Syllabus

CYB 201 – Fundamentals of Cyber Security II (2 Units LH 15; TH 15)

Department of Cyber Security

Faculty of Computing

University of Delta, Agbor, Nigeria

Lecturer: Ms N. Isitor

Office Location: FOC Room 13

Email: nkechi.isitor123@gmail.com

Phone: 08109980934

Office Hours: Monday, Wednesday, Thursday; 10:00am – 2:00pm

There are many ways to reach me but I strongly encourage you to take advantage of my Office hours. Questions during class or immediately after class are always welcomed.

Meeting Time and Place: Friday, 08:00am to 10:00am.

Attendance

You are expected to attend every class. If you must miss a class, it is your responsibility to make up for the work that you missed.

Methods of Instruction

This syllabus contains an overview of what will be covered in class; for specific information, students are referred to the class web page maintained on the University website. Assignments will be given in class or posted on University of Delta LMS.

Overview

The Cyber Security fundamentals course trains you in developing and implementing security solutions for small and large organizations, protecting systems and network infrastructures. The IT Security Fundamentals skill path includes an understanding of computer hardware, software, and network security. Cybersecurity refers to protecting systems, networks, programs, devices, and data from cyber-attacks using technologies, processes, and controls. The basic cybersecurity concepts involve reducing cyber-attack risks and preventing unauthorized access to systems, networks, and technologies.

Objectives

The objectives of this course are to: (i) Introduce students to the basic concepts of operating system protection mechanism; (ii) Provide understanding of the main issues related to security in modern networked computer systems and IT infrastructure; (iii) Provide fundamental cryptographic concepts like encryption and signatures; (iv) Provide basic concepts of vulnerability assessment and penetration testing; (v) Discuss Government regulation of information technology; (vi) Describe denial of service and other attack strategies.

Learning Outcomes

Upon completion of this course, students should be able to: (i) Protect and defend computer systems and networks from cybersecurity attacks; (ii) Effectively communicate in a professional setting to address information security issues; (iii) Analyze and evaluate the cyber security needs of an organization; (iv) mplement cyber security solutions; (v) Measure the performance and troubleshoot cyber security systems

Course Contents

Operating system protection mechanisms, intrusion detection systems, formal models of security, cryptography, Steganography, network and distributed system security, denial of service (and other) attack strategies, worms, viruses, transfer of funds/value across networks, electronic voting, secure applications, homeland cybersecurity policy, and government regulation of information technology.

Week	Content	Lecture notes/slide
1	Operating System Protection Mechanism	Lecture note
2	Intrusion Detection Systems	✓
3	Formal Models of security	✓
4	Cryptography, Steganography	✓
5	Network and Distributed System Security	✓
6	Denial of Service and other Attack Strategies, worms, Viruses.	✓
7	Transfer of funds / values across networks.	✓
8	Electronic Voting, Secure Applications	✓
9	Test	
10	Homeland Cybersecurity Policy	✓
11	Government Regulation of Information Technology	✓
12	Revision	
13	Revision	
14	Revision	
15	Final Exams	

Examination schedule

- Attendance
- Homework
- Class Test
- End of Semester Exam

Grading
Attendance: 10% of grade
Homework: 10% of grade
Class Test : 10% of grade
Final Exam: 70% of grade

Text and References

Jacob N.M. & Wanjola M.Y. (2017), A Review of Intrusion Detection Systems.
Landwehr C.E. (2007), Formal Models for Computer Security.
Harrison M.A., Ruzzo .W.L. & Uilman J. D. (2017), On Protection in Operating Systems.

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behaviour conducive to a positive learning environment. The code of student conduct is described in detail in the student handbook or University website.

Academic Honesty

"All students enrolled at the University shall follow the tenets of common decency and acceptable behaviour conducive to a positive learning environment". It is the policy of the University, that no form of plagiarism or cheating will be tolerated. Plagiarism is defined as the deliberate use of another's work and claiming it as one's own. This means ideas as well as text or code, whether paraphrased or presented verbatim (word-for-word). Cheating is defined as obtaining unauthorised assistance on any assignments. Proper citation of sources must always be utilised thoroughly and accurately. If you are caught sharing or using other people's work in this class, you will receive a 0 grade and a warning on the first instance. A Subsequent instance will result in receiving an F grade for the course, and possible disciplinary proceedings. If you are unclear about what constitutes academic dishonesty, ask.