THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

A Comparative Study of Intrusion Detection Tools for Wireless LAN

Dr. Harmeet Singh, Assistant Professor, Department of Computer Science & Engineering, SBBS University, Jalandhar

Dr.Vijay Dhir,Professor, Department of Computer Science & Engineering, SBBS University, Jalandhar

Abstract:

Today it is vitally primary to furnish a high-level security to protect highly sensitive and confidential knowledge. IDS is an essential technology in network security. Intrusion-detection systems has ability to detect attacks in computer system and against networks. This paper presented the history of Intrusion Detection Systems tools for detecting intrusions in Wireless LAN. Thirty-two research and commercial tools are evaluated based on some common parameters. An intrusion detection systems taxonomy is designed to compare the performance and features of IDS tools. This work identifies a number of important design and implementation issues, which provide a framework for evaluating or deploying commercial intrusion detection systems.

Keyword: IDS, Wireless, LAN

1. Introduction

IDS scrutinize to collect the information of network and any other mishandlings [1][2][3]. The conventional Intrusion detection system (IDS) had been construct for wired network and system to identify mishandling and intrusion. In past due, wireless LAN was focused for employing the Intrusion detection system constructed [10]. Monitoring and analyzing system and user activities, identifying extraordinary network activity, recognizing patterns of attacks and detect coverage violations for wireless LANs are the features of those wireless Intrusion detection system. Wireless intrusion detection systems gather all local wireless communication and rely both on predefined anomalies and Signatures in the traffic to generate alerts [4] [5]. Wireless IDS detects and identify attackers to minimize the misuse communication network and information systems. There are number of problems in wireless related to protection and to cop up this situation. A number of security methods are available to prevent unauthorized used, duplication and wireless attacks [6].A number of information security methods are available these days for information systems protection in opposition to, alteration, duplicate data and various and virus intrusions[7].

1.1 Intrusion & Intrusion Detection Systems

Intrusion is an unwanted active series of similar events which denied the services and try to cause harm such as system failing to respond, and accessing unauthorized data or manipulate data. In other words, intrusions are described same as an attacks.

"Intrusion detection refers to all processes used in discovering unauthorized use of network or information system". It is the technique to monitor and analyzing all the activities happened related to the intrusion and tries to accommodate the availability, confidentiality, Integrity in an information system or communication network. The IDS checks communication information and raises security alarm or message to administrator [8].

1.2 Classification of Intrusion Detection System

Basically, it is classified in to two categories; Host Based IDS and Network Based IDS. [9]

1.2.1 Host-based IDS

A host based IDS tracks and monitors the directories and essential files change reside on systems. It takes current system files snap shot for matching with the earlier snap shot. In case that the critical system either deleted or modified, the alert message or notification is send for investigate to system administrator. To monitor the malicious activities Host-based IDS load a small piece of application software on the system.

1.2.2 Network-based IDS

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

The intrusion comes from various directions the network-based IDS analyze and watches/monitors the traffic on communication network to detect the same. An Intrusion detection system can be built from number of sensors, each and every sensor monitoring the traffic in and out by its owned network segments [10].

2. Intrusion Detection techniques

2.1 Signature-based intrusion detection approach

Also termed as misuse detection intrusion detection system. In this mechanism attack patterns are stored inside the database. Each packet of the network traffic is as compared with the attack patterns for abnormal behavior detection. Signature based intrusion detection approach works similar to the antivirus software. Same as the antivirus to detect the attack it matches the signatures/patterns that are already stored in database. It detects known attacks only. It has very high detection accuracy of attacks [11].

2.2 Anomaly-based Detection

Anomaly-based detection systems are also called as behaviors based intrusion detection system. It is based on network behavior. The network behavior is defined by the administrator or is learned by dataset for the duration of the training segment of the improvement of IDS. Rules are described for abnormal behavior and normal behavior. They rely upon the data that intrusions may be detected with the aid of observant deviations of the behaviors of system watched/monitored. Anomaly detection model creates a baseline profile of normal traffic activities this process is termed as training part of the system [12] [13].

3. Methodology

The comparison of the different intrusion detection products for the different parameters, we study about the product from documents available in markets and published conference material. As this paper is an analysis of design specifications rather than a test of execution.

4. Intrusion Detection Tools Parameters

In this survey we have not implement or perform and test in laboratory. Following are some parameters [14].

i. Detection Time: To identified the intrusion detection mainly two parameters for the intrusion detection system i.e Real-time or Non Real-Time. Real-time detection the intrusion and process data without any delay and on the other hand data process with some delay in time of detection is Non Real-time. The most of intrusion detection system are working on the Real-time and few number of intrusion detection system are working on Non Real-time. The system that is under the real time type can again run off-line on historical data.

ii. Granularity of data-processing: The granularity of data processing refers to that data processed in continuously manner or in batches at an interval. The granularity of system is linked with the detection time, but it should not overlap to each other, because an intrusion detection system keeps processing the data batches without an abundant delay or some cases process data continuously with some considerable delay.

iii. Response on Attack: it refers the response of system to detect the attack from network or on information system. The intrusion detection system can either *Passive* or *active* on the basis of intrusion response. A passive system gives some kinds of response like alarm or alert when attacks are detected. The active response of intrusion detection system refers to the proactive (terminate the service when seek to harm). The active intrusion detection system reacts to the attack actively. They actively change the state of victim's system or some time mitigates the effect of attack. Terminating the network connection and logging security are the active response.

iv. Degree of inter-operability: Degree to measure the ability of intrusion detection system to cooperate with another similar intrusion detection system. The inter-operability is not to that the system can perform in conjunction with another IDSs, accept audit data from divergent sources, etc. This is not the same at various levels in platform serving number of purposes.

v. Reporting Capability: This is associated to the ability to intrusion detection system how quick give the report about the attacks on network or an information system to the administrator. The basic classification use high, medium and low scale.

vi. Data-processing Location: The processing of data is done basically with two fashions either processed in a Centralized i.e. from central location or processed in distributed in fashion means data processed from different sites or sources.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

vii. Data-collection Location: The processor collects the data for the processing either from the one location using Centralized method or from the different location in a distributed method.

5. Systems analyzed

In this survey the total 32 (Thirty-Two) commercial and research intrusion detection tools were analyzed they were developed by organization that are shown in following table [14] [15].

Table 5.1: Analyzed Tools

S. No.	Name of IDS	Year of Publication	Organization
1.	Haystack	1988	Haystack Lab
2.	Snort	1998	Snort Corporation
3.	MIDAS	1988	National Computer Security Centre (NCSC), SRI International
4.	Dragon	1988	Enterasys Corporation
5.	IDES	1988	SRI International
6.	Cisco Secure IDS	1998	Cisco system, Inc.
7.	Shadow	1994	Lawrence Berkeley Lab
8.	Comp Watch	1990	Secure-Systems Department at AT&T Bell Laboratories
9.	EMERALD	1997	SRI International
10.	Hyperview	1992	Altair Engineering
11.	Net Ranger	1995	Cisco Systems, Inc.
12.	Bro	1998	Centrax Corporation
13.	Cyber cop	1998	Network Associates, Inc.
14.	NADIR	1991	Los Alamos National Laboratory
15.	NIDES	1995	SRI International
16.	RealSecure	1996	Internet Security Systems
17.	GrIDS	1995	University of California at Davis
18.	Net Prowler	1997	Axent Corporation
19.	USTAT	1993	University of California Santa Barbara
20.	T-Sight		EnGarde Systems, Inc.
21.	JiNao	1997	MNC and NCSU
22.	SecureNet Pro	1996	MimeStar, Inc.
23.	Net Stat	1998	University of California at Santa Barbara
24.	DPEM	1994	
25.	Session Wall 3	1998	AbirNet
26.	Intruder Alert	1992	Axent Technologies, Inc.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

27.	IDIOT	1994	Purdue University
28.	Entrax	1998	Centrax Corporation
29.	ASAX	1992	University of Namur
30.	ID-Trak	1999	Internet Tools, Inc
31.	OSSEC	2008	Third Brigade and the OSSEC
32.	Suricata	2010	Open Information Security Foundation (OISF)

The analysis of the intrusion detection tools according to the above mentioned parameters. Almost all the intrusion detection tools are detecting the intrusion in Real-time and Haystack, shadow, comp watch, T-sight and few more detection tools are detecting intrusion in Non Real-Time.

The Granularity of almost all intrusion detection tools is continuous and some of tools processed data in batch. Snort and IDES tools processed the data in continuous manner. The snort is the open source IDS and IPS [16]. Snort tools have two modes packet logger and sniffer if the snort in a sniffer mode it will refer the network packet and also display packet on the console on the other hand on packet logger mode if it will log the packets to storage/disk.

The response of attack of system to detect the attack from network or on information system. The intrusion detection system cans either *Passive* or *active* on the basis of intrusion response. Passive systems give some kinds of response like alarm or alert when attacks are detected. There are number of system that supports the passive response mechanism. But the Cisco Secure IDS and snort use a passive as well as active response mechanism.

Interoperability for intrusion detection system may also be carried out in a number of different areas. Exchange of security policies; Exchange of alarm report, response and notifications; and Exchange of audit data record are the three major area of Interoperability.

The data are processed and collect are basically two mechanisms centralized and distributed. Most of the IDS tools data processed and collect in centralized manner but the NADIR and T-sight data are processed in centralized manner and collect in distributed fashion. On the other hand, Session Wall 3 data are processed in distributed manner and collect in centralized fashion.

Cyber cop is a host based intrusion detection system that operate under Solaris and Windows

It exists in host system, but moreover to analyzing log files on the host system, it is equipped to participate in packet sniffing. Hyperstack intrusion detection system detect the intrusion in multiple user in US air force information system. Hyperstack reduce the system audit trails, anomaly and other harmful events that occur on the information system. Hyperstack IDS employee two detection approaches signature based and anomaly based detection. The combination of two approaches gives better performance to detect the intrusion and handle all the problems related to the intrusion. Shadow (Secondary Heuristic Analysis for Defensive Online warfare) is the combination of tcpdump and Perl. The shadow IDS run on salaries operating system that is the excellent platform to run.

EMERALD is a tool designed to detect malicious activity enlarge wireless network. It combines features of both the system (misuse and anomaly detection system)

Suricata is a real time detection system for detecting intrusion in faster way. It can detect in complex treats using extensive rules and signature language [17].

OSSEC is an open source host based intrusion detection system. By using OSSEC the storage overhead can be reducing as only alert one stored. It has a powerful analysis engine, file integrity checking, lock analysis facility etc. to detect DDoS attack. It is customizable and easy to installed and can support multi-platform. OSSEC can keep track a distributed server. It gets the information from agent, which distribute detail to server for analysis and correlation [18].

Table: 5.2 Functional aspects

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

S.No	Name of IDS	Detection Time	Granularity	Response on Attack	Intero-perability	Reporting Capability	Data Processing	Data Collection
1.	**Haystack**	Non RealTime	Batch	Passive	Low	Low	Centralized	Centralized
2.	**Snort**	Real-Time	Continuous	Passive/ Active	Medium	High	Centralized	Centralized
3.	**MIDAS**	Real-Time	Continuous	Passive	Low	Low	Centralized	Centralized
4.	**Dragon**	Real-Time	Continuous	Passive	High	High	Distributed	Distributed
5.	**IDES**	Real-Time	Continuous	Passive	Low	Low	Centralized	Distributed
6.	**Cisco Secure IDS**	Real-Time	Continuous	Passive/ Active	Medium	High	--	--
7.	**Shadow**	Non RealTime	Batch	Active	--	Medium	Centralized	Centralized
8.	**Comp Watch**	Non RealTime	Batch	Passive	Low	Low	Centralized	Centralized
9.	**Emerald**	Real-Time	Continuous	Passive	High	Medium	Distributed	Distributed
10.	**Hyperview**	Real-Time	Continuous	Passive	Low	Low	Centralized	Centralized
11.	**Net Ranger**	Real-Time	Continuous	Active	Medium	High	Distributed	Distributed
12.	**Bro**	Real-Time	Continuous	Active	Low	High	Centralized	Centralized
13.	**Cyber cop**	Real-Time	Continuous	Active	Medium	High	Centralized	Centralized
14.	**NADIR**	Non RealTime	Continuous	Passive	Low	Low	Centralized	Distributed
15.	**NIDES**	Real-Time	Continuous	Active	Low	High	Centralized	Centralized
16.	**RealSecure**	Real-Time	Continuous	Active	Medium	High	Centralized	Centralized
17.	**GrIDS**	Non RealTime	Batch	Passive	Low	Low	Distributed	Distributed
18.	**Net Prowler**	Non RealTime	Batch	Active	--	--	Distributed	Distributed
19.	**USTAT**	Real-Time	Continuous	passive	Low	Low	Distributed	Distributed
20.	**T-Sight**	Non Real-Time	Batch	Passive	--	--	Centralized	Centralized
21.	**JiNao**	Real-Time	Batch	Passive	Low	Low	Distributed	Distributed
22.	**SecureNet Pro**	Real-Time	Continuous	Active	Low	High	Centralized	Centralized
23.	**Net Stat**	Real-Time	Continuous	Passive	--	--	Distributed	Distributed
24.	**DPEM**	Real-Time	Batch	Active	Low	Low	Distributed	Distributed
25.	**Session Wall 3**	Real-Time	Continuous	Active	Medium	High	Distributed	Centralized

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

26.	**Intruder Alert**	Real-Time	Continuous	Active	Medium	High	Distributed	Distributed
27.	**IDIOT**	Real-Time	Continuous	Passive	High	Low	Centralized	Centralized
28.	**Entrax**	Real-Time	Continuous	Active	Low	Medium	Centralized	Centralized
29.	**ASAX**	Real-Time	Continuous	Passive	High	Low	Centralized	Centralized
30.	**ID-Trak**	Real-Time	Continuous	Active	Low	Medium	Distributed	Centralized
31.	**OSSEC**	Real-Time	Continuous	Active	High	Medium	Centralized	Centralized
32.	**Suricata**	Real-Time	Continuous	Active	Medium	High	Centralized	Centralized

5.1 Audit Source and Detection Method

(a) Audit data source: It mentions to the source of the IDS. The audit data source of IDS totally based upon the input information. On the behalf of input information there are two major source of audit data host based and network based audit trails (Security logs). The host based security logs includes system kernel logs, application logs and intrusion detection alerts etc. The host based system data are present in the local host of system. On the other hand, network based observe the audit data and whole network traffic directly from the network. In the analyzed tools there are six intrusions detection tools that have ability for both Host based as well as network based functionally. Mostly tools support either Network based or Host based IDS. OSSEC and Haystack are based on the host based IDS.

(b) Detection Method: it mentions the ability of IDS to detect the attack of different types on the network or an information system. There are some intrusion detection systems is anomaly based and some systems are rule based [19].

Table: 5.3 Audit Source and Detection Method

S. No.	Name of IDS	Audit Source	Anomaly Based	Rule Based
1.	Haystack	HBIDS	Yes	Yes
2.	Snort	NBIDS	No	Yes
3.	MIDAS	HBIDS	Yes	Yes
4.	Dragon	HBIDS/NBIDS	Yes	Yes
5.	IDES	HBIDS	Yes	Yes
6.	Cisco Secure IDS	NBIDS	No	Yes
7.	Shadow	NBIDS	No	Yes
8.	Comp Watch	HBIDS	Yes	No
9.	EMERALD	HBIDS/NBIDS	Yes	Yes
10.	Hyperview	HBIDS	Yes	No
11.	Net Ranger	NBIDS	No	Yes
12.	Bro	NBIDS	No	Yes
13.	Cyber cop	HBIDS/NBIDS	No	Yes
14.	NADIR	HBIDS	Yes	Yes
15.	NIDES	HBIDS	Yes	Yes
16.	RealSecure	HBIDS/NBIDS	No	Yes
17.	GrIDS	HBIDS/NBIDS	No	Yes

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

18.	Net Prowler	HBIDS	No	Yes
19.	USTAT	HBIDS	No	Yes
20.	T-Sight	NBIDS	No	Yes
21.	JiNao	HBIDS	Yes	Yes
22.	SecureNet Pro	NBIDS	No	Yes
23.	Net Stat	NBIDS	Yes	Yes
24.	DPEM	HBIDS	Yes	No
25.	Session Wall 3	NBIDS	No	Yes
26.	Intruder Alert	HBIDS/NBIDS	No	Yes
27.	IDIOT	HBIDS	No	Yes
28.	Entrax	HBIDS	No	Yes
29.	ASAX	HBIDS	No	Yes
30.	ID-Trak	NBIDS	No	Yes
31.	OSSEC	HBIDS	No	Yes
32.	Suricata	NBIDS	Yes	Yes

5.2 Platform and protocols supported

(a) Platform (Operating System): The different types of intrusion detection system surveyed they are developed by different vendors and all the intrusion detection system supports different operating system from that systems the number of IDS support UNIX operating system. Table contains the intrusion detection systems against the supported platform.

(b) Protocol: The most of the intrusion detection tools support the TCP/IP protocol suite. Table gives the detail of protocols supported by each product.

Table: 5.4 Platform and protocols supported of Intrusion detection tools

S. No.	Name of IDS	Protocols	Platform Supported
1.	Haystack	TCP/IP	Microsoft Windows, Mac OS X, Linux
2.	Snort	TCP/IP	Microsoft window, Linux
3.	MIDAS	TCP/IP	UNIX
4.	Dragon	TCP/IP	Microsoft window, Solaris, Linux
5.	IDES	TCP/IP	SunOS 4.0, Sun C2, UNIX
6.	Cisco Secure IDS	TCP/IP	Microsoft window, UNIX
7.	Shadow	TCP/IP	UNIX
8.	Comp Watch	TCP/IP	UNIX
9.	EMERALD	TCP/IP	Microsoft window, UNIX
10.	Hyperview	TCP/IP,HTTP	Microsoft window
11.	Net Ranger	TCP/IP,UDP	Solaris
12.	Bro		UNIX
13.	Cyber cop	TCP/IP	Solaris, Window NT

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

14.	NADIR	TCP/IP	Sun OS
15.	NIDES	TCP/IP	Sun OS
16.	RealSecure	TCP/IP	Solaris, NT
17.	GrIDS	TCP, UDP, and ICMP	UNIX
18.	Net Prowler	TCP/IP	Microsoft window, U/
19.	USTAT	TCP/IP,UDP	Sun OS, UNIX
20.	T-Sight	NA	Microsoft Window
21.	JiNao	OSPF, TCP/IP SNMP	
22.	SecureNet Pro	TCP/IP	Solaris, Linux
23.	Net Stat	TCP/IP,UDP	UNIX
24.	DPEM	TCP/IP	UNIX
25.	Session-Wall 3	TCP/IP	Window NT, Window 95/98
26.	Intruder Alert	TCP/IP, IPX/SPX	Sun OS, Solaris
27.	IDIOT	TCP/IP	
28.	Entrax	TCP/IP	NT, UNIX
29.	ASAX	TCP/IP	UNIX-Like
30.	ID-Trak	TCP/IP	NT
31.	OSSEC	TCP/IP,UDP	Linux, Windows, Solaris, and Mac OS
32.	Suricata	TCP/IP, UDP,FTP	Linux, unix ,MAC, windows etc.,

6. Conclusion

Internet and local networks have grown to be all over the place. So organizations are more and more employing quite a lot of intrusion detection system that monitor IT security breaches because intrusion events are developing day by day. In this survey paper, we describe the different types of IDS and highlights the intrusion detection techniques. In this survey the total 32 (Thirty-Two) commercial and research intrusion detection tools were analyzed they were developed by organization. The analysis of the intrusion detection tools according to the different parameters. Almost all the intrusion detection tools are detecting the intrusion in Real-time and Haystack, shadow, comp watch, T-sight and few more detection tools are detecting intrusion in Non-Real-Time. IDS is also a high performance network component with extremely high availability and dependability requirements. As most office PC users are painfully aware, availability and dependability are not part of the vocabulary of software vendors. It is the author's belief that most ID systems originate from traditional software vendors rather that from network infrastructure vendors. Most of today's IDS are not yet mature enough for large scale, enterprise wide deployment.

References

[1] Axelsson, S. (2000), Intrusion detection systems: A survey and taxonomy. Tech. Rep.99-15, Dept. of Computer Engineering, Chalmers University of Technology, SE-412 96 Gteborg, Sweden.

[2] Rupinder Gill, Jason Smith and Andrew Clark (2006), "Specification-Based Intrusion Detection in WLANs", Information Security Institute, Queensland University of Technology GPO Box 2434, Brisbane, 4001, QLD, Australia. doi.ieeecomputersociety.org/10.1109/ACSAC,48

[3] Zhang, Y and W. Lee. (2000), "Intrusion Detection in Wireless Ad-Hoc Networks", In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, Boston: Massachussetts.

ISSN:0971-1260

Vol-22-Special-Issue-27-December-2019

[4] S Sahu, M Pandey (2014)," Distributed Denial of Service Attacks: A Review" I.J. Modern Education and Computer Science, 1, pp.65-71.

[5] Adam Carlson, Jingmin Z., Mark H. and B.R. (2007), "Modeling network intrusion detection alerts for correlation", ACM Transactions on Information and System Security (TISSEC), Vol.10, No.1, pp 1-12.

[6] Barbara, D., Couto, J., Jajodia, S., & Wu, N. (2003), "An architecture for anomaly detection", Applications of Data Mining in Computer Security pp. 63--76.

[7] Denning D. (1987), "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp.222-232.

[8] Nong Ye (2001), "A Scalable Clustering Technique for Intrusion Signature Recognition", IEEE Workshop on Information Assurance and Security United States Military Academy.

[9] Pharate, A., Bhat, H., Shilimkar, V., & Mhetre, N. (2015). Classification of Intrusion Detection System. International Journal of Computer Applications, 118(7), 975–8887.

[10] Hofmeyr, S., Forrest, S., & Somayaji, A. (1998),"Intrusion detection using sequences of system calls", Journal of Computer Security, 6, pp.151--180.

[11] Ilgun, K., Kemmerer, R.A., & Porras, P.A. (1995),"State Transition Analysis: A Rule-Based Intrusion Detection Approach," IEEE Transactions on Software Engineering, Vol. 21, No. 3 pp. 181-199., Information and System Security.

[12] Estevez-Tapiador, J. M., Garcia-Teodoro, P., Diaz-Verdejo, J. E. (2004), "Anomaly Detection Methods in Wired Networks: A Survey and Taxonomy," Computer Communications Vol. 27, No. 1, pp.1569–1584.

[13] Zonghua Zhang and Hong Shen (2005),"A Brief Observation-Centric Analysis on Anomaly-Based Intrusion Detection", Springer-Verlag Berlin Heidelberg.

[14] Stefan Axelsson (2000),"Intrusion Detection Systems:A Survey and Taxonomy" Chalmers University of Technology G¨oteborg, Sweden Pages 1-27.

[15] Jatinder Singh, Lakhwinder Kaur, Savita Gupta (2009) "Analysis of Intrusion Detection Tools for Wireless Local Area Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7 pages 168-177.

[16] Fu T. An Analysis of Packet Fragmentation Attacks vs. Snort Intrusion Detection System. International Journal of Computer Engineering Science (IJCES), May 2012.

[17] Day, David, Burns B. A performance analysis of snort and suricata network intrusion detection and prevention engines. Fifth International Conference on Digital Society, Gosier, Guadeloupe. 2011.

[18] OSSEC website, http://www.ossec.net/, 30 Oct 2013.

[19] Ko, C. (2000), "Logic induction of valid behavior specifications for intrusion detection" . In M. Reiter & R. Needham (Eds.), Proceedings of 2000 IEEE symposium of security and privacy IEEE Computer Society, Los Alamitos, CA pp. 142--153.