

Auditoría Wireless



Martínez Avila Israel
Hernandez Cantador Jorge Luis



¿Qué necesitas?

- **Tener una red inalámbrica en casa o en el trabajo.**
- **Una laptop o PC con tarjeta inalámbrica.**
- **S.O Linux.**
- **Software: Aircrack-ng, Macchanger, Ettercap y Meta Exploit.**

Distribuciones Linux



- BackTrack.
- Wifislax.
- Ubuntu

Primer paso



- Instalar software
 - Aircrack-ng
 - # apt-get install aircrack-ng
 - Ettercap
 - # apt-get install ettercap
 - Macchanger
 - # apt-get install macchanger
 - Meta exploit
 - Instalar desde fuentes.

Paso dos



- Configurar modo monitor.
 - # ifconfig wlan0 down
 - # iwconfig wlan0 mode monitor
 - # ifconfig wlan0 up

Paso dos (opcional)



- Configurar mac (mac falsa)
 - # macchanger -m 00:11:22:33:44:55 wlan0

Paso tres



- Airodump-ng, se usa para capturar paquetes wireless 802.11 y es útil para ir acumulando IV's
 - `# airodump-ng -w nombre_del_archivo -c # wlan0`

Paso cuatro



- Aireplay-ng, su función principal es generar tráfico para acumular IV's.
 - Ataque 0: Deautenticación
 - Ataque 1: Falsa autenticación
 - Ataque 2: Selección interactiva del paquete a enviar
 - Ataque 3: Reinyección de una petición ARP (ARP-request)

Paso cuatro



- Ataque 4: Ataque chopchop
- Ataque 5: Ataque de Fragmentación

Ejemplo:

- `# aireplay-ng -3 -b ##### -h ##### wlan0`

Paso cinco



- Aircrack-ng, es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK
 - `# aircrack-ng nombre_archivo.cap`