CONSULTORIA ASESORIA Y CAPACITCION EN SEGURIDAD INFORMATICA Y COMPUTO FORENSE

Descripción jerárquica del temario correspondiente al curso “Android Hacking”

El curso está compuesto por 11 sesiones en las cuales se abordan los siguientes temas:

- ✓ Inducción a Android Hacking
- ✓ Teoría de ataques Android
- ✓ Extracción de información y códigos QR
- ✓ Comprometiendo Android con MSFVenom y Metasploit
- ✓ Modificación de APK’S
- ✓ Identificación de directorios y aplicaciones en el dispositivo comprometido
- ✓ Descarga de archivos desde el dispositivo comprometido
- ✓ Decrepitado de base de datos de WhatsApp (crypt 12)
- ✓ Interacción con el hardware del dispositivo comprometido
- ✓ Configuración de ataques hacia afuera de la red local (tunelizando protocolos
- ✓ Acceso grafico a un dispositivo Android

Cada sesión contiene clases de forma teórica y practica en video, las cuales proveen al participante de los conocimientos necesarios para realizar la intervención de un dispositivo móvil o una tableta electrónica con sistema operativo Android.

Descripción jerárquica del temario correspondiente al curso “Informática Forense”

El curso está compuesto por 14 sesiones en las cuales se abordan los siguientes temas:

- ✓ Inducción al cómputo forense
- ✓ Toma de evidencia volátil
- ✓ Toma de evidencia no volátil (unidades de almacenamiento)
- ✓ Toma de evidencia no volátil (historiales y portapapeles)
- ✓ Toma de evidencia no volátil (variables, tareas programadas y enlaces)
- ✓ Toma de evidencia no volátil (historiales y estructura de carpetas)
- ✓ Toma de evidencia no volátil (captura de usuarios y passwords)
- ✓ Toma de evidencia no volátil (modificación de extensiones)
- ✓ Toma de evidencia no volátil (extracción de contraseñas a nivel hexadecimal)
- ✓ Análisis de malware dinámico
- ✓ Análisis forense de dispositivos móviles
- ✓ Análisis de metadatos
- ✓ Análisis forense a sistemas Linux
- ✓ Conversión de imágenes forenses

Cada sesión contiene clases de forma teórica y práctica en video, las cuales proveen al participante de los conocimientos necesarios para realizar procedimientos de análisis digital forense.

CONSULTORIA ASESORIA Y CAPACITCION EN SEGURIDAD INFORMATICA Y COMPUTO FORENSE

Descripción jerárquica del temario correspondiente al curso “Data Recovery”

El curso está compuesto por 16 sesiones en las cuales se abordan los siguientes temas:

- ✓ Bienvenida al curso
- ✓ Funcionamiento de un disco duro
- ✓ Errores al intentar recuperar datos
- ✓ Daños lógicos
- ✓ Revisión de discos duros
- ✓ Pasos para la recuperación de datos
- ✓ Comprobación de discos duros
- ✓ Hardware de recuperación de datos
- ✓ Software de recuperación de datos que NO debe utilizarse
- ✓ Recuva vs Diskdigger
- ✓ Recuperación de datos desde una imagen forense
- ✓ Utilización de herramientas comerciales para recuperación de datos
- ✓ Validación de firmas a nivel hexadecimal (file signatures)
- ✓ Recuperación de datos a nivel hexadecimal
- ✓ Recuperación de datos en entorno Linux
- ✓ Recuperación de particiones
- ✓

Cada sesión contiene clases de forma teórica y práctica en video, las cuales proveen al participante de los conocimientos necesarios para realizar procedimientos de recuperación de datos en unidades de almacenamiento dañas a nivel lógico o unidades que han sido formateadas.

A T E N T A M E N T E

Rodrigo E. Palou Zubiaur

Director General Data Security