UNIVERSITI TEKNOLOGI MARA

Simple Port Knocking Method against TCP Replay Attack and Port Scanning

MOHD AZUAN B MOHAMAD ALIAS

Dissertation submitted in partial fulfilment of the requirements

for the degree of

Master of Science in Computer Networking

Faculty of Computer Science and Mathemathical Science

January 2012

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and Merciful. With His permission, this study has been completed. I would like to express my grateful appreciation to all individuals who have contributed and help me in finishing this thesis. I am very thankful to my supervisor, Dr. Fakariah Mohd Ali for all his guidance and advices. Besides, I wish to express my sincere appreciation to Mr. Krishna Ramasamy my security guru and Mr Yusrul Nidzuan who has provided assistance at various occasions. Thanks to Micheal Rash, a guy who introduced Fwknop + SPA that share his experience.

Finally I would like to deliver sincere gratitude to my beloved wife, . my son beloved parents and the whole family for their encouragement and motivations during the period of study in UiTM Shah Alam, Selangor. Last but not least to all colleagues, to who has given their support that will be remembered forever.

TABLE OF CONTENTS

CONTENT

CHAPTER 1

INTRODUCTION

CHAPTER 2

LITERATURE REVIEW

CHAPTER 3
METHODOLOGY

ABSTRACT

Port knocking is technique first introduce in the Black Hat to prevent attackers from discovering and exploiting potentially vulnerable service on a network host, while allowing authenticated users to access these service. Despite being potentially useful tool, it suffers various vulnerabilities such as TCP replay, port scanning and etc. Most work in this area is proposed complex method to harden port knocking. This study presents an improved scheme over the existing Port Knocking by employ the Source Port sequences that will simplify a technique for port knocking system. Source port usually was automatic generate by operating system. Source Port is pre assign to generate a sequence. A technique to control when certain service start and stop was introduced to mitigate problem with TCP replay attack and port scanning. In addition, a proposed method doesn't need to integrate with firewall like other port knocking method. Experiment indicates that packet capture was able to grab port sequence but doesn't define what the service request is. In term of performance, proposed method work faster than others method like Basic port knocking and Fwknop + SPA. The performance of the proposed method was evaluated by measuring the authentication time to knock the server. The proposed port knocking method was useful to system administrators who need to access the server remotely but has a strict firewall rules.