SOUTHWEST TECH

SOUTHWEST TECHNICAL COLLEGE

TEIT 2200 - Security + (4 Credits)

Course Description

Security+ provides instruction on assessing the security posture of enterprise environments and implementing appropriate security solutions. Instruction is given to identify, analyze, and respond to events and incidents. This course aligns with the objectives of the CompTIA Security+ certification exam.

Course Objectives

- Explain security functions and purposes as they relate to network devices.
- Identify and implement risk mitigation techniques and strategies.
- Distinguish and evaluate different network and physical security threats.
- Implement network intrusion detection and prevention technologies.
- Identify and execute appropriate cryptography measures.

Course Outline

- Threats, Attacks, and Vulnerabilities
- Network and Device Security
- Securing Devices and Infrastructure
- Identity, Access, and Account Management
- Cryptography and Wireless Threats
- Virtualization, Cloud and Mobile Device Threats
- Securing Data and Assessments
- Risk Management and Compliance

Textbook & Reading Materials

TestOut Security Pro, Test Out, ISBN: 9781935080442

Assignments and Assessments

Course Introduction and Standards
Meet Your Instruction Team
Rules of the Lab
CS Code of Conduct Policy
Submitting Assignments in Canvas
Taking a Screenshot
Orientation
Syllabus Agreement
Kali Linux VM
1.1 - Security Introduction
1.1.5 - Practice Questions
1.2.4 - Practice Questions
2.1.8 - Practice Questions
2.2. 7 - Identify Social Engineering
2.2.8 - Social Engineering Techniques
2.2. 9 - Practice Questions
2.3.6 - Configure Microsoft Defender
2.3.7 - Analyze Indicators of Malware-Based Attacks
2.3.8 - Practice Questions
OPTIONAL - Social Engineering Example.mp4
Checkpoint Meeting Module 1
Student Acknowledgement Statement Module 1
3.1 - Cryptography
3.1.7 - Identify Cryptographic Modes of Operation
3.1.11 - Hide Files with OpenStego
3.1.14 - Practice Questions
3.2.5 - Practice Questions
3.3.5 - Compare an MOS Hash
3.3.6 - Practice Questions
3.4.3 - Encrypt Files with EFS
3.4.8 - Configure Bitlocker with a TPM
3.4.10 - Practice Questions
3.5.6 - Manage Certificates
3.5.9 - Certificates and Certificate Authorities
3.5.10 - Practice Questions
4.1.6 - Practice Questions
4.2.9 - Practice Questions
Checkpoint Meeting Module 2
Student Acknowledgement Statement Module 2
4.3 - Authorization
4.3.5 - Implement an Access Control Model
4.3.6 - Practice Questions
4.4.5 - Create OUs
4.4.6 - Delete OUs
4.4.10 - Create and Link a GPO
4.4.11- Create User Accounts
4.4.12 - Manage User Accounts
4.4.13 - Create a Group
4.4.14 - Create Global Groups
4.4.15 - Practice Questions
4.5.5 - Configure Account Password Policies
4.5.7 - Restrict Local Accounts
4.5.8 - Secure Default Accounts
4.5.9 - Enforce User Account Control
4.5.12 - Configure Smart Card Authentication
4.5.14 - Practice Questions
4.6.4 - Create a User Account
4.6.6 - Delete a User
4.6.7 - Change Your Password
4.6.8 - Change a User's Password
4.6.9 - Lock and Unlock User Accounts
4.6.14 - Practice Questions
4.7.3 - Rename and Create Groups
4.7.4 -Add Users to a Group
4.7.5 - Remove a User from a Group
4.7.6 - Practice Questions
4.8.5 - Practice Questions
4.9.5 - Practice Questions
Checkpoint Meeting Module 3
Student Acknowledgement Statement Module 3
5.1 - Enterprise Network Architecture
5.1.3 - Practice Questions
5.2. 7 - Configure a Security Appliance
5.2.8 - Configure Network Security Appliance Access
5.2.13 - Practice Questions
5.3.3 - Configure a Screened Subnet
5.3.5 - Practice Questions
5.4.5 - Configure a Perimeter Firewall
5.4.6 • Practice Questions
5.5.4 - Configure a Remote Access V PN
5.5.5 - Configure a VPN Connection iPad
5.5.9 - Implement Secure Remote Access Protocols
5.5.10 - Practice Questions
5.6.3 - Practice Questions
5.7.6 - Secure a Switch
5.7.7 - Practice Questions
5.8.4 - Practice Questions
5.9.7 - Harden a Switch
5.9.8 - Secure Access to a Switch
5.9.9 - Secure Access to a Switch 2
5.9.10 - Practice Questions
5.10.5 • Restrict Telnet and SSH Acoess
5.10.6 - Permit Traffic
5.10.7 - Block Source Hosts
5.10.8 - Practice Questions
6.1.3 - Implement Physical Security
6.1.4 - Practice Questions
6.2. 7 - Practice Questions
6.3.4 - Implement Intrusion Prevention
6.3.5 - Practice Questions
6.4.4 - Practice Questions
Checkpoint Meeting Module 4
Student Acknowledgement Statement Module 4
6.5 - Analyzing Network Attacks
6.5.4 - Poison ARP and Analyze with Wireshark
6.5.6 - Poison DNS

6.5.8 - Analyze a SYN Flood Attack
6.5.12 - Practice Questions
6.6.4 - Crack Password with Rainbow Tables
6.6.7 - Crack a Password with John the Ripper
6.6.8 - Practice Questions
7.1.7- Identify Types of Vulnerabilities
7.1.8 - Practice Questions
7.2.6 - Scan for Cleartext Vulnerabilities
7.2.7 - Scan for FTP Vulnerabilities
7.2.8 - Scan for TLS Vulnerabilities
7.2.9 - Scan for Windows Vulnerabilities
7.2.10 - Scan for Linux Vulnerabilities
7.2.11- Scan for Domain Cont roller Vulnerabilities
Skills Check: Al Assisted Scanning
7 .2.12 - Practice Questions
7 .3.8 - Practice Questions
7.4.5 - Practice Questions
8.1.5 - Configure Automatic Updates
8.1.7 - Configure Microsoft Defender Firewall
8.1.8 - Practice Questions
8.2.5 - Configure NTFS Permissions
8.2.6 - Disable Inheritance
8.3.6 - Practice Questions
Checkpoint Meeting Module 5
Student Acknowledgement Statement Module S
8.4 - Wireless Overview
8.4.5 - Configure a Wireless Network
8.4.6 - Practice Questions
8.5.4 - Configure Rogue Host Protection
8.5.5 - Practice Questions
8.6.6 - Harden a Wireless Network
8.6.7 - Configure WIPS
8.6. 9 - Practice Questions
8.7.4 -Allow SSL Connections
8.7.8 - Modify Enterprise Capabilities to Enhance Security
8. 7. 9 - Practice Questions
8.8.6 - Clear the Browser Cache
8.8.11- Perform an SQL Inj ection Attack
8.8.12 - Practice Questions
8.9.8 - Implement Application Allowed Lists with AppLocker
8.9.10 - Implement Data Execution Preventions
8. 9 .12 - Practice Questions
9.1.5 - Summarize Incident Response Procedures
9.1.6 - Practice Questions
9 .2.11 - Practice Questions
Checkpoint Meeting Module 6
Student Acknowledgement Statement Module 6
9.3 - Digital Forensics
9.3.10 - Practice Questions
9.4.6 - Practice Questions
9.5.6 - Back Up Files with File History
9.5.7 - Recover a File from File History
Skills Check: File Recovery
9.5.10 - Backup a Domain Cont roller
10.1.10 - Practice Questions
10.2.6 - Create Virtual Switches
10.2.7 - Practice Questions
10.3.4 - Practice Questions
10.4.6 - Analyze Infrastructure Types and Functions
10.4.7 - Practice Questions
10.5.7 - Implement Mobile Device Management
10.5.8 - Practice Questions
10.6.6 - Practice Questions
10.7.4 - Secure an iPad
10.7.6 - Create a Guest Network for BYOD
10.7.7 - Practice Questions
10.8.6 - Practice Questions
10.9.5 - Configure Email Filters
10.9.7 - Secure Email on iPad
10.9.8 - Practice Questions
Checkpoint Meeting Module 6
Student Acknowledgement Statement Module 6
11.1 - Policies, Standards, and Procedures
11.1.4 - Apply Appropriate Policies and Regulations
11.1.5 - Practice Questions
11.2.3 - Practice Questions
11.3.3 - Practice Questions
12.1.7 - Practice Questions
12.2.3 - Practice Questions
12.3.4 - Configure Advanced Audit Policy
12.3.6 - Enable Device Logs
12.3.7 - Practice Questions
13.1.9 - Privacy and Data Sensitivity Concepts
13.1.10 - Practice Questions
13.2.5 - Practice Questions
Student Feedback Survey
Course Completion Checkpoint Meeting
End of Course Student Acknowledgement Statement
TestOut EduApp Guide (DO NOT PUBLISH)
Purchasirng a TestOut Activation Code
LabSim to Canvas Grading Process
TestOut Access

Subject to change. Please consult your Canvas course for the most current instructions and updates.

Classroom Hours

Mo, Tu, W, Th, Fr
8:00 AM - 11:00 AM
12:00 PM - 3:00 PM

For a full list of course hours visit: Course Schedule

Instructor Contact Information

Greg Davis — gdavis@stech.edu
Austin Prince — aprince@stech.edu

Office Hours: By appointment

Email is the preferred method of communication; you will receive a response within 24 hours during regular business hours.

Canvas Information

Canvas is the where course content, grades, and communication will reside for this course.

- stech.instructure.com
- For Canvas passwords or any other computer-related technical support contact Student Services.
- For regular Hours and Weekdays call (435) 586 - 2899.
- For after Hours & Weekends call (435) 865 - 3929 (Leave a message if no response).

Course Policies

Course Grading: All assignments in this course require 100% score with unlimited submissions. All quizzes require a minimum score of 80%.

High School Power School Grades: Quarter student grades will be determined by student progress percentage. Faculty will use the higher percentage of either 1) quarter progress, or 2) cumulative progress for the current training plan year.

Grade Scale: The following grading scale will be used to determine a letter grade.

- A : 94 - 100%
- A- : 90 - 93%
- B+ : 87 - 89%
- B : 83 - 86%
- B- : 80 - 82%
- C+ : 77 - 79%
- C : 73 - 76%
- C- : 70 - 72%
- D+ : 67 - 69%
- D : 63 - 66%
- D- : 60 - 62%
- F : 0 - 59%

Course Policies: You are required to keep your progress and attendance at 67% minimum. You must complete this program within 150% estimated program length. You are permitted one 15 minute break every 90 minutes. If you take more than one break in a 90 minute period or your break lasts longer than 15 minutes, your attendance will be penalized. 10 consecutive absences will lead to being withdrawn from the program. Please notify your instructors about absences as soon as possible. If absence is due to illness, please email your instructors prior to end of day. Cell Phone/Electronics – Cell phones cannot be used during class time. You may bring your personal computers to class. You must be on topic in the lab while clocked-in. Industry Environment – computer science typically is very sedentary. This means you may sit at a desk for long hours. Be sure to move and get what exercise you can.

Additional Information

InformaCast Statement: Southwest Tech uses InformaCast to ensure the safety and well-being of our students. In times of emergency, such as weather closures and delays, this app allows us to promptly deliver notifications directly to your mobile devices. To stay informed and receive real-time updates, we encourage all students to sign up for notifications. Your safety is our priority, and staying connected ensures a swift response to any unforeseen circumstances. More information and directions for signing up are available at: https://stech.edu/emergency-notifications/

Internet Acceptable Use Policy: The student is expected to review and follow the Southwest Technical College Internet Safety Policy at: https://stech.edu/students/policies/

Student Code of Conduct Policy: The student is expected to review and follow the Southwest Technical College Student Code of Conduct Policy at: https://stech.edu/students/policies/

Accommodations: Students with medical, psychological, learning, or other disabilities desiring accommodations or services under ADA, must contact the Student Services Office. Student Services determines eligibility for and authorizes the provision of these accommodations and services. Students must voluntarily disclose that they have a disability, request an accommodation, and provide documentation of their disability. Students with disabilities may apply for accommodations, based on an eligible disability, through the Student Services office located at 757 W. 800 S., Cedar City, UT 84720, and by phone at (435) 586-2899. No diagnostic services are currently available through Southwest Technical College.

Safety and Building Maintenance: The College has developed and follows a variety of plans to ensure the safe and effective operation of its facilities and programs. The following plans are available online:
1) Facilities Operations and Maintenance Plan; 2) Technical Infrastructure Plan; and 3) Health and Safety Plan.

Withdrawals and Refunds: Please refer to the Southwest Technical College Refund Policy at:
https://stech.edu/students/policies/

Any high school or adult student, who declares a technical training objective is eligible for admission at Southwest Technical College (Southwest Tech). Program-specific admissions requirements may exist and will be listed on the Southwest Tech website. A high school diploma or equivalent is not required for admission but is mandatory for students seeking Title IV Federal Financial Aid.

Non-Discriminatory Policy: Southwest Technical College affirms its commitment to promote the goals of fairness and equity in all aspects of the educational enterprise, and bases its policies on the idea of global human dignity.

Southwest Tech is committed to a policy of nondiscrimination. No otherwise qualified person may be excluded from participation in or be subjected to discrimination in any course, program or activity because of race, age, color, religion, sex, pregnancy, national origin or disability. Southwest Technical College does not discriminate on the basis of sex in the education programs or activities that it operates, as required by Title IX and 34 CFR part 106. The requirement not to discriminate in education programs or activities extends to admission and employment. Inquiries about Title IX and its regulations to STECH may be referred to the Title IX Coordinator, to the Department of Education, and/or to the Office for Civil rights.

If you believe you have experienced discrimination or harassment on our campus, please contact the Title IX Coordinator, Cory Estes: cestes@stech.edu, (435) 865-3938.

For special accommodations, please contact the ADA Coordinator, Cyndie Tracy: ctracy@stech.edu, (435) 865-3944.
Southwest Technical College
757 West 800 South
Cedar City, UT 84720
info@stech.edu
(435) 586-2899