Auditoría de Sistemas de VoIP

MADRID

8 de Marzo de 2023

DOSIER DE FORMACIÓN

/Rooted

Días 6-8 de Marzo
Tres días de trainings y workshops

HOTEL Eurostars iHotel
Pozuelo de Alarcón

Días 9-11 de Marzo
Ponencias presentadas por speakers internacionales y expertos técnicos.

KINEPOLIS
Pozuelo de Alarcón

Presentación

- **Misión**: queremos compartir conocimientos, atraer diferentes culturas, exponer el talento local y marcar la diferencia.
- **Visión**: ser responsables haciendo algo diferente, compartiendo cultura y construyendo una red de conocimiento. Ser un evento honesto, confiable, beneficioso

Profesor: José Luis Verdeguer

- Ingeniero Técnico de Sistemas Informáticos por la Universidad de Alicante
- Máster Oficial de Desarrollo y Programación de Servicios Web por la Universidad de Alicante
- Autor del módulo de seguridad Secfilter de Kamailio
- Autor del software de pentesting sobre sistemas de VoIP: SIPPTS
- Más de 10 años como ponente en diferentes congresos de VoIP y seguridad informática
- Más de 25 años en el mundo de la seguridad informática
- 12 años como administrador y desarrollador de sistemas de VoIP
- CTO en Zoon Suite

Objetivos

Hoy en día casi todas las empresas disponen de soluciones de VoIP que están interconectadas con aplicaciones de gestión, como CRMs o ERPs, y es un vector de ataque que normalmente no se tiene muy en cuenta a la hora de auditar un sistema informático.

El objetivo de este taller es estudiar las diferentes técnicas para realizar un test de penetración sobre un sistema de VoIP, realizando ataques tanto sobre la señalización (protocolo SIP), como el media (protocolo RTP) y los diferentes dispositivos.

Se dará un breve repaso acerca del funcionamiento de un sistema de VoIP y de los protocolos involucrados, y se analizarán diferentes técnicas que pueden permitir a un atacante robar credenciales de usuario, realizar escuchas o atacar cifrados.

A quién va dirigido

- Auditores de seguridad
- Administradores de sistemas
- Administradores de VoIP

Requisitos: Conocimientos

Conocimientos básicos de:

✓ No se requiere ningún conocimiento especial

Requisitos: Técnicos

Para el correcto funcionamiento del training será necesario que los alumnos dispongan de equipos con acceso de administrador para poder añadir, eliminar software o cambiar cualquier configuración del mismo.

Las máquinas deben contar con las siguientes características mínimas:

- ✓ Kali Linux (no es imprescindible)
- ✓ Conexión Wifi para conectar con la red del taller
- ✓ Tener instalado (por ahorrar tiempo) SIPPTS (https://github.com/Pepelux/sippts)

Agenda (i)

- Ataque contra servicios de VoIP (Proxy, PBX, …)
  - Escaneo, reconocimiento y fingerprinting
  - Análisis de vulnerabilidades conocidas
  - Enumeración de extensiones
  - Cracking de contraseñas
  - Generación de llamadas sin autenticación (INVITE Attack)
  - Suplantación de identidad en llamadas (CallerID Spoofing)
  - Pruebas de proxy SIP abierto
  - Verificación de cifrados en señalización
  - Simulación de denegación de servicio (DoS)
    - Flood con mensajes bien formados (INVITE, BYE, UPDATE, etc)
    - Flood con mensajes mal formados (Fuzzing de cabeceras)

Agenda (ii)

- Ataque en redes locales
  - Envenenamiento ARP
  - Monitorización de tráfico SIP y RTP
  - Crackeo offline de contraseñas
  - Secuestro de sesiones (Session Hijacking)
  - Denegación de servicio
    - Colgado de llamadas (BYE Teardown)
    - Cancelación de peticiones (CANCEL)
    - Redirección de llamadas (Re-INVITE)
    - Modificación de sesiones activas (UPDATE)
    - Desconexión de usuarios (REGISTER Expire=0)
  - Ataques contra cifrados
    - Ataques contra TLS

Agenda (iii)

- Ataque contra el media
  - Simulación de denegación de servicio (DoS)
    - Flood de paquetes RTP
    - Ataque RTP Bleed
  - Inyección de tráfico RTP
  - Eavesdropping
  - Ataques contra cifrados
    - Ataques contra SRTP
- Ataque contra dispositivos
  - Escaneo, reconocimiento y fingerprinting
  - Análisis de vulnerabilidades conocidas
  - Auto-aprovisionamiento
  - Ataque SIP Digest Leak
  - Crackeo offline de contraseñas

Costes

- El precio final de este **RootedLAB** es **250 €**

- **Puedes registrarte y formalizar el pago en: https://reg.rootedcon.com**

IMPORTANTE:

Se requiere un mínimo de **SEIS (6)** asistentes para que el curso pueda celebrarse.

/Rooted

FAQ

- Dónde se celebra la formación?
  - A diferencia del Congreso RootedCON, las formaciones se celebran en el Hotel Eurostarts i-Hotel
  - Aquí puedes encontrar el mapa de la zona: Google Maps
- Qué diferencia hay entre BootCamp y RootedLab?
  - Diferenciamos los training por horas de formación. Un RootedLab tiene 8 horas de formación, mientras que un BootCamp tiene unas 24h.
- Qué horario tiene la formación?
  - La formación comienza a las 9 de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8 :)
  - Las formaciones suelen acabar entre las 19h y 20h.
- Como puedo registrarme?
  - Para el registro, ve directamente al RootedManager: https://reg.rootedcon.com. Ahí, una vez registrado podrás seleccionar la formación y pagar directamente. Una vez se imparta la formación podrás solicitar la factura siguiendo los pasos indicados.
- Puedo pagar con transferencia bancaria?
  - Si, desde el propio RootedManager podrás gestionar el pago mediante transferencia bancaria.
- El training incluye comida?
  - Los training no incluyen comida. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto:

info@rootedcon.com