JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

"A Study on SIEM and Packet sniffing"

Vijay Kumar Gandam[1],

[1]Research Scholar, Dept. of Computer Science & Engineering,

SCET, Hyderabad

ganavijaykumar@gmail.com

Abstract: A security information and event management system and packet sniffing are an industry-specific term in computer information security used to denote the type of information that an average log document or celebration logs into a centralized repository from multiple sources for further analysis. Event logs are generated by numerous Internet site device, program, and computer software updates. This paper provides an overview of a security information event management system and Packet sniffing.

Key Words: Security information and Event Management, Virtual Private Network, Packet sniffing, Active Packet, Passive packet. Graphical user interface.

1.INTRODUCTION

SIEM (Security Information and Event Management) Technology provides a Platform for real-time monitoring of information security events from Networks, Servers, Systems, Applications and more. SIEM Solutions can also be used for Regulatory Compliance reporting requirements. SIEM Solutions supports Forensic Analysis on Real Time and Post Incident analysis by retrieving & storing the events based on their Timestamp.

SIEM Formation

SIEM is a combination of SIM (Security Information Management) and SEM (Security Event Management). SIEM Centralizes the Events Information and Log Management from various devices and locations. SIEM uses either Rule-based or Correlation Engines for Identifying the Anomalies by Combining Multiple Events and Information.

Correlation Engine is a programed software, which uses Predictive Analytics and Fuzzy Logic to understand the inter-relatedness between the events and triggers the alerts if found any anomalies.

SEM (Security Event Management)

Provides Real-time Monitoring, Correlation of Events or Combination of Multiple Events, Improve security incident response, Effective response to internal and external threats

SIM (Security Information Management)

Reporting and analysis, Regulatory compliance

Advantages of SIEM – Security Information and Event Management Solutions:

SIEM solutions help identify network threats in real time by capture and analysis of logs from thousands of devices in multiple branches.SIEM solutions enable quick forensics as they can store and retrieve all log data from any device for any period.SIEM solutions provide a GUI based dashboard with a uniform format of reporting of logs and events from multiple devices' solutions can correlate events from logs generated by multiple network devices and report only if there were real network breaches of high priority, hence reducing the number false positives and saving a lot of time for the administrators' solutions enable administrators to study the root causes of errors and security breaches by looking in to the log information and reports. Users can identify what exactly caused the errors (like configuration changes, etc) and which systems are vulnerable. SIEM solutions generally come with ready-made reports and report formats for various security compliance regulations like HIPAA, ISO27001, etc so that the security administrators can focus on more important network security enhancement activities.SIEM solutions can give reports like top 'n' users of specific applications and bandwidth consumption levels for each device on the network, etc.SIEM solutions generally consist of Central Appliance/ Software at the head office (where all the logs from various devices are finally sent to for analysis) with additional software agents (near to or within the network devices that need to be monitored) or hardware appliances to collect all the logs from network devices in various branches/ locations. SIEM is sometimes given as a security service by organizations where all the logs are collected and monitored remotely (in the service provider premises) and ready-made reports are made available to the customers according to their requirements.

Packet sniffing is a technology which captures the packets passing through the network in which it is installed. Packet sniffer is a tool which monitors all the network data. Furthermore, it can intercept and log incoming and outgoing traffic across the network.
Packet sniffer can also be referred as network analyzer or protocol analyzer.

Packet sniffers are of two objectives: Active,Passive.

Passive packet:Passive packet sniffers do not respond back, i.e. they only collect data and are impossible to detect them. Passive sniffers are useful in areas such as telecommunication, Radar systems, medical equipments, etc. Colasoft Capsa, TCPDUMP and Wireshark are examples of passive packet sniffers.

Active packet sniffers:Active packet sniffers can send the data in the network and hence could be detected by other systems through different techniques. For example, active packet sniffer can fake replies to the broadcast or can forward it to a legitimate host. Scapy, smart RF and network ACTIV protocol packet sniffer are some of the active packet sniffers.

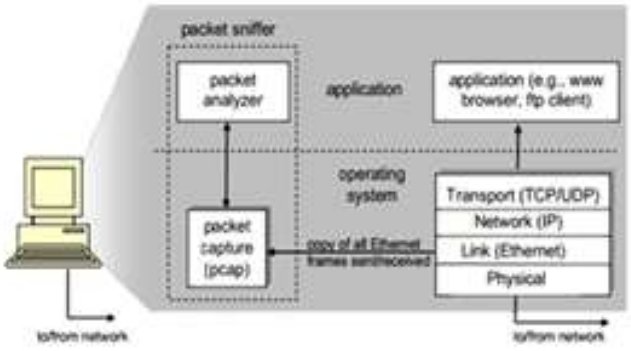

Fig. 1. structure of packet sniffer

.2. **Related Works:**

Network Traffic Analysis: Network infrastructure - traffic will be analyzed on the internal, external and DMZ interfaces of the firewall. To obtain a view of the traffic on our network and an insight into any suspicious behavior.

Security Event Collection, Correlation and Normalization

Devices within TSA infrastructure which will have software installed on them to collect data.

This aspect of the project involves collating logs from various devices in our infrastructure and checking the correlation of the data gathered from these logs against certain use case scenarios. The idea being to build a picture of malicious activity in our environment and thereafter rectify this behavior, as well as gather what would be best practice in regard to building IT policies Essentially, this is an insight into using a Security Information and Event Management (SIEM) tool in our environment to identify risks and gain threat visibility.

3. RESEARCH METHODOLOGY

IT or Security managers who wish to implement a Security Information and Event Management (SIEM) solution at their organization. Organizations that want additional security and visibility into their network activity. Organizations under stringent compliance obligations. Select an appropriate SIEM solution based on vendor research. Create an implementation roadmap. Define your SIEM architecture. Measure the continued value of your SIEM.

4 Outcomes of this Research.

A formalized selection process to identify which SIEM solution is best for your organization to gain full visibility and analyze activity across your network.

An evaluation of the current SIEM products and vendors that can be customized to your organization through the Vendor Shortlist tool.

A completed selection process through the use of a Request for Proposal (RFP) template and a Vendor Demo Script to ensure that you are obtaining the correct information.

An implementation plan that includes the overall defining architecture of your final SIEM solution.

5. SCOPE OF SOLUTION:

The Security information and Event Management & Packet analysis Solution is expected to collect and Capture logs/network traffic from network devices, servers, application security logs, Anti-virus, Proxy server, access control system, Security solutions like DAM, PIM/PUM, SSL VPN Gateway, WAF, VA Tool, Anti-phishing and Anti-malware etc. In addition, the logs being generated by the solutions deployed as part of the SOC implementation need to be collected by the SIEM.Before the start of a SIEM&Packet Sniffing environment installation, it is very important to set a Scope of solutions and a focus of this project. The scope is the driver behind SIEM and can be related to Compliance, security, or operations. It can be a combination of all three and should encompass the entire network infrastructure. If there is a compliance scope needed for one part of the network and a security scope needed for another, the work for a SIEM environment should take both into account. It might be that the company is too large to start implementing SIEM everywhere at once. If that is the case, the focus should be limited. The focus defines an area where SIEM is applied: a certain subset of the entire company. This focus can be as narrow as needed if the primary process of the organization is present.

6. FUTURE SCOPE AND FUTURE ENHANCEMENT OF THE PROJECT

Security Information and event management technologies saw some consolidation in 2017. EMC acquired Network Intelligence, Novell acquired eSecurity, IBM acquired Micromuse, which had acquired

Guardednet, and IBM also acquired Consul. Today there are lots of large, established broad-scoped vendors and point solution vendors trying to capture the roughly $300 million in revenue the SIEM market was estimated to be in 2019.

First let's define where the market has been. Initially these tools were designed for threat management against a noisy external threat environment, namely worms. Their orientation was primarily network and systems with real-time analysis of events to support incident response (Security Event Management). There were also vendors that provided long-term storage, historical analysis and trending against a large back-store to support forensic activities (Security Information Management). So we had real-time analysis to support incident response and long-term storage and historical analysis to support trend reporting and forensics. Threat drove sales and SEM was pushing the space, then the noisy threat environment quieted down and compliance became a larger issue for organizations. Auditors began looking for SIM functions, that is more long-term storage of data, and the vendors all scrambled to grab compliance dollars by adding compliance-oriented templates and repositioning their technology as a compliance solution. There were still some vendors that focused primarily on SEM or SIM, although the leading point solution vendors provided both with variable efficiency. The market, of course, wanted it all. So we now had convergence of SEM and SIM, thus was born the term SIEM that Mark Nicolett (Great analyst) and I coined at Gartner in 2005, although the actual convergence began en masse in 2004. At the time there was no separate log management market and we also included vendors that provided these functions, if they met certain inclusion criteria, in the SIEM market.

Compliance buoyed a market that was nearing stagnation and it created requirements for integration with identity and access management systems (IAM), auditors were looking for user monitoring and auditing against critical servers and applications, not just visibility into threats against the network and devices. The vendors were all scrambling to add this user perspective to their solutions and large, established IAM vendors began to enter the market or expand their capabilities and integrate their technologies into their SIEM solutions. SIM, driven by compliance initiatives, became the main catalyst pushing the SIEM market. The one major anomaly to this trend was Cisco, which purchased Protego and began to sell it as MARS, a component of its Cisco Security Management Suite. MARS also has NBA-like functions (here) and is primarily a network centric, threat oriented SEM. As a side note Cisco deserves a lot of credit for taking an obscure and relatively unknown product in Protego and making it one of the most visible and arguably successful SIEM technologies on the market. Although Cisco will not disclose its penetration, it is fair to assume they have MARS deployed at 2-3,000 customers.

In addition to the SEM vs. SIM and network vs. user centric views there is another dynamic affecting the market. The majority of SIEM vendors filter the data, either at the point of collection or at an aggregation/correlation server. Log management systems collect all the data. The folks who filter claim that 80% of the log files are junk and they only provide the 20% that is relevant, the folks who collect it all say it is a requirement for compliance and how do you know what will be relevant tomorrow.

Today we have a market demanding a solution that addresses all their needs and vendors attempting to provide it. SEM/SIM functions delivered in a single converged tool to support network, system, application,

and user centric views into the environment. We also have log management vendors, basically syslog servers on steroids, creating a lot of disruption with the traditional SIEM vendors, who are now positioning new solutions that provide log management appliances.

7. **Conclusion**

In this paper, we tend to propose a novel. Security information and Event management and Packet sniffing have been reviewed in this paper. This paper also reviewed structure of packet analysis describing the various types of SIEM techniques, and methodology . Various applications of SIEM solutions and many tools needed for processing are also being reviewed. The Security information and Event Management & Packet analysis Solution is expected to collect and Capture logs/network traffic from network devices, servers, application security logs, Anti-virus, Proxy server, access control system, Security solutions like DAM, PIM/PUM, SSL VPN Gateway, WAF, VA Tool, Anti-phishing and Anti-malware etc. Information Security is to protect the valuable resources of an organization such as hardware, software, and skilled people. Through the selection and application of appropriate safeguard, security helps the organization to meet its business objectives or mission by protecting its physical and financial resources, reputation, legal position, employees and other tangible and intangible assets.

Information systems security begins and ends with the people within the organization and with the people that interact with the system, intentionally or otherwise. The end-users who try to access the information which the security professionals are trying to protect could be the weakest link in security chain.

By understanding some of the behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles. These measures, along with appropriate policy and training can substantially improve the performance of end users and result in a more secured information system.

8. References:

1.SIEM Books By David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke,
2.Information Security Resources: Bibliography Creators:Dotson, Daniel S.
3.Publisher:Haworth Press, Inc. URI: http://hdl.handle.net/1811/47924
4.International Journal of Innovations in Engineering and Technology (IJIET) http://dx.doi.org/10.21172/ijiet.161.04
5.International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.3, June 2013Kiran and Hari
6.https://www.wireshark.org/
7.Security Operations Center – SIEM Use Cases and Cyber Threat Intelligence by Arun
8. Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan
9. https://www.manageengine.com/log-management/white-papers.html