International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Internal Intrusion Detection Systems

Bhingardive Deepali R[1], Ranmalkar Vrushali S[2]

[1]Vishwabharati Academy's College of Engineering, Ahmednagar, Maharashtra 414201, India

[2]Professor, Vishwabharati Academy's College of Engineering, Ahmednagar, Maharashtra 414201, India

Abstract: ***Now a day's computer systems use user IDs and passwords as the login patterns to validate users. However, most of the people share their login patterns with co-workers and request them to assist co-tasks. There are new attacks are appear everyday due to that the system makes the insecure even the system wrapped with number of security measures. To detect the intrusion, an Intrusion Detection System (IDS) is used. To detect the intrusion and respond in timely manner is its main function. In other words IDS function is limited to detection as well as response. The IDS is unable to capture the state of the system when an intrusion is disclosed. So that, in original form, it fails to preserve the evidences against the attack. New security system strategy is very much needed to maintain the completeness and reliability of proof for later examination. In this research work, there proposed an automated Digital Forensic Technique with Intrusion Detection System. It sends an alert notification message to capture the state of the system, to administrator followed by invoke the digital forensic tool Once an IDS catch an intrusion. To prove the damage Captured image can be used as evidence in the court of law.***

Keywords: Intrusion Detection Systems, Digital Forensic, Logs, Cryptography

1. Introduction

In the past decades, people exploit powerful capabilities and processing power of computer system, security has been one of the very serious problems in the computer domain.

In today's scenario, to safeguard the organization electronic assets, Intrusion Detection System is crucial requirement. To find whether the traffic is malicious or not Intrusion detection is a process of analyzes and monitor the traffic on a device or network. It can be a physical appliance or software that monitors the traffic which violates organization security policies and standard security practices. To catch the respond and intrusion in timely manner as a result risks of intrusions is diminished it continuously watches the traffic. Based on the deployment IDS (Intrusion Detection System) broadly divided into two types such that Host based Intrusion Detection System (HIDS) and the second is Network based Intrusion Detection System (NIDS). Host-based Intrusion Detection System (HIDS) is configured on a particular server/ system. It continuously analyzes and monitor the activities the system where it is set up or configured. Whenever an intrusion is detected Host based Intrusion Detection System triggers an alert notification. For instance, when an attacker tries to modify or create or delete key system files alert will be generated. Wide advantages of the HIDS that it analyzes the incoming encrypted traffic which cannot be detected NIDS. To catch the attack like Port Scans, Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attack, etc. Network Intrusion Detection System continuously analyze and monitor the network traffic. To classify as non-malicious or malicious traffic it inspect the incoming network traffic. If any predefined signatures or patterns of malicious behavior are present it re-assembles the packets, examine the payload/ headers portion and determine. Recently "Intrusion investigations with data-hiding for computer Log-file Forensics" system technique has been designed. In this approach, log file is stored in two different area as well as in two different forms. On target host the Log file in plain text form is stored and a copy of same log file is stored in another host called log manager and it is covered in image using steganography. Intrusion Detection System running on target host detects an intrusion and sends an alert message notification to the security administrator about the intrusion when an intruder tries struggle to alter log file on target host. Security administrator use the stego image to extract log file and compares it with log file available in the target host. To justify whether the intrusion occurred or not. Intrusion is confirmed If the result of the comparison is not equal else not. Forensic technique system is unable to capture the proof of the attack is the major limitation of this approach. So to secure the log file damage for forensic analysis, it is not possible and to show in the court of law, proof cannot be collected immediately against the attack. In this work automated Digital Forensic Technique with Intrusion Detection System IDS is proposed to overcome this limitation. Because the current IDS are not designed to protect and collect evidence against the attack this new technique is crucial requirement. Digital forensics plays very important role by providing scientifically proven methods to process, gather, interpret and use digital evidence to bring a decisive description of attack.

2. Literature Survey

Computer forensics science, which views computer systems as crime scenes, goal to preserve, identify, analyze, recover and present opinions and facts on information collected for a security event [1]. It investigate what attackers have done like as spreading computer malwares, viruses, and malicious codes and conducting Distributed Denial of Service attacks [2]. Most intrusion catching techniques focus on how to detect malicious network behaviors [3] and acquire the characteristics of attack packets, such that attack patterns, based on the histories recorded in log files [4]. Qadeer et al [5] used self-developed packet sniffer to gather network packets with which to discriminate network attacks with the help of packet distribution and network states. O'

Shaughnessy and Gray [6] obtained attack patterns and network intrusion from system log files. These files keep traces of computer misuse. It means, from synthetically produced log files, these patterns or traces of misuse can be more correctly reproduced. Wu and Banzhaf [7] acquired research progress of assigning methods of computational intelligence, including fuzzy systems, artificial neural networks, evolutionary computation, swarm intelligence and artificial immune systems to catch malicious behaviors. The authors systematically compared and summarized different intrusion detection methods, thus allowing us to clearly view those existing research challenges.

These aforementioned applications and techniques truly contribute to network security. However, they cannot simply authenticate remote-login users and detect specific types of intrusions, example, when an undefined user logs in to a system with a valid password and user ID. In our previous work, a security system, which includes forensic quality for users at command level rather than at SC level, by invoking forensic techniques and data mining, was developed. Moreover, if attackers use more sessions to issue attacks, e.g., launch DDoS attacks or multistage attacks, then it is not easily for that system to determine attack patterns. Hu et al' [8] presented an intelligent lightweight Intrusion Detection System that utilizes a forensic technique to profile user behaviors and a data mining technique to carry out the cooperative attacks. The authors claimed that the system could catch intrusions efficiently and effectively in real time. However, they did not define the SC filter. Giffin et al. [9] provided another e.g., of integrating computer forensics with a knowledge-based system. The system choose a predefined model, which, grant SC-sequences to be simply executed, is employed by a detection system to bound program execution to ensure the security of the protected system. This is helpful in catching applications that issue a series of malicious SCs and identifying attack sequences having been stored in knowledge bases. When an undetected attack is presented, the system frequently finds the attack sequence in 2s as its computation overhead. Fiore et al'. [10] explored the effectiveness of a detection approach which is based on machine learning using the Discriminative Restricted Boltzmann Machine technique to combine the expressive power of generative models with better classification accuracy capabilities to infer part of its knowledge from incomplete training data so that the network anomaly finding scheme can provide an adequate degree of protection from both external and internal menaces. Faisal et al' [11] examine the possibility of using data stream mining to improve the security of advanced metering infrastructure through an Intrusion Detection System. The advanced metering infrastructure, which is one of the most important components of smart card, serves as a bridge for providing bidirectional information flow between the utility domain and user domain. The authors treat an Intrusion Detection System (IDS) as a second-line security measure after the first-line of primary advanced metering infrastructure security system techniques such as authorization, authentication and encryption.

3. Conclusion

In this work, intrusion detection system is proposed. IDS is used to determine the intrusion. We can easily catch which activities are performed by user. So that we can recover all the modified file. By using web cam system take images of user which performs malicious activities and save that activity in folder and send that activity log and picture of user on clients email id. So that we know that user. So that our system is very effective and efficient for detecting intrusion of system.

References

[1] M. K. Rogers and K. Seigfried, "The future of computer forensics: A needs analysis survey," Comput. Security ,vol. 23, no. 1, pp.12–16, Feb. 2004.
[2] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting web based DDoS attack using MapReduce operations in cloud computing environment," J. Internet Serv. Inf. Security , vol. 3, no. 3/4, pp. 28–37, Nov. 2013.
[3] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming," in Proc. IEEE INFOCOM , San Diego, CA, USA, 2010, pp. 1–5.
[4] A. Garcia, R. Monroy, L. A. Trejo, and C. Mex-Perera, "Analyzing log files for postmortem intrusion detection," IEEE Trans. Syst., Man, Cybern., Part C: Appl. Rev. , vol. 42, no. 6, pp. 1690–1704, Nov. 2012.
[5] M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in Proc. Int. Conf. Commun. Softw. Netw. , Singapore, 2010, pp. 313–317.
[6] S. O'Shaughnessy and G. Gray, "Development and evaluation of a data set generator tool for generating synthetic log files containing computer attack signatures," Int. J. Ambient Comput. Intell. , vol. 3, no. 2, pp. 64–76, Apr. 2011.
[7] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," Appl. Soft Comput. , vol. 10, no. 1, pp. 1–35, Jan. 2010.
[8] B. Hu, J. Su, and V. P. Shirochin "An intelligent lightweight intrusion detection system with forensics technique," in Proc. IEEE Workshop Intell. Data Acquisition Adv. Comput. Syst.: Technol. Appl. , Dortmund, Germany, 2007, pp. 647–651.
[9] J. T. Giffin, S. Jha, and B. P. Miller, "Automated discovery of mimicry attacks," Recent Adv. Intrusion Detection , vol. 4219, pp. 41–60, Sep. 2006
[10] U. Fiore, F. Palmieri, A. Castiglione, and A. D. Santis, "Network anomaly detection with the restricted Boltzmann machine," Neurocomputing , vol. 122, pp. 13–23, Dec. 2013.
[11] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-stream- based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," IEEE Syst. J. , vol. 9, no. 1, pp. 1–14, an. 2014.