**Wayland 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.

**Contact Information**

**Course**

: MISM 4306 VC01 – Information Systems Security

**Campus**

: WBUonline

**Term/Session**

**:** Spring 2 2022

**Instructor**

**:** Jimmy Fikes

**Office Phone Number/Cell #**

**:** 806-831-3918

**WBU Email Address**

**:** Jimmy.Fikes@wayland.wbu.edu

**Office Hours, Building, and Location**

**:** Students may request remote conferences with the instructor

**Class Meeting Time and Location**

**:** This class will be conducted entirely online on Blackboard.

**Textbook Information**

**Required Textbook(s) and/or Required Materials**

**:**

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

*The textbook for this course is part of the* ***Wayland’s Automatic eBook*** *program. You will have access to an eBook and interactive learning material on the first day of class through your Blackboard course site. The cost of this Automatic eBook will be billed directly to your student account when you register for the course. You will be notified via email with access instructions and additional information. If you do not wish to participate in the Automatic eBook program, you will have the first 12 days of class to opt-out of the program (additional details will be outlined in your email instructions). For more information on the Automatic eBook program, visit the Wayland Bookstore* [*Automatic eBook FAQ*](https://bookstore.wbu.edu/site_inclusive.asp) *page.*

**Course Information**

**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.

**Prerequisite:**

None

**Course Outcome 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

**Attendance Requirements**

WBUonline

Students are expected to participate in all required instructional activities in their courses. Online courses are no different in this regard; however, participation must be defined in a different manner. Student “attendance” in an online course is defined as active participation in the course as described in the course syllabus. Instructors in online courses are responsible for providing students with clear instructions for how they are required to participate in the course. Additionally, instructors are responsible for incorporating specific instructional activities within their course and will, at a minimum, have weekly mechanisms for documenting student participation. These mechanisms may include, but are not limited to, participating in a weekly discussion board, submitting/completing assignments in Blackboard, or communicating with the instructor. Students aware of necessary absences must inform the professor with as much advance notice as possible in order to make appropriate arrangements. Any student absent 25 percent or more of the online course, i.e., non-participatory during 2 or more weeks of an 8-week session, may receive an F for that course. Instructors may also file a Report of Unsatisfactory Progress for students with excessive non-participation. Any student who has not actively participated in an online class prior to the census date for any given session is considered a “no-show” and will be administratively withdrawn from the class without record. To be counted as actively participating, it is not sufficient to log in and view the course. The student must be submitting work as described in the course syllabus. Additional attendance and participation policies for each course, as defined by the instructor in the course syllabus, are considered a part of the university’s attendance policy.

**University Policies**

**Statement on Plagiarism and 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.

**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 Director of Counseling, Career and Disability Services serves as the coordinator of students with disability and should be contacted concerning accommodation request at (806) 291-3765. Documentation of a disability must accompany any request for accommodations.

Accessibility issues with content in WBUonline courses or in Blackboard should be addressed to the WBU accessibility coordinator, Dr. Trish Ritschel-Trifilo, [trifilot@wbu.edu](mailto:trifilot@wbu.edu) or call (806) 291-3745.

**Student Grade Appeals**

**:** 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 to the 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.

**Course Requirements and Grading Criteria**

TestOut Assignments

* Students will complete all assignments in TestOut up through section 14.3 (as shown in the Tentative Schedule below)
* Each assignment shown in the Tentative Schedule is made up of a variety of instructional materials such as video lessons, fact sheets, lab sims and a section quiz. Students are expected to complete all instructional materials for each lesson.
* All instructional materials that have not been completed by the last day of term will be assigned a grade of zero and these zeros will be averaged in with all work that has been completed during the term.
* Students may take the TestOut Security Pro Certification test, but it is not required to pass the class.
* TestOut provides a practice test and other materials to help students prepare to take the certification test. These additional preparation materials are not required and grades earned in these materials are not included in the final term grade.
* The final term grade will be calculated as follows:
  + All grades for TestOut instructional materials up through section 14.3 will be averaged and will make up 90% of the total term grade.
  + Up to 10% of the term grade is reserved for students who take the TestOut Security Pro Certification test. Students who pass the certification test will receive the full 10%. Students who attempt the test, but do not pass it, will receive a portion of the 10% equal to the score they earn on the test.

**The University has a standard grade scale:**

A = 90-100, B = 80-89, C = 70-79, D = 60-69, F= below 60, W = Withdrawal, WP = withdrew passing, WF = withdrew failing, I = incomplete. An incomplete may be given within the last two weeks of a long term, within the last week of an 8-week session, or within the last two days of a microterm to a student who is passing, but has not completed a term paper, examination, or other required work for reasons beyond the student’s control. A grade of “incomplete” is changed if the work required is completed prior to the last day of the next long 16-week term or 8-week session, unless the instructor designates an earlier date for completion.  If the work is not completed by the appropriate date, the I is converted to an F.

**Tentative Schedule**

|  |  |  |
| --- | --- | --- |
| **Week** | **Content Covered** | **Estimated Time to Complete in Minutes** |
| 1st week | 01.1: Security Overview | 24 |
| 1st week | 01.2: Defense Planning | 24 |
| 1st week | 01.3: Using the Simulator | 26 |
| 1st week | 02.1: Understanding Attacks | 45 |
| 1st week | 02.2: Malware | 52 |
| 1st week | 02.3: Social Engineering | 84 |
| 1st week | 02.4: Vulnerability Concerns | 32 |
| 1st week | 03.1: Physical Threats | 34 |
| 1st week | 03.2: Device and Network Protection | 30 |
| 1st week | 03.3: Environmental Controls | 31 |
| 1st week | 04.1: Manageable Network Plan | 33 |
| 1st week | 04.2: Windows System Hardening | 77 |
| 2nd week | 04.3: File Server Security | 62 |
| 2nd week | 04.4: Linux Host Security | 43 |
| 2nd week | 05.1: Security Appliances | 101 |
| 2nd week | 05.2: Demilitarized Zones | 38 |
| 2nd week | 05.3: Firewalls | 49 |
| 2nd week | 05.4: Network Address Translation | 47 |
| 2nd week | 05.5: Virtual Private Networks | 63 |
| 2nd week | 05.6: Web Threat Protection | 41 |
| 2nd week | 05.7: Network Access Control | 22 |
| 2nd week | 05.8: Network Threats | 24 |
| 2nd week | 05.9: 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 | 06.1: Access Control Models | 50 |
| 3rd week | 06.2: Authentication | 44 |
| 3rd week | 06.3: Authorization | 30 |
| 3rd week | 06.4: Windows User Management | 57 |
| 3rd week | 06.5: Active Directory Overview | 146 |
| 4th week | 06.6: Hardening Authentication | 112 |
| 4th week | 06.7: Linux Users | 126 |
| 4th week | 06.8: Linux Groups | 58 |
| 4th week | 06.9: Remote Access | 33 |
| 4th week | 06.10: Network Authentication | 58 |
| 4th week | 07.1: Cryptography | 91 |
| 4th week | 07.2: Cryptography Implementations | 33 |
| 4th week | 07.3: Hashing | 42 |
| 5th week | 07.4: File Encryption | 70 |
| 5th week | 07.5: Public Key Infrastructure | 76 |
| 5th week | 08.1: Wireless Overview | 43 |
| 5th week | 08.2: Wireless Attacks | 52 |
| 5th week | 08.3: Wireless Defenses | 85 |
| 5th week | 09.1: Host Virtualization | 60 |
| 5th week | 09.2: Virtual Networking | 46 |
| 5th week | 09.3: Software-Defined Networking | 22 |
| 5th week | 09.4: Cloud Services | 46 |
| 5th week | 09.5: Cloud Security | 38 |
| 6th week | 09.6: Mobile Devices | 42 |
| 6th week | 09.7: Mobile Device Management | 39 |
| 6th week | 09.8: BYOD Security | 65 |
| 6th week | 09.9: Embedded and Specialized Systems | 42 |
| 6th week | 10.1: Data Transmission Security | 71 |
| 6th week | 10.2: Data Loss Prevention | 22 |
| 6th week | 10.3: Web Application Attacks | 110 |
| 6th week | 10.4: Application Development and Security | 94 |
| 6th week | 11.1: Penetration Testing | 36 |
| 7th week | 11.2: Monitoring and Reconnaissance | 56 |
| 7th week | 11.3: Intrusion Detection | 44 |
| 7th week | 11.4: Security Assessment Techniques | 99 |
| 7th week | 11.5: Protocol Analyzers | 26 |
| 7th week | 11.6: Analyzing Network Attacks | 101 |
| 7th week | 11.7: Password Attacks | 62 |
| 7th week | 12.1: Incident Response | 29 |
| 7th week | 12.2: Mitigation of an Incident | 28 |
| 7th week | 12.3: Log Management | 62 |
| 7th week | 12.4: Windows Logging | 40 |
| 8th week | 12.5: Digital Forensics | 61 |
| 8th week | 12.6: File and Packet Manipulation | 58 |
| 8th week | 12.7: Redundancy | 60 |
| 8th week | 12.8: Backup and Restore | 90 |
| 8th week | 13.1: Organizational Security Policies | 50 |
| 8th week | 13.2: Risk Management | 38 |
| 8th week | 13.3: Email | 58 |
| 8th week | 14.1: Audits | 56 |
| 8th week | 14.2: Controls and Frameworks | 32 |
| 8th week | 14.3: Sensitive Data and Privacy | 66 |
|  | Grand Total | 4325 |