الجامعة الافتراضية السورية
SYRIAN VIRTUAL UNIVERSITY

Computer Network Security

Course Definition

Information

Technology

Engineering

Powered by: KNOWLGICA
KNOWLEDGE SOLUTIONS & TECH

Syrian Arab Republic		الجمهورية العربية السورية
Ministry of Higher Education and Scientific Research		وزارة التعليم العالـــي والبحث العلمي
Syrian Virtual University		الجامعة الافتراضية السورية

1. Basic Information:

Course Name	Computer Network Security
Course Code	NSS601
Number of Presentational Sessions*	20
Number of Synchronous Sessions**	10
Number of Shorter Tests***	2
Number of Exams***	1
Theoretical Sessions Work Load (hrs.)	60
Practical Sessions Work Load (hrs.)	30
Credit Hours	6

***Each presentational session comprises both recorded lecture (1.5 hrs.) and interactive learning content (1.5 hrs.).**

****Each synchronous session comprises the interactive lecture carried out in real time in a virtual class (1.5 hrs.).**

*****Each shorter test is 0.5 hr. long. The final exam is 2 hrs. long.**

N.B.

Generally, each chapter requires two presentational sessions: one for the recorded content and one for the interactive content (unless the chapter is too long, in which case it may require more sessions (. This note applies to synchronous sessions as well, where each chapter requires one synchronous session generally.

2. Prerequisites courses:

Course	Code
Information System Security	BIS601

3. Course Objectives:

This course provides the student with the essentials of computer network security. The student will explore the most important basics, standards and technologies in this field. The course starts with an overview of security concepts in general, with an emphasis on the concepts related to network security, then the course explains the techniques of building mutual trust between communicating parties, and based on these concepts and techniques, the course elaborates the most common network and internet security technologies, protocols and standards.

4. Learning Outcomes (LO):

By the end of this course the learner is expected to:

- Acquiring the knowledge of the basic concepts in computer and network security.
- Gaining the ability to select and use the key management and distribution techniques according to the application.
- Studying the different types of remote user authentication and network access control.
- Gaining the ability to use the different techniques of transport level security and Email security.
- Acquiring the knowledge of the basic concepts and mechanisms of wireless network security.
- Studying the standards and protocols of IP security.

5. Assessment Results:

Chapter Number	Chapter Title	General Objectives	Assessment Type				
			Interactive Content & Recorded Sessions	Applied Activities (Synch. Sessions)	Final Exam*/ Shorter Tests**	Presentations and Interviews	Reports
CH1	Computer and Network Security Concepts	Comprehension –Analytical Thinking –Tools and Application Hands– On	√	√	√	√	√
CH2	Key Management and Distribution	Comprehension –Analytical Thinking –Tools and Application Hands– On	√	√	√	√	√
CH3	User Authentication	Comprehension –Analytical Thinking –Tools and Application Hands– On	√	√	√	√	√
CH4	Network Access Control	Comprehension –Analytical Thinking –Tools	√	√	√	√	√

		and Application Hands– On					
CH5	Transport– Level Security	Comprehension –Analytical Thinking –Tools and Application Hands– On	√	√	√	√	√
CH6	Wireless Network Security	Comprehension –Analytical Thinking –Tools and Application Hands– On	√	√	√	√	√
CH7	Electronic Mail Security	Comprehension –Analytical Thinking –Tools and Application Hands– On	√	√	√	√	√
CH8	IP Security	Comprehension –Analytical Thinking –Tools and Application Hands– On	√	√	√	√	√

***The final exam is two hours long and is given at the end of the course.**

****Shorter tests are about 30 minutes long and are given after three or four lectures throughout the semester during synchronous sessions.**

Syrian Arab Republic		الجمهورية العربية السورية
Ministry of Higher Education and Scientific Research		وزارة التعليم العالـــي والبحث العلمي
Syrian Virtual University		الجامعة الافتراضية السورية

***Presentations, interviews, and reports are submitted once after each three or four lectures throughout the semester during synchronous sessions.

Syrian Arab Republic		الجمهورية العربية السورية
Ministry of Higher Education and Scientific Research		وزارة التعليم العالـــي والبحث العلمي
Syrian Virtual University		الجامعة الافتراضية السورية

6. Course Syllabus:

Chapter	Subject	Content	Number of Learning Objects	Number of synchronous Learning Objects
CH1	**Computer and Network Security Concepts**	1. Computer security concepts. 2. Computer challenges 3. The OSI security architecture. 4. Security attacks. 5. Security services. 6. Security mechanisms. 7. A model for network security. 8. Conclusion	8	4
CH2	**Key Management and Distribution**	1. Introduction 2. Distribution of symmetric keys. 3. Asymmetric key distribution 4. Distribution of public keys. 5. X.509 certificates. 6. Public-Key Infrastructure.	6	3
CH3	**User Authentication**	1. User authentication principles 2. User authentication using symmetric encryption 3. User authentication using asymmetric encryption	6	3

		4. Kerberos service. 5. Unified identity management. 6. Personal identity verification..		
CH4	**Network Access Control**	1. Introduction 2. Elements and methods. 3. Extensible Authentication Protocol. 4. IEEE 802.1X port-based network access control.	**4**	**2**
CH5	**Transport-Level Security**	1. Introduction 2. Web security considerations. 3. Transport Layer Security. 4. HTTPS. 5. Secure Shell (SSH)	**5**	**2**
CH6	**Wireless Network Security**	1. Introduction 2. Finally, security networks. 3. Take the necessary measures to receive wireless networks. 4. Mobile devices 5. Renewable IEEE 802.11i 6. IEEE 802.11i rubber services 7. IEEE 802.11i rubber target 8. Working phases on IEEE 802.11i 9. Conclusion	**9**	**4**

CH7	**Electronic Mail Security**	1. Email threats. 2. S/MIME. 3. Pretty Good Privacy. 4. DNS-based authentication. 5. Sender Policy Framework. 6. DomainKeys Identified Mail. 7. Domain-based Message Authentication, Reporting and Conformance. 8. Conclusion	**8**	**4**
CH8	**IP Security**	1. IP security overview. 2. IP security policy. 3. Encapsulating Security Payload. 4. Combining security associations. 5. Internet Key Exchange.	**5**	**2**

7. Practical Activity:

- **Tools and Labs:**

Tool Name	Description
Cryptool	Cryptographic tool (online / offline)
OpenSSL	Cryptography and internet Security

- **Practical Activities per Chapters:**

Chapter	Activities Type	Remarks
CH1	☐ Exercises ☐ Homework ☐ Webinars ☐ Project ☐ Experiment ☐ Other	
CH2	☑ Exercises ☑ Homework ☐ Webinars ☐ Project ☐ Experiment ☐ Other	
CH3	☑ Exercises ☐ Homework ☐ Webinars ☐ Project	

	☐ Experiment ☐ Other	
CH4	☑ Exercises ☐ Homework ☐ Webinars ☐ Project ☐ Experiment ☐ Other	
CH5	☑ Exercises ☑ Homework ☐ Webinars ☐ Project ☐ Experiment ☐ Other	
CH6	☑ Exercises ☐ Homework ☐ Webinars ☐ Project ☐ Experiment ☐ Other	
CH7	☑ Exercises ☑ Homework ☐ Webinars ☐ Project ☐ Experiment ☐ Other	

CH8	☑ Exercises ☐ Homework ☐ Webinars ☐ Project ☐ Experiment ☐ Other	

8. References:

- Stallings, W., and L. Brown. “Computer Security: Principles and Practice, Global Edition”, 2018.
- Stallings, William. “Cryptography and network security”, 2017.