CDS244 Cyber Security

(3 credit hours)

Course Syllabus

Course Description

This course introduces the fundamentals of cybersecurity, including network security; compliance and operational security; malware attacks; threats, vulnerabilities and risks; application, data, and host security; access control and identity management; and cryptography. The course covers new topics in cybersecurity as well, including Web application attacks, cloud computing security, application development security and psychological approaches to social engineering attacks.

Course Learning Outcomes

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

1. Identify and prioritize risks to information assets.
2. Identify network attacks and defense strategies.
3. Explain how businesses apply cryptography in maintaining information security
4. Describe the principles of risk management, common response techniques, and issues related to recovery of IT systems.
5. Discuss authentication, authorization, and access control methodologies.

Prerequisites/Corequisites

CDS152 or CST155

Required Textbook(s) and Resources

Ciampa, Mark (2022), CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition, Cengage Learning

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, forum posts, labs 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 forum 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

A significant part of the assignments relies on the lab exercises you are going to do to apply the concepts you have learned in the course. They are called Live Virtual Machine Labs, or shortly LVM, as we refer to them on Moodle. These lab exercises are included in Cengage MindTap, but the links will take you to the lab website hosted by Practice Labs.

By completing these labs, you will access one or more virtual machines which are specifically built with a secure or vulnerable configuration and you will use the software tools to perform the tasks as given in step-by-step instructions. You will take screenshots as you proceed and submit the lab reports on Moodle.

You will also complete written assignments or participate in discussion forums in this course. Finally, you will take module quizzes covering two or three modules completed in a particular week.

Note that all grading will be done on Moodle. You will find some quizzes or activities on MindTap but they are for practice purposes only.

Grading and Points Distribution

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

Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Total
Forum Activity 1.1 (n/a) Activity 1.2 (30)	**Forum** Activity 2.1 (30)	**Forum** Activity 3.1 (30)	**Forum** Activity 4.1 (30)	**Forum** Activity 5.1 (30)	**Forum** Activity 6.1 (30)	-	**180**
Quiz Activity 1.3 (20)	**Quiz** Activity 2.2 (20)	**Quiz** Activity 3.2 (20)	**Quiz** Activity 4.2 (20)	**Quiz** Activity 5.2 (20)	**Quiz** Activity 6.2 (20)	**Quiz** Activity 7.4 (20)	**140**
Labs Activity 1.4 (40) Activity 1.5 (40)	**Labs** Activity 2.3 (40) Activity 2.4 (40)	**Labs** Activity 3.3 (40) Activity 3.4 (40) Activity 3.5 (40)	**Labs** Activity 4.3 (40) Activity 4.4 (40)	**Labs** Activity 5.3 (40) Activity 5.4 (40)	**Labs** Activity 6.3 (40) Activity 6.4 (40)	**Labs** Activity 7.1 (40) Activity 7.2 (40)	**600**
-	-	-	-	-	-	**Assignment** Final Activity 7.3 (80)	**80**
130	**130**	**170**	**130**	**130**	**130**	**180**	**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: What is Information Security? Vulnerabilities, threats, and attacks Penetration testing and vulnerability analysis Cybersecurity resources Social engineering	❏ WED: Activity 1.2: Protecting a Company's Information Systems ❏ SAT: Activity 1.3 Quiz: Week 1 ❏ SUN: Activity 1.4: Week 1 Lab: Gathering Intelligence on Threat Actors and Vectors ❏ SUN: Activity 1.5: Week 1 Lab: Social Engineering Techniques and Exploits
Week 2: Penetration tests Pen test Vulnerability scanning Cybersecurity resources	❏ WED: Activity 2.1: Addressing the Vulnerabilities Found ❏ SAT: Activity 2.2 Quiz: Week 2 ❏ SUN: Activity 2.3: Week 2 Lab: Penetration Testing Techniques ❏ SUN: Activity 2.4: Week 2 Lab: Control Mechanisms, Standards and Frameworks
Week 3: Malware and application attacks Threat Actors Adversarial artificial intelligence attacks	❏ WED: Activity 3.1: Endpoint Attack ❏ SAT: Activity 3.2 Quiz: Week 3 ❏ SUN: Activity 3.3: Week 3 Lab: Identifying Different Cyber Attacks ❏ SUN: Activity 3.4: Week 3 Lab: Determining Security Vulnerabilities ❏ SUN: Activity 3.5: Week 3 Lab: Identifying Different Application Exploits
Week 4: Network attacks and assessment tools Physical security	❏ WED: Activity 4.1: Endpoint Security ❏ SAT: Activity 4.2 Quiz: Week 4 ❏ SUN: Activity 4.3: Week 4 Lab: Application and Host Hardening Techniques ❏ SUN: Activity 4.4: Week 4 Lab: Application Hardening Deployment Techniques

Security appliances and technologies Configuration management	
Week 5: Hash, symmetric, and asymmetric cryptographic algorithms Cryptography and cryptographic attacks Mitigation techniques, software restriction policies, and firewall rules	❑ WED: Activity 5.1: Cryptography Systems ❑ SAT: Activity 5.2 Quiz: Week 5 ❑ SUN: Activity 5.3: Week 5 Lab: Cryptographic Basic Concepts ❑ SUN: Activity 5.4: Week 5 Lab: Securing an Environment using Mitigating Techniques
Week 6: Attacks on authentication Implementing authentication security solutions	❑ WED: Activity 6.1: Securing Authentication Processes ❑ SAT: Activity 6.2 Quiz: Week 6 ❑ SUN: Activity 6.3: Week 6 Lab: Authentication and Authorization Implementation Techniques ❑ SUN: Activity 6.4: Week 6 Lab: Authentication and Authorization Solutions
Week 7: Risk Data Privacy Privacy and data protection	❑ THU: Activity 7.1: Week 7 Lab: Data Protection Implementation ❑ THU: Activity 7.2: Week 7 Lab: Identity and Account Management Mechanisms ❑ THU: Activity 7.3 Final: Risk Analysis ❑ SAT: Activity 7.4 Quiz: Week 7

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.