



## **CDS491 Cyber and Information Assurance Seminar (3 credit hours) Course Syllabus**

---

### **Course Description**

This course provides a capstone experience for cyber defense. It synthesizes advanced skills in intrusion detection techniques, network vulnerability assessments, and effective countermeasures against intrusion techniques. The culmination of their coursework in the cyber program will allow them to identify and utilize penetration testing matrices to assess the security of networks. Additionally, they will develop a defense-in-depth network security strategy, create local policies and protocols for responding to cyber attacks, and gain insights into the future threat landscape for cyber defense.

### **Course Learning Outcomes**

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

1. Understand intrusion detection techniques.
2. Perform network vulnerability assessments.
3. Analyze intrusion technique and provide effective countermeasure.
4. Identify and utilize penetration testing matrices to test networks.
5. Develop defense – in – depth network defense model.
6. Develop local policy and protocols for responding to a cyber-attack.
7. Identify future threat landscape for cyber defense.

### **Required Textbook(s) and Resources**

No textbook is assigned for this course. Students will pull from the knowledge they have gained leading to this final project.

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

Throughout the course, you will participate in weekly discussion forums to share and observe one another's journey through the project process. You will also complete assignments that involve addressing prompts related to specific sections of your paper and providing peer feedback. These assignments will involve submitting sections of your paper for review by the instructor. The culminating task will be the creation of a capstone paper, wherein you will develop a Cybersecurity Strategy Proposal that encompasses most aspects of the cybersecurity skillset and addresses a real-world scenario. Finally, you will create a narrated presentation to defend your proposal and showcase your ability to present your knowledge as an authority in the cybersecurity field.

## 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       |
|--|---|---|---|---|---|--|-------------|
| <b>Forum</b><br>Activity 1.1 (n/a)<br>Activity 1.2<br>(50) | <b>Forum</b><br>Activity 2.1<br>(50)      | <b>Forum</b><br>Activity 3.1<br>(50)      | <b>Forum</b><br>Activity 4.1<br>(50)      | <b>Forum</b><br>Activity 5.1<br>(50)      | <b>Forum</b><br>Activity 6.1<br>(50)                      | <b>Forum</b><br>Activity 7.1<br>(50)                                   | <b>350</b>  |
| <b>Assignment</b><br>Activity 1.3<br>(80)                  | <b>Assignment</b><br>Activity 2.2<br>(80) | <b>Assignment</b><br>Activity 3.2<br>(80) | <b>Assignment</b><br>Activity 4.2<br>(80) | <b>Assignment</b><br>Activity 5.2<br>(80) | (n/a)   | (n/a)  | <b>400</b>  |
| (n/a)  | (n/a)                                     | (n/a)                                     | (n/a)                                     | (n/a)                                     | <b>Assignment</b><br>Final Paper<br>Activity 6.2<br>(150) | <b>Assignment</b><br>Narrated<br>Presentation<br>Activity 7.2<br>(100) | <b>250</b>  |
| <b>130</b>   | <b>130</b>                                | <b>130</b>                                | <b>130</b>                                | <b>130</b>                                | <b>200</b>  | <b>150</b>   | <b>1000</b> |

## 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   | <input type="checkbox"/> MON: Activity 1.1: What interests you? - Initial Post   |
| Week 1:<br>Capstone Projects<br>Career Relevance<br>Cybersecurity Analysis   | <input type="checkbox"/> WED: Activity 1.1: What interests you? - Secondary Post<br><input type="checkbox"/> WED: Activity 1.2: Scenario Choice - Analysis - Initial Post<br><input type="checkbox"/> SAT: Activity 1.2: Scenario Choice - Analysis - Secondary Post<br><input type="checkbox"/> SUN: Activity 1.3: Outline & Introduction and Analysis Sections |
| Week 2:<br>Intrusion Detection Techniques<br>Comprehensive Cybersecurity Strategy<br>Measures Selection Rationale<br>Chosen Measures Justification | <input type="checkbox"/> WED: Activity 2.1: Strategy Steps and Challenges - Initial Post<br><input type="checkbox"/> SAT: Activity 2.1: Strategy Steps and Challenges - Secondary Post<br><input type="checkbox"/> SUN: Activity 2.2: Development Section  |
| Week 3:<br>Cybersecurity Strategy Implementation Documentation<br>Steps and Tools in Implementation<br>Addressing Implementation Challenges        | <input type="checkbox"/> WED: Activity 3.1: Implementation Challenges - Initial Post<br><input type="checkbox"/> SAT: Activity 3.1: Implementation Challenges - Secondary Post<br><input type="checkbox"/> SUN: Activity 3.2: Implementation Section   |
| Week 4:  | <input type="checkbox"/> WED: Activity 4.1: Vulnerability and Penetration Testing Challenges - Initial Post  |

|   |  |
|---|--|
| <p>Systematic Vulnerability Assessment Process</p> <p>Vulnerability Mitigation Strategy Development</p> <p>Comprehensive Vulnerability Analysis and Penetration Testing</p> <p>Best Practices and Tools Application</p> | <ul style="list-style-type: none"> <li><input type="checkbox"/> SAT: Activity 4.1: Vulnerability and Penetration Testing Challenges - Secondary Post</li> <li><input type="checkbox"/> SUN: Activity 4.2: Vulnerability and Penetration Testing Section</li> </ul>   |
| <p>Week 5:</p> <p>Evaluation Process and Effectiveness Measurement</p> <p>Outcomes Analysis for Strengths and Weaknesses</p> <p>Adjustments Identification for Vulnerabilities/Shortcomings</p>                         | <ul style="list-style-type: none"> <li><input type="checkbox"/> WED: Activity 5.1: Evaluation Challenges - Initial Post</li> <li><input type="checkbox"/> SAT: Activity 5.1: Evaluation Challenges - Secondary Post</li> <li><input type="checkbox"/> SUN: Activity 5.2: Evaluation Section</li> </ul>               |
| <p>Week 6:</p> <p>Comprehensive Strategy Proposal Creation</p> <p>Proposal Structure with Clear Sections</p> <p>Effective Academic Writing Skills</p>   | <ul style="list-style-type: none"> <li><input type="checkbox"/> WED: Activity 6.1: Putting it all together - Initial Post</li> <li><input type="checkbox"/> SAT: Activity 6.1: Putting it all together - Secondary Post</li> <li><input type="checkbox"/> SUN: Activity 6.2: Strategy Proposal Submission</li> </ul> |
| <p>Week 7:</p> <p>Effective Narrated PowerPoint Presentation</p> <p>Communication of Project Findings</p> <p>Oral Communication and Presentation Skills Improvement</p>   | <ul style="list-style-type: none"> <li><input type="checkbox"/> WED: Activity 7.1: Presentation Challenges - Initial Post</li> <li><input type="checkbox"/> SAT: Activity 7.1: Presentation Challenges - Secondary Post</li> <li><input type="checkbox"/> SAT: Activity 7.2: Narrated Presentation</li> </ul>        |

## 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.

## For More Information:

Be sure to review the [Support, Policies, and Procedures](#) addendum.