**ITSY 1342**

**Information Technology Security**

**Summer 2017**

|  |  |
| --- | --- |
| Instructor: | Michael Slaughter |
| Email: | mslaughter@southplainscollege.edu |
| Office Number: | (806) 716-2242 |
| Course Name: | ITSY 1342.151 |

# Course Description

This course provides instruction in security for network hardware, software, and data, including physical security; backup procedures; relevant tools; encryption; and protection from viruses.

# Internet

This is an internet format class. All communication and homework will be completed online using Blackboard and TestOut.

# Textbook and Hardware Requirements

We will be using TestOut LabSim for this course, as well as Security + SY0-401 by David Prowse. You will need to purchase an activation code from the SPC bookstore or online at the link mentioned below. Once activated, you will need to enroll in the course mentioned below. Also below is a link to a video with instructions on how to enroll in the LabSim course. This software will provide you with a virtual environment that we will use for labs, homework assignments and exams. It will also provide you with a wealth of information, reading materials, and videos to aid in your learning experience. **LabSim:**

|  |  |
| --- | --- |
| Promo Code: | 14-232TA |
| Course Product: | TestOut Security Pro 5.0 ISBN: 978-1-935080-44-2 |
| School Name: | South Plains College |
| Instructor Name: | Michael Slaughter |
| Course Name: | SU2017-ITSY1342.151 |
| Purchase Link: | <http://www.testout.com/home/student-resources/student-purchasing> |
| Instructions Link: | <http://www.testout.com/home/student-resources/how-to-tutorials> |

(View the [“Getting Started - Student Accounts Not Activated by Teachers”](http://www.testout.com/docs/tutorial/labsim5_getting-started-student-accounts-not-activated-by-teachers.pdf?sfvrsn=8) PDF) **Textbook**:

Title: CompTIA Security+ SY0-401 3rd Edition by David L. Prowse ISBN: 978-0-7897-5333-5

# Assumed Knowledge

It is assumed that you possess basic computer skills relating to using the internet, applications and other basic computing tasks. It is also assumed that you have taken or possess the needed knowledge equal to ITNW1325 Fundamentals of Networking and ITSC1325 PC Hardware. If you have not taken those courses, or question your knowledge, please contact me ASAP about how to proceed. It is also assumed that if you run into content you do not understand; you will research that content on your own as well as ask the instructor for assistance.

# Software Requirements

Because some of the assignments will be done and submitted outside of class, you will need access to the following programs outside of the classroom:

* Internet Connection and Web Browser (Chrome or IE)
* TestOut Account

# Communication

Communication for this class will be conducted through SPC email. All students will be required to check their SPC student email accounts regularly for course updates and announcements. Please include your name, course name, and section number in all email communication. Other important announcements may be given during in class meetings, so attendance is key for complete communication.

# Attendance Policy

Attendance is measured by how often you access Blackboard and TestOut. You are required to check in weekly and complete all homework assignments within the due dates indicated. If participation drops or you do not check in for two full weeks, you will be dropped from the class.

# Reading/Study Assignments

Mandatory, assigned reading is a requirement for this course. Reading assignments includes all material in the LabSim course content that is assigned for a given week, chapters assigned in the Security+ SY0-401 textbook, and articles posted for online discussions. Study assignments include all lectures in LabSim, demonstrations in LabSim, notes taken from your in-class lectures, and other content presented throughout the course. Although reading/study assignments are not taken for a grade, they are required to be successful in this course.

# Assignments and Lab Projects

Procrastination will not serve you well in this course. Most assignments will be available through the LabSim software. Each chapter will have several small assignments and labs that will count toward your homework grade. For the TestOut LabSim section assigned, all labs and exams are pulled for homework grades.

There will also small homework assignments and projects that will be assigned periodically throughout the semester. These assignments and/or projects will be announced in class and available in Blackboard. **NO LATE WORK IS ACCEPTED!** In-class labs will also be completed throughout this course. It is expected that you take care of all equipment and check that equipment in/out with the instructor.

# Exams

There will be two exams given in this class, a midterm and a final exam. **Make-up exams will not be given.** If the midterm exam is missed, then the final exam grade will count as both the final and midterm grade. Also, if a student does better on the final than the midterm, I will substitute the final grade as the midterm grade.

# Grades

Grades will be calculated as follows:

|  |  |
| --- | --- |
|  | Possible Points |
| Assignments (TestOut Assignments) | 30% |
| Midterm | 30% |
| Final Exam | 40% |

All assignments are mandatory. **I reserve the right to drop or fail you if homework assignments are frequently missed or incomplete.**

Grades will be available through LabSim (Homework/Exam Grades) and Blackboard. Blackboard grades will show a running average of how you are performing throughout the semester. Blackboard grades will be updated regularly throughout the semester.

**Instructional and Outside Course Time Estimation:**

TestOut LabSim Time: 13.6hrs/wk x 5wks = 68 hrs

Midterm Exam Prep: 4 hrs/wk x 2 wks = 8hrs

Final Exam Prep: 4hrs/wk x 3wks = 12 hrs

Security Pro Cert Exam: 2hrs x 1 = 2 hrs

Exam Time: 2hrs/exam x 2 = 4 hrs

**Total Course Time = 110 hrs**

**Total Time/Week = 22 hrs**

# In-Class Computer, Cell Phone and iPod Use

Students will **not** be allowed to surf the web, check their personal e-mail or social media accounts, or do work for any other course while class is in session.

**Students will not be allowed to use their cell phones during class**. If the student is found using social media, surfing the web, or using their cell phone, they will be asked to leave the class and they will be counted absent for that day. If the incident reoccurs, they will be reported to the dean of students. In cases of emergency, the student is asked to leave the classroom to use their cell phone. **If a student has a cell phone or other device out during an exam, they will be asked to leave and will get a zero for that exam.**

# Food and Drinks

No food or drinks are allowed in the Technology Center. Do not bring those to class. If you do, you will be asked to leave class and counted as absent. If this happens more than once you may be dropped from the class.

# Drop Policy

You may be dropped from this course for the following reasons:

* Attendance o You do not check in to Blackboard for two weeks
* Participation, completion of homework, exams, and team project o You have missed 2-3 classes and several homework assignments o You have missed several homework assignments
  + You have missed two or more exams without rescheduling with the instructor
* Academic Integrity o Cheating, plagiarism, or sharing your work with others
  + Offensive, degrading, or off topic discussion posts

# Academic Integrity

It is the aim of the faculty at South Plains College to foster a spirit of complete honesty and a high standard of integrity. The attempt of any student to present as his or her own any work which he or she has not honestly performed is regarded by the faculty and administration as a most serious offense and renders the offender liable to serious consequences and possible suspension. Please refer to the SPC General Catalog regarding consequences for cheating and plagiarism. **I reserve the right to administratively drop with an “F” any student whom I suspect of academic dishonesty.**

**\*\*Do not, under any circumstances, turn in another student’s file as your own. Do not, under any circumstances, give your file to anyone else to turn in as their own. Both situations are representative of academic dishonesty and will be treated as such.\*\* Disclaimer**

Because we will use Blackboard to conduct a portion of this class, please note that the materials you may be accessing in chat rooms, bulletin boards or unofficial web pages are not officially sponsored by South Plains College. The United States Constitution rights of free speech apply to all members of our community regardless of the medium used. We disclaim all liability for data, information or opinions expressed in these forums.

# Diversity Statement

In this course, the teacher will establish and support an environment that values and nurtures individual and group differences and encourages engagement and interaction. Understanding and respecting multiple experiences and perspectives will serve to challenge and stimulate all of us to learn about others, about the larger world, and about ourselves. By promoting diversity and intellectual exchange, we will not only mirror society as it is, but also model society as it should be and can be.

# Special Services

*4.1.1.2 Disabilities Statement*

Students with disabilities, including but not limited to physical, psychiatric, or learning disabilities, who wish to request accommodations in this class should notify the Disability Services Office early in the semester so that the appropriate arrangements may be made. In accordance with federal law, a student requesting accommodations must provide acceptable documentation of his/her disability to the Disability Services Office. For more information, call or visit the Disability Services Office through the Guidance and Counseling Centers at Reese Center (Building 8) 716-4606, or Levelland (Student Services Building) 716-2577.

# Counseling

If at any point in the semester you find yourself having trouble with stress or feel depressed please stop in and see a counselor. Counseling services are available at all campuses. The number for the counseling office is 806-716-2366. Below is a link to SPC’s personal counseling services.

[http://www.southplainscollege.edu/information-for/current-spc-students/counselingcurrent/personal-counseling.php](http://www.southplainscollege.edu/information-for/current-spc-students/counseling-current/personal-counseling.php)

# Course Schedule

|  |  |  |
| --- | --- | --- |
| **Week** | **Date** | **Chapter** |
| 1 | June 5 – 11 | TestOut 1.0 - 3.6 Security + Ch. 1, 10, 13, 14 |
| 2 | June 12 – 18 | TestOut 4.0 – 5.6  Security + Ch. 9, 16  MIDTERM EXAM (Covers 1.0-5.6) |
| 3 | June 19 – 25 | TestOut 6.0 – 7.7 Security+ Ch. 5 - 8 |
| 4 | June 26 – July 2 | TestOut 8.0 – 10.5 Security+ Ch. 2-4, 15 |
| 5 | July 3 – 11 | TestOut 11.0-11.5  TestOut Security Pro Practice Exam Domain 5- Security Pro Practice Exam  (SECURITY PRO CERT EXAM OPEN IF STANDARDS ARE MET) FINAL EXAM (Comprehensive) |

# Approximate Time for the Course

The total time for the LabSim Security Pro course is approximately 91 hours and 35 minutes. The time is calculated by adding the approximate time for each section which is calculated using the following elements:

* Video/demo times
* Approximate time to read the text lesson (the length of each text lesson is taken into consideration)
* Simulations (5 minutes assigned per simulation)
* Questions (1 minute per question)

*The total amount of LabSim content we will be covering comes to about 69 hours, which breaks down to about 4.5 hours of homework per week, plus time to read the content from the Pearson Security+ Cert Guide and do the Blackboard Discussions. The reason for the intensity in this course, is because this is what the industry expects you to know coming out of school. Dedicate the time to LEARNING the content and you will appreciate it when you graduate. –M. Slaughter* The breakdown for this course is as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Module Sections** | **Time** | **Total** | **HR:MM** |
|  |  |  |  |
| **1.0 Introduction** |  |  |  |
| 1.1 Security Overview | 70 |  |  |

1.2 Using the Simulator 25 95 1:35

|  |  |  |
| --- | --- | --- |
|  |  | |
| **2.0 Access Control and Identity Management** |  | |
| 2.1 Access Control Models | 30 | |
| 2.2 Authentication | | 60 |
| 2.3 Authorization | | 30 |
| 2.4 Access Control Best Practices | | 30 |
| 2.5 Active Directory Overview | | 30 |

2.6 Windows Domain Users and Groups 50

|  |  |  |
| --- | --- | --- |
| 2.7 Linux Users | 70 |  |
| 2.8 Linux Groups | 20 |  |
| 2.9 Linux User Security | 25 |  |
| 2.10 Group Policy Overview | 35 |  |
| 2.11 Hardening Authentication 1 | 90 |  |
| 2.12 Hardening Authentication 2 | 30 |  |
| 2.13 Remote Access | 35 |  |
| 2.14 Network Authentication | 70 |  |
| 2.15 Identity Management | 20 625 | 10:25 |
|  |  |  |
| **3.0 Cryptography** |  |  |
| 3.1 Cryptography | 45 |  |
| 3.2 Hashing | 35 |  |
| 3.3 Symmetric Encryption | 35 |  |
| 3.4 Asymmetric Encryption | 25 |  |
| 3.5 Public Key Infrastructure (PKI) | 70 |  |

3.6 Cryptography Implementations 40 250 4:10

|  |  |
| --- | --- |
|  |  |
| **4.0 Policies, Procedures, and Awareness** |  |
| 4.1 Security Policies | 80 |
| 4.2 Manageable Network Plan | 35 |
| 4.3 Business Continuity | 20 |
| 4.4 Risk Management | 30 |
| 4.5 Incident Response | 65 |

4.6 Social Engineering 55

|  |  |
| --- | --- |
| 4.7 Certification and Accreditation | 40 |
| 4.8 Development | 35 |
| 4.9 Employee Management | 40 |

4.10 Third-Party Integration 20 420 7:00

|  |  |
| --- | --- |
|  |  |
| **5.0 Physical Security** |  |
| 5.1 Physical Security | 50 |
| 5.2 Hardware Security | 20 |
| 5.3 Environmental Controls | 45 |
| 5.4 Mobile Devices | 40 |
| 5.5 Mobile Device Security Enforcement | 40 |

5.6 Telephony 25 220 3:40

|  |  |
| --- | --- |
|  |  |
| **6.0 Networking** |  |
| 6.1 Networking Layer Protocol Review | 65 |
| 6.2 Transport Layer Protocol Review | 35 |
| 6.3 Perimeter Attacks 1 | 50 |
| 6.4 Perimeter Attacks 2 | 50 |
| 6.5 Security Appliances | 35 |
| 6.6 Demilitarized Zones (DMZ) | 30 |
| 6.7 Firewalls | 40 |
| 6.8 Network Address Translation (NAT) | 30 |
| 6.9 Virtual Private Networks (VPN) | 40 |
| 6.10 Web Threat Protection | 25 |
| 6.11 Network Access Control (NAC) | 45 |
| 6.12 Wireless Overview | 60 |
| 6.13 Wireless Attacks | 50 |

6.14 Wireless Defenses 80 635 10:35

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| **7.0 Network Defenses** |  | | | |
| 7.1 Network Devices | 15 | | | |
| 7.2 Network Device Vulnerabilities | 20 | |  |  |
| 7.3 Switch Attacks | 10 | |  |  |
| 7.4 Router Security | 15 | |  |  |
| 7.5 Switch Security | 90 | |  |  |
| 7.6 Intrusion Detection and Prevention | 50 | |  |  |
| 7.7 SAN Security | 30 | | 230 | 3:50 |
|  |  | |  |  |
| **8.0 Host Defenses** |  | |  |  |
| 8.1 Malware | 75 | |  |  |
| 8.2 Password Attacks | 20 | |  |  |
| 8.3 Windows System Hardening | 105 | |  |  |
| 8.4 Hardening Enforcement | 35 | |  |  |
| 8.5 File Server Security | 50 | |  |  |
| 8.6 Linux Host Security | 20 | |  |  |
| 8.7 Static Environment Security | 10 | | 315 | 5:15 |
|  |  | |  |  |
| **9.0 Application Defenses** |  | |  |  |
| 9.1 Web Application Attacks | 75 | |  |  |
| 9.2 Internet Browsers | 105 | |  |  |
| 9.3 E-mail | 45 | |  |  |
| 9.4 Network Applications | | 25 | | |
| 9.5 Virtualization | | 55 | | |

9.6 Application Development 75 380 6:20

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| **10.0 Data Defenses** |  | | | |
| 10.1 Redundancy | 65 | | | |
| 10.2 Backup and Restore | | 55 |  |  |
| 10.3 File Encryption | | 75 |  |  |
| 10.4 Secure Protocols | | 75 |  |  |
| 10.5 Cloud Computing | | 30 | 300 | 5:00 |
|  | |  |  |  |
| **11.0 Assessments and Audits** | |  |  |  |
| 11.1 Vulnerability Assessment | | 85 |  |  |
| 11.2 Penetration Testing | | 30 |  |  |
| 11.3 Protocol Analyzers | | 20 |  |  |
| 11.4 Log Management | | 50 |  |  |
| 11.5 Audits | | 40 | 225 | 3:45 |

|  |  |  |
| --- | --- | --- |
| **Security Pro Practice Exams** |  | |
| Domain 1: Access Control and Identity  Management (22 sims) | 110 | |
| Domain 2: Policies, Procedures, Awareness (1 sim) | | 5 |
| Domain 3: Physical Security (2 sims) | | 10 |
| Domain 4: Perimeter Defenses (10 sims) | | 50 |
| Domain 5: Network Defenses (7 sims) | | 35 |

Domain 6: Host Defenses (7 sims) 35

|  |  |
| --- | --- |
| Domain 7: Application Defenses (10 sims) | 50 |
| Domain 8: Data Defenses (6 sims) | 30 |
| Domain 9: Audits and Assessments (5 sims) | 25 |

Security Pro Certification Practice Exam (15 sims) 90 440 7:20

|  |  |
| --- | --- |
|  |  |
| **Security+ Practice Exams** |  |
| Domain 1: Network Security (172 questions) | 172 |

Domain 2: Compliance and Operational Security

|  |  |  |
| --- | --- | --- |
| (128 questions) | 128 |  |
| Domain 3: Threats and Vulnerabilities (178 questions) | 178 |  |
| Domain 4: Application, Data and Host Security (70 questions) | 70 |  |
| Domain 5: Access Control and Identity  Management (98 questions) | 98 |  |
| Domain 6: Cryptography (92 questions) | 88 |  |
| Security+ Certification Practice Exam (100 questions) | 100 834 | 13:54 |
|  |  |  |
| **SSCP Practice Exams** |  |  |
| Domain 1: Access Control (60 questions) | 60 |  |
| Domain 2: Security Operations & Administration (64 questions) | 64 |  |
| Domain 3: Monitoring and Analysis (21 questions) | 21 |  |
| Domain 4: Risk, Response, and Recovery (38 questions) | 38 |  |
| Domain 5: Cryptography (90 questions) | 90 |  |

Domain 6: Networks and Communications (68

questions) 68

|  |  |
| --- | --- |
| Domain 7: Malicious Code and Attacks (85 questions) | 85 |

SSCP Certification Practice Exam (125 questions) 125 551 9:11

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Total**    **Time** | **5495** | **91:35** |