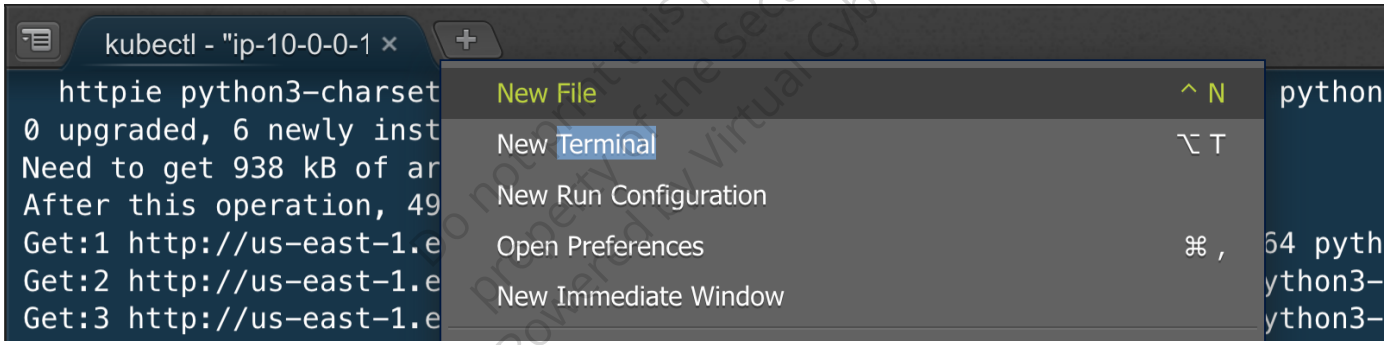
Lab: Exploiting Private Docker registry

In containerized infrastructure, a private Docker registry stores all the Docker images used by the organization. This centralized registry can be a potential security concern because it often contains sensitive data. For example, Docker images could have application source code, environment variables, or configuration files that might hold secrets, such as API keys or database credentials. If unauthorized individuals gain access to this registry, they could potentially access this sensitive data, which could lead to data breaches or misuse of the organization's resources.

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`

```
mkdir -p course/4.6_misconfigkind_scenario/private_registry
cd course/4.6_misconfigkind_scenario/private_registry
ls
```

```
docker run -d -p 5000:5000 --restart=always --name registry -v docker-
registry:/var/lib/registry registry:2
```

This command will start a Docker registry container and map port 5000 on the host to port 5000 in the container. The --restart=always option ensures that the container will automatically restart if it stops or the host reboots. The -v option is used to mount the /data/docker-registry directory on the host to the /var/lib/registry directory in the

container, which is where the Docker registry data is stored.

```
DOCKER_REGISTRY_IP=$(docker inspect registry | grep IPAddress | cut -d '"' -f 4
| head -n 2 | awk '{print $1}' | tr -d '\n')
echo "{ \"insecure-registries\": [\"$DOCKER_REGISTRY_IP:5000\"] }" | tee
/etc/docker/daemon.json
```

```
systemctl restart docker
```

```
docker pull nginx:latest
docker tag nginx:latest $DOCKER_REGISTRY_IP:5000/nginx:latest
```

```
docker push $DOCKER_REGISTRY_IP:5000/nginx:latest
```

```
wget -qO- http://$DOCKER_REGISTRY_IP:5000/v2/_catalog
```

- After completing these steps, you should be able to access the nginx image from the insecure registry using `docker pull $DOCKER_REGISTRY_IP:5000/nginx:latest` .