Network Based Intrusion Detection System using Protocol Standardization Techniques

D. Parameswari, V. Khanaa

Abstract: ***The IDS system identifies the anomaly device which connected in the network communication process through evaluating the MAC address compared with the registered list of devices. In completion, this research work ensures that all the devices which are involved in the network communications are authenticated and secured, which increases the security of the network and prevents the intruder. This research work attempts to increase the quality of service of network communication, ensuring error-free communication through monitoring the network.***

Keywords: IDS, ICMP, MAC

I. INTRODUCTION

Network based IDSs are typically aloof gadgets that tune in on a system wire without meddling with the ordinary activity of a system [14]. Along these lines, it is normally simple to retrofit a system to incorporate system based IDSs with insignificant exertion. System based IDSs can be made secure against assault and even imperceptible to numerous aggressors. System based IDSs may experience issues handling every one of the bundles in an enormous or occupied system and, in this manner, may neglect to perceive an assault propelled during times of high traffic.
System based IDSs can't break down scrambled data. This implies after a system based ID identifies an assault, chairmen should physically examine each assaulted host, to decide if it was without a doubt entered. Some system based IDSs have issues managing system based assaults that include dividing parcels. These distorted bundles cause the IDSs to end up precarious and crash. There are two essential ways to deal with investigating occasions to distinguish assaults: abuse location and inconsistency discovery. Abuse discovery, in which the investigation targets something known to be "awful", is the strategy utilized by most business frameworks. Peculiarity discovery, in which the examination searches for anomalous examples of movement, has been, and keeps on being, the subject of a lot of research. Peculiarity location is utilized in a constrained structure by various IDSs. There are qualities and shortcomings related with each methodology, and it gives the idea that the best IDSs use for the most part abuse identification strategies, with a sprinkling of inconsistency location segments. Interruption recognition frameworks play out the accompanying capacities well: Monitoring and investigation of framework occasions and client conduct, and testing the security conditions of framework setups.

Revised Manuscript Received on December 08, 2019
* Correspondence Author
D.Parameswari , Research Scholar Department of Computer Science and Engineering Bharath Institute of Higher Education and Research, Chennai-600073,India,
Dr.V.Khanaa, Dean-Info, Department of IT Bharath Institute of Higher Education and Research Chennai-600073,India,

Perceiving examples of framework occasions that relate to known assaults, and perceiving examples of action that measurably fluctuate from ordinary action. IDS overseeing working frameworks review and log the instruments and the information they produce. The system protections are given through firewalls, ID and verification, connect encryption, get to control instrument and infection identification. The IDS procedure is an extra one to expand the security of dynamic procedures. In the IDS discovery process programmed examination is a test in the system security process.The IDS system has hundreds of tools in open and commercial tools based networks as well as open source based ones. But it ends up with many false positives and most of the system administrators' tend to ignore the warnings. The identification of the IDS policy is very difficult.

II. LITERATURE SURVEY

Ghosh et al. [1] have tested, utilizing haphazardly created occasions to speak to peculiar conduct, so as to prepare the neural systems that give the examination to their IDS. In experimental tests, those systems that were prepared with arbitrarily created strange information reliably out-played out those that did not get this preparation; by diminishing the quantity of false negatives in the framework (none of the systems delivered any bogus positives). While these methodologies are extremely encouraging, they propose that the neural systems prepared with irregular information performed well. The ordinary informational collection with which they were prepared characterized a tight scope of conduct that in all respects intently looked like the typical information that the framework was tried against. In such a case, the framework could sensibly have been required to create at any rate few false positives as a portion of the haphazardly produced occasions prepared as peculiarities would fall into the scope of typical movement. It is further vague how well a framework prepared over arbitrary strange information would perform in accurately recognizing real assaults, as the assault information against which this framework was tried likewise comprised of haphazardly created occasions [2]. EleazarEskin [3, 4] has built up a procedure that utilizations learned likelihood disseminations to prepare an oddity framework over loud information. This procedure uses AI to make a likelihood dispersion of the preparation information and after that applies a factual test to recognize irregularities [5]. Strikingly, Eskin's system [4] requires no area explicit information. It does, be that as it may, work on three suspicions about the preparation information: typical information can be successfully demonstrated utilizing a likelihood appropriation; strange occasions vary essentially enough from ordinary

occasions that they can be distinguished; and the quantity of atypical occasions is contrasted with the quantity of ordinary occasions. Versatile irregularity frameworks have been recommended as an answer, which would consider frameworks to advance their typical conduct models bit by bit, as ordinary conduct develops [6]. Path and Bradley's [7] AI framework is a case of a framework that utilizes this strategy. This framework keeps up a limited estimated word reference of typical occasion successions, and utilizations a Least-Recently Used (LRU) strategy, to supplant only occasionally happening groupings with new ones that are resolved to be ordinary. Note that frameworks which utilize versatile preparing procedures face the issue of keeping an aggressor from continuously preparing the framework after some time, to acknowledge a scope of irregular conduct as typical. Settling this trouble remains an open test. Brother [8] is propelled from a content that can perceive if the framework ever crashes, in which case it dispatches TCP dump so as to accumulate the information. This information would then be able to be broke down Vern Paxson [9] recommends that such frameworks perform "triage" against approaching streams: if the framework identifies that it is nearing depletion, it can shed the heap by disposing of the state for observed streams that don't give off an impression of being gaining ground. This proposal works under the presumption that an assailant is less inclined to have complicity from hosts on the two sides of the screen, hence making it hard for the aggressor to counterfeit countless dynamic associations.

III. ICMP SEGMENT STRUCTURE

ICMP messages are developed at the IP layer, more often than not from a typical IP datagram that has created an ICMP reaction. IP embodies the fitting ICMP message with another IP header (to recover the ICMP message to the first sending host) and transmits the subsequent datagram in the typical way. Despite the fact that ICMP messages are contained inside standard IP datagrams, ICMP messages are generally prepared as an extraordinary case, recognized from ordinary IP handling, instead of handled as a typical sub-convention of IP. As a rule, it is important to examine the substance of the ICMP message and convey the fitting blunder message to the application that produced the first IP parcel, the one that incited the sending of the ICMP message. The ICMP section structure gives the point by point substance of the parcels.

Header

The ICMP header begins after the IPv4 header as introduced in Table 1, given beneath

Table 1 ICMP header

Bits	**0-7**	**15-Aug**	**16-23**	**24-31**
0	Type	Code	Checksum	
32	ID		Sequence	

In this structure - Type gives the kind of ICMP as indicated. The Code indicates further determination of the ICMP type; e.g.: an ICMP Destination Unreachable may have this field set to 1 through 15 each bearing various implications. The Checksum field contains mistake checking information determined from the ICMP header information, with an estimation of 0 for this field. The ICMP ID field contains an ID esteem, which ought to be returned if there should be an occurrence of ECHO REPLY. Arrangement field contains a succession esteem that ought to be returned in the event of ECHO REPLY. The structure gives the data of the sort and check entirety, to decide the parcel properties. The caught bundle is exhibited in Table 2, given beneath.

No. Time Source Destination Protocol Info

28104 263.016677 172.15.2.226 172.15.7.171 ICMP Destination unreachable (Host unreachable)

Frame 28104 (70 bytes on wire, 70 bytes captured)

Arrival Time: Apr 11, 2010 16:13:10.297220000

0.000765000 seconds]

0.000765000 seconds]

263.016677000 seconds]

Frame Number: 28104

Frame Length: 70 bytes

Ethernet II, Src: Cisco_a3:32:b9 (00:09:7c:a3:32:b9), Dst: 00:1e:c9:58:f3:a0 (00:1e:c9:58:f3:a0)

Destination: 00:1e:c9:58:f3:a0 (00:1e:c9:58:f3:a0)

Address: 00:1e:c9:58:f3:a0 (00:1e:c9:58:f3:a0) ....0 .... = IG bit:

Individual address (unicast)

Source: Cisco_a3:32:b9 (00:09:7c:a3:32:b9)

Address:Cisco_a3:32:b9 (00:09:7c:a3:32:b9)

....0 .... = IG bit: Individual address (unicast)

.... ..0. .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 172.15.2.226 (172.15.2.226), Dst: 172.15.7.171 (172.15.7.171)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

....0 = ECN-CE: 0

Total Length: 56

Identification: 0x4dc9 (19913)

IV. ANALYSIS OF THE PROTOCOL

In this work, the ARP, SNMP-ALG and ICMP packets and their structure components are described. All the three packets are used in the network communication system,dependent on the IP address of the correspondence and the MAC address along with the trailer or data value. The data values are adjustable according to the data which is sent along with the packets. The protocol objectives and its applications are unique in nature, but the components are similar to one another. All the three protocols packet structure contains the frame details and the IP address just as MAC address. In the location preparing of the parcels, the IP address mismatches as well as the return address are taken into account to evaluate the network. If the communication process does not provide proper values then the packet could be considered as a suspected packet. In all the three-structure analyses, the protocol type and the hardware types are considered for the communication confirmation process. The hardware resources, which act as a sender or receiver, are registered over the network in the current active directory to ensure security in and across the network. Therefore, packet components are identified from the three protocol structures and uniform contents are presented in 64 byte representation for the intrusion detection system. The network process covered with the basic network, transmission control and network management. The basic network is focused to identify the network peripherals and its addresses. The ARP protocol is responsible for the connectivity process and the addressing scheme. The ICMP handles the discarded and unreachable packets along with its routers. The communication process is taken care by the ICMP. The SNMP-ALG ensures the network management activities, to share the resource as well as optimize it. If these three network protocols are effectively executed, then the network could be secured. Therefore, this research work has adopted and implemented the ARP, SNMP-ALG and ICMP protocols for these IDS.

V. EXPERIMENTAL RESULT

From the ARP, SNMP-ALG and ICMP packet structure, the common 64-byte common information packet is proposed, to generate the identification of anomaly detection. The proposed packet structure is constructed from the standard structure of the collected packet information, using the wire shark network observer tool.

The sequence structure information is described in Table 3, given below.

Table 3 Description of the 64 byte information

Bytes	Description	Values
1-8	Frame information	ff|ff|ff|ff|ff|ff|00|18
9-16	Source Information	f3|0f|7f|63|08|06|00|01
17-24	Destination information	f3|0f|7f|63|ac|10|06|39
25-40	Source and destination MAC address	08|00|06|04|00|01|00|18|00|00|00|00|00|00|ac|10
41-64	Hardware and data	3f|cf|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|

In this, the first eight byte represents the frame information, 9-16 byte represents the source information, 17-24 byte represents the destination information, 25-40 byte represents the MAC address of the source and destination. 41-64 bytes represent the information about the hardware and data. Though the protocol information order differs in the fetching process, the standardization parts adopted the corresponding bit value, and reposition the structure for the intrusion detection process. As per the proposed structure, the designed protocol structure is common for all the three ARP, SNMP-ALG and ICMP protocols. The structured and standardized protocol has components, which are common for all the three selected protocols. The value differs but the format is the same. The location and size of the MAC and IP address are similar; therefore, the mapping and identification process of the communication device is made easy. The above constructed 64 byte protocol structured information is imported as an initial population for the anomaly detection process.

VI. CONCLUSION

The common 64byte protocol structure standardization process is identified and fetches the required attributes from same location, so it is required to minimize the search time of the identification of the MAC and IP address from the packets.

The ARP protocol, which is used to provide IP address, the SNMP-ALG intended for the maintenance and the ICMP which controls the internet communications, observe the basic components, and the available frame details used for the construction of the common protocol structure. This common protocol structure is used as an input for the Genetic algorithm; crossover and mutation functions are used to predict the intruder from device list.

REFERENCES

1. Ghosh, A., and Schwartzbard, A. "A study in using neural networks for anomaly and misuse Detection". 8th USENIX Security Symposium, pp. 141-151, 1999.
2. Lee, W., &Stolfo, S.J. (2000). "A framework for constructing features and models for intrusion detection systems". *ACM Transactions on Information and System Security, 3* (4) (pp. 227-261).
3. Eskin E, Lee W, Stolfo SJ. "Modeling System Calls for Intrusion detection with dynamic Window Sizes". Proceedings of DISCEX II, 2001.
4. Eskin E, Miller M, Zhong ZD, Yi G, Lee W, Stolfo S. "Adaptive Model Generation for Intrusion Detection Systems". Workshop on Intrusion Detection and Prevention, 7th ACM Conference on Computer Security, 2001.
5. Ning, P., Jajodia, S., & Wang, X.S. (2001). "Abstraction-based intrusion detection in distributed environments". *ACM Transactions on Information and System Security, 4* (4), 407--452.
6. Lee W., Stolfo S., and Mok K., "Adaptive Intrusion Detection: A Data Mining Approach," Artificial Intelligence Review, 14(6), December 2000, pp. 533-567.
7. Lane ,T.Broadley ,C.E, "Approaches to Online learning and concept drift for user identification in computer security". In 4th International conference on Knowledge Discovery and Data Mining (1998) .
8. Paxson V., Bro, "A System for Detecting Network Intruders in Real-Time," Computer Networks, vol. 31, no. 23-24, 1999, pp. 2435-2463.
9. Paxson, Vern. 1998. Bro "A System for Detecting Network Intruders in Real-time." *In Proceedings of 7th USENIX Security Symposium*, pp. 31-51. San Antonio, Texas.
10. Porras P.A. and R. Kemmerer, "Penetration State Transition Analysis C a Rule-Based Intrusion Detection Approach". The 8th Annual Computer Security Application Conference,pp. 220-229, 1992.
11. PostelJ . E., ed., "Internet Control Message Protocol," RFC 792, Sept. 1981.
12. Puketza N., K. Zhang, M. Chung, B. Mukherjee, R. Olsson, "A Methodology for Testing Intrusion Detection Systems," IEEE Transactions Software Engineering, vol. 22, no. 10, 1996, pp. 719-729.
13. Quinlan J. R. "Discovering rules by induction In Expert Systems in the Micro-Electronic Age", Edinburgh University Press, 1993.
14. Quinlan, J.R. (1985b). "Decision trees and multi-valued attributes". In J.E. Hayes & D. Michie (Eds.),Machineintelligence 11. Oxford University Press .
15. Quinlan, J.R. (1986). "Induction of decision trees. Machine learning" 1, 81-106.
16. Sadiq Ali Khan, "Rule-Based Network Intrusion Detection Using Genetic Algorithm", International Journal of Computer Applications, No: 8, Article: 6, 2011, DOI: 10.5120/2303-2914.
17. SandyaPeddabachigari, Ajith Abraham, CrinaGrosan, Johanson Thomas. "Modeling Intrusion Detection Systems Using Hybrid Intelligent Systems", Journal of Network and Computer Applications-2005.
18. Saniee M., Habibi J., Lucas C. "Intrusion detection using a fuzzy genetics-based learning algorithm". Journal of Network and Computer Applications, 30(1), pp. 414 – 428. January 2007.
19. Sathyabama.S, IrfanAhmed.M.S, Saravanan.A,"Network Intrusion Detection Using Clustering: A Data Mining Approach", International Journal of Computer Application (0975-8887), Sep-2010, Vol: 30, No: 4, ISBN: 978-93-80864-87-5.
20. Sekar R., Y. Guang, S. Verma, T. Shanbhag, "A High-Performance Network Intrusion Detection System," Proc. 6th ACM Symp. Computer and Communication Security, ACM Press, New York, N.Y., 1999.

AUTHORS PROFILE

D.Parameswari received his Master of Technology in Computer Science and Engineering from Bharath Institute of Higher Education and Research, Chennai. Currently she is working as Professor in Department of Information Technology, Jerusalem College of Engineering since 2002 and doing Research in the field of Network Security in BIHER. Her areas of interests Networking, Data Mining, Cloud Computing.

Dr.V.Khanaa is self- directed, enthusiastic educator with a commitment on student development. He is with Bharath University, Chennai, Tamil Nadu, India as Professor and Dean of IT . He has over 35 years of rich experience in teaching along with student administration. He has guided more than 500 UG, PG projects and organized various national level conferences. He served as Senior Chair, Technical advisor in various national level conferences and Technical Committee member in International Conferences. He is an active member in CSI, IEEE, ISTE, ACM etc., His area of interests includes Computer Networks, Cloud Computing, Networks and Software Engineering.