Republic of the Philippines<br>
**SULTAN KUDARAT STATE UNIVERSITY**<br>
Isulan, Sultan Kudarat<br>
**College of Computer Studies**<br>
S.Y. 2024-2025

# IAS322

# Information Assurance and Security 2

2nd Semester

School Year 2024 – 2025

Prepared by:

KRISTINE MAE H. AMPAS, MIT

## UNIVERSITY VISION

A trailblazer in arts, science and technology in the region.

## UNIVERSITY MISSION

The University shall primarily provide advance instruction and professional training in Science and Technology, Agriculture, Fisheries, Education and other related field of study. It shall undertake research and extension services, and provide progressive leadership in its area specialization.

## UNIVERSITY GOAL

To produce graduates with excellent and dignity in arts, science na technology.

## UNIVERSITY OBJECTIVES

a. Enhance competency development, commitment, professionalism, unity and true spirit of service for public accountability, transparency and delivery of quality services;
b. Provide relevant programs and professional trainings that will respond to the development needs of the region;
c. Strengthen local and international collaborations and partnership for borderless programs;
d. Develop a research culture among faculty and students;
e. Develop and promote environmentally-sound and market-driven knowledge and technologies at par with international standards;
f. Promote research-based information and technologies for sustainable development;
g. Enhance resource generation and mobilization to sustain financial viability of the university.

**Program Objectives and its relationship to University Goals:**

| PROGRAM OBJECTIVES (PO) | OBJECTIVES | | | | | | |
|---|---|---|---|---|---|---|---|
| A graduate of BS in Information Technology can: | | | | | | | |
| a. Innovate technological concepts and ideas underpinning desired IT solutions; | **a** | **b** | **c** | **d** | **e** | **f** | **g** |
| b. Administer competently the computer networks, system development, software applications, hardware and maintenance; | / | / | / | / | / | / | / |
| c. Design industry-based applications, infrastructures and technologies that will promote the advancement and development of the community; | / | / | / | / | / | / | / |
| d. Adopt to various national and international industries standards in the practice of the profession; and; | / | / | / | / | / | / | / |
| e. Demonstrate professionalism in the social, environmental and legal aspects of Information Technology. | / | / | / | / | / | / | / |

2. **Course Code** : IAS322
3. **Course Title** : Information Assurance and Security 2
4. **Prerequisite** : Information Assurance and Security 1
5. **Credits** :3 UNITS

1. **Course Descriptions**

   This course will provide learners with advanced topics in cybersecurity, including network security, incident response, secure software development, penetration testing, and cloud security. Students will gain hands-on experience with tools like Kali Linux and Metasploit while learning to identify vulnerabilities, implement security measures, and manage risk in modern IT and cloud environments. The course prepares students to tackle complex security challenges and ensure business continuity through effective backup and recovery strategies.

### 6. Course Learning Outcomes and Relationship to Program Educational Objectives

| COURSE LEARNING OUTCOMES | PROGRAM OBJECTIVES | | | | |
|---|---|---|---|---|---|
| At the end of the semester, the students can: | | | | | |
| a. Apply advance security techniques to protect networked systems, cloud environments, and virtual infrastructures from emerging threats and vulnerabilities. | **a** | **b** | **c** | **d** | **e** |
| b. Conduct penetration testing and vulnerability assessments using tools such as Kali Linux, Metasploit, and Nmap, following ethical and structured methodologies | / | / | / | / | / |
| c. Develop and implement risk management strategies, security policies, and incident response plans | / | / | / | / | / |

### 7. Course Content

| Course Objectives, Topics, Time allotment | Desired Student Learning Outcomes | Outcomes-Based Assessment (OBA) Activities | Evidence of Outcomes | Course Objectives | Program Outcomes | Values Integration |
|---|---|---|---|---|---|---|
| **Topic: SKSU VMGO, Classroom Policies, Course Overview, Course Requirements, Grading System (2 hours)** | | | | | | |
| 1. Discuss the VMGO of the university, classroom policies, scope of the course, course requirements and grading system | 1.1 Student can be aware of and appreciate of the university's VMGO, classroom policies, course overview, | Individual participation in class discussion and group presentation | Individual participation in class discussion and group presentation | | | Value of appreciation |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  | requirements and grading system. |  |  |  |  |  |
| **1. Advanced Cryptography (lec:6hrs)** |  |  |  |  |  |  |
| 1.1 Public Key infrastructure (PKI)<br>1.2 Digital certificates and signatures<br>1.3 Hashing algorithms (SHA, HMAC)<br>1.4 Cryptographic protocols (SSL/TLS) | 1.1 Demonstrate the process of secure communication using PKI-based authentication encryption<br>1.2 Identify the different digital certificates and signature<br>1.3 Apply and compare hashing algorithms such as SHA and HMAC in verifying data integrity<br>1.4 Describe the functions and structure of cryptographic protocols | Discussion<br>Activities<br>Recitation | Recitation<br>Quizzes<br>Laboratory activity | a | a, d, e | Unity and team work<br>Value of participation<br>Communication<br>Challenge<br>Achievement |

| | | | | | | |
|---|---|---|---|---|---|---|
| **2. Network Security (lec:6hrs)** | | | | | | |
| 2.1 Firewalls and VPNs<br>2.2 Intrusion Detection and Prevention Systems (IDS/IPS)<br>2.3 Secure network design<br>2.4 Wi-fi security (WPA2-WPA3) | 2.1 Describe the functions and types of firewalls and VPNs<br>2.2 Differentiate between Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS)<br>2.3 Design a secure network architecture<br>2.4 Evaluate common Wi-Fi security protocols | Discussion<br>Review | Rubrics score cards of laboratory exercise output accomplished by the instructor | b, c, d | | Unity and team work<br>Value of participation<br>Communication<br>Challenge<br>Achievement |
| **3. Operating System Security (lec:6hrs)** | | | | | | |
| 3.1 Security Windows and Linux systems<br>3.2 User account management<br>3.3 System hardening and patch management | 3.1 Compare and implement basic security measures in Windows and Linux systems<br>3.2 Demonstrate effective user | Discussion<br>Recitation | Recitation<br>Quizzes<br>Laboratory activity | b, c, d | | Unity and team work<br>Value of participation<br>Communication<br>Challenge |

| | | | | | | |
|---|---|---|---|---|---|---|
| | account management<br>3.3 Apply system hardening techniques and patch management practices | | | | | Achievement |
| **4. Application Security (lec:3hrs)** | | | | | | |
| 4.1 Secure software development lifecycle (SDLC)<br>4.2 Common web vulnerabilities (XSS, SQL Injection, CSRF) | 4.1 Describe the stages of the Secure Software Development Lifecycle (SDLC)<br>4.2 Identify and explain common web vulnerabilities<br>4.3 Demonstrate basic techniques for preventing and mitigating web application vulnerabilities | Discussion<br>Recitation | Recitation<br>Quizzes<br>Laboratory activity | b, c, d, e | | Unity and team work<br>Value of participation<br>Communication<br>Challenge<br>Achievement |
| **5. Incident Responses and Handling (lec:3hrs)** | | | | | | |
| 5.1 Phases of incident response | 5.1 Describe the key phases of | Discussion<br>Recitation | Quizzes<br>Laboratory activity | b, c, d, e | | Unity and team work |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5.2 Forensics basics<br>5.3 Evidence handling and chain of custody | incident response<br>5.2 Explain fundamental digital forensics concepts<br>5.3 Demonstrate proper procedure for handling digital evidence | | | | | Value of participation<br>Communication<br>Challenge<br>Achievement |
| **6. Security Policies and Procedures (lec:3hrs)** | | | | | | |
| 6.1 Policy development and enforcement<br>6.2 Risk management and assessment<br>6.3 Security frameworks (ISO/IEC 27001, NIST) | 6.1 Develop and evaluate organizational security policies<br>6.2 Conduct risk assessments<br>6.3 Compare and apply major security frameworks such as ISO/IEC 27001 and NIST to guide the implementation of security protocols | Discussion<br>Activities<br>Recitation | Quizzes<br>Laboratory activity | b, c, d, e | | Unity and team work<br>Value of participation<br>Communication<br>Challenge<br>Achievement |

| | | | | | | |
|---|---|---|---|---|---|---|
| **7. Disaster Recovery and Business Continuity (lec:3hrs)** | | | | | | |
| 7.1 Backup strategies<br>7.2 Business Impact Analysis (BIA)<br>7.3 Recovery Time Objective (RTO) & Recovery Point Objective (RPO) | 7.1 Design and implement effective backup strategies<br>7.2 Conduct a Business Impact Analysis (BIA)<br>7.3 Define and calculate Recovery Time Objective (RTO) and Recovery Point Objective (RPO) | Discussion<br>Recitation | Quizzes<br>Laboratory activity | b, c, d, e | | Unity and team work<br>Value of participation<br>Communication<br>Challenge<br>Achievement |
| **8. Ethical Hacking and Penetration Testing (lec:3hrs)** | | | | | | |
| 8.1 Tools (Kali Linux, Metasploit, Nmap)<br>8.2 Pen testing methodology<br>8.3 Social engineering awareness | 8.1 Utilize penetration testing tools<br>8.2 Apply a structured penetration testing methodology<br>8.3 Recognize and defend against social | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | engineering attacks and understand the psychological principles behind common social engineering techniques. | | | | | |
| **9. Cloud and Virtualization Security (lec:3hrs)** | | | | | | |
| 9.1 Security in cloud computing environments<br>9.2 Virtual machine vulnerabilities<br>9.3 Cloud services models (IaaS, PaaS, SaaS) and their risks | 9.4 Security in cloud computing environments<br>9.5 Virtual machine vulnerabilities<br>9.6 Cloud services models (IaaS, PaaS, SaaS) and their risks | | | | | |
| **10. Legal, Ethical, and Professional Issues (lec:6hrs)** | | | | | | |
| 10.1 Cyberscrime Laws (Philippine Cyberscrime Prevention Act of 2012 -RA 10175 | 10.1 Identify and address security risks<br>10.2 Analyze virtual machine vulnerabilities | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 10.2 Intellectual property and privacy rights<br>10.3 Ethics in cybersecurity | 10.3 Understand the different cloud service models (IaaS, PaaS, SaaS) | | | | | |
| Examination (4 hours)<br>Lectures (42 hours)<br>**Total No. of Hours: 42 hours** | | | | | | |

## 7. Course Evaluation

**Course Requirement: Demonstrate Problem Solving skills in python programming language.**

**Grading System:**

**MIDTERM TERM**

Exam 40%
Attendance 10%
Assignment/Quizzes 15%
Laboratory Exercise/Project 35%

**FINAL TERM**

Exam 40%
Attendance 10%
Assignment/Quizzes 15%
Laboratory Exercise/Project 35%

**MTG+FTG/2=FG**

**Schedule of Examination**

| | |
|---|---|
| Midterm | - March 25-28, 2025 |
| Final Term | - May 20-23, 2025 |

## References:

### TextBooks:

1. Death, D. (2017). Computer and information security handbook. Birmingham: Packt Publishing
2. Supporting Learning Flow Through Integrative Technologies, Edited by,Tsukasa Hirashima, Urich Hoppe, Shelley Shwu-Ching Young
3. Combining Multiple Knowledge Representation Technologies into Agent Programming Languages, Mehdi M. Dastani, Koen V. Hindriks, Peter Novák, Nick A. M. Tinnemeier

### Supplemental:

1. https://content.sciendo.com/view/journals/rput/26/42/article-p127.xml
2. https://ascelibrary.org/doi/abs/10.1061/(ASCE)1527-6988(2008)9:2(61)
3. https://academic.oup.com/bioinformatics/article/36/3/982/5554700
4. https://www.igi-global.com/chapter/building-integrative-enterprise-knowledge-portals/24415

| | |
|---|---|
| Prepared by: | Reviewed by: |
| **KRISTINE MAE H. AMPAS, MIT** | **ESNEHARA P. BAGUNDANG, MSIT** |
| Faculty | Faculty Program Chairperson, BSIT |

Approved:

**ELBREN O. ANTONIO, DIT**

Dean, College of Computer Studies