prevention which devices are vulnerable to it.	Large data to process. Human intervention is required. Manual prevention of attacks.	System can be automated to reduce dependence on human.
13.	Signature based NIDS	Snort IDS with Custom built programs in PHP.	Yes	Yes	No	No	Prevents static ARP spoofing attack.	Cannot handle dynamic ARP spoofing attack.	Attack detection on dynamic IP addresses should be included.

14.	Signature based NIDS	Snort IDS + Net Filter Firewall.	Yes	Yes	No	No	IRC malicious bots can be detected and barred from establishing contact with their master. Analyzes packets to detect maliciousness.	Prevention is manual and awaits administrator for action.	Prevention can be automated with swift response.
15.	Anomaly based NIDS	Statistical and probabilistic approach with information theory.	No	No	Yes	Yes	Normal and abnormal traffic classification. Less data to analyze.	False alarm is typically high in anomaly detection. System become vulnerable if amount of SYN packet attack, increases in number.	Misuse detection approach can be included to analyze data packet header and content portion for checking possible maliciousness.
16.	Signature based NIDS	Snort IDS with Ntop	Yes	No	No	No	Detect bottle neck in network. High rate of threat detection.	High failure and distorting rate. Cannot detect encrypted data packages.	Fail rate and distorting rate can be improved. Threat detection in encrypted packages can be added.
17.	Signature based NIDS	Snort IDS with router to act as firewall.	Yes	Yes	No	No	High availability and instant response. Static IP addresses can be blocked.	Limited to misuse detection. High error rate while detecting DoS attacks. Only Static IP addresses are blocked.	Dynamic IP prevention support and malicious packet prevention can be added.
18.	Signature based NIDS	Rules creation in Snort to detect DoS attacks.	Yes	Yes	No	No	Faster detection. Prevention from different DoS attacks.	Cannot counter mix attacks, like U2R,R2L,etc.	Support for anomaly detection should be added.
19.	Anomaly based NIDS	Support Vector Machine technique.	No	No	Yes	Yes	Minimum error rate and omission rate.	False positive rate is high cannot be used in in-line mode.	Misuse detection should be added.
20.	Hybrid NIDS	Conditional random fields and layered framework for signature based approach	Yes	No	Yes	No	Framework model is used to label network signatures. Conditional random fields method is used to increase attack detection rate.	High False alarm rate.	Minimize false alarm rate. Include Prevention Support.

Conclusion

In this paper, we have critically analyzed various approaches on intrusion detection and prevention systems proposed in the contemporary literature. We only evaluated those approaches in this paper which are based on snort IDS. Snort IDS has limitation in detection of novel attacks and lacks prevention support. "Bsnort" is one such approach which provides better detection and reasonable prevention capability by using Aho-Corasick, Boyer-Moore and K-Nearest Neighbor (KNN) algorithms. Another scheme of IDPS uses iptables firewall with Snort IDS for attack detection and prevention[3], but this model has shortcoming while detecting novel attacks. There are numerous challenges faced by IDPS technology. IDPS can be helpful in mitigating and blocking the attacks entering into the network. Although IDPS technology has come a long way, but still it needs considerable improvements. The further advancements should be focused towards countering new and novel attacks and minimizing false positive rate as well as decreasing computational overheads. This paper expresses diverse approaches and architecture of a number of disparate NIDS with numerous configurations. Various configuration options are used in a network. Special focus has been given to analyze signature-based and anomaly-based approaches. A meticulous consideration was paid towards listing merits and demerits of different NIDS schemes, along with carrying out assessments of various types of attack and vulnerabilities. All NIDS approaches are critically analyzed to make judgment about them. Although IDS itself does not make network hack-proof, but as a whole, IDS improves security of the network making it harder for intruders to break in. We believe this paper could provide basic understanding of IDPS (primarily based on snort IDS) for network security purposes.

Future Work: Nowadays, NIDS systems are facing numerous challenges related to fast and accurate processing of network packets to swift automatic action. The techniques discussed in critical analysis section help us better understand the problems in this field. The solution provided by Santosh[1] is hybrid based, but lacks support of parallel packet processing. As a potential future work, this technique can be improved with multi-processing of packets on signature and anomaly modules simultaneously. Salehi[8] suggested a technique which is solely based on signature detection. Upgrading this technique with anomaly support can further increase detection capability of the system. Patil[15] provided a solution for classification of network packet signatures. This technique can be implemented with approaches suggested in [12, 13] to enhance their efficiency in detection and prevention of novel attacks.

References

1. Santosh K., Technical Problems Especially Web Security Related With World Wide Web, *ISCA J. Engineering Sci.,* **1(4)**, 53-56 **(2012)**

2. Shivlal M., Kumar U S., Performance Analysis of Secure Wireless Mesh Networks, *ISCA J. Engineering Sci*., **1(3)**, 80-85 **(2012)**

3. Yadav S K.., Rizvi S A A., Cybernetics Security Requirements and Reuse for Improving Information Systems Security, *ISCA J. Engineering Sci.*, **1(5)**, 51-54 **(2012)**

4. Baba B D., Routing Protocols in Mobile Ad Hoc Networks, *ISCA J. Engineering Sci.,* **1(6)**, 36-39**(2012)**

5. Arnab P., Tahavranil., Blue-Soft: A Bluetooth based Wireless Secure download and upload station, *ISCS Engineering Sci.,* **2(8)**, 12-17 **(2013)**

6. Padmashani R., Sathyadevan S., Dath D., BSnort IPS, In proceedings of 12th International Conference on Intelligent Systems Design and Applications, Kochi, India, 46-51**(2012)**

7. Kalbande D, Singh M, Incidence Handling and Response System,. *International Journal of Computer Science and Information security*, **2(1)**, **(2009)**

8. Salehi H., Shirazi H., Moghadam R., Increasing overall network security by integrating Signature-Based NIDS with Packet Filtering Firewall, In Proceeding of International Joint Conference on Artificial Intelligence, Hainan Island, 357-362 **(2009)**

9. Alshubhi K., Aib I., Francois J., Boutaba R., Policy–Based Configuration Management Application to Intrusion Detection and Prevention, In proceedings of International Conference on Communication, Dresden, 1-6 **(2009)**

10. Tang H., Xu C., Xi, Luo X., OuYang J., Traceback-based Bloomfilter IPS in defending SYN flooding attack In Proceedings of 5th International Wireless Communications, Networking and Mobile Computing, Beijing, 1-6 **(2009)**

11. Xi J., A Design and Implement of IPS Based on Snort, In Proceedings of 7th International Conference on Computational Intelligence and Security, Hainan, 771-773 **(2011)**

12. Tuteja A., Shanker R., Optimization of Snort for Extrusion and Intrusion Detection and Prevention, *International Journal of Engineering Research and Applications*, **2(3)**, 1768-1774 **(2012)**

13. Hou X., Jiang Z., Tian X., The detection and prevention for ARP spoofing based on snort, In Proceedings of International Conference on Computer Application and System Modeling, Taiyuan, 5137-5139 **(2010)**

14. Lee N-Y., Chiang H.J., The research of botnet detection and prevention,. In Proceeding of International Conference of Computer Symposium , Yang-Kang, Taiwan, 119-124 (**2010)**

15. Patil S., Meshram B.B., Network Intrusion Detection and Prevention techniques for Dos attacks, *International Journal of Scientific and Research Publication,* **2(7)**, **(2012)**

16. Peng Y., Wang H., Design and Implementation of Network Instruction Detection System Based on Snort and NTOP, In Proceedings of International Conference on Systems and Informatics , Yantai, 116-120 **(2012)**

17. Naveed M., Nihar S., Babar M., Network Intrusion Prevention by Configuring ACLs on the Routers, based on Snort IDS alerts, In Proceedings of 6th International Conference on Emerging Technologies, Islamabad, 234-239 **(2010)**

18. Patil S., Meshram B.B., Intrusion Prevention System, *International Journal of Emerging trends in Engineering and Development*, **4(2)**, **(2012)**

19. Li H., Liu D., Research on Intelligent Intrusion Prevention System Based on Snort, In Proceedings of International Conference on Computer, Mechatronics, Control, and Electronic Engineering, Changchun, 251-253 **(2010)**

20. Sandip S., Ajit M., Bapusaheb D., An Improved Approach for Signature Based Intrusion Detection and Prevention, In Proceedings on International Conference in Computational Intelligence, New York, **(2012)**