INFORMATION DETECTION WITH COVERT CHANNEL

NURUL FAZREEN BINTI NOORASHID

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

INFORMATION DETECTION WITH COVERT CHANNEL

NURUL FAZREEN BINTI NOORASHID

This report is submitted in partial fulfillment of the requirements for the

Bachelor of Computer Science (Computer Security)

FACULTY OF INFORMATION AND COMMUNICATION TECHNIOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

BORANG PENGESAHAN STATUS TESIS

JUDUL : INFORMATION DETECTION WITH COVERT CHANNEL

SESI PENGAJIAN : 2016 / 2017

Saya, NURUL FAZREEN BINTI NOORASHID

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat Salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat Salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/ badan di mana penyelidikan dijalankan)

_____ TIDAK TERHAD

(TANDATANGAN PENULIS)

Alamat tetap : No 2 Jalan Tanjung Penawar
30/128 Taman Sri Orkid 40460
Shah Alam Selangor

Tarikh: 24/8/17

(TANDATANGAN PENYELIA)

Prof Madya Dr Mohd Faizal Bin Abdollah

Tarikh: 24/8/17

DECLARATION

I hereby declare that this project report entitled

INFORMATION DETECTION WITH COVERT CHANNEL

Is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _______________ DATE: 24/5/17

(NURUL FAZREEN BINTI NOORASHID)

SUPERVISOR : _______________ DATE: 24/5/17

(PM DR. MOHD FAIZAL BIN ABDOLLAH)

DEDICATION

Alhamdulillah

All praise belongs to Allah.

To my parents Noorashid Bin Omar and Laila Manja Binti Mohd Yunus, thank you for your unwavering support and encouragement during the past three years of my bachelor journey.

Finally, I would like to thank lecturer and supervisor, PM DR. Mohd Faizal Bin Abdollah cause without his early inspiration, coaching and enthusiasm none of this would have happened.

ACKNOWLEDGEMENT

Thanks to Almighty ALLAH for giving me strength and ability to learn and complete this Projek Sarjana Muda.

To my beloved parents, Noorashid Bin Omar and Laila Manja Binti Mohd Yunus thanks for always being there for me during the good and bad. Thanks for supporting and encouraging me to do my best. Most of all, thanks for always believing in me, even when I didn't believe in myself.

To my friends, thank you for listening, offering me advice, and supporting me through this entire project. Special thanks to my TKJBlueHouse's members A'aisyah Mardhiyyah, Nafisatun Naja, Nur Ameera Natasha, Nur Liyana Nadhirah, Ernees Insyirah, Nur Hazwani, Nurul Fazlizah and Elyna Najiha who is my housemates and also course mates. We all have been together having each other back for these past few months and keep supporting each other to finishing up our individual final year project. I wholeheartedly appreciate everything you all have done for me. Thank you so much.

Last but not least, I would like to thank my supervisor PM Dr. Mohd Faizal Bin Abdollah for his guidance, support and encouragement to me throughout this project.

ABSTRACT

The term covert channel was first introduced by Lampson and designates an information flow that violates a system's security policy. In a system, this policy can define who is allowed to communicate with whom, through which channels, and forbid all exchanges other than these legitimate ones. A covert channel is a misuse use of a system by two legal users. These users have access to system's functionalities, but use them in a way that bypasses the security policy (for instance to create a communication channel between two users that are not allowed to communicate usually the user is in different privilege, or to pass information between authorized users without paying for it, etc.). One usual assumption is that both corrupted users know perfectly the system, and have agreed on a particular use of the functionalities to encode and decode information. The problem statements are user might not have any knowledge about what is covert channel, user are exposed to malicious data that is embedded in network, it is difficult to identify the culprit that involved in covert communication channel and covert channel can result to exploitation of communication channel to transfer information in manner that is violates the system security policy. The objectives in this project are to study and describe what covert channel is, develop rules that can detect covert channel in network and test the rules in the IDS system rules. Methodology used in this project is incremental model and the project contribution for this project is comparing the normal tcp/ip header with the tcp/ip header which contain covert message. From that a rules can be created on detecting covert channel in TCP/IP by using snort program.

ABSTRAK

Saluran rahsia mula diperkenalkan oleh Lampson dan ia merupakan aliran maklumat yang melanggar dasar keselamatan sistem. Dalam sesebuah sistem, polisi akan menentukan siapa yang dibenarkan untuk berkomunikasi dengan siapa, menerusi saluran apa, dan melarang semua urusan yang tidak sah. Sistem Saluran rahsia ini digunakan oleh dua pengguna yang diiktiraf. Pengguna ini mempunyai akses kepada fungsi sistem, tetapi menggunakannya dengan cara yang melanggar dasar keselamatan (sebagai contoh dengan mewujudkan satu saluran komunikasi antara dua pengguna yang asalnya tidak dibenarkan untuk berkomunikasi dimana pengguna tersebut mungkin mempunyai keistimewaan yang berbeza atau untuk menghantar maklumat antara pengguna yang diberi pelepasan tanpa perlu membuat pembayaran.). Satu andaian yang biasa ialah bahawa kedua-dua pengguna saluran rahsia ini tahu kegunaan sistem,ini dan telah bersetuju mengenai kegunaan tertentu daripada fungsi untuk mengekod dan menyahkod maklumat. Permasalahan di sini ialah terdapat pengguna yang mungkin tidak mempunyai apa-apa pengetahuan tentang apa itu saluran rahsia, menyebabkan pengguna seperti ini terdedah kepada datatidak baik yang tertanam dalam rangkaian, dan adalah sukar untuk mengenal pasti siapa yang terlibat dalam saluran komunikasi rahsia dan saluran rahsia boleh mengakibatkan eksploitasi komunikasi dalam menyalurkan dan memindahkan maklumat dengan cara yang melanggar dasar keselamatan sistem. Objektif dalam projek ini adalah untuk mengkaji dan menggambarkan saluran rahsia, membangunkan peraturan yang dapat mengesan saluran rahsia dalam rangkaian dan menguji peraturan dalam peraturan sistem IDS. Metodologi yang digunakan dalam projek ini adalah model tambahan dan sumbangan projek untuk projek ini adalah membandingkan tajuk tcp / ip biasa dengan header tcp / ip yang mengandungi mesej rahsia. Daripada itu peraturan boleh dibuat untuk mengesan saluran rahsia dalam TCP / IP dengan menggunakan program snort.

TABLE OF CONTENT

LIST OF TABLE

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Introduction

This introduction of this project will be contained in this chapter. It will discuss the problem statement of the project. Besides that, it also going to identify the project question that can be used to develop the project later. In addition to that, the objective of the project will be stated in this chapter, also what the project can contribute which is called as project contribution, the scope of the project, expected output from the project and finally how this report is organized.

The purpose of this project is to working out for rules to detect covert channel in TCP/IP. These days, people are too eager to protect their communication by using encryption platform from being decoded by unauthorized parties. But do they actually know that there is another platform where you can hide the very existence of the communication and it is known as covert channel. In 1973, the covert channel term was introduced by Lampson and it is designates an information flow that violates a system's security policy. Basically in a system a policy is made to define who is allowed to communicate with whom, by which channel, also refuse to allow all exchanges other than these legitimate ones. At this point, a covert channel is a perverted use of a system by two legal users. These users are given access to system's functionalities, but use them in a way that bypass the security policy maybe to create a communication channel between both users that are not allowed to communicate. One assumption can be made where both user know the system perfectly and agreed on a particular functionalities to encode and decode information.

There are two kind of covert channels which is Storage channels and Timing channels. Storage channels are used in a way where some individuals may communicate by modifying a "storage location" meanwhile for timing channels it perform an operations that affect the real response time observed by the receiver.

1.2 Problem Statement

Basically, covert channel is an alternative way used by individuals to communicate with other parties where at the same time it is exploiting by a process to transfer the information in a manner which can violates the system. This technique is created to allow multiple parties to communicate unnoticeable whereas there is an activity of communication occurring where the facts is. This technique is intent to hide the fact that communication is even occurring. This project will highlight the way for detecting the covert channel. Actually, covert channel is totally different from encryption because by using encryption, the communication is obvious but it is obscured meanwhile for covert channel, they hide the communication itself. Below are the statements of this project.

Table 1.1: Research Problem

No	Problem Statement
PS1	User might not have any knowledge about what is covert channel
PS2	User are exposed to malicious data that is embedded in network
PS3	It is difficult to identify the culprit that involved in covert communication channel.
PS4	Covert channel can result to exploitation of communication channel to transfer information in manner that is violates the system security policy

1.3 Project Question

Several questions are based on this project problem statement. These questions are done to help develop the objective of this project itself. The question is focused on how exactly to unhide or detect the hidden information that is using covert channel technique.

Table 1.2: Research Question

PS	PQ	Project Question
PS1	PQ1	What is covert channel?
PS3	PQ2	What is the rules to detect covert channel?

1.4 Project Objective

Objective is a statement that is specific and easier to measure of what will be done to answer the research question of this project. As the goal of this project is to best describe what is covert channel is about and how to detect the covert channel.

Table 1.3: Research Objective

PS	PQ	PO	Project Objective
PS1	PQ1	P01	To study and describe what is covert channel
PS3	PQ2	PO2	To develop rules that can detect covert channel in network
PS3	PQ2	PO3	To test and evaluate the rules with the IDS system rules

1.5 Project Scope

The scope of this project is to come out with the behavior and rule of covert channel in TCP/IP that is been used to share any secret information between both parties using the legal channel but actually violates the system's security policy. Covert communication normally is tunneled in normal where authorized traffic using techniques that make them largely undetectable to be examine by administrator and network filter. For this project, I will examine a few covert TCP packet from covert

TCP program and compare the behavior with the normal TCP packet in order to identify the rules for covert TCP/IP channel by using heuristic evaluation technique.

1.6 Project Contribution

This research contribution of the project helps determine what the project will achieve besides its objective. The parameter of this project will be determine by description of what is covert channel is about and the way to identify the covert channel in TCP/IP protocol.

Table 1.4: Project Contribution

PO	PC	Research Objective	Project Contribution
PO2	PC1	To develop rules that can detect covert channel in network	Proposed a rules on detecting covert channel in TCP/IP protocol that alert network administrator to distinguish a normal TCP traffic with covert TCP traffic.

1.7 Thesis Organization

The report of this project are consists of seven chapters overall. Below are the summarization and description of each chapter in this report:

Chapter 1: Introduction

This chapter will explain about the project introduction, project problem statement, research questions, the objective of this project , the project scope, the project contribution, the report organization of the project and the summary of chapter one.

Chapter 2: Literature Review

This chapter will discuss the related or previous work done regarding of this project, proposed a solution and preview of current problem and justification.

Chapter 3: Project Methodology

This chapter will discuss the method shall be used in developing this project and also project milestones which show progress of each stage of project development.

Chapter 4: Analysis and Design

This chapter will discuss about the design and list of software and hardware that will be used in developing this project.

Chapter 5: Implementation

This chapter will discuss on how the system works and show step by step in configuring and managing the system. It also will state the status of the project implementation.

Chapter 6: Testing

This chapter will discuss about analysis and testing of this project. The result of testing and test plan can be shown which include the organization, environment, schedule and strategy.

Chapter 7: Project Conclusion

This last chapter will make the conclusion of this project. Project limitation and contribution of this project will be explained and also the brief of project summarization and suggestion for future work.