IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IX (Feb. 2014), PP 108-112
www.iosrjournals.org

Intrusion Detection system: A Review of the state of the art

[1]Ajay kaurav,[2]S.Sibi Chakkaravarthy,[3]Pravin R.Patil, [4]M.Vimal Karthik
[1, 2] *M.Tech Scholar,* [3]*Asst Professor,* [3#]*Asst.Professor*
[1, 2]*Centre for development of advanced computing*
[1, 2, 3#]*Vel Tech University, Chennai*
[3] *Pune Institute of Computer Technologies, Pune*

Abstract: *Intrusion detection system is a software which is used to monitor network for anyintrusion .There are various types of IDS which are stated as Anomaly based, Host based, Network based and Signature based. In this paper, a review is made on various intrusion detection systems. The review analysis the whole active intrusion detection system. Through the extensive survey we analysed the whole pose of the active intrusion detection system. We employed the survey towards overall IDS not only for the specific. Since the security threats are in increased level, hence the study and survey about IDS has paid a lot of attentions.*

Keywords:*IDS, IPS, Intrusion, WSN*

I. Introduction

With the increased amount of network technology and throughput characteristic of network the security parameters such as IDS,IPS,firewall,UTM has acquired a lot of attention in study and review the state of the art. Here we are going to discuss about the various IDS proposed by various researchers and research forums. The typical architecture of WSN (Wireless sensor network) IDS and wired IDS has been demonstrated in Figure 1.

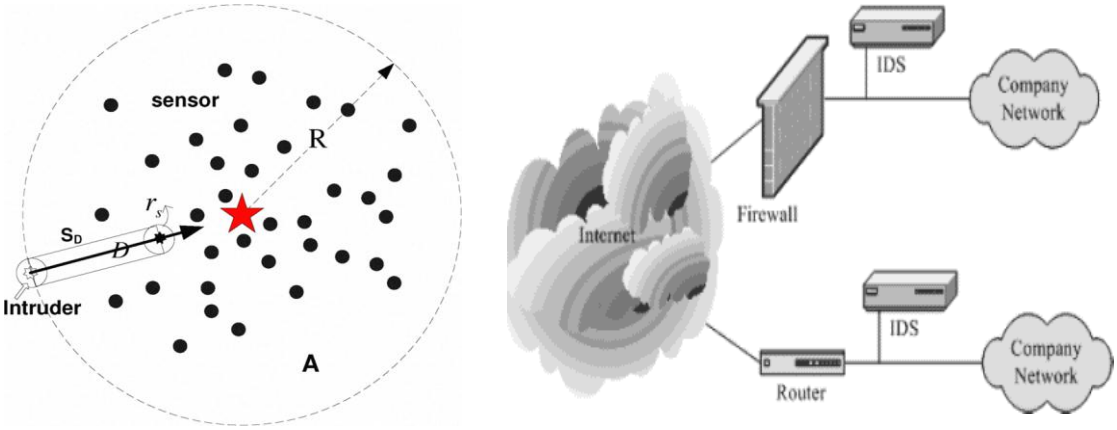

Figure 1: Wireless & Wired env IDS

II. Evolution of IDS

First IDS ever developed was host based, since they are used to analyse the system log i.e., for analysing the operating system log by evaluating the signatures with the small set of patter or model. This leads to the development of various IDS, yet the security flaws were in increased numbers; the system performance were degrading due to these security flaws. This scenario leads to full-fledged development of IDS at the earliest. Later IDS gained all the protocol awareness, used to analyse the packet, packet structures etc., which predicts the known packet traffic defined to be malicious. Now a days recent IDS can predict the various attacks or types of intrusion through the network because the recent development in IDS leads to host communication, in built security features , protocol awareness, packet examining etc.

Types of IDS-Survey [1]:

NIDS–Network based Intrusion Detection System [1][2]

Network Intrusion Detection Systems are placed at a intentional point or points within the network to monitor traffic with inbound and outbound of all devices on the network. Network-based IDS's are mostly passive devices that monitor on-going network activity without adding significant overhead or interfering with network operation. They are easy to secure against attack and may even be undetectable to attackers; they also require little effort to install and use on existing networks. Ideally you would scan all inbound and outbound traffic; however doing so might create a bottleneck that would impair the overall speed of the network.

HIDS– Host based Intrusion Detection System [1]
Host Intrusion Detection Systems will run on individual hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the user or administrator of suspicious activity is detected

SignatureBasedIntrusion Detection System [1]
A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat [1].

Anomaly BasedIntrusion Detection System [1]
An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

Survey Table – IDS

S No	Year	Author	Methodology
1	1980	J. P. Anderson,	Computer Security Threat Monitoring and Surveillance.
2	1990	R. Heady, G. Luger, A. Maccabe and M. Servilla	The Architecture of a Network Level Intrusion Detection System
3	1993	James Cannady and Jay Harrell,	A ComparativeAnalysis of Current Intrusion Detection Technologies
4	1994	B. Mukherjee, L. T. Heberlein and K. N. Levitt	Network Intrusion Detection
5	1995	K. Ilgun, R. A. Kemmerer and P. A. Porras	State Transition Analysis: A Rule-Based Intrusion Detection Approach,
6	1996	D. Wagner and B. Schneier,	"Analysis of the SSL 3.0 protocol," in Proc. 2nd USENIXWorkshop Electron. Commerce,
7	1997	C. E. Landwehr and D. M. Goldschlag,	Security issues in networks with internet access,
8	1998	D. Bleichenbacher,	Chosen Ciphertext attacks against protocols based on the RSA encryption standard PKCS
9	1999	H. Debar, M. Dacierand A. Wespi	Towards a Taxonomy of Intrusion-Detection Systems
10			
11	2001	Ning, P., Jajodia, S., & Wang, X.S.	Abstraction-based intrusion detection in distributed environments.
12	2001	J.-P. HuBaux, L. Buttyan, and S. Capkun.,	The quest for security immobile ad hoc network
13	2002	Robert F ErbacherKennierth L Waller Deborah A frienche	Intrusion and misuse detection in large-scale system
14	2002	A. Bivens, C. Palagiri, R. Smith, B. Szymanski, and M. Embrechts,	"Network-based intrusion detection using neural networks,"
15	2003	Sung-Bae Cho,	Incorporating Soft Computing Techniques Into aProbabilistic Intrusion Detection System
16	2004	KiranDhangar Prof. Deepak KulhareArif Khan	Intrusion Detection System (A Layered Based Approach for Finding Attacks)
17	2005	T. Law, J. Lui, and D. Yau	You can run, but you can't hide: An effectivestatistical methodology to trace back DDoS attackers
18	2005	Salvatore Pontarelli, Giuseppe Bianchi, Simone Teofili	Traffic-aware Design of a High Speed FPGANetwork Intrusion Detection System
19	2005	S. P. Joglekar and S. R. Tate,	ProtoMon: Embedded monitors for cryptographicprotocol intrusion detection and prevention,"
20	2006	SarangDharmapurikar John W. Lockwood	Fast and Scalable Pattern Matching forNetwork Intrusion Detection Systems
21	2007	LAHEEB MOHAMMAD IBRAHIM	Anomaly network Intrusion Detection System Based on Distributed Time Delay Neural Network
22	2007	T. Taleb, Z. M. Fadlullah, K. Hashimoto, Y. Nemoto, and N. Kato,	Tracing back attacks against encrypted protocols,"
23	2008	AbhishekDas,DavidNguyen,JosephZambreno,GokhanMemik,AlokChoudhary,	An FPGA-Based Network Intrusion Detection Architecture
25	2010	Zubair M. Fadlullah,TarikTaleb Athanasios V. Vasilakos, Mohsen Guizani, Nei Kato,	DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis
26	2010	Shrestha, R.	A Novel Cross Layer Intrusion Detection System in MANET
27	2011	Hyun Jin Kim, Hong-Sik Kim, and Sungho Kang	A Memory-Efficient Bit-Split Parallel StringMatching Using Pattern Dividing for IntrusionDetection Systems
28	2011	RavneetKaur	Advances in Intrusion Detection System for WLAN
29	2011	Noman Mohammed, HadiOtrok, Lingyu Wang,	Mechanism Design-BasedSecure Leader Election Model for Intrusion Detection in MANET
30	2012	Karen A. Garc´ıa, Ra´ulMonroy, Luis A. Trejo, Carlos Mex-Perera, and Eduardo Aguirre	Analyzing Log Files for PostmortemIntrusion Detection
31	2012	Gholam Reza Zargar, Tania Baghaie	Category-Based Intrusion Detection Using PCA
32	2013	Elhadi M. Shakshuki, Nan Kang,Tarek R. Sheltami,	EAACK—A Secure Intrusion-DetectionSystem for MANETs
33	2013	Xiaofei Wang, Yang Xu, Junchen Jiang, Olga Ormond, Bin Liu, and Xiaojun Wang	StriFA: Stride Finite Automata for High-SpeedRegular Expression Matching in NetworkIntrusion Detection Systems
34	2013	KamalanabanEthala, R. Shesadri and N.G. Renganathan	The Use Of Random Forest Classification And Kmeans Clustering Algorithm For Detecting Time Stamped Signatures In The Active Networks
35	2013	KamalanabanEthala, R. Seshadri, N.G. Renganathan and M.S. Saravanan	A Role Of Intrusion Detection System For Wireless Lan Using Various Schemes And Related Issues
36	2013	KamalanabanEthala, R. Seshadri	Combatting Cyber terrorism - Assessment of log for malicious signatures
37	2013	KamalanabanEthala, R. Seshadri	

Parameters for evaluating performances of IDS

Detection Rate: The number of intrusion cases detected by the system(True Positive) divided by the total number of intrusion cases present in the test set
False Alarm Rate: The number of 'normal' outlines classified as attacks(False Positive) divided by the total number of 'normal' outlines
True Positive: A real attack which activates an IDS to create an alarm
False Positive: An event signing an IDS to create an alarm when no attack has taken place.
False Negative: A failure of an IDS to detect an actual attack.
True Negative: When no attack has taken place and no alarm is raised.
Noise: Data or intrusion that can activate a false positive.

Case for evaluating performance of various IDS

	Primary Focus	Data Sources	reporting tools
DShield.org	Information is shared about the attack	Individual/corporate firewall	ISP responses to all hosts
myNetWatchman	Notify the owner of the compromised system	Individual/corporate firewall	Auto tracking the information/ security ISP
DeScan.net	Scans network for the malicious packets	Individual/ corporate Linux based	Automatically agent receives a copy
Symantec	Threat information to the customer	Corporate/individual for connected pc's	Manual reporting and automatically log will be generated and updated
Cyberroam	Scans the network/privileged user accounts	Corporate	Log will be updated
Sonic wall	Similar to cyberroam	Corporate/ individual connected PC's	Log and Agent will be informed with alerts

III. Conclusion

Finally we conclude the discussion in this survey paper, we demonstrated the whole architecture of the IDS in wired and wireless environment. The types of IDS are defined carefully and tabular illustration of the active IDS from the earliest to up to date were updated in this paper, section " Survey Table" defines clearly about the IDS evolution from the early days to present day.Various researchers has proposed various Intrusion detection system and supports for various attacks, some of the IDS has most advantages over some attacks some may have some challenges. Our hope is that this review will help the researchers to know about the various IDS with its strength and challenges.

References

[1] S. Jacobs, S. Glass, T. Hiller, and C. Perkins, "Mobile IP authentication, authorization, and accounting requirements," Request for Comments 2977, Internet Engineering Task Force, October 2000.
[2] K. Sanzgiri, B. Dahill, B. N. Levine, E. B. Royer, and C. Shields, "A Secure Routing Protocol for Ad-hoc Networks," in the Proceedings of International Conference on Network Protocols (ICNP), 2002.
[3] Yih-Chun Hu, Adrian Perrig, and David Johnson. Ariadne: "A Secure On-Demand Routing Protocol for ad hoc Networks," in the Proceedings of MobiCom, 2002.
[4] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM J. Wireless Networks, pp. 545-556, 2003.
[5] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad-Hoc Networks," in IEEE Wireless Communications, pp. 48-60, February 2004.
[6] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in the Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS) Providence, pp. 478-487, 2003.
[7] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion Detection for Routing attacks in Sensor Networks," in International Journal of Distributed Sensor Networks, pp. 313-332, october-December 2006.
E. Eskin, A. Arnold, M. Prerau, L. Portnoy, S. Stolfo, "A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data," in Applications of Data Mining in Computer Security. Kluwe, 2002.
[8] A. Goldsmith and S. B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks," in IEEE Wireless Communications, pp. 9(4): 8-27, August 2002. (Pubitemid 35426991)
[9] C. J. John Felix, A. Das, B. C. Seet, and B. S. Lee, "Cross Layer versus Single Layer Approaches for Intrusion Detection in MANET," in IEEE International Conference on Networks, Adelaide, pp. 194-199, November, 2007.
[10] J. S. Baras and S. Radosavac, "Attacks and Defenses Utilizing Cross-Layer Interactions in MANET," in workshop on Cross-Layer Issues in the Design of Tactical Mobile ad hoc Wireless Networks: Integration of Communication and Networking Functions to Support Optimal Information Management, Washington, DC, June 2004.
[11] L. Yu, L. Yang, and M. Hong, "Short Paper: A Distributed Cross-Layer Intrusion Detection System for ad hoc Networks," in Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece, pp. 418-420, September 2005.
[12] C. J. John Felix, A. Das, B. C. Seet, and B.-S. Lee, "CRADS: Integrated Cross Layer Approach for Detecting Routing Attacks in MANETs," in IEEE Wireless Communications and Networking Conference (WCNC), Las Vegas, CA, USA, pp. 1525-1530, March 2008.
[13] R. Shrikant, "Fast algorithm for mining association rule and sequential pattern," PhD Thesis, University of Wisconsin, Madison, 1996.

[14] S. J. Hua and M. C. Xiang, "Anomaly Detection Based on Data-Mining for Routing Attacks in Wireless Sensor Networks," in Second International Conference on Communications and Networking in China, CHINACOM '07, pp. 296-300, August 2007.
[15] R. Shrestha, K. H. Han, J. Y. Sung, K. J Park, D. Y. Choi, S. J. Han, "An Intrusion Detection System in Mobile Ad-Hoc Networks with Enhanced Cross Layer Features," KICS conference, Suncheon University, pp. 264-268, May 2009.
[16] A. Patcha and J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Elsevier Computer Networks, Vol. 51, Issue 12, pp. 3448-3470, 2007.
[17] L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion detection with unlabeled data using clustering," in proceedings of the Workshop on Data Mining for Security Applications, November 2001.
[18] C. Loo, M. Ng, C. Leckie, and M. Palaniswami, "Intrusion Detection for Routing attacks in Sensor Networks," in International Journal of Distributed Sensor Networks, pp. 313-332, October-December 2006. OPNETmodeler, http://www.opnet.com.
[19] T. Phit and K. Abe, "Protocol Specification-based Intrusion Detection System for VoIP," Technical Report of IEICE, vol. 107, pp. 5-10, February 2008.