COMPUTER SECURITY

(AKA "SEGURIDAD DE SISTEMAS INFORMÁTICOS", SSI)

Presentation

Source: zona-militar.com

José Manuel Redondo López *"S-81 Isaac Peral"* Project v3.0

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

WELCOME!

José Manuel
Redondo López

- **Welcome to our Computer Security course!**
- **In this course we will try to allow you to 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 ☺
  - From zero to hero! ☺
- **But 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

José Manuel
Redondo López

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

SEMINAR TOPICS

José Manuel
Redondo López

- **Tools for Internet Research**
  - Current issues on security contexts and applications: tools for investigating them
- **Physical Security**
  - A review on physical security procedures and methods
- **Automated Vulnerability Scanning Tools**
  - Tools to automatically evaluate the security of remote systems
- **Introduction to Reversing**
  - Brief introduction of executable analysis and “dissection”
- **Input Validation**
  - Practical approaches to validate user inputs
- **HTTP Headers and CSP**
  - State-of-the-art HTTP protocol security applications

LABORATORY TOPICS

José Manuel
Redondo López

- **"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!**
- **System Setup**
  - Basic machine setup of the VM we are going to use in the labs
- **Information Discovery and OSINT**
  - Obtaining information about people and entities using public resources
- **Cryptography Applications (I) and (II)**
  - Different actions to provide authentication, integrity and confidentiality with PGP
- **Non-automatable OS Security**
  - Manual hardening of OS key parts
- **Automatable OS security and Security Policies**
  - Automatic hardening of Linux OS using trusted and widely used policies
- **Network security**
  - Setting up network protection tools
- **Network Enumeration Techniques**
  - Remote machine analysis and information gathering
- **Defending a Web Application**
  - Setting up a WAF and other defenses
- **Introduction to Exploiting**
  - Typical exploiting techniques
- **Introduction to Privilege Scalation**
  - Typical privilege scalation techniques

Assessment

José Manuel
Redondo López

- **Please, do not attempt to do any lab topic without reading and properly understanding their corresponding theory and lab topics first**
- **The learning assessment consist in self-evaluating what you have learned**
  - Each **theory and seminar topic** have **a list of leveled self-evaluation badges** at the end
    - You must be able to answer to the concepts they describe to ensure you have properly understood each theory topic
  - Each **laboratory** have a list of **leveled self-evaluation badges** at the end
    - You must be able to **document** a complete procedure to perform each activity of the lab reports
    - Additionally, each activity have an **"Expected Results" box**
      - With the outcome of the activity you must achieve
      - Only attaining this expected outcome, you can consider you have properly understood each activity
    - Once you do this, **try to relate it with the theory and seminar topics**: labs are synchronized with them!

WHAT IS THE GOAL OF THIS COURSE?

José Manuel
Redondo López

- **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 degree 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 aims to make attempting this initial certification easier
- **Give you enough security skills to improve your software as a future software engineer**

The "Cobra Kali" initiative

José Manuel
Redondo López

- **This course is the initial one that integrates this initiative of six courses**
  - Part of the Rank 1 (introductory courses)
- **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**

The "*Cobra Kali*" initiative by *José Manuel Redondo López*

Computer Security
Introduction to Cybersecurity
Bachelor of Software Engineering
S-81 "Isaac Peral"

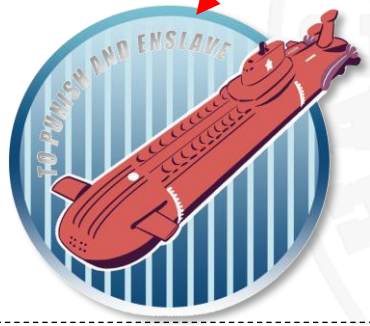
Cybercrime Defense
Techniques against cybercrime and cyberfraud
Public talks, courses, *Onda Cero* radio...
"Nautilus"

Rank 1 (Security Aficionado)

Operating System Administration
Infrastructure as Code
Master Degree and PhD in Web Engineering
R-11 "Príncipe de Asturias"

Rank 2 (Security Enthusiast)

Web Security Systems
Offensive Security
Master Degree and PhD in Web Engineering
TK-210 "красный октябрь" (Red October)



Web Server Administration
Defensive Security
Master Degree and PhD in Web Engineering
F-103 "Blas de Lezo"

Rank 3 (Security Specialist)

Secure Software Development
Secure Platform Engineering
<No destination yet>
F-113 "Menéndez de Aviles"

Rank 4 (Security Champion)

COMPUTER SECURITY

Source: zona-militar.com