OWASP EKS GOAT

BSIDES BANGALORE

W3-CS

BSIDES BANGALORE ANNUAL CYBER SECURITY CONFERENCE -2025

BSIDES BANGALORE ANNUAL CYBERSECURITY CONFERENCE 2025

FORTIFYING DIGITAL DEFENSE | RESILIENCE | COMPLIANCE

OWASP EKS GOAT

Your Kubernetes on AWS Is Probably Misconfigured and Here's How to Fix It

OWASP EKS GOAT

BSIDES BANGALORE ANNUAL CYBERSECURITY CONFERENCE 2025

FORTIFYING DIGITAL DEFENSE | RESILIENCE | COMPLIANCE

BSIDES BANGALORE

W3-CS

Divyanshu Shukla
Senior Security Engineer

Anjali Shukla
Senior Security Engineer

#ACSC2025

AGENDA

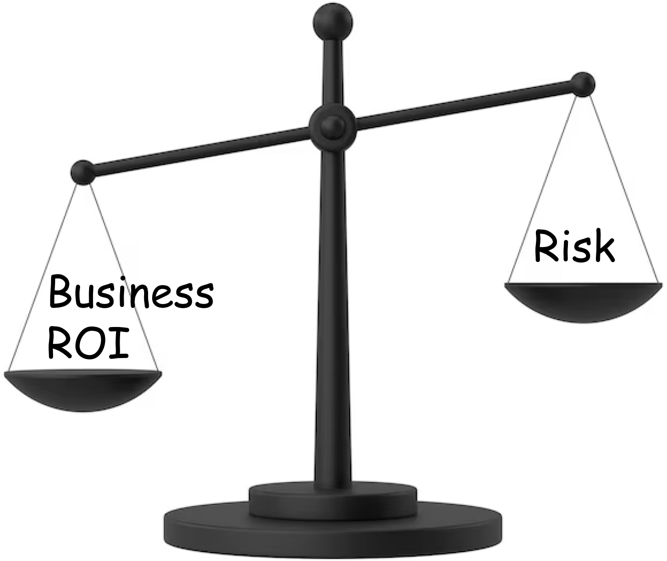
- Architecture of Kubernetes
- How Attackers Break into Kubernetes on AWS using OWASP EKS Goat (Demo)
- EKS Security Best Practices

Why Does It Matter ?

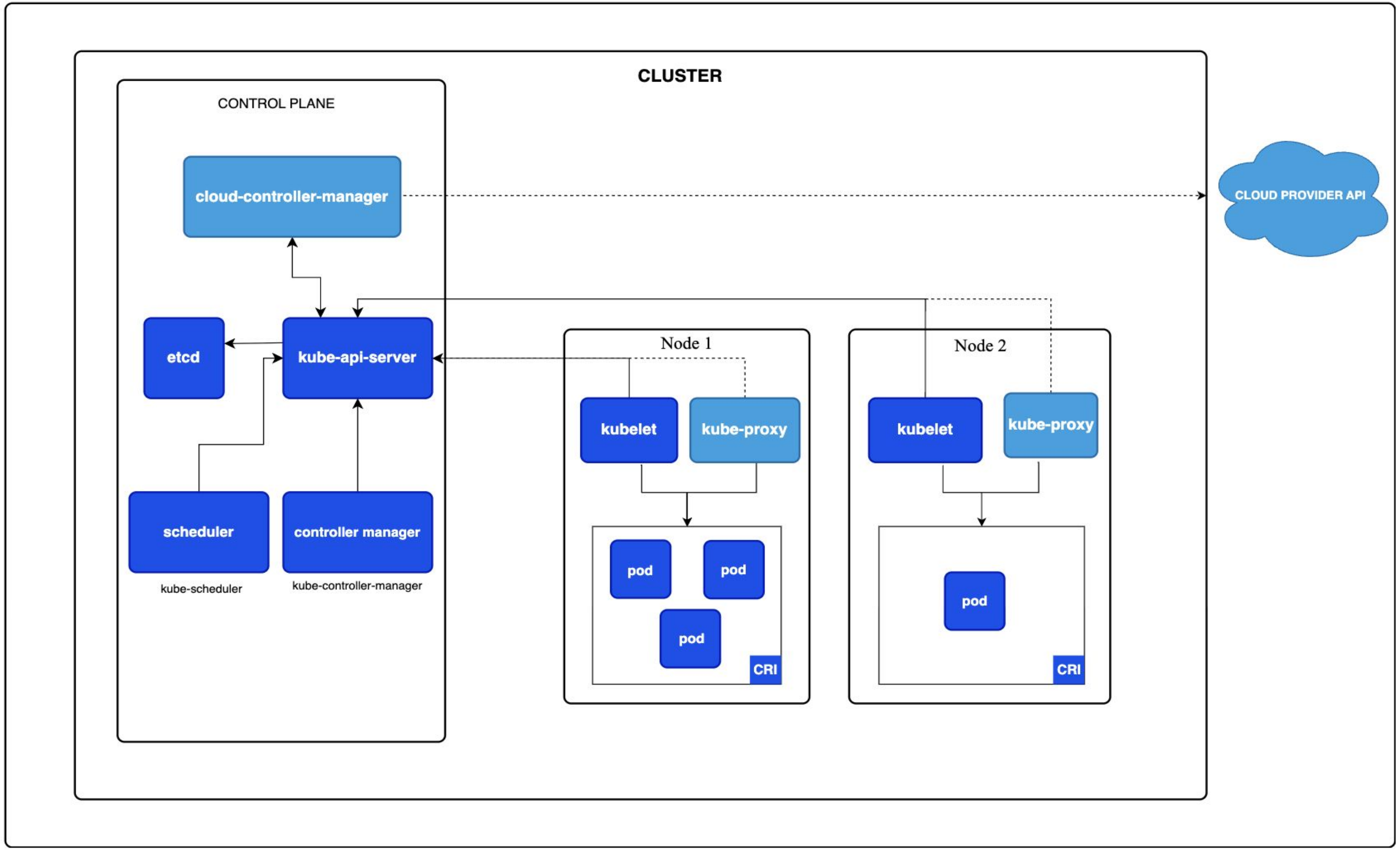
Amazon EKS

Attack Surface (K8s)

Attack Surface (K8s + Cloud)



Architecture of Kubernetes



#ACSC2025

Ref:
https://kubernetes.io/docs/concepts/architecture/

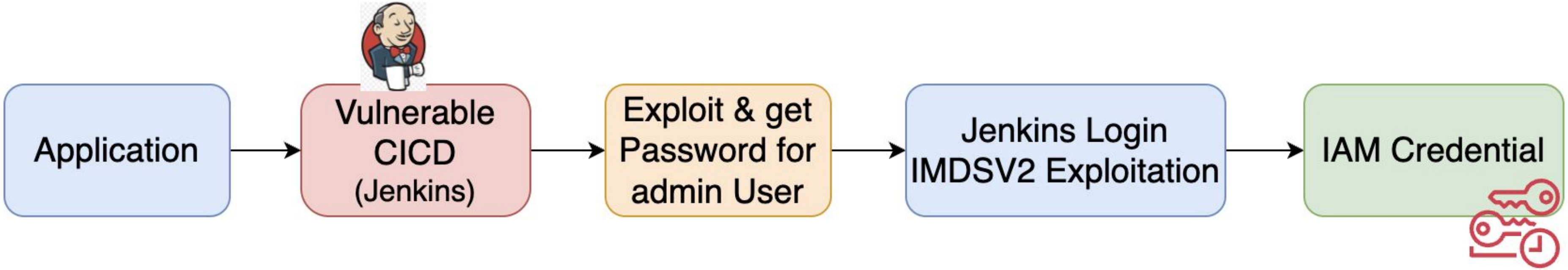
How Attackers Break Kubernetes on AWS (Demo using OWASP EKS Goat)

Documentation:

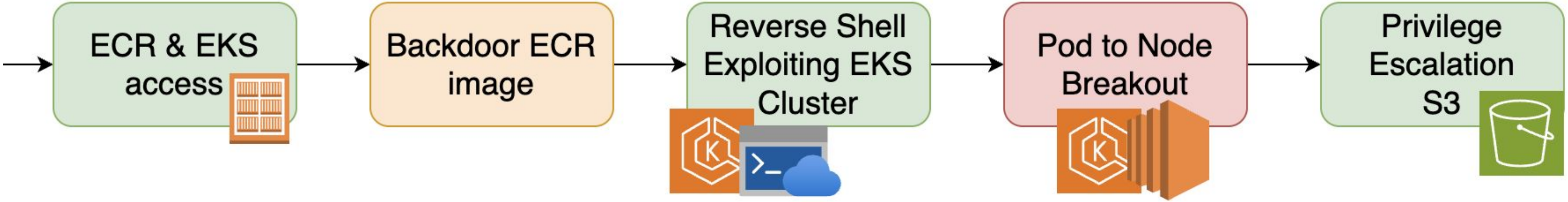
https://eksgoat.kubernetesvillage.com/

Vulnerable Lab IP:

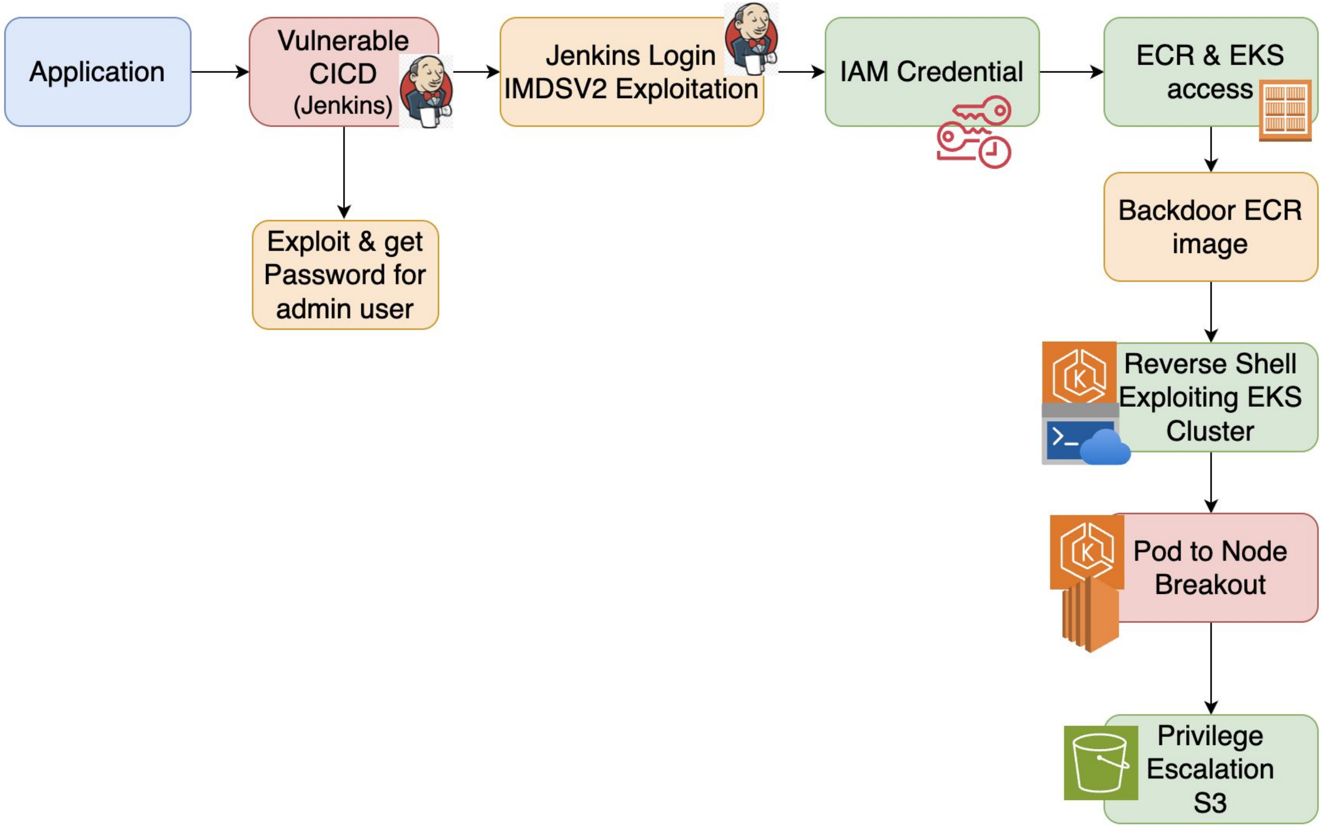
Inside the Attack: OWASP EKS GOAT


Application
Vulnerable CICD (Jenkins)
Exploit & get Password for admin User
Jenkins Login IMDSV2 Exploitation
IAM Credential

Inside the Attack: OWASP EKS GOAT



Inside the Attack: OWASP EKS GOAT



Application

Vulnerable CICD (Jenkins)

Exploit & get Password for admin user

Jenkins Login IMDSV2 Exploitation

IAM Credential

ECR & EKS access

Backdoor ECR image

Reverse Shell Exploiting EKS Cluster

Pod to Node Breakout

Privilege Escalation S3

#ACSC2025

EKS Security Best Practices

01 Insecure EKS API Server Access

02 Securing Images from Repositories

03 Encrypting Data at Rest

04 Minimise Pod’s IAM Permissions

05 Securing Node Group IAM Roles

EKS Security Best Practices

06 Unsecured Load Balancers

07 Enforce Network Segmentation

08 Realtime Monitoring with GuardDuty

09 Poor Secrets Management

10 Enforce Security with Admission Controller

QUIZ TIME!

Q1. In Kubernetes, what is a 'Pod'?

A. The smallest deployable unit
B. A single container
C. A virtual machine
D. A network policy

Q1. In Kubernetes, what is a 'Pod'?

A. The smallest deployable unit
B. A single container
C. A virtual machine
D. A network policy

Q2. What is RBAC in Kubernetes?

A. Route-Based Access Control
B. Resource-Based Access Control
C. Rule-Based Access Control
D. Role-Based Access Control

Q2. What is RBAC in Kubernetes?

A. Route-Based Access Control
B. Resource-Based Access Control
C. Rule-Based Access Control
D. Role-Based Access Control

Q3. What is the purpose of a Kubernetes 'Namespace'?

A. To provide high availability
B. To isolate resources within a cluster
C. To manage storage
D. To define network policies

Q3. What is the purpose of a Kubernetes 'Namespace'?

A. To provide high availability

B. To isolate resources within a cluster

C. To manage storage

D. To define network policies

Q4. What is the purpose of Pod Security Standards (PSS) in Kubernetes?

A. To limit CPU and memory usage per pod

B. To enforce security settings on pods

C. To manage data encryption

D. To monitor node resource utilization

Q4. What is the purpose of Pod Security Standards (PSS) in Kubernetes?

A. To limit CPU and memory usage per pod

B. To enforce security settings on pods

C. To manage data encryption

D. To monitor node resource utilization

Q5. Which of the following is a container runtime security tool?

A. Falco
B. Kube-dns
C. Helm
D. Prometheus

Q5. Which of the following is a container runtime security tool?

A. Falco
B. Kube-dns
C. Helm
D. Prometheus

BSIDES BANGALORE ANNUAL CYBERSECURITY CONFERENCE 2025

FORTIFYING DIGITAL DEFENSE | RESILIENCE | COMPLIANCE