



Course Number and Title: ISY 251 Hardening the Infrastructure

Campus Location:

Georgetown, Dover, Wilmington

Effective Date:

2018-51

Prerequisite:

CNE 192

Co-Requisites:

None

Course Credits and Hours:

3.00 credits

2.00 lecture hours/week

2.00 lab hours/week

Course Description:

This course examines tools, techniques, and a technology used in the securing of information assets and is designed to provide in-depth information on the software and hardware components of information security and assurance. Topics covered include firewall configurations, network security, virtual private networks (VPNs), and security monitoring tools.

Required Text(s):

Obtain current textbook information by viewing the [campus bookstore - https://www.dtcc.edu/bookstores](https://www.dtcc.edu/bookstores) online or visit a campus bookstore. Check your course schedule for the course number and section.

Additional Materials:

USB flash-drive for lab work and broadband Internet access

Schedule Type:

Classroom Course

Disclaimer:

None

Core Course Performance Objectives (CCPOs):

1. Evaluate firewall planning and design. (CCC 1, 2, 3, 5; PGC 1, 2, 5, 7, 9)
2. Create firewall configurations, and perform administration. (CCC 1, 2, 3; PGC 1, 2, 3,5)
3. Explain and evaluate proxy servers. (CCC 1, 2, 3, 5; PGC 1, 3, 5, 7, 9)
4. Analyze and implement encryption schemes. (CCC 1, 2, 3; PGC 1, 3, 5, 9)
5. Evaluate and select an identity management structure. (CCC 1, 2, 3, 5; PGC 1, 2, 3, 4,5, 7, 9)
6. Analyze and evaluate the setup of a Virtual Private Network (VPN). (CCC 1, 2, 3; PGC 2, 3, 5, 7, 9)
7. Explain and configure intrusion detection and prevention systems. (CCC 1, 2, 3, 4; PGC 1, 2, 5)

See Core Curriculum Competencies and Program Graduate Competencies at the end of the syllabus. CCPOs are linked to every competency they develop.

Measurable Performance Objectives (MPOs):

Upon completion of this course, the student will:

1. Evaluate firewall planning and design.
 1. Identify common misconceptions about firewalls.
 2. Explain why a firewall is dependent on an effective security policy.
 3. Compare and contrast types of firewalls.
 4. Identify the limitations of firewalls.
 5. Evaluate and recommend suitable hardware and software for a firewall application.
2. Create firewall configurations, and perform administration.
 1. Set up firewall rules that reflect security policies.
 2. Identify and implement different firewall configuration strategies.
 3. Modify existing firewall configurations to meet new needs and threats.
 4. Examine and analyze firewall log files, and follow the basic initial steps in responding to security incidents.
3. Explain and evaluate proxy servers.
 1. Discuss proxy servers, and explain how they work.
 2. Evaluate the value of implementation of a proxy server.
 3. Discuss and recommend options for proxy server configuration.
 4. Explain how to deploy and use a reverse proxy server.
4. Analyze and implement encryption schemes.
 1. Describe the role encryption plays in firewall architecture.
 2. Explain how digital certificates work and why they are important security tools.
 3. Analyze the workings of secure socket layer (SSL), pretty good privacy (PGP), and other popular encryption schemes.
 4. Discuss and implement internet protocol security (IPSec).
5. Evaluate and select an identity management structure.
 1. Describe the role identity management plays in network security.
 2. List the advantages and disadvantages of centralized authentication systems (CAS).
 3. Identify the weaknesses of password security systems.
 4. Employ password security tools.
 5. Summarize identity management.
6. Analyze and evaluate the setup of a virtual private network (VPN).
 1. Explain the components and essential operations of VPNs.
 2. Describe the different types of VPNs.
 3. Choose the right tunneling protocol for a VPN.
 4. Enable secure remote access for individual users via a VPN.
 5. Recommend best practices for effective configuration and maintenance of VPNs.
7. Explain and configure intrusion detection and prevention systems.
 1. Describe the various technologies used to implement intrusion detection and prevention.
 2. Configure intrusion detection system (IDS) and intrusion prevention system (IPS) rules.
 3. Discuss honey pots and honey nets systems.

Evaluation Criteria/Policies:

Students must demonstrate proficiency on all CCPOs at a minimal 75 percent level to successfully complete the course. The grade will be determined using the Delaware Tech grading system:

92	-	100	=	A
83	-	91	=	B
75	-	82	=	C
0	-	74	=	F

Students should refer to the [Student Handbook - https://www.dtcc.edu/handbook](https://www.dtcc.edu/handbook) for information on the Academic Standing Policy, the Academic Integrity Policy, Student Rights and Responsibilities, and other policies relevant to their academic progress.

Core Curriculum Competencies (CCCs are the competencies every graduate will develop):

1. Apply clear and effective communication skills.
2. Use critical thinking to solve problems.
3. Collaborate to achieve a common goal.
4. Demonstrate professional and ethical conduct.
5. Use information literacy for effective vocational and/or academic research.
6. Apply quantitative reasoning and/or scientific inquiry to solve practical problems.

Program Graduate Competencies (PGCs are the competencies every graduate will develop specific to his or her major):

1. Identify and remediate vulnerabilities.
2. Design, plan, and install network systems.
3. Install and configure operating systems.
4. Demonstrate the ability to write and debug scripts.
5. Demonstrate professionalism and ethical responsibility.
6. Communicate effectively to diverse groups of stakeholders.
7. Perform change management analysis and documentation.
8. Perform evidence collection and forensics analysis.
9. Create, modify, and/or implement security policies.

Disabilities Support Statement:

The College is committed to providing reasonable accommodations for students with disabilities. Students are encouraged to schedule an appointment with the campus Disabilities Support Counselor to request an accommodation needed due to a disability. A listing of campus Disabilities Support Counselors and contact information can be found at the [disabilities services - https://www.dtcc.edu/disabilitysupport](https://www.dtcc.edu/disabilitysupport) web page or visit the campus Advising Center.