Atizapán de Zaragoza a 16 de enero 2013

INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS CIUDAD DE MEXICO
ESCUELA DISEÑO, INGENIERIA Y ARQUITECTURA
DEPARTAMENTO DE COMPUTACION

Datos curso y profesor

Materia: Seguridad Informática
Carrera: 7 ISC11, 7 ITC11, 8 ITIC11
Profesor: Dr. Roberto Gómez Cárdenas
e-mail: rogomez@itesm.mx
Home Page: http://cryptomex.org
Clave-Gpo: TC2010-01
Requisito: Haber cursado TC2002 o TC2008 o TC2018
Cubículo: Sin Oficina, Profesor de Catedra
twitter: @cryptomex

Objetivo General

Al finalizar el curso el alumno tendrá un visión general de área de seguridad informática con los fundamentos necesarios para entender los riesgos, amenazas, vulnerabilidades a los que se ven sometidos los sistemas computacionales en la actualidad, así como los controles y métodos de protección contra posibles ataques, que son necesarios para el funcionamiento adecuado de estos sistemas en la empresa moderna. Además conocerá el estado actual de las leyes que competen a la seguridad de sistemas informáticos en el Ã¡mbito nacional e internacional.

Competencias

- Distinguir los conceptos básicos de la seguridad informatica en un ambiente real.
- Evaluar una política de seguridad de una empresa.
- Aplicar recursos criptográficos para asegurar la confidencialidad y autenticidad de la información.
- Seleccionar los mecanismos adecuados para cubrir los requerimientos de seguridad informática de una organización.
- Identificar los diferentes tipos de código malicioso y sus contramedidas.
- Listar los elementos de la legislación mexicana e internacional vigente, aplicados a la seguridad informatica.
- Relatar las tendencias de investigación en el área de seguridad computacional.

Contenido Temático Oficial

Durante el curso se abordarán los siguientes temas:

1. Conceptos básicos
    - Estrategia de seguridad informática
    - Mecanismos de seguridad informática
    - Actores en el área de seguridad informática
    - Certificaciones en el área de seguridad informática

2. Políticas de Seguridad
    - Conceptos básicos de políticas de seguridad
    - Análisis de riesgos
    - Elaboración de políticas de seguridad
3. Criptologia
    - Criptografia simétrica
    - Criptografia asimétrica
    - Criptografia e integridad de información
    - Criptografía y autenticidad
    - PKI
    - Redes privadas virtuales (VPNs)
4. Herramientas de Seguridad
    - Analizadores de protocolos
    - Analizadores de vulnerabilidades
    - Firewalls
    - Sistemas de detección de intrusos
5. Código malicioso
    - Ataques a nivel aplicación
    - Metodologías de mitigación
6. Legislación informática
    - Legislación mexicana
    - Legislación internacional
7. Tendencias futuras

Recursos Didácticos

- *Security in Computing*, C. Pfleeger, Prentice Hall, 1996, 2nd edition
- *IT Auditing: Using Controls to Protect Information Assets* Chris Davis,Mike Schiller,Kevin Wheeler, McGraw-Hill Osborne Media; 2006
- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Bruce Schneier, 1995, 2nd Edition
- *Practical Cryptography* Niels Ferguson, Bruce Schneier; Ed. Wiley; 2003
- *Network Intrusion Detection*, Stephen Northcutt, Judy Nova Ed. Sams; 2002, 3 edition
- *Computer Security Basics*, D. Russell and G.T. Gangeni, O'Reilly & Associates; 1991
- *Network Security, Private Communication in a Public World*, C. Kaufman, R. Perlman, M. Speciner, Ed. Prentice Hall, 2002, 2da. Edición
- *Building DMZs for Enterprise Networks*, R.J. Shimonski, W. Schmied, V. Chang, T.W. Shinder, Ed. Syngress; 2003
- *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems*, S. Northcutt, L. Zeltser, S. Winters, Karen Fredrick, Ronald W. Ritchey, Ed. Sams; 2005, 2da. Edición

Otras fuentes de consulta

- *Podcasts*
  - Security Now
  - Risky Business
  - The Silver Bullet Security Podcast
  - Pauldotcom Security Weekly
  - Crimen Digital
- *Twitter*
  - teamcymru
  - Security by default
  - Help Net Security
  - Fausto Cepeda
  - Adolfo Grego
  - Roberto Martínez
- *Grupos Interés LinkedIn*
  - LFPDPPP
  - Information Security Commun
  - Computer Security Institute (CSI)
  - (ASIMX) Asociación de Seguridad Informática Mexicana
  - Alapsi Group Members
- *Revistas*
  - IEEE Security & Privacy
  - Hakin9
  - Bsecure
- *Sitios web*
  - Security Focus
  - Security by Default

Plataforma Tecnológica

- Correo eléctronico
- Twitter
- Podcast
- Blackboard

Calendarización actividades del semestre

Fecha	Tema	Recurso Didacttico	Actividades Aprendizaje
16 enero	Presentación Curso	Diapositivas	Exposición Profesor
23 enero	Conceptos básicos	Diapositivas	Exposición Profesor
30 enero	Actores y certificaciones	Diapositivas	Exposicion Profesor
6 febrero	Políticas de seguridad	Diapositivas	Exposición Profesor
13 febrero	Conceptos básicos criptografia	Diapositivas	Exposición Profesor
20 febrero	Criptografia simétrica y asimétrica	Diapositivas	Exposicion Profesor
27 febrero	PKI y VPNs	Diapositivas	Exposición Profesor
6 marzo e	Analizadores de protocolos	Diapositivas	Exposicion Profesor
13 marzo	Scaners de vulnerabilidades	Diapositivas	Exposicion Profesor
20 marzo	Firewalls	Diapositivas	Exposición Profesor
3 abril e	Sistemas detección de intrusos	Diapositivas	Exposicion Profesor
10 abril	Código malicioso	Diapositivas	Exposicion Profesor
17 abril	Ataques a nivel aplicación	Diapositivas	Exposicion Profesor
24 abril	Metodologías de mitigación	Diapositivas	Exposicion Profesor
8 mayo	Legislación informática y Tendencias Futuras	Diapositivas	Exposicion Profesor

Fechas de examenes

Las fechas de los examenes ya fueron definidas por el sistema y se encuentran especificadas en el calendario escolar. Este último puede ser consultado a través de la página del campus. Las fechas son fijas y no pueden cambiarse.

En base a dicho calendario se definen las siguientes fechas de examenes parciales y final

1er. Parcial: 20 febrero
2do. Parcial: 10 abril
Final: 15 mayo

Evaluaciones

Las evaluaciones parciales y final estan compuestas por los siguientes porcentajes:

Parciales

Examen: 70 %
Proyecto: 30 %

Final

Prom. Parciales: 50 %
Examen Final: 20 %
Proyecto Final: 20 %
Promedio Tareas: 10 %

En caso de que durante un parcial no se haya dejado ningún proyecto la calificación parcial será la obtenida en el exámen. Si en la evaluación final no se deja ningún proyecto el 20 % sera repartido de la siguiente forma: 10 % examen final y 10 % parciales.

Políticas del curso

Las siguientes políticas aplican al curso de Seguridad Informática, no están a discusión y cualquier caso no cubierto en este documento será resuelto de acuerdo al criterio del profesor.

Generales

- El curso cuenta con una página, en la cual se encuentra parte de la información aquí presentada. La dirección de la página es: `http://cryptomex.org/seguridad.htmll`.
- Algunos temas del curso serán impartidos auxiliandose de acetatos. Estos se encuentran disponibles en la sección de *Material de Apoyo* de la página del curso.
- El temario es el mismo para todos los campus del sistema, si desea obtener una copia puede bajarlo de la página del sistema, `http://www.sistema.itesm.mx/va/planes/2_1.htm` Es obligación del alumno revisarlo.
- Después de 5 minutos de la entrada del profesor al salón, ningún alumno podrá entrar a clase **NO HAY RETARDOS!!!**
- La calificación es sobre 100, por lo que no habra discusiones de redondeo. La calificación mínima aprobatoria es 70.
- Es obligación del alumno revisar constantemente, (al menos una vez al día) su correo electrónico (el asignado por la institución). En cualquier momento el profesor puede enviar mensajes importantes de naturaleza académica a los alumnos.
- Esta estrictamente prohibido utilizar, o tener abierta, cualquier tipo de computadora durante el tiempo que dura la clase. Si un alumno es sorprendido consultando una computadora deberá abandonar el salón de clases, y se le asignará una falta.
- En caso de contar con un teléfono celular, debe apagarlo al inicio del curso y activarlo al final de la clase.
- Se espera un comportamiento maduro y de respeto por parte del alumno. El alumno que no cumpla con dicho comportamiento deberá abandonar el salón de clases, y se le asignará una falta.

Tareas o actividades

- El termino *actividades* se aplica a las tareas en los cursos rediseñados. En este documento el termino de actividades/tareas se usa indistintamente.
- La fecha de entrega de las tareas, salvo indicación contraria por parte del profesor, es una semana después de que se haya dejado.
- Cualquier evidencia de copia se sancionará de acuerdo al artículo 63 y 64 del capítulo noveno del Reglamento Académico de Carreras Profesionales.
- Las tareas son individuales, salvo indicación contraria del profesor, y deberán entregarse en el salón de clases **dentro de los primeros cinco minutos del día especificado**. No se aceptará ninguna tarea fuera del salón de clases, ni después de la hora y día convenidos. Evitar excusas como no sirve la impresora, no tengo papel, el servidor no responde, etc.
- La presentación de las tareas debe ser digna de un alumno de nivel licenciatura y elaborada de una manera legible.
- Se manejarán tres tipos de tareas:
  - Lecturas de artículos.
  - Investigaciones/reportes.
  - Programas

  Cada tipo de tarea cuenta con su propio formato.

- En el caso de las lecturas de artículos, se pedirá un reporte por artículo. Estos reportes deberán contener el resumen, el análisis de las referencias y los comentarios de artículo. El resumen debe ser de tipo ejecutivo,es decir no deberá de exceder el tamaño de una cuartilla. El análisis debe ser lo más consiso y preciso posible, y los comentarios deberán ocupar al menos una página. Los datos a incluir y el formato se encuentran descritos dentro del documento de *formato de lectura de artículos*. Se deben examinar al menos tres referencias del artículo y definir su relación con el artículo analizado.

Requisito	**Porcentaje**
Formato (letra,titulo)	10 %
Calidad del resumen	30 %
Calidad del análisis presentado	30 %
Calidad de las refencias examinadas	30 %

  - En caso de que se indique que no se examinen referencias, el 30 % será repartido entre los 3 otros rubros.

- Los reportes de las investigaciones que se efectuen deberán cumplir con un formato de artículo de investigación. Los datos de la tarea y su autor deben estar centrados en la parte alta de la primera página. El reporte debe estar dividido en secciones. Los datos a incluir y el formato se encuentran descritos dentro del documento de *formato de investigación*.

- Para este tipo de tareas (investigación) se solicita una busqueda bibliográfica de al menos cuatro fuentes, una de estas fuentes NO debe ser electrónica. Una de las fuentes electrónicas debe ser de la biblioteca digital (las bases de datos de la IEEE y ACM son muy buenas fuentes). La estructura de la investigación debe ser lo más lógica posible, evitar realizar copy/paste de las referencias a diestra y siniestra. Se aplicará la siguiente rúbrica para asignar la calificación a este tipo de tareas:

Requisito	**Porcentaje**
Formato (letra,titulo, margenes)	10 %
Secciones presentadas	10 %
Longitud del trabajo	10 %
Referencias	20 %
Calidad de lo investigado (no copy/paste)	50 %

- En el caso de códigos de programas, este debe incluir los datos del código y del autor a nivel comentarios. No se aceptará nada escrito a mano. Los datos a incluir y el formato se encuentran descritos dentro del documento de *formato de códigos de programas*. La sección de programas de este documento proporciona más información con respecto a la entrega de programas.

- Para evitar confusiones se anexan los formatos de las tres tipos de tareas anteriormente mencionados.

- Cada formato cuenta con su propio tamaño de letra el cual se debe respetar.

- En caso de que la tarea ocupe más de una hoja, estas deben estar engrapadas (no clips, no rasgaduras por la esquina).

- No debe entregar la tarea en folders.

- En caso de que no se cumpla con cualquiera de los puntos anteriores se asignará un tercio de la calificación original.

- El lenguaje de presentación de las tareas es el español, tarea en cualquier otro idioma tendrá una calificación de cero.

- Si la tarea debe enviarse por correo electrónico esta debe cumplir con los siguientes puntos:

- La hora límite de recepción es la hora de inicio de clase, después de esa hora no se tomará en cuenta, no hay excusa de que el servidor no sirve, o de que se tienen problemas con su laptop
- La hora de recepción que se toma en cuenta es la de la computadora del profesor, no la del alumno
- El subject debe ser: `T<num> Segu` donde `<num>` es el número de tarea. (p.e. `T4 Segu`, es la tarea 4 del curso de Seguridad Informática)
- El nombre del archivo que contenga la tarea, debe cumplir con el formato: `T<num>-<matricula>`, donde `<num>` es el número de la tarea y `<matricula>` es la matrícula del alumno, (por ejemplo `T5-445566` es la tarea 5 del alumno con matrícula 445566.
- El cuerpo del correo debe incluir lo siguiente:

```
Envio de la tarea xxx del curso de Seguridad Informatica
<Descripcion de la tarea>
<Fecha y hora de envio>
Nombre completo matricula
```

  Debe contar con el nombre completo y matrícula de todos los integrantes del equipo (si es que se dejo en equipo). La descripción de la tarea no debe ocupar más de una línea.

Tarea que no cumpla con lo anterior no se tomará en cuenta.

Exámenes

- Los exámenes deben realizarse de la manera más clara y limpia posible. Respuesta que no se entienda, respuesta que esta mal, (cero puntos).
- Los exámenes se deben contestar con tinta, si el examen no se resuelve con tinta tendra una penalización de 20 puntos.
- Las aclaraciones sobre calificaciones de tareas y/o examenes se harán fuera del salón de clase. Se deberá de concertar una cita con el profesor para tal efecto. La revisión tendrá lugar en el cubículo del profesor.
- Después de una semana de entregada la calificación, (tanto de tareas como de examenes), no se aceptará ninguna demanda de aclaración. Esto implica que el alumno esta de acuerdo con dicha calificación.
- Una tarde antes de la aplicación del exámen y el mismo día de su aplicación, no se dará ningún tipo de asesoría.
- Cualquier evidencia de copia se sancionará de acuerdo al artículo 63 y 64 del capítulo noveno del Reglamento Académico de Carreras Profesionales.

Programas

Uno de los conocimientos que debe dominar una persona que labora en el área de sistemas es la programación. Durante el curso el alumno implementará diferentes programas. (ya sea como tareas o proyectos), dichas implementaciones deben tomar en cuenta lo siguiente:

- Salvo indicación contraria, se deben desarrollar en lenguaje C/C++ que se probarán sobre sistemas Unix/Linux.

- Los programas se probarán sobre una distribución Open Suse 11. Una imagen de esta distribución esta disponible en la oficina del profesor. Para poder trabajar sobre esta imagen es necesario contar con el software VMWare, ya sea su versión Server o Player. Lo anterior lo puede bajar de `http://www.vwmare.com/download`. Si decide desarrollarlo en otra plataforma y no este no funciona en la plataforma de prueba, se atendrá a la rúbrica abajo descrita. No importará si el programa funciona bajo otra plataforma.
- No se dará ninguna asesoría con respecto a instalación y administración de sistemas linux.
- Para mayores informes sobre como compilar un programa con con gcc, se sugiere consultar la *Miniguía de compilación de programas C en Unix*, que puede encontrarla en la página `http://homepage.cem.itesm.mx/rogomez/compiUnix.html`.
- También se recomienda leer los siguientes artículos, disponibles en la sección de *Apuntes* de la página : `http://homepage.cem.itesm.mx/rogomez/publi.html`
  - Comandos básicos de Unix
  - Compilando y depurando programas C en Unix
  - Creación, ejecución y muerte de procesos
- Se debe entregar una impresión del código, de preferencias dos páginas por hoja, y enviar el código fuente por correo electrónico
- En el caso de que la tarea/proyecto cuente con diferentes archivos, todos deberán estar dentro de un archivo, NO comprido (i.e. `xxxx.tar`). Lo anterior lo puede hacer con el comando `tar`. El archivo debe cumplir con la sintaxis `T<num>-<matricula>.tar`, donde `<matricula>` es la matrícula del autor. En caso de que se trate de un trabajo en equipo se debe considerar la matrícula de menor valor. Cuando los archivos se extraigan (comando `tar -xvf <archivo>` se debe crear un directorio donde se depositarán los archivos. Suponiendo que la matrícula es 445566, y que se trata de la tarea 4, un script ejecutará los siguientes comandos de forma automática:

```
$ tar -xvf T2-445566.tar
$ cd T2-445566
$ gcc client.c -o client
$ gcc server.c -o server
$ ls
client server
$ server &
```

- Lo solicitado en el punto anterior se hace con el comando `tar`. Como ejemplo consideremos el caso en que la tarea del alumno con matrícula 676767 cuenta con tres archivos `a1.c b1.c` y `lib.h`.

```
$ ls
a1.c  b1.c  lib.h
$ mv a1.c b1.c lib.h T4-676767/
$ tar -cvf T4-676767.tar T4-676767/
T4-676767/
T4-676767/a1.c
T4-676767/b1.c
T4-676767/lib.h
$ ls
T4-676767  T4-676767.tar
$
```

el archivo `T6-676767.tar` contiene los archivos de la tarea 4 del alumno con matrícula 676767.

- Si el programa solo requiere de un archivo, debe enviar el archivo cumpliendo con la sintaxis descrita en el punto anterior (`T<num>-<matricula>.c`).
- Los programas seran evaluados de acuerdo a la siguiente tabla:

Requisito	**Porcentaje**
Compilación programa	20 %
Ejecución sin errores	30 %
La ejecución hace lo especificado	40 %
Cumplimiento de especificaciones (.tar, comentarios, directorio, etc)	10 %

Es decir si un programa no compila tendra una calificación de 5/100. Si el programa compila y al ejecutarlo resulta en un error (p.e. `Segmentation fault core dumped`) tendrá una calificación de 20/100. Por otro lado, si el programa no despliega ninguno de los errores anteriores, pero no hace lo que se pidio, tendrá una calificación de 50/100. Dependiendode que es lo que haga tendra una calificación entre 50 y 80. Los últimos 20 puntos los obtendra si cumple con las especificaciones de los programas, etc).

Actividades de Aprendizaje

- Exámenes parciales
- Exámen final
- Ejercicios
- Tareas
- Proyectos de programación

Breve semblanza del profesor

- Ingeniero en Sistemas Electrónicos, ITESM-CEM
- Maestría en Sistemas Computacionales, ITESM-CEM
- DEA - Informatica Fundamental, Universidad de Paris 7
- Doctorado Informatica, Universidad de Paris 8 e INRIA Rocquencourt.
- Gerente de Seguridad de la Información de Invex Grupo Financiero.
- Profesor-Investigador, ITESM-CEM
- Coordinador e instructor del Diplomado en Seguridad Informática impartido por el ITESM y ALAPSI
- Miembro del Consego Editorial de la revista B-Secure