SEGURIDAD DE SISTEMAS INFORMÁTICOS

PRESENTACIÓN

"APIs, scripts, inputs...demasiados hacks, y tan poco tiempo..."

José Manuel Redondo López Proyecto *"S-81 Isaac Peral"* v4.0

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

¡BIENVENIDO!

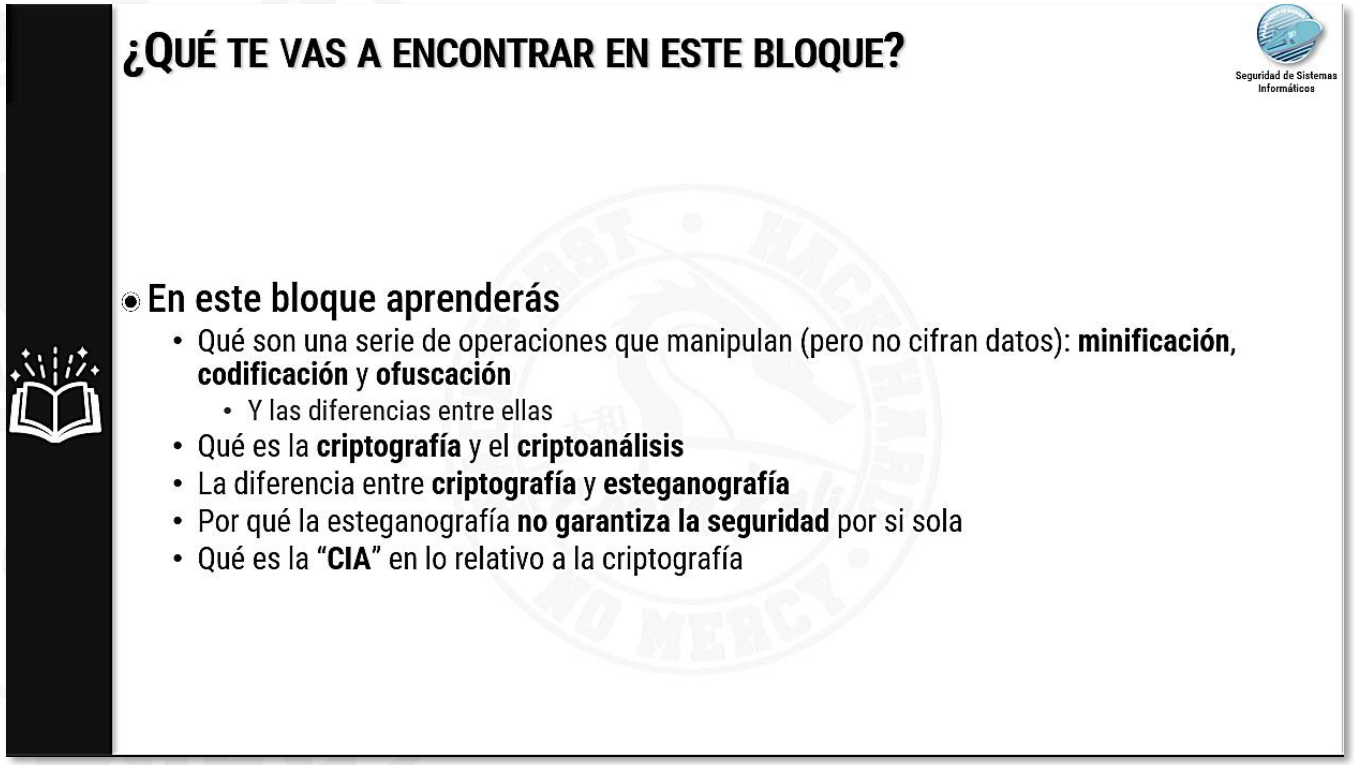
- ¡Bienvenido a nuestra asignatura **Seguridad de Sistemas Informáticos**!
- En esta asignatura intentaremos hacerte comprender y usar **más que lo básico** sobre diferentes aspectos clave del campo de la seguridad informática
  - Cubriendo tanto amenazas...como defensas contra las artes oscuras ☺
  - **Suponiendo que no conoces nada de este mundo**: To the moon! ☺
- Es imposible cubrir todos los conceptos y subcampos de seguridad en una sola asignatura
  - Sin embargo, ¡es suficiente para introducirte en todos los principales!
- ¿Listo? ¡VAMOS!

TEMAS DE TEORÍA

1. **Introducción**
   - Conceptos básicos para entender el resto de la asignatura
2. **Aplicaciones de la criptografía**
   - Cómo utilizar correctamente la criptografía para proporcionar confidencialidad, integridad y autenticación
3. **Seguridad de sistemas operativos**
   - Reglas básicas para mejorar la seguridad de los sistemas operativos manualmente
4. **Políticas de seguridad**
   - Descripción general de las políticas de seguridad y cómo aplicarlas para proporcionar seguridad con un alto grado de automatización
5. **Seguridad perimetral y de red**
   - Firewalls, sistemas de detección y prevención de intrusiones y otros conceptos de seguridad de red
6. **Seguridad de aplicaciones**
   - Procedimientos para crear software seguro y validar los datos de entrada
7. **Introducción a las operaciones Red Team: explotación y escalación de privilegios**
   - Una introducción a las técnicas de explotación y escalado de privilegios con énfasis en CTF

Transparencias "Especiales": Las que tienen un libro

- **Si te encuentras con una transparencia de este tipo, no es material evaluable**
  - Es contenido para ayudarte a estudiar la asignatura
- **En este caso es un pequeño resumen de los principales conceptos que se van a impartir en una sección**
  - Permite hacer búsquedas rápidas y estructurar bien lo que se estudia en cada parte



TRANSPARENCIAS "ESPECIALES": LAS QUE TIENEN UN "?"

- Este tipo de transparencia tampoco es evaluable, pero te ayuda mucho con la evaluación
- Contiene preguntas clave que debes asegurarte poder responder para saber qué has entendido los contenidos de una sección
- Es un mecanismo para que autoevalúes tu propio aprendizaje

?

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

Seguridad de Sistemas Informáticos

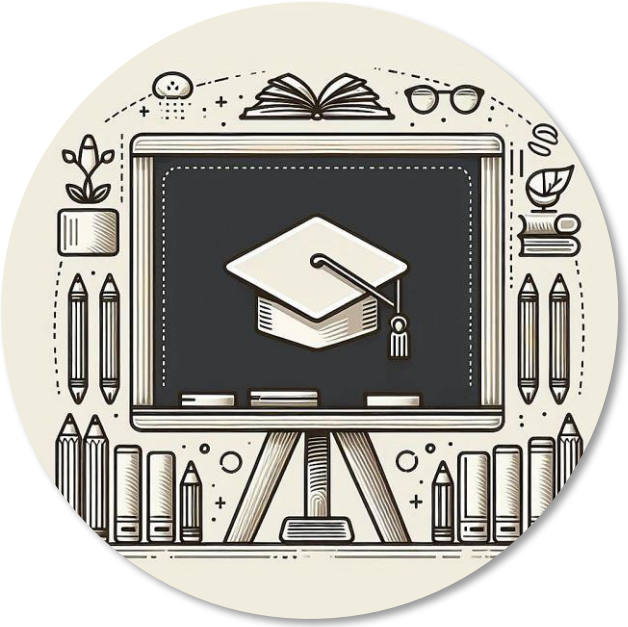
- Eres capaz de hacer lo siguiente
  - *Entender que minificar, codificar y ofuscar tienen sus usos, pero NO SON cifrado*
  - *Comprender que, si un código minificado ocupa menos, aparte de ser menos legible mejora el rendimiento de carga de las webs*
  - *Ser consciente de que la criptografía (y su "contraria", el criptoanálisis) son ciencias matemáticas muy antiguas*
  - *Tener claro que la esencia de la esteganografía, independientemente del software o método usado para hacerla, es enviar información sin que nadie lo sepa y sin que, por tanto, sea evidente a simple vista*
  - *Entender que la esteganografía sin criptografía no sirve para garantizar la seguridad, porque ocultar la información solamente nunca es seguro*

TEMAS DE SEMINARIOS

1. **Herramientas para investigar en Internet**
   - Temas actuales sobre contextos y aplicaciones de seguridad: herramientas para investigarlos
2. **Seguridad física**
   - Una revisión de los procedimientos y métodos de seguridad física
3. **Herramientas automatizadas de análisis de vulnerabilidades**
   - Herramientas para evaluar automáticamente la seguridad de los sistemas remotos
4. **Introducción al reversing**
   - Breve introducción del análisis y “disección” de ejecutables
5. **Validación de entradas**
   - Enfoques prácticos para validar las aportaciones de los usuarios
6. **Cabeceras HTTP y CSP**
   - Aplicaciones de seguridad de protocolo HTTP de última generación
7. **Write-up de una máquina CTF**
   - Aplicación de los conceptos de la asignatura en un escenario CTF real

Transparencias "Especiales": El icono de "seminario"

- La teoría también está integrada con los seminarios
- Los seminarios son complementos de carácter más práctico a los conceptos de teoría
  - Como tales, están vinculados a los temas de teoría que impartiremos
- Aunque pueda aparecer menciones a un seminario previamente, donde realmente encajan sus contenidos es en la transparencia donde veas este icono
- De esta manera sabrás como se relacionan unos con otros dentro del programa de la asignatura



Icono hecho con Bing Chat AI

TEMAS DE LABORATORIO

- "Lab 0": Creación de la MV de la asignatura
  - **¡Trabajo autónomo a preparar para el resto de la misma!**
  - **¡Sigue las instrucciones del laboratorio 00A y 00B en cuanto puedas!**

1. **Configuración del sistema**
   - Configuración básica de la máquina virtual que vamos a usar en los laboratorios
2. **OSINT y navegación segura**
   - Obtención de información sobre personas y entidades que utilizan recursos públicos y seguridad en la navegación
3. **Aplicaciones de criptografía (I) y (II)**
   - Diferentes acciones que proporcionan autenticación, integridad y confidencialidad con PGP
5. **Seguridad del sistema operativo no automatizable**
   - Mejora de la seguridad manual de partes clave del sistema operativo
6. **Seguridad de SSOO automatizable y políticas de seguridad**
   - Mejora de la seguridad automática del sistema operativo *Linux* utilizando políticas confiables y ampliamente utilizadas
7. **Seguridad de la red**
   - Configuración de herramientas de protección de red
8. **Técnicas de enumeración de red (2 sem.)**
   - Análisis remoto de máquinas y recopilación de información
10. **Defensa de una aplicación web**
    - Configuración de un WAF y otras defensas
11. **Introducción a la explotación**
    - Técnicas de explotación típicas
12. **Introducción a la escalación de privilegios (2 sem.)**
    - Técnicas típicas de escalado de privilegios

Transparencias "Especiales": Las que tienen ejercicios

Seguridad de Sistemas Informáticos

Teoría

- Estas SÍ SON evaluables
- Se trata de contenido teórico estándar, pero con ejercicios asociados
  - *¿Se te resiste un concepto?* Prueba a practicarlo con los ejercicios vinculados al mismo
- En esta asignatura teoría y práctica están muy fuertemente integrados
  - Y la relación es explícita, como veréis en estas transparencias
  - Cada ejercicio tiene un **código único** para buscarlo en los informes de labs

Guardar claves: Key Derivation Function (KDF)

Seguridad de Sistemas Informáticos

- Técnicas típicas para adivinar contraseñas a partir de datos almacenados
  - **Fuerza bruta pura**: cubrir todo el espacio de claves posible y normalmente con un coste prohibitivo
  - **Diccionarios** (EDI) de claves potenciales que pueden corresponder a datos almacenados
    - Comprobamos menos valores, pero consume más memoria y puede no tener éxito (la clave no está en los diccionarios usados)
  - **Tablas Rainbow**: estructuras de datos que permiten almacenar grandes cantidades de contraseñas
    - Consume menos memoria, pero requiere más potencia computacional que los diccionarios simples
- ¿Podemos resistir estos ataques?
  - Sí, pero no usando algoritmos hash simples
  - ¡Sino las funciones de derivación de claves especializadas (Key Derivation Functions, KDF) que mencionamos antes!

➢ Ejercicios **L3B3_SSLCRACK, L3B3_PASS, L3B3_BRUTE**

LXBY significa "Laboratorio X, Bloque Y"

Laboratorio

Ejercicio L3B3_SSLCRACK: *John the Ripper* para romper OpenSSL

Descripción de la actividad / Aplicación práctica

Necesitas **crackear la contraseña de un fichero cifrado** con `openssl` que usa una password común

Resultados Esperados

Esta actividad finaliza **cuando se descifra la hash de la contraseña del mensaje cifrado** en un ejercicio anterior con `openssl` (por eso insistimos en usar "`password`" como contraseña 😊). Puedes contestar a las siguientes preguntas:

PLANIFICACIÓN

- **En la web de la asignatura en OCW puedes encontrar la planificación prevista para la misma, pero solo a modo de guía**
  - Teoría, seminarios y laboratorios están enlazados y coordinados para que sea más fácil seguirla
- **Se puede seguir a tu propio ritmo**
  - Está pensada para hacerse **de manera totalmente offline** y sin prisas
- **Solamente asegúrate de entender bien la teoría vinculada a los seminarios y laboratorios antes de hacerlos ☺**
  - Para eso he incorporado las transparencias de “autoevaluación”
- **Y para evaluar el trabajo práctico tienes otras formas también de hacerlo tú**
  - ¡Que explicaré en la parte práctica!

¿CUÁL ES EL OBJETIVO DE ESTA ASIGNATURA?

- **Prepararte para comenzar tu carrera en ciberseguridad (¡si quieres! ☺)**
  - Te presentaremos todas las principales áreas de la ciberseguridad para iniciarte en ellas
  - Nos sincronizamos con el resto de los cursos de la titulación para poner la carrera en contexto
    - ¡Tenemos relación con hasta 24 asignaturas diferentes!
  - Te pondremos mucho más cerca de intentar la certificación **eLearnSecurity Junior Penetration Tester** (eJPT) (https://elearnsecurity.com/product/ejpt-certification/)
    - Necesitarás practicar más para dominar los conceptos, revisar cuidadosamente el programa de eJTP para completar tus “huecos" y completar la parte de **Windows** por tu cuenta
      - https://infosecwriteups.com/ultimate-guide-to-pass-ejpt-in-the-first-attempt-by-mayur-parmar-75effc877394?gi=68a0a4c21353
      - https://github.com/tejasanerao/eJPT-Cheatsheet
    - Pero esta asignatura hace que intentar esta certificación inicial sea mucho más fácil
- **Pero, sobre todo, darte suficientes habilidades de ciberseguridad para mejorar las aplicaciones que crees como ingeniero de software**
  - Aunque no te dediques a la seguridad, queremos que esta asignatura te ayude a crear mejores productos en el futuro
  - Te daremos herramientas usables en tu día a día, para que puedas **usar la seguridad sin odiarla** ☺

La iniciativa "Cobra Kali"

- Esta asignatura es la primera de una iniciativa que integra diez asignaturas
  - Parte de su **Rango 2**
- Si cursas todas tendrás un entrenamiento en seguridad más avanzado
- Es una iniciativa para intentar poner en marcha un entrenamiento en ciberseguridad más completo en la Universidad de Oviedo
- ¡Es por tanto nuestro "dojo" de ciberseguridad! ☺

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"

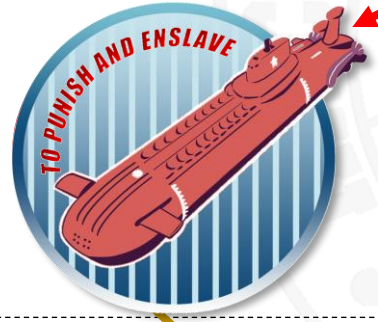
Seguridad de Sistemas Informáticos

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)

SEGURIDAD DE SISTEMAS INFORMÁTICOS

PRESENTACIÓN

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo