JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

VOL. 7 NO. 2 FEBRUARY 2022
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v7i2.2786

WIRELESS COMPUTER NETWORK MANAGEMENT SECURITY ANALYSIS

Dwipo Setyantoro[1*]; Vivi Afifah[2]; Rika Astuti[3], Novia Aprilia[4], Novia Permata Sari[5]

Institut Teknologi dan Bisnis Bank Rakyat Indonesia [1 2 3]
www.bri-institute.ac.id
dwipo.setyantoro@gmail.com [1], vivi.afifah@gmail.com[2], rika.astuti93@gmail.com[3]

Universitas Persada Indonesia YAI [4 5]
www.upi-yai.ac.id
novia.apriliaaa@gmail.com[4], noviapermata2@gmail.com[5]

(*) Corresponding Author

Abstract— The use of a wireless computer network in some institutions has become a very flexible option to connect all users of the existing computer network in the institution. This flexibility also has the disadvantage that anyone with a network password can take advantage of the wireless network. The possibility of threats to information security is very large, such as the presence of intruders on the network. Therefore, it is necessary to manage wireless networks that pay attention to information security issues on the network. The Directorate General of New, Renewable Energy and Energy Conservation at the Ministry of Energy and the Human Resources Republic of Indonesia was chosen as the research location given that computer network users in this institution are diverse and have also used The Dude MikroTik application to manage wireless computer networks, which are instruments to analyze information security. in this institution. The analysis was conducted to identify the activities and effectiveness of information security management in this institution. This study concludes that the use of The Dude MikroTik application is quite helpful in analyzing information security on wireless computer networks in this institution.

Keywords: Information Security, The Dude MikroTik, Wireless Network

Abstract— *Penggunaan jaringan komputer nirkabel pada sebuah institusi telah menjadi pilihan yang sangat fleksibel untuk menghubungkan semua pengguna jaringan komputer yang ada pada institusi tersebut. Fleksibilitas ini juga memiliki kelemahan di mana setiap orang yang memiliki password jaringan dapat memanfaatkan jaringan nirkabel tersebut. Kemungkingan terjadi ancaman terhadap keamanan informasi sangat besar, seperti adanya penyusup pada jaringan. Oleh sebab itu diperlukan pengelolan jaringan nirkabel yang memperhatikan masalah keamanan informasi pada jaringan tersebut. Direktorat Jendral Energi Baru, Terbarukan dan Konservasi Energi di Kementrian Energi dan Sumbar Daya Manusia Republik Indonesia menjadi pilihan lokus penelitian ini mengingat bahwa pengguna jaringan komputer di institusi ini beragam dan juga telah menggunakan aplikasi The Dude MikroTik untuk mengelola jaringan komputer nirkabel, yang menjadi instrumen untuk menganalisa keamanan informasi di institusi ini. Analisis dilakukan untuk mengidentifikasi aktivitas dan efektifitas pengelolaan keamanan informasi di institusi ini. Kesimpulan dari penelitian ini adalah penggunaan aplikasi The Dude MikroTik cukup membantu dalam menganalisis keamanan informasi pada jaringan komputer nirkabel di institusi ini.*

Kata Kunci*: keamanan informasi, aplikasi the Dude MikroTik, jaringan nirkabel*

INTRODUCTION

The development of computer networks today is very rapid and popular, so computer networks are often used to communicate in a building, office, home, internet cafe, and even between buildings. Computer networks are very supportive of the use of computers by many agencies and other businesses to facilitate users to exchange data and find the information needed quickly and accurately in carrying out activities as needed.

In the beginning, computer networks used cables to communicate with each other, but slowly this changed towards the use of wireless networks or often called Wireless Local Area Network (WLAN). Wireless Local Area Network (WLAN) devices serve to reach Local Area Network (LAN) areas that are difficult to reach by cable and also to reach mobile users. [1] One example of the application of wireless devices today is the use of

cellular phones. These wireless network applications provide a significant enough impact of change that allows people to expand their workspace because they are not tied to the use of cables. In wireless communication, some advantages are high mobility but also have disadvantages, namely the possibility of interference with fellow wireless connections on other computers, so it is necessary to do data security on the wireless network.

Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Human Resources (ESDM) has the task of carrying out the formulation and implementation of policies in the field of fostering, controlling, and supervising geothermal activities, bioenergy, various new and renewable energies, and energy conservation [2]. This institution which is located on Jalan Merdeka Selatan, Central Jakarta [3] has computer networks using from the 2nd floor up to the 7th floor. According to that so many network users on these 6 floors, it's conceivable that issues can happen connected with the progression of information correspondence through the organization (for example the bottleneck situation when a lot of users using the same channel) [4] and it is necessary to do an analysis related to network management, especially on the 4th floor where the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) is located

The purpose of this research is to observe and analyze the management of computer networks in this institution. In this research, observations were made on the implementation of wireless network management in the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Human Resources (ESDM). The results of this study are the results of an analysis of information security in wireless network management in the institution.

MATERIALS AND METHODS

Computer Network Management

Network management is the ability to apply a method to design, monitor, control a network, and plan (planning) resources (resources) as well as system components and computer networks to obtain good quality of service at all times a proportionate and optimal capacity [5].

Network management can be defined as the operational, administration, maintenance, and provisioning of networks and services. Types of operations related to day-to-day operations in providing services [6].

Method

This research was conducted using a qualitative approach that observations are made on the use/management of computer networks, especially on the 4th floor where the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) is located.

At this research, the author observed the current system, interviewed the IT Staff who maintain the network, and read some literature about computer network management and MikroTik. And then the author analyzed the computer network used, the use of The Dude MikroTik application to manage computer networks, which was performed in several stages: 1) Analysis of security hole sources, 2) Firewall device analysis, dan 4) Analysis by monitoring the system using The Dude MikroTik application

RESULTS AND DISCUSSION

Analysis of Security Hole Sources

An administrator often makes mistakes in analyzing the initial design of the network system. Sometimes they unwittingly have opened a gap that contains a security hole, either caused by a wrong design or a hole in the service operating system used. Security holes occur due to several things, namely [7]

1. Poor Implementation

Security holes caused by implementation errors are common. Many programs are implemented in a hurry, so they are less careful in coding. As a result, checks or testing that should have been carried out were not carried out. For example, The source of security holes caused by a poor implementation is strange characters that are entered as input from a program so that the program can access files or information that should not be accessed. The computer network system at the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) has been tested, so that network security is quite safe.

2. Faulty design

Security holes created by faulty designs are rare. However, if it occurs it is very difficult to repair, even if the system is implemented properly, the weaknesses of the system will still exist.

For example, a security hole that can be categorized as a design error is the design sequence numbering (sequence numbering) of TCP/IP. This error can cause a problem known as "IP Spoofing" where a host pretends to be another host by creating fake packets after observing the sequence of packets from the host to be attacked. The network

Accredited Rank 3 (Sinta 3) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti
No. 28/E/KPT/2019, September 26, 2019. Published by PPPM STMIK Nusa Mandiri

VOL. 7 NO. 2 FEBRUARY 2022
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v7i2.2786

design at the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) has been implemented quite well so that security holes can be properly covered.

2. Configuration Mistakes

Even if the program is implemented properly, security holes can still occur due to misconfiguration. Example: The problem caused by a misconfiguration is that a file that should not be able to be changed by the user accidentally becomes "writeable". If the file is an important file the effect will be a security hole. Network configuration the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) has been implemented properly so that important company data and files can be well protected.

Firewall Equipment Analysis

The network security system at the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) is very wide because it is connected to a LAN network starting from the 2nd floor to the 7th floor with the central room being on the 2nd floor. Firewalls are network devices that enforce an organization's security policy [8]. The firewall device used is the CISCO ASA 5520 Firewall which has the following specifications: [9][10]

Table 1. Firewall CISCO ASA 5520 Specification

Feature	Description
Firewall Throughput	Up to 450 Mbps
Maximum Firewall and IPS Throughput	- Up to 225 Mbps with AIP SSM-10 - Up to 375 Mbps with AIP SSM-20 Up to 450 Mbps with AIP SSM-40
VPN Throughput	- Up to 225 Mbps
Concurrent Sessions	- 280,000
Psec VPN Peers	- 750
SL VPN Peer License Levels	- 2,10, 25, 50, 100, 250, 500, or 750
Security Contexts	- Up to 20
Interfaces	- 4 Gigabit Ethernet ports and 1 Fast Ethernet port
Virtual Interfaces (VLANs)	- 150
Scalability	- VPN clustering and load balancing
High Availability	- Active-Active, Active-Standby

The utilities of Firewall CISCO ASA 5520

1. Simplify security management, reporting, and reduce operational costs. Deploy security with a mix of security functions and enable to support existing systems.
2. Provides high performance for enterprises that require real-time network security services.

Security System Analysis using System Monitoring

According to Chopra [11] Network Security consists of provisions and policies adopted by a network administrator to preclude and monitor unauthorized access, alterations, perversion, declination of a computer network, and network-accessible resources

Monitoring of security systems is usually done with a special tool, this is applied so that holes or connections to the internet can be seen. In this way, it is hoped that we can find out the weaknesses and holes of the system made.

The system monitoring program used on the computer network of the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) is The Dude MikroTik. The Dude is a MikroTik application that is used for network management. Besides the application could be used as a regulator of Internet data bandwidth and filtering sites that can interfere with computer network connectivity [12], and used for network security [13]. The Dude can perform automatic scanning on all devices connected to a particular network subnet. The results of the scan can be in the form of a network configuration image that appears. The network configuration will describe whether the network condition is up/down [14].

Network Monitoring using The Dude MikroTik

Based on the analysis carried out at the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) to monitor the security network located on the Fl. 4 using The Dude MikroTik application [15]

Figure 1. Network Access

Accessing the Network at the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) and using the Wireless Network Connection of EBTKE Office which is on Floor 4 to monitor the security network on that floor.

Menu Display of Device Discovery The Dude

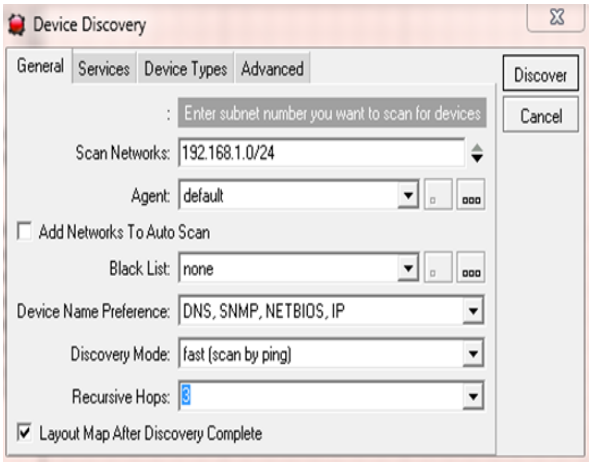


Figure 2. Menu Device Discovery

Figure 3 shown below displays a networking map by entering the subnet address at the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) which is 192.168.1.0 and The Dude will automatically scan the network in that subnet.

The Display of Networking Map

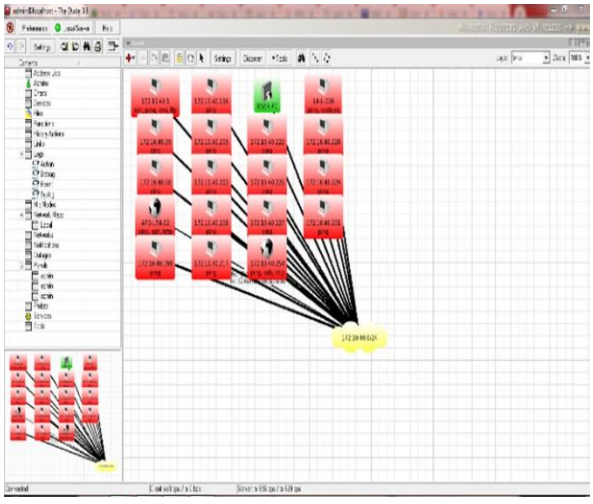


Figure 3. Networking Map

Figure 4 below displays the existing networking map at the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM)

1. The Yellow one is a subnet located on the 4th floor of the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM).
2. The green color indicates network devices and equipment that have been detected are connected and can function properly (UP).
3. Red colors indicate network devices and equipment have encountered network problems (DOWN).

The display of the problem of the Network (DOWN)

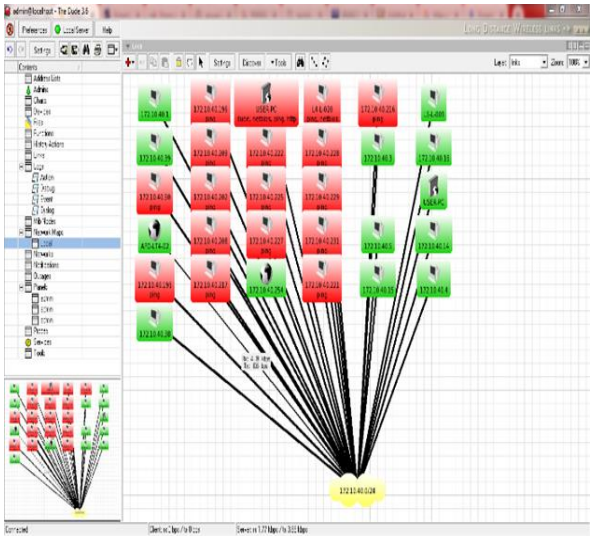


Figure 4. The network has Problems (DOWN)

Displays that the status of network devices that are on the Fl. 4 is experiencing a down or shutdown problem so that all computers that use the network cannot be used to access the internet. And it turns out that quite a lot of devices have connection problems at the time of the observation.

Network Traffic using Traffic Flow Analysis

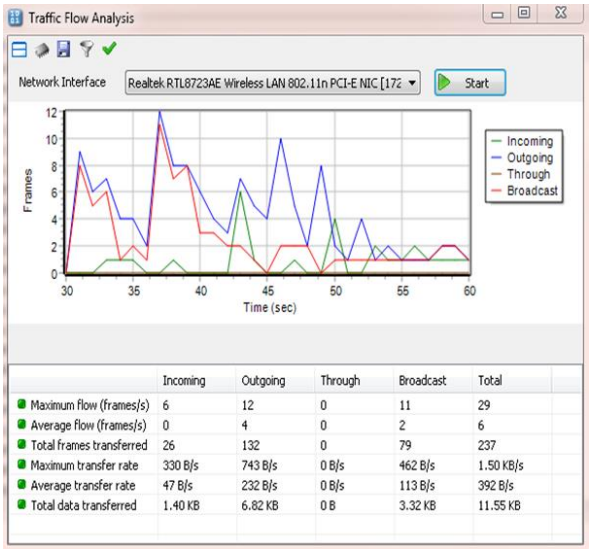
Figure 5 show the direct network services traffic:

1. Green Traffic Incoming is information that incoming data from the connection used at EBTKE Office Fl.4.
2. Blue Outgoing Traffic is the outcoming information from the connection used at EBTKE Office Fl.4.
3. Traffic Red Broadcast is a service from server devices to client devices in sending data to several client computers.

Accredited Rank 3 (Sinta 3) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti
No. 28/E/KPT/2019, September 26, 2019. Published by PPPM STMIK Nusa Mandiri

VOL. 7 NO. 2 FEBRUARY 2022
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v7i2.2786

4. Maximum flow (frames/s) used are Incoming 6, Outgoing 12, and Broadcast 11. So the Total Maximum flow is 29.
5. The average flow (frames/s) used is Incoming 0, Outgoing 4, Broadcast 2. So the Total Average flow is 6.
6. The total Transferred frames used are Incoming 26, Outgoing 132, Broadcast 79. So the total of Transferred frames is 237.
7. Total Data Transferred used are 1.40KB Incoming, 6.82KB Outgoing, and 3.32KB Broadcast. So the total of Data Transferred is 11.55KB.



	Incoming	Outgoing	Through	Broadcast	Total
Maximum flow (frames/s)	6	12	0	11	29
Average flow (frames/s)	0	4	0	2	6
Total frames transferred	26	132	0	79	237
Maximum transfer rate	330 B/s	743 B/s	0 B/s	462 B/s	1.50 KB/s
Average transfer rate	47 B/s	232 B/s	0 B/s	113 B/s	392 B/s
Total data transferred	1.40 KB	6.82 KB	0 B	3.32 KB	11.55 KB

Figure 5. Network Traffic

The diagram above showed that the outgoing transfer rate is higher than the incoming transfer rate.

CONCLUSION

The computer network management security system at the Directorate General of New, Renewable Energy and Energy Conservation (EBTKE) of the Ministry of Energy and Mineral Resources (ESDM) is made with a fairly good design and configuration so that security holes can be covered to protect data from being read by people. unauthorized persons and insert data or delete the data. The Dude MikroTik application could be used by a wireless computer network management security system to monitor network activities so that data security can be guaranteed, and it can be known whether the network is having problems or is in good condition. Unfortunately, based on the observations in this study, it can be seen that there are quite a several problematic devices that need further handling on the computer network used.

REFERENCE

[1] W. Stallings, *Data and Computer Communications*, 8th ed. New Jersey: Pearson Education, Inc., 2007.

[2] N. Y. Permana, "Tugas dan Fungsi," *Direktorat Jenderal EBTKE - Kementerian ESDM*, 19-Feb-2014. [Online]. Available: https://ebtke.esdm.go.id/profile/2/tugas.dan.fungsi. [Accessed: 01-Mar-2022].

[3] Kementerian Energi dan Sumber Daya Mineral, "Lokasi & Kontak," *ESDM*, 2007. [Online]. Available: https://www.esdm.go.id/id/profil/lokasi-kontak.

[4] S. Sujalwo, B. Handaga, and H. Supriyono, "Manajemen Jaringan Komputer Dengan Menggunakan Mikrotik Router (Computer Network Management Used With Microtic Router)," *Komuniti J. Komun. dan Teknol. Inf.*, vol. 2, no. 2, pp. 32–43, Jan. 2011.

[5] M. Subramanian, *Network management: principles and practice*. India: Pearson Education, 2010.

[6] J. S. Beasley and P. Nilkaew, *Networking Essentials*. United Kingdom: Pearson, 2012.

[7] J. Sen and S. Mehtab, *Computer and Network Security*. London: IntechOpen, 2020.

[8] R. Dube, *Internal Firewalls For Dummies®, VMware Special Edition*, 1st ed. Hoboken: John Wiley & Sons, Inc., 2021.

[9] H. Andrea, *Cisco ASA Firewall Fundamentals*, 3rd ed. Scotts Valley: CreateSpace Independent Publishing, 2014.

[10] H. Andrea, "Cisco ASA 5505 5510 5520 5540 5550 5580 Throughput and Performance," *Network Training*. [Online]. Available: https://www.networkstraining.com/cisco-asa-5505-5510-5520-5540-5550-5580/#Cisco_ASA_5520_Features_and_Specs. [Accessed: 10-Mar-2022].

[11] A. Chopra, "Security Issues of Firewall," *Int. J. P2P Netw. Trends Technol.*, vol. 22, no. 1, pp. 4–9, Jan. 2016.

[12] Sumarno, D. Hartama, I. Gunawan, H. S. Tambunan, and E. Irawan, "Optimization of Network Security Using Website Filtering With Microtic Routerboard," *J. Phys. Conf. Ser.*, vol. 1255, no. 1, p. 012076, Aug. 2019.

[13] A. A. Astari, "Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik," Universitas Nusantara PGRI Kediri, Kediri, 2018.

[14] MikroTik, "The Dude," *MikroTik*. [Online]. Available: https://mikrotik.com/thedude. [Accessed: 10-Mar-2022].

[15] Mikrotik ID, "Monitoring dengan aplikasi The Dude," *Mikrotik ID*, 2022. [Online].

Available: http://mikrotik.co.id/artikel_lihat.php?id=172. [Accessed: 01-Mar-2022].