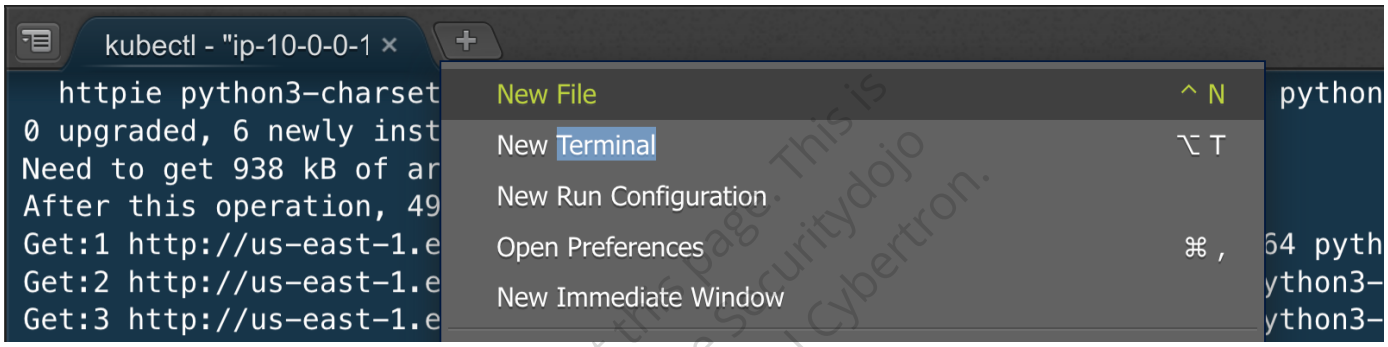
Post-exploitation: Common Attack Techniques & Demo Setup

Open New Terminal (Optional)

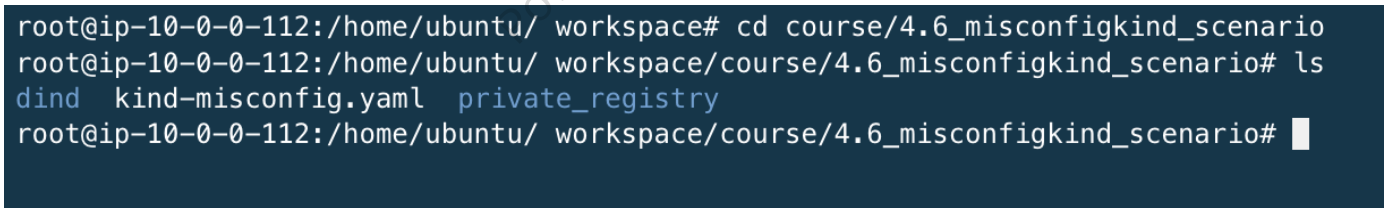
If current working directory is not `workspace/course` .

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



- Keep current working directory as `workspace/course`

```
cd course/4.6_misconfigkind_scenario
ls
```



- Introducing anonymous true and public access & mounting docker.sock for the demo lab.

```
cat kind-misconfig.yaml
```

- Explanation of `kind-misconfig.yaml` .
  - This configuration is for the Kubernetes cluster setup using "kind". It defines a cluster with one control-plane node and two worker nodes.
  - The control-plane node is configured to listen on all network interfaces (node-ip:

0.0.0.0) which has a port mapping for the Kubernetes API server accessible on the host at port 6443.

- The worker nodes are configured with an "extraMount" each. This mounts the Docker socket from the host into the worker nodes. This allows containers running in the worker nodes to communicate with the Docker daemon on the host.
- The network's default Container Network Interface (CNI) is disabled.
- The second part of the configuration makes the API server accept connections on all network interfaces (via the "bind-address": "0.0.0.0" and "insecure-bind-address": "0.0.0.0" settings). It also allows anonymous authentication ("anonymous-auth": "true") and sets the insecure port to 8080.
- The timeoutForControlPlane field sets a timeout of 1 hour for the control-plane to start. If it doesn't start within this time, the operation will fail.
- This configuration is insecure and is not recommended for production. It might be used for learning purposes or for local development and testing.

```
root@ip-10-0-0-112:/home/ubuntu/ workspace/course/4.6_misconfigkind_scenario# cat kind-misconfig.yaml
kind: Cluster
apiVersion: kind.x-k8s.io/v1alpha4
nodes:
- role: control-plane
  kubeadmConfigPatches:
  - |
    kind: InitConfiguration
    nodeRegistration:
      kubeletExtraArgs:
        node-ip: 0.0.0.0
  extraPortMappings:
  - containerPort: 6443
    hostPort: 6443
    protocol: TCP
- role: worker
  extraMounts:
  - hostPath: /var/run/docker.sock
    containerPath: /var/run/docker.sock
- role: worker
  extraMounts:
  - hostPath: /var/run/docker.sock
    containerPath: /var/run/docker.sock
networking:
  disableDefaultCNI: true
---
apiVersion: kind.sigs.k8s.io/v1alpha3
kind: Cluster
kubeadmConfigPatches:
- |
  apiVersion: kubeadm.k8s.io/v1beta2
  kind: ClusterConfiguration
  metadata:
    name: config
  apiServer:
    extraArgs:
      "bind-address": "0.0.0.0"
      "insecure-bind-address": "0.0.0.0"
      "insecure-port": "8080"
      "anonymous-auth": "true"
    timeoutForControlPlane: 1h
```

Trainer-Specific Demo Setup (Not for Students)

- Delete the old cluster

```
kind delete cluster
```

```
root@ip-10-0-0-112:/home/ubuntu/ workspace/course/4.6_misconfigkind_scenario# kind delete cluster
Deleting cluster "kind" ...
root@ip-10-0-0-112:/home/ubuntu/ workspace/course/4.6_misconfigkind_scenario#
```

- Resetup the cluster

```
kind create cluster --config kind-misconfig.yaml
```

```
root@ip-10-0-0-112:/home/ubuntu/ workspace/course/4.6_misconfigkind_scenario# kind create cluster --config kind-misconfig.yaml
Creating cluster "kind" ...
 ✓ Ensuring node image (kindest/node:v1.25.3) 🖼
 ✓ Preparing nodes 📦 📦 📦
 ✓ Writing configuration 📜
 ✓ Starting control-plane 🕹️
 ✓ Installing StorageClass 💾
 ✓ Joining worker nodes 🚜
Set kubectl context to "kind-kind"
You can now use your cluster with:

kubectl cluster-info --context kind-kind

Thanks for using kind! 😊
```

- Resetup the cilium

```
cilium install
```

```
root@ip-10-0-0-112:/home/ubuntu/ workspace/course/4.6_misconfigkind_scenario# cilium install
🔮 Auto-detected Kubernetes kind: kind
✨ Running "kind" validation checks
✅ Detected kind version "0.17.0"
ℹ️  Using Cilium version 1.13.2
🔮 Auto-detected cluster name: kind-kind
🔮 Auto-detected datapath mode: tunnel
🔮 Auto-detected kube-proxy has been installed
ℹ️  helm template --namespace kube-system cilium cilium/cilium --version 1.13.2 --set cluster.id=0,cluster.name=kind-kind,encryption.nodeEncryption=false,ipam.mode=kubernetes,kubeProxyReplacement=disabled,oper
ator.replicas=1,serviceAccounts.cilium.name=cilium,serviceAccounts.operator.name=cilium-operator,tunnel=vxlan
ℹ️  Storing helm values file in kube-system/cilium-cli-helm-values Secret
🔑 Created CA in secret cilium-ca
🔑 Generating certificates for Hubble...
🚀 Creating Service accounts...
🚀 Creating Cluster roles...
🚀 Creating ConfigMap for Cilium version 1.13.2...
🚀 Creating Agent DaemonSet...
🚀 Creating Operator Deployment...
⌛ Waiting for Cilium to be installed and ready...
✅ Cilium was successfully installed! Run 'cilium status' to view installation health
```