Analyze and Designing Low-Cost Network Monitoring System Using Icinga and Raspberry Pi

H Maulana¹, Al-Khowarizmi²

¹,² Information System Department, Faculty of Computer Science and Information Technologies
Universitas Muhammadiyah Sumatera Utara, North Sumatera, Indonesia

Email: halimmaulana@umsu.ac.id¹, alkhowarizmi@umsu.ac.id²

Abstract. The development of information and data communication technology field in the world has now increasingly led to the development of the Internet of Things devices. The development of network technology in an organization/university has triggered the need for a system that can monitor computer networks and their devices in an organization/university environment that is quite extensive and complex. At this time, network monitoring becomes quite difficult to do if the computer network in a corporate environment has become very broad and complex. The wider the network and the complex network and multimedia topology that is built, the more difficult it is for network administrators to monitor the network. However, in its application to build a monitoring system it will require devices and hardware and computer requirements and specifications that are above average, which of course will also require substantial costs and large resources as well. In this research, a network monitoring and bandwidth management system will be built by using Raspberry-Pi and Icinga as the main modules in network management. Raspberry Pi is an alternative of computers that has many capabilities and has a high ability which is generally used as a Mini-Server at a very cheap price when compared with existing servers. And Icinga is an open source-based application platform that functions to monitor various types of variables contained in servers and infrastructure of the network such as availability and performance and provides easy access for network administrators to important data and to improve maintenance of network conditions. So, it is hoped that by applying this, a good and optimal network monitoring and bandwidth management tool can be produced at a low cost.

1. Introduction

Network security is a method or a system used to provide protection or protection on a network to avoid external threats that can damage the network. The purpose of making network security is to anticipate network risks in the form of physical and logical threats, either directly or indirectly that can interfere with ongoing activities in the network. One thing to remember is that no network is not bugging or no network is safe, because the nature of the network is to communicate, and every communication can fall into the hands of others and in the wrong use. Therefore, network security is needed. [1][2]. Network security that effectively manages access to the network; including how to monitor network activity, detect threats, and prepare systems to deal with them. Along with its evolution and development, malware can combine several vectors to carry out infections, for example, like in a hashing file where the file can be duplicated so it is very difficult to do analysis, next is the use of anti-forensic techniques that are used to inhibit detection, disguise the code so that the code they are not considered dangerous by analytical tools [3][4]. The development of technologies in the computer science and information technology field is very rapid at present. The role of that field is needed to ease various
problems in all aspects of life. Moreover, the impact caused by the spread of the COVID-19 virus is very much felt by all people in the world. Utilization of the digital field is something that must be required to prevent a greater impact [5][6][7].

With the increased use of digital resources and the use of digital media in all aspects, of course, there will also be an increase in the use of resources in the network where connections are needed to channel the internet, which is the main requirement for the use of digital media. All of these resources will be available and through a computer network from either the local or public network. The increasing use of online media will also affect traffic on the local network within the organization or institution. High network traffic will cause various problems to the existing network and server of the Local Network and the potential for data leakage caused by viruses, worms, and various similar things will also increase. A computer network is a complex matter where the level of complexity is not limited to the number of devices or devices but also affects the variety of systems and technologies that are in it, as well as the wide network area coverage. Even good infrastructure cannot be a guarantee that the network function can work optimally without the support of a good monitoring or management system or called the Network Monitoring System (NMS) [8][9][10].

NMS is a system consisting of software combined with hardware in the network that has the function to monitor and manage all network devices with the aim that the level of reliability and availability is maintained and can be known early if there is an anomaly or network outage. And with the monitoring system of a data network that is distributed to be “safer” even though it is far from safe, it can prevent other parties who infiltrate the network from knowing important data contained in the network. For these monitoring devices quite a lot that offer features that are reliable and easy to use such as Cisco Work, IBM Tivoli Net view, and others, but the device is quite expensive and other costs such as servers that require no small cost. These alternatives can use a mini-computer that is raspberry-pi and combined with Icinga open-source software [11][12][13]. The role of network monitoring or management is very important to facilitate the regulation and supervision of the network. The wider the network and the complex network and multimedia topology that is built, the more difficult for network administrators to monitor the network. However, in its application to build a monitoring system it will require devices and hardware and computer requirements and specifications that are above average, which of course will also require substantial costs and large resources as well [14][15][16].

Raspberry Pi is a capable small computer, can be used for electronic projects and can do many things like your desktop PC or computer. Like running an office program to make reports, create documents, browse the internet, and even play games. Also, this tool can play high-resolution videos. The Raspberry Pi Foundation is the first non-profit foundation that developed this product. The initial goal of producing Raspberry pi was to be used by adults and children around the world to learn digital programming [17]. Raspberry-Pi has a high ability which is generally used as a Mini-Server and has extraordinary capabilities that have capabilities similar to Server computers. Icinga is a monitoring system based on open-source that is used to monitor the health of devices and services on the network and monitor load and uptime of devices, availability of storage devices, memory usage in cache services, and so forth. This research will focus on building a network monitoring system using Raspberry Pi and Icinga devices that can be accessed with a web interface and the operating system used in this study is Linux-based so that it is free. Where later Icinga Core and Icinga Web Interface will be available that run on Raspberry Pi [18][19].

2. Methodology
2.1 Research Methodology
This study aims to conduct studies and/or studies on network monitoring using raspberry pi and Icinga. The aspects examined in This research includes the study of intranet/internet networks, studies of content and applications, problems, and development plans in the future and provide recommendations for improving network performance in the future.
To achieve the goals set above, this research will use an approach Qualitative using triangulation) from the study of documents and related literature, as well as observing research objects. Based on data and information obtained then analysed and described descriptively to get the expected conclusions [20][21][22].

2.2 Network Monitoring Topology

In the design of a network system so that it can run well and smoothly needed a network topology that is used so that the system can run well on the network with available devices [23][24]. Figure 2 is a picture of the network topology design that will be used in this study. In the picture, the raspberry pi device is connected directly to the internet through a router and also switches and wireless access point devices which are then connected to other devices such as computers or laptops. And the network that is connected to the raspberry network be monitored by a network monitoring system that will be built in this research.

![](network_topology.png)

**Figure 2. Network Topology**

In Figure 2 can be seen the main router has two networks, namely a public network that has internet access called eth1 which will be shared via a local network, namely eth0 which is connected directly with raspberry-pi. In this topology, raspberry-pi holds the main key in managing the existing network in the local network.

2.3 Implementation Process

1. **Installing Icinga 2**

To get the latest version of Icinga, we first need to add a software repository managed by the Icinga team. We will then install the software with apt-get and run through several screen configurations to set the Icinga backend database. First, download the Icinga developer package signing key and add it to the apt system. This key will be used to verify the integrity of each software that we automatically download from the Icinga repository. Now we need to add the repository address to the appropriate configuration file. Then open the file in the following way

```bash
dsudonano/etc/apt/sources.list.d/icinga2.list
```

2. **Installing Icinga Web 2**

The main system of Icinga is fully configurable and can be used without a web interface, but Icinga Web provides an overview that can be explored about the health of hosts and services that are on the local network, and allows us as managers or network administrators to schedule downtime, detect problems,
triggering a health check manually, and sending notifications, right from your browser. To install Icinga can be done by typing the following command: `sudo apt-get install icingaweb2`

3. **Icinga System Configuration**

Before we switch to the browser for the web-based setup process, we need to create a token setting. This is the key that we generate on the command line that allows us to use the web settings tool. To get the key, you can use the command with icingacli: `sudo icingacli setup token create`. After inputting the code will appear and copy the token to the clipboard, then switch to your browser and load the Icinga Web address. By default, this is the domain name or server IP address followed by / icingaweb2 in this case as follows: `https://192.168.115.132/icingaweb2`

![Figure 3. Display Icingaweb Installation](image)

Figure 3 is an Icinga installation page that uses a web-based interface. In the picture, you will be asked token as needed to be able to proceed to the next stage. We already have this token in the previous process. At this stage enter the token and click Next then the next step will appear as in Figure 2.

![Figure 4. Module Installation For Icinga](image)

In the picture is a list of modules available for use in the monitoring system provided by Icinga. Where the Modules are Document, Migrate, Monitoring, Test, and Translation. After selecting the module that we will use then we will click Next it will appear as shown in Figure 4.

![Figure 5. Select a DataBase Resource](image)

Figure 5 is the configuration for the selection of database sources that Icinga will use to store data in the column to be filled in with the appropriate database accounts that have been previously configured. After all the columns are filled in well then check by checking the Validation button then click Next.
Next, we will make adjustments to the Command Transport where in this section we can choose the command model that will be used in the monitoring process as shown in Figure 6.

The next step is to choose a name for Monitoring your Backend account. After that click Next.

In Figure 8 you will see the adjustment module for Icinga Web 2. Click Next.

In Figure 9 you can see all the configurations that we have adjusted and if there is a discrepancy we can return to the previous menu and if it is appropriate, we click Next.

Next is the stage of adjusting the configuration for the application. Here is the same as the previous stage, which includes the type of configuration used, such as Logging Type, Logging Level, Application Prefix, and so forth. After all, is done, a display will appear that the installation process has been successful as shown in Figure 11.
3. Result and Discussion

3.1 Login System

After the system is successfully designed and built, we will log into the system with the configuration we have done before. We will access http://192.168.152.129/icingaweb2/ the login page will appear as shown in Figure 12.

On that page enter a username and password that is following the configuration that we have done before then click Login.

After logging in successfully the user will be directed to the system home page. On the system homepage, a summary of the network and host conditions are monitored.

3.2 System Monitoring

1. Host Problem

In Figure 14, it appears that no significant problems occur within the host connected to the network.

2. Service Problem
Figure 15 shows that several problems occur in the network system for this type of service problem. In the picture, 4 problems appear 2 of them are critical or important for immediate further action and 2 more problems are just a reminder about system updates. To see more complete details, we can click on one of the critical warning notifications, it will look like in Figure 15. In the figure, there is a problem with the service where there are new processes that appear to increase significantly, reaching 342 processes that must be followed up immediately so that it does not harm the server and network.

![Figure 15: Network Monitoring System Problems](image)

3.3 Discussion

In its use, the network monitoring system that has been built can work following previously designed. The system can easily detect problems that arise on the network and devices that are connected to the network and are registered in the monitoring system.

![Figure 16: Service Problem Detail](image)

For example, we will burden a host registered in the system by using a stress module. Stress modules are used to put pressure on hardware. Then the system will be detected with a display like in Figure 17. In the picture, it can be seen that there is excessive load in the system with an average of 447,11,186,39,70,22 so that further handling is needed.

![Figure 17: Excessive Load Detected](image)

![Figure 18: Load Detail](image)
The results of this research are that a network monitoring system has been built in the Faculty of Computer Science and Information Technology using Raspberry Pi and Open Source Icinga Software, where the system can run smoothly and can function to detect problems that occur in the local network and fix these problems. The next stage plan is to add Hosts or devices that will be monitored by the monitoring system to expand the scope of the devices that will be monitored so that the system's range of monitoring systems will be even better.

4. Conclusion
Based on the results and discussion above, the writer can draw the following conclusions:
1. A network monitoring system has been built in the Faculty of Computer Science and Information Technology using Raspberry Pi and Open Source Icinga Software, where the system can run smoothly and can function to detect problems that occur in the local network and fix this problem.
2. The level of sensitivity of the system to interference is accurate and precise so that appropriate handling can be done in response to problems on the network.

5. References
[1] Syahputra E.R., Sembiring B.O., Dewi A.R., Hasdiana H., and Maulana H. 2018 Ads block management system using open Virtual Private Network on Ubuntu operating system International Journal of Engineering Technology 7 58-61 2018
[2] Y. Kong, B. Lyu, F. Chen, and Z. Yang, "The Security Network Coding System With Physical Layer Key Generation in Two-Way Relay Networks," in IEEE Access, vol. 6, pp. 40673-40681, 2018
[3] A. Lara and B. Ramamurthy, "OpenSec: Policy-Based Security Using Software-Defined Networking," in IEEE Transactions on Network and Service Management, vol. 13, no. 1, pp. 30-42, March 2016
[4] H. Xie, Z. Yan, Z. Yao and M. Atiquzzaman, "Data Collection for Security Measurement in Wireless Sensor Networks: A Survey," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2205-2224, April 2019
[5] W. Shen, C. Yang and L. Gao, "Address business crisis caused by COVID-19 with collaborative intelligent manufacturing technologies," in IET Collaborative Intelligent Manufacturing, vol. 2, no. 2, pp. 96-99, 6 2020
[6] V. Chamola, V. Hassija, V. Gupta and M. Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact," in IEEE Access, vol. 8, pp. 90225-90265, 2020, doi: 10.1109/ACCESS.2020.2992341.
[7] M. Quayson, C. Bai and V. Osei, "Digital Inclusion for Resilient Post-COVID-19 Supply Chains: Smallholder Farmer Perspectives," in IEEE Engineering Management Review
[8] A. Abdou, P. C. van Oorschot, and T. Wan, "Comparative Analysis of Control Plane Security of SDN and Conventional Networks," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3542-3559, Fourth quarter 2018
[9] A. Shameli-Sendi, Y. Jarraya, M. Pourzandi, and M. Cheriet, "Efficient Provisioning of Security Service Function Chaining Using Network Security Defense Patterns," in IEEE Transactions on Services Computing, vol. 12, no. 4, pp. 534-549, 1 July-Aug. 2019
[10] J. S. Aidan, H. K. Verma and L. K. Awasthi, "Comprehensive Survey on Petya Ransomware Attack," 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), Jammu, 2017, pp. 122-125
[11] J. Ko, J. Jo, D. Kim, S. Choi, and J. Kwak, "Real Time Android Ransomware Detection by Analyzed Android Applications," 2019 International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, 2019, pp. 1-5
[12] A. O. Almashhadani, M. Kaialii, S. Sezer, and P. O’Kane, "A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware," in IEEE Access, vol. 7, pp. 47053-47067, 2019
[13] S. Iqbal and M. Zulkernine, "SpyDroid: A Framework for Employing Multiple Real-Time Malware Detectors on Android," 2018 13th International Conference on Malicious and Unwanted Software (MALWARE), Nantucket, MA, USA, 2018, pp. 1-8

[14] O. P. Samantray, S. N. Tripathy and S. K. Das, "A study to Understand Malware Behavior through Malware Analysis," 2019 IEEE International Conference on System, Computation, Automation, and Networking (ICSCAN), Pondicherry, India, 2019, pp. 1-5

[15] S. M. Pudukotai Dinakarrao, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafaatirad and H. Homayoun, "Lightweight Node-level Malware Detection and Network-level Malware Confinement in IoT Networks," 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 2019, pp. 776-78

[16] H. Garg and M. Dave, "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6

[17] R. W. Sudibyo, N. Funabiki, M. Kuribayashi, K. I. Munene, M. M. Islam and W. Kao, "A TCP Fairness Control Method for Two-Host Concurrent Communications in Elastic WLAN System Using Raspberry Pi Access-Point," 2019 2nd International Conference on Communication Engineering and Technology (ICCET), Nagoya, Japan, 2019, pp. 76-80, doi: 10.1109/ICCET.2019.8726907.

[18] N. S. Yamanoor and S. Yamanoor, "High quality, low cost education with the Raspberry Pi," 2017 IEEE Global Humanitarian Technology Conference (GHTC), San Jose, CA, 2017, pp. 1-5, doi: 10.1109/GHTC.2017.8239274.

[19] N. S. Yamanoor and S. Yamanoor, "High quality, low cost education with the Raspberry Pi," 2017 IEEE Global Humanitarian Technology Conference (GHTC), San Jose, CA, 2017, pp. 1-5, doi: 10.1109/GHTC.2017.8239274.

[20] S. M. Lord, M. M. Camacho, C. E. Brawner, C. Mobley and J. Main, "Have you ever wondered why? Qualitative research methods to investigate engineering education," 2017 IEEE Global Engineering Education Conference (EDUCON), Athens, 2017, pp. 1851-1853, doi: 10.1109/EDUCON.2017.7943102.

[21] A. Bliss, N. Hudyma, S. Brown, J. Oglesby and A. Harris, "Qualitative assessment of surface roughness of limestone specimens from the orientation of unwrapped triangulated point clouds," SoutheastCon 2017, Charlotte, NC, 2017, pp. 1-5, doi: 10.1109/SECON.2017.7925385.

[22] S. Rady, A. Wagner and E. Badreddin, "Hierarchical localization using entropy-based feature map and triangulation techniques," 2010 IEEE International Conference on System, Man and Cybernetics, Istanbul, 2010, pp. 519-525, doi: 10.1109/ICSMC.2010.5642024.

[23] Maulana H. and Syahputra E. R. 2017 Analysis of Multiple Data Hiding Combined Coloured Visual Cryptography and LSB Journal of Physics: Conference Series 930

[24] Syahputra E.R., Sembing B.O., Dewi A.R., Hasdiana H. and Maulana H. 2018 Ads block management system using open Virtual Private Network on Ubuntu operating system International Journal of Engineering Technology 7 58-61 20182018