SEGURIDAD EN VOZ SOBRE IP Y TELEFONÍA POR INTERNET

CURSO TEÓRICO-PRÁCTICO

DIRIGIDO A:
Estudiantes en las áreas de computación, informática, telecomunicaciones y sistemas. Profesionales y técnicos superiores que quieran implantar plataformas de telefonía IP y comunicaciones unificadas. Administradores de redes, centrales telefónicas y call centers. Desarrolladores, programadores, consultores, gerentes de seguridad, auditores de sistemas, pentesters e investigadores forenses. Público en general interesado en las nuevas tecnologías de comunicación.

MODALIDAD: El curso se realiza a distancia, de forma no-presencial, utilizando un DVD como material de apoyo, complementado con reuniones en línea. En ese 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 e Internet. Conocimiento instrumental del idioma inglés.

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

DESCRIPCIÓN DEL CURSO:
La utilización de los protocolos de Internet para voz (VoIP), telefonía y comunicaciones unificadas (UC) es cada vez más popular, ya que permite abaratar los costos en las comunicaciones e integrar las soluciones de voz con aplicaciones corporativas multimedia, por ejemplo videoconferencia. Sin embargo estos sistemas están expuestos a peligrosos ataques que buscan aprovecharse de sus vulnerabilidades para espiar las conversaciones, usar de forma fraudulenta los servicios o impedir su uso. Para poder defenderse, se deben estudiar las diferentes arquitecturas, plataformas y productos, sus debilidades y luego implantar medidas de protección para frustrar los ataques.

El curso incluye clases teóricas donde se explican los temas más relevantes y experiencias prácticas donde se aplican los conocimientos y se completa el adiestramiento. Las prácticas se basan en productos y herramientas disponibles en Internet que los propios participantes instalan y utilizan.

Tomando en cuenta la importancia de conocer la tecnología subyacente a los sistemas de VoIP, la primera parte del curso está dedicada a explicar aspectos tales como: red de paquetes, códec de audio, central telefónica privada (PBX), teléfono IP, etc. Se realizan prácticas sobre comunicación en línea, compresión del habla, captura y análisis de tráfico. Además se describen los estándares y protocolos existentes (RTP, RTCP, H.323, SIP, etc.). Se realizan prácticas sobre telefonía IP mediante SIP (*Session Initiation Protocol*), comunicaciones unificadas y PBX virtual, configuración y operación de una PBX básica y avanzada (Asterisk). Además se trata el tema de la calidad de servicio en VoIP y la problemática de la congestión y el retardo.

En la segunda parte del curso se analizan los fundamentos de la seguridad de la información y el participante aprende cómo se atacan las plataformas de VoIP, explotando las vulnerabilidades y las brechas existentes en el sistema. También aprende cómo mitigar los riesgos, tomando en cuenta los pilares de la seguridad informática (confidencialidad, integridad y disponibilidad). Se hace hincapié en la necesidad de usar mecanismos de encriptación como TLS para proteger la señalización y SRTP para proteger la voz. Se realizan prácticas sobre interceptación de llamadas mediante *sniffers*, ataques de falsificación de paquetes ARP, protección de la confidencialidad en VoIP, identificación de hablantes y tonos de marcación DTMF.

Al completar el curso, el participante poseerá amplios conocimientos y habrá alcanzado una visión integrada de amenazas, vulnerabilidades y riesgos existentes en VoIP, telefonía por Internet y Comunicaciones Unificadas. 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.

OBJETIVO GENERAL:
Conocer las características y funcionalidades de los modernos sistemas de voz sobre IP y telefonía por Internet, con énfasis en los aspectos de seguridad que puedan afectar la confidencialidad, integridad y disponibilidad de las comunicaciones, aprendiendo cómo implantar medidas de protección para defender a los sistemas de ataques internos y externos.

OBJETIVOS ESPECÍFICOS:
- Evaluar los beneficios técnico-económicos de VoIP y telefonía por Internet en lugar de las soluciones tradicionales.
- Visualizar las oportunidades y desafíos que presentan las tecnologías de VoIP y Comunicaciones Unificadas.
- Identificar los componentes y la arquitectura de los sistemas de VoIP.
- Integrar los servicios disponibles en la PBX con las redes de datos corporativas.
- Seleccionar el equipamiento requerido en telefonía IP, tal como PBX, proxy, servidores, teléfonos y softphones.
- Examinar cómo la voz es digitalizada y empaquetada, a fin de utilizar el códec más apropiado.
- Comparar los distintos protocolos y estándares que se utilizan en los sistemas de VoIP.
- Interpretar los mensajes de señalización SIP que se transmiten durante las llamadas.
- Distinguir el contenido de los paquetes UDP y RTP que llevan el tráfico de voz o video.
- Utilizar instrumentos como Wireshark para decodificar y analizar el flujo de las llamadas.
- Instalar, configurar y operar una PBX real (Asterisk) o basada en la nube.
- Especificar los factores que afectan la calidad de la voz, tales como retardo, jitter y congestión.
- Estimar los requisitos de ancho de banda y el dimensionamiento del sistema de acuerdo al tráfico cursado.
- Examinar los fundamentos de la seguridad de la información y los requisitos básicos (confidencialidad, integridad, disponibilidad).
- Identificar amenazas y riesgos inherentes a los sistemas de VoIP.
- Utilizar herramientas y técnicas para la detección de vulnerabilidades y brechas.
- Evaluar la robustez de autenticación utilizada en SIP, probando distintas formas de ataque.
- Realizar pruebas de interceptación de llamadas y de tonos de marcación.
- Realizar ataques de falsificación de paquetes ARP para capturar contraseñas y otras credenciales de autenticación.
- Diagnosticar problemas en los sistemas de VoIP causados por ataques o abusos.
- Identificar mecanismos criptográficos tales como TLS, SRTP y ZRTP para proteger la confidencialidad de las comunicaciones de VoIP.
- Implantar medidas de protección contra amenazas internas y externas.

CONTENIDO PROGRAMÁTICO

Primera parte: Tecnología de Voz sobre IP

Introducción a VoIP y Telefonía por Internet
Clasificación de las redes de comunicación. Redes telefónicas, redes celulares, redes de datos. ¿Qué es la señalización telefónica? Establecimiento y liberación de una llamada. Conmutación de circuitos y conmutación de paquetes. ¿Cómo opera una red de paquetes? Problemas de congestión y retardo y en redes de paquetes. Empaquetamiento de la voz. Compresión de la voz y códecs de audio. Estándares UIT-T para la codificación del audio (G.711, G.723, G.729). Otros códecs (GSM, ILBC, Speex, CELT, Opus). Calidad de la voz comprimida. ¿Qué es VoIP? Redes modernas: Integración de voz y datos. Telefonía por Internet. Número telefónico virtual (Virtual number DID). Comunicaciones Unificadas (UC). Teletrabajo y reuniones virtuales.

Productos y Servicios
Central telefónica privada (PBX) e IP-PBX. PBX virtual en la nube (Hosted PBX). Equipamiento para telefonía IP: Diferentes tipos de PBX. Asterisk y sus derivados. FXO (Foreign Exchange Office) y FXS (Foreing Exchange Station). Teléfonos IP. Dispositivos ATA (Analog Telephone Adapters). Teléfonos en software (softphones).

Calidad de la Voz sobre IP, Estándares y Protocolos

¿Qué es calidad de serv icio (QoS)? 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: 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.

Segunda parte: Seguridad en Voz sobre IP

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). 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.

Inseguridad en VoIP
Ejemplos de amenazas, vulnerabilidades y riesgos en VoIP. 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 en VoIP
Implantación de controles. 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

Comunicación en línea, compresión del habla y voz sobre IP (VoIP)
Objetivo: Familiarizarse con las novedosas soluciones tecnológicas que permiten establecer comunicaciones multimedia y mensajería instantánea sobre redes de paquetes como Internet, así como conocer los distintos sistemas de compresión disponibles para reducir el ancho de banda requerido por el habla.

Telefonía IP mediante SIP (Session Initiation Protocol)
Objetivo: Familiarizarse con estándares y protocolos en que se basa la telefonía IP, la cual proporciona presencia, movilidad y comunicaciones unificadas utilizando SIP (*Session Initiation Protocol*) para señalización y control, junto con SDP (*Session Description Protocol*) y RTP (*Real Time Protocol*) para el el flujo de los datos multimedia.

Comunicaciones Unificadas y PBX virtual
Objetivo: Familiarizarse con las funcionalidades ofrecidas por las Comunicaciones Unificadas, resultado de la convergencia de las redes de voz y datos, y además aprender a configurar y manejar un sistema telefónico privado basado en una PBX virtual.

Configuración y operación de una PBX básica (Axon)
Objetivo: Familiarizarse con las características y funcionalidades de los sistemas telefónicos privados conocidos como PBX, los cuales posibilitan las Comunicaciones Unificadas como resultado de la convergencia de las redes de voz y datos, y además aprender a configurar y operar una PBX avanzada como Axon, instalándola sobre una PC.

Configuración y operación de una PBX avanzada (Asterisk)
Objetivo: Familiarizarse con las características y funcionalidades de los sistemas telefónicos privados conocidos como PBX, los cuales posibilitan las Comunicaciones Unificadas como resultado de la convergencia de las redes de voz y datos, y además aprender a configurar y operar una PBX avanzada como Asterisk, instalándola sobre una máquina virtual.

Interceptación de llamadas en telefonía y voz sobre IP
Objetivo: Familiarizarse con la captura, escucha, edición y grabación de conversaciones de VoIP en llamadas efectuadas mediante teléfonos IP y Skype, a fin de identificar los riesgos a la privacidad de las comunicaciones inherentes a estas nuevas formas de comunicación.

Interceptación avanzada de llamadas en voz sobre IP
Objetivo: Familiarizarse con la captura, escucha y grabación de conversaciones de VoIP usando codecs de alta compresión, así como la captura en ambiente de LAN conmutada utilizando sniffer de paquetes y técnicas especiales.

Ataque a la autenticación en telefonía IP
Objetivo: Familiarizarse con los mecanismos de autenticación de personas en telefonía IP y en particular estudiar la robustez de autenticación basada en resumen utilizada en SIP (*Session Initiation Protocol*), probando distintas formas de ataque.

Ataques de falsificación de paquetes ARP mediante Cain
Objetivo: Familiarizarse con la técnica de *ARP spoofing* utilizada para realizar ataques de hombre en el medio (MITM) en redes de área local (LAN) mediante la herramienta Cain, capturando así contraseñas y otras credenciales de autenticación utilizadas en numerosos protocolos.

Ataques de falsificación de paquetes ARP mediante Ettercap
Objetivo: Familiarizarse con la técnica de *ARP spoofing* utilizada para realizar ataques de hombre en el medio (MITM) en redes de área local cableadas (LAN) o inalámbricas (WLAN) mediante la herramienta Ettercap, capturando así contraseñas y otras credenciales de autenticación utilizadas en numerosos protocolos.

Protección de la confidencialidad en voz sobre IP
Objetivo: Familiarizarse con las medidas de seguridad que se pueden implantar en VoIP y en particular el uso de SIPS, SRTP y ZRTP para proteger la confidencialidad en la comunicaciones basadas en SIP.

Identificación de hablantes y tonos de marcación en telefonía
Objetivo: Familiarizarse con el análisis de espectro de frecuencias para identificar la persona que habla en grabaciones de voz, así como decodificar los símbolos marcados mediante el teclado de tonos de marcación multifrecuencial (DTMF) utilizado en telefonía.