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

Network Security Laboratory (NS Lab) design

Version 0.2

Author(s)/Organisation(s):

Zarko Stanisavljevic / UB-ETF

Pavle Vuletic / UB-ETF

Igor Tartalja / UB-ETF

Date of final release:

TBD

Relevant Work Package(s):

WP3 – Lab development

Short Description:

Network security laboratory design description.

Keywords:

Network Security Laboratory

Revision History:

Revision	Date	Author(s)	Status	Description
V0.1	Nov 05, 2019	Zarko Stanisavljevic	Working draft	First edition
V0.2	Mar 11, 2020	Zarko Stanisavljevic	Working draft	Added lab equipment setup figure

CONTENTS

1 Lab equipment list

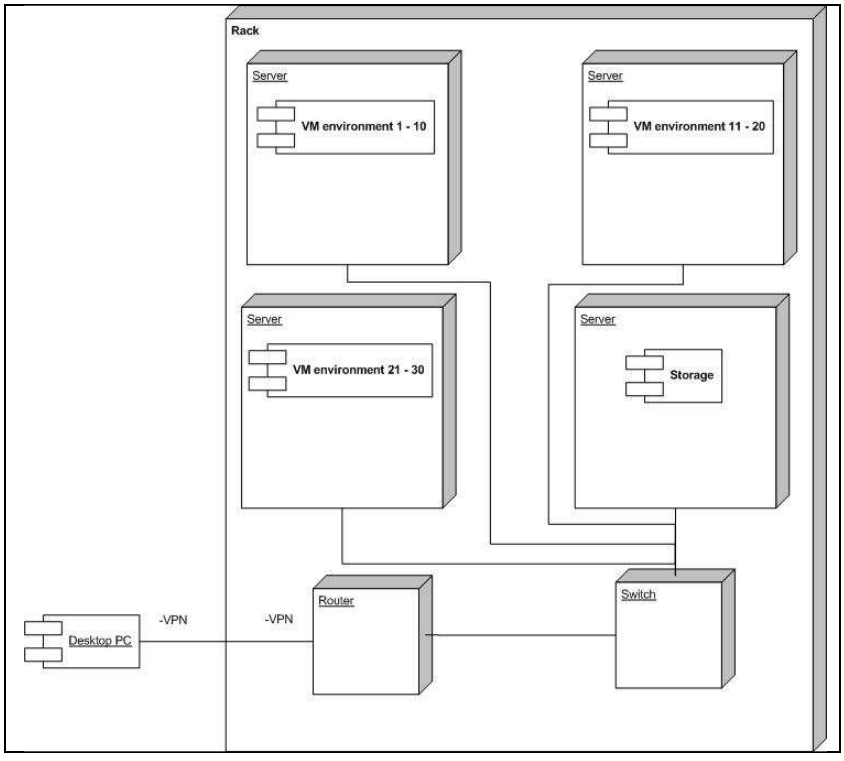
- Acquired through ISSES – Information Security Services Education in Serbia project, supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Type of equipment	Specification	Quantity
Server	2 x 14C/28T CPU (Xeon Gold 5120, 2.2GHz), 128GB RAM, 4 x 800GB SSD Total 56 Threads	4
Switch L2/L3	L2/L3 24 x 1G + 4 x SFP/SFP+	1
Rack	42U	1

- Available from home institution

Type of equipment	Specification	Quantity
Desktop PC	Intel Core i5-2320 @ 3.00GHz, 8GB DDR3 RAM, 500GB SATAIII HDD or similar	200+

- 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 or similar
OS	Windows 10, Kali Linux, Ubuntu
E-learning	Moodle
Network security	Nmap, Wireshark, tcpdump, 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**
Reconnaissance	Packet capture, Wireshark, tcpdump, netstat, nmap , Shodan
Network attack examples	ARP spoofing, DNS spoofing,…
System attack examples	SQL injections, EternalBlue and similar
Network protection	Firewall, IPS, IDS, packet filters (iptables)
Log management	SIEM
DDoS	Attack/defense
Penetration testing	Final exam

Note: Presentations for all above mentioned laboratory exercises, printed to PDF files, will be available through ISSES web site (page: https://isses.etf.bg.ac.rs/advanced-network-and-systems-security-2-6/)