sepian

Seguridad Digital
de Andalucía

Ficha técnica

Gestión de amenazas en suplantación de identidades y prevención de ataques físicos

JUNTA DE ANDALUCIA
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

ÍNDICE

1. Datos generales

Título:

Gestión de amenazas en suplantación de identidades y prevención de ataques físicos.

Modalidad:
Curso presencial Junio.

Fecha:
19 y 20 de junio.

Lugar de celebración:
Instalaciones SANDETEL, Pabellón de Francia-PCT Cartuja.

Duración:
10 horas.

Horario:
9:00 a 14:00.

Dirigido a:
Responsables de seguridad TIC de la Junta de Andalucía, profesionales TIC de la Junta de Andalucía y entidades vinculadas.

2. Ponentes

Pedro Candel aka “s4ur0n”

Docente en IMF, ha sido docente en Deloitte CyberSOC Academy, profesor colaborador en el Máster en Ciberseguridad (MCS) de la Universidad de La Salle, Universidad Camilo José Cela, Universidad Católica de Ávila (España), etc. y mediante la red Ilumno en las principales Universidades de los países de América Latina.
Especializado en Seguridad Ofensiva, Reversing, Malware, Desarrollo Seguro y Forense. Ponente habitual en congresos, conferencias, eventos y otras instituciones nacionales e internacionales en materia de ciberseguridad. Anteriormente, docente en las formaciones de Seguridad, Redes y Sistemas, Desarrollo del Servicio de Formación y Empleo de la Junta de Comunidades de Castilla-La Mancha.

María Monfort “C4T”

María M. aka “C4T_13” es especialista en Hardware Hacking, OSINT y Pentesting. Ha colaborado en la creación de diferentes herramientas y distribuciones bajo GNU/Linux especializadas para Pentesting de Redes Inalámbricas y diversos foros WiFi. Ha colaborado con FFCCSE y participado en numerosos Congresos de Seguridad Informática tanto nacionales como internacionales. Ha realizado auditorías en Infraestructuras Críticas del Estado y

colaborado con diferentes CERTs a nivel nacional en materia de Ciberseguridad asesorando a altos cargos sobre las diferentes amenazas a los que se encuentran expuestos..

3. Calendario y lugar de celebración

Días **19 y 20 de junio** de 2018 de 9:00h a 14:00h.

Instalaciones SANDETEL, Pabellón de Francia-PCT Cartuja.

4. Objetivos

-Conocer las amenazas físicas y de suplantación de identidad con los diferentes métodos existentes.

- Gestionar mediante los protocolos y canales adecuados las amenazas de suplantación de identidades y ataques físicos.

- Concienciar y formar al personal de las Administraciones de la necesidad de inspeccionar el lugar de trabajo en búsqueda de dispositivos anómalos y reconocer diferentes formas de suplantación de identidades.

5. Contenido

Módulo 1: SEGURIDAD "VISUAL" EN EL PUESTO DE TRABAJO

1.1- Ingeniería Social

1.1.1.- Introducción a la Ingeniería Social

1.1.2.- Hacking con Buscadores (OSINT) (Tinfoleak) (Busqueda linkedin, B.O.J.A y B.O.E, etc...)

1.1.3.- Suplantación de Identidad

1.1.4.- Robo de Contraseñas

1.1.5.- Phishing

1.1.6.- Spear Phishing

1.2.- Hardware Hacking

1.2.1.- Keyloggers

1.2.2.- Rubber Ducky

1.2.3.- Lan Turtle

1.2.4.- Comunicaciones inalámbricas

1.2.5.- SDR (HackRF, BladeRF, etc.)

1.2.6.- Seguridad perimetral (CAMARAS Y BARRERAS)

1.2.7.- Lockpicking

Módulo 2: SUPLANTANCIÓN DE IDENTIDADES

2.1.- Acceso físico al sistema

2.1.1.- Cookies
2.1.2.- Historial de navegación
2.1.3.- Recordar contraseña
2.1.4.- Almacenes de contraseñas
2.1.5.- Hashes
2.1.6.- Técnicas Pth (Pass the Hash)
2.1.7.- Mimikatz

2.2.- Man in the Middle

2.2.1.- Interceptación de credenciales de acceso
2.2.2.- Interceptación de credenciales de acceso con cifrado TLS/SSL
2.2.3.- Otras técnicas

2.3.- Man in the Browser

2.3.1.- BeEF

2.4.- Ataques remotos

2.4.1.- Credenciales
2.4.2.- Falsificación
2.4.3.- Intercepción
2.4.4.- Explotación

2.4.5.- Ingeniería Social
2.4.6.- Mercados negros

2.5.- Protocolo de actuación ante un ataque físico
2.5.1.- Buenas prácticas
2.5.2.- Herramientas y/o contramedidas
2.5.3.- Contacto con CERTS
2.5.4.- Contacto con FFCCSE
2.5.5.- Otros contactos

6. Material necesario

No es necesario que el participante disponga de ningún tipo de equipo para poder atender a las dos sesiones, pero si sería recomendable debido al carácter práctico de las sesiones donde podrán poner en marcha diferentes técnicas empleadas por ciberdelincuentes para realizar una suplantación de identidades y diferentes tipos de ataques físicos contra la Organización.

En este caso, el participante deberá llevar instalada una distribución Kali Linux 2018-2 (http://cdimage.kali.org/kali-2018.2/kali-linux-2018.2-amd64.iso) debidamente instalada en su

equipo con la red en modo NAT. Deberá de contar al menos con 2 GB libres de RAM para su ejecución y 1-2 núcleos de procesador y al menos 20 GB de espacio libre en el disco.