Abstract

Macdara Tinney

2020

The modern internet remains a hostile environment, with various malicious actors launching attacks against any internet facing system that shows any sign of vulnerability. While the former naïve approaches to computer security are being abandoned, the rate at which attacks grow in complexity continues to outpace developments in securing computer systems.

With the growth in cloud computing architectures such as Platform as a Service and Infrastructure as a Service, much of the progress made in securing traditional deployments is now not strictly applicable in the new paradigm. This risks opening a further gap between system implementations and the attackers attempting to break them. This could lead to a rise in security incidents in cloud environments unless something is done to mitigate the potential harm.

Cloud service providers are aware of this threat, and are actively working on securing deployments from external threats. This research proposes a system that can help secure a deployment from internal threats, via use of honeypots in containerised cloud deployments and listener containers that can detect when suspicious traffic such as port scanning is circulating within the cloud deployment.

Existing work in this area has already explored the use of honeypots and honeynets in this role in traditional deployment scenarios. It has also demonstrated them in a research role in the cloud. This work separates itself from this prior work by investigating the use of these intrusion detection systems in a containerised cloud environment, in particular a Kubernetes based cloud deployment, in combination with a port scanner detector.