Abstracts

rd

4th ICIBA

International Conference on Information Technology and Engineering Application

February 20 - 21, 2015

IT & Engineering For a Better Life

PALEMBANG - INDONESIA

Hosted by

Universitas Bina Darma

Program Pascasarjana

In Cooperation with

UTM

epon : 0711-515679, 515582
: 0711-515582
osite : http://iciba.binadarma.ac.id
il : iciba@binadarma.ac.id

COMPUTER SCIENCE & INFORMATION SYSTEMS

Search

Categories

Select Category

Meta

Register

Log in

Entries RSS

Comments RSS

WordPress.com

Researcher ID

ICIBA

ICIBA2015, Universitas Bina Darma, Palembang 20-21 February 2015 have been released.

Table of contents

1. **Music Retrieval using Mood Tags in Folksonomy** | *Chang Bae Moon, HyunSoo Kim, Dong-Seong Kim, Sung-Phil Heo, Byeong Man Kim (Kumoh National Institute of Technology,Gumi, Gyeongbuk, South Korea)*

2. **Geographic Information System for Optimization of Lane Road in Bandar Lampung Using Dijkstra Algorithm** | *Triyugo Winarko (STMIK Mitra Lampung)*

3. **Implementation and Analysis of LCAS (Link Capacity Adjustment Scheme) Encapsulation on Ethernet Over SDH (Synchronous Digital Hierarchy) for A Reliable Network** | *Beny Nugraha, Abdaul Hidayatir Ridho*

Follow ⟨ 93

my **Linked** in profile

Goodreads

Borobudur & Peninggalan Nabi Sulaiman
by Fahmi Basya

7 Keajaiban

(Universitas Mercu Buana)

4. **Password Designing Using Programmable Logic Device (PLD)** | *Muhammad Irmansyah, Era Madona, Nasrul (Polytechnic State of Padang Limau Manis Padang)*

5. **Risk Management Framework in Information Technology Outsourcing Project** | *Arif Ridho Lubis, Husni Lubis, Ihsan Lubis (Sekolah Tinggi Teknik Harapan)*

6. **Systems Engineering: Why is it Important ?** | *Beni Suranto (Universitas Islam Indonesia)*

7. **Tsukamoto Method in Decision Support System for Realization of Credit on Cooperative** | *Ginanjar Wiro Sasmito, Oman Somantri (Politeknik Harapan Bersama)*

8. **Prediction of Understanding of Students Under Course Lecturer Professional Use Neural Network Backpropogation** | *T. Henny Febriana Harumy, Darmeli Nasution, Yuyun Yusnida Lase (Universitas Pembangunan Pancabudi Medan)*

9. **Performance Analysis of Multiple-Computer as Real Application Clusters (RAC) Based on Storage Area Network (SAN)** | *Iyoga Don Frima Tarigan, Dong-Seong Kim (Kumoh National Institute of Technology,Gumi, Gyeongbuk, South Korea)*

10. **IPV6 Readiness Survey: The Case of Indonesian Organizations** | *Dedy Syamsuar, Peter Dell (Universitas Bina Darma, Curtin University Australia)*

11. **Similarity Analysis of Audio Steganography Combined With Rijndael Cryptography Algorithm** | *Hudson Leroy Simanjuntak, Anggoro Suryo Pramudyo, Rian Fahrizal (Universitas Sultan Ageng Tirtayasa)*

LAA's club
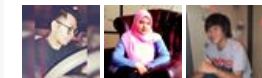
Calendar

July 2015

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

[« May](#)

12. **The Real Monitoring of Three Phases Power Based on Microcontroller Which Can Be Readed Online (Case Study in Laboratory of Microprocessor of Padang State Polytechnic)** | *Anggara Nasution, Rusfandi, Era Madona (Padang State Polytechnic)*

13. **History of Indonesian Independence Learning Media Using Interactive Story Telling For Elementary Schools Based on Android Platform** | *Yuliana Nyonata, T. Arie Setiawan Prasida, Birmanti Setia Utami (Satya Wacana Christian University)*

14. **A Type-2 Fuzzy Logic for Measurement of Meta-Management Success in Virtual Organisation** | *Muhammad Ridwan Andi Purnomo (Universitas Islam Indonesia)*

15. **Audio/Video Bridging (AVB) Protocol for Industrial Application** | Syamsul Rizal, Dong-Seong Kim (Kumoh National Institute of Technology,Gumi, Gyeongbuk, South Korea)

16. **New Pheromone Updating Mechanism for Ant Colony Optimization in Designing DNA Sequence** | *T. B. Kurniawan, Misinem, M.Z. Ahmad Nazri (Universitas Bina Darma, Univesiti Kebangsaan Malaysia)*

17. **Maximize E-Learning To Improve Students Knowledge and Interest In Learning** | *Burham Isnanto, Bambang Adiwinoto, Ellya Helmud (STMIK Atma Luhur, Bangka Belitung)*
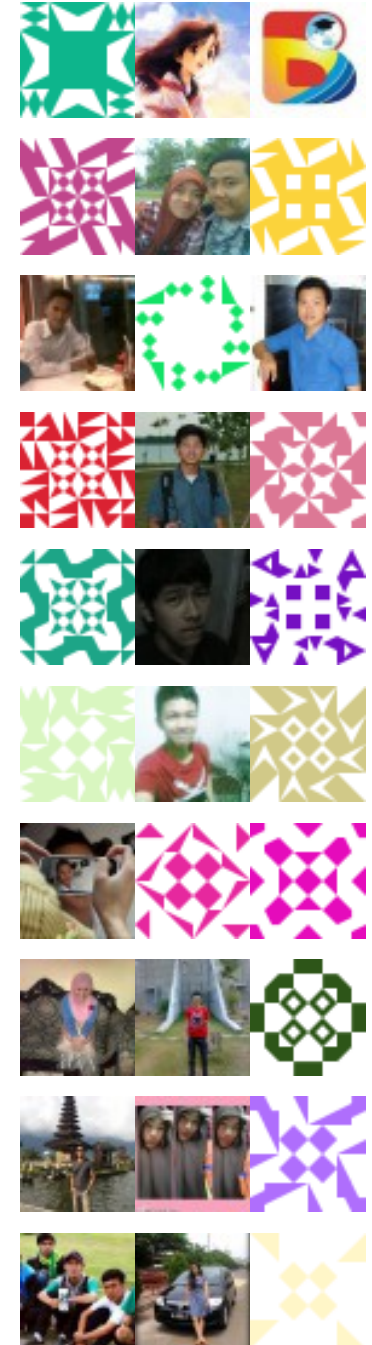
18. **Information System of Follow Up Evaluation Report Multi User Based On The Bangka Belitung Inspectorate Department** | *Ellya Helmud, Burham Isnanto, Sujono (STMIK Atma Luhur, Bangka Belitung)*

19. **Extracting Keyword for Disambiguating Name Base on The Overlap Principle** | *Mahyuddin K. M. Nasution (Universitas Sumatera Utara)*

Community

Tags

Pages

About

Fenton Reagent Accelerated Stress Test | *Muhammad Taufiq Salleh, Juhana Jaafar, Noorul Anam Mohd Norddin, Ahmad Fauzi Ismail, Mohd Hafidz Dzarfan Othman, Mukhlis Abdul Rahman, Norhaniza Yusof, Wan Norharyati Wan Salleh (Universiti Teknologi Malaysia)*

28. **The Characteristics Study of Titanium Dioxide Nanofibers Prepared by Electrospinning Method** | *Nor Azureen Mohamad Nor , Juhana Jaafar, Ahmad Fauzi Ismail, Mohd Hafiz Dzarfan Othman, Mukhlis A. Rahman, Wan Norharyati Wan Salleh, Norhaniza Yusof, Lau Woei Jye (Universiti Teknologi Malaysia)*

29. **Design of Experiment (DOE) of Compessive Strength Test For Block Paving Prototype Using Thermoplastic Waste** | *Dian Janari (Universitas Islam Indonesia)*

30. **Study of Wavelet Transformation Method for Feature Extraction Characteristics Based in Identifying Authenticity Indonesian Batik** | *Fikri (Universitas Dian Nuswantoro)*

31. **Distributed Penetration of Wireless Passwords For Wired Protected Access Type Security** | *Taqrim Ibadi, Muhammad Izman Herdiansyah, Yesi Novaria Kunang (Universitas Bina Darma)*

32. **Correspondence Archival Information Systems in Bina Darma University** | *Edo Pratama, Leon Andretti Abdillah, Susan Dian Purnamasari (Universitas Bina Darma)*

33. **Android-Based Bus Ticket Reservation Application** | *Fitriani, Leon Andretti Abdillah, Deni Erlansyah (Universitas Bina Darma)*

34. **Web Design As Support Promotion and Dissemination of Information Using Tabloid B-Smart Rich Internet Application (RIA)** | *Sri Solmawati, Yesi Novaria Kunang, Wydyanto (Universitas Bina Darma)*

Mendeley

Leon Abdillah is a member of Computer and Information Science on Mendeley.

Bib

35. **Analysis Network Security of Local Area Network (LAN) and Wifi in Dishub Kominfo Banyuasin** | *Ririn Pratama Endra Wijaya, Yesi Novaria Kunang, Widyanto (Universitas Bina Darma)*

36. **Dictionary of Prabumulih Language-Based Android** | *Murdianto, Leon Andretti Abdillah, Febriyanti Panjaitan (Universitas Bina Darma)*

37. **Geographic Information Systems of Android-Based Residential Locations in Palembang** | *Lia Novita, Leon Andretti Abdillah, Ari Muzakir (Universitas Bina Darma)*

38. **The Evaluation of Academic System of Bina Darma University on Students Satisfaction** | *Rahayu Amalia, Firdaus, Ahmad Haidar Mirza (Universitas Bina Darma)*

39. **Application of Data Mining to Determine Students Interest in Reading University Library Building Bina Darma Palembang Using Clustering Method** | *Lemi Iryani, Alex Wijaya, Andri (Universitas Bina Darma)*

40. **Decision Support System To Determine The Loan Nominal at KUD Mupakat Jaya Using Decision Tree Method** | *Mulia Puspita Sari, Ahmad Haidar Mirza, Fatmasari (Universitas Bina Darma)*

41. **SMS Security System With Encryption Decryption Blowfish Algorithm Based on Mobile Android** | *Fitri Andiyani, Yesi Novaria Kunang, Evi Yulianingsih (Universitas Bina Darma)*

Share this:

1

The 4th ICIBA 2015, International Conference on
Information Technology and Business Applications
Palembang-Indonesia, 21-22 February 2015

ANALYSIS NETWORK SECURITY OF LOCAL AREA NETWORK (LAN) AND WIFI IN DISHUB KOMINFO BANYUASIN

Ririn Pratama Endra Wijaya, Yesi Novaria Kunang, Widyanto

Informatics Engineering

Bina Darma University

r_pra_tama@yahoo.co.id, yesi_kunang@mail.binadarma.ac.id,

widyanto@mail.binadarma.ac.id

Abstract

Advances in technology have increased very rapidly, especially in the field of computer technology. That's because computer technology can help meet human needs, is why all institutions both government and non-government has a lot to take advantage of advances in computer technology. Advances in computer technology have always hand in hand with the progress of the Internet. As the Transportation Communications and Information Technology Banyuasin, government agencies have been using the Internet in the implementation of their daily activities either LAN or wifi. The existence of the LAN network and wifi gained a lot of convenience, but not necessarily the security of the data / information can be assured of the attacker. Therefore, author will conduct a LAN Network Security Analysis and Wifi on Transportation Kominfo Banyuasin using NIST standards that has three main stages, namely planning, execution, and post-execution. This study successfully tested using a technique Network Sniffing, Ping of Death / DDOS, UDP Flooding, and Social Engineering.

Keywords: Analysis, Security, *LAN*, *Wifi, NIST*

1 INTRODUCTION
1.1 Background

Advances in technology today has increased very rapidly, especially in the field of computer technology. That's because computer technology can help meet human needs, such as data processing, compute, store and present data / information. Therefore, throughout both government agencies and non-government has much to take advantage of advances in computer technology have. Advances in computer technology is always in line with the advancement of internet technology. Internet is now a requirement that must be met. Because of the internet users can get information faster. The Internet provides a lot of convenience. But behind the convenience provided by the internet there are also dangers posed by the Internet. The hazard can occur if the computer network security elements are not met. Thus the computer network security is very important to maintain the confidentiality, integrity, and avalibility, (CIA) of the data. With the use of the internet is a lot of convenience gained by Transportation Kominfo Banyuasin, but not necessarily the security of the data / information in Transportation Communications and Information Technology assured of the threat the attacker. To determine the existing security network so as to provide recommendations for improvement, so in this study, author took the title "ANALYSIS NETWORK SECURITY OF LOCAL AREA NETWORK (LAN) AND WIFI ON DISHUB KOMINFO BANYUASIN" by implementing Information Security Testing and Assessment by NIST Standards.

Sumber : Dishub Kominfo Kabupaten Banyuasin. (2011). *Rencana Induk e-Government Kabupaten Banyuasin Tahun 2012-2016.* Palembang: Publishing

1.2 Problem of Research

From the above background, this research, issues to be discussed by the author is the "How to analyze network security Local Area Network (LAN) and Wifi on Transportation Kominfo Banyuasin by applying NIST Standards?"

1.3 Scope of Problem

In order to carry out this research is focused on the issues that have been set, then the scope of this study are as follows:

a. Analyzing network security Local Area Network (LAN) and Wifi on Transportation Kominfo Banyuasin to perform penetration tests;
b. Only limited security testing, there is no prototype;
c. Looking for security holes and then make recommendations to the administrator to close loopholes;
d. Applying NIST Standards.

1.4 Purpose of Research

The purpose of this study was to determine the vulnerabilities that have not been known by the network manager Transportation Kominfo Banyuasin. So that in the future network development Transportation network administrator can perform Kominfo Banyuasin closing loopholes in order to produce a more secure network than ever and can be protected from unauthorized access or interception.

1.5 Benefit of Research

The benefits gained from this study are as follows:

a. For Kominfo Transportation Banyuasin, this research may reveal vulnerabilities that exist, so the convenience of the use of the Internet can be realized;
b. For admin Transportation network manager Kominfo Banyuasin, this research can be a reference to close security holes found networks;
c. For author, this study is as the application of science that has been obtained in college, and as an introduction to the real world;
d. For readers, the results of this study may be an additional reference materials and knowledge regarding network security Local Area Network (LAN) and Wifi.

2 RESEARCH METHODOLOGY
2.1 Object of Research

Object of research in the Department of Transportation, Communication, and Information located at office complex Pemkab Banyuasin No. 20, Sekojo Pangkalan Balai.

2.2 Method of Collecting Data

Data collected by:

a. Observation, author conducted a review directly to the object of research and then make observations, record, and analyze the existing network in the research object;
b. Interview, the author asks questions to the speakers, which have an interest in the network on the research object;
c. Literature, author conducted a literature study to locate the material on the internet and reading books related to the research conducted.

2.3 *NIST* Standarization

Planning, execution, and post-execution is working step by NIST standardization.
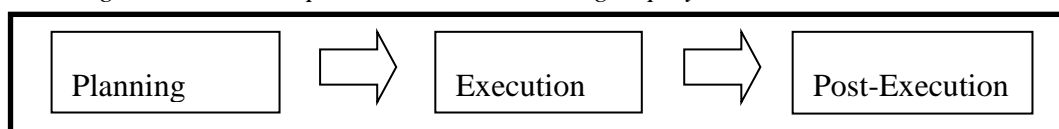
Images 1. *NIST* Standarization

Sumber : Scarfone, Karen, dkk. (2008). *Technical Guide to Information Security Testing and Assessment.* Gaithersburg: U.S. Departement of Commrce

2.3.1 Planning

It is important for the success of network security testing, the planning stage is used for gathering the necessary information in the next stage of the testing phase / execution, such assets will be analyzed / security testing, threats to assets, security controls that will be used to reduce the threat and develop a testing approach security. Network security assessment should be carried out like the other project plans, scope / object of research, requirements, test team roles and responsibilities, limitations, success factors, resources, and time.

2.3.1.1 Review Techniques

Various techniques are used by the attacker / researcher in penetrating into the LAN and WLAN networks are applied in this study are as follows:

a. Network Port and Service Identification

Network Port and Service Identification is one of the techniques that are useful for information gathering, to find an open port. The data collection was done by scanning the LAN and WLAN networks using tools that have been available on the operating system Backtrack 5R3.

b. Wireless Scanning

Wireless Scanning is the process of collecting data by scanning wifi wifi network to determine the current to then be able to do the next step is password cracking. Wireless Scanning can be done using airodump-ng tool.

3. Network Discovery

Network Discovery is the process of collecting data by scanning the network to find active devices to then be offensive to the active device and tool for network discovery is netdiscover.

4. Social Engineering

Social engineering is a hacking technique which utilizes the weakest element is human. The objective of this technique which collects data as much as possible in order to meet the needs of the data when the process is executed and the execution of this technique is usually done manually or using tools, such as network administrators interviewed.

5. System Configuration Review

System Configuration Review is the process of analyzing the configuration of the WLAN network security system. The purpose of this technique is to determine the configuration ditahap security system, a way to open / view the configuration that has been made. With so author can see if wifi is already configured with safe or unsafe.

6. Password Cracking

Password cracking is the process of identifying weak passwords. This technique aims to find a password that is used on a particular network. This technique can be run manually or by using a tool like aircrack-ng.

7. Network Sniffing

Network Sniffing is the man-in-the-middle attacker to install a tool that is in the middle of the track network used by the user. The purpose of this attack is to monitor packets passing through the network, so that the attacker can capture the username and password that the user uses the network. In this study, author used a script ettercap as a tool for network sniffing.

8. Ping of Death / DDOS

Ping of Death / DDOS attack is to send ICMP packets to a computer as many users who are connected to the network is available. The purpose of this attack is to overwhelm the user computer ICMP packets so that the user will have uninterrupted connection to the network as a buffer over flow. This attack can be done manually and by using the tool mdk3.

9. UDP Flooding

UDP Flooding is the attack by sending a UDP packet to a computer as many users connected to the network is available. The purpose of this attack is to flood the user's computer with UDP packets so that the computer will experience disruption to the network or even disconnect. This attack uses UDP Flooder tool of application NetTool.

3 RESULTS AND DISCUSSION

3.1 Execution

3.1.1 Target Identification and Analysis Techniques

Testing techniques can identify a network of potential vulnerabilities. Identification can be done manually and using tools. But in general, the testing is done by using the tools in accordance with the technique and ability of the test team / author.

3.1.1.1 Network Port and Service Identification

To apply the techniques of network ports and service identification Zenmap author used tool. Zenmap is the same tool nmap but differs in its use. Zenmap is a graphical tool nmap is tool-based and CLI (Command Line Interface). Zenmap useful for gathering information gathering like finding open ports, the router MAC address, operating system used, the router is being used, what version, and others. In this study, author used Zenmap tool that has been found on the operating system backtrack 5R3.

3.1.1.2 Wireless Scanning

To implement wireless scanning techniques author use airodump-ng tool. Airodump-ng is a tool to identify the current wireless. With this tool, author can know the BSSID / MAC address, channel, encryption, cipher, and the ESSID of the access point. This tool found on the operating system backtrack 5R3.

3.1.1.3 Network Discovery

To implement network discovery techniques author use tool NetDiscover. NetDiscover is a tool to determine the IP and MAC addresses of users who are connected to a network. This tool has been installed on the operating system backtrack 5R3.

3.1.1.4 Social Engineering

At this stage, investigators probing the target to find the data that is relevant to the network on the object of research by interviewing the network administrator.

3.1.1.5 System Configuration Review

To apply technique system configuration review, but author do not use the tool manually. At this stage investigators probing the target by looking out of the wifi network configuration.

3.1.2 Target Vulnerability Validation Techniques

This stage is a test to confirm the existence of vulnerabilities, and can be done manually or by using the tools, depending on the particular technique used and the skill test team. Target validation techniques including password cracking susceptibility, penetration testing, social engineering, and testing of network security.

3.2 Post-Execution

Post-Execution is the final stage of testing by NIST standardization. This stage is the evaluation of the test results of the previous stage. At this stage the priority vulnerabilities or grouped based on the impact caused by the vulnerability. Analyze the root cause of the existence of these vulnerabilities and provide recommendations on how the response. This stage is the final report of the study the author did.

3.2.1 Testing Results

Test results are reports of testing LAN network, wifi KOMINFO, and wifi PPID 2014 by applying the techniques that have been determined in the previous stage.

Table 1. Network security testing results

No	Attack Techniques	Network			Tools	Description
		LAN	Wifi KOMINFO	Wifi PPID 2014		
01	Password Cracking	not success	not success	not success	Manual, aircrack-ng	Matching Password obtained from interviews to related parties
02	Network Sniffing	Success	not success	not success	Ettercap	Capture the network packets that pass through in-sniffing, such as username and password
03	Ping of Death / DDOS	Success	Success	Success	Manual, mdk3	Send package as much as possible and continuously to the network used

| 04 | UDP Flooding | Success | Success | Success | NetTools | Send UDP packets as much and continuously to the user computer |
| 05 | Social Engineering | not success | Success | Success | Manual | Utilizing human weakness, to seek information about the passwords on the network used |

3.2.2 Identification of Causes and How to cope
a. Password Cracking

From the use of password cracking techniques investigators failed to get the password from LAN network or wifi network. It can be concluded that the password used either technology or combination of characters is good enough so that the author did not succeed in penetrating.

b. Network Sniffing

By using the tool Ettercap author succeeded in intercepting or wifi LAN network path. But here which can be monitored only user who uses http protocol only, not the https protocol. Therefore the user must be careful in using the network again. Do not visit sites that do not have a certificate for security validation. Username and password so that we use can not be monitored by the attacker.

c. Ping of Death / DDOS

Using the technique of Ping of Death / DDOS author managed to test the security of the LAN network and wifi. Even if done using a laptop and a few a long time, this technique can make down the server or Wifi / Access Point that is used in the research object. Because the technique with this technique, an attacker can easily send packets continuously and as much as possible to make available the network down. When the network is down, then the elements of availability has not met again. How to overcome it is to install the Firewall / IP Tables because when there ICMP packets or packets that can make down the network can be rejected / in-drop so that the package can not create a buffer over flow available networks and availability elements remain unfulfilled.

d. UDP Flooding

Using UDP Flooding engineering author succeeded in making the user to decrease the performance of your computer. In this technique the attacker sends UDP packets continuously and as much as possible to the user's computer. Even if the attack was allowed to continue for a long time, it can make the user's computer to hang. The solution of this attack is to install a firewall / IP Tables so that such attacks can be rejected.

e. Social Engineering

Using this technique, the author managed to get the password of wifi but not the LAN network password. In this technique the author exploit human weaknesses in creating a password. Solution of attack using this technique is returned to the user itself. How to maintain the confidentiality of the data created themselves.

4 CONCLUSION

Based on the results of research and discussion that has been described in previous chapters, in this study, entitled Analysis Network Security of Local Area Network (LAN) and Wifi in Dishub Kominfo Banyuasin, it can be concluded that many cracks were found by author that can be executed so as to cause lose one element (CIA), the results of this study can contribute suggestions for improvement in terms network security of LAN and wifi on the next phase of network development and testing techniques in LAN network and wifi Transportation Kominfo Banyuasin still so much that has not been tested in this study and that means not all the cracks in the LAN network and wifi in the Transportation Communications and Information Technology Banyuasin the author found.

References

Dishub Kominfo Kabupaten Banyuasin. (2011). *Rencana Induk e-Government Kabupaten Banyuasin Tahun 2012-2016.* Palembang: Publishing

Scarfone, Karen, dkk. (2008). *Technical Guide to Information Security Testing and Assessment.* Gaithersburg: U.S. Departement of Commerce