# Kubernetes Security Testing


Kubernetes security is the practice of protecting Kubernetes clusters, pods, and containers from potential threats and vulnerabilities. It involves safeguarding the infrastructure, applications, and data from malicious actors, malware, broken container images, and

compromised and insider threats.

By implementing robust security measures, organizations can ensure the resilience, integrity, and confidentiality of their applications and infrastructure is mantained.

## Major Security Risks

- Increased Attack Surface: Containers running within the cluster can have a different attack surface and its own unique vulnerabilities which can be exploited by attackers.
- Vulnerable container images: Container images may have inherent weaknesses or vulnerabilities. Securing Kubernetes aids in preventing these vulnerabilities from being exploited by malicious parties.
- Malicious threat actors: Attackers looking to exploit vulnerabilities in the system, posing a threat to the integrity and confidentiality of the Kubernetes clusters.
- Unauthorized malicious containers: Malware, such as viruses or ransomware, can potentially infect containers and compromise the security of the applications running inside them.
- Insider threat: Users with access to the Kubernetes cluster, either due to being compromised or acting with malicious intent, can pose a risk to the security and stability of the system.

Do not print this page. This is property of the Security Dojo Powered by Virtual Cyberforce.

## Security Best Practices

- Following Authentication & Authorization best practices.
- Network security best practices.
- Running a CIS Security Scan on a Kubernetes Cluster.
- Self-assessment of security in Kubernetes Cluster.
- Infrastructure Pentesting & Patching.