Contents List available at RAZI Publishing
Acta Electronica Malaysia (AEM)
Journal Homepage: http://www.actaelectronicamalaysia.com

ISSN: XXXX (Print)
ISSN: 2590-4043 (online)

NETWORK MONITORING SYSTEM TO DETECT UNAUTHORIZED CONNECTION

Isredza Rahmi A Hamid, Nurul Hatun Ab Sukor, Cik Feresa Mohd Foozy, Zubaile Abdullah

Information Security Interest Group, Faculty Science Computer and Information Technology, Universiti Tun Hussein Onn, 86400, Johor Malaysia
****Corresponding author Email: rahmi@uthm.edu.my, nurulhatun@yahoo.com, feresa@uthm.edu.my, zubaile@uthm.edu.my***

ARTICLE DETAILS

Article History:

Received 3 July 2017
Accepted 3 October 2017
Available online 6 November 2017

Keywords:

Network Monitoring, Unauthorized, Local Area Network (LAN).

ABSTRACT

The Network Monitoring System to Detect Unauthorized Connection is a network analytic tool that use to review local area network usage. The main purpose of the application is monitoring the internet protocol traffic between local area network and Internet. In addition, this system aimed to detect unauthorized Internet Protocol addresses that are inside the network range. It also can prevent network intruders from Local Area Network connection (LAN). It is a computerized system that complete with element of confidentiality, integrity and availability. The system was built using waterfall methodology that begins with system analysis, design, implementation, testing, installation and maintenance. The system is using Visual Studio 2013 with SQL Server as server operations. There are ten modules in this system which are user main page, register admin module, register staff module, login admin module, login staff module, admin menu module, staff menu module, scan view module, status view module and report module. There are about 30 respondents who agreed and satisfied with the system. As a result, this system was successfully built to detect and block the unauthorized access in the network.

1. INTRODUCTION

Large organizations always require fast and efficient network monitoring system which reports to the network administrator as soon as a network problem arises. Most of the large organizations like universities, companies and other business sectors use the manual network monitoring that is very difficult to handle [1]. The Network Monitoring System to detect unauthorized connection was developed to solve the problem occurred. Network monitoring describes systems that continuously monitors the whole network topology for jamming, slowing down or failing components and notify the responsible person in case of any problem. The ideal network monitoring system should have the following properties:

i. It should be automatic and continuously monitor the network.

ii. It should quickly inform the administrator about the problem as soon as it arises.

iii. It should be intelligent enough to identify the problem effects on the rest of the network and the services that will become unavailable.

iv. It should keep a record of the changes in the network which makes easier to find the cause of the problem due to configuration changes [2].

The monitoring system of Local Area Network connection is very important to remote and records all Internet Protocol (IP) address that has been captured in the network. Besides that, this system may help to reduce the intrusion from unauthorized access because user can block the illegal IP address immediately from entering the network. Most of the networking monitoring system did not offer this feature. Hence, this will have caused lack of monitoring mechanism in Local Area Network connection. The objectives of this paper are as follows:

i. To design a network monitoring system that can identify list of illegal IP address in the network.

ii. To develop a network monitoring system with high security features that meet user needs such as user login authentication to prevent by blocking unauthorized access.

iii. To test the system functionality and user acceptance towards the proposed system.

2. RELATED WORKS

Network detection and prevention are the process of monitoring network to trap and block the activity that may compromise the network security.

2.1 Intrusion Detection and Prevention System (IDPS)

IDPS is used for analysing events that may indicate possible incidents. Network Intrusion Detection System (NIDS) also used as a tool that provides the intrusion detection functionality by sniffing the network traffic in real-time. Such event is then logged, and the administrator of the system is automatically notified. However, for the detection, Intrusion Detection and Prevention System (IDPS) also execute automated responses to the detected malicious behaviour. This is useful in cases when the attack against the network is carried out very quickly. These rules can be based on internet protocol address matching, TCP port matching or traffic anomaly detection. Then the response carried out by IDPS could drop the suspicious traffic and further block the traffic based on IP address or port. The benefits of detection and prevention technology system are the ability in taking immediate action based on a set of rules, as configured by the network administrator.

2.2 Security Technique to Protect Internet Connection

There are a few security capabilities in securing network connection, which are information gathering, logging, detection, and prevention. In traditional method, the administrators cannot see the details of attackers [3]. Then, the attackers can crack the wifi password easily and hide themselves from the monitors system. However, few techniques can be used to complete the requirement of wireless security network:

1) Signature-based will compare known threat signatures to observe events to identify incidents. This is very effective at detecting known threats but largely ineffective at detecting unknown threats and many variants on known threats. The detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

2) Anomaly-based detection is a sample network activity to compare the traffic that is known to be normal. When measured activity is outside baseline parameters or clipping level, IDPS will trigger an alert. The detection can trap new types of attacks. It requires much more overhead

and processing capacity than signature-based, and it may generate many false positives.

3) Stateful analysis protocol can natively decode application-layer network protocols, like HTTP or FTP. Once the protocols are fully decoded, the IPS analysis engine can evaluate different parts of the protocol for anomalous behavior or exploits against predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state [4].

2.3 Network Monitoring System

Studies on current network monitoring system were done to analyse and identify the advantages and disadvantages of the current system. The three existing systems are Fanatech Advanced IP Scanner, Microsoft Network Monitor and Total Network Monitor system.

Table 1 shows the comparison between current network monitoring systems with the proposed system. The proposed system is Network Monitoring System to Detect Unauthorized Connection. All monitoring systems are web-based system. However, the Microsoft Network Monitor does not have a log in module as compared to others. Moreover, only Total network monitor system can be assessed remotely while, other systems required the user to go to the workstation to examine the network connection. The Fanatech Advanced IP Scanner and Microsoft Network Monitor did not provide the automated reporting features. Our proposed Network Monitoring System to Detect Unauthorized Connection differs than other network monitoring system in such a way that, the system is able to block unauthorized access based on its IP address.

Table 1: Comparison on network monitoring system

Features	Fanatech Advanced IP Scanner	Microsoft network monitor	Total network monitor	Network monitoring system
Log in module	No	Yes	Yes	Yes
Easy Access of user identification	No	Yes	No	Yes
Remote access	No	No	Yes	No
Automated Reporting	No	No	Yes	Yes
Block function	No	No	No	Yes

3. METHODOLOGY

The Network Monitoring system is used to detect unauthorized connection by using waterfall methodology as shown in Figure 1. This methodology can easily identify the user requirements for the system. There are five phases which are Requirement analysis phase, System design phase, System development phase, System testing phase and System implementation phase. At the end of each phase, a review is done to determine if the system runs smoothly and either continue or discard the system. In this model, the testing phase starts after the development is completed. The model phase did not overlap in waterfall methodology. All phases must finish one at a time to ensure that the real system meets the user requirements [5-7].

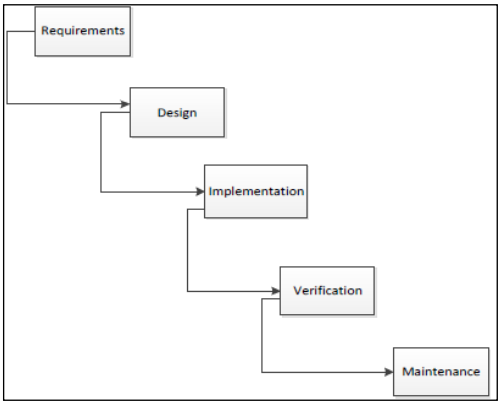

Figure 1: Waterfall Methodology

The Network Monitoring System to Detect Unauthorized Connection as shown in Figure 2 consists of various processes such as login, scanning active Internet Protocol (IP) address, blocking IP address, generating report for the end result and log out. System admin is able to detect and block unauthorized access based on the IP address. All recorded IP will be stored in the database. Staff also can do three processes which are scanning active internet protocol, view IP status and block IP address. They also can generate report that list all unauthorized IP address that have been blocked by the system.

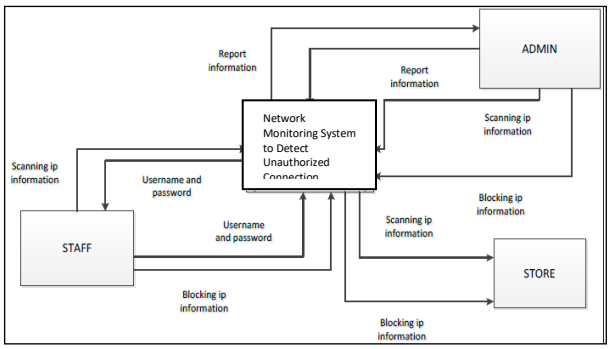

Figure 2: Network Monitoring System to Detect Unauthorized Connection

4. RESULT AND DISCUSSION

The system is designed and developed to be applied by the company which has Internet connection. The proposed system can prevent the unauthorized access based on IP address. The system includes username, password, user identification, IP address, time of invasion, type of data and size of data. The system is developed using Visual Studio 2013, SQL server management studio and some additional techniques to monitor network from unauthorized access based on IP address.

The network monitoring system to detect unauthorized connection is developed to reduce illegal activity by external users who want to access the Internet connection without permission. By using this system, the administrator or staff can take immediate action if there was any breach happened. In addition, the intrusion activities will be recorded in the database. This system can generate a report consists of list of active connections and blocked IP.

The network monitoring system to detect unauthorized connection is well developed and capable to detect the unauthorized IP address. The system also can generate complete instruction information pertaining the invasion of activities, data entry into the system, store data in the database and displays report active connection information. In addition, this system can assist administrator and staff to detect any unauthorized access more accurately.

a. System Design

The interface of a system is designed to suit the needs and requirements of the users. The system interface is designed to be more user friendly and not too complex to ensure users can access the system more easily.

1) The main page as shown in Figure 3 is designed for staff and administrators. It provides login, updates, and help button before assessing the login page. User have to choose either login as Admin or Staff.

Figure 3: Main page

2) Login page as display in Figure 4 requires admin and staff to input valid username and password for authentication.

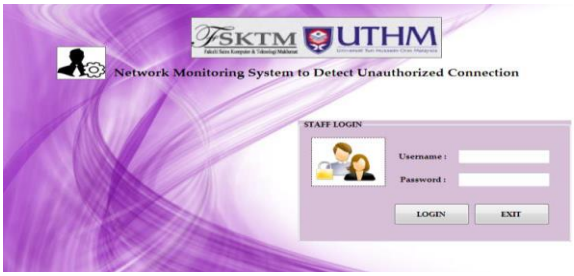

Figure 4: Login Page

3) Admin page in Figure 5 shows that the admin can choose to scan IP address, view status of the scanned Internet Protocol (IP) address, and print report. Otherwise, the admin can click the exit button to logout from the system.

Figure 5: Admin Page

4) This scan IP page in Figure 6 provides function to scan IP for any adapter including Local Area Network (LAN). Scanning process take about 2 to 3 minutes. Then, the user press stop button to see list of scanned IP(s). User can see the unauthorized IP address, source IP, destination IP, type of packet and tra can, user can block illegal IP in the network. The blocked ffic data. After s IP address will be saved and recorded in the database. Thus, the blocked IP address cannot access the network (Figure 7).

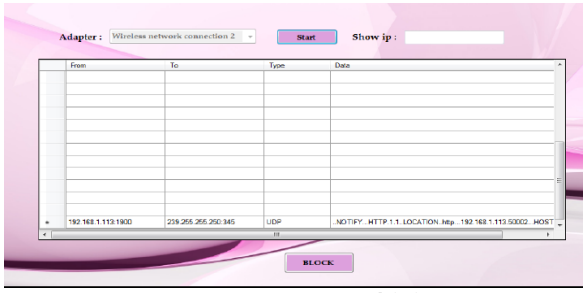

Figure 6: Scan Internet Protocol (IP) Page

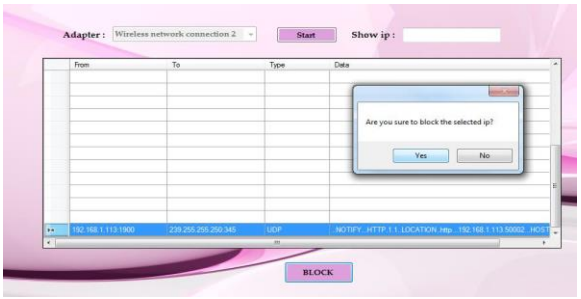

Figure 7: Block Internet Protocol (IP) Function

5) When user clicks the view the status button, they can see the status of IP addresses that has been captured before either Active or Blocked in the network range (Figure 8).

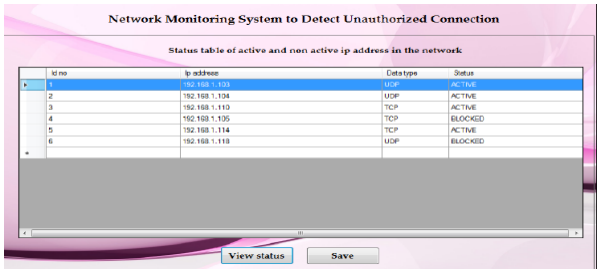

Figure 8: Status Internet Protocol (IP) Page

6) After scanning and blocking process, admin can generate and print the report. Admin will load the document that he wants to print from the database and connect with the printer. Finally, user can logout from the system.

b. Implementation and Testing

System implementation phase has a prior relationship between analysis and design phase. The implementation phase becomes much easier because it is entirely based on the design of systems that have been drawn before. This system has been developed to replace manual methods that have been used previously. This phase involves the installation of software including Visual Studio 2013 and MySQL as server operations. It is also used to produce the modules in this system such as login, scanning active Internet Protocol (IP) address, blocking IP address, generating report for the end result and log out. The editing image in this system is used Adobe Photoshop CS3 and Microsoft Visio.

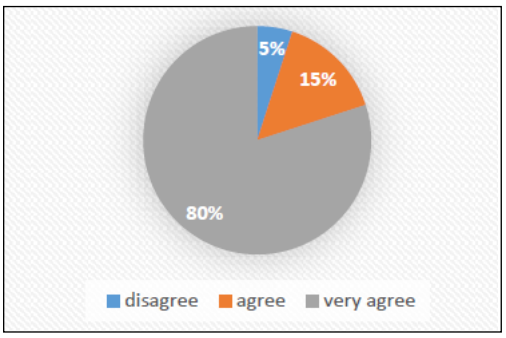

Figure 9: Status Internet Protocol (IP) Page

1) System Functionality Testing is very important to determine either the system that has been developed achieved the user requirement. The testing phase is also intended to identify system weaknesses and find solution to overcome these weaknesses. The testing is done by making an appointment with a client to test the usability of the system. A total of 10 respondents took part to answer the questionnaire on the effectiveness of the system. Figure 5.15 shows pie chart of level of flow system facilities from testing questionnaire from Section B. Based on pie chart in Figure 9, about 80% respondents strongly agree that this system is well-function, 15% of respondents agreed and only 5% disagree. This show that this system function well specially to record, update and generate report for the user. The modules that has been run in system functionality testing are user main page, register admin module, register staff module, login admin module, login staff module, admin menu module, staff menu module, scan view module, status view module and report module. Based on the comments provided by respondents during the testing phase is done, the improvement in the future must be made. Among the proposed improvements are:

i. Produce system with strong antivirus
ii. Make detection with sound alert
iii. Make accessibility control for more than one administrator

5. CONCLUSIONS

As a conclusion, the network monitoring system to detect unauthorized connection can work well and meet the objectives of the development of the system which is to develop a system for detection, blocking and record data of active unauthorized internet protocol by staff and administrators to produce final reports. The phases of construction of the system is plan and draw based on the waterfall methodology which is always follow step by step of the process. Besides that, some interview, observation and small research has been made to get best result in system development. The advantages of this network monitoring system are:

i. This system has ability to save and keep all the information automatically related to unauthorized access to the internet connection such as internet protocol address, data, and type of data.

ii. This system provides intelligence popup in which every capture of unauthorized access to internet connection will produce popup block to give alertness to the user of the system to make fast response in order to protect the network connection.

ACKNOWLEDGMENT

The authors express appreciation to the Universiti Tun Hussein Onn Malaysia (UTHM). This research is supported Short Term Grant vot number U653 and Gates IT Solution Sdn. Bhd. under its publication scheme.

REFERENCES

[1] Shirbhate, R.S., Patil, P.A. 2012. Network Traffic Monitoring Using Intrusion Detection System. International Journal of Advanced Research in Computer Science and Software Engineering, 2 (1), 1-5.

[2] Khan, R., Khan, S.U., Zaheer, R., Babar, M.I. 2013. An Efficient Network Monitoring and Management System. International Journal of Information and Electronics Engineering, 3 (1), 122.

[3] Abiona, A., Aladesanmi, T., Onime, C., Oluwaranti, A., Oluwatope, A., Adewara, O., Anjali, T. 2009. A Scalable Architecture for Network Traffic Monitoring and Analysis Using Free Open Source Software. International Journal Communications, Network and System Sciences, 2 (6), 528–539.

[4] Report, C. T. 2015. Overview of the Local Network Monitoring. 1–15.

[5] Cannistra, R. 2007. Angry IP – An IP Scanner Tool a Product Analysis and User Tutorial IDCP Internet Security. Marist College, pp. 1–32.

[6] Pai, V.S. The Practicality of End-User Network Monitoring. 131.107.65.14, pp. 5–6.

[7] Adenowo, A.A.A., Adenowo, B.A. 2013. Software Engineering Methodologies: A Review of the Waterfall Model and Object-Oriented Approach. International Journal of Scientific & Engineering Research, 4 (7), 427–434.