Demo: Misconfigured Kube API Server Setup

The Kubernetes API server is the main management component of a Kubernetes cluster. If it's misconfigured to allow anonymous access, it means that anyone can access it without needing to authenticate. They could access sensitive information about the cluster, like the names and configurations of your namespaces, via the URLs you mentioned.

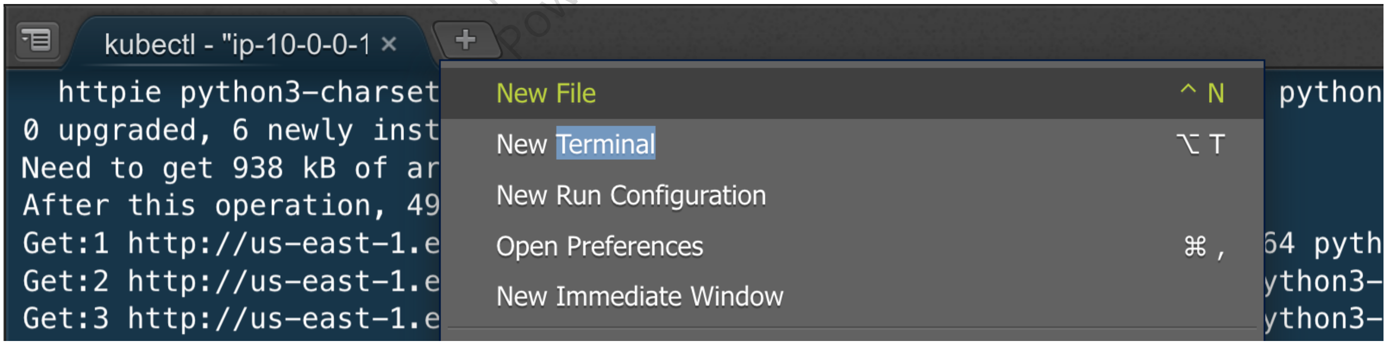
An attacker could exploit this to read, modify, or delete your cluster's resources, possibly disrupting the cluster or even taking it over. For example, they could launch pods that consume all your resources, or alter existing services to redirect traffic to their own servers.

Trainer-Specific Demo Setup (Not for Students)

Open New Terminal (Optional)

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

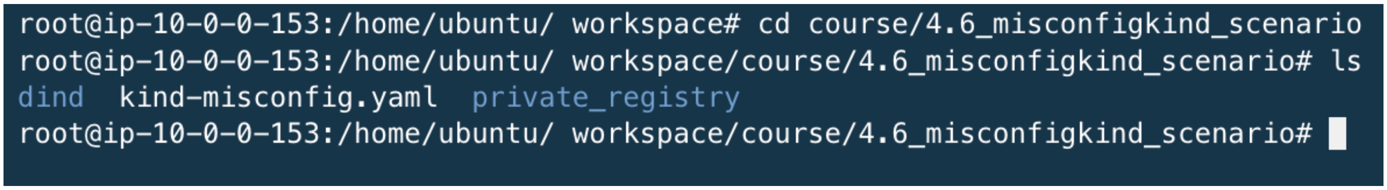
- Click on `+` icon, then select `new terminal` to open new terminal.



```
  httpie python3-charset                                    python
0 upgraded, 6 newly inst
Need to get 938 kB of ar
After this operation, 49
Get:1 http://us-east-1.e                                   64 pyth
Get:2 http://us-east-1.e                                   ython3-
Get:3 http://us-east-1.e                                   ython3-
```

- Keep current working directory as `workspace/course`

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



```
root@ip-10-0-0-153:/home/ubuntu/ workspace# cd course/4.6_misconfigkind_scenario
root@ip-10-0-0-153:/home/ubuntu/ workspace/course/4.6_misconfigkind_scenario# ls
dind  kind-misconfig.yaml  private_registry
root@ip-10-0-0-153:/home/ubuntu/ workspace/course/4.6_misconfigkind_scenario#
```

```
kubectl proxy --address='0.0.0.0' --disable-filter=true --address 0.0.0.0 >
/dev/null 2>&1 &
```

`fg` to bring the process to foreground & `ctrl + c` to kill the process.

The --disable-filter flag is used with the kubectl proxy command to disable the filtering of non-local requests. When this flag is set to true, the kubectl proxy will allow requests from any IP address, including those that are not on the local network.

- Access the endpoint

```
echo $(curl -s  ifconfig.me):8001
```

use the -s or --silent flag with the curl command. This flag will prevent curl from displaying any output to the terminal, including the progress meter.

- Access the namesapces endpoint.

```
echo $(curl -s  ifconfig.me):8001/api/v1/namespaces
```