ETHICAL HACKING: Seguridad inalámbrica y móviles

Objetivos generales

Formar al alumno para que conozca medios de engaño existentes a través de la telefonía celular moderna y las computadoras. Prepararse para utilizar el celular como una herramienta más. Para esto obtendrá fuertes conocimientos modernos sobre telefonía, así como nociones de redes, programación, virus y troyanos (que más adelante puede elegir reforzar con otros cursos).

Conocimientos previos necesarios

Buen manejo de PC.

Destinatarios

Público en general sin conocimientos previos.

Temario

1. **Auditoría Inalámbrica.**

   Conocer las diferentes maneras de vulnerar una clave Wifi, con el objetivo de brindar para protección adecuada.

   Creación de pen drives booteables para pentesting

   Sumario de ataques inalámbricos de penetración y su efectividad

   Ataques wifi de evil twin

   Ataques wifi por diccionario (handshaker / brutus)

   Ataques wifi WPS (reaver)

   Ataques wifi WEP

   Expulsión de dispositivos conectados a un WIFI mediante paquetes de deauth

2. **Monitoreo Inalámbrico.**

   Aprender a recabar información detallada de las redes wifi cercanas, así como accesorios de la gente conectada a ellas. Aprender a montar un operativo de vigilancia personal.

   Airodump. Captura manual de handshakes / paquetes de datos probes.

   Scripts.

   Kismet

   Localización geográfica de redes wifi

   Fing

Mylanviewer

3. **Vigilancia en Windows.**

Aprender tanto a realizar como eludir diferentes métodos de espionaje en Windows (contraseñas, teléfonos conectados, programas de espionaje).

Keyloggers y antikeyloggers.

Modo de depuración USB / robo de datos de celulares via ADB.

Arranque de Windows / troyanos.

4. **RaspBerry Pi.**

Aplicar técnicas de hacking inalámbrico desde pequeños dispositivos portátiles usados para espionaje / interferencia / seguridad.