COMPUTER SECURITY
PRESENTATION

"APIs, scripts, inputs...too many hacks,
so little time..."

JOSÉ MANUEL REDONDO LÓPEZ *"S-81 ISAAC PERAL"* PROJECT V4.0

Source: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

WELCOME!

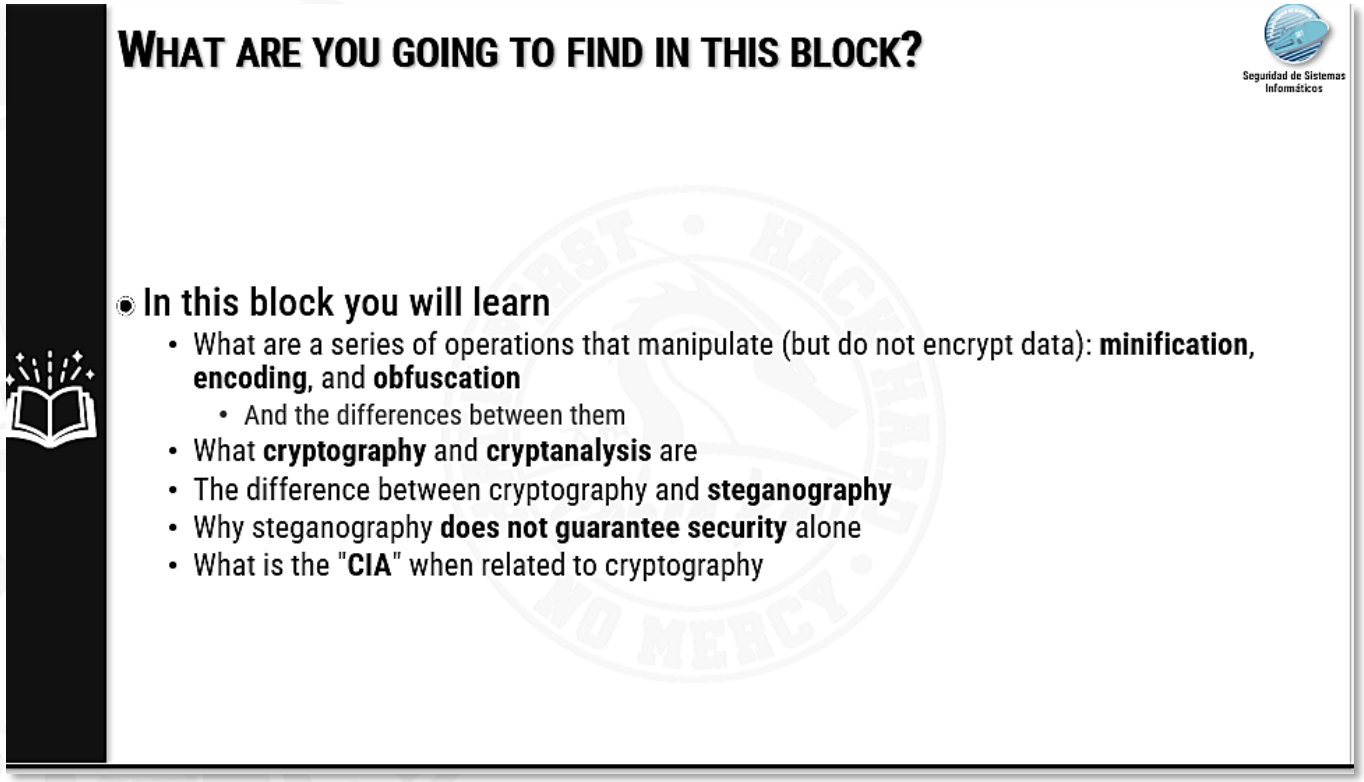
- Welcome to our **Computer Security** course!
- In this course we will try to make you understand and use **more than the basics** about different key aspects of the computer security field
  - Covering both threats…and defenses against the dark arts ☺
  - **With a zero-knowledge approach**: To the moon! ☺
- It is impossible to cover all the security concepts and sub-fields in just one course
  - However, it will be enough to get you started on all major ones!
- Ready? **GO!**

THEORY TOPICS

1. **Introduction**
   - Basic concepts to understand the rest of the course
2. **Cryptography Applications**
   - How to properly use cryptography to provide confidentiality, integrity and authentication
3. **OS Security**
   - Basic rules to manually harden operating systems
4. **Security Policies**
   - Overview of security policies and how to apply them to provide maximum hardening with a high degree of automation
5. **Perimeter and Network Security**
   - Firewalls, intrusion detection and prevention systems and other network security concepts
6. **Application Security**
   - Procedures to create secure software and validate input data
7. **Introduction to Red Team Operations: Exploiting and Privilege Scalation**
   - An introduction to exploiting and privilege scalation techniques with emphasis on CTF

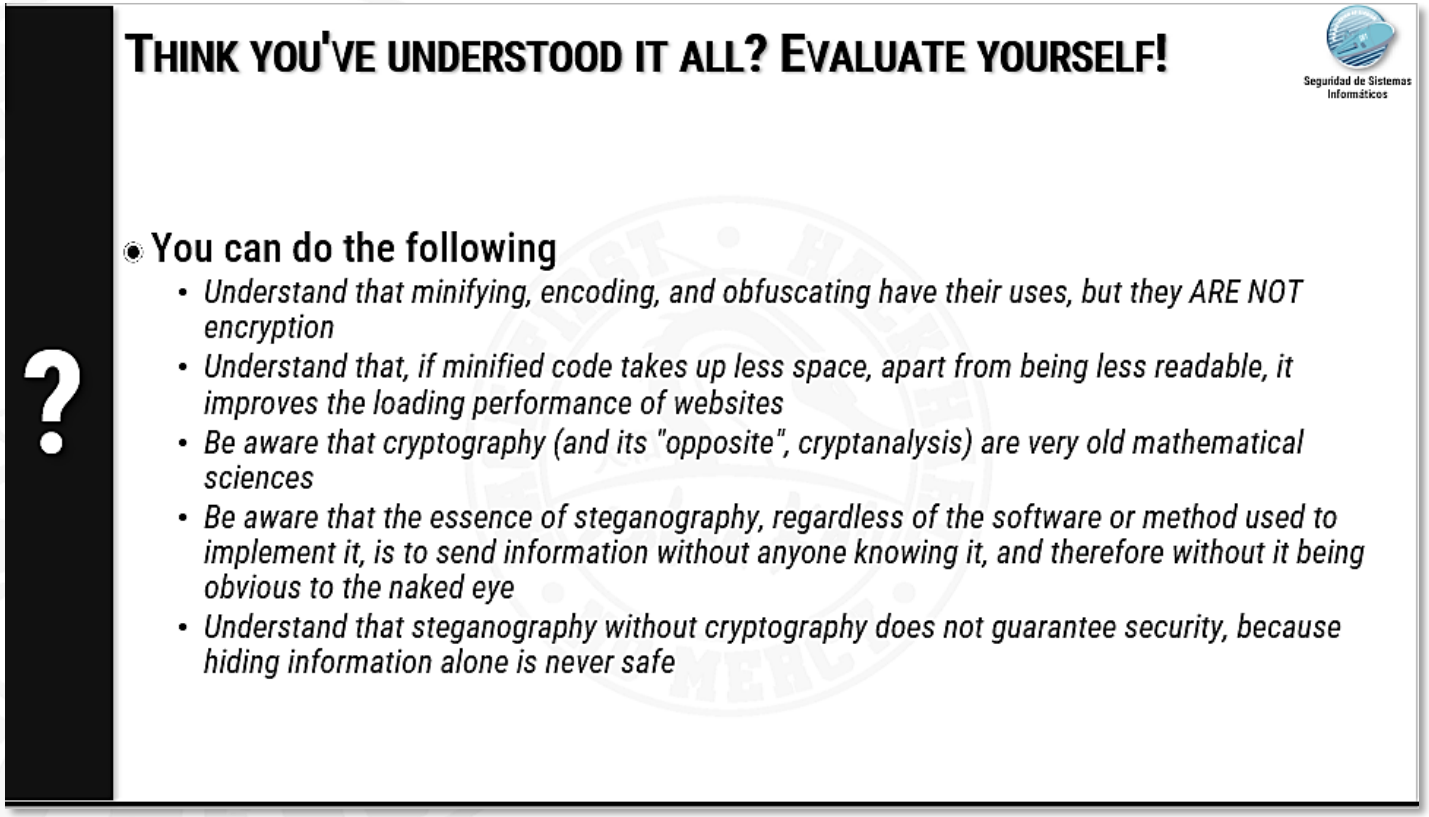
"Special" Slides: Slides with a book

- If you come across this type of slide, it is not evaluable material
  - It is content to help you study the course
- In this case, it is a small summary of the main concepts that are going to be taught in a section
  - It allows you to make quick searches and better structure what is studied in each part



"SPECIAL" SLIDES: SLIDES WITH A "?"

- This kind of transparency is also not assessable, but it helps you a lot with the evaluation
- It contains key questions that you should make sure you can answer to know that you have understood the contents of a section
- It's a mechanism for you to self-evaluate your own learning
  - The aim is to avoid "unpleasant surprises" in the exams ☺

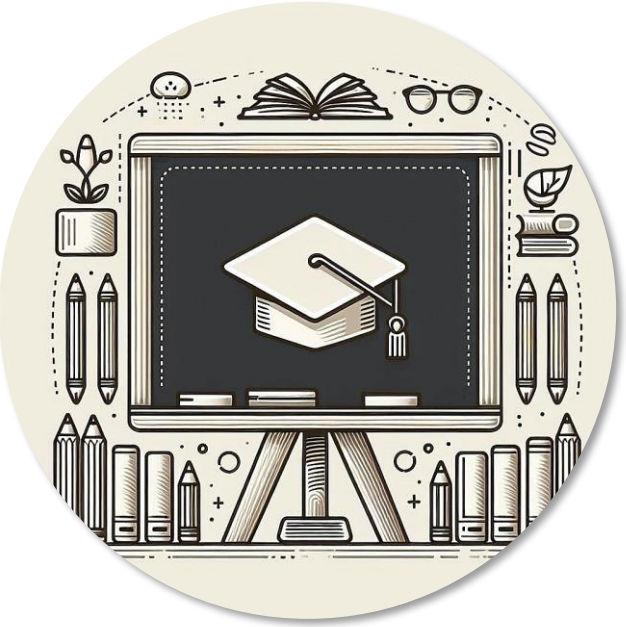


Seminar Topics

1. **Tools for Internet Research**
   - Current issues on security contexts and applications: tools for investigating them
2. **Physical Security**
   - A review on physical security procedures and methods
3. **Automated Vulnerability Scanning Tools**
   - Tools to automatically evaluate the security of remote systems
4. **Introduction to Reversing**
   - Brief introduction of executable analysis and “dissection”
5. **Input Validation**
   - Practical approaches to validate user inputs
6. **HTTP Headers and CSP**
   - State-of-the-art HTTP protocol security applications
7. **Write-up of a CTF machine**
   - Applying course concepts on a real CTF scenario

"Special" Slides: The "seminar" icon

- Theory is also integrated with seminars
- Seminars are more practical complements to the concepts of theory
  - As such, they are linked to the theory topics we will be teaching
- Although there may be previous mentions to a seminar, where its contents really fit is in the transparency where you see this icon
- In this way, you will know how they relate to each other within the syllabus of the course



Icon created with Bing Chat AI

Laboratory Topics

- "Lab 0": Creating your VM for the course
  - **Autonomous work to prepare for the rest of the course!**
  - **Follow the instructions of labs 00A and 00B as soon as possible!**

1. **System Setup**
   - Basic machine setup of the VM we are going to use in the labs
2. **OSINT and secure browsing**
   - Obtaining information about people and entities using public resources and how to browse in a secure way
3. **Cryptography Applications (I) and (II)**
   - Different actions to provide authentication, integrity and confidentiality with PGP
5. **Non-automatable OS Security**
   - Manual hardening of OS key parts
6. **Automatable OS security and Security Policies**
   - Automatic hardening of Linux OS using trusted and widely used policies
7. **Network security**
   - Setting up network protection tools
8. **Network Enumeration Techniques (2 weeks)**
   - Remote machine analysis and info gathering
10. **Defending a Web Application**
    - Setting up a WAF and other defenses
11. **Introduction to Exploiting**
    - Typical exploiting techniques
12. **Introduction to Privilege Scalation (2 weeks)**
    - Typical privilege scalation techniques

"Special" Slides: Slides with exercises

- These ARE evaluable
- This is standard theory content, but with associated exercises
  - You cannot understand a concept? Try practicing it with the exercises linked to it
- In this course, theory and laboratories are very strongly integrated
  - And the relationship is explicit, as you will see in these slides
  - Each exercise has a **unique code** to search it in the lab reports

Password storage: Key Derivation Function (KDF)

- Typical techniques to guess plain-text passwords from stored data
  - **Pure brute-force**: covering all the possible key space and normally with a prohibitive cost
  - **Dictionaries** (EDI) of potential keys that may correspond to stored data
    - We check less values, but consume more memory and may be unsuccessful (key not present in the dictionaries we used)
  - **Rainbow tables**: data structures that allow to store large password quantities
    - Consuming less memory but requiring more computational power that plain dictionaries
- **Can we resist them?**
  - Yes, but not using plain hash algorithms
  - But specialized Key Derivation Functions (KDF) ones!

➢ Exercises **L3B3_SSLCRACK, L3B3_PASS, L3B3_BRUTE**

LXBY means "Laboratory X, Block Y"

Laboratory

Exercise L3B3_SSLCRACK: *John the Ripper* to break OpenSSL

Description of the activity / Practical application

You need **to crack the password of an openssl-encrypted file** that uses a common password

Expected results

This activity ends **when the password hash of the encrypted message** with `openssl` in a previous exercise **is decrypted** (that is why we insist on using "`password`" as the password 😊). You can answer the following questions:

PLANNING

- **On the OCW course website you can find the suggested planning for it, but only as a guide**
  - Theory, seminars, and labs are linked and coordinated to make it easier to follow
- **You can follow them at your own pace**
  - It is designed to be **done completely offline** and without haste
- **Just make sure you have a good understanding of the theory associated with seminars and labs before you do them ☺**
  - That's why I've incorporated the "self-assessment" transparencies
- **And to evaluate the practical work, you have other ways to do it yourself**
  - Which I'll explain in the practical part!

What is the goal of this course?

- **Prepare you to start your cybersecurity career (if you want! ☺)**
  - We will introduce all major cybersecurity areas to get you started
  - We synchronize with the rest of the courses in the degree to put it in context
    - We have links with up to 24 different courses!
  - We put you much closer to attempt the **eLearnSecurity Junior Penetration Tester** (eJPT) Certification (https://elearnsecurity.com/product/ejpt-certification/)
    - You will need to practice more to master the concepts, carefully review the eJTP syllabus to complete your "knowledge gaps", and complete the **Windows** part on your own:
      - https://infosecwriteups.com/ultimate-guide-to-pass-ejpt-in-the-first-attempt-by-mayur-parmar-75effc877394?gi=68a0a4c21353
      - https://github.com/tejasanerao/eJPT-Cheatsheet
    - But this course make attempting this initial certification much easier
- **But, above all, to give you enough security skills to improve the applications you create as a future software engineer**
  - Even if you do not pursue a career path in cybersecurity, we want this course to help you creating better software products in the future
  - We will give you tools to use daily, so you can **integrate security in your routine without hating it** ☺

The "Cobra Kali" initiative

- This course is the initial one that integrates this initiative of six courses
  - Part of the **Rank 2**
- Taking all of them will give you a more advanced cybersecurity training
- It is an initiative to have a more complete cybersecurity training inside the University of Oviedo
- It's our cybersecurity dojo! ☺

La iniciativa "*Cobra Kali*" por *José Manuel Redondo López*

Ciberdefensa Personal

Técnicas contra el cibercrimen y fraudes
Cursos G-9, PDI, Proyecto *UNIDIGITAL*
"BPM P-51 Asturias"

x6

OSINT

Técnicas de investigación con fuentes abiertas
TBA
"A-21 Poseidón"

Fraudes y Timos Cibernéticos

Técnicas contra el cibercrimen y fraudes
Charlas públicas, cursos, radio *Onda Cero*...
"P-45 Audaz"

Rango 1 (Aficionado a la Seguridad)

Seguridad de Redes

Threat hunting
TBA
L-52 "Castilla"

Administración de Sistemas Operativos

Infrastructure as Code
Máster en Ingeniería Web
L-62 "Princesa de Asturias"

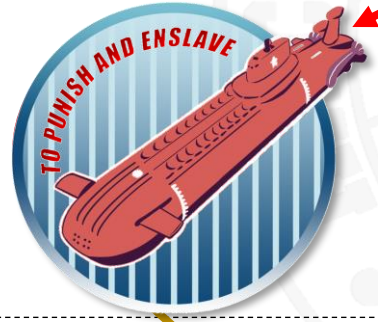
Seguridad de Sistemas Informáticos

Introducción a la seguridad
Grado en Ingeniería del Software
S-81 "Isaac Peral"

Rango 2 (Entusiasta de la Seguridad)

Sistemas de Seguridad en la Web

Seguridad ofensiva: Reconocimiento y Explotación
Máster en Ingeniería Web
TK-210 "красный октябрь" (Octubre Rojo)



Administración de Servidores Web

Seguridad defensiva
Máster en Ingeniería Web
D-73 "Blas de Lezo"

Rango 3 (Especialista en Seguridad)

Post-Exploiting e Intrusión en Sistemas

Seguridad ofensiva: Post-Explotación
TBA
K-329 "Belgorod"

Desarrollo Seguro de Software

Platform Engineering Seguro
Guías nacionales INCIBE,
TBA
F-113 "Menéndez de Avilés",

Rango 4 (Profesional de la Seguridad)

COMPUTER SECURITY
PRESENTATION

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo