SEGURIDAD DE LA INFORMACIÓN

CURSO TEÓRICO-PRÁCTICO

DIRIGIDO A: Estudiantes, profesionales y técnicos superiores en informática, computación, sistemas, telecomunicaciones y áreas afines, así como a gerentes de sistemas, gerentes de seguridad (CISO), administradores de redes, consultores, analistas, desarrolladores, programadores, pentesters, auditores, peritos forenses, abogados, fiscales y jueces que se ocupan de delitos informáticos.

MODALIDAD: El curso se realiza a distancia, de forma no-presencial, utilizando un DVD como material de apoyo, complementado con consultas en línea o por correo electrónico. En el DVD se encuentran las presentaciones de las clases, artículos técnicos y libros electrónicos, guías para las experiencias prácticas, así como los programas y herramientas para efectuar dichas prácticas.

EQUIPAMIENTO: Disponer de PC o laptop de buenas prestaciones y acceso a Internet, preferiblemente sin restricciones impuestas por proxies y firewalls.

REQUISITOS DESEABLES: Conocimientos en el área de telecomunicaciones, redes y protocolos, especialmente TCP/IP. Familiaridad con el uso de computadoras, sistemas operativos (Windows, Linux, Android), redes de área local (LAN), redes inalámbricas Wi-Fi, Internet. Conocimiento instrumental del idioma inglés.

EVALUACIÓN: A lo largo del curso el participante deberá realizar una serie de actividades. La realización con esmero, dedicación y constancia de las actividades planificadas, determinará el nivel de conocimientos, destrezas y competencias que el participante habrá adquirido al completar el curso. La evaluación del aprendizaje se realiza básicamente mediante cuestionarios y exámenes parciales (tests) sobre la teoría e informes sobre las prácticas.

- Al menos 8 cuestionarios sobre 8 tópicos de teoría: 25%
- Al menos 8 exámenes parciales (tests) sobre 8 tópicos de teoría: 25%
- Al menos 6 informes sobre 6 experiencias prácticas: 25%
- Examen final (test general) sobre al menos 8 tópicos de teoría: 25%

DOCENTE: Ing. Vincenzo Mendillo - Profesor Titular (UCV - USB - UNIMET - UCAB)

- Ingeniero Electricista (Especialidad: Telecomunicaciones) - Universidad Central de Venezuela
- Master of Science in Electronics - University of Southampton
- Live Senior Member IEEE - Institute of Electrical and Electronics Engineers
- Miembro de CriptoRed - Red de Criptografía y Seguridad de la Información
- Coordinador del Diplomado STIT en Seguridad en Tecnología Informática y Telecomunicaciones.
- Presidente y miembro fundador de ASOVESINFO (Asociación Venezolana de la Seguridad de la Información)

DESCRIPCIÓN DEL CURSO:
En esta era de conectividad global, de Internet y de comercio electrónico, de fraudes informáticos y de teléfonos interceptados, de virus y de hackers, la seguridad de la información se ha vuelto un asunto de vital importancia. El crecimiento explosivo de sistemas informáticos y sus interconexiones a través de redes públicas como Internet, ha aumentado la dependencia, tanto de las organizaciones como de los individuos, de los datos almacenados, procesados y transmitidos de forma digital. Esto a su vez ha llevado a una mayor necesidad de resguardar la confidencialidad, la integridad y la disponibilidad de la información, de garantizar la autenticidad de los datos y de las personas, así como poder de defenderse de ataques internos y externos. Por otro lado las técnicas de protección han madurado, estando a disposición una multiciplicidad de productos comerciales y open source que ofrecen un alto grado de seguridad.

En este curso se estudian los distintos aspectos de la seguridad de la información, tal como confidencialidad, integridad, disponibilidad y autenticidad. Después de explicar la terminología pertinente, se identifican las amenazas, vulnerabilidades y riesgos que podrían afectar la seguridad. Se muestran las herramientas usadas por los hackers para

penetrar en los sistemas y las aplicaciones Web, explotando las brechas de los sistemas operativos, los programas y el descuido de los usuarios. Se analizan distintas formas de ataque y se llevan a cabo prácticas de adiestramiento sobre captura de tráfico (*sniffer*), captura de teclado (*keylogger*), interceptación de llamadas telefónicas, programas espía y puertas traseras, negación de servicio (*DoS*), revelación de contraseñas, etc. Se explican las medidas de seguridad que se deben utilizar en ambiente corporativo y en las transacciones electrónicas, haciendo énfasis en la importancia de desarrollar una estrategia de seguridad integral con políticas, normas, procedimientos y planes de contingencia, conjuntamente con un análisis de riesgos. Se llevan a cabo prácticas de adiestramiento en auditoría de seguridad, pruebas de penetración, criptografía, esteganografía, gestión de contraseñas, respaldo y restauración de datos, forénsica digital, barreras de protección (*firewalls*), sistemas de detección de intrusos (IDS), redes privadas virtuales (VPN), firma digital, seguridad en voz sobre IP y telefonía por Internet, seguridad en el correo electrónico, seguridad en las comunicaciones inalámbricas, etc.

Al completar el curso, el participante habrá obtenido una amplia visión de las amenazas, vulnerabilidades y riesgos existentes en el campo de la informática y las comunicaciones. Además, será capaz de implantar medidas de seguridad de carácter preventivo, correctivo e investigativo, así como utilizar las herramientas adecuadas para frustrar los ataques, mitigar los riesgos y garantizar un alto grado de seguridad.

Las empresas valoran cada vez más la posesión de una certificación profesional que avale los conocimientos de su personal clave, además de un título formal universitario. Por tal razón durante el curso se trata de preparar al participante para que pueda aspirar a obtener las certificaciones internacionales de más alta reputación, tal como CISSP (*Certified Information Systems Security Professional*), SSCP (*Systems Security Certified Practitioner*), CCFP (*Certified Cyber Forensics Professional*), CCSP (*Certified Cloud Security Professional*), CISA (*Certified Information Systems Auditor*), CISM (*Certified Information Security Manager*), CSX Practitioner, GIAC (*Global Information Assurance Certification*), CompTIA Security+, CEH (*Certified Ethical Hacker*), CHFI (*Computer Hacking Forensic Investigator*), etc.

OBJETIVO GENERAL:
Proporcionar una visión integrada de las diferentes vertientes la seguridad de la información: estratégica, táctica y operativa. Conocer cómo los problemas de seguridad afectan a las organizaciones que manejan sistemas informáticos y están conectadas a Internet. Aprender cómo se seleccionan e implantan medidas de protección para resguardar la confidencialidad, integridad y disponibilidad de la información; garantizar la autenticidad de los datos y de las personas, así como defender a los sistemas de ataque internos y externos.

OBJETIVOS ESPECÍFICOS:

- Identificar las amenazas y vulnerabilidades, evaluando los riesgos asociados al manejo de la información en los sistemas informáticos y en las redes de comunicación.
- Analizar las situaciones de una red o un equipo que facilitan la penetración de intrusos y hackers y cuáles son los métodos de ataque empleados.
- Evaluar las condiciones de seguridad que imponen a las organizaciones los nuevos entornos de trabajo, tales como Internet, acceso remoto, teletrabajo, comunicaciones unificadas, redes inalámbricas, teléfonos inteligentes.
- Implantar las medidas de seguridad para defenderse de las amenazas internas y externas a través de controles apropiados, tomando en cuenta las nuevas amenazas y vulnerabilidades que continuamente aparecen.
- Administrar la seguridad física y ambiental en centros de datos y oficinas.
- Elaborar planes de contigencia y y reactivación de operaciones ante desastres.
- Investigar incidentes de seguridad y realizar el análisis forense de sistemas informáticos y dispositivos móviles.
- Prepararse para obtener algunas de las certificaciones profesionales en el campo de la seguridad de la información.

CONTENIDO PROGRAMÁTICO

1. FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN
¿Por qué es importante la seguridad? Requisitos básicos para la seguridad de la información: Confidencialidad, integridad, disponibilidad. Otros requisitos: privacidad, secrecía, anonimato, autenticidad, autorización, trazabilidad, no repudiación. Conceptos básicos en seguridad (activo, amenaza, vulnerabilidad, incidente, ataque, exploit, impacto, riesgo, control). Amenazas internas y externas. Amenazas avanzadas persistentes (APT). Las vulnerabilidades y su clasificación. Bases de datos de vulnerabilidades (CVE, Bugtraq, etc.). Introducción a la gestión de riesgos. Tres

principios de la seguridad de la información. Introducción a las medidas de protección. Tipos de controles (disuasivo, preventivo, correctivo, investigativo). Ejemplo de controles. Seguridad física, técnica y administrativa. Seguridad en profundidad. Estrategia de defensa estratificada.

2. AMENAZAS, VULNERABILIDADES Y RIESGOS

Principales problemas para la información que se trasmite, procesa o almacena (interceptación, divulgación, uso no autorizado, interrupción, alteración, manipulación, fabricación). Interceptación ilegal de llamadas telefónicas. IMSI IMSI catcher. Stingray. Interceptación legal y LIMS (*Lawful Interception of Telecommunication Services*). Ley CALEA. Interceptación de datos mediante sniffers. Interceptación de actividades en el teclado mediante keyloggers. Divulgación de información. Wikileaks. Uso no autorizado de recursos. Robo de servicio. Alteración, manipulación y fabricación de información. Vandalización de páginas Web. Interrupción e indisponibilidad de la información. Congestión y retardo en redes y servicios. Fallas: causas y costos. Censura y bloqueo de sitios Web. Interferencia intencional en redes inalámbricas. Robo de cable. Ley de Murphy y sus corolarios. Accidentes y desastres (inundación, terremoto, incendio, calor, falla de energía eléctrica, apagón).

3. ATAQUES Y DELITOS INFORMÁTICOS

El blanco de los ataques. Modalidad de ataques (activo, pasivo). Clases de ataques (hardware, software, datos). Ataques de negación de servicio (DoS, DDoS). Programas malévolos (virus, gusano, caballo de Troya, ransomware, spyware, adware). Botnets (Zeus, SpyEye). Actividades malévolas (hoax/bulo, spam/correo indeseado, phishing, spear phishing). Hackers y crackers. Ataques de hackers. Rootkit y shellcode. Espionaje gubernamental, militar, comercial, industrial, laboral y personal. Guerra cibernética y terrorismo. Ataques a los sistemas industriales de control y supervisión (SCADA). Ciberarmas (Stuxnet, Flame). Cibercrimen y delitos informáticos (fraude, estafa, extorsión, lavado de dinero, pornografía infantil). Triángulo del fraude. Fraude bancario y falsificación de datos. Robo en telecajeros. Delitos utilizando las redes. A la caza de datos personales (redes sociales, Google, Pipl, Maltego, i2). Robo de identidad. Ingeniería social. Phreakers y fraude telefónico. Fraude en telefonía celular. Robo de teléfonos inteligentes, alteración del código IMEI y liberación. Piratería de software. Piratería en audio y video.

4. INSEGURIDAD EN REDES Y EN APLICACIONES WEB

El reto de las redes empresariales. Inseguridad en las redes externas (WAN) y en Internet. Ataques a DNS (*Domain Name System*). DNS spoofing y DNS poisoning. Inseguridad en la nube (*cloud*). Inseguridad en las redes internas (LAN). El peligro del hub y la ventaja del switch. Interceptación mediante puerto espejo (SPAN). Falsificación y envenenamiento de paquetes ARP. Cain y Ettercap. Inseguridad en SSL/TLS y HTTPS. Ataque a SSL mediante ARP spoofing. SSL stripping, FREAK, POODLE. Inspección del tráfico SSL. Inseguridad en IPv6. Inseguridad en redes inalámbricas y dispositivos móviles. Inseguridad en Wi-Fi. Sniffers inalámbricos. Inseguridad en Bluetooth (bluejacking, bluesnarfing, bluebugging). Interferencia y negación de servicio (DoS). Inseguridad en redes sociales. Inseguridad en aplicaciones Web. Vulnerabilidades más graves según OWASP. Desfiguración de páginas Web. Ataques a la autenticación HTTP básica, digest o basada en formularios GET/POST. Ataques hidden fields, directory traversal, session fixation. Secuestro de sesión. Ataques del lado del cliente (browsers, PDF, Flash...). Ataques por desbordamiento de buffer, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), XML External Entity (XXE), SQL Injection. Ambiente de entrenamiento en línea (Hack-a-Server, Hack.me, PentesterLab, MDSec, Altoro Mutual, Acuforum, FreeBank, Gruyere) y Live-DVD (Metasploitable, WebGoat, InsecureWebApp, DVWA, Samurai Web Testing Framework, Web Security Dojo). Inseguridad en VoIP y telefonía por Internet. Captura de tráfico de VoIP mediante sniffers. Interceptación y decodificación de tonos de discado DTMF. Otros tipos de ataques: Enumeración, inundación, negación de servicio, desconexión forzada, spam sobre telefonía IP (SPIT), phishing, fuzzing, etc.

5. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Planificación de la seguridad. Desarrollo de un sistema de gestión de seguridad de la información (SGSI). Gestión de riesgos. Riesgo empresarial (estratégico, financiero, incumplimiento, operativo, tecnológico). Riesgos naturales y del medio-ambiente, riesgos de desastres. Estándares y normas (ISO 27005, UNE 71504). Metodologías para la gestión de riesgos (ISO 31000, MAGERIT, COBIT, COSO, NIST, OCTAVE, CORAS, CRAMM, IRAM, SOMAP, FAIR). Enfoque cualitativo y cuantitativo. Expectativa de pérdidas anualizadas (ALE) y retorno de la inversión en seguridad (ROSI). Políticas, normas, estándares y procedimientos de seguridad. Políticas generales y específicas. Ejemplos (clasificación y privacidad de la información, uso aceptable, almacenamiento y borrado seguro). Madurez de una organización en seguridad y CMMI. Estándares internacionales, metodologías, recomendaciones y buenas prácticas para la seguridad de la información: ISO ISO 27000, X.805, TCSEC, ITSEC, FIPS 140, NIST SP800, Common Criteria (ISO 15408), COBIT, PCI DSS, ITIL.

6. AUDITORÍA DE SEGURIDAD, HACKING ÉTICO Y PRUEBAS DE PENETRACIÓN

¿Qué se entiende por auditoría? Tipos de auditorías. Auditoría interna y externa. Auditoría de sistemas. El proceso de auditoría. Metodologías y buenas prácticas (ISACA, COSO). Gobernabilidad de TI. Auditoría de seguridad. Áreas de la

auditoría de seguridad (física, lógica, administrativa). Tipo y alcance de la auditoría. Auditoría tipo black box, white box y gray box. Equipo rojo y equipo azul. Ejemplos de cuestionarios para auditoría de redes y sistemas. Metodología OSSTMM (*Open Source Security Testing Methodology Manual*). The OWASP Testing Framework. OWISAM (*Open WIreless Security Assessment Methodology*). Hacking ético. Pruebas de penetración. Alcance y limitaciones. Metodología PTES (*Penetration Testing Execution Standard*). Tipos de pruebas (interna/externa, a ciegas/con conocimiento). Fases de las pruebas de penetración. Recopilación de información (*footprinting*). Uso de *competitive intelligence*. Whois. Google hacking. Traceroute. Reconocimiento activo. War dialing. ICMP y *ping sweep.* Escaneo de puertos. Nmap. Enumeración. Identificación y evaluación de vulnerabilidades. Herramientas ((LanGuard, Nessus, OpenVAS, NeXpose, Retina, McAfee Vulnerability Manager). Ataques y escalada de privilegios. Rootkit. Shellcode. Explotando vulnerabilidades del lado del cliente. Actividades de post-penetración. Borrando los rastros. Herramientas avanzadas para auditoría y pruebas de penetración (CORE Impact, Kali Linux, Metasploit). Hacking y pruebas de penetración con Android. Auditoría de aplicaciones Web. Metodologías. Escaners de vulnerabilidades Web (Paros, Burp, ZAP, Webscarab, Nikto). Auditoría Web automatizada (Acunetix, Nessus, W3AF, VEGA, Arachni, IBM AppScan, HP WebInspect, Cenzic, MileSCAN, Netsparker, Klypex, RETINA Web, WebSecurify, Qualys).

7. FORÉNSICA DIGITAL, LEY Y ÉTICA

Incidentes de seguridad. Clasificación. Ataques internos y externos. Malware y DoS/DDoS. Botnets y ransomware. Escenarios y análisis de casos. Plan de respuesta a incidentes. Gestión de incidentes (preparación, identificación, clasificación, análisis, contención, erradicación, recuperación, investigación, resolución, lecciones aprendidas, documentación). Operación de un centro de respuesta CSIRT/CERT. Proyecto AMPARO de LACNIC. Norma ISO 27035. Guías 800-61 y 800-184 del NIST. Prevención, detección y respuesta para fraudes bancarios y fraudes telefónicos. Investigación forense. Evidencia física y digital. Tipos de evidencia: Total, relevante y admisible. Manejo de la evidencia. Imagen bit-a-bit. Herramientas (Autopsy, FTK, EnCase, CAINE, DEFT, PALADIN, SIFT, OSForensics, X-Ways Forensics, HELIX). Ejemplos de escenario. Resolución de casos. Análisis forense de dispositivos móviles. actividades ilícitas por medio de teléfonos celulares. Procedimiento forense en dispositivos móviles. Herramientas forenses (Cellebrite, MobilEdit, MicroSystemation XRY, Oxygen Forensics, NowSecure, Magnet Axiom, Paraben, Andriller). Adquisición manual, lógica y física. Extracción lógica mediante ADB (*Android Debug Bridge*). Rootear Android. Extracción física mediante DD. Análisis de datos extraídos mediante FTK Imager Lite, PhotoRec, strings, Autopsy. Identificación forense de hablantes. Decodificación de tonos de discado DTMF (*Dual-Tone Multi-Frequency*). Aspectos jurídicos en la seguridad de la información. Sistemas jurídicos en el mundo. Legislación venezolana: Ley contra delitos informáticos, Ley de telecomunicaciones, Código penal, Código orgánico procesal penal (COPP). Legislación internacional: Sarbanas-Oxley, HIPAA, PCI-DSS. La propiedad intelectual y la protección del software. Digital Millennium Copyright Act (DMCA). Aspectos éticos y morales. Deodontología y teleología. Ética e Internet. RFC 1087. Códigos de ética (IEEE, CIV, ISACA, CISSP, EC-COUNCIL, SANS). Ética en el sector bancario y financiero.

8. SEGURIDAD FÍSICA Y AMBIENTAL

Las 3 categorías de la seguridad: administrativa, técnica (lógica) y física. Niveles y anillos de seguridad. Protección física de los equipos. Protección perimetral de un sitio (guardias, casetas, barreras, cercas, iluminación, vigilancia electrónica y CCTV, detección de intrusos). Acceso vehicular y peatonal. Controles de entrada para empleados y visitantes. Acceso a locales y oficinas (llaves y cerraduras, tarjetas de identificación, RFID, NFC, biometría). Identificación por huella dactilar, iris, voz. Reconocimiento facial. Selección de un sitio seguro. Ejemplos de Data Center. Sala “cofre”. Seguridad ambiental y protección contra desastres naturales. Protección contra transitorios eléctricos y apagones. Utilización de filtros, UPS y plantas de emergencia. Protección contra incendio. Detección y extinción de incendios. Clases de incendios y agentes extintores. Rociadores. Normas NFPA y COVENIN. Sistemas de ventilación y aire acondicionado (HVAC). Requerimientos para centros de datos. Normas y estándares (NFPA, COVENIN, ANSI/TIA-942, ANSI/NECA/BICSI-002). Seguridad industrial y salud ocupacional. Radiación electromagnética y salud. El ambiente de trabajo (físico, psicológico y social). Estrés laboral. Ergonomía. Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (LOPCYMAT). Organización Internacional del Trabajo (OIT).

9. DEFENSA CONTRA FALLAS, ACCIDENTES Y DESASTRES

Gestión de fallas y FCAPS (*failure, configuration, accounting, performance, security*). Diferencia entre fallas, eventos, errores, problemas. Notificación de eventos. Detección y resolución de problemas. Sistema de boletín de avería (*trouble ticket*). Soporte al usuario y *help desk*. Herramientas para detectar y resolver problemas (*troubleshooting*). Herramientas de diagnóstico para computadores. Causas de fallas en discos duros. Predicción de fallas y SMART (*Self-Monitoring, Analysis and Reporting Technology*). Sistemas tolerantes a fallas. Tecnología RAID (*Redundant Array of Independent Disks*). Failover. Duplicación del servidor. Clustering. Prevención de pérdida de datos (DLP). Eliminación de datos de forma irrecuperable. Respaldo y restauración de datos. Recuperación de archivos borrados. Recuperación de datos en discos dañados. Plan de contingencia y recuperación ante desastres. Plan de continuidad de negocio (BCP) y análisis de impacto en el negocio (BIA). Norma ISO/IEC 24762 e ISO 22301. Plan de continuidad en el sector financiero. Alerta temprana y telecomunicaciones de emergencia. Protección de infraestructuras críticas para la seguridad nacional.

Fundamentos de confiabilidad y mantenimiento. Tasa de fallas y curva de la bañera. Mantenibilidad y disponibilidad. MTTF, MTBF y MTTR. Confiabilidad de sistemas (serie, paralelo, stand-by, failover). Redundancia 1:1 y 1:N. Confiabilidad de sistemas electrónicos.

10. DEFENSA CONTRA INTRUSOS Y BARRERAS DE PROTECCIÓN

Defensa contra virus, troyanos y software malintencionado (*malware*). Sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS). Falsos positivos y falsos negativos. NIDS e HIDS. WIPS (*Wireless intrusion prevention system*). Técnicas de evasión contra IDS. Plataformas SIEM (*Security Information and Event Management*). OSSIM (*Open Source Security Information Management*). SOC (*Security Operations Center*). Señuelos y cebos (*honeypots*). Productos y soluciones (*Snort, Suricata, Snorby, Tripwire, OSSEC*). Barreras de protección y cortafuegos (*firewalls*). Arquitectura y topología de firewalls. DMZ (*demilitarized zone*). Filtros de paquetes. Firewall de Windows. IPtables. Configuración de filtros. Firewalls comerciales y firewalls personales. Firewalls para aplicaciones Web (*ModSecurity, GreenSQL, SecureSphere*). Ataques y auditoría de firewalls. Servidores proxy. Squid. Proxy transparente. Proxy inverso. Proxy anónimo. TOR (*The Onion Routing*). FreeNet. Túneles mediante HTTP. Canales encubiertos y canales inversos. RAT (*Remote Administration Tool*s). NetCat.

11. CRIPTOGRAFÍA Y PROTECCIÓN DE LA CONFIDENCIALIDAD

Criptología, criptografía, criptoanálisis y esteganografía. Criptografía clásica. Cifrado por sustitución y por transposición. Criptografía moderna. El algoritmo DES (*Data Encryption Standard*) y Triple DES. Otros algoritmos de cifrado (IDEA, SAFER, CAST, Blowfish, RC2, RC4, RC5, AES, Serpent, Twofish). Algoritmos en telefonía celular. Encriptación en discos duros y medios extraíbles. OTFE (*On The Fly Encryption*) con PGPdisk, TrueCrypt, EFS (*Encrypted File System*), BitLocker. PBE (*Password Based Encryption*). Desarrollos futuros: Criptografía cuántica. Distribución de claves criptográficas. Uso de KDC (*Key Distribution Center*). Generación de números aleatorios. Criptografía de clave pública. Ataque del hombre en el medio (MiTM) Sistema DH (*Diffie-Hellman*). Sistema RSA (*Rivest-Shamir-Adleman*). Criptografía de curva elíptica (ECC). Bases matemáticas: Exponencial discreta, factorización de números primos. Aplicaciones: Firma digital, distribución de la clave de sesión, digital envelope, criptomonedas (Bitcoin). Esteganografía e información oculta. Técnicas esteganográficas. Canales encubiertos. Huevos de Pascua. Estegoimagen. Estegoanálisis. Marca de agua digital.

12. INTEGRIDAD Y AUTENTICIDAD DE LA INFORMACIÓN

El problema de la integridad de datos. Medios físicos de transmisión y almacenamiento. Ruido térmico. Filtros eléctricos. Relación señal a ruido S/N. Ruido impulsivo e interferencia. Fuentes de interferencia electromagnética (EMI). Cable trenzado y cable coaxial. Fibra óptica. Atenuación y distorsión en los cables. Ecualización de la línea. El problema de la diafonía. Medios de transmisión inalámbricos. Interceptación y jamming. Medios transportables (cinta magnética, memoria SD, CD-ROM, DVD). Control de errores (paridad, CRC). Corrección de errores (Hamming, confirmación). Chequeo de integridad mediante hash. Funciones hash: MD5, SHA, RIPEMD, Whirpool. Uso de MAC (*Message Authentication Code*) y HMAC. Árbol de hashes (Merkle tree) y blockchain. Dinero digital. Firma electrónica. Código Seguro de Verificación (CSV). Firma electrónica avanzada/cualificada. Modos de firma (implícito, explícito). Firmas múltiples: Cofirma y contrafirma. Normativa nacional e internacional: ESIGN, EIDAS. Firma digital. Generación con RSA y DSA. Sobre digital (*digital envelope*). PGP. Certificados digitales X.509. Estándares PKCS. Obtención y revocación de certificados digitales. Certificados digitales para servidores web. Seguridad con EV-SSL. Certificados de raíz y certificados autofirmados (*self-signed*). Generación de certificados con OpenSSL, MakeCert, SelfSSL. Infraestructura de clave pública (PKI). Autoridades de certificación (CA). Aplicaciones de PKI: Navegación segura con HTTPS, banca en línea, compras por Internet, correo electrónico seguro, VPN, fechado digital (*time stamp*). Formatos de firma electrónica: PKCS#7, CMS, XMLdSig, CAdES, XAdES, PAdES, ODF, OOXML. Modos de operación de firma XML (*detached, enveloping, enveloped*). Productos y servicios. @Firma (Gobierno de España). Factura electrónica.

13. AUTENTICACIÓN DE PERSONAS Y CONTROL DE ACCESO

Modelo de un sistema de autenticación y control de acceso. ¿Qué se entiende por autenticación de personas? Credenciales para la autenticación. Identidad digital. Credenciales contextuales. Autenticación robusta. Autenticación HTTP básica. Autenticación digest. Autenticación mediante formularios GET/POST. Otros sistemas de autenticación: CHAP (*Challenge Handshake Protocol*); EAP (*Extensible Autentication Protocol*); OAuth (*Open Authorization*); FIDO (*Fast IDentity Online*) Alliance. Autenticación basada en lo que la persona sabe, posee o es. Contraseñas estáticas y contraseñas dinámicas (OTP). Sistema de dos o más factores y desafío-respuesta. Autenticación en la banca electrónica. Autenticación en Internet mediante CAPTCHA. Dispositivos de autenticación: tarjeta, RFID, ficha (*token*), biometría. Certificado digital. Transacciones bancarias. Normativa de SUDEBAN. ¿Cómo se guardan las contraseñas en el sistema? Contraseñas en Windows. Hash LM y NTLM. El archivo SAM (*Security Accounting Manager*). Contraseñas en Unix/Linux. Uso de *salt*. El archivo */etc/shadow.* Hash moderno: PBKDF2. PBE (*Password Based Encryption*). Recomendaciones para contraseñas seguras. Generadores de contraseñas. Gestión de contraseñas.¿Cómo saltarse la contraseña de Windows? Autologon. Recuperación de contraseñas olvidadas en Windows y Linux. Recuperación de

contraseñas para documentos de Office y PDF. Ataques a contraseñas (offline/online). Técnicas de diccionario y de fuerza bruta. Uso de tablas Rainbow. Pass-the-Hash. Ingeniería social y phishing. Autenticación, autorización y accounting (AAA). RADIUS, TACACS, DIAMETER. Sistema de autenticación Kerberos. Gestión de identidad en las empresas (*Identity Management*). Registro único mediante SSO (*Single Sign On*). OpenID. Control de acceso. El principio del mínimo privilegio. Control de acceso a red (NAC). Modelos de control de acceso. Control de acceso discrecional (DAC) y mandatorio (MAC). Control de acceso basado en roles (RBAC). Modelos Bell-LaPadula, Biba, Clark-Wilson. Control de acceso en Windows y Unix/Linux. Control de ejecución para el software. Uso de CPUID.

14. SEGURIDAD EN REDES Y EN INTERNET

¿Existen redes realmente seguras? SIPRnet, NIPRnet y Tor. Seguridad mediante LAN virtual (VLAN). Seguridad para la nube (*cloud computing*) y modelos (SaaS, PaaS, IaaS). Seguridad en DNS (*Domain Name System*).Uso de la criptografía en las comunicaciones. Cifrado en el modelo de capas OSI. Seguridad mediante LAN virtual (VLAN). Protocolos de seguridad en las capas altas (SSL/TLS, HTTPS). Seguridad en compras por Internet. Seguridad en aplicaciones bancarias, cajeros automáticos y puntos de venta. Seguridad en redes sociales (Facebook, Twitter). Seguridad en mensajería instantánea (Skype, WhatsUp, Telegram, LINE, Signal, Cryptocat, Blackberry). Seguridad en correo electrónico (S/MIME, PGP). Seguridad en dispositivos móviles y smart phones. Seguridad en aplicaciones Web. Web application firewalls (WAF). Seguridad en acceso remoto. Herramientas de remoto (VNC, TeamViewer, LogMeIn, Escritorio Remoto de Windows). Túneles mediante Redes Privadas Virtuales (VPN). VPN mediante proxies, Hamachi, PPTP. VPN mediante SSL, OpenVPN, SSH. VPN mediante IPSec. DirectAccess en Windows Server. Soluciones open source para VPN con IPSec: StrongSwan y OpenSwan.

15. SEGURIDAD EN COMUNICACIONES INALÁMBRICAS

El problema de la seguridad en redes inalámbricas. Autenticación y asociación en WLAN. Autenticación abierta (OSA) y por clave compartida (SKA). Control de acceso básico mediante SSID y filtros MAC. Encriptación mediante WEP (*Wired Equivalent Privacy*). Gestión de claves compartidas. Problemas y limitaciones de WEP. Ataques a WEP y Aircrack. Nuevos mecanismos de seguridad. WPA (*Wi-Fi Protected Access*). TKIP (*Temporal Key Integrity Protocol*). Autenticación robusta mediante EAP (*Extensible Authentication Protocol*) con clave compartida (EAP-PSK). Instalación y configuración fácil mediante WPS (*Wi-Fi Protected Setup*). Autenticación avanzada con servidor RADIUS y 802.1X. Seguridad moderna con WPA2/802.11i y AES (*Advanced Encryption Standard*). Seguridad adicional con túneles VPN (*Virtual Private Network*). WIMP (*Wireless Intrusion Prevention System*). Auditoría de redes inalámbricas. Seguridad en Bluetooth. Autenticación y encriptación. Seguridad a nivel del servicio y nivel del enlace. Emparejamiento. Visibilidad y descubrimiento.

16. SEGURIDAD EN VOZ SOBRE IP Y TELEFONÍA POR INTERNET

Redes telefónicas y redes de datos. Redes de circuitos y redes de paquetes. Congestión y retardo en redes de paquetes. Compresión de la voz y códecs de audio. Introducción a la voz sobre IP (VoIP) y sus características. Integración de voz y datos. Telefonía por Internet. Proveedores de telefonía IP. Número telefónico virtual y DID. Comunicaciones Unificadas (UC). Mensajería Instantánea (IM). Teletrabajo. Central telefónica privada (PBX) e IP-PBX. PBX virtual en la nube (*hosted*). Equipamiento para telefonía IP: PBX, Asterisk y sus derivados, teléfonos IP, softphones. Calidad de servicio (*QoS*) en VoIP. Parámetros de QoS: Retardo (latencia), fluctuación del retardo (jitter), tiempo de respuesta, pérdida de paquetes, disponibilidad, tasa de errores, eco. Algunas opciones para suministrar calidad de servicio (QoS): Differentiated Services (*DiffServ*), IEEE_802.1p/Q y VLAN. Estándares y protocolos para VoIP y aplicaciones multimedia (RTP, RTCP, H.323, SIP, etc.). Dimensionamiento de sistemas de telefonía IP. La inseguridad en VoIP. Ejemplos de amenazas, vulnerabilidades y riesgos en la telefonía IP. Escucha y grabación legal/ilegal de conversaciones. Interceptación de llamadas telefónicas en telefonía fija y móvil. Captura de tráfico de VoIP mediante sniffers. Interceptación y decodificación de tonos de discado DTMF. Otros tipos de ataques: Enumeración, inundación, negación de servicio, desconexión forzada, spam sobre telefonía IP (SPIT), phishing, fuzzing, etc. Medidas de protección: Segmentación VLAN, autenticación por digest MD5, Secure SIP (SIP over TLS). Encriptación con SRTP y ZRTP. Túneles VPN (*Virtual Private Network*). Sistemas de detección de intrusos (IDS).

PRÁCTICAS DE ADIESTRAMIENTO

Las prácticas pueden seleccionarse según los tópicos que más interesan.

1. Configuración y operación de Windows
2. Configuración y operación de Linux
3. Máquinas y redes virtuales
4. Captura y análisis de tráfico en redes

5. Captura y análisis de tráfico en WLAN (Wi-Fi)
6. Captura de teclado y programas espía
7. Servicios básicos de Internet con TELNET, SSH, FTP, TFTP
8. Supervisión de redes y servicios
9. Correo electrónico mediante SMTP, POP3 y MIME
10. Navegación en Internet con HTTP y autenticación de usuarios
11. Servidores proxy y navegación anónima
12. Comunicaciones seguras con Red Privada Virtual (VPN)
13. Gestión de contraseñas
14. Ataques a las contraseñas de Windows
15. Ataques a las contraseñas de servicios en línea
16. Inseguridad en aplicaciones Web: Cross-Site Scripting (XSS)
17. Inseguridad en aplicaciones Web: SQL Injection (SQLi)
18. Ataques de falsificación de paquetes ARP mediante Cain
19. Ataques de falsificación de paquetes ARP mediante Ettercap
20. Auditoria de seguridad mediante Nmap y LanGuard
21. Auditoria de seguridad mediante Nmap y Nessus
22. Auditoría de aplicaciones Web mediante Nessus
23. Auditoría de aplicaciones Web mediante Acunetix
24. Auditoría de aplicaciones Web mediante W3AF
25. Pruebas de penetración de sistemas informáticos
26. Pruebas de penetración avanzadas de sistemas informáticos
27. Pruebas de penetración con troyanos y ofuscación de código
28. Ataques de ingeniería social mediante SET y Kali Linux
29. Introducción a la forénsica digital
30. Forénsica digital y marcas de tiempo
31. Análisis forense mediante el Registro de Windows
32. Investigación de casos de forénsica digital
33. Análisis forense de un servidor web vulnerable
34. Análisis forense de dispositivos móviles
35. Gestión de fallas en redes y sistemas informáticos
36. Respaldo y restauración de datos
37. Recuperación de datos borrados o dañados
38. Protección contra intrusos y software malintencionado
39. Barreras de protección y firewalls
40. Firewalls para aplicaciones Web (WAF)
41. Redes P2P y entornos NAT
42. Criptografía clásica y moderna
43. Criptografía de clave pública
44. Certificados digitales e infraestructura de clave pública PKI
45. Firma digital y sellado de tiempo
46. Navegación segura en Internet con SSL/TLS y HTTPS
47. Correo electrónico seguro
48. Protección de datos en laptops y medios extraíbles
49. Marcas de agua, esteganografía e información oculta
50. Acceso remoto a equipos y sistemas
51. Control de acceso mediante RADIUS
52. Túneles, canales secretos y puertas traseras
53. Red Privada Virtual (VPN) con PPTP
54. Red Privada Virtual (VPN) con SSL y OpenVPN
55. Red Privada Virtual (VPN) con L2TP e IPSec
56. Redes inalámbricas de área local (WLAN)
57. Configuración de puntos de acceso inalámbricos
58. Redes inalámbricas ad-hoc y AP virtual
59. Puntos de acceso falsos en redes Wi-Fi
60. Control de acceso en WLAN mediante filtros MAC
61. Seguridad básica en WLAN mediante WEP
62. Seguridad robusta en WLAN mediante WPA
63. Control de acceso a WLAN mediante RADIUS
64. Bluetooth y redes de área personal (PAN)

65. Comunicaciones avanzadas con Bluetooth
66. Comunicación en línea, compresión del habla y voz sobre IP (VoIP)
67. Telefonía IP mediante SIP (*Session Initiation Protocol*)
68. Comunicaciones Unificadas y PBX virtual
69. Configuración y operación de una PBX básica (Axon)
70. Configuración y operación de una PBX avanzada (Asterisk)
71. Interceptación de llamadas en telefonía y voz sobre IP
72. Interceptación avanzada de llamadas en voz sobre IP
73. Ataques a la autenticación en telefonía IP
74. Protección de la confidencialidad en voz sobre IP
75. Identificación de hablantes y tonos de marcación en telefonía

BIBLIOGRAFÍA BÁSICA

- Charles P. Pfleeger, *Security in Computing*, Prentice Hall, 2015.
- Jie Wang and Zachary A. Kissel: *Introduction to Network Security - Theory and Practice*, John Wiley & Sons, Inc., 2015.
- Seymour Bosworth et al., *Computer Security Handbook*, John Wiley & Sons, Inc., 2014.
- Eric Maiwald, *Network Security - A Beginner's Guide*, McGraw-Hill, 2013.
- Jason Andress, *The Basics of Information Security in Theory and Practice*, Elsevier Inc, 2011.
- Mark Stamp, *Information Security Principles and Practice*, John Wiley & Sons, Inc., 2011.
- James Graham, Richard Howard and Ryan Olson, *Cyber Security Essentials*, CRC Press, 2011.
- Alejandro Corletti Estrada, *Seguridad en Redes*, Madrid, 2016.
- Alejandro Corletti Estrada, *Seguridad por Niveles*, Madrid, 2011.
- Javier Medina, *Evaluación de Vulnerabilidades TIC*, España, 2013.
- Daniel Reis, *Seguridad para la Nube y la Virtualización*, John Wiley & Sons, Inc. 2013.