UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

TEMARIO

- Introducción a la seguridad de la información y el mercado profesional: se presenta la seguridad como servicio y los temas relacionados con la demanda de profesionales en las empresas y organizaciones.

- Gestión de la seguridad de la información: identificación de los activos de una organización y desarrollo, documentación e implementación de políticas, estándares, procedimientos y guías.

- Arquitectura y modelos de seguridad: conceptos, principios, estructuras y estándares empleados para diseñar, monitorizar y asegurar sistemas, equipos, redes, aplicaciones y controles usados para reforzar la disponibilidad, integridad y confidencialidad.

- Sistemas y metodología de control de acceso: mecanismos que permiten crear una arquitectura segura para proteger los activos de los sistemas de información. Protocolos y sistemas utilizados en redes y sistemas operativos.

- Seguridad en el desarrollo de software: técnicas y procesos utilizados en el desarrollo de aplicaciones y sistemas. Metodologías, estándares y buenas prácticas de desarrollo seguro. Procesos de testing y QA.

- Seguridad de las operaciones: identificación de controles sobre el hardware, medios y operadores, y administrador con privilegios de acceso a recursos.

- Criptografía: principios, medios y métodos de protección de la información para asegurar su integridad, confidencialidad y autenticidad.

- Seguridad Física Defensiva: componentes y técnicas de protección de instalaciones, incluyendo los recursos de los sistemas de información y su gestión.

- Seguridad en Internet, Redes y Telecomunicaciones: dispositivos de red, métodos de transmisión, formatos de transporte, medidas de seguridad y autenticación.

- Recuperación ante Desastres y Planificación de la Continuidad del Negocio: Dirige la preservación del negocio en el caso de producirse situaciones de parada para la restauración de las operaciones.

- Leyes, investigaciones y ética: legislación y regulaciones de los delitos informáticos, técnicas de investigación, recuperación de evidencias y códigos éticos.

- Informática forense: identificación y recolección de evidencia, preservación y análisis de información, cadena de custodia. Recuperación de datos. Procesos de investigación.

- Cibercrimen y ciberactivismo: contexto mundial de la ciberdelincuencia, activismo informático y operaciones ilegales, incluyendo aspectos técnicos y no técnicos.

- Evaluaciones de seguridad: determinación de la necesidad de procesos de evaluación de la seguridad en organizaciones, detalles de su contratación y ejecución. Análisis de los tipos de evaluaciones.

- Introducción a Ethical Hacking: pruebas de penetración, el rol del hacker ético, objetivos, metodologías y entregables.Conceptos de seguridad ofensiva. Fuga de información, vulnerabilityresearch, hacking y hackers.

- Fases del proceso de Ethical Hacking: proceso completo de evaluación de seguridad técnica. Recopilación de información, uso de los buscadores en la investigación, escaneo y enumeración. Explotación de vulnerabilidades.

- Malware y Botnets: conceptos y categorías de software malicioso, métodos de propagación, técnicas evasivas en el malware. Botnets. Ataques de Phishing.

- Ataques a redes: detección y ataques a dispositivos de red, técnicas ofensivas básicas utilizadas en redes e Internet. Aplicaciones según entornos. Análisis de tráfico con fines ofensivos. Contraseguridad. Ataques a redes inalámbricas.

- Passwordcracking: métodos y técnicas de ataque a contraseñas. Escenarios típicos, sistemas estáticos y dinámicos. Técnicas físicas avanzadas. Herramientas útiles.

- Seguridad web: estudio de los principales tipos de vulnerabilidades encontrados en entornos web, su análisis y explotación mediante herramientas especializadas. Técnicas de anonimización. Uso del email como herramienta ofensiva.

- Ingeniería Social: uso de métodos no técnicos para el engaño de las personas con el fin de obtener información acerca de los sistemas que éstos utilizan.

- Seguridad Física Ofensiva: técnicas de ataque a la seguridad física, análisis de vulnerabilidades de la seguridad electrónica y ambiental, apertura de cerraduras y candados.

- Ingeniería reversa y seguridad en el software: introducción a las técnicas de reversing, uso de las herramientas básicas, descompilación y desensamblado, análisis estático y dinámico, análisis de binarios.

- Metodologías de PenetrationTesting: análisis y aplicación de las diferentes metodologías utilizadas en la tarea profesional. Confección de informes y presentación de entregables. Marco legal.

CRONOGRAMA DE CLASES

Clase 1
- Introducción
  - La seguridad como servicio
  - El mercado de la seguridad de la información
  - Certificaciones profesionales
  - Perfiles profesionales y trabajo
  - Educación en seguridad
  - Eventos y congresos especializados
  - Recursos y referencias
  - Bibliografía y lecturas complementaria

Clase 2
- Gestión de la Seguridad
  - Conceptos y definiciones
  - Gestión del riesgo
  - Procedimientos y políticas
  - Clasificación de la información
  - Responsabilidades y roles
  - Planes de concientización
  - Fuga de información
  - Ingeniería social

Clase 3
- Arquitectura y Modelos de Seguridad
  - Conceptos de control y seguridad
  - Modelos de seguridad
  - Criterios de evaluación
  - Seguridad en entornos cliente/servidor y host
  - Seguridad y arquitectura de redes

- Arquitectura de la seguridad IP

Clase 4

- Sistemas de Control de Acceso
  - Conceptos y tópicos
  - Identificación y autenticación
  - Sistemas single sign-on
  - Centralización del acceso
  - Metodologías de control
  - Monitorización y tecnologías

Clase 5

- Seguridad en el Desarrollo de Aplicaciones y Sistemas
  - Definiciones y conceptos
  - Amenazas y metas de seguridad
  - Ciclo de vida
  - Arquitecturas seguras
  - Control de cambios
  - Medidas de seguridad y desarrollo de aplicaciones
  - Bases de datos y data warehousing
  - Knowledge-basedsystems

Clase 6

- Seguridad de las Operaciones
  - Recursos
  - Privilegios
  - Mecanismos de control
  - Abusos potenciales
  - Controles apropiados
  - Principios

Clase 7

- Criptografía (I)
  - Historia y definiciones
  - Aplicaciones y usos
  - Conceptos y elementos
  - Protocolos y estándares
  - Tecnologías básicas
  - Sistemas de cifrado
  - Criptografía simétrica y asimétrica

Clase 8

- Criptografía (II)
  - Firma digital
  - Seguridad en el correo electrónico
  - Protección de datos locales y en tránsito
  - Criptografía enInternet

- Publickeyinfrastructure (PKI)
- Esteganografía y esteganálisis
- Ataques y criptoanálisis
- Aspectos legales

Clase 9

- Seguridad física y ambiental
  - Componentes de seguridad física
  - Tipos de amenazas
  - Gestión de las instalaciones
  - El plan de seguridad física
  - Seguridad del personal
  - Defensa en profundidad
  - Perímetro e interiores
  - Protecciones en datacenters
  - Sistemas de vigilancia y detección
  - Accesos físicos
  - Trashing y dumpsterdiving
  - Sistemas de suministro
  - Detección y supresión de incendios

Clase 10

- Seguridad en Internet, Redes y Telecomunicaciones (I)
  - Gestión de las comunicaciones
  - Redes de datos
  - Tecnologías de comunicaciones
  - Protocolos de red
  - Internet y Web

Clase 11

- Seguridad en Internet, Redes y Telecomunicaciones (II)
  - Firewalls
  - Sistemas de detecciónde intrusos (IDS)
  - Honeypots
  - Conexiones a escritorios remotos
  - Redes virtuales:VPN y VLAN
  - Tecnología inalámbrica

Clase 12

- Recuperación ante Desastres y Continuidad del Negocio
  - Conceptos de recuperación ante desastres y de negocio
  - Procesos de planificación de la recuperación
  - Gestión del software
  - Análisis de Vulnerabilidades
  - Desarrollo, mantenimiento y testing de planes
  - Prevención de desastres

UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Clase 13

- Cibercrimen
  - Fundamentos y funcionamiento
  - Malware y Botnets
  - Deep Web
  - Phishing y Spam
  - Operaciones internacionales
  - Casos de estudio
  - Prevención y acciones

Clase 14

- Leyes, investigaciones y ética
  - Legislación y regulaciones
  - Gestión de incidentes
  - Respuesta ante incidentes
  - Conducción de investigaciones
  - Análisis forense informático
  - Ética y seguridad
  - Códigos de ética

Clase 15

- Evaluaciones de seguridad
  - Servicios de evaluación
  - Marco legal de un test
  - Alcances y tipos de pruebas
  - Testing funcional y auditorías
  - Ethical Hacking y PenetrationTesting
  - Metodologías de evaluación
  - Etapas del proceso
  - Vulnerabilityresearch
  - Herramientas y software
  - Informes y entregables

Clase 16

- Desarrollo de Trabajo práctico grupal.

Clase 17

- Evaluación del módulo.
- Debate y devolución de resultados

Clase 18

- Introducción a Ethical Hacking
  - Las evaluaciones de seguridad.

- El hacker ético.
- Metodología de ataque.
- Entregables.
- Bibliografía.

Clase 19

- Fundamentos de seguridad de la información.
  - Conceptos y definiciones.
  - Fuga de información.
  - Vulnerabilityresearch.
  - Ingeniería social.
  - Control de accesos.

Clase 20

- Recopilación de información.
  - Método de recopilación.
  - Footprinting.
  - Sistema DNS.
  - Consultas de whois.
  - Traceroute.
  - Herramientas y sitios.

Clase 21

- Sistemas de inteligencia
  - Conceptos fundamentales
  - Datos e información
  - Análisis y correlación
  - Procesos y metodología
  - Equipo de investigación
  - Búsqueda de personas

Clase 22

- Escaneo y enumeración.
  - Tipos de escaneo.
  - Método de escaneo.
  - Escaneo de puertos.
  - OS Fingerprinting.
  - Banner Grabbing.
  - Tipos de Enumeración.
  - Escaneo de vulnerabilidades.
  - Explotación de vulnerabilidades.
  - Herramientas y sitios.

Clase 23

- Búsquedas online
  - Funcionamiento de los buscadores.
  - Uso avanzado de Google y Bing.

- Metabuscadores.
- Buscadores específicos.

Clase 24

- Malware y Botnets
  - Conceptos y categorías.
  - Métodos de propagación.
  - Formato de un ataque con malware.
  - Método de ataque de Phishing.
  - Cibercrimen.
  - Botnets.
  - Herramientas y sitios.

Clase 25

- Seguridad en redes
  - Tecnología, Internet y las empresas.
  - Firewalls.
  - Sistemas de detecciónde intrusos (IDS).
  - Honeypots.
  - Conexiones a escritorios remotos.
  - Redes virtuales (VPN y VLAN).
  - Tecnología inalámbrica.
  - Componentes y Autenticación inalámbrica
  - Protocolos inalámbricos y técnicas de ataque.

Clase 26

- Técnicas de ataque y análisis de tráfico
  - Sniffing.
  - Spoofing.
  - Hijacking.
  - PacketCrafting.
  - Poisoning.
  - Herramientas.

- Password Cracking
  - Conceptos.
  - Métodos de ataque.
  - Técnicas de ataque.
  - Herramientas.
  - Contramedidas.
  - Pruebas de fortaleza.

Clase 27

- Seguridad y correo electrónico
  - Conceptos.
  - Análisis de encabezados.
  - Anonimización.

  - Cuentas temporales.
  - E-mail tracking.
  - SPAM y filtrado.
  - Herramientas y sitios.

- Anonimidad web
  - Conceptos.
  - Proxies anónimos.
  - HTTP Tunneling.
  - Sistema TOR.
  - Servicios privados.
  - Recursos web.

Clase 28

- Vulnerabilidades web
  - A1: Inyección de código.
  - A2: Secuencia de Comandos en Sitios Cruzados (XSS).
  - A3: Perdida de Autenticación y Gestión de Sesiones.
  - A4: Referencia Directa Insegura a Objetos.
  - A5: Falsificación de Petición en Sitios Cruzados (CSRF).
  - A6: Configuración Defectuosa de Seguridad.
  - A7: Almacenamiento Criptográfico Inseguro.
  - A8: Falla de restricción de acceso a URL.
  - A9: Protección Insuficiente en la Capa de Transporte.
  - A10: Redirecciones y Destinos No Validados.

Clase 298

- Ingeniería Social
  - Conceptos y comportamientos vulnerables.
  - Fases de un ataque.
  - Ingeniería social inversa.
  - Tipos de ataque.
  - Dumpsterdiving.
  - Herramientas y sitios.

- Seguridad física ofensiva
  - Sistemas de suministro.
  - Perímetro e interiores.
  - Evasión de cámaras y CCTV.
  - Evasión de la detección.
  - Controles de acceso físico.
  - Ataques a datacenters.
  - Cerraduras y candados

Clase 30

- Ingeniería inversa y seguridad en el software
  - Conceptos fundamentales.

  - Desensambladores.
  - Debuggers.
  - Editores de encabezados.
  - Patchers y loaders.
  - Otras herramientas.
  - Buffer overflow.

Clase 31

- Metodologías de Penetration Testing
  - Conceptos principales.
  - Etapas de un Penetration Test.
  - Herramientas automatizadas.
  - Uso de Maltego.
  - Marco legal de un test.
  - Informes y Entregables.
  - Metodologías más utilizadas.

Clase 32

- Práctica final demostrativa
- Repaso de temas y técnicas

Clase 33

- Trabajo práctico final: Penetration Test sobre un objetivo.

Clase 34

- Debate y devolución de resultados.
- Cierre del curso.