ISSN 2320-9984
Volume 4 Issue 3 | September 2016 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

Critical Study and Survey of IDS form Malicious Activities using SNORT

Javed Akhtar Khan
Assistant Professor
Department of Computer Science & Engineering
Takshshila Institute of Engineering & Technology,
Jabalpur (M.P.) [INDIA]
Email:er.javedkhan@gmail.com

***Abstract*—*Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from the malicious or abnormal activities like virus, worms, backdoor attacks etc. e-Government infrastructure network requires a strong security to guarantee the confidentiality of national data and the availability of government services. Most current Intrusion Detection System are signature based or machine learning based methods. Designing a high speed network intrusion detection system has attracted much attention recently due to increasing of network traffic. To examine performance and detecting intrusions we introducing SNORT for high speed and packet reassembly. In this paper I am collect the information about the Intrusion Detection System(IDS) which is technically provide the security of networks from various types of intrusion activities. A part from that in this paper I am also compare the various existing solutions regarding.*

***Keywords:*—*Intrusion, IDS (Intrusion Detection system), Type of IDS, Protocols attacks, Analysis, SNORT.*

1. INTRODUCTION

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intrusion detection systems fall into two basic categories: signature-based intrusion detection systems and anomaly detection systems. Intruders have signatures, like computer viruses, that can be detected using software. You try to find data packets that contain any known intrusion related signatures[2] or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts. Anomaly based intrusion detection usually depends on packet anomalies present in protocol header parts. In some cases these methods produce better results compared to signature-based IDS. Usually an intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it. Snort is primarily a rule-based IDS, however input plug -ins are present to detect anomalies in protocol headers.[3]

SNORT rules stored in text files that can be modified by a text editor. Rules are grouped in categories. Rules belonging to each category are stored in separate files. These files are then included in a main configuration file called snort.conf. Snort reads these rules at the start-up time and builds internal data structures or chains to apply these rules to captured data. Finding signatures and using them in rules is a tricky job, since the more rules you use, the more processing power is required to process captured data in real time. It is important to implement as many signatures as you can using

as few rules as possible. Snort comes with a rich set of pre-defined rules to detect intrusion activity and you are free to add your own rules at will. You can also remove some of the built-in rules to avoid false alarms.[1]

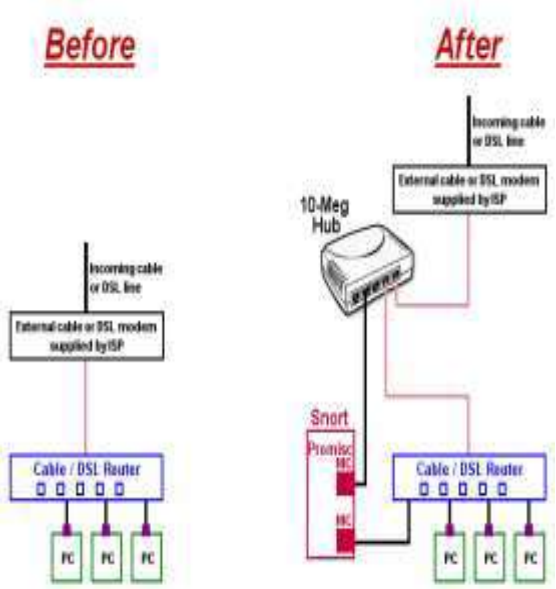

Figure 1: Intrusion Defection System with SNORT

2. INTRUSION

Intrusion is an active chronological sequence of concomitant events that intentionally try to cause damage, making system unusable, accessing illegitimate information, or act upon such information. This definition refers to both successful and unsuccessful attempts. Free dictionary define, the act or an instance of intruding; an unwelcome visit, interjection, etc. an intrusion on one's privacy[2].

2.1 Intruder

Intruder is, one who intrudes; one who thrusts himself in, or enters without right, or without leave or welcome; a trespasser, person, who enters a private residence or place of business with the intention to perform a criminal act. Another definition given by hitach-id.com, an intruder is a person who attempts to gain illegitimate access to a system, to spoil that system, or to disturb data on that system. in brief, person/program attempts to breach security by interfering with system availability, data integrity or data confidentiality in context of computer, the more refine definition of intruder by heady, intrusion as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". an intruder is a hacker attempting to break into or abuse the resources of a computer system. intruders come from outside an organizations network and may attempt to go around firewalls to attack machines on the internal network.

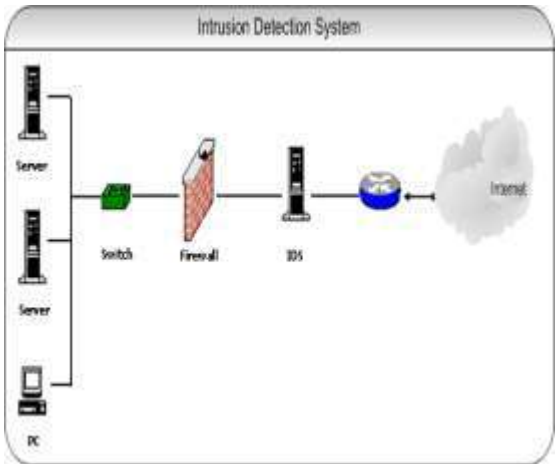

Figure 2: Intrusion Defection System in SERVER

2.2Firewall

The conventional method of network security is Firewall. Firewall was most of what an administrator needed to protect a network from attack. It was easy to establish where your network ended and the Internet began. In other words, Firewalls are usually the first component of any outside defense. Firewalls works as a barrier of security among networks of different levels of confidence or security, utilizing network level access control politics. The major functional requirement of a firewall is to protect a private (internal) network from unauthorized external access. A firewall is governed by a set of rules or filters defined by the administrator [6]. A typical firewall will permit or reject incoming packets based on the port that the TCP or UDP request is arriving on. It is designed to refuse visibly suspicious traffic but is also designed to allow some traffic through. This behavior has a major disadvantage, as any packet is allowable through an open port in the firewall. Figure 1 shows the, how firewall is work. Many

exploits take advantage of weaknesses in the very protocols that are allowed through the perimeter firewalls and once the web server has been compromised, this can often be used as a springboard to launch additional attacks on other internal servers. Once a "rootkit" or "back door" has been installed on a server, the hacker has unfettered access to that server at any point in the future. Differentiate firewall, NIDS and NIPS, Firewalls filter undesirable traffic based on RULES (policies) to check packet headers. NIDS passively watch traffic on a network and perform more advanced checks, including inspection of protocols and its content, to determine indications of possible attacks. Network Intrusion Prevention Systems (NIPS) is the combination of NIDS and firewalls, performing in-depth inspection and using this information to block possible attacks.

3. DIFFERENT PROTOCOL ATTACKS

3.1 ICMP

ICMP is used by the IP layer to send one -way informational messages to a host[4]. There is no authentication in ICMP which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets. There are a few types of attacks that are associated with ICMP shown as follows:

ICMP DOS Attack: Attacker could use either the ICMP "Time exceeded" or "Destination unreachable" messages. Both of these ICMP messages can cause a host to immediately drop a connection. An attacker can make use of this by simply forging one of these ICMP messages, and sending it to one or both of the communicating hosts. Their connection will then be broken. The ICMP "Redirect" message is commonly used by gateways when a host has mistakenly assumed the destination is not on the local network. If an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host.

Ping of death: An attacker sends an ICMP echo request packet that's larger than the maximum IP packet size. Since the received ICMP echo request packet is larger than the normal IP packet size, it's fragmented. The target can't reassemble the packets, so the OS crashes or reboots.

ICMP nuke ***attack:*** Nukes send a packet of information that the target OS can't handle, which causes the system to crash

ICMP Ping flood attack: A broadcast storm of pings overwhelms the target system so it can't respond to legitimate traffic

3.2 TCP

If one application wants to communicate with another via TCP, it sends a communication request. This request must be sent to an exact address. After a handshake between the two applications, TCP will set up a full-duplex communication between the two applications. The full-duplex communication will occupy the communication line between the two computers until it is closed by one of the two applications. There are security problem in TCP, some attack are describe below

TCP SYN or TCP ACK Flood Attack -

This attack is very common. The purpose of this attack is to deny service. The attack begins as a normal TCP connection: the client and the server exchange information in TCP packets. The TCP client continues to send ACK packets to the server, these ACK packets tells the server that a connection is requested. The server thus responds to the client with a ACK packet, the client is supposed to respond with another packet accepting the connection to establish the session. In this attack the clients continually send and receive the ACK packets but it does not open the session. The server holds these sessions open, awaiting the final packet in the sequence. This cause the server to fill up the available connections and denies any requesting clients access.

TCP Sequence Number Attack - This is when the attacker takes control of one end of a

TCP session. The goal of this attack is to kick the attacked end of the network for the duration of the session. Only then will the attack be successful. Each time a TCP message is sent the client or the server generates a sequence number. The attacker intercepts and then responds with a sequence number similar to the one used in the original session. This attack can then hijack or disrupt a session. If a valid sequence number is guessed the attacker can place himself between the client and the server. The attacker gains the connection and the data from the legitimate system. The only defense of such an attack is to know that it is occurring.

TCP Hijacking - This is also called active sniffing, it involves the attacker gaining access to a host in the network and logically disconnecting it from the network. The attacker then inserts another machine with the same IP address. This happens quickly and gives the attacker access to the session and to all the information on the original system.

TCP reset attack: This is also known as "forged TCP resets", "spoofed TCP reset packets" or "TCP reset attacks". These terms refer to a method of tampering with Internet communications

3.3 ARP

ARP maps any network level address (such as IP Address to its corresponding data link address. Some of the ARP attacks are describe below

ARP flooding: Processing ARP packets consumes system resources. Generally, the size of an ARP table is restricted to guarantee sufficient system memory and searching efficiency. An attacker may send a large number of forged ARP packets with various sender IP addresses to cause an overflow of the ARP table on the victim. Then the victim cannot add valid ARP entries and thus fails to communicate. An attacker may also send a large number of packets with irresolvable destination IP addresses. When the victim keeps trying to resolve the destination IP addresses to forward packets, its CPU will be exhausted.

User spoofing : An attacker may send a forged ARP packet containing a false IP-to-MAC address binding to a gateway or a host. The forged ARP packet sent from Host A deceives the gateway into adding a false IP-to-MAC address binding of Host B. After that, normal communications between the gateway and Host B are interrupting.

In DoS attack target hosts are denied from communicating with each other, or with the Internet. This is done simply by corrupting their ARP caches with fake entries including nonexistent MAC addresses, or by disabling the IP packet routing option in the malicious host, so that received redirected traffic will not be forwarded to its real destination.

Connection Hijacking & Interception Packet interception is the act in which client can be victimized into getting their connection manipulated in a way that it is possible to take complete control aver

3.4 UDP

UDP uses a simple transmission model without implicit handshaking dialogues for providing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service and datagram may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. [3].some UDP attacks are describe below

UDP flood attack: Similar to ICMP flood attack, UDP flood attack sends a large number of UDP messages to the target in a short time, so that the target gets too busy to transmit the normal network data packets.

Fraggle - A fraggle attack is similar to a smurfing *attack* with the exception that the User Datagram Protocol (UDP) is used instead of using ICMP.

Teardrop - A teardrop type of DoS attack The attack works by sending messages fragmented into multiple UDP packages. Ordinarily the operating system is able to reassemble the packets into a complete message by referencing data in each UDB packet. The teardrop attack works by corrupting the offset data in the UDP packets making it impossible for the system to rebuild the original packets. On systems that are unable to handle this corruption a crash is the most likely outcome of a teardrop attack.

4. ANALYSIS

A. Traffic Data

We used two-way traffic traces provided by the Umass Trace Repository. The traces were measured at the Umass Internet gateway router. The UMass campus is connected to the Internet through Verio, a commercial ISP, and Internet. Both of these connections are Gigabit Ethernet links. In particular, we used the "Gateway Link 3 Trace" that was measured every morning from 9:30 to 10:30 from July 16, 2004 to July 22, 2004. All of these data are manually labeled, but we did not use the labels with the proposed method.

B. Effectiveness of the Time-Periodical Packet Sampling

First, we confirmed our conjecture that the time-periodically sampled traffic would contain normal packets with higher ratio than the original traffic before sampling. For comparison, the mixing ratio of the anomalous packets to the original traffic and randomly sampled traffic of which the sampling rate per packet is *p*. the mixing ratio of anomaly packets to the time-periodically sampled traffic much smaller than that to the original traffic before sampling, whereas the mixing ratio of anomaly packets to the randomly sampled traffic is almost identical to that to the original traffic before sampling. This result indicates that the time-periodical packet sampling is useful for extracting normal packets from the unlabeled original traffic which may include anomalous traffic. However, we have to remember that the time-periodically sampled traffic might be biased towards a specific aspect of normal traffic. Therefore, we investigated the performance of baseline distributions that were trained with time-periodically sampled traffic data. e numbers of normal behaviors incorrectly identified as anomalies (FP: False Positive) and missed anomalies (FN: False Negative) regarding TCP SYN packets for the baseline distributions trained with different types of traffic data, i.e., normal traffic data, original traffic data before sampling, 10 sets of time-periodically sampled traffic data, and 10 sets of randomly sampled traffic data

C. Effectiveness of Ensemble Anomaly Detection

This indicates that the unsupervised ensemble method can avoid the worst performance of the individual baseline distributions for the time-periodically sampled traffic. In addition, the resulting performance for the time-periodically sampled traffic is nearly identical to when the baseline distribution is trained by using the normal traffic data. Note that the unsupervised ensemble anomaly detection is effective even when the baseline distribution is trained by using randomly sampled traffic data. However, the resulting performance for the randomly sampled traffic is nearly identical to when the baseline distribution is trained with the original traffic data. Therefore, we still cannot provide any justification for using randomly sampled traffic data to train the baseline distributions.

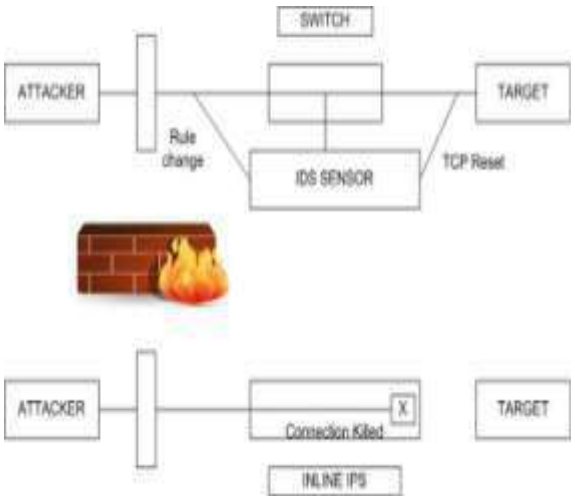

Figure 3: Ensemble Anomaly Detection Model

5. TYPES OF IDS

IDS has usually divides into two types

1.Technology based

According to technology, IDS has divided into two types Host IDS and Network IDS[7].

Host based IDS (HIDS)

HIDSs are live in on a single system or host and filter traffic or events based on a known pattern (signature) record for that specific operating system. The well known HIDSs are Norton Internet Security and Cisco Security Agent (CSA). Warning: Many worms and Trojans can turn off an HIDS[5].

Network based IDS (NIDS)

Network-based IDSs detect intrusions by examining packets that travel on network links. In NIDS the individual packets passing (travel) through the network are analyzed. Mostly NIDSs consist of a sensors (or software agents) or hosts are spread in a network for monitoring of network traffic, performing local analysis of that traffic and report back to central management console or platform (in case of mobile agent). NIDSs examine network traffic across the network in much greater detail than a firewall. Therefore, NIDSs can detect malicious packets unseen by a firewall[4]l. NIDSs also watch for attacks that originate from within a network. That is why, they are complement for firewalls.

In brief, Host-based IDSs detect intrusions by examining file system modifications, application execution logs, system calls, and so on; while network-based IDSs detect intrusions by monitoring packets that pass through on network links.

Compared to network-based IDSs, host-based IDSs have access to more refined resources, such as file system and system calls. On the other hand, network-based IDSs are able to detect intrusions at an earlier stage and they have global views of the networks. As a result, these two systems can complement each other to provide high quality detection. DoS is the most popular attack to target the host system (or network) or. It prevents users (legitimate) to use services by- consumption of resources or destruction or modification of valuable information or media (physical), Attackers used DoS to prevent service of legitimate users. In a network, Exhaustion of network bandwidth and alteration of nodes are most dangerous attack, immune to any type of attack is the essential property of network device for strengthen the protection.

Pattern matching based NIDS used following types of attribute for enhancing detection process- immunity to algorithmic complexity attack, to match multiple strings at a time, fast updating of signature on database, high throughput and minimum delay.

2. Method of Detection

Two well known methods are used to detect and prevent the attack, Misuse and Anomaly detection or hybrid of both. Misuse detection also called signature or rule based detection method.

Misuse or Signature based IDS - Misuse detection defines a set of "unacceptable" behaviors and alerts when system activities match this set [9]Misuse detection looks for a specific attack that has already been recognized (Vulnerabilities and known attack patterns). Misuse detection recognized those types of attack which have known but new (unknown) pattern and characteristic of intrusion might not be identified using this technique

Anomaly Detection based IDS - Anomaly detection, works better to detect unknown attacks [8]. Anomaly detection believes that an intrusion will always reflect some deviations from normal patterns [6]. In Anomaly detector modeled a normal profile, if anything (network or behavior) deviated from normal treated as a anomalous behavior (or action). [8] Attacks like snooping network or abusing vulnerabilities in protocol's can be detected by analyzing header or traffic. But in case of the abusing by program vulnerabilities such as malcodes (worms or viruses) can't be handled by analyzing header information. Such

types of attacks may be be[8]tter detected by inspecting of packet payload (data field).

5. CONCLUSION AND FUTURE WORK

The profiling, pattern matching was considered a performance bottleneck because the entire payloads in the connections, particularly the long ones, are scanned, but the problem can be alleviated by precisely specifying the locations of the signatures in the detection rules, besides hardware solutions. Moreover, the generic analysis with the policy scripts and stream processing including connection tracking and packet reassembly are also essential components that deserve serious considerations and studies for their acceleration. In future our first task is to work on anomaly based IDS system that can protect against DOS and SYN flood attack as well as preventing the Zero day Attack. And final result will be compared as per author's parameters (guideline) mentioned in the article [1] such as speed, performance (response) and the CPU utilization during attack.

REFERENCES:

[1] Po-Ching Lin and Jia-Hau Lee "Re-examining the performance bottleneck in a NIDS with detailed profiling", Elsevier Science Direct, Journal of Network and Computer Applications 36 (2013) 768–780, 2013.

[2] Intrusion Detection and Correlation: Challenges and Solutions By Christopher Kruegel, Fredrik Valeur, Giovanni Vigna.

[3] How To Guide-Implementing a Network Based Intrusion Detection System By Brian Laing.

[4] Subramanian Neelakantan, Shrisha Rao, "A Threat-Aware Signature Based Intrusion-Detection Approach for Obtaining Network-Specific Useful Alarms", The Third International Conference on Internet Monitoring and Protection, 2008 IEEE DOI 10.1109/ICIMP.2008.24

[5] V. Jyothsna, V. V. Rama Prasad and K. Munivara Prasad, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, August 2011

[6] Morin B., and M'e L., "Intrusion detection and virology: an analysis of differences, similarities and complementariness," Journal in computer virology, vol. 3, pp. 39-49, 2007.

[7] Hashem Mohammed Alaidaros, Massudi Mahmuddin, and Ali Al Mazari, "From Packet-based Towards Hybrid Packet-based and Flow-based Monitoring for Efficient Intrusion Detection: An overview", ICCIT 2012.

[8] Aho AV, Corasick MJ. Efficient string matching: an aid to bibliographic search. Communications of the ACM 1975;18(6):333–40.