IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

A Comprehensive Review on Automated Visualization Techniques for Intrusion Detection Systems

Sujata. B[1], Priyanka. M[2], Anurag De[3]

PG Scholar, Dept of CSE, MVGRCE, Vizianagaram, India[1]

Assistant Professor, Dept of CSE, MVGRCE, Vizianagaram, India[2, 3]

Abstract: The Intrusion Detection Systems (IDS), applied with visual analysis has now become an advantage for intrusion detection. With more information systems being attacked and attack techniques evolving, the task of intrusion detections is becoming an increasingly difficult job in current scenario. Efficient information visualization is an important portion required for detection of intruders. In this paper a survey on using some of the visualization techniques in intrusion detection system is presented.

Keywords: Intrusion detection, Visualization, Statistical analysis, Real time monitoring.

I. INTRODUCTION

Intrusion detection (ID) is the process used to identify intrusions that is identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are exceeding their privileges. [1][2]

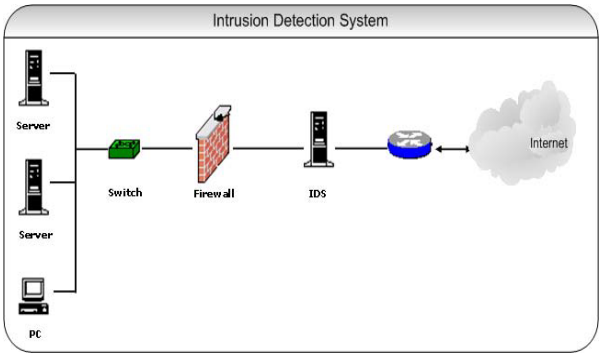

Figure 1: A Computer network and intrusion detection system

Figure 1 displays how a computer network can be incorporated with an IDS [9]. Intrusion Detection Systems (IDS) quests for specific pattern of attack signatures that normally indicate distrustful or mischievous content. IDS works like asecurity controlling tool for computer network administratorsto monitor systems/networks. According to previous surveys,it was proved that the quality of current IDS tools is poor for security administrators. There are two main complications in current IDS: detection techniques, and user interfaces (UIs) that enables the recognition and response by administrators to attacks. Applying better detection techniques can significantly improve the IDS performance. However, previous studies shows that users do not use advanced technical solutions which can fail if their user interfaces are not upgraded to the users. Large volumes of complex data can be seen and understood by people by using Visualization techniques. The ID investigation and reporting process are being assisted by the use of graphicsto help the analyst identify important occurrences and false conditions (positives, negatives and alarms) will get decreased. A broader level audience use Visualization in reporting incidents. In an easy to understand and persuasive manner, complex patterns can be clearly displayed.

Presently, the intrusion detection techniques areencouragingstudy on network security visualization toimportantly focus on alarm as its explorationentity, whereby the use of 2D/3D charts, alarms are examined and their measure and dissemination are represented. In this paper section II shows the various tools used for visualization techniques like Tudumi, a log information visualization system for intrusion detection and SnortView a visualization tool for log files and ELVIS a visualization tool for intrusion detection at the web level and CORGI. These are the various visualization technique tools adopted by the IDS to improve the performance and the comparison among them is also briefed in section III.

II. VISUALIZATION SYSTEMS

A. Tudumi: Log for Intrusion Detection by TetsujiTakada, Hideki koike, September 2000

Takada and Koike [3] proposed Tudumi, a log information visualization system for intrusion detection. Three kinds of log information is visualized here. When the information is visualized, contents are eternally understood by the users. Suspicious information can be cleared with the help of visualization information. As anoutcome, log information investigation task can be supported by

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

Tudumi. To get the access log informationtcp_wrapper and wtmpx log file and sulog log file were used to get user's login status and the replacement status.

Tudumiuses a stratified concentric disk mechanism. Here access host information is classified into numerous groups according to the rule based on its domain name and shows them on each layer andthis classification rule has to be defined by the system administrator.

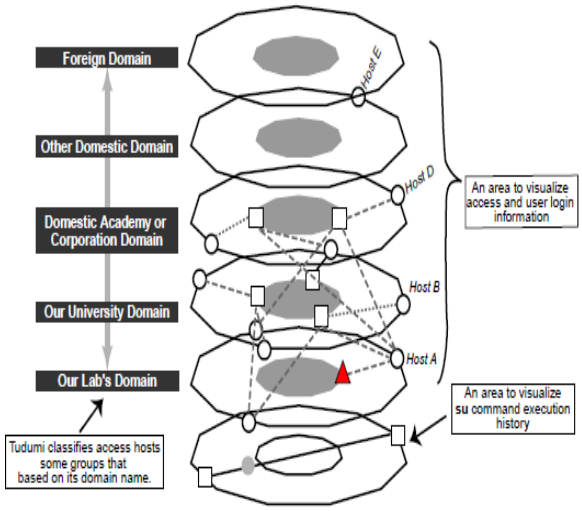

Figure 2: Visualization framework for Tudumi

Figure 2 shows the Visualization framework for Tudumi where Tudumi is incorporated with various disks at different levels so that the information related to IDS gets stored.

ADVANTAGES
1. This tool connects to a specific server in a 3-D visualization mode by taking several log files (e.g., syslog, sulog, wtmpx, etc.) as input
2. Inthe tool, stack of circles are used for displaying connecting hosts which are categorized by their network domain.
3. Investigative support by interactive operation.
4. Extraction of specific information by an object selection.
5. Display control of access hosts by summarizing domain names.
6. Display information control by specifying data span.

DISADVANTAGES
1. Real time monitoring capability is a major drawback.
2. The simple stack of circles cannot store large volumes of data.
3. Storing web data is not supported.

B. Meilog: A Highly Interactive Visual Log Browser using Information Visualization and Statistical Analysis by Takada and Koike, November 2002.

Takada and Koike [4] proposed In Mielog, some visualization techniques are utilized by an interactive log browser. Each log event in Meilog is visualized as a coloured line to obtain an intellectual view of the log.
Frequency of the word is calculated in each event message and the colours of the lines are also calculated.This tool also performs statistical analysisto observehow many logs are made in a unit time.

ADVANTAGES
1. Statistical analysis is performed to observe the number of logs formed in a unit time.
2. The NIDS logs can be monitored by using this tool.

DISADVANTAGES
1. The essential information in NIDS cannot be explicitly shown by Meilog, as for instance, source/destination IP, time, etc.

C. SnortView: Visualization System of Snort Logs by Koike and ohno, October 2004.
Koike and Ohno [5] proposed SnortView, a visualization system for NIDS logs where administrators can analyse NIDS alerts quickly and easily. Utilizing visualization,recognizeseach alert and performs false detectionsinstead of adapting signature DB.

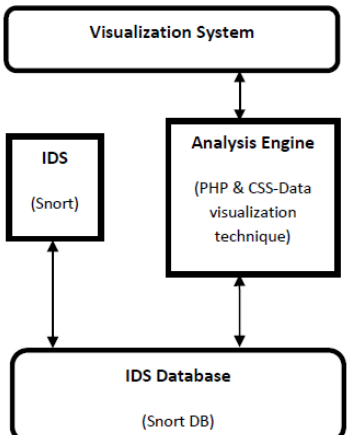

Figure 3: IDS with snort

In Figure 3[8], a visualization systems for Snort IDS [10] is shown where the visualization system uses the PHP-CSS data visualization technique.
The alerts in the systemare shownwith the help of a 2-D time diagram in the form of icons with assortedclasses and colors. The method alsopresents some of the visualization techniques like overplayed statistical information, source destination matrix, etc. Real attacks are also being detected by the system while identifying some false detections.

ADVANTAGES
1. Real-time monitoring capability by applying the information visualization technique.
2. By the ease of visualization, administrators find more benefitin false detection.
3. Statistical information used here thwarts the visualization from being flabbergasted by the series of the same attack.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

DISADVANTAGES
1. Alerts related to each packet header information and URLs are not displayed.
2. Unexpected code may be written in packet headers in the form of Dos attacks.
3. This visualization technique is utilized, so that the system can presently shows 40 attacks which are not in succession periods of time. The system might not visualize some sequence of attacks for which the events may differ depending on the environment.

D. ELVIS: Extensible Log VISualization by Humphries and Prigent, October 2013.

Humphries and Prigent [6] proposed ELVIS (Extensible Log VISualisation), through relevant representations this log visualization tool which is completely security oriented, allows security experts to visually discovermanykinds of log files. A summary view is displayed when ELVIS loads a log file. Thelog starts exploring at this particular view.Assured sets of fields from the dataset can be reconnoitered by the analyst. Pertinentdepictions are selected by ELVIS,conferring to the fields chosen by the expert for demonstration.

Security experts are allowed by ELVIS for importing log files with several formats (e.g, apache standard logs and syslog files such as authlog) and they arediscovered through appropriatedemonstrations that can be spontaneously selected and createdconferring to the displaying of theselected data. ELVIS consists of interaction process with two important stages where the required log files can be imported by the user through the techniques of Log acquisition and Summary view so that the resulting datasets are then inevitablydeveloped by the system and the summary visualizations can be displayed for each of the logs with the help of small multiples.

ADVANTAGES
1. Security experts will be benefited from sufficient visual representations of log files.
2. This is a versatile toolwhich can handle many types of log files and can beextensible in handling additional formats.
3. Users can explore data and can truly make use of each representation by adding, brushing and zooming.

DISADVANTAGES
1. Interacting with the summaries of dataset are the only source of depiction presently.
2. Isolation of each dataset or each log file is performed from the others and multiple datasets cannot be combined for analysisin the contemporary state.

E. CORGI: Combination, Organization and Reconstruction through Graphical Interactions by Humphries and Prigent, November 2014.

Humphries and Prigent [7], proposed CORGI (Combination, Organization and Reconstruction using Graphical Interactions). Security experts can visually investigate and relatemanysorts of log files through relevant depictions and over-all filteringby using thissecurity-oriented log visualization tool.CORGI is a web-based visualization tool

ADVANTAGES
1. Numerous categories of log files can be imported and visualizing their contents is allowed to the expert upon usage of this tool.
2. Exploiting various log file formats, and new log file formats can simply be added with the help of a direct and reliable description of log file formats.
3. An iterative process can also be implemented in CORGI by some techniques used in IT forensics so that any analyst for instancecan use the values of interest found in a given dataset to screen out events in other datasets, hencediscreetly relating these datasets.

DISADVANTAGES
1. This tool can only rely upon local files and handling abilities of browsers.

III. COMPARISON OFTOOLS

TABLE I COMPARISON OF TOOLS

Authors	Tool	Techniques used	Merits	Demerits
Takada and Koike	Tudumi [3]	tcp_wrapper, wtmpx log files, sulog log files.	3-D visualization, hosts categorized by network domain.	No real time monitoring capability.
Takada and Koike	Meilog [4]	Log Conversion, Frequency Information extraction, Visual representation and Interactive functions.	Statistical analysis of logs, observes NIDS logs	The essential information in NIDS is not shown explicitly, such as source/ destination IP, time, etc.
Koike and Ohno	SnortView[5]	Source address frame, Alert frame, Source-Destination Matrix frame.	Real time monitoring capability, false detection visualization.	Information related to header of each packet and URL alerts are not recognized.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

Humphries and Prigent	ELVIS [6]	Log file organization, log file acquisition, log file augmentation.	Adequate visual representations of log files, versatile in handling many types of log files.	Multiple datasets cannot be combined for exploration, lacks zooming and brushing facilities.
Humphries and Prigent	CORGI [7]	Importing logs, using time view panel, values of interest box.	Synchronized views, fast data cube type filtering, values of interest for filtering multiple logs.	Relies on local files

IV. CONCLUSION

IDS activities can be visualized with the help of various visualization techniques provided by the different tools, for the benefitof users or the administrators of the organizations. This paper presents a review on some of the visualization tools of IDS. The first among the discussed is the Tudumi where the IDS related data is stored in the disks however the visualization of IDS related data can be more easily stored and visualized with the help of GUI and web, hence vast data can also be provided with a provision to get stored. In that road map Meilog and SnortView came into the limelight where with the support of PHP and CSS visualization system was generated and then came the next web based visualization technique named ELVIS which helped to overcome some of the drawbacks in Snort and CORGI is the tool which found to be more efficient web based visualization tool for visualization of log information in IDS as compared in the previous section.

REFERENCES

[1] Elhenawy, I., Riad, A. E. D., Hassan, A., &Awadallah. N, "Visualization Techniques For Intrusion Detection- A Survey," International Journal of Computer Science and Engineering Survey(IJCSES), Vol.2, no.3, August 2011.

[2] Riad, A. E. D., Elhenawy, I., Hassan, A., &Awadallah.N, "Data visualization technique framework for intrusion detection," International Journal of Computer Science Issues (IJCSI), 8(5), September 2011.

[3] Koike, T. T. H. "Tudumi: Log Information Visualization System for Intrusion Detection," Technical Report (UEC-IS-TR-2000-08), September 2000.

[4] Tetsuji Takada, Hideki Koike, "Mielog: A Highly Interactive Visual Log Browser Using Information Visualization and Statistical Analysis," Proc. of LISA XVI Sixteenth Systems Administration Conference, The USENIX Association, pp.133–144, 2002.

[5] Koike, H., &Ohno, K. "SnortView: Visualization system of Snort logs," In Proceedings of the 2004, ACM workshop on Visualizationand data mining for computer security (pp. 143-147). ACM.'

[6] Humphries, C., Prigent, N., Bidan, C., &Majorczyk, F. "ElVIS: Extensible Log Visualization," In Proceedings of the Tenth Workshop on Visualization for Cyber Security (pp. 9-16). ACM, October 2013.

[7] Humphries, C., Prigent, N., Bidan, C., &Majorczyk, F. "CORGI: Combination, Organizationand Reconstruction through Graphical Interactions," In Proceedings of the Eleventh Workshop on Visualization for Cyber Security (pp. 57-64). ACM, November 2014.

[8] Snort – the de facto standard for intrusion detection/prevention. http://www.snort.org/.

[9] Amit Kumar Choudhary, Akhilesh Swaroop "Neural Network Approach for Intrusion Detection," ICIS 2009, November 24-26, 2009, Seoul, Korea.

[10] M. Roesch, Snort - Lightweight Intrusion Detection for Networks, Proc. of the 1999, USENIX LISA conference (1999).