



# STARK STATE COLLEGE

## GENERAL SYLLABUS

### Course Information

**Course Name:** Cyber Defense Fundamentals  
**Course Number:** CFS210

### Required Materials

**Textbook(s):** TestOut CyberDefense Pro 2nd Edition, TestOut, ISBN 978-1-935080-73-2  
**Required Readings:** None  
**Additional Materials:** 1. TestOut minimum system requirements  
<https://support.testout.com/hc/en-us/articles/234567528-What-are-the-system-requirements-for-the-TestOut-software->  
 2. Additional material furnished by the instructor or available online.

### Course Outline/Calendar

The date of coverage and order of coverage may be modified based on the faculty member and events beyond the control of faculty members that interfere with class times and teaching.

Week	Chapter/Topic/Lab
Week 1	CH2: Vulnerability Response, Handling, and Management (Part 1) <ul style="list-style-type: none"> <li>• Discussion: Introduce Yourself</li> <li>• THM Lab: Common Attacks</li> </ul>
Week 2	CH2: Vulnerability Response, Handling, and Management (Part 2) <ul style="list-style-type: none"> <li>• REV2</li> <li>• THM Lab: Cyber Kill Chain</li> </ul>
Week 3	CH3: Threat Intelligence and Threat Hunting <ul style="list-style-type: none"> <li>• REV3</li> <li>• THM Lab: Threat Hunting Introduction</li> <li>• THM Lab: Intro to CTI</li> <li>• 3.2.8 PBQ: Performing Threat Intelligence</li> </ul>
Week 4	CH4: System and Network Architecture (Part 1) <ul style="list-style-type: none"> <li>• THM Lab: Vulnerabilities 101</li> <li>• 4.2.9 PBQ: Analyzing Network Infrastructure</li> <li>• Discussion: Current Cyber News 1</li> </ul>
Week 5	CH4: System and Network Architecture (Part 2) <ul style="list-style-type: none"> <li>• REV4</li> <li>• TestOut Labs: 4.5.9, 4.5.10, 4.5.11)</li> <li>• THM Lab: Security Principles</li> </ul>
Week 6	CH5: Vulnerability Assessments (Part 1)

Week	Chapter/Topic/Lab
	<ul style="list-style-type: none"> <li>• THM Lab: Google Dorking</li> <li>• TestOut Labs: 5.1.5, 5.1.10, 5.1.12, 5.1.15, 5.2.10, 5.2.12, 5.2.13, 5.2.14, 5.2.15</li> <li>• TestOut PBQ: 5.2.6, 5.4.3</li> </ul>
Week 7	CH5: Vulnerability Assessments (Part 2) <ul style="list-style-type: none"> <li>• REV5</li> <li>• THM Lab: OpenVAS</li> <li>• TestOut Labs: 5.3.10, 5.3.11, 5.3.12, 5.4.15, 5.4.16</li> <li>• TestOut PBQ: 5.4.4, 5.4.5</li> </ul>
Week 8	CH6: Network Security (Part 1) <ul style="list-style-type: none"> <li>• REV6A</li> <li>• TestOut Labs: 6.1.12, 6.1.13, 6.2.5, 6.2.6, 6.2.7, 6.2.8, 6.4.8, 6.4.9, 6.5.9, 6.5.10, 6.5.1</li> <li>• TestOut PBQ: 5.5.4</li> </ul>
Week 9	CH6: Network Security (Part 2) <ul style="list-style-type: none"> <li>• REV6B</li> <li>• THM Lab: Wuzuh</li> <li>• TestOut Labs: 6.6.6, 6.6.7, 6.9.10, 6.9.11, 6.9.12</li> <li>• TestOut PBQ: 6.7.4</li> </ul>
Week 10	CH7: Host-Based Attacks (Part 1) <ul style="list-style-type: none"> <li>• THM Lab: Malware Introductory</li> <li>• Discussion: APT Profiling</li> </ul>
Week 11	CH7: Host-Based Attacks (Part 2) <ul style="list-style-type: none"> <li>• REV7</li> <li>• THM Lab: Bash Scripting</li> <li>• THM Lab: Intro to SIEM</li> </ul>
Week 12	CH8: Security Management <ul style="list-style-type: none"> <li>• REV8</li> <li>• THM Lab: SOC Fundamentals</li> <li>• THM Lab: Servidae Log Analysis in ELK</li> </ul>
Week 13	CH9: Post-Attack <ul style="list-style-type: none"> <li>• REV9</li> </ul>
Week 14	Cyber Threat Intelligence Report <ul style="list-style-type: none"> <li>• Introduction of final paper</li> <li>• CySA+ Domain Exams</li> </ul>
Week 15	CompTIA CySA+ Bootcamp <ul style="list-style-type: none"> <li>• CompTIA CySA+ Practice Exam</li> </ul>
Week 16	FINALS <ul style="list-style-type: none"> <li>• Final Exam</li> <li>• CTI Report (Final Practical) due</li> </ul>