IJID International Journal on Informatics for Development, *e-ISSN :2549-7448*
Vol. 6, No. 2, 2017, Pp. 21-27

Design and Implementation of Network Monitoring System on Local Area Network with Social Media Twitter Notification

Bima Putra Winasis[1], Bambang Sugiantoro[2]
Department of Informatics
Faculty of Science and Technology
UIN Sunan Kalijaga Yogyakarta
Yogyakarta, Indonesia
Bambang.sugiantoro@uin-suka.ac.id[2]

***Abstract*—A network administrator has responsibility and important role in a computer network. Network security and its services depend on the treatment performed by the administrator. Network administrators who understand the workings of a computer network is needed to obtain the necessary computer networks. One of the obligations of the administrator is to monitor a network which can be done by using the system monitor. Monitoring system is a task to check the computer, operating system and services of computer network to keep the network always work in optimal conditions. In an effort to monitor the condition of the network, one of the technologies that can be used is the notification on twitter social media for providing information in real time to the administrator. Twitter is a social media that is very widely used, free, and secure. Moreover, the use of social media twitter experiencing rapid development. Therefore, the selection of twitter as a medium for the use of the notification is expected to be the right strategy. This system will be made by sending notification via twitter when a LAN network is disconnected or attacked by intruders.**

Results from the development of systems that have been made based on testing the functionality of the system shows all functions of the system has been running well. While usability testing calculation of the total score of the test system interface to get a score of 38.75 out of a maximum scale of 50. This score is in the range 34-42 value (Satisfied) which means that the respondents were satisfied with the system interface. Therefore, this interface is good to be implemented in the system.

Keywords-Local Area Network Monitoring System; IDS Twitter; LAN Monitoring Twitter

I. INTRODUCTION

Computer Networks are a group of autonomous computers that are connected to one another by using communication protocols through ata media communication media so that the presence of these protocols allows sharing of data or information, applications, and can even share hardware such as printers, hard drives, etc. (Oetomo, 2004). In a network of computers connected two or more computers that can communicate with each other and the computer - the computer is connected to one or several servers, in other words there is a function as a client and some that function as servers. The server is a computer that is functioned to serve delivery, serve reception of data, and regulate how to send and receive data between computers that are connected. (Wahana Komputer, 2003).

A network monitoring system that will be created will be used by the administrator to monitor the condition of the network. The first time an administrator has to do is enter his data as an administrator who is responsible for his computer network. In addition, administrators are required to have a Twitter account because the administrator also has to enter a username from a twitter account to get notifications via the application. Network monitoring system LAN (Local Area Network) with notifications on social media Twitter is a system used in monitoring networks that can provide network conditions information to administrators effectively and efficiently. The system is created on a computer with the Ubuntu 12.04 operating system with the Luna distro. As for IDS (Intrusion Detection System), the application used is snort. Snort is an IDS tool that uses a signature detection pattern. The selection of snort as an IDS (Intrusion Detection System) is done because snort has integration with the MySQL database making it easier to access the snort database.

II. PURPOSE

One of the obligations of the administrator is to monitor the network. The description of the monitor system is the task of checking computers, operating systems and services that exist on a network so that they always work at optimal conditions. In conducting an examination, a network administrator must maintain the stability of the system and if possible, he must also try to improve the performance of the network being handled (Wahana Komputer, 2005). Network administrators are required to be able to monitor the network from various possible attacks. Common types of attacks on the network include Port Scanning and DoS (Denial of Service). Port Scanning is needed to identify which ports are open, and recognize the target OS and DoS are used to spend resources from the target so that other users cannot gain access from the target computer (Rafiudin, 2009). In the case of LAN networks, common and frequent attacks include spoofing, port scanning, Sniffing, and Backdoor. While DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks are more common in large networks such as WAN (Wide Area Network). If these attacks occur, a system that can detect accurately and can identify specifications of the attack on the network is required and then give a warning to the network administrator.

III. METHODOLOGY

Stages - stages of research are determined to meet the research objectives to be achieved. The research stages used in this study are as follows :

A. *Literature Study Phase*

At this stage researchers conduct reference searches related to the research topics raised. References needed in research include sources related to computer networks and types of attacks on computer networks, network monitoring systems
on LANs (Local Area Networks), network intrusion detection systems, systems that can determine the condition of hosts in the network, and study Twitter API. In addition, researchers also studied the process of creating areport host conditionon the network and creating an intrusion detection report via Twitter social media.

B. *System Development Phase*

In the development phase of the development of this system using the System Development Life Cycle with the Waterfall method. System Development Life Cycle is a process of making and changing systems and models and methodologies for the process of making and changing systems and models and methodologies for creating and developing systems. To implement the method through the following stages (Pressman, 2005):

- Needs Analysis
  In this stage the researcher collects complete needs. Then analyzed and defined what needs are needed in the system. In this stage also analyzed the functionality of the system to be built to find out the importance of this system being built.
- Design
  At this stage the researcher designs the model for the parts of the system to be built. The parts of the system that will be built include:

1. *Ping host system*
2. *Intrusion detection system*

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. See for details: https://creativecommons.org/licenses/by-nc-nd/4.0/

3. GUI (*Graphical User Interface*) *monitoring system*
4. *Reporting system* through API Twitter

- Implementation

  At this stage the system models that have been designed at the stage design will be made. The system components that will be created include the ping host system to find out whether the host is up or down, the Intruder Detection System to find out if the network is being infiltrated, the reporting system via the Twitter API to provide information via a twitter administrator account. In this stage also created functions - functions that support the use of network monitoring systems.

- Testing

  In this stage the system that has been built will be tested. Testing is done to find out if the system is in accordance with the expected based on the needs and whether it has fulfilled the function

  1. Alpha Testing
  2. Beta Testing

- Maintenance

  System maintenance is done by repairing errors and gaps in the system and making adjustments to the system in the event of unplanned changes.

IV. SYSTEM ANALYSIS AND DESIGN

Analysis is the process of deciphering concepts into simpler parts with the aim of identifying and evaluating problems, so that solutions and logical structures become clear (Fatta, 2013). Problem analysis at this stage is to describe the problems that have been explained previously. At this stage the researcher conducts an analysis to find out the system needs that will be used at the system design and implementation stage. These needs include the use of software and the use of hardware. This system analysis activity is carried out so that the system can function optimally without any constraints related to the devices used by the system to meet the purpose of the system. With the analysis of system requirements, it is expected that the system can monitor the LAN (*Local Area Networknetwork*) optimally and send monitoring notifications to Twitter social media.

A. Systen Description

Network monitoring system that will be created will be used by the administrator to monitor the condition of the network. The first time an administrator has to do is enter his data as an administrator who is responsible for his computer network. In addition, administrators are required to have a Twitter account because the administrator also has to enter a username from a twitter account to get notifications via the application.

B. Designing System

Monitoring System for a LAN (Local Area Network) network with notifications on social media Twitter is a system used in monitoring networks that can provide administrators with information on network conditions effectively and efficiently. The system is created on a computer with the Ubuntu 12.04 operating system with the Luna distro. As for IDS (Intrusion Detection System), the application used is snort. Snort is an IDS tool that uses a signature detection pattern. Any interruption or attack that occurs is identified with the appropriate rule and then given a signatuture on the attack. The selection of snort as an IDS (Intrusion Detection System) is done because snort has integration with the MySQL database making it easier to access the snort database.

1. Network Topology in the System Network

   Topology of the system that will be run if described in a simple way is as follows:

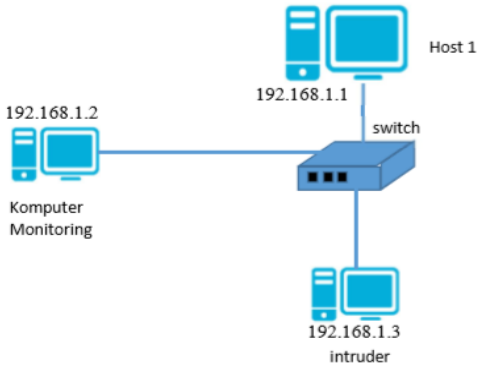

Figure 1. System Topology

In the topology in the picture above can be explained that the monitoring system is placed on a computer that is used as a network monitor. The monitoring computer is connected to a switch where the switch is also connected to the host computer and to the computer that is used as an intruder. The use of a separate monitoring system from the host and server is done with the aim if the server or host is down, the system can still run and connect to the internet network so that it can still send notifications to the administrator.

2. System Flow Diagram

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. See for details: https://creativecommons.org/licenses/by-nc-nd/4.0/

Monitoring system developed is divided into two processes when the system is running, the first is the process of pinging all hosts in the network, and the second is the IDS process or intruder detection process. The workflow of the system is described in the following figure:

Figure 2. The ping system workflow

In Figure 2 describes the workflow of the ping system that is intended to determine whether the host is alive or not. In the picture above it is explained that the system starts by sending ICMP packets to see whether each host will respond or not later. If the host provides a response, the system checks the initial status of the host and provides notification based on the initial status of the host.

3. Database Design

The first step in the development process of this application is to prepare a database. A network monitoring system that is built using the MySQL database to store host data, administrator data, and data alerts derived from the IDS snort database. The system will retrieve data from the snort database which is then created a new database to store messages that will be sent to the administrator in full.

Snort IDS has its own database installed when installing Snort IDS. The structure of the snort database is as follows:

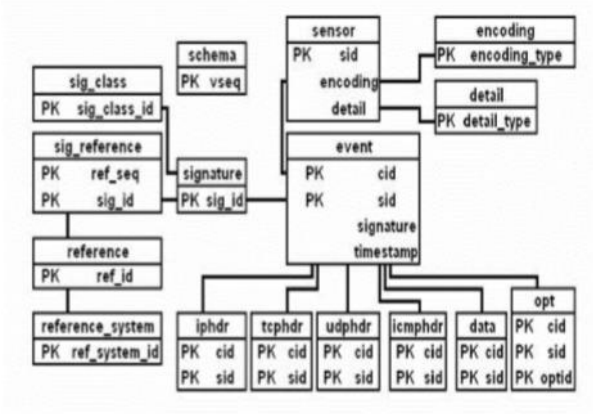

Figure 3. Snort Database Structure (sumber : faculty.nps.edu)

The snort database is used as a reference for sending notifications to the user. Researchers use PHP script to retrieve data needed by the system and enter it into a new database which in this case the researcher uses a database called monitoring. The monitoring database is only used to store attack data that is feasible to be processed by the system, administrator data, signature type data.

4. Design Interface

The system interface is used to help and facilitate the user in performing system management which includes registering a new admin and editing admin, inputing attack type settings that are allowed, and seeing a list of alerts detected by the system.

V. Result and Discussion

At this stage is an explanation of the making of the system starting from the tools used both hardware and software, installation of the main device and supporting devices, to the program code used.

A. Software

The software needed in monitoring the LAN (Local Area Network) network with notifications on Twitter social media is with the following specifications:

a) Monitoring system software specifications:
   1. Ubuntu 12.04 operating system Distro Elementary.
   2. Snort IDS(*Intrusion Detection System*) version 2.9.7.0.
   3. MySQL database.
   4. Apache webserver.
   5. Mozilla Firefox browser.

b) Host software specifications :
   1. Windows 7 operating system.

c) Specifications of testing software (intruder) :

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. See for details: https://creativecommons.org/licenses/by-nc-nd/4.0/

1. Windows 7 operating system.
2. Nmap 6.25

B. Hardware

The hardware required by the system is as follows:

a) Monitoring system hardware specifications :
   1. Intel core i3 – 2310M @2.10 GHz processor.
   2. RAM 4096 Mb.
   3. Hard disk 100 Gb free space.
   4. Ethernet card.
   5. Huawei GSM Modem.

b) Host hardware specifications :
   1. Intel Core 2 duo.
   2. RAM 2048 Mb.
   3. Hard Disk 100 Gb free space.
   4. Ethernet card.

c) Specifications System hardware teaters :
   1. Intel Core 2 duo.
   2. RAM 2048 Mb.
   3. Hard Disk 100 Gb free space.
   4. Ethernet card.

d) Network hardware specifications :
   1. UTP cable.
   2. RJ-45 connector.
   3. Switch.

C. Functional Testing System

Testing on the system to determine the extent to which the system can function whether it has fulfilled the initial objectives of the system or not. This test is categorized intesting *alpha*. The stages of this test are carried out in three types of tests, namely:

a. Testing of sending Twitter notifications in the case of host up / down

This test is carried out using the ping method. In this test 3 hosts are prepared, namely:

1. Computer monitoring, with nip address : 192.168.1.1
2. Host 1, with address nip : 192.168.1.2
3. Intruder, with nip address : 192.168.1.3

connected to a switch. the two hosts are up and respond to the ping given from the monitor computer. Then the researcher unplugged the UTP cable on host 1 and host 1 did not respond to the ping from the monitor computer. Under these conditions the system will send a notification to the administrator via twitter notification. The picture below shows the results of the twitter notification sent.

Figure 4. Host down notification on Twitter

The next test is to reconnect the UTP cable to the host 1. The system will check again whether host 1 is back up and send a notification. In the picture below, a notification from Twitter that shows host 1 with ip address 192.168.1.2 has been returned.

Figure 5. Notification of host up on Twitter

b. Testing of sending Twitter notifications in case of intruder detection

1. Ping Testing

When ping is done, snort gives positive alarm and the computer that is pinged requires a resource of :

a. Memory usage is 0,3% of the total memory of 2048 MB, is 6,144 MB
b. Use of the Processor requires 0% *resource processor.*

The notifications provided by snort are as follows:

Figure 6. Twitter Notifications when the network is pinged by another computer

2. Testing *Port Scanning*

At this testing stage it is done using Nmap

Figure 7. Notification on Twitter when the network is scanned by Nmap

When port scanning done, snort gives *positive alarm* and the computer that is scanned requires a resource of:

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. See for details: https://creativecommons.org/licenses/by-nc-nd/4.0/

a. Memory usage is 0,3% of the total memory of 2048 MB, which is 6,144 MB
b. Use of the processor requires 1% *processor resources*

3. Testing *flooding.*
   After the program starts, the target computer requires a resource of:
   a. Memory usage, 4% of the total memory of 2048 MB, which is 81,92 MB
   b. Use of the processor requires 4% *processor resources.*

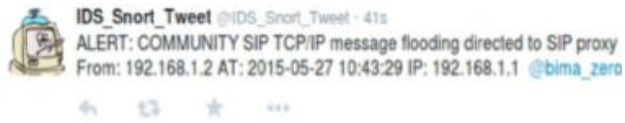

Figure 8. Notification if the system is attacked by TCP flooding

TABLE I. RESULT OF FUNCTIONAL TESTING

NO	Parameter Tests	Expected	Result Test	
			S	TS
1	System runs a ping system	System can ping all registered host periodically	√	
2	Implementation of the ping system for host status	System can determine the status of the host and update the status of the host (wether up / down) if there is a change in status on the host.	√	
3	Implementation of network monitoring with IDS	The system can find out if there is an intruder on the network by reading the database IDS	√	
4	Implementation of Twitter Notifications	System can send notifications to Twitter when there is interface with the network	√	
5	Implementation of selection of types attack for Twitter notifications	System can send notifications based on the type of attack permitted the administrator	√	

ACKNOWLEDGMENT

Thanks to both parents and all family members who always pray for and always provide support, Mrs. Dr. Maizer Said Nahdi, M.Si as Dean of the Faculty of Science and Technology of Sunan Kalijaga State Islamic University. Mr. Sumarsono, M.Kom as chairman of the Informatics Engineering Study Program UIN Sunan Kalijaga Yogyakarta. Mr. Bambang Sugiantoro, MT as a Supervisor who provides direction, advice, guidance during study on campus, especially during the final assignment process. Mr. Aulia Faqih Rifai, M. Kom as Academic Advisor who gave advice and input, direction and advice while studying at the Sunan Kalijaga UIN campus. Mr. and Mrs. Informatics Engineering Lecturer at UIN Sunan Kalijaga Yogyakarta who have provided knowledge from the beginning of the lecture. Friends of the Informatics Engineering Study Program, especially the 2011 classmates who have provided a lot of support. Saudari Miftakhul Intan Naimah who always provides support and assistance in the process of working on the thesis.

REFERENCES

[1] Ariyus, Doni. 2007. Intrusion Detection System. Yogyakarta: Andi.
[2] Dirga. 2012. Keamanan Jaringan. http://dirpratama.wordpress.com/tag/ keamanan-komputer/. accessed December 7, 2014.
[3] D'Monte, Leslie (April 29, 2009). "Swine Flu's Tweet Tweet Causes Online Flutter". Business Standard. 'SMS of the internet', Twitter is a free social networking and micro-blogging service'. accessed December 7, 2014.
[4] Fadhony. 2011. Mengupas Perintah Ping pada Command Prompt. http://edu3003.blogspot.com/2011/09/mengupas-perintah-ping-padacommand.html. accessed December 7, 2014.
[5] Fatta, Hanif Al. 2013. Analisis Dan Perancangan Sistem Informasi. Yogyakarta:Andi.
[6] http://www.alexa.com/siteinfo/twitter.com. accessed December 7, 2014.
[7] Kumar, S. (2010). "Denial of Service Due to Direct and Indirect ARP Storm Attacks in LAN Environment*". Journal of Information Security
[8] 01 (2): 88– 80.
[9] Mulyono. 2013. Perancangan dan Implementasi Sistem Monitoring Jaringan LAN (Local Area Network) dengan Notifikasi SMS. essay. UIN Sunan Kalijaga Yogyakarta.
[10] Oetomo, Budi Sutedjo Dharma. 2003. Konsep dan Perancangan Jaringan Komputer.Yogyakarta : Andi.
[11] Prakoso, Samuel. 2005. Jaringan Komputer Linux : Konsep Dasar, Aplikasi, Keamanan, dan Penerapan. Yogyakarta: Andi.
[12] Preesman, Roger. 2005. Software Engineering : A Practitioner's Approach. McGraw-Hill, New York.
[13] Rafiudin,Rahmat.2009.Investigasi Sumber - Sumber Kejahatan Internet. Yogyakarta : Andi.
[14] Rehman, Rafeeq Ur. 2003. Intrusion Detection Systems with Snort : Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID. New Jersey: Prentice Hall PTR.
[15] Twitter. 2012. Getting Started. https://dev.twitter.com/start. Diakses 7 desember 2014.

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. See for details: https://creativecommons.org/licenses/by-nc-nd/4.0/

[16] Wahana Komputer, Tim Penelitian dan Pengembangan. 2003. Konsep Jaringan Komputer dan Pengembangannya. Jakarta : Salemba Infotek.

[17] Wahana Komputer, Tim Penelitian dan Pengembangan. 2005. Seri buku pintar : Menjadi administrator Jaringan Komputer. Yogyakarta: Andi.

This article is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. See for details: https://creativecommons.org/licenses/by-nc-nd/4.0/