Anomaly Based Intrusion Detection And Prevention System

Vasima Khan
Computer Science & Engg.
All Saint Inst. Of Tech
Bhopal, M.P, India

ABSTRACT

Automatic discovery of intrusions into computer systems is central issue to stop unauthorized activity. Implementing intrusion detection systems on networks and hosts requires a broad perceptive of computer security. Most of the IDS and IPS are based on two fundamental mechanisms; Misuse detection or signature based detection. It defines a set of "unacceptable" behaviors and raise alerts when system behavior matches this set. The common attempts can be easily detected by Signature based IDS and the defense can be provided against such type of attack by either matching string pattern or signature. But in the prevailing scenario where there are new intrusions/ attempts reported almost every day, the existing signature-based detection proves futile. Many IDPS have been proposed but all of them lacks on some points and are not accurate as desired, they use to signature to detect the attacks and these signature based methods are fast and simple but it fails to detect unknown attacks. To fill the gap we require an efficient fast and real time Intrusion Detection and Prevention system to provide defense against intrusions/attacks. This paper presents Anomaly-based intrusion detection and prevention system which makes it more efficient and dynamic as it is able to detect novel (unknown) attack with without generating low positive false rate.

Keywords

Anomaly, Anomaly Detection, Intrusion, IDS, IPS, IDPS.

1. INTRODUCTION

The increasing popularity of Internet is exposed to an increasing number of security threats [1]. Implementing intrusion detection systems on networks and hosts requires a broad perceptive of computer security. The complexity of information technology infrastructures is growing rapidly beyond any one person's ability to understand them, let alone administer them in a way that is operationally secure. The term Network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

According to the report of CERT [2], the quantity of attacks, their complexity, and extent of damage, caused by criminal attacks in the internet rapidly increase every year [3]. The development of the fast speed internet services created an environment in which millions of users across the globe (World Wide Web) are all connected to each other. Furthermore, the cost of accessing the network is so cheap, allows criminal (Hackers, Crackers and Thieves) to target to your system, regardless of their physical location. Personal computers are also cheap. Attackers can easily setup computers with different operating systems and they search for vulnerable system for launch an attack. In addition, the international and distributed nature of Internet makes it very difficult to regulate and control attacks against computer system [4].

Automatic discovery of intrusions into computer systems is central issue to stop unauthorized activity. While firewalls are is key point to restrict access to computers inside a sheltered network, but their defense is not perfect nor do they provide protection against malicious activities. Manual intrusion detection is painstaking through supervising of access logs or monitoring of users activities. As well as they have much delay (a long reaction time).

Most of the IDS and IPS are based on two fundamental mechanisms; Misuse detection or signature based detection. It defines a set of "unacceptable" behaviors and raise alerts when system behavior matches this set. Such systems are simple to create and efficient to operate, but are only effective against known types of attack that has fixed pattern. SNORT [5] is well known IDS based on misuse concept. Moreover, it is difficult to maintain an up-to-date knowledge base of acceptable behaviors and thus this mechanism is ineffective against unknown or unusual attack patters. Anomaly detection mechanisms, on the other hand, create a profile of typical behavior for a user and raise an alert when a user attempts an activity that does not fit his/her profile. This approach tends to be highly complete in that it can detect a previously unknown attack pattern, but it requires significant effort to develop algorithms that can create accurate user profiles.

The common attempts can be easily detected by Signature based IDS and the defense can be provided against such type of attack by either matching string pattern or signature. But in the prevailing scenario where there are new intrusions/ attempts reported almost every day, the existing signature-based detection proves futile. Many IDPS have been proposed but all of them lacks on some points and are not accurate as desired, they use to signature to detect the attacks and these signature based methods are fast and simple but it fails to detect unknown attacks. To fill the gap we require an efficient fast and real time Intrusion Detection and Prevention system to provide defense against intrusions/attacks. In this paper we presents Anomaly-based intrusion detection and prevention system which makes it more efficient and dynamic to detect and prevent suspicious activity in the network.

Rest of the paper is organized as follow, section 2 give brief details about the types of anomalies and their methods of detection used in IDPS, section 3 insights the previous work on anomaly based intrusion detection, section 4 explains our proposed approach, section 5 outlines the conclusion.

2. Types of Anomalies

Generally there are two types of anomalous behavior have been studied – Host and Network based Anomaly.

a. **Host Based Anomalies–** Host based anomalies calculation dealt with operating system call traces. The intrusions are in the form of anomalous subsequences (collective anomalies) of the traces. The anomalous subsequences translate to malicious programs, unauthorized behavior and policy abuse. The data is sequential in nature and the alphabet consists of individual system calls like open, close, create etc.

b. **Network Based Anomalies–** It deals with the network traffic. Usually capturing through different types of tools like tcpdump, wireshark, Nmap and Netflow or ourmon.

2.1 Network Protocols Anomaly

Author's of [7] has addressed many anomalies that cause serious damage in network as well as system. Some of them are following –

2.1.1 UDP flood

A UDP flood attack is a category of DoS attack commenced by sending a large number of UDP packets to random ports on a remote host. As a consequence, the remote system will check for the application listening on this port. After seeing that no application listens on the port, the host will respond with an ICMP "Destination Unreachable" packet. Thus, for a large number of UDP packets, the victimized system will be forced into sending many ICMP packets, eventually leading it to unreachable by other clients. If enough UDP packets are delivered to the ports on the victim, the system will go down.

In order to detect UDP flooding attack, we need to work with the traffic (flow) size and number of packet's (packet count) in the incoming traffic.

For measuring this we have define two metrics (indicator) for UDP flood attack:

a. TotalBytes: total volume of flows in bytes.

b. TotalPackets: total packets in incoming traffic.

2.1.2 ICMP Flood

Also known as ping flood is simplest types of attack in which attacker launches large number of ICMP Echo Request (ping) packets with different sizes to the host. ICMP flooding is a successor of the Ping-of-Death (PoD) attack. PoD tries to send an extra-large ping packet to the destination with the hope to bring down the destination system due to the system's lack of ability to handle huge ping packets. Ping flood brings the attack to a new level by simply flood the victim with huge ping traffic. The attacker hopes that the victim will too busy responding to the ICMP Echo Reply packets, thus consuming outgoing bandwidth as well as incoming server bandwidth.

Analogous to UDP flood, ICMP attack also generate a massive amount of data towards the destination. Thus same metrics TotalBytes and TotalPackets is enough to measure such types of attack. Certainly, using the same method creates ambiguity to distinguish ICMP from UDP flood. To resolve this issue we used another metric for monitoring the total number of ICMP or UDP traffic going into the network.

2.1.3 TCP SYN Attack

This method takes advantage of a flaw in how many hosts implement the TCP three-way handshake. When host B receives the SYN request from host A, it must keep track of the partially opened connections in a "listening queue" for at least n seconds (e.g.: 75 seconds). Many host implementations can only keep track of a very limited number of connections. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never reply to the sent back SYN and ACK. By doing so, the destination host's listening queue will be quickly filled up, and it will stop accepting new connections. Figure 1 show the typical scenario of TCP SYN attack.

The effect of this attack on network traffic is pretty different from the above two attacks. It has values (only SYN and ACK bit). Thus we can't rely on TotalBytes or TotalPackets determine the effect of this attack; for this we need to define a new metric:

- DestSocket: number of flows with similar volume (e.g. SYN) to the same destination socket.

In other words, the detection of TCP/SYN has been carrying out with the help of following metrics-

a. The number of TCP flows per minute

b. The average number of packets in each TCP flow per minute

c. The average number of bytes in each TCP flow per minute

d. The number of unique IP addresses seen per minute.

2.1.4 Port scan

A portscan attack is carried out with a port scanner, a piece of software to search a network host for open ports. A port scanner is often used by network administrators to check the security of their networks, and it also used by hackers to compromise the system security. Many exploits rely upon port scans, for example to find open ports and send large quantities of data in an attempt to trigger a condition known as buffer overflow, or to send some specific port data packets with malicious purposes …

A portscan operation will result a big number of packets sent from a remote host to a destination on the network, but with different destination ports. Flows in portscan are small flows with the size of only several bytes and packet count of 2 or 3. This malicious activity cannot be detected with the three metrics we already have. In order to gather together all flows in a portscan attack for the detection purpose, we need to define another metric that has the capability to aggregate all these flows:

- DPort: number of flows that have a similar volume, same source and destination address, but to different ports.

2.1.5 DNS Reflector Attack

In this type of attack, the attacker sends a flood of DNS requests with a spoofed IP address (the one of the victim) to one or more DNS servers which results in a flood of DNS responses sent to the victim. If enough traffic is generated this can lead to a denial of service.

The detection of DNS reflector attacks is either done by checking for a very high rate of DNS request flows from the same (spoofed) IP address to a DNS server inside the network or by filtering hosts which receive an unusually high number of UDP flows with source port 53, which corresponds to the port from which a DNS server is sending his responses. False positives will be occur if legitimate host (user) sending a large number of DNS requests in a short duration of time.

Most commonly used Ports are 21, 25, 53, 110, 135, 139 and 445 these are the well known port and offer important services for the network, for example port 110 and 25 is use for email in which plays a vital role in today's business communication [8], while port 53 is important because it is the reference center for mapping IP address to DNS, if it is attacked the whole network will be in catastrophic [9]. Moreover these ports are the most popular target for attack activity especially for worm virus and port scanning.

3. Related work

In this section we insight the previous works had been done. The section has logical divided into two section detection approach and advantages of anomaly (Novelty) approach and second the agent based approach.

According to [10], misuse relies on a set of attack metaphors, also called attack signatures [11]. These descriptions are matched to the stream of audit data, at-tempting to verify that the definite signature is occurring. Misuse based IDS are fast as compared to anomaly based ids, but they are incapable of identifying new (unknown) types of attacks or variations of known attacks [12]. While Anomaly detection checks the some deviations from normal patterns [13]. Authors of [13] divide anomaly detection into two categories, static and dynamic. A static anomaly detector assumed that there is a part of the system being monitored that does not change. It concentrates on the software (software code) portion of a system and assuming that the hardware need not be checked. For example Bootstrap file of an OS, never be changed, if changed (or deviation in file) that has the signed of anomaly. The center of attention in static anomaly detector is integrity checking [14][15], while Dynamic anomaly detection operates on audit record or on monitored network traffic data.

Advantage of Anomaly detection over misuse is that, it can to detect unknown attacks and privileges abuse of legitimate users as well [16].Authors of [17] talked about the application level anomalies most often used by today's attackers to target the vulnerabilities of specific systems or applications as mentioned in [18].Another advantage of anomaly detection is to defense against Zero-day attack [19].

4. Proposed System and Architecture

Our proposed solution is to automatic discovery of intrusions into computer systems is central issue to stop unauthorized activity. Implementing intrusion detection systems on networks and hosts requires a broad perceptive of computer security. Most of the IDS and IPS are based on two fundamental mechanisms; Misuse detection or signature based detection. It defines a set of "unacceptable" behaviors and raise alerts when system behavior matches this set. The common attempts can be easily detected by Signature based IDS and the defense can be provided against such type of attack by either matching string pattern or signature. But in the prevailing scenario where there are new intrusions/ attempts reported almost every day, the existing signature-based detection proves futile. Many IDPS have been proposed but all of them lacks on some points and are not accurate as desired, they use to signature to detect the attacks and these signature based methods are fast and simple but it fails to detect unknown attacks. To fill the gap we require an efficient fast and real time Intrusion Detection and Prevention system to provide defense against intrusions/attacks.

Our proposed work is based on two articles [20] and [21], the reason behind choosing these two is following-

1. The author of [20] presents a new approach "BANDIT (Behavioral Anomaly Detection for Insider Threat)" to detect illegitimate insider attacker or threat using the concept of behavioral detection also term as anomaly detection. Author uses three metrics to detect insider threat- Motive, Means, and Opportunity.

We want to expand and apply authors idea to detect outside attack came from network traffic due to insider attack has less probability of exploit rather than outside.

But the idea of three metrics MMO will be applied to the outside threat detection.

2. Author of [21] has integrated the idea of agents in anomaly detection for faster reaction against intruder activity. The idea of this article, our proposed work utilized is anomaly detection technique and real time network is interesting one. Authors future will be considered in our proposed work i.e. prevention methods to ensure zero attacks on the system.

Briefly summarized the proposed system is to develop an IDPS based on anomaly approach to detect novel attacks [21], using MMO concept given by [20].

5. Conclusion

This article outlines and surveys about anomaly based intrusion detection system and that is around, as well as highlights the deficiencies. In this paper we have discuss the types of anomalies and anomalies and theoretical methods to detect them. To overcome theses deficiency of existing methods of security a new Anomaly based IDPS approach has been proposed and provides a cost effective solutions than any hardware and software based IDPS. Proposed system will provides a solution that has low false rate and high detection capability.

6. REFERENCES

[1] P. Garcı´a-Teodoro, J. Dı´az-Verdejo, G. Macia´-Ferna´ndez and E. Va´zquez "Anomaly-based network intrusion detection: Techniques, systems and challenges", computer and security, science direct, 2009.

[2] CERT, http://www.cert.org/

[3] Igor Kotenko and Mihail stepashkin “Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages Computer Network Life Cycle” Computer Network Security ,Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2005, St. Petersburg, Russia, September 24-28, 2005.

[4] Earl Carter and Jonathan Hogue "Intrusion Prevention Fundamentals", CICCO PRESS, 2006.

[5] Snort; Available from: http://www.snort.org.

[6] Ourmon anomaly detection tool, http://sourceforge.net/projects/ourmon/

[7] Huy Anh Nguyen, Tam Van Nguyen, Dong Il Kim AND Deokjai Choi “Network Traffic Anomalies Detection and Identification with Flow Monitoring”, IEEE, 2008.

[8] Mark Ciampa, “Security + Guide to Network Security Fundamentals Second Edition”, Canada. Thomson Course Technology, 2003.

[9] Wang, L., Zhao, X., Pei, D., Bush, R., Massey, D. & Zhang, L “Protecting BGP Routes to Top-Level DNS Servers” ,In Proceeding of IEEE Transaction on Parallel and Distributed Systems, Vol.14, No.9, 2003.

[10] Farah Barika KTATA, Nabil EL KADHI and Khaled GHEDIRA “Distributed agent architecture for intrusion detection based on new metrics”, IEEE, Third International Conference on Network and System Security, 2009.

[11] S.Kumar and E.Spafford,“A Software Architecture to Support Misuse Intrusion Detection”, Department of Computer Sciences, Purdue University, 1995.

[12] Paulo M. Mafra, Vinicius Moll, Joni da Silva Fraga and Altair Olivo Santin “Octopus-IIDS: An Anomaly Based Intelligent Intrusion Detection System”, IEEE, 2010.

[13] V´aclav Sn´aˇsel, Jan Platoˇs, Pavel Kr¨omer and Ajith Abraham” Matrix Factorization Ap-proach for Feature Deduction and Design of Intrusion Detection Systems”, The Fourth International Conference on Information Assurance and Security, IEEE, 2008.

[14] S. Forrest, A.S. Perelson, L. Allen, R. and Cherukuri, ”Self-Nonself Discrimination in a Computer”, Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy,Los Alamitos, CA: IEEE Computer Society Press (1994)

[15] Gene H. Kim, Eugene H. Spafford,”Experiences with Tripwire:Using Integrity Checkers for Intrusion Detection”, http://citeseer.ist.psu.edu/kim95experiences.html (1995).

[16] Dalila Boughaci, Habiba drias, Ahmed Bendib, Youcef Bouznit and Belaid Benhamou “A Distributed Intrusion Detection Framework based on Autonomous and Mobile Agents” , Proceedings of the International Conference on Dependability of Computer Systems (DEPCOS-RELCOMEX’06) , IEEE,2006.

[17] Like Zhang, Gregory B. White” Anomaly Detection for Application Level Network Attacks Using Payload Keywords”, Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007).

[18] H. J. Wang, C. Guo, D. R. Simon, and A. Zugenmaier, “Shield: A Vulnerability-Driven Network Filters for Preventing Known Vulnerability Exploits”, ACM SIGCOMM’04, Port-land, USA, August, 2004.

[19] Levy, E., “Approaching Zero”, IEEE Security & Privacy Magazine, vol. 2, issue 4, pp. 65-66, 2004.

[20] Vincent H. Berk, George Cybenko, Ian Gregorio-de Souza, and John P. Murphy “Managing Malicious Insider Risk through BANDIT”, IEEE, 45th Hawaii International Conference on System Sciences, 2012.

[21] Rathore, J.S. , Saurav, P. and Verma, B. “AgentOuro: A Novelty Based Intrusion Detection and Prevention System”, IEEE, Fourth International Conference on Computational Intelligence and Communication Networks (CICN), 2012.