GNITED MINDS
Journals

International Journal of Information Technology and Management

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

"CYBER SECURITY AND NETWORK INTRUSION PREVENTION SYSTEM"

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

"Cyber Security and Network Intrusion Prevention System"

Nagendra Mani Tripathi

Director Global College Chauradih Chail Kaushambi

Abstract – In this paper we present about cyber security and network intrusion prevention system. Cyber refuge has materialized as an established obedience for computer systems. Different information security techniques are available today to protect information systems against illegal use, duplication, modification, destruction and virus attacks. Defense system and system monitoring has becomes essential constituent of computer security to predict and stop assaults. Intrusion Prevention System has extra features to secure computer complex system. In this paper, we are presenting mapping problem and challenges of Intrusion Prevention System dedicated in hybrid apparatus. All through this paper, we reviewed the concept of mapping and challenges in IPS.

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

---------------------------♦-----------------------------

INTRODUCTION

Computer security is distinct as the protection of computing systems next to threats to privacy, integrity, and ease of use. Confidentiality means that information is disclosed merely according to plan; reality means that in order isn't shattered or corrupted and that the system performs correctly ease of use. Computing systems pass on to computers, computer networks, and the in sequence they handle. Security threats come from unlike sources such as ordinary forces, accidents, failure of services and people known as intruders.

There are two types of Intruders-

External intruders - who are unconstitutional users of the equipment they attack.

Internal intruders - who have approval to access the system with some boundaries, the traditional deterrence techniques such as user verification, data encryption, keep away from programming faults and firewall is used as the first line of defense for computer safety.

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 next to 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.

Lately, intrusion detection system uses to association move in real-traffic for rising the correctness discovery and decreasing false alarm pace. In some instance, IPS adopts techniques from disruption discovery, such as detection approach, monitoring antenna, and alert instrument. On contrary, IPS can be used to panic for attacks within a network and give for acting on attack suspicious with Firewall and IDS purpose device. Performed work [5], outline the prospect trends of IPS and its functionality inspection/prevent.

IPS is alike to IDS. It intended and procedure to recognize and recognized possible security violations in brook network. However, the main intrusion avoidance use signature device to recognize activity in network transfer and host where carry out detect on inbound – outbound small packages and would be to chunk that action before the injure and access network capital.

An IPS can be distinct and identifies blocking hateful network activity [4]. IPS integrates the method of firewall by means of that of the IDS properly with practical technique, it is a novel come up to system to protection networking systems and averts attacks from entering the network by analytical various data evidence and avoidance manner of example credit sensor. When an attack is recognized, interruption avoidance blocks and logs the aberrant data.

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 [6], they present real-time disturbance avoidance and indiscretion system, major difficulty IPS is notice only attack they know from name, and then Schultz [7], 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.

Psychoanalysis of detection

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], [10], [11], and [12]:

(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 [17], [8], and [9], there are two classifications based according to the discovery technique small packages are shown in Figure 3: (i) anomaly-based discovery, and (ii) misuse-based uncovering.

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 [17], 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] G. Ollmann, “Intrusion Prevention Systems, destined to replace legacy routers,” Network Security, volume 11, 2003, pp. 18-19.

[6] 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.

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

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

[9] 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.

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

[11] 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.

[12] 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.

[13] A. Seleznyov, S. Puuronen, “HIDSUR: A Hybrid Intrusion Detection System Based on Real-time User Recognition,” IEEE Proceeding, 11th International Worskhop Database and Expert Systems Applications - 2000, pp. 41-45.

[14] X. Yu “A New Model of Intelligent Hybrid Network Intrusion Detection System” IEEE Proceeding International Conference Bioinformatics and Biomedical Technology , 2010, pp. 386-389.

[15] W. Xiaoping, Y. Qing, H. Geofeng, “A Hybrid Model of RST and DST with Its Application in Intrusion Detection,” IEEE Computer Society, International Symposium on Inteligent Information Technology and Security Informatics - 2010, pp. 202-205.

[16] A. Momenzaideh, M.S. Abadeh, M.B. Pouyyan ,A. Foroughifar “Misuse Detection via a Novel Hybrid System” 2009 Third UKSim European Symposium on Computer Modeling and Simulation - 2009, pp. 11-16.

[17] 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.

[18] A. Seleznyov ,S. Puuronen, “A Hybrid Intrusion Detection System Based on Real-time User Recognition ” IEEE Proceeding - 11th International Worskhop Database and Expert Systems Applications - 2000, pp. 41-45.

[19] Mohd. Yazid Idris ,Deris Stiawan, Abdul Hanan Abdullah, “Characterizing Network Intrusion Prevention System” International Journal of Computer Application 0975 – 8887, Volume 14, No.1, January 2011.