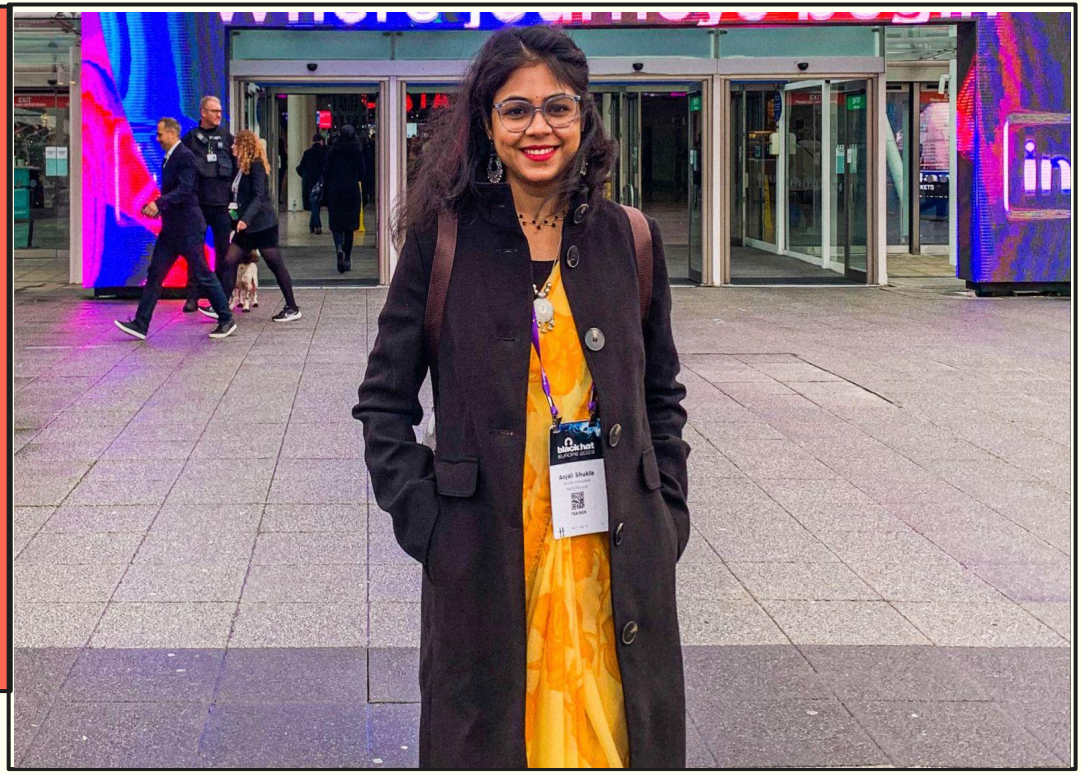
OWASP appsec days SINGAPORE

How Attackers Exploit Misconfigured AWS EKS: Lessons from OWASP EKS Goat

Who I am - Anjali

- Senior Security engineer, 6+ years across DevSecOps, Kubernetes security (EKS/GKE), and AWS/Azure/GCP
- Founder of Kubernetes Village
- Lead, **OWASP EKS Goat** project focused on AWS EKS security
- YouTube & Instagram channel @peachycloudsecurity.
- **AWS Community Builder** & Volunteer at Cloud Village (DEFCON) & BSides.
- Speaker at **Black Hat USA (Spring)**, **Black Hat Europe**, **Nullcon**, **Seasides Goa**, **BSides Bangalore**, **CSA Bangalore**, and **C0c0n**



@peachycloudsecurity

Who I am - Divyanshu

- Senior Security Engineer with 8+ years in Web, Cloud, Kubernetes Security, DevSecOps, Threat Modelling
- Reported vulnerabilities to Google, Apple, Microsoft, Airbnb, AWS, Samsung, Amazon, Zomato, Amazon, Apple & more
- CVEs: **CVE-2019-8727**, **CVE-2019-16918**, **CVE-2019-12278**, **CVE-2019-14962**
- Co-lead of **OWASP EKS Goat**; Author of *Burp-o-mation* & ***very-vulnerable-serverless*** app
- **AWS Community Builder** (Security) & **DEFCON Cloud Village** Crew (2020–2022)
- Speaker at **Black Hat Europe**, **BruCON**, **Nullcon, C0c0n**

Why Does It Matter ?

≠

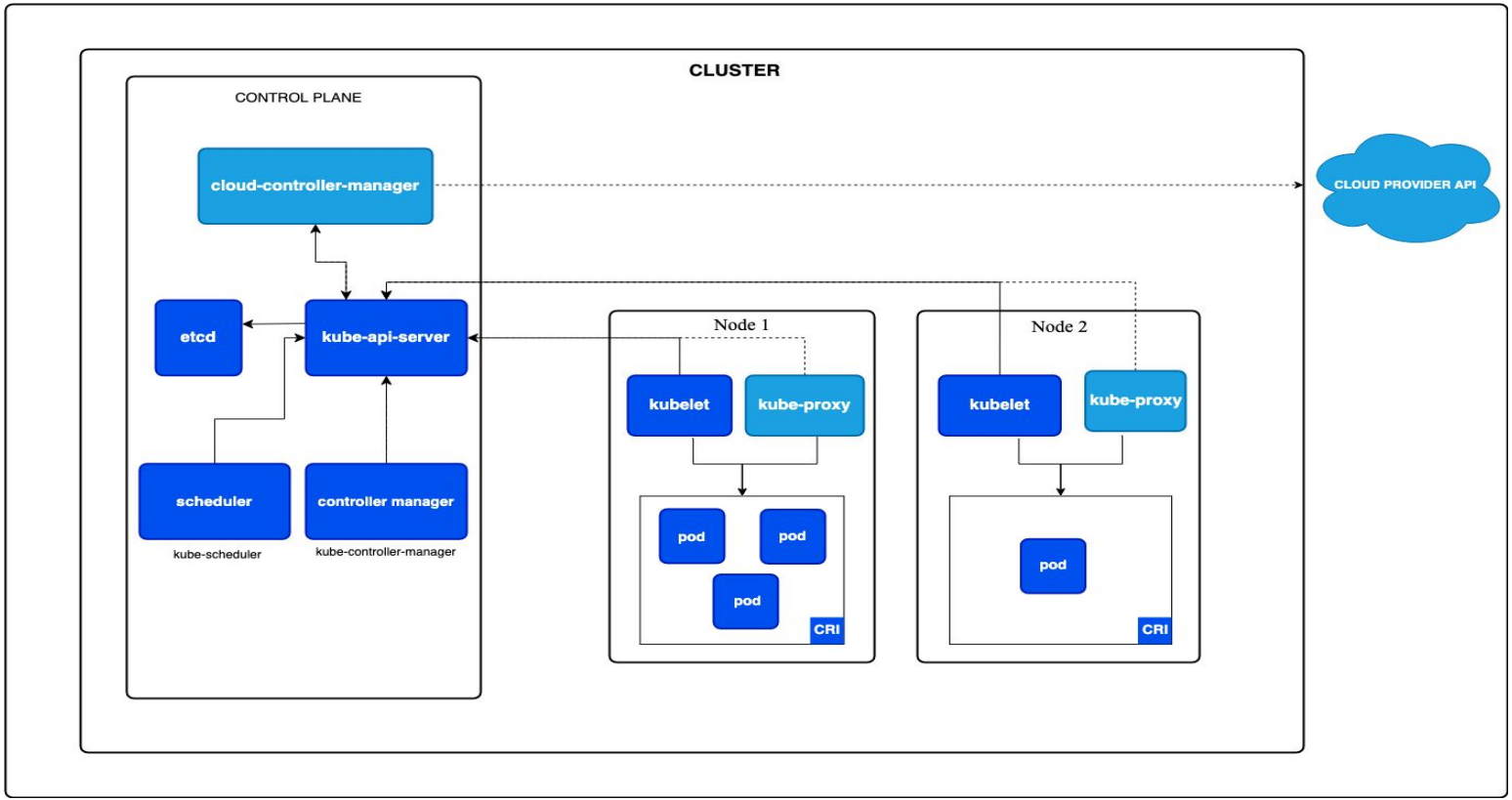
Amazon EKS

Attack Surface
(K8s)

Attack Surface
(K8s + AWS Cloud)

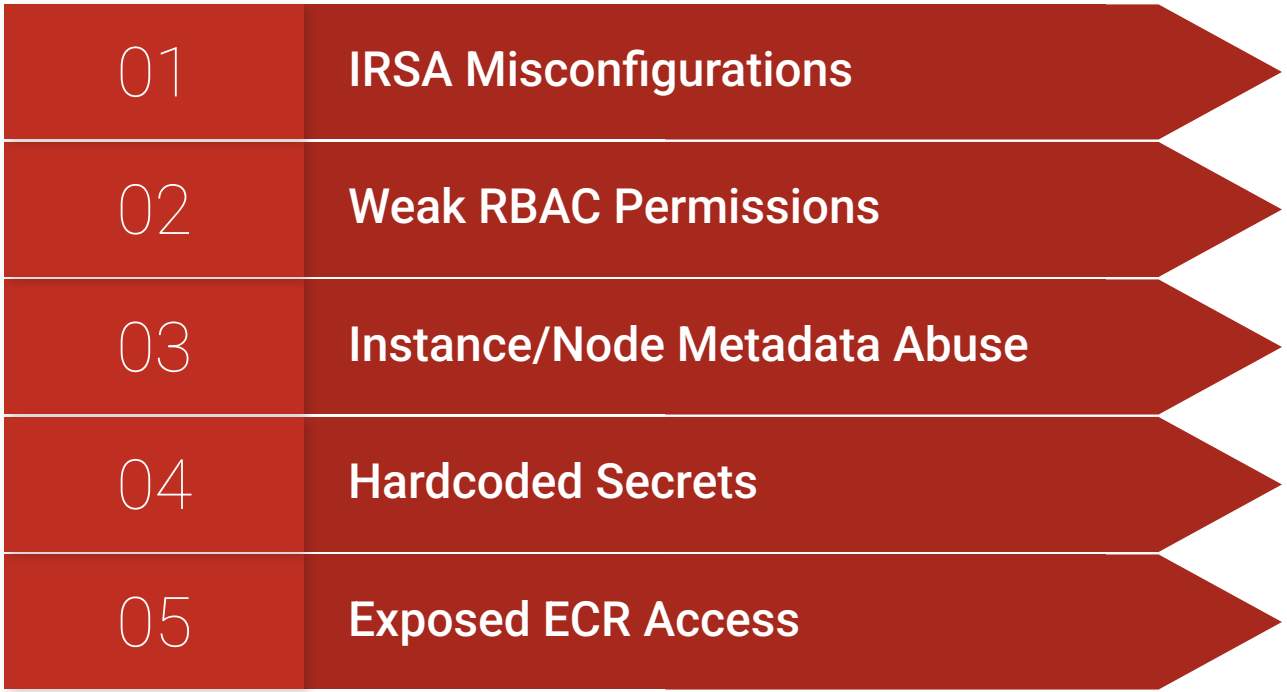
Ref:
https://kubernetes.io/

Kubernetes Architecture

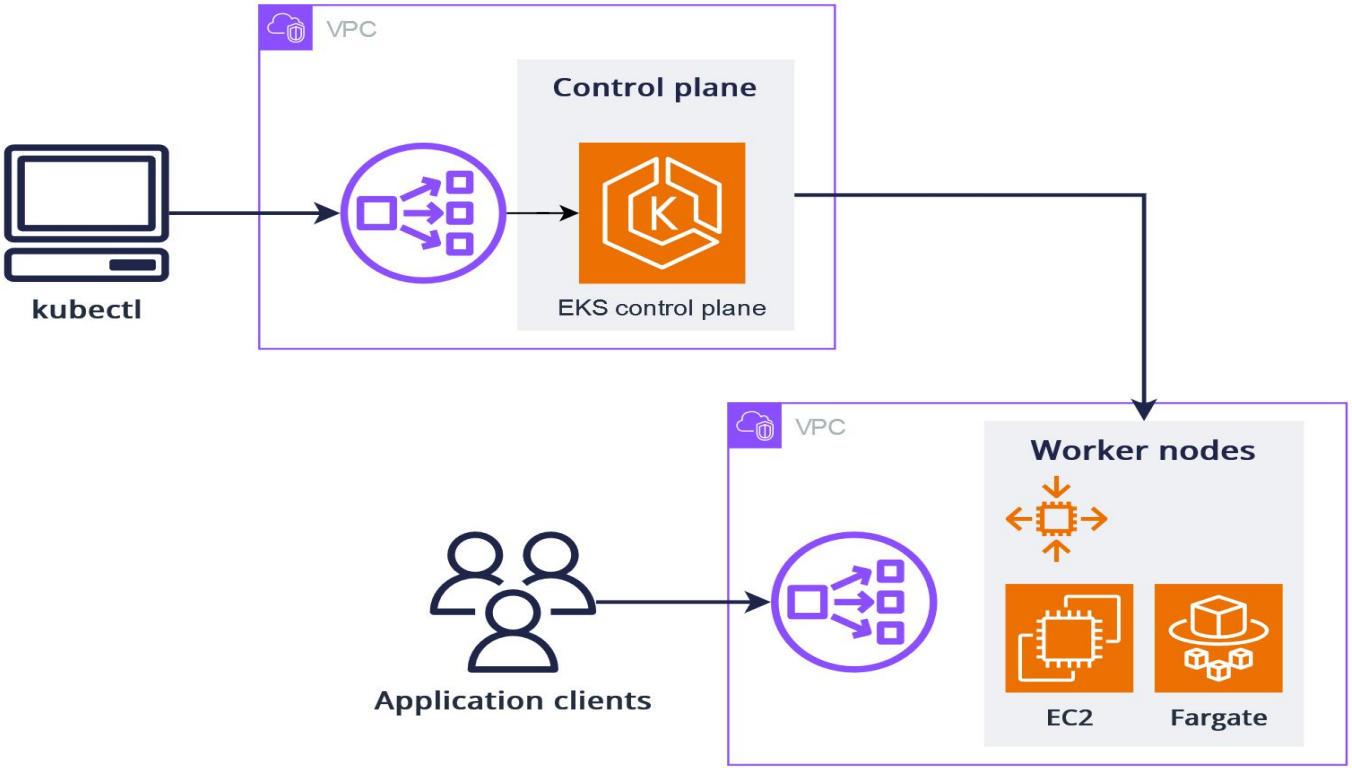


Ref:
https://kubernetes.io/

Common EKS Misconfigurations

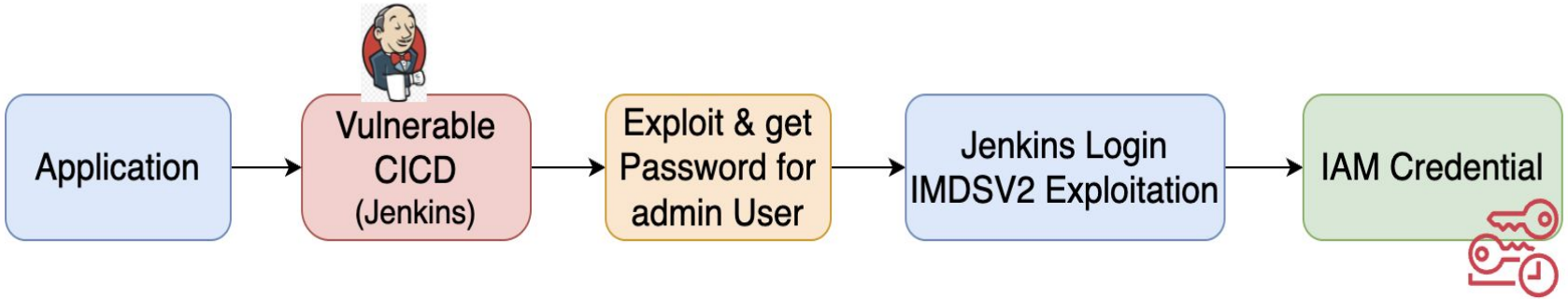


Architecture of AWS EKS



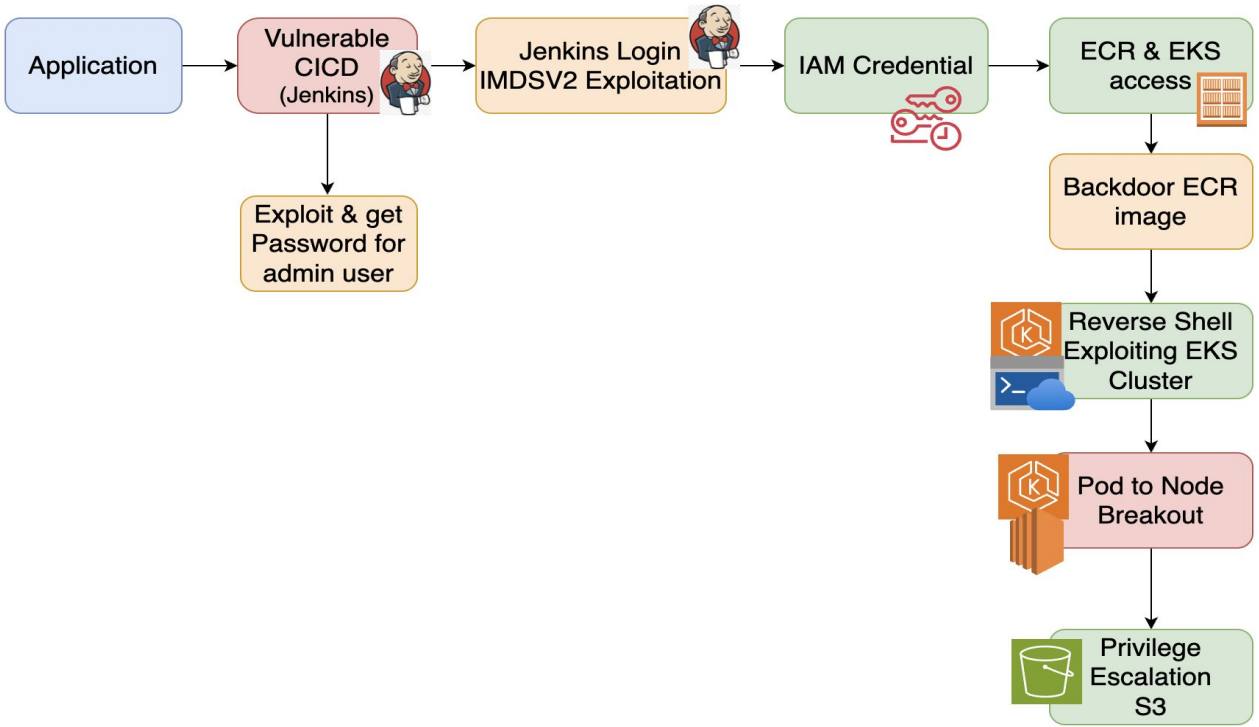
Ref:
https://docs.aws.amazon.com/eks/latest/userguide/eks-architecture.html

Inside the Attack: OWASP EKS GOAT



Inside the Attack: OWASP EKS GOAT

Inside the Attack: OWASP EKS GOAT



How Attackers Break Kubernetes on AWS (Demo using OWASP EKS Goat)

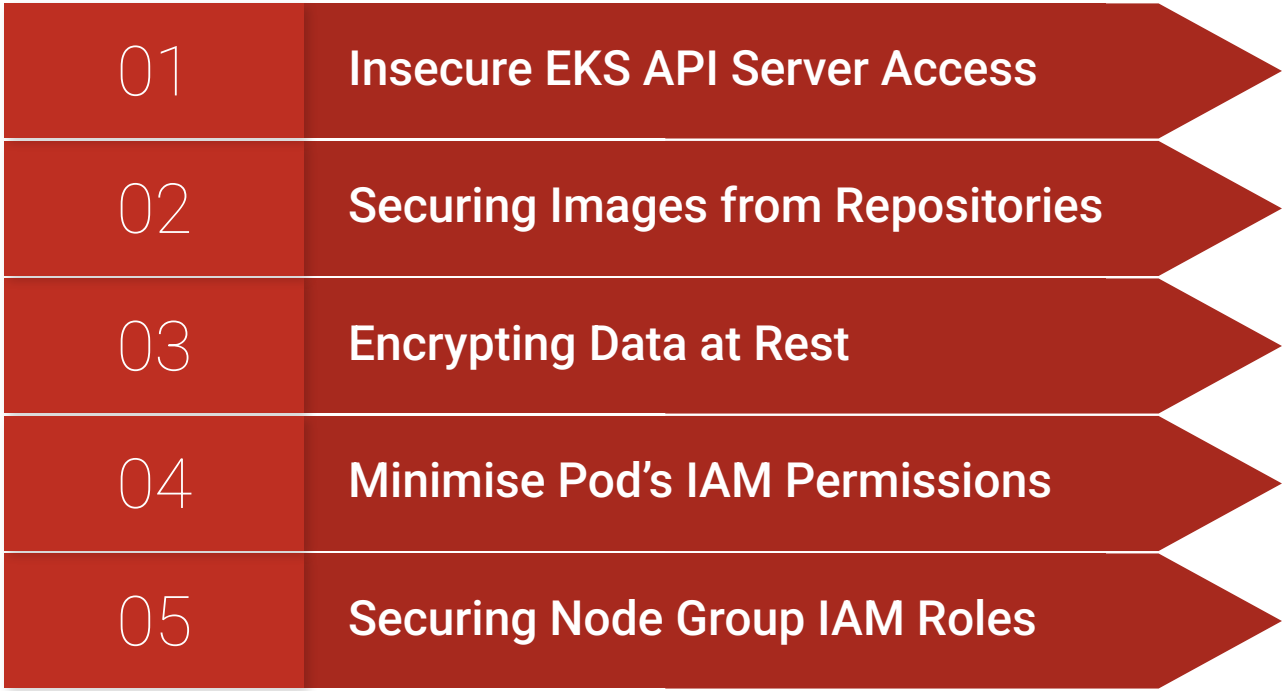
Documentation:
https://eksgoat.kubernetesvillage.com/

Vulnerable Lab IP: http://54.187.23.116

Solve Lab & Win Credit

Be the first to finish and reach out via Linkedin to us to win AWS credits [USD]

EKS Security Best Practices



EKS Security Best Practices

06	Unsecured Load Balancers
07	Enforce Network Segmentation
08	Real-time Monitoring with GuardDuty
09	Poor Secrets Management
10	Enforce Security with Admission Controller

Announcement

(Upcoming Project: OWASP GKE Goat)

THANKS