

A Project Documentation Presented

To the Faculty of School of Computing and Information Technology

Asia Pacific College

Magallanes, City of Makati

**Development of NETSEC MANAGER:**

**A Network Security Utility System**

In partial fulfillment

Of the Requirements in

Software Development (SOFTDEV)

Class of 3rd Term for School Year 2015-2016

Presented by:

Abinal, Arianne Wisdom M. (Project Developer)

Cejoco, Pamela Kimberly T. (Project Developer)

Lachica, Aliana Marie R. (Project Manager/Documenter)

Reyes, Maria Herminia C. (Project Researcher)

Presented to:

Mr. Edmundo Casino

April 2016

**TABLE OF CONTENTS**

**PRELIMINARIES**

Title PageI

Table of ContentsII

**INTRODUCTION**

Project Objectives1

Abstract2

Background3

System Analysis4

Recommendations5

**SYSTEM DIAGRAMS**

Figure 16

Figure 27

Figure 2.18

Figure 2.29

Figure 2.310

Figure 2.411

Figure 2.512

Figure 2.613

Figure 2.714

Figure 2.815

Figure 316

Figure 417

Figure 518

**PROJECT MODULE SCREENSHOTS**

Figure 619

Figure 6.120

Figure 6.221

Figure 6.322

Figure 6.423

Figure 6.524

Figure 6.625

Figure 6.726

Figure 6.827

Figure 6.928

**SOURCE CODE LISTING**

Login Module29

Main Menu Module31

Data Analysis Module33

Attack Adviser Module36

Rules Module39

System Information Module56

Open Configuration File Module59

Cheat Sheet Module61

Process Module (Scripts)66

**APPENDIX**70

**BIBLIOGRAPHY**72

**PROJECT OBJECTIVES**

The general objective of the study is to develop a Network Utility System that will cater the needs of the network administrator in network security.

Specifically the study aims:

1. To design and develop utility system with the following features:
2. ***Network Scanner*** compose of python scripts that was intended to scan the network to determine the details of each packets passing through the network.
3. ***Intrusion Detection System*** that detects the rules that was set to the network and the data allowed by the system’s firewall.
4. ***Network Mapper*** uses NMAP third party software to create a map of the network to scan active and inactive hosts, open and closed ports within a network.
5. ***Network-Attack Adviser*** helps the administrator to mitigate common network attack.
6. ***Logs Generator*** is the one responsible in collecting the scan results and saving it to a database.
7. To design and develop a utility system that will help network administrator in mitigating common network attacks
8. To design and develop a utility system that will generate a logs which will serve as a report for the network administrator while the system is running.

**ABSTRACT**

NetSec Manager: A Network Security Utility Software developed to support network administrators in scanning network for active ports, mapping the network to locate up and down host, detects the rules that was set to the network for managing network activities, generate logs results and advise common network attacks. **Network Scanner** helps administrator to scan active ports within the network, scan result will be saved in a database where the administrator can access and view the result via **Logs Generator.** Another feature of NetSec Manager is the **Network-Attack Adviser** which contains a list of common network attacks together with its countermeasure or mitigation. The fourth feature is the **Network Mapper** which to create a map of the network to scan up and down host, open and closed ports within a network. Lastly, it has **Intrusion Detection System** that can be used to detect the rules set within the network and the data allowed by the firewall. The proponents used Visual Basic to create the graphical user interface of the system because of its complexity and easy to use. It has also the capability of connecting process like Python programming language that the proponents use to create the process of each features. On the other hand, MySQL was considered to be the storage or database for result generator. Beneficiaries of the study will be the network and security administrator because the level of knowledge will fit the application. NetSec Manager was created to measure the data security in the network, robustness of the application, user-friendliness and timeliness of the application.

**BACKGROUND**

The world’s interconnection has become complex due to the improvements in technology and the Internet. With the advent in the development of these improvements, computer and network security has become a major concern. For instance, a certain person access a malicious site without knowing that there is an attacker behind that site that can destroy or retrieve important data in a computer or a server. Because of this occurrence, a lot of important transactions can be affected. Worst, most of these destructive programs have the capabilities of not being detected by an antivirus or an intrusion detection system. In addition, these strategies is not common to all people and several software can detect it. Every year, there are reports of security issues – not only in individual devices, but also through the network. Though there are different security and protection tools available online, still threats are becoming more sophisticated as time passes.

A number of tools are available online developed by the open source community – where most of these open-source programs are helpful in protecting the network itself, regardless of the number of clients connected to the network. With proper configuration and execution, these programs will be helpful for network administrators in managing the network.

Because of these observations, the need for a program that protect a system increase. The proponents planned creating a new type of system that will serve as a multi-tool for network administrators that will not only view and manage a network, but can also generate results and can detect rules that was set for the network.

**SYSTEM ANALYSIS**

Data loss, hacking and fraud are now encountered by IT people every day. Every hour, a new malware is created that can destroy or steal millions of data, this scenario can happen inside and outside of IT field. This problem has been occurring for the past years and increases the damage percentage every day. With this problem, the developers created a system which will help to lessen this problem by monitoring the network with a scanner that network administrators can use to locate the active ports, a system that can map the up and downs host and detect data allowed by the firewall. The system also aims to lessen the reports of malicious activities happening in a specific network where several people created tunnels and pathway from outside causing damages not only to data and department but also to one’s company name. The developers hope that after this system has been used and deploy into several system, it can prove that a small system can solve a huge crime within the cyber world.

**RECOMMENDATIONS**

The NetSec Manager was developed based on a theory that there exists a behavior in each and every network activity – either malicious or not. It has the capability to detect some of the malicious activities and the common attacks; scan packets passing through the network; map the network through the up and down hosts, and open and closed ports; and save logs to the database. The NetSec Manager used two third party applications, namely NMap and Snort, in order to produce more accurate results. The system was created using Python 2.7.11 and Visual Basic, and tested in Windows 8/8.1/10 operating systems. The logs were saved in MySQL database using XAMPP. Since this program focuses on network analysis, As per NetSec Manager operations, the possible beneficiaries of the system are the network and security administrator since the main features of this system is about scanning the network, generating scan results for monitoring, advising mitigation for common network attacks, intrusion detection system that will detect data allowed by the firewall and the event viewer which will display the processes in the terminal. Other beneficiaries may be the IT specialist who is also aware of this features.