Security of Virtual Infrastructures: Assessing Kubernetes Attack Automation

Thomas Fowley, Master in Computer Science
University of Dublin, Trinity College, 2021

Supervisor: Stefan Weber

Virtual infrastructures are collections of resources and components that are assigned to software to allow for efficient development and scaling of the infrastructure. Due to these improvements in efficiency and efficacy that virtual infrastructures such as Kubernetes provide, they have quickly become common practice to implement in industry. However, due to the steep learning curve and relatively new technologies involved, many industry infrastructures have security concerns associated with them.

Traditional penetration testing has developed and become sophisticated since its inception with many automated tools and frameworks developed for ease of use and efficiency. This sophistication has not yet been fully achieved for virtual infrastructure testing. However, the area can potentially offer insights into what the next steps for infrastructure testing could entail.

The aim of this dissertation is to assess the current state of virtual infrastructure implementation practices and analyse traditional penetration methodology to infer how virtual infrastructure security could move forward towards more sophisticated techniques.

The research proposes a unified testing framework, similar to current frameworks such as Metasploit, for security testing virtual infrastructures. This tool is based on research carried out on automated tools currently available for Kubernetes.

The proof of concept for the framework developed during the research is then tested and compared with the current tooling to assess the viability and relevance of a testing framework for these infrastructures and its potential benefit.