International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Smart Network Intrusion Detection System

Kishor Shirke[1], Akshay Salve[2], Samir Shelke[3], Vrushali Bhamare[4]

[1-3]B.E.Student, Department of Computer Engineering, Shivajirao S. Jondhale College of Engineering, Dombivli East, Thane, Maharashtra 421201, India.
[4]Asst. Professor, Department of Computer Engineering, Shivajirao S. Jondhale College of Engineering, Dombivli East, Thane, Maharashtra 421201, India.

Abstract:- *This paper describes the novel's method of detecting dangerous network traffic using neural input networks that should be used in deep package testing programs. Test results using a variety of network path data (dynamic link library, files, and selection of various other files such as logs, and text scripts) and malicious shellcode files found for cyber bullying and risk exploitation have proven to be an art. The proposed input is able to distinguish between a network and a network. The construction of the proposed input network achieves an average accuracy of 99%, the central area below the receiver of 0.99, and a standard value of less than 1% with 10 repetitive verifications. This indicates that the proposed separation process is robust, accurate, and precise. The novel's method of detecting malicious traffic proposed in this paper has the potential to significantly improve the use of intrusion detection systems used in conventional neural network analysis and network of cyber-physical systems such as smart-grids.*

***Key words*: Machine learning, Access plans, Computer security, Artificial intelligence.**

2. INTRODUCTION

Increased attacks on computer networks and the need for automatic detection. Internet and computer programs have raised many security and privacy issues. Explosive use of networks for many reasons e.g. internet, wireless networks, cloud computing. As a result, vicious attacks on networks have increased year on year. You need to customize the systems that receive this attack. Based on known attacks. Network Access Programs are essential to modern computer infrastructure to help monitor and identify unwanted and dangerous network traffic (such as unauthorized access to the system or malicious systems). Many NIDS activities have been signed, where specific rules have been set to determine what affects network vulnerability by monitoring patterns on that road. While such schemes are most effective at known threats, natural disasters fail naturally when the detection of an unknown attack or known attack is transformed around those rules.

2. LITERATURE SURVEY

In a paper entitled 'Intelligent Intrusion Detection System Based On Artificial Neural Network' by 'Jian Li, Guo-Yin Zhang, Guo-Chang Gu', they aim to design, implement and test an intelligent Intrusion System based on artificial neural network which can quickly detect attacks, whether they are known or not. In this program, neural networks are used to learn the behavior of ordinary users to create network traffic that contains only information about normal users. When the study is complete, the system is tested with network traffic that contains both attacks and standard data. A built-in computer network designed to monitor system performance. In the test, the effectiveness of the program has been compared with other research activities and the results in the tests are very promising.

In a paper entitled 'Intrusion Detection using Neural Network Committee Machine' by 'Alma Husagic-Selman, Rasit Koker, Suvad Selman', they say that the detection of intrusion plays an important role in modern computer and communication technology. It is therefore very important to design an effective Intrusion Detection System (IDS) system that is both low, False Positive Rate (FPR) and False Negative Rate (FNR), but high precision detection. To that end, the paper proposes IDS for the Neural Network Committee Machine (NNCM). The NNCM IDS consists of an Input Reduction System based on Principal Component Analysis (PCA) and an Intrusion Detection System, represented by a three-level committee, each based on the Back-Propagation Neural Network. To download FNR, the system uses Offline System Update, which updates networks when new attacks are introduced. The plan shows a 99.8% attack recovery success

In a paper entitled 'Deep Learning Approach for Intelligent Intrusion Detection System' by 'Vinayakumar R, Mamoun Alazab, Soman Kp, Prabaharan Poornachandran, Ameer Al-Nemrat and Stitalakshmi Venkatraman', they said that electronic learning methods are widely used to improve the IDS) to detect and differentiate cyber-attacks at network level and in a timely and automated manner.

However, there are many challenges as malicious attacks are constantly evolving and occur at very high rates that require a serious solution. There are various malware databases available publicly for research into the cyber security community. However, no available research has shown a detailed analysis of the performance of various machine learning algorithms in the various public databases. Due to the instability of malware by continuous attack methods, publicly available malware data sets will be systematically reviewed and branded. In this paper, a deep neural network (DNN), a type of deep learning model tested to develop a flexible and effective IDS to detect and differentiate unexpected and unpredictable cyber-attacks. The ongoing changes in network behavior and the rapid evolution of attacks make it necessary to examine various data sets generated over the years using static and dynamic methods. This type of study helps identify the best algorithm that can be effective in detecting future cyber-attacks. Complete testing of DNN tests and other classical classification classifiers are displayed in a database of various public malware. Appropriate network parameters and DNN network topologies are selected according to hyper parameter selection methods with Database KDDCup 99. All DNN tests are conducted up to 1,000 epochs at a reading level varying in grade [0.01-0.5]. The DNN model that works well in KDDCup 99 is used in other data sets such as NSL-KDD, UNSW-NB15, Kyoto, WSN-DS and CICIDS 2017 to make the measurement mark. Our DNN model learns the representation of the abstract and high-level IDS data by transferring it to many hidden layers. Through complex experimental testing it is confirmed that DNNs perform better compared to classical machine learning classifiers. Finally, we propose a scary and hybrid DNNs framework called Scale-Hybrid-IDS-AlertNet (SHIA) that can be used in real time to effectively monitor network traffic and host-level events to strictly detect cyber-attacks.

In a paper entitled 'High Performance Adaptive System for Cyber Attacks Detection' by 'Myroslav Komar, Volodymyr Kochan, Lesia Dubchak, Anatoliy Sachenko, Vladimir Golovko, Sergei Bezobrazov, Ihor Romanets', say today, computer security protection cyber-attacks are an important and urgent issue. Special software is used to protect computer systems from cyber-attacks. However, these days, most malware can compete with a lot of anti-virus software. Therefore, this software is at risk of intrusion. App activities can be captured during an attack. This prevents detection of identity and malware by special software. In addition, malware can compromise software that works specifically, track its activity, detect malicious processes, change settings in the system register, and so on. According to the techniques used, experts describe four basic types of network attacks: denial of service attacks, user-to-root attacks, remote and local attacks and investigative attacks, and a few particles of these attacks. Let us briefly consider these species. Denial Service (DoS) (or service distribution) attacks are considered network attacks on computer programs where the system can no longer answer a user's question and provide access to users. This attack is characterized by the production of large amounts of traffic leading to overloading and server blocking. DoS Attack contains six types of network attacks: back, earth, Neptune, pod, smurf and teardrop.

3. Software Development

The design of the software provides an overview of the software, the interaction between each component and the advanced design of the software applications. However, various descriptions of software development are available by a distributed program. The following are some of the most quoted descriptions of software development:

• Bass, Clements, and Kazman, 1998: A software program for a program or a computer program is a structure or structure of a program, including software components, the external features of those components, and the relationships between them. With "external" features, we refer to what other components consider in part, such as the services provided, performance features, error management, shared resource usage, and so on.

• Garlan and Perry, 1995: The structure of system components, their relationships, and the principles and guidelines that govern their formation and evolution over time.

• Garlan and Shaw, 1993: ... apart from algorithms and data computation frameworks. A simple software design showing the key element of IDS.

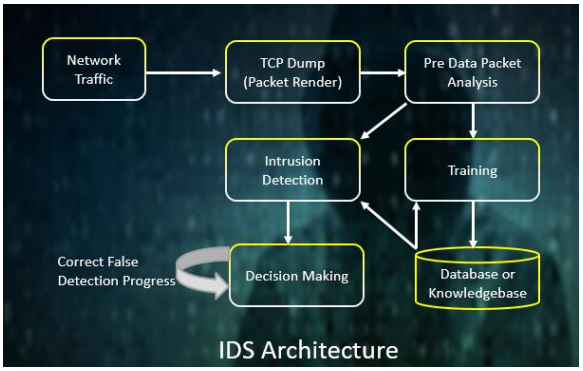

Fig -1 IDS Architecture

4. PROPOSED SYSTEM

Finding shellcode within complex network traffic poses many challenges to network access systems due to low code (usually machine code), small size, and common exploit environment. This is even more complicated to see that, in signature-based signature methods, binary patterns in the shellcode are usually more visible. Inseparable from many other types of malicious network traffic.

The work presented was inspired by that of the authors working as a network security coordinator for the UK's largest online retailer. Using standard network access tools such as Snort and Sguil to provide event analysis of NIDS alerts produces a high level of false positives - many of these warnings are generated by legitimate binary and image files. On the other hand implementing the same on our model makes it the replica of the main model with many additional Neural Network Technologies considering the integrity and reliability of our model.

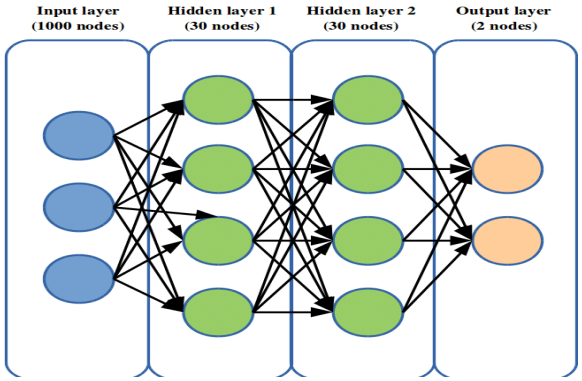

Fig-2 Final design of artificial network.

The byte rate data from the used network traffic data set was converted to total feeds for the neural input network. Care was taken to avoid the "magical numbers" that are common at the beginning of files, as this can be tricky enough to detect and detect (especially when designing a bound shellcode). 1000 bytes of aggregated data are extracted and used as an input to ANN (using zero padding where required). Preliminary testing and viewing of data showed specific patterns within different file types, although there were significant differences between files of the same class.

The ANN of these tests was performed using the MATLAB (2016b) Neural Network Toolbox [21]. The excellent ANN structure was detected by a grid search process, with an excellent (depending on the precision) of the ANN which is found to be a multi-layer perceptron (MLP) with two 30-layer secreted hidden neurons each. The primary model created works with 2-layer cross integrity model just to ensure integrity for small datasets and later on developing a massive defensive algorithm. The usefulness of the ANN structure was used for double 10-point verification to test the composition of the separation.

5. FLOWCHART

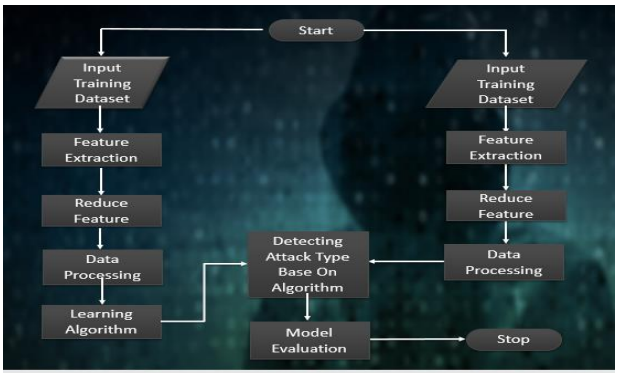

Fig -3 SNIDS Flowchart

6. Result

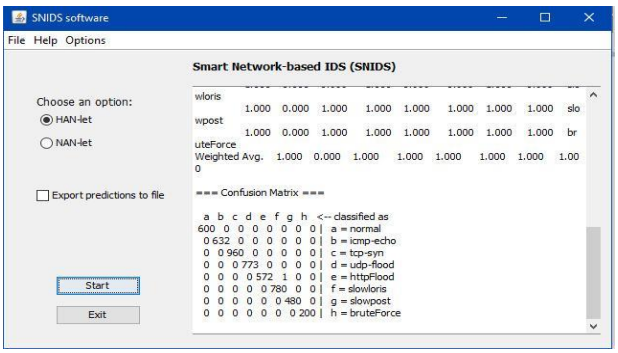

Fig –4 Result Confusion Matrix.

7. CONCLUSION

The smart access detection system described in this paper greatly improves the performance of signature-based methods using neural network fragmentation to identify shellcode patterns in network traffic. The research presented in this paper describes an online way to find shellcode patterns within data using CNN. Finally here we look at systems for getting real-time network access and testing real-time network data, with real-time live network traffic and active development.

8. REFERENCES

1) I.Access Programs - Wikipedia URL: http://en.wikipedia.org/wiki/Intrusion-detection_system accessed October 03, 2009
2) II. Log in and out John McHugh, Alan Christie, Julia Allen Software Engineering Institute, CERT Coordination Center URL: http://www.cs.virginia.edu/~jones/IDS-research/Papers.html accessed at October 05, 2009
3) III.Properties https://www.researchgate.net/figure/4-Basic-architecture-of-intrusion-detection-system-IDS_fig2_226650646#:~:text=This%20chapter%20provides%20the%20overview,them%20for%20signs% 20of% 20intrusions.reached on October 01, 2009
4) IV. What is a network intervention program? URL: https://www.sciencedirect.com/topics/computer-science/network-based-intrusion-detection-system accessed on Oct 01, 2009
5) V. H.-J. Liao, C.-H.R. Lin, Y.-C. Lin, K.-Y. Tung, Intrusion Discovery System: Complete Review, J. Netw. Computer. Application 36 (1) (2013) 16–24.
6) VI. UJM Vidal, A.L.S. Orozco, L.J.G. Villalba, a standardized method of correction of warning nids based on anomalies, IEEE Latin Amer. Trans. 13 (10) (2015) 3461-3466.
7) VII. W.S. McCulloch, W. Pitts, A reasonable number of wet ideas in sensory functions, Bull. Statistics. Biophys. 5 (4) (1943) 115–133