International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Various Techniques for Classifying Attacks in NIDS

Ruchira Gurav[1], Aparna Junnarkar[2]

[1]Pune University, Progressive Education Society's, Modern College of Engineering, Pune-4110005, Maharashtra, India

Abstract: ***Intrusion Detection System (IDS) is the most powerful system that can handle the intrusions of the computer environments by triggering alerts to make the analysts take actions to stop this intrusion. IDS's are based on the belief that an intruder's behavior will be noticeably different from that of a legitimate user. A variety of intrusion detection systems (IDS) have been employed for protecting computers and networks from malicious attacks by using traditional statistical methods to new data mining approaches in last decade's .The conventional system is not efficient for unseen data and they need to be updated frequently to work properly. There are several techniques which classify data into only normal and threat or attack type, further classification is not done which leads to less accuracy. In several approaches dimensionality of input set is large which makes the problem complex and redundancy might increase. So basically in today's world of internet and automation, it is important to maintain a security, authenticity. There must be a proper efficient technique which can detect attacks and classify them into proper attack categories. The further classification into sub-attack categories plays a vital role in IDS as likewise preventive actions can be taken. So basically in this paper we are going to focus on various techniques for classifying attacks in NIDS.***

Keywords: Intrusion Detection System, Promiscuous mode, dimensionality, alerts, legitimate user

1. Introduction

The highly connected computing world has also equipped the intruders and hackers with new facilities for their destructive purposes. The costs of temporary or permanent damages caused by unauthorized access of the intruders to networks and computer systems have urged different organizations to, increasingly; implement various systems to monitor data flow in their networks. These systems are generally referred to as Intrusion Detection Systems (IDSs)

1.1 There are Basically Four Types of Attacks

- **Denial of Service (DoS)**
  A DoS attacks is a type of attack in which the hacker makes a memory resources too busy to serve legitimate networking requests and hence denying users access to a machine e.g. apache, smurf, Neptune, ping of death, back, mail bomb, UDP storm, etc.
- **Remote to User attacks (R2L)**
  A remote to user attack is an attack in which a user sends packets to a machine over the internet, and the user does not have access to in order to expose the machines vulnerabilities and exploit privileges which a local user would have on the computer, e.g. x lock, guest, send mail dictionary etc.
- **User to Root Attacks (U2R)**
  These attacks are exploitations in which the hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges, e.g. Perl, x term.
- **Probing**
  Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system. This technique is commonly used in data mining, e.g. satan, saint, ports weep, m scan, n map etc.

1.2 Types of IDS

Signature based (Misuse) IDS

This type of intrusion detection system contains a database of know vulnerabilities. It monitors traffic and seeks a pattern or a signature match. This means, it operates in much the same way as a virus scanner, by searching for a known identity or signature for each specific intrusion event. It can be placed on a network to watch the network vulnerabilities or can be placed on a host. Signature-based IDS examine ongoing traffic, activity, transaction, or behavior for matches with known patterns of even specific to known attacks and it raises alarm only when the so called match is found.

2. Anomaly based IDS

Also known as Heuristic or Behavior based, Anomaly based IDS analyzes the traffic patterns and determine normal activities. After that, it applies statistical or heuristic measures to event to determine if they match with this normal behavior. Events which do not match with the accepted normal behavior patterns are considered as attacks . By creating patterns of normal behavior, anomaly based IDS systems can observe when current behavior deviates statistically from the normal. This capability theoretically gives anomaly-based IDSs abilities to detect new attacks that haven't been seen before or close variants to previously known attacks. It means, these types of IDS may identify any possible attacks

1. Host based IDS (HIDS):
Host-based IDS can analyze activities on the host it monitors at a high level of detail. It can often determine which processes and/or users are involved in malicious activities. It can monitor events that are local to a host and can detect successful or failure of attacks that cannot be seen by a network-based IDS.

2. Network based IDS (NIDS):
Network based IDS monitors the traffic on its entire network segment. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic segments. These network traffic packets are checked network by the IDS to find the attacks. Network based IDS can reassemble packets, look at headers, determine if there are any predefined patterns or signature match.

3. Features

There are in all 41 features available with the help of which attacks can be detected. Instead of describing all the features, here we divide them into three groups and provide descriptions and examples for each group.

Group 1 includes features describing the commands used in the connection (instead of the commands themselves). These features describe the aspects of the commands that have a key role in defining the attack scenarios. Examples of this group are number of file creations, number of operations on access control files, number of root accesses, etc.

Group 2 includes features describing the connection specifications. This group includes a set of features that present the technical aspects of the connection. Examples of this group include: protocol type, flags, duration, service types, number of data bytes from source to destination, etc.

Group 3 includes features describing the connections to the same host in last 2 seconds. Examples of this group are: number of connections having the same destination host and using the same service, % of connections to the current host that have a rejection error, % of different services on the current host, etc.. During inspection of the data it turned out that the values

3.1 NIDS Architecture General Flow

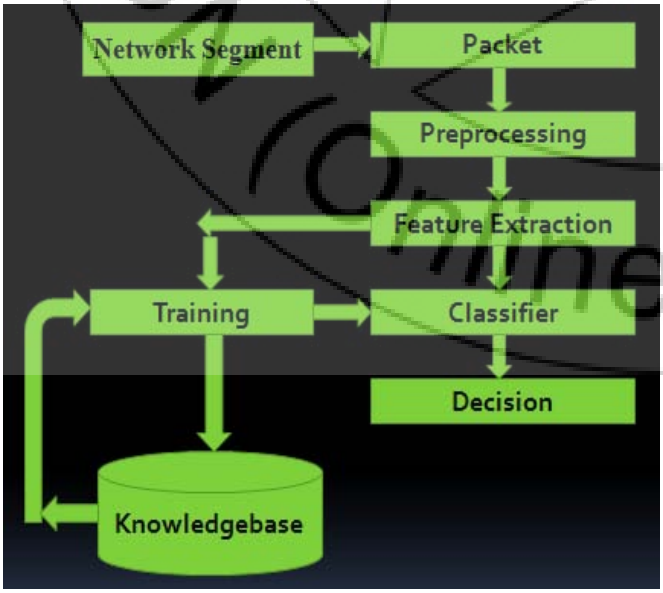

Figure: NIDS Architecture

3.2 Description of the Architecture

- **Packet Monitor:** This module monitors network stream real time and capture packets to serve for the data source of the NIDS.
- **Preprocessor:** In preprocessing phase, network traffic collected and processed for use as input to the system. Classifying attacks in NIDS Using MLP and Naive Bayes
- **Feature Extractor:** This module extracts feature vector from the network packets (connection records) and submits the feature vector to the classifier module.
- **Classifier:** The function of this module is to analyze the network stream and to draw a conclusion whether intrusion happens or not.
- **Decision:** When detecting that intrusion happens, this module will send a warning message to the user.
- **Knowledgebase:** This module serves for the training samples of the classifier phase. As you know, the artificial neural networks can work effectively only when it has been trained correctly and sufficiently. The intrusion samples can be perfected under user participation, so the capability of the detection can improve continually. All of these modules together make the NIDS architecture system based on the artificial neural networks.

3.2 Tables

Table 1: Literature Survey

Title (Authors and Publication)	*Technique*	*Results/Conclusion*
1] Intrusion Detection Using Artificial Neural Network with Reduced Input Features. (P. Ganesh Kumar, D.Devaraj) Published in: ICTACT, JULY 2010	For Feature Extraction SVD	•Reduced Feature set to reduce redundancy •Training-validation strategy was used in order to maximize the generalization capability of the ANN. •The result of multiple training sessions also led to an average of 86% correct classification on unseen data. •Disadvantages: Offline classifier and Training Time consuming
2] Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks. (Mohammad Reza Norouzian, Sobhan Merat) Published in: ICACT 2011	Multilayer Perceptron (MLP)	•Acts as a Online classifier with 90.78% accuracy. •Classification of attacks in 6 attack types so that preventive actions can be taken accordingly. •Disadvantages: Disadvantage is generates False Positive alarms.
3]Network Intrusion Detection Using Tree Augmented Naïve-Bayes	Naïve Bayes and Tree Augmented Naïve Bayes	•Experimental results showed that Naïve-Bayes is faster. •Has better accuracy rate and detection rate, and

(R. Naja, Mohsen Afsharchi) Published in: IEEE (Iran) 2012		also has less false positive alarm rate.
4]Implementation of Intelligent Multi-Layer Intrusion Detection Systems (IMLIDS) (Sherif M. Badr) Published in: International Journal of Computer Applications (January 2013)	MLP, C5 Decision tree, Exhaustive	As C5 algorithm can work efficiently for generalizing attack and detection of new attacks. •Disadvantages: •Use of C5 decision tree leads to high false alarm rate. •Exhaustive Algorithm shows Low classification rate for U2R attacks
5] Detecting User-To-Root (U2R) Attacks Based on Various Machine Learning Techniques - (S. Revathi , Dr. A. Malathi) Published in: IJARCCE (2014)	-MLP -Random Forest -Naïve Bayes -JRIP	MLP is efficient for identifying user to root attack with better accuracy

4. Conclusion

So basically, there are many techniques to classify attacks in NIDS but it is important that the system should classify attacks not only in normal or attack type but also in sub-attack categories so that likewise preventive actions can be taken, and with better accuracy, less false alarm rate, with reduced feature set which results in reduced redundancy and dimensionality reduction.

References

[1] P. Ganesh Kumar and D. Devaraj , Intrusion Detection Using Artificial Neural Network with Reduced Input Features, ICTACT JOURNAL ON SOFT COMPUTING,JULY 2010, ISSUE: 01
[2]]Mohammad Reza Norouzian, Sobhan Merati, Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Network s , ICACT 2011.
[3] R. Naja, Mohsen Afsharchi, Network Intrusion Detection Using Tree Augmented Naive-Bayes, CICIS'12, IASBS, Zanjan, Iran, May 29-31, 2012
[4] Sherif M. Badr, Implementation of Intelligent Multi-Layer Intrusion Detection Systems (IMLIDS), International Journal of Computer Applications (0975 8887) Volume 61 No.4, January 2013.
[5] S. Revathi, Dr. A. Malathi, Detecting User-To-Root (U2R) Attacks Based on Various Machine Learning Techniques, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 4, April 2014

Author Profile

Ruchira Gurav received the B.E. degree in Information Technology Engineering from BVCOEW, Pune University in 2013. She is now pursuing M.E. degree in Computer Engineering from P.E.S.'s Modern College of Engineering and her area of interest is Networking and Security.