Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
IJMTER
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

A THROUGH INVESTIGATION OF FLOW-BASED AND INFORMATION FLOW BASED ANALYSIS METHODS FOR INTRUSION DETECTION SYSTEM

[1]R. Dhanapakkiyam, [2]Dr. K. Saraswathi

[1]*M.Phil Scholar, Department of Computer Science, Government Arts College, Coimbatore.*
[2]*Assistant Professor, Department of Computer Science, Government Arts College, Coimbatore.*

Abstract–Security threats for computer systems have increased immensely with viruses, denial of service, vulnerability break-in, etc in the recent years. In recent work several number of security mechanisms have been introduced to determine the threats in computer system. But none of the security mechanisms might absolutely detect in computer system. Intrusion Detection System (IDS) is an important area of study to detect attacks in computer system. Conventionally, the IDS scheme is taken into the account to discover attacks to study the contents of every packet. Though, packet inspection mightn't straightforwardly be performed on high-speeds. In recent work researchers considered an Information Flow-Based IDS (IFB-IDS) to recognize attacks in computer network systems. In those flow-based IDS, the flow of packet transmitted throughout the network is considered, as an alternative of the inside of every individual packet. The major objective of this paper is towards survey the issues of Information Flow-Based Intrusion Detection System. The survey starts with an initial stage of the work for researchers to know the procedure of IFB-IDS. The concept of existing Information Flow-Based IDS (IFB-IDS) is explained in detail and appropriate standards are identified. IFB-IDS methods are able to be used to identify several numbers of attacks such as worms, Botnets and Denial of Service (DoS) attacks and classify those attacks. The existing Information flow-based Seclius method is consider ably decrease human being involvement via automatically learning system characteristics with easy mechanism with the intention of administrators be able to use to describe security requirements is also studied at end of the work.

Keywords–Intrusion Detection Systems (IDS), system security metric, flow based analysis and information flow-based analysis.

I. INTRODUCTION

Currently hackers are constantly violating network systems, it would be motivating toward examine the network and their users is attacker or not. Taking into consideration the damage basis through the attacks (billions of U.S. dollars) [1], it is significant toward distinguish attacks as soon as probable, and obtain, if possible, appropriate actions on the way to stop them. This assignment is predominantly difficult appropriate to the variety of structure in the form of information gathering, password theft, viruses, Trojan horses, Denial of Service (DoS) attacks. The increasing amount of safety incidents [2] designate with the purpose of existing approaches to building systems mightn't adequately deal with variety of threats and attacks earlier than systems are cooperating. Consequently, organizations should choice toward trying to notice malicious action with the purpose of occurs; therefore well-organized intrusion detection systems (IDSes) [3] are organized toward observe the systems and recognize

misbehavior. On the other hand, IDSes alone are not adequate to permit operators to identify with the safety condition of their organization, since monitoring sensors frequently report each and every one potentially malicious traffic not including regard to the concrete network configuration, vulnerabilities, and mission collision.

To the discovery of network attacks, some of the systems have been introduced in recent work which is named as Network Intrusion Detection Systems (NIDS). In an effort to discover well-known attacks, these NIDS systems conventionally examine the consignment of each packet [4]. The difficulty of packet examination, on the other hand, is inflexible, to achieve it at the speed of numerous Gigabits per second (Gbps) [5]. Designed for high-speed lines, it is consequently significant to examine substitute to packet examination.

Flooding attacks broad cast numerous spurious packets to the destination node, waste Central Processing Unit (CPU), memory, and network assets. In case of Transmission Control Protocol (TCP) Synchronization (SYN)flood, the casualty receives packets with the intention of go beyond buffer of the information structure boundary and stops its service. Moreover Internet Control Message Protocol (ICMP),Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) flooding attacks have been disseminated over the network through sending inadequate transmission of packets. Some attacks, such as Smurf and Fraggle, intensify traffic through via reflecting services of the Third Party.

To detect the attacks, Network-Based Intrusion Detection Systems (NIDS) is proposed in recent work some of the NIDS system such as snort, in a packet header or payload. The present NIDS techniques designed for the security-state estimation difficulty usually categorized into two major aspects. Firstly, presented methods majorly depend on human information and participation. The NIDS scheme administrator should examine the triggered IDS alert and physically assess their difficulty, which is able to rely on the alerts' accurateness, the fundamental system arrangement, and sophisticated safety requirements. If the size of computer networks rise, the labor-intensive inspection of alerts frequently becomes extremely tedious, if not impossible, in practice. Second, previous NIDS schemes designed for IDS alert association and system security condition evaluation frequently focus simply on the attack paths [6] and following concession escalations [5], not including considering dependencies among system assets. On the other hand, in practice, there are often ineffective to detect Web server crash, thus results ineffective defense overflow utilization.

Signature-based detecting systems have been also introduced in recent work to detect IDS, but it needs an enormous database which encloses information on each attack. But it results high communication overhead toward evaluate each packet through the signatures in the database. As a result, these Signature-based detecting systems are not suitable in a high-speed network. Since if new attacks come into sight, these system mightn't catch it. In adding together, packet information might be inadequate, since a number of types of attack are able to be detected simply through using from a series of packets information.

To solve the problem above mentioned IDS systems, Flow based Intrusion Detection System (FB-IDS) have been proposed in recent work and it is mainly focused by researchers. In FB-IDS approach, the communication patterns inside the network are examined, as an alternative of the consideration of packets information. Flow based Intrusion Detection System (FB-IDS) contains two major stages to detect attacks. At the primary stage, Flow based Intrusion Detection System (FB-IDS) approaches is able to be used to identify certain attacks. At the second stage, packet examination is able to be second-

hand to additionally defend serious servers, designed for which the initial stage has exposed suspicious actions. The major objective of this paper is towards survey the issues of Information Flow-Based Intrusion Detection System. The survey starts with an initial stage of the work for researchers to know the procedure of IFB-IDS. This means that IFB-IDS consider simply contributions in NIDS with the purpose of construct precise make use of network flows as their major input. An IFB-IDS method doesn't regard as payload-based methods [6-8]. Since IFB-IDS majorly focus on network flows. The remaining section of the paper is summarized as follows. In Section 2 provides an overview of the existing Flow-Based analysis methods. In section 3 provides the overview of Information Flow-Based Methods and issues of the existing Flow-Based analysis and Information Flow-Based Methods arede scribed in Section 4. Finally conclude the paper in Section 5 and scope of the future work is also specified in Section 5.

II. FLOW BASED ANALYSIS METHODS

Moore et al [9] discuss the overview of DoS attacks and how often it is disseminated over the network also discussed. Moore et al approximations conducted over numerous one-week traces used for a period of three years, on standard the numeral of diverse victim IPs on the complete Internet is 24.5/hours. But still they mightn't study the details of brute force or semantic attacks, since the information clearly describes the overview of DoS attack detection only. So it is useful to provide the information of Dos attack for researchers.

To solve the problem in [9] some of the anomaly-based DoS detection is proposed in recent work [10-11] with high-speed networks via the use of flow information based schemas. Li et al [10] and Gao et al [11], proposed a Flow based Intrusion Detection System (FB-IDS) schema depending on aggregate flow measures composed in suitable information structures, named sketches. A sketch is formerly a one-dimensional hash table appropriate designed for quick storing of information: it essentially calculation incidence of an occasion. These works majorly focus on the procedure of 2D sketches, a further in fluential expansion of the unique ones, in which, designed for every dimension, a position of flow-derived playing field is hashed. Sketches authorize to statistically differentiate how the traffic varies greater than time, basically through tracking the existence of a flow in a particular occasion frame. Anomaly-based intrusion detection schemas are relying on a forecast value of determining the scheme is theoretical to examine: a sharp variation beginning the mean is flagged as an anomaly. A comparable schema is proposed through Zhao [12]. In this case, data-streaming schemas are second-hand toward filter measurement of the interchange, and recognize IPs with the intention to shows an irregular amount of relations.

In recent years several numbers of methods have been introduced to detect the irregular network traffic depending on the following attacks such as internet worms [13], Do Sand scanning. Here the examiner network traffic is performed based on the number of flows, which is definite as group of packets with the intention of travel among the identical end points. Through aggregating packets through the purpose of belong to the in distinguish able flow be able to reduce processing overhead in the scheme. Distinguish traffic patterns with the intention of appear throughout attacks. As a result of using these traffic patterns, it can easily notice even altered attacks with the purpose of make use of a new port number. Furthermore, the method determination recognize attacks with the purpose of cannot be detected through investigative simply packet information, via the use of entire traffic information.

Hansmanet al [14] proposed a new Network-Based Intrusion Detection Systems (NIDS) to detect and categories the Network attacks into various attacks such as spoofing, session hijacking and parameter tampering. The previous categories must not be considered as mutual restricted classes of attacks. For instance consider, buffer overflows and port scans are able to be observing as divide group of attacks, although some of the specific techniques second-hand through worms and DoS attacks detection, Botnets attacks also identified by Lee et al [15]. Furthermore, Botnets are the great transportation designed for background up and sustaining any category of disseminated attack, such as DoS attacks and SPAM.

III. INFORMATION FLOW-BASED ANALYSIS METHODS

Several number of investigation schemas is proposed in recent work to detect and identify the DDOS attacks. A dynamic method is one of the most recently used methods to detect DDOS attack depending on graph examination [16] method. The major objective of this paper is to study and determine the system vulnerabilities, and then mine each and every one probable attack paths. The created graphis able to be second-hand to decide safety metrics [17], assess the security potency of a network [18], to recognize the largest part critical belongings in the association. They are able to also be second-hand predicatively toward rank IDS alerts.

In particular, [16] proposed a new flow based approach to find the malefactor's actions, building of attack graphs and calculation of diverse safety metrics. The approach is designed for using together at design and development phase of computer networks. The graph based schema uses a schema known as Topological Vulnerability Analysis (TVA) [19] to go with set of connections configuration through attack recreation in arrange to optimize IDS sensor assignment and to prioritize IDS alerts. TVA method examines the dependence among various vulnerabilities and shows each and every one potential attack paths addicted to a network. TVA discovers possible paths of vulnerability all the way through a network, showing precisely how attackers might break through a network. The main issue found from the attack-graph-based techniques is that it needs to know the assumption of attacker ability and vulnerabilities. There have been a number of efforts to take into account unidentified vulnerabilities throughout the scheme security examination.

On the other hand Zhang et al. [20] also proposed a schema to discover the design of predicting unidentified vulnerabilities in recognized software applications all the way through examination of the past accessible historical information. Zhang et al [20] make a conclusion with the purpose of the vulnerabilities mightn't go behind a specific pattern and therefore it is not appropriate for predictable accurately.

Of [21] develops a new schema based on logic hypothetical examination to determine which components of the system majorly affected by vulnerability attacks. In MulVAL, concise groups of Datalog rules confine general attack scenarios, together with make use of a variety of kinds of software vulnerabilities, and other common attack techniques. The hypothetical examination of unidentified vulnerabilities offers an enormous resolution to examine the impact of vulnerability in several specific points in the scheme; on the other hand, an absolute scheme safety examination would necessitate hypothesizing vulnerabilities in each possible scheme, but it is not easily applicable for large-scale transportation.

In [22] considerable enhancement of Net SPA attack graph method necessary to model additional present-day threats as well as countermeasures. Point-to-point reach ability algorithms as well as structures were expansively redesigned toward support "reverse" reach ability computation furthermore personal firewalls. Host-based vulnerability scans are imported along with analyzed. Investigation of a prepared network with 84 hosts demonstrates with the intention of client-side attacks pose a serious threat. These techniques make use of manually filled knowledge basis of alert applicability, organization configuration, and otherwise objective importance to combine a context through each alert as well as to provide situational awareness accordingly. To conclude security impact software vulnerabilities encompass on a particular network, individual must consider connections among several network elements. For a vulnerability investigation tool toward be useful during practice, two features are crucial. First, the representation used in the analysis must be able to repeatedly incorporate formal vulnerability qualifications from the bug-reporting community. Second, the investigations required to be able toward scale to networks through thousands of machines. Seclius offer practical solution as a result of minimizing as well as simplifying the required manual inputs. It does so through learn low-level system characteristics mechanically during order toward estimate accurately the extent toward which alerts influence critical components of the organization. Such damage assessment characteristics have earlier been explored by the use of file-tainting study used for malware detection offline forensic examination using backtracking and designed for online damage situational awareness.

At the network level, [23] developed a new vulnerability schema depending on definition language (OVAL) and create a dependency graph to determine the probable impact of vulnerabilities. In [23], information flow is tracked across manifold layers, specifically at the instruction stage and at the OS process stage. When compared all IFB-IDS schemes, the OVAL mechanism mightn't suffer from the issues of unidentified vulnerabilities and imperfect attack exposure. But the major limitation of defense-centric mechanism mightn't accurately track information which is processed by software. In addition it also initiates inaccurate associations among information objects.

IV. INFERENCE FROM EXISTING METHODS

During this process several numbers of issues were found which is described as follows,

- The main issue found from the attack-graph-based techniques is that it needs to know the assumption of attacker ability and vulnerabilities. There have been a number of efforts to take into account unidentified vulnerabilities throughout the scheme security examination.
- Zhang et al [20] make a conclusion with the purpose of the vulnerabilities mightn't go behind a specific pattern and therefore it is not appropriate for predictable accurately.
- The hypothetical examination of unidentified vulnerabilities offers an enormous solution to examine the impact of vulnerability in several specific points in the scheme; on the other hand, an absolute scheme safety examination would necessitate hypothesizing vulnerabilities in each possible scheme, but it is not easily applicable for large-scale transportation.
- Compared to earlier schemas cross-layer schema is more accurate, however it necessitate implementation in a virtual environment and be able to cause most important performance degradation.
- Compare to all of the methods Selicus based IFB-IDS schemas solve and overcome three major problems. First, it captures the distinguishing information admission and handing out actions of malware, and thus mightn't be straight forwardly evaded. Second, it discovers a malware relying on the hardware-level information and makes extremely small statement at software level, and

therefore cannot be easily cheated. Third, it is execute totally exterior of the victim scheme, and consequently strongly protected from being subverted.

- When compared all IFB-IDS schemes, the defense-centric mechanism mightn't suffer from the issues of unidentified vulnerabilities and imperfect attack exposure. But the major limitation of defense-centric mechanism mightn't accurately track information which is processed by software. In addition it also initiates inaccurate associations among information objects.

V. CONCLUSION AND FUTURE WORK

The major objective of this paper is to present a survey of issues of Information Flow-Based Intrusion Detection System. The survey starts with an initial stage of the work for researchers to know the procedure of IFB-IDS, particularly designed for examination of high-speed networks. The concept of existing Information Flow-Based IDS (IFB-IDS) is explained in detail and appropriate standards are identified. The major issues of the Flow Based schema are solved by using Information Flow-Based IDS (IFB-IDS) methods. In literature when compared to all of the methods Selicus based IFB-IDS schemas overcome three major problems. First, it captures the distinguishing information admission and handing out actions of malware, and thus mightn't be straightforwardly evaded. Second, it discovers a malware relying on the hardware-level information and makes extremely small statement at software level, and therefore cannot be easily cheated. Third, it is execute totally exterior of the victim scheme, and consequently strongly protected from being subverted.

So Selicus based IFB-IDS are able to be straight forwardly distinguish new types of attacks. But Seclius frequently assess the scheme safety to be close to complete, however not 100 % secure. Currently Seclius schema using static threshold values to determine the attackers. But this static threshold value is not appropriate to all network environments. Therefore, we necessitate finding a new method to establish the threshold value adaptively designed for a variety of network conditions.

REFERENCES

1. Computer Economics, "2007 malware report: The economic impact of viruses, spyware, adware, botnets, and other malicious code," Jul. 2008.
2. B. Schneier, ''Attack Trees,'' Dr. Dobb's J., vol. 24, no. 12, pp. 21-29, 1999.
3. S. Axelsson, ''Intrusion Detection Systems: A Survey and Taxonomy,'' U.S. Dept. Energy, Washington, DC, Tech. Rep. 99-15, 2000.
4. M. Roesch, "Snort, intrusion detection system," Jul. 2008.
5. M. Gao, K. Zhang, and J. Lu, "Efficient packet matching for gigabit network intrusion detection using TCAMs," in proceedings 20th international conference on advanced information networking and applications,2006 , 2006, pp. 249–254
6. P. Xie, J.H. Li, X. Ou, P. Liu, and R. Levy, ''Using Bayesian Networks for Cyber Security Analysis,'' in Proc. IEEE/IFIP Int'l Conf. DSN, 2010, pp. 211-220
7. H. Debar and J. Viinikka, "Intrusion detection: Introduction to intrusion detection and security information management," in foundation security analysis and design III , Sep. 2005, pp. 207–236.
8. A. Lazarevic, V. Kumar, and J. Srivastava, "Intrusion detection: A survey," Managing cyber threats, pp. 19–78, June 2005
9. D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring Internet denial-of-service activity," ACM Transcation on computer system, vol. 24, no. 2, pp. 115–139, May 2006.
10. Z. Li, Y. Gao, and Y. Chen, "Towards a highspeed router-based anomaly/intrusion detection system," http://conferences.sigcomm.org/sigcomm/2005/poster-121.pdf, Aug. 2005.
11. Y. Ago, Z. Li, and Y. Chen, "A dos resilient flow-level intrusion detection approach for high-speed networks," in proc of the 26th IEEE international conference on distributed computing system, 2006, p. 39.

12. Q. Zhao, J. CSU, and A. Kumar, "Detection of super sources and destinations in high-speed networks: Algorithms, analysis and evaluation," IEEE journal on selected areas in communications, vol. 24, no. 10, pp. 1840–1852, Oct. 2006.
13. Kun-canal, AlefiyaHussain, and DebojyotiDutta, "Effect of Malicious Traffic on the Network," Proc. of PAM 2003, San Diego, California, April 2003.
14. S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," computer and security, vol. 24, no. 1, pp. 31–43, Feb. 2005
15. Botnet detection .Countering the largest security threat. Spinger, 2008, vol. 36.
16. S. Noel and S. Jajodia, ''Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs,'' J. Netw. Syst. Manage., vol. 16, no. 3, pp. 259-275, Sept. 2008.
17. L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, ''An Attack Graph based Probabilistic Security Metric,'' in Proc. Data Appl. Secur. XXII, 2008, pp. 283-296.
18. L. Wang, S. Noel, and S. Jajodia, ''Minimum-Cost Network Hardening Using Attack Graphs,'' Comput. Commun., vol. 29, no. 18, pp. 3812-3824, Nov. 2006.
19. S. Jajodia and S. Noel, ''Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection, and Response,'' in Indian Statistical Institute Monograph Series. Singapore: World Scientific, 2008.
20. S. Zhang, D. Caragea, and X. Ou, ''An Empirical Study on Using the National Vulnerability Database to Predict Software Vulnerabilities,'' in Proc. Database Expert Syst. Appl., 2011, pp. 217-231.
21. X. Ou and A.W. Appel, A Logic-Programming Approach To Network Security Analysis. Princeton, NJ, USA: Princeton Univ. Press, 2005.
22. P.A. Porras, M.W. Fong, and A. Valdes, ''A Mission-Impact- Based Approach to INFOSEC Alarm Correlation,'' in Proc. Symp. RAID, 2002, pp. 95-114
23. A. Goel, K. Po, K. Farhadi, Z. Li, and E. de Lara. The taser intrusion recovery system. In Proceedings ofthe 20th ACM Symposium on Operating Systems Principles (SOSP'05), October 2005.

