# 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 2021

# **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 6 | 2017 | TestOut | 9781-93508-0442 | 10/3/17 |

The keycode for TestOut is available through the WBU Bookstore at <https://bookstore.wbu.edu>

# 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 participate in weekly discussion boards:
	+ Post your reply to the instructor’s posted question.
	+ Post any comments, questions, or anything that supportive of classmates. TestOut
* Students will complete all assignments in TestOut and take the certification test as their final exam for this class. A grade for each week will represent the progress and effort made by the student.

Grade calculation for this course

* All work in TestOut will make up 75% of the total term grade.
* Grades from the two discussion forums will make up 25% 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 1

| **Chapter** | **Section** | **Time** |
| --- | --- | --- |
| 01. Introduction | 1.01: Security Overview | 24 |
| 01. Introduction | 1.02: Using the Simulator | 16 |
| 02. Security Basics | 2.01: Understanding Attacks | 41 |
| 02. Security Basics | 2.02: Defense Planning | 19 |
| 02. Security Basics | 2.03: Access Control | 28 |
| 02. Security Basics | 2.04: Cryptography Basics | 17 |
| 02. Security Basics | 2.05: Network Monitoring | 23 |
| 02. Security Basics | 2.06: Incident Response | 67 |
| 03. Policies, Procedures, and Awareness | 3.01: Security Policies | 59 |
| 03. Policies, Procedures, and Awareness | 3.02: Risk Management | 26 |
| 03. Policies, Procedures, and Awareness | 3.03: Business Continuity | 14 |
| 03. Policies, Procedures, and Awareness | 3.04: Manageable Network Plan | 26 |
| 03. Policies, Procedures, and Awareness | 3.05: Social Engineering | 51 |
| 03. Policies, Procedures, and Awareness | 3.06: App Development and Deployment | 27 |

Week 2

| **Chapter** | **Section** | **Time** |
| --- | --- | --- |
| 03. Policies, Procedures, and Awareness | 3.07: Employee Management | 39 |
| 03. Policies, Procedures, and Awareness | 3.08: Mobile Devices | 22 |
| 03. Policies, Procedures, and Awareness | 3.09: Third-Party Integration | 18 |
| 04. Physical | 4.01: Physical Threats | 40 |
| 04. Physical | 4.02: Device Protection | 19 |
| 04. Physical | 4.03: Network Infrastructure Protection | 15 |
| 04. Physical | 4.04: Environmental Controls | 30 |
| 05. Perimeter | 5.01: Recon and Denial | 50 |
| 05. Perimeter | 5.02: Spoofing and Poisoning | 68 |
| 05. Perimeter | 5.03: Security Appliances | 39 |
| 05. Perimeter | 5.04: Demilitarized Zones (DMZ) | 27 |
| 05. Perimeter | 5.05: Firewalls | 40 |
| 05. Perimeter | 5.06: Network Address Translation (NAT) | 33 |

Week 3

| **Chapter** | **Section** | **Time** |
| --- | --- | --- |
| 05. Perimeter | 5.07: Virtual Private Networks (VPN) | 51 |
| 05. Perimeter | 5.08: Web Threat Protection | 27 |
| 05. Perimeter | 5.09: Network Access Protection | 31 |
| 05. Perimeter | 5.10: Wireless Overview | 54 |
| 05. Perimeter | 5.11: Wireless Attacks | 44 |
| 05. Perimeter | 5.12: Wireless Defenses | 60 |
| 06. Network | 6.01: Network Threats | 19 |
| 06. Network | 6.02: Network Device Vulnerabilities | 28 |
| 06. Network | 6.03: Network Applications | 23 |
| 06. Network | 6.04: Switch Attacks | 16 |
| 06. Network | 6.05: Switch Security | 60 |

Week 4

| **Chapter** | **Section** | **Time** |
| --- | --- | --- |
| 06. Network | 6.06: Using VLANs | 32 |
| 06. Network | 6.07: Router Security | 43 |
| 06. Network | 6.08: Intrusion Detection and Prevention | 53 |
| 06. Network | 6.09: Vulnerability Assessment | 64 |
| 06. Network | 6.10: Protocol Analyzers | 29 |
| 06. Network | 6.11: Remote Access | 50 |
| 06. Network | 6.12: Network Authentication | 62 |
| 06. Network | 6.13: Penetration Testing | 32 |
| 06. Network | 6.14: Virtual Networking | 34 |
| 06. Network | 6.15: Software-Defined Networking (SDN) | 17 |
| 06. Network | 6.16: Cloud Services | 26 |

Week 5

| **Chapter** | **Section** | **Time** |
| --- | --- | --- |
| 07. Host | 7.01: Malware | 55 |
| 07. Host | 7.02: Password Attacks | 34 |
| 07. Host | 7.03: Windows System Hardening | 60 |
| 07. Host | 7.04: Hardening Enforcement | 37 |
| 07. Host | 7.05: File Server Security | 52 |
| 07. Host | 7.06: Linux Host Security | 36 |
| 07. Host | 7.07: Embedded Systems | 21 |
| 07. Host | 7.08: Log Management | 57 |
| 07. Host | 7.09: Audits | 36 |
| 07. Host | 7.10: Email | 46 |

Week 6

| **Chapter** | **Section** | **Time** |
| --- | --- | --- |
| 07. Host | 7.11: BYOD Security | 33 |
| 07. Host | 7.12: Mobile Device Management | 55 |
| 07. Host | 7.13: Host Virtualization | 50 |
| 08. Application | 8.01: Access Control Models | 55 |
| 08. Application | 8.02: Authentication | 44 |
| 08. Application | 8.03: Authorization | 30 |
| 08. Application | 8.04: Web Application Attacks | 52 |
| 08. Application | 8.05: Internet Browsers | 62 |
| 08. Application | 8.06: Application Development | 68 |

Week 7

| **Chapter** | **Section** | **Time** |
| --- | --- | --- |
| 08. Application | 8.07: Active Directory Overview | 31 |
| 08. Application | 8.08: Windows Domain Users and Groups | 49 |
| 08. Application | 8.09: Linux Users | 62 |
| 08. Application | 8.10: Linux Groups | 33 |
| 08. Application | 8.11: Linux User Security | 26 |
| 08. Application | 8.12: Group Policy Overview | 47 |
| 08. Application | 8.13: Hardening Authentication 1 | 71 |
| 08. Application | 8.14: Hardening Authentication 2 | 38 |
| 09. Data | 9.01: Data Management | 38 |
| 09. Data | 9.02: Advanced Cryptography | 28 |
| 09. Data | 9.03: Cryptography Implementations | 24 |

Week 8

| **Chapter** | **Section** | **Time** |
| --- | --- | --- |
| 09. Data | 9.04: Cryptographic Attacks | 30 |
| 09. Data | 9.05: Symmetric Encryption | 30 |
| 09. Data | 9.06: Asymmetric Encryption | 23 |
| 09. Data | 9.07: File Encryption | 59 |
| 09. Data | 9.08: Public Key Infrastructure (PKI) | 64 |
| 09. Data | 9.09: Hashing | 27 |
| 09. Data | 9.10: Data Transmission Security | 67 |
| 09. Data | 9.11: Data Loss Prevention (DLP) | 14 |
| 09. Data | 9.12: Redundancy | 63 |
| 09. Data | 9.13: Backup and Restore | 61 |
| 09. Data | 9.14: Cloud Storage | 13 |