Título: Técnicas de ataque sobre clientes Wi-Fi

Fecha: Jueves, 30 de octubre – 9:30 a 20:00h

Formador: Raúl Siles

Raúl Siles es fundador y analista de seguridad de DinoSec. Durante más de una década ha aplicado su experiencia en la realización de servicios técnicos avanzados de seguridad e innovado soluciones ofensivas y defensivas para organizaciones internacionales de diferentes industrias. Raúl es ponente habitual en conferencias y eventos de seguridad internacionales e instructor certificado del SANS Institute. Raúl es uno de los pocos profesionales a nivel mundial que ha obtenido la certificación GIAC Security Expert (GSE). Más información en http://www.raulsiles.com (@raulsiles) y http://www.dinosec.com (@dinosec).

Descripción y objetivos:
Las tecnologías de comunicación inalámbricas, y en particular Wi-Fi, son usadas diariamente por millones de personas para transmitir información cada vez más sensible. Durante la última década, el principal objetivo de los ataques Wi-Fi ha evolucionado de las infraestructuras Wi-Fi hacia los clientes Wi-Fi y los dispositivos móviles.

El curso “Técnicas de ataque sobre clientes Wi-Fi” es una formación/workshop eminentemente técnica y práctica. El objetivo principal del curso es conocer en detalle las debilidades actuales de los clientes Wi-Fi y profundizar en las últimas amenazas y técnicas ofensivas, incluyendo recomendaciones de protección y defensa.

Durante el curso se realizan múltiples demostraciones prácticas por parte del instructor, pero el curso ha sido diseñado para que los asistentes puedan poner en práctica todas y cada una de las técnicas descritas de manera individualizada. Se proporciona la teoría y conceptos básicos necesarios para profundizar posteriormente en técnicas de ataque más avanzadas y en los aspectos más prácticos, mediante la utilización de múltiples herramientas ofensivas.

A lo largo de los diferentes módulos del curso los asistentes tienen la oportunidad de practicar con ataques y explotar vulnerabilidades reales que afectan a los clientes Wi-Fi hoy en día. Adicionalmente se proporcionarán

técnicas y trucos avanzados para la realización de auditorías de seguridad sobre clientes Wi-Fi basados en investigación propia.

Al finalizar el curso, los asistentes dispondrán de un entorno ofensivo (conocimientos, software y hardware) completamente operativo para evaluar la seguridad Wi-Fi de su compañía o de sus clientes, y que les permitirá tanto la realización de auditorías de seguridad y pruebas de intrusión (pen-tests) avanzadas sobre clientes Wi-Fi, como realizar tareas de investigación y descubrimiento de nuevas vulnerabilidades Wi-Fi.

El precio del curso incluye para cada asistente una tarjeta Wi-Fi USB minuciosamente seleccionada como la mejor tarjeta disponible actualmente para la auditoría de redes y clientes Wi-Fi con capacidades 802.11 a/b/g/n (300 Mbps), multi-frecuencia (2.4 & 5Ghz), conector de antena externo (RP-SMA), modo cliente, monitor, AP, inyección, etc.

Contenidos: (*actualizados respecto al RootedLab 2014 de marzo*)

1. **Tecnologías 802.11 (Wi-Fi)**
    1. Tecnologías 802.11a/b/g/n/ac
    2. Canales Wi-Fi, RF, ancho de banda y dominios de regulación
    3. Tramas Wi-Fi
    4. Estado actual de la seguridad de las tecnologías Wi-Fi
    5. Hardware Wi-Fi
2. **Reconocimiento e identificación de clientes Wi-Fi**
    1. Comportamiento de los clientes Wi-Fi
    2. Lista de redes preferidas (PNL, Preferred Network List)
    3. Redes Wi-Fi ocultas
    4. Deficiencias y anomalías de los clientes Wi-Fi
    5. Gestión de la PNL
    6. Vulnerabilidades de los clientes Wi-Fi
        a) Dispositivos móviles
    7. Ataques dirigidos y ataques masivos
    8. Identificación de objetivos: MAC y PNL fingerprinting

9. Ataques contra la privacidad y geolocalización
10. Análisis de la ubicación y señal para la realización de los ataques

3. **Suplantación de la red Wi-Fi legítima: requisitos**
    1. Redes abiertas
    2. Redes WEP
    3. Redes WPA/WPA2-Personal (PSK)
    4. Redes WPA/WPA2- Empresarial basadas en 802.1x/EAP
    5. Suplantación completa de la infraestructura
        a) Punto de acceso (AP), servidores DHCP, DNS, RADIUS, enrutamiento, NAT, etc.
4. **Ataques sobre los clientes Wi-Fi**
    1. Ataques karma
    2. Redes abiertas
    3. Redes WEP
        a) Caffe Latte
        b) Hirte
    4. Redes WPA/WPA2-Personal (PSK)
        a) 2-way / 4-way WPA/WPA2-PSK handshake
    5. Redes WPA/WPA2- Empresarial basadas en 802.1x/EAP
        a) Ataques sobre PEAP/TTLS (MSChapv2)
        b) Ataques EAP Dumb-Down
        c) Diferentes escenarios de ataque
    6. Ataques posteriores sobre TCP/IP
        a) MitM (Man-in-the-Middle)
        b) Proxies de interceptación

7. Otros ataques sobre clientes Wi-Fi
    a) Ataques de denegación de servicio (DoS)
    b) Ataques web vía el SSID
        - Dispositivos embebidos
8. Creación de herramientas de ataque propias (ej. Python)

5. **Mecanismos de protección, estrategias y recomendaciones defensivas en los clientes Wi-Fi**
    1. Estado del interfaz Wi-Fi
    2. Gestión de la PNL
    3. Gestión de redes Wi-Fi ocultas
    4. Gestión de redes abiertas, WEP, y WPA/WPA2-Personal
    5. Gestión de redes WPA/WPA2-Empresarial
        a) Gestión de certificados, validación del servidor RADIUS, EAP-TLS, etc
    6. Gestión de dispositivos móviles (MDM)
    7. WIDS
    8. Posibles modificaciones en la especificación 802.11
6. **Referencias**

Herramientas: Para crear el entorno ofensivo avanzado de investigación y ataques sobre clientes Wi-Fi se emplearán múltiples herramientas incluidas en Kali Linux, y de elaboración propia, como por ejemplo wireshark, tshark, aircrack-ng suite (varias herramientas), kismet, iStupid, python & scapy, iptables, dnsmask, hostapd, FreeRadius, FreeRadius-WPE, asleap, john the ripper, etc.

Duración: 8 horas

Público objetivo:
Profesionales de seguridad informática, auditores, pen-testers, analistas, consultores e investigadores de seguridad, administradores de redes y sistemas, administradores de entornos y dispositivos móviles, administradores de otros equipos cliente y de usuario.

Conocimientos previos: Conocimientos básicos de Linux (y en particular, Kali Linux). Conocimientos básicos de redes Wi-Fi y redes TCP/IP.

Requisitos tecnológicos: Ordenador portátil (Windows, Linux, Mac OS X, etc) con VMware (Player, Workstation, Fusion) y al menos un puerto USB libre.
Máquina virtual basada en Kali Linux (* - descargarla previamente).
Opcionalmente:

- Dispositivos móviles que actúen como clientes Wi-Fi víctimas.
- Otros dispositivos cliente con capacidades Wi-Fi.

Conexión a Internet en el aula de formación.

(*) Dirección web para la descarga previa de la imagen VMware de Kali Linux versión 1.0.6: http://images.offensive-security.com/kali-linux-1.0.6-vm-i486.7z.

Entre otros ataques Wi-Fi, se analizarán y profundizará en las diferentes técnicas mostradas en la presentación “Wi-Fi: Why iOS (Android & others) Fail inexplicably” de Raúl Siles en la RootedCON 2013 (presentación en PDF, y video). Se recomienda leer/ver su contenido, así como familiarizarse con el entorno Kali Linux.

El precio del curso incluye para cada asistente una tarjeta Wi-Fi USB minuciosamente seleccionada como la mejor tarjeta disponible actualmente para la auditoría de redes y clientes Wi-Fi con capacidades 802.11 a/b/g/n (300 Mbps), multi-frecuencia (2.4 & 5Ghz), conector de antena externo (RP-SMA), modo cliente, monitor, AP, inyección, etc.

Cualquier pregunta dirigirse directamente en el formulario de contacto de la web.
sección: FORMACIONES

Precio: 290€ (impuestos incluidos). Incluye desayuno y bufet libre.

La inscripción y pago de todas las formaciones incluyen la entrada gratuita al Congreso No cON Name edición 2014. Todas las formaciones tienen un mínimo de 10 alumnos. En caso de no realizarse se devolvería el importe integro.

Para efectuar el pago los solicitantes deben hacer su inscripción a través de la web: http://www.noconname.org/inscripcion/