Co-funded by the Erasmus+ Programme of the European Union

ISSES

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Cloud Security Laboratory (CS Lab) (SU Lab) design

Version 0.3

Author(s)/Organisation(s):

Bojan Kuljic, (VTS), Igor Furstner (VTS)

Date of final release:

Relevant Work Package(s):

WP3 – Lab development

Short Description:

Cloud Security laboratory design description.

Keywords:

Cloud Security Laboratory

Revision History:

Revision	Date	Author(s)	Status	Description
V0.1	Feb 05, 2021	Bojan Kuljic, Igor Furstner	Working draft	First edition
V0.2	Apr 01, 2021	Bojan Kuljic, Igor Furstner	Working draft	Added lab equipment setup figure
V0.3	Apr 12, 2021	Bojan Kuljic	Final draft	Revised lab equipment setup

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

CONTENTS

1 Lab equipment list

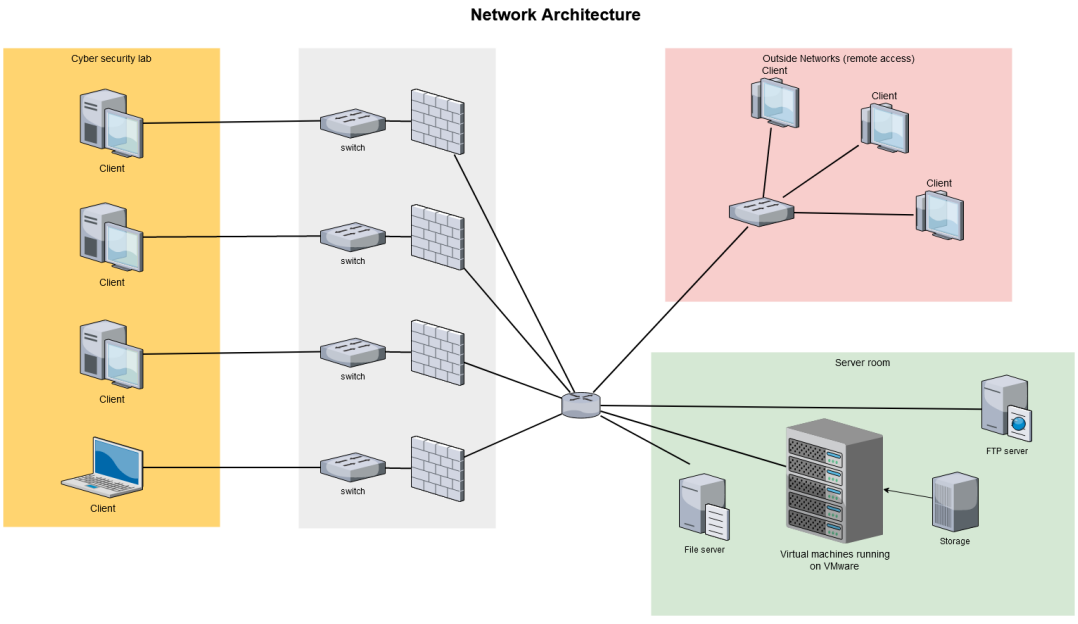
- Acquired through ISSES – Information Security Services Education in Serbia project, supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Type of equipment	Specification	Quantity
Server	Lenovo ThinkSystem SR550 Server (Xeon SP Gen 1)	4
Switch L2/L3	JUNIPER EX2300-24T L2/L3 24 x 1G + 4 x SFP/SFP+	4
Switch optic	Lenovo B300 FC SAN Switch	1
UPC	SOCOMEC NETYS RT 5000VA, NRT2-500K	1
Storage	HDD HP 900 GB 6G SAS SFF	15

- Available from home institution

Type of equipment	Specification	Quantity
Desktop PC	Lenovo Think 10SQSOMT00 THINKCENTRE M720T CORE	28
Desktop PC	Lenovo Think 10SQSOQ800 THINKCENTRE M720T CORE	3

- Lab equipment setup



2 Lab software list

- Acquired through ISSES – Information Security Services Education in Serbia project, supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP:
  None

- Available from home institution

Type of software	**Specification**
Virtualization	WMWare
OS	Windows 10, Kali Linux, Ubuntu
E-learning	Moodle, BigBlueButton
Network security	Nmap, Wireshark, tcpdump, Nagios other free tools

3 Lab exercise list

- Developed through ISSES – Information Security Services Education in Serbia project, supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Area of exercise	**Specification**
Attacking the IoT system	Three examples shows use of the Node MCU microcontroller for building an IoT system. The NodeMCU (Node MicroController Unit) is an open-source software and hardware development environment built around an inexpensive System-on-a-Chip (SoC) called the ESP8266.
Finding and monitoring nearby Wi-Fi devices	This lesson demonstrates tools in Kali Linux for finding near Wi-Fi devices.
Disable a Wi-Fi Security Camera with Aireplay-ng	This lesson demonstrates an attack on a specific device, an IP camera. Kismet tool will be used to find the MAC address of the device, and attack only it, not the whole network.
Crack WPA2 PSK Passwords Using Aircrack Ng Tool	This lesson explains so called Dictionary attack method (brute force attack technique).
Evil Twin Attack	An evil twin attack is a type Wi-Fi attack that works by taking advantage of the fact that most computers and phones will only see the "name" or ESSID of a wireless network.
IoT Security: Tips to Protect your Device from Bad Hackers	This Lesson focuses on methods to secure your Raspberry Pis using Firewall, IDS, and SSL/TLS
XSS (Cross Site Scripting) attacks testing and protection against them	In this exercise XSS (Cross Site Scripting) attacks on one web form will be introduced. Web form could be any web interface for some IOT project that is collecting, storing, processing and presenting some kind of data.
Access restriction to the website at the level of program code	This exercise demonstrates techniques for designing websites with access restrictions.
Weather info screen	This exercise demonstrates creating a web page to display weather data from the *iot* database, *city* and the *city_data* tables for three cities: Subotica, London and Athens. For getting weather data for these cities *OpenWeatherMap API* is used. Weather data is presented in three columns with the image of city on the top of the each column. API returns a large set of data in JSON format.