REAL TIME WARNING SYSTEM DESIGN FOR WEB DEFACE BASED ON SHORT MESSAGE SERVICE

[1]ERI PRASETYO WIBOWO, [2]FITRAH ELLY FIRDAUS and [3]METTY MUSTIKASARI

[1]Assoc. Prof. , Department of Computer sciences, Gunadarma University, Indonesia

[2]Master Student, Information Technology, Gunadarma University, Indonesia

[3]Asstt. Prof., Department of Computer sciences, Gunadarma University, Indonesia

E-mail: eri@staff.gunadarma.ac.id, th3nux3r@firdauslinux.info, metty@staff.gunadarma.ac.id

ABSTRACT

Currently the internet is becoming more important in many aspects of human life. The number of people who use the internet in daily activities is also increasing. The rapid growing of computer networks and the interconnection among them has entailed some security problems. There are a growing number of bad-intentioned people trying to take advantage of the security problems. In the manner of existence problem, then needed a certain warning system which can prevent or give warning for crime possibility in the web. This paper proposes a system design to protect system from intruders and develop warning system via short messages service.

Keywords : *agent systems, short message service, warning system, intrusion detection System*

1. INTRODUCTION

Web defacement attacks alter the contents of web pages in an unauthorized manner with an intention to cause embarrassment, inconvenience and possible business loss to the website owner. They are a major challenge to the integrity of websites and attacks statistics are indeed astonishing: there are approximately 600 attacks in one hour [7]. Therefore organizations need to protect their systems from these intruders and consequently, new network security tools are being developed. The most widely used tool of this kind is Intrusion Detection Systems (IDSs). Intrusion detection systems have proved to be an effective instrument for protecting computer and network resources. They monitor the activity of the network with the purpose of identifying intrusive events and can take actions to abort these risky events. Currently, Intrusion Detection System only could give information about sniffing and intruder via website [2],[1],[8]. But for high secure, real time information is needed.

Cyber Crime can be detected by Intrusion Detection System such as using PHP Injection, SQL Injection, and Cross Side Scripting. Using Intrusion Detection Systems, systems still have some weaknesses. The weaknesses are the systems could not check property file and also they could not detect a problem before attack occurred. In this paper, we added is property of detection. This property is a checking property of file. This application system could also detect the hole before Web Server is cracked by cracker. In general, we developed warning system in real time base on short message service (SMS).

To check the system from cracker action used 3 methods. First, Wapiti was used to check any holes. From this holes report, an interface was made for time schedule checking and sending Short Messages Services. Second, Snort is used to detect an attack from cracker. From snort report, a script was made to update database LogNIDS, time schedule checking and sending Short Messages Services. Third, a script was made to check property of file. From this script a Time schedule was made for checking and sending Short Messages Services.

2. RESEARCH METHOD

2.1. Design System

2.1.1. Design Agent Architecture

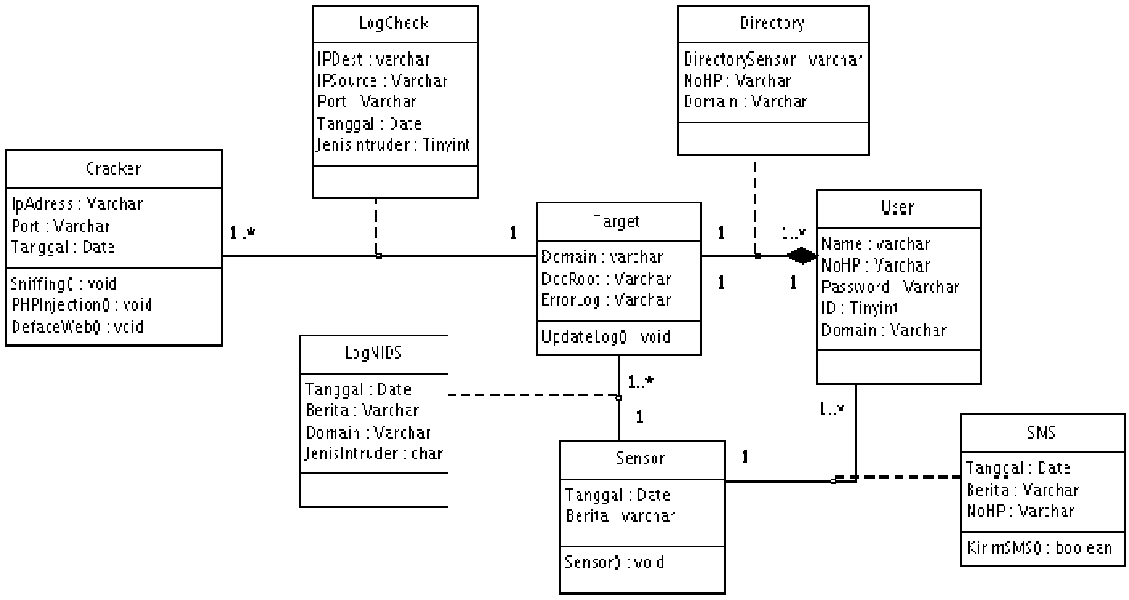

Figure 1. Data Model

In the following, we will present our approach for the development of system. The system that has been developed consists of two kind of agent: agent Sensor and agent target.

- Agent Sensor

Agent Sensor The Function of Agent Sensor[3],[6] is to check intruder via network, by checking log file. This agent can also check the holes as a hole for PHP Injection (The Method is used for crack website via try and error in URL Address), Mysql Injection (The Method is used for cracking website with input the SQL Script in URL Address) and Cross Site Scripting (The Method is used for crack website with remote target from cracker machine via URL Address). If the agent found an intruding, sensor Machine will send Short Messages Services to Person who has domain and update Database.

- Agent Target

Agent Target The Function of Agent Target is to check file in target machine. If the file has been modified, the Target machine will send a Short Messages Service to person who has domain.

2.1.2. Design Data Model

To design the data model system, we use an object oriented approach. This approach has several advantages. This model enriched modeling capabilities. In addition it allows new abstract data types to be built from existing types. The model data also enforce serializability on concurrent transactions to maintain database consistency. Object oriented data model allows the real world to be modeled more closely.

Class Diagram that shown in the figure 1, has 4 entity classes. They are Cracker, Target, User and Sensor. The Association Classes have been developed are LogNIDS, Directory, LogCheck and SMS. Class Cracker contains 3 attributes, such as IpAddress with var-char data type, Port with varchar data type, and date with date data type. Some of methods from Class Target are Domain, ErrorLog and DocRoot with varchar data type. Class Target involves Update-Log. Class Sensor contains two attributes. They are date with date data type, and News with varchar data type. This class have 1 method is Sensor. Class User contains Name and No-HP with Var-char data-type. This data model has 4 association classes. Class Log-NIDS contains Domain, Ip-

Address and Port with varchar datatype and Date with date data-type. This Class is made from relationship between class Craker and class Target. Multiplicity of this relationship is 1...* to 1. Class Directory has 3 attributes. They are Directory-Sensor, NoHP and Domain with varchar datatype. This class is made from relationship between class Target and User. Multiplicity of this relationship is 1 to 1...* with composite aggregation. Class LogCheck has 4 attributes. They are Date with date datatype, News and Domain with varchar datatype, and IntruderType with char datatype. This Class is made from relationship between Class Target and Class Sensor. Multiplicity of this relationship is 1...* to 1. Class SMS consist 3 attributes, such as Date with Date datatype, News and NoHP with varchar datatype. Class SMS has 1 Method that is Send SMS. This Class is made from relationship between class User and Sensor. Multiplicity of this relationship is 1...* to 1.

2.2. Implentation System

2.2.1. Snort Detection System

This system was used to detecting sniffing and intruding. For this detection, we used *Snort Network Intrusion Detection System.* The Snort did not have an interface to send *Short Messages Services* [4]. For this reason, we made Script with PHP for connecting Snort and Short Message Services System. This script would check /var/log/snort/snort.log file. The Cyber crime can be detected by Snort such as using WEB-PHP Remote, XSS, Etc. Script algorithm was a script read file which is exploded by space and its input into array. Array has input wich would read. Information need is first row and third row from each part. First Row refers to type of crime and third row refer to time, IP Address source and IP Adress destination. In third row, we need exploded line by space. Array zero refer time of crime, array first refer IP Address Cracker and IP Address target. After we get all information, script will update database and sending Short Messages Service.

2.2.2. Early Warning System

The warning system is used to detect any domain before the domain is intruded by cracker. For this detection, we used Wapiti. The Phase of building of this script is running wapiti then reading the output file from Wapiti. Output file from Wapiti has 2 parts, GET part and POST part. In order to read the output file, the program reads zeroth array from each row. This array contains the crime that may be occurred in the web server. The Zeroth array may contain XSS (Cross Site Scripting) which indicates that a secure hole is a cross side scripting crime. Usually the hole is located in GET method, while in POST method the array contains FOUND. Warning that refers to secure hole which is a PHP injection usually is located in POST method, while in GET method , the array contains 500. MySQL indicates that the secure hole is an SQL injection crime. After the script gets the zeroth array, it will examine the next array. If the zeroth array contains XSS, the script will check the sixth array. The array contains the intrusion way of CSS. If the zeroth array contains Found or waning, the script then checks the third and the seventh array, then combines the third and the seventh array in order to get the way of intrusion. If the zeroth array contains 500, then the script checks the seventh array to get the way of intrusion.

Furthermore the script will be connected to database server in order to update a report if the report is available. The script will create a report if it is not available in server database.

After the report is executed, the script will send a short message of the secure hole in each category to the owner of domain. The message is not sent in intrusion way because it needs many short messages processing. In order to show the detail of the intrusion way, owner of domain can access web-based page report.

2.2.3. Web Deface Detection System

This system is used to detect a web deface attack. The way of detection is by reading a file property then time of modication of the le is examined. If the hour of modication is in the range of checking, then the program will give a warning via short message service to the owner of domain. First, the program is connected to the database server, then it takes all of directory that will be censored using query. Next, the program takes the hour that is available in target machine. After that the program checks all the file in the directory.

If the file has been checked has a php or html extension, then the program takes the time modication property of that file. The time

modication property is in unix format. Therefore the program should change the format to the form that will be understood. Then the modication time can be analyzed.

Furthermore, the year, month and day are analyzed. If the file property is the same as the year, month, and day of the target machine, then the program will check further the hour and minutes. If the difference of hour in that property and hour at that time is equal to zero, then the program will count the difference of minutes. If the difference of minutes is less than or equal to ve then the program will give instruction to Short Message service machine to send short Message service warning to the user. If the difference of hour of that property and hour at that time is equal to one and the difference of minutes is -59 or less than or equal to -55 then the program will give instruction to Short Message service machine to send short message service warning to the user.

2.2.4. Short Message Services System

As already mentioned earlier, we use a system design to protect system from intruders and develop warning system via short message service. This system sends short mes sages services to the owner of domain, if the system gets crime or holes. This script receives input from Hand Phone Number and messages that will be sent. To send short mes sages services, Gammu is used as SMS Gateway.

2.3. Testing

The system has been tested using Virtual Machine, 1 host computer for SMS Gateway, and 4 Guest Computer for Target machine, Sensor Machine, Admin Machine and Cracker Machine. Web Application is used for testing the system is sisfokampus made in Indonesia. This application is used for campus information system. URL address of web application is http://www.sisfokampus.net. Mechanism of testing is cracker machine which is connected to virtual machine with NAT (Network Address Translation, but System connected in Host Only Network ing. Cracker Machine can intrude into target machine with WEB-REMOTE PHP, Cross Side Scripting, and Snifng in SSH (Secure Shell) or FTP Port. Sensor Machine runs a Warning system in order to check any holes, then runs Snortand Warning Web Deface System in order to check the target machine from cracker action.

3. RESULTS

3.1. Short Message Service

As already mentioned earlier, we use a system design to protect system from intruders and develop warning system via short message service. The following is some examples of short message services. Some of short message services will send to a person who has domain such as the following :

• Short Message Service From Snort Detection If Snort Detects an intruding, The system will send a Short Message Service to a person who has Domain. The message is ”Domain target.info are Cracked with WEB-REMOTE PHP from IP 70.86.29.178”.

• Short Messages Services From warning System This Short Message Services will Send to a Person who has Domain, If System detect holes. The message is ”Domain target.info have hole. There are Cross Side Scripting 54 holes, PHP injection 756 holes, MySQL Injection 88 holes”.

• Short Message Services From Warning Web Deface System This Short Message Services will be Send to a Person who ha Domain, if Warning Web Deface System de tect a file that has been modied. The message is ”File test.php in domain target.info has been modied from IP 70.86.29.178”

3.2. Graphics

Web application is used for testing the system is sisfokampus version 3.2, The result can be seen as follow.

3.2.1. Snort

Figure 2 shows a graphic snort. This graphic is generated by intruder has sensor report during 1 month. Graphic is shown in the figure 2 has 2 bars. Blue bar is illustrated for WEB-PHP Remote (Method for crack website with remote target from cracker machine via SSH Port) and orange bar is illustrated for cross side scripting. This graphic refers to amount of cracker act in month. In the experiment, done WEB PHP

Remote as 5 times and system can detect 3 times. For Cross Side Scripting, experiment is done 3 times but system detected 1 time. The system can not detect all of cracker because in the experiment used virtual machine where one CPU divided to five machine, so detection is not optimal. This Snort Inspection used Sensor_intruder.php script.

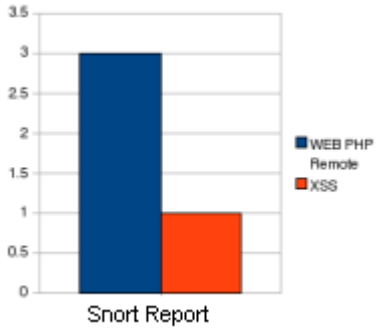

Figure 2. Graphics of Snort

3.2.2. Warning System

Figure 3 illustrates a graphic of warning system. This graphic is not generated by time, but this graphic generate report from checking hole. The system used script of Sensor_Inject.php to inspection. Graphic is seen in the figure 3 has 3 bars. Yellow bar is illustrated for cross site scripting, Orange bar for PHP Injection, Blue bar is illustrated for MySQL Injection. This graphic refers to amount of each hole.

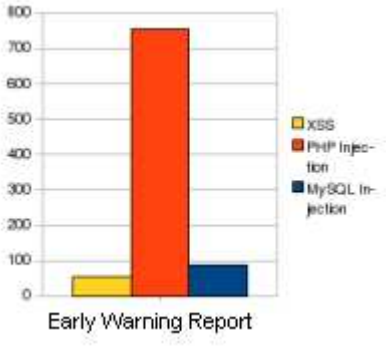

Figure 3. Graphic of Warning System

3.2.3. Warning Web Deface System

Figure 4 shows a graphic of web deface system. This Graphic is generated from Warning Web Deface System in 1 month. Graphic is shown in the figure 4 has 1 bar. This bar refers to amount of Web Defacing act. During 1 month experiment , System can detect 2 web deface of 2 web deface testing. System used a script of Sensor_Deface.php to inspection.

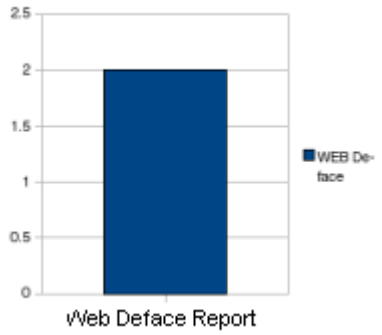

Figure 4. Graphic of Web Deface System

4. CONCLUSIONS AND PERSPECTIVES

This system is proposed to help administrator web server and person who has a domain to guard website from cracker. As Warning systems used is short Messages Service, web server administrator or person who has domain can quickly response an attack. In addition this system can detect holes before the system attacked by cracker. This system can also detect a file which has been modifed, not only Directory Index but also other files in web server. Eventhough the system has been developed successfully, but this system should be increased their performance.

There are two perspectives for developing this system. The first one is this System should be developed in distributed systems. Distributed system can accommodate web server requirement, therefore system performance would be improved.

The second, administrator page should be developed with Advanced Java Servlet using MVC (Model View Controller) framework such as Spring, Using security Frame work such as Spring Security would improve the level of security of the system.

REFERENCES:

[1] D.Liesen. Requirements for Enterprise-Wide Scaling Intrusion Detection Products. 2002.

[2] J.Denton. Slackware snort installation guide. http://www.cochiselinux.org/?les/slackware-snort-0.2.txt, 2007.

[3] ----------. Object Oriented : An agent based system for identifying and refining objects from software requirements based on object based formal specification, February 2003.

[4] T. S. Team, Snort Users Manual. Home page : http://snort.org, March 2008.

[5] R. S. Wahono, Intelligent agents for object model creation process in object oriented analysis and design, Thesis, Department of Information and Computer Sciences Graduate School of Science and Engineering Saitama University, Jepang, 2001.

[6] R.S. Wahonno. *Pengantar software Agent: Teori dan Aplikasi,* proceedings of the IECI Japan Workshop. Tokyo 2001. 3.1.

[7] Karsten Bsufka, Olaf Kroll-Peters and Sahin Albayrak. Intelligent network-Based Early Warning Systems. *Lecture Notes in Computer Sciences Springer*. *2006*: Vol. (4347/2006):103-111.

[8] Arjita Ghost and Sandip Sen. Agent-Based Distributed Intrusion Alert System. *Lecture Notes in Computer Sciences Springer*. *2005*: Vol.(3326/2005):7-47.

[9] Mariana Hentea. Intelligent System for Information Security management: Architecture and Design Issues. *Informing Sciences and Information Technology*. 2007: Vol(4):29-43.