DESCRIPCIÓN Y HORARIO DE CURSOS III-2019

Curso: **PF-3893 Seguridad aplicada a infraestructura**
Profesor: **Mag. Jorge Castro** **nachix_cr@yahoo.com**
Horario: **Lunes y Jueves 17-20:50**
Aula: **103 IF**

El curso seguridad aplicada infraestructura introduce al estudiante en el mundo de los conocimientos teóricos y prácticos que se requieren hoy día para conectar un computador de forma segura a una red. Además de aprender los fundamentos teóricos para asegurar un computador y su entorno de red, se estudiarán técnicas comúnmente usadas por "hackers" en intrusión de sistemas informáticos. En el curso se considera la información en sus tres estados: cuando se encuentra almacenada, en procesamiento o mientras es transmitida; también considera los servicios de seguridad usualmente requeridos como son disponibilidad, integridad, autenticación, confidencialidad y no repudio; y propone la definición de políticas y procedimientos en conjunto con la implementación de contoles tecnológicos para contrarestar las vulnerabilidades en los sistemas estudiados.

El curso cubre temas de seguridad perimetral de red, como firewalls, y seguridad de host donde se analizan aspectos del sistema de archivos, confinamiento, cajas de arena para protección de servicios y canales de comunicación encubiertos. En autenticación se estudian temas de single-sign-on y manejo de llaves. En el área de criptografía se estudian protocolos para encripción de canales de comunicación, como es el caso del protocolo SSL que soporta las comunicaciones seguras en el World Wide Web a través del protocolo HTTPS, así como el protocolo IPSec para configuración de redes privadas virtuales (VPNs), entre otros. En el curso de laboratorio (para estudiantes de maestría profesional) se desarrollará un trabajo de investigación en temas variados, por ejemplo seguridad de máquinas virtuales, seguridad en cloud computing, análisis de malware u otros temas de interés que podrían servir de base para desarrollar el TFIA.

La metodología de trabajo contempla un alto componente práctico, para cada tema relevante se hará una tarea/laboratorio que involucra configuración y aplicación de controles de seguridad o técnicas de hacking estudiadas en clase. Por el tipo de temas a tratar se requiere que el estudiante disponga de un computador de trabajo que permita instalar máquinas virtuales en ambientes Windows y Linux, de forma que se puedan aislar las tareas sin afectar otros computadores conectados en el mismo ambiente de red o incluso Internet, como es el caso del análisis de malware. En ocasiones anteriores ha sido suficiente un computador portátil con alguno de los sistemas operativos mencionados, al menos 2 Gb de memoria RAM (preferiblemente 4 Gb) y suficiente espacio en disco para correr dos o tres máquinas virtuales a la vez.

El curso está orientado a estudiantes de nivel de maestría con énfasis en infraestructura y/o desarrollo de software y que tengan interés por aprender temas de seguridad de la infraestructura tecnológica sobre la cual corren todas las aplicaciones computacionales hoy día.

IMPORTANTE

Los estudiantes de maestría profesional deben matricular el curso laboratorio asociado al curso teórico.

Teléfono 2511-8017
Correo electrónico: posgrado@ecci.ucr.ac.cr