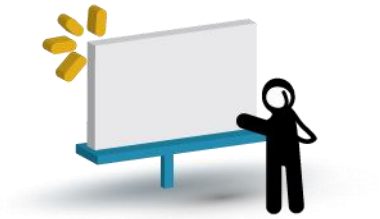
Experto Universitario en Hacking Ético (Ethical Hacking)

Centro de e-Learning SCEU UTN - BA.
Medrano 951 2do piso (1179) // Tel. +54 11 4867 7589 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



Presentación:

La generalización y expansión del uso de las tecnologías, telecomunicaciones e informática en los diferentes contextos empresariales, académicos, personales y públicos, hacen de las TICs una base común para todas nuestras actividades.

Esta plataforma además de ser mantenida en su funcionamiento, debe ser protegida con el fin de controlar que los activos informáticos no sean presa de ataques, fraudes o mal uso por los delincuentes informáticos, empleados desleales o terceros mal intencionados.

El entendimiento de la seguridad de la información desde la función del oficial de seguridad, hace de éste una posición clave en la gestión y entendimiento de la protección de estos activos. Entender como los elementos informáticos, los activos de información, los procesos y la concientización de las personas conforman la consolidación de la seguridad en la organización.

Objetivos:

Que los participantes:

- *Conozcan los conceptos generales de las redes de comunicación, los protocolos, los diferentes dispositivos y sus funciones.*
- *Aprendan a armar, configurar y administrar una pequeña red fácilmente.*
- *Conozcan sobre el mundo de los servidores informáticos, existentes en toda infraestructura informática de mediana y alta gama.*
- *Conozcan los conceptos básicos referentes a la implementación, configuración, mantenimiento y soporte de servidores de infraestructura en tecnologías Windows o Linux.*
- *Conozcan las herramientas esenciales y las buenas prácticas necesarias para obtener el nivel máximo de seguridad en una red de servidores de arquitectura Microsoft Windows Server ó Linux Server, protegiéndola de potenciales amenazas.*
- *Aprendan a planear, diseñar, estructurar e implementar una infraestructura de red informática de manera segura, protegiéndola de potenciales amenazas.*
- *Conozcan sobre los sistemas criptográficos y sus aplicaciones prácticas existentes, abordando sus vulnerabilidades más comunes y los potenciales ataques y amenazas.*
- *Aprendan sobre los conceptos del mundo del Hacking*

- *Conozcan las herramientas y metodologías necesarias para realizar tareas de análisis de vulnerabilidades y tests de penetración, con una filosofía enfocada a la ética profesional.*

Temario:

Módulo 1: Diseño de redes seguras

- Introducción a las redes informáticas
- Instalación y Configuración de redes
- Redes informáticas potenciales riesgos
- Redes informáticas seguridad aplicada

Módulo 2: Administración de Servidores (Windows ó Linux)

- Introducción a los servidores informáticos / Roles y Funciones
- Conociendo Linux (Práctica-Lab)
- Instalando y configurando nuestro servidor (Práctica-Lab)
- Soporte, mantenimiento y solución de problemas (Práctica-Lab)

Módulo 3: Hardening (Windows Servers ó Linux Servers)

- Introducción a implementaciones de seguridad.
- Configuraciones y Servicios (Parte 1)
- Configuraciones y Servicios (Parte 2)
- Seguridad Aplicada

Módulo 4: Ethical Hacking

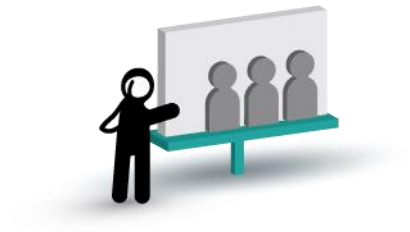
- Introducción sobre el Ethical Hacking
- Metodos de Control de Vulnerabilidades
- Introducción sobre Criptografía
- Introducción sobre un Pentesting

Módulo 5: Ethical Hacking

- Reconocimiento Pasivo y Activo
- Vulnerability Scanning (Explicación y Práctica-Lab).
- Ingeniería Social.
- Seguridad Wireless

Módulo 6: Ethical Hacking

- System Hacking (Explicación y Práctica-Lab)/ Denegación de Servicio /
- Password Cracking (Explicación y Práctica-Lab) / Phishing / Pharming (Explicación y Práctica-Lab).
- Seguridad Mobile
- Cross-Site scripting / SQL Injection (Explicación y Práctica-Lab)



Destinatarios:

Administradores de sistemas, técnicos informáticos, administradores de redes, y analistas, consultores, desarrolladores y auditores de seguridad

Requisitos previos:

Preferentemente conocimientos de operación,redes y uso de computadoras.

Modalidad:

La modalidad es totalmente a distancia a través del Campus Virtual FRBA. Las actividades que se realizarán serán:

- Foros proactivos de discusión semanal propuestos por el docente.
- Consultas al docente a través de e-mail o chat.
- Clases a través de medios virtuales en tiempo real (Aula virtual Sincrónica)
- Materiales de lectura complementarios.
- Actividades individuales y/o grupales de aplicación práctica, sobre la base del aprovechamiento pedagógico de comunidades de aprendizaje (foros, Web 2.0 y contextos laborales-profesionales).
- Evaluaciones integradoras finales por módulo sobre la base de trabajos prácticos de aplicación de los conocimientos adquiridos.

Duración y Carga horaria:

Duración:

24/30 semanas.

Carga horaria:

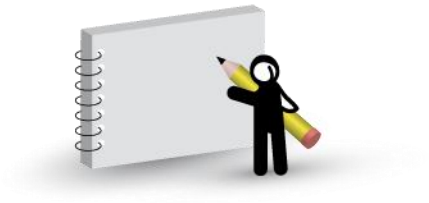
180 horas.

Metodología de enseñanza-aprendizaje

Se trata de una instancia de formación online, basada en la modalidad asincrónica complementada por instancias sincrónicas (Aula Virtual Sincrónica).

Nuestra metodología, basada en el e-learning colaborativo, se sostiene en:

- Los conocimientos expertos, experiencias laborales y profesionales y competencias para llevar adelante las tutorías proactivas y el e-learning colaborativo, de nuestros docentes; quienes, además de su sólida formación académico-profesional, reciben una capacitación continua de actualización y perfeccionamiento.
- El Modelo de E-learningconstructivista colaborativo (MEC) de nuestro Centro de e-learning, que se basa en un diseño instruccional que explota en forma teórico-operativa y pedagógica tres comunidades de aprendizaje fundamentales: 1) Los foros proactivos,2) La Web 2.0 y 3) Los contextos laborales-profesionales de los participantes.
- La puesta en acto de la idea maestra de que quienes aprenden son los participantes y, por lo tanto, deben ser incentivados y estimulados para investigar y construir conocimientos desde posiciones propias y originales.



Tomen Notas

Recomendaciones a los participantes para el mejor aprovechamiento de esta instancia de enseñanza-aprendizaje

Leer todos los mensajes que el instructor envía (no olvidarse que los mismos serán enviados a la casilla de mail que registraron) (Chequear Correo no Deseado)

Decálogo de acciones clave para el mejor aprovechamiento de la instancia de formación:

1. Leer críticamente el material obligatorio (unidades didácticas), sin quedarse con ninguna duda respecto a los contenidos, esto es, las teorías, conceptos, ideas y propuestas. Para ello, es fundamental verter las preguntas, consultas y opiniones críticas en los foros asociados a cada una de las unidades.
2. También es importante tomar posición y opinar críticamente respecto de dichas teorías, conceptos e ideas, compartiéndolas en los foros para dar lugar a debates y discusiones.
3. Realizar los ejercicios propuestos en las unidades didácticas, que remiten a las tres comunidades de aprendizaje que vertebran el e-learning colaborativo en el que se sostiene nuestro modelo de enseñanza-aprendizaje.
4. Compartir en los foros proactivos los resultados de las reflexiones y ejercicios realizados.
5. Intervenir activa y comprometidamente en los foros proactivos dirigidos y coordinados por el profesor-tutor, considerados como la herramienta fundamental de socialización, colaboración y aprendizaje de conjunto.
6. Leer críticamente y aprovechar los materiales complementarios sugeridos por el profesor-tutor.
7. Investigar en la Web respecto de recursos y materiales complementarios y proponerlos a la consideración del profesor-tutor, para su discusión en los foros proactivos que este último dirige y coordina.
8. Ser consciente de la importancia del aprendizaje entre pares, para lo cual es fundamental el compromiso, la intervención y los intercambios en los foros.
9. Saber explotar al profesor-tutor mediante preguntas, consultas y búsqueda de apoyo, quien le agrega valor a la instancia de formación a partir de sus conocimientos expertos sobre el tema, experiencias laborales y profesionales y competencia para llevar adelante las tutorías proactivas y el e-learning colaborativo.
10. Realizar las evaluaciones finales integradoras en el marco del debate entre pares dirigido y coordinado por el profesor-tutor.

Modalidad de evaluación

Aquí es necesario explicar de qué tipo es la Evaluación Final Integradora Obligatoria (EFIO). Puede ser un Cuestionario del tipo MultipleChoice (CMC), o una Actividad de Elaboración (AE) por parte de los alumnos.

Recuerden que cada uno de los módulos deberá contar, por lo menos, con una EFIO. Por lo tanto, en el caso de una Diplomatura o Experto, se deberá consignar de qué tipo es cada una de las evaluaciones.

Siendo la evaluación un momento esencial en cualquier proceso de enseñanza-aprendizaje, nuestras instancias de formación se desarrollan a partir de dos tipos de ejercitaciones y prácticas evaluativas: 1) No obligatorias y 2) Obligatorias.

1) No obligatorias:
    a. La intervención y participación en los foros de los participantes, a partir de las cuales se producen ricos debates y discusiones, dirigidas y coordinadas por el profesor-tutor. La retroalimentación que aquí se produce conforma una excelente instancia de avaluación.
    b. La realización de las reflexiones y elaboración de las actividades propuestas que, en la medida en que sean compartidas en los foros, también constituyen ricas instancias de autoevaluación para los participantes y evaluación para los profesores-tutores.

También los participantes, si lo deseen, pueden solicitarle a los profesores-tutores que realicen una evaluación y de devolución de aquellas actividades que les parezcan importantes.

Recordemos que estas actividades están pensadas desde el aprovechamiento teórico operativo y pedagógico de las tres comunidades de aprendizaje que hemos señalado: 1) Los foros proactivos,2) La Web 2.0 y 3) Los contextos laborales-profesionales de los participantes.

2) Obligatorias:

Son los trabajos, que pueden ser cuestionarios tipo multiplechoice, o distintas actividades, tales como análisis y resolución de casos, ejercicios prácticos de investigación y desarrollo, ejercicios prácticos con consignas específicas, distintos tipos de informes, monografías, etc., que denominamos Evaluación Final Integradora Obligatoria del Módulo (porque, por lo menos, debe haber una por módulo, si se trata de una Diplomatura o Experto, o por curso).

Su obligatoriedad se fundamenta en tres puntos: 1) La evaluación integra todos los temas o los más importantes, desarrollados en el módulo; 2) Por sus exigencias, su resolución obliga a los participantes a haber desarrollado las acciones señaladas en el “decálogo de acciones clave para un mejor aprovechamiento de la instancia de formación” (ver página 12) y 3) Es un requerimiento para acreditar la aprobación del curso, diplomatura o experto universitario.

Acreditación y Certificación

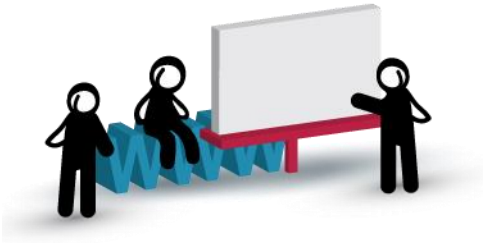
Incentivación pedagógica a través de la acreditación y certificación

Nuestros objetivos de calidad nos exigen poner el acento en los aprendizajes más que en las certificaciones. No obstante, existen participantes que sobrevaloran la certificación por sobre los aprendizajes1. Esto quiere decir que, para ellos, la obtención de un certificado en una Universidad tiene un peso, a veces, mayor que el crecimiento laboral y profesional a partir de la obtención de más y mejores conocimientos.

Frente a esta realidad, nuestros objetivos de incentivación pedagógica basados en la estimulación y motivación a partir de plantear actividades en distintas comunidades de aprendizaje y el accionar proactivo de los profesores-tutores en los foros, pierde fuerza y eficacia. Por lo tanto, nos parece adecuado incentivar a partir de la acreditación y certificación, lo que, tal como lo planteamos, también, por sus resultados, termina siendo una incentivación pedagógica. ¿Cómo lo hacemos?

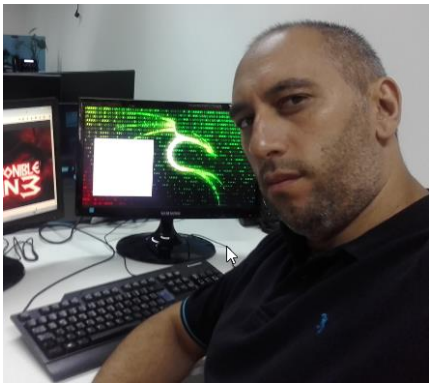
La herramienta de que disponen los profesores-tutores para lograrlo es acreditativa, aunque tienen efectos pedagógicos. Se trata de una escala de calificaciones: Bueno, Muy bueno, Excelente y Sobresaliente, que el profesor-tutor utilizará para evaluar el nivel de compromiso y la cantidad y calidad de su participación en el curso. Por ejemplo, aquellos alumnos que no realicen ninguna de las actividades opcionales y tengan una mínima participación en los foros, aunque hayan aprobado las Evaluaciones Finales Integradoras Obligatorias, tendrán un Bueno en su certificado. Si bien la condición para aprobar el curso es rendir satisfactoriamente las Evaluaciones Finales Integradoras Obligatorias, para obtener un sobresaliente en su certificado, deberán demostrar un verdadero desempeño activo, comprometido y de calidad en lo que hace a todas las actividades opcionales. De no conseguirlo plenamente, el docente avaluará si la corresponde un Bueno, un Muy bueno, un Excelente o un Sobresaliente, de acuerdo, por supuesto, al nivel de participación y compromiso demostrado por el participante.

1Esto se debe a la alta valoración de las certificaciones en nuestro imaginario social.



Dirección y cuerpo docente

Profesor: OSCAR LEONARDO BANCHIERO



Mi nombre es Oscar Leonardo Banchiero, y me recibí de Especialista de Seguridad de la Información &EthicalHacking , en EC COUNCIL (academia internacional), CODSP (Certified Offensive & Defensive Security Professional) y en CISCO (Argentina), entre los años 2005/2014, posteriormente me gradué de CertifiedEthical Hacking V 8.0 (ultima versión) en EC COUNCIL (academia internacional de seguridad informática), en el año 2014.

Mi historial como docente comienza en ISEC (Information Security) & Telefónica Argentina, habiéndome desempeñado en varios países de LatinoAmerica (Uruguay, Bolivia, Colombia, Ecuador, Venezuela, Costa Rica, Paraguay) Actualmente lo estoy haciendo en los mismos países y a nivel local en UTN, ISEC y Telefónica Argentina.

Mi trayectoria laboral–profesional comienza en CIEVI (Centro de eliminación de virus Informáticos) (1995), desempeñándome como Analista de seguridad, recibido en Escuelas Leicester / IAC.

Actualmente trabajo como Especialista de Seguridad, en Telefónica Argentina, para grandes empresas.

He participado en jornadas y congresos de actualización y perfeccionamiento, como por ejemplo Seguridad en dispositivos Móviles (CXO Community) , Seguridad en la nube (ISEC), Seguridad Ethical Hacking (ISEC), Seguridad en redes (Telefónica Argentina)

También he publicado artículos referidos a la seguridad informática, como "la entrevista que los bancos no querrían publicar" (http://www.dragonjar.org/la-entrevista-que-los-bancos-no-querrian-publicar.xhtml), Mobile Pentesting (ICIC), "Ingrese en la mente de un cibercriminal", revista IT NOW (http://revistaitnow.com/2014/03/seguridad/ingrese-en-la-mente-de-un-cibercriminal/), "Teclados virtuales, son seguros?", (http://blog.segu-info.com.ar/2012/04/teclados-virtuales-son-seguros.html), y varios artículos y charlas más.

Participe activamente de charlas y cursos en eventos relacionados con la Seguridad Informática, como CXO Community, InfosecurityLatinoamerica, ICIC, Televisión.

Coordinador: OSCAR ANDRES SCHMITZ

Mi nombre es Oscar Andrés Schmitz, y me recibí de Ingeniero en Sistemas de la Información, en la Universidad Tecnoloógica Nacional, en el año 1997, posteriormente me gradué en el MBA (Maestría en Negocios) en la Universidad del CEMA, en el año 2005. Poseo una amplitud de cursos de perfeccionamiento vinculados con la seguridad, tecnología y negocios. Me encuentro en el registro de expertos de la CONEU en referencia a gestión de sistemas de información, gestión de TICs y Seguridad de la Información.

Mi historial como docente comienza en 1998, desempeñándome en como profesor titular de Computación y Seguridad en la Licenciatura de Seguridad del IUPFA, sumando otras materias vinculadas durante los años siguientes. Actualmente lo estoy haciendo en la UADE, SIGEN, CAECE y Fundación Libertad, en las temáticas a fin a mi especialidad, tecnología, seguridad y negocios.

Mi trayectoria laboral–profesional comienza en 1994, desarrollando mi carrera profesional en todos los puestos del Banco Internacional ING Bank. Actualmente trabajo como Director Ejecutivo en CXO Community desarrollando actividades de Business DevelopmentAccelerator, Mentoring en Negocios y Tecnología, Coaching Ejecutivo y Organizacional, Challenge Security Integration, etc.

He participado en jornadas y congresos de actualización y perfeccionamiento, como director y moderador y orador vinculados con CXO Community, Foro Level 3, entre otros.

También he publicado varios papers incluidos en ***http://www.oscarschmitz.com/informes*** y artículos que desarrollo quincenalmente en ***http://www.oscarschmitz.com*** o mismo en ***https://www.linkedin.com/today/author/1573471***

Mis especialidades: IT Management (Gestión y Gobierno de IT) - IT Strategy (Estrategia de IT) - Changemanagement (Gestión del Cambio) – Business Development (Desarrollo de Casos de Negocios) - OrganizationalRestructuring (Reestructuración Organizacional) – Project Management (Gestión de Proyectos) – Cost&Benefit Business Analisys (Análisis de Costo/Beneficio del Negocio) - OperationalEfficiency (Eficiencia Operacional) - Leadership (Liderazgo) – Coaching (Coaching) – Mentoring – Information Security (Seguridad de la Información) – BIO (Business InnovationOfficer – Dirección de Innovación en los Negocios) - CIO (ChieffInformationOfficer – Dirección de IT) – CSO (Chieff Security Officer – Dirección de Seguridad) – CISO (ChiefInformation Security Officer – Dirección de Seguridad de la Información)

Bibliografía

Libros y otros manuscritos

El material semanal será entregado en formato digital desarrollado por la dirección y el docente.

Asimismo como material complementario ofrecemos la lectura de:

McClure Stuart, Kurtz George y Scambray Joel. “Hackers 4”.Editorial McGraw Hill. 2003. ISBN 8448139798.

PerezAgudin Justo, Matas García Abel Mariano, MiguezPerez Carlos, Picouto Ramos Fernando y Ramos Varón Antonio Angel. “La Biblia del Hacker”. Editorial Anaya Multimedia. 2006. ISBN 441519226.

Caballero Gil Pino y Hernandez Goya Candelaria. “Criptología y Seguridad de la Información”. 2000. ISBN 8478974318.

Jan L. Harrington. “Manual práctico de seguridad de redes”. Editorial Anaya Multimedia. 2006. ISBN 8441520291.

William Stallings. “Fundamentos de seguridad en redes”. Editorial Pearson Education. 2004. ISBN 8420540021.

Andrew Lockhart. “Seguridad de redes”. Editorial Anaya Multimedia. 2007. ISBN 8441521859.

Link complementarios:

Carlos Tori. “Hacking Ético”. 2004. Disponible desde: ***http://www.cxo-community.com/editorial/libros-publicaciones/4678-hacking-etico.html***

Sebastián Bornik. “Malware y Cibercrimen”. CXO Community. 2011. Disponible desde: ***http://youtu.be/nL3jlUhX6wk***

Ref Varios. “Hackers vs CSOs 2011: El ciberdelito y los paradigmas que afectan a las organizaciones”. CXO Community. 2011. Disponible desde: ***http://youtu.be/EcJKXg-JXw8***

Ref Varios. “Ekoparty 2011: Panel de Hackers vs CSOs - La unión hace la Fuerza”. CXO Community. 2011. Disponible desde: ***http://youtu.be/9981Qp4Qjzw***

Ref Varios. “Hackers vs CSOs 2010: Hackers ingresan al mundo Corporativo”. CXO Community. 2011. Disponible desde: ***http://youtu.be/SQamstzvpiU***