ICS/OT Lab – Quick Start

1. Start the lab:
   1. cd **ics-security**
   2. **docker compose start**
      1. if docker compose start does not work, go to **Token Fix section**
2. login to Kibana at: localhost:5601
   1. username = elastic
   2. password = utsautsa
3. Generate some traffic to see in Kibana
   1. # open a shell in the attacker container
   2. **docker** exec -it ics-security-pentest-1 /bin/bash -lc '
   3. **echo** "--- L3 SCADA (192.168.3.20) ---";

ping -c2 192.168.3.20 || true;

nmap -Pn -sS -T4 --top-ports 50 192.168.3.20 -oA /tmp/scan\_scada || true;

echo "--- L2 PLC (192.168.2.10) ---";

ping -c2 192.168.2.10 || true;

nmap -Pn -sS -T4 --top-ports 100 192.168.2.10 -oA /tmp/scan\_plc || true;

echo "--- DMZ transfer (172.16.0.21) ---";

curl -I http://172.16.0.21 || true

“

**View the traffic in Kibana**

1. Go to [**http://localhost:5601**](http://localhost:5601) → log in (see step 2).
2. If prompted to add data, go straight to **Stack Management → Data Views → Create data view** and add:
   * **Name:** Suricata  
     **Pattern:** suricata-\*  
     **Time field:** @timestamp
   * **Name:** Zeek  
     **Pattern:** zeek-\*  
     **Time field:** @timestamp
3. Open **Discover** (top left). Set time range to **Last 15 minutes**.
4. Useful filters (KQL bar at top):
   * Suricata flows from/to the attacker:
   * **event\_type:**flow AND (src\_ip:192.168.3.30 **OR** dest\_ip:192.168.3.30)

**If Kibana won’t load (Token fix)**

If the Kibana page won’t connect, add a **service account token** to .env and restart Kibana.

1. **Create a token** (inside Elasticsearch):

docker exec -it elasticsearch \

/usr/share/elasticsearch/bin/elasticsearch-service-tokens create elastic/kibana kibana-token

Copy the long token it prints (starts with AAEAAW...).

1. **Put the token in .env** (no quotes, one line):

nano /opt/ics-security/.env

# add or replace this line:

KIBANA\_SERVICE\_TOKEN=<paste\_token\_here>

# save & exit

1. **Restart Kibana** (Compose is already wired to use the token):

cd /opt/ics-security

docker compose up -d --force-recreate kibana

1. **Try Kibana again:** <http://localhost:5601>