

**University of Computer Studies, Yangon**  
**Faculty of Information Science**  
**2019-2020 Academic Year**

<b>Subject Code</b>	CS-503	<b>Course Title</b>	Information Assurance and Security
<b>credit</b>	3	<b>Course Coordinator</b>	Dr. Nyein Myint Myint Aung Lecturer
<b>Semester hours</b>	37.5 Hours		
<b>Period</b>	30 Periods (2 Periods per week/1period-75mins)		
<b>Semester</b>	First Semester		

### **Course Description**

This course aims to motivate the topic of information security for final year students. After completing the detailed look at the basic components of general information security mode, this course is focused on helping students acquired the skills sought in the professional workforce. At the outset, system administration introduces the basics setup and usage of the virtual machine (distribution of the CentOS

Linux OS to be installed as a virtual machine using virtual box). The instructions are detailed enough for students to be able to complete the exercises on their own. After this, the fundamentals of encryption technologies are described as security control. The rest of the course is devoted to how to identify and manage their privileges in enterprise systems and what are the most essential and best known controls.

Finally, the course wrap up many of the concepts and ideas reviewed in the past chapters into the narrative of an incident via incident handling and incident analysis. Finally, the course will also step away the students from the technical world and discuss administrative mechanisms (policies, standards and guidelines) available to security analysts and system administrators. At the end of the course, students will have an awareness of how information security concerns have evolved in our society and how they can use contemporary frameworks to respond to these concerns in a professional environment.

The book comes with a full set of end-of-chapter exercises. There are four kinds of exercises at the end of every chapter:

1. Traditional end of chapter questions are designed to improve student understanding and recall of common topics in information security.
2. An example case at the end of each chapter allows students to apply the knowledge in the chapter to business contexts.
3. A critical thinking exercise introduces students to analogous situations and relates the ideas from the chapter to these situations.
4. Finally each chapter has a detailed hands-on activity using a customized distribution of the CentOS Linux OS to be installed as a virtual machine using virtual box.

### **Learning Outcomes**

Students who complete the course will be able to

- Understand how information security and assurance is important and impact of organizations, and the importance of system administration for information security.
- Design, implement, test and debug a BASH shell script that uses each of the following fundamental programming construct and system administrative configurations: basic computation, simple I/O, standard conditional and iterative structures, methods and parameter

- passing and handling user interaction and the usage of common UNIX tools to parse and manipulate text files.
- Test and debug their script by: Developing test cases and output redirecting to discover their program's behavior.
  - Understand the standard, practical implementation of encryption technologies used in information exchange, and PKI infrastructure to make encryption convenient and practical. Understand the strengths and weaknesses of the major authentication technologies, and information security control best practices.
  - Identify the major components of dealing with an incident, the incident handling lifecycle. Prepare a basic policy outlining a methodology for the handling of an incident. Develop a better understanding on how to protect our information assets and defend against attacks, as well as how to apply these concepts practically.
  - Help to develop better security practices for any organizations in real world practice. Drive security projects and policies, in order to mitigate some of the issues which are usually encountered in any organization.

### **Prerequisites**

- Basic Information Security Model
- The fundamental concepts to information security and assurance.

### **Major Topic Covered in the Course**

- System Administration
- Encryption Controls
- Identity and Access Management
- Hardware and Software Controls
- Shell Scripting
- Incident Handling
- Incident Analysis
- Policies, Standards, and Guidelines
- IT Risk Analysis and Risk Management

### **Textbook**

- "INFORMATION SECURITY and IT RISK MANAGEMENT", 1st Edition, Wiley. Manish Agrawal, Alex Campoe and Eric Pierce, 2014

### **Reference Book**

- "INFORMATION SECURITY: The Complete Reference", 2nd Edition, McGraw Hill, Mark Rhodes-Ousley, 2013
- "Network Security : A Beginner's Guide", 3rd Edition, Eric Maiwald, ISBN:9780071785715, McGraw-Hill, 2013

## Learning Assessment

Paper Exam	:	60%
Tutorial Test	:	10%
Project	:	10%
Practical Assessment	:	10%
Assignment	:	5%
Class Participation	:	5%

## Team Project Description

The project topics can be choose from the following topics but not limited to:

1. SQL Injection
2. Password (Password hacking tools)
3. Network Scan
4. Intrusion Detection (Host-based intrusion detection system)
5. Cross-site scripting
6. Cross-site request forgery
7. Key logger
8. Social engineering (with scenario)
9. Packet sniffing
10. Network monitoring tools
11. Denial of service (DOS)
12. Phishing
13. Buffer overflow
14. Unrestricted Uploads
15. Vulnerability Assessment tools (OpenVas, Acunetix, Vega, etc.)
16. Shell script security
17. Pretty good privacy (pgp)
18. Secure emailing
19. Multi-factor authentication
20. Steganography (at least 5 different ways in demonstration)

**Presentation and demonstration** time is grant **20 minutes, questions and answers** session **10 minutes.**

To get started on your project, your assignment consists of the following tasks:

### Project Outlines

1. Title
2. Project Group Members
3. Resource Assignment of the tasks
4. Description
5. Objective & Motivation
6. Project Concerned Contents
7. Practical Demonstration

- 8. Counter-measures
- 9. Conclusion

### Course Policy

Attendance is not mandatory but highly recommended.

- Individual deliverables are to be submitted individually and group work is collaborative.
- All exams and assignments are to be completed by the student alone with no help from any other person.
- Students are allowed to discuss about homework and project problems with others.
- Students are not allowed to copy the solutions from another colleague.
- If so, all students (with same answers) must be deducted 1% of their marks (assignment).
- If you hand in a late assignment, you must identify (1) how late this assignment is and (2) how many total slip days you have left.
- After you have used up your slip time, any assignment handed in late will be marked off 0.5% per day. That is, after 5 days, the mark must be zero.

## University of Computer Studies, Yangon

### B.C.Sc.(Fifth Year)

**CS-503 - Information Security and Assurance**

**Textbook - Information Security and IT Risk Management**

**by ManishAgrawal, Alex Campoe, Eric Pierce**

**Periods - 30 periods (15 periods for Lecture, 15 periods for Lab)**

No.	Chapter	Page	Period	Detailed Lecture
1.	<b>Chapter 3–System Administration</b>		3	<b>Practical Oriented</b>
	Overview, Operating system structure, The command-line interface, Files and directories Moving around the file system		1	Explain Details
	Listing files and directories, shell expansions		1	

	File management, viewing files, Searching for files			
	Access control and user management, Access control lists File ownership, Editing files Command-line user administration		1	Explain Details
<b>2.</b>	<b>Chapter 7 - Encryption Controls</b>	<b>176-206</b>	<b>2</b>	
	Encryption Basics Encryption Types Overview		1	Explain Details
	Example Case – Nation Technologies Chapter Review Questions Hands-On Activity (Encryption) Critical Thinking Exercise		1	<b>Assignment</b>  <b>Lab</b>  <b>Assignment</b>
<b>3.</b>	<b>Chapter 8 - Identity and Access Management</b>	<b>207-245</b>	<b>3</b>	
	Identity Management Access Management		1	Explain Details
	Authentication		1	Explain Details
	Example Case - Markus Hess Chapter Review Questions		1	<b>Assignment</b>
	Hands-On Activity (Two-factor authentication) Critical Thinking Exercise			<b>Lab</b>  <b>Assignment</b>
<b>4.</b>	<b>Chapter 9 - Hardware and Software Controls</b>	<b>251-275</b>	<b>4</b>	
	Access Control Firewall		1	Explain Details
	Intrusion Detection/Prevention Systems Patch Management for Operating Systems and		2	Explain Details

	Applications			
	Example Case - AirTight Networks Chapter Review Questions Hands-On Activity (OSSEC) Critical Thinking Exercise		1	<b>Assignment</b>  <b>Lab</b>  <b>Assignment</b>
<b>5.</b>	<b>Chapter 10 – Shell Scripting</b>	<b>277-304</b>	<b>8</b>	<b>Practical Oriented</b>
	Introduction Output Redirection Text Manipulation Variables		2	Explain Details
	Conditionals User Input Loop Put It All Together		2	Explain Details
	Hands-On Activity		4	<b>Lab</b>
<b>6.</b>	<b>Chapter 11 - Incident Handling</b>	<b>306-331</b>	<b>3</b>	
	Incidents Overview Incident Handling The disaster		2	Explain Details Explain Details Definition
	Example Case – on-campus piracy Chapter Review Questions Critical Thinking Exercise		1	<b>Assignment</b>  <b>Assignment</b>

<b>7.</b>	<b>Chapter 12 - Incident Analysis</b>	<b>333-358</b>	<b>2</b>	
	Log Analysis Event Criticality		1	<b>Lab</b>
	General Log Configuration and Maintenance Live Incident Response		1	
	Example Case - Backup Server Compromise Chapter Review Questions Critical Thinking Exercise			<b>Assignment</b>  <b>Assignment</b>
<b>8.</b>	<b>Chapter 13 - Policies, Standards and Guidelines</b>	<b>360-381</b>	<b>2</b>	
	Guiding Principles Key Policy Issues		2	
	Example Case - HB Gary Chapter Review Questions Critical Thinking Exercise			<b>Assignment</b>  <b>Assignment</b>
<b>9.</b>	<b>Chapter 14 – IT Risk Analysis and Risk Management</b>	<b>382-401</b>	<b>3</b>	
	Risk Management as a Component of Organizational Management The NIST 800-39 Framework Risk Assessment		2	
	Example Case - Online Marketplace Purchases Chapter Review Question		1	<b>Assignment</b>