UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

COORDINACIÓN DE FORMACIÓN BÁSICA
COORDINACIÓN DE FORMACIÓN PROFESINAL Y VINCULACIÓN UNIVERSITARIA
PROGRAMA DE UNIDADES DE APRENDIZAJE POR COMPETENCIAS

I. DATOS DE IDENTIFICACIÓN

1. Unidad Académica: Facultad de ciencias

2. Programa (s) de estudio: (Técnico, Licenciatura) Licenciatura en Ciencias Computacionales 3. Vigencia del plan: 2008-1

4. Nombre de la Unidad de Aprendizaje: **Seguridad en Cómputo** 5. Clave: **9857**

6. HC: 2 HL: 2 HT: 2 HPC: HCL: HE: CR: 8

7. Ciclo Escolar:2009-1 8. Etapa de formación a la que pertenece: Terminal

9. Carácter de la Unidad de Aprendizaje: Obligatoria Optativa: **X**

Requisitos para cursar la Unidad de Aprendizaje: Se recomienda tomar las materias de Fundamentos de Telecomunicaciones, Redes de Datos

Formuló: M.C. Evelio Martínez Martínez
M.C. Carlos González Sanchez

VoBo. Biol. Marcelo Rodríguez Meraz
Cargo: Subdirector

II. PROPÓSITO GENERAL DE LA UNIDAD DE APRENDIZAJE

Al término del curso el estudiante tendrá las nociones fundamentales de la seguridad en redes de cómputo para diseñar esquemas de red seguros, proteger información sensible, configurar servicios de red seguros y administrar redes seguras utilizando herramientas de distribución libre. El curso servirá como introducción para que el estudiante pueda instalar y configurar herramientas más utilizadas en el ámbito del software libre. Además, el estudiante estará preparado para resolver situaciones y/o problemas reales.

La materia de Seguridad en Cómputo es una materia optativa y pertenece a la etapa terminal. Las materias consecuentes relacionadas con ésta son sistemas distribuidos (obligatoria), arquitecturas de protocolos de red, seguridad en cómputo, tópicos selectos de redes y otras materias optativas.

III. COMPETENCIA (S) DE LA UNIDAD DE APRENDIZAJE

Aplicar los diversos métodos para garantizar la seguridad y confiabilidad de los datos que circulan en las redes, asegurando el libre transito de información y manteniendo las condiciones de privacidad definidas por los usuarios y los administradores de los sistemas con ética y responsabilidad.

IV. EVIDENCIA (S) DE DESEMPEÑO

Exámenes teóricos, tareas extraclase, exposición oral y escrita, reportes, prácticas de laboratorio y proyecto final.

V. DESARROLLO POR UNIDADES

Unidad 1. La necesidad de protección

Competencia:

Comprender la importancia de la protección de la información en las redes de cómputo analizando el impacto de la seguridad como el siguiente desafío de la tecnología de las redes en las organizaciones con ética y responsabilidad.

Contenido temático **Duración** 8 hrs.

1. **La necesidad de protección**
   - 1.1. Motivación
   - 1.2. ¿Cuál puede ser el valor de los datos?
   - 1.3. Definiciones
   - 1.4. Seguridad global
   - 1.5. Impacto en la organización
   - 1.6. Repaso de interconexión de redes (internetworking)

Unidad 2
Conceptos Generales de seguridad

Competencia:

Analizar los conceptos generales de seguridad analizando los diferentes tipos de ataques, amenazas, vulnerabilidades, estándares y niveles de trabajo para comprender la dimensión de la problemática y las posibles soluciones centrándose en un análisis de riesgos para proteger la información de las organizaciones con una actitud ética y responsable.

Contenido temático **Duración** 8 hrs

2. Conceptos Generales de seguridad

- 2.1. Principios fundamentales
- 2.2. Ataques, servicios y mecanismos
- 2.3. Ataques de seguridad (activos, pasivos)
- 2.4. Virus, gusanos y caballos de troya
- 2.5. Modelo multiniveles de seguridad
- 2.6. Análisis de riesgos
  - 2.6.1. Amenazas y vulnerabilidades
  - 2.6.2. Modelos de análisis de riesgos
- 2.7. Estándares de Internet y RFCs
- 2.8. Niveles de trabajo
  - 2.8.1. Confidencialidad
  - 2.8.2. Integridad
  - 2.8.3. Autenticidad
  - 2.8.4. No-repudio
  - 2.8.5. Disponibilidad de los recursos de la información
  - 2.8.6. Consistencia
  - 2.8.7. Control de acceso a los recursos
  - 2.8.8. Auditoría

Unidad 3

El lado humano de la seguridad

Competencia:

Aplicar los conceptos del lado humano de la seguridad analizando las políticas, normas y procedimientos así como los aspectos jurídicos y éticos que juegan los usuarios, programadores y administradores para la protección de la información en las organizaciones con una actitud ética y responsable.

Contenido temático **Duración 4 hrs**

3. El lado humano de la seguridad
- 3.1. Políticas, normas y procedimientos
- 3.2. Programas de educación
- 3.3. Aspectos jurídicos y éticos

Unidad 4

Confidencialidad e integridad de la información

Competencia
Aplicar los diferentes mecanismos de confidencialidad e integridad de la información mediante el análisis de los diferentes algoritmos para el cifrado de la información y de las tecnologías emergentes para la protección de la información y la infraestructura de cómputo de las organizaciones con ética y responsabilidad.

Contenido temático **Duración 10 hrs.**

3. Modulación y codificación
- 3.1. Modulación
  - 3.1.1. Razones para modular
  - 3.1.2. Modulación analógica (AM, FM, PM)
  - 3.1.3. Modulación digital (ASK, FSK, PSK, QAM)
  - 3.1.4. Modulación por codificación de pulsos (PMC)
- 3.2. Codificación
  - 3.2.1. Razones para codificar
  - 3.2.2. Codificaciones digitales
    - 3.2.2.1. Unipolar
    - 3.2.2.2. Polar (NRZ, RZ, NRZI, Manchester, Manchester diferencial)
    - 3.2.2.3. Bipolar (AMI, B8ZS, HDB3)

Unidad 5

Introducción a las redes de datos

Competencia
Analizará los conceptos básicos de las redes de datos mediante el estudio de las topologías, métodos de acceso al medio, servicios y demás elementos que le permitirán tomar decisiones en el diseño de una red en la organización de una manera crítica y propositiva.

Contenido temático **Duración 10 hrs.**

4. Confidencialidad e integridad de la información

- 4.1. Criptografía
  - 4.1.1. Características de la criptografía
- 4.2. Cifrado y autentificación
  - 4.2.1. Algoritmos de llave privada
  - 4.2.2. Algoritmos de llave pública
  - 4.2.3. Infraestructura de llave pública (PKI)
- 4.3. Firmas digitales
- 4.4. Certificados
- 4.5. Autoridades de certificación
- 4.6. Aplicaciones criptográficas
  - 4.6.1. PGP, SSL, SSH, S/MIME
  - 4.6.2. VPNs & IPSec
- 4.7. Secure Socket Layer (SSL)
  - 4.7.1. SSL handshake

Unidad V

Fortalecimiento de sistemas

Competencia

Aplicar los conceptos fundamentales de seguridad en cómputo para la protección de la información utilizando herramientas especializadas en los niveles de red (perimetral), sistemas operativos (nivel de host), aplicaciones (sistemas/programas) de la organización con ética y responsabilidad.

Contenido Temático Duración: **12 horas**

5. Fortalecimiento de sistemas

- 5.1. Seguridad perimetral
  - 5.1.1. Firewalls
  - 5.1.2. Proxies
- 5.2. Seguridad en sistemas operativos
- 5.3. Seguridad en aplicaciones

5.4. Detectores de intrusos
5.5. Respuesta a incidentes
5.6. Análisis de estándares y guías
    5.6.1. Orange book
    5.6.2. Common criteria
    5.6.3. BS 7799

Unidad VI

Tipos de ataques y vulnerabilidades

Competencia

Aplicar los diferentes mecanismos y herramientas que existen para contrarrestar los diferentes ataques y vulnerabilidades que existen en las redes de datos para la protección de la información de la organización con ética y responsabilidad.

Contenido Temático Duración: **24 horas**

6. Tipos de ataques y vulnerabilidades
6.1. Contraseñas
6.2. Email bombing & spamming
6.3. Problemas de seguridad en FTP
6.4. Problemas de seguridad en WWW
6.5. TFTP
6.6. Telnet
6.7. Los commandos “r”
6.8. Seguridad en NetBios
6.9. Negación de servicio (DOS)

Unidad VII

Herramientas de seguridad

Competencia

Aplicar las diferentes herramientas de seguridad de uso libre que existen para mitigar los efectos causados por los ataques, así como herramientas para el control y seguimiento de accesos e integridad para la protección de la información de la organización con ética y responsabilidad.

Contenido Temático Duración: **24 horas**

7. Herramientas de seguridad

7.1. Herramientas de control y seguimiento de accesos:

7.1.1. tcp-wrappers, Netlog, Argus, tcpdump, Satan, ISS, Courtney, Gabriel, tcplist, nocol,…

7.2. Integridad del sistema

7.2.1. Cops, tiger, crack, tripwire, chkwtmp, chklastlog, spar, lsof, cpm, ifstatus, osh,noshell, trinux,…

IV. ESTRUCTURA DE LAS PRÁCTICAS

No. de Práctica	Competencia(s)	Descripción	Material de Apoyo	Duración
1	Instalación y configuración del sistema operativo de manera segura.	Se instalará y se configurará el sistema operativo (windows/linux) dependiendo del uso que se le vaya a dar a la computadora (desarrollo, desktop, servidor,..). Una vez instalado el sistema operativo verificar los servicios/puertos habilitados utilizando herramientas como netstat, aports, etc. Deshabilitando aquellos servicios que no se utilicen o que no necesiten ser accedidos remotamente. También se le enseñara a elegir el esquema de contraseñas que mejor convenga para el tipo de instalación.	Computadora con sistema operativo Linux/windows . Netstat Aports	1:30 horas
2	Generación de llaves públicas para el intercambio de e-mail	Se generarán llaves públicas para el intercambio de e-mail utilizando GnuPG u OpenPGP en conjunto con un cliente de email (e.g. Kmail) Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux . Utilerias: GnuPG Kmail Kgpg	2 horas
3	Generación de llaves públicas de host.	Generación de llaves publicas de host utilizando SSH para el intercambio de comandos remotos a través de canales seguros e incluso para hacer conexiones remotas sin la necesidad de mandar el password por la red. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux. Utilería: OpenSSH	1 hora

4	Instalación y configuración de Infraestructura con VPNs	Instalacion y configuracion de Infraestructura con VPNs utilizando FreeS/WAN (IPsec & IKE) u OpenVPN (SSL/TLS). Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux IPSec/ IKE	1 hora
5	Configuración de un Firewall/Router utilizando IPtables Routed.	Configuración de un Firewall/Router utilizando IPtables, Routed o Zebra. (Zebra tiene una interfaz de configuración igual que Cisco) Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux. IPTables/ Zebra	2 horas
6	Detección de intrusos a nivel de red	Detección de intrusos a nivel red utilizando herramientas como Snort o Prelude. Instalación, configuración y ejecución de Snort para encontrar patrones irregulares en el tráfico de red, tal como exploits, virus, entre otras. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux. Snort	2 horas
7	Detección de intrusos a nivel de host	Detección de intrusos a nivel de host utilizando la herramienta Tripwire. Instalación, configuración y ejecución de Tripwire creando una imagen de firmas digitales del sistema de archivos para detectar cambios en el mismo. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux	2 horas

8	Auditoria a sistemas	Auditoria a sistemas empleando la herramienta Nessus. Instalación, configuración y ejecución de Nessus para encontrar vulnerabilidades existentes en sistemas de diferentes plataformas. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux	2 horas
9	Auditoria a tráfico de red.	Auditoria a tráfico de red utilizando Tcpdump y Ethereal. Instalación, configuración y ejecución de tcpdump para auditar tráfico de red utilizando comandos en línea. Instalación, configuración y ejecución de Ethereal utilizando ambiente grafico. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux. Ethereal tcpdump	2 horas
10	Monitoreo de trafico de red	Monitoreo de trafico de red utilizando una herramienta Ntop para conocer el patrón que forma el tráfico de red. Se entregará un reporte escrito con los resultados y conclusiones	Computadora con sistema operativo Linux. Ntop	2 horas
11	Control de acceso a servicios de red	Control de acceso a servicios de red utilizando la herramienta TCPWrappers Instalación, configuración y ejecución de TCPwrapper para controlar la entrada a servicios de red que ofrece un servidor.	Computadora con sistema operativo Linux. TCPwrapper	2 horas

VII. METODOLOGÍA DE TRABAJO

Investigación

La investigación será empleada en los trabajos extraclase que se pedirán al estudiante sobre temas de actualidad o sobre temas que se verán posteriormente en clase. El propósito de estos trabajos es que el estudiante aprenda hacer investigación en medios electrónicos (Internet), libros, y revistas sobre temas del área. Las fuentes serán tanto en el idioma inglés como español para fomentar la enseñanza del idioma extranjero. Los reportes deberán contener las referencias que se utilizaron para la realización del trabajo y debe contar imprescindiblemente una conclusión personal acerca de la investigación. El maestro debe enfatizar a los estudiantes que los reportes escritos sean claros y bien redactados, recalcándoles también las faltas de ortografía.

Exposición oral

El alumno debe ser capaz de desenvolverse oralmente al exponer un tema o al establecer una discusión sobre una temática en particular del curso. El maestro debe involucrar a los estudiantes en la exposición oral ya sea de una noticia reciente o de un tema particular el alumno haya tenido el tiempo necesario para investigarlo.

Prácticas de Laboratorio

Llevar a la práctica los conocimientos teóricos vistos en clase es el mejor método de enseñanza-aprendizaje, por eso es importante que el estudiante desarrolle habilidades que le permitan resolver problemas reales en el área de telecomunicaciones y redes.

Exámenes de conocimientos

El maestro deberá aplicar al menos 2 exámenes de conocimientos durante el curso, de tal manera que refuercen los conocimientos aprendidos durante la clase. Los exámenes podrán ser de varios tipos, tales como: de preguntas abiertas, opción múltiple, crucigramas o mapas mentales.

Proyecto final

El maestro les asignará un proyecto final, el cual se hará en equipo en donde apliquen o configuren las herramientas para problemas específicos. Aquí se fomentará el trabajo en equipo, la ética y la responsabilidad. El proyecto se expuesto oralmente al final del semestre.

VIII. CRITERIOS DE EVALUACIÓN

La evaluación general del curso consistirá de exámenes teóricos, tareas-reportes, prácticas de laboratorio y una exposición oral con un reporte escrito.

Los porcentajes de evaluación serán los siguientes:

Exámenes	40%
Tareas/prácticas	30%
Proyecto final	30%
Total	100%

Criterio de acreditación

- Resolver al menos 2 exámenes parciales en tiempo y forma.
- Las tareas y las prácticas serán estrictamente individuales
- Deberán ser al menos 10 prácticas y tareas extraclase por semestre
- Cumplir con las prácticas y tareas extraclase en tiempo y forma.
- Cumplir con el proyecto final, su presentación oral y reporte escrito en tiempo y forma.

Criterio de evaluación

- Las tareas, prácticas y exámenes serán resueltos en clase posterior de la entrega para que el estudiante conozca inmediatamente la solución propuesta en cada uno de los trabajos o exámenes.

- En el caso de la exposición final por equipo, la evaluación se dividirá en dos: reporte escrito y exposición, en el primer caso la calificación será por equipo y los puntos a evaluar serán, contenido, claridad y forma, así como ortografía y redacción; para la exposición oral ésta se calificará de manera individual y los puntos a evaluar serán, dominio del tema, claridad y estructura. Los alumnos puede ayudarse en la exposición mediante apoyos visuales tales como proyector de transparencias, acetatos u medios multimedia.
- El proyecto final será por equipos y constara de la aplicación funcionando, un reporte escrito y la exposición oral. La exposición oral se evaluara individualmente, el reporte escrito y la aplicación funcionando se calificará por equipo.

IX. BIBLIOGRAFÍA

Básica

Hacking Exposed Linux, 2nd edition
Brian Hatch, James Lee
McGrawHill Osborne Media
ISBN 0072225645

Practical Unix & Internet Security
Simson Garfinkel, Gene Spafford
O'Reilly & Associates
ISBN 1565921488

Maximum Linux security, 2nd. Edition
John Ray, A Anonymous
Sams
ISBN 0672321343

Network security: private communication in public world
Charlie Kaufman, Radia Perlman, Mike Specimer
Prentice Hall
ISBN 0130460192

Network security Essentials
William Stallings

Complementaria

Hack proofing Linux
James Stanger, Patrick T. Lane, Edgar Danielyan
Singress
ISBN 1928994342

Security Complete
Sybex, Mark Lierley
Sybex, Inc.
ISBN 0782129684

Guide to Linux Networking and Security
Nicholas Wells
Course Technology
ISBN 0619000945

Computer Security: Art and science
Matt Bishop
Addison-Wesley
ISBN 0201440997

Computer Security Institute
http://www.gocsi.com

Prentice Hall ISBN 0130351288 CERT – Computer Emergency Response Team http://www.cert.org/ Federal Computer Incident Response Team http://www.fedcirc.gov/ Internet Storm Center http://www.isc.sans.org/ UNAM-CERT http://www.seguridad.unam.mx/	CSRC-NIST http://csrc.nist.gov/ National Security Agency http://www.nsa.gov/ National Infrastructure Protection Center http://www.nipc.gov/