Análisis forense y gestión de incidentes

Guía de asignatura

Última actualización: julio de 2020

1. Información general

Nombre de la asignatura	Análisis forense y gestión de incidentes
Código	11310058
Tipo de asignatura	Electiva
Número de créditos	2
Tipo de crédito	1A+1B
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 y Jueves 7:00 a 9:00 am
Líder de área	Daniel Díaz Correo: danielo.diaz@urosario.edu.co
Salón	Salón virtual. Link en e-aulas o aquí: https://urosario.zoom.us/j/8615986392

2. Información del profesor y monitor

Nombre del profesor	**Daniel Díaz**
Perfil profesional	Doctorado en Ciencias de la Computación de la Universidad de Murcia (España). Daniel realiza investigaciones en ciberseguridad y tiene experiencia en la gestión de infraestructura tecnológica para centros de datos, diseño de redes de comunicación seguras e implementación de sistemas de gestión de seguridad de la información. Sus áreas de investigación son: Técnicas para ciberinteligencia, mecanismos de preservación de la privacidad, ciclo de vida seguro de desarrollo de software, piratería ética y seguridad para IoT.

Correo electrónico institucional	danielo.diaz@urosario.edu.co
Lugar y horario de atención	Miércoles de 2:00 a 3:00 pm (Atención virtual) Viernes de 3:00 a 4:00 pm (Atención virtual)
Página web u otros medios (opcional)	Github Profile Google Scholar Profile URosario Pure Profile Whatsapp

3. Resumen y propósitos del curso

La informática forense permite determinar las circunstancias en las cuales ocurre un incidente con el fin de identificar evidencia y atribución que pueda ser usable (si aplica) en un proceso legal. Para garantizar que la evidencia es procesada de manera correcta se debe seguir una metodología de recolección y análisis, al igual que se tienen que tener competencias técnicas en el uso de herramientas forenses adecuadas para cada caso.

El propósito de este curso es formar a los estudiantes en las capacidades básicas de un analista forense, para lo cual es indispensable entender la importancia de los procedimientos y la necesidad de la rigurosidad de los mismos, con el fin de poderlos convertir en pruebas irrefutables del hecho analizado.

El objetivo de este curso es conocer las metodologías para realizar pruebas forenses informáticas, validar las técnicas de recolección de evidencia - según el tipo de fuente a procesar, aprender el uso de algunas herramientas open source que permiten realizar los procesos forenses y conocer cómo tratar y gestionar evidencias digitales.

4. Conceptos fundamentales

1. Principio de Locard aplicado en informática
2. Recolección de evidencia en sitio
3. Análisis de capturas de tráfico de red
4. Análisis de Malware básico y avanzado
5. Mantenimiento de la cadena de custodia
6. Integridad de la evidencia
7. Recolección de evidencia según el tipo de fichero

5. Resultados de aprendizaje esperados (RAE)

1. Reconocer el **rol** de un miembro de un equipo de primera respuesta de incidentes cibernéticos, en la fase de recolección de evidencias.
2. Conocer las **técnicas apropiadas para la recolección de evidencias** según el tipo de fuente a analizar.
3. Realizar a**nálisis de eventos** para dirigir investigaciones
4. Realizar **análisis de malware** (básico y avanzado) como parte de un proceso de análisis forense
5. Realizar copias forenses informáticas

6. Modalidad del curso

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

7. Estrategias de aprendizaje

- Análisis de casos
- Desarrollo de un proyecto de curso
- Talleres o ejercicios
- Enfoque de Aprender a Aprender: Aprendizaje activo, autorregulado, colaborativo, significativo, reflexivo

8. Actividades de evaluación

Se evalúa a través de 14 laboratorios (aproximadamente 1 semanal) los cuales representan el 80% de la nota del curso, es decir 4 cortes. Adicionalmente existe un proyecto final de curso que los estudiantes comienzan desde la semana 7 aproximadamente y terminan en la última semana de clase, el cual vale el 20% de la nota total del curso. Un laboratorio puede ser intercambiado por un test u otra actividad de evaluación en función de la temática y la necesidad. Una tabla que representa lo anterior se muestra a continuación:

Corte	Actividad de evaluación	Porcentaje
Corte 1 (20%)	Laboratorio 1	5 %
	Laboratorio 2	5 %
	Laboratorio 3	5 %
	Laboratorio 4	5 %

Corte 2 (20%)	Laboratorio 5	5 %
	Laboratorio 6	5 %
	Laboratorio 7	5 %
	Laboratorio 8	5 %
Corte 3 (20%)	Laboratorio 9	6.66 %
	Laboratorio 10	6.66 %
	Laboratorio 11	6.66 %
Corte 4 (20%)	Laboratorio 12	6.66 %
	Laboratorio 13	6.66 %
	Laboratorio 14	6.66 %
Corte 5 (20%)	Proyecto	20%

9. Programación de actividades

Fecha	Tema	Descripción de la actividad	Trabajo independiente del estudiante	Recursos que apoyan la actividad
Sesión 1 Martes 4/08	Cybersecurity Concepts			
Sesión 2 Jueves 6/08	Cybersecurity Concepts		AWS Security Badges	AWS Educate
Sesión 3 Martes 11/08	Malware analysis primer			Practical Malware Analysis
Sesión 4 Jueves 13/08	Basic Static Techniques		Lab of Malware analysis	Practical Malware Analysis
Sesión 5 Martes 18/08	Analysis using VM			Practical Malware Analysis

Sesión 6 Jueves 20/08	Basic Dynamic Analysis		Lab with sandbox	Practical Malware Analysis
Sesión 7 Martes 25/08	Disassembly			Practical Malware Analysis
Sesión 8 Jueves 27/08	IDAPro		Lab with IDA Pro Reversing	Practical Malware Analysis
Sesión 9 Martes 1/08	Code constructs			Practical Malware Analysis
Sesión 10 Jueves 3/09	Code constructs		Lab Code C with IDA Pro	Practical Malware Analysis
Sesión 11 Martes 8/09	Windows malware			Practical Malware Analysis
Sesión 12 Jueves 10/09	Windows malware		Lab Exe with IDA Pro	Practical Malware Analysis
Sesión 13 Martes 15/09	Modifying execution			Practical Malware Analysis
Sesión 14 Jueves 17/09	Modifying execution		Lab WinDBG , OllyDBG	Practical Malware Analysis
Lunes 21/09	Semana Rosarista			
Miércoles 23/09	Semana Rosarista			
Sesión 15 Martes 29/09	Malware as a service	*Lineamientos del Proyecto*		
Sesión 16 Jueves 1/10	Malware as a service		Lab Keitaro	Practical Malware Analysis, Análisis Forense Digital
Sesión 17 Martes 6/10	Threat intelligence			Practical Malware Analysis, Análisis Forense Digital
Sesión 18 Jueves 8/10	Threat intelligence		Lab IoC, VPN, TOR, TTP, OTX	Practical Malware Analysis, Análisis Forense Digital

Sesión 19 Martes 13/10	Recolección de evidencia			Practical Malware Analysis, Análisis Forense Digital
Sesión 20 Jueves 15/10	Recolección de evidencia		Lab Volcado de memoria ram y copia de disco duro	Practical Malware Analysis, Análisis Forense Digital
Sesión 21 Martes 20/10	Recolección de evidencia			Practical Malware Analysis, Análisis Forense Digital
Sesión 22 Jueves 22/10	Recolección de evidencia		Lab Recolección de emails y ficheros	Practical Malware Analysis, Análisis Forense Digital
Sesión 23 Martes 27/10	Análisis de evidencia			Practical Malware Analysis, Análisis Forense Digital
Sesión 24 Jueves 29/10	Análisis de evidencia		Lab Secuencia Temporal	Practical Malware Analysis, Análisis Forense Digital
Sesión 25 Martes 3/11	Análisis de evidencia			Practical Malware Analysis, Análisis Forense Digital
Sesión 26 Jueves 5/11	Análisis de evidencia		Lab Análisis de Vulnerabilidades	Practical Malware Analysis, Análisis Forense Digital
Sesión 27 Martes 10/11	Procedimiento de respuesta a incidentes			Practical Malware Analysis, Análisis Forense Digital
Sesión 28 Jueves 12/11	Procedimiento de respuesta a incidentes		Lab Procedimiento de respuesta a incidentes	Practical Malware Analysis, Análisis Forense Digital
Sesión 29 Martes 17/11	Análisis avanzado de Malware			Practical Malware Analysis, Análisis Forense Digital
Sesión 30 Jueves 19/11	Análisis avanzado de Malware		Lab Wannacry, Morris worm	Practical Malware Analysis, Análisis Forense Digital
Sesión 31 Martes 24/11	Análisis avanzado de Incidentes y Delitos			Practical Malware Analysis, Análisis Forense Digital

Sesión 32 Jueves 26/11	Análisis avanzado de Incidentes y Delitos		Lab Snowden, Art of war	Practical Malware Analysis, Análisis Forense Digital
Sesión 33 Semana 30 Noviembre	**PRESENTACIÓN DE PROYECTO FINAL Martes 1 de diciembre o Jueves 3 de Diciembre**			

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

- Análisis Forense Digital. Miguel López Delgado, Hackers & Seguridad, Edición 2a, Junio 2007.
- Practical Malware Analysis, The hands-on Guide to Dissecting Malicious Software. Michael Sikorski and Andrew Honing, No starch press, 2012.

- Técnicas de Análisis Forense informático para Peritos Judiciales profesionales. 0xword. Pilar Vila Avendaño. 978-84-697-7700-8. 240 páginas.

12. Bibliografía y recursos complementarios

- Análisis Forense Digital en Entornos Windows. 3ª Edición. 0xword. Juan Garrido Caballero, Juan Luis G. Rambla y Chema Alonso. 978-84-616-0392-3. 253 páginas.

13. Acuerdos para el desarrollo del curso

- Los estudiantes se deben conectar a la sesión de Zoom en el horario establecido.
- Los estudiantes podrán hacer intervenciones a través del chat o levantando la mano por medio de la herramienta disponible en zoom.
- En el momento de la intervención y según la calidad de la conexión a internet, se solicita que el estudiante active su cámara.
- Mientras no esté haciendo una intervención se solicita al estudiante desactivar su micrófono.
- 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.

14. Respeto y no discriminación

Si tiene alguna discapacidad, sea este 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).

Universidad del Rosario