# Una iniciativa del Colegio Tres Olivos

## Serie Hackers

**Docente:** Jose Antonio García Cañizares

Experto formador en diferentes áreas tecnológicas


**Dirigido a:**
Alumnas y alumnos de secundaria, Bachillerato y Formación Profesional
Amantes de la tecnología y la seguridad informática.
No requiere conocimientos previos.

**Edad recomendada:**
**13** a **100** años.

**Idiomas:**
☒ Español

**Duración:**
4 h y 30 minutos, de 9.30 a 14.00

**Tecnologías:**
Redes y Sistemas. TCP/IP. Identidades basadas en máquinas y procesos. Ataques de reconocimiento, test y técnicas de penetración. Ataques a credenciales, gestión de contraseñas. Análisis y detección del Malware. Mercado Negro. Google Hacking. Vulnerabilidades y Exploit. Internal Hacking.

**Temática Principal:**
Seguridad y Hacking Ético.

**Beneficios:**
Todos los asistentes **serán beneficiados con 2 cursos gratuitos online de nuestro Partner de formación Cisco Networking Academy.**
Se requiere inscripción anticipada y correo electrónico.

**Precio:**
30 € precio general, con descuentos para alumn@s, familias (20 €) y exalumn@s (25€)

**Inscripción:**
Debes solicitar plaza a través del siguiente formulario
https://goo.gl/forms/1B4pZ3vZd3vYY3Uu1

**Los profesionales de la Ciberseguridad deben tener las mismas habilidades que los hackers, especialmente que los hackers más peligrosos y habilidosos de la red global, para ofrecer protección contra los ataques. Una diferencia entre un hacker y un profesional de la Ciberseguridad es que el profesional de la Ciberseguridad debe trabajar dentro de los límites legales.**

TYP

**Ejercicios y entrenamiento:**

**Reto 1: ¿Quién son los buenos y los malos?**
¿De qué lado estas? Servicios de Inteligencia y agencias gubernamentales.
Los estados como agentes de las amenazas.
Tipo de Hackers y sus motivaciones.
Salidas profesionales.

**Reto 2: Desciframiento de un ataque conseguido.**
Metodología de un ataque. Ante todo, discreción.
Selección de la Victima. El ataque.
Introducirse en el sistema y garantizar el acceso.
Mitigación: Evaluación de riesgos, implantación de un plan de seguridad, revisión y mejora.

**Reto 3: Búsqueda de información**
Toma de Huellas. Servicios Whois.
Enumeración DNS. Escáneres de puertos.
Motores de búsqueda de dispositivos conectados.
Google Hacking.
Mitigación de enumeración. Filtrado IP.

**Reto 4: Extraer, romper, cambiar una contraseña.**
¿Cómo extraer una contraseña en un equipo?
¿Cómo extraer una contraseña desde la red?
¿Por qué las contraseñas robustas no son de utilidad en Internet?
Mitigación: Autenticación Multifactor y
Gestor de contraseñas.

**Reto 5: Crear tus propias herramientas de hacking.**
Crear un Keylogger. Capturar pantallas.
Capturar sonido.
Mitigación: Antivirus, IPS, IDS y análisis en línea.

**Demostración 1:** ¿Cómo acceder a sistemas de control Industrial?
Mitigación.

**Demostración 2:** ¿Cómo acceder a sistemas Multimedia? Mitigación.

**Demostración 3:**
¿Cómo acceder a impresoras conectadas?
Mitigación.

**Demostración 4:** ¿Cómo acceder a Smartphones?
Mitigación.

**Demostración 5:** ¿Cómo acceder a ficheros jugosos?
Mitigación.

**Demostración 6:** ¿Cómo acceder a ficheros personales?
Mitigación.

## Metodología:

- La metodología será mixta, aunque con un predominio de la metodología práctica sobre la expositiva.
- Se realizarán ejercicios prácticos que se resolverán en la propia aula de informática donde impartiremos el taller.

## ¿Por qué?:

- La revolución digital está generando nuevos modelos de relación dentro de la Sociedad, y términos como G2C, G2G, G2E, B2B, B2C, C2C y M2M son hoy una realidad en las sociedades avanzadas.
- Sin embargo**, también se está generando un escenario con nuevos riesgos** que deben ser identificados y evaluados para crear un entorno de protección que facilite un adecuado desarrollo de la Comunidad Digital. Amenazas tales como **ciberterrorismo, la ciberguerra, el fraude online, el hacktivismo, el robo de información**, etc. se benefician del desconocimiento de los usuarios y de los profesionales para perjudicar a individuos, administraciones públicas y empresas.
- En la Unión Europea, **el impacto económico de los ciberataques en 2012 se estimó en 12 mil millones de euros.** Por su parte, el Foro Económico Mundial, en 2013, calificó los ciberataques como una de las cinco mayores amenazas, en términos de probabilidad, para el desarrollo global.
- Uno de las principales barreras a las que se enfrentan las organizaciones a la hora de gestionar adecuadamente **estos nuevos riesgos es la de la falta de personal cualificado.**
- A nivel global, el 2014 Annual Security Report, del **fabricante Cisco, estimaba que, para 2014, más de un millón de vacantes en materia de ciberseguridad** quedarían desiertas por falta de capacitación de profesionales.
- En España, **el informe de Infoempleo y Adecco, Los + buscados**, en su edición de 2013, estimaba que **solo en España se necesitan hasta 20.000 profesionales dedicados a esta materia** y sus puestos no se cubren por falta de formación y especialización en la materia.

Por todo ello, **el colegio Tres Olivos no puede quedarse al margen de este nuevo reto tecnológico y la importante demanda de especialistas que conlleva**. Desde el departamento de **Formación Profesional del colegio se toma la iniciativa de ofertar este curso relacionado con Ciberseguridad con el propósito de cubrir las necesidades en formación especializada tanto de recién titulados, como de jóvenes y mayores interesados en formarse en un área con tanta demanda.**