ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Survey on Evolution and Advances in Intrusion Detection Techniques

Sonali A. Deo

Lecturer, Department of IT, Modern College of Engineering, Pune, India

ABSTRACT: Intrusion Detection Systems (IDS) are very useful in monitoring and detecting malicious activities. There are various techniques to implement intrusion detection system. But it is observed that no single IDS technique is useful all the time and different techniques are required at different circumstances. Recent trends in IDS combine one or more IDS techniques to get equally better results in all circumstances. CONDOR is a Hybrid IDS technique which combines Signature based and Anomaly based techniques of intrusion detection, Hybrid Packet based and Flow based technique combines Packet based and Flow based IDS techniques and MLH-IDS is combination of Supervised, Unsupervised, and Outlier based method. To enhance and speed up the IDS techniques different design approaches of IDS have been proposed. Distributed NIDS works in distributed manner to achieve speed up while Parallel NIDS performs many actions in parallel to improve system performance.

KEYWORDS: CONDOR, Distributed NIDS, Intrusion Detection System(IDS), Multi-Level Hybrid IDS, Network Intrusion Detection System(NIDS), Packet and Flow based IDS , Parallel NIDS.

I. INTRODUCTION

Intrusion is set of actions which compromise the security of computer and network components in terms of its confidentiality, integrity and availability. Intrusion can be done by an agent to gain unauthorized entry and control of the security mechanism of the system and they are called as intruder. Intruders have become a biggest threat to the computer world. Researchers have provided numerous security tools such as firewalls, encryption etc. to prevent such attacks from intruder but intruders are also becoming successful in penetrating such tools. IDS is a relatively new technology for intrusion detection that have emerged in recent years. It works to help computer systems to deal with the network attacks. Intrusion detection functions include 0:

- Monitoring and analyzing user and system activities
- Analysis of system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns specific to attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

An IDS performs vulnerability assessment to assess the security of a host or a network. Intrusion detection works on the basic assumption that intrusion activities are noticeably different from normal system activities and so they are detectable.

II. LITERATURE SURVEY

IDS is divided into two categories: host-based (HIDS) and network-based (NIDS). An HIDS resides on a particular host and looks for indications of attacks on that host. On the other hand an NIDS resides on a separate system that watches network traffic, looking for indications of attacks that traverse that portion of the network. The current trend in intrusion detection is to combine information from both host based and network based systems to develop hybrid IDS.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

2.1 Host Based Intrusion Detection (HIDS)

As stated in **Error! Reference source not found.** an HIDS exists as a software process on a system. Traditionally, HIDS systems have examined log entries for specific type of information. A new form of HIDS examines operating system calls. HIDS has following properties:

1.The HIDS will not miss attack traffic that is directed at a system as long as the attack generates a log message.
2.The HIDS can determine if an attack was successfully examining log messages or other indications on the system.
3. The HIDS can be used to identify unauthorized access attempts by legitimate system users.

2.2 Network Based Intrusion Detection (NIDS)

As stated in **Error! Reference source not found.** an NIDS exists as a software process on a dedicated hardware system. The NIDS contains network interface card on the system into promiscuous mode, meaning that the card passes all traffic on the network to the NIDS software. The traffic is then analyzed according to a set of rules and attack signatures to determine if it is traffic of interest. If it is then event is generated. Properties of an NIDS include:

1.The NIDS is completely hidden on the network so attacker will not know that he is being monitored.
2.A single NIDS can be used to monitor traffic to a large number of potential target systems.
3.The NIDS can capture the contents of all packets travelling to the target system.

Intrusion Detection Techniques are also classified as [2].

1. Anomaly Intrusion Detection
2. Misuse Intrusion Detection

2.3 Anomaly Intrusion Detection

This method works by using the definition “anomalies are not normal”. The method tries to determine whether the packet deviating from normal packet is part of intrusion. Anomaly IDS detects intrusion based on abnormal behavior and abnormal use of resource. In this approach IDS watch for unknown intrusion with abnormalities in traffic patterns, system use basic rule that something that is abnormal is suspicious.

2.4 Misuse Intrusion Detection

Misuse intrusion detection is the approach mainly used in the commercial IDS. It uses the pattern of known attacks or weak spots of the system to match and identify the attacks. There are various ways to store attack patterns so that different patterns of same attack can also be identified. It finds intrusion based on the knowledge of previous attacks.

III. IMPROVED IDS TECHNIQUES

Various types of IDS techniques have been evolved to reduce false alarm rate but it is found that no single technique is useful at all the time so recent IDS techniques combines two or more techniques to get better results. Here in this section three such hybrid Intrusion Detection Techniques.

3.1 CONDOR: A Hybrid IDS

Day, Flores and Lallie introduced technique named CONDOR[3]. CONDOR (COmbined Network intrusion Detection ORientate) combines different models to form new model for Distributed Anomaly Detection and Automated Signature Generation. Three modules under CONDOR are: the user interface, the signature detection component (S), and the anomaly detection component (A); as shown in figure 1.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

In CONDOR User Interface plays main role of communication and is in charge of coordinating the administrator, the

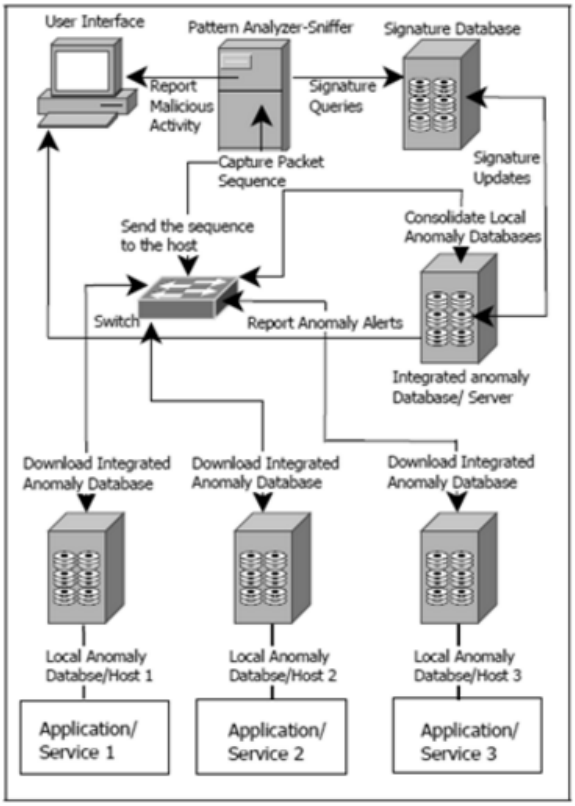


Figure 1 : Structure of CONDOR combining a Signature Based IDS and a Distributed Anomaly Based IDS with Signature Generation and Anomaly Detection Capabilities [3]

signature detection component, and the anomaly detection component. CONDOR's console displays the alert messages and helps administrator to configure both components.

3.1.1 The Signature Detection Component

Signature detection component is formed by a pattern analyzer and signature database. Pattern analyzer captures and process system call sequences from packets received and sent by hosts. Analyzer compares the captured sequences with the patterns in the signature database. If an attack is detected analyzer send alert message to console to inform administrator and kill message to host so as to terminate process detected as malicious. It pattern doesn't matches with any of the signature then considering that sequence is false negative it is further send to anomaly detection component to determine whether it normal or malicious.

3.1.2 The Anomaly Detection Component

Anomaly detection component performs analysis of the sequences assumed as false negatives. It contains one integrated anomaly database stored at anomaly based server, and a set of local anomaly databases stored at n hosts or anomaly-based clients. Integrated anomaly database is used to collect anomalous behavior from all different local anomaly-based clients. CONDOR's employs both the server and clients to form one single anomaly based IDS, as shown in figure 1. Three engines in the anomaly detection component are: the local anomaly analyzer, the anomaly database integration engine, and the signature generation engine.

Local Anomaly Analyzer When sequence arrives at client it is analyzed against the replicated database. If arrived sequence doesn't matches with any of the rule in the replicated database, then analyzer sends a message to console for administrator intervention. So administrator has to check and decide whether the new sequence is anomalous or normal. If administrator decides sequence as normal, then this new sequence is added to the replicated database which is copied at local site.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Anomaly Database Integration Engine In order to merge the new sequences from local database to integrated anomaly database the majority algorithms are suggested. The sequences collected from local client's database may contain various normal events which are also common in other clients. So anomaly database server collects sequences from all clients and defines how many clients have reported the same sequence. Then sentinel value is assigned to each set of sequences based on the number of clients reporting the sequence as normal. After the all local databases have been assessed if a given sequence contains a much smaller sentinel value than others, the server judges the sequence as anomalous, and then sequence is added to CONDOR's integrated database.

Signature Generation Engine CONDOR's anomaly-based server uses signature generation engine when it receives any abnormal system call from any of the anomaly based clients. New signatures are generated to update signature database when abnormal system calls are bypassed signature detection component and have passed through anomaly detection component.

3.2 Hybrid Packet Based and Flow Based IDS Technique

As proposed in [4] there are two NIDS methods based on the source of data to be analyzed: packet-based NIDS and flow-based NIDS. Packet-based NIDS analyze the whole payload contents of the packet. Flow NIDS observes all packets going through a network link and looks at aggregated information of related packets of network traffic in the

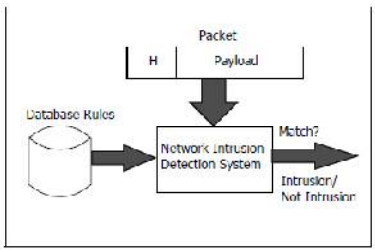


Figure 2: Packet Based NIDS[5]

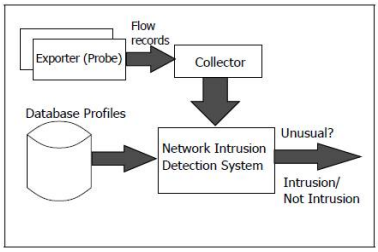


Figure 3: Flow Based NIDS[6]

form of flow, so the amount of data to be analyzed is reduced.

3.2.1 Packet Based NIDS

In packet-based, also named as “Deep Packet Inspection” (DPI), the header and payload scan determines whether a packet is a suspicious or not. All incoming packets are checked against every single rule in a database as shown in Figure 2**Error! Reference source not found.** [5].

3.2.2 Flow-Based NIDS

Packet-based techniques are not suitable for high speed networks. One solution to this is flow-based intrusion detection. Flow-based data source technique is widely used in applications like network monitoring, traffic analysis and security. Flows don't consider any packet payload unlike packet-based approach. It rather relies on network flow information and statistics. A flow is a unidirectional data stream between two computer systems communicating with each other where all transmitted packets have characteristics like: source and destination address, source and destination port number and protocol value. Recently special measurement systems provide other characteristics in addition to the above, for instance:

- The number of packets and amount of bytes transferred in a flow
- The start and end time of a flow (in millisecond)
- The disjunction of all TCP flog occurring in the flow.

3.2.3 Hybrid-Based IDS

The Hybrid-IDS technique which is combination of packet based and flow based technique is proposed in [4]. According to them performance issues faced by packet-based NIDSs have been solved by flow-based NIDS but flow-based NIDS still suffers from high false alarm rate. However the combination of both models can be used to power their advantages and overcome their disadvantages. In Hybrid-IDS two-phase detection process is used in order to improve NIDS accuracy without affecting its performance. In the first step, flow-based method detects specific intrusion and mark packets as suspicious. If suspicious flows are detected in the first step then the second step is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

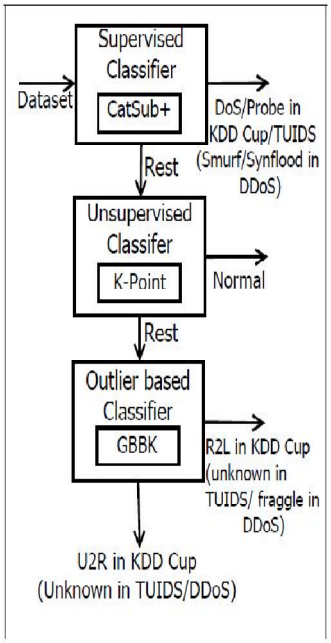
Vol. 5, Issue 6, June 2016

executed. Only suspicious packets marked in first step are fed to packet-based to additionally inspect the payload to make certain decision. As the packet selection strategy is applied, not all incoming packet's payload has to be inspected. Only the packets marked as a suspicious by flow-based method are inspected.

3.3 MLH-IDS(Multi-Level Hybrid IDS Technique)

Anomaly detection techniques based on machine learning methods are classified into two categories supervised and unsupervised. Supervised anomaly detection builds normal behavior model of systems or networks by using training with a labeled or purely normal dataset. Unsupervised anomaly detection approaches does not require any training data or

these models can be trained on even unlabelled or unclassified data and they attempt to find intrusions inside the data. The approach of unsupervised method which is popular in network intrusion detection is outlier-based.



Outliers are

Figure 4: Architecture of a multi-level hybrid classifier [7]

the data points that are very different from the rest of the data based on some appropriate measures.

Gogoi et.al presented new technique in [7] MLH-IDS i.e. Multilevel Hybrid Intrusion detection system is capable to detect network attacks with high accuracy. MLH-IDS use three level attack detection: a supervised method, an unsupervised method and an outlier-based method. The overall structure of the multi-level hybrid classifier is shown in Figure 4.

The first level of classification is supervised classifier to which dataset in feed into. Here test data is classified into 3 categories DoS, Probe and Rest (unclassified). So here U2R and R2L, and the Normal connections are classified as Rest in the first level. At level 1 the purpose is to extract as many U2R, R2L and Normal connections as possible accurately from the data. This is so because U2R and R2L are quite similar to normal connections. On the other hand DoS and Probe attack connections more different than normal one. The second level further classifies Rest from level 1 as Normal and Rest categories using an unsupervised classifier model. The Rest from second level is feed into third level which separates it into U2R and R2L. The U2R category data are extracted from Rest using the outlier-based classifier model and the remaining elements in the Rest category are classified as R2L. Other than U2R category records, the remaining items are classified as R2L category attacks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

IV. MODERN DESIGN APPROACHES

The above discussed techniques will reduce false alarm rate and will improve result accuracy but they are not speedy and today in the era of high speed network IDS systems needs to be worked with the speed of network. So researchers have proposed different system architectures which can be used to implement any of the IDS techniques to get faster results.

4.1 Distributed NIDS

The distributed NIDS system's architecture is proposed in [8]. The architecture contains more than one stand alone machines which use the computing power of their graphics hardware. Communication and synchronization between elementary NIDS stations is controlled by initial station called as Mentor. These all elementary nodes are connected to the single node in a network where all network traffic is mirrored and send to every standalone station in parallel. Architecture of the system is shown in Figure 5. The architecture is made up of three different parts.

Network Activity Capturing Layer: This layer captures entire network traffic. Node represents a high performance switch which supports port mirroring. For NIDS stations it is necessary to set network adapter on the packet capturing layer into promiscuous mode to accept packets which are not addressed to them

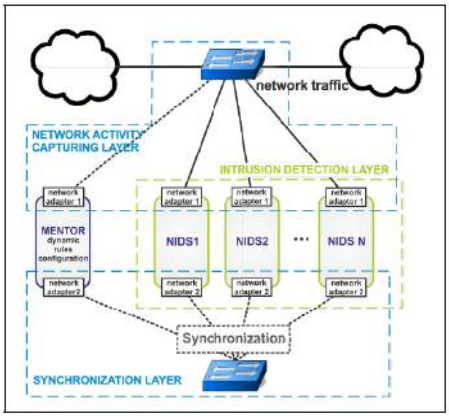


Figure 5:Architecture of Distributed NIDS [8]

Intrusion Detection Layer: It is formed by many elementary stations and it is very important and main performing part of the system. It represents distribution of workload of whole intrusion detection system.

Synchronization Layer: It represents a way to divide load on certain NIDS stations and dynamically configures them. It is a separate hardware detached from a LAN which takes care of the synchronization of the system parts via messages.

4.1.1 Elementary NIDS Station

Every elementary station has two hardware divided network interfaces. Amongst them Network adapter 1 is used to capture packet sent from capturing layer of the network activity. Network adapter 2 is the part of the synchronization layer and it is used to send and receive message between parts of the system.

4.1.2 Synchronization and Communication Sub layer

Synchronization layer consist of network interfaces of elementary NIDS stations and switch taking care of transferring. As mentioned above NIDS station works on rule comparison basis and rules in a database must be updated according to detection of intrusion. This can achieved by exchanging messages between station and this task is performed by synchronization and communication sub layer. It is also possible to use synchronization communication is case of system disruption such as network activity overload and direct NIDS attack. Synchronization messages types can be dynamic configuration of rules, control and management of elementary station activity, remote control of elementary station, System behavior statistics, and communication results of the detection mechanism.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

4.1.3 Control I/O System Node

As it can be seen in figure 5 the model consist of control I/O node of the whole system called as Mentor Station is implemented. It's main task is to control and maintain whole IDS architecture. Mentor node consists of following components. Central Database of Results It contains all results and records gathered from all elementary NIDS stations as well as patterns of the main setting of dynamic configuration rule for every station.

5.2 Parallel Design for NIDS

Packet processing function in NIDS contains many stages. Figure 6 shows major steps in packet processing. Packets from network are captured by Packet Processing module and further decoded in packet decoder. Preprocessor does preprocessing of the packets and forwards that packet to the detection Engine. Detection engine scans payload of the packet for suspicious data by comparing it with signature set and create logs and send to the output unit. As it can be seen Detection Engines operations are complex and require more resources. In pre-filter phase payload is checked for occurrences of fingerprints

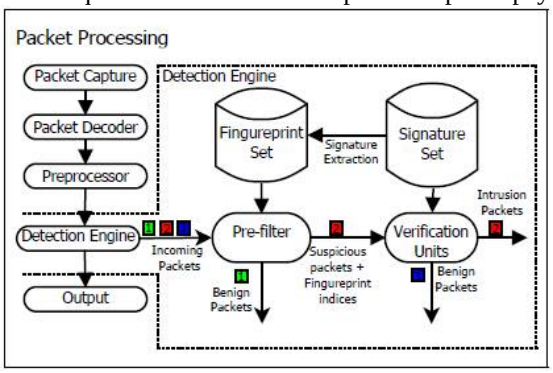


Figure 6: Packet processing in NIDS and detection engine [9]

from signature database, verification stage receives packet which contains at least one matched fingerprint in the pre-filtering stage and performs in-depth checks. Both Data and pipeline parallelism have been achieved in NIDS. In pipeline parallelism Packet Processing is divided into several stages and each stage runs on different execution unit. On the completion of processing from one stage in Packet Processing packet is feed into pipeline of the nest stage. On the other hand in data parallelism entire Packet Processing loop is implemented on each core so that large number of packets can be processed simultaneously

SUMMARY

Intrusion Detection System is relatively new technology for detection of attacks from intruders. Anomaly based and signature based techniques are basic IDS techniques which can be implemented using different technologies. In the recent years researchers have proposed hybrid IDS systems which combine one or more IDS techniques. CONDOR is a combination of signature based and anomaly based technique specially designed to reduce false positive rate and administrative intervention. It contains centralized signature based component, distributed anomaly based component and automatic signature generation component. Hybrid Packet based and Flow based technique combines packet based and flow based intrusion detection techniques. This technique is specially designed for high speed networks and requires very less resource utilization. MLH-IDS combines supervised, unsupervised and outlier based method. They are specially designed for detection of attacks like DOS, DDOS, Probe, R2L and U2R. To increase the speed and performance of the IDS techniques, many design approaches have been proposed. Distributed NIDS contains number of NIDS stations controlled by single mentor station and they all together form single intrusion detection system. Parallel NIDS contains several packet processing module to achieve parallelism and get faster results.

REFERENCES

[1] A..S.Ashoor and P.S.Gore, "Importance of Intrusion Detection System (IDS)," International Journal of Scientific and Engineering Research,2011.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

[2] S. Sonawane, S. Pardeshi, and G. Prasad, "A survey on intrusion detection techniques," World Journal of Science and Technology, 2012.

[3] D. J. Day, D. A. Flores, and H. S. Lallie, "CONDOR: A Hybrid IDS to Offer Improved Intrusion Detection," IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,2012.

[4] H. M. Alaidaros, M. Mahmuddin, and A. A. Mazari, "From Packet-based Towards Hybrid Packet-based and Flow-based Monitoring for E_cient Intrusion Detection: An overview," ICCIT, 2012.

[5] S. N. and J. N., "Network Intrusion Detection," New Rides, 2003.

[6] Claise and B, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information," RFC 5101, 2008.

[7] P. Gogoi, D. Bhattacharyya, B. Borah1, and J. K. Kalita, "MLH-IDS: A Multi-Level Hybrid Intrusion Detection Method," The Computer Journal Advance Access, 2013.

[8] L. Vokorokos and M. Ennert, "A Distributed Network Intrusion Detection System Architecture Based on Computer Stations Using GPGPU," IEEE 17th International Conference on Intelligent Engineering Systems, 2013.

[9] H. Jiang, G. Zhang, G. Xie, and K. S. Mathy, "Scalable High-Performance Parallel Design for Network Intrusion Detection Systems on Many-Core Processors," IEEE,2013.