TEXAS A&M UNIVERSITY
SAN ANTONIO

CSEC 5306, **Computer Networks and Security**

Department of Computing, Engineering and Mathematical Sciences, College of Arts and Science

Course Syllabus

Class Meeting Time and Place: M 5:30 pm - 08:15 PM, Online

Class Duration: 01/21 to 05/13/2025

Instructor: Dr. Izzat Alsmadi, Tel: 210-784-2313 E-Mail: ialsmadi@tamusa.edu

Office Hours:

Tuesday….02:00 pm -0400 pm Online

Thursday…..200 pm – 5:30pm Online

Catalog Course Description:

CSEC 5306: This course will cover advanced topics in computer networks, such as, wireless networks, cloud and Big Data networks. Students will gather knowledge on the vulnerabilities in different types of networks, detection methods, and "state-of-the-art" techniques to prevent them.

Other subjects include: Wireless, mobile and cloud network vulnerabilities and detection methods, defense techniques, moving target techniques and network access controls.

Prerequisite: CCS Department Approval.

Course Objectives: The objective of the course is to:

- Understand security protocols for protecting data on networks
- Understand vulnerability assessments and the weakness of using passwords for authentication
- Be able to perform simple vulnerability assessments and password audits
- Be able to configure simple firewall architectures
- Understand the most common type of cryptographic algorithms
- Understand Virtual Private Networks
- Identify network security tools and discuss techniques for network protection.
- Describe the fundamental functions performed by firewalls.
- Describe network security implementation strategies and the roles each can play within the security life cycle.
- Identify network security management best practices and strategies for responding when security measures fail.

Learning Outcomes

After successful completion of the course, the learners would be able to:

- Provide security of the data over the network.
- Do research in the emerging areas of network security.
- Implement various networking protocols.
- Protect any network from the threats in the world.
- Identify and assess current and anticipated security risks and vulnerabilities
- Create ACLs to filter traffic through the firewall
- Establish a VPN to allow IPSec remote access traffic
- Protect network from internal and external threats
- Control enterprise network traffic
- Monitor, evaluate and test security conditions and environment
- Monitor, report and resolve security problems