

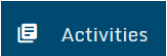


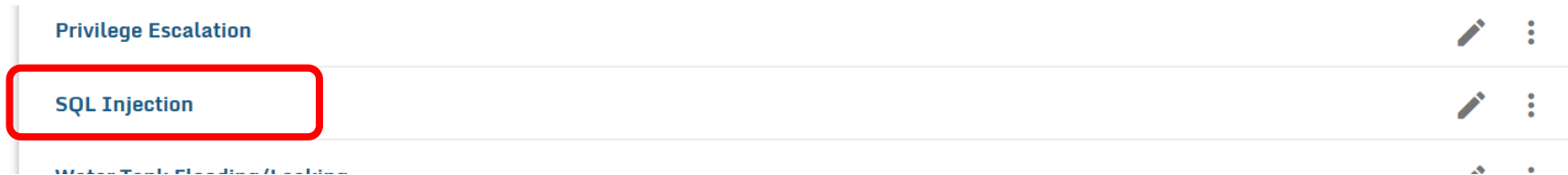
CYBERWISER.EU

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://clustering.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 “SQL Injection”, click on the *name* of the activity:



CYBERWISER.eu workspace

SQL Injection

A SQLi scenario

Topics

Questionario di valutazione

01-Dec-20, 14:18

Alta fine dell'esercitazione, compilare il questionario che trovate al seguente link:

<https://forms.gle/HAHaTx7Vu9f1kE3f7>

Fill the questionnaire at the end!

Add



Documents

Add

No documents to display.

Scenario Environments

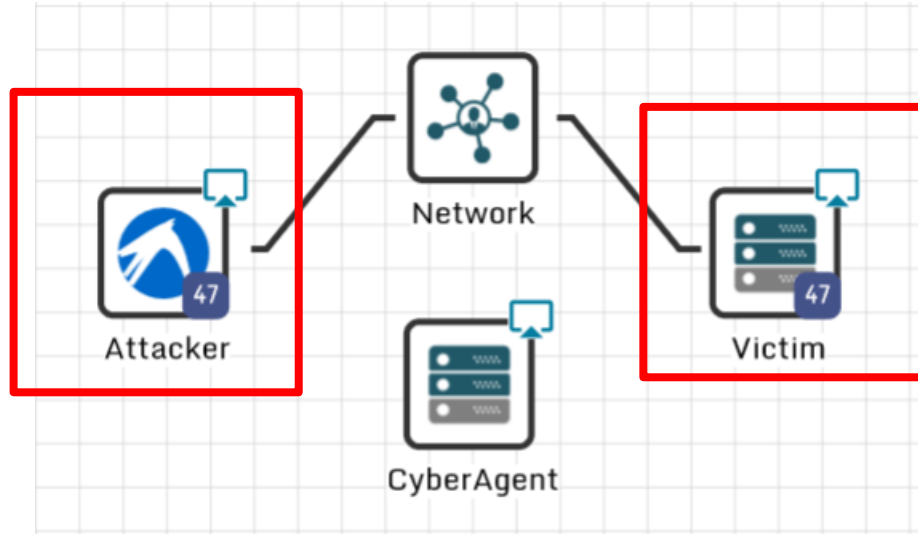
Add

SQL Injection v2



Access to the cyber range

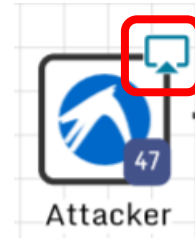
Scenario: Network Topology



CYBERWISER.eu cyber range

1. You have the right to access to a single VM called “**Attacker**”. You can access it with the little screen icon on the top right of each VM icon:

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



Control screen


Full screen

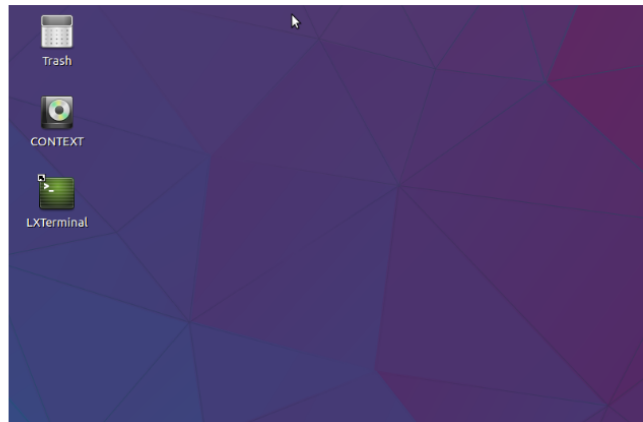
Open in a new Tab

Connected to VM Attacker [1]/QEMU (one-3785)

Send CtrlAltDel



Your generated password for Dario is 



CLOSE

Scenario: How to use the VM

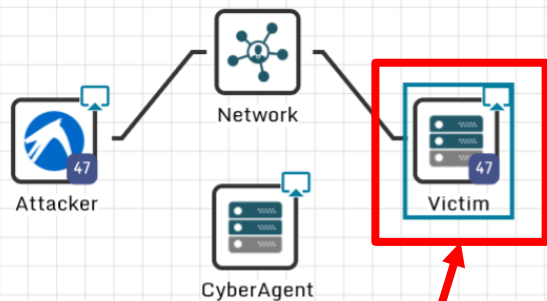
- **“Attacker”:**
 - It is the VM using which you can attack the “Victim”.
- **“Network”:**
 - It is your local network
- **“Victim”:**
 - The machine to attack.
 - To know its IP check next slide

* Depending on your keyboard layout, open a terminal and write:

`setxkbmap it` (for the Italian keyboard)

`setxkbmap us` (for the us keyboard)

Victim: Obtain the IP



1. Click on the Victim

Management Layer. 5 element(s)

2. If your username is StudentX, then
your Victim is VMX, e.g.:

Student1 → VM1

Student2 → VM2

APPLICATION ... NETWORK

General

Asset

Virtual Machine

Network Interfaces

Network

~ VM network configuration

> VM1: 192.168.100.1 / 255.255.255.0

> VM2: 192.168.100.3 / 255.255.255.0

> VM3: 192.168.100.4 / 255.255.255.0

> VM4: 192.168.100.5 / 255.255.255.0

> VM5: 192.168.100.6 / 255.255.255.0

Evaluation questionnaire

- When you completed the training session don't turn off the VMs, just close the Browser!
- After closing the training session, go to the following address using your PC:
 - <https://forms.gle/9Qpp6EcUruZeK7Pe8>
- Fill the questionnaire to evaluate your experience on the CYBERWISER.eu platform;
- The questionnaire is completely anonymous.