Classification of Intrusion Detection System

Abhishek Pharate
Department of Computer Engineering,
Smt. Kashibai Navale College of Engineering,
University of Pune

Harsha Bhat
Department of Computer Engineering,
Smt. Kashibai Navale College of Engineering,
University of Pune

Vaibhav Shilimkar
Department of Computer Engineering,
Smt. Kashibai Navale College of Engineering,
University of Pune

Nalini Mhetre
Department of Computer Engineering,
Smt. Kashibai Navale College of Engineering,
University of Pune

ABSTRACT
Use of internet is increasing to great extent and with it abnormal and malicious activities. Solving problem of these attacks is becoming a prime need of network services. Till date many techniques and algorithms are developed. All these can be summed to intrusion detection systems and firewall. In this paper we present the classification of these intrusion detection systems on the basis of their properties. So it will help in understanding different IDS and their properties accordingly. With different types IDS classification it also enlists pros and cons of systems.

General Terms
NIDS, Intrusion, Network security

Keywords
NIDS, HIDS, Intrusion Detection, DoS, Probe, Genetic Algorithm.

1. INTRODUCTION
Intrusion detection system is a software application or a device that monitors the network for abnormal or malicious activities and alerts the administrator. Intrusion detection systems (IDS) are used to detect various attacks. These attacks are classified as:

1. Denial of Services (DoS): A DoS attack is an attack in which the attacker floods a computing or memory resource with false requests so that it is unable to serve legitimate requests and thus denying users access to the service.
2. Probing: Probing is an attack with the goal of gaining the configuration of the target machine or network.
3. User-to-Root (U2R): These attacks have the goal of gaining administrative access to a machine in which the attacker has a user level access.
4. Remote-to-Local (R2L): R2L is an attack in which a user sends packets to a machine over internet which the user does not have access to in order to expose the vulnerabilities and exploit privileges which a local user would have on the computer.

The classification of intrusion detection system is based on following factors:

1. Location
2. Functionality
3. Deployment Approach
4. Detection Mechanism

2. LOCATION
2.1 Host Based Network Intrusion Detection:
HIDS is single computer specific intrusion detection system which monitors the security of that system or computer from internal and external attacks. The internal attacks refer to the situation where it detects which program access which resource and is there any security break. For example word-processor suddenly starts accessing system password database and starts modifying it. In second part that is external attacks HIDS analyses packets to and from that system (computer) on its interfaces. HIDS responds by logging the activity and informing about it to designated authority. In HIDS anti threat applications such as antivirus, spyware are installed on a system which monitors security.

Examples of HIDS are Open source tripwire [33], intrust event admin aelita, ELM3.0 TNT software, GFI LAN guard S.E.L.M

Pros:

1. HIDS can protect off the LAN.
2. HIDS is versatile.
3. Requires lesser training than NIDS.
4. HIDS does not requires land bandwidth.
5. HIDS provides local machine registry scan.

Cons:

1. Passive system that have to wait for an event to be an indication of an attack and cannot proactively prevent it
2. Data collection occurs on a per-host basis
3. Writing to log or reporting activity will generate extra load for network
4. Clever hackers can attack and disable HIDS while attacking HIDS does consume processing time, storage, memory and other system resources

2.2 Network Intrusion Detection System:
Network intrusion detection system (NIDS) monitors network traffic and analyzes the passing traffic for attacks. On identification of an attack or when an abnormal behavior is sensed an alert can be sent to the administrator. NIDS can

detect 4 major types of attacks: denial of services, Probe, user to root and remote to user.

Examples of NIDS implementation are Snort ISS, Cisco Secure IDS and Dragon Enterasys. [1][29][30]

Pros:

1. Adaptable to cross platform environment.
2. NIDS is centrally managed.

Cons:

1. Requires more training.
2. Uses up LAN bandwidth.
3. Failure rate is higher.

3. FUNCTIONALITY

3.1 Intrusion Detection System

Intrusion detection is process of identifying malicious activity targeted to computing and network resources. There are two types of intrusion detection systems 1) HIDS 2) NIDS. Intrusion detection systems detects if there is any intrusion and reports about it to administrator. There are two types intrusion detection techniques 1) Anomaly detection 2) Misuse detection. Anomaly detection analyses information gathered and compares to the baseline which is seen as normal service behavior. Misuse detection is based on signature for known attacks. It does not anything to stop them. It simply detects them. IDS uses different algorithms such as Adaptive Resonance theory, Self-organizing m p, and genetic algorithm. [2][3]

3.2 Intrusion Prevention System:

IDS was only capable of detection of intrusion without prevention action. Intrusion Detection system Proactive technique which prevents attack before entering a network by examining packets and their pattern and blocks them. IPS is active and smart and system which provides early detection attack. IPS works on 2, 3, 4 and 7 layer of OSI. IPS has the functionality of doing activity of Early Detection, proactive technique, early prevent the attack, when an attack is identified then blocks the offending data. [4]

3.3 Intrusion Detection and Prevention System:

Do not Firewall does not provide security against network attacks on open ports required for network services (i.e. Denial of service attack).So IDPS could be used to protect network services with firewall. Mainly there are three parts in IDPS 1) preprocessing 2) classification 3) protection. In preprocessing part packet sniffer is used capture information from packets. Then the preprocessed data is classified into mainly two types attack packet and normal packet .this information is passed to protection part which takes appropriate action according to type of packet for prevention. [5]Examples of IDS and IDPS are Snort (IDS) [31] [32], Cisco IPS Sensor Software (IDPS) [27].

4. DEPLOYMENT APPROACH

4.1 Single Host:

In single host deployment of network intrusion detection system, the system is installed on a single host in network that may be a router, a server or network switch. The whole traffic enters and leaves the network via that node, where it is checked for attacks and normal packets by the NIDS.

Examples of single host intrusion detection systems are GrIDS, Bro and NetRanger. [24][25][26]

Pros:

1. A single NIDS can monitor a wide subnet
2. The impact on the system is very little, it is a passive device which just listens

Cons:

1. It is difficult to process all packets in a busy network.

4.2 Multiple Host (Distributed Agents):

In distributed deployment of NIDS, the system is installed on all (or may be few) the nodes in the network, can be called as NIDS agents. These agents then monitor the traffic that is routed through that particular node and generate appropriate results. These results are then sent to central NIDS controller (NIDS management system). This NIDS management system coordinated with the agents and generates alarms for appropriate packets and broadcasts it on network.

Examples of multiple host intrusion detection system are AAFID [22][23] and Micael. [6][7][8].

Pros:

1. The problem of processing all packets by single NIDS which was present in single host NIDS is solved.

Cons:

1. It is harder to manage and must be configured for each different host.
2. It's hard to coordinate between NIDS agents.

5. DETECTION MECHANISM

5.1 Signature Based:

In signature based detection mechanism the attack patterns are saved in the database. Each packet of the network traffic is compared with the attack patterns to detect abnormal behavior. Signature based intrusion detection system detects only know attacks.

Examples Suricata [20] [21] is a signature based intrusion detection system. [9]

Pros:

1. If attack signatures are clearly defined then it has low false positive.
2. Easy to use.

Cons:

1. Requires specific knowledge of intrusion behavior and collect data before the intrusion could be out of date.
2. Difficult to detect unknown attacks.
3. Raises alerts regardless of the outcome. Example if a windows worm tries to attack a Linux system then the IDS sends many alerts of unsuccessful attack.
4. The knowledge of the attacks is dependent on the specific environment.

5.2 Anomaly Based Intrusion Detection System:

Anomaly based intrusion detection system is based on the network behavior. The network behavior is defined by the administrator or is learned by the dataset during the training phase of the development of IDS. Rules are defined for normal behavior and abnormal behavior.

Example, Snort and Bro-IDS are anomaly based intrusion detection system. [10]

Pros:

1. It has the ability to detect unknown attacks.

Cons:

1. Defining the rule set for intrusion detection is difficult.
2. Efficiency of system depends on the fitness of the rules and its testing on the testing datasets.

6. DETECTION MECHANISM

6.1 Rule Engine:

Rule based intrusion detection system detects anomalous behavior by comparing the features of the packets to some predefined rules which are defined by the administrator or which are created by some algorithm through learning. Rule based systems use highly distributable predefined signatures to detect known attacks. [11][12]

Pros

1. It has a very high detection rate for known attacks.

Cons

1. The selection of features to identify each attack is difficult.
2. For the intrusion detection system to have high detection rate the rules must be carefully specified.

6.2 . Artificial Intelligence/ Neural Network/ Genetic Algorithm Based Intrusion Detection:

Artificial intelligence based intrusion detection system is different from all the algorithms is that artificial intelligence is used to define new set of rules for attack detection. Neural networks are the most common type of artificial intelligence type for intrusion detection. Neural network is a set of cells that have a weighted connection to other cells. Through training the weights of connections are altered and the output is compared to desired output. Iterations are carried out until desired accuracy is not obtained for a test data set. In genetic algorithm rules are defined. Each rule consists of features which can distinctly identify a class of attack. These rules are tested and after each iteration the rules with higher fitness factor are selected and modified to create new rules till desired detection rate is not achieved. [13][14][15]

Pros:

1. Unknown attack detection rate is increased by using combination of genetic algorithm with signature based intrusion detection system.

Cons:

1. Careful selection of features to define rules needs knowledge of the domain.
2. Detection rate depends on the training data and the rules provided.

I. Supervised learning

Supervised learning is used when a set of training data is available. The training data set consists of input values which are connected to specific output. In supervised learning the training data is used to learn the attack pattern. The output values are used to calculate the fitness factor of the rules. [16]

II. Unsupervised Learning

The system learns to represent input pattern to find the statistical structure in the input. The inputs having similar features are divided into clusters. Mean is calculated for each cluster. On adding a new input to a cluster the mean is recalculated. These clusters are used to determine unknown attack patterns. [17].

7. DETECTION MECHANISM

7.1 Real-Time:

Real-time intrusion detection systems work online i.e. these intrusion detection systems capture packets from the network (live) for detecting abnormal activities. The performance of real time intrusion detection systems highly depends upon the number of features selected as it has to compare those features with the features of the incoming packets at a very high rate. The number of features also affects the resource consumption of the real time system. [18]

Pros:

1. Real-time systems detect abnormal behavior while it is happening which is desired from an intrusion detection system.

Cons:

1. Real-time systems require more resources.
2. Real-time systems may become bottleneck.

7.2 Offline:

Offline intrusion detection systems work offline i.e. these intrusion detection systems process saved attack data sets like KDD cup 99 data set. Offline intrusion detection systems provide information about the attack and help repair the damage caused by the attack. These detection systems help in understanding the attack mechanism and reduce the possibilities of future attacks of the same type. [19]

8. CONCLUSION

This paper presents various classifications of intrusion detection system. The performance of any intrusion detection system depends upon the features of the packet which are selected for detection of attack. There are pros and cons in each category but combination of various categories complemented with appropriate packet features helps in building a good intrusion detection system.

9. REFERENCES

[1] Marion Bogdanov ,"An approach to developing an information assurance environment"

[2] Sanjay Kumar Sharma, Pankaj Pande, Susheel Kumar Tiwari and Mahendra Singh Sisodia ,"An Improved Network Intrusion Detection technique based on k-means clustering via naïve Byes Classification" IEEE-International Conference On Advances In Engineering,

Science And Management (ICAESM -2012) March 30, 31, 2012

[3] Thanvarat Komviriyavut, Phurivit Sangkatsanee, Naruemon Wattanapongsakorn, "Network intrusion detection and classification with decision tree and rule based approach" IEEE, 2009

[4] Deris Stiawan, Ala' Yaseen Ibrahim Shakhatreh, Mohd. Yazid Idris, Kamarulnizam Abu Bakar, Abdul Hanan Abdullah, "Intrusion prevention system: a survey" Journal of Theoretical and Applied Information Technology 15 June 2012. Vol. 40 No.1

[5] N. Wattanapongsakorn, S. Srakaew, E. Wonghirunsombat, C. Sribavonmongkol, T. Junhom, P. Jongsubsook, C. Charnsripinyo, "A Practical Network based Intrusion Detection and Prevention System" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications

[6] K.B.Chandradeep, "A scheme for the design and implementation of a distributed ids" 2009 First International Conference on Networks & Communications

[7] Kjetil Haslum, Ajith Abraham and Svein Knapskog, "Fuzzy online risk assessment for distributed intrusion prediction and prevention systems" Tenth International Conference on Computer Modeling and Simulation

[8] Hakan Albag, "Network & agent based intrusion detection systems"

[9] Vinod Kumar, Dr. Om Prakash Sangwan, "Signature based intrusion detection system using Snort" International Journal of Computer Applications & Information Technology Vol. I, Issue III, November 2012 (ISSN: 2278-7720)

[10] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad, "A review of anomaly based intrusion detection systems" International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, August 2011

[11] Maithili Arjunwadkar, R.V. Kulkarni, "The rule based intrusion detection and prevention model for biometric system" VOL. 1, NO. 2, Oct 2010 Journal of Emerging Trends in Computing and Information Sciences

[12] Todd Vollmer, Jim Alves-Foss, Milos Manic, "Autonomous rule creation for intrusion detection" 2011 IEEE Symposium on Computational Intelligence in Cyber Security

[13] Matti Manninen, "Using Artificial Intelligence in intrusion detection systems"

[14] Shaik Akbar, Dr. K. Nageswara Rao, Dr. J.A. Chandulal. "Implementing rule based genetic algorithm as a solution for intrusion detection system" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011

[15] Zorana Bankovic, Dusˇan Stepanovic, Slobodan Bojanic, Octavio Nieto-Taladriz, "Improving network security using genetic algorithm approach" Computers and Electrical Engineering 33 (2007) 438–451

[16] Borgersen Gustav, Karlsson Linus, "Supervised learning in artificial neural networks"

[17] Peter Dayan, "Unsupervised Learning" Appeared in Wilson, RA & Keil, F, editors. The MIT Encyclopedia of the Cognitive Sciences

[18] Phurivit Sangkatsanee, Naruemon Wattanapongsakorn, and Chalermpol Charnsripinyo, "Real-time intrusion detection and classification"

[19] Richard Lippmann, Joshua W. Haines, David J. Fried, Jonathan Korba, Kumar Das, "The 1999 DARPA offline intrusion detection evaluation"