Universiti Teknologi MARA

Automation Testing of Firewall Using Scapy

Fatin Nur Amirah Binti Rohimi

Thesis submitted in fulfilment of the requirements for Bachelor of Computer Science (Hons.) Data Communication and Networking

Faculty of Computer and Mathematical Sciences

July 2020

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful. Alhamdulillah, praise and thanks to Allah SWT, for all the graces and blessings and also Selawat and Salam to the Prophet Rasulullah SAW, hopefully His syafa‟at will be abundant in days later. I wish to thank God for giving me the opportunity to embark on my degree and for completing this long and challenging journey successfully.

Firstly, alhamdulillah I was in contact with many people, researches, lecturers, academicians, and friends. Special thanks to my supervisor Dr Zolidah binti Kasiran for helping me with this project and for encouragement, guidance critics and assistance. Her willingness to motivate and inspire me greatly to work harder in finishing this project until the end. I appreciate every single “walk” she taught me.

Thanks also to all the lecturers in the course of Bachelor of Science (Hons) Networking & Data Communications at UiTM Shah Alam for their patience and kind advice during the process of completing the project. Special appreciation goes to my parent Rohimi Bin Yakob and

and also my inspiring brother and sister, Farah Nur Izzati Binti Rohimi, Ahmad Faiz Irfan Bin Rohimi, Nur Aleya Aisyah Binti Rohimi and Nur Amalin Sofea Binti Rohimi that always motivated me to carry on.

Finally, thank you so much to all those who supported me in any way during the completion of this proposal report by discussing, sharing or exchanging ideas and everyone who is directly or indirectly involved in writing this report. Thank you so much.

ABSTRACT

Firewall tests must be performed to verify that the firewall works as specified. A test case generation approach is built in this project, identifying test cases based on the rule sequence of the firewall and using a real traffic database to prepare test packets. Test packets can be used or inserted to check if the design of the firewall is incorrect, i.e. the rules do not suit the firewall actions. Although literature accepts injection-based firewall testing as an inefficient way to test firewall implementations, no alternative method has yet been developed. Most academic work focuses on checking firewall rules where the implementation of firewall is error-free. Even if the implementation of the firewall is error-free, it is possible to hack and program a firewall to act differently from the intended security policy. In that case, testing based on real-time injection is one of the ways of revealing the breach of security. Automation testing is a technique for software testing to test and compare the actual results with the expected results. This can be done by writing the test script or by using any testing tool for automation. Test automation is used to automate recurring tasks that are hard to perform manually.

TABLE OF CONTENT

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter addresses the project definition and other related project histories. This chapter also discusses the problem declaration of the project to provide a good insight into the nature and priorities of the project. This chapter will be the guiding principle for all the work to be done later.

1.2 Project Background

Today, safety or cyber protection are important computer and network problems. It is also not enough to solely secure networks containing data on residents, companies and government agencies. Network infrastructure, routers, domain name servers and switches do not fail to connect all devices. Computers cannot interact correctly or efficiently if either of these fails. (Monsignor, 2003). Simply said that a defensive system is a firewall. It offers a controlled entrance point in computer resources and out of them. The firewall is a first line defense network security too. Scapy is one firewall tool that can be used. Scapy is a powerful module for manipulating packets. It can decode and create a wide range of protocols. Scapy is a tool for multipurpose. It can be used in Python programs to scan, test, and discover networks. (Spanish version 2017).

Different tools for security assessment are available for network tasks like Nmap, tcpdump and arpspoof, but Scapy is only one tool outstanding from others. While Scapy can create a whole new networking world, most of the instruments, like Nmap for network scanning or Wireshark for sniffing, have been designed for something very specific. Unfortunately, Scapy produces a brutal result in any query, as opposed to the other tools that provide an interpreted request. This particular tool value is very useful for advanced network research. By using