Development of Host Based Intrusion Detection System for Log Files

Firkhan Ali Bin Hamid Ali
Faculty of Computer Science & Information Technology
Universiti Tun Hussein Onn Malaysia
Batu Pahat, Johor
firkhan@uthm.edu.my

Yee Yong Len
Faculty of Computer Science & Information Technology
Universiti Tun Hussein Onn Malaysia
Batu Pahat, Johor

***Abstract*— Nowadays, computer security has become important issue in many organizations in this world. There are many ways to handle this issue including by using Intrusion Detection System on the computer system. It takes the role as a detector for any intrusion that is occurring from the computer system. The study is to develop host based intrusion detection system for Microsoft Windows XP environment. Method that had used in the study was applying 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. The system is hoping to evolve into IDS that include any kind of intrusion detection technique in future.**

Keywords- Host based intrusion detection system; pattern matching technique; Security Event Lo; Windows XP.

I. INTRODUCTION

Nowadays, there is a lot of passive and active attack on the computer network system. As the Internet has rapidly grown year by year, there are more vulnerabilities and threats for hacker and malicious cracker to compromise network system especially through the Internet. One way to keep the computer network system in secure is implementing of an Intrusion Detection System or IDS.

IDS are a security system that detects intrusion made by malicious cracker whose intends to compromise a system. The system will alert the host or server if an intrusion is detecting. The intrusion may be stop by some mechanism to block the intrusion from a specific source. The basic activity of IDS is to monitor the network packet and system behavior. Then, it shows an alert if abnormal behavior of network packet or traffic is detecting. Intrusion detection has become an integral part of the information security process since it can implement and manage the identified information security controls [1].There are two types of approaches for IDS to make this an analysis.

First is a Signature-based detection method where the intrusion is detecting by using predefined rules or user defined rules. The rules will determine pattern of the packet that need to be detecting. If the packet patterns match with the defined pattern, the intrusion is occur. The collection of these signatures composes a knowledge base that use by the IDS to compare all packet options that pass by and check if they match a known pattern [2]. Misuse detection techniques in general are not effective against novel attacks that have no matched rules or patterns yet [3]. The advantage of this approach is, it can be use to detect well-known type of attacks. The disadvantage is, it difficult to detect a new attack pattern or modified attack which may by pass the system.

Second approach is anomaly detection method where the system will learn the normal and anomaly packet traffic and it detects intrusion on modified attack or unknown attack. This approach is required some artificial intelligence's element where the system can learn the normal pattern of the packet traffic and make detection on intrusion if the behavior of the packet is changed. The advantage of this approach is, it can be use to detect unknown attack. The disadvantage of this approach is, it is slow in detecting intrusion. The intrusion may have occurred more than one time after the IDS detect the intrusion. The disadvantage of this model is that network has produced all types of behavior in the IDS learning phase that hide from the user, so it may cause a high number of false-positive alerts [4].

There are few types of IDS such as Network IDS, Host-based IDS, Protocol-based IDS, and Application Protocol-based IDS. The study had focus in development of Host-based IDS. Host-based IDS is a type of IDS that is allocating on a specific host on the network. Its major benefit is the detection of intrusion is making to intended host or local host. 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.

Another scope in the study is, it focus on system log file monitoring where log file of host system are analyze from time to time to detect intrusion. The content of the log file will be compare to IDS rules or pattern that is predefined. File system monitor can check files on a large number of different characteristics such as permissions, anode, and number of links, owner/group, size, directory size, checksum, type, link, and active changing [5].

978-1-4577-1549-5/11/$26.00 ©2011 IEEE

II. METHODOLOGY

There are six phases, which had to go through in order to develop this system. The phases are System Analysis, System Design, System Development, System Implementation, System Testing and System Evaluation. For this project, only four phases had used to develop the system because of limitation of time and effort.

First phase is System Analysis phase, which is information according to the study, will gather as much as needed. Second phase is System Design phase, which is the Host-based IDS, had designed according to the study and requirement of the project. The user and system requirement for this project are specify and project had reanalyzed according to the needs of requirement. The interface and architecture of the system had designed. The system analysis and design had modeled by using structured method.

The third phase is the System Implementation phase, which is system, had implemented according to the design of system. Programming had done in this phase to transform the system from logical concept to a usable system by using Microsoft Visual Basic programming. The final phase is System Testing phase, which is system, had tested according to test case and the overall functionality of the system.

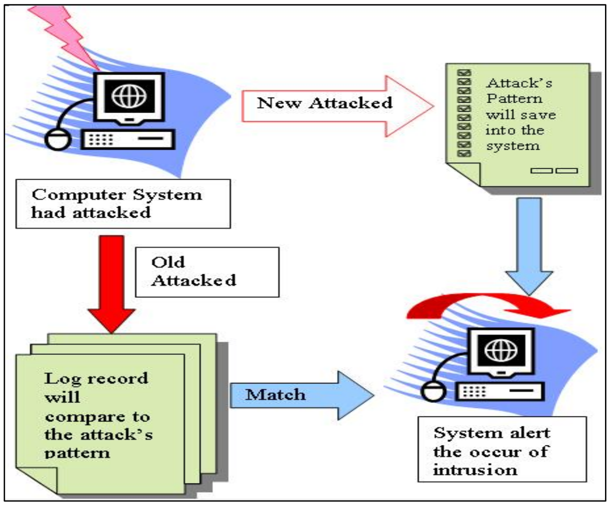

New Attacked
Attack's Pattern will save into the system
Computer System had attacked
Old Attacked
Log record will compare to the attack's pattern
Match
System alert the occur of intrusion

Figure 1. System Architecture

The system will recognize two types of attack and its pattern. If an attack is unknown pattern, the system needs to keep that pattern in the database for the future assessment. Then, if an attack knows pattern, the systems will match that pattern in their database and alert the host user about the attack or intrusion. Therefore, within that alert, user can take any possible action to react with the intrusion [6].

A context diagram in following Figure 2 is show how this system interacts with the end users to analysis log file in Windows XP and gets possible intrusion.

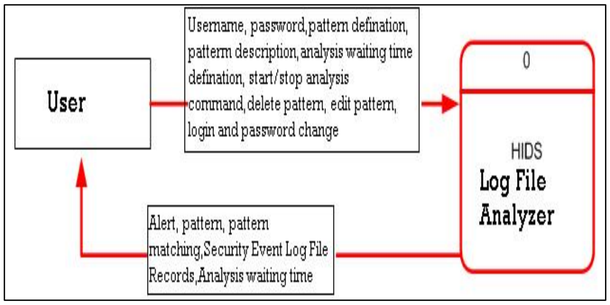

User
Username, password,pattern defination, pattern description, analysis waiting time defination, start/stop analysis command, delete pattern, edit pattern, login and password change
0
HIDS
Log File Analyzer
Alert, pattern, pattern matching,Security Event Log File Records,Analysis waiting time

Figure 2. Context Diagram

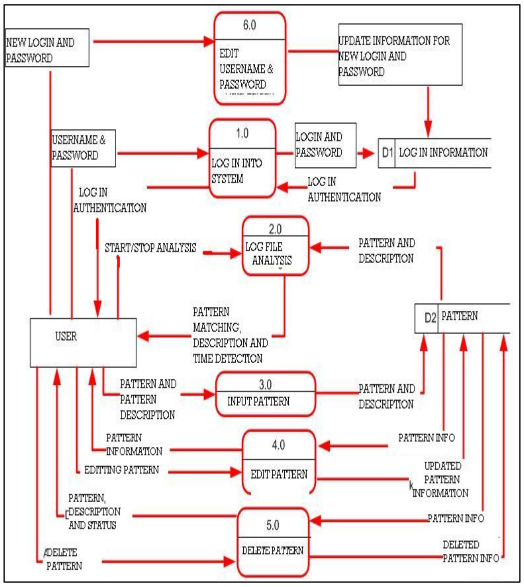


Figure 3. Diagram 0

In Figure 3 is show about Diagram 0 for the system. Diagram 0 will elaborate more details about the system's modules rather than in the Context Diagram.

III. IMPLEMENTATION

The focus for this IDS is about to make it detect intrusion through security log file that provided by Microsoft Windows XP operating system. Therefore, this section will discuss about the implementation and result for this study. Actually, it is about the modules and its processes.

TABLE 1. SYSTEM MODULES

Index	System's Module	Description
1	Log in	Log in into the system by using login and password
2	Log File Analysis	Analysis Event Log file
3	Pattern Input	Input pattern of intrusion
4	Pattern Edit	Edit pattern of intrusion.
5	Pattern Delete	Delete pattern of intrusion
6	Username and Password Edit	Change information of login and password.

There are six main modules reside in the system as stated in Table 1. In this system, firstly, users need to have an account of login and password. By using these login and password, user can access into the system.

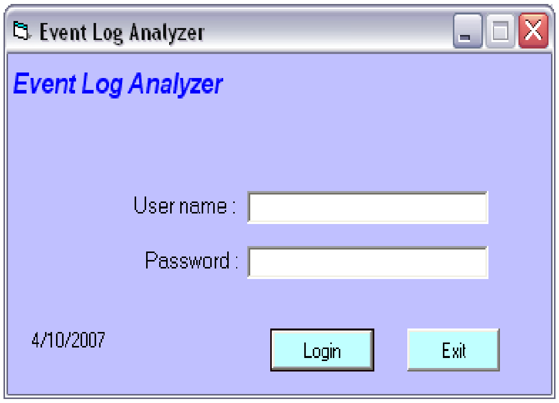


Figure 4. Login and Password Input for IDS Event Log Analyzer

A successful authentication will prompt the user main interface of this system within the five modules as state in Figure 5 below.

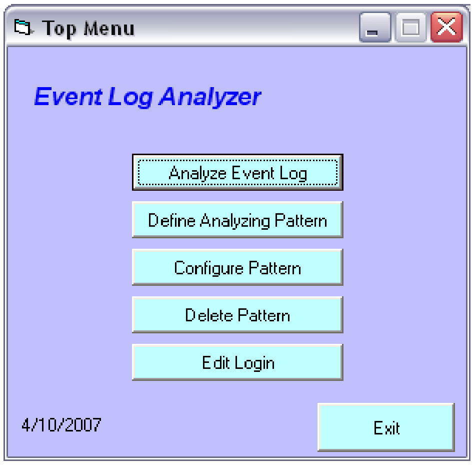
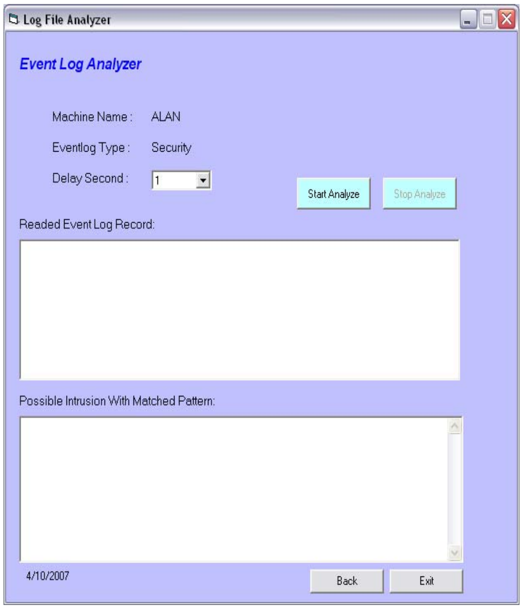


Figure 5. Main Menu

In Analyze Event Log, after click that button in the system, it will show to the user about login name, type of log file that need to be analyze and delay time in second to do analyze. Then, it have "*Start Analyze*" button that need to be click to begin the analyze process. Event log records for security had read that show in "*Readed Event Log Record*" and process matching with the intrusion pattern had done which had stated in "*Possible Intrusion with Matched Pattern*" button. It can refer to the Figure 6.



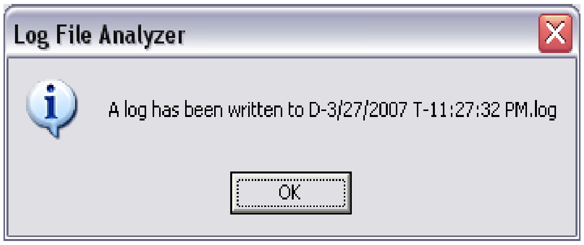
Machine Name : ALAN

Eventlog Type : Security

Delay Second : 1

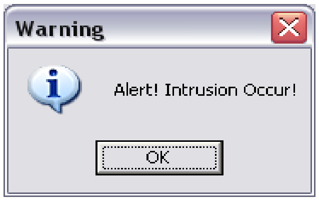
Figure 6. Analyze Event Log Module

Analyze process can be stop by clicking "*Stop Analyze*" button and one window will prompt to give a message that one log file had made according to the analyze process including the information of the time and date that the file had made as state in Figure 7. Then, if the system finds an intrusion or matching pattern, warning message is also prompt the user as state in Figure 8.



A log has been written to D-3/27/2007 T-11:27:32 PM.log

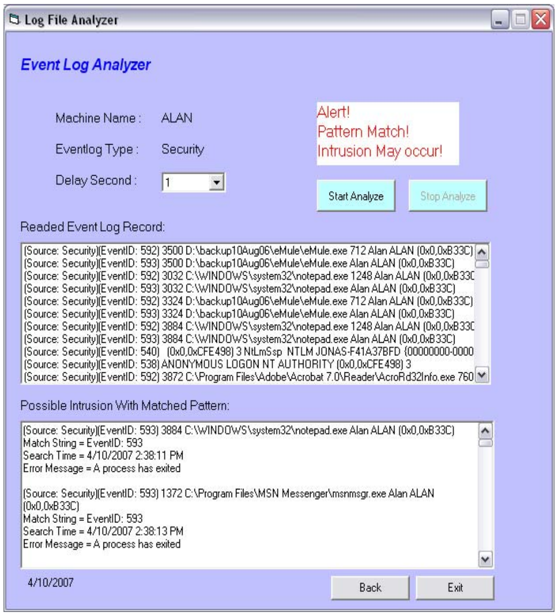
Figure7. File Information Message



Alert! Intrusion Occur!

Figure 8. Intrusion Warning Message

In the following Figure 9 is an example if the system had found a matching pattern of intrusion and will alert the user about that intrusion.


Log File Analyzer

Event Log Analyzer

Machine Name : ALAN

Eventlog Type : Security

Delay Second : 1

Alert!
Pattern Match!
Intrusion May occur!

Readed Event Log Record:

```
(Source: Security)(EventID: 592) 3500 D:\backup10Aug06\eMule\eMule.exe 712 Alan ALAN (0x0,0xB33C)
(Source: Security)(EventID: 593) 3500 D:\backup10Aug06\eMule\eMule.exe Alan ALAN (0x0,0xB33C)
(Source: Security)(EventID: 592) 3032 C:\WINDOWS\system32\notepad.exe 1248 Alan ALAN (0x0,0xB33C
(Source: Security)(EventID: 593) 3032 C:\WINDOWS\system32\notepad.exe Alan ALAN (0x0,0xB33C)
(Source: Security)(EventID: 592) 3324 D:\backup10Aug06\eMule\eMule.exe 712 Alan ALAN (0x0,0xB33C)
(Source: Security)(EventID: 593) 3324 D:\backup10Aug06\eMule\eMule.exe Alan ALAN (0x0,0xB33C)
(Source: Security)(EventID: 592) 3884 C:\WINDOWS\system32\notepad.exe 1248 Alan ALAN (0x0,0xB33C
(Source: Security)(EventID: 593) 3884 C:\WINDOWS\system32\notepad.exe Alan ALAN (0x0,0xB33C)
(Source: Security)(EventID: 540)   (0x0,0xCFE498) 3 NtLmSsp  NTLM JONAS-F41A37BFD {00000000-0000
(Source: Security)(EventID: 538) ANONYMOUS LOGON NT AUTHORITY (0x0,0xCFE498) 3
(Source: Security)(EventID: 592) 3872 C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32Info.exe 760
```

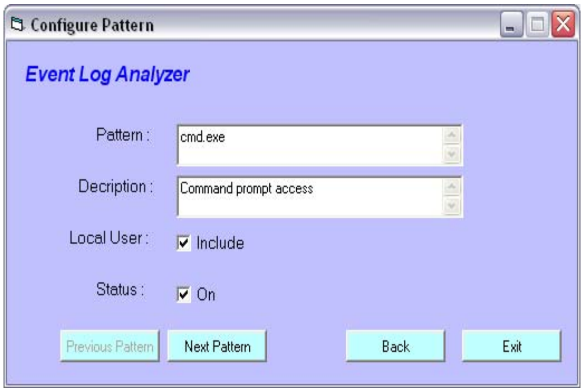
Possible Intrusion With Matched Pattern:

```
(Source: Security)(EventID: 593) 3884 C:\WINDOWS\system32\notepad.exe Alan ALAN (0x0,0xB33C)
Match String = EventID: 593
Search Time = 4/10/2007 2:38:11 PM
Error Message = A process has exited

(Source: Security)(EventID: 593) 1372 C:\Program Files\MSN Messenger\msnmsgr.exe Alan ALAN
(0x0,0xB33C)
Match String = EventID: 593
Search Time = 4/10/2007 2:38:13 PM
Error Message = A process has exited
```

4/10/2007

Figure 9. Pattern Matching


Configure Pattern

Event Log Analyzer

Pattern : cmd.exe

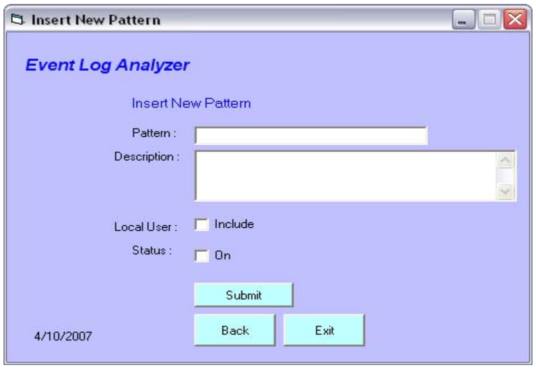
Decription : Command prompt access

Local User : ☑ Include

Status : ☑ On

Figure 10. Configure the Intrusion’s Patterns

In Figure 10, it shows about the function of the system to edit the status of each Intrusion pattern that keeps in the system. Then in Figure 11, it shows about the function of the system that can insert a new intrusion pattern inside the system.


Insert New Pattern

Event Log Analyzer

Insert New Pattern

Pattern :

Description :

Local User : □ Include

Status : □ On

4/10/2007

Figure 11. Insert New Intrusion’s Patterns

IV. CONCLUSION

This paper is about a developed a log file analyzer, which is able to detect intrusion and show an alert of intrusion to user through the system. The usage of the log files analyzer IDS is limited used to the host-based level.

The study had done by the system can read security event log files from Windows XP. Then, the system can make comparison for that file with the intrusion pattern files that reside inside the database. Therefore, if these two files had matching structure, the system will assume this file is an intrusion and give an alert to the user.

Security event log files from Windows XP are needed to be analyze by any system like log file analyzer IDS for security purposes in host or Computer. Then types or structure of intrusion pattern needs to be revising and update regularly.

The most important things are the organizations have a system to detect any threats in a computer host. It will support to prevent an organization from any threats [7].

Finally, the use of ICT facilities has a good support and budget from the high level of management in organizations. Therefore, it could be do to the implementation of digital security in organization to make the usage of ICT facilities secure, available and efficient [8].

ACKNOWLEDGMENT

Thanks to Universiti Tun Hussein Onn Malaysia, Malaysia on supporting this presentation.

REFERENCES

[1] Martin Botha et al., (2002), The Utilization of Artificial Intelligence in a Hybrid Intrusion Detection System, Proceedings of SAICSIT 2002.

[2] Pedro Bueno (2002), Intrusion Detection Systems, Linux Journal, Volume 2002, Issue 97 (May 2002), Specialized Systems Consultants, Inc.

[3] Wenke Lee et al., (2000), A Framework for Constructing Features and Models for Intrusion Detection Systems, ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue 4, ACM Press.

[4] Richard A. Kemmerer et al., (2002), Intrusion Detection: A Brief History and Overview, SECURITY & PRIVACY–2002, Reliable Software Group, Computer Science Department, University of California Santa Barbara.

[5] Boer P. et al., (2005), Host-based Intrusion Detection Systems, Revision1.10 – February 4, 2005, SNB student projects 2004 - 2005M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[6] Firkhan Ali, H. A etl., “Development of Vulnerability and Security Reporting System for Computer System and Networking” in SITIA 2008: Proceedings of the Seminar In The Intelligent Applications 2008, Surabaya, Indonesia, 2008.

[7] Firkhan Ali, H. A., “ An Analysis of Possible Exploits in the Computer Network’s Security “ in ISC 2005 : Proceedings of the International Science Congress 2005. PWTC, Kuala Lumpur, 2005. pp.338.

[8] Firkhan Ali, H. A., “Vulnerability Analysis on the Computer Network Security: Implementation and practices”, Lambert Academic Publishing, 2010.