IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Proactive Web Security

Venu S N[1*], Shilpa N R[2], Krishna Badiger [3]

[1,2,3] School of Computer and Information Technology, Reva University, Bangalore, India

Corresponding Author: venusn99@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si14.474478 | Available online at: www.ijcseonline.org

***Abstract*—** Key benefit of this paper is to provide solution to reduce the time gap between the attacker to compromise the organization and organization to detect it has been compromised. It can be done through real time monitoring the organization data activities. These activities can be from the network assets such as firewall, servers, active directory, IPS, IDS, etc. Studies show that on an average this time gap will be 4 to 6 months, by this time the attacker would have caused severe potential damage to the enterprise which might bring us huge financial loss, confidential data might be breached. To Proactively protect enterprises from such threats It is necessary to have a security operational center which helps organization in real-time monitoring and proactive analysis.

Keywords: Splunk, system logs, correlation, CSV-comma separated values.

I. INTRODUCTION

We live in the age of digitalization. Technology has made a drastic change to our lives in few decades by making things robust, simple, faster and convenient. One way or other we are connected with internet. Websites play major role in business and marketing sector. If you have a business, websites help you to target the most likeminded people out there. Where is the major population exist? i.e. Internet. Websites can be used for marketing. For example, purpose of e-commerce websites is to sell its products to end users. “Web analytics is the practice of measuring, collecting, analyzing and reporting online data for the purposes of understanding how a web site is used by its visitors and how to optimize its usage.” User activities are stored as logs in web server, Server have capable to storing activity logs into a file format which is used for product analysis and forensic analysis. Based on the log analysis reports are generated. Web analysis also helps in analyzing the customer data so that the companies like Dominos can gather data such as payments which are successful, failed, pending, total number of orders per day and customer interested products etc. For the web analysis to work logs from various sources such as web server where log files need to append all the activities from a pinch to peak events to the log file. In the organization where the network architecture is well designed web server is always placed outside the firewall in DMZ (**demilitarized zone).** The reason they are placed at DMZ is that Web server is only the assets has to be accessible to both Public and Private user. This makes the web server more vulnerable by the hackers that any other assets in the organization. So thus it make really necessary to protect and prevent the attacks on web server. Even though there are many industry leading anti hack software but still they are failing to meet the promise. Thus to Proactively protect these assets(web server) of organization SIEM tools comes into play. SIEM tools such as mcafee security enterprise , Splunk , Qradar etc. This paper focus on Industry leading SIEM tool Splunk.

II. RELATED WORK

K.SANKARI,R. LAVANYA, S. AMALAGRACY Paper Titled “**REAL TIME MONITORING SYSTEM USING SPLUNK**” [1] in this project authors used traditional hotel management system to demonstrate “new generation smart log management system” using splunk. To keep track of every transaction done in hotel management successive logs are generated and stored in log file. Activities such as online hotel room booking where there should be a flexible for checking type and availability of rooms and other details such as mode of payment, transaction details of payments done, check-in and check-out time. Business make investment on splunk for deploying, developing implementing and usage of it. splunk is used to provide valuable information to business users with respect to various departments of Hotel. Splunk helps to investigate and resolve issues much faster than earlier and it can also be used to detect the error and issues before they make valuable impact on customer experience intern which may affect business.

III. PROPOSED WORK

Splunk is “Security Information and Event Management”(SIEM) software works on the security of systems and analysis of data. SIEM is combination of two tools i)SIM-“Security Information Management” and ii)

SEM-"Security Event Management" tools. This allows you to do a real-time analysis and offline analysis with the data that you can retain for a long time. Everything with data collection SIM comes into play. you can move data or upload data to a centralized place. It helps in doing real-time analysis or forensic analysis using data. With this data you can perform searches for troubleshooting and create reports and pictorial views to make sense of the collected data. When SIEM comes to the table Things get interesting. After we receive identified patterns in the data, you can correlate the data to automate notifications and actions based on the correlation rules written. For example, you can set it to trigger an alert because there are too many failed logins. By looking at the logs, you can then correlate the requests to see that someone might be trying to find a backdoor (loophole/exploit) in your system.

SPLUNK

Splunk Enterprise is industrial leading tool for analyzing, real-time monitoring, troubleshooting and security investigations. The Security Operations Team helps in visualizing through dashboards generating alerts and reports related network health like bandwidth consumption, CPU usage and monitors for error events and peculiar patterns. The security analyst team uses Splunk for analyzing, monitoring and corelate patterns to generate security related reports and alarms and Splunk generate alerts proactively when the abnormal patterns behavior is observed and thus helps in investigation on attacks. Source data is provided to the splunk. Splunk collects data, indexes , normalizes and provide a user-friendly dashboard.

Mongo DB

Unlike other famous database with are relational database MongoDB is a document database. It is used at high level at organizations, where most of database as databases, tables, columns and as rows whereas in MongoDB data we have database, collections and documents. Similar to the relational database data is grouped in MongoDB and a database (Mongo database) is a set of collections. MongoDB was designed for high performance from ground level. Its performance is measurable over relational database.

DEVELOPMENT TOOL

ATOM IDE is integrated development environment (IDE) which is used for designing and developing the Java or java-based applications.

ATOM IDE

Atom was developed by GitHub (Atom – A Hackable Text and Source Code Editor for Linux) which is a free and nonproprietary text and source code editor. Atom is also known as "hackable text editor for the 21st Century" (Atom 1.0) by developers. Atom allows users to insert in external packages and themes which can be used to customize the options and appears of the editor, therefore you'll be able to set it up in line with your preferences and with ease (Atom). It is as hospitable to a initiate because it is for a full-fledged developer. Atom has been making a large contribution in the field of data science as it allows you to work with R and Python in a consistent manner. And Atom doesn't support only these two languages (R and Python) are not the only supported languages, Atom's default packages can be used to apply syntax highlighting for the different programming languages and file format such as C, C++, C#, CSS, COBOL, Go, HTML, Java, JavaScript, JSON, Perl, PHP, Ruby, Scala, SQL and lots of others also (Atom).

Node JS

"Node.js is a JavaScript runtime built on Chrome's V8 JavaScript engine." As Node.js is based on JavaScript as a developer one need to have a strong understanding on JavaScript which is for developing application servers, web applications, general purpose programming language apparently it is well known for server-side development, It is also simple language and flexible. JavaScript being unreliable made it to have bad reputation . It is unreliable because of its Document object model. As Node.js has event-driven architecture thus making it different from common application server. Because of it memory footprint is low, performance is high, latency under load is better and is simpler. Node.js helps in writing JavaScript based applications outside of web browsers. It is easy to write HTTP server in Node.js

IV. METHODOLOGY

Splunk has forwarder which does function of collecting logs by either pull or push method. It collects logs from sources database, servers, firewall, IPS, IDS etc. Organization does have a large number of IT assets and logs from each device has to forwarded to Splunk here comes the hectic problem as each and every vendor provides there own log format. First in the splunk collected logs are indexed , normalized as the logs have a different format. Normalized logs are aggregated and based on the fields we extract correlation rules are written on the peculiar activates in the network when the correlation rules are met the reports are generated , alerts are raised and relevant actions are triggered.

Web server: web server is configured to log the all the events that happens and export to centralized log source. To showcase different methods of intrusion activities that might occur. This project requires 3 Webpages i.e. login, registration, reset password pages. The suspicious activities can be: (i) When a user fails to login multiple time (ii) A new account is created (iii) Users password is changed Log Generation: Each and every activities that take over the web server has to be logged because in the critical state puny information play a versatile role in detecting the intrusion. In this project logs are necessarily generated using log4js package. User activities such as successful or failure attempts

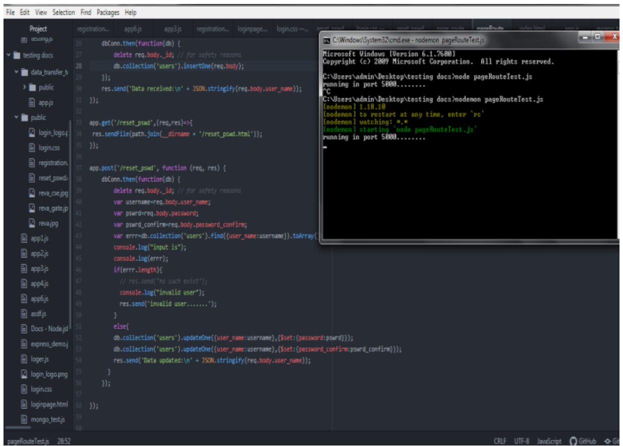
, change of password by user, new account created or deleted. System activities such as change in system architecture, number of active connections, server errors and wake up and log-off time. Thus logs generated are append in the regular format such as CSV, raw logs, The logs are required for later part of the project for analysis using Splunk.

Search Head: Is the only UI based Component of the Splunk. Splunk has its own format of search language called Search Processing Language (SPL). SPL language consists of two fields one for searching required data from logs and other to representing data such as tables, charts, etc.

V.RESULT

All the activities done by the user such as Login, Logout, password change, failed login attempts and even success are recorded and logged in log file. The generated logs are imported to this splunk, Splunk indexes, normalize and correlates. When the specific condition is met the alert is raised

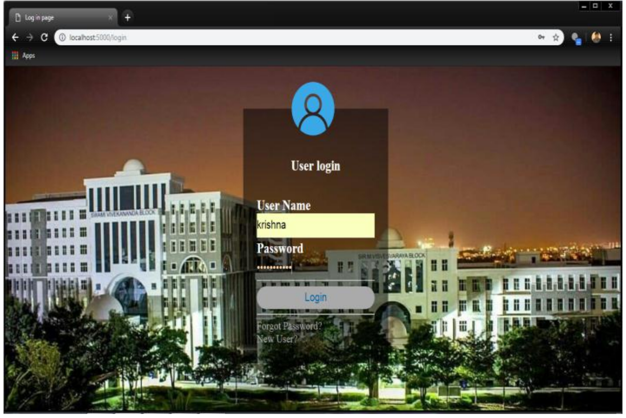
Alerts and Actions: The correlation rule set contains rules that correlate incoming events based on previously defined relationships. When the correlation or specified events are met, alerts or notifications are generated. Based on its priority these alerts are handled by respective member or script is invoked to perform respective task to handle these alerts.



```
    dbConn.then(function(db) {
        delete req.body._id; // for safety reasons
        db.collection('users').insertOne(req.body);
    });
    res.send('Data received:\n' + JSON.stringify(req.body.user_name));
});

app.get('/reset_pswd',(req,res)=>{
 res.sendFile(path.join(__dirname + '/reset_pswd.html'));
});

app.post('/reset_pswd', function (req, res) {
    dbConn.then(function(db) {
        delete req.body._id; // for safety reasons
        var username=req.body.user_name;
        var pswrd=req.body.password;
        var pswrd_confirm=req.body.password_confirm;
        var errr=db.collection('users').find({user_name:username}).toArray(
        console.log("input is");
        console.log(errr);
        if(errr.length){
          // res.send("no such exist");
          console.log("invalid user");
          res.send('invalid user.......');
        }
        else{
        db.collection('users').updateOne({user_name:username},{$set:{password:pswrd}});
        db.collection('users').updateOne({user_name:username},{$set:{password_confirm:pswrd_confirm}});
        res.send('Data updated:\n' + JSON.stringify(req.body.user_name));
      }
    });

});
```

C:\Windows\System32\cmd.exe - nodemon pageRouteTest.js

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin\Desktop\testing docs>node pageRouteTest.js
running in port 5000........
^C
C:\Users\admin\Desktop\testing docs>nodemon pageRouteTest.js
[nodemon] 1.18.10
[nodemon] to restart at any time, enter `rs`
[nodemon] watching: *.*
[nodemon] starting `node pageRouteTest.js`
running in port 5000........
```

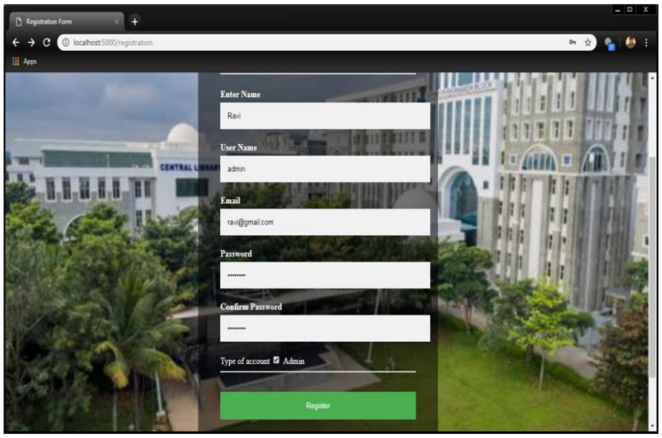


User login

User Name
krishna

Password
••••••••••

Forgot Password?
New User?



Enter Name
Ravi

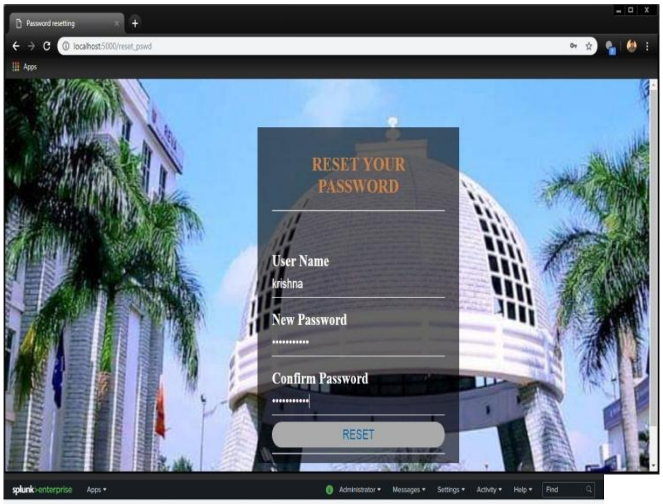
User Name
admin

Email
ravi@gmail.com

Password
••••••••

Confirm Password
••••••••

Type of account ☑ Admin

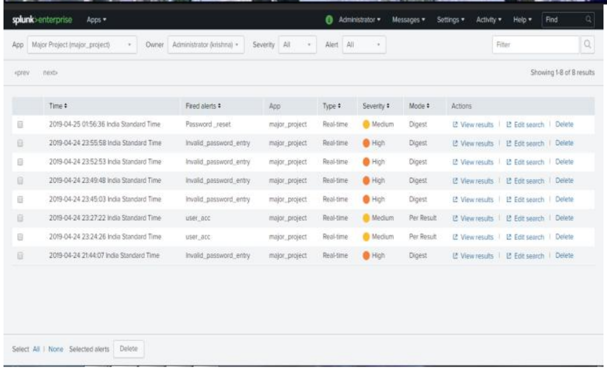


RESET YOUR PASSWORD

User Name
krishna

New Password
••••••••••

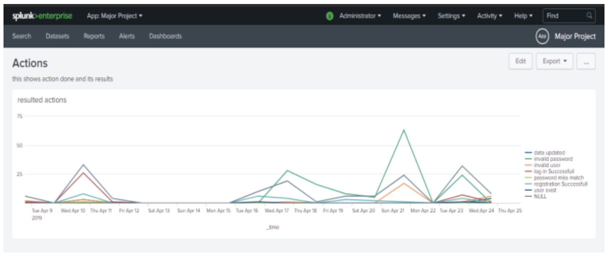
Confirm Password
••••••••••

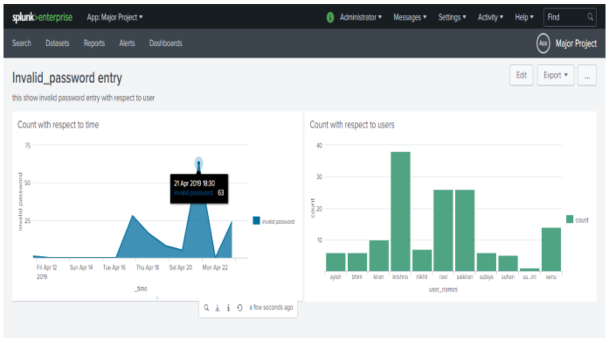


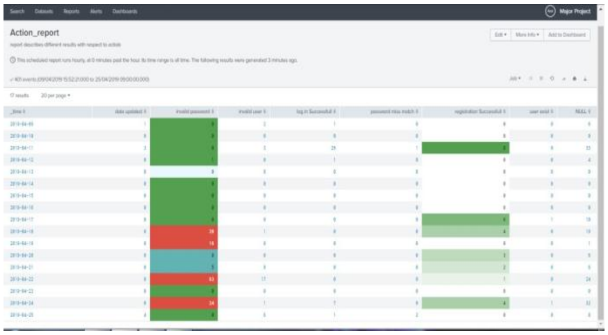
App Major Project (major_project) Owner Administrator (krishna) Severity All Alert All Filter

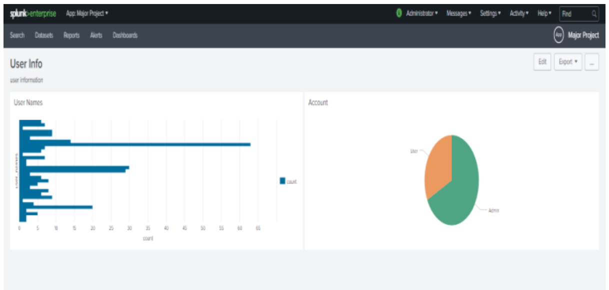
Showing 1-8 of 8 results

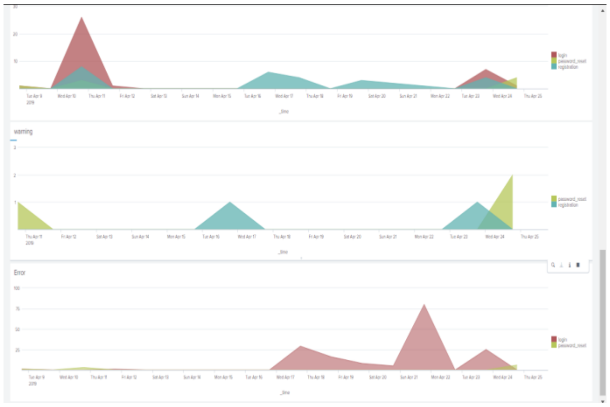
	Time	Fired alerts	App	Type	Severity	Mode	Actions
□	2019-04-25 01:56:36 India Standard Time	Password _reset	major_project	Real-time	● Medium	Digest	View results | Edit search | Delete
□	2019-04-24 23:55:58 India Standard Time	Invalid_password_entry	major_project	Real-time	● High	Digest	View results | Edit search | Delete
□	2019-04-24 23:52:53 India Standard Time	Invalid_password_entry	major_project	Real-time	● High	Digest	View results | Edit search | Delete
□	2019-04-24 23:49:48 India Standard Time	Invalid_password_entry	major_project	Real-time	● High	Digest	View results | Edit search | Delete
□	2019-04-24 23:45:03 India Standard Time	Invalid_password_entry	major_project	Real-time	● High	Digest	View results | Edit search | Delete
□	2019-04-24 23:27:22 India Standard Time	user_acc	major_project	Real-time	● Medium	Per Result	View results | Edit search | Delete
□	2019-04-24 23:24:26 India Standard Time	user_acc	major_project	Real-time	● Medium	Per Result	View results | Edit search | Delete
□	2019-04-24 21:44:07 India Standard Time	Invalid_password_entry	major_project	Real-time	● High	Digest	View results | Edit search | Delete











friendly dashboards from raw log data with good visualization effects which gives us quick glance about the activities that are happening in the network. Reports are generated periodically at specified time intervals to monitor and analyze transaction. Alerts are triggered when correlation rule are met i.e. suspicious activities are recognized and recorded, different priority levels are set to differentiate between high and low risk alerts, based on these priority levels important issue are resolved first. Splunk provide facility to perform specific actions when alert was triggered.

VI. CONCLUSION

In this project we have successfully generated log file. Each and every activity/transaction is recorded and monitored continuously to check suspicious activities that are happening in the system. Splunk helps us to create user friendly dashboards from raw log data with good visualization effects which gives us quick glance about the activities that are happening in the network. Reports are generated periodically at specified time intervals to monitor and analyze transaction. Alerts are triggered when correlation rule are met i.e. suspicious activities are recognized and recorded, different priority levels are set to differentiate between high and low risk alerts, based on these priority levels important issue are resolved first. Splunk provide facility to perform specific actions when alert was triggered.

FUTURE WORK

Splunk Enterprise is powerful tool for real-time monitoring and analyze raw log which are generated. with good dashboard visualization, report and alert generation system it helps to improve operational excellence. Splunk can also be extracted to improve business and security in the network which are exposed
to the internet.

REFERENCES

[1]K.SANKARI,R.LAVANYA,S.AMALAGRACY *"Real Time Monitoring System Using Splunk"* IJCSMC, Vol. 4, Issue. 3, March 2015, pg.434 – 441, pp. ISSN 2320–088X

[2] KAVITA AGRAWAL1, READER HEMANT MAKWANA *"Data Analysis and Reporting using*
Different Log Management Tools" IJCSMC, Vol. 4, Issue. 7, July 2015, pg.224 – 229 pp. ISSN 2320–088X

[3]Harikrishnan V N, Gireesh Kumar T *"Advanced Persistent Threat Analysis using*
Splunk" Volume 118 No. 20 2018, 3761-3768

[4] Aron Warren *"Setting up Splunk for Event Correlation in Your Home Lab"* Accepted : SANS Institute Information Security Reading Room on November 19th 2013 ((GCIA) Gold Certification).

[5] Igino Corona, Giorgio Giacinto *"Detection of Server-side Web Attacks"* JMLR: Workshop and Conference Proceedings 11 (2010) 160–166.

[6] William Geiger *“Proactively Guarding Against Unknown Web Server Attacks”* Accepted: SANS Institute Information Security Reading Room on 2001.

[7] Kavita Agrawal, Hemant Makwana “*A Study on Critical Capabilities for Security Information and Event Management”* International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438.

[8] S.Padmaja , Dr.Ananthi Sheshasaayee “*Web Server Logs To Analyzing User Behavior Using Log Analyzer Tool*” International Journal of Advance Research In Science And Engineering http://www.ijarse.com IJARSE, Vol. No.3, Special Issue (01), September 2014 ISSN-2319-8354(E).

[9] Varsha R Mouli, KP Jevitha “*Web Services Attacks and Security- A Systematic Literature Review*” 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India.

[10] L.K. Joshila Grace, V.Maheswari, Dhinaharan Nagamalai “*Analysis Of Web Logs And Web User In Web Mining* ” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

Author’s Profile:

Mr. Krishna Badiger He is currently pursuing Bachelor of Computer Science from REVA University, Bengaluru since 2015. His areas of interest include Algorithms, Programming Languages such as C, C++, JAVA, Node js , Data Mining, IoT and Web Development.

Mrs. Shilpa NR holds M. Tech. Degree in Computer Science and Engineering from VTU. She has 2 years of industry and 5 years of teaching experience. Her areas of interest include C Programming and Data Structures, Database management system, Algorithms, System modeling and simulation. She is interested in pursuing research in the field of Wireless sensor networks. She has presented 6 technical papers at National and International conferences organized in various colleges.

Mr. VENU S N He is currently pursuing Bachelor of Computer Science from REVA University, Bengaluru since 2015. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT.