International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Intrusion Detection System with Automatic Forensic Data Acquisition and Firewall

Laimayum Bulbul Sharma[1], J. Dharani[2]

[1]Research Scholar, Information Security and Cyber Forensics, Department of Information Technology, SRM University, Chennai, India

[2]Assistant Professor, Department of Information Technology, SRM University, Chennai, India

Abstract: ***With the emerging of highly advance technology, risks in systems are also increases which even cannot be prevented by many security measures. Attacks in different form are being used to exploit the system through network. Intrusion Detection System (IDS) is used to detect the intrusion from such attack. IDS have certain limitation to detect and response in timely manner as well as to prevent the intrusion. On the other hand, IDS does not have the capability to capture the state of the system when an intrusion is detected Therefore it fails to preserve the evidences against the attack in original form and hence, digital evidence which is necessary in judicial proceedings for legal purpose cannot be produced in the court. The existing system used automatic digital forensic tool to capture the state of system when the intrusion occurs. But the damage control is yet to be considered. If the Alert log generated by IDS is altered tracking of intrusion will be fail. Our Primary aim is to focus on mitigation of damages done by an intrusion using firewall. We also used database to store the output log on another system to secure it.***

Keywords: Intrusion Detection System, barnyard2, Snortsam, Firewall Logs, mysql database, Snort Rule, Digital forensics

1. Introduction

In today's world many of us are dependent on Computer and Internet. All these technologies are evolving and are more vulnerable to threat as we use. Detection and prevention is one of the main security challenges that we should emphasize. With the introduction of many Intrusion detection technologies, we are able to detect and prevent the system and network from threat and intrusion but not up to greater extend. Also there are many security tool available such as Firewall, Antivirus, etc which cannot protect the computer and network from being exploit.

In this paper, we focus on analysing the security threat to the computer system. We used the Intrusion Detection system in order to detect any intrusion in the system and alert it if any intrusion encounter.

We also focus on preserving the evidence of the attack by mean of forensic method that we can prove in the court of law as the actual attack was occurred for legal purpose. This forensic method will give us the fine description of the intrusion that occurs in the system.

Intrusion detection system is broadly categories into two types i.e. Host based Intrusion Detection System and Network based Intrusion Detection System. Host based Intrusion Detection System is configured on a particular system or server. It focuses on constant monitoring and analysing the process and activities of the system where it is configured. HIDS will trigger an alert if it encounter or detect any intrusion in the system. Whereas Network Based Intrusion Detection System monitor and analyse the network traffic. If any attack such as Denial of service (DoS), port scans attack, etc is detected and trigger an alert.

In the existing paper, Intrusion detection system was used in order to detect an intrusion and trigger an alert which will invoke the forensic tool to capture the current state of the system. This forensic evidence will not only use for the proof of attack in the court of law but also it will give the brief description of the attack. However, it does not control the further destruction of the system resource. Therefore we proposed to use a Firewall to block the traffic that is responsible for an intrusion. We also used database to store the alert log so that it is secure and also sort out the source responsible for an intrusion.

2. Related Work

In Automated Digital Forensic Technique with Intrusion Detection Systems [1] it uses forensic tool to capture the image of both log and RAM when Snort (IDS) detects an intrusion. The system log is store in the log server in another system but it does not have the capability to prevent the damage done by an intrusion.

In Development of Host Based Intrusion Detection System for Log Files [2] it focuses on the development of host based intrusion detection system for Microsoft Windows XP environment. Method that applies is intrusion detection pattern matching technique on the Security Event Log File for Microsoft Windows XP. The intrusion had identified when there was matching of intrusion pattern that is create with Security Event Log in Microsoft Windows XP.

Host based IDS provide an extra protection to the host where it monitor more aspect of host such as monitoring file system integrity, host access, network packet that send to the host, System registry and system log file.

In Collaborative Intrusion Detection System Using Log Server and Neural Networks [3], it aimed to provide a secure way to the log files since they are very important for intrusion detection systems. KIT-I is the actual project which composed of two modules—

- **Transferring module**, in which Remote logging server (RLS) mechanism is used for transferring the log files to server from the clients at intervals. The SSL mechanisms of Java and certificate authority (CA) are adopted to establish an encrypted channel between the client and the server. Even if some clients are comprised, using KIT-I, we can get the backup data from the server.
- **NN module** which is used to find abnormal activities and give a notice to the administrator. Signature Based Intrusion Detection System Using SNORT [4] proposes the implementation process of Snort in Debian. This IDS System demonstrated that it can detect and analyze the intrusion in real time network traffic. Once the Snort will identify any intrusion then it will send alert to security person and security person will take required action immediately. To implement Signature based Intrusion detection System; we need to install some network security tools, such as Snort, BASE and TCP Replay. Snort is the IDS which will take the major role in detecting the intrusion.

3. Proposed Work

In proposed system, we used snort which can be downloaded from internet. We also used Snortsam which is the snort output plug-in responsible for the connection between the snort with any third party firewall in order to mitigate the damage done by the intruder by blocking the ip address and port responsible for an attack.

When an intrusion is detected, the IDS trigger an alert which is followed by Invoking of forensic tool to capture the system log image and RAM image and also the firewall. Output module takes the responsibility to invoke the forensic tool as well as firewall.

We also used mysql database [5] in order to store the alert output log. Barnyard2 [6] which is require for connection between snort and mysql database or any other database. Database output was supported in the older version of the snort but after snort 2.9.1 they remove the database output option. Therefore it is necessary to used barnyard2 for the connection between snort and mysql database.

Since we are going to implement in the windows 7, barnyard2 is not yet build for windows version. So we need to install cynwin which will compile any linux based application. Cynwin can be easily downloaded from the internet. We also used Dumpit which is the combination of win32dd and wind64dd for memory data acquisition.

Snort uses Rules which are written in simple language to detect intrusion. Intrusion are detected according to the rules define. Rule format are given below.

```
action protocol any any -> any any(rule option)
```

Figure 1: Snort rule format

According to the rules written, intrusion is going to be detected which includes signature for the past known attack.

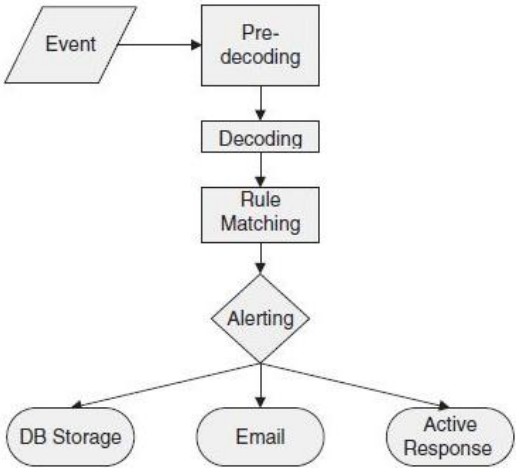

Figure 2: Simple flow chart

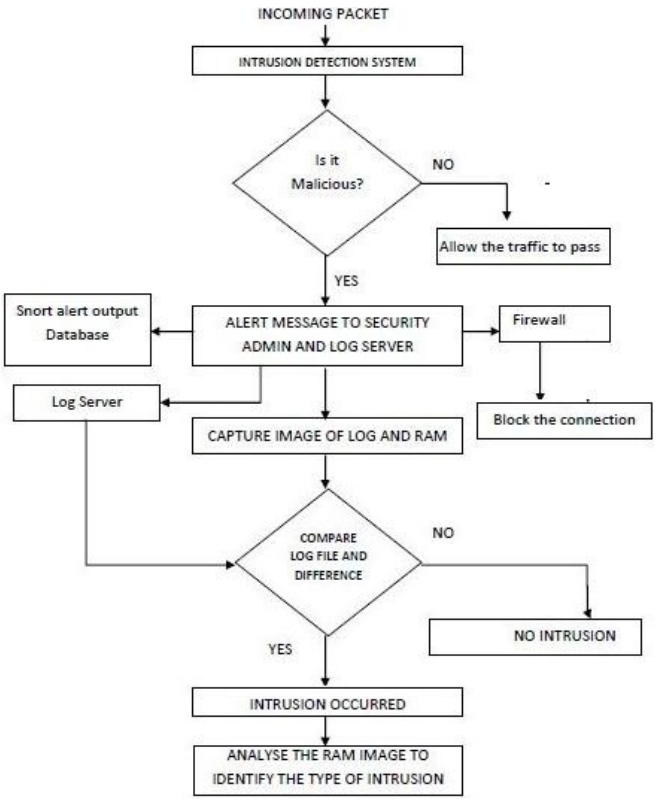

Figure 3: Flow chart for the proposed system

4. Experimental

We performed the demo experiment using one attack system and a target system and one remote system. We attack the target system by sending the malicious program or let's say a icmp ping which we set a rule to detect it as a malicious packet. The target system periodically takes log file image backup and store in the remote system. Once the snort in the target system triggers the alert, it the forensic tool in the target system captures the system log image and RAM image for the state of the system. Further the output module of the snort invokes the firewall present in the target system to close the connection responsible for the attack. It also sends the alert output log into the mysql database located in remote system. Using virtual machine environment, we create

Remote system to store the system log image as well as mysql database to store the snort alert output log.

5. Conclusion

The existing as well as the proposed system is designed to protect the system from any intrusion that will compromise the system information and security. Our main focus is to deploy security prevention mechanism in an easiest way yet very potential to prevent any intrusion.

References

[1] Komal Barhate, Jaidhar CD, "Automated Digital Forensic Technique with Intrusion Detection Systems", 2013 3rd IEEE International Advance Computing Conference (IACC), 978-1-4673-4529-3/12/$31.00_c 2012 IEEE.
[2] Firkhan Ali Bin Hamid Ali, Yee Yong Len, "Development of Host Based Intrusion DetectionSystem for Log Files", 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA), Langkawi, Malaysia, 978-1-4577-1549-5/11/$26.00 ©2011 IEEE
[3] Donghai Guan, Kejun Wang, Xiufen Ye and Weixing Feng, "A Collaborative Intrusion Detection System Using Log Server and Neural Networks", Proceedings of the IEEE International Conference on Mechatronics & Automation Niagara Falls, Canada • July 2005
[4] Vinod Kumar, Dr. Om Prakash Sangwan, "Signature Based Intrusion Detection System Using SNORT", International Journal of Computer Applications & Information Technology Vol. I, Issue III, November 2012
[5] http://dev.mysql.com/doc/refman/5.6/en/
[6] https://github.com/firnsy/barnyard2