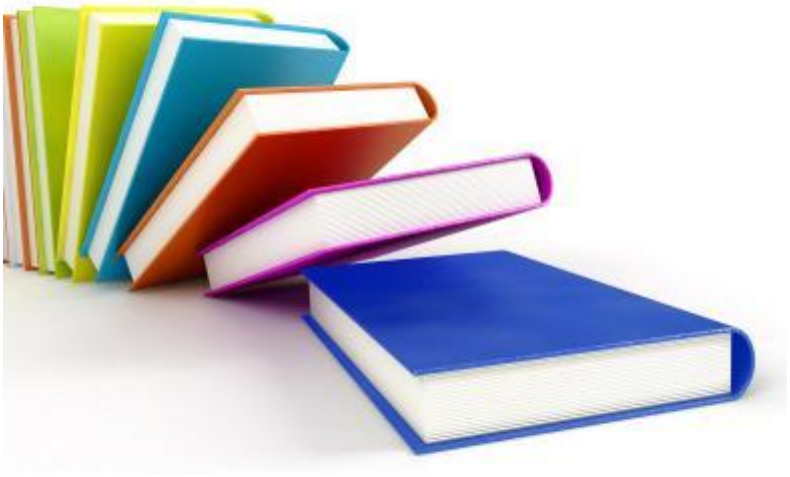
ANEXO D



ANEXO D

Credenciales para investigadores forenses en informática

Dr. Jeimy J. Cano
jcano@uniandes.edu.co
Ingeniero de Sistemas y Computación
Universidad de los Andes
COLOMBIA
Artículos de Seguridad Informática y Seguridad de Redes
http://www.virusprot.com/Art15.html

Es un hecho que durante la última década las intrusiones e incidentes de seguridad han crecido de manera exponencial estableciendo un escenario oscuro sobre la seguridad de las infraestructuras de computación en el mundo.

En este sentido, las organizaciones han adelantado análisis de su seguridad, instalando múltiples mecanismos de protección y efectuando múltiples pruebas con el fin de mejorar las condiciones de seguridad existentes en cada uno de sus entornos de negocio. Sin embargo, dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre se tiene, por tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente.

Por un lado, un incidente representa un reto de la gerencia corporativa para demostrar la diligencia de su organización para enfrentar el hecho, tomar el control, recoger y analizar la evidencia, y finalmente generar el reporte sobre lo ocurrido, que incluye las recomendaciones de seguridad y concepto sobre los hechos del incidente. Por otro, es un

compromiso de las instancias técnicas por estar preparadas para actuar y regular el efecto que dicho incidente puede ocasionar a la corporación.

Estas dos visiones, nos ofrecen un marco de reflexión alrededor de la seguridad y la preparación requerida por los profesionales que se encuentran a cargo de las funciones de seguridad informática en las organizaciones. En este sentido, administrar un incidente de seguridad requiere experiencia y habilidades técnicas para controlar las acciones del atacante, pero al mismo tiempo habilidad y pericia para establecer los rastros y registros de dichas acciones con las cuales relacionar las acciones y efectos ocasionados por el intruso dentro del sistema.

En este breve documento nos concentraremos en la habilidad, preparación y pericia requerida para identificar, recoger, analizar, conceptuar y reportar sobre evidencia digital presente en un incidente de seguridad.

Los investigadores forenses en informática, profesionales que contando con un conocimiento de los fenómenos técnicos en informática, son personas preparadas para aplicar procedimientos legales y técnicamente válidos para establecer evidencia en situaciones donde se vulneran o comprometen sistemas, utilizando métodos y procedimientos científicamente probados y claros que permitan establecer posibles hipótesis sobre el hecho y contar con la evidencia requerida que sustente dichas hipótesis.

Con el fin de desarrollar este perfil forense en informática, se han adelantado esfuerzos importantes en el mundo para contar con documentación, entrenamiento y procedimientos de aplicación generalmente aceptada que permitan validar actuaciones y valoraciones de profesionales forenses en informática de manera estándar en el mundo. En este sentido, **la IACIS - International Association of Computer Investigative Specialist (http://www.cops.org) y la HTCN (http://www.htcn.org) - High Technology Crime Netwok,** dos

asociaciones internacionales han desarrollado programas de certificación forenses en informática, que permiten detallar las habilidades requeridas y las capacidades deseables en los investigadores informáticos.

La IACIS ofrece la certificación internacional denominada CFEC - Computer Forensic External Certification, la cual se encuentra diseñada para personas que no pertenezcan a instituciones judiciales o de policía, para los cuales el programa cuenta con algunas diferencias, dada su función, pero con el mismo contenido para los aplicantes externos. Para aplicar a esta certificación, es necesario girar US$1250 a IACIS, diligenciar una forma de aplicación con múltiples datos del aspirante, la cual es evaluada por el comité de IACIS. Si esta forma es aceptada, se inicia el proceso de evaluación el cual consiste en el análisis de seis diskettes especialmente preparados y un disco duro con una disposición especial. Cada uno de los diskettes establece un problema técnico y forense para el aplicante el cual debe resolver correctamente, documentando sus hallazgos en un reporte donde detalle sus análisis. Al final del proceso, cuya duración máxima es cinco meses, se efectúa un examen sobre el proceso y las conclusiones del investigador en cada uno de los ejercicios, el cual requiere que el aplicante demuestre su competencia y claridad para el desarrollo de las actividades forenses.

La certificación CFEC, exige que los nuevos investigadores forenses en informática certificados posean experiencia y destreza en:

- Identificación y recolección de evidencia en medios magnéticos
- Comprensión y práctica en procedimientos de revisión y análisis forenses
- Comprensión y práctica de los estándares de ética que rigen las ciencias forenses en informática
- Comprensión de los aspectos legales y de privacidad asociados con la adquisición y revisión de medios magnéticos.
- Comprensión y práctica de mantenimiento de la cadena de custodia de la evidencia cuando se realiza una investigación.

- Comprensión de los diferentes sistemas de archivos asociados con sistemas operacionales, particularmente FAT de Microsoft.
- Conducir de manera detallada recuperación de datos de todas las porciones de un disco.
- Comprensión de como tener acceso a los archivos temporales, de caché, de correo electrónico, de web, etc.
- Comprensión de los aspectos básicos de Internet.
- Comprensión de técnicas de rompimiento de contraseñas.
- Comprensión general de los temas relacionados con investigaciones forenses.

Esta certificación es avalada y reconocida en diferentes tribunales y cortes del mundo, dada la seriedad y rigurosidad de proceso de certificación. Así mismo, las personas que obtienen su certificación requieren actualización permanente en los nuevos procedimientos y formas de mejorar las técnicas de seguimiento y análisis, lo cual hace que los profesionales certificados estén constantemente enterados y capacitados para afrontar nuevas formas de análisis forense en informática.

De otra parte la HTCN, ofrece diversas certificaciones en la línea forense en informática. En particular comentaremos sobre CCCI - Certified Computer Crime Investigator, nivel básico y avanzado. Cada una de las certificaciones requiere que el aplicante cuente con un curso de entrenamiento con un número de horas y exámenes escritos debidamente aprobados, en centros de entrenamiento autorizados, con el fin de contar con las destrezas requeridas para otorgar la certificación. El propósito de la certificación es desarrollar un alto nivel de profesionalismo y entrenamiento continuo que soporte investigaciones de crímenes de alta tecnología en la industria y las organizaciones. El costo de la certificación es de US$250, los cuales son requeridos para evaluar la forma de aplicación y analizar la experiencia del aspirante, así como para cubrir los

gastos relacionados con el registro ante notaría de la experiencia certificada y los títulos adjuntos.

La certificación CCCI Nivel básico requiere del aplicante:

- Dos años de experiencia en investigaciones en cualquier disciplina o poseer un grado de college y un año de experiencia en investigaciones en cualquier disciplina.
- Seis meses de experiencia investigativa directamente relacionada con la disciplina en que busca certificarse.
- Haber completado satisfactoriamente un curso de 40 horas sobre delitos informáticos o computación forense provista por una agencia, organización o empresa.
- Haber demostrado de manera satisfactoria su conocimiento técnico en la disciplina de la certificación que desea obtener, a través de un examen escrito.

La certificación CCCI Nivel avanzado requiere del aplicante:

- Dos años de experiencia en investigaciones en cualquier disciplina o poseer un grado universitario y un año de experiencia en investigaciones en cualquier disciplina.
- Dos años de experiencia investigativa directamente relacionada con investigaciones de delitos informáticos.
- Haber completado satisfactoriamente un curso de 80 horas sobre delitos informáticos o computación forense provista por una agencia, organización o empresa.
- Haber demostrado de manera satisfactoria su conocimiento técnico en la disciplina de la certificación que desea obtener, a través de un examen escrito.

	Técnica	Jurídica	Procedimientos	Comentarios
IACIS	**X**	**X**	**X**	Ofrece una certificación balanceada y basada en el ejercicio práctico de los

				investigadores en el área. Se verifica actividad permanente en el sitio Web.
HTCN	**-**	**-**	**-**	Se basan en la validación de la experiencia de los aplicantes y los cursos que han tomado en el tema de informática forense.
IISFA	**X**	**-**	**X**	Ofrece una certificación orientada a los aspectos técnicos y de procedimiento.
ISFCE	**X**	**X**	**X**	Ofrece una certificación semejante a lo que se tiene en Iacis, dado que su fundador fue miembro del cuerpo directivo de esa asociación.
SANS GIAC	**X**	**-**	**X**	Ofrece una certificación fuertemente orientada a los elementos técnicos informáticos. Es ideal para aquellos que quieren profundizar en los detalles de la implementación de las tecnologías.

Como hemos visto, la labor de la investigación forense en informática requiere unas credenciales y perfiles que requieren entrenamiento y formación, no solamente en las especificaciones técnicas sino también en procedimientos y habilidades forenses que permitan al profesional certificado enfrentar con la seriedad y diligencia requerida la difícil tarea de reconstruir escenarios, establecer y reconocer evidencia, procesar y analizar datos para formular hipótesis que orienten la

investigación de un delito informático o incidente de seguridad, con el fin de descubrir y sustentar las causales y autores del hecho.

La computación forense como ciencia naciente, ofrece una nueva frontera para todos aquellos que reconociendo su formación técnica o experiencia en aspectos de tecnología, avanzan en medio de los estrictos paradigmas forenses de investigación, procedimientos de análisis y formación legal y penal para enfrentar a todos aquellos que desafían los límites de las seguridades y controles de las organizaciones, con el fin de establecer un frente de resistencia e investigación que al igual que los intrusos, continuamente aprenden y buscan nuevas formas de alcanzar nuevas fronteras en el conocimiento técnico y científico.

Referencias

- IACIS - http://www.cops.org
- HTCN - http://www.htcn.org

Otras asociaciones

- http://www.acfe.org - Assoc. Certified Fraud Examiners
- http://www.icsa.com - International Information Systems Security Assoc.
- http://www.htcia.org - High Technology Crime Investigation Association

Compañías especializadas en Computación Forense

- http://www.forensics.com - Computer Forensics, Inc.
- http://www.computer-forensics.com - Computer Forensics Ltd.
- http://www.forensics-intl.com - New Technologies, Inc. (NTI).
- http://www.cftco.com - Computer Forensic Training Center Online.