CS 281 INTRODUCTION TO CRYPTOGRAPHY AND COMPUTER SECURITY
IES Abroad Madrid

DESCRIPTION:
Fundamental introduction to the broad area of computer security. Topics will include fundamentals of cryptography, network security, operating system security, and common vulnerabilities in computer systems.

CREDITS: 4 credits

CONTACT HOURS: 60 hours

LANGUAGE OF INSTRUCTION: English

PREREQUISITES: Data structures, Programming principles, and Computer Ethics/Philosophy (recommended)

ADDITIONAL COST: None

METHOD OF PRESENTATION:
This course will be presented in modules; each module discusses a topic in computer security. Lectures, labs, assignments, in-class activities will be used as teaching and learning tools.

REQUIRED WORK AND FORM OF ASSESSMENT:

- Final exam- 30%
- Midterm exam - 20%
- Quizzes & In-Class Activities - 20%
- Assignments - 20%
- Attendance and Participation - 10%

All class activities and quizzes must be submitted during the class session. Late submissions will receive a grade of zero.
Assignments must be submitted before the specified deadline. Late submissions will incur the following penalties:

- 10% penalty for submissions within 24 hours of the deadline.
- 20% penalty for submissions within 48 hours of the deadline.
- 30% penalty for submissions within 72 hours of the deadline.
- Assignments submitted more than 3 days after the deadline will receive a grade of zero.

Course Element

1. **Introduction to Security Concepts:**
    - Overview of course rules, evaluation methods, and basic security concepts.
2. **Threat Models:**
    - Challenges in security, including policy, threat models, and mechanisms.
3. **Encryption Systems:**
    - **Symmetric Key Encryption:** Study of classic encryption systems.
    - **Asymmetric Key Encryption:** Exploration of public and private key encryption methods.
    - **Post-Quantum Encryption Methods:** Analysis of the vulnerabilities in current encryption algorithms and an introduction to quantum-resistant cryptographic techniques.
4. **Linux for Computer Security:**
    - Introduction to Linux commands and their applications in security.
5. **Buffer Overflow Attacks:**
    - Understanding device structure, CPU, RAM, stack, and how to exploit buffer overflow vulnerabilities.
6. **Web Vulnerabilities & Security:**
    - Exploration of web design vulnerabilities, ethical hacking, and penetration testing.
7. **Network Security:**
    - Detailed study of network layers, associated vulnerabilities, and security protocols.
8. **Proxy & VPN:**
    - Understanding the functionality and differences between proxies and VPNs.
9. **Machine Learning and AI for Network Security**
    - An overview of recent advancements in research methods and algorithms within the field.

LEARNING OUTCOMES:

By the end of the course, students will be able to:

1. Describe detailed features of fundamental computer security concepts.
2. Describe network security designs which are commonly used in organizations.
3. Be familiar with fundamentals of cryptography, including private and public key cryptography.
4. Have knowledge with the network security threats and countermeasures, including common attacks and defensive strategies.
5. Understand security within and Software-Defined Networking (SDN), including common attacks and defensive strategies.
6. Recognize common vulnerabilities on various operating systems, web applications and can compare and contrast various features provided on popular operating systems.
7. Explain common vulnerabilities in programs, such as buffer overflows and lack of input sanitization.

ATTENDANCE POLICY:

As a member of our class community, you are expected to be present and on time every day. Attending class has an impact on your learning and academic success. For this reason, attendance is **mandatory for all IES Madrid classes**, including course-related excursions. Absences will only be excused in cases of documented medical or family emergencies. Any assessed work, including exams, tests, and presentations, will be rescheduled if the absence is justified; otherwise, it will be graded as 0. You are allowed a maximum of 1 unexcused absence for once-a-week courses and 2 unexcused absences for twice-a-week courses. Each additional absence will deduct 5 points from your final grade. **Accumulating 7 or more absences in twice-a-week courses, or 4 or more in once-a-week courses, may lead to a failing grade.** Students arriving more than 11 minutes after the scheduled start time will be marked as 'late.' Three 'late' arrivals will be counted as 1 absence. Any student arriving 30 minutes or more after the scheduled start time will be marked as 'absent.' For more information, please refer to the full Attendance and Punctuality Policy document.

CONTENT:

Session	Content	Assignments
Session1	**Class Intro and Intro to Security Concepts** • To introduce course rules syllabus evaluation methods, the aim of this course and security concepts.	Reading assignment: • vulnerabilities & • essay: Ransomware protection: How to keep your data safe in 2023)
Session2	**Threat Models** • Why is security hard? • Problems with security policy & solutions • Problems with treat model (assumptions) & solutions. • Problems with the mechanism (bugs) and & solutions.	**Reading**: Threat Modeling
Session3	**Encryption System- I** • This module we will study the classic encryption systems and symmetric key encryption methods and applications.	**Assignement1**: implementing classic encryption
Session5	**Encryption System- I** • Cryptanalysis of symmetric key encryption.	**Class activity**- Cryptanalysis
Session6	**Encryption System- II** • Asymmetric key encryption will be covered in this module.	
Session7	**Encryption System- II** • Hands-on DES	**Assignment (2)-** DES encryption Algorithm
Session8	**Encryption System- II** • RSA encryption	
Session9	**Post Quantum Computing Cryptography** • The Post-Quantum Threat • Evaluation of Encryption Algorithms in the Context of Post-Quantum Cryptography	**Reading** /presentation **Assigning Midterm Project**
Session10	**Introduction to Linux I** • Hands-on Linux command	**Lab1**- introduction to Linux commands
Session11	**Introduction to Linux II** • Kali Linux for Penetration test	**Lab2**- Linux for computer security.
Session12	**Buffer Overflow attack** • Background on devise structure • CPU, Registers, RAM, and stack. • How to use tools to read registers, RAM and stack content.	**Lab3**- understands the RAM, Stack, Register and how to read the content.
Session13	**Buffer Overflow Exploits and Defense** • How to use tools to read registers, RAM and stack content.	**Lab4**- Implementing exploit

Session	Content	Assignments
Session14	**Web Vulnerabilities & Security** • Web design and structure. • Threat and vulnerabilities on web app structure.	**Lab5**- Hand-on web design.
Session15	**Web Vulnerabilities & Security** • Use ethical hacking references and tools to implement XXS attack and penetration test.	**Lab6**- Practicing penetration test (XSS-Attacks).
Session17	**Network Security-I** • Introduction to network structure • Network protocols and vulnerabilities	**Lab7**- Hands-on Client-Server communication, Implementing DoS attack, and mitigation.
Session18	**Network Security-II** • Hands-on Network testing, and information gathering	**Lab8** Testing network connection, using sniffing tools (e.g., Linux Commands, Wireshark).
Session19	**Network Security-III** • Hands-on advanced information gathering tools, and how use gathered information for hacking.	
Session20	**Network Security-IV** • Social engineering attacks- Spoof email	**Assignment6**- Information gathering advanced tools, and spoofing attack.
Session21	**Proxy & VPN** • Understand how each of them works. • To know the differences between them.	
Session 22	**Machine Learning and AI for network security** • Review the current methods and Algorithms	Reading and Presentation
Session 23	Reading and Presentation	
Session20	Reading and Presentation	

COURSE-RELATED TRIPS:

- None

REQUIRED READINGS:

- Course lecture notes.

REQUIRED TOOLS AND TECHNOLOGY:

- **Virtual Machine**: There are several free virtual machine options available. Feel free to choose the one that best fits your computer's specifications. For example, you may consider using VirtualBox.
- **Kali Linux Image**: Select a Kali Linux image that is compatible with the virtual machine you have chosen.

Please, be aware that it's impossible for the teachers to provide technical support for the installation in your own computer of the required tools or other related issues

RECOMMENDED READINGS:

- Kali Linux Penetration Testing – Bible. 1st edition by Gus Khawaja (Author)
- Hands-On Penetration Testing with Kali NetHunter