World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:15, No:07, 2021

Adversary Emulation: Implementation of Automated Countermeasure in CALDERA Framework

Authors : Yinan Cao, Francine Herrmann

Abstract : Adversary emulation is a very effective concrete way to evaluate the defense of an information system or network. It is about building an emulator, which depending on the vulnerability of a target system, will allow to detect and execute a set of identified attacks. However, emulating an adversary is very costly in terms of time and resources. Verifying the information of each technique and building up the countermeasures in the middle of the test is also needed to be accomplished manually. In this article, a synthesis of previous MITRE research on the creation of the ATT&CK matrix will be as the knowledge base of the known techniques and a well-designed adversary emulation software CALDERA based on ATT&CK Matrix will be used as our platform. Inspired and guided by the previous study, a plugin in CALDERA called Tinker will be implemented, which is aiming to help the tester to get more information and also the mitigation of each technique used in the previous operation. Furthermore, the optional countermeasures for some techniques are also implemented and preset in Tinker in order to facilitate and fasten the process of the defense improvement of the tested system.

Keywords : automation, adversary emulation, CALDERA, countermeasures, MITRE ATT&CK
Conference Title : ICICTI 2021 : International Conference on Industrial Cybersecurity and Threat Intelligence
Conference Location : Rome, Italy
Conference Dates : July 22-23, 2021