

DEREE COLLEGE SYLLABUS FOR:

ITC 4346 INTRUSION DETECTION & INCIDENT RESPONSE
 (Previously: ITC 4446 INTRUSION DETECTION & INCIDENT RESPONSE)
 (Updated Fall 2023)

3/0/3
UK LEVEL: 6
UK CREDITS: 15

PREREQUISITES:	ITC 2024 Computer Networks & Cybersecurity Fundamentals ITC 2088 Introduction to Programming ITC 2093 Operating System Concepts								
COREQUISITES:	None.								
CATALOG DESCRIPTION:	Intrusion prevention, detection, and response; defensive and offensive techniques and tools; network traffic analysis.								
RATIONALE:	The course prepares students for timely and effective response to organizational cyber threats, through the use of modern tools and technologies, and the results of state-of-the-art research on intrusion detection systems. Special emphasis is given to related AI and machine learning techniques.								
LEARNING OUTCOMES:	As a result of taking this course, the student should be able to: <ol style="list-style-type: none"> 1. Compare and contrast network intrusion detection and prevention systems, tools, and techniques. 2. Analyse methods for recognizing and profiling attack patterns. 3. Assess the application of AI and ML techniques in intrusion detection and prevention. 4. Develop incident and post-incident activity plan, policy, and operational procedures. 								
METHOD OF TEACHING AND LEARNING:	In congruence with the teaching and learning strategy of the college, the following tools are used: <ul style="list-style-type: none"> • Classroom lectures, laboratory practical sessions using various simulations tools and progress meetings. • Office hours held by the instructor to provide further assistance to students. • Use of the Blackboard Learning platform, where instructors post lecture notes, assignment instructions, timely announcements, as well as additional resources. 								
ASSESSMENT:	<p>Summative:</p> <table border="1"> <tr> <td>1st assessment: Midterm Exam Short essay questions and case problems.</td> <td>30%</td> </tr> <tr> <td>2nd assessment: Portfolio of student work, including project progress, and oral assessment (not eligible for 2nd marking)</td> <td>10%</td> </tr> <tr> <td>Final assessment: Individual Project Situational incident response plan including attack tracing, evidence collection and evidence tracing.</td> <td>60%</td> </tr> </table> <p>Formative:</p> <table border="1"> <tr> <td>Take-home short problems</td> <td>0%</td> </tr> </table> <p>The formative assessments aim to shape teaching and prepare students for the summative assessments.</p>	1 st assessment: Midterm Exam Short essay questions and case problems.	30%	2 nd assessment: Portfolio of student work, including project progress, and oral assessment (not eligible for 2 nd marking)	10%	Final assessment: Individual Project Situational incident response plan including attack tracing, evidence collection and evidence tracing.	60%	Take-home short problems	0%
1 st assessment: Midterm Exam Short essay questions and case problems.	30%								
2 nd assessment: Portfolio of student work, including project progress, and oral assessment (not eligible for 2 nd marking)	10%								
Final assessment: Individual Project Situational incident response plan including attack tracing, evidence collection and evidence tracing.	60%								
Take-home short problems	0%								

	<p>The 1st summative assessment tests the LOs 1 and 2. The 2nd summative assessment tests the LOs 1-4. The final summative assessment tests the LOs 1-4.</p> <p><i>The final grade for this module will be determined by averaging all summative assessment grades, based on predetermined weights for each assessment. If students pass the final summative assessment, which tests all Learning Outcomes for this module, and the average grade for the module is 40 or above, students are not required to resit any failed assessments.</i></p>
INDICATIVE READING:	<p>REQUIRED READING:</p> <ol style="list-style-type: none"> 1. Johansen, G., (2020). Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats (2nd Edition). Packt <p>RECOMMENDED READING:</p> <ol style="list-style-type: none"> 1. Pathan, A. (2016). The State of the Art in Intrusion Prevention and Detection. Routledge 2. Monnappa, A. (2018). Learning Malware Analysis: Explore the concepts, tools, and techniques to analyse and investigate Windows malware. Packt
INDICATIVE MATERIAL: (e.g. audiovisual, digital material, etc.)	<p>REQUIRED MATERIAL: N/A</p> <p>RECOMMENDED MATERIAL: N/A</p>
COMMUNICATION REQUIREMENTS:	<p>Daily access to the course’s site on the College’s Blackboard CMS and the acg email. Communication using proper written and oral English. Use of word processor, spreadsheet, and presentation SW for documentation and presentation of assignments.</p>
SOFTWARE REQUIREMENTS:	<p>MS-Office Kali Linux (latest version) Cisco Packet Tracer Wireshark VMware Pro</p> <p>ID List: OSSEC (Open Source Security) Snort Suricata Bro Network Security Monitor Open WIPS NG Samhain Fail2Ban AIDE (Advanced Intrusion Detection Environment) Security Onion (Linux Distro)</p> <p>IR List: Cynet 360 Cyphon Volatility AlienVault OSSIM TheHive Project</p>

<p>WWW RESOURCES:</p>	<ul style="list-style-type: none"> • https://www.first.org/ • https://www.infosecurity-magazine.com/intrusion-prevention-detection/ • https://www.dnsstuff.com/intrusion-detection-system • https://www.hitachi-systems-security.com/blog/benefits-incident-response-plan/ • https://www.cert.govt.nz/business/guides/responding-to-incidents/incident-response-plan/
<p>INDICATIVE CONTENT:</p>	<ol style="list-style-type: none"> 1. Foundations of Incident Response 2. Managing Cyber Incidents 3. Analyzing Network Evidence 4. Analyzing System Memory 5. Analyzing System Storage 6. Analyzing Log Files 7. Writing the Incident Report 8. Malware Analysis Response 9. Leveraging Threat Intelligence