UNIVERSIDAD DEL ROSARIO

Guía de asignatura

Formato institucional – Rev. Abril 2013

Información general

Asignatura	HACKING ETICO				
Código	11310047				
Tipo de asignatura	**Obligatoria**	**Electiva X**			
Tipo de saber	**Obligatoria básica o de fundamentación**	**Obligatoria profesional**	**Obligatoria complementaria**		
Número de créditos	2 (dos)				
Tipo de crédito	2A				
Horas de trabajo con acompañamiento directo del profesor	32	**Horas de trabajo independiente del estudiante**	64	**Total de horas**	96
Prerrequisitos	Programación de computadores				
Correquisitos	Ninguno				

Horario		Lunes 9:00 a 11:00
Salón		Sala informática - HIPATIA
Profesor	**Nombre**	Daniel Orlando Díaz López
	Correo electrónico	danielo.diaz@urosario.edu.co
	Lugar y horario de atención	Edificio Cabal. Jueves de 14:00 a 16:00
	Página web	https://dodiazlopez.github.io/main/
Profesor auxiliar o monitor	**Nombre**	
	Correo electrónico	
	Lugar y horario de atención	
	Página web	

UNIVERSIDAD DEL ROSARIO

Resumen y propósitos de formación 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 mas oportunos y proponer medidas de mitigación. La forma de desarrollar el curso es completamente práctica buscando una mayor apropiación de conocimientos y un acercamiento a las necesidades actuales de la industria.

Temas

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

Resultados de aprendizaje esperados (RAE)

1. Usar diferentes mecanismos para el reconocimiento de infraestructura tecnológica
2. Escanear redes para conocer la topología de una organización
3. Identificar vulnerabilidades conocidas en sistemas de información
4. Desarrollar de actividades de hacking ético sobre sistemas informáticos
5. Identificar amenazas de malware
6. Usar diferentes técnicas para adelantar actividades de ingeniería social y sniffing de

red
7. Ejecutar ataques de denegación de servicios y secuestro de sesión
8. Evadir componentes de seguridad perimetral tales como IDS, Firewalls y Honeypots
9. Realizar actividades de hacking ético a servidores y aplicaciones web
10. Ejecutar ataques a bases de datos
11. Desarrollar ataques a redes inalámbricas
12. Identificar los principales aspectos de la seguridad en móviles
13. Reconocer la forma de proteger ambientes IoT y de nube
14. Comprender los aspectos fundamentales de la criptografía

Actividades de aprendizaje

1. Clases magistrales donde se ilustrarán los conceptos asociados a cada uno de los temas de hacking ético
2. Laboratorios donde se resolverán retos de hacking
3. Proyecto final donde se profundizará en uno de los temas del curso y se socializarán los resultados

Actividades de evaluación

Tema	Actividad de evaluación	Porcentaje
	Laboratorio 1	5.625%
	Laboratorio 2	5.625%
	Laboratorio 3	5.625%
	Laboratorio 4	5.625%
	Laboratorio 5	5.625%
	Laboratorio 6	5.625%
	Laboratorio 7	5.625%
	Laboratorio 8	5.625%
	Laboratorio 9	5.625%
	Laboratorio 10	5.625%
	Laboratorio 11	5.625%
	Laboratorio 12	5.625%
	Laboratorio 13	5.625%
	Laboratorio 14	5.625%

	Laboratorio 15	5.625%
	Laboratorio 16	5.625%
	Proyecto	10%

Programación de actividades por sesión

Fecha (Sesión)	Tema	Descripción de la actividad	Trabajo independiente del estudiante	Recursos que apoyan la actividad
29 jul	Footprinting and reconnaissance			[1] Cap. 1 y 2
5 ago	Scanning networks			[1] Sec. 3.1 a 3.7
12 ago	Enumeration and Vulnerability Analysis			[1] Sec. 4.1 a 4.5
19 ago	System Hacking			[1] Sec. 5.1 a 5.4
26 ago	Malware Threats			[2] Sec. 1.9 a 1.12
	1er corte			
2 sep	Sniffing and Social Engineering			[2] Cap. 2
9 sep	Denial-of-service and Session Hijacking			[2] Cap. 3
16 sep	Evading IDS, Firewalls and Honeypots			[2] Cap. 4
23 sep	Hacking Web Servers			[2] Sec. 5.1 a 5.7
30 sep	Hacking Web Applications			[2] Sec. 5.8 a 5.11
7 oct	SQL injection			[2] Cap. 6
	2do corte			
21 oct	Hacking Wireless Networks			[2] Sec. 7.1 a 7.13
28 oct	Hacking Mobile Platforms			[2] Sec. 7.14 a 7.22
4 nov	IoT Hacking			[2] Cap. 8 y Cap. 9
11 nov	Cloud Computing			[2] Cap. 11 y Cap. 20
18 nov	Cryptography			[2] Cap. 12 y Cap. 13
	3er corte			

UNIVERSIDAD DEL ROSARIO

Bibliografía

[1] CEH Certified Ethical Hacker Practice Exams, Fourth Edition, Matt Walker, McGraw Hill Professional (2019)

[2] Beginning Ethical Hacking with Kali Linux: Computational Techniques for Resolving Security Issues, Sanjib Sinha, Apress (2018)

[3] Cracking Codes with Python: An Introduction to Building and Breaking Ciphers, Al Sweigart, No Starch Press (2018)

[4] Open Source Intelligence Techniques, Michael Bazzel, 6th Edition, CreateSpace Independent Publishing Platform (2018)

Bibliografía complementaria

[5] https://github.com/trustedsec/social-engineer-toolkit/

[6] https://github.com/certtools/intelmq

[7] https://www.misp-project.org/

[8] https://www.elastic.co/es/

Acuerdos de funcionamiento (Reglas de juego)

No está permitido comer o usar dispositivos móviles dentro de clase. 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.

ASISTENCIA AL CURSO

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 tormo 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.

PROCESOS DISCIPLINARIOS-FRAUDE EN EVALUACIONES

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.