



Water Tank flooding hands on

Formal Methods for Secure Systems - A.A. 2019/2020

25 May 2020

The cyber range platform: CYBERWISER.eu

1. The CYBERWISER.eu cyber range platform is going to be developed in the scope of the CYBERWISER.eu European Project;
2. The purpose of the CYBERWISER.eu platform is **to form** multidisciplinary and highly skilled **experts** in the **cybersecurity** field;
3. Users can act both as **attacker** and **defender**, in different and highly configurable **scenarios**;
4. A **scenario** is composed by:
 - a. A set of **virtual resources** simulating a real network;
 - b. The **software** running on such resources.
5. **To each scenario it is possible to associate one or more cyber range exercise.** Users are asked to complete the exercise, by interacting with the virtualized environment, to acquire additional knowledge;
6. The CYBERWISER.eu platform is entirely **web-based**.

How to reach the CYBERWISER.eu platform

1. Open a browser (FireFox, Chrome, Safari or Edge) and go to the following address:
<https://clusting.itc.unipi.it/>;
2. Login to the CYBERWISER.eu platform using the credentials which you should have received;
3. In the **left** menu, click on “Activities”: 
4. You should see “Water Tank Flooding/Leaking”, click on the *eye* icon, on the **right**: 

Name ^	Actions
Ethical Hacking	
Water Tank Flooding/Leaking	

2 total

CYBERWISER.eu workspace

Water Tank Flooding/Leaking

A cyber training scenario for the Water Tank Flooding/Leaking lab

Topics

Cyber-Physical system security

19-May-20, 09:46

Exploit a web application managing a water tank cyber-physical system.

At the end of the lab, please fill the following questionnaire: bit.ly/cyberraange09



Documents

No documents to display.

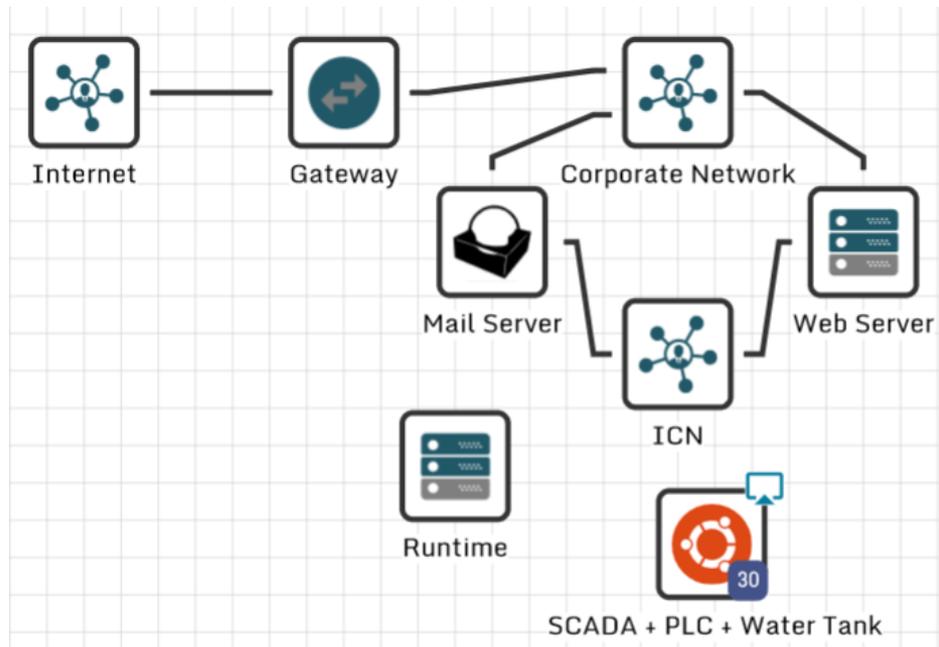
Scenario Environments

Water Tank Flooding/Leaking

Fill the questionnaire at the end!

Access to the cyber range

Scenario: Network Topology



CYBERWISER.eu cyber range

1. You have the right to access to two VMs called “**SCADA + PLC + Water Tank**”. You can access it with the little screen icon on the top right of each VM icon:

2. The login credentials for both are:
 - a. Login: student
 - b. Password: student



Control screen

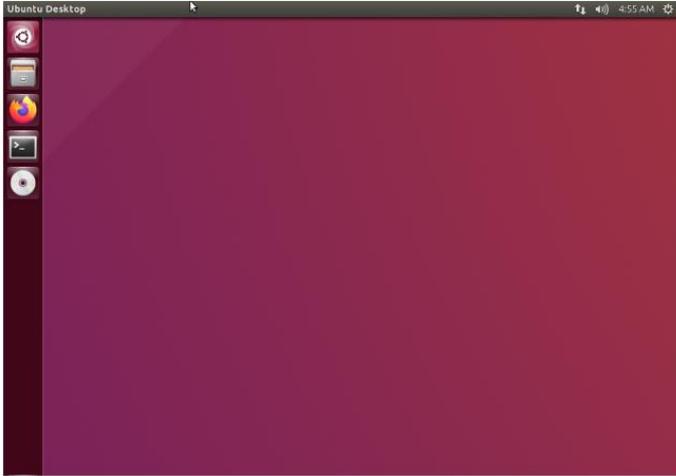
Full screen

Open in a new Tab

Connected to VM SCADA + PLC + Water Tank [1]/QEMU (one-2626)

Send CtrlAltDel

Your generated password for Student1 is 



CLOSE

The image shows a web-based control interface for a virtual machine. At the top, it indicates the connection to 'VM SCADA + PLC + Water Tank [1]/QEMU (one-2626)'. Below this, there are three control buttons: a red 'Send CtrlAltDel' button, a blue button with a download icon, a blue button with a full-screen icon (highlighted with a red box), and a blue button with an 'open in new tab' icon (highlighted with a green box). A text field displays a generated password for 'Student1' as a series of dots, with an eye icon to toggle visibility. The main area contains a screenshot of an Ubuntu desktop environment with a dark red background and a sidebar of application icons. A 'CLOSE' button is located at the bottom right of the interface.

Scenario: How to use the VM

- ***“SCADA + PLC + Water Tank”***:

- You have a full access to an Ubuntu 16.04 Desktop machine, on which a web server is running. The web server controls the Water Tank management system.
- Open a Browser and connect to localhost on port 5000: <http://localhost:5000>
- Try to cause a water flooding!

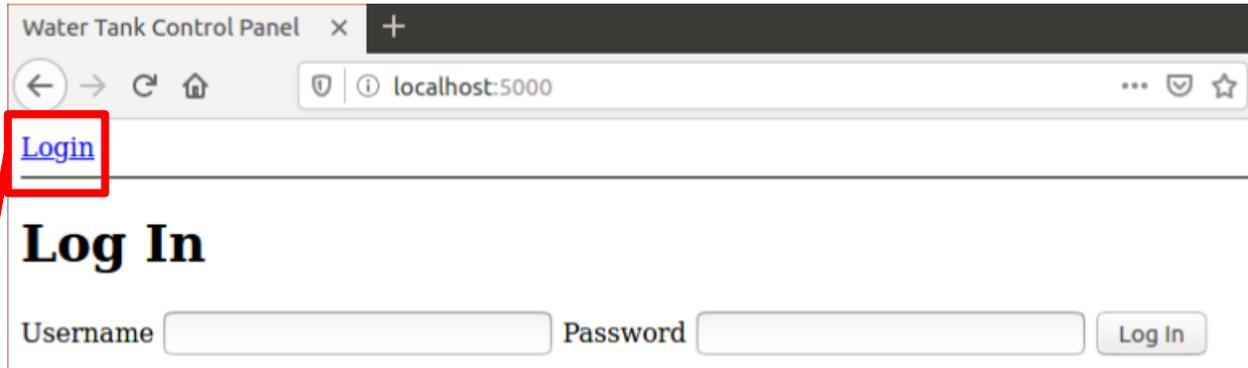
* Depending on your keyboard layout, open a terminal (on both VMs) and write:

```
setxkbmap it (for the Italian keyboard)
```

```
setxkbmap us (for the us keyboard)
```

Exercise (part 1)

1. Obtain **admin** credentials



Water Tank Control Panel x +

localhost:5000

[Login](#)

Log In

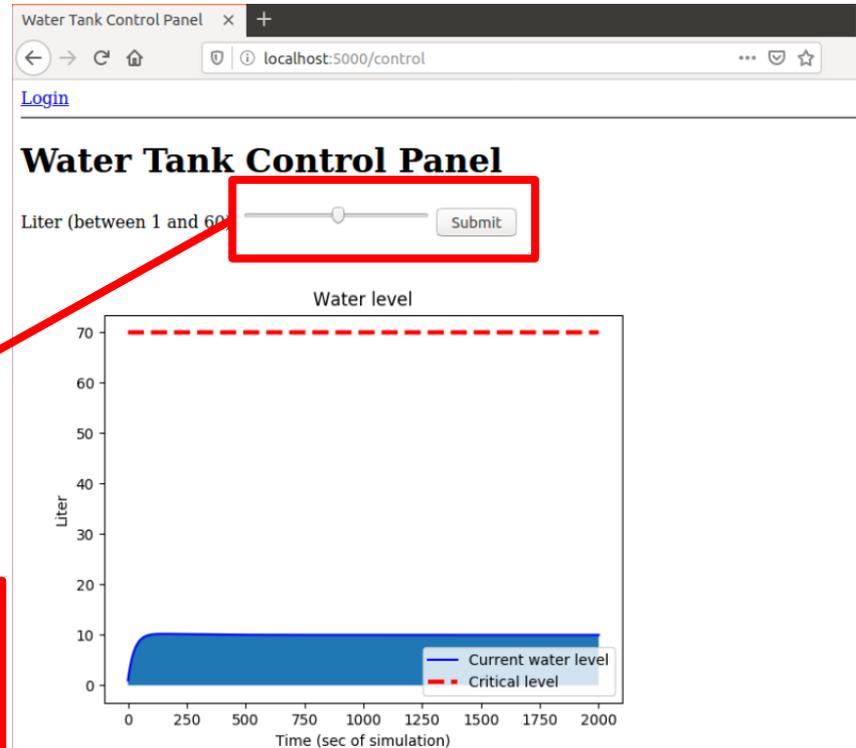
Username Password

You can always go back to the login page using this link

Exercise (part 2)

2. Cause a **water leaking**, by overflowing water tanking with a value higher than the maximum admitted water level, or **water flooding**, by pouring the water tank

You can set the water level using this control bar (Pressing "Submit" will take some time to run again the simulation)

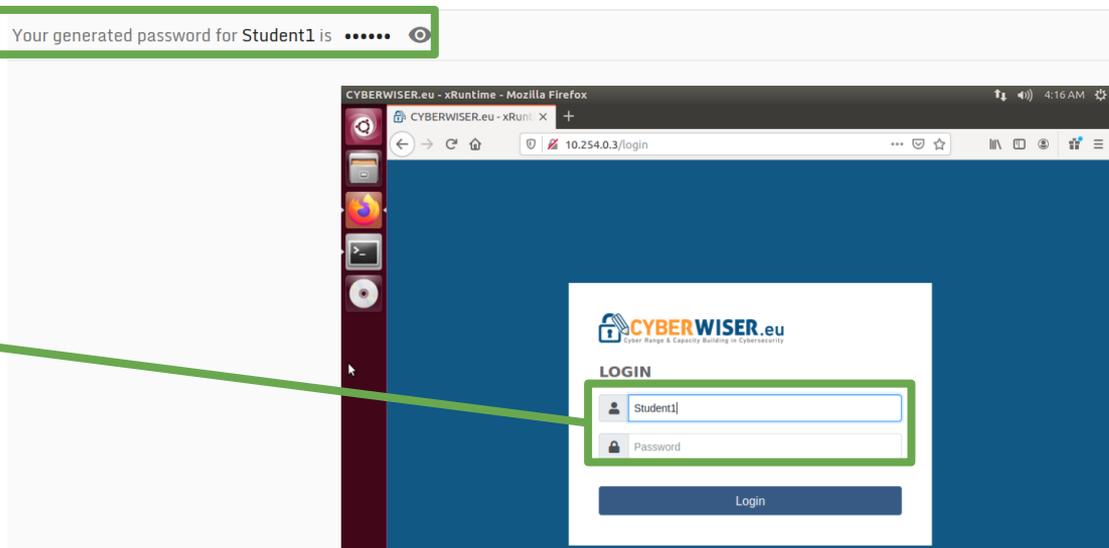


Hints (1)

If you are stuck with the exercise, you have the **Vulnerability Assessment Tool** at your disposal:

- Open a tab of the Browser and go to: <http://10.254.0.3>

Insert the
credentials written
above



Hints (2)

Select **SCANS**:



You have 2 vulnerability scans at your disposal:

1. Broken Access:
 - Scan the web application for we vulnerabilities in the login management;
2. Change Setpoints:
 - Scan the water tank control page for weakness in the input management;

The screenshot shows the 'SCANS' interface. At the top right, there is a breadcrumb 'HOME > SCAN CONFIGURATION'. Below this is a 'Filters' section with three dropdown menus: 'Scan type:' (set to 'All'), 'Owner:' (set to 'All'), and 'Status:' (set to 'All'). Below the filters is a table with the following data:

Name	Owner	Status	Submitted	Actions
Change Setpoints	Student1	done	22.05.2020 04:43:21	
Broken Access Control	Student1	done	22.05.2020 04:42:41	

Hints (3)

To use one of the scans:

Filters

Owner: Status:

Name	Owner	Status	Submitted	Actions
Change Setpoints	Student1	done	22.05.2020 04:24:35	
Broken Access	Student1	done	22.05. 04:23:59	

1

FILES

Main	Name	Edit
	script.sh	   

Upload Create

Back **Next**

2

ENVIRONMENT VARIABLES

Key	Value	Edit
-----	-------	------

Add new

Back **Next**

3

Hints (3)

To use one of the scans:

RUN OPTIONS

Start immediately
 Yes

Repeat
 No

Run infinitely
 No

5

Back Next

TASK DETAILS

Name*
COPY: Change Setpoints

Indicator id

Tool*
Bash

Timeout
60 s

Exposed ports

4

Back Next

RUN OPTIONS

Start Immediately

Schedule Disabled

6

Back Run scan configuration

Hints (3)

1. Reload the Browser page;
2. Check results:

EXECUTIONS ^			
Started	Finished	Result	Output urls
22.05.2020 04:38:22	22.05.2020 04:38:25	Success	container_output_1590147504292.txt

Evaluation questionnaire

- When you completed all the three exercises don't turn off the VMs, just close the Browser tabs!
- Before exiting the room, open a new Tab on the browser and go to the following address:
 - **bit.ly/cyberrange09**
- Fill the questionnaire to evaluate your experience on the CYBERWISER.eu platform;
- The questionnaire is completely anonymous.