IJCSMS (International Journal of Computer Science & Management Studies) Vol. 14, Issue 10
Publishing Month: October 2014
(An Indexed and Referred Journal) ISSN (Online): 2231 –5268
www.ijcsms.com

Application-protocol based Intrusion Detection System

Rama Prabha[1] and K.P. Jayanthi R[2]

[1,2]School of Information Technology and Engineering
VIT University, Vellore, India
[1]*ramaprabha.kp@vit.ac.in*, [2]*jayanthi.r@vit.ac.in*

Abstract

Intrusion detection system is a type of security management for computers connected in a network.IDS monitors the network for security breach to analyze and identify the intruders. Intrusion detection can be further classified as host and network based, this paper provides analysis of Intrusion Detection System(IDS) on the application layer protocols, by allowing packets for deep packet inspection(DPI),intended for selective protocol non-compliance. By using the defence in depth strategy and passing the traffic into a snoop server all the packets are be captured. This paper is limited to OSI layer 7 application protocols and their corresponding port numbers for traffic analysis.

Keywords: *IDS, DPI, DID, Layer 7 application protocol*.

I. Introduction

Intrusion detection system(IDS) has been in use for many years to identify unauthorized access and malicious traffic. They are used for detecting and gathering information's concerning anomalous activities. Intrusion detection system can provide monitoring, auditing and analysis of abnormal activities. Intrusion detection system can be generally categorized into host-based and network-based IDS[1]. Host based intrusion detection(HIDS) system focuses on comparing the host based performance snapshot with the current and existing system to identify the intrusions. Whereas Network based intrusion detection system(NIDS) inspect the entire network. The detection can be based upon protocols and port numbers, digital signatures or anomaly, packets and network traffic spike. Intrusion detection formulates an information system for creating logs and statistics. As a result of updating from different networks , security breach can be reduced.IDS as a hardware or as a software can be implemented within the border along with a firewall.IDS is positioned in a network architecture in an in-line to receive or send and to capture the traffic in promiscuous mode. To protect today's network an effective IDS needs to provide an accurate and timely information about an ongoing attack. Intrusion detection provides pattern matching, statistical analysis, monitoring and auditing the logs. Once the log files are created by the IDS it is analyzed by the network security expert, for implementing high-level of security in the entire network.

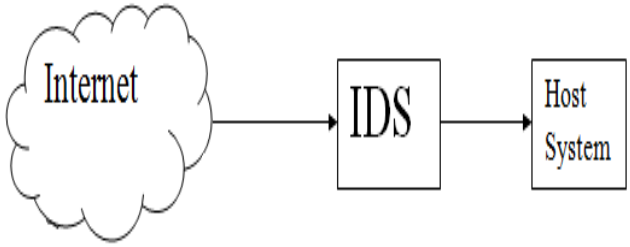

Figure 1 A general IDS implementation

II.Literature survey

Most of the intrusion detection systems that are in use have major issues. The first and the foremost of all is generating false alarms. A good IDS in use should not generate too many false alarms. Moreover any IDS needs a human involvement to identify or inspect the attacks. It takes a long time to analyze the traffic on a entire network. The ID Systems that are currently in use cannot identify attacks from packets. A good IDS in use has to alert when an attack occurs, rather than generating too many false alarms. The more the false alert the more the human labor contribution to identify the real intruder attack. An effective IDS is identified not by the occurrence of detecting attacks, instead by the less number of false alarm rate. Every alarm an IDS generates a network security engineer has to identify if it is a real threat or a false alarm. IDS can be further categorized as active and passive IDS, knowledge and behavior based ids. An active IDS can be called as an Intrusion Prevention System[2]. Though IPS does not require human intervention to identify the threats or alarms, it may flood the entire network with false alarms if implemented in-line a network boundary. A passive IDS is not active as an IPS because it is used only for identifying the threats. Knowledge based IDS maintains a database of attack profiles that happened earlier and identify system vulnerability. Knowledge based IDS generates less false alarm rate. The disadvantage of a knowledge based ID system is that the digital signature has to be updated and maintained as a database and it cannot detect new signature attacks. Behavior based IDS maintains a pattern of a normal active system , deviation from the basic normal activity triggers alarms as

intrusions. Since the base patterns of a system changes quite often knowledge based ID system triggers high false alarms. The networking attacks involved are Scanning, DoS and Penetration attack. Scanning attacks could be used for gathering information about the network architecture , ip address used and port scanning the entire network. By this the active hosts in a network can be recognized to acquire information about the applications used in that computer. The intruder usually goes with a stealth SYN scan, to do a half open scan in the TCP port connection. The intruder sends a SYN if he receives and ACK from the host, so as to identify the port. Dos denial of service attacks is used for making the service unavailable for the host computers. It usually involves flooding of malformed packets to tcp and udp. If the victims system acknowledges the attackers SYN packet and when waiting for an ACK in response, the entire victim network is flooded with mal-formed or fake packets to flood the entire host system for denial of service. Penetration attacks consists of all sorts of attack, it may also be performed by a penetration tester to find the high vulnerability of an entire network. Some of the well known protocol based attacks are Smurf, SYN, UDP, ICMP, DNS attacks[3].

III. Problems with the existing system

There are lot of ID systems available in the market. Some of the well know existing open source IDS are SNORT,BRO,OSSEC. Snort-an open source IDS system capable of detecting signatures and anomaly based, protocols. Bro-An Unix based open source IDS which divides the network traffic, to analyze the framework and compare the troublesome activity with an existing prototype. OSSEC-An open source host based IDS which uses security event manager and security information manager to log the files for root kit detection and active response. In almost all the existing IDS systems, false negative alarms are higher which leads to more human contribution to verify the logs and audits, moreover attacks are on the rise gradually. Hence ID systems ought to be updated frequently, sometimes numerous times in a day. Volume of alerts are devastating. Identifying more serious threats due to false alarms is tough. Intrusion detection systems installed as separate programs in a network, can either be disabled or modified by an attacker or by an inside intruder. It can also be made by crackers hired by the competitors. So far any IDS system needs a human contribution, today's IDS cannot do historical analysis over a period of time.IDS system needs to be proactive rather than being reactive, some systems updates to the latest attack logs and audits or signature detections, but till date the IDS create log files and audits which needs to be monitored after the attack has happened rather than immediately updating, alerting when a deviation occurs.

IV. Proposed System

OSI layer 7 application protocols and their corresponding port numbers that are took into consideration in this paper are HTTP 80,HTTPS 443,FTP 21, SMTP 25.By analyzing the network traffic in the above specified protocols and port numbers and by identifying the malicious traffic spike and intrusion the intruders are detected. Though it is difficult to identify the attack occurring from a specific port, IDS has resolved this complication. Recently developing protocols are used to penetrate firewall without a need for port numbers. Nowadays, many intruders attack a network by using non-standard port or by using the ports assigned for different OSI layers of protocol. Therefore it is compelling to analyze specific application layer 7 protocols port for inspecting the packets passing through. Backdoor security breach happens in OSI layer 7.Protocol based IDS are capable of analyzing the behavior of generated traffic logs from the specific protocol ports.

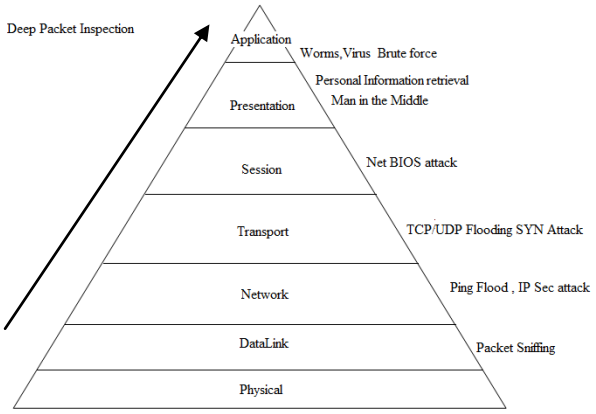

Figure 2 OSI layer attacks in each layer

Using a snoop server all packets can be captured in promiscuous mode for sniffing the packets, the packets sniffed are then inspected for packet filtering by Deep packet inspection(DPI),for specific protocols and their corresponding port numbers. Deep packet inspection(DPI) checks the data part of a header for packet filtering and searching for selective protocol non-compliance. DPI combines both intrusion detection system and intrusion prevention system functionality and can detect certain. Deep packet inspection sometimes goes through OSI layers 2-7 Data link layer till Application layer, to verify the attacks, caused in each layers of the OSI model. Recent study in an university network showed an unwanted network traffic deviation of 35% from non-standard ports. Thus, protocol-port based network intrusion detection system is used to identify the traffic obtained from unspecified ports in order to detect the intrusion[4].

By using defense in depth strategy we can implement Firewall ,IDS,DPI, packet capturing and sniffing in a network for providing more security.

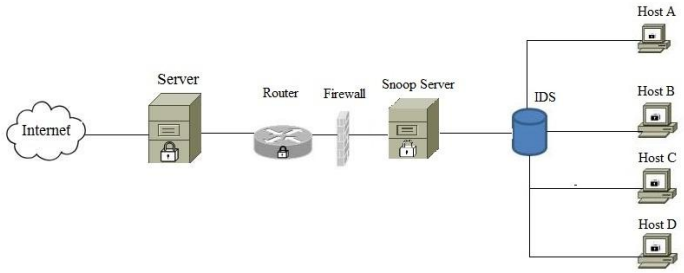

Figure 3 Proposed IDS.

In Fig the packet travels all the way through internet to the network and finally reaches the Host systems. Before the packet reaches the host system it goes through a security server which is a multi layered protection from well-known and unfamiliar threats. A security router like Cisco 500 series protects the entire network from virus, worms. Cisco routers uses security protocols like TACACS+ and RADIUS to access into a network. TACACS uses TCP whereas RADIUS uses UDP a AAA protocol, authorization, authentication and accounting. A hardware firewall is used for stateful inspection, the packets are then passed to snoop server where all the packets are captured and deep packet inspected and sent to an IDS. In the proposed system IDS, the layer 7 protocols and their corresponding port numbers are verified for intrusions. By verifying the 24 hour full packet trace from Munich Scientific network and comparing port based detection with signature based detection the result obtained is shown below[5].

Comparison of signature-based detection vs. port-based detection (# connections).

Method	HTTP	%	IRC	%	FTP	%	SMTP	%
Port (successful)	93,429K	68.14	75,876	0.06	151,700	0.11	1,447K	1.06
Signature	94,326K	68.79	73,962	0.05	125,296	0.09	1,416K	1.03
on expected port	92,228K	67.3	71,467	0.05	98,017	0.07	1,415K	1.03
on other port	2,126K	1.6	2,495	0.00	27,279	0.02	265	0.00

Table1:Comparing Signature and Port based IDS

From the comparison table it is clearly understood that many connections are made from unknown ports, Intruders usually try to attack a network from unknown ports. The proposed system in this paper can not only captures the packets for deep packet inspection, but also verifies the port numbers and the protocols. Not all packets from unknown ports are malicious, there are possibilities some users use various different ports for known protocols if they are not authorized the administrator privilege. It may end up with a false positive alarm.

V. Future Implementation

Comparing active and passive ids for implementing an effective IDS. An active response ids alerts when the attack is in progress, whereas the passive ids collects or provides information after the attack has occurred. Though Passive ids helps in understanding the intruders behavior.

A intends that the Intruder tries to breach a host system or a network, alarms or alerts are passed immediately. Log files or alarms are generated. Active IDS

B intends that the Intruder has breached a host system or a network and stole information. Log files or alarms are generated after the intruder has attacked the system and stole information. Passive IDS

C Security expert verifies the logs, understands the IDS potential and the intruders method used for breaching the system.

If **A>B** the system is an active ids, logs are created when the attack happens.

If **A<B** the system is not an active ids, still logs are created for further understanding.

Either A or B it leads to C, that is log files are created when the attack happens or after the attack has occurred. Both the log files are used for further understanding by the security expert to enhance more security.

But if **A = C**, the attacks are identified as it happens, alerts are passed, the intruder can be prevented further, from breaching the system, still logs are created.

The proposed methodology in this paper could be enhanced further by implementing Genetic Algorithm(GA). GA are machine learning optimization algorithms which follows the concept of Darwin's theory. By implementing GA in this papers proposed system the IDS systems can maximize the detection and minimize the false alarm.

References

[1] Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. “Time Based
[2] Intrusion Detection on Fast Attack for Network Intrusion Detection System”, Second International Conference
[3] On Network Applications, Protocols and Services, IEEE, 2010 [2] Understanding IPS and IDS :Using IPS and IDS together for Defense in Depth-Ted Holland G&EC Practical v1.4b, Option 1,Feb23,2004.

[4] Protocol attacks by Sushant Rewaskar http://www.cs.unc.edu/~jeffay/courses/nidsS05/slides/5-Protocol-Attacks
[5] Protocol anomaly detection in network based IDS , Erwan Lemonnier - Defcom,28th June 2011
[6] Dynamic application layer protocol analysis for network intrusion detection , Holger , Anja , Michael , Vern , Robin http://www.icir.org/robin/papers/usenix06/
[7] Protocol Anomaly Detection for Network - based intrusion detection, Kumar Das , version 1.2f ,August 13, 2011
[8] S. A. Baset and H. Schulzrinne. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. In Proc. IEEE Infocom 2006, 2006
[9] Farah J., Mantaceur Z. & Mohamed BA. (2007). A Framework for an Adaptive Intrusion Detection System
[10] Using Bayesion Network. Proceeding of the Intelligence and Security Informatics, IEEE, 2007
[11] Garuba, M., Liu, C. & Fraites, D. (2008). Intrusion Techniques: Comparative Study of Network Intrusion
[12] Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New
[13] Generation, IEEE, 2008
[14] Wang Y., Huang GX. & Peng DG. (2006). Model of Network Intrusion Detection System Based on BP
[15] Algorithm. Proceeding of IEEE Conference on Industrial Electronics and Applications, IEEE, 2006.