Temas de examen

▼ Ciencias de la seguridad

Análisis de tráfico

Interceptación y análisis de patrones de comunicación de mensajes incluso encriptados

Biometría

Ciencia de la verificación de identidad anatómica

Criptografía

Estudio de métodos y técnicas para encriptar y desencriptar. Abarca criptografía simétrica y asimétrica

Criptoanálisis

Disciplina que estudia las técnicas (autorizadas y no autorizadas) por las que se pueden obtener passwords o reducir un criptograma a texto plano

Criptoanálisis acústico

Intercepción de emanaciones de equipos electrónicos, térmicos u ópticos para comprometer passwords.

Las antenas pueden ubicarse a 20 o 30 metros de la fuente

Cripto-matemáticas

Estudia la fortaleza o vulnerabilidad de un sistema informático

Cripto-computación

Disciplina que estudia algoritmos y tecnologías más eficientes para encriptar o desencriptar

Ciencia en redes

Estudio de representaciones de redes físicas, biológicas y de fenómenos sociales que pueden ser predecibles

Ciphony

Ciencia que estudia y hace operativa la comunicación telefónica encriptada

Cómputo forense

Disciplina que aplica técnicas para identificar, preservar, analizar y presentar datos válidos en un proceso legal para perseguir criminales

Esteganografía digital

Esconder datos en archivos como imágenes

Goniometría, radiogoniometría, telemetría o ARDF

Encontrar la ubicación de un objeto en base al conteo de ticks desde varias estaciones de escucha

Lingüística computacional

Disciplina de IA que busca interpretar sonidos y lenguajes humanos para transcribirlos a texto

Lingüística estadística

Estudio de frecuencia en palabras y letras de un idioma

Procesamiento de señales

Disciplina que busca poder detectar, amplificar, aislar e interpretar señales mezcladas y tenues, usado en instalaciones militares

Seguridad de operaciones

Procesos y controles de una organización para garantizar prácticas seguras de sus usuarios

Vibrometría laser

Reconstrucción de diálogos a partir de la distorsión de cristales golpeados por ondas sonoras

▼ Ataques

Definición: Cualquier acción que explota una vulnerabilidad

Tipos de ataques

▼ Pasivos

Solo observan comportamientos o leen información, sin alterar el estado o información del sistema

- Preparan un ataque activo
- Solo afectan la confidencialidad y privacidad

Ejemplos de ataques pasivos

▼ Intercepción

Alguna parte no autorizada accede a un sistema

Técnicas

- Análisis de tráfico
- Espionaje de mensajes
- Autenticación: Por diccionario, 10K, Password Database, Biográfico, Fuerza Bruta, Rainbow o ataques tipo réplica
- Monitoreo: Customs, dropmire, magnetic, ocean, PBX, sniffer, vagrant, warchalking o wardrivers

▼ Activos

Modifica la información o estado de un sistema

Fabricación

Una parte no autorizada fabrica objetos falsos en el sistema

Técnicas

- Implantes baliza
- Homograph attack

- Sabotaje
- Spoofing
- Source Routing

Interrupción

Un archivo se pierde, se hace no disponible o inutilizable

Técnicas

- DoS
- Robo de tiempo de procesador
- Zombies

Modificación

Una parte o autorizada logra acceso al sistema y manipula archivos

Técnicas

- Blackheart
- Bombas lógicas
- Caballos de troya
- Defacement
- Dewsweeper
- DNS Poisoning
- Filtro de información
- Highlands
- Keylog
- Lifesaver
- Man in the middle
- Micrófonos ocultos
- Mineralize
- Quantum Insertion

- Radon
- RAM scrapper
- SQL Injection
- Tampering
- Virus

▼ Grupos y hacktivismo

Acción online encubierta

Ejemplos

- Deny, Disrupt, Degrade, Deceive (4 D’s)
- Trampas de miel
- Cambiar fotos en redes sociales
- Mandar emails a personas
- Impedir la comunicación de alguien
- Impedir el funcionamiento de la computadora de alguien
- Llevar un ataque DoS en una computadora
- Estrategias de desbaratamiento

▼ Tipos de hackers

Hacktivista

Se guía por la ética, busca hacer obsoleta la realidad y reemplazarla por una mejor

Pro Privacidad y en contra del realismo maquiavélico

Whistleblower

Obtiene un documento oficial y lo hace público, a modo de denuncia pública

Cripto-Libertarios

Fomentan la encriptación de paquetes y comunicaciones pues saben que el gobierno guarda el contenido de internet

Anti-Ubicación

Limitan las cámaras públicas y los RFID

Saboteadores

Crasher

Defacer: Dejan firmas en servidores, muestran su vulnerabilidad

DOS: Sabotean un servidor

Viruxer: Script kiddle

De la propiedad intelectual

Cracker: Rompe la seguridad de un sistema, usar material sin pagar por él

Warez: Toma un crack y lo hace público

Phreaker

Consumidores indignados

Contra la obsolescencia programada

Libre

FS, Wikipedia, Creative Commons, Gutenberg, DOAJ, IntechOpen, Wikibooks, Research Gate

Cruncher

Boinc

Dona sus ciclos de reloj a proyectos

Anti manipulación THC

▼ Servicios de seguridad

Definición: Característica que debe tener un sistema para satisfacer una política de seguridad

Autenticación

Definición: Que la información provenga de fuentes autorizadas

Tipos

- **De identidad**
- **De origen de datos**
- **Directa:** Solo intervienen las partes interesadas
- **Indirecta:** Invierte una tercera parte confiable
- **Unidireccional:** Solo una se autentifica
- **Mutua:** Ambas se autentifican

Se basa en

Algo que se sabe: Contraseñas

Algo que se tiene: Dispositivos, archivos, llaves o celular

Algo que se es: Biometría, huellas digitales, iris, voz

Confidencialidad

Definición: La información solo la conocen quienes tienen acceso a ella, se basa en la criptografía

Tipos

- Con conexión
- Sin conexión
- Selectiva de campo
- De flujo de tráfico

Integridad

Definición: La información no es alterada sin autorización, se integra con funciones de dispersión (hash)

Tipos

- Con conexión con recuperación
- Con conexión sin recuperación
- Con conexión selectiva de campos
- Sin conexión
- Sin conexión selectiva a campos

No repudio

Definición: Protección contra la posibilidad de que una de las partes niegue haber enviado o recibido un mensaje o haber sido el destinatario de una acción

Tipos

- Con prueba de origen
- Con prueba de entrega

Control de acceso

Definición: Control de la penetración física, en persona

Disponibilidad

Definición: Que se pueda acceder a la información cuando se requiere

- Respuesta puntual
- Asignación justa

Mecanismos de seguridad

Definición: Procedimientos concretos para implementar un servicio de seguridad

- Cifrado (simétrico y asimétrico)
- Control de encajamiento
- Firma digital
- Notarización (certificados digitrales)
- Tráfico espurio

- Hash