IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. VI (May-Jun. 2014), PP 23-27
www.iosrjournals.org

The Approaches to Amalgamate the Anti-Network Attacks Technologies in Intrusion Detection and Prevention Systems

Aaruni Goel[1], Madhup Sharma[2], K.M. Pandey[3]
[1](Assistant Professor, Department of Information Technology, MIET, Meerut, India)
[2,3](Assistant Professor, Department of Computer Science, IIMT Engg. College, Meerut India)

Abstract: *A Network Intrusion Detection Prevention System (IDPS) is a mechanism that continuously monitors the network traffic and finds out the malicious, suspicious and undesired network activities. After identifying any illegitimate activity it simply blocks it and changes the security environment as per the rules set by policy maker(s). It should be noted that this task of monitoring is accomplished in real-time mode so that the only genuine network traffic is allowed to pass through the IPS without noticeable delay. Additionally, some organizations employ many other technologies on the place of IDPSs that present the same ability as IDPSs does and also match with the competencies of IDPSs. In this paper, we will focus on some of these matching technologies: network forensic analysis tools, anti-malware technologies (antivirus software) and firewalls and routers. Each of these technologies are now briefly explained giving the information how its use help in detecting intrusion and its avoidance stating relationship of these technologies with IDPSs. Suggestion will be added to appropriation telling how we should use these technologies along with IDPSs.*

Keywords: *Forensics Tools, Antivirus technologies, Firewalls, Routers, Host Intrusion Detection System (HIDS), Wireless Intrusion Detection System (WIDS)*

I. Introduction

The security problem appears especially important with the rapid development of network and information technology today. As a standard solution of monitoring and identification attacks, Intrusion Detection System has become an important component of security defense system in depth. IDS collect network traffic information from some points on the network or computer system which to be then analyzed to find whether there is any violation of system security strategy and the signs of being attacked [1]. Each and every aspects of technology has its own benefits and disadvantages. The same rule is also applied in network security in terms of detection and prevention especially by identifying performances, accuracies and time to respond issues. This all should also be achieved by taking consideration of lower rates of false positives and false negatives aspects or some sort of optimized form of tuning between them. Different organizations have their different needs and therefore different workings, for example a network-based IDPSs cannot monitor wireless protocols likewise a host based IDPS cannot analyze the network based IDPS effectively. Further variety of other technologies like Firewalls, Anti-viruses, Forensic Tools, Sniffers and so on, can be also associated to enhance the detection proficiencies to handle any type of incident and thereby to make network systems more secure. Using multiple technologies also verifies the validity of alerts which in result makes the task of any forensic expert more sophisticated and accurate.[3][4]

In this paper we summarized two categories in which IDPS related securities can be classified on the basis of their deployment:

In the first case all the related products (NIDS, HIDS, WIDS) are assumed to be manufactured by same vendor. This can provide the opportunity of data sharing without any extra effort to be done by network administrator. Using multiple technologies from same vendor is very time savvy and makes the task of traffic analysis and correlation very easy since all the concerned data fields are same and there is in general no need to transform the format of one data field into another. The only disadvantage in this type of

integration is that if one technology fails then it may impact or compromise the result of another IDPS technology. [9][14]

In the second case a spate dedicated software is used which is designed to import information from various security-related logs of different anti-attacks technologies and correlate events among them. Log types commonly supported by this software include IDPSs, firewalls, antivirus software, and other security software (e.g., audit logs); application servers (e.g., web servers, email servers). This software generally works by receiving copies of the logs from the logging hosts over secure network channels, then converting the log data into standard fields and values through normalization, and finally identifying related events by matching IP addresses, timestamps, usernames, and other characteristics[2]. The above mentioned anti-attack technology can identify malicious activity such as attacks and malware infections, as well as misuse and inappropriate usage of systems and networks. On the basis of outcome this dedicated initiates prevention responses for designated events.

This dedicated software has the advantages that it can identify some types of events that individual IDPSs cannot because of its ability to correlate events logged by different technologies. The consoles for this software can make data from many sources available through a single interface, which can save time for users that need to monitor multiple IDPSs. The console of this software also may offer analysis and reporting tools that certain IDPSs' consoles do not. At last users can more easily verify the accuracy of IDPS alerts because this dedicated software may be able to link each alert to supporting information from other logs. This can also help users to determine whether or not certain attacks succeeded[7].

The only disadvantage is that it is very time consuming to configure this software. Further it also requires expertise to handle the tradeoff between false positive and false positive.

Recently an alternative approach is used for centralized logging based primarily on the syslog protocol. Syslog provides a simple framework for log generation, storage, and transfer that any IDPS could use if designed to do so. Some IDPSs offer features that allow their log formats to be converted to syslog format. Syslog is very flexible for log sources, because each syslog entry contains a content field into which logging sources can place information in any format. However, this flexibility makes analysis of the log data challenging. Each IDPS may use many different formats for its log messages, so a robust analysis program would need to be familiar with each format and be able to extract the meaning of the data within the fields of each format. It might not be feasible to understand the meaning of all log messages, so analysis might be limited to keyword and pattern searches. Generally, the use of syslog for centralized collection and analysis of IDPS logs does not provide sufficiently strong analysis capabilities to support incident identification and handling since it they are in their phase of beginning [9][11].

II. Anti Network Attack Technologies

Some of these technologies which we considered are necessary to discuss so far are as follows:

2.1 Network Forensics Tool (NFT)

Network forensic analysis tool (NFT), on the primary base, work collecting as well as analyzing the traffic of a wired network. Differing from IDPSs based on the network, that works for performing a deep analysis and capture the traffic of network that is essential, an NFT on the contrary first captures nearly all the network traffic that it covers out and then do an analysis of the traffic that has been stored or captured by it. Besides the forensic abilities, some of the other abilities are also there which can be performed by the NFT software to give analysis as a major work[6]. Few of them are as follows[11]:

-Rebuilding of events with the help of replay of network traffic only inside the limits of tool, that have the range starting from an individual session (for example, use of Instant Messaging among the two users) till all the sessions that occur in that particular period. On the need basis, adjustment can be made to replaying speed.

-Creating a picture of traffic flows and the relation created between the hosts. There are some tools which can bind IP addresses, domain name or data related to physical locations and create a picture map for the activity done.
-Creating a picture of profiles for the distinctive activities and recognition of important variations.
-Searching the matter of application for particular keywords (for example, "threat", "virus").But in NFT value is given for the use for network forensics and decrease its value for the detection of intrusion and anticipation unlike a distinct IDPSs based on network[13].
A balance is made for IDPSs by NFT software in several ways which consists of the following:
-On the basis of its value, NFT software come a step ahead over IDPSs software for the network forensics due to the reason of its wide packet logging.
-Reduction of load on IDPSs, based on the network, can be done by performing packet logging using NFT software.
-NFT software may show its best suitability for customization, particularly for content searches (for example, keywords), if compared with other technologies used for IDPSs.
-Unlike the console of IDPSs, graphical user interface (GUI) of NFT software might shows its ability for analyzing, for visualization and moreover for reporting purposes too[4].
There are some restrictions that NFT software faces which can be concluded as:
-Detection of intrusion cannot be made using NFT software particularly for IDPSs that are based on network.
-Usually, there are no capabilities of prevention of intrusion that is offered by NFT software.

2.2 Antivirus Technologies

Technically, for the control of threats caused due to malware detection, on the majority, antivirus software have been employed at the common level. Malware that can be detected using this software consists of viruses, worms, Trojan horses, malicious mobile code, and a mixture of several threats, along with attacker tools such as keystroke loggers and backdoors. Antivirus software usually keep an eye over dangerous OS components, system files, and activities that show sign of presence of malware in an application, and efforts made by files that are either disinfect or quarantined which may consist of malware. Most of the organizations now make use of antivirus software on both ways, firstly, central base i.e., email servers, firewalls and lastly, local base i.e. file servers, laptops, etc. so as to ensure complete scrutiny of each entry for malware detection.

Primarily, threats are detected by analysis that is signature-based with the use antivirus products. Experience based methods and techniques are also deployed by it that look at the activities of some doubtful characteristics for recognizing the unknown threats which were previously detected. Signatures of new threats are created and being released by the vendors of the product so as to keep software up-to-date with information of malware that help detecting threats by the product.[13]
There are several ways that antivirus software accompanies IDPSs, some of which are:
-IDPSs unremarkably know minor malware uncovering capabilities; therefore so many threats can be detected with the help of antivirus software rather with the use of IDPSs.
-IDPS application might denote that spreading of worm is basically based on remarkable flow of traffic, but there is the chance that type of worm is not detected. On the contrary, antivirus software has the ability to identify the worm, if software is well updated to the signatures for the threats to be detected.
-Few loads can be taken by antivirus software through IDPSs, like identification of typical worm and to disable the signature of that worm that IDPSs sensors have. This is especially useful during a widespread malware contamination, when IDPSs strength overwhelmed with alerts and new useful events occurring at the unvaried indication might be ignored by users of IDPSs[14].

There are several boundaries that antivirus software has in relation to IDPSs which may be described as:
-No threats can be detected by antivirus software other than malware.

On the contrary, NBA software and IDPSs based on network show their capabilities more to identify worms of network service due to the reason that only few applications protocol are detected by antivirus software. But, NBA software and network based IDPSs have the ability to detect any type of protocol.

Till the revision of signatures of new threats by the vendors, threats are not detected by antivirus software. In few cases, mainly for the threats that have easily recognized characteristics, an IDPS can find the new danger during this pane of time because IDPS administrators can configure his IDPS accordingly. On the other hand Antivirus software typically does not permit administrators to compose signatures.

2.3. Firewalls and Routers

Firewalls (network-based and host-based) and routers filter meshwork reciprocation supported on TCP/IP characteristics such as the seed and instruction IP addresses, the major protocols (e.g., TCP, UDP, ICMP), and primary protocol assemblage (e.g., TCP or UDP port book, ICMP type and encrypt). Most firewalls and routers logs attempt of attackers; the closed manifestation is often generated by unofficial way attempts from automated tools, active and passive scanning, and malware. Some network-based firewalls also act as proxies[10]. When a agent is misused, each thriving transportation effort actually results in the beginning of two separated connections: one between the guest and the placeholder server, and another between the placeholder server and the admittedly goal. Numerous proxies are specific to application, and few usually carry out an analysis and common application protocols like HTTP are validated. The request of client may be rejected if proxy finds it invalid (that may have some type of attacks) and create a log file for such type of requests[5].

Network-based firewalls and routers oftentimes fulfill system code translation (NAT), which is the outgrowth of process addresses on one material to addresses on other textile. NAT is most oftentimes realized by function snobbish addresses from an inner system to one or solon unrestricted addresses on a meshwork that is joined to the Cyberspace. Firewalls and routers that action NAT typically disk each NAT speak and procedure. IDPS users may beggary to pass use of this mapping substance to determine the literal IP direct of a multitude behind a device performing NAT.

If a latest network-bome threat like worm in network service or attack on service, etc. cannot be stopped by IDPSs and other softwares of security like antivirus software then configuration of firewall or routers is reconstructed to stop that threats.

On the basis of above discussion, typical threats can be blocked by reconfiguring firewalls or routers using IDPSs.

There are several restrictions that firewalls and routers exhibit in relation to IDPSs. These can be as follows:

-Mostly, there is no detection of malicious activity by firewalls and routers.

-Firewalls and routers typically log relatively short aggregation, much as the canonic characteristics of denied form attempts exclusive and they rarely record the substance of any packets.

III. Conclusion

At last we have mentioned that how secured system can be designed in terms of networking. But still many bottleneck problems persists like the installation and maintenance cost of complete setup, expertise hands on IDPS and above said tools and components specially the configuration of tuning between false positive and false negative to check out the data traffic are the name of few. Further, by default, these products function completely independently of each other. This has some notable benefits, such as minimizing the impact that a failure or compromise of one IDPS product has on other IDPS products. However, if the products are not integrated in any way, the effectiveness of the entire IDPS implementation may be somewhat limited. IDPS products can be directly integrated, such as one product feeding alert data to another product, or they can be indirectly integrated, such as all the IDPS products feeding alert data into a security information and event management system.

References

[1]. Denning and Dorothy, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, 1987.
[2]. Lee W andStolfo S J. "A framework for constructing features and models for intrusion detection systems". ACM Transactions on Information and System Security, 2000.
[3]. Alessandri D, Chichin C and Dacier M, "Towards a taxonomy of intrusion detection systems and attacks",2001.
[4]. Matthew Tanase, The Future of IDS, 2002. http://www.securityfocus.com/infocus/1518
[5]. Kayacik.G. and Zincir-Heywood A. N., "Evaluation of the Cisco 10.9 Firewall with Darpa 99 Dataset", Technical Report, Faculty of Computer Science, Dalhousie University, November 2002.
[6]. Gou, X. , W. Jin, and D. Zhao, Multi-agent system for Worm Detection and Containment in Metropolitan Area Networks. Journal of Electronics (China), 2006. 23(2): p. 259-265.
[7]. Bolzoni, D. and S. Etalle, APHRODITE: an Anomaly-based Architecture for False Positive Reduction. 2006, Centre for Telematics and Information Technology, University of Twente: Enschede.
[8]. Open Source Host-based intrusion detection system, 2007. http://www.ossec.net/
[9]. Stakhanova N., Basu S., Wong J.: A Taxonomy of Intrusion Response Systems. International Journal of Information and Computer Security, Volume 1, Issue ½, Jannuary (2007).
[10]. Paper, W. (n. d.). Firewalls – Overview and Best Practices. www.decipherinfosys.com/Firewall.pdf
[11]. Distributed Intrusion Detection System. http://www.dshield.org/
[12]. Li, Y. , Yao, H. , Chen, M. , Jaggi, S. , Rosen, A. Ripple authentication for network coding (2010) Proceedings of the 29th Conference on Information Communications, pp. 14-19. , March 15-19, 2010, San Diego.
[13]. Berkenkopf, R. B. S. , G Data Malware Report. 2010.
[14]. Mcafee and Lab, 2013 Threats Predictions. 2013.

This heading is not assigned a number.

A reference list **MUST** be included using the following information as a guide. Only cited text references are included. Each reference is referred to in the text by a number enclosed in a square bracket (i.e., [3]). References **must be numbered and ordered according to where they are first mentioned in the paper,** NOT alphabetically.

Examples follow:

Journal Papers:

[1] M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116. (8)

Note that the journal title, volume number and issue number are set in italics.

Books:

[2] R.E. Moore, Interval analysis (Englewood Cliffs, NJ: Prentice-Hall, 1966). (8)

Note that the title of the book is in lower case letters and italicized. There is no comma following the title. Place of publication and publisher are given.

Chapters in Books:

[3] P.O. Bishop, Neurophysiology of binocular vision, in J.Houseman (Ed.), Handbook of physiology, 4 (New York: Springer-Verlag, 1970) 342-366. (8)

Note that the place of publication, publisher, and year of publication are enclosed in brackets. Editor of book is listed before book title.

Theses:

[4] D.S. Chan, Theory and implementation of multidimensional discrete systems for signal processing, doctoral diss., Massachusetts Institute of Technology, Cambridge, MA, 1978. (8)

Note that thesis title is set in italics and the university that granted the degree is listed along with location information

Proceedings Papers:

[5] W.J. Book, Modelling design and control of flexible manipulator arms: A tutorial review, Proc. 29th IEEE Conf. on Decision and Control, San Francisco, CA, 1990, 500-506 (8)