IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. IV (Jul.-Aug. 2016), PP 85-89
www.iosrjournals.org

Security Suite for IT and Telecom Industries

Ruda Khare[1], Prof. Nandana Prabhu[2]
[1]*(Information Technology, K.J. Somaiya College of Engineering, India)*
[2]*(Information Technology, K.J. Somaiya College of Engineering, India)*

Abstract: *Security is the biggest concern nowadays faced by various companies as security threats are more prevalent. This 'openness' is the reason because of which protecting networks and business data is even more difficult. The solution in response to this threat is to provide a single aggregated view of all the threats observed in the network, to prioritize them so the worst are dealt first. It can happen only through "Security Suite". It offers insight of Front-end-Perimeter protection (FEP), Advanced Breach Detection (ABD), Distributed Denial-of –Service(DDOS) protection. But, what when they are not accessed from the same simulator. This paper refers to the working of Security Suite in real time, to provide a more user friendly working and reduce the tedious task of switching between simulators. It states how the products of the organization and the Security Suite can go hand in hand.*

Keywords: *Alerts, Security Suite, Simulators*

I. Introduction

Cyber threats are very common. No one is secure. Various organizations, institutions are constantly working on keeping their system safe and secure. They take several measures for the same. Thus, for the betterment and security of entire network, Security Suite is introduced. Compounding the problem is that each tool has its own set of alerts, so we track multiple simulators. The number of threats and attacks against service providers and strategic industries mask this task nearly impossible. Security officers in strategic industries are often lost in sea of unorganized alerts. This Security Suite is nothing but the software, which will display the vulnerabilities and security health of the entire network and its network elements in a graphical format. Currently this Security Suite provides the alerts such as Distributed Denial-of-Service (DDOS), Advance Breach Detection (ABD), Front-end-Perimeter (FEP) and Check Point (CP). It has its products such as Network Management System (NMS) and Element Management System (EMS). These are the two products that are added in the Security Suite and the working of them and security logs are observed but it is a tedious task to every time switch between the simulators to observe the alerts and again add each alert separately on the software application. In this paper we will discuss the existing system, proposed system and its advantages.

II. Security Suite

Due to constant change it is becoming difficult to maintain an environment that is safe and secure. No one and no organization is completely secure. This suite leverages security expertise with best of breed solutions to bring to you the most comprehensive security suite in the market. For cyber security this change is the greatest obstacle in maintaining safe and secure environments. As cyber terrorists are becoming smarter security threats are targeted every day. In this atmosphere, no organization or individual is completely secure. The Security Suite is chosen by variety of customers to provide solutions that ensure secure and global communication. Security in telecom industries is equally essential as it is in the IT industries. It leverages its telecom security expertise to bring the industry a comprehensive security solution starting from physical layer. This security solution provides a holistic and robust protection to the entire organization. Multiple hardware and software based features are provided by this Security Suite. The Security Suite is a virtual one-stop-shop, securing all seven layers and provides behavioral analytics. This Security Suite provides a variety of security applications such as encryption, firewall, Supervisory Control and Data Acquisition (SCADA) protection, Virtual Private Network (VPN), big data, network anomaly detection, DDOS protection, cyber .analytics, strong authentication, and more. Till today, customers were using services which did not provide them all the above mentioned features at a single place for each individual features customers were using single application. We face increasingly complex and diverse security challenges as critical infrastructure provider [3]. Threats are observed everywhere and are faced by all kind of organizations. Such kind of application is needed which will upgrade the entire system and will be a standalone program which will support all features and in near future more can be added to it.

1.1 Security Threats

Recently various cyber threats have come in picture: Cyber Espionage, Information Warfare, Cracking, Cyber Crime, Cyber Terror and Hacktivism. Protecting the network from cyber-attacks is a global issue faced by all. Gathered reports signify that organizations that are energy based are the latest targets. Network shut down would be extremely costly if long power shut downs occurs as it will disrupt lives of people all around the globe as daily activities and services will be disrupted including water, food, healthcare. Hence, expert's advice that there are more chances that a successful attack can take place but the owners have to be prepared with the solutions [4]. Due to this substantial amount of data that flows within the Smart grid networks, used to connect between the distributed energy sources and multiple consumers in a smart, balanced and controlled way. The information flow is sometimes accessible to the public networks (e.g. Internet), exposing this Smart Grid network to potential multi-layered cyber-attacks. Many typed of attacks combine several attack vectors into the target network.

1.2 Security Suite Protection Approach

The right approach for providing a proper Security Solution is to define a holistic, intuitive and customized approach that provides secure network against multilayer cyber-attacks including zero day attacks. In order to provide comprehensive and coherent protection, one must design and set in place defense mechanisms through layer 1 till 7 of the OSI model [6], at user's layer adding Layer 8. The Security Suite provides different protection approaches such as-

1. *L2-L3 encryption-* It provides data integrity and confidentiality to data that is in shared environments, attacking the virtual servers of another tenant. Entire network is monitored to provide security and avoid traffic. Moreover, third user is granted permission to preserve the keys that are used in encryption. Applications are protected by virtual servers, policies are enforced, centralized key encryption and policy management is done.[1]
2. *Firewall-* Based on an applied set of rules, the firewall controls incoming and outgoing network traffic. It creates a barrier known as security barrier between two networks to accept and reject connections and services. They are present at the boundary of internet and internal network. It is a type of code that is executable and is executed on independent machines. Traffic flow is observed by it. It is used to provide controls such as- User control, direction control, behavior control and service control.
3. *SCADA DPI protection (Supervisory Control and Data Acquisition Deep Packet Inspection-* It is used to provide matching pattern mechanism. Awareness of enhanced states and per-packet deep inspection. Similar signatures within a same packet are identified quickly. Signatures are matched with the help of pre-defined rules. Traffic should not be affected when signatures are loaded during runtime. Dynamically updating signatures. Engine is fully-agnostic. Insights of operational incidents of cyber security. It quickly filters out the vast majority of traffic that is clearly an obstacle (identifying simple signatures at a low CPU cost). All the traffic that is behaving like an obstacle it is filtered out. This technology does deep packet analysis.[7]
4. *Front-end-Perimeter-* A demilitarized zone or DMZ also known as perimeter network, larger and un-trusted usually (the internet) network. Its purpose is to add an extra security layer to internal network of the organization. DMZ is accessed directly externally but not to any other network part.
5. *Big Data Cyber Analytics-* Making the sense of historical data and terabytes of current this solution provides toolbox of cyber–analytics without using any rules that are predefined. Generic, terabytes of current algorithms that are based on machine learning that discovers the patterns, convert activity from within security logs that are in terabytes size. Dashboard and reports include queries that provides fast results of security analysts allowing them to add recent features one of it is Network Function Virtualization solution [5]
6. *Network Anomaly Detection-* The breach/anomaly or abnormality is solution that provides detection and prevention provides. It connects to the switches in the network internally, find stolen and vulnerable endpoints credentials proactively, and proceed to flag and prevent them. It has three stages such as detect, remediate, illuminate.
7. *Distributed Denial-of-Service (DDoS) protection-* This attack is behavior based it brings down the entire system. When a user accesses any of the websites online there are various malware present. When he reaches any malicious website without the concern of the user malicious data is downloaded to the user's machine. This malicious data is nothing but a Trojan which is extremely small in size and is resting in the user's system like a zombie which get activated when a third party sends active command when the zombie(Trojan) is activated entire system is crashed and brings down the entire network from the command that was sent from remote location.

The software is in its initial developing stage from the above mentioned protection approaches the ones that are currently provided by the security suite are as follows-[4]

1. Distributed Denial–of-Service (DDoS) – This attack is behavior based. It brings down the entire system. When a user accesses any of the websites online there are various malware present. When he reaches any malicious website without the concern of the user malicious data is downloaded to the user's machine and is activated when it receives a command.
2. Advance Breach Detection (ABD) – After a breach has occurred, this type of systems are used to detect malicious activities in the system. To protect against advanced threats especially unidentified malware, breach detection systems are used. Breach detectors identify the attacks that were not identified previously. It determines the attacks by assessing combinations of heuristics, risk assessment, traffic analysis, and data policy and if any violation of reports has taken place.[2]
3. CP (Check Point) – It provides software and hardware products internationally around the globe for Information Technology, security including network security, data security and security management. It is a vital point in software that observes the abnormal behavior, an important feature is of this technology is that check point provides scene information is collected at checkpoint.
4. FEP (Front-end-Perimeter) – A demilitarized zone or DMZ also known as perimeter network, larger and un-trusted usually (the internet) network. Its purpose is to add an extra security layer to internal network of the organization. DMZ is accessed directly externally but not to any other network part.

III. Existing System

The existing system consists of the following features and advantages

1. *Unified Dashboard* –It provides all the alerts in the same view with advantages such as- from multiple points' cyber security alerts can be gathered, it shows a pictorial view of all the data that is gathered, reports and notification are generated and it is also suitable for mobile phones, computers and tablets.
2. *Aggregated Events* – Significant security engines are observed and all together all events are generated and displayed, root causes can be pin pointed easily, predefined heuristics or signatures are not needed and entire data is displayed smoothly on the dashboard.
3. Threats that are calculated are displayed properly.
4. Cyber security suite provides a real-time and centralized view of all the threats in the system.
5. Many more widgets and threats can be added in the near future.

IV. Issues In Existing System

The existing has the above mentioned alerts, for running those alerts only a single simulator (console) is available The add plugin (alerts) window is displayed where alerts are added to the Security Suite. It consists of the information to be added such as – Name, Description, Type, Username, Password, Server and Port Number

Here, the issue is every alert has the same console. To check the functioning of each alerts every time the previous alert has to be removed so that a new alert can be configured in the Security Suite. It is a very tedious task to every time configures an alert separately. At a time it can be handled by one person. It is time consuming which leads to a tedious task to the staff. To explain the issue in existing system following example is illustrated:

The Security Suite provides various protection approaches but as the suite is in the initial level following alerts are included– DDOS, ABD, CP, and FEP. The Security Suite is a software solution that gives the security health of the entire network of the system. The security alerts are needed to be configured/connected with the Security Suite. The add alert window is displayed where DDOS, FEP, CP, ABD, NMS and EMS are added/configured in the Security Suite. As the Security Suite is for IT and telecom industries hence, DDOS, FEP, CP, ABD are the information security alerts whereas NMS and EMS are the network security alerts which display alerts for telecom industry products. To configure/add DDOS alert following steps are followed-

- To login you have to be a registered user.
- The Security Suite dashboard is displayed.
- There are other tabs present on the dashboard such as- Reports, Notification, Plugins, and Settings.
- Go the Plugins tab. Plugins tab is nothing but the window where you have to add/configure alerts in the Security Suite.
- In the add plugin option the details of the alert is to filled as name, description, type, username, password, server, port. To add/configure DDOS-
  Name- DDOS
  Description- Distributed Denial-of-Service
  Server- Simulator IP address.
- The plugin/alert is configured in the Security Suite.

Once the DDOS alert is configured in the Security Suite now to see its working following procedure is to be carried such as Open visual editor. Be a super user. // to edit visual editor (VI). Give path to open simulator. List of alerts will be displayed. Enable DDOS. Manually gives input script for DDOS. DDOS alerts will appear in Security Suite dashboard.

V. PROPOSED SYSTEM

The security Suite provides the security health of the entire system in a pictorial format. This security Suite is useful for both IT industries and Telecom industries. The suite is useful for IT industries as it displays information security threats. As this software is in its initial stage selected threats are configured such as DDOS, ABD, CP and FEP. This security suite is recommended for telecom industries as it can handle customers network entirely because keeping in mind that individually all the elements cannot be protected whether you are protecting your transport network or IT infrastructure. This Security Suite provides optimal security and a centralized real-time view and control of security threats. As this Suite can be used in IT infrastructure as well it has own flaws and considering the above mentioned issues a solution is proposed for the same. Here, for configuring alert such as DDOS, ABD, FEP and CP it is observed that a single simulator is available. This simulator is nothing but the platform for executing the alerts and seeing them appear in the Security Suite dashboard. This simulator has a IP address through which alerts can be configured with the Security Suite. All the alerts have this one simulator because of which only one alert can be configured at a time and alerts for only one alert is observed. To execute all the alerts each time the previous alert has to be disconnected/disabled from the simulator. A script is written to display DDOS alert on the Security Suite dashboard. The entire alert has the same simulator. In the add plugin window a “Server” option is displayed where the IP address of simulator is to be entered to establish connectivity of simulator and Security Suite. Now, as all alerts have same simulator at a time only one simulator can be used to added/configure any of the alerts. To avoid these following solutions are proposed is-

1. *Each alert should have separate simulators*
   When DDOS alert is to be observed in Security Suite it should have its separate simulator to run upon. All the DDOS commands are to be executed from the same simulator.
   Advantages-
   If this solution is used there will be no need of disabling the current active alert that is running on the simulator, It will be less time consuming, it will not be a tedious task for the customer and as well as the testers.

2. *Adding simulator in “Add Plugin” window GUI*
   “Add Plugin” window is displayed when alert is to be added in the Security Suite so that alerts will be reflected in the dashboard of Security Suite. In the add plugin window in ‘server’ option the simulator IP address is to be entered. If separate simulator is allotted for each of the alerts directly the simulator IP address can be entered.
   Advantages-
   If this solution is used there won’t be any need of manually disabling the active alert on simulator to execute a separate alert, directly a script can be executed to observe any alert any time or all the time, more than one number of users can use the simulator, less time consuming, it won’t be tedious a task for the customer and the staff as will be more users friendly.

VI. Conclusion

Security Suite is an application that provides the entire security health of the system. It displays the alerts, priority and severity of the alerts in a pictorial format. But, handling and running those alerts one at a time is a tedious task which has to be looked upon. This paper has highlighted the same issue and has proposed a solution for the same.

Acknowledgements

I want to thank K.J Somaiya College of Engineering for giving me this opportunity. We would like to thank our contributors, supporters, colleagues, friends and relatives for encouraging and motivating us. We would like to thank our professors for their constant guidance.

References

[1]. Sajjad Arshad , Maghsoud Abbaspour , Mehdi Kharrazi , Hooman Sanatkar, “An Anomaly-based Botnet Detection Approach for Identifying Stealthy Botnets”, 2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE) , Penang, Malaysia, 4-7 December 2011, *ISBN: 978-1-4577-2058-1, IEEE Catalog Number: CFP1189L-PRT.*

[2]. Hayawardh Vijayakumar, Joshua Schiffman, and Trent Jaeger, “A Rose by Any Other Name or an Insane Root? Adventures in Name Resolution ”, 2011 Seventh European Conference on Computer Network Defence (ECCND), Gothenburg, Sweden, 6 – 7 September 2011, ISBN: 978-1-4673-2116-7, IEEE Catalog Number: CFP1136F-PRT.

[3]. Junfeg Tian, Jianlei Feng, “Trust Model of Software Behaviour Based on Check point Risk Evaluation”, Third International Symposium on Information Science and Engineering, , Pages 54-57, IEEE Computer Science Washington , DC, USA, 2010, ISBN:978-0-7695-4360-4,DOI:10.1109/ISISE.2010.79

[4]. S. Massoud Amin, Anthony M. Giacomoni, “Smart Grid Safe Secure Healing”, IEEE Power and Energy, January 2012, 1540-7977/12, DOI: 10.1109/MPE.2011.943112

[5]. Jean Gorordon Kocienda, “User Access Controls”, To Succeed with Big Data, Enterprises Must Drop an IT-Centric Mindset; Securing IoT Networks Requires New Thinking (Cisco Blog, October 2014).

[6]. International Standard ISO/IEC standard 7498-1:1994-11-15, “Information Technology –Open Systems Interconnection-Basic Reference Model: The basic Model”, ISO/IEC 7498-1:1994(E).

[7]. General (Ret). Michael Hayden, Curt Hebert Susan Tierney , “Cyber security and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat”, Bipartisan Policy Center’s (BPC) Electric Grid Cyber security Initiative, February 2014.