International Journal of Engineering Research and Development
ISSN: 2278-067X, Volume 2, Issue 1 (July 2012), PP. 63-69
www.ijerd.com

Network Intrusion Detection Types and Analysis of their Tools

Abhishek Gupta, Mohit Kumar, Anamika Rangra, Vikas Kumar Tiwari, Pravesh Saxena

Department of Computer Science and Information Technology, Jaypee University of Information Technology, Waknaghat, Distt. Solan, (H.P), India

Abstract—This paper aims at providing the detail study of the techniques and types of the intrusion detection systems in a manner which is more suitable for analytical environment and then covers the performance assessment of various network intrusion detection tools.

Keywords—Intrusion Detection Types, Local Landline Network Intrusion Detection (LLNID) ,Intrusion prevention,tools.

I. INTRODUCTION

Every hacker in the world is one's neighbor on the Internet,which results in attack defense and detection being pervasive both at home and work. Although hundreds of papers have been written on a large variety of methods of intrusion detection—from log analysis, to packet analysis,statistics, data mining, and sophisticated computational intelligence methods—and even though similar data structures are used by the various types of intrusion analysis, apparently little has been published on a methodical mathematical description of how data is manipulated and perceived in network intrusion detection from binary network packets to more manageable data structures such as vectors and matrices.

The systems of detection and prevention of intrusion,IDS and IPS, are among the most recent tools of security. According to their features, we can classify them in different kinds, for example, their techniques of detection and prevention, their architecture or the range of detection [3]. In spite of their utility, in practice most IDS/IPS experience two problems: the important number of false positives and false negatives. The false positives, the false alerts, are generated when the IDS/IPS identifies normal activities as intrusions, whereas the false negatives correspond to the attacks or intrusions that are not detected, and then no alert is generated [4]. The IDS/IPS inventors try to surmount these limitations by developing new algorithms and architectures.

Therefore, it is important for them to value the improvements brought by these new devices. In the same way, for the network and systems administrators, it would be interesting to assess the IDS/IPS to be able to choose the best before installing it on their networks or systems, but also to continue to evaluate its efficiency in operational method. Unfortunately, many false positives and false negatives persist in the new versions of the IDS/IPS, then, the brought improvements are not worthy of the continuous efforts of research and development in the domain of the detection and the prevention of intrusion. In general, it is essentially due to the absence of efficient methods of assessment of the security tools, and of the IDS/IPS in particular..

II. LLNIDS TYPES OF INTRUSION DETECTION

The new types are explained below, but first some terminology needs to be stated in order to later describe the types. An Intrusion Detection System (IDS) is software or an appliance that detects intrusions. A Network Intrusion Detection System (NIDS) is an appliance that detects an intrusion on a network. In this research, network means a landline network. Local network intrusion detection refers to the instant case of network intrusion detection. Figure 1 illustrates the location of a Local Landline Network Intrusion Detection System (LLNIDS) as used in this research.The LLNDS in Figure 1 is represented by the rounded box in the center labelled "Local NIDS". It is an IDS on a landline between a local network and the Internet. The point of view of this research is from inside the LLNIDS. Users on the local network may have other ways of accessing the Internet that bypass the LLNIDS, such as wireless and dialup. This research is restricted to the LLNIDS as described here.

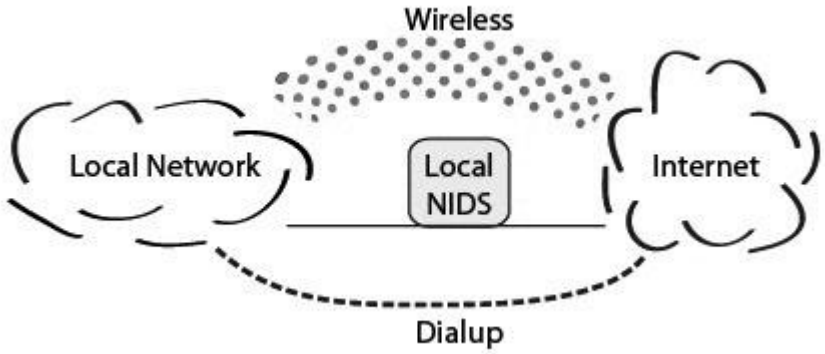

Figure 1: A Local Landline NIDS

Examples of detection which are not Local Landline Network Intrusion Detection (LLNID) include detection on the host computer, detection by someone else out on the Internet, or detection by someone out in the world, such as someone witnessing a perpetrator bragging in a bar. This research concerns LLNID and the new types described in this paper refer to LLNID. A network intrusion in this context means one or more transmissions across the network that involves an intrusion. A single Internet transmission is often called a packet. Therefore, using this terminology, the physical manifestation of an intrusion on a network is one or more packets, and intrusion detection is the detection of these packets that constitute intrusions. In this context, intrusion detection is similar to data mining. Intrusion detection research needs a model of types of intrusions and types of intrusion detection that benefits analysis of methods. This research focuses only on LLNID. These are the proposed types of intrusions for the special case of local landline network intrusion detection that facilitate intrusion detection research analysis in the LLNID context:

Type 1 Intrusion: An intrusion which can be positively detected in one or more packets in transit on the localnetwork in a given time period.
Type 2 Intrusion: An intrusion for which one or more symptoms (only) can be detected in one or more packets in transit on the local network in a given time period.
Type 3 Intrusion: An intrusion which cannot be detected in packets in transit on the network in a given time period.

These three types of intrusions are necessary for analytical research in order to indicate and compare kinds of intrusions. A positive intrusion is different than only a symptom of an intrusion because immediate action can be taken on the first whereas further analysis should be taken on the second. Both of these are different than intrusions which have been missed by an LLNIDS. To show that these three types are mutually exclusive and are complete for a given time period, consider all of the intrusions for a given time period, such as a 24-hour day. The intrusions which were positively identified by the LLNIDS are Type1 intrusions. Of the remaining intrusions, the ones for which the LLNIDS found symptoms are Type 2. Here the hypothesis is that the LLNIDS can only find an intrusion positively or only one or more symptoms are found. No other results can be returned by the LLNIDS. Therefore, the remaining intrusions are Type 3, which are intrusions not detected by the LLNIDS. No other types of intrusions in this context are possible.

Figure 2 is a diagram that illustrates the types of intrusions as described above. An intrusion is either Type 1, Type 2, Type 3, or it is not an intrusion. Those were the types of intrusions. Next are the types of intrusion detection.

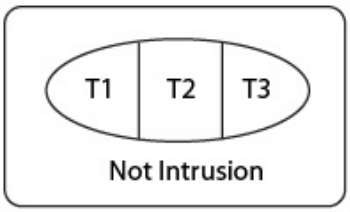

Figure. 2. Types of Intrusions for LLNIDS

There are three types of network intrusion detection that correspond to the three types of intrusions in the LLNID context:

- **Type 1 Network Intrusion Detection:** A Type 1 Intrusion is detected in a given time period.
- **Type 2 Network Intrusion Detection**: One or more symptoms (only) of a Type 2 Intrusion are detected in a given time period.
- **Type 3 Network Intrusion Detection**: No intrusion is detected in a given time period.

Admittedly, Type 3 is not a detection but the lack of detection. It is included because these three types of detection correspond to the three types of intrusions and Type 3 Intrusion Detection facilitates analysis of intrusion detection methods. Examples of Type 3 Intrusion Detection are nothing was detected; no attempt was made at detection; an intrusion occurred

but was not detected by the LLNIDS; and, no intrusion occurred. All of these have the same result: there was no detection of an intrusion by the LLNIDS.

Each of the three network intrusion detection types is necessary to describe all of the types of intrusion detection. A positive detection of an intrusion is different than just a symptom of an intrusion because a positive detection can be immediately acted upon while a symptom indicates that further analysis is needed. Both of these are different than intrusions that are missed by network intrusion detection. To show that these types are mutually exclusive and complete for a given time period, consider an LLNIDS looking at network packets for a given time period, say a 24-hour day.

For all packets that the LLNIDS determines positively indicates an intrusion the LLNIDS has accomplished Type 1 intrusion detection. Of the remaining packets, for each packet that the LLNIDS determines is a symptom of an intrusion the LLNIDS has accomplished Type 2 intrusion detection. The remaining packets represent Type 3 intrusion detection. These three types of network intrusion detection are complete in this context because they cover all possibilities of intrusion detection. In common language, Type 1 is a certainty, Type 2 is a symptom, and Type 3 is an unknown.

Those were types of intrusion detection. Next are types of methods and alerts. LLNID methods can be defined in terms of the three intrusion types:

- **Type 1 NID Method/Alert**: A method that detects a Type 1 Intrusion and an alert that indicates a Type 1 Intrusion.
- **Type 2 NID Method/Alert**: A method that detects a symptom of a Type 2 Intrusion and an alert that indicates a symptom (only) of a Type 2 Intrusion.
- **Type 3 NID Method/Alert**: A method that does not exist, thus there is no alert.

These types of methods and alerts are necessary to differentiate that some methods are positively correct, other methods only indicate symptoms of intrusions, and some methods do not exist. They are mutually exclusive because a local method either positively indicates an intrusion (Type 1), it only detects a symptom of an intrusion (Type 2), or it does not exist (Type 3). They are complete because there are no other types of methods in this context.

Those were types of methods and alerts. Next are types of false positives. The term false positive generally has meant that an intrusion detection system has sent a false alarm. False positives are generally undesirable because the false positive rate of intrusion detection systems can be high and can use up a lot of seemingly unnecessary, and limited, resources. However, with these new types, the concept of a false positive is different for different intrusion detection types in the LLNIDS context.

- Type 1 False Positive: A Type 1 Method produces an alarm in the absence of an intrusion.
- Type 2 False Positive: A Type 2 method produces an alarm in the absence of an intrusion.
- Type 3 False Positive: Does not exist because no alarm is produced.

A Type 1 False Positive indicates a problem with the Type 1 method which should be corrected. Type 2 False Positives are expected because Type 2 Methods do not positively detect intrusions, they only detect symptoms of intrusions. There is no Type 3 False Positive because no detections and alerts are produced for Type 3 Intrusion Detections. These types of false positive are necessary because they each indicate separate network intrusion detection issues. Type 1 is a network intrusion detection problem which needs to be corrected and Type 2 is expected. The two types of false positive are mutually exclusive and complete because only Type 1 NetworkIntrusion Detection can produce a Type 1 False Positive and only Type 2 Network Intrusion Detection can produce a Type 2 False Positive. No other types of false positives in this context are possible. Since Type 1 and Type 2 of local network intrusion detection methods are mutually exclusive, these are also mutually exclusive.

Figure 3 is a Venn diagram which illustrates types of intrusion detection in the LLNIDS context. The horizontal line separates intrusions at the top from non-intrusions at the bottom. A Type 1 detection is in the upper left of the circle if it is actually an intrusion or it is in the lower left of the circle if it is a false positive. A Type 2 detection is in the upper right of the circle if it is actually an intrusion or it is in the lower right of the circle if it is a false positive. Everything outside of the circle is Type 3 detection whether it is an intrusion or not.

This typing system allows illustration that empirically most intrusion detection is not Type 1 (positive detections), but Type 2 (symptoms of detections), and Type 3 (missed detections). This differentiation is essential in proceeding in a scientific way for improved intrusion detection. Previously labeled types of intrusion detection do not fit neatly into these three new types. Misuse detection, for example, in some cases could indicate a definite intrusion and would then be Type 1, or it could indicate only symptoms of intrusions in other cases and would then be Type 2. The comparison of false positives of different methods of Misuse Detection is an invalid technique unless Type methods are compared only with Type 1 methods and Type 2 methods are compared only with Type 2 methods. Anomaly detection, for example, would tend to be Type 2, but some anomalies could clearly indicate intrusions and would be Type 1. Type 1 and Type 2 methods of Anomaly Detection should be separated before making any comparisons. Likewise with intrusion detection labels based on activity, appearance, authentication analysis, behavior, knowledge, models, profiles, rules, signature, static analysis, statistics, and thresholds. These are still useful as descriptive terms, but they are not as useful in analyzing methods of determining whether or not an intrusion has occurred because they allow the comparisons of apples and oranges in numerous ways. The labels Type 1 and Type 2 give us more analytical information: either an intrusion has occurred or else only a symptom of an

intrusion has occurred. Type 3 intrusions tell us that we should find out why an intrusion was not detected in the network traffic so that we can create new rules to find more intrusions in the future. Previously labeled types of intrusion detection do not give us as much analytical information as do types 1, 2, and 3.

Using this system, one can clearly state objectives of LLNID research in a new way which was previously only implied. The significance of given time period is apparent in the descriptive of these objectives because the objectives are stated in terms of progress from one time period to another time period. Here are specifics for LLNID research:

- **Type 3 NID Research:** Find ways of detecting intrusions that are currently not being detected, moving them up to type 2 or 1 intrusion detection.
- **Type 2 NID Research:** Improve Type 2 Intrusion Detection with the goal of moving it up to Type 1 Intrusion Detection.
- **Type 1 NID Research:** Improve Type 1 Intrusion Detection so that it is faster, uses fewer resources, and has fewer false positives.

Each of these types of research are necessary because finding new methods of intrusion detection is different than improving symptom detection which is different than making Type 1 Intrusion Detection more efficient. They are also complete because there are no other types of intrusion detection research in this context.

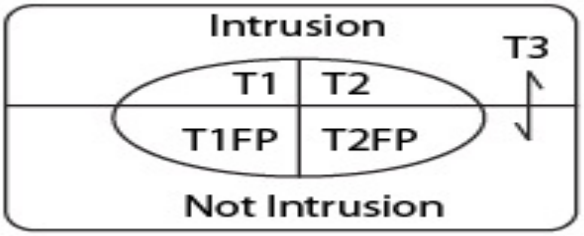

Figure 3. Types of Intrusion Detection for LLNID

Table 1 summarizes the types discussed in this section. These are some ways of how researchers can use these types: research that compares false positive rates of Type 1 methods with false positive rates of Type 2 methods is not valid because Type 1 methods are not supposed to have false positives whereas Type 2 methods are expected to have false positives. Discounting Type 3 intrusion detection because of the amount of time taken may be irrelevant if otherwise the intrusion would not be found, at all. Proposing that intrusion prevention will replace intrusion detection is a false claim so long as types2 and 3 intrusions continue to exist. Rather than disregarding Type 2 methods, research should attempt to fuse the results of Type 2 methods in order to move them up to Type 1.

TABLE I
SUMMARY OF LLNID TYPES

	Type 1	Type 2	Type 3
Intrusion	This can be positively detected by LLNIDS	A symptom of this can be detected by LLNIDS	This is not detected by LLNIDS
Intrusion Detection	This positively detects an intrusion	This detects one or more symptoms (only) of an intrusion	An intrusion is not detected
Method	How to positively detect an intrusion	How to positively detect a symptom of an intrusion	An intrusion is not detected
Alert	This positively signifies an intrusion	This signifies a symptom of an intrusion	This does not occur
False Positive	An alert positively signifies an intrusion, but there is no intrusion	An alert signifies a symptom of an intrusion, but there is no intrusion	An alert does not occur
Research	Improve Type 1 Intrusion Detection, such as by increasing the speed of detection, using less resources, and having fewer false positives	Improve Type 2 Intrusion Detection so that it becomes Type 1 Intrusion Detection	Detect Type 3 intrusions so that they become Type 2 or Type 1

III. TOOLS OF NIDS

In order to ensure an invulnerable security of data, various tools are available. They are mainly used altogether in order to secure the system as a whole. There is no perfectly complete system. The optimum security is achieved as a esult of the combination of several systems. Moreover, most of these solutions are developed by the leading companies of securities. These solutions are complete and can be easily put in work in a network, which is also true for the updates. The modular format used by these allows them to have several agents for a centralized interface. However, these solutions are particularly very expensive.

The table below shows a study of the most used solutions of detection and prevention in the domains of commerce and open sources.

Tools	CA eTRUST Intrusion Detection 3.0	Juniper IDP	McAfee Intrushield série I	McAfee Entercept 5.0	Snort 2.1.3	SonicWALL IPS service
Analysis of real-time traffic	Yes	Yes	Yes	Yes	Yes	Yes
Detection of viruses / worms / Trojans	Yes	Yes	Yes	Yes	Yes	Yes
Detecting external attacks	Yes	Yes	Yes	Yes	Yes	Yes
Detection of internal attacks	Yes	Yes	Yes	Yes	Yes	Yes
Ability to block attacks	Yes	Yes	Yes	Yes	Yes	Yes
Detection of external probes	Yes	Yes	Yes	Yes	Yes	Yes
Detection of internal Probes	Yes	Yes	Yes	Yes	Yes	Yes
Probes Ability	Yes	Yes	Yes	Yes	Yes	Yes
Definitions of blocking	Yes	Signatures with state data, protocol anomaly detection, backdoors, abnormal traffic, protection of layer 2, Syn Flood, Profiling enterprise security	Updates, block lists and user-defined customizable rules	Updates, block lists and user-defined customizable rules	Update, third-party integration, user-customizable	Updates
Real-time alert	E-mail, pager, application performance, SNMP, console	E-mail, syslog, SNMP, log file, external SMS	Console, email, pager, SMS email	Console, email, pager, SNMP, generation of process	Log files, email, console, third-party applications	Log files, email, syslog, SGMS
Getting logs data packets	Workspace, ODBC database	Syslog, internal database	Oracle, MySQL	Microsoft SQL Server	SS	SS
Search for content	Yes	Yes	SS	SS	Yes	Yes
Content Filtering	Yes	Yes	SS	SS	Yes	Yes
Filtering methods	URL database	Set by the administrator	SS	SS	Set by the administrator	Blacklist, third, set by the administrator
Reporting tools	Yes	Yes	Yes	Yes	SS (sold separately)	SS (sold separately)
Compatible operating system	Win 2000, Win 2000/2003/XP for the engine remotely	Windows, Linux, Solaris	Windows	Windows, Solaris, HP/UX	Linux, Windows	All IP environment

IV. CONCLUSION

This paper provided a new way of looking at network intrusion detection research including intrusion detection types that are necessary, complete, and mutually exclusive to aid in the fair comparison of intrusion detection methods and to aid in focusing research in this area. We are working on the implementation of a screening tool of attack and the characterization of test data. We also focus on the collection of exploits and attacks to classify and identify. Further work is under way and many ways remain to be explored. Then it would be interesting to conduct assessments of existing IDS following the approaches we have proposed and tools developed in this work.

REFERENCES

[1]. Langin, C. L. A SOM+ Diagnostic System for Network Intrusion Detection. Ph.D. Dissertation, Southern Illinois University Carbondale (2011)

[2]. Amoroso, E.: Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Intrusion.Net Books (1999)

[3]. Denning, D.: An Intrusion-Detection Model. IEEE Transactions on Software Engineering 13(2), 118-131 (1986)

[4]. Young, C.: Taxonomy of Computer Virus Defense Mechanisms. In : The 10th National Computer Security Conference Proceedings (1987)

[5]. Lunt, T.: Automated Audit Trail Analysis and Intrusion Detection: A Survey. In : Proceedings of the 11th National Computer Security Conference, Baltimore, pp.65-73 (1988)

[6]. Lunt, T.: A Survey of Intrusion Detection Techniques. Computers and Security 12, 405-418 (1993)

[7]. Vaccaro, H., Liepins, G.: Detection of Anomalous Computer Session Activity. In : Proceedings of the 1989 IEEE Symposium on Security and Privacy (1989)

[8]. Helman, P., Liepins, G., Richards, W.: Foundations of Intrusion Detection. In : Proceedings of the IEEE Computer Security Foundations Workshop V (1992)

[9]. Denault, M., Gritzalis, D., Karagiannis, D., Spirakis, P.: Intrusion Detection: Approach and Performance Issues of the SECURENET System. Computers and Security 13(6), 495-507 (1994)

[10]. Crying wolf: False alarms hide Newman attacks, Snyder & Thayer Network World, 24/06/02, http://www.nwfusion.com/techinsider/2002/0624security1.html

[11]. F. Cikala, R. Lataix, S. Marmeche", The IDS/IPS. Intrusion Detection/Prevention Systems ", Presentation, 2005.

[12]. Hervé Debar and Jouni Viinikka, "Intrusion Detection,: Introduction to Intrusion Detection Security and Information Management", Foundations of Security Analysis and Design III, Reading Notes in to Compute Science, Volume 3655, 2005. pp. 207-236.

[13]. Hervé Debar, Marc Dacier and Andreas Wespi, "IN Revised Taxonomy heart Intrusion Detection Systems", Annals of the Telecommunications, Flight. 55, Number,: 7-8, pp. 361-378, 2000.

[14]. Herve Schauer Consultants", The detection of intrusion…", Presentation: excerpt of the course TCP/IP security of the Cabinet HSC, March 2000.

[15]. ISS Internet Risk Impact Summary - June 2002.

[16]. Janne Anttila", Intrusion Detection in Critical Ebusiness Environment ", Presentation, 2004.

[17]. D K. Müller", IDS - Systems of intrusion Detection, Left II ", July 2003, http://www.linuxfocus.org/Francais/July2003/article294.shtml

Biographies

Abhishek Gupta received his B.TECH in CSE from UPTU Lucknow in 2010. He is currently pursuing his M.TECH in CSE from JUIT, WAKNAGHAT, SOLAN (H.P.). His area of interest includes network security and computer networks.

Mohit Kumar received his B.TECH in CSE from PUNE UNIVERSITY in 2009. He is currently pursuing his MTECH in CSE from JUIT, WAKNAGHAT, SOLAN (H.P.). His area of interest includes network security and computer networks.

Anamika Rangra currently pursuing B.TECH in CSE from JUIT, WAKNAGHAT, SOLAN (H.P.). Her area of interest includes network security, computer networks and adhoc networks.

Vikas Tiwari received his B.TECH in CSE from RGTU Bhopal in 2010. He is currently pursuing his M.TECH in CSE from JUIT, WAKNAGHAT, SOLAN (H.P.). His area of interest includes network security and computer networks

Pravesh Saxena received his B.TECH in CSE from Chhattisgarh Swami Vivekanand Technical University (CSVTU) in 2010. He is currently pursuing his M.TECH in CSE from JUIT, WAKNAGHAT, SOLAN (H.P.). His area of interest includes network security and computer networks