Implementation of Advanced Intrusion Detection & Prevention System based on Hybrid Approach

[1]Dr.A.B.Pawar, [2]Dr.M.A.Jawale, [3]Dr.D.N.Kyatanavar

[1]Associate Professor, [2]Professor, [3]Principal, Sanjivani College of Engineering, Kopargaon SPPU Pune, India, [1]anil.pawar1983@gmail.com, [2]jawale.madhu@gmail.com, [3]kyatanavar@gmail.com

Abstract **The current scenario in information security shows that attacks are evolving at very fast rate. With the level of automation in attack tools continuing to increase, the expertise requires to breach the security is minimizing, the complexity also increases proportionally, making the tasks of security professional very challenging. These well-travelled pathways make networks more susceptible than ever before and with relative little expertise, hackers have ominously obstructed the networks of leading brands or government agencies. Cyber-crime is also no longer the privilege of lone hackers. Today, discontented employees, unethical corporations, even terrorist organizations all look to the internet as a portal to gather sensitive data and start economic, social and political disruption. To protect, enterprise and government networks against the complete spectrum of threats and susceptibilities, all three methodologies of intrusion detection must be engaged together *i.e.* Signature Detection, Anomaly Detection, and Denial of Service Detection. In addition, Intrusion Detection System (IDS) must do more than just detect attacks. It should do accurate detection to prevent attacks from reaching and damaging critical network resources and data. Without this range of detection methods, many IDS products are simply unused in such cases. It is clear that enterprises and government agencies need to step up and deliver innovative solutions that effectively protect their networks from malicious attacks and misuse. The proposed research work intended for innovative solution to provide computer security with instant prevention strategies with the advantages of data mining techniques and sentiment analysis in the field of intrusion detection system.**

Keywords* — *Anomaly Detection, Cyber Attacks, Denial of Service Detection, Intrusion Detection, Signature Detection

I. INTRODUCTION

Today every business is depending on network. Mostly, because of business needs, enterprises and government agencies have developed their own specialized, complex information networks, incorporating technologies as varied as distributed data storage systems, encryption techniques, Voice over IP (VoIP), remote and wireless access, and web services. These networks have become more penetrable as business partners access services via extranets, customers interact with the network through e-commerce transactions or Customer Relationship Management (CRM) processes and employees tap into company systems through Virtual Private Networks (VPN) [1], [11], [12].

A joint report by CSI and FBI published in year 2010[2],[11], [12] indicates that hacking and malware are the most popular attack methods. Malware was an issue in about half of the year 2010 caseload and was responsible for almost 80 percent of lost data. The most common kinds of malware found in the caseload were those involving sending data to an outside entity; opening backdoors, and key logger functionalities. Ineffective, fragile or stolen credentials continue to cause devastation on enterprise security. Failure to change default credentials remains a matter, particularly in the financial services, retail and hospitality industries [3], [4].

From this, it is clear that enterprises and government agencies need to step up and deliver innovative solutions that effectively protect their networks from malicious attacks and misuse [4]. The proposed research work is intended to research and develop such innovative solution to provide computer security with instant prevention strategies with the advantages of data mining techniques and sentiment analysis in the field of intrusion detection system.

II. IMPACTS OF CYBER SECURITY ON INDIVIDUAL, SOCIETY AND ORGANIZATIONS

The economic consequences of cyber-attacks have many traits. They are different at societal level, organizational level, and individual level too. United States spends a major chunk of resources like cash flow and intelligence on developing the weapons, and training and maintaining large army and military bases. On the contrary, today these

DOI : 10.35291/2454-9150.2019.0237

resources have to be mobilized and shared with information technology (IT) risks and cyber-attacks. This means that along with the security of this country's nationals, now enormous amount of resources have to capitalize in cyber security, as it is a threat of an equivalent magnitude of risk.

An example that involves all the above three levels of impacts, i.e. societal, organizational, and individual levels, is of United States cyber-war with China. Mason in year 2011 explores the People's Republic of China's (PRC) intentions of targeting American companies and government networks [5], [6],[11] Following the example of China, it clearly indicates that instead of spending most of the resources on creating weapons and machinery, the resources have to consume on IT in the security direction, and on the U.S. Cyber Command within the Department of Defense (DOD). These cyber squadron people should provide with all the possible technical support with solid infrastructure at their clearance to defend the American companies and the government networks. If there is a cyber-attack, then the economic impact would be great. The privacy would no longer exist. To exemplify this situation, in 2010, Google Inc. exposed that there was a Chinese origin attack. With the help of spear-phishing techniques, Gmail accounts of the Chinese rebels were accessed. The concerns of such situations led to the acceptance of strict security measures towards the mission of keeping our infrastructure in place and maintain a close-fitting and effective protection safeguard. The problem is that the development of software and installation of infrastructure by employing fiber-optic cable, routers, and servers through Internet Service Providers (ISPs) is not enough. The United States is fronting such cyber-attacks since 1982. Therefore, American leaders are also fronting critical decision-making forecasts with limited information in extremely shortened timeframes while under outbreak.

III. Benefits of Integrating Features OF INTRUSION Prevention SYSTEM (IPS) with IDS

IPSs are a sophisticated class of network security implementation that not only has the capability to sense the presence of intruder and their actions, but also has the ability to avoid them from such attacks. IPS includes the security features of firewall technology and that of IDSs. They can be observed as a successful addition of both security technologies for advanced and bigger security measures. Because IPS chains all the levels of firewall and IDS technologies, they often end up with systems that can operate at all levels of the network stack [6], [7].

IV. Objectives of System

For IDS performance enhancement, main objective of the proposed research work set as: "How to automatically and systematically build adaptable and extensible advanced intrusion detection system using Data Mining techniques and how to provide in-built prevention policies in the detection system so that it will reduce network administrator's system re-configuration efforts and application of sentiment analysis to enhance its performance."

Supplementary, it knows that no single method or technology is the "magic bullet" to assurance protection in contradiction of current or future attacks. To protect enterprise and government networks against the complete spectrum of threats and vulnerabilities, IDS must do further than detect attacks. The review of the state-of-the-art IDSs has modelled the following problems to consider into research [5] [6].

- ***Problem No.1:*** What are the major drawbacks of using single technique based IDSs
- ***Problem No.2:*** Can we integrate various types of IDS?
- ***Problem No.3:*** Is it possible to prevent computer and network resources from data loss and damages with the provision of prevention steps invoked automatically, once known or unknown attack detected in single IDS instead of separate deployment of IPS to do protection?
- ***Problem No.4:*** What are the Data Mining algorithms and which algorithm best suites the intrusion detection application.
- ***Problem No.5*:** How to propose an architecture better than the misuse-based or the anomaly-based intrusion detection taking into consideration the large data set and also the dynamic nature of the network environment and its management by network administrator?
- ***Problem No.6*:** Effective parameters for evaluation of IDSs?
- ***Problem No.7*:** is it possible for implement
- *ting IDS and IPS features in integrated fashion?
- ***Problem No.8*:** Will sentiment analysis study help to deal with false positives and false negatives in the IDS alerts effectively?

The strategy applied for answering these questions is to engage in a study of the literature concerned with similar studies initially, and then to proceed with a theoretical and empirical analysis.

V. Research Methodology

During the study of existing IDS architectures, it perceived that not a single architecture could be made as common since each one is having their own merits and demerits.

DOI : 10.35291/2454-9150.2019.0237

Initially, the theoretical formulation illustrated which gives an overview about the steps carried out while designing the architecture of research work. Subsequently, the mathematical basis for this architectural design introduced and mathematical model is developed. To simplify the functionality details of architecture, it is broken into following modules: Input Data and Data Pre-processing Module, Intrusion Detection Module (including known & unknown attack detection as sub-modules), Data Correlation Module, Intrusion Prevention Module, and Management Console Module for system administrator. Finally, it concludes with description about Evaluation Test Bed for proposed IDS along with evaluation parameter details [5], [6].

VI. Findings of work

Based on this study, the following key findings identified.

- ✓ Intrusion Detection Systems are like burglar alarm for computer system. They detects unauthorized access attempts and other related security events.
- ✓ IDS are first line of defense for computer system and network and have more benefits with its deployment in comparison with traditional firewalls in the network.
- ✓ IPS is additional layer of protection available, but need to be deploy separately in organization network for its benefits.
- ✓ IDS are designed based on either Misuse / Signature-based or Anomaly based intrusion detection techniques and found very rarely mixed-up together in commercial scenarios.
- ✓ By combining the merits of Signature-based IDS and Anomaly-based IDS, it is possible to get effective IDS to cover known as well as unknown attacks at optimum level.
- ✓ Considering today's growth of network traffic and Internet data, existing IDS or IPS data analysis strategies are not enough to detect and cover the maximum classes of intrusions or attacks, so modern technology like Data Mining can help to speed up the operation of IDS/IPS with their huge data handling capabilities [4]. For this, Knowledge Discovery in Database (KDD), Data Mining Algorithms, Assistance of DM in Intrusion Detection, IDS related DM applications are studied.
- ✓ Additionally, it observed that to enhance computational power of any IDS design; one has to concentrate of types of data analysis required by IDS as part of detecting intrusions.
- ✓ In IDS, Data analysis is the process of organizing the various elements of data related to intrusion detection and their inter-relationships to identify any malicious activity. It is studied that intrusion data analysis is divided into four phases namely, Pre-processing, Analysis, Response and Refinement.
- ✓ Data Mining is promising solution to do intrusion data analysis effectively and correctly at each phase of it[2].
- ✓ False positive and false negative are major concerns with any IDS usage, so the introduction of sentiment analysis technique can be possible at the administration stage of IDS to reduce the fake false positives and false negatives.
- ✓ Additionally, it is clear that to implement efficient Intrusion Detection System, one has to understand the intrusion or attack concept, attack models used by attackers, attack types, attack information sources thoroughly.
- ✓ It found that based on attack behavior study, IDSs performance greatly vary if they focus on just identifying major types of attacks in the input data of IDS and does not look after on minority attack detection at the same time in real-world network data traffic.

- “Rome was not built in a day.” If organization is inadequate with financial resources then use of simple single-tiered architecture is best option to develop IDS/IPS architecture. As organization grows, more resources are available, functionalities of intrusion detection and intrusion prevention efforts become clearly visualize, then architecture change is possible.
- KDD Cup 1999 Data set used during the time of proposed system performance evaluation. Another data set found used for IDS evaluation other than KDD Cup 1999 Data Set is the Defcon Capture The Flag (CTF) data set obtained from Defcon competition and convention conducted yearly. This data set has many properties that make it very different from the real world network traffic data expected by user. The differences lie with extremely high volume of attack traffic, the background traffic is unavailable, and the very few number of IP addresses are available in data set. Therefore, other missing network traffic details are in this dataset give the opportunity and the initial decision to use DARPA data set as first choice for IDS performance evaluation. In addition, while handling the real data traffic, it observed that there is always the lack of the information required about the status of the traffic.
- The main aim of implementation details was to make aware the readers about the contribution of the research work and how it is helpful to achieve the objective set for the proposed research work. Before this work, the individual implementations and simulations for signature based and anomaly based IDS detection methodologies

DOI : 10.35291/2454-9150.2019.0237

are studied and are found their merits and demerits. Additionally, identified how the integration of these intrusion detection methodologies is possible and what are the earlier research work carried out in the proposed research work. It found; these methodologies rarely mixed up together. However, the proposed research work integrated these detection technologies altogether by considering the merits of each of the intrusion detection methods. The main advantage of this integration lies in the support of flexibility and extensibility attributes of any IDS development. Because of this integration, the attacks and their maximum attack coverage is possible. Therefore, all major attacks like Probe, DoS, R2L and U2R along with their sub attack types can detected by this module of the developed proposed system.

- It is the system where the immediate response for the detection attack provided with the help of prevention policies provide for the network administrators of the IDS. Therefore, implemented IDS in the research work is advance in this nature and no previous attempt found in sense of IDS and IPS fusion. Also, the given prevention policies are quite flexible for their use, so the user of the system can apply them as per the need to prevent the similar attack penetrations into the host or network of business organization.

- The use of sentiment analysis techniques in intrusion detection field introduced with the theoretical basis to reduce the detected attacks and their signature database volume by removing false positives and it will prevent system administrators from doing unwanted and time consuming attack analysis rather than doing the monitoring and managing the networks more securely.

- So, based on detected attacks, undetected attacks, the percentage of detection and false alarm rate against KDD Cup 1999 data set is calculated. It shown that the percentage of detected attacks by IDS Snort on input data set was 31.28 % and by IDS PHAD, detection rate was 27.27%, whereas proposed advanced IDS got 81.81% of detected attacks as improved one.

- The main reason behind this improved detection rate is the proposed advanced IDS is quite flexible and updating of new attack signature is done instantly, once any undetected attack is reported by the system because of non-existence of signature for the corresponding attack in existing signature database during the detection of attacks.

- However, the percentage of undetected attacks is found less (18%) in proposed advanced IDS over Snort (27%) and PHAD (36%).Based on the percentage of undetected attack, following key factors are identified with respect to IDS performance evaluation.

✓ It sense that, there is huge need to keep updating existing attack database to get efficient performance from IDS and hence, this percentage of undetected attack is another indicator for the attack signature database updates requirement into the IDS after certain time.

✓ Even, from this undetected attack database, there would be opportunity to get new attack signature trends and could help to cover maximum attack types under certain attack class for IDSs.

✓ Researchers always keep focus on detection of known attacks as parameter to evaluate IDS performance. However, percentage of undetected attacks is able to highlight improvement requirement in IDS performance and corresponding attack signature generation for executing IDSs [5],[6].

- The proposed advanced IDS is able to reduce the false alarm rate (11 %) as compared to IDS Snort (43%) and PHAD (70%) over KDD Cup 1999 Data set Test File. This reduction in false alarm rate is significant one because it minimizes unnecessary processing of data from the network administrator point of view, which seems attack prone but normal traffic in real sense. Additionally, it helps to concentrate on more secure actions from the network administrator side rather than keeping them busy in intensive data analysis work, which is always the main objective of intruders to find loopholes to attack on organization information infrastructure during this time.

- The main goal in IDS evaluation is always the requirement for improvement in both precision as well as recall values, so for this purpose the P-Test parameter is used. It is another parameter, which used to compare IDSs based on the trade-off between precision and recall values with respect to attack detection of IDS.

- There is no magic bullet for security. Even, not a single existing intrusion detection technology is able to protect our resources and information infrastructure. There are always loopholes in a certain part of security deployment. However, irrespective of detection methodologies and location specific deployment, all these IDSs are limited with their detection capabilities and hence, provide only single layer of protection. In addition, they are sensitive with characteristics of underlying software infrastructure to cause increase in false positive rate. This drawback causes many IDSs as Maginot of line only. In comparison with firewall, IDSs are superior but without protection for detected attacks, they just become useless. In order to answer this issue, the IPSs introduced but IPSs found protection against specific attack types and there delayed response is of no use [8], [9], [10].

- Today's security need is at very high demand to protect organization's information infrastructure resources and

DOI : 10.35291/2454-9150.2019.0237

data from attackers. On other hand, with little expertise with computer, internet knowledge one can havoc information security network. In addition, it is found that there is need of dual layer of protection i.e. detection plus prevention with cover of all intrusion/ attack detection and quick response from the same system. To cover all spectrums of intrusions i.e. Probe, U2R, R2L and DOS attack classes, the detection methodologies i.e. signature based and anomaly based IDSs are integrated with support for DoS detection too.

- Issue of deployment of IDSs is also resolved with proposed system. It is possible to use at host network and at certain server or agents side too. Since, the proposed IDS can invoke its functionalities of detection of intrusion and immediate response with provided management console which could be used on any platforms or OS running on underlying host, network and at agent or sever. This also support extensibility feature of proposed IDSs which is found very limited with IDS snort, PHAD etc. during the performance evaluation of proposed system.
- The IDS Snort and PHAD cannot give detection performance greater than 50%. As there is no rule generation and their updating facility provided with them. Most of detection was not possible with Snort and PHAD since, there is no generation of instant intrusion rule.

For proposed research, with the rule generation methods, admin can perform quick response task for detection as well as for detection of resources. The IDS Snort and PHAD are slowdown in the performance, as the data traffic needs to be processed before actual use. The IDS Snort has good packet fragmentation and processing capabilities. The PHAD IDS needs packet header attribute values and hence, it requires extensive processing capabilities enhanced with the use of data mining techniques, so it can give better performance with increased volume of data. The proposed research work is experimented on real time as well as offline packet traffic data with selection facility provision for training as well as testing data file [6]. Since, the selection provision for packet feature attribute give flexibility to user to analyze data at various levels like at packet content level, at traffic feature level, and at packet payload level too [9].

VII. Conclusion

This paper has explored the flexibility of collecting information over certain network as well as adoptability for any network system that is more useful and efficient solution than any data had been used before as results of various existing IDSs. This opens multiple opportunities for future exploration and research, and may lead towards more efficient reliable and effective solution in intrusion detection field. An integration of IDS made more efficient and extensible by incorporating more number of individual IDSs and their components with better performances. Along with signature based and anomaly based detection methodologies, denial-of-service based, flow-based, packet-based methodologies can be included for covering maximum attack spectrum with enhanced results.

Multiple prevention mechanisms introduced in this work as if drop packets, log packets, configure firewall settings, terminate session, etc. These strategies can be increased and adopted properly in any IDS as per the response need in future work for better security.

Acknowledgment

We would like to thank Sanjivani Management, Kopargaon for providing necessary facilities for proposed research work.

References

[1] A.B.Pawar, M,.A.Jawale, D.N.Kyatanavar, https://research.ijcaonline.org/volume106/number13/pxc3899853.pdf

[2] CSI and FBI, “CSI & FBI Report 2010”, 2010, pp.1-2.

[3] Muamer N. Mohammad, Norrozila Sulaiman, Osama Abdulkarim Muhsin, “A Novel Intrusion Detection System by using Intelligent Data Mining in Weka Environment”, Science Direct, Procedia Computer Science ,2011, pp. 1237–1242.

[4] Rezk, H. Ali, M. El-Mikkawy and S. Barakat , “Minimize the false positive rate in a database intrusion detection system”, International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 5, 2011,pp.29-38.

[5] S.Sathya Bama, et al. , “Network Intrusion Detection using Clustering: A Data Mining Approach”, International Journal of Computer Applications (0975 – 8887) Volume 30– No.4, 2011,pp.14-17

[6] Adeeb Alhomoud, Rashid Munir,Jules Pagna Disso,Irfan Awan,A. Al-Dhelaan, “Performance Evaluation Study of Intrusion Detection Systems”, Procedia Computer Science ,2011,pp.173–180.

[7] Hesham Altwaijry, Saeed Algarny, “Bayesian based intrusion detection system”, Journal of King Saud University – Computer and Information Sciences, 2012,pp. 1–6.

[8] A.B. Pawar, D.N.Kyatanavar, M.A. Jawale, Advanced Intrusion Detection System with Prevention Capabilities, International Journal of Computer Applications (0975 – 8887) Volume 106 – No. 13, November 2014, pp.17-24.

[9] A.B.Pawar, M.A.Jawale, D.N.Kyatanavar, “Fundamentals of Sentiment Analysis: Concepts and Methodology, ” Chapter in Sentiment Analysis and Ontology Engineering part of Studies in Computational Intelligence book series (SCI, volume 639), 2016, pp. 25-48

[10] Sachin B Jadhav, Anil B Pawar, Design and “Development of Hybrid Intrusion Detection System For Wireless Sensor Network,” In Vol-3 Issue-1 2017 IJARIIE-ISSN (O)-2395-4396, 2017, pp.148-151.

[11] A.B.Pawar, M,.A.Jawale, D.N.Kyatanavar, https://research.ijcaonline.org/icrtet/number2/icrtet1316.pdf

[12] https://shodhgangotri.inflibnet.ac.in/bitstream/123456789/1000/1/1.introduction.doc

DOI : 10.35291/2454-9150.2019.0237