International Journal of Information Technology and Management

Vol. VII, Issue No. IX, August-2014, ISSN 2249-4510

"EFFICIENCY OF NETWORK INTRUSION PREVENTION SYSTEMS (IPS) AND INTRUSION DETECTION IN NETWORKS SECURITY"

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VII, Issue No. IX, August-2014, ISSN 2249-4510

"Efficiency of Network Intrusion Prevention Systems (IPS) and Intrusion Detection in Networks Security"

Pradeep Kumar

Assistant Professor, Sityog Institute of Technology, Aurangabad, Bihar

Abstract – Intrusion Prevention System (IPS) has extra features to protected computer network scheme. Computer systems are opposite main threat in the form of hateful data which causing denial of service, in sequence theft, financial and trustworthiness loss etc. No defense technique has been proved successful in handling these threats.

Intrusion Detection and Prevention Systems (IDPSs) being best of available solutions.

Defense system and system monitoring has becomes essential constituent of computer security to predict and stop assaults. Different conventional Intrusion Detection System Intrusion Prevention System has additional features to secure computer complex system. In this paper, we are presenting mapping problem and challenges of Intrusion Prevention System dedicated in hybrid apparatus. Throughout this paper, we reviewed the concept of mapping and challenges in IPS.

Keywords: Intrusion Prevention System, Security, IPS, Mapping Problem

----------♦----------

INTRODUCTION

Intrusion Prevention System (IPS) technology protects networks from both known and unknown threats, blocking attacks that might otherwise take advantage of network vulnerabilities and unpatched systems.

Assault, threat or intrusions, next to computer system and network have become normal events, many system device and tools are available to improve and find answer the threat of these assault. Analyzed from proposal [1] and [2] highlighted currently countermeasure next to from security breach, such as

(I) Firewall, make stronger in implementing executing rules and rule but it cannot do anything about attack and its performance from within system.

(II) Interruption Detection, only send the alert to activate after attacked has reached to the network, and does not anything to discontinue attacks.

Currently, IDS technology is not very effectual against predict a new device of attack. There are several limits, such as presentation, suppleness. When an attack is identified, intrusion avoidance blocks and logs the offending data. Ghorbani [3], He advised work to describe IPS and its uses to secure the system.

INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

There are several ways to categorize IDS:

- **Misuse detection** vs. **anomaly detection**: in misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network

segments to compare their state to the normal baseline and look for anomalies.

- **Network-based** vs. **host-based systems**: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.

- **Passive system** vs. **reactive system**: in a passive system, the IDS detect a potential security breach, log the information and signal an alert. In a reactive system, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Though they both relate to network security, AN ID differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

The main functions of a network intrusion detection system include:

- Detecting attacks: such a system detects security threats and attacks as and when they happen by providing real-time network monitoring.

- Offer information: If this system detects an attack, then it put forward information about the attack.

- Take corrective steps: Once an attack is detected by the system, the active systems also take measure to tackle the attack.

- Storage: It also stores the events either locally or otherwise in case of an attack.

MAPPING AND CHALLENGES IPS

At this time, necessary a system to give early warning from interruption security breach with knowledge based has turn out to be a necessity. The system should be smart in classifying of packet data, if inquisitive or naughty are detected, alert is triggered.

IPS - can be defined as a formation produce which focuses on recognize and blocking hateful network in real time [4].

IPSs prolonged on the functionality make available by IDS by enabling to stop attack next to of network. By means of admiration from suggestion [5], they present real-time disturbance avoidance and indiscretion system, major difficulty IPS is notice only attack they know from name, and then Schultz [6], has forecast the future technology, such as-

(I) improved underlying interruption detection; (II) progression in application-level psychoanalysis, (III) more complicated reply capabilities, and (IV) addition of interruption avoidance into other security devices. Moreover, they forecast about interruption avoidance technology is very optimistic in market.

DETECTION ANALYSIS

One difficulty faced by all discoveries in IPS is that hard to be familiar with and documented analyzing packet in real-time transfer. To notice doubtful danger, there are two move toward [3], [9], [10], and [11]:

(i) Host-based move toward : Host-based are currently well-liked technologies, it is make sure for uncertain activity at operating system stage , the monitoring place use the agent module, which is useful to identify attack. The alarm triggered and gives all-encompassing this activity, and

(ii) Network-based move toward, the sniff and recognize small packages every inbound-outbound inside outside of the network.

As stated by some reported task [7], and [8], there are two classifications based according to the discovery technique small packages.

Irregularity-based, irregularity-based discovery, the key to the request of irregularity detection methods to the field known as danger consists in a simple but dangerous theory. Hence, irregularity detection has the ability of notice new types of interruption and builds replica of standard appearance and automatically notice any break of it to make fear.

Misuse-based, psychoanalysis form previously work by [12], mistreatment discovery identifies intrusions by corresponding experiential data with pre-defined account of all-encompassing behavior. Furthermore, in this method threat find at the network transport in search of straight matches to recognized pattern of small package.

CONCLUSION:

IPS has extra features to secure and sound computer network system. The supplementary features recognize and distinguish cynical threat activate alarm, incidence announcement, from side to side accountable response. In this beginning surveillance from before researcher, amalgam

techniques are one of solution for association and judgment interference threat. Future cross IPS takes the compensation to add to rightness and accuracy usual or distrustful danger.

REFERENCES:

[1] Y. Colorado, D. Padilla, and E. Guillen "based Intrusion Detection and Prevention Systems," Latin-American Conference Communications, 2009, pp. 0-4.

[2] L. Jiren, L. Tie, B. Cao, Y. Zhongde, and Z. Zhihong, "A Study on Performance Improvement of Gateway Anti-Virus System Based on File Scanning," Control and Decision Conference 09, 2009, pp. 2293-2295.

[3] Lu, A.A., T. Ghorbani, W., Network Intrusion Detection and Prevention : Concepts and Technique, Springer - 2009.

[4] A. Fuchsberger "Intrusion Detection Systems and Intrusion Prevention Systems" Information Security Technical Report, volume 10, 2005, pp. 134-139.

[5] N. Tymoshyk, A. Piskozub, and T. Dutkevych, "Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks," IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems Technology and Application - 2007, pp. 599-602.

[6] E. Ray and E.E. Schultz "Future of Intrusion Prevention," Computer Fraud & Security- 2007, pp. 11-13.

[7] W.K. Lee, S.H. Oh "An anomaly intrusion detection method by clustering normal user behavior" Computers & Security, volume 22, 2003, pp. 596-612.

[8] J.M. Estevez-Tapiador, J.E. Diaz-verdejo and P. Garcia-Teodoro, "Anomaly detection methods in wired networks : a survey and taxonomy," Computer Communications volume 27, 2004, pp. 1569-1584.

[9] J.H.P. Eloff, H.S. Venter "A taxonomy for information security technologies," Information Security - 2003, pp. 299-307.

[10] L. Fan, J. Li, X. Chen ,S. Zhang, "Building network attack graph for alert causal correlation," Computers and Security, volume 27, 2008, pp. 188-196.

[11] A. Salah, H.M. Faheem, M. Shouman, "Surviving cyber warfare with a hybrid multi agent-based intrusion prevention system" IEEE Potentials- 2010, pp. 32-40.

[12] W. Banzhaf, A. Foroughifar, S.X. Wu "The use of computational intelligence in intrusion detection systems- A review" Applied Soft Computing, volume 10, 2010, pp. 1-35.

[13] http://www.webopedia.com/TERM/I/intrusion_ detection_ system.html

[14] Muhammad Imran Shafi, Muhammad Akram, Sikandar Hayat, and Imran Sohail "Effectiveness of Intrusion Prevention Systems (IPS) in Fast Networks" Journal of computing, volume 2, issue 6, june 2010, ISSN 2151-9617