FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

PROGRAMA DE CURSO

Código	Nombre			
EMC130	Seguridad en Redes			
Nombre en Inglés				
Network Security				
SCT	Unidades Docentes	Horas de Cátedra	Horas Docencia Auxiliar	Horas de Trabajo Personal
6	10	5	1	6
Requisitos			Carácter del Curso	
Ninguno			Electivo	

Resultados de Aprendizaje
El estudiante al termino del curso demuestra que: • Diseña redes razonablemente seguras de acuerdo al tipo de servicios y usuarios en dicha red. • Es capaz de implementar la entrega de servicios seguros, aplicando políticas, protocolos y herramientas adecuadas. • Es capaz de detectar, responder y prevenir incidentes computacionales, siguiendo las buenas practicas aprendidas en el curso y de acuerdo al marco legal vigente.

Metodología Docente	Evaluación General
El curso consta de a) Clases expositivas b) Laboratorios tipo hand-on para desarrollar algunas temáticas expuestas en el curso.	Tareas Controles y Examen

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS UNIVERSIDAD DE CHILE

Unidades Temáticas

Número	Nombre de la Unidad	Duración en Horas
1	Introducción a la seguridad en redes	3,5

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Incidentes de seguridad informática 2. CSIRTS 3. Seguridad informatica en Chile 4. Cibercrimen, hacktivistas, ciberwar 5. Honeypots, darknets	El estudiante demuestra que: 1. Puede identificar cuando esta en presencia de un incidente de seguridad computacional 2. Comprende las funciones de un CSIRT y conocen algunos proyectos habituales que estos realizan 3. Diferencia entre los diversos tipos de ataques que pueden producirse a un sistema computacional	[1] [21] cap 5

Número	Nombre de la Unidad	Duración en Horas
2	Criptografía	4

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Historia 2. Encriptacion simétrica, ejemplos: DES, 3DES, AES, vulnerabilidades 3. Encriptacion asimétrica: establecimiento de claves Diffie-Hellman. Ejemplos: RSA, ElGamal, estándar PKCS#7 4. Funciones de Hash: MD5, SHA1 5. Message Authentication Codes (MACs) 6. Mecanismos de autenticación	El estudiante: 1. Comprende los mecanismos para transmitir datos en forma segura a través de redes publicas. 2. Entiende los protocolos para garantizar confidencialidad, integridad, no repudio y los mecanismos de autenticación. 3. Explica los mecanismos de encriptacion simétrica y asimétrica y entiende los algoritmos detrás de cada uno de ellos.	[2] [17] [18]

Número	Nombre de la Unidad	Duración en Horas
3	TCP/IP	6

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Modelo OSI 2. IP 3. TCP/UDP 4. ICMP, ARP 5. Switch, router 6. VLAN,ACL 7. IPV6 8. Envenenamiento de ARP 9. Denegación de Servicio (DoS), Flood, spoofing 10. Ataques amplificación	El estudiante: 1. Entiende el modelo TCP/IP e identifica las capas que lo componen. 2. Conoce los componentes físicos que integran una red. 3. Entiende los mecanismos de encapsulacion de las diversas capas de TCP/IP y sus vulnerabilidades 4. Se familiariza con el protocolo IPv6 y los problemas de seguridad que puede enfrentar	[3] [20] cap 3

Número	Nombre de la Unidad	Duración en Horas
4	Firewall, IDS/IPS	4

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Filtrado de paquetes 2. Inspección de estado 3. Filtros dinámicos 4. Filtros de aplicación 5. Proxies 6. Otros dispositivos (reguladores de ancho de banda, balanceadores de carga) 7. Iptables 8. IDS: Arquitectura, Fuentes de información,Métodos de análisis, Timing	El estudiante: 1. Entiende las funciones de un firewall y un IDS 2. Diseña arquitecturas de red seguras, introduciendo y configurando los dispositivos adecuados	[4] [5]

Número	Nombre de la Unidad	Duración en Horas
5	SMTP/SPAM	4

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Protocolo SMTP 2. Analizando encabezados del correo electrónico 3. Métodos de protección automáticos: spamassassin, blacklist, greylist, SPF 4. PGP	El estudiante: 1. Entiende el protocolo SMTP y sus vulnerabilidades 2. Comprende el problema del correo spam y los métodos para enfrentarlo 3. Utiliza PGP como mecanismo de confidencialidad e integridad de correo	[3] cap 24

Número	Nombre de la Unidad	Duración en Horas
6	DNS/DNSSEC	3

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Descripción del protocolo 2. Zonas y parámetros principales 3. Ataques comunes: cache poisoning, domain hickjacking, DoS 4. DNSSEC	El estudiante: 1. Entiende la función del protocolo DNS y su importancia en el funcionamiento de la red 2. Conoce alguna de sus principales debilidades y los ataques que lo han afectando. 3. Comprende el protocolo DNSSEC y su implementación	[6] [7] [3] cap 23

Número	Nombre de la Unidad	Duración en Horas
7	Escaneo de vulnerabilidades	2

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Auditorías de red vs auditorías externas 2. nmap y otros escáner 3. Desafíos de escanear	El estudiante: 1. Aprende las ventajas y desafíos de las auditorías. 2. Aprende a manejar las herramientas mas comunes para auditorías de red	[8]

Número	Nombre de la Unidad	Duración en Horas
8	Malware	6

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Clasificación de Malware 2. Métodos de infección 3. Tipos de phishing 4. Pharming, Botnets 5. Fast-Flux: DNS-Round Robin, single y double flux, detección 6. Nuevos fraudes, proyecciones y posibles soluciones	El estudiante: 1. Conoce las diferentes amenazas de malware que afectan los sistemas 2. Identifica los diversos ataques de phishing que circulan 3. Comprende el funcionamiento de las botnets y los mecanismos de estas para expandirse y ocultarse	[9] [21] cap 1, 2,4,6

Número	Nombre de la Unidad	Duración en Horas
9	Protocolos seguros	4

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Canal seguro, uso de túneles encriptados, autentificados y con validación de integridad. 2. IPSec, protocolo para sustentar VPN. 3. VPN, virtual private networks, diseño de un sistema de acceso remoto seguro para mover la oficina a través de las redes. 4. SSH, conexión remota a computadores usando canales seguros 5. SSL/TLS, protección para la capa de aplicación.	El estudiante: 1. Entiende el concepto de canal seguro 2. Diferencia los protocolos seguros de acuerdo a la capa en que ellos se implementan 3. Entiende los mecanismos criptográficos que sustentan cada uno de los protocolos de seguridad expuestos.	[10] [11][12][13]

Número	Nombre de la Unidad	Duración en Horas
10	Seguridad en 802.11	3.5

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Diseño y revisión de la seguridad original. 2. Estándares 802.11g, 802.11n, 802.11ac 3. Mejoras incorporadas hasta llegar a IEEE 802.11i 4. Consideraciones de diseño	El estudiante: 1. Entiende las diferencias entre los diversos estándares del protocolo 802.11 2. Entiende las vulnerabilidades una red wifi y los ataques mas comunes 3. Es capaz de implementar redes inalámbricas seguras en una organización	[14] [19] cap 2,5,6,12,13

Número	Nombre de la Unidad	Duración en Horas
11	Consideraciones legales	2,5

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Protección de datos. 2. Delitos informáticos.	El estudiante: 1. Conoce la ley chilena que norma la protección de datos 2. Conoce la actual ley de delitos informáticos.	[15] [16]

Número	Nombre de la Unidad	Duración en Horas
12	Laboratorios hand-on	7,5

Contenidos	Resultado de Aprendizaje de la Unidad	Referencias a la Bibliografía
1. Laboratorio de netflow • Sniffing de trafico • tcpdump, wireshark 2. Laboratorio de análisis de intromisiones • Herramientas de sistemas operativos • Nociones forenses • Análisis online, offline 3. Laboratorio wifi • Ejercicios de auditoría y protección	El estudiante: 1. Aprende a utilizar herramientas de análisis de trafico de la red y a detectar anomalías 2. Entiende como realizar análisis a sistemas comprometidos y los resguardos que debe tomar 3. Aprende a utilizar herramientas de penetración en redes inalámbricas y comprende los riesgos que enfrentan dichas redes	[19] cap 16

Bibliografía General
Bibliografía Básica [1] Handbook for Computer Security Incident Response Teams (CSIRTs) http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305 [2] Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography. CRC Press. 1997. http://www.cacr.math.uwaterloo.ca/hac/ [3] D. Comer: Internetworking witch TCP/IP, Vol I , 6ta edicion, 2014 [4] S. Northcut, L. Zeltserm, S. Winters, K. Fredrick, R. W. Ritchey, Inside Network Perimeter Security. [5] Kaufman, Perlman: Netwok Security: private communication in a public world, 2da edicion [6] Liu, Albitz, DNS and BIND (5th Edition) [7] Michael W. Lucas, DNSSEC Mastery: Securing the Domain Name System with BIND [8] G. Lyon: Nmap network scanning [9] Christopher C. Elisan, Malware, Rootkits & Botnets: A Beginner's Guide ,McGraw Hill, 2012 [10] IPSEC: The New Security Standard for the Internet, Intranets [11] Barret, Silverman, SSH: The Secure Shell [12] E. Rescorla, SSL and TLS: Designing and Building Secure Systems. Addison Wesley. 2000. [13] C. Scott, P. Wolfe, M. Erwin, Virtual Private Networks. [14] B. Potter, B. Fleck, 802.11 Security O'Reilly. [15] Ley 19.628 sobre protección de la vida privada, 1999 [16] Ley 19.223 sobre delitos informáticos, 1994 **Bibliografía Complementaria** [17] Schneier, Applied Cryptography. John Wiley Sons. Segunda edicion 1996. [18] A.W. Dent y C.J. Mitchell, User's Guide to Cryptography and Standards. Artech House, 2005 [19] Earle,Aaron E. Wireless security handbook, 2005 [20] Erickson, Hacking the art of explotation [21] Jakobsson, Markus Phishing and Countermeasures, 2007

Vigencia desde:	Otoño 2015
Elaborado por:	Sergio Miranda
Revisado por:	MIRC