

Course Description:

The nature of a seminar course is to explore areas of interest common to both the students and the instructor. The explorations are designed to help the students grow toward specific goals. Computer Seminar is an advanced level computer science course designed to allow students to explore advanced topics.

This semester, the course will introduce students to the following: Linux and Cyber Security. The first part of the course will introduce the students to the UNIX/LINUX family of operating systems. This general overview of the Linux operating systems will include topics such as the LINUX user environment, basic commands, file system, processes, and utilities, as well as UNIX/LINUX history and philosophy. Specific emphasis will be given to the bash shell and the user environment. The second part of the course will introduce the students to the foundations of security, basic procedures of security, desktop, network, and information security, administering windows security, security threats and attacks, incident response, secure Internet access, working securely on the Internet and working with VMWare, and VMWare tools. Students will examine the impact of cyber security issues on the implementation of the SDGs. Students' learning will take place through exploration and presentations.

INSTRUCTOR(S):

- Name(s): Namrata Pandya
- Office Number(s) (When and where you are available for help.): A157
9:00 am – 10:00 am
- Telephone number(s): 630-907-5965
- Email address(es): npandya@imsa.edu

Meeting Days, Time and Room(s)

2:20pm – 4:00pm in A152 on AC days

Text(s) / Materials:

There is no required text for this course. A number of online resources will be used extensively and handouts will be provided for reading material.

Teaching and Learning Methodology and Philosophy:

The teaching and learning philosophy in this course is to expose students to a variety of concepts, ideas and problem-solving strategies, which are developed and extended through reading, class discussion and interactive exploration. The course is intended to prepare students to work independently on advanced projects. Much of the learning is expected to take place

through class exercises, students creating and delivering lessons which act as stepping stones to concept development and subsequent growth in computer science.

Student Expectations:

All students are expected to

- be involved in class discussions and explorations, both large and small group.
- attend all the classes and be on time.
- complete all daily assignments, and projects in a timely manner.
- take responsibility for learning certain basic skills and relationships.
- take responsibility for seeking additional help as it is needed.
- collaborate with each other and contribute to each other's learning
- follow the guidelines of Students Handbook about ethical behavior and plagiarism.

Student Outcomes/Objectives:

At the end of this course, students will be expected to be able to:

LINUX:

- Know the history and philosophy behind Linux
- Use basic Linux commands from the command line (from a terminal window)
- Organize and manage the files within the Linux file system
- Organize and manage the processes within Linux
- Use a command line text editor
- Use command line manual pages to learn the syntax of commands
- Be knowledgeable enough about basic shell scripting to be able to successfully read and write bash shell scripts
- Know how to use the resources to find additional information about Linux commands

Cyber Security:

- define essential terminology for cyber security and be able to identify cyber crime
- understand the legal, ethical, and professional issues in cyber security
- learn about the current threats in cyber security
- understand security procedures to secure a desktop, or a network
- learn about security technology: Firewalls, VPNs, and wireless
- recognize various threats and attacks
- restrict site access and identify secure sites
- install and work with VMWare tools
- examine the impact of the security issues on implementation of the SDGs

Topics to be covered: (subject to change)

Week 1-2: Installing Linux and setting up username and password. History and philosophy of UNIX/Linux. Multiple users and permissions and Linux directory structure. Finding your way around files and folders

Week 3-4: System security and various UNIX/Linux distributions. The structure of commands, file system navigation and listing directories. Using command line text editor. Getting familiar with the terminal environment

Week 5-6: Writing and executing the shell script. Shell variables and shell commands.
Network operations

Week 7: Work on the quarter project

Week 8-9: Fundamentals of Security, Some security history, How to harden security, Creating strong passwords, Computer security, Information security, Network security

Week 10-11: Current cyber-attacks, ever present threats and attacks, web attacks and Internet vulnerabilities, incident response, security scenarios, Virtual machine

Week 12-13: SQL injections, Man-in-the-middle attacks, DDOS attacks, VPN, Password hacking, Network traffic, Cryptography and Steganography

Week 14: Forensics challenges and VMWare tools

Week 15-16: Impact of security issues on SDGs. Quarter Project and/or research paper

Quarterly grades will be averaged using the following weighting:

Projects/Presentations	40%
Quizzes/Labs	30%
Exercises/Assignments	25%
Participation/Organization	5%

Semester grades will be averaged using the following weighting:

Cumulative semester work	90%
Semester Final Exam/Research Paper	10%