Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey over Recent Intrusion Detection Systems

Poonam Choubey, Priyanka Vijayavargiya
Computer Science & RGPV University
Madhya Pradesh, India

Abstract: ***The field of intrusion detection has received increasing attention in present years. First reason is the explosive growth of the internet and the large number of networked systems that exist in all types of organizations. The intrusion detection techniques using data mining have attracted more and more interests in recent years. As an important application of data mining these techniques aim to meliorate the great burden of analyzing huge volumes of audit data and realizing performance optimization of detection rules. In this paper, we have proposed a survey over recent intrusion detection systems.***

Keywords: NIDS, HIDS, IDS

I. INTRODUCTION

The term MANET (Mobile Ad hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration.

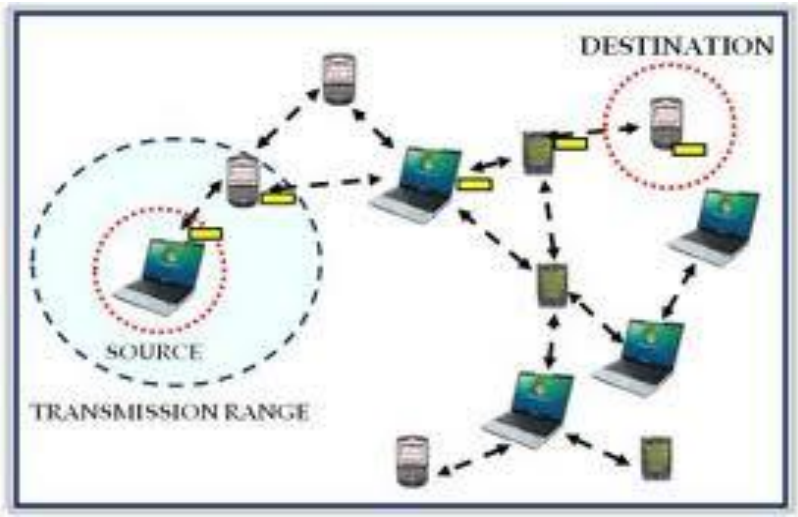

Figure 1: Structure of MANET

The field of intrusion detection has received increasing attention in present years. First reason is the explosive growth of the internet and the large number of networked systems that exist in all types of organizations.

Because they only scrutinize network traffic [1] the NIDS do not benefit from running on the host. They are often run on dedicated machines that observe the network flows sometimes in conjunction with a firewall. In this case they are not affected by security vulnerabilities on the machines they are monitoring. Only a limited number of information can be inferred from data gathered on the network link. The widespread adoption of end-to-end encryption further limits the amount of information that can be gathered at the network interface.

One major shortcoming of NIDS is that they are oblivious to local root attacks. The authorized user of the system that attempts to gain additional privileges will not be deleted if attack is performed locally. The authorized user of the system may be able to set up an encrypted channel when accessing the machine remotely.

The HIDS have an ideal vantage point [6]. An HIDS runs on the machine it monitors, HIDS can theoretically observe and log any event occurring on the machine. The complexity of current operating system often makes it difficult if not impossible to accurately monitor certain events. There are many difficulties faced by security tools that rely on system calls interposition to monitor a host.

In addition to cons resulting from an incorrect or incomplete understanding of the operationg system, the race conditions in the operating system make the implementation of such tools delicate. The HIDSs are also confirmed with difficulties arrived from arising from potential tampering by the attacker. Also a secure logging mechanism is necessary to prevent logs from being erased if the attacker compromises with the machine. Even if such a secure mechanism is available, the attacker obtaining super user privilege on the host can disable the HIDS. If HIDS is a user process, then an attacker can simply terminate the process. If HIDS is embedded in the kernel, then the attacker can modify the kernel by loading a kernel module or by writing directly in the kernel memory. It means that an HIDS can only be trusted up to the point where the system was compromised.

II. LITERATURE SURVEY

In this paper [1] the author has we discussed the security issues and their current solutions in the mobile ad hoc network. The nature of the mobile ad hoc network is vulnerable. There are many security threats for the mobile adhoc network. The author has first analyze the main vulnerabilities in the mobile ad hoc networks. It is more vulnerable to these attacks in comparison to the traditional wired network. Then they discuss the security criteria of the mobile ad hoc network and the main existing attacks available in the modern era.

The *ad hoc network [2]* is a collection of wireless mobile computers or nodes. The individual nodes in the mobile adhoc network cooperate to each other by forwarding packets. It helps them in increasing their range. The research done in the past in ad hoc networking is basically analyzed the routing problem in a trusted environment. In this paper, the authors have present attacks against routing in ad hoc networks. They also presented the design and performance evaluation of a new secure on-demand ad hoc network routing protocol called Ariadne. The proposed new protocol prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes. It also prevents many types of Denial-of-Service attacks. It is efficient using only highly efficient *symmetric* cryptographic primitives.

The work in [3] defined the Mobile Ad hoc Network of Networks as a group of large autonomous wireless nodes. All such nodes communicates with each otherThese nodes communicates on a peer-to-peer basis in a heterogeneous environment with no predefined infrastructure. Every node behaves like an ad hoc network. Also every node performs the self management. Prevention and detection of malicious nodes is one of the major problems in such networks. Recovery is also suggested as equally problematic in such networks. The paper [3] proposes a novel behaviour detection algorithm combined with threshold cryptography digital certificates to satisfy prevention and detection to securely manage our system.

As per the work done in [4], adhoc network is a collection of nodes without any centralized or decentralized management. Authors of paper [4] proposed a protocol for routing data in the ad hoc network. This work is based on dynamic source routing. This proposed protocol has the ability to adopt according to the routing changes. Also the overhead of the proposed protocol is quite low. Based on results from a packet-level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates..

In paper [5], the author has developed model. This model is based on the sequential probability ratio. This test identifies the misbehaving nodes. It categorizes the routes in two categories: one which contains the jamming nodes & one which does not contain jamming nodes. Our evaluation shows that the localized approach is not only the better architectural choice for ad hoc networks but also results in a more accurate exposure of misbehaving nodes while incurring low false positives and low false negatives.

III. CONCLUSION

We have analyzed the existing intrusion detection systems. We can conclude that many of the current intrusion decision system are signature-based systems. The SIDS or signature based IDS are also known as misuse detection looks for a specific signature to match or signaling an instruction. They are provided with the signatures or patterns, but SIDS are of little use for as yet unknown attack methods. It means that an IDS using misuse detection will only detect known attacks . Rate of false positives is small to nil but these types of systems are poor at detecting new attacks or variations of known attacks or attacks that can be masked as normal behavior. The Statistical Based Intrusion Detection Systems (SBIDS) can alleviate many of the aforementioned pitfalls of a Signature Based IDS. The Statistical Based Systems rely on statically models such as the Bayes' Theorem, the decision trees, etc. to identify anomalous packets on the network. So still there is need of intrusion detection system, which can detect new unknown attacks and should be more accurate.

REFERENCES

[1] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[2] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23

[3] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.

[4] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[5] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, L. Benini, "Modeling and Optimization of a Solar Energy Harvester System for Self-Powered Wireless Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 7, pp. 2759-2766, July 2008.

