Programación de computadores

Guía de asignatura

Última actualización: julio de 2020

1. Información general

Nombre de la asignatura	Hacking Etico
Código	11310047
Tipo de asignatura	Electiva
Número de créditos	2
Tipo de crédito	2A
Horas de trabajo semanal con acompañamiento directo del profesor	4
Horas semanales de trabajo independiente del estudiante	2
Prerrequisitos	Bases de datos
Correquisitos	Ninguno
Horario	Martes de 11:00 a 13:00 Jueves de 11:00 a 13:00
Líder de área	Daniel Orlando Díaz López Correo: danielo.diaz@urosario.edu.co
Salón	Salón virtual. Link en e-aulas.

2. Información del profesor y monitor

Nombre del profesor	**Diego Espitia**
Perfil profesional	Ingeniero electrónico, especialista en seguridad de redes y certificado como ethical hacker de EC-Council. Cuenta con 15 años de experiencia en proyectos de implementación, análisis y pruebas de ciberseguridad en múltiples entornos empresariales, siendo parte del equipo de respuesta en eventos de incidentes multinacionales con procesos de contención y análisis forense en casos de Ransomware y de fugas de información. Además, he participado en los equipos

	de desarrollo en sistemas de análisis forense basado en parseo de eventos en sistemas Linux.
Correo electrónico institucional	diegos.espitia@urosario.edu.co
Lugar y horario de atención	Jueves de 2:00 a 3:00 pm (Atención virtual) Viernes de 2:00 a 3:00 pm (Atención virtual)
Página web u otros medios (opcional)	Linkedin Profile Github Profile

3. Resumen y propósitos del curso

Este curso de hacking ético se desarrolla con el objetivo de formar profesionales orientados a mejorar la seguridad de una organización por medio de la detección y corrección de brechas. Particularmente, este curso le brindará al estudiante los conocimientos necesarios para desarrollar labores de identificación de vulnerabilidades en infraestructuras tecnológicas, estimar los mecanismos de explotación más oportunos y proponer medidas de mitigación.

El curso se desarrollará usando la práctica como base fundamental para la apropiación de conocimientos y un acercamiento a las necesidades actuales de la industria.

4. Conceptos fundamentales

1. Scanning networks
2. System Hacking
3. Footprinting and reconnaissance
4. Enumeration and Vulnerability Analysis
5. Malware Threats
6. Sniffing and Social Engineering
7. Denial-of-service and Session Hijacking
8. Evading IDS, Firewalls and Honeypots
9. Hacking Web Servers
10. Hacking Web Applications
11. SQL injection
12. Hacking Wireless Networks
13. Hacking Mobile Platforms
14. IoT Hacking and Cloud Computing

5. Resultados de aprendizaje esperados (RAE)

1. Identificar las fases de una prueba de penetración de hacking ético.
2. Aprender el uso de técnicas y herramientas asociadas a cada fase de la prueba de penetración.
3. Detectar las diferentes calificaciones de vulnerabilidades conocidas en los sistemas informáticos.
4. Aprender técnicas activas y pasivas usadas habitualmente para el aprovechamiento de brechas de seguridad.
5. Conocer los diferentes mecanismos de evasión de los componentes de seguridad usuales de una red.
6. Realizar pruebas de seguridad en servicios y servidores.
7. Identificar y validar brechas de seguridad en motores de bases de datos.
8. Realizar pruebas de seguridad en redes inalámbricas.
9. Identificar los principales riesgos de las aplicaciones móviles.
10. Reconocer e identificar debilidades en sistemas de IoT.

6. Modalidad del curso

Remota: Todos sus estudiantes estarán conectados remotamente desde sus casas o ubicaciones externas a la Universidad.

7. Estrategias de aprendizaje

La secuencia de aprendizaje que se trabajará en el curso es la siguiente:

- Antes de clase: El estudiante debe estudiar el material propuesto por el profesor: Videos, documentos, etc.
- Durante la clase: El profesor mostrará los conceptos principales de cada uno de los temas, con ejemplos prácticos o basados en situaciones vividas durante la ejecución de estos procesos. Esto se reforzará con un taller o ejercicio práctico según el tema a tratar.
- Después de clase: Los estudiantes terminan el trabajo o taller realizado en clase, buscando terminar todos los retos de hacking propuestos.
- Proyecto de semestre, en el que los estudiantes, por grupos, aplican los conocimientos adquiridos en la solución de un problema particular

8. Actividades de evaluación

Tema	Actividad de evaluación	Porcentaje
Corte 1 (20%)	Laboratorio 1: Introducción, footprinting y Reconocimiento	4%
	Laboratorio 2: Escaneo de redes y enumeración	8%
	Laboratorio 3: Análisis de Vulnerabilidades y hacking de sistemas	8%
Corte 2 (20%)	Laboratorio 4: Análisis de malware y sniffing	8%
	Laboratorio 5: Ingeniería Social	4%
	Laboratorio 6: Denegación de Servicio y Hijacking	8%
Corte 3 (20%)	Laboratorio 7: Hacking web	8%
	Laboratorio 8: SQLi	8%
	Laboratorio 9: Hacking de Wireless	4%
Corte 4 (15%)	Laboratorio 10: Hacking en Móviles	7.5%
	Laboratorio 11: Cloud Hacking	7.5%
Corte 5 (25%)	Proyecto curso	25%

9. Programación de actividades

Fecha	Tema	Descripción de la actividad	Trabajo independiente del estudiante	Recursos que apoyan la actividad (bibliografía y otros recursos de apoyo)
26 - Julio	Introducción al hacking			[1] Modulo 1
28 - Julio	Footprinting and Reconnaissance			[1] Modulo 2
2 - Ago	Footprinting and Reconnaissance	Laboratorio		[1] Modulo 2
4 - Ago	Scanning Networks			[1] Modulo 3
9 - Ago	Enumeración			[1] Modulo 4
11- Ago	Enumeración	Laboratorio		[1] Modulo 4

18 – Ago	Análisis de vulnerabilidades			[1] Modulo 5
23 - Ago	Análisis de vulnerabilidades			[1] Modulo 5
25 - Ago	Hackear sistemas			[1] Modulo 6
30 - Ago	Hackear sistemas			[1] Modulo 6
1 - Sep	Hackear sistemas	Laboratorio		[1] Modulo 6
6 - Sep	Análisis de Malware			[1] Modulo 7
8 - Sep	Sniffing	Laboratorio		[1] Modulo 8
13 - Sep	Ingeniería Social			[1] Modulo 9
15 - Sep	Ingeniería Social	Laboratorio		[1] Modulo 9
20 - Sep	Denegación de servicio			[1] Modulo 10
22 - Sep	Session Hijacking	Laboratorio		[1] Modulo 11
27 - Sep	Evasión de medidas de seguridad			[1] Modulo 12
29 - Sep	Hacking Web server			[1] Modulo 13
4 - Oct	Hacking Web			[1] Modulo 13 y 14
6 - Oct	Hacking Aplicaciones Web	Laboratorio		[1] Modulo 14
11 - Oct	SQLi			[1] Modulo 15
13 - Oct	SQLi	Laboratorio		[1] Modulo 15
	Semana Rosarista			
	Semana Rosarista			
25 - Oct	Hacking en Wireless			[1] Modulo 16
27 - Oct	Hacking en Wireless	Laboratorio		[1] Modulo 16
3 - Nov	Hacking en Moviles			[1] Modulo 17
8 - Nov	Hacking en Moviles	Laboratorio		[1] Modulo 17
10 - Nov	IoT Hacking			[1] Modulo 18
18 - Nov	Cloud Hacking	Laboratorio		[1] Modulo 19

10. Factores de éxito para este curso

A continuación se sugieren una serie de acciones que pueden contribuir, de manera significativa, con el logro de metas y consecuentemente propiciar una experiencia exitosa en este curso:

1. Planificar y organizar el tiempo de trabajo individual que le dedicará al curso

2. Organizar el sitio y los materiales de estudios

3. Tener un grupo de estudio, procurar el apoyo de compañeros

4. Cultivar la disciplina y la constancia, trabajar semanalmente, no permitir que se acumulen temas ni trabajos

5. Realizar constantemente una autoevaluación, determinar si las acciones realizadas son productivas o si por el contrario se debe cambiar de estrategias

6. Asistir a las **horas de consulta del profesor**, participar en clase, no quedarse nunca con la duda

7. Utilizar los espacios destinados para consultas y resolución de dudas, tales como **Sala Gauss y Sala Knuth**

8. Propiciar espacios para el descanso y la higiene mental, procurar tener buenos hábitos de sueño

9. Tener presente en todo momento valores como la honestidad y la sinceridad, al final no se trata solo de aprobar un examen, se trata de aprender y adquirir conocimientos. El fraude es un autoengaño.

11. Bibliografía y recursos

[1] Ethical Hacking and Countermeasures, EC-Council, Versión 10 (2018)

12. Bibliografía y recursos complementarios

[2] Mastering Python for Networking and Security: José Manuel Ortega, www.packt.com; 2nd Edition(2020

[3] Ethical Hacking: teoría y práctica para la realización de un pentesting, 0xWord, 2da Edición (2020)

13. Acuerdos para el desarrollo del curso

- Ser puntual al asistir a clase. En modalidad virtual, mantener el micrófono apagado y pedir la palabra para intervenir. No está permitido comer o usar la computadora o dispositivos móviles para realizar actividades no relacionadas con la clase durante su duración.
- Todas las sesiones y actividades del curso son de carácter teórico-práctico; es decir, incluyen clases magistrales, discusiones, ejercicios o talleres.
- Para todas las sesiones se espera que el estudiante realice un trabajo independiente previo que permita un avance continuo en los temas y facilite el entendimiento de los mismos.

- No se realizará aproximación de notas al final del semestre. Las notas solo serán cambiadas con base en reclamos OPORTUNOS dentro de los límites de tiempo determinados por el Reglamento Académico. Si por motivos de fuerza mayor el estudiante falta a algún parcial o quiz, deberá seguir el procedimiento regular determinado por el Reglamento Académico para presentar supletorios. No habrá acuerdos informales al respecto. No se eximirá a ningún estudiante de ningún examen.
- Todas las sesiones serán grabadas y quedarán disponibles en el aula virtual del curso y en el repositorio institucional. Este material es de consulta y repaso y no pretende reemplazar la participación de los estudiantes en las sesiones. Sin embargo, es de gran utilidad en los casos eventuales en los que alguno de los participantes presente fallas en la conexión.
- Con el propósito de afianzar el modelo pedagógico contemplado en el Proyecto Educativo Institucional y promover un rendimiento académico óptimo, es necesario asegurar un espacio de interacción entre estudiantes y profesores que facilite la reflexión y el debate académico en torno al conocimiento. En este sentido, se valora la participación en las actividades académicas y esta se considera como un deber y un derecho del estudiante. (Artículo 48 Reglamento Académico). **De no asistir a más del 80% de las clases el 15% se pierde con 0.0.**
- Si el estudiante se presenta 20 minutos luego de dar inicio a alguna evaluación parcial o final, no podrá presentarla y deberá solicitar supletorio siguiendo la reglamentación institucional.
- Teniendo en cuenta el reglamento formativo-preventivo y disciplinario de la Universidad del Rosario, y la certeza de que las acciones fraudulentas van en contra de los procesos de enseñanza y aprendizaje, cualquier acto corrupto vinculado a esta asignatura será notificado a la secretaría académica correspondiente de manera que se inicie el debido proceso disciplinario. Se recomienda a los estudiantes leer dicho reglamento para conocer las razones, procedimientos y consecuencias que este tipo de acciones pueden ocasionar, así como sus derechos y deberes asociados a este tipo de procedimientos.
- La asignatura no tiene ningún tipo de Bono. Los exámenes parciales se realizarán de forma sincrónica a través de la plataforma zoom, durante el examen el estudiante debe tener la cámara encendida.

14. Respeto y no discriminación

Si tiene alguna discapacidad, sea esta visible o no, y requiere algún tipo de apoyo para estar en igualdad de condiciones con los(as) demás estudiantes, por favor informar a su profesor(a) para que puedan realizarse ajustes razonables al curso a la mayor brevedad posible. De igual forma, si no cuenta con los recursos tecnológicos requeridos para el desarrollo del curso, por favor informe de manera oportuna a la Secretaría Académica de su programa o a la Dirección de Estudiantes, de manera que se pueda atender a tiempo su requerimiento.

Recuerde que es deber de todas las personas respetar los derechos de quienes hacen parte de la comunidad Rosarista. Cualquier situación de acoso, acoso sexual, discriminación o matoneo, sea presencial o virtual, es inaceptable. Quien se sienta en alguna de estas situaciones puede denunciar

su ocurrencia contactando al equipo de la Coordinación de Psicología y Calidad de Vida de la Decanatura del Medio Universitario (Teléfono o WhatsApp 322 2485756).