University of Mosul
College of Engineering
Computer Engineering Dept.

Network Security
Theory
Instructer: Asst. Prof. Dr. Mayada Faris Ghanim

Course Objectives:

By the end of this course, students will be able to:

1. State the basic concepts of network security, including security policies, security models, and security mechanisms
2. State the main terminologies of computer security, including assets, vulnerability, threats and types of threats.
3. Explain C-I-A triad or the security triad.
4. Explain concepts related to applied cryptography, including plain-text, cipher-text, crypto-analysis, symmetric cryptography, asymmetric cryptography, message authentication code, hash functions, and modes of encryption operations.
5. State and explain the basics of cryptosystem including the steps and details of DES, AES algorithms.
6. Explain the concepts of malicious code, including virus, Trojan horse, and worms.
7. Explain common vulnerabilities in computer programs, including buffer overflow vulnerabilities, time-of-check to time-of-use flaws, incomplete mediation.
8. Outline the requirements and mechanisms for identification and authentication.
9. Explain issues about password including all the steps and details of hash code
10. Explain and compare security mechanisms for conventional operating systems, including memory, time, file, object protection requirements and techniques and protection in contemporary operating systems.

Course Details:

This course includes the following topics:

1. Introduction to network security: Basic concepts: threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies and C-I-A triad.
2. The OSI Security Architecture: Security attack (passive and active attack), security mechanisms and relationship between security services and mechanisms
3. Identification and Authentication: authentication mechanisms, authentication based on something the user knows, the user is, or the user has.
4. Hash Function: One-Way Hash Functions, Message Digests and secure Hash algorithms, SHA-512 (all the processing steps and round function).

5. Cryptography: Problems Addressed by Encryption, Encryption, decryption, cryptosystem, plaintext, ciphertext, Encryption Keys, Encryption Keys, Stream and Block Ciphers, Work Factor.
6. Data Encryption Standard (DES): Double DES, Triple DES, Depiction of DES Encryption Algorithm, DES Round Function.
7. Advanced Encryption Standard (AES): General Structure of AES, AES Encryption Process, AES Data Structures, AES Parameters and Detailed Structure, AES Encryption and Decryption, AES Encryption Round, AES Transformation Functions, AES Key Expansion, Strength of the Algorithm, Comparison of DES and AES.
8. Access Control: Access Policies, Effective Policy Implementation, Tracking, Granularity, Access Log, Limited Privilege, Implementing Access Control, Reference Monitor, Access Control Directory, Access Control Matrix, Access Control List, Privilege List.
9. Security in conventional operating systems: Memory, time, file, object protection requirements and techniques.
10. Security in conventional operating systems: Protection in contemporary operating systems
11. Program Security Defenses: Software development controls, Testing techniques.
12. Program security Flaws: Malicious code: viruses, Malware, Trojan horses, worms.
13. Program Security Flaws: buffer overflows, time-of-check to time-of-use flaws, incomplete mediation
14. Introduction to human recognition as systems of authentication mechanisms for providing security of computer and networks.
15. Introduction to artificial intelligence and network security.
16. IP Security, IP Security modes, IP Security protocols, Internet Key Exchange (IKE) and Virtual Private Network.
17. Transport layer security including SSL Architecture and Protocols
18. Application layer security including E-mail Security, Pretty Good Privacy (PGP) and Key Rings.

Text Books:

1. Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, Prentice Hall, fifth edition, ISBN-13: 978-0-13-408504-3, 2015.
2. Cryptography and Network Security Principles and Practice, William Stallings, Pearson Education, seventh edition, ISBN 978-0-13-444428-4, 2017

Weekly teaching plan

Subject	No. of Weeks
Introduction to Network Security: Network Security in Layers, Vulnerability, threat, controls, C-I-A triad, availability, integrity and confidentiality	1

The OSI Security Architecture: Security attack, Security mechanism and Security service	1
Authentication: Authentication mechanisms, Hash Function, Message Digests and Secure Hash Algorithms, SHA-512, Round Function	1
Cryptography: Encryption, decryption, Problems Addressed by Encryption, Encryption Keys, Symmetric and Asymmetric Encryption Systems, Stream and Block Ciphers	1
Work factor and Data Encryption Standard (DES): Overview of the DES Algorithm, Double DES, Triple DES, General Depiction of DES Encryption Algorithm, DES Round function	1
Advanced Encryption Standard (AES): General Structure of AES, AES Parameters, Detailed Structure, AES Encryption Round, AES Transformation Functions, AES Key Expansion, Strength of the Algorithm	1
Access Control: Access Policies, Effective Policy Implementation, Tracking, Granularity, Access Log, Limited Privilege, Implementing Access Control	1
Introduction to Artificial intelligence applications in network security	2
Security in operating system	1
IP Security, IP Security modes, IP Security protocols, Internet Key Exchange (IKE) and Virtual Private Network	2
Transport layer security	1
Application layer security	1
Term exam	1
Total	**15**