Técnicas de Hacking

Presentación de la asignatura

Universidad Rey Juan Carlos

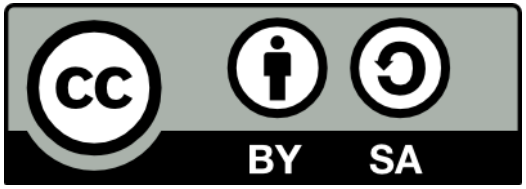
Licencia

Sergio Pérez Peló

sergio.perez.pelo@urjc.es

Raúl Martín Santamaría

raul.martin@urjc.es



Profesor/es

- ***Sergio Pérez Peló***
  - Email: sergio.perez.pelo@urjc.es
  - Despacho 104 – Departamental II

- ***Raúl Martín Santamaría***
  - Email: raul.martin@urjc.es
  - Despacho 104 – Departamental II

Para contactar con nosotros con cualquier tema relacionado con la asignatura, escribirnos un correo **con copia a ambos profesores.**

Cómo seguir la asignatura

Universidad Rey Juan Carlos

- **Clases:**
  - Horario:
    - **Lunes de 11:00 a 13:00**
    - **Miércoles de 09:00 a 11:00**
  - Aula: 109 del Aulario I.

- Todo el material estará disponible en el Aula Virtual de la asignatura.

- Avisos por campus virtual:
  - **Mirar con asiduidad la página web de la asignatura.**
  - No contestar estos avisos a través de campus virtual.

Objetivos

Universidad Rey Juan Carlos

- Nos encontramos ante la primera asignatura de **seguridad ofensiva**.
- Nos permitirá conocer las **técnicas que usan los atacantes**.
- También conoceréis las estrategias de prevención, de detección y de respuesta.
- Se verán técnicas básicas de explotación de vulnerabilidades en Windows y Linux, ingeniería inversa, desbordamientos de memoria, inyecciones… etc.

Habilidades

Universidad Rey Juan Carlos

- Las habilidades que se pretende que alcance el alumno son:
  - Capacidad para evaluar y asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos.
  - Aprender nuevas técnicas de seguridad ofensiva de manera autónoma.
- Se recomienda al alumno haber superado satisfactoriamente las asignaturas:
  - Introducción a la Ciberseguridad.
- El temario se compone de 10 temas distribuidos en 4 bloques

Temario de la asignatura

Universidad Rey Juan Carlos

- **Bloque I: Técnicas de recogida de información**
  - Tema 1: Introducción
    - Seguridad ofensiva: conceptos básicos. Anatomía de un ataque y *kill chain*. TTPs, estándares y clasificaciones. Hacking ético.
  - Tema 2: Footprinting y OSINT
    - Hacking con buscadores. Metadatos. Otras fuentes abiertas de inteligencia.
  - Tema 3: Fingerprinting
    - Reconocimiento y enumeración. Análisis de tráfico. Escaneo de puertos y de vulnerabilidades. Fuzzing. Anonimato.
  - Tema 4: Ingeniería Social
    - Técnicas que atacan el factor humano: no invasivas e invasivas. Phising y diseño de campañas. Hacking en el lado del cliente.

Temario de la asignatura

Universidad Rey Juan Carlos

- **Bloque II: Hacking de sistemas**
  - Tema 5: Técnicas básicas de explotación en Windows
    - Particularidades de los sistemas operativos de Microsoft (registro, WMI, APIs, PowerShell, etc.). Autenticación, autorización y escalada de privilegios en Windows.
  - Tema 6: Técnicas básicas de explotación en Linux
    - Particularidades de los sistemas operativos de tipo Linux. Escalada de privilegios, ataques a contraseñas.

Temario de la asignatura

Universidad Rey Juan Carlos

- **Bloque III: Hacking de aplicaciones tradicionales y web**
  - Tema 7: Ingeniería inversa y desbordamientos
    - Ingeniería inversa y análisis de código en Windows y en Linux. Funcionamiento de la pila. *Buffer overflow*. Otros desbordamientos.
  - Tema 8: Inyecciones y *forgeries*
    - Inyección de comandos. Inyección SQL. Otras inyecciones. XSS y XSRF.
- **Bloque IV: Hacking de redes y comunicaciones**
  - Tema 9: Envenenamientos, MitM, suplantaciones y secuestros.
    - ARP *poisoning* y *Man in the Middle*. *Spoofing* a diferentes niveles. Secuestros de sesión (UDP y TCP *hijacking*).
  - Tema 10: Denegación de servicio
    - Denegaciones de servicio volumétricas. Ataques en la capa de infraestructura: inundaciones y reflejos. Ataques en la capa de aplicación.

Temario de la asignatura

Estamos ante una asignatura eminentemente práctica, en la que memorizar será de muy limitada utilidad

Resultados de aprendizaje: generales

Universidad Rey Juan Carlos

- CG1. Capacidad para **resolver problemas con iniciativa**, buena toma de decisiones, autonomía y creatividad.
- CG3. Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar documentos que tengan por objeto definir, **planificar, especificar, resumir proyectos y planes en el ámbito de la ciberseguridad**.
- CG6. Capacidad para **conocer**, comprender y **aplicar la legislación y código ético** necesario para la labor profesional en el sector de la ciberseguridad.
- CG7. Capacidad para evaluar y **asegurar la confidencialidad, integridad y disponibilidad** de los activos tecnológicos.
- CG11. Conocimiento para la **realización de** mediciones, cálculos, valoraciones, tasaciones, **peritaciones, estudios, informes, planificación de tareas** y otros trabajos análogos.
- CG12. Capacidad para **analizar y valorar el impacto social** y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad en el ámbito de la ciberseguridad.

Resultados de aprendizaje: generales

Universidad Rey Juan Carlos

- CG13. Capacidad para **concebir, desarrollar, implantar y mantener sistemas, servicios y aplicaciones** informáticas empleándolos métodos de la ingeniería como instrumento para el aseguramiento de su calidad.
- CG15. Capacidad para aplicar conocimientos a su trabajo o vocación de una forma profesional. Capacidad para **elaborar y defender argumentos y resolver problemas** dentro de su aérea de estudio.
- CG16. Capacidad de **reunir e interpretar datos relevantes** (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- CG17. Capacidad para **transmitir información, ideas, problemas y soluciones** a un público tanto especializado como no especializado.
- CG18. Capacidad para aplicar las habilidades de aprendizaje adquiridas necesarias para **emprender estudios posteriores con un alto grado de autonomía**.

Resultados de aprendizaje: específicos

Universidad Rey Juan Carlos

- CE19. Comprender los **algoritmos criptográficos de clave pública y de clave privada** más importantes y conocer sus aplicaciones en ciberseguridad.
- CE20. Analizar las etapas o pasos que los atacantes siguen para construir sus ataques de manera que se puedan comprender los **patrones de ataque más graves e importantes y llevarlos a cabo en entornos de seguridad ofensiva.**
- CE26. **Conocer** los distintos **tipos de malware** en función de su vector de infección, mecanismos de propagación, replicación y protección, de sus objetivos, etc.

Planificación orientativa

Universidad Rey Juan Carlos

Lunes	Actividad	Miércoles	Actividad
09/09/2024	Presentación (¡Hoy!)	11/09/2024	Tema 1
16/09/2024	Tema 2	18/09/2024	Tema 3
23/09/2024	Tema 4, ejercicios	25/09/2024	Ejercicios
30/09/2024	Examen Bloque 1	02/10/2024	Tema 5
07/10/2024	Tema 5	09/10/2024	Tema 5
14/10/2024	Tema 6	16/10/2024	Tema 6
21/10/2024	Tema 6	23/10/2024	Práctica 2
28/10/2024	Presentaciones 1	30/10/2024	Presentaciones 2

Planificación orientativa

Universidad Rey Juan Carlos

Lunes	Actividad	Miércoles	Actividad
04/11/2024	Presentaciones 3	06/11/2024	Tema 7
11/11/2024	Tema 7	13/11/2024	Tema 7
18/11/2024	Tema 8	20/11/2024	Tema 8
25/11/2024	Tema 8	27/11/2024	Práctica 2
02/12/2024	Práctica 2	04/12/2024	Práctica 2
09/12/2024	Tema 9	11/12/2024	Tema 9, 10
16/12/2024	Tema 10	18/12/2024	Repaso / Dudas

Evaluación de la asignatura

Universidad Rey Juan Carlos

Actividad	Fecha	Peso	Nota mínima
Parcial 1	Tras finalizar Bloque 1 (Aprox. **semana del 23/09**)	25 %	5
Parcial 2	Fecha examen ordinaria	30 %	5
Prácticas con ordenador	A lo largo del cuatrimestre	30 %	5
Resolución de problemas y casos prácticos	Semanas 14 y 15	15 %	5

Evaluación de la asignatura

Universidad Rey Juan Carlos

- Tenemos fecha de examen para la convocatoria ordinaria:

15 de Enero de 2025 (de 13:00 a 15:00)

Podéis consultarlo en

https://gestion2.urjc.es/examenes/

Bibliografía

- **Ethical Hacking and Penetration Testing Guide.** Rafay Baloch.
- **Gray Hat Hacking The Ethical Hacker's Handbook**. Sims et.
- **Learn Ethical Hacking from Scratch**. Zaid Sabih.
- **Hacking For Dummies**. Kevin Beaver.
- **Kali Linux 2018: Assuring Security by Penetration Testing – Fourth Edition**. Ali et. Al.

- Todos estos libros (y muchos más) son de O'Reilly, lo que significa que tenéis acceso a ellos a través de https://brain.urjc.es/.

Técnicas de Hacking

Presentación de la asignatura

Universidad Rey Juan Carlos