WHITEHAT ACADEMY

Extracción de Información en Redes

Este curso es una revisión de las técnicas más importantes para extraer información de las redes de datos. Con el dominio de estos laboratorios, se ejercitará el ataque a redes complejas, intercepción de correos, secuestros de sesión e implementación de ataques de fuerza bruta a dispositivos y servicios con alto valor de explotación.

Módulo 1. Conceptos y comandos basicos de redes CISCO
- Conceptos de redes
- Sniffers
- Configuracion IPs y puertos
- Port mirror: captura y sniffeo de información de la red
- Explotación de SNMP, secuestro de sesiones, etc.

Módulo 2. Ataques de Capa 2
- Tecnicas de sniffeo de hubs
- Tecnicas de sniffeo de un switch
- CAM Table attack
- ARP spoofing
- Ataques de MITM: ataque a SSL
- Tecnicas de sniffeo VoIP
  - Laboratorios de ETTERCAP
  - Laboratorios de CAIN
- Laboratorios de YERSINIA: Otros ataques

Módulo 3. Ataques a redes BlueTooth
- Uso de BlueAuditor
- Uso de BlueHack
- Laboratorios de hackeo a celulares

Módulo 4. Ataques de fuerza Bruta a dispositivos
- Laboratorios de fuerza bruta a routers
- Laboratorios de fuerza bruta
  - TELNET
  - SNMP
  - SSH
  - HTTP

Material requerido:

- Lap top Windows XP+, al menos 1G en RAM, DD 8G
- Conceptos de Networking y protocolos
- Conocimientos básicos de LINUX

Extracción de Información en Redes está dirigido al personal de áreas como Sistemas, Telecomunicaciones, Redes, personal de Soporte Técnico, administradores de la seguridad, así como a Consultores de Seguridad.

Como parte del Curso, te entregaremos una Carpeta conteniendo toda la información analizada, así como un Certificado Oficial de Asistencia. No solamente te llevarás las herramientas utilizadas, sino toda una máquina virtual del Framework de ataque.

Informes: (55) 5681 5921 **capacitacion@whitehatconsultores.com**