ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Intrusion Detection System in Wireless LANs: A Review

Sonali Nemade, Madhuri.A. Darekar, Jyoti Bachhav

Assistant Professor, Dept. of Computer Science, Dr.D.Y.Patil A.C.S. College, Pune, India

Assistant Professor, Dept. of Computer Science, Dr.D.Y.Patil A.C.S. College, Pune, India

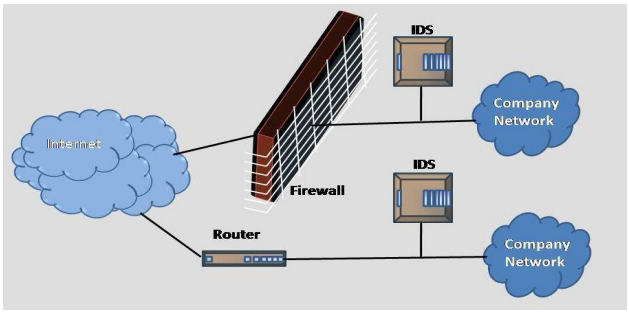
Assistant Professor, Dept. of Computer Science, Dr.D.Y.Patil A.C.S. College, Pune, India

ABSTRACT: Intrusion detection system is software application or a device which is used to monitor system or network for any type of malicious activity or policy violations. Intrusion detection system identifies the abnormal network security. It access integrity of crucial system and data files. In this paper, We have discussed a review of various intrusion detection systems like host based , signature based, network based intrusion detection system and analysis of active intrusion detection system.

Wireless LANs provide mobility, flexibility, scalability

KEYWORDS: IDS, IPS, Intrusion, WSN

I. INTRODUCTION



Intrusion detection is the process of monitoring computers or network for unauthorized data detecting. The main goal of the system is network attack such as a denial of service attack.

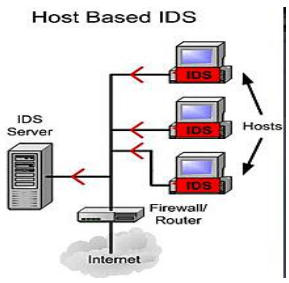
Intrusion Detection System is any hardware, software, or a combination of both that monitors a system or network of systems against any malicious activity. Intrusion detection system is used for detecting or preventing break-ins or misuse of the network.

It uses a security policy to detect unusual activities which are defined by the administrator based on the needs of the organization. Updating policies regularly is required to keep up with the threats and needs. IEEE 802.11 Wireless LAN technology is used for Intrusion detection system which is used to access remotely locates. WLANs generally refer to the physical and data link layer of the OSI model.

II. TYPES OF INTRUSION DETECTION SYSTEM

There are following types of Intrusion Detection Systems:

A. HOST BASED



Intrusion Detection System is installed on a host in the network. HIDS generally collects and analyzes the traffic. It is used to monitor and analyze the internals of a computing system and the network packets on its network interfaces. Host based system includes workstation, server, mobile devices. In host based detection system it is able to watch the misuse of password files in UNIX and the Registry in Windows.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

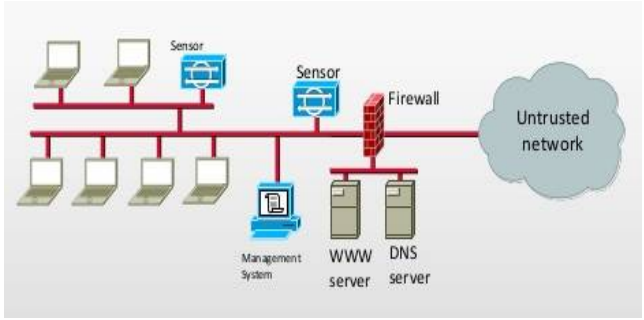
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

B. NETWORK BASED

Network IDSs (NIDS) are placed in key areas of network infrastructure and monitors the traffic as it flows to other host. Unlike HIDS, NIDS have the capability of monitoring the network and detecting the malicious activities intended for that network. Monitoring criteria for a specific host in the network can be increased or decreased with relative ease.



C. STACK BASED

Stack based IDS works by integrating closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers. Stack based watch the packet from the stack before the OS or application has a chance to process the packets.

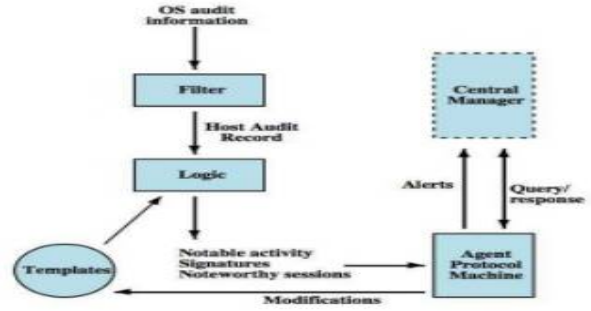


Fig. - Stack Based IDS

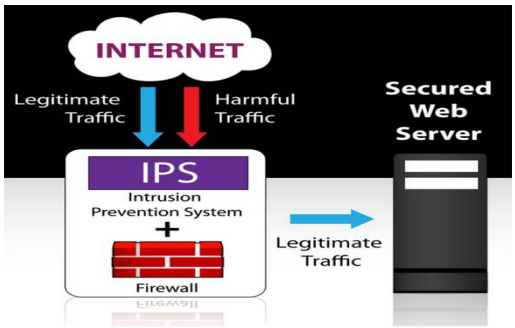
D. SIGNATURE BASED

Signature-Based IDS use a rule set. It is identify intrusions by watching for patterns of events specific to known and documented attacks. Signature based IDS are connected to a large database. It compares the information it gathers against those attack signatures to detect a match.

If the database is not updated with regularity then new attacks could slip through. It also Detect new attacks that share characteristics with old attacks, e.g., accessing 'cmd.exe' via a HTTP GET request.

E. ANOMALY BASED

Anomaly detectors monitor network segments to compare their state to the normal baseline and look for current behaviour which deviate statistically from the normal. This capability theoretically gives anomaly-based IDSs abilities to detect new attacks that are neither known nor for which signatures have been created.



III. WHY USE IDS FOR WIRELESS LAN

Wireless intrusion detection system implemented in physical layer and data link layer which makes passive access to the medium a trivial and limited bandwidth available to wireless physical layers efficient restriction on intrusion detection techniques.

Wireless network consist of mobile client station like laptops and handheld computers which has limited battery life and computing resources and introducing further constraints on the technique that may be adopted by a WIDS.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

In wireless LANs (WLAN), it can be difficult to control the area of access. The range of a wireless network reaches outside their physical boundaries of an organization. With such a problem with wireless security, developing and implementing WIDS systems is definitely a step in the right direction.

IV. DIFFERENCE BETWEEN INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM

IPS systems also differ from IDS in the way that they detect attacks. IPS systems tend to rely on packet inspections. The IPS will examine inbound packets and determine what those packets are really being used for before making a determination as to whether or not to allow those packets to make it onto your network. IDS are a device or software application that monitors a network or system for malicious activity or policy violations.

There are some important differences between IDS and IPS systems. For example if you are shopping for an effective security device, your network will usually be more secure if you use an IPS rather than IDS.

V. TECHNIQUES OF INTRUSION DETECTION SYSTEM

1. **Artificial Neural Networks (ANNs):**
   System is trained by inserting related input/output data. This training is used afterwards to recognize arbitrary patterns, given as an input to the system.
2. **State Transition Tables**
   Intrusion occurs or not is detected by comparing the behavior of the system with intruder's state transition diagram
3. **Genetic Algorithms (GAs)**
   Mimic the natural reproduction system in nature where after certain changes, only the fittest individuals in a generation will be reproduced in subsequent generations
4. **Fuzzy Logic**
   Handles vagueness and imprecision

VI. CONCLUSION

Wireless intrusion detection systems are an important security of wireless local area networks. While there are drawbacks to implementing a wireless IDS, the benefits will most likely prove to outweigh the downsides. It is used for a variety of 802.11 attacks. WLANs require a number of other security measures improve the security posture of the entire network. With the immense rate of wireless adoption, the ever-increasing number of threats to WLANs, and the growing complexity of attacks, a system to identify and report on threat information can greatly enhance the security of a wireless network.

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. A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad-Hoc Networks," in IEEE Wireless Communications, pp. 48-60, February 2004.
3. 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.
4. 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.
5. T. Phit and K. Abe, "Protocol Specification-based Intrusion Detection System for VoIP," Technical Report of IEICE, vol. 107, pp. 5-10, February 2008.
6. 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)
7. Asmaa Shaker Ashoor (Department computer science, Pune University) Prof. Sharad Gore (Head department statistic, Pune University)," Importance of Intrusion Detection System (IDS)", International Journal of Scientific & Engineering Research, Vol. 2, Issue 1, Jan 2011.
8. V. Jaiganesh et al., "Intrusion Detection Systems: A Survey and Analysis of Classification Techniques", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

9. Deris Stiawan et al., "Characterizing Network Intrusion Prevention System", International Journal of Computer Applications (0975 – 8887), Vol. 14, No.1, January 2011.
10. Ratna Deepika Kannan, Dr. Martin Reed, School of Computer and Electronic Engineering University of Essex, "An Experimental Study of detecting and correlating different Intrusions (Chapter#3)".
11. K. Shafiullah, "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks," The International rab Journal of Information Technology , Vol. 7, No. 4, 2010, pp. 50-55.
12. R. Kaur , "Study of Intrusion Detection Systems for Wireless Networks," International Journal of Wireless Networks and Communication, Vol. 13, 2011,In Press.