ISSN: 2321-7782 (Online)
Volume 2, Issue 6, June 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Intrusion Detection System Using Data Mining

Sweta Vinay Kamat
Assistant Professor
Computer Engineering Department
Shree Rayeshwar Institute of Engineering and IT
Shiroda, Goa – India

Abstract: ***The purpose of Intrusion detection on server using data mining is to help network administrators using squid as their proxy server to free their networks from malicious activities effectively. It will relieve them from tedious task of monitoring huge logs and also save their time. This application will improve the ability of network administrators to understand the unauthorized events of logs and take necessary action.***

Keywords: Intrusion; IDS; Data Mining; Proxy; Squid; Network; Security; Detection System; IP Tables.

I. INTRODUCTION

Intrusion detection is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise your system and network resources. For a computer system attached to a network and perhaps even to the internet it is sensible to allow access to that computer system from the network only by authorised people. An unauthorised access to that system should not be allowed. A firewall or authentication system of some kind will be used to prevent unauthorised access. Sometimes, however, simple firewall or authentication systems can be cracked. Intrusion detection is the set of mechanisms which deals with unauthorised access to the computer. Intrusion detection systems should be able to take some steps to deny access to would-be intruders.

The goal of intrusion detection is to discover intrusions into a computer or network, by observing various network activities or attributes, given the explosive growth of the Internet and the increased availability of tools for attacking networks, intrusion detection becomes a critical component of network administration. While such detection usually includes some form of manual analysis, we focus on software systems for automating the analysis. The Existing system contains various tools for monitoring squid log files and analysing them. The analysers such as sawmill, squint calamaris, webalizer, squidalizer, squeezer, scalar and many more create reports based on information about Squid's internal performance and eficiency of relationship, finds bottlenecks, shows data transfer speed, most visited sites, sorting by hit count or by bytes count. The advantage of the proposed system over the existing system is to develop a system that provides misuse detection of intruders based on signature analysis. The proposed Intrusion Detection system will be running on the server as compared to Existing system shown in Fig 1.

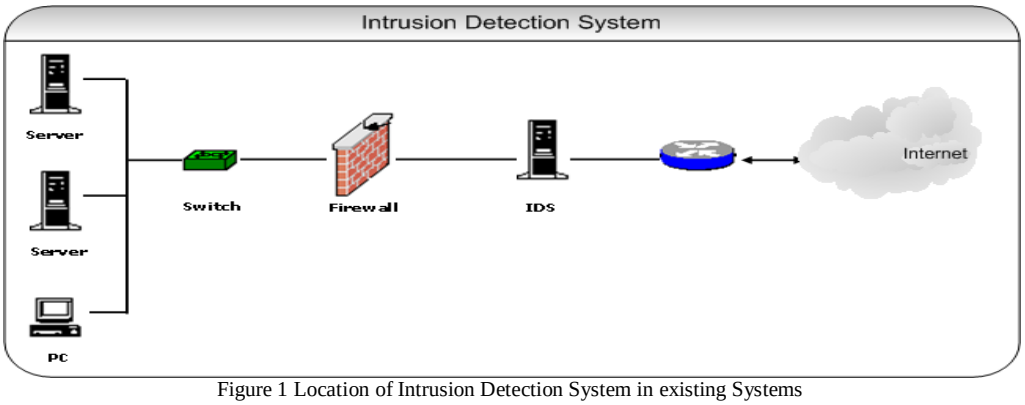

Figure 1 Location of Intrusion Detection System in existing Systems

II. System Architecture

The paper deals with the development of NIDS [9] to detect intruders on squid proxy server by log analysis using data mining.

This application will work as a combination of both misuse detection and anomaly detection methods.

The modules of the project are

- Pre-processing
- Log analysis
- Detection
- Blocking

Access.log file will be configured to display the required parameters. It will be analyzed for patterns that are logged as a result of intrusion. The detected intruder will be blocked using IP Tables rules which can be unblocked by the administrator.

Figure 2 depicts the block diagram of the System architecture of Intrusion Detection using Data Mining. The basic functions includes

- When the system is initiated the User Interface will be displayed to the user.
- The user clicks the Start button to start the application.
- The logs are preprocessed to get required features.
- Signature analysis is performed for analyzing logs.
- if an intruder is detected, its IP address will be blocked and logs will be refreshed.
- The blocked IP address of the intruder can be unblocked by the network administrator if not found malicious upon investigation

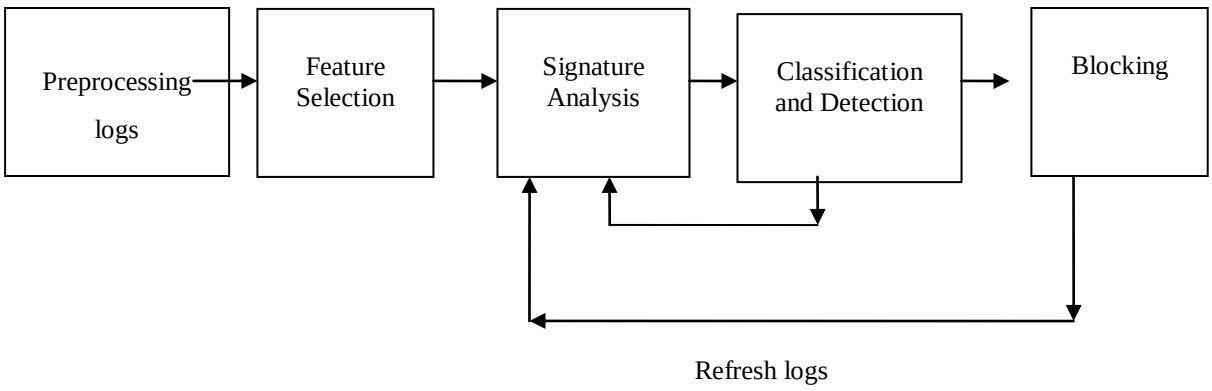

Figure 2 Architecture of Implemented IDS

A. *Preprocessing logs and Feature Selection*

The logs are a valuable source of information about Squid workloads and performance. The logs record not only access information, but also system configuration errors and resource consumption. There are several log file maintained by Squid.

cache.log - file contains the debug and error messages that Squid generates.

access.log - Most log file analysis program are based on the entries in this log

Intrusion detection system uses squid proxy logs stored in access.Log file. These logs need to be preprocessed to be in required format. The parameters required are kept and not required are deleted. The time and date of native log files in UTC format are changed to dd/mm/ss:hh:mm:ss format as shown if figure 3

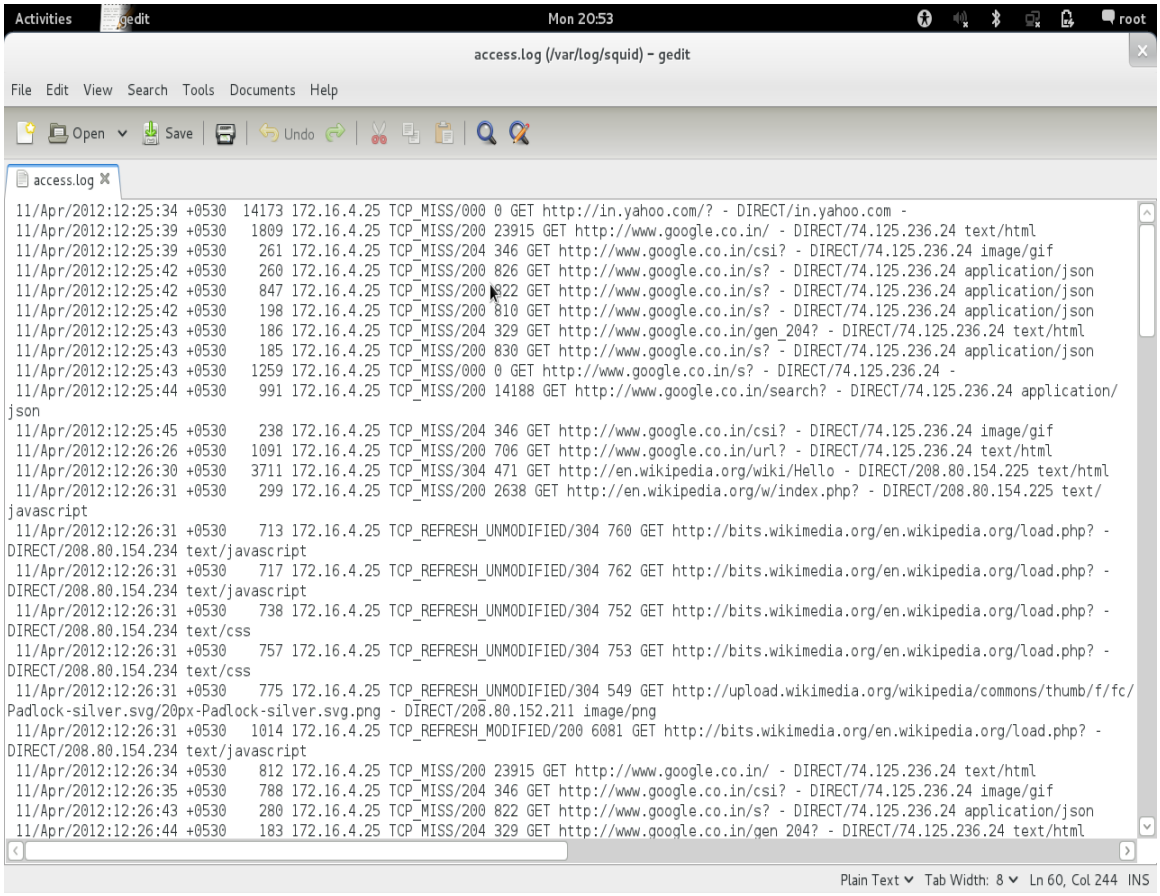

Figure 3 Squid Proxy Log file after preprocessing and feature selection

B. Signature Analysis

Intrusion detection system uses preprocessed squid proxy logs to detect the following types of attacks

- Detection of Internal users scanning or attacking outside systems

The logs are checked for multiple (5) 400 error codes from the same source ip within a small period of time(1 min). It ignores jpeg , png and gif extensions

- Detection of Internal users with worms, Trojans or virus.

The logs are checked for blst.php and xxx3.php combination in logs.

- Detection of Denial of Service attack.

The logs are checked fop the number of times a IP address has accessed the server. If an ip address has accessed server more than 60 times in a minute. The IP is considered as a intruder.

- Detection of Policy violations attack

The logs are checked for the IP address who is trying to access the prohibited pages. It checks for multiple errors from the same source ip. It checks for 401,403 and 407 error.

- Indication of an internal compromised system

The logs are checked for Multiple 500/600 error codes (server error).

- Detection of Proxy misuse or access violations

The logs are checked for same ip and TCP_DENIED and 403 error codes combinations.

- Detection of Invalid users in the network

The logs are checked for the user does not have valid credentials, a log will be generated. It checks for multiple authentication errors from the same source IP within a small period of time (1 min)

C. Classification and Detection

Intrusion detection system classifies the IP address into the categories mentioned in B based on the signature analysis and the corresponding IP address is detected as a intruder.

D. Blocking

In blocking phase if the IP address falls under any of the categories mentioned in B which is detected as a intruder then that IP address is blocked with the help Deny action of IP TABLES.

The system provides option for the network administrator to unblock a blocked IP address also by using the allow action of IP TABLES upon investigation if it is not found to be malicious.

III. IMPLEMENTATION RESULTS AND TESTING

The following are the Snapshots of the System upon implementation

A. Application User Interface on start up

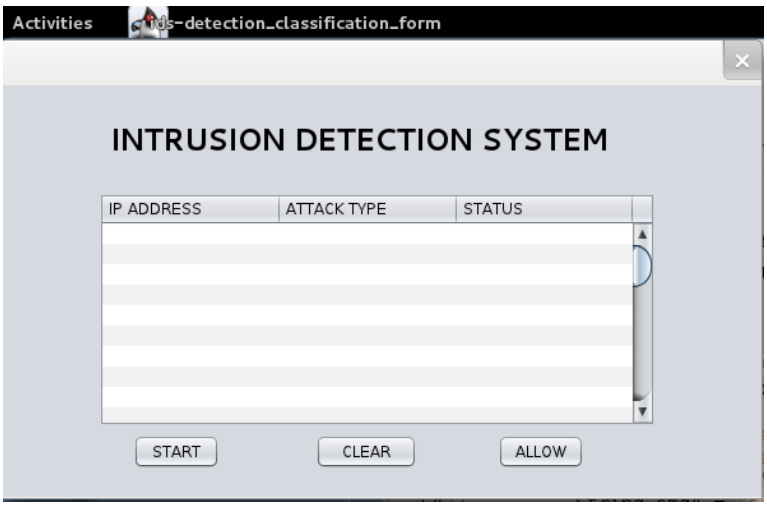

Figure 4 Application Interface

B. IP Address blocked after detected for Various attacks

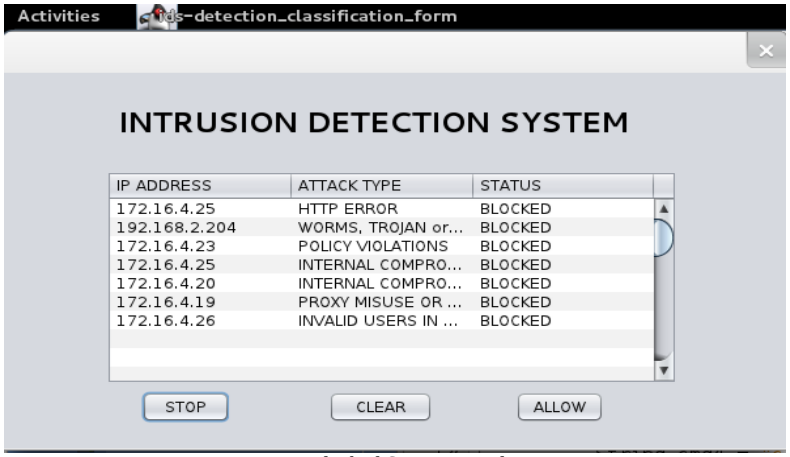

Figure 4 Blocked System Details

C. Unblocking of Ip Address by network administrator upon investigation

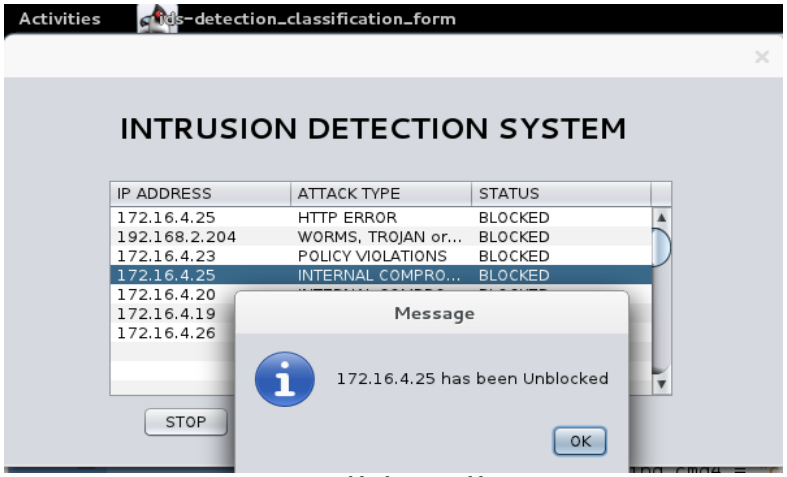

Fig. 5 Unblocking IP address

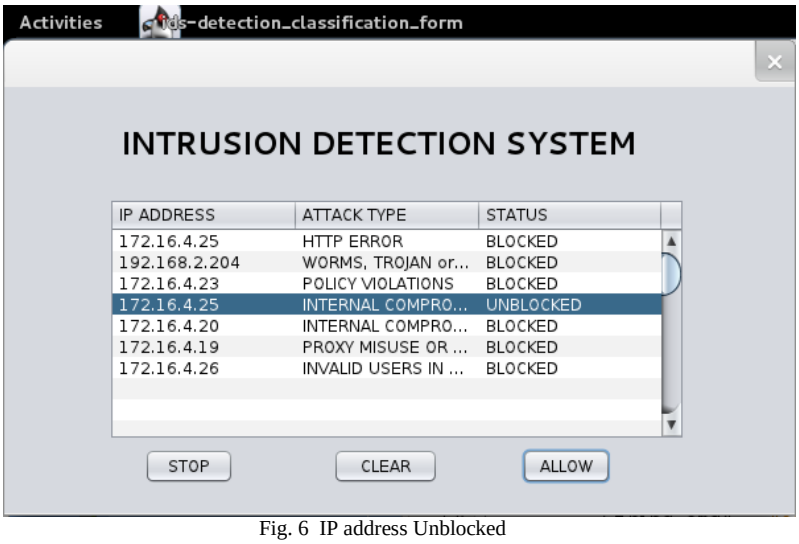

Fig. 6 IP address Unblocked

D. Testing

Testing is the most important part of any software application. The developed intrusion detection system was tested using different attack patterns and was found to be successful.

IV. CONCLUSION

A. Conclusion

The system described in this paper is to develop a system that uses intrusion Detection to help network administrator save time and stress caused in analyzing a log for detection of intruder from set of continuous generating logs.This application will improve the working environment of networks by reducing the number of intrusions caused in the network.

This Application System will help network administrators to

1. Detect the intruder based on log analysis
2. Inform the administrator
3. Block the intruder from accessing the network
4. The administrator can unblock the intruder.

B. Further Enhancements

- The System can be extended for different operating system proxy server.
- The reports based on various criteria's in the network analysis can be generated
- The detection module can be extended to detect some more different types of intrusions

References

1. MODERN INTRUSION DETECTION, DATA MINING, AND DEGREES OF ATTACK GUILT Steven Noel Center for Secure Information Systems George Mason University, Fairfax VA 22030-4444, USAsnoel@gmu.edu Duminda Wijesekera, Center for Secure Information Systems, George Mason University, Fairfax VA 22030-4444, USA dwijesek@gmu.edu Charles Youman Center for Secure Information Systems George Mason University, Fairfax VA 22030-4444, USA charles.youman@att.net
2. http://wiki.squid-cache.org/SquidFaq
3. A Data Mining Framework for Building Intrusion Detection Models_Wenke Lee Salvatore J. Stolfo Kui W. Mok Computer Science Department, Columbia University 500 West 120th Street, New York, NY 10027 {wenke,sal,mok}@cs.columbia.edu
4. An Automatically Tuning Intrusion Detection System Zhenwei Yu ; Tsai, J.J.P. ; Weigert, T. Volume: 37 , Issue: 2 Digital Object Identifier: 10.1109/TSMCB.2006.885306 Publication Year: 2007 , Page(s): 373 - 384 Cited by: Papers (11) | Patents (1) IEEE JOURNALS & MAGAZINES
5. Intrusion detection system based on systembehavior Tomasek, M. ; Cajkovsky, M. ; Mados, B. Applied Machine Intelligence and Informatics (SAMI), 2012 IEEE 10th International Symposium on Digital Object Identifier: 10.1109/SAMI.2012.6208971 Publication Year: 2012 , Page(s): 271 - 275
6. Development of host based intrusion detectionsystem for log files Bin Hamid Ali, F.A. ; Yee Yong Len Digital Object Identifier: 10.1109/ISBEIA.2011.6088821 Publication Year: 2011 , Page(s): 281 - 285
7. The Design and Implementation of Host-BasedIntrusion Detection System Lin Ying ; Zhang Yan ; Ou Yang-jia Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium on Digital Object Identifier: 10.1109/IITSI.2010.127 Publication Year: 2010 , Page(s): 595 - 598
8. Intrusion Detection System (A Layered Based Approach for Finding Attacks Kiran Dhangar Prof. Deepak Kulhare Arif Khan M.Tech Scholar,CSE Dept. Faculty CSE Dept. Faculty CSE Dept Indore, India. CIIT Indore, India. CIIT Indore, India.
9. http://www.whitehelm.com/intru-det.html
10. http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf
11. http://www.linofee.org/~jel/proxy/Squid/accesslog.shtml
12. http://devel.squid-cache.org/customlog/logformat.html
13. http://www.manageengine.co.in/products/firewall/squid-proxy-report.html
14. http://gofedora.com/how-to-configure-squid-proxy-server/

AUTHOR(S) PROFILE

Sweta Vinay Kamat is working as Assistant Professor in the department of Computer Engineering, Shree Rayeshwar institute of Engineering and IT, Goa University, Goa. She did M.E. in Internet Technology from Padre Conceicao college of engineering, Verna Goa University and B.E. in computer Engineering from Shree Rayeshwar institute of Engineering and IT, Goa University, Goa. India

