Exec into container

Attackers who have permissions, can run malicious commands in containers in the cluster using exec command (“kubectl exec”). In this method, attackers can use legitimate images, such as an OS image (e.g., Ubuntu) as a backdoor container, and run their malicious code remotely by using “kubectl exec”.

Info

ID: MS-TA9006
Tactic: Execution
MITRE technique: T1609

Mitigations

ID	Mitigation	Description
MS-M9003	Adhere to least-privilege principle	Adhere to least-privilege principle to prevent users from exec into containers
MS-M9010	Restrict Exec Commands on Pods	Restrict exec commands on pods using admissions controller.
MS-M9011	Restrict Container Runtime using LSM	Restrict container runtime capabilities using LSM.