Computer Network Audit using Wireshark and Metasploit Framework
(Case Study: STMIK STIKOM Bali Jimbaran Campus II)

Rifky Lana Rahardian [1], Muhammad Anshari[2], Nyoman Putra Sastra[3]
[1][2] Department of Electrical and Computer Engineering, Post Graduate Program, Udayana University,
Email: hellboy.kiki@gmail.com
[3]Department of Electrical and Computer Engineering, Udayana University

Abstract--Advances in Information and Communication Technology (ICT) has been widely used by various organizations including educational institutions. One of the educational institutions that always take advantage of ICT in business processes as well as lectures there STIKOM Bali Jimbaran Campus II. STIKOM Bali Jimbaran Campus II is a private college branch of STMIK STIKOM Bali located at Jl. Raya Kampus Udayana Bali Jimbaran. The campus is still relatively new, a new due process entered its second year in the lecture. In terms of information systems and business processes that run STIKOM Bali Jimbaran Campus II refers to the Campus Master in Renon. Network architecture on STMIK STIKOM Bali Campus II Jimbaran arguably not perfect, for the authors will try to conduct an audit of computer networks using Wireshark and Metasploit on STMIK STIKOM Bali Campus II Jimbaran order to produce an output in the form of advice in the development of network architecture at STMIK STIKOM Bali Campus II Jimbaran future.
Keywords: Audit, Wireshark, Metasploit, STMIK STIKOM Bali

I. PRELIMINARY

A. Background

Network architecture is the most expensive to be expanded or built on an institution. Company executives assess the development of a network architecture expend too many resources, so keep using network architectures that are less secure. In this study, the authors will review the issue of network security at educational institutions that STMIK STIKOM Bali Jimbaran Campus II by conducting audits.

STMIK STIKOM Bali Jimbaran Campus II is an agency in the field of education is one of the many colleges are aware of the importance of a secure network architecture. STMIK STIKOM Bali Jimbaran Campus II is a private college branch of STMIK STIKOM Bali located at Jl. Raya Kampus Udayana Bali Jimbaran. The campus is still relatively new, a new due process entered its second year in the lecture. In terms of information systems and business processes that run STIKOM Bali Jimbaran Campus II refers to the Campus Master in Renon.

Network architecture on STMIK STIKOM Bali Campus II Jimbaran arguably not perfect, for the authors will try to conduct an audit of computer networks using Wireshark and metasploit on STMIK STIKOM Bali Campus II Jimbaran order to produce an output in the form of advice in the development of network architecture at STMIK STIKOM Bali Campus II Jimbaran future.

B. Problem Formulation

The formulation of problem in this study is:

1. How to Use Wireshark and Metasploit in the audit process in STMIK STIKOM Bali Jimbaran Campus II.
2. Security How STMIK STIKOM network architecture on Bali Jimbaran Campus II.

C. Objective

Assess the level of maturity (Maturity Level) the extent to which a standard computer network security in Bali from 2 STIKOM STMIK audit methods in Wireshark and Metasploit.

D. Benefits Research The

Benefits of the implementation of the audit is the result of research is expected to be used as a reference to assess the level of maturity that is useful to measure the standard of computer network security in STMIK STIKOM Bali Jimbaran Campus II.

II. LITERATURE REVIEW

A. STMIK STIKOM Bali

Starting from the convergence of the observer, lovers and practitioners are Prof. Dr. Made Bandem, MA., (Then Rector of ISI Jogjakarta), Dr. Dadang Hermawan (practitioner education), Drs. Ida Bagus Dharmadiaksa, M.Sc., Ak. (Lecturer) and Drs. Satria Dharma (education practitioners) in the year 2000 were so pay attention to the rapid and dynamic development of information and communication technology (ICT) in the world, including in Indonesia and Bali, but on the other hand, college field of ICT up to undergraduate level yet.

Then on May 20, 2001, stood Widya Dharma Shanti will be Organized Agency Colleges and subsequent construction permit is referred STMIK STIKOM Bali to the Directorate General of Higher Education Ministry of National Education. With a variety of businesses and the twists and turns permits and prayer, then on August 10, 2002 exit permits referred to by number 157 / D / O / 2002 with two departments / study

programs namely Computer Systems (S1) and Information Management (D3) ago in 2009 there was an additional new courses namely information System (S1).

Currently, STIKOM Bali has become international university that is trusted by society, as evidenced by the number of college students who are not less than 6,000 people and alumni of nearly 4,000 people (2015). In addition, various tri dharma cooperation in higher education has been carried out by various parties, both government agencies, agencies / private companies, state enterprises, enterprises, universities both within and outside the country.

STIKOM Bali Jimbaran Campus II is a private college branch of STMIK STIKOM Bali located at Jl. Raya Kampus Udayana Bali Jimbaran. The campus is still relatively new, a new due process entered its second year in the lecture. In terms of information systems and business processes that run STIKOM Bali Campus II Jimbaran refers to the Campus Master in Renon[1].

B. Wireshark

Wireshark Network Protocol Analyzer is a software application (software) used to be able to see and try to capture the network packets and attempt to show all information on the package as detailed as possible. Open Source of Wireshark to use Graphical User Interface (GUI).

Wireshark Network Protocol Analyzer has become very popular and has become standard in many industries, and is a follow-up project that started in 1998. Developers worldwide have contributed develop this software. With all the capabilities it has, Wireshark is used by network professionals for analysis, troubleshooting, software and protocol development, and is also used for educational purposes. Wireshark is able to capture the packets of data that exist on the network. All types of packet protocols of information in various formats will be easily captured and analyzed[2].

C. Measurement Rate Maturity (Maturity Level)

Maturity models are a method for measuring the level of management development roses, which means is to measure the extent to which the management capabilities. How better development or management capability depending on the achievement of the objectives COBIT. For example, there are some critical processes and systems that require tighter security management than other processes and systems that are not so critical. On the other hand, the degree of satisfaction and control needed to be applied to a process of risk appetite was boosted on Enterprise and compliance requirements are applied.

Proper application on IT governance in an Enterprise environment, depending on the achievement of the three aspects of maturity (capability, coverage and control). Increased maturity will reduce risk and improve efficiency, encourage the reduction of errors and increase the quantity of processes that can be expected to encourage quality and cost efficiency associated with the use of IT resources[3].

Maturity models can be used to map:

a. Status of IT management company at the time.
b. Status industry standard in IT today (as a comparison) the
c. status of international standards in the field of IT today (as a comparison)
d. strategic management of IT companies (expectations of the company to the position of managing IT company)

Calculation of Index *Maturity* Level:

$$Index\ Maturity\ Attribute\ = \frac{\sum(Total\ Solution)}{number\ of\ Respondents} \quad (1)$$

D. Metasploit

Metasploit is a widely-used application as exploitation tools in hacking and IT security, this tool is widely used both by a beginner or a professional. Metasploit is defined as a framework to carry out cyber exploitation, as a framework so has support to create an exploit unknown vulnerabilities in a network.

III. RESEARCH METHODOLOGY

The study was conducted in Campus II STMIK STIKOM Bali Jimbaran within 1 week. Stages of the audit is carried out as follows:

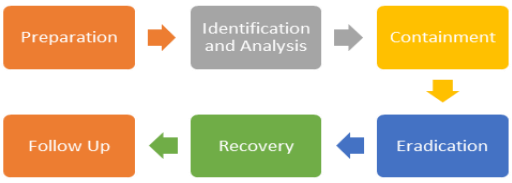

Figure 1 Audit Trails

1. Preparation

   Preparation is the most important step in dealing with attacks on computer networks. Procedures and guidelines are clear and complete to be prepared thoroughly before the attack occurred. Each organization may be a victim of an attack on the network, either directly or indirectly. Having a solid plan will help reduce the risk and mitigate the adverse effects of attacks[4].

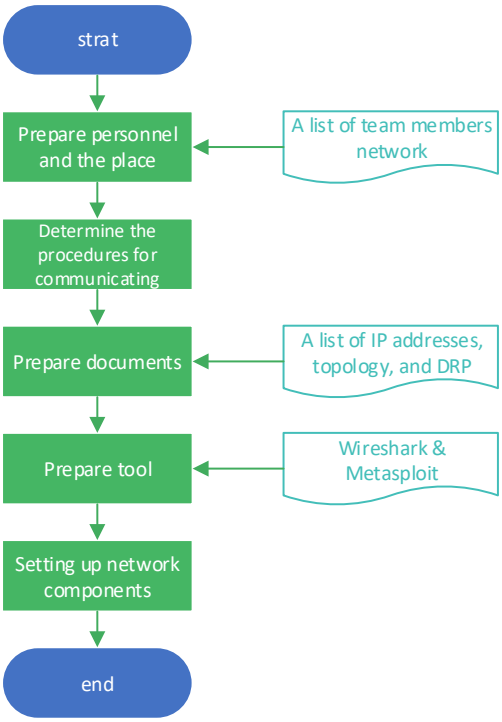

Figure 2 Stages of Preparation

2. Identification and Analysis

Early indicators that there was an attack on the network is covering poor network performance, service can't be accessed or crash. Ability system to identify and understand the nature of the attack and the target will assist in the containment and recovery. To this end, organizations require tools that provide visibility of information technology to infrastructure they manage. Before the attack occurred on the network, reconnaissance of targets made by attackers, including vulnerability scanning contained in the target tissue, the vulnerability can be determined by sending packets to the target host defects to analyze changes within a certain response time.

These surveillance activities may be difficult to detect, especially since it can occur before an attack occurs. An attacker also has the knowledge to ensure traffic scanning does not pass the threshold required to trigger the alarm from network monitoring tools. However, there is a possibility provided intelligence techniques which indicates an increased likelihood of attacks against computer networks of an organization[4].

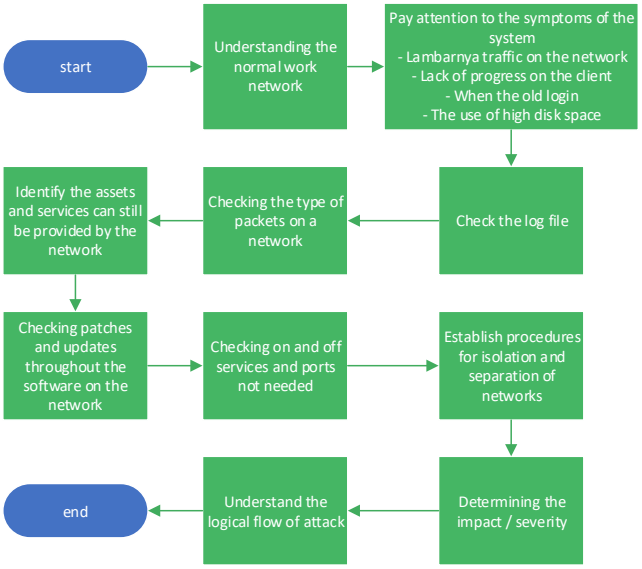

Figure 3 Stages of Identification and Analysis

3. Containment

Having a plan of detention that have been determined before the attack for a number of scenarios will significantly improve the speed of response and the damage caused by the attack on the network. For example, the containment strategy for a mail server may be different from the one for the web server. Underestimate the importance of this phase can lead to errors and significant damage. Therefore, understanding the nature of the attacks on the network and document-related decision-making process is very important. An organization must clearly identify the perimeter of the network and assets affected by the attack. Load balancers, firewalls modern technology (Deep Packet Inspection, proxy, application layer filtering) of content caching, dynamic DNS service are some of the tools that organizations can utilize to accommodate an attack on ongoing network attack[4].

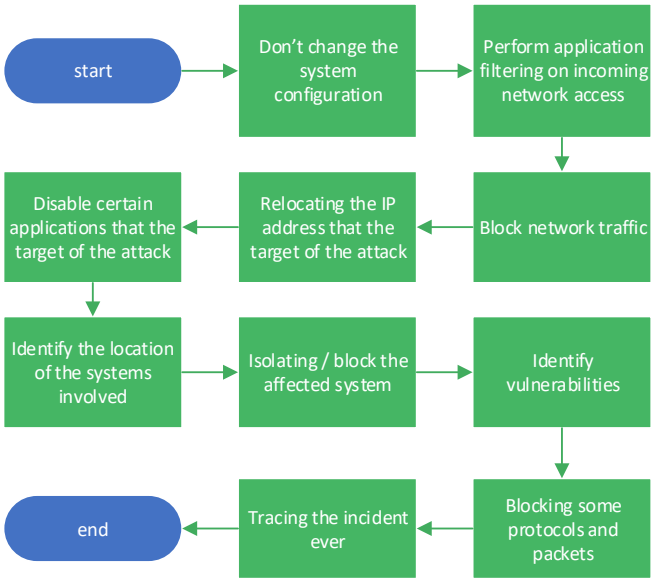

Figure 4 Stages of Containment

4. Eradication

Eradication stage is the stage to do a deeper analysis of the evidence that had been held, at this stage of the analysis process multiple log files on the server, network-enabled devices, IDS, firewall, file systems, and applications. At this stage, the forensic analysis of forensic evidence success of the process is determined by the quality and quantity of information collected. Log files can be an important source of information for the forensic process. Log files contain information about various system resources, processes and user activity. Protocol analyzer, sniffer, SMTP, DHCP, FTP and WWW, router, firewall, and almost all system activity or user can be collected in a log file. But if the system administrator can't be recorded, then the facts needed to connect actors with no incidents. Unfortunately, the clever attackers and criminals know this and its first objective is damage or alter log files to hide their activities.

The second thing that is important but often forgotten is the system clock. Recording a file associated with a time stamp and date stamp that allows the forensic analyst to determine the sequence of events. But if the system clock is not corrected / calibrated periodically can be turned off from anywhere from a few seconds up to several hours. This causes a problem because the correlation between log files from different computers. Different clock system would make it difficult if not impossible to correlate events. The simple solution to synchronize clocks across server and the system is running on a UNIX daemon like NTPD daemon, time and date of the system must periodically have synchronized with an atomic clock that is provided by the government[4]

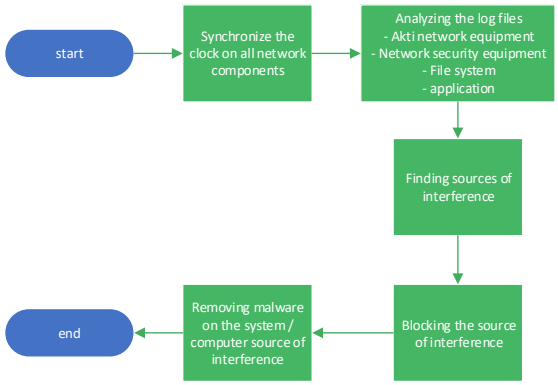

Figure 5 Stages of Eradication

5. Recovery

Depending on the strategy of the work at this stage of detention and sensitivity to the impact caused, the organization may be at different pressures to recover from network attacks. Understanding the characteristics of the attack required for rapid recovery and proper[4].

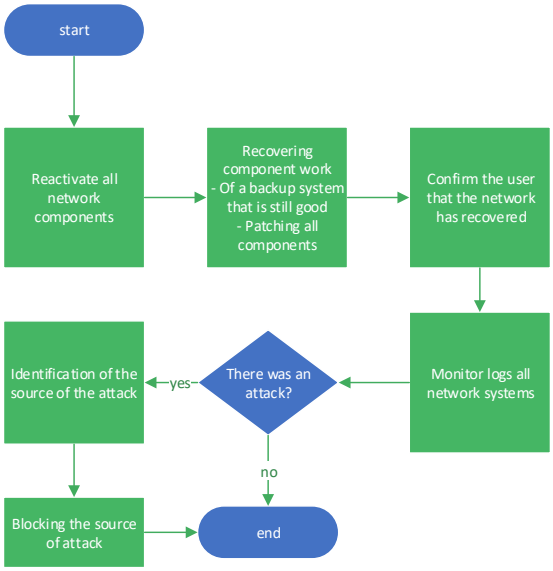

Figure 6 Recovery

6. Phase Follow-up

Stage where all the previous stages have been passed, the purpose of this phase is to,

a. Reporting, a report on the steps and the results have been obtained on the handling of the incident that has been done. Documenting the impact and cost of incidents of attacks on the network.
b. Learning, is a very important step that is often overlooked. Lessons should be learned from the activities as soon as possible after the incident handling over. All the decisions and measures taken throughout the cycle of incident response should be

reviewed. All procedures should be reviewed to see where improvements can be made.

c. Increased awareness of network security, to conduct a review after each event, will allow organizations to perform continuous improvement and potentially at a significant reduction due to the impact of incidents.

d. Allows renewal of the following documents:
   - Standard Operating Procedures
   - Emergency Operating Procedures
   - Disaster Recovery Plan (DRP)[4]

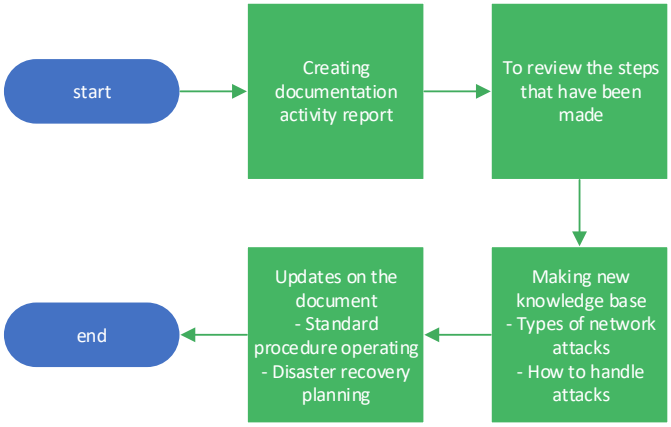

Figure 7 Phase Follow-up

IV. DISCUSSIONS

After conducting the audit process, it can result in the following:

1. Port frequently used
2. site frequented
3. types of files that are often downloaded

Table 1 Frequently used ports

PORT	TCP	UDP	KETERANGAN
7	TCP	UDP	Echo protocol (protokol untuk ping)
15	TCP	UDP	Netstat service (melihat aktivitas jaringan)
20	TCP		FTP (File Transfer Protocol, Default data)
21	TCP		FTP (File Transfer Protocol, control, connection dialog)
22	TCP		SSH (Sistem secure shell), SCP (SSH untuk copy)
23	TCP		Telnet
25	TCP		SMTP (outgoing email)
43	TCP		Whois protocol (command untuk melihat informasi host dalam jaringan)
53	TCP	UDP	Domain name server (DNS)
67		UDP	Dinamic Host Connection Protocol (DHCP)
80	TCP	UDP	HTTP
110	TCP	UDP	Pop 3 (incoming email)
137	TCP	UDP	Netbios name service
138	TCP	UDP	Netbios Datagram service
139	TCP	UDP	Netbios Session service
220	TCP	UDP	Internet message Access protocol (IMAP) vertion 3
389	TCP	UDP	Lighweight Directory Access Protocol (merupakan DHCP di Linux)
443	TCP		HTTPS (versi HTTP yang secure / aman)
513	TCP		Remote login (melakukan login remote desktop)
520		UDP	Routing information protocol (untuk melihat routing jaringan)
1194	TCP	UDP	openVPN (virtual private network) untuk konek ke komputer di luar jaringan
5900	TCP	UDP	Virtual network computing (VNC) , remote komputer
8080	TCP		HTTP web proxy
10000	TCP		Webmin Linux

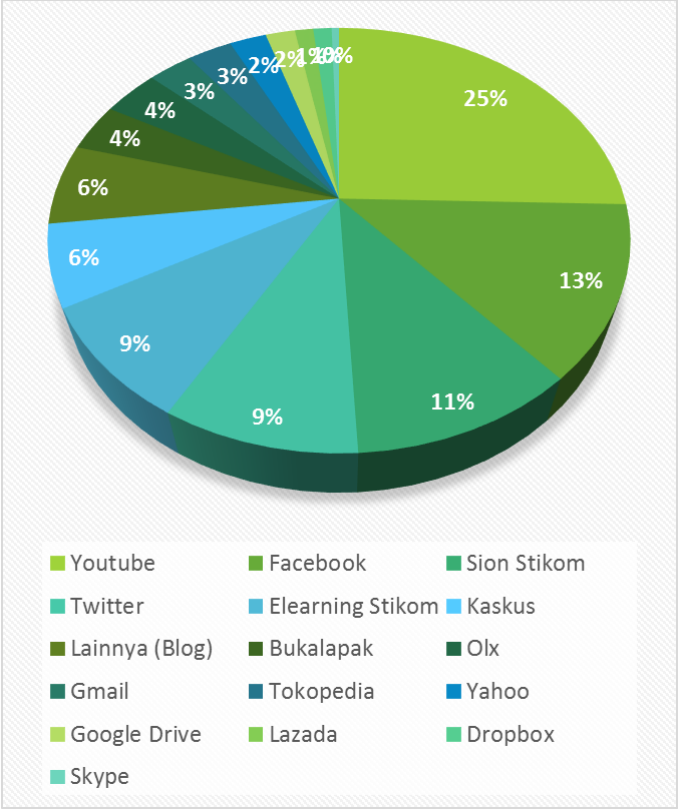

Figure 8 Frequently visited sites

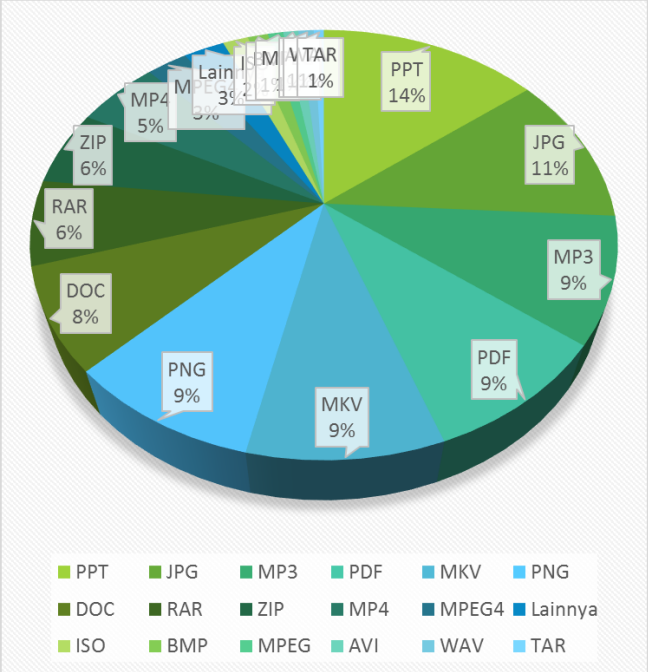

Figure 9 File Types Frequently downloaded

V. CONCLUSIONS AND RECOMMENDATIONS

A. Conclusions

From the research and design of network audit computer by using Wireshark and metasploit on STMIK STIKOM Bali Campus II Jimbaran can be concluded as follows:

1. Scanning is done using Wireshark and metasploit rated stable as STMIK STIKOM Bali Jimbaran Campus II is already implementing network management and sharing of good bandwidth, so the author does not take long in the scanning process audit. Only STMIK STIKOM Bali Campus II Jimbaran still rely on one internet service provider (ISP) that is only BIZNET, so if there is an interruption in the ISP business processes that exist in STMIK STIKOM Bali Campus II Jimbaran will be disturbed because the whole system of processing data at STMIK STIKOM Bali Jimbaran Campus II WEB based
2. Port that is often used is HTTP and HTTPS ports.
3. Frequently visited sites is YouTube, Facebook and SION STIKOM.
4. The file types are frequently downloaded PPT.

B. Recommendations

Advice can be given related to this research is to perform additional internet service provider (ISP) and carry out the implementation of disaster recovery planning (DRP) on a computer network in STMIK STIKOM Bali Jimbaran Campus II.

REFERENCES

[1] S. STIKOM Bali, "Sejarah STMIK STIKOM Bali, http://www.stikom-bali.ac.id/act/profile/sejarah.html." Accessed on Desember 9, 2016.
[2] W. Sarono, "Computer Network Monitoring With Static Routing-Based DNS Server Wiresharking," 2015.
[3] O. Roland, L. Sihombing, and M. Zulfin, "Performance Analysis of Traffic WEB Browser With Ethereal Network Protocol Analyzer On Client-Server System," Jun. 2013.
[4] "Standart Operating Procedur." Direktorat Keamanan Informasi, Direktorat Jendral Aplikasi Informatika.