Open in app

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

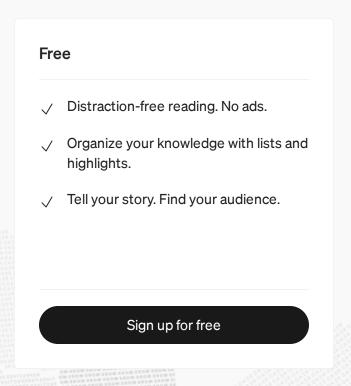
Sign in

X



Kubernetes Namespace Breakout using Insecure Host Path Volume — Part 1

Medium





This is Dart 1 of a 2 nart corios on socurity implications of insocure host Dath

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

Part 2 deals with the mitigation

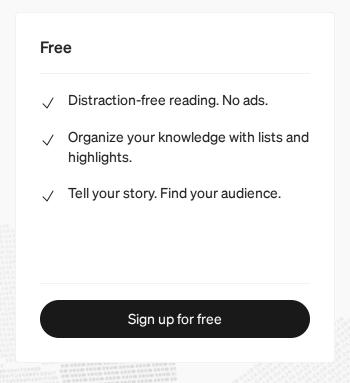
Prevent hostPath based Kubernetes attacks with Pod Security Policies

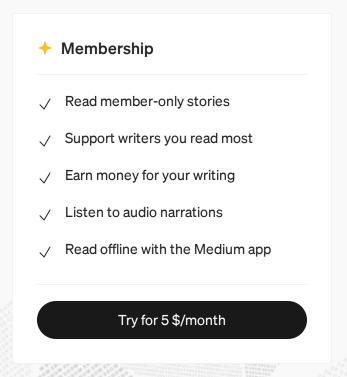
Mitigation for insecure hostPath volume mounts using pod security policies

blog appeaced com

CO

Medium





This ability can in turn be leveraged to eventually gain maximum privilege

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

Abusing hostPath volume mounts for a Pod namespace escape Video

```
→ research export KUBECONFIG=./developer-kubeconfig
→ research
→ research kubectl auth can-i create pods
no
→ research kubectl auth can-i list secrets -n kube-system
no
→ research kubectl auth can-i create pods --namespace=developers
yes
```

Medium





Create kubeconfig for service account

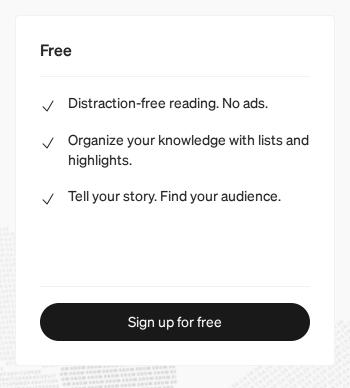
To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

The config above creates a <u>Namespace</u> developers, a <u>Service Account</u> developer-sa and binds <u>Role</u> to allow <u>CRUD</u> on Pod resource to developer-sa but restricted only to the developers Namespace.

Attacker Starting Point

As attacker in the scenario, we will start by having access to the cluster using

Medium





Our objective is to breakout of this namespace restriction and gain access to

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

Namespace Escape Steps

We will use hostPath volume feature of Kubernetes to deploy a Pod in developers namespace but with the underlying Node's / (root filesystem) mounted inside our Pod at /host. We will also use additional features of Pod such as hostIPC, hostPID, hostNetwork to allow us access to all processes in the underlying Node. Our PodSpec (pod-to-node.yml) that we use in the example below is available here.

Medium





At this point we can access all Docker Containers running in the node

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

root@pool-qt7kkl8wt-zn6c:/# docker ps

CONTAINER ID IMAGE

COMMAND CREATED STATUS

PORTS NAMES 622b9f408fde ubuntu

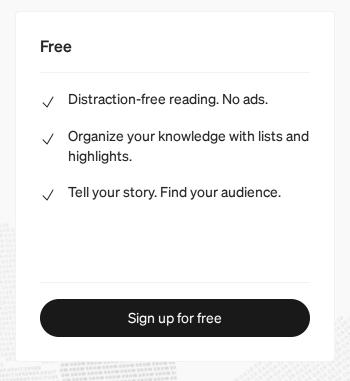
"/bin/sh -c 'sleep i..." 8 minutes ago Up 8 minutes

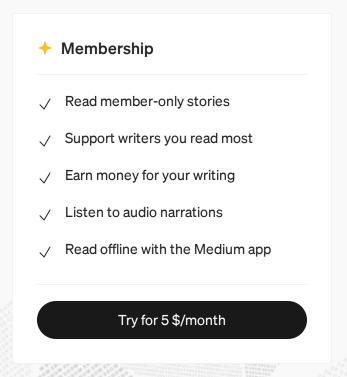
k8s_attacker-pod_attacker-pod_developers_d261db9d-84e4-4b73-83fb-

dbf42444e4d4_0

e329436h98dc k8s gcr in/nause·3 1

Medium





- to In addition to this we can use nodeName or nodeSelector in DodSnec to
- To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

Privilege Escalation

CO

We have gained an attack primitive where we can deploy a Pod, which is scheduled in arbitrary Node by Kubernetes. Through the Pod, we are able to access the Node's *Docker daemon* and in turn have full access to any container running on the Node.

Medium





We can use the same config to list AII Dods in the cluster

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

root@pool-qt7kkl8wt-zn6c:/# kubectl \
--kubeconfig=/etc/kubernetes/kubelet.kubeconfig get pods -A

This lists all Pods in the cluster

NAMESPACE NAME PEADV

Medium

Sign up to discover human stories that deepen your understanding of the world.

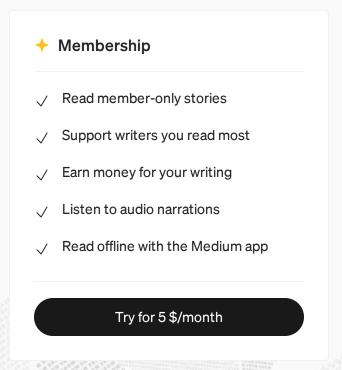
Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

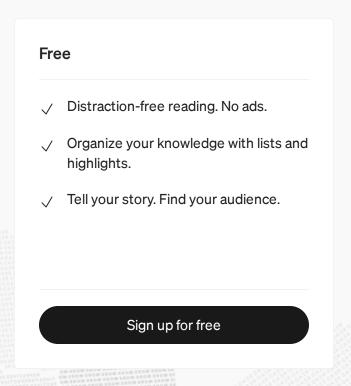


cat /var/run/secrets/kubernetes.io/serviceaccount/ca.crt

The above information can be used, along with cluster-info to generate a kubeconfig using which an attacker can interact with the API server. Refer to our script for generating kubeconfig

Mitigation

Medium





assurance for withstanding real world attackers by gotting us to do a black how

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

We run a hands-on training course "Attacking and Auditing Kubernetes Clusters" for cluster operators and pentesters.

Drop us an email, <u>contact@appsecco.com</u> if you would like us to assess the security of your K8S infrastructure or if you would like your security team trained in advanced pentesting techniques against K8S.

Medium





Written by Abhisek Datta

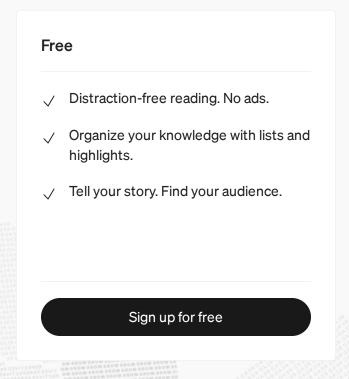




157 Followers · Writer for Appsecco

Security Researcher | Security Engineering | Personal tweets @abh1sek | Workshop https://github.com/abhisek

Medium





Riyaz Walikar in Appsecco

Nodejs and a simple RCE exploit

While reading the blog post on a RCE on demo.paypal.com by @artsploit, I wanted to...

Abhisek Datta in Appsecco

Prevent hostPath based Kubernetes attacks with Pod...

Mitigation for insecure hostPath volume

Medium

Sign up to discover human stories that deepen your understanding of the world.

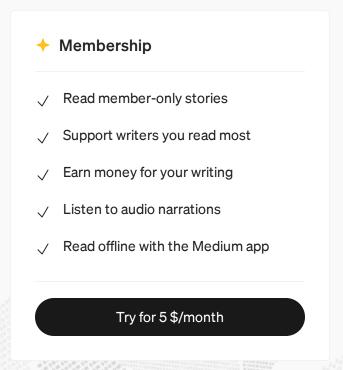
Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free



Neetrox in InfoSec Write-ups

Intrusion Detection: Implementing Suricata on Windows Systems

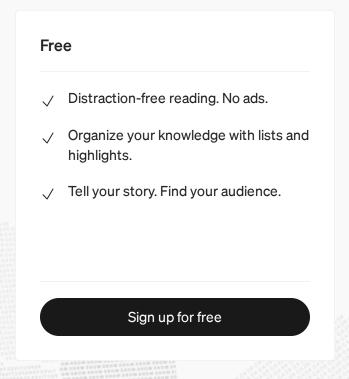
Validating Intrusion Detection Efficacy

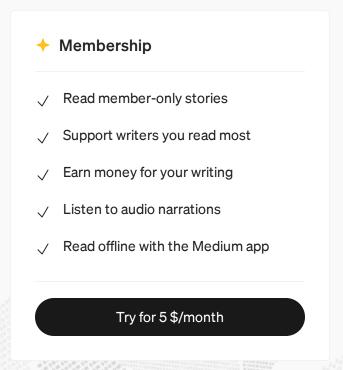
Ankita Patel

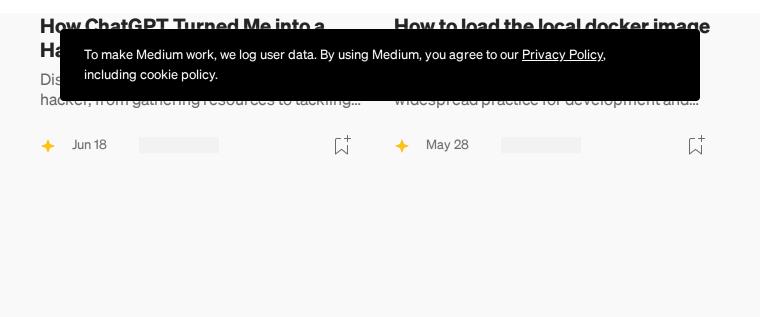
Kubernetes Service Mesh: What It Is and How to Use It

As the adoption of microservices architecture

Medium







Medium

