The Design and Implementation of Simulated Threat Generator based on MITRE ATTCK for Cyber Warfare Training - Notes

Cameron Noakes

November 2021

1 Sentence Overview

The proposal consists of using an automation “generator” script to issue simulated threats to train professionals with practical methods for defensive real world scenarios.

2 Introduction - Notes

A cyberspace was explained and what is referenced. A clear, concise explanation of how these simulations work is shown through a test bed simulation that requires the cyber professional to analyze the situation and take action on the threat to remove or isolate it. This method can be unique in training cyber professionals and to also help mitigate overall risk of an internal infrastructure network.

The cyber warfare threat simulation is explained to be for Blue Team (defense) but some applications for Red Teaming depending on refactoring the purpose since Blue Teaming is about stopping threats and the simulation performs Penetration Testing scenarios to aid in Blue Team training to prevent cyber warfare.

3 Analysis of existing studies

Existing studies were used to carry out concise definitions of terminology and the relatability of it to the threat simulation. It summarises what Penetration

Testing is and its common responsibilities to outline more about how the simulation can be adapted for more commercial purposes. It speaks about how Penetration Tests actively evaluate internal and external infrastructure or web applications to outline exploited vulnerabilities and how to secure environments, the generator automation provides real world training for such security audits.

4 Designing a simulated threat generator

Brief overview mention of the Mitre Attack Framework was detailed as a result of the threat simulations being modelled after the framework to provide key, up-to-date real world scenarios of exploitation relating to the Mitre Attack Framework. The Mitre Attack Framework played a key part in the designing and development of the testbed cyber threat simulation.

5 Research Gaps and Questions

One limitation is that of how no examples were mentioned in the introduction for where Mitre Attack Framework is also used within the industry and how it was a short paragraph that could have been expanded to include some information on Mitre Attack Framework and its association with this research not just for the testbed simulation.

6 What problem does this solve?

The proposed method of a testbed simulation aids in creating a successful solution at securing network environments to ensure that adversarial attackers cannot penetrate company digital perimeters.

Adversarial attackers are continuously finding new ways to exploit systems and the methods today are outdated by tomorrow, using a testbed simulation based off of the Mitre Attack Framework provides real world threats that can aid in the development of the skill-set behind any defense team.

7 How do they solve it?

The outlined problem was solved by proposing a solution of a testbed simulation to further train cyber professionals at picking up threats early on as they arise, allowing a more secure infrastructure testing team. This can also help reduce the overall cyber risk of an organisation by remediating any vulnerabilities the cyber professionals pick up from their expanded knowledge from the testbed simulation.

8 How do they assess it?

They assess the overall success of the testbed simulation by gauging if the simulation was informative and aided in the development of knowledge and skills from the cyber professionals.

9 Conclusion - Notes

The paper delineated a simulation that can be applied to the cyber warfare training sector for design and implementation examples to help better protect networks and devices. This paper correlated analysis of studies to come to the conclusion of creating a testbed simulation for cyber warfare.