International Journal of Information Technology and Management

Vol. V, Issue No. I, August-2013, ISSN 2249-4510

NETWORK INTRUSION DETECTION USING DATA MINING

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. V, Issue No. I, August-2013, ISSN 2249-4510

Network Intrusion Detection Using Data Mining

Praveen Dutt

Research Scholar, Sai Nath University, Ranchi, Jharkhand

Abstract – Network Intrusion detection has a critical section of network management because of the number of attacks persistently threaten our computers. Network intrusion detection systems are limited and do not provide a complete solution for the problem. They search for potential malicious activities on network traffics; they sometimes succeed to find true security attacks and anomalies. However, in many cases, they fail to detect malicious behaviours or they fire alarms when nothing wrong in the network.

Keywords: Network, Intrusion, Internet

----------♦----------

INTRODUCTION

An Intrusion Detection System is an important part of the Security Management system for computers and networks that tries to detect break-ins or break-in attempts. Internet is using in social networking, healthcare, e-commerce, bank transactions, and many other services. These Internet applications need a satisfactory level of security and privacy. On the other hand, our computers are under attacks and vulnerable to many threats. There is an increasing availability of tools and tricks for attacking and intruding networks. An intrusion can be defined as any set of actions that threaten the security requirements (e.g., integrity, confidentiality, availability) of a computer/network resource (e.g., user accounts, file systems, and system kernels) [1, 2]

REVIEW OF LITERATURE -

Misuse IDS suffer from a number of major drawbacks, first, known intrusions have to be hand coded by experts. Second, signature library needs to be updated whenever a new signature is discovered, network configuration has been changed, or a new software version has been installed [3]. Third, misuse IDS are unable to detect new (previously unknown) intrusions that do not match signatures; they can only identify cases that match signatures. Thus, the system fails to identify a new event as an intrusion when it is in fact an intrusion, this is called false negative. On the other hand, current anomaly detection systems suffer from high percentage of false positives. An additional drawback is that selecting the right set of system features to be measured is ad hoc and based on experience. A common shortcoming in IDS is that for a large, complex network IDS can typically generate thousands or millions of alarms per day, representing an overwhelming task for the security analysts. Table 1 shows a comparison between the two types of intrusion detection

Table1: a comparison between the two types of intrusion detection [3].

	Misuse Detection	Anomaly Detection
Characteristics	use patterns of well-known attacks (signatures) to identify intrusions, any match with signatures is reported as a possible attack	use deviation from normal usage patterns to identify intrusions, any significant deviations from the expected behaviour are reported as possible attacks
Drawbacks	- False negatives - Unable to detect new attacks - Need signatures update - Known attacks has to be hand-coded - Overwhelming security analysts	- False positives. - Selecting the right set of system features to be measured is ad hoc and based on experience - Has to study sequential interrelation between transactions - Overwhelming security analysts

OUTLIER DETECTION SCHEMES -

Most anomaly detection algorithms require a set of purely normal data to train the model, and they implicitly assume that anomalies can be treated as patterns not observed before. Since an outlier may be defined as a data point which is very different from the rest of the data, based on some measure, we employ several outlier detection schemes in order to see how efficiently these schemes may deal with the problem of anomaly detection. In statistics-based outlier detection techniques [4] the data points are modeled using a stochastic distribution and points are determined to be outliers depending upon their relationship with this model. However, with increasing dimensionality, it becomes increasingly difficult and inaccurate to estimate the multidimensional distributions of the data points [5]. However, recent outlier detection algorithms that we utilize in this

study are based on computing the full dimensional distances of the points from one another [6, 7] as well as on computing the densities of local neighborhoods [8].

APPROACHES TO SOLUTION -

- Signature-Based
- Anomaly Based
- Network-Based
- Host-Based

Table 2: Network intrusion detection techniques

Technique			
Signature Based	**Anomaly Based**	**Network-Based**	**Host-Based**
Model well-known attacks	Are trained using normal behavior of the system	Are installed on N/W Switches	Are installed locally on host machines
Use these known patterns to identify intrusion.	Try to flag the deviation from normal pattern as intrusion	Detect some of the attacks that host-based systems don't. E.g. DOS, Fragmented Packets.	

TYPES OF INTRUSION DETECTION

- Real Time
- After-the-fact (offline)
- Network Based
- Host Based

CONCLUSION:

In this paper we found that a combination of different approaches may overcome the limitations in current IDS and leads to high performance ones. Traditional IDS undergo from dissimilar evils that limit their efficiency and competence.

REFERENCES:

[1] Jiawei Han and. Micheline Kamber, Data Mining: Concepts and Techniques, Morgan Kufmann, 2nd edition 2006, 3rd edition 2011.

[2] S.J. Stolfo, W. Lee. P. Chan, W. Fan and E. Eskin, "Data Mining – based Intrusion Detector: An overview of the Columbia IDS Project" ACM SIGMOD Records vol. 30, Issue 4, 2001.

[3] Ahmed Youssef and Ahmed Emam "Network intrusion detection using data mining and network behaviour analysis " International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Dec 2011 DOI : 10.5121/ijcsit.2011.3607 87

[4] V. Barnett, T. Lewis, Outliers in Statistical Data, John Wiley and Sons, NY 1994.

[5] C. C. Aggarwal, P. Yu, Outlier Detection for High Dimensional Data, Proceedings of the ACM SIGMOD Conference, 2001.

[6] E. Knorr, R. Ng, Algorithms for Mining Distance-based Outliers in Large Data Sets, Proceedings of the VLDB Conference, 1998.

[7] S. Ramaswamy, R. Rastogi, K. Shim, Efficient Algorithms for Mining Outliers from Large Data Sets, Proceedings of the ACM SIGMOD Conference, 2000.

[8] M. M. Breunig, H.-P. Kriegel, R. T. Ng, J. Sander, LOF: Identifying Density-Based Local Outliers, Proceedings of the ACM SIGMOD Conference, 2000.

[9] Paul Dokas, Levent Ertoz, Vipin Kumar, Aleksandar Lazarevic, Jaideep Srivastava, Pang-Nig Tan "Data Mining for Network Intrusion Detection"