UNC Universidad Nacional de Córdoba

FAMAF Facultad de Matemática, Astronomía, Física y Computación

PROGRAMA DE CURSO
PARA SER CONSIDERADO COMO
CURSO DE EXTENSIÓN DE FAMAF

Título del curso: Introducción a la Seguridad Informática orientada a CTFs.

Profesores responsables de FAMAF: Nicolás Wolovick

Profesores que dictarán el curso (si alguno no es de FAMAF adjuntar CV):

Gastón Aznarez
Maico Molina Aoki

Antecedentes: La seguridad informática es uno de los campos de mayor crecimiento en la industria tecnológica. En octubre de 2025, durante el Mes de la Ciencia organizado por FAMAF, Gastón Aznarez dictó una charla sobre seguridad que despertó un notable interés entre los estudiantes, quienes luego le solicitaron un espacio para seguir aprendiendo sobre la temática. Esto evidencia una demanda concreta de formación en seguridad informática dentro de la comunidad de la facultad. Este curso viene a llenar un vacío en la formación de InfoSec que solamente se ve de manera transversal en la carrera y que anteriormente fuera ocupado temporalmente por Ricardo Corín 2009 a 2013 "Seguridad Informática" y por Joshep Cortéz Sánchez 2020-2021 "Seguridad Ofensiva". Los CTFs (Capture The Flag) son competencias internacionales de seguridad informática en las que los participantes resuelven desafíos prácticos para encontrar una "bandera" (un código oculto). Este formato es ampliamente utilizado tanto en la industria como en la academia para el aprendizaje y evaluación de habilidades en seguridad. El curso sigue el modelo exitoso del Curso de Extensión de Programación Competitiva de FAMAF, adaptando su estructura de clases semanales y desafíos progresivos al ámbito de la seguridad informática.

Objetivos: Introducir a los estudiantes en el mundo de la seguridad informática a través de un formato competitivo y práctico, desarrollando habilidades en las principales áreas de la disciplina.
Crear un espacio en FAMAF donde los interesados en seguridad puedan aprender, practicar y encontrar una comunidad con sus mismos intereses.
Motivar la participación de los estudiantes en competencias CTF nacionales e internacionales.

Destinatarios y cupo de alumnos: El curso está destinado principalmente a estudiantes con conocimientos básicos de programación y manejo de sistemas Linux. También está abierto a estudiantes con experiencia previa en seguridad que deseen profundizar sus conocimientos. El cupo de alumnos está dado por la capacidad de un laboratorios de FAMAF o un máximo de 50 alumnos.

Contenidos:

Parte 1: Introducción a la Seguridad Informática

- Panorama de la seguridad informática: principios fundamentales (confidencialidad, integridad, disponibilidad), actores del sector, marcos legales y éticos.
- La industria de la seguridad: roles y especialidades (pentester, analista de malware, ingeniero de seguridad, investigador, entre otros), certificaciones relevantes y posibles caminos de carrera.
- Introducción a los CTFs: historia y formato de las competencias, plataformas más utilizadas, cómo iniciarse. Herramientas y entorno de trabajo. Linux y scripting básico.

Parte 2: Seguridad Web (WEB)

- Fundamentos: protocolo HTTP, herramientas de interceptación (Burp Suite), reconocimiento y enumeración web.
- Técnicas: inyección SQL, cross-site scripting (XSS), server-side template injection (SSTI), inclusión de archivos.

Parte 3: Ingeniería Inversa

- Fundamentos: arquitectura x86/x64, lenguaje ensamblador, herramientas de análisis estático (Ghidra).
- Técnicas: análisis dinámico, crackmes, ofuscación y anti-debugging.

Parte 4: Pentesting

- Reconocimiento y enumeración: escaneo de puertos, identificación de servicios, enumeración de usuarios y recursos.
- Explotación y post-explotación: uso de exploits públicos, escalada de privilegios, movimiento lateral.

Parte 5: Explotación de Binarios

- Fundamentos: memoria de procesos, desbordamiento de buffer, shellcoding.
- Técnicas: Buffer overflow, return-to-libc, cadenas ROP (Return-Oriented Programming), protecciones modernas y cómo superarlas.

Parte 6: Práctica Integradora

- Mini-CTF interno: desafíos integradores que combinan las categorías vistas, con resolución guiada.
- CTF final y cierre: competencia final con desafíos en todas las categorías. Repaso general y orientación sobre cómo continuar aprendiendo.

El programa es tentativo y está sujeto a cambios que veamos necesarios según el nivel de los alumnos y posibles temas en los que los asistentes quieran profundizar.

Bibliografía:

- Trail of Bits. *CTF Field Guide*. Disponible en: https://trailofbits.github.io/ctf/
- pwn.college. Plataforma de educación en seguridad informática. Disponible en: https://pwn.college/
- Jon Erickson. *Hacking: The Art of Exploitation*, 2nd edition. No Starch Press, 2008.
- Dafydd Stuttard, Marcus Pinto. *The Web Application Hacker's Handbook*, 2nd edition. Wiley, 2011.
- Plataforma HackTheBox: https://www.hackthebox.com/
- Plataforma CTFtime: https://ctftime.org/
- Plataforma picoCTF: https://picoctf.org/

Duración, carga horaria y fechas estipuladas de las clases: Del 31 de marzo al 16 de junio de 2026, con una carga horaria de 24 horas, dictando 2 horas de clases semanales los días martes de 18:00 a 20:00 hs.

Requisitos de Aprobación: Saber poner en práctica los contenidos enseñados para resolver desafíos CTF de dificultad introductoria. Se entregarán desafíos de cada categoría y los estudiantes deberán resolver un porcentaje mínimo de ellos.

Modalidad: Presencial. El objetivo es que todas las clases sean presenciales. En caso de que alguna clase deba dictarse de forma remota, se avisará con anticipación.

Lugar en que se dictará el curso: Laboratorios de FAMAF y videollamada de Google Meet.

Equipamiento necesario para el dictado: Proyector y computadoras con acceso a internet, incluidos en el aula que solicitamos. Para las instancias remotas: cuenta de Google Meet que permita grabar videollamadas.

Factibilidad económica (arancel estipulado, en caso que corresponda, y destino de los fondos): No se necesitan fondos de ningún tipo ya que todos los docentes trabajarán ad-honorem.

Otra información: Para consultas comunicarse con Gastón Aznarez (gastonaznarez@gmail.com).