Tools for Security Senario Setup

Submitted by

Sun Mingyang

In partial fulfilment of the

requirements for the Degree of

Bachelor of Engineering (Computer Engineering)

National University of Singapore

B.Eng. Dissertation

Tools for Security Senario Setup

Orchestration Tool for IT Network Traffic Generation
and Human Behavior Simulation in Web Browsing

By

Sun Mingyang

National University of Singapore

2018/2019

Project ID: H0041300

Project Supervisor: Assoc Prof Change Ee-chien

Deliverables:

- Report: 1 Volume
- Manual: 2 Volumes
- Program: 1 Git Repository

Abstract

Normally, during Cyber Defence Exercise (CDX), it would be relatively easy to perform an attack or deploy an exploit once the vulnerability is known, however, setting up an appropriate security senario or target system will be rather difficult. In a particular example, during a Cyber Defence Exercise targeting a virtual enterprise-scale network, the attacking traffic performed by the Red Team (who will conduct the attacks) may be too obvious to be spotted or identified by the Blue Team (who will defense the network) when the attacks are performed in the an 'empty' virtual network where there is no background noise or "normal" web traffic. The goal of this project is to build tools that could help to simulate the real-world scenario and generate normal and benign network traffics in the virtual environment during the CDX similar to what has been described above. This project will consist of two compoents, while the first one is to build an orchestration tool for generating a sufficiently large amount of network traffic in a distributed system senario, and the second one is to simulate human behaviors in web browsing to make the web traffic more realistic. The evaluation and demonstration of this project will be conducted in the virtual network provided by the National Cyber-Security R&D Lab (NCL) and the final product may have international impacts on the CDX held by KYPO Cyber Range in Czech Republic.

Subject Descriptor:
C.2.4: Distributed Systems
D.2.2: Design Tools and Techniques
D.2.3: Coding Tools and Techniques
D.2.13: Reusable Software
G.3: Probability and Statistics

Keywords:
Cyber Defence Exercise Setup, Orchestraction Framework, IT Network Traffic Generation, Network Security, Distributed System, Human Behavior Simulation

Implementation Software:
Ubuntu Linux 18.04 Bionic Beaver, Python 3.6, Flask 1.0, Flask-Marshmallow 0.10, Flask-SQLAlchemy 2.3, Marshmallow-SQLAlchemy 0.16, Selenium 3.141, SQLAlchemy 1.3, osBrain 0.6, APScheduler 3.5, ntlk 3.4, React 16.6+, Ant Design 3.10+

Acknowledgements

I wish to express my sincere thanks to Chang Ee-Chien, Associate Professor from School of Computing, National University of Singapore, for providing me with all the necessary information and facilities for this project.

I place on record, my sincere thank you to Dr. Jan Vykopal from National Cyber-Security R&D Lab (NCL), for the continuous help. I am extremely thankful and indebted to him for sharing expertise, and sincere and valuable guidance and encouragement extended to me.

I am also grateful to Ivo Nutar from the Institute of Computer Science, Masaryk University, Brno, Czech Republic, for sharing with me lots of relevant work and past experience while I am developing the project.

Finally, I will also take this opportunity to express gratitude to all of the members in NCL who everlent their hands to me along this project for their help and support.

Contents