Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Snehal Chincholkar, IJPRET, 2014; Volume 2 (9): 895-900 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW ON UNSUPERVISED NETWORK ANOMALY DETECTION

SNEHAL P.CHINCHOLKAR[1], PROF. P.D.GAWANDE[2]

1. Student, M.E(Digital Electronics), Sipna college of engineering and technology, Amravati Maharashtra, India.
2. Associate Professor, Department of Electronics and Telecommunication, Sipna college of engineering and technology, Amravati Maharashtra, India

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: We always define communication as transfer of information from source to destination. But when there are more than on source and destination in existence, the main question arises about security. Today number of internet users is tremendous due to this large research work is going on making the communication of internet users as safe as possible. In this paper I have made a sincere try to provide a review of technique for intrusion detection that will be proved as milestone in NIDS i.e. Network Intrusion Detection Systems. In this paper I am going to discuss approach for intrusion detection without having any previous knowledge about that intrusion or we can say abnormality. So this approach will provide an online technique of UNADA (unsupervised network intrusion detection) by combining the concept of clustering and outlier detection.

Keywords: Intrusion Detection Systems, Artificial Intelligence, Network Security.

PAPER-QR CODE

Corresponding Author: MS. SNEHAL P.CHINCHOLKAR

Access Online On:

www.ijpret.com

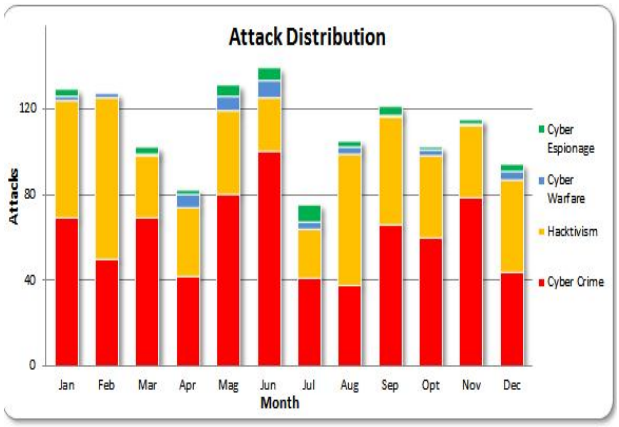
How to Cite This Article:

Snehal Chincholkar, IJPRET, 2014; Volume 2 (9): 895-900

INTRODUCTION

An intrusion detection system (IDS) is software that automates the intrusion detection process If we analyze the network attack detection systems they are categorized into two basic parts one is misuse detection that means detecting the attack which is previously known and another is anomaly detection which means that detection of such anomalies which are not previously happened.

Objective of my paper is to detect such attacks and then try for some filtering rules so that these attacks may not get repeated in future. Here in this paper I have given the review of such techniques those are used for online intrusion detection. There are different types of attacks as Denial of Service attacks (DoS) Distributed DoS (DDoS), network/host scans, and spreading worms or viruses while detecting such attacks the unsuperwised intrusion detection system detect unknown attacks also. The statistics of network attack in the year 2012 is as given in following diagram. This tremendous measure of attack is only the motivation for the work in the area of network security.



I. LITERATURE REVIEW

After studying various papers, the technologies implemented were found to be as follows:

In UNADA: Unsupervised Network Anomaly Detection using Sub-Space Outliers Ranking, Pedro Cases, Johan Mazel, and Philippe Owezarski stated that the principal challenge in automatically detecting and analyzing network attacks is that these are a moving and ever-growing target. Taxonomy allows for previous knowledge to be applied to new attacks as well as providing a structured way to view such attacks. The proposed taxonomy aims to create categories that enable this to occur easily so that similarities between attacks can be highlighted and used to combat new attacks. It uses exclusively unlabeled data to detect traffic anomalies, without

assuming any particular model or any canonical data distribution, and without using signatures of anomalies or training. Despite using ordinary clustering techniques to identify traffic anomalies, UNADA, an Unsupervised Network Anomaly Detection Algorithm avoids the lack of robustness of general clustering approaches, by combining the notions of Sub-Space Clustering, Density-based Clustering, and multiple Evidence Accumulation. [1].

In 2003,M. Thottan and J. Chuanyi, proposed A non-exhaustive list of methods that include the use of signal processing techniques (e.g., ARIMA, wavelets) on single-link traffic measurement in "*Anomaly Detection in IP Networks*" . In this, authors proved that signal processing technique is effective at detecting several network anomalies use a single-linkage hierarchical clustering method to cluster data from the KDD'99 data-set, based on the standard Euclidean distance for inter-patterns similarity. Paper concludes that By improving the capability of predicting impending network failures, it is possible to reduce network downtime and increase network reliability. Rigorous statistical analysis can lead to better characterization of evolving network behavior and eventually lead to more efficient methods for both failure and intrusion detection.[2]

In 2005 in "*Combining Multiple Clusterings Using Evidence Accumulation*", A. Fred and A. K. Jain basically measure the separation between clusters, relative to the total variance within each cluster. The vast majority of the unsupervised detection schemes proposed in the literature are based on clustering and outliers detection. The paper proposed a simple framework for extracting a consistent clustering, given the various partitions in a clustering ensemble. According to the EAC concept, each partition is viewed as an independent evidence of data organization, individual data partitions being combined, based on a voting mechanism, to generate a new *n £ n*similarity matrix between the *n* patterns. The data partition of the *n* patterns is obtained by applying a hierarchical agglomerative clustering algorithm on this matrix. [6]

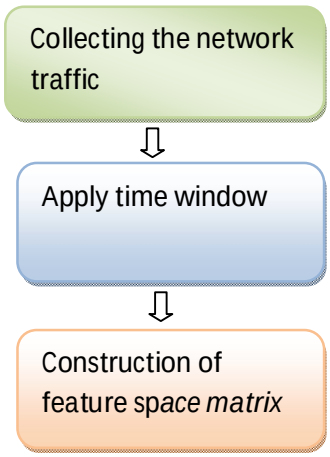
Intrusion detection is an important area of research. Traditionally, the approach taken to find attacks is to inspect the contents of every packet. However, packet inspection cannot easily be performed at high-speeds. Therefore, researchers and operators started investigating alternative approaches, such as flow-based intrusion detection. In that approach the flow of data through the network is analyzed, instead of the contents of each individual packet. The goal of this paper is to provide a survey of current research in the area of flow-based intrusion detection. The survey starts with a motivation why flow-based intrusion detection is needed. The concept of flows is explained, and relevant standards are identified. The paper provides a classification of attacks and defense techniques and shows how flow-based techniques can be used to detect scans, worms, Botnets and Denial of Service (DoS) attacks.[7]

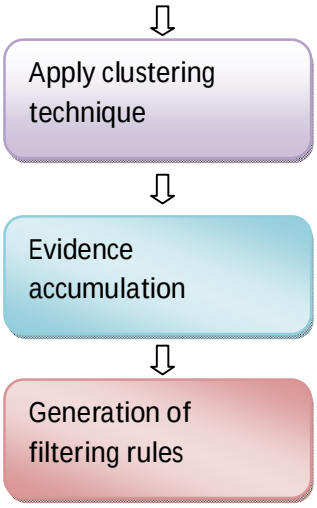
" Steps towards Autonomous Network Security: Unsupervised Detection of Network Attacks" published by Pedro Casas Johan Mazel and Philippe Owezarski in 2011 allows to detect new previously unseen network attacks, even without using statistical learning. By combining the notions of Sub-Space Clustering and multiple Evidence Accumulation, the algorithm avoids the lack of robustness of general clustering approaches, improving the power of discrimination between normal-operation and anomalous traffic. Paper shows how to use the algorithm to automatically construct signatures of network attacks without relying on any kind of previous information. Paper claims that such an approach can be used do devise autonomous network security systems, in which the SSC-EA-based algorithm runs in parallel to any standard security device, producing specific signatures to unknown anomalous events. [8]

II. SYSTEM DESIGN

The methodology for unsupervised is overviewed in the following flow chart. The process starts from capturing the network traffic and converting the particulars into the log file. For creation of log file I am using Network Active PIAFCTM. Network Active PIAFCTM is a network data capturing utility that provides both packet capturing and HTTP (Web) based file capturing. This can allow you to see the data coming in from- and going out to- your computer, such as instant messages, e-mails, and Web pages.

In the beginning work starts with data Gathering and documentation required. Once the required data is gathered next job is to create log file and find out maximum data flow. After this we will apply sliding time windowing & aggregation process for traffic flow.[1]. In the very next step we will create feature space matrix and apply clustering algorithm required trace back outlier in feature space matrix and log file. At last we will use traces data to create signature for anomalous flow and updated the signature table & signature table can be use for online detection of anomalous flow.





Flow chart for methodology

1. Detecting Anomalous Time Slot:

Initially traffic is captured and packet are analyzed by aggregating them in multi resolution flow. On the top of these flow, different time series is built. And anomalous change is defined by change-detection algorithm based on time-series analysis.

2. Determining degree of abnormality:

There is the use of robust clustering algorithm like Sub-Space Clustering (SSC) , Density-based Clustering , and Evidence Accumulation Clustering (EAC) as combination of these approaches for providing traffic structure.[8] This traffic

structure are used as the evidence for determining by how much degree the traffic is not normal. thus the output of second stage are outlying flow.

3. Declaring anomalies:

Using a simple threshold detection approach, outlying flow which are top ranked are flagged as anomalies.

III. CONCLUSION

In this paper I have revised the different techniques used for network intrusion detection. As this area of detecting the unsupervised network attack is very vast the large research work has been done on this serious issue so I have made a sincere try to collect the work done by different people in this area and I have proposed the new intrusion detection system which can

be used for detection of network attack in online basis. This system will be proved as milestone in designing NIDS that is software used for detection of network attack.

V. REFERENCES

1. Pedro Casas, Johan Mazel and Philippe Owezarski," *UNADA: Unsupervised Network Anomaly Detection using Sub-Space Outliers Ranking"*, UPS, INSA, INP, ISAE; LAAS; F-31077 Toulouse, France.

2. Portnoy, E. Eskin, and S. Stolfo, "*Intrusion Detection with Unlabeled Data Using Clustering*", in Proc. ACM DMSA Workshop, 2001.

3. M. Thottan and J. Chuanyi, "*Anomaly Detection in IP Networks*", in IEEE Trans. Sig. Proc., vol. 51 (8), pp. 2191-2204, 2003.

4. Rui Xu, Student Member, IEEE and Donald Wunsch II, Fellow, IEEE, *"Survey of Clustering Algorithms",* IEEE TRANSACTIONS ON NEURAL NETWORKS, VOL. 16, NO. 3, MAY 2005

5. S. Hansman, R. Hunt "*A Taxonomy of Network and Computer Attacks*",in Computers and Security, vol. 24 (1), pp. 31-43, 2005

6. A. Fred and A. K. Jain, "*Combining Multiple Clusterings Using Evidence Accumulation*", in IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 27 (6), pp. 835-850, 2005

7. Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller," *An Overview of IP Flow-Based Intrusion Detection*", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 12, NO. 3, THIRD QUARTER 2010.

8. Pedro Casas , Johan Mazel, and Philippe Owezarski *," Steps Towards Autonomous Network Security: Unsupervised Detection of Network Attacks ",* IEEE 2011 .

9. Pedro Casas, Johan Mazel, and Philippe Owezarski, CNRS and Université de Toulouse," *Knowledge-Independent Traffic Monitoring: Unsupervised Detection of Network Attacks*", IEEE Network January/February 2012