

AN APPROACH TO HOST-BASED INTRUSION DETECTION SYSTEM USING SYSTEM CALL PATTERNS

Dhikhi T^{*1}, Dr. M. S. Saravanan^{*2}

¹Research Scholar and Assistant Professor, ²Research Guide

^{*}Department Of Computer Science and Engineering

Saveetha School of Engineering, Saveetha University, Chennai

dhikhi@gmail.com, saravananadu@gmail.com

Abstract - Host-based anomaly intrusion detection system design is very demanding and versatile form of IDS due to the well-known high false alarm rate. The paper presents a new host-based anomaly intrusion detection approach to increase the detection of anomalies using discontinuous system call patterns by reducing false alarms. The basic concept is to employ a semantic structure to kernel level system calls to understand program anomaly behavior to reflect intrinsic activities hidden in high-level programming languages. Furthermore, the new semantic method retains an inherent flexibility to mimic attacks, and established a high level of compactness between different operating system versions. There are two broad classifiers which can be applied to IDS. First, IDS can be considered as either a host based or network-based system. Host-based systems are designed to protect a single computer, and to prevent the execution of malicious code on that single system. Network-based IDS (NIDS) provide a different form of protection by examining network traffic in an attempt to detect intrusions. Intrusion detection systems can be further classified as anomaly centric or signature-based. An anomaly IDS operates by first establishing a robust baseline of normal behavior for the protected system. Theoretically, if this baseline is sufficiently accurate and extensive then any divergence from the baseline would be considered as an intrusion alarm. Signature-based systems, on the other hand, compare observed behavior against a database of templates representing identifiable features from previously seen attacks. If behavior matches a template then an alert is raised, but otherwise all activity is deemed legitimate.

Keywords: Intrusion Detection system, Anomaly detection, Port scanner, Protocol filtering.

I. INTRODUCTION

An intrusion detection system (IDS) checks for the network traffic and finds any abnormal suspicious activity and warns the system or network administrator. In some cases the IDS may also counter to anomalous or abnormal traffic by controlling the user or source IP address from retrieving the network. Intrusion Detection System are categorized in various methods and it approaches the objective of identifying suspicious traffic in different ways.

1.1 IDS Intrusion Detection

Intrusion detection systems are classified into network based (NIDS) and host based (HIDS) intrusion detection systems. One type of IDS can detect attacks based on explicit signatures of known threats, similar to the way antivirus software typically detects and protects against malware. The other IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. NIDS, Network Intrusion Detection Systems are placed in the network to find traffic. NIDS also scans all inbound and outbound traffic but doing so might have a drawback that would damage the overall speed of the network. HIDS, Host Intrusion Detection Systems run on individual hosts or devices on the network that monitors the inbound and outbound packets from the device and will alert the user or administrator of suspicious activity is detected.

1.2 Signature Based IDS:

A signature based IDS will detect attacks by monitoring packets on the network and look them against database of signatures or known malicious instruction

sequences used by threats in the same way as virus scanner. The advantage of using this IDS is that to develop signatures are easy if the network behavior is known. Already known signatures that are trying to exploit a particular attack like buffer overflow vulnerability can be looked in the database for detecting the attack. Thus the Signature based IDS can only detect known attacks. Novel attacks, for which no pattern is available cannot be detected by this IDS. Signature engines are likely to false positives as greater the number of signatures searched for. This increase complexity and cost.

1.3 Anomaly Detection:

Intended to reveal the abnormal behavior, the IDS creates a baseline of normal usage patterns, and anything that widely differs from the normal behavior is labelled as a possible intrusion. Events in this type of IDS are caused by any behaviors that deviates from the predefined or accepted model of behavior. For example if an abnormal user is trying to login by using different passwords for many times rather than 1 or 2 times. This can be considered as a suspicious activity. This kind of detection can detect only the unknown activities. The disadvantage anomaly based detection is it is difficult to define rules. Another drawback is malicious activity that falls within standard usage pattern cannot be detected.

1.4 Objective

The objective of this is to measure the performance that would lead to achieving the goal of better intrusion detection. In this a new intrusion detection approach is proposed for achieving a level of security in the networks, while allowing them to operate in their current exposed mode. The aim of IDS is to recognize unapproved use, misuse, and abuse of computer systems by both insiders and external penetrators in a system. The difficulty of intrusion detection is becoming a challenging task due to the multiplying of diverse computer networks and the enlarged connectivity of computer

systems gives greater contact to outsiders and makes it easier for intruders to evade identification. Intrusion detection systems (IDSs) are based on the beliefs that an intruder's behavior will be noticeably different from that of a legitimate user and that many unauthorized actions are detectable.

II. RELATED WORK

Fang-Yie Leu, Kun-Lin Tsai proposed Internal Intrusion Detection and Protection System (IIDPS) security scheme to identify the attackers inside the host at system call level by the data mining and forensic methods. This helps to check the user's behaviors and form the forensic features to check whether user is valid having an account to access. Computer forensics science, considers computer systems as crime scenes that is intended to identify, preserve, recover, analyze on the data collected for a security event what are the functions done by the attackers like scattering the viruses, malicious code and conducting different attacks. It analyzes what attackers have done such as spreading computer viruses, malwares, and malicious codes and conducting DDoS attacks. IDS emphasis on different detection techniques to identify the behavior of attack pattern based on the data in the audit record.

Qadeer et al. represents a packet sniffer by using network states and packet distribution to gather network packets O' Shaughnessy and Gray developed a network intrusion that can accurately suggest the misuse pattern by testing the attack patterns from system log files. Wu and Banzhaf focus on the growth of implication of different methods of computational intelligence like artificial neural networks, fuzzy systems, evolutionary computation, artificial immune systems, and swarm intelligence to identify abnormal behaviors.

Disadvantages of Existing System

- Constant Network Monitoring, Cannot detect novel or unknown attacks.
- Versatility of the System.
- Telling Threat From Friend
- Heavy processing overhead.

- Vulnerable to attack while creating time consuming, statistically significant baseline

III. PROPOSED SYSTEM

The proposed system can work with any IP plan with the same efficiency. The proposed system can deal with different temporal behaviors of target attacks. The proposed system structure and components. Our system captures packets in real time using a packet capture engine that presents the packets to a preprocessing stage using two pipes. Intrusion Detection Systems (IDSs) allow to understand or detect any of the following information to the other supportive systems such as identification of the intruder, location of the intruder whether single node or regional node, time or date of the intrusion, intrusion activity like active or passive, and intrusion type layer where the intrusion is occurred.

The paper proposes an intelligent host-based anomaly intrusion detection system to improve the identification rate of network attacks by inserting the temporal behavior of the attacks into a TDNN neural network structure. Network attacks usually destroy the data or the network itself and the information is altered with intent to corrupt start by performing network discovery on the different attacks, which includes host sweep and port scan attacks. Host sweep attack determines hosts which are live in the network; the attacker tries to find an entryway to start with or enter into the network. So, intruders will be penetrating for weak points to compromise the system. The three common types of host sweep scan techniques are TCP ECHO, UDP ECHO, and ICMP Sweep. Port Scan Attacks: Port scanning tries to discover the running services on the victim machine, or tries to check the availability of certain service on the victim.

Advantages of Proposed System

- Analyzes ongoing traffic, activity, transactions, and behavior for anomalies.
- Potential to detect previously unknown types of attacks.

- Catalogs the differences between baseline behavior and ongoing activity.

3.1. System Design

In the architecture diagram shown in figure fig.3 the router will be connected to the network and flow the data records through a Network intrusion detection and host intrusion detection system. It will alert the port scans from an administrator. It passes through the MINDS attack through the relevant data of upcoming queries. In HIDS & NIDS can pass through anomaly detection. Finally alerts the administrator after the port scan is done. Forensics queries are provided by the administrator for the user to identify any malicious activity thereby deciding on the detection of an abnormal user.

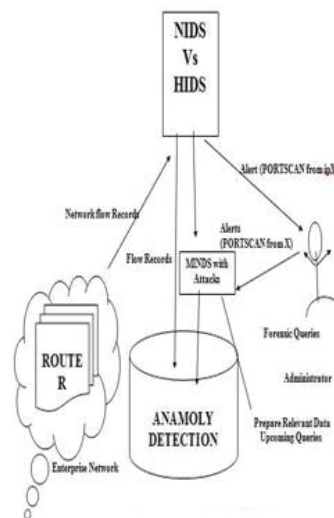


Fig. 3 Architecture Diagram

3.2 Modules

The work in this paper is divided into different modules which consists of

- Port Scanner
- Network Port Scanner
- Packet Sniffing tools
- Types of protocol filtering

- Intruder Logging
- Data Loss from IP

Description

Port Scanner

Scans and detects all the open ports of a system. The “Network Port Scanner” detects all the open ports of an individual system or several other systems connected in a LAN network. The open ports are detected because, all the intruders enter the system only through these ports.

Network Port Scanner

NETWORK PORT SCANNER is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. NETWORK PORT SCANNER uses raw IP packets in different ways to determine availability of the types of hosts on the network, and the diverse services (application name and version) the host’s offers, the versions of operating system used by the host, the kind of firewalls or packet filters used and many more related characteristics. This works sound in the host system and also scans large networks. All major computer operating system works on the network port scanner. It also supports the classic command-line network port scanner executable. Moreover the network port scanner suite includes an advanced GUI and results viewer, a flexible data transfer, redirection, and debugging tool, a utility for comparing scan results, and a packet generation and response analysis tool. The standard ports are identified along with its service e.g., 80/HTTP. If the service of a particular port is not defined then it is displayed as “NONE”. Here the source IP and destination IP are identified, the source sends the request and destination sends its response to the source.

Intruder Logging

When the IDS detect an intrusion attempt on a port, it enters a record of this event in the Intrusion Log. The Intrusion Log lists the port number, the IP address of the intruding device namely the source and destination IP,

services of ports, status of packets and the system time and date. We can create several other Log Reports which can be saved and used for future analysis

Types of Protocols Filtering

Wireshark is the tool analyzed the protocol traffic going out and coming into the machine. The filtering language used by Wireshark is display filters that permit to focus on the packets that are interested and hiding the rest of the packets. This kind of filters agree to select packets by giving the protocol name in the filter tab, presence and values of a field, a comparison between fields etc. it is easy to select packets based on protocol type, simply type the protocol in which you are interested in the filter tab of the Wire shark window and then will initiate the filter.

Data Loss from IP

IP-guard Data Loss Prevention solution enables to protect the sensitive data in the organization that helps organizations effectively manage the threats and risks to organizations information, and takes safety measure on the value of an organization. It conveys important and matchless features to defend against data security threat also prevent accidental and mischievous data leakage of an organization. It successfully controls and enables to get a handle on the critical information by preventing costly loss and intellectual property will be safeguarded.

This filters the protocols and ports of protocols and sends a real time messages to users if any illegal actions are committed. The output lists the report of the infected protocols with source and destination IP address and port number. Moreover monitors the data usage, computer activity of each users.

IV. OUTPUT

Output for the system is shown below for Load capture in fig.4.1, then the filtering of the protocols as in figure 4.2 and then filtering the port of protocols is shown in figure 4.3 and finally the output in figure 4.4.

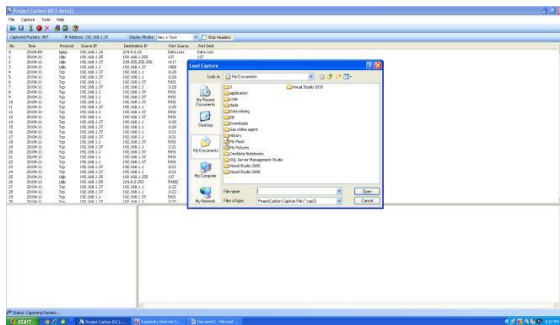


Fig. 4.1. Load Capture

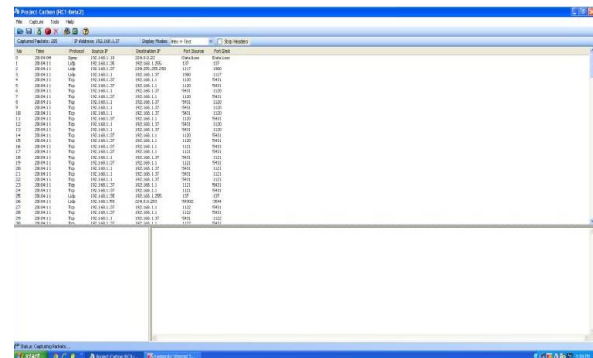


Fig 4.4. Output

V. CONCLUSION

This paper introduced a novel approach to host-based intrusion detection system using system call patterns. This method allow the intruders or malicious activity to be identified in a better for a host system. This method used different methods such as load capture, network Port Scanning, packet Sniffing, protocol filtering is done, intruder logging is identified and data loss from IP of packets is identified. The results shows that average detection accuracy is achieved. The further study can be done by improving the performance and adding a third party system.

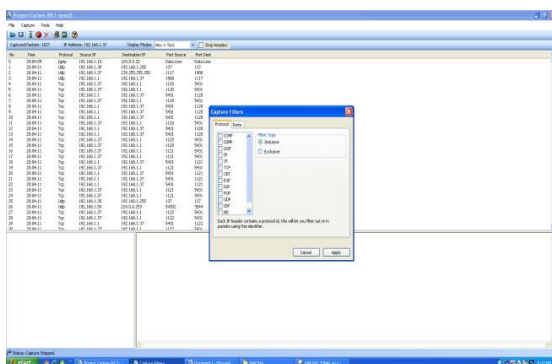


Fig. 4.2. Filter the Protocols

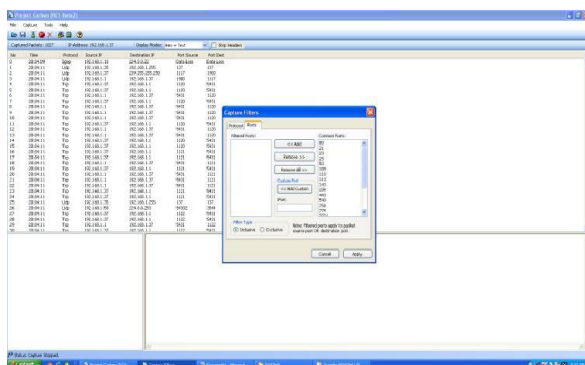


Fig. 4.3. Filter the ports of protocols

VI. REFERENCES

- [1] Fang-Yie Leu, Kun-Lin Tsai, Member, IEEE, Yi-Ting Hsiao, and Chao-Tung Yang, An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques IEEE SYSTEMS JOURNAL, Vol.11, Issue: 2, Pages: 427 – 438.2017
- [2] Sundaram Aurobindo. An Introduction to Intrusion Detection. <http://www.acm.org/crossroads/xrds2-4/intrus.html>
- [3] Przemyslaw kazienko, Piotr Dorosz. Intrusion Detection Systems (IDS)–Part 2- Classification, Methods and Techniques. IT FAQ 2003; 1(4):17-22.
- [4] Minnesota Intrusion Detection System (MINDS). [Online] [Accessed 2006]. Available from URL <http://www.cs.umn.edu/research/minds>
- [5] Vigna, Kemmerer. NetSTAT: A Network-Based Intrusion Detection System. Computer Security 1999; 7(1): 37-71

- [6] Wu Yang, Bin-Xing Fang, Bo Liu, Hong-Li Zhang. Intrusion Detection System for High Speed Network. *Computer Communications* 2004 August 15; 27(13): 1288-1294.
- [7] Thomas H. Ptacek. Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection. Secure Network Inc.; October 2002.
- [8] Dennis Hollingsworth. Towards threat, attack, and vulnerability taxonomies. 44th IFIP WG 10.4 Meeting. Monterey, CA, USA; June 25- 29, 2003
- [9] Faizal Abdollah, Mohd Mas'ud, Shahrin Sahib, Asrul Yaacob, Robiah Yusof, Siti Selamat, Host Based Detection Approach Using Time Based Module for Fast Attack Detection Behavior, *Lecture Notes in Electrical Engineering*, Volume 157, 2012, pp 163-171
- [10] Rung-Ching Chen, Kai-Fan Cheng, and Chia-Fen Hsieh. Using Rough Set and Support Vector Machine for Network Intrusion Detection. *International Journal of Network Security & Its Applications (IJNSA)*, Vol 1, No 1, April 2009.
- [11] Kristopher Kendall. A Database of Computer Attacks for the Evaluation Of Intrusion Detection Systems. Master thesis, MASSACHUSETTS INSTITUTE OF TECHNOLOGY; 1999.
- [12] Rebecca Cao. RSWATCHER: A PORT SCANNING DETECTOR. Master thesis, Florida State University; 1999
- [13] Jaeyeon Jung, Vern Paxson, Arthur W. Berger, and Hari Balakrishnan. Fast Port scan Detection Using Sequential Hypothesis Testing. *IEEE Symposium on Security and Privacy* 2004. Oakland, CA; May 2004.
- [14] J.Choi,C.Choi,B.Ko,D.Choi,andP.Kim,“DetectingwebbasedDDoS attack using MapReduce operations in cloud computing environment,” *J. Internet Serv. Inf. Security*, vol. 3, no. 3/4, pp. 28–37, Nov. 2013.
- [15] 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.
- [16] Z. A. Baig, “Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks,” *Comput. Commun.*, vol. 34, no. 3, pp. 468–484, Mar. 2011.
- [17] H. S. Kang and S. R. Kim, “A new logging-based IP traceback approach using data mining techniques,” *J. Internet Serv. Inf. Security*, vol. 3, no. 3/4, pp. 72–80, Nov. 2013.
- [18] K. 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.
- [19] 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.
- [20] 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.AmbientComput.Intell.*,vol.3,no.2,pp.64–76, Apr. 2011.
- [21] 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.

