**DEREE COLLEGE SYLLABUS FOR:**

**ITC 4446 INTRUSION DETECTION & INCIDENT RESPONSE** **3/0/3**
(Fall 2020) **UK LEVEL: 6**
**UK CREDITS: 15**

| | |
|---|---|
| **PREREQUISITES:** | ITC 2024 Computer Networks & Cybersecurity Fundamentals<br>ITC 2088 Introduction to Programming<br>ITC 3121 Computer Networks Modelling and Analysis<br>MA 2010 Statistics I ***or***<br>MA 2021 Applied Statistics for Business ***or***<br>MA 2025 Applied Statistics for Science |
| **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:<br>1. Compare and contrast network intrusion detection and prevention systems, tools, and techniques.<br>2. Analyse methods for recognizing and profiling attack patterns.<br>3. Assess the application of AI and ML techniques in intrusion detection and prevention.<br>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:<br>• Classroom lectures, laboratory practical sessions using various simulations tools and progress meetings.<br>• Office hours held by the instructor to provide further assistance to students.<br>• Use of the Blackboard Learning platform, where instructors post lecture notes, assignment instructions, timely announcements, as well as additional resources. |
| **ASSESSMENT:** | **Summative**:<br>1st assessment: Midterm Exam<br>Short essay questions and case problems. — **30%**<br>2nd assessment: Portfolio of student work, including project progress, and oral assessment (not eligible for 2nd marking) — **10%**<br>Final assessment: Individual Project<br>Situational incident response plan including attack tracing, evidence collection and evidence tracing. — **60%**<br><br>**Formative:**<br>Take-home short problems — **0%** |

| | |
|---|---|
| | The formative assessments aim to shape teaching and prepare students for the summative assessments.<br>The 1st summative assessment tests the LOs 1 and 2.<br>The 2nd summative assessment tests the LOs 1-4.<br>The final summative assessment tests the LOs 1-4.<br><br>*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.* |
| **INDICATIVE READING:** | **REQUIRED READING:**<br>1. Johansen, G., (2020). Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats (2nd Edition). Packt<br><br>**RECOMMENDED READING:**<br>1. Pathan, A. (2016). The State of the Art in Intrusion Prevention and Detection. Routledge<br>2. Monnappa, A. (2018). Learning Malware Analysis: Explore the concepts, tools, and techniques to analyse and investigate Windows malware. Packt |
| **INDICATIVE MATERIAL:**<br>*(e.g. audiovisual, digital material, etc.)* | **REQUIRED MATERIAL**: N/A<br><br>**RECOMMENDED MATERIAL**: N/A |
| **COMMUNICATION REQUIREMENTS:** | Daily access to the course's site on the College's Blackboard CMS and the acg email.<br>Communication using proper written and oral English.<br>Use of word processor, spreadsheet, and presentation SW for documentation and presentation of assignments. |
| **SOFTWARE REQUIREMENTS:** | MS-Office<br>Kali Linux (latest version)<br>Cisco Packet Tracer<br>Wireshark<br>VMware Pro<br>**ID List:**<br>OSSEC (Open Source Security)<br>Snort<br>Suricata<br>Bro Network Security Monitor<br>Open WIPS NG<br>Samhain<br>Fail2Ban<br>AIDE (Advanced Intrusion Detection Environment)<br>Security Onion (Linux Distro)<br>**IR List:**<br>Cynet 360<br>Cyphon<br>Volatility |

| | |
|---|---|
| | AlienVault OSSIM<br>TheHive Project |
| **WWW RESOURCES:** | • https://www.first.org/<br>• https://www.infosecurity-magazine.com/intrusion-prevention-detection/<br>• https://www.dnsstuff.com/intrusion-detection-system<br>• https://www.hitachi-systems-security.com/blog/benefits-incident-response-plan/<br>• https://www.cert.govt.nz/business/guides/responding-to-incidents/incident-response-plan/ |
| **INDICATIVE CONTENT:** | 1. Foundations of Incident Response<br>2. Managing Cyber Incidents<br>3. Analyzing Network Evidence<br>4. Analyzing System Memory<br>5. Analyzing System Storage<br>6. Analyzing Log Files<br>7. Writing the Incident Report<br>8. Malware Analysis Response<br>9. Leveraging Threat Intelligence |