Contribution ID: **9** Type: **Paper presentation**

Honeypot generator using software defined networks and recursively defined topologies

Friday 16 September 2022 09:40 (20 minutes)

The domain of cyber security represents a constant struggle between researchers and hackers, a continuous competition where the global digital infrastructure is at stake. Throughout the years, various protective measures have been developed to prevent against an increasing number of exploits that are becoming more and more complex and refined. Instead of concentrating on general mitigating techniques, our proposal orients towards creating performant honeypots which are safe and isolated environments that attract malicious users for the purpose of studying their invasive techniques. Firstly, this paper introduces an original method of describing, from a mathematically point of view, recursively defined topologies and presents a proposed algorithm used in constructing them. Secondly, we suggest a novel architecture which combines recursively defined topologies (RDT), software-defined networks (SDN) and an orchestrator engine for containerized infrastructure in order to develop a high-interaction honeypot which simulates an entire data center using a single physical host. The proposed implementation may represent a promising framework used as a developing platform for more complex honeypots used in either researching malicious human behavior or in the IT industry as a defensive measure. Regarding achieved results, the proposed implementation accomplishes notable results in deceptive techniques, isolation and effortless configurability.

Authors: BONTAS, Carol Sebastian (POLITECHNICA UNIVERSITY OF BUCHAREST FACULTY OF AUTOMATIC CONTROL AND COMPUTERS COMPUTER SCIENCE DEPARTMENT); STAN, Ioan-Mihail (University Politehnica Bucharest); RUGHINIȘ, Răzvan Victor (University Politehnica of Bucharest)

Presenter: STAN, Ioan-Mihail (University Politehnica Bucharest)

Session Classification: Session 1A - Cloud Computing and Network Virtualisation

Track Classification: Cloud Computing and Network Virtualisation