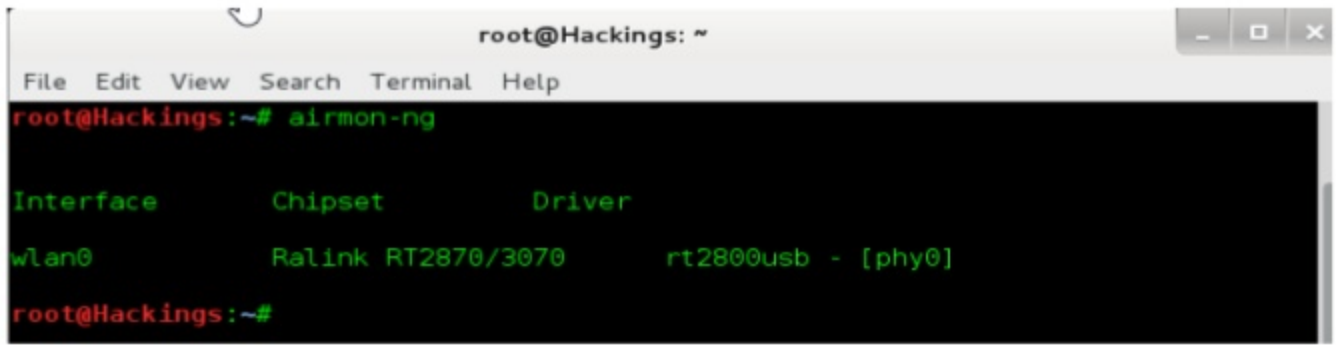
Certified Penetration Testing Engineer (CPTE) Eğitimi

KABLOSUZ AG SALDIRILARI

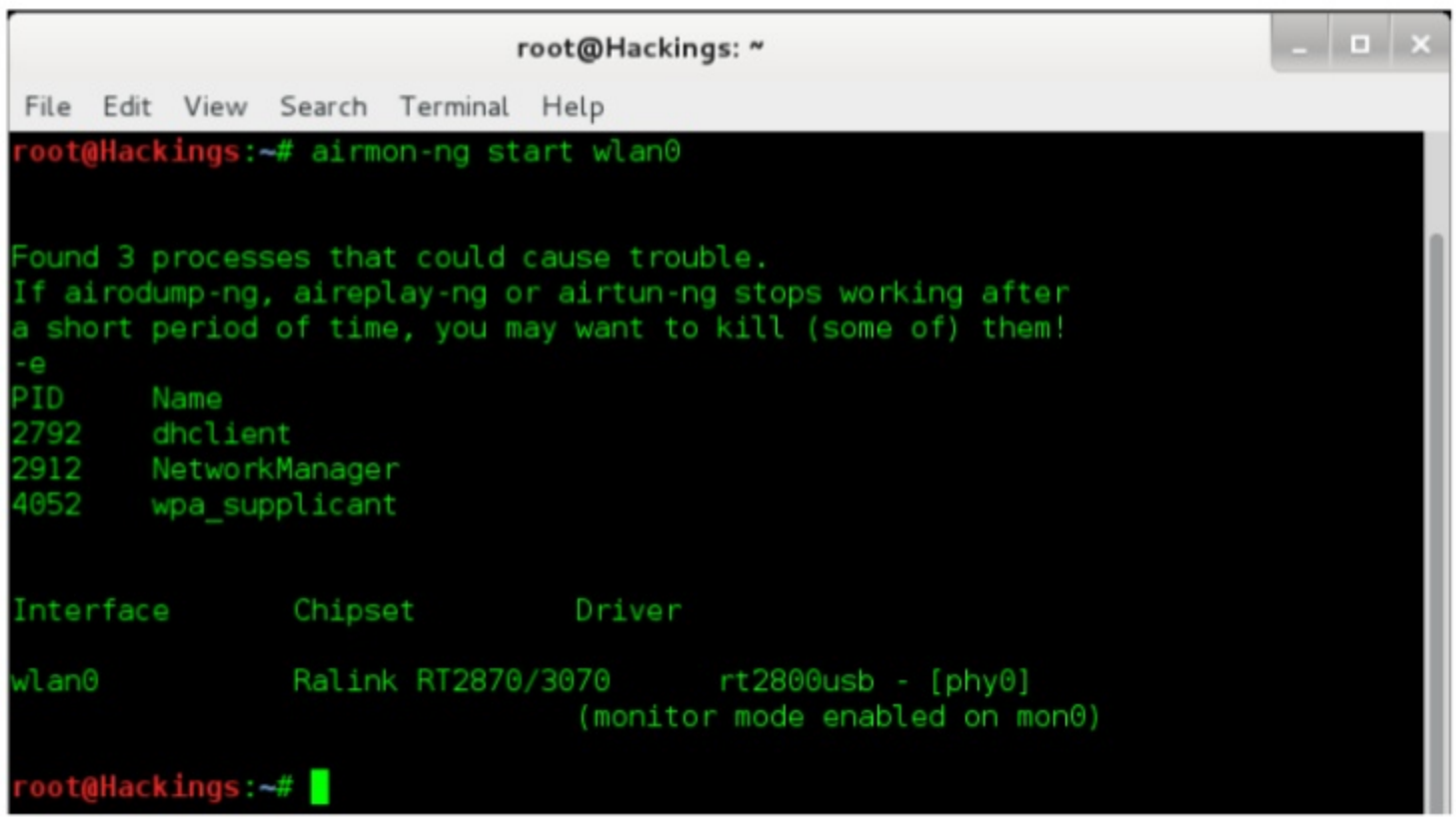
-WPA / WPA2 ŞIFRELI AĞLARA SALDIRI

WPA/WPA2 şifreli ağlar wep şifreli ağlara göre daha güvenlidir, nedeni ise brute force ve wordlist yöntemine dayanmasıdır, kullanılması önerilen şifreleme türü WPA2-PSK'dır.

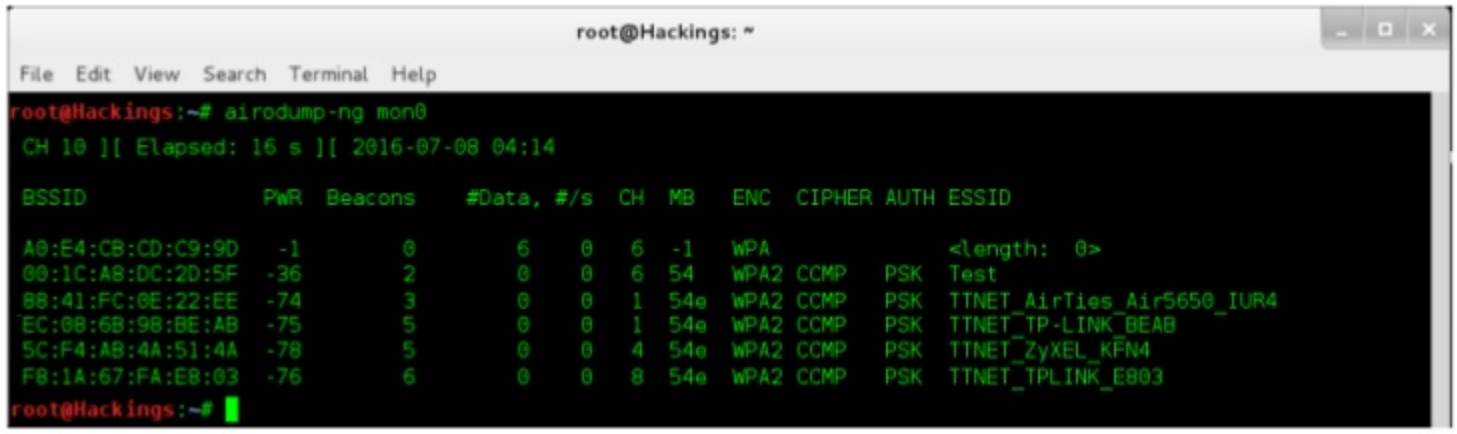
Öncelik olarak <airmon-ng> komutu ile kablosuz Ağ interfacesi öğrenilir.



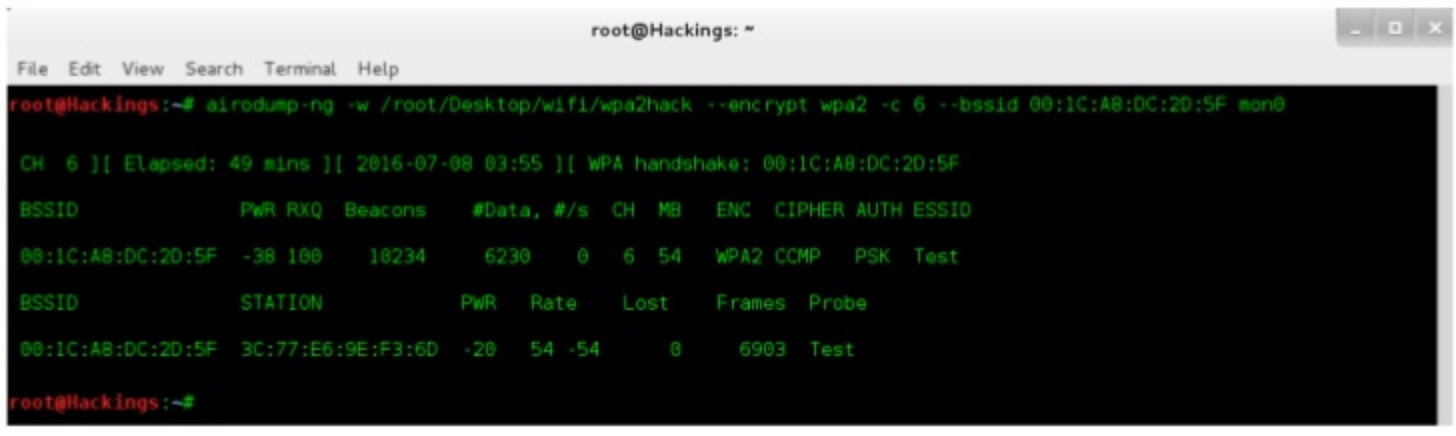
<airmon-ng start wlano> komutu ile kablosuz Ağ kartı aktif edilir.



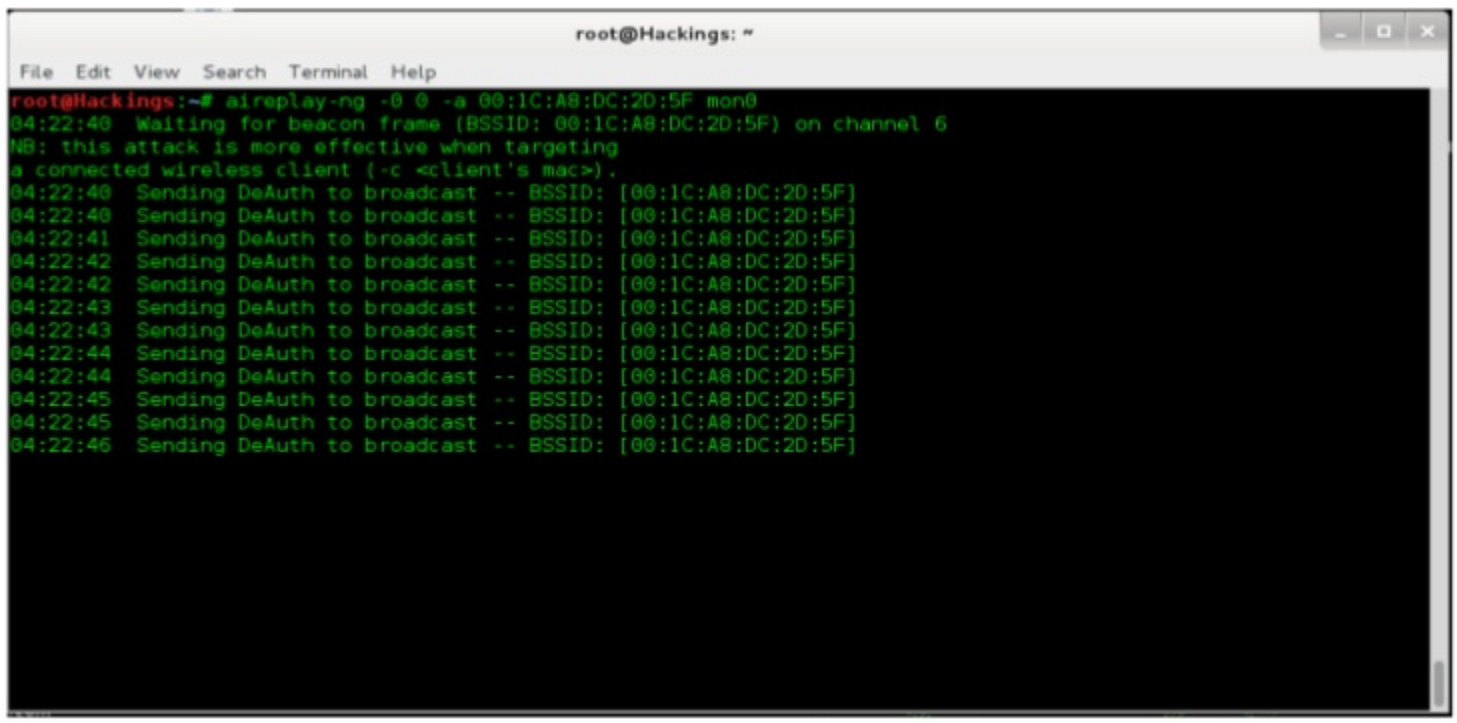
<airodump-ng mono> komutu ile çevredeki kablosuz ağlar hakkında gerekli bilgilerin alınması için tarama işlemi başlatılır.



Görüldüğü gibi çevredeki bazı kablosuz ağlar ve hakkındaki bilgiler çıktı, BSSID, CH, ENC, ESSID. Şimdi handshake toplama işlemi başlatılması gerekir. Bunun için öncelik olarak, hedef router'ın mac adresi olan "BSSID" numarası alınır, ardından ise "CH" yani kanal numarası alınır. "**airodump-ng –w /root/Desktop/isim.cap <.cap dosyasının kayıt edileceği path> --encrypter <şifreleme algoritması> -c <kanal numarası> --bssid <hedef router mac adresi> mono <aktif edilen ağ kartı>**" son olarak "**WPA Handshake**" yazısı görüntülendiği zaman paket toplama işlemi gerçekleşmiş ve parola kırma saldırısı başlatılabilir demektir.



Fakat paket gelmeme durumlarında "**aireplay-ng -o <kaç adet broadcast paketi gönderileceği belirtilir>**" o yapılır ise sonsuz döngüye girer "**–a <hedef routerin MAC adresi>**", "**mono <wireless interface>**" şeklinde deaut paketleri gönderilir.



Son olarak yakalanmış olan handshake dosyasına bruteforce saldırısı yapılır. “**aircrack-ng –w <wordlist dosyasının bulundugu yer>**”, “**<.CAP dosyasının bulundugu path.>**” şeklinde parola kırma saldırı başlatılır. Wordlist üzerinden deneme yanılma yöntemi ile parolayı doğrulanır ve "**KEY FOUND!**" kısmında gözükmektedir.