|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Course Name** | Computer security | | | | | |
| 1. **Course Code** | BCS 3201 | | | | | |
| 1. **Course Level** | Year 3 Semester 2 | | | | | |
| 1. **Contact Hours** | 60 | | | | | |
| 1. **Credit Units** | 4 | | | | | |
| 1. **Course Leader** | Samuel OCEN | | | | | |
| 1. **Course Description** | | | | | | |
| Computer security is a branch of technology concerned with digital security or information security applied to computers. Since the largest part of the computer that users interact with is software, computer security plays a big role in the development of secure software. | | | | | | |
| 1. **Course Objectives** | | | | | | |
| The specific objectives of the course are to: -   1. Introduce students to threats faced by computers in the connected digital world. 2. Discover all threats of a computer. 3. Introduce students to techniques that are used to protect computers against various threats. 4. Learn the fundamentals of computer security, including Principles of computer security, Basic cryptography, Authentication, secure network protocols (Kerberos, SSL), program security. | | | | | | |
| 1. **Course Learning Outcomes** | | | | | | |
| By the end of this course, students will be able to; -   1. Set security measures on a computer system. 2. Secure the operating system. 3. Describe the requirements for database security, and describe techniques for ensuring database reliability and integrity, secrecy, inference control, and multi-level databases. 4. Implement core applications for securing data in form of voice, text and images. | | | | | | |
| 1. **Detailed Course Content/topics and required time** | | | | | | |
| **Content** | | | **Method** | | **LH, TH, PH** | **Session** |
| Introduction to Computer Security   * An overview of Computer Security * Prospects of Computer Security. | | | Face-to-Face, | | 2 LH | 1 |
| Digital Security Principles   * Definition and Concepts of Digital Security * Information Security * Objectives of System Security | | | Face-to-Face,  Online. | | 3 LH, 3 PH | 02-03 |
| Hardware Based Security Mechanisms.   * Physical Security * Authentication * Authorisation * Accounting * Data Encryption * Packet Filters. | | | Face-to-Face,  Online. | | 3 LH | 04 |
| Practical One: Encryption of Text. | | | Practical, F2F | | 3 PH |  |
| Practical Two: Encryption of Sound | | | Practical, F2F | | 3 PH |  |
| Practical Three: Encryption of Images | | | Practical, F2F | | 3 PH |  |
| Secure Operating Systems.   * Data Exchange Prevention * Address Space Layout Randomization (ASLR) * Structured Exception Handler Overwrite Protection (SEHOP). * User Account Control (UAC). * DNS System Security Enhancements (DNSSEC) | | | Face-to-Face,  Practical,  Online. | | 4 | 05 |
| Mid Term Assessment. | | |  | |  | 06 |
| Security Architecture.   * Bit Locker * Improved Cryptography. | | | Face-to-Face,  Practical,  Online. | | 4 | 07 |
| Security by Design.   * Designing Secure Operating Systems. * Controls to enforce security services. * Information Security Models. | | | Face-to-Face,  Practical,  Online. | | 4 | 08-09 |
| Secure Coding (Software Security).   * Malicious Code. * Worms * Intruders * Error Detection and Correction. * OS Protection Policies. | | | Face-to-Face,  Practical,  Online. | | 8 | 10-11 |
| Access Control Lists.   * ACLs Types. * Placement of ACLs * Create and apply named ACLs. * ACLs types. * Placement of ACLs * Create and applying named ACLs. | | | Face-to-Face,  Practical,  Online. | | 8 | 12-13 |
| Security Applications.   * Keepas * Veracrypt * Windows 10 Shareware * Bit Locker * AxCrypt | | | Face-to-Face,  Practical,  Online. | | 8-45 | 14-15 |
| Course Project. | | | Face-to-Face,  Practical,  Online. | | 17. |  |
| Final Examination | | | Face-to-Face,  Practical. | | 3 Hours | 16-17 |
| **Total** | | |  | | **62** |  |
| 1. **Summary of time needed/mode of instruction** | | | | | | |
| Contact hours | | 60 | | | | |
| Lecture hours  Tutorial hours  Practical hours | | 20  20  20 | | | | |
| Total | | 60 | | | | |
| 1. **Tools needed/teaching aid**   A computer with the following software installed: o Python 3.4.3 or later o Anaconda Distribution o Git o GitHub Desktop | | | | | | |
| 1. **Course Evaluation** | | | | | | |
| Practical Exercises | | | | 20% | | |
| Continuous Assessment (assignments and test) | | | | 20% | | |
| End of Semester Written Examination | | | | 60% | | |
| 1. **Reference Materials** 2. Rose J. Anderson (2001). Security Engineering: A guide to building | | | | | | |