	Universitas Negeri Surabaya Faculty of Engineering, Undergraduate Study Program in Informatics Engineering	Document Code

SEMESTER LEARNING PLAN

Courses	CODE	Course Family	Credit Weight			SEMESTER	Compilation Date
Data and Information Security	5520203140		T=3	P=0	ECTS=4.77	4	July 18, 2024

AUTHORIZATION	SP Developer	Course Cluster Coordinator	Study Program Coordinator
	.....	.....	Aditya Prapanca, S.T., M.Kom.

Learning model	**Project Based Learning**	
Program Learning Outcomes (PLO)	**PLO study program that is charged to the course**	
	PLO-2	Able to design and simulate multi-platform technology applications that are relevant to the needs of industry and society using theoretical concepts in the field of computer science/informatics knowledge (KNO-02)
	PLO-5	Able to communicate the results of studies on the implications of developing or implementing information technology science (SKI-02)
	PLO-7	Ability to design, implement, and evaluate multi-platform computing-based solutions that meet organizational needs (COM-02)
	Program Objectives (PO)	
	PO - 1	Students will be able to understand the concepts and attack techniques used by attackers/hackers in carrying out attacks on information system security gaps
	PO - 2	Students will be able to know applications for reading and analyzing information system security gaps
	PLO-PO Matrix	

P.O	PLO-2	PLO-5	PLO-7
PO-1			
PO-2			

PO Matrix at the end of each learning stage (Sub-PO)

P.O	Week															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
PO-1																
PO-2																

Short Course Description	This course contains basic concepts of computer network communication flow, protocols, layers, addressing, topology, configuration and testing of computer networks.	
References	**Main :**	

1. William Stallings. 2017. Cryptography and Network Security Principles and Practice Seventh Edition Global Edition. Pearson.
2. William Stallings. 2017. Network Security Essentials : Applications and Standards Sixth edition Global edition. Pearson
3. Joseph Migga Kizza. 2020. Guide to Computer Network Security Fifth Edition. Springer.
4. Susanti, Palupi, Wibawa, Nerisafitra. 2020. SOSIALISASI TENTANG PRIVACY DAN KEAMANAN INTERNET PADA PESERTA DIDIK SMP NEGERI 1 WARU
5. Suartana, Prapanca, Putra. 2021. PENGENALAN PENTINGNYA CYBER SECURITY AWARENESS PADA UMKM

Supporters:

Supporting lecturer	I Made Suartana, S.Kom., M.Kom.

Week-	Final abilities of each learning stage (Sub-PO)	Evaluation		Help Learning, Learning methods, Student Assignments, [Estimated time]		Learning materials [References]	Assessment Weight (%)
		Indicator	Criteria & Form	Offline (*offline*)	Online (*online*)		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Students are able to explain the types of devices, operating systems and computer machine virtualization technology at least 80% correctly.	1.Can find out the devices that will be used in information system security simulations 2.Can understand virtual machine technology 3.Can know the types of computer operating systems 4.Can find out the types of attackers / hackers	**Form of Assessment** : Participatory Activities, Project Results Assessment / Product Assessment	lecture, discussion 2x50			0%
2	Students are able to explain the steps and methodology of footprinting information system security attacks at least 80% correctly	1.Can find out the steps taken by the attacker in attacking the security of the information system 2.Can understand the methodology and function of footprinting attacks on information systems 3.Can find out the equipment used to carry out footprinting of information systems		lecture, discovery learning, discussion 2x50			0%
3	Students are able to explain the steps and methodology of network scanning information system security attacks at least 80% correctly	1.Can find out the steps taken by attackers in attacking information system security 2.Can understand the methodology and function of scanning network attacks on information systems 3.Can find out the equipment used to scan information system networks	**Form of Assessment** : Participatory Activities, Project Results Assessment / Product Assessment	simulation, discussion 2x50			0%

4	Students are able to explain the steps and methodology of information system security attacks enumeration at least 80% correctly	1. Can find out the steps taken by attackers in attacking information system security 2. Can understand the methodology and function of enumeration attacks on information systems 3. Can find out the equipment used to carry out information system enumeration	**Form of Assessment** : Participatory Activities				0%
5	Students are able to explain the steps and methodology of hijacking information system security attacks at least 80% correctly.	1. Can find out the steps taken by attackers in attacking information system security 2. Can understand the methodology and function of system hacking attacks on information systems 3. Can find out the equipment used to hack information systems	**Form of Assessment** : Participatory Activities	simulation, discussion 2x50			0%
6	Students are able to explain the types and characteristics of malicious software such as trojans and backdoors at least 80% correctly.	1. Can find out the types of malicious software 2. Can understand the characteristics of malicious software such as trojans and backdoors		simulation, discussion 2x50			0%
7	Students are able to explain the types and characteristics of malicious software such as viruses and worms at least 80% correctly.	1. Can find out the types of malicious software 2. Can understand the characteristics of malicious software such as viruses & worms		simulation, discussion 2x50			0%
8	Midterm exam						0%
9	Able to explain the steps and methodology of sniffing information system security attacks at least 80% correctly.	1. Can find out the steps taken by attackers in attacking information system security 2. Can understand the methodology and function of sniffing attacks on information systems 3. Can find out the equipment used to sniff information systems		simulation, discussion 2x50			0%

10	Students are able to explain the steps and methodology of social engineering information system security attacks at least 80% correctly	1. Can find out the steps taken by attackers in attacking information system security 2. Can understand the methodology and function of social engineering attacks on information systems 3. Can find out the equipment used to carry out social engineering of information systems		cooperative learning 2x50			0%
11	Students are able to explain the steps and methodology of Denial of Service information system security attacks at least 80% correctly	1. Can find out the steps taken by attackers in attacking information system security 2. Can understand the methodology and function of Denial of Service attacks on information systems 3. Can find out the equipment used to carry out information system denial of service		contextual instruction 2x50			0%
12	Students are able to explain the steps and methodology of Session Hijacking information system security attacks at least 80% correctly.	1. Can find out the steps taken by attackers in attacking information system security 2. Can understand the methodology and function of session hijacking attacks on information systems 3. Can find out the equipment used to conduct information system hijacking sessions		contextual instruction 2x50			0%

13	Students are able to explain the steps and methodology for information system security attacks hacking web applications at least 80% correctly.	1.Can find out the steps taken by attackers in attacking information system security 2.Can understand the methodology and function of hacking web attacks on information systems 3.Can find out the equipment used to hack web information systems		simulation, discussion 2x50			0%
14	Students are able to explain the steps and methodology of SQL Injection information system security attacks at least 80% correctly.	1.Can find out the steps taken by attackers in attacking information system security 2.Can understand the methodology and function of SQL injection attacks on information systems 3.Can find out the equipment used to perform SQL injection of information systems		Contextual instructions 2x50			0%
15	Students are able to explain information system security support software at least 80% correctly.	1.Can find out the format of data content in communication between computers 2.Can find out the equipment used to detect the contents of data packets in communications between computers		simulation, discussion			0%
16	Final exams						0%

Evaluation Percentage Recap: Project Based Learning

No	Evaluation	Percentage
		0%

Notes

1. **Learning Outcomes of Study Program Graduates (PLO - Study Program)** are the abilities possessed by each Study Program graduate which are the internalization of attitudes, mastery of knowledge and skills according to the level of their study program obtained through the learning process.
2. **The PLO imposed on courses** are several learning outcomes of study program graduates (CPL-Study Program) which are used for the formation/development of a course consisting of aspects of attitude, general skills, special skills and knowledge.
3. **Program Objectives (PO)** are abilities that are specifically described from the PLO assigned to a course, and are specific to the study material or learning materials for that course.
4. **Subject Sub-PO (Sub-PO)** is a capability that is specifically described from the PO that can be measured or observed and is the final ability that is planned at each learning stage, and is specific to the learning material of the course.
5. **Indicators for assessing** ability in the process and student learning outcomes are specific and measurable statements that identify the ability or performance of student learning outcomes accompanied by evidence.

6. **Assessment Criteria** are benchmarks used as a measure or measure of learning achievement in assessments based on predetermined indicators. Assessment criteria are guidelines for assessors so that assessments are consistent and unbiased. Criteria can be quantitative or qualitative.
7. **Forms of assessment:** test and non-test.
8. **Forms of learning:** Lecture, Response, Tutorial, Seminar or equivalent, Practicum, Studio Practice, Workshop Practice, Field Practice, Research, Community Service and/or other equivalent forms of learning.
9. **Learning Methods:** Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, and other equivalent methods.
10. **Learning materials** are details or descriptions of study materials which can be presented in the form of several main points and sub-topics.
11. **The assessment weight** is the percentage of assessment of each sub-PO achievement whose size is proportional to the level of difficulty of achieving that sub-PO, and the total is 100%.
12. TM=Face to face, PT=Structured assignments, BM=Independent study.