

Secure Operating System Master of Science in Cybersecurity Orientation show

عرض توجيہی

Dr. Eng. : Hesham Abou Elfetouh Salman

Lecture 0 - Overview



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

www.midocean.ae

بسم الله الرحمن الرحيم

اللهم صلي و سلم و بارك على اشرف المرسلين سيدنا محمد و على آله وأصحابه أفضل التسليم
يسعدني أن أرحب بكم ترحيبا خاصا في مستهل هذا الفصل الدراسي الجديد، الذي نتطلع فيه إلى المزيد من العمل
المثمر والجاد من أجل بلوغ الأهداف التي إجتمعنا من أجلها في هذا الصرح العلمي العظيم، راجيا من الله العلي
القدير أن يوفقنا جميعا لتأدية مهامنا الأكاديمية والإدارية والتربوية على الوجه الذي يحبه و يرضاه.

كل عام وأنتم بخير



• **Dr. Eng. : Hesham Abou Elfetouh Salman**

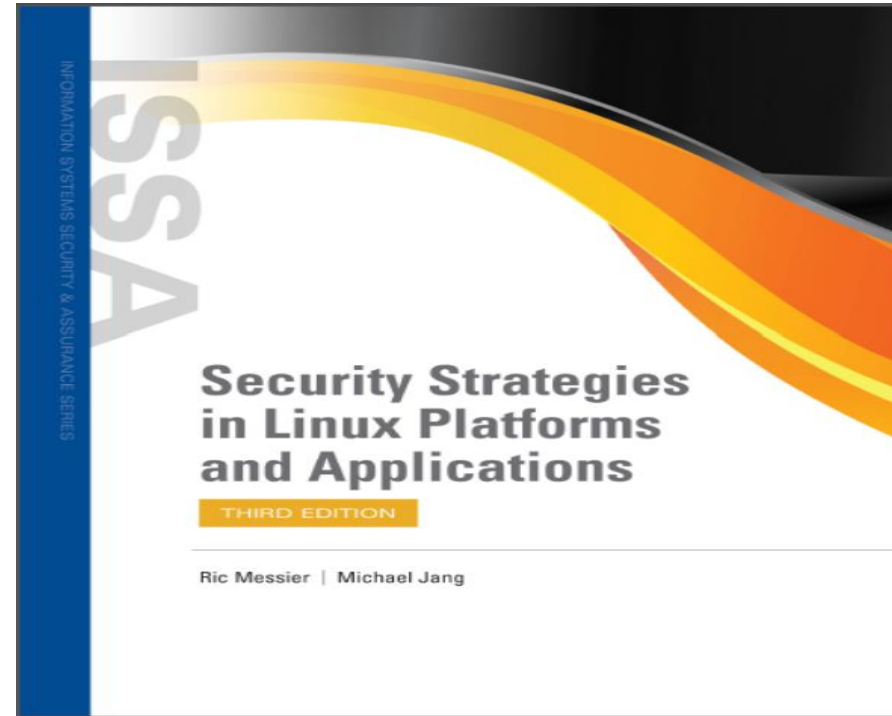
- **Doctor of Philosophy Ph.D.** , Department Of Computer Systems, Faculty Of Computer & Information Sciences, Ain Shams University.
- **Master Degree** of Computer Engineering, Engineering faculty of Ain shams university
- **Diploma In Information Systems Management**, Fort Gordon -Georgia - USA
- **B. S. c:** Bachelor of Computer Engineering , Military technical College.

- Higher Institute for Computers & Information Technology, Management Information system Dep. ElShorouk, Cairo, Egypt.
- Faculty of Computing and Information Technology, Information System Department, King Abdulaziz University.
- General Manager of the Technology Competency Centre, Ministry of Commerce and Industry, Cairo, Egypt.
- I have about 41 years of experience in the fields of network engineering, Data Base Centres and programming applications.
- I have publications in the area of networks, data mining, wire and mobile networks planning and network security.

- By email at hesham.salman@esu.ac.ae
(please include “Secure Operating Systems” in subject line)

❖Office hours

- Discussion Time (Monday at 9:00 PM) every Week



Introduction

- **In Previous Courses you learned:**
 - The concepts of computer security, cryptography, digital money, secure protocols, detection, and other security techniques.
 - The essential techniques in protecting information systems, IT infrastructure, analyzing and monitoring potential threats and attacks, devising security architecture, and implementing security solutions.
 - Various network technologies and cyber-attacks and their issues.

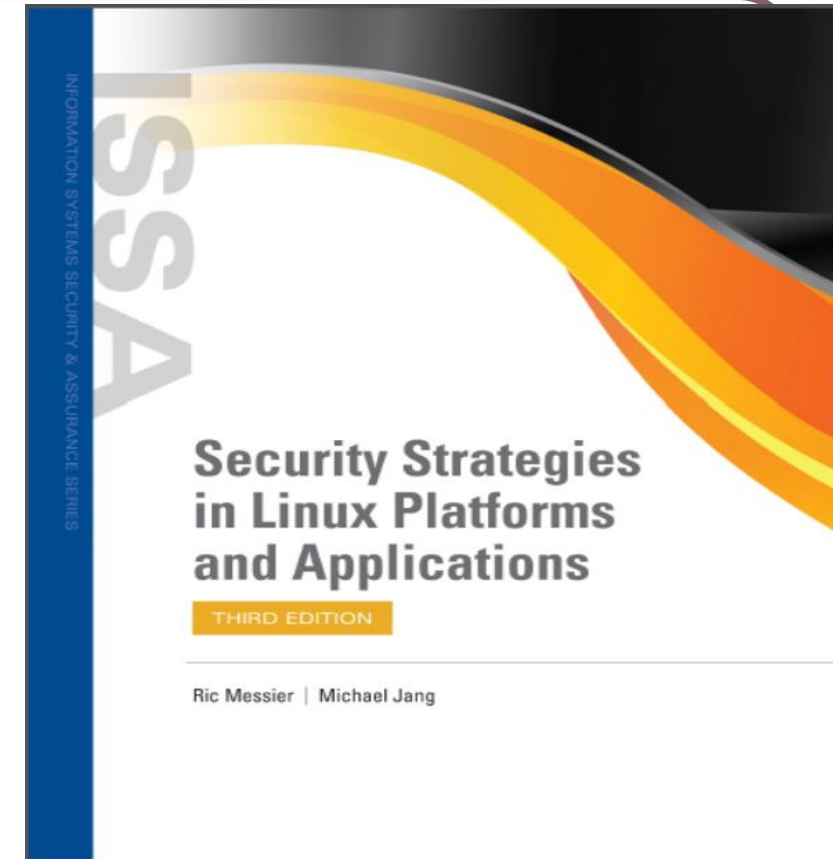
Introduction

- The origin of Malware, and its security.
- How to Identify & Evaluate vulnerabilities in information systems and apply security measures to real-time scenarios.
- Security Protocols for avoiding the basic level threat.
- The use of standards to enhance information security in the development process and infrastructure protection.
- Recognize the appropriate steps for information security risk, response, and recovery.
- Demonstrate the ability to assess and implement access controls.

➤ **Credit Hours:** 3 credit hours.

➤ **Required Textbook:**

- Jang M. and Messier R., “Security Strategies in Linux Platforms and Applications”, 2024, Jones and Bartlett Learning, ISBN 9781284255850



- In this course, you understand how hardware and software constructs protect modern operating systems.

Upon successful completion of this course, you should be able to:

- Explain what operating system and network security means.
- Explain how viruses, worms, and trojan horses spread.
- Explain encryption and authentication methods and how they are used.
- Create account naming and security strategies.
- Implement directory, folder, and file security.

- Configure the firewall capabilities in operating systems.
- Explain physical security methods for workstations, servers, and network devices.
- Configure security for wireless interfaces in workstation operating systems.
- Explain how e-mail can be secured through certificates and encryption.
- Explain how to use disaster recovery techniques to secure operating systems, prevent data loss, and reduce downtime.

- Module 1: Introduction, and an overview about OS Security Threats and basic components of OS Security.
- Module 2: User privileges, Permissions and Files systems and encryption.
- Module 3: Securing services.
- Module 4: Firewalls, Remote Access, Secure NAS.

- Module 5: Network application security.
- Module 6: Managing security alerts and updates.
- Module 7: Detecting and responding to security breaches.

➤ Assessment Method:

• Short Exam

- 80% marks
 - Count of short Exam 10 (Weekly)
 - 8 Marks for every each of short Exam.
- 20% Final Examination



الفترة الزمنية التعليمية في
الفصل الدراسي مدتها
١٣ أسبوع
(منهم أسبوع للاختبار
النهائي)

