CDS152 Introduction to Cyber Defense

(3 credit hours)

Course Syllabus

Course Description

This course will provide a foundational overview of the computer network operations, their vulnerabilities, the various types of automated network intrusions, and some basic defense strategies-to include Defense in Depth. The basic elements of access control process, application security, operating system security, human element security and physical security will be examined. Essential cryptographic concepts will be introduced. Students will also become familiar with laws and regulations applicable to information security and privacy.

Course Learning Outcomes

By the end of this course, you will be able to:

1. Define the Confidentiality-Integrity-Availability triad.
2. Express threats, vulnerabilities and risks to information assets.
3. Identify cyber defense methods at application, host and network level.
4. Describe elements of access control process.
5. Explain attacks to and defenses for human element and physical security.
6. Outline major laws and regulations for privacy protection and information security.

Required Textbook(s) and Resources

There are no required resources for this course. All course materials are included as links within the course.

Be sure to also review the weekly **Explore** sections for additional library or web resources. For access to databases, research help, and writing tips, visit the Tiffin University Library.

Time Commitment

Effective time management is possibly the single most critical element to your academic success. To do well in this online class you should plan your time wisely to maximize your learning through the completion of readings, discussions, and assignments. Because of our accelerated, seven-week term, TU online courses are designed with the expectation that you dedicate a little over **six (6)** hours per credit hour to course activities and preparation **each week**. For example, for successful completion of a three-credit, seven-week online course you should reserve roughly **twenty (20) hours per week**.

To help plan your time and keep on track toward successful course completion, note the distinctive rhythm of assignment due dates:

1. All times assume Eastern Time (GMT-4).
2. Weeks begin at 12:00 a.m. ET on Monday and end at 11:55 p.m. ET on Sunday.
3. Unless otherwise noted, initial assignments or discussion posts are due by **11:55 p.m. ET** on **Wednesdays.**
4. Additional assignments or follow-up discussion posts are due by **11:55 p.m. ET** on **Saturdays, and**
5. Major assignments and reflections are typically due by **11:55 p.m. ET** on **Sundays.**

Learning Activities

Learning activities for this course include discussion blog posts, four essays, and an overarching case study that consists of three reports and one PowerPoint presentation. The purpose of this term-long case study is to understand, analyze, and apply key topics to a security breach scenario spanning from initial observation and evaluation to final incident reporting and presentation. The case study is broken down over three weeks, consisting of four deliverables. Each deliverable will reflect on and incorporate key topics learned during previous weeks.

Grading

The chart below identifies the individual contributions from each type of activity, per week.

Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Total
Discussions Activity 1.1 (n/a) Activity 1.2 (35)	**Discussion** Activity 2.1 (35)	**Discussion** Activity 3.1 (35)	**Discussion** Activity 4.1 (35)	**Discussion** Activity 5.1 (35)	**Discussion** Activity 6.1 (35)	**Discussion** Activity 7.1 (35)	**245**
Assignment Activity 1.3 (90)	**Assignment** Activity 2.2 (90)	**Assignment** Activity 3.2 (115)	**Assignment** Activity 4.2 (90)	**Assignment** Activity 5.2 (90)	**Assignment** Activity 6.2 (115)	**Assignments** Activity 7.2 (120) Activity 7.3 (45)	**730**
125	**125**	**150**	**125**	**125**	**150**	**200**	**1000**

Grading Scale

A: 90-100% | B: 80-89% | C: 70-79% | D: 60-69% | F: <60%

Course Schedule and Weekly Checklist

Topic	**Learning Activities** (Due by 11:55 p.m. ET on day designated)
Start Here	❑ MON: Activity 1.1: Driving Force - Initial Post
Week 1: Cyberattack Methods Cyber Defense Methods	❑ WED: Activity 1.1: Driving Force - Secondary Post ❑ WED: Activity 1.2: Cyberattacks - Initial Post ❑ SAT: Activity 1.2: Cyberattacks - Secondary Post ❑ SUN: Activity 1.3: Cyberattacks and Defense
Week 2: Attack Methods Defense Methods	❑ WED: Activity 2.1: Social Engineering Methods - Initial Post ❑ SAT: Activity 2.1: Social Engineering Methods - Secondary Post ❑ SUN: Activity 2.2: Current Social Engineering Defenses
Week 3: Security breaches	❑ WED: Activity 3.1: Security Breach Evaluation - Initial Post

Access controls Incident responses	❑ SAT: Activity 3.1: Security Breach Evaluation - Secondary Post ❑ SUN: Activity 3.2: Security Breach Part 1: Initial Evaluation
Week 4: Defense in Depth Security Postures	❑ WED: Activity 4.1: Defense in Depth Security Controls - Initial Post ❑ SAT: Activity 4.1: Defense in Depth Security Controls - Secondary Post ❑ SUN: Activity 4.2: Defense in Depth Security Posture
Week 5: Explaining Security Policies Developing a Basic Security Policy	❑ WED: Activity 5.1: Explaining a Security Policy - Initial Post ❑ SAT: Activity 5.1: Explaining a Security Policy - Secondary Post ❑ SUN: Activity 5.2: Writing a Security Policy
Week 6: Incident Response Triage Security Policies	❑ WED: Activity 6.1: Security Breach Response - Initial Post ❑ SAT: Activity 6.1: Security Breach Response - Secondary Post ❑ SUN: Activity 6.2: Security Breach Part 2: Follow-Up and Security Recommendations
Week 7: Security Breach Aftermath Lessons learned Incident Reports	❑ WED: Activity 7.1: Security Breach Aftermath - Initial Post ❑ THUR: Activity 7.2: Security Breach Part 3: Incident Report ❑ SAT: Activity 7.1: Security Breach Aftermath - Secondary Post ❑ SAT: Activity 7.3: Security Breach Presentation

Tips for Success

Successful online learning requires a good deal of self-discipline and self-direction. As seekers of the truth, we should be willing to challenge and review one another's academic work in a spirit of respectful comradery and constructiveness. Your course is a place for you to stretch and grow as you benefit from the expertise, knowledge, experience and diverse perspectives of your instructor and peers. Constructive feedback will challenge you to stretch your own thinking, thereby expanding your knowledge, understanding and application.

To get the most out of your learning experience, you should actively engage (participate) in **ALL** course activities. Course elements are arranged chronologically. To complete a week, simply work your way "down the page" through all of the course materials and activities.

For More Information:

Be sure to review the Support, Policies, and Procedures addendum.