International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Issue 2; March 2018; Page No. 673-675

Network security assessment for vulnerabilities and intrusion detection

Ajay Kumar, Dr. Saurabh Srivastava
Mewar University, Rajasthan, India

Abstract
During the past two last decades we observed the origin and the expansion of a technology that has very much changed the way we work and live. Interconnection of computers through networking and the innovation of the internet were foundation stone of the new technology age. This feature leads to more computing power, improved flexibility and better execution/value ratio. The present enhancements in current technology have empowered the utilization of systems in leading business and in assembling and sharing data in companies and scholarly organizations using the Internet. Today, banks utilization of systems to perform its budgetary operations, clinics has the records of their patients in databases, and numerous organizations have been displayed on the Internet etc. Network and system security are major issues for any association that employs information technology (IT) to attain its tactical and operational goals. While information system (IS) security concerns typically spotlight on those which are from parties that outside to the associations, as a matter of fact information systems are also vulnerable to internal attacks. An IDS examine all inbound and outbound network movements, system logs and actions, and identifies any malicious patterns that may specify a network of system attack from somebody who tried to smash into or compromise a system. This work identifies a number of important issues related to design and implementation and for assessing or deploying commercial

Keywords: network security, intrusion detection

Introduction

It is understood that different attacks threaten the confidentiality, integrity and availability of the information. The more the reliance on the data given by the networks has been increased, the more the danger and vulnerabilities of secure transmission of data over the networks has increased. As the valuable information residing on networks, many network defenses have been designed and layered to combat possible attacks.

Amid the previous two last decades we have seen the conception and the development of an innovation that has all that much changed the way we work and live. Systems administration of computers and the development of the Internet were foundations of the new innovation age. This element has prompted additionally figuring force, expanded adaptability and better execution/value proportion. The present enhancements in current innovation have empowered the utilization of PC systems in leading business and in assembling and sharing data in companies and scholarly organizations utilizing the Internet. Today, banks make utilization of systems to perform its budgetary operations, clinics have the records of their patients in databases, and numerous organizations have been displayed on the Internet etc.

Network and system security are major issues for any association that employs information technology (IT) to attain its tactical and operational goals. While information system (IS) security concerns typically spotlight on those which are from parties that external to the associations, in fact that ISs are vulnerable to internal attacks as well. As a case in point, a poll by Verizon Security Business Solutions estimated that "insiders account [ed] for 17 per cent of corporate data-hacking incidents. At the 2011 Info security Europe gathering in London, 40% of 500 participants pronounced that they would "think that it's simple to utilize their insight into encryption keys, shared passwords and provisos in information security projects to stroll off with any data they wanted." 31 percent said they had the capacity to "hack in remotely and snoop, covertly adjust scrapes or close down the information system" independent of whether they were still utilized with the organization. This pivotal reliance on systems has produced an interest for components that guarantee a certain level of security. Without sufficient system security, many people, organizations, and even governments are at danger of losing that advantage.

Open source intrusion detection tools

There are many easily available open-source and proprietary intrusion detection systems available. Here we are mainly concentrating on Snort, Surakarta and Bro.

Snort

It is a network based IDS examines the traffic and tries to find the suspicious activities. A rule set which is a group of specific byte pattern indicates a particular attack. This type of IDS is generally called signature based intrusion detection system. The signature of the assaults can be downloaded from snort web site and once they are configured they can be then used by snort to identify that assault. Snort is not only can identify the assault but can also work as a packet sniffer and packet logger. Snort can discover thousands of worms through content searching, port scans, vulnerability attempts and trough other suspicious behavior. It is also reliable method for

performing real-time traffic analysis and packet logging on IP networks. The only difficulty with snort is that it is complex from the perspective of installation and maintenance thus it needs considerable amount of tuning for avoiding false positives. The preprocessor, the detection rules, and the alert output components of Snort are all plug-ins, which can be individually configured and turned on or off.

1. Packet capture library
It is a software module and assembles the packets from the network adapter while taking into account the libpcap library for UNIX like systems and for windows systems WinPacap is utilized.

2. Packet Decoder
Decoder fits the packets that are caught into data structures and recognize the level protocols. At that point, it takes the following level, decode IP, and afterward TCP or UDP with a specific end goal to get valuable data like ports and addresses. Grunt will alarm in the event that it finds twisted headers (irregular length TCP options, and so on.) Packet information is then decoded and arranged for further handling.

3. Preprocessors
Preprocessors can be dealt with as filters, which distinguish things, for example, suspicious connection endeavors to some TCP/UDP ports or an excess of TCP SYN packets sent in a brief time of time (port scan). Preprocessors capacity is to take packets conceivably unsafe for the detection engine to try to find known patterns. Preprocessors can alarm on, classify, or drop a packet before sending it to detection engine arrange, or drop a parcel before sending it to location motor.

4. Detection Engine
The most significant part of Snort is this engine which works on the OSI transport and application layers and investigates the packet contents based on the detection rules including signatures for attacks.

5. Output Plug-ins
It bolster an assortment of ready and logging systems. The point where a preprocessor or rule is activated, an alert is logged in Snort's own text or binary file logging formats, database or syslog.

6. Rule Files
Rules are nothing but plain content records and includes list of rules with a syntax including protocols, addresses, output plug-ins related and

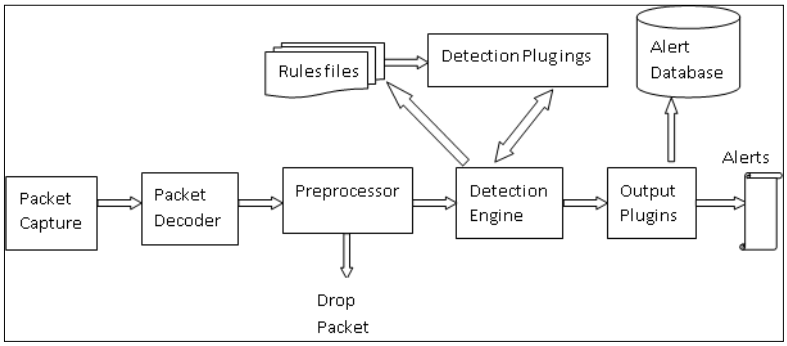

Fig 1: Snort model some other things.

7. Detection Plug-ins
These are modules referenced from its definition in the rules files. They recognize patterns at any time when a rule is evaluated.
Snort makes use of a single-threaded engine, considering that nowadays multi-CPU and multi-core hardware is commonplace. As a result, by default Snort can only fully employ one processor core.

Suricata
Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine.
This is an Open Source software and owned by a society run non-profit foundation, the Open Information Security Foundation (OISF) [19]. Suricata was released in 2010 and work mainly with version 1.2 released in January 2012. All the code of Suricata is original but still the developers of suricata have made no efforts for covering the different ways in which they are borrowing from the Snort architecture. Suricata can also be utilized with the same rule sets as used by Snort. Suricata's exclusive multithreaded architecture can carry high performance multi-core and multiprocessor systems. The real advantages of the multi-threaded design is that it offers high speed and more productivity in network traffic investigation and can help Lessing the IDS/IPS workload in view of where the processing needs are. the engine is constructed in such a manner that it makes use of the increased processing power offered by the recent multi-core CPU chip sets. Suricata in general has been produced for simplicity of execution, joined by a regulated beginning documentation and user manual. The engine is additionally composed in C and intended to scale.

Bro
Bros is an open-source system. It is unix based Network Intrusion Detection System (NIDS). It was written by Vern Paxson at the Lawrence Berkeley National Lab and the International Computer Science Institute. It is a type of passive type of intrution detection system. And examines network traffic for finding the malicious activity. Bro's inner

architecture varies from its open-source alternatives in its script-driven policy engines. By using its script decision options to drop sample, redirect packets it presents its new characteristics.

Bro-ids Architecture
Bro IDS architecture contains mainly 4 modules.

Packet Capture
Bros clustering options for high throughput environment acquires packet from libraries such as libcap. The logic of Packets filtering is based on ports and bits in IP or TCP headers.

Event Engine
The main purpose of the event engine is to s performs certain integrity checks that are used to confirm that the packet headers are well-framed. It also confirms that the IP header checksum is right, Bro reassembles the IP pieces so that the network layer analyzer can highlight to finish IP datagrams.

Signature Engine
The Signature Engine then checks and reviews the packet stream and it creates an event, every time a signature is coordinated. Such types of events can then be investigated by an policy script.
Record to

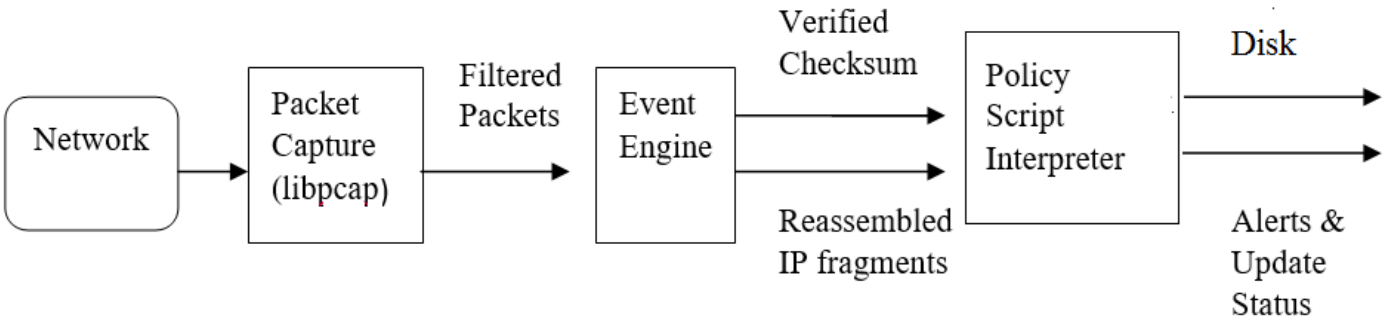

Fig 2: Bro's Architecture

Policy Layer
The policy script translator executes scripts written in a specific Bro dialect. These scripts indicate event handlers the happenings got for the Event.

Conclusion
The primary objective of the proposed technique is to reduce the IDS false alarm rate and increase the accurateness of the attack detection rate. We have performed various experiments to determine the execution of our proposed concept and the results of experiments justify that this method is effective and feasible. For future work, we have various directions. We should also focus more on data mining process while applying on intrusion detection process. Moreover more work is need to be done on creating high quality labeled training data. In order to meet with some general challenges in data mining, it might be preeminent to generate specific - purpose alternates that are customized to intrusion detection.

References

1. Memon VI, Chandel GS. A Design and Implementation of New Hybrid System for Anomaly Intrusion Detection System to Improve Efficiency, International Journal of Engineering Research and Applications (IJERA) ISSN: (Version1). 2014; 4(5):2248-9622, 01-07.
2. Oludele Awodele, Sunday Idowu, OmotolaAnjorin, and Vincent J. Joshua, A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS), Babcock University, 2009, 6.
3. Wankhade K, Patka S, Thool R. An efficient approach for Intrusion Detection using data mining methods", International Conference on Advances in Computing, Communications and Informatics (ICACCI), Print ISBN: 978-1-4799-2432-5 INSPEC Accession no. 13861274, (2013) August 22-25, 1615-1618.
4. Yiwu Zhejiang. Study on Genetic Algorithm Optimization for Support Vector Machine in Network Intrusion Detection Xiaoqiang WANG.
5. Sufyan T. Faraj Al-Janabi, HadeelAmjed Saeed "A Neural Network Based Anomaly Intrusion Detection System" 2011 Developments in E-systems Engineering IEEE Publication, 2011.19, 978-0-7695-4593-6 /11, DOI 0.1109/DeSE.
6. Mohammad SazzadulHoque, Md. Abdul Mukit "International Journal of Network Security & Its Applications, 2012; 4(2).
7. Pratibha Soni, Prabhakar Sharma-An Intrusion Detection System Based on KDD-99 Data using Data Mining Techniques and Feature Selection‖, International Journal of Engineering Research & Technology. 2014; (3):11.