UTN.BA
DEPARTAMENTO
INGENIERIA EN SISTEMAS DE INFORMACION

ASIGNATURA:	SEGURIDAD ACTIVA DE LAS COMUNICACIONES
DEPARTAMENTO:	ING. EN SIST. DE INFORMACION
AREA:	ELECTIVAS
BLOQUE	TECNOLOGÍAS APLICADAS

MODALIDAD:	Cuatrimestral
HORAS SEM.:	6 horas
HORAS/AÑO:	96 horas
HORAS RELOJ	72
NIVEL:	5º
AÑO DE DICTADO:	2018

Objetivos

- Comprender las características técnicas y funcionalidades vinculadas a la seguridad activa del hardware y del software en las redes y equipos terminales de redes fijas o celulares, tanto de conmutación digital de paquetes como de circuitos.
- Analizar y comprender los principios y estructura de las tecnologías activas de seguridad de comunicaciones telefónicas.
- Adquirir destrezas para operar estaciones de trabajo de protección activa para detección y bloqueo de intercepciones digitales ó spyware.
- Adquirir destrezas para hacer geolocalizaciones finas y trazabilidad directas e inversas de identificación con técnicas híbridas de triangulación, simulación y coordenadas polares.
- Adquirir habilidades para desempeñarse como perito proponiendo a la Justicia procedimientos y requerimientos a las prestadoras telefónicas y ejecutando las pericias ordenadas tanto de seguridad activa como de geolocalización fina y trazabilidad e identificación de móviles y celulares.
- Desarrollar y mejorar productos de software tanto para detección y bloqueo de intercepciones digitales como los aplicativos para geolocalizaciones finas y trazabilidad dentro de las redes teleinformáticas. Ensayos no determinísticos sobre prueba y error de laboratorio y de campo. Auditorias

Contenidos Mínimos (Programa Sintético).

- Seguridad activa en las redes
- Tecnlogías Comsec
- Detección y bloqueo de intercepciones digitales
- Geolocalizaciones finas

- Pericias comsec
- Pericias de geolocalización y trazabilidad
- Software de aplicación Comsec. Programas fuentes e insumos.
- Ensayos de laboratorio y de campo. Auditorias

Programa Analítico - Contenidos Pedagógicos:

Unidad 1: Seguridad pasiva y activa en redes digitales conmutadas

Proyecto Intercomunicación de microcontroladores presentado por UTN en el XI Congreso de Teleinformática

Características técnicas y funcionalidad del hardware y del software en las redes y equipos terminales analógicos y digitales de redes fijas o celulares, de conmutación digital de paquetes y de circuitos.

Seguridad pasiva y activa en las redes de telecomunicaciones. Encriptación de mensajes y de canales. Diferencias técnicas entre escuchas, intercepciones, capturas, adquisiciones, acumulación y administración de los mensajes digitales en las redes. DVCRAU pasivos y activos. Reliable technology vs tecnologías propietarias.

Unidad 2: Tecnologías Comsec

Comsec. Definiciones, principios y estructura de las tecnologías activas de seguridad de comunicaciones telefónicas. Orígenes, know how secreto y publicaciones filtradas. Tecnologías de seguridad abiertas y cerradas. Ejecución de códigos remotos huésped. Evolución global y local. Ventajas y desventajas tecnológicas. l. Proyecto Nacional de Seguridad Teleinformática.Peritajes judiciales de Gendarmería Nacional y UBA. Certificaciones de UTN. Convalidación Judicial.Pericias en causas judiciales nacionales y del exterior.

Unidad 3: Detecciones y Bloqueos.

Plataformas de los programas de espionaje global. Desde el Echelon al Prisma. Sistemas administradores de intercepciones integradas para las redes ip y pcm. Fortalezas y debilidades. Objetivo comsec: la Interface IMShost. Niveles app y físico. Administrador remoto desde la RTDC. Control universal del interceptor desde la RTPC mediante modems telefónicos. Detección y bloqueo de intercepciones digitales dentro de las redes telefónicas conmutadas digitales fijas y celulares. Comandos AT y códigos ejecutables en forma remota. Función Killapp. Estaciones de trabajo de protección activa para detección y bloqueo de intercepciones digitales ó spyware.

Unidad 4: Pericias de Seguridad y Geolocalización

Estudio de documentación y videos de redes unidades interceptoras en allanamientos a operadoras telefónicas en diversas causas judiciales.

Actas e informes periciales. Oficios de la Justicia Federal para la detección y neutralización de delitos de espionaje telefónico. Polémica y evaluación de los resultados en las pruebas de laboratorio y de campo. DVCRAU, IMS y Spyware.

Geolocalización fina por técnicas híbridas de triangulación, simulación y coordenadas polares de móviles y celulares, directas e inversas. Cálculos y mediciones con antenas. Estaciones radiobase y Centros de Conmutación. Bases de datos HLR y VLR. Pericias. Oficios a las operadoras telefónicas. Análisis de causas judiciales.

Unidad 5: Software de aplicación

Presentación y análisis del código fuente de un aplicativo de detección y bloqueo de intercepciones desde la RTDC y de un aplicativo carrier de bombardeo teleinformático.

Unidad 6: Insumos

Modelos Determinísticos y Estocásticos.Insumos troyanos. Mutación estocàstica. Ensayo prueba y error. Encriptación propietaria orientada al objeto. Semillas y update de los insumos DBA.exe y FOJ.exe: .3KEXP32. Control de calidad de insumos.

Carrier y Topologías para protección teleinformática activa COMSEC. Eficiencia y Redundancia.

Unidad 7: Ensayos y auditorías

Ensayos y análisis de laborstorio y campo desde líneas ip. Detección y bloqueo de un IMS simulando operadores remotos y envío de troyanos killapp. Auditoría de los Archivos troyanos DBA.cfg y DBAFOJ.cfg usando PC.

Bibliografía y/o Fuentes en Línea

- La seguridad de las telecomunicaciones y las tecnologías de la información. Recomendaciones UIT-T existentes. Union Internacional de Telecomunicaciones 2006
- Viruses, malware and remote attacks defined .KB Solution ID: KB186 |Document ID: 11136|Last Revised: September 9, 2016 ESET.
- Proyecto Intercomunicación de microcontroladores. Grupo Investigaciones Teleinformáticas- UTN - XI Congreso de Teleinformática.

- Interception Capabilities 2000 - Report to the Director General for Research of the European Parliament .Scientific and Technical Options Assessment programme office. Report by : Duncan Campbell, IPTV Ltd Edinburgh, Scotland : April, 1999. http://www.cyberrights.org/interception/stoa/interception_capabilities_2000.htm
- Certificado sobre el Carrier de Bombardeo Teleinformático para líneas telefónicas y sus insumos DBA112 y FOJ112 . Ingenieros Hugo Aparicio, Mauricio Vistosi y Andrés Mutti - Departamento de Electrónica - Facultad Regional Buenos Aires - UTN Diciembre de 2000
- Pericia Teleinformática sobre el software DBA . Dirección de Informática y Telecomunicaciones de Gendarmería Nacional. Septiembre de 2003. Juzgado Federal Nro 1 . Secretaria 24
- Intelligence Solutions . Lawful Interception and Monitoring .Using telecommunications to target terrorism and crime . Copyright © 2007 Nokia Siemens Networks . https://assets.documentcloud.org/documents/815861/1001-nokia-siemens networks-product-description.pdf
- Acta de Convalidación del Software DBA. Ingenieros Federico Pacheco, Hugo Aparicio, Mauricio Vistosi y Ariel Garbarz- Departamento de Sistemas- Facultad Buenos Aires - UTN - Agosto 2016 .
- Paquete del Software DBA : Carrier.scp, Dba.exe, Dba.cfg, Dbafoj. cfg . Ing Ariel Garbarz. Dirección Nacional de Derecho de Autor - Octubre 2016

Correlativas

Para Cursar:

Cursadas:

- Administración de Recursos
- Redes de Información
- Simulación
- Ingeniería de Software

Aprobadas:

- Diseño de Sistemas
- Sistemas Operativos
- Gestión de Datos

Para rendir:

Aprobadas:

- Administración de Recursos
- Redes de Información
- Simulación
- Ingeniería de Software