

Secure Operating Systems (CYB610)

Master of Science in Cybersecurity



Dr. Ibrahim Gomaa

Faculty of Informatics
Midocean University



Lecture-Intro

Dr. Ibrahim Gomaa



Assistant Prof.
Midocean Univ., UAE



Information Security
Network Security
Cloud Security
Internet of Things
Blockchain Technology



<https://www.linkedin.com/in/ibrahim-gomaa-366b3371/>

Certified Trainer (ToT)



Secure Operating Systems (CYB610)

The course that will be taught



Secure Operating Systems



A brief about OS



- **Operating System** is a software, that manages all hardware resources associated with the computer.
- Generally, Operating System is comprised of number of pieces such as
 - ✓ the Boot loader,
 - ✓ the Kernel,
 - ✓ Daemons,
 - ✓ Desktop environment and
 - ✓ Applications.
- Typically, OS is deployed in any system when **multi-tasking** required to be performed, which is achieved by resource management functionality of the OS.
- Along with that, the user also requires interface with the system to interact and invoke various applications. In modern day OS, these interfaces (**popularly known as GUI**) are expected to provide best-in-class User Experience (UX) to the users, by making it easy to use the system.



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.
- The origin of Malware, and its security.



In Previous Courses you learned:

- 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.

Primary Goal of This Course



In this course,

- The goal is to gain an understanding of how **hardware** and **software** constructs **protect** modern **operating systems**.

Units of Course Contents



Module	Course Unit
1	Module 1: Introduction, and an overview about OS Security Threats and basic components of OS Security.
2	Module 2: User privileges, Permissions and Files systems and encryption.
3	Module 3: Securing services.
4	Module 4: Firewalls, Remote Access, Secure Network-attached storage (NAS).
5	Module 5: Network application security.
6	Module 6: Managing security alerts and updates.
7	Module 7: Detecting and responding to security breaches.

Teaching Methodology



Recorded Lectures

المحاضرات المسجلة

Live Sessions

جلسات وحلقات النقاش

Virtual Labs

المعامل الافتراضية

References

المراجع المعتمدة للمقرر الدراسي

منهجية التدريس

Study System



يتم احتساب الغياب من خلال حل الطالب للاختبار القصير المصاحب للمحاضرة الأسبوعية المسجلة، وفي حال تغيب الطالب عن 4 اختبارات قصيرة يعتبر الطالب في هذه الحالة حرمان.

آخر موعد للاعتذار عن أي اختبار قصير يكون قبل إغلاق موعد الاختبار مع إرفاق الدلائل الثبوتية لأي أعذار قهرية أو مرضية عبر نموذج الأعذار عن اختبار قصير عبر منصة (SIS).

آخر موعد للاعتذار عن الاختبار النهائي يكون قبل موعد عقد الاختبار مع إرفاق الدلائل الثبوتية لأي عذر قهري أو طبي عبر نموذج الأعذار عن اختبار نهائي عبر منصة (SIS)، ولن يتم احتساب أي أعذار بعد نهاية الموعد، ويحق لإدارة الجامعة مراعاة بعض الظروف القهرية.

www.midocean.ae

الأعمال وتوزيع درجات الفصل الدراسي الثالث 2023 - لمرحلي البكالوريوس والماجستير

توزيع الدرجات - 100%

حضور المحاضرة - حل الأسئلة المصاحبة

8 درجات لكل اختبار قصير -
بمجموع 80 %

الحضور اختياري

20%

الأعمال

محاضرة مسجلة أسبوعيًا -
السبت من كل أسبوع

اختبار قصير مصاحب للمحاضرة
بشكل أسبوعي

حلقة نقاش افتراضية أسبوعية
لمناقشة محتوى المحاضرة المسجلة

الاختبار النهائي



➤ Assessment Method:

▶ Short Exam

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



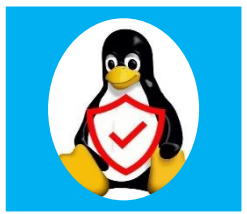
Learning Outcomes



After completion of this course, the students 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.

Learning Resources:



➤ **Credit Hours:**

3 credit hours.

➤ **References:**

- 1- Jang M. and Messier R., “Security Strategies in Linux Platforms and Applications”, 2024, Jones and Bartlett Learning, ISBN 9781284255850.
- 2- Trent Jaeger, Operating System Security. Synthesis Lectures on Information Security, Privacy, and Trust, Springer International Publishing 2022, ISBN 978-3-031-01205-1.





Thank You