Internetwork Security

- **Course number and name:**

CC 535 – Internetwork Security

- **Credits and contact hours**

Credits Hours: 3Hrs
Contact Hours: In Lecture 2Hrs, and In Tutorial 2Hrs

- **Instructor's or course coordinator's name**

Coordinator Name: Dr. Rowayda Sadek

- **Text book, title, author, and year**
  - McClure, Scambray, and Kurtz, "Hacking Exposed", McGraw-Hill, latest edition.

- **Specific course information**
  - **a. Catalog description**

    Hacking and the Law, Network Mapping, Vulnerability Assessment, Network Mapping tools, Vulnerability Scanners, Sniffing, Defenses, Denial of Service Techniques using address spoofing, Man-in-the-middle, Defenses, Stack-Based Buffer Overflow Attacks and Password Attacks and Cracker tools, Web Attacks, RootKits, Trojans and Backdoors, Intrusion Detection tools, Writing new intrusion detection signatures, HoneyNets, Forensics.
  - **b. prerequisites or co-requisites**

    Prerequisites: CC431
  - **c. Types of Course (required, elective, or selected elective course) in the program**

    Elective Course

- **Specific goals for the course**
  - **a. Specific outcomes of instruction**

    After the completion of this course the students will be able to:

	Course Learning Outcomes	SO
1	Have hands on experimentation and evaluation of Internet Security theory, principles, and practices.	B,H
2	Perform ethical hacking and access the security of networks and computer systems.	F,K

Topics to be covered

- Legal and Moral Responsibilities
- Network Reconnaissance Techniques
- IP Address Spoofing
- Gaining Access
- Maintaining Access
- Intrusion Detection
- Firewalls
- Wireless Networks Security
- Worms and Viruses
- Virtual Private networks
- Web Servers Security
- Ethical Hacking
- Overall Computer and Network Security Assessment