JOHANNES KEPLER
UNIVERSITY LINZ

Bachelor's Thesis

Kubernetes Attack Catalog

Dipl.-Ing. Dr.
Markus Weninger, BSc
Institute for System Software

P +43-732-2468-4361
F +43-732-2468-4345
markus.weninger@jku.at

Student: Carina Hauber
Advisor: Dipl.-Ing. Dr. Markus Weninger, BSc
Dynatrace Supervisor 1: Gierlinger Markus, MSc
Dynatrace Supervisor 2: Dipl.-Ing. Mario Kahlhofer, BSc
Start date: February 2022

The research at Dynatrace's cloud native security research team is primarily focused on the defense of cloud environments and resources. For any conducted research they currently often make assumptions about attacks, for example about how realistic and feasible they are.
To best inform their research, it makes sense to get first-hand experience evaluating and finding full-fledged attacks (from external reconnaissance to final escalation and exfiltration).
Having experience of several attack chains could lead to better informed assumptions for further research (e.g., priority of k8s components, danger of certain attack vectors, etc.).

Goals of this thesis:

- Research at least 2-3 attack chains, maybe informed by the MITRE ATT&CK framework or Microsoft's Threat Matrix for Kubernetes
- Perform these attack chain in a realistic environment
  - An attack chain is a sequence of attacks across phases, including reconnaissance, initial exploitation, privilege escalation, pivoting, and finally a final action on the objective (e.g., gain full access of k8s Control Pane)
  - Use and extend the *Unguard* environment for this
- Document any learnings
  - Score how easy/hard certain attack steps were, which should reflect the likelihood of being exploited
- Ideally, the thesis should lead to better insights on
  - the value of certain cloud/k8s components
  - usefulness of security controls
  - priority of IAM, secrets management, resources management, network policy, etc.
- (nice to have) Automate attacks as adversary emulation
  - Goal: Given an attack scenario (e.g., web application attacks), emulate an attacker
  - Preferably, use existing tools to perform one or more instances of this type of attack scenario
  - (Play around with the tools and maybe come up with a set of "playbooks" that can be used to perform attacks with a bit of variability)

Further Readings:
https://developer.squareup.com/blog/threat-hunting-with-kubernetes-audit-logs/

Modalities:
The progress of the project should be discussed at least every two weeks with the Dynatrace supervisors and at least once per month with the advisor. A time schedule and a milestone plan must be set up within the first 3 weeks and discussed with the advisor and the supervisors. It should be continuously refined and monitored to make sure that the thesis will be completed in time. The final version of the thesis must be submitted not later than 15.08.2022.