CDS424 Applied Network Security
(3 credit hours)
Course Syllabus

Course Description

This course offers a unique, in-depth look at the major business challenges and threats that organizations are facing when they are connected to public networks. This course provides a comprehensive explanation of network security basics, including how hackers gain access to online networks, and the use of firewalls and Virtual Private Networks (VPNs) to provide countermeasures. Using examples and exercises from the field, this course incorporates hands-on activities to prepare the students to disarm threats and prepare for future attacks and emerging technologies.

Course Learning Outcomes

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

1. Discuss the fundamental concepts of network security
2. Implement network security measures on a given network
3. Appraise the elements of firewall and VPN implementation and management
4. Set up a Firewall on a Client and on a Server
5. Set up a VPN on a Client and on a Server

Required Textbook(s) and Resources

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

A digital version of your book is included automatically as part of your course fees. You can access your book through the Cengage MindTap tool in Moodle.

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. You

might consider registering for one of the library's many webinars on library research, source evaluation, copyright, and other topics, at the Library Events - Upcoming Events web page. For further assistance email a librarian, at: library@tiffin.edu.

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 in this course will include one forum post per week in which students will share their understanding of key terms and themes introduced in the course materials. Discussion is encouraged. In addition, weekly assignments will require students to participate in hands-on online lab activities every week. The final project will result in a technical paper in which students will reflect on what they have learned about firewalls and VPNs and apply it to a real-world scenario.

Grading and Points Distribution

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
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)	**Forum** Activity 7.1 (30)	**210**
Labs Activity 1.3 (40) Activity 1.4 (40)	**Labs** Activity 2.2 (40) Activity 2.4 (40)	**Labs** Activity 3.2 (40) Activity 3.3 (40) Activity 3.4 (40)	**Labs** Activity 4.2 (40) Activity 4.3 (40)	**Labs** Activity 5.2 (40) Activity 5.3 (40)	**Labs** Activity 6.2 (40) Activity 6.3 (40)	**Labs** Activity 7.2 (40)	**560**
Quiz Activity 1.5 (20)	**Quiz** Activity 2.4 (20)	**Quiz** Activity 3.5 (20)	**Quiz** Activity 4.4 (20)	**Quiz** Activity 5.4 (20)	**Quiz** Activity 6.4 (20)	**Quiz** Activity 7.3 (20)	**140**
(n/a)	(n/a)	(n/a)	(n/a)	(n/a)	(n/a)	**Assignment** Technical Report **(Due Fri)** Activity 7.4 (90)	**90**
130	**130**	**170**	**130**	**130**	**130**	**180**	**1000**

Grading Scale

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

Please see the Academic Bulletin for grade appeal information.

Course Schedule and Weekly Checklist

Topic	**Learning Activities** (Due by 11:55 p.m. ET on day designated)
Start Here	❑ MON: Activity 1.1: Meet Your Peers
Week 1: Resilience Redundancy Security Policies	❑ WED: Activity 1.1: Meet Your Peers ❑ WED: Activity 1.2: Cybersecurity Resilience ❑ SUN: Activity 1.3: Week 1 Lab: Cybersecurity Backup and Restore Strategies ❑ SUN: Activity 1.4: Week 1 Lab: Organizational Risk Management and Policies ❑ SUN: Activity 1.5: Quiz: Module 14 Cybersecurity Resilience
Week 2: Cybersecurity Incidents Incident Response Policy Incident Response Tools	❑ WED: Activity 2.1: Incident Preparation and Response ❑ SUN: Activity 2.2: Week 2 Lab: Incident Response Policy and Procedures ❑ SUN: Activity 2.3: Week 2 Lab: Incident Response Tools ❑ SUN: Activity 2.4: Quiz: Module 13 Incident Preparation, Response, and Investigation
Week 3: Network Attacks Network Security Physical Security	❑ WED: Activity 3.1: Network and Physical Security ❑ SUN: Activity 3.2: Week 3 Lab: Identifying Indicators of a Network Attack ❑ SUN: Activity 3.3: Week 3 Lab: Network Security Assessment Tools ❑ SUN: Activity 3.4: Week 3 Lab: Physical Security Control Mechanisms ❑ SUN: Activity 3.5: Quiz: Module 13 Incident Preparation, Response, and Investigation
Week 4: Network Security Appliances Firewalls	❑ WED: Activity 4.1: Network Security Technologies ❑ SUN: Activity 4.2: Week 4 Lab: Implementing Secure Network Solutions ❑ SUN: Activity 4.3: Week 4 Lab: Enterprise Network Security

VPNs	❏ SUN: Activity 4.4: Quiz: Module 09 Network Security Appliances and Technologies
Week 5: Cloud Technology Cloud Infrastructure Virtualization Technology	❏ WED: Activity 5.1: Cloud and Virtualization Security ❏ SUN: Activity 5.2: Week 5 Lab: Cloud and Virtualization Concepts ❏ SUN: Activity 5.3: Week 5 Lab: Securing a Cloud Infrastructure ❏ SUN: Activity 5.4: Quiz: Module 10 Cloud and Virtualization Security
Week 6: Cloud Technology Cloud Infrastructure Virtualization Technology	❏ WED: Activity 6.1: Wireless Network Security ❏ SUN: Activity 6.2: Week 6 Lab: Implementation of Secure Protocols ❏ SUN: Activity 6.3: Week 6 Lab: Implementing Wireless Security Configurations ❏ SUN: Activity 6.4: Quiz: Module 11 Wireless Network Security
Week 7: Public Key Infrastructure Cryptographic Protocols Digital Certification	❏ WED: Activity 7.1: Public Key Infrastructure (PKI) ❏ FRI: Activity 7.2: Technical Report - Firewalls and VPNs ❏ SUN: Activity 7.3: Week 7 Lab: Implementing a Public Key Infrastructure ❏ SUN: Activity 7.4: Quiz: Module 07 Public Key Infrastructure and Cryptographic Protocols

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. Your Instructor Will Expect You to:

- Thoroughly review orientation materials (Start Here) within the first 48 hours of the term.
- Monitor your TU email account **daily** for important updates and announcements.

- Take ownership of your learning experience and act in a proactive, self-directed manner. That means:
    - Fully participate in all learning activities.
    - Complete assignments as described in rubrics or other instructions.
    - Submit all work on time and in the specified format (e.g. APA format for citations).
    - Utilize and incorporate instructor provided feedback to improve your work.
    - Ask questions so you can better understand course material or assignments.
    - Use the highest standards of intellectual honesty and integrity. For more information, see the TU Library guide: Digital Literacy: Netiquette and Internet Safety.
    - Treat others respectfully and demonstrate "netiquette" (online politeness and respectfulness) at all times. TU celebrates cultural uniqueness and expects all students to be considerate and thoughtful throughout their learning experiences.

You Should Expect Your Instructors to:

In general, your instructors should advocate for your success as a learner and help guide you toward successful completion of the course activities and most importantly, attainment of the course learning outcomes. To accomplish this, your instructors should:

- Post an introductory announcement/email at the beginning of each week to provide updates and help you prepare for the week's activities.
- Maintain an active and engaged presence in all course activities and throughout the course.
- Respond to your emailed questions within 48 hours, if not sooner.
- Clearly communicate any absences or expected non-participation due to extenuating circumstances. For example, "I will be traveling to attend a funeral this week and may not be able to respond to questions or participate in forums for a couple of days."
- When grading your work, your instructors should:
    - clearly indicate their grading approach (what they like to see in submitted work as well as what types of errors they tend to penalize more harshly),
    - thoroughly review and evaluate your submissions in a timely manner (in less than 5 days for most assignments), and
    - provide constructive feedback that indicates the strengths and weaknesses of your work and provides suggestions on how you can improve your performance on future assignments.

Accommodations

The **Office for Disability Services** supports the institutional commitment to diversity by providing educational opportunities for qualified individuals with disabilities through accessible programs and services in compliance with Section 504 of the Rehabilitation Act of 1973 and Title III of the Americans with Disabilities Act (ADA) of 1990. If you need reasonable accommodations due to a documented disability, contact the Office for Equity, Access, & Opportunity 419.448.3021 or via email at disabilityservices@tiffin.edu.

Additional Resources & Support

For technical support, either email moodlesupport@tiffin.edu or call the 24/7 Technical Support Call Center at 855-664-1200.

If you need to consult an academic advisor refer to TU's Meet the Team page.

For information about TU's peer tutoring program see the Murphy Center's Tutoring Policies and Procedures page. Veterans and active military can seek assistance from TU's Veteran and Military Services Web Page.

Comments or Concerns

TU's online programs are designed to be student *driven*: to empower you with a voice and stake in your learning. Our courses feature multiple and varied ways that you can share feedback, and we invite you to become an active voice and help drive our improvement efforts. In addition to providing in-course feedback, we encourage you to submit questions or comments directly to the online team at online@tiffin.edu.