DEREE COLLEGE SYLLABUS FOR:

ITC 4648 ETHICAL HACKING & PENETRATION TESTING **3/1.5/3**
(Fall 2020) **UK LEVEL: 6**
UK CREDITS: 15

<table>
<tr><td><b>PREREQUISITES:</b></td><td>ITC 1070 Information Technology Fundamentals
ITC 2088 Introduction to Programming
ITC 2024 Computer Networks and Cybersecurity Fundamentals
ITC 2193 Operating System Concepts
ITC 3160 Fundamentals of RDBMS</td></tr>
<tr><td><b>COREQUISITES:</b></td><td>ITC 4214 Internet Programming</td></tr>
<tr><td><b>CATALOG DESCRIPTION:</b></td><td>Principles of ethical hacking and penetration testing using Kali Linux, Nessus, Metasploit Framework, and Tor. Reconnaissance/Footprinting, weaponization, privilege escalation, exfiltration. Scanning networks; enumeration; sniffing; vulnerability analysis. Denial-of-Service attacks; web apps hacking and patching; SQL injection & parameter binding. Buffer overflow attacks and defenses. Introduction to hacking wireless networks and IoT. Structured security testing aimed at finding focused security vulnerabilities, flaws, risks and unreliable environments.</td></tr>
<tr><td><b>RATIONALE:</b></td><td>The course capitalizes on the theoretical knowledge that students acquired in several other courses. The focus is on the development of a structured approach towards discovering vulnerabilities and the recommendation of solutions for improving network security and protecting data from potential attackers.</td></tr>
<tr><td><b>LEARNING OUTCOMES:</b></td><td>As a result of taking this course, the student should be able to:
1. Critically discuss the ethical and legal dimensions of professional ethical hacking and penetration testing and classify permitted activities.
2. Explain social engineering and associated techniques.
3. Perform planning, reconnaissance, scanning, exploitation/post-exploitation, and result reporting in the context of penetration testing on selected targets.
4. Deduce security flaws by implementing ethical hacking best practices in preparing and generating a variety of attacks.</td></tr>
<tr><td><b>METHOD OF TEACHING AND LEARNING:</b></td><td>In congruence with the teaching and learning strategy of the college, the following tools are used:
• 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.</td></tr>
<tr><td><b>ASSESSMENT:</b></td><td><b>Summative</b>:<table><tr><td>1st assessment: Midterm Exam
Short essay questions and case problems.</td><td><b>20%</b></td></tr></table></td></tr>
</table>

2nd assessment: Portfolio of student work, including project defence and presentation.	**10%**
Final assessment: Group Project Development of an ethical hacking procedure and recommendation of defense measures for a given set of conditions.	**70%**

Formative:

Take-home short problems, in-lab practice	**0%**

The formative assessments aim to shape teaching and prepare students for the summative assessments.
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 2, 3, 4.

Students are required to resit failed assessments in this module.

INDICATIVE READING:	**REQUIRED READING:** 1. Sabin, Z., (2018). *Learn Ethical Hacking from Scratch: Your steppingstone to penetration testing.* Packt **RECOMMENDED READING:** 1. Diogenes, Y., & Ozkaya, E. (2019). Cybersecurity – Attack and Defence Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals (2nd Edition). Packt 2. Singh, G. (2019). Learn Kali Linux 2019: Perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark. Packt 3. Allsopp, W. (2017). Advanced Penetration Testing: Hacking the World's Most Secure Networks. Wiley 4. Wagner, A. (2020). Hacking: How to Hack Penetration testing Hacking Book. Independently published 5. Bramwell, Ph. (2018). Hands-On Penetration Testing on Windows: Unleash Kali Linux, PowerShell, and Windows debugging tools for security testing and analysis. Packt 6. Khan, F. (2019). Hands-On Penetration Testing with Python: Enhance your ethical hacking skills to build automated and intelligent systems. Packt
INDICATIVE MATERIAL: *(e.g. audiovisual, digital material, etc.)*	**REQUIRED MATERIAL**: N/A **RECOMMENDED MATERIAL**: N/A
COMMUNICATION REQUIREMENTS:	Daily access to the course's site on the College's Blackboard CMS and the acg mail. Communication using proper written and oral English. Use of word processor and presentation SW for documentation and presentation of assignments.
SOFTWARE REQUIREMENTS:	MS-Office Kali Linux (latest version) Metasploitable

	Cisco Packet Tracer Wireshark VMware Pro Kali Linux Tools John the Ripper Metasploit Nmap OpenVAS IronWASP Nikto SQLMap SQLNinja Wapiti Maltego AirCrack-ng Reaver Ettercap Canvas
WWW RESOURCES:	• https://latesthackingnews.com/ • https://thehackernews.com/ • https://www.welivesecurity.com/ • https://gbhackers.com/ • https://www.youtube.com/user/BlackHatOfficialYT/featured • https://news.hitb.org/ • https://www.cybrary.it/ • https://www.eccouncil.org/ • https://www.offensive-security.com/ • https://www.hackthissite.org/ • https://www.hackthebox.eu/ • https://www.hacking-tutorial.com/
INDICATIVE CONTENT:	1. Legal and Ethical Aspects of Hacking 2. Pre-Connection Attacks 3. Network Penetration Testing 4. Post-Connection Attacks 5. Man-in-the-Middle Attacks 6. Gaining Access to Computer Devices 7. Scanning Vulnerabilities Using Tools 8. Client-Side Attacks – Social Engineering 9. Website Pentesting 10. SQL Injection Vulnerabilities