# Wayland Logo

Virtual Campus

School of Business

# 2. UNIVERSITY MISSION STATEMENT

Wayland Baptist University exists to educate students in an academically challenging, learning-focused and distinctively Christian environment for professional success, and service to God and humankind.

# 3. COURSE NUMBER & NAME:

MISM 4306-VC01, Information Systems Security

# **4. TERM**:

Spring 2 2022

# **5. INSTRUCTOR**:

Jimmy Fikes

# **6. CONTACT INFORMATION**:

Cell phone: 806-831-3918

WBU Email: Jimmy.Fikes@wayland.wbu.edu

# **7. OFFICE HOURS, BUILDING & LOCATION**:

Students may request personal conferences with the instructor on any day, and at any time.

# **8. COURSE MEETING TIME & LOCATION**:

This class will be conducted entirely online on Blackboard.

# **9. CATALOG DESCRIPTION**:

Designed to provide security knowledge mastery of an individual with two years on-the-job networking experience, with emphasis on security. Industry wide topics including communication security, infrastructure security, cryptography, access control, authentication, and operational security. Students have the opportunity at no extra cost to take the Certification Exam [Testout Security Pro] at the completion of the course.

# 10. PREREQUISITE:

COSC 2311

# **11. REQUIRED TEXTBOOK AND RESOURCE MATERIAL**:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **BOOK** | **AUTHOR** | **ED** | **YEAR** | **PUBLISHER** | **ISBN#** | **UPDATED** |
| Security Pro LabSim | Testout | Ver 7 | 2020 | TestOut | 9781-93508-0442 | 1/11/21 |

# 12. OPTIONAL MATERIALS

None

# **13. COURSE OUTCOMES AND COMPETENCIES**:

* Describe the vulnerabilities of an information system and establish a plan for risk management
* Demonstrate how to detect and reduce threats in Web security
* Describe the authentication and encryption needs of an information system
* Demonstrate how to secure a wireless network

# 14. ATTENDANCE REQUIREMENTS:

As stated in the Wayland Catalog, students enrolled at one of the University’s external campuses should make every effort to attend all class meetings. All absences must be explained to the instructor, who will then determine whether the omitted work may be made up. When a student reaches that number of absences considered by the instructor to be excessive, the instructor will so advise the student and file an unsatisfactory progress report with the campus executive director. Any student who misses 25 percent or more of the regularly scheduled class meetings may receive a grade of F in the course. Additional attendance policies for each course, as defined by the instructor in the course syllabus, are considered a part of the University’s attendance policy.

# **15. STATEMENT ON PLAGIARISM & ACADEMIC DISHONESTY**:

Wayland Baptist University observes a zero-tolerance policy regarding academic dishonesty. Per university policy as described in the academic catalog, all cases of academic dishonesty will be reported and second offenses will result in suspension from the university.

# **16. DISABILITY STATEMENT**:

In compliance with the Americans with Disabilities Act of 1990 (ADA), it is the policy of Wayland Baptist University that no otherwise qualified person with a disability be excluded from participation in, be denied the benefits of, or be subject to discrimination under any educational program or activity in the university. The Coordinator of Counseling Services serves as the coordinator of students with a disability and should be contacted concerning accommodation requests at (806) 291-3765. Documentation of a disability must accompany any request for accommodations.

# **17. COURSE REQUIREMENTS and GRADING CRITERIA**:

* Students will complete all assignments in TestOut and take the certification test as their final exam for this class. Grade calculation for this course
* All work in TestOut will make up 100% of the total term grade.
* **WBU Grading Scale:**

A 90-100

B 80-89

C 70-79

D 60-69

F Below 60

**17.1 Grade Appeal Statement:** “Students shall have protection through orderly procedures against prejudices or capricious academic evaluation. A student who believes that he or she has not been held to realistic academic standards, just evaluation procedures, or appropriate grading, may appeal the final grade given in the course by using the student grade appeal process described in the Academic Catalog. Appeals may not be made for advanced placement examinations or course bypass examinations. Appeals are limited to the final course grade, which may be upheld, raised, or lowered at any stage of the appeal process. Any recommendation to lower a course grade must be submitted through the Vice President of Academic Affairs/Faculty Assembly Grade Appeals Committee for review and approval. The Faculty Assembly Grade Appeals Committee may instruct that the course grade be upheld, raised, or lowered to a more proper evaluation.”

# 18. RECOMMENDED SCHEDULE – Students may work ahead, but the following tables should be viewed as the minimum progress per week.

|  |  |  |
| --- | --- | --- |
| **Week** | **Content Covered** | **Estimated Time to Complete in Minutes** |
| 1st week | 01.01: Security Overview | 24 |
| 1st week | 01.02: Defense Planning | 24 |
| 1st week | 01.03: Using the Simulator | 26 |
| 1st week | 02.01: Understanding Attacks | 45 |
| 1st week | 02.02: Malware | 52 |
| 1st week | 02.03: Social Engineering | 84 |
| 1st week | 02.04: Vulnerability Concerns | 32 |
| 1st week | 03.01: Physical Threats | 34 |
| 1st week | 03.02: Device and Network Protection | 30 |
| 1st week | 03.03: Environmental Controls | 31 |
| 1st week | 04.01: Manageable Network Plan | 33 |
| 1st week | 04.02: Windows System Hardening | 77 |
| 2nd week | 04.03: File Server Security | 62 |
| 2nd week | 04.04: Linux Host Security | 43 |
| 2nd week | 05.01: Security Appliances | 101 |
| 2nd week | 05.02: Demilitarized Zones | 38 |
| 2nd week | 05.03: Firewalls | 49 |
| 2nd week | 05.04: Network Address Translation | 47 |
| 2nd week | 05.05: Virtual Private Networks | 63 |
| 2nd week | 05.06: Web Threat Protection | 41 |
| 2nd week | 05.07: Network Access Control | 22 |
| 2nd week | 05.08: Network Threats | 24 |
| 2nd week | 05.09: Network Device Vulnerabilities | 45 |
| 2nd week | 05.10: Network Applications | 28 |
| 3rd week | 05.11: Switch Security and Attacks | 111 |
| 3rd week | 05.12: Using VLANs | 35 |
| 3rd week | 05.13: Router Security | 69 |
| 3rd week | 06.01: Access Control Models | 50 |
| 3rd week | 06.02: Authentication | 44 |
| 3rd week | 06.03: Authorization | 30 |
| 3rd week | 06.04: Windows User Management | 57 |
| 3rd week | 06.05: Active Directory Overview | 146 |
| 4th week | 06.06: Hardening Authentication | 112 |
| 4th week | 06.07: Linux Users | 126 |
| 4th week | 06.08: Linux Groups | 58 |
| 4th week | 06.09: Remote Access | 33 |
| 4th week | 06.10: Network Authentication | 58 |
| 4th week | 07.01: Cryptography | 91 |
| 4th week | 07.02: Cryptography Implementations | 33 |
| 4th week | 07.03: Hashing | 42 |
| 5th week | 07.04: File Encryption | 70 |
| 5th week | 07.05: Public Key Infrastructure | 76 |
| 5th week | 08.01: Wireless Overview | 43 |
| 5th week | 08.02: Wireless Attacks | 52 |
| 5th week | 08.03: Wireless Defenses | 85 |
| 5th week | 09.01: Host Virtualization | 60 |
| 5th week | 09.02: Virtual Networking | 46 |
| 5th week | 09.03: Software-Defined Networking | 22 |
| 5th week | 09.04: Cloud Services | 46 |
| 5th week | 09.05: Cloud Security | 38 |
| 6th week | 09.06: Mobile Devices | 42 |
| 6th week | 09.07: Mobile Device Management | 39 |
| 6th week | 09.08: BYOD Security | 65 |
| 6th week | 09.09: Embedded and Specialized Systems | 42 |
| 6th week | 10.01: Data Transmission Security | 71 |
| 6th week | 10.02: Data Loss Prevention | 22 |
| 6th week | 10.03: Web Application Attacks | 110 |
| 6th week | 10.04: Application Development and Security | 94 |
| 6th week | 11.01: Penetration Testing | 36 |
| 7th week | 11.02: Monitoring and Reconnaissance | 56 |
| 7th week | 11.03: Intrusion Detection | 44 |
| 7th week | 11.04: Security Assessment Techniques | 99 |
| 7th week | 11.05: Protocol Analyzers | 26 |
| 7th week | 11.06: Analyzing Network Attacks | 101 |
| 7th week | 11.07: Password Attacks | 62 |
| 7th week | 12.01: Incident Response | 29 |
| 7th week | 12.02: Mitigation of an Incident | 28 |
| 7th week | 12.03: Log Management | 62 |
| 7th week | 12.04: Windows Logging | 40 |
| 8th week | 12.05: Digital Forensics | 61 |
| 8th week | 12.06: File and Packet Manipulation | 58 |
| 8th week | 12.07: Redundancy | 60 |
| 8th week | 12.08: Backup and Restore | 90 |
| 8th week | 13.01: Organizational Security Policies | 50 |
| 8th week | 13.02: Risk Management | 38 |
| 8th week | 13.03: Email | 58 |
| 8th week | 14.01: Audits | 56 |
| 8th week | 14.02: Controls and Frameworks | 32 |
| 8th week | 14.03: Sensitive Data and Privacy | 66 |
|  | Grand Total | 4325 |