IEEE 802.11 KABLOSUZ AĞLARDA GÜVENLİK

Mustafa ABDULKAREEM

YÜKSEK LİSANS TEZİ
BİLGİSAYAR BİLİMLERİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

HAZİRAN 2012
ANKARA

Mustafa ABDULKAREEM tarafından hazırlanan IEEE802.11 KABLOSUZ AĞLARDA GÜVENLİK adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Suat ÖZDEMİR
Tez Yöneticisi

Bu çalışmada, jürimiz tarafından oy birliği ile Bilgisayar Bilimleri Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Başkan : Doç. Dr. Ayhan ERDEM

Üye : Doç. Dr. Suat ÖZDEMİR

Üye : Yrd. Doç. Dr. Hacer KARACAN

Üye :

Üye :

Tarih : 21 / 9 / 2012

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Mustafa ABDULKAREEM

IEEE 802.11 KABLOSUZ AĞLARDA GÜVENLİK

(Yüksek Lisans Tezi)

Mustafa ABDULKAREEM

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2012

ÖZET

Kablosuz ağlarda bağlantı hızının kullanıcılar için makul seviyelere çıkması kablosuz ağ kullanımını yaygınlaştırmıştır. Kablosuz ağların geniş bir şekilde kabul görmesi ve bu ağlara olan gerekliliğin artması, kablosuz ağların güvenliği ile ilgili bazı endişeleri de beraberinde getirmiştir. Kablosuz ağ güvenliği için birçok yöntem mevcuttur ve her geçen gün geliştirilmektedir. Kullanılan bu yöntemlerden bazıları güvenlik açıklarına sahiptir. Bu açıklardan dolayı kablosuz ağlar tehdit altındadır. Bu çalışmada kablosuz ağların korunması için geliştirilen IEEE güvenlik algoritmalarının açıkları anlatılmış ve bu açıklardan yararlanılarak kablosuz bir ağa nasıl dâhil olunacağı gösterilmiştir.

Bilim Kodu : 902
Anahtar Kelimeler : IEEE 802.11, WPA, WPA2, kablosuz ağ güvenliği
Sayfa Adeti : 101
Tez Yöneticisi : Doç. Dr. Suat ÖZDEMİR

IEEE 802.11 WIRELESS SECURITY

(M.Sc. Thesis)

Mustafa ABDULKAREEM

GAZİ UNIVERSITY

INFORMATION INSTITUTE

June 2012

ABSTRACT

The increase of connection speed of wireless networks up to satisfactory levels has increased the usage of wireless networks. A wide acceptance and the need for the wireless networks led to certain concerns regarding the overall security of these networks. There are various methods for wireless network security which are improved every day. Some of these methods which are put into use have some security gaps. Hence, due to these gaps the wireless networks are under threat. In this study, the gaps of the developed IEEE security algorithms to protect the wireless networks have been explained and ways to join a wireless network with the use of these gaps have been shown.

Science code : 902
Key Words : IEEE 802.11, WPA, WPA2, wireless network security
Page Number : 102
Adviser : Assoc. Prof. Dr. Suat ÖZDEMİR

TEŞEKKÜR

Çalışmalarım boyunca yardım ve katkılarıyla beni yönlendiren değerli Hocam Doç. Dr. Suat ÖZDEMİR'e ve tecrübelerinden faydalandığım değerli Hocam Doç. Dr. Ayhan ERDEM 'e teşekkürü bir borç bilirim. Ayrıca verdikleri maddi ve manevi destekten dolayı değerli aileme ve Seda KIRAÇ'a teşekkür ederim. Yine değerli arkadaşlarıma manevi destekleriyle beni hiçbir zaman yalnız bırakmayan Mohammad DAOUD, Talha KARADENİZ, Hüseyin RİZA, Usame KEMALİ, Mustafa KÖPÜRLÜ, Alper GERÇEK ve Ramazan KOCAOĞLU 'na teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BSS	Basic Service Set
DDoS	Distribution Denial of Service
DES	Data Encryption Standart
DOS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
FIPS	Ferderal Information Processing Standart
FHSS	Frenquency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronic Engineers
IV	Initialization Vector
LLC	Logical Link Control
MAC	Medium Access Control
MIC	Message Integrity Code
MITM	Man in The Middle
PBC	Push Button Configuration
PIN	Personal Identification Number

Kısaltmalar	Açıklama
PSK	Preshared Key
PTK	Pairwise Transient Key
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

1. GİRİŞ

Kablosuz iletişim teknolojisi; en basit tanımıyla, noktadan noktaya veya bir ağ yapısı şeklinde bağlantı sağlayan, bir teknolojidir. Bu açıdan bakıldığında, kablosuz iletişim teknolojisi, günümüzde yaygın olarak kullanılan kablolu veya fiber optik iletişim yapılarıyla benzerlik göstermektedir. Kablosuz iletişim teknolojisini diğerlerinden ayıran nokta ise; iletim ortamı olarak havayı kullanmasıdır.

On yıl önce, neredeyse kimse kablosuz interneti duymamıştır. Ancak bugün, Bilişim teknolojisi büyük ölçüde kablosuz ağ cihazlarının etkin kullanımıyla kablosuz bağlantı sağlayabilmektedir [1]. Kablosuz Yerel Alan Ağlarında (Wireless Local Area Network - WLAN), yaşanan en büyük sorunlar, güvenlik ile ilgilidir. WLAN'ın hava ortamında yaydığı kablosuz iletişim sinyalleri, tüm yönlere eş zamanlı olarak hava yoluyla iletilmektedir. Yetkisiz kullanıcı, WLAN'ın saldırıya açıklığından faydalanmak için ücretsiz yazılım araçlarını kullanarak bu sinyali kolaylıkla yakalayabilir. WLAN'lar, kablosuz cihazlar için kolaylık, taşınabilirlik ve bütçeye uygun fiyatları ile evlerde ve iş ortamlarında büyük ölçüde kullanılmaktadır. WLAN, kullanıcılara evde, hava alanı ve kampüsler gibi etkin ve açık alanlarda taşınabilirlik ve esneklik sağlar. Bu ağların güvenliğini sağlamak için günümüzde çoğunlukla WEP (Wired Equivalent Privacy) ve WPA (Wi-Fi Protected Access) / WPA2 (Wi-Fi Protected AccessII) gibi şifreleme yöntemleri kullanılır [2]. Bu yöntemler, ağ içinde taşınan verilerin şifrelenmesine izin verir. Buna rağmen, bilginin kodlandığının söylenmesi, bilgisayar korsanlığı uzmanlarının ille de ona erişemeyeceği anlamına gelmez [1].

Kablosuz ağlar beraberinde güvenlik sorunlarını da getirmişlerdir. Bilindiği üzere kablosuz ağlarda iletim ortamı olarak hava kullanılmaktadır. Bu, RF sinyalinin havanın götürebildiği yere kadar gidebilmesi anlamına gelmektedir. Bunun dışında, kablosuz ağ teknolojileri de kablolu ağlara benzer güvenlik özelliklerine sahiptir.

Bu araştırmada, WLAN teknolojileri ve sorunları ortaya koyulmuştur. Amaç, kablosuz ağ güvenliklerine dair genel bir bakış açısı sağlamak ve WLAN güvenlik konularını değerlendirmektir

WLAN iletişimine dair üç ana şifreleme teknolojisi vardır: WEP, WPA ve WPA2. Bu teknolojiler, Gizlilik, Bütünlük ve Kimlik Doğrulamayı sağlama konularında çözümde bulunur. Ancak, tüm bu işleri başaramazlar ve WLAN'ları dışarıdan yapılacak saldırıya karşı savunmasız bırakırlar. Yaptıkları iş sadece şifrenin elde edilme süresinin uzatılmasını sağlamaktır.

802.11 ağlarında kullanılan ilk koruma, WEP olarak bilinir. WEP'in güvensizliğine dair ilk araştırma, 2000 yılında Walker tarafından yapıldı; Walker, WEP'in herhangi şifre büyüklüğünde güvenli olmadığını ve kablolu ağ seviyesinde veri gizliliğini sağlamak olan tasarım amacını karşılayamadığını ifade etti. Borisov, 2001 yılının başında büyük bir ihtilaf ortaya çıkaran WEP güvensizliği üzerine ilk ciddi makaleyi sundu. Sadece bir ay sonra, 2001 yılında WEP kodlama algoritması RC4 Fluhrer, Mantin ve Shamir tarafından kırıldı, bu yüzden WLAN güvenliğinde kullanılan WEP kötü bir üne sahip oldu. Fluhrer, Mantin ve Shamir (FMS) WEP tarafından kullanılan şifre programlama algoritmasına bir saldırıyı ifade eden "Weaknesses in the Key Scheduling Algorithm of RC4" adında bir makale yayımladırlar. FMS saldırısı sadece teorik değildi, gerçek dünyaya uyumlu hale getirilmesi çok da uzun sürmedi. Bununla beraber FMS, WEP'in çöküşünü başlatmış oldu [3].

Ancak, bu tamamen deneysel, kullanımı kolay olmayan araçlar ve yapılması zor olan testler, dış dünyadaki insanların kullanımına kapalıydı. Oysa ki, bilgisayarı olan ve ağ kurma bilgisi olan herkesin Kablosuz LAN'ı hackleme olanağı sağlayan Linux için BackTrack adında açık kaynak aracının sürülmesi ile değişti.

Bu saldırıya karşı atak yapmak için ilk girişim, "WEPPlus" ya da WEP+ olarak adlandırılan daha güvenli WEP versiyonunu geliştiren Agere Sistem tarafından yapıldı. Normal WEP uygulamaları tarafından üretilen zayıf IV miktarını büyük ölçüde düşürdü ve kendi erişim noktaları için donanım yazılımı güncellemesi olarak

piyasaya sürüldü [4]. Eş zamanda, 2001 yılında Cisco Aironet WLAN ürünlerine farklı bir yaklaşım geliştirmeyi dinamik WEP şifrelerini ortaya çıkarmaya karar verdi. Ne yazık ki, yukarıda bahsedilen çözümlerle konu, satıcıya özel ve birbiriyle uyumsuz olduğudur. Korek2 olarak bilinen bir bilgisayar korsanı 2004 yılında WEP güvenliği hakkındaki Netstumbler forumundaki saldırıya yanıt verdiğinde WEP için işler ters gitti. Açıkladığı saldırı, zayıf IV'e daha fazla bağlı değişmesiyle ilgiliydi. Korek saldırısı, istatistiksel kod analizini kullandı ve FMS saldırısından daha verimli olduğunu kanıtladı [5].

2007 yılında, Pyshkin, Tews ve Weinmann tarafından yeni bir nesil WEP saldırıları yayımlandı. PTW adındaki saldırıları, bir dakikadan az zaman içinde WEP'e girmeye izin veren yeni kavramları ortaya koydu. KoreK ve PTW saldırıları, WEP kırma ve WLAN denetim araçlarına hızlı bir şekilde uyumlu hale getirildi ve WEP korumalı WLAN'lara saldırmak için standart haline getirildiler [6] .

WEP algoritmasındaki zayıflık ve yapılan değişik saldırı türleriyle ününü zehirlemesi bilişim insanlarını yeni teknolojiler bulmaya yöneltti. Bunlardan ilki donanım değişikliğine gidilmeden sadece algoritma olarak değiştirilen ve yeni ismi WPA olan bir güvenlik protokolü oldu.

2003 yılında, Kablosuz Korumalı Erişim, Wi-Fi Alliance tarafından sürüldü. Standart değildi, ancak zamanında kablosuz güvenliğe geçici bir çözüm sağlamak için kullanıldı. Bu süre boyunca, kurumlar kablosuz ağlarını korumak için WPA'ları alternatif bir güvenlik çözümü olarak kullandılar.

WLAN'lardaki artan güvenlik seviyesi, WEP gibi güvenlik algoritmalarının açıklarının ortaya çıkması ve yaygınlaşması ile WPA güvenlik algoritması geliştirildi. WPA üzerine çalışma, WEP'in ihlalinin ilk raporlarından sonra hemen başlatıldı ve sonrasında dünya çapında yayıldı [7].

WPA şifreleme, WEP'ten daha güvenli ve saldırılara daha dayanıklı olsa da WEP şifre algoritmasının çalıştığı bir donanım üzerinde çalıştırabilir. Buna rağmen, WPA, WEP'in açıklığından daha fazlasını paylaşmıştır. Takashi 2004 yılında, WPA'ya karşı kaba kuvvet çevrim dışı sözlük saldırısına izin veren kavram kanıtlama olan WPAcrack adı verilen bir araç geliştirmiştir [8]. Wi-Fi Alliance'ın yirmi karakterden uzun şifrelerin kullanılması yönündeki önerisinin, WPA kullanıcıları tarafından pratikte büyük olasılıkla uygulanmayacağını belirtmiştir.
Ne yazık ki çoğu kişi, uzun şifrelerin oluşturulmasına ve gelecekte meydana gelebilecek sonuçlarına gereken önemi vermez.

2009 yılında McMillan, önceden paylaşılmış anahtarın (PSK) güvenli olmadığını kısa ve güvensiz şifrelerin WEP ile hemen hemen aynı derecede dezavantajlı olduğunu bildirmiştir.

2004 yılın sonunda, Elektrik Elektronik Mühendisliği Kurumu (IEEE) yeni bir kimlik doğrulama protokolü olan – Gelişmiş Şifreleme Standardı (AES) ile Şifre Blok Zincirleme Mesajı Kimlik Doğrulama Kod Protokolüne sahip (CCMP) Sayaç Modu olarak adlandırılan çok güçlü bir kodlama modu ortaya koydular. Sonuçta, WLAN güvenliği olgunlaştı ve güvenli çözüm ve ün sağlanırmıştır [2].

2008 yılında, güvenlik araştırmacıları Beck ve Tews, WPA2'yi kısmen kırmak için sistematik bir yol geliştirdiklerini bildirdiler. Bu saldırı öncesinde, bilinen diğer yöntemler, zayıf bir şekilde seçilen önceden paylaşılmış anahtara karşı bir sözlük saldırısını içermiştir. Ancak yeni saldırı metodu, WPA2'ye ufak bir tehdit oluşturmuştur olsa da, AES'e karşı etkili olmadığı görülmüştür. [9].

2011 yılında Kizza, WPA2 protokolünün frekans sıkışması, hizmet bütünleşme ya da kimlik doğrulama ve bağlantı kuramama atakları gibi saldırılara karşı korumayı tam manasıyla yapamadığını kaydetmiştir [10].

Aralık 2011 yılında, kablosuz erişim noktası cihazlarına karşı Cisco, D-Link, Netgear ve benzeri pek çok erişim noktası sağlayıcısı tarafından uygulanan Kablosuz Korumalı Kurulumun (WPS) özelliğinin zayıflığını kullanan yeni bir saldırı bulunmuştur. Zayıflığı bulan Stefan Viehböck, tehdit hakkında ayrıntılı bir şekilde bilgi vermişti, WPA2 anahtarı gibi hassas konfigürasyon verilerine erişim sağlamak için kablosuz erişim noktasının WPS uygulamasının nasıl kaba kuvvet kullanabileceğini açıklamaktadır. Başarılı bir saldırı, kablosuz cihaza bağlı olarak 4 ila 10 saat yürütülebilir. Bu tür saldırıları daha kolaylaştırmak için bir dizi araç vardır. Bu araçlardan biri BackTracktaki Reaver'dır .

Bu tezin geri kalan kısmı aşağıdaki bölümden oluşur; 2. kısımda, kablosuz ağların avantaj - dezavantajları ve kullanılan standartları 802.11 a,b,g,n incelenmiştir.

3. kısımda, 802.11 standardını kullanan kablosuz yerel alan ağlarındaki güvenlik mekanizmaları incelenmiştir; güvenlik açıkları ve sistemin zayıflıkları ve ağa yapılan saldırıların neler olduğu ele alınmıştır. 4. kısımda, kablosuz bir ağ üzerinde farklı güvenlik mekanizmaları yapılandırılıp, bu ağa saldırılar gerçekleştirmek suretiyle BackTrack 5 araçları kullanarak uygulamalar yapılmıştır. WEP'in ne kadar kolay kırılabileceği gösterilmiştir, WPA/WPA2 algoritması kullanan kablosuz ağlara saldırılar yapıp sonuçları gözlenmiştir. 5. kısımda tezin sonuç ve önerileri yer almaktadır.

Bu tezin temel amacı; kablosuz ağların bireysel olarak kullanımdan en kapsamlı ve gelişmiş kurumsal kullanım alanlarına kadar, güvenli bir kablosuz yerel alan ağı oluşturmak için izlenmesi gereken politikaları belirlemek ve olası saldırılara karşı alınması gereken önlemleri irdelemektir. Kablosuz ağ kullanımının getirdiği güvenlik zafiyetlerini göstererek ve bu açıklardan faydalanarak kablosuz bir ağa dahil olmanın yolları gösterilmiştir. Bu şekilde kablosuz ağ kullanımın güvenlik alanında bireylere farkındalık kazandırması hedeflenmiştir.

2. KABLOSUZ AĞLAR

Kablosuz kelimesi genel bir terimdir, bir noktadan başka bir noktaya bakır kablo gibi fiziksel bir bağlantı kullanmadan yapılan veri, ses veya görüntü taşınmasına denir [11]. Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan çalışma biçimine, bilgisayar ağı (Computer Network) denir. Bir bilgisayar ağında çok sayıda bilgisayar yer alır. Bu bilgisayarlar; yan yana duran iki bilgisayar olabileceği gibi, tüm dünyaya yayılmış binlerce bilgisayar da olabilir.

Bilgisayar ağlarının ilk uygulamaları 1960'lı yılların sonlarında başlamıştır. Ancak yerel bilgisayar ağlarının yaygınlaşması 1980'li yıllarda başlamış ve gelişmiştir. 1980'li yıllarda, kişisel bilgisayarların çoğalması, bilgisayar teknolojisindeki ve iletişim teknolojilerindeki gelişmeler bilgisayar ağlarının daha yararlı olmasını sağlamıştır. Bu ağlar; özel amaçlı, eğitim amaçlı, ulusal veya halka açık olarak kurulabilirler. Kablolu iletişim teknolojilerine kıyasla birçok üstünlüğü bulunan kablosuz iletişim teknolojilerin 1990'lı yıllarda büyük gelişmelere sahne olmuştur [12].

Kablosuz ağlar, kablo limiti olmaksızın geleneksel ağ teknolojilerinin bütün imkan ve avantajlarını sağlar. Kablosuz sistemler tamamıyla kablodan arınmış vaziyette değildir. Bu sistemler geleneksel ağlara bağlanmak üzere, standart mikroişlemciler ve sayısal devreler kullanırlar. Kablosuz aygıtlar, kodlama, sıkıştırma, taşıma ve sinyal alma işlemleri için geliştirilmektedirler [13].

Genelde kablosuz ağlarda kullanılan aygıtlar, taşınabilir bilgisayar, masaüstü bilgisayar, el bilgisayarı, kişisel sayısal yardımcı (PDA-Personal Digital Assistant), cep telefonu ve çağrı cihazlarını kapsamaktadır. Kablosuz teknolojiler birçok kolaylık sağlar. Örneğin cep telefonu kullanıcıları, e-postalarına erişmek için cep telefonun kablosuz ağlara bağlanma özelliğini kullanabilirler. Taşınabilir bilgisayar ile seyahat edenler, hava alanlarında, tren istasyonlarında ve diğer genel noktalarda kurulu baz istasyonları aracılığıyla internete bağlanabilirler. Evdeki kullanıcılarsa

veri eşitleme ve dosya aktarımı için masaüstlerindeki aygıtlarla bağlanabilirler [14]. Şekil 1'de kablosuz ağ sistemleri ve kullanım alanları gösterilmiştir.

Şekil 2.1. Kablosuz sistemin kullanım alanları

2.1. Kablosuz Ağların Avantajları

- **Taşınabilirlik:** Kablosuz ağların yaşantımıza en büyük katkısı, şüphesiz ki kablo olmaksızın sunduğu erişim imkanıdır. Bu sayede ağa bağlı olan kişilerin sabit bir yere bağlı kalma zorunluluğu yoktur. Bu insanlara büyük bir ölçüde özgürlük sağlamakta ve verimliği arttırmaktadır [15].

- **Kolay kurulum:** Kolay kurulumun da kendi içinde iki faydası vardır :
  - **Zaman:** Radyo dalgaları ile iletişim yapılmasından dolayı kablolu bir ağ tasarımından önce gerekli olan kablolama planı ve kablolama işlemi için harcanan zamandan kazanılmış olur.

  - **Maliyet:** Yukarıda belirtildiği gibi kablolama yapılmadığı için kablo maliyeti ağ kurulumunda yer almamaktadır.

- **İşletme Kolaylığı:** Kablo koptu, yerinden çıktı gibi dertler yaşanmaz. Hub ve anahtar ilaveleriyle yeni kablolara yer açma sıkıntısı yoktur.

2.2. Kablosuz Ağların Dezavantajları

- **Güvenlik:** Yapılan iletişim dalgalar halinde yayıldığı için davetsiz misafirlere açıktır. Özel tedbirler alınmadığı sürece ağ trafiğinin dinlenmesi ve izlenmesi çok kolaydır.

- **İletişim Kalitesi:** Dış dünyadaki birçok sinyal kaynağından etkilenebileceğinden iletişim kalitesi, dalga girişimine bağlı olarak düşebilir. Ayrıca çok noktadan sağlanan erişimler için dikkatlice hazırlanmış hücre planlaması gerektirir.

- **Standartlara Uyma Zorunluluğu:** Üretilen cihazların tüm dünya standartlarında olması gerekmektedir. Uluslararası enstitüler bazı konularda sınırlamalar getirmekte ve bu da gelişmelerin daha yavaş olmasına neden olmaktadır [15].

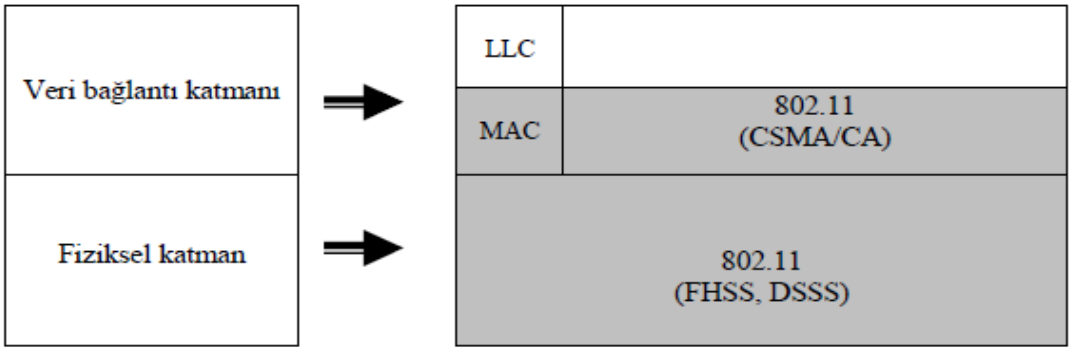
2.3. Kablosuz Ağ Standartları

İlk olarak WLAN aygıtları düşük hızları, standart eksikleri ve yüksek maliyetleri ile kullanışlı değildi. Toplam bant genişliğinin 1-2 Mbps gibi bir hızla kısıtlı olması, farklı firmalar tarafından üretilen ağ arayüz kartı (Network Interface Card - NIC) ve erişim noktalarının (Access Point - AP) birbirleri ile uyumlu çalışamama probleminden dolayı tercih edilmiyordu. Ancak 2000'li yıllardan itibaren, standartlaşmayla birlikte WLAN sistemleri hızla yayılmaktadır. Çünkü standartlaşma sonucunda bir çok marka WLAN donanımı aynı kablosuz ağ içinde kullanılabilmektedir. Bugün Wi-Fi (Wireless Fidelity/Kablodan bağımsızlık) kablosuz ağlar için endüstri standarttı olarak yaygın şekilde kullanılmaktadır [15,16].

Kablosuz iletişim teknolojisinin büyük kitleler tarafından kabul görebilmesi için, cihazların üretici firmaları arasındaki uyum ve güveni sağlayan endüstri standartları geliştirilmesi ile birlikte, çeşitli standartlar oluşturulmuştur. En çok tercih edilen standartlar aşağıdaki gibidir.

2.3.1. IEEE 802.11 standartları

IEEE, OSI (Open System Interconnection) referans modeline göre veri bağlantı katmanını MAC (Media Access Control) ve LLC (Logical Link Control) olarak iki alt katmana ayırmıştır. Bunun nedeni üst katmanların, ağ donanım yapısına ve türüne bakmaksızın aynı arabirimle çalışabilmesini sağlamaktır. 802.11, 1997 yılında standart olmuştur. 802.11 IEEE tarafından kablosuz ağlar için geliştirilmiş bir standarttır. İlk geliştirilen standart olan 802.11; 2.4 GHz frekansında, saniyede 1 Mb veya 2 Mb veri transferine izin verir. Bu standardın fiziksel katmanda, FHSS ve DSSS olmak üzere kullandığı iki farklı modülasyon yöntemi bulunmaktadır. Bu yöntem ile elverişli ortamlarda FHSS ile 2 Mbps, sinyal gürültüsü olan ortamlarda ise DSSS ile 1 Mbps veri iletim hızları sağlamaktadır. Günümüzde kullanılan teknolojiler 802.11a, 802.11b, 802.11g, 802.11n standartlarıdır [16].



Şekil 2.2. OSI referans modeli ve 802.11 standardı

2.3.2. IEEE 802.11a standardı

802.11a standardı 1999 yılında kablosuz Asenkron Transfer Modu (ATM) için geliştirilmiştir. 802.11 standardı; 5 GHz bandında, 54 Mbps bant genişliği sunan WLAN teknolojisidir. Bu standardın kullanım bulacağı alanlar, verilerin ve içeriğin yüksek veri hızlarında iletilmesi gereken durumlarda kullanılır. Bu standart; birçok ülkede, sivil amaçlar için kullanımı kısıtlanan 5 GHz bandında çalışması ve diğer standartlardan farklı olarak üretilmesi ve bunun sonucunda pahalı olduğu için çok tercih edilen bir standart değildir.

2.3.3. IEEE 802.11b standardı

802.11b standardı 1999 yılında tamamlanmış ve 2001 yılından itibaren kablosuz ürün pazarında yer almıştır. 802.11b standardı 2.4 GHz bandında, 11 Mbps bant genişliği sunan bir teknolojidir. Kapsama alanı kapalı alanlarda 30 – 45 metredir. Bu standart; genelde ofisler, hastaneler, fabrikalar gibi yerlerde kullanılmaya uygundur. 802.11b; WLAN'lar, taşınabilirliğin gerekli olduğu ve orta hızlı ağ bağlantılarına ihtiyaç duyulan alanlarda kullanılır [17].

2.3.4. IEEE 802.11g standardı

802.11g standardı 2003 yılında adını verdiği yeni bir kablosuz iletişimi duyurmuştur. 2.4 GHz frekans spektrumunu kullanır ve maksimum 54 Mbps bant genişliğine sahiptir. 802.11b'nin geliştirilmiş halidir de denilebilir. Teknolojik olarak 2.4 GHz bandında çalıştığı için; onun özelliklerini taşır, ancak toplam 54 Mbps bant genişliği sunar. Çizelge 2.3'te 802.11 standartlarının karşılaştırılması gösterilmiştir.

2.3.5. IEEE 802.11n standardı

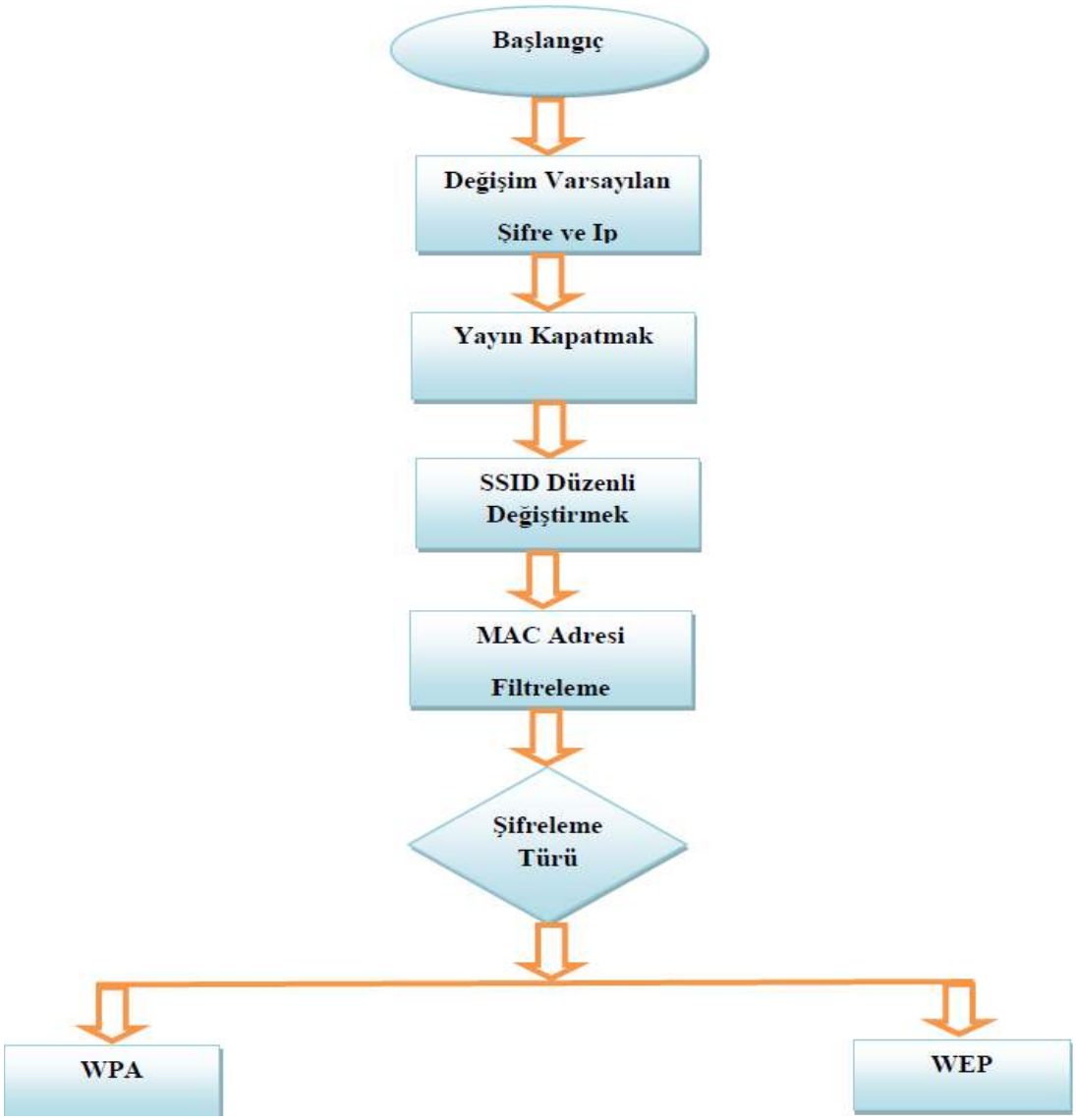
802.11n standardı 2007 itibariyle tamamlanmamasına rağmen geliştirilme aşamasında taslak duyurulmuştur. IEEE 802.11n: şu anda taslak aşamasında, maksimum veri transfer hızını 540 Mbps çıkarmaya, bunun yanında eş zamanlı çoklu veri iletişimi yapılmasına imkân tanıyan yeni bir standarttır. Kablosuz ağlar yapılanma şekillerine göre altyapısız ağlar ve altyapılı kablosuz ağlar olarak iki kısımda çalışmaktadır.

Çizelge 2.1. IEEE 802.11 standartlarının karşılaştırılması

Kablosuz Standarttı	**802.11b**	**802.11a**	**802.11g**	**802.11n**
Kullanım Oranı	Yaygın	Kısıtlı	Yaygın	Yaygın
Hız	11Mbps	54Mbps	54Mbps	540Mbps
Ortalama Maliyet	Düşük	Yüksek	Yüksek	Yüksek
Frekans	2.4 GHz	5 GHz	2.4 GHz	2.4GHz veya 5 GHz
Kapsama Alanı(Metre)	30 – 45	25 – 75	30 – 45	50 – 125
Açık Erişim Noktaları	Yaygın	Çok az (pahalı)	Yaygın	Yaygın
Uyumluluk	802.11g ile uyumlu	802.11b,g ile uyumsuz	802.11b ile uyumlu	802.11a,b,g ile uyumlu

3. KABLOSUZ AĞLARDA GÜVENLİK TEKNOLOJİLERİ

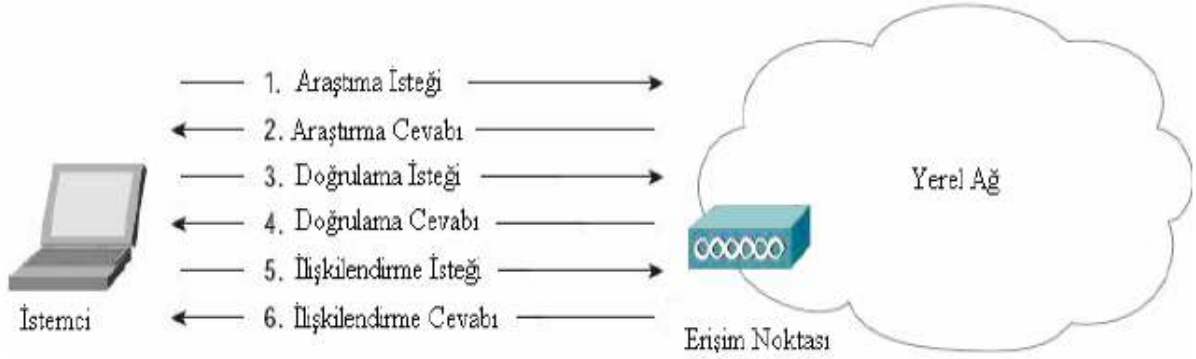
Kablosuz ağların kullanıldığı ilk yıllarda güvenlik büyük bir sorun olarak görülmemekteydi. Donanımlar üreticilere özel, pahalı ve bulması zordu. Kablosuz ağların yaygınlaşmasıyla güvenlik amaçlı yapılan çalışmalar, kablosuz ağlara saldırıların artık kolay olmadığını göstermiştir, yetersiz algoritmaların yerini daha kuvvetli algoritmalar almıştır. Kablosuz istemciler ve erişim noktaları üzerinde etkin olan birkaç güvenlik seviyesi aşağıdaki şekilde gösterilmektedir [18].



Şekil 3.1. Kablosuz güvenlik seviyeleri

3.1. Servis Seti Tanımlayıcı (SSID-Service Set İdentifier)

Servis seti tanımlayıcı (SSID), kablosuz ağın mantıksal adıdır. Kablosuz ağa bağlanmak isteyen kablosuz cihazlara ağın kimliğini verir. SSID, istemci ve erişim noktalarına girilebilen 1'den 32'ye kadar ASCII dizgidir. SSID olmadan asla bir WLAN'e bağlantı kurulamaz. Bazı erişim noktaları SSID yayınlama ve seçilen bir SSID'ye izin verme gibi seçeneklere sahiptir. Herhangi bir SSID seçeneğini kullanmak erişim noktasının boş SSID'li bir isteminin erişimine izin verir. İlk kuşak kablosuz ağlar SSID'yi güvenliğin temel şekli olarak kullanmışlardır [19].



Şekil 3.2. 802.11 istemci doğrulama süreci

3.2. SSID Yayının Önlemek

Bir WLAN'a bağlanabilmenin temel şartları arasında SSID tanımlayıcısının bilinmesi yer alır. Terminal ve erişim noktalarına SSID bilgisi statik olarak elle tanımlanabileceği gibi, SSID bilgisinin erişim noktası tarafından yayınlanması da sağlanabilir.

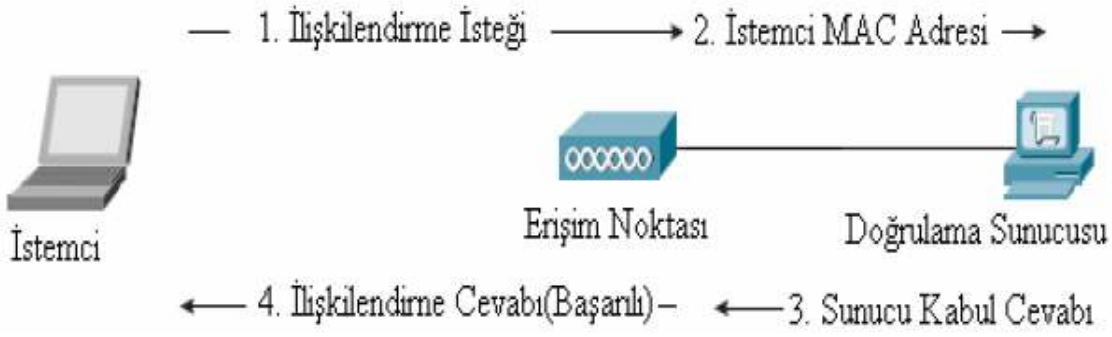
WLAN servisleri için, erişim noktalarının SSID yayını yapması işletmenin gerekliliği olarak düşünülebilir. Ancak, ev veya ofis türü WLAN'lar için SSID yayınının yapılması bir gereklilik değildir. Fakat bu tür WLAN'lar kullanıcıları belli olduğundan SSID tanımlayıcısı tüm terminallere elle girilebilir. Nispeten küçük WLAN'lar için SSID tanımlayıcısını terminallere elle girmek çok zor bir işlem değildir. NetStumbler, Airodump gibi birçok araç, SSID tanımlayıcısını bulup

gösterebilir. Ağda, güvenlik ve kimlik denetim servisleri kullanılmıyorsa sadece SSID bilgisi ile üçüncü şahıslar ağa erişebilir. Bu nedenle, güvenlik servislerinin durumuna bağlı olarak SSID bilgisinin yayınlanması bir güvenlik açığı olarak düşünülebilir [19].

3.3. MAC Adresi ile Doğrulama

MAC tabanlı doğrulama 802.11 standardında tanımlanmıştır. Bununla birlikte birçok tedarikçi MAC tabanlı doğrulamayı uyarlamıştır. Tedarikçilerin çoğu basitçe, her erişim noktasının geçerli bir erişim kontrol listesi olmasına ihtiyaç duyarlar. Bazı tedarikçiler erişim noktasının merkezi sunucu üzerindeki MAC adres listesini sorgulamasına izin verirler. Erişim kontrol listeleri, kullanıcının ağı kullanmasını bu erişim kontrol listelerine göre sınırlandırırlar. Eğer kullanıcının MAC adresi listede varsa ve ağa ulaşım için izin verilmişse ağ kaynaklarına erişime izin verilir. Farklı durumda erişim engellenecektir.

1. Kullanıcı erişim noktasına doğrulama isteği gönderir.
2. Erişim noktası, kullanıcının MAC adresini doğrulama sunucusuna gönderir.
3. Sunucu kabul ya da ret cevabını erişim noktasına gönderir.
4. Erişim noktası kullanıcıyı doğrular.



Şekil 3.3. MAC adresi ile doğrulama

3.4. 802.11 Güvenlik

Bir kablolu ağda; kimlik denetimi yapmanın ilk yolu, kullanıcının ağa giriş yapabilmek için aşması gereken fiziksel engeller uygulamaktır. Böyle engeller, sinyalleri bir binanın duvarlarının ötesinde dolaşan kablosuz ağlar için uygun değildir. Bir güvenlik mekanizması, kablosuz ağı koruyacak bir yere yerleştirilmelidir. Kablosuz ağdaki güvenlik 802.11 olarak adlandırılır. 802.11'in esas güvenlik mekanizması olan WEP'i (Wired Equivalent Privacy) kırmanın ne kadar kolay olduğuna dair bilgiler çoktur. WEP protokolü, 802.11'in orijinal güvenlik mekanizmasıdır. WEP, yetersizliklerinden dolayı, şifrelemeyi sağlamak amacıyla kablosuz ağlarda nadiren kullanır, onun yerine girişin kontrolü tescilli yöntemlerle yapılır. 802.11i güvenlik standardı; WEP protokolündeki zayıflıkların düzeltilmesi için, WEP üzerinde yapılan değişikliklerle elde edilmiştir. Ancak bu değişimi desteklemek için yeni ve daha güçlü erişim noktasına ve geliştirilmiş donanımlarıyla yeni mobil istasyonlara gerek duyulacaktır. Bu nedenlerden dolayı ; Wi-Fi konsorsiyumu, Wi-Fi Protected Access (WPA) diye adlandırılan bir ara güvenlik çözümü tanımlamıştır. WPA 802.11'nin bir türevidir. İkisi de 802.1X standardına benzer çalışırlar.

3.5. Güvenlik Anahtarı

Güvenlik anahtarı, Kabloluya Eşdeğer Gizlilik (WEP) anahtarını veya Wi-Fi Korumalı Erişim (WPA) anahtarı, Çok Güvenli Ağ (WPA2) şifresini ifade eder. Güvenlik anahtarı, ağın yetkisiz kullanımını önlemek üzere kablosuz ağ güvenliğini sağlamak için kullanılır. Yönlendirici veya erişim noktasında yapılandırılır ve kablosuz ağa erişen her kablosuz aygıta aynı anahtarın girilmesi gerekir. Aygıtların doğru güvenlik anahtarı yoksa kablosuz ağda iletişim kurmalarına izin verilmez. WEP en düşük düzeyde güvenlik sağlarken, WPA daha yüksek güvenlik sağlar. WPA'dan daha iyi bir şifreleme yöntemi kullanan WPA2, küçük ve kablosuz ağların çoğu için en iyi güvenlik seçeneğidir. Yönlendirici (Router) yeniyse, üç güvenlik türünün (WEP, WPA ve WPA2) hepsini desteklemektedir. Daha eski yönlendiriciler

WEP ve WPA'yı destekleseler de WPA2'yi desteklemezler. Birkaç yıllık kablosuz ekipman büyük ihtimalle yalnızca WEP'i destekleyebilir [20].

ASCII (American Standard Code for Information Interchange) Amerikan karakter kodlama sistemidir. ASCII sisteminde 33 tane yazılamayan karakter ve 95 tane yazılabilen karakter bulunur. Farklı güvenlik protokollerinde anahtar olarak ASCII karakterler kullanılmaktadır.

Güvenlik Anahtarı	Özellikler
WEP	Tam 10 veya 26 onaltılık karakterden oluşmalıdır. Onaltılık karakterler: A-F, a-f ve 0-9. veya Tam 5 veya 13 ASCII karakterinden oluşmalıdır. ASCII karakterleri, klavyede bulunan harfler, sayılar ve sembollerdir.
WPA **WPA2**	En fazla 64 onaltılı karakterden oluşmalıdır. Onaltılı karakterler: A-F, a-f ve 0-9. veya 8 ila 63 ASCII karakterinden oluşmalıdır.

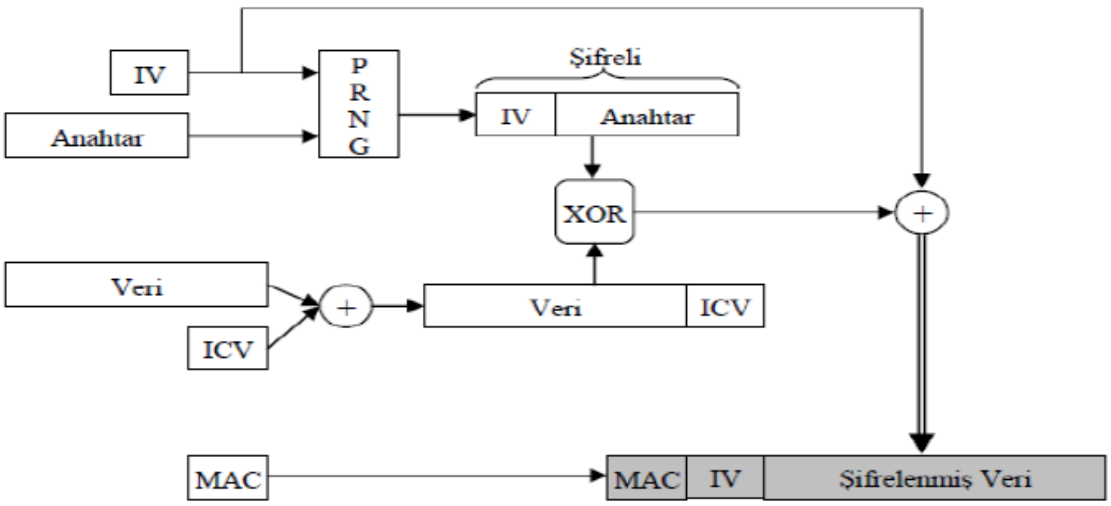
Çizelge 3.1. Güvenlik anahtarın özellikleri

3.5.1. Kabloluya eşdeğer gizlilik (WEP-Wired Equivalent Privacy)

Wired Equivanlent Privacy (WEP), orijinal 802.11 güvenlik tanımlamasıdır. Bilgi; ağın kablosuz kısmında ilerlerken, bilgiyi korumak için tasarlanmıştır. WEP, erişim noktasının ötesinde koruma sağlamaz ve 802.11a,b,g,n standartları için güvenlik sağlar. WEP'in teknik altyapısı Ron Rivest tarafından bulunan RC4 (Rivest Cipher) akış şifreleme algoritmasına dayanır. RC4'ün amacı, verilen bir gizli anahtar ile geniş uzunlukta rastgele sayılar üretmek ve daha sonra bu akışla göndericide düz metin mesajı şifrelemektir. Alıcı, verilen anahtarla aynı akışı üretebilecek ve alınan mesajın şifresi çözülebilecektir [21].

WEP'in çalışması şu şekildedir: [22]

1. Veri bütünlüğünü sağlamak amacıyla, veri bir doğrulama algoritmasına (Integrity Check) tabi tutularak, doğrulama bitleri (ICV – Integrity Check Value) elde edilir.
2. Bu doğrulama bitleri verinin sonuna eklenir.
3. 24 bitlik IV(Initialization Vector) statik anahtarın başına eklenir; 64 bitlik paket oluşturulur.
4. 64 bitlik bu paket statik RC4 (Rastgele Sayı Üretici – Pseudo Random Number Generator - PRNG) algoritması ile şifrelenir.
5. İkinci adımda elde edilen veri ile dördüncü adımda elde edilen veri bir XOR işleminden geçer.
6. Elde edilen bu verinin başına tekrar IV eklenir ve iletilecek şifreli veri elde edilir. Şifreli verinin elde edilmesi şekil 3.4'te gösterilmiştir. Elde edilen bu verinin başına, alıcı ve vericinin MAC adresi eklenerek kablosuz ortama gönderilir.
7. Şifreli veri, karşı tarafta aynı işlemler tersi yönde uygulanarak açılır.



Şekil 3.4. WEP şifreleme akış diyagramı

Zayıflıkları:

- **Doğrulatma:** Ağı dinleyen saldırgan, erişim noktasından açık metin ve istemciden şifrelenmiş metni elde edebilir.

- **Tekrar saldırıları:** WEP'te tekrar saldırlar için herhangi bir güvenlik önlemi yoktur. Aynı mesaj defalarca gönderilebilir ve bu alıcı tarafından anlaşılamaz. Sisteme giriş yapan bir kullanıcı sistemden çıktıktan sonra dinlenilen mesajlar doğrulayıcıya gönderilirse araya giren kişi, mesaj içeriğini bilmese de kendini doğrulatabilir.

- **Bit değiştirme:** ICV bütünlük kontrol verisinin oluşturulma şeklinden kaynaklanmaktadır. ICV lineer bir metotla oluşturulup asıl verinin sonuna eklenip şifrelenmektedir.

- **IV'lerin tekrar kullanılması:** IV 24 bittir, 2^{24} den yaklaşık olarak 17 milyon farklı IV oluşabilir. Tekrarlanmadan birer artırarak kullanıldığında 802.11b standardına göre yaklaşık 7 saatte tüm IV'ler kullanılmış olacaktır [22].

- **RC4 Zayıf anahtarlar üretmesi:** RC4 algoritmasının anahtar üretim algoritması (Key Scheduling Algorithm) zayıf akış anahtarları üretmektedir. Bu zayıflıktan faydalanarak şifrelenmiş metinden akış şifresini buradan da anahtarı elde etmek mümkün olabilir. Anahtarların önce başlangıç bitleri ve daha sonra ardışık şekilde diğer kısımları çözülebilmektedir.

3.5.2. Wi – Fi korumalı erişim (WPA / Wi – Fi Protected Access)

Wi – Fi Protected Access (WPA), WEP'in zayıflıklarını gidermek amacıyla 2003 yılında Wi - Fi Alliance tarafından geliştirilmiştir. Wi- Fi Korumalı Erişim, TKIP algoritmasını kullanarak WEP'de var olan şifreleme zayıflıklarını güçlendirir ve şifreleme anahtarlarını otomatik olarak üretmek ve dağıtmak için bir yöntem sunar. Bu çözüm ayrıca, iletişimde alınıp verilen bilgi paketlerinin saldırganlar tarafından değiştirilmemesi için veriler üzerinde bütünlük denetimi de sunar. Kuruluş düzeyinde kullanıcı kimlik doğrulamasını geliştirmek için, Wi – Fi korumalı erişim ağdaki her kullanıcının kimliğini doğrular ve bu kullanıcıların aldatıcı ağlara katılmalarını engeller. WPA var olan teknolojileri temel alıp, 802.11i ile ileri doğru uyumluluk ve var olan 802.11 çözümleriyle geriye doğru uyumluluk sunarak, WEP ile ilgili zayıflıklara pratik bir çözüm sağlar [23].

WPA, WEP 'ye göre birçok yarar sağlar:

- WEP'den daha iyi güvenlik sağlar.
- Sadece yazılımda olacak değişiklikleri talep eder.
- Var olan donanıma uygulanabilir bir çözüm sağlar.
- WEP tabanlı istemcilere karıştırılmış (WPA/WEP) ağlarda işletim için izin verir [24].

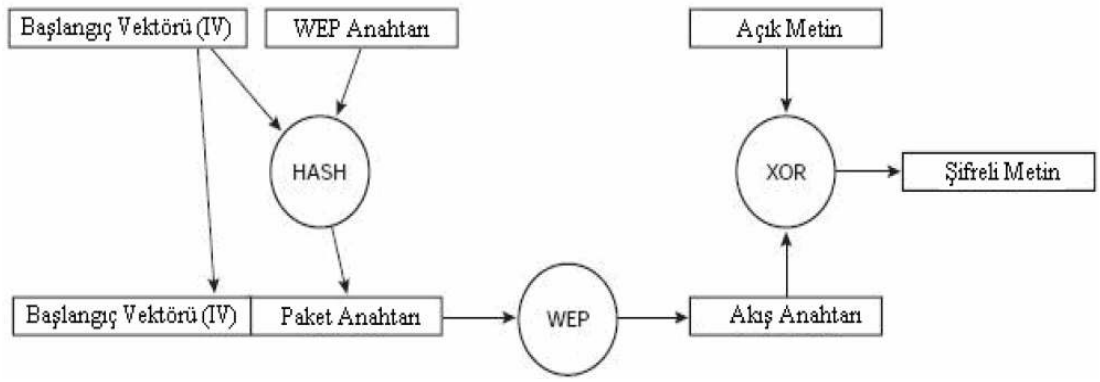
Geçici anahtar bütünlüğü protokolü (TKIP)

TKIP; WEP'in zayıflıklarını adreslemek ve var olan donanımı kullanarak daha güvenli WLAN için bir çözüm yolu sağlamak için geliştirilmiştir. TKIP; WEP'den daha fazla hesaplama gücü gerektirir, AES ve WPA2 'den daha az hesaplama gücü gerektirir.

TKIP özellikleri şunlardır:

- Her pakete yeni anahtar karıştırma fonksiyonu.
- Michael olarak adlandırılan yeni mesaj bütünlük kontrolü.
- Daha uzun başlangıç vektörü (WEP'de 24 bitken TKIP'da 48 bittir).
- Anahtarları yenileme mekanizması.

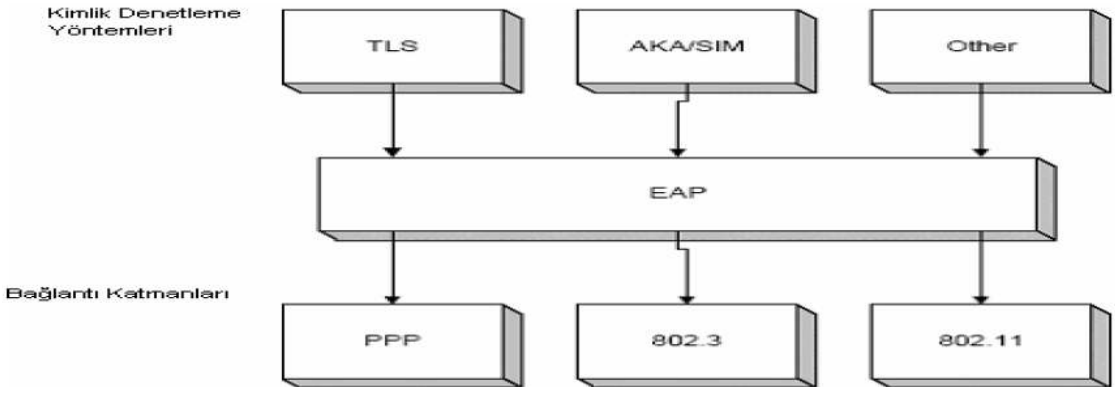
TKIP'de başlangıç vektörü 48 bit'e çıkarılmıştır. IV, hem paketlere sıra numarası vermek hem de her paket için tek kullanımlık anahtar üretiminde kullanılır. Paketlere sıra numarası vermek tekrar saldırılarını önlemek içindir. Ayrıca sırasız gelen paketler alıcı tarafından atılmaktadır [25].



Şekil 3.5. TKIP paket anahtarı oluşturma

Kimlik denetimi paket akışı (EAP)

Extensible Authentication Protocol (EAP) , geniş bir kimlik denetimi protokolü çeşitliliğini içeren genel bir kimlik denetleme paket akışıdır. Şekil 3.6 EAP paket akışının blok diyagramını göstermektedir. EAP, PPTP (Point To Point Tunneling Protocol) ile kullanım için geliştirilmiştir. 802.1X; EAP'ı kablosuz ağ için, ağın giriş kontrol mekanizmasının bir parçası olarak kullanmaktadır. Buna göre, EAP veri bağlantılarının geniş bir çeşitliğinin üstünde kullanılabilir [26].



Şekil 3.6. Kimlik denetimi paket akışı diyagramı

3.5.3. Çok güvenli ağ (WPA2 / Wi – Fi Protected AccessII)

IEEE 802.11 i standardı, son haliyle 2004 yılında IEEE tarafından onaylanmıştır. Bu protokol WEP üzerine kurulmamış yeni ve farklı bir yapı olarak geliştirmiştir. WEP'i desteklemez, WPA ile uyumlu olarak çalışmaktadır. WPA2; ön kimlik denetimini de destekler ve erişim noktasından erişim noktasına yeniden kimlik denetimi işlem zamanını yaklaşık 600 milisaniyeden 30 milisaniyeye indirir.

WPA2'de Kullanılan yöntemler genel hatlarıyla WPA'da kullanılanlarla aynıdır. WPA2'yi WPA'dan farklı kalan tek özellik ise şifreleme algoritmasında ortaya çıkmaktadır. RC4 şifreleme algoritmasından kaynaklanan zayıflıkları gidermek amacıyla, WPA2 farklı bir şifreleme algoritması kullanmaktadır. AES (Advanced Encryption Standard) adı verilen bu algoritma ile gerçekleştirilen şifreleme günümüzde tam bir güvenlik sunmaktadır. WPA2'de güvenlik AES şifreleme algoritmasını kullanan CCMP (Counter Mode – CBC MAC Protocol) protokolü ile sağlanır [23].

Gelişmiş şifreleme standardı (AES)

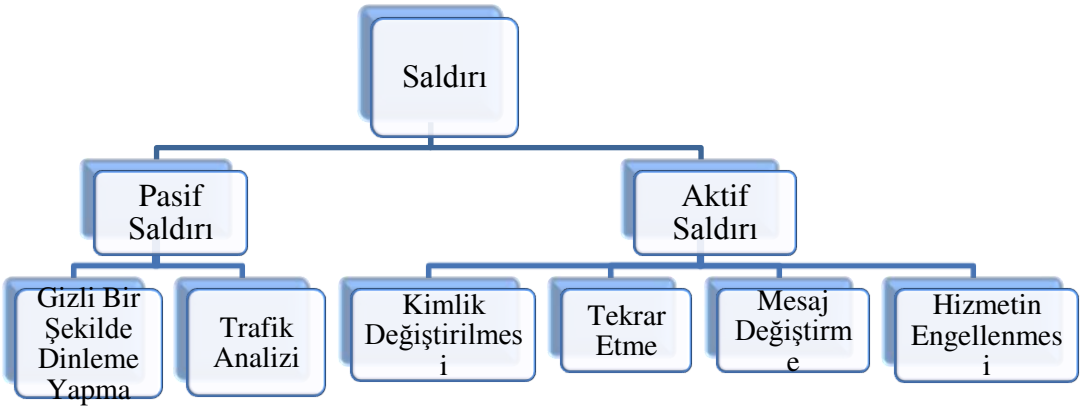
Bu standart; şimdiki Federal Information Processing Standart (FIPS) Şifreleme tanımlaması olan, DES'in (Data Encryption Standart) yerine tasarlanmıştır. AES; şimdiye kadar bilinen bir kusuru olmayan ve bütün şifre çözücülere karşı direnen çok güçlü bir şifreleme algoritmasıdır. Aşağıdaki çizelgede buraya kadar anlatılmış olan kablosuz güvenlik protokollerinin bir karşılaştırması verilmektedir [27].

Çizelge 3.2. WEP, WPA ve WPA2 ‘nin karşılaştırılması

Özelik	WEP	WPA	WPA2
Giriş Kontrolü	Yok	802.1x	802.1x
Kimlik Denetimi	Yok	EAP	EAP
Şifreleme Algoritması	RC4	TKIP	AES
Anahtar Bit Uzunluğu	40 bit veya 104 bit	128 bit şifreleme. 64 bit kimlik denetimi için	128 bit
Paket Anahtarı	Birbirine bağlı	Karışık fonksyon	İhtiyaç yok
Anahtar Yöntemi	Statik	802.1x + TKIP	802.1x + CCMP

3.6. Kablosuz Ağlarda Gereksinimler

802.11 WLAN veya Wi–Fi endüstrisi gelişmeye başlamıştır ve günümüzde önemli bir hıza sahiptir. Tüm göstergeler önümüzdeki yıllarda pek çok organizasyonun 802.11 WLAN teknolojisi kullanacağını göstermektedir. Dükkânlar, hastaneler ve hava alanları dâhil olmak üzere, pek çok organizasyon kablosuz hale gelmenin yararlarından faydalanmayı planlamaktadır. Ancak büyük gelişme ve başarı elde edilmiş olsa da, 802.11 WLAN’lar ile ilgili olan her şey pozitif olmamıştır. Organizasyonları güvenlik risklerine maruz bırakmış olan 802.11 kablosuz ağlara yapılan saldırıları tanımlayan basılı pek çok rapor ve çalışma vardır. Bu alt bölümde özet olarak güvenlik risklerine yapılan saldırıları kapsayacaktır [28]. Şekil 3.7 organizasyonlara ve kullanıcıların WLAN’lara karşı yapılan saldırılardan bazılarını anlamalarına yardım etmek için güvenlik risklerinin genel bir tanımını vermektedir.



Şekil 3.7. WLAN'lara karşı yapılan saldırılar

1. **Pasif saldırı**: Yetkisiz biri tarafından bir varlığa erişimin sağlandığı ve bu varlığın içeriğini değiştirmediği bir saldırıdır. Pasif saldırılar gizli bir şekilde dinleme yapma veya trafik analizi olabilir (bazen trafik akış analizi olarak da adlandırılır). Bu iki pasif saldırı aşağıda tanımlanmıştır.

    - **Gizli bir şekilde dinleme yapma:** Saldırgan mesaj içerikleri için aktarımları izler. Bu saldırının bir örneği iki iş istasyonu arasında bulunan LAN üzerinde dinleme yapma veya kablosuz bir telefon cihazı ile ana istasyon arasındaki aktarımlara giren bir kimsedir [29].

    - **Trafik analizi:** Saldırgan daha ustaca bir yolla haberleşme örüntüleri için aktarımları dinleyerek istihbarat elde eder. Haberleşen taraflar arasındaki mesaj akışında önemli miktarda bilgi bulunur.

2. **Aktif saldırı:** Yetkisiz tarafından bir mesajda, veri akışında veya dosyada değişiklikler yaptığı bir saldırıdır. Aktif saldırılar dört türdendir. Bu saldırılar aşağıda tanımlanmıştır.

    - **Kimlik değiştirilmesi:** Saldırgan yetkili bir kullanıcıyı taklit eder ve böylece belirli bazı yetkisiz ayrıcalıklara sahip olur.

- **Tekrar etme:** Saldırgan aktarımları izler ve uygun bir kullanıcı olarak mesajı tekrar gönderir.

- **Mesaj değiştirme:** Saldırgan uygun bir mesajı silerek, ekleme yaparak veya yeniden düzenleyerek değiştirir.

- **Hizmetin engellenmesi:** Saldırgan haberleşme araçlarının normal kullanımını veya yönetimini engeller. 802.11 ile ilişkili olan riskler bu saldırılardan birinin veya daha fazlasının sonucudur [29].

3.7. Kablosuz Ağlarda Güvenlik Açıkları

Kablosuz ağlarda zayıflıklar, sistemin tasarımı sırasında gözden kaçan, kötü tasarlanan sistemlerde bulunan veya sistem tasarımının bir parçası olan donanım veya yazılım kusurlarıdır. 1990 öncesi bu zayıflıklar bilişim ve ağ teknolojilerinde iyi bilinmiyordu ve genellikle ihmal ediliyorlardı. Ancak bilgisayar ağlarının çok yaygın bir şekilde kullanılmaya başlanması, onun güvenli bir hale getirilmesi ihtiyacını da beraberinde getirmiş ve zayıflıkların giderilmesi için bilimsel çalışmalara büyük maddi kaynaklar ayrılmıştır [30].

Ağlarda veri paketleri göndericiden alıcıya teller aracılığı ile switch (anahtar), router (yönlendirici) ve gateway (ağ geçidi) üzerinden iletilmektedir. Ağa bu donanımlar üzerinden fiziksel bir bağlantı kurabilen herhangi biri veri paketlerini toplayabilir, inceleyebilir, okuyabilir ve daha fazla olarak da bu verileri bozabilir veya silebilir. Ağlardaki bu zayıflıkları sınıflandırırsak:

***Paket çekme*:** Paket Çekme (packet sniffing), ağa iliştirilmiş bir aygıtta çalışan ve paket çekici (packet sniffer) olarak adlandırılan programlarla, bu aygıtın ağ bağdaştırıcısından geçen tüm veri bağlantı katmanı çerçevelerini alma işlemidir. Örneğin Ethernet ağlarında, Ethernet bağdaştırıcısının geçen tüm Ethernet

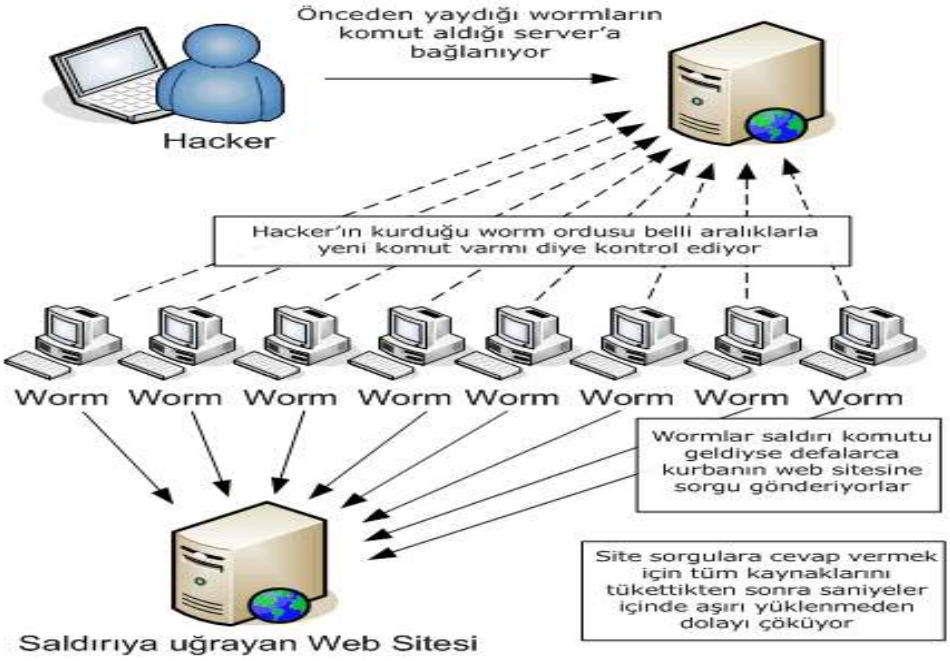
çerçevelerini alabilmesi için rastgele kipine ayarlanması gerektiğinden, Ethernet kartı olan herhangi bir bilgisayar, kolaylıkla bu tür bir program gibi kullanılabilir. Sonra bu çerçeveler, uygulama düzeyi verileri ayıklayacak uygulama programlarına aktarılabilir [31].

Paket çekme işlemi, ağın izlenmesi ve yönetimi için çok önemlidir, ancak kötü niyetli kişiler tarafından da kullanılabilir. Ayrıca, birçok web sitesinde bu tür programların hem ücretsiz, hem de ticari sürümleri vardır.

***Paket izleme*:** Ağdaki herhangi iki veya daha çok bilgisayar birbirleri ile iletişim kurarken birbirlerine yolladıkları paketler okunabilir, analiz edilebilir. Bu yöntemde yol alan paketler şifrelenmemiş iseler tam anlamıyla saldırıya açıktırlar. Eğer paketler şifrelenmiş ise de sadece iletişim kurulan alıcı tespit edilebilir ve aralarında ne kadar veri transferi yapıldığı, sıklığı tespit edilebilir.

***Hizmeti engelleme saldırıları (Denial of Service - DoS)* :** Bu tür saldırılar, bilgisayar ağlarına yönelik güvenlik tehditlerinin en yaygınlarıdır. Tahmin edilebileceği gibi bu tür saldırılar, bir bilgisayar ağını, ağda bir bilgisayarı ya da başka bir aygıtı kullanılamaz duruma getirmeyi amaçlar. Her ağ bilgisayarının hem bellek hem bant genişliği hem de işlem gücü anlamında belirli bir kapasitesi vardır ve bu kapasitenin gereksiz işlere kanalize edilmesi onun verimini büyük ölçüde düşürebilir [32].

DoS saldırıları birden çok paket yollayarak sistemi yavaşlatıp durdurmaya yöneliktir. Bazen bu paketler çok büyük ve içerisinde çalıştırılması istenen kodları içerebilir. Bu paketler ve kodlar sistemin yükünü arttırmakla beraber sistemin durmasına hatta kilitlenmesine yol açabilir. Şekil 3.8'de Denial of Service yapısını gösterilmiştir [33].



Şekil 3.8. Denial of service yapısı

Hizmeti engelleme saldırılarından korunmak oldukça zor olabilmektedir ve bu saldırılar doğrudan verilere yönelik olmasalar da, bilgisayar sistemlerinin görevlerini yapmalarını engelleyerek verilerin erişilebilirlik özelliklerini kaybetmelerini sağlayabilirler. Ayrıca "ortadaki adam saldırıları " gibi diğer saldırı yöntemleri için gereken ortamı oluşturmak amacıyla da kullanılabilirler [34].

Dağıtılmış hizmeti engelleme saldırıları (Distributed Denial of Service-DDoS) **:** DDoS saldırıları DoS saldırılarının gelişmiş bir türevidir. Bu yöntemde saldırgan girmek istediği bir ağın dışarıya açık bir servisini veya güvenlik duvarını, zombi bilgisayarlar kullanarak durdurup, ağa sızmaya olanak hazırlar [35].

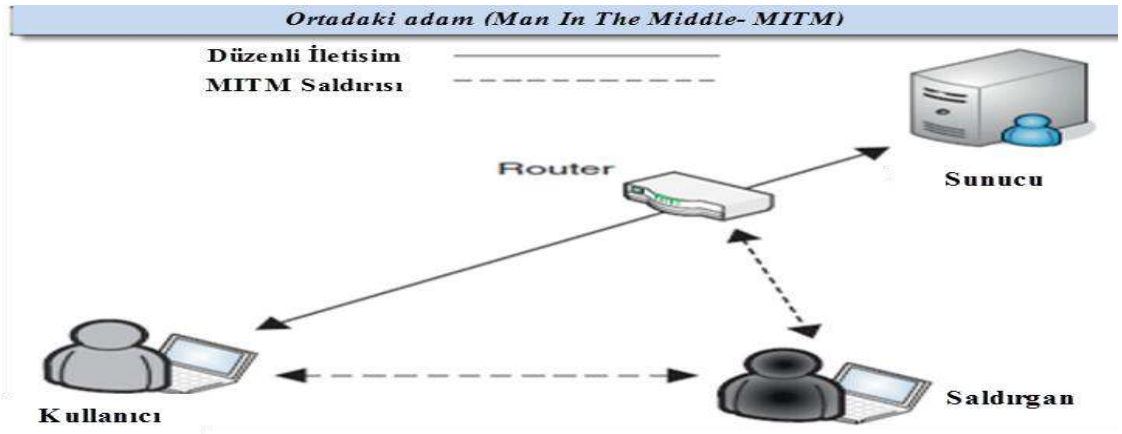
Zombiler, trojan ve virüs bulaştırılmış bilgisayar gruplarıdır ki saldırganlarca belli bir amaç için programlanabilir ve uzaktan kullanılabilirler. Zombi bilgisayarlar belli bir zamanda önceden belirlenmiş bir sisteme sürekli olarak sahte paket yollamaya başlarlar. Bu, saldırılan sistemde bir yüke sebep olur ve saldırgan için sistemi aşmak için en iyi zamandır. Günümüzde en çok kullanılan yöntemlerden biridir [36].

***Sahte AP*:** Bir güvenlik riskidir, kötü niyetli veya yetkisiz bir kullanıcı sahte AP'i gizli bir odaya, konferans salonundaki masanın altına veya bina içindeki diğer gizli bölgelere ekleyebilir. Sahte AP; yetkisiz kullanıcılar tarafından, ağa girmek için kullanılır ve kablosuz istemciler arasındaki kablosuz trafiği yakalayabilir. Bu yöntem basit ama teknik anlamda erişim çalma ve diğer saldırılara ön ayak olmada en etkilisidir. Kablosuz ağın yakınlarına aynı SSID ile başka bir AP kurulur. Ağa bağlanmak isteyen yetkili kullanıcılar, bu sahte AP'ye kullanıcı adı ve şifrelerini bildirecekler ve böylece saldırgan bu bilgileri elde edecektir. Saldırgan, bu yöntemde çok kolay bir şekilde ortadaki adam saldırılarını gerçekleştirebilir [37].

***Sahte kullanıcılar*:** Kablosuz ağlara diğer kullanıcıları izleyerek, MAC adreslerini alarak, sinyallerini kopyalayarak yetkisiz erişime sahip olabilirler.

Açık AP'ler: Birçok AP fabrika çıkışı açık şeklinde üretilirler. Bu AP'lerden erişim yetkilendirmeleri istenmez. Bu AP'ler sayesinde internet erişimi ve daha önemli ağa giren bir kapı elde edilir.

***Ortadaki adam (Man In The Middle- MITM)* :** Bazı bağlantılar, iki bilgisayar arasında birtakım güvenlik protokollerinin işletilmesinden sonra kurulur. Bu protokollerin işleme sürecinin iki taraf için de olumlu geçmesi, birbirlerine güvenmelerini ve güven içinde veri alışverişi yapmalarını sağlar. Ancak ağ paketlerini dinleyen birisi bu güveni suiistimal edebilir. Sonuçta ağı dinliyor olması ona paketlerin sıra numarasını, iki bilgisayarın da IP ve port numaralarını elde edebilme olanağı sağlar. Bu yöntemde saldırgan değişik yollardan birini kullanarak saldırdığı bilgisayardan gönderilen tüm paketleri kendisine yönlendirir ve kendisinden gelen paketleri veya cevap paketlerini dışarıdan geliyormuş gibi gösterir. Örneğin; kurban Microsoft'tan bir güvenlik paketi indirmek istediğinde saldırgan istediği herhangi bir dosyayı mesela virüslü veya sistemi bozan bir dosyayı kullanıcının indirmesini ve çalıştırmasını sağlayabilir. Şekil 3.9'da ortadaki adam saldırısında saldırganın durumunu gösterilmiştir [38].



Şekil 3.9. Ortadaki adam saldırısında saldırganın durumu

Ortadaki adam saldırılarında saldırgan iki nokta arasındaki iletişimi keserek, iletişim noktasından birini taklit eder ve diğer istemciyle bilgi alışverişine girer. Dinlediği ağdan elde ettiği paketten mesaj doğruluğunu belirleyen veriyi bozarak 2 nokta arasındaki iletişimi koparır. Yetkilendirilmiş kullanıcının paketleriyle kendini erişim noktasına doğrulatabilir [39].

Virüsler - Truva atları – solucanlar saldırı yazılımları: Tüm bu varyasyonlar basit bir mantıkla işlerler. Çalıştırılabilir kodu içeren dosyayı indir ve çalıştır. Kurbanlar çeşitli şekillerde e-posta, resim ve mp3 dosyası şeklinde bürünmüş dosyaları indirip çalıştırırlar ve kod sisteme sızmış olur.

Virüsler – Çalışma mantıkları biyolojik virüslere benzediği için bu ismi almışlardır. Virüsler için en basit anlamda, bilgisayar kaynaklarını kullanıp kendi kopyalarını üreterek yayılacak şekilde yazılmış kodlardır denilebilir. Bir virüs kodu, katlanarak artan bir yayılım hızına sahip olabilir. Ayrıca yazılımlara, donanımlara ve verilere zarar verebilir. Virüsler, daha hızlı yayılmak ve daha zor tespit edilmek için mümkün olduğunca küçük kodlar olmalıdırlar. Bu nedenle genellikle assembly veya c gibi dillerle yazılırlar.

Virüsler, 1960'lardan beri vardır, ancak bu yıllarda araştırma merkezlerinde deneme amacıyla kullanılmışlardır. 1986 yılında yazılan ilk PC virüsü Brain'den itibaren ise bugün bilinen virüslerin sayısı 60 bini geçmiştir, her ay da listeye 500 yeni virüs

eklenmektedir. Örneğin 1993'te, bilinen virüslerin sayısı 3.200 idi. Her gün 6-12 yeni virüs ortaya çıktığı tahmin edilmektedir. Ayrıca, önceki yıllara göre virüslerin yayılma hızları da çok artmıştır. Daha önce aylar ya da yıllar alan bu süreç, günümüzde dakikalar içinde tüm dünyaya yayılabilmektedir.

Truva atları **–** Adları, tarihi Truva kentinin ele geçirilmesi için kullanılan at şekilli büyük yapıdan gelmiştir. Çalışma stratejileri, bu yapıyla uygulanan stratejiye fazlaca benzemektedir. Truva atı yazılımları da tarihteki benzerleri gibi oldukça tehlikesiz görünmekte ancak içlerinde bilgisayarın kontrolünü ele geçirmek amacıyla yazılmış bazı özel kodlar barındırmaktadırlar. Truva atları da birer programdır. Amaçları, girdikleri bilgisayarı başkalarına açmaktır. Girdikleri sistemde, belirli bir kapının (port) açık tutulmasına ve bir programla sistemin denetlenebilmesine neden olurlar. Truva atları, temelde çalıştırılabilir dosyalardır (exe), yani çalıştırılmadıkları sürece zarar veremezler. Ancak son yıllarda bir dosyaya patch olarak eklenip gönderilebilmektedirler.

Solucanlar **–** Ağ üzerindeki yazılım veya donanım anlamındaki zayıflıkları suiistimal ederek kendisini yayan yazılımlardır. Onları diğer zararlı yazılımlardan ayıran özellikleri de budur. Solucanlar, ağ üzerinde yayılmak için virüsler gibi herhangi bir programa yerleşip kullanıcının kendisini çalıştırmasına ihtiyaç duymazlar. Solucanlar, Truva atları gibi birilerinin kendilerini başka bir bilgisayar göndermesine gerek yoktur. Solucanlar için gerekli olan tek şey, ortamda suiistimal ederek kendisini yaymasını sağlayacak bir hata veya zayıflıktır.

3.8. Kablosuz Ağlara Yapılan Saldırılar

Kablosuz ağlar için geliştirilen farklı güvenlik mekanizmalarına rağmen, onlara saldırı için birçok yol vardır. WEP, WPA ve WPA2'ın açıklarından yararlanılarak yapılan saldırılar bilinmektedir. Bu saldırıları gerçekleştirmek için birçok araç mevcuttur.

3.8.1. WEP'e yapılan saldırılar

WEP güvenlik açıklarının temelinde kimlik doğrulama ve şifreleme anahtar yönetiminin zayıf olması yatar. WEP anahtar yönetiminin zayıflığı, tüm terminallere statik olarak elle atanıp, her trafik aktarımında değiştirilmeden kullanılmasından kaynaklanır. Bu duruma ilaveten, alıcı tarafta verinin yeniden sıralanabilmesi için kullanılan IV değerinin 24 bit olması ve her paket gönderiminde IV değerinin sırayla artarak belirli bir trafik hacmine ulaşılınca kendini tekrarlaması, anahtar yönetimi daha da zayıf hale getirir. Çok sayıda kullanıcıya sahip olan ve üzerinde ciddi trafik akışı olan WLAN'lar için yeterli sayıda tekrarlanan IV'leri elde etmek nispeten daha kolay bir iştir. WEP ile şifrelenmiş kablosuz ağlara karşı yapılan iki tür saldırı yöntemi vardır. Birincisi zayıf IV'lerin toplanmasına; ikincisi ise tekrar etmeyen IV'lerin toplanmasına ihtiyaç duyar [40].

Zayıf IV kullanımına karşı yapılan saldırılar

WEP'in RC4 şifreleme algoritmasını kullanmasından ileri gelen zayıflıkları temel alır. Şifrelenmiş paketler içindeki IV'ler toplanarak WEP anahtarının elde edilmesi şeklinde çalışır. Toplanan IV'ler içinden tekrar edenlerin incelenmesi prensibine dayanır. 5 milyon şifreli paket içinden süzülmüş 3.000 zayıf IV toplanarak WEP anahtarı başarıyla elde edilebilmektedir. Zayıf IV'ler toplandıktan sonra, şifreleme aşamaları ters yönde uygulanarak anahtarın ilk byte'ı elde edilir. Bu işlem WEP anahtarı ele geçirilene kadar her byte için tekrarlanır [41].

IV'ye karşı vuruş saldırıları

Vuruş saldırıları, yeterli sayıda şifreli paket toplanması esasına dayanır. Vuruş saldırılarının bir yöntemi olarak, tekrar etmeyen IV'ler toplanarak paketin son byte'ı paketten çıkarılır ve anahtar doğru bir şekilde tahmin edilmeye çalışır. Son byte ICV bitlerini içerir. Son byte 0 olduğunda, paket içindeki son 4 byte ile XOR işlemine tabi tutularak ICV bitleri ele geçirilebilir. Sonra bu paket tekrar gönderilerek şifresi kırılır.

3.8.2. WPA'ya yapılan saldırılar

WPA'ya yapılan saldırılarda WEP'te olduğu gibi çok sayıda paket toplamaya ihtiyaç yoktur. Önemli bir nokta da; WPA'ya karşı yapılan saldırıların başarılı olması için WPA'nın ön paylaşımlı anahtar (PSK) modunda çalışıyor olması gerektiğidir. WPA-PSK'ya karşı başarılı bir saldırı gerçekleştirmek için EAPOL mesajlarını (dörtlü anlaşma mesajları) yakalamak gerekir. Bu mesajları yakalamak için yetkili bir asılama işleminin yapılması beklenebilir ya da asıllanmamış paketleri AP'ye bağlanmış istemcilere göndererek yeni bir asılama işlemi için zorlanabilir. Yeniden asılama yapılırken de EAPOL mesajları yakalanabilir [45].

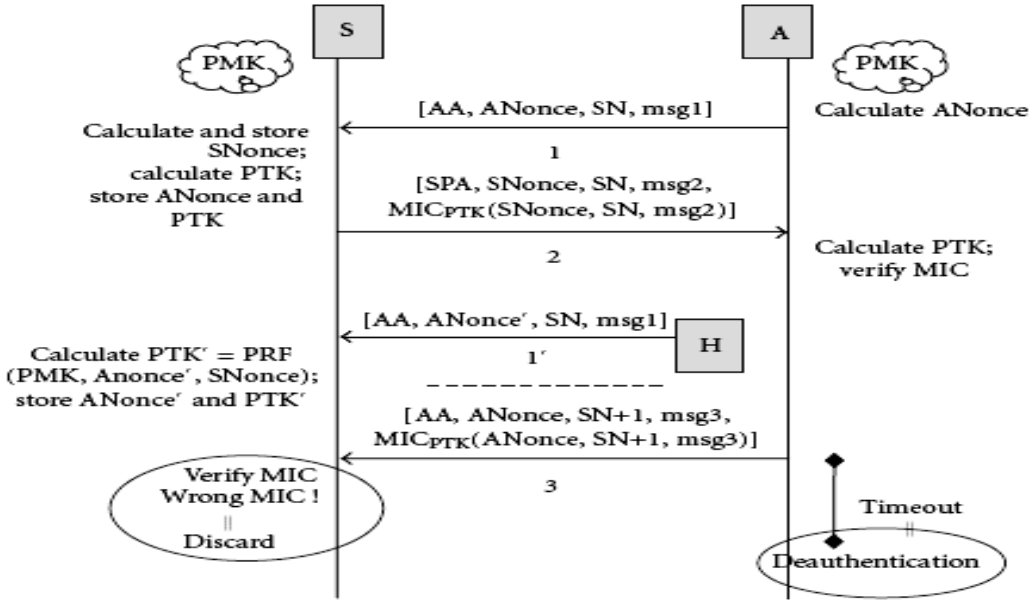
Bu tür saldırıların başarılı olması ihtimallere bağlıdır ve başarı için PSK anahtarının 21 karakterden az olması gerekir. Ancak bazı anahtar sözlükleri ile bu sınır genişletilebilir. Bu tür anahtar sözlükleri piyasada ücretsiz olarak temin edilebilmektedir [42].

Dörtlü anlaşma(Handshake) protokolüne yapılan DoS ve DoS taşma saldırılar

Dörtlü anlaşma protokolünün zayıflığı Msg1 mesajından kaynaklanmaktadır. Çünkü bu mesaj veri bütünlüğünü sağlayacak olan MIC değerini içermez. Asıllayıcıdan kullanıcıya gönderilen Msg1 mesajı, saldırgan tarafından elde edilerek ANonce, SN ve mesaj tipi bilgileri belirlenebilir. Saldırgan (H), Msg2 mesajı gönderildikten sonra araya girerek Msg1 mesajına benzer bir mesajı ($Msg1'$) kullanıcıya tekrar gönderir. Bu yeni $Msg1'$ değeri Msg1 değerinden sadece ANonce değeri bakımından farklıdır. Çünkü ANonce değeri rastgele üretilen bir değerdir. Bu noktada kullanıcı, saldırgan tarafından gönderilen bu yeni mesaja tepki olarak yeni bir PTK değeri (PTK') hesaplayacak ve yine bununla ilişkili olan $Msg2'$ mesajını asıllayıcıya gönderecektir. Asıllayıcı $Msg2'$ mesajını dikkate almayacak ve Msg3 mesajını kullanıcıya gönderecektir. Bu noktada kullanıcı, en son hesapladığı PTK' değeri ile Msg3 mesajını denetleyeceği için ve bu işlem sonucunda bir eşitlik sağlanamayacağı için Msg3 mesajını reddedecektir. Belli bir zaman sonunda asıllayıcı Msg4 mesajını alamadığı için Msg3 mesajını tekrar göndermeyi deneyecektir. Ancak cevap alması

mümkün değildir ve belli bir deneme sonunda asılama işlemi iptal edilecektir. Bu durum şekil 3.10'da gösterilmiştir [43].

Kullanıcı her bir Msg1 mesajını aldıktan sonra ANonce ve PTK değerlerini saklamaktadır. Saldırgan DoS taşma saldırıları ile çok sayıda saldırıda bulunduğunda kullanıcı çok sayıda ANonce ve PTK değerini saklamak zorunda kalacak ve bu da kullanıcı tarafında bellek yorulmasına ve kilitlenmelere sebep olacaktır [44].



Şekil 3.10. Dörtlü anlaşmaya karşı DoS saldırısı

Dörtlü anlaşmada, 3 tür mesaj tanımlanmıştır. Bu mesajlar:

Msg1 : [AA, ANoce, SN,Msg1]

Msg2 : [SPA, SNonce, SN,Msg2,MIC(SNonce, SN,Msg2)]

Msg3: [AA, ANonce, SN+1, Msg3, MIC (ANonce, SN+1, Msg3)]

S: Kullanıcı,

A: Asıllayıcı,

MIC: Mesaj bütünlük kodu,

AA: Asıllayıcının MAC adresi,

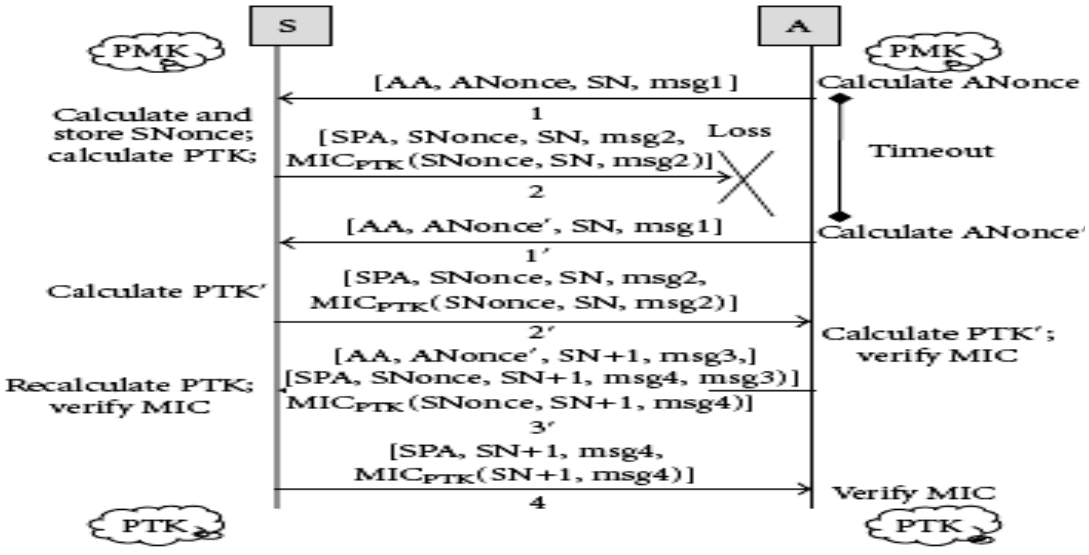
SPA: Kullanıcının MAC adresi,

ANonce: Asıllayıcı (Erişim noktası) tarafından üretilen rastgele bir değer,

SN: Mesajın sıra numarası.

WPA2 standardı ile bu saldırılara karşı önlemler alınmıştır. WPA2 ile Msg1 mesajı içine PMKID adı verilen yeni bir alan eklenir. PMKID değeri, PMK, AA ve SPA değerlerinin 128 bit SHA harmanlama (hash) fonksiyonu ile elde edilmektedir. Saldırgan PMK değerini bilmediği ve SHA fonksiyonunu tersine çeviremeyeceği için Msg1 mesajın kullanıcıya gönderemez. Bu şekilde WPA2 ile DoS saldırıları engellenmiş olur [43].

WPA2 ayrıca bellek yorgunluğu problemine de çözüm getirmiştir. Bu çözüm gereği kullanıcı şu şekilde davranmaktadır: Msg1 mesajını aldıktan sonra SNonce değerini üretir, PTK değerini hesaplar ve Msg2 mesajını asıllayıcıya gönderir. Fakat ANonce ve PTK değerini saklamaz. Bunun yerine sadece SNonce değerini saklar. Her bir yeni Msg1 mesajını aldığında ise yeni bir PTK değeri hesaplar. Msg3 mesajını aldıktan sonra da yine bu mesajla gelen ANonce değeri ve daha önceden saklamış olduğu SNonce değerini kullanarak PTK değerini hesaplar. Hesaplanan bu PTK değeri ile MIC değeri kontrol edilir ve asılama işlemi tamamlanır. Bu uygulama sayesinde Msg2 mesajı kayıp olsa dahi asılama işlemi tamamlanabilmektedir. Şöyle ki; Msg2 kaybolduktan belli bir süre sonra, asıllayıcı yeni Msg1 mesajını (Msg1/) yeni bir ANonce değeri (ANonce/) ile birlikte kullanıcıya gönderir. Bu izin verilen bir durumdur ve kullanıcı tarafından kabul edilecektir. Şekil 3.11'de bu asılama işlemi gösterilmiştir [42] .



Şekil 3.11. WPA2 ile DoS saldırılarından korunma ve asılama işleminin yapılması

4. YAPILAN ÇALIŞMA

IEEE 802.11 kablosuz ağlar için güvenlik standartlarını belirler. Ayrıca, WLAN'larda kablosuz veri ve güvenlik sistemleri için güçlü kriptolama teknolojileri, kriptoyu çözme, kimlik denetimi ve anahtar yönetim stratejilerini belirler. Bu çalışmanın temel amacı kablosuz ağ güvenlik seçeneklerinin gözden geçirilmesi ve özellikle WPS, WPA ve WPA2 güvenlik standartlarının açıklarını ortaya çıkarmaktır.

4.1. Kablosuz Ağlarda Linux Tabanlı Sistemler

Linux 1991 yılında Linus Torvalds adında bir üniversite öğrencisi tarafından geliştirilmiştir. UNIX tabanlıdır ve UNIX'in bir türevidir. Açık kaynak kodlu ve özgür bir yazılımdır. Böylece tüm dünyadaki programcılar tarafından geliştirilmiş ve yaygınlaşmıştır. Ağ işletim sistemi olarak da yaygın bir şekilde kullanılmaktadır. Linux sistemler kablosuz ağ yapılandırması için zengin seçeneklere sahiptir. Her Linux dağıtımının kendi grafik ara birimli yapılandırması olduğu gibi tüm Linux dağıtımları için geçerli komutları kullanmak da her zaman hazır olarak durmaktadır.
Linux, internet üzerinde ilgili ve meraklı birçok kişi tarafından ortak olarak geliştirilmekte olan ve başta IBM – PC uyumlu kişisel bilgisayarlar olmak üzere birçok platformda çalışabilen ve herhangi bir maliyeti olmayan bir işletim sistemidir.
Linux gerçekten son yıllarda hızlı bir gelişme göstermiş, çeşitli ülkelerden birçok kullanıcıya erişmiş ve yazılım desteği günden güne artmıştır. Değişik kuruluşlar Linux sistemi ve uygulama yazılımlarını bir araya getirerek dağıtımlar oluşturmuşlar ve kullanımını yaygınlaştırmışlardır [46].

4.1. BackTrack 5

BackTrack, program değildir. Offensive Security Grubu tarafından geliştirilen tamamen özgür olan bir işletim sistemidir. Hacking denilince akla gelen ilk Linux yazılımıdır. Aslında güvenlik uzmanları tarafından ağ ve sistem güvenliğini sağlamak amacıyla kullanılmaktadır.

BackTrack, içinde birçok gelişmiş araç barındıran, sistem ve ağlarda bulunan güvenlik açıklarını test etmek için, diğer bir ifade ile penetrasyon (sızma); hedef sistem ve ağdaki zayıflıkları kullanarak sisteme sızmaya çalışma simülasyonudur [47]. Bu şekilde sistemdeki zayıflıkları raporlanarak tedbir alınması sağlanır. Testlerinde kullanılmak üzere oluşturulmuş, Debian / Ubuntu tabanlı bir Linux dağıtımıdır. Uzmanlarının sıklıkla kullandıkları bir denetim platformudur.

Şekil 4.1. BackTrack arayüzü

Hackerlerin kullandıkları teknikler kullanılarak hedef sistem ve ağdaki güvenlik zafiyetleri açığa çıkarlara raporlama yapılıp tedbir alınması sağlanır. Sayısal dünyadaki gerçek saldırıların aynısı simüle edilerek, bir hackerin yapabileceği tüm saldırı senaryoları uygulanabilir [47].

BackTrak'te bulunan araçların her biri pratik kullanım şekil ve saldırı tekniklerinin uygulanmasındaki başarılarıyla ön plana çıkmaktadır. Zaten üstün özellikleri bulunan bu Linux dağıtımının amacı da budur.

BackTrack, literatürde hack machine diye geçen içinde bir pentesterin (sistem mühendisinin) ihtiyaç duyabileceği neredeyse bütün yazılımların olduğu bir sistemdir. Bu yazılımların hepsini kullanmak mümkün değildir, BackTrack'in release ekibi bile tam anlamıyla tüm özelliklerini kullanamamaktadır. Örnek olarak bir tarayıcı kit içindeki bütün tarama araçlarının ne işe yaradığını ezbere bilmek (tam anlamıyla, kendi yazmış gibi) mümkün değildir. Bu uygulamalar temel olarak iki kategoride incelenir.

1-Tarama amaçlı (scan)

2-Saldırı amaçlı (attack)

Bu zamana kadar tüm BackTrack versiyonları milyonlarca kullanıcı tarafından indirilmiştir. Çok da eski olmayan tarihsel sürece baktığımızda, ilk BackTrack dağıtımının 26 Mayıs 2006 tarihinde, BackTrack 1.0 Beta adıyla yayınlandığını görürüz. Daha sonra 6 Mart 2007 (BackTrack 2 Final), 19 Haziran 2008 (BackTrack 3 Final), 9 Ocak 2010 (BackTrack 4), 8 Mayıs 2010 (BackTrack 4 R1), 22 Kasım 2010 (BackTrack 4 R2), 10 Mayıs 2010 (BackTrack 5), 20 Ağustos 2011 (BackTrack 5 R1) ve 1 Mart 2012 (BackTrack 5 R2) şeklinde bir tarihsel süreçle şu anki son haline gelmiştir ve geliştirilmesine devam edilmektedir [49].

4.2. BackTrack Test Metodolojisi

BackTrack5, bünyesinde barındırdığı yüzlerce pentest aracı ile güvenlik profesyonelleri için çok önemli bir platformdur. Bu araçları kullanmak için de bir metot belirlenmeli ve bu metoda göre düzenli bir çalışma sağlanmaktadır. Şimdide bu metotları inceleyelim.

1. Hedef Belirleme: İlk olarak bir hedefin olması gerekir. Bilgisayar korsanları da işe ilk olarak hedef belirleyerek başlarlar.

2. Bilgi Toplama: Hedef sistem hakkında bilgi toplanmalıdır. Güvenlik uzmanı, kamuya açık kaynaklardan hedef hakkında genel bilgiler toplar. Bu kaynaklar; internet kaynakları, forumlar, sosyal paylaşım siteleri şeklinde sıralanabilir. BackTrak'te tüm bu kaynaklardan bilgi toplamak için araçlar bulunmaktadır.

3. Keşif: Hedef sistem hakkında toplanan bilgilerden yararlanarak keşif yapılır. Hedef sistemin ağ yapısı, kullanılan güncel teknolojiler, aktif sistemler ve kullanılan işletim sistemleri gibi bilgiler elde edilir.

4. Hedef Hakkında Elde Edilen Bilgilerin Kategorileşmesi: Bu aşamaya kadar elde edilen bilgiler kullanılarak sistemli bir gruplama işlemi yapılır.

5. Zayıflıkların Haritalanması: Bu aşamada hedef sistemde bulunan açıklık ve zayıflıklar tespit edilerek bir şablon oluşturulur.

6. Sosyal Mühendislik: Sosyal mühendislik, insanların güven duygusunu sömürerek istenilen bilgilere ulaşma metodudur. Sistemlerde bulunan en önemli zayıflık, insan psikolojisinin manipüle edilmesiyle oluşur. BackTrack5 işletim sisteminde sosyal mühendislik saldırılarında kullanılan birçok araç bulunmaktadır.

7. Hedefin Exploit Edilmesi: Keşfettiğimiz açıkları analiz ettikten sonra, bu açıkları kullanarak sisteme yetkisiz erişim sağlamaya çalışabiliriz. Bu aşama saldırının en tehlikeli aşamasıdır. BackTrack 5'te gelişmiş exploit araçları bulunmaktadır.

8. Yetki Yükseltme: Sisteme erişimi sağladık fakat normal kullanıcı (user) haklarına sahibiz. Ama biz yönetici haklarına sahip olup sistemde tam

anlamıyla etkin olmak ve istediğimiz değişiklikleri yapmak istiyoruz. Windows sistemlerde Administrator, Linux sistemlerde ise Root en yetkili kullanıcıdır. BackTrack 5'te bunun için çeşitli metotlar bulunmaktadır.

9. Erişimi Devam Ettirme: Bu aşamada yapılması gereken şey sisteme istediğimiz zaman girip çıkabileceğimiz ve uzun süre kendimizi ele vermeden kullanabileceğimiz bir yol bulmak.

10. İzleri Temizleme: Sistemde güvenliğe yardımcı olması ve yanlış kullanımların raporlanabilmesi için kayıt altına alma mekanizması çalışmaktadır. Bir hacker sisteme kaçak giriş yaptığı zaman sistemde yaptığı eylemler loglanmaktadır. Hacker, yasal suçlamalara maruz kalmamak ve sisteme erişimini uzun süre devam ettirebilmek için bu log dosyalarını silmeye çalışacaktır.

11. Dokümantasyon ve Raporlama: Güvenlik testlerini yaptığınız sistem / kurumdaki idari ve teknik ekip, penetrasyon yöntemi ve bulunan zayıflık ve açıklıkları incelemek isteyecektir. Çünkü güvenlik boşluklarını görüp buna uygun tedbirler alacaktır. Bunun için de test süreci ve sistem zayıflıkları, güvenlik zafiyetleri ayrıntılı olarak belgelendirilmeli ve raporlanmalıdır.

Şekil 4.2. BackTrack test metodolojisi

4.3. Test Amaçlı Kablosuz Ağ Ortamının Kurulumu

Wireless penetration testi uygulanabilir bir konudur ve öncelikle bu tezdeki tüm farklı deneyleri güvenilir ve kontrol edilebilir bir ortamda deneyebilmek ve sonra da gerçek hayatta uygulamak önemlidir.

Bu kısımda aşağıdakiler incelenecektir:

- Donanım ve yazılım gereksinimleri
- Bir erişim noktası kurmak ve ayarlamak
- Kablosuz ağ kartının kurulumu

- **Donanım gereksinimleri**

Kablosuz ağları kurmak için aşağıdaki donanıma ihtiyaç duyulmaktadır:

- Dahili kablosuz kartı olan iki laptop: Bunlardan biri laboratuvardaki kurban olarak, diğerini de penetration yapan laptop olarak kullanılacaktır. Aslında herhangi bir laptop bu iş için uygun olsa da, en az 3 GB RAM'i olan bir laptop istenmektedir. Bunun nedeni, pek çok hafıza gerektiren deney gerçekleştiriyor olmamızdır.

- Alfa kablosuz adaptör: Packet injection ve packet sniffing destekleyen ve BackTrack'in desteklediği bir USB Wi-Fi karttır. Tezde Alfa AWUS036H kartı kullanılmıştır.

- Erişim noktası: WEP/WPA/WPA2 standartlarında şifreleme destekleyen herhangi bir erişim noktası. Bu tez uygulamasında D-LINK DIR- 600 N Router kullanılmıştır.

- **Yazılım gereksinimleri**

Kablosuz laboratuvarı kurabilmek için aşağıdaki yazılıma ihtiyaç bulunmaktadır:

- BackTrack 5 resmi sitesinden indirilebilir. http://www.backtrack-linux.org.

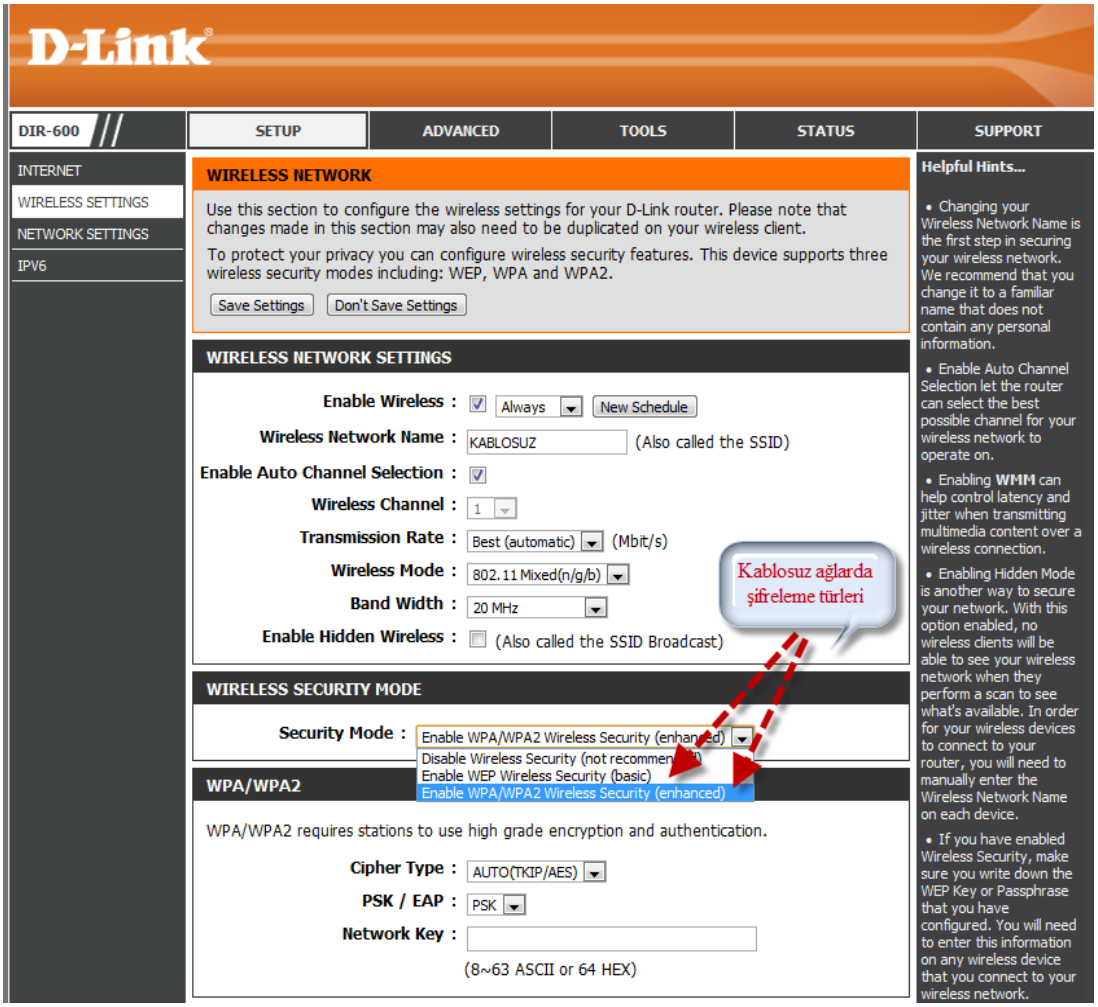
- Windows XP/Vista/7: laptoplardan birinde Windows'un bu versiyonlardan biri kurulu olmalıdır. Bu laptop kurban laptop olarak kullanılmaktadır.

Şekil 4.3. Donanım gereksinimleri gösterilmektedir

- **Erişim noktasının ayarlanması**

Erişim noktasının yayın yaptığı kablosuz ağ SSID'si (Service Set İdentifier) açık kimlik doğrulama kullanarak ayarlanmıştır. Erişim noktasının ayarlarının yapılabilmesi içim Ethernet kablosu kullanılarak diz üstü bilgisayar ile erişim noktası birbirlerine bağlanır. Diz üstü bilgisayarın internet tarayıcısına erişim noktasının IP adresi girilir. DIR -600 için 192.168.0.1 olarak girilecektir.(IP adresini bulmak için erişim noktanıza ait kullanım kılavuzunu kullanılabilir). Erişim noktasına ait kılavuz doküman yoksa route –n bağlanıldığında bir konfigürasyon portal görülecektir.

Login olduktan sonra farklı ayarları incelendiğinde yeni bir SSID ayarlamak için gereken ayarlar bulunacaktır.



Şekil 4.4. Kablosuz ağlarda şifreleme türleri ve erişim noktasını ayarlamak

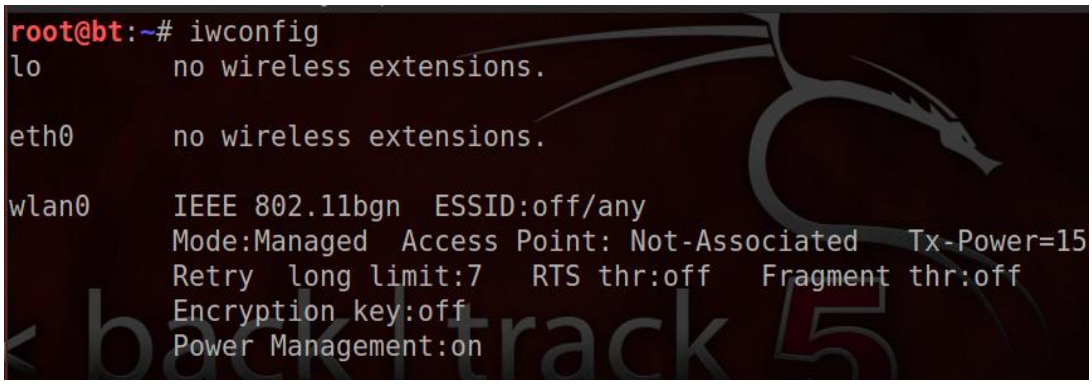
Benzer şekilde kimlik doğrulama ile ilgili olan ayarlar bulunmalıdır ve ayarı açık kimlik doğrulama olarak değiştirilmelidir. İncelediğimiz durumda, güvenlik modu ayarı “None” olarak ayarlanmıştır (açık kimlik doğrulama olması için).

Erişim noktası ayarları kaydedilmeli ve gerekiyorsa yeniden başlatılmalıdır. Bundan sonra erişim noktası SSID kablosuz ile açık ve çalışıyor olacaktır. Bunun doğrulamanın kolay bir yolu Windows’taki wireless configuration menüsünü kullanmak ve erişilebilir ağları gözlemlemektir. Kablosuz ağ, listedeki ağlardan biri olarak görülmelidir. Böylece, erişim noktası SSID kablosuz ile başarıyla kurulmuştur. Erişim noktasının sınırları içerisinde yayın yapmakta olduğunu Windows laptop üzerinden görebilmektedir.

Monitör modu için arayüz yaratmak

Alfa kartı görüntüleme moduna alınmalıdır.

1. BackTrack'a Alfa kartı bağlı olarak giriş yapılır. Konsol içinde olduktan sonra, iwconfig komutuyla kartınızın algılandığı ve sürücülerin doğru yüklendiği kontrol edilmelidir.

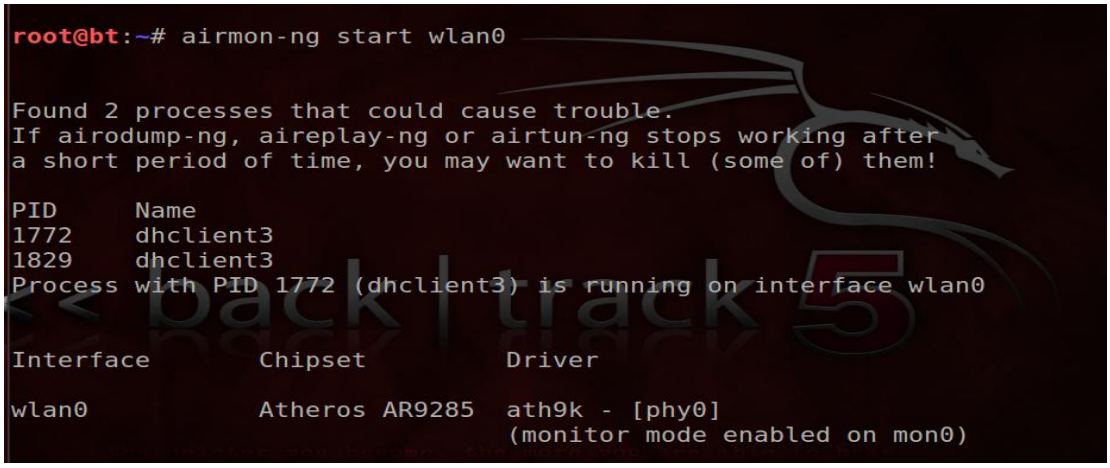


Şekil 4.5. iwconfig komutu ile kablosuz ağ sürücüsünün doğrulanması

2. Kartı görüntüleme moduna sokmak için, airmon –ng aracını kullanırız. Önce airmon –ng komutunu uygun olan kartları bulması için kullanılmıştır. Wlan0 arayüzünü listede görüntüleniyor olmalıdır.

Şekil 4.6. Wlan0 arayüzü

3. Airmon –ng start wlan0 komutu kullanarak, wlan0 ait görüntüleme modu arayüzü oluşturulmalıdır. Bu yeni görüntüleme modu arayüzü mon0 adında olacaktır. Bu ara yüzün yaratıldığını, airmon –ng komutu tekrar kullanılarak doğrulanabilir.

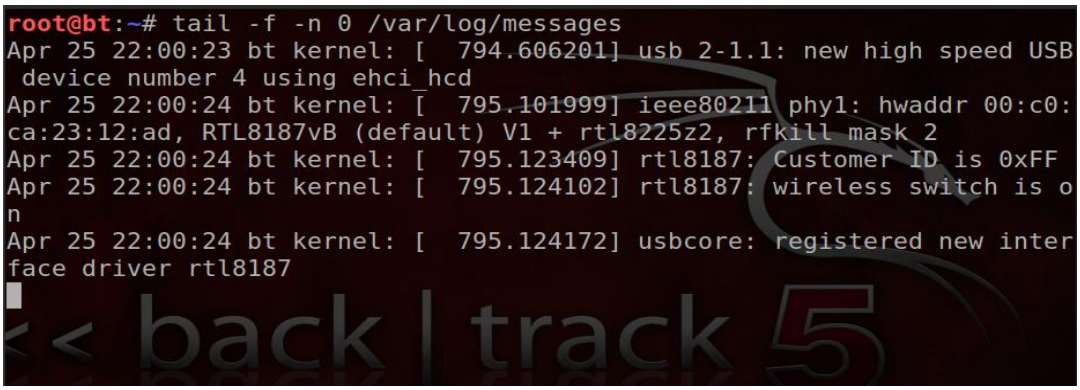


Şekil 4.7. Wlan0 görüntüleme modu ara yüzü oluşturmak

Alfa Kartını Denemek:

Aşağıdaki adımlar takip edilmelidir

1. Bilgisayar yeniden başlatılmalı ve alfa kartı henüz bağlı olmamalıdır.
2. Login olduktan sonra kernel mesajları tail komutuyla takip edilmelidir.
3. Alfa kartı yerleştirildiğinde, aşağıdaki gibi bir ekranla karşılaşılacaktır. Bu kartınıza uygulanan varsayılan kuralların gösterildiği ayarlardır.



Şekil 4.8. Alfa kartının yerleştirildiğinin gösterilmesi

4.4. WLAN Kriptolama Akışları

WLAN kriptolama mekanizmaları kripto grafik saldırılara karşı savunmasız olmaları ile ünlü uzun bir geçmişe sahiptir. Bu, 2000 yılının başlarında WEP ile başladı ve tamamen kırıldı. Yakın zamanlarda, saldırılar yavaş yavaş WPA'yı hedef almaktadır.

Her ne kadar, WPA'yı tüm koşullarda kıracak genel anonim bir saldırı olmasa da, özel durumlarda uygulanabilir bazı saldırılar vardır.
Bu bölümde, aşağıdakiler incelenecektir.

- WLAN'daki farklı kriptolama şemaları
- WEP kriptolamayı kırmak.
- WPA kriptolamayı kırmak.

4.5. WLAN Kriptolama Şemaları

WLAN'lar havadan veri gönderirler ve bu yüzden veriyi korumak için bir ihtiyaç bulunmaktadır. Bu en iyi kriptolama ile gerçekleşir. WLAN komitesi(IEEE 802.11) veri kriptolama için aşağıdaki protokolleri gerçekleştirmiştir.

WEP (Kablolu Eşdeğer Gizlilik)
WPA (Kablosuz Korumalı Erişim)
WPA2 (Kablosuz Korumalı Erişim Versiyon 2)

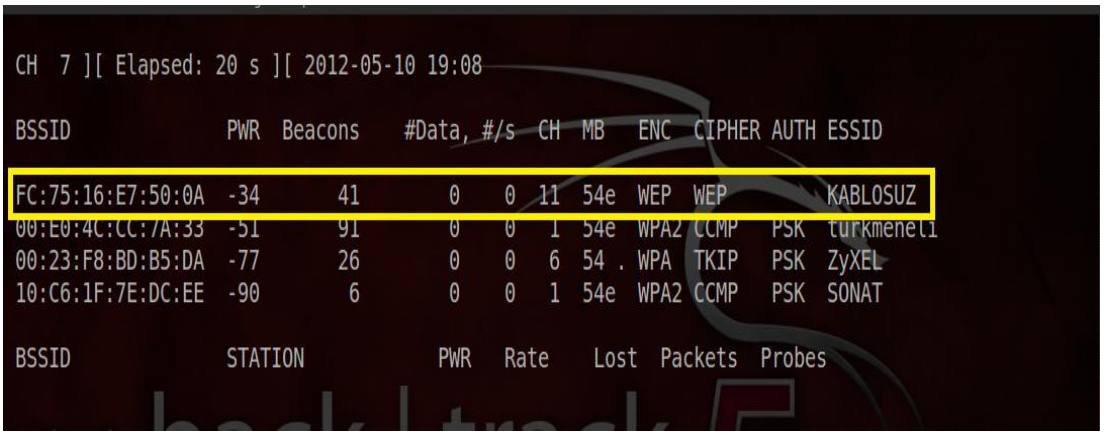
Burada bu kriptolama protokollerini ve bunlara yapılan olası saldırıları incelenmiştir.

4.6. WEP Kriptolamayı Kırmak

WEP protokolü 2000 yılında hatalı olarak bulunmuş olmakla beraber, yine de kullanılmakta ve erişim noktaları hala WEP kabiliyetleri olarak piyasaya sürülmektedir. WEP'te oldukça fazla kripto grafik zayıflıklar bulunmaktadır ve Walker, Arbaugh, Fluhrer, Martin, Shamir, Korek ve diğerleri tarafından keşfedilmişlerdir.

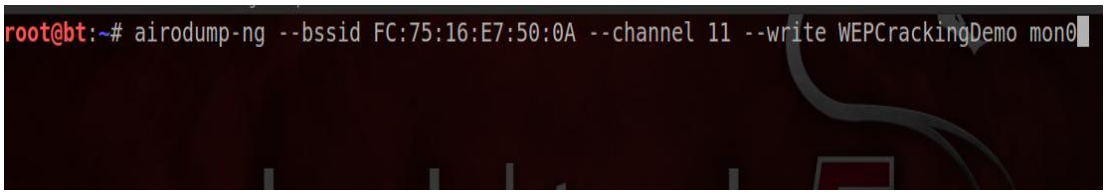
Burada, WEP kriptolamasını BackTrack platformundaki hazır uygulanabilir araçlar kullanılarak nasıl kırılacağı incelenecektir. (airmon-ng, aireplay-ng, aircrack-ng ve diğer komutları kullanılarak)

1. airodump -ng komutunu KABLOSUZ erişim noktamızın yerini bulmak için airodump -ng mon0 komutunu kullanarak çalışmaktadır. Ekran görüntüsünde görüldüğü üzere, KABLOSUZ erişim noktasının WEP ile çalıştığı görülebilir.



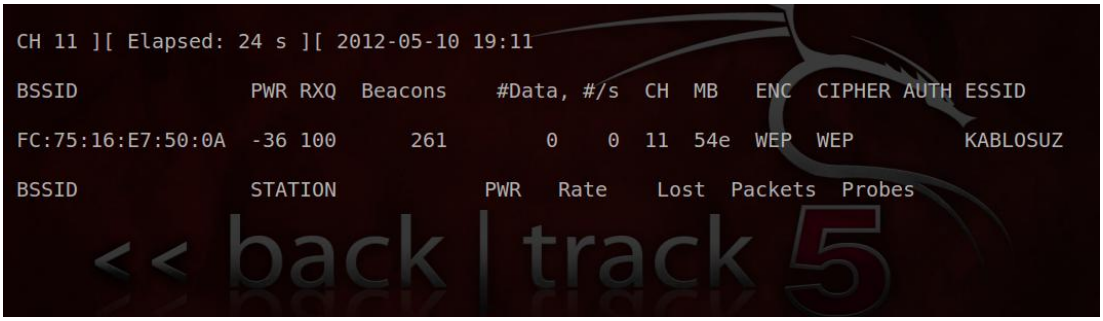
Şekil 4.9. Ağ kartı ile hedefi tespiti

2. Bu uygulama sırasında, sadece KABLOSUZ SSID'sine sahip ağ ile ilgilenilmektedir. Bu yüzden sadece bu ağa ait olan paketleri görmek için, airodump-ng --bssid FC:75:16:E7:50:0A --channel 11 --write WEPCrackingDemo mon0 yazılır. Buna ek olarak, airodump -ng yi bir dosyasına kaydetmek için --write ile kullanılmıştır.



Şekil 4.10. Hedefin MAC adresi şifrelenmiş WEP için dinlenmesi

İstemci başarılı olarak bağlandıktan sonra, airodump-ng aşağıdaki gibi bir ekran raporlar.



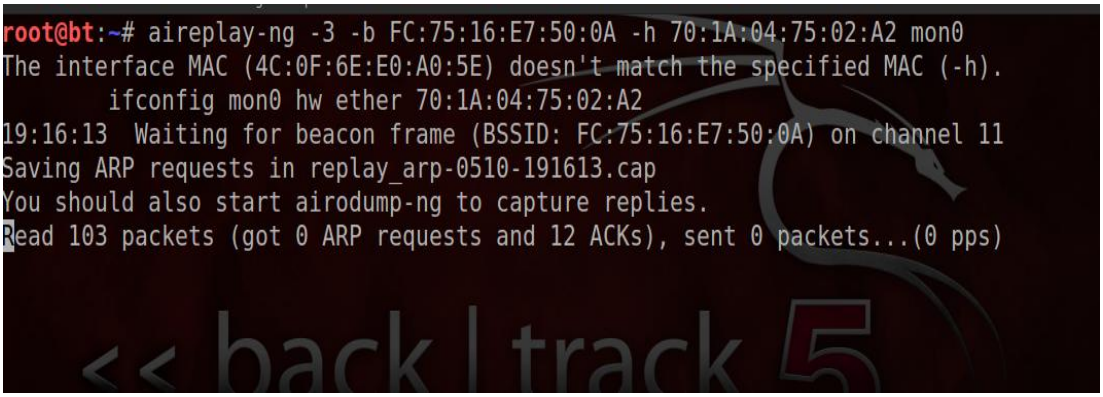
Şekil 4.11. Airodump'dan paket raporlanması

Airodump-ng ekranını gördüyseniz, #Data kolonu altında listelenen veri paketleri miktar olarak çok azdır (sadece 68). WEP kırmada, oldukça fazla sayıda veri paketine ihtiyaç duyulmaktadır. Bu veri paketleri de protokoldeki zayıflıkları açığa çıkarmak için aynı anahtarla kriptolamıştır. Böylece ağı daha fazla paket üretmeye zorlanmaktadır. Bunu yapmak için**,** ***aireplay -n*** komutu kullanılacaktır.

3. Aireplay-ng ile kablosuz ağdaki ARP paketleri yakalanacaktır ve ARP tepkilerini simüle etmek için ağa tekrar geri enjeksiyon edilecektir. Bir sonraki ekranda görüldüğü üzere aireplay-ng yi yeni bir pencerede çalıştırılacaktır. Bu paketleri birkaç bin defa geri oynatarak, ağda oldukça fazla miktarda trafik yaratılacaktır. aireplay-ng WEP anahtarını bilmese dahi, ARP paketlerinin paket büyüklüklerine bakılarak teşhis edebilir. ARP sabit header olan bir protokoldür ve ARP paketleri teşhis edilmek üzere kriptolamış trafikte dahi bulunabilir. aireplay -ng yi aşağıdaki seçeneklerle çalıştıracaktır:

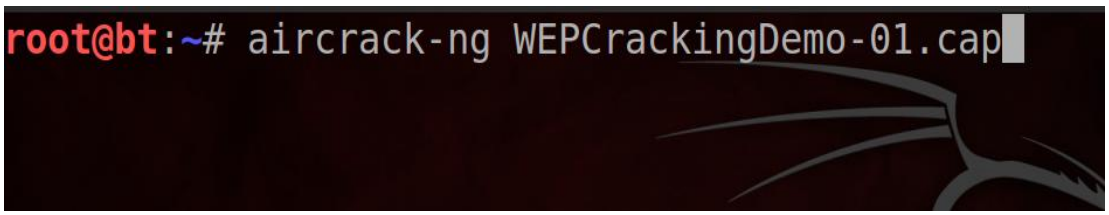
-3 seçeneği ARP replay etmek için,
-b ağımızın BSSID si için
-h spoof edeceğimiz client ın MAC adresini belirlemek için.

Hemen sonrasında, aireplay-ng nin ARP paketlerini sniff ettiği ve daha sonra ağda geri oynattığı görülebilir.



Şekil 4.12. Aireplay-ng komutu ile ARP paketlerinin sniff edilmesi

4. Şifrenin kırılacağı asıl adım olan, kırma(crackleme) kısmı aşağıdadır. Aircrack–ng yi WEPCrackingDemo-01.cap ile yeni bir pencerede çalıştıralım. Bu, aircrack-ng yazılımını başlatacak ve WEP anahtarı kırma işlemine dosyadaki veri paketlerini kullanarak başlatılacaktır. Dikkat edilmesi gereken nokta, aynı anda, airodump-ng WEP paketlerini toplamak, aireplay-ng replay saldırısı gerçekleştirmek ve aircrack-ng de WEP anahtarını yakalanan paketleri kullanarak kırmaya çalışmaktır.

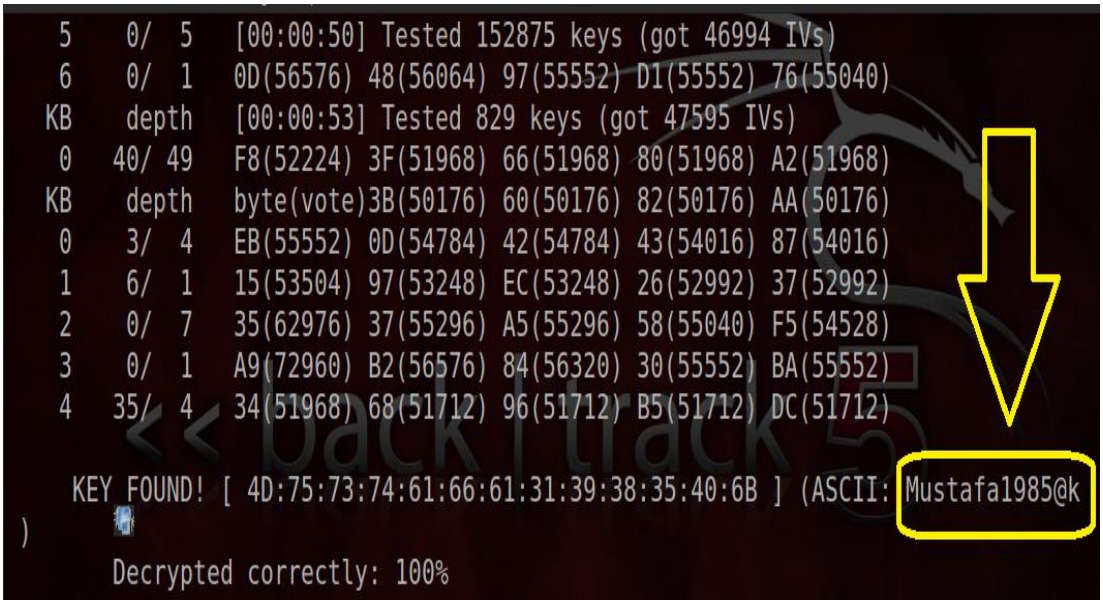


Şekil 4.13. WEP anahtarının yakalanan paketlerin kullanarak kırılması

Anahtarı kırmak için gereken veri paketleri deterministtik değildir; ancak genelde yüz bin ya da daha fazladır. Hızlı bir ağda (ya da aireplay-ng komutuyla) bu en fazla 5-10 dakika alacaktır. Eğer dosyadaki veri paketleri yeterli değilse, o zaman aircrack-ng aşağıdaki şekilde olduğu gibi başarısız olarak sona erecektir ve yakalanmak üzere

daha fazla paket için bekleyecek ve daha sonra crackleme işlemine yeniden başlayacaktır.

Yeterince veri paketi yakalanıp işlendikten sonra, Aircrack-ng anahtarı kırıyor olmalıdır. Bu olduğunda, terminal ekranında bu bilgi gösterilir ve aşağıdaki şekildeki gibi ekranda çıkış yaptığı görüntülenir.



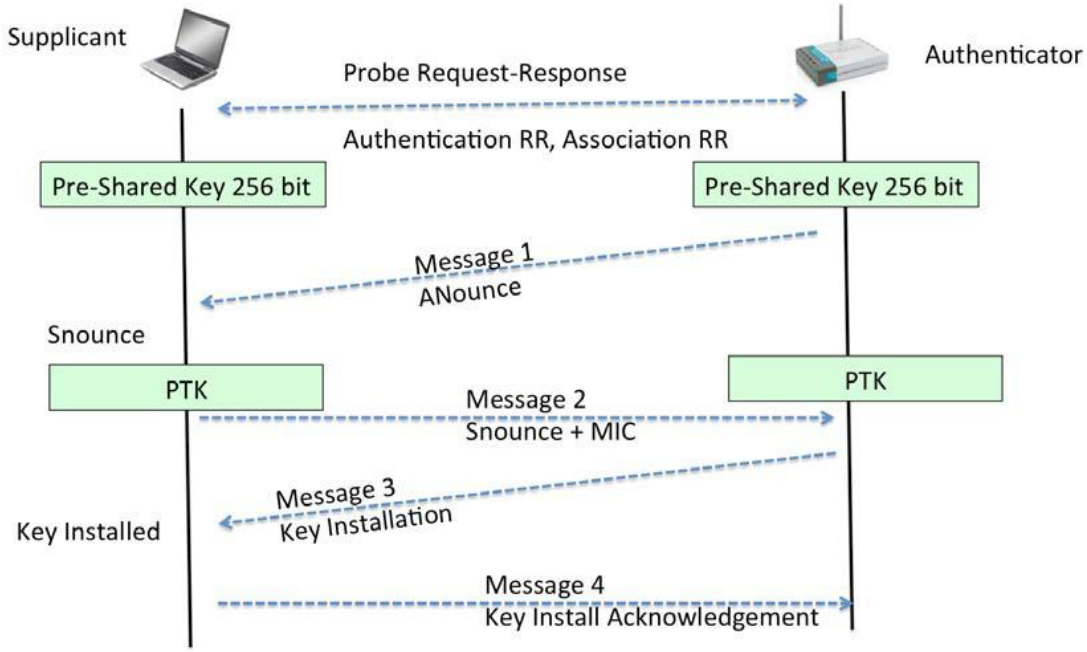
Şekil 4.14. WEP'in elde ettiğimiz şifreyi göstermektedir

WEP şifreleme algoritması ile şifrelenen kablosuz ağın laboratuvar ortamında başarıyla kırıldığı görülmüştür. Bunu yapmak için, ilk önce geçerli bir ağ client (istemci) nin erişim noktasına bağlanması beklenmiştir. Bundan sonra, aireplay -ng aracını ARP paketlerini ağda yeniden oynatması için kullanılmıştır. Bu işlem, ağın ARP geri oynatma paketlerini tekrar kullanmasını ve böylece havadan gönderilen veri paketi sayısının artmasını sağlamıştır. Bundan sonra ile WEP anahtarını kırmak için bu veri paketlerindeki kripto grafik zayıflıkları inceleyerek kırması için aircrack-ng yi kullanılmıştır.

4.7. WPA/WPA2 Kriptolamayı Kırmak

WPA (ya da bazen adlandırıldığı üzere WPA versiyon 1) öncelikle TKIP kriptolama algoritmasını kullanmaktadır. TKIP WEP i, yeni bir donanım kullanmadan iyileştirme amacıyla çıkartılmıştır. Bunun tersine, WPA2, TKIP den daha güçlü ve daha dayanıklı olan AES-CCMP algoritmasını kriptolama amacıyla kullanmaktadır. WPA/WPA2 PSK sözlük saldırısına açıktırlar.

Bu saldırı için gerekli olan inputlar, istemci ile erişim noktası arasındaki 4-yönlü WPA handshake ve en sık kullanılan anahtar parolalarının olduğu bir kelime listesidir. Daha sonra, aircrack -ng kullanarak WPA/WPA2 PSK anahtar parolasını kırmayı deneyebiliriz. Dörtlü anlaşma handshake'in bir gösterimi, aşağıdaki şekilde verilmektedir.

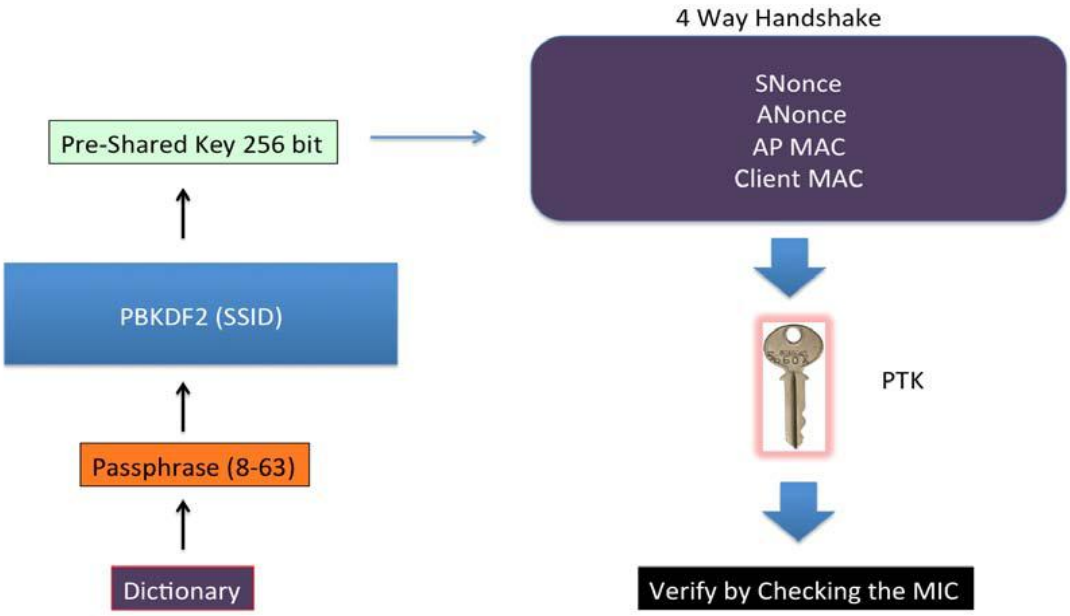


Şekil 4.15. Dörtlü anlaşma protokolü

WPA/WPA2 PSK'nın çalışma şekli, oturum başına, Önceden Paylaşımlı Anahtar ve Beş Farklı parametre daha kullanarak Pairwise Transiet Key (PTK) oluşturur.

Bu 5 parametre: Ağın SSID'si, Doğrulayıcı Nounce'u, sağlayıcı Nounce'u, Doğrulayıcı MAC adresi (erişim noktası MAC adresi), ve sağlayıcı MAC adresi (Wi-Fi istemci MAC i) olarak belirtilebilir.

Bu anahtar daha sonra, erişim noktası ve istemci arasındaki tüm veriyi kriptolamak amacıyla kullanılır. Tüm bu iletişimi havadaki paketleri alarak dinlemiş olan saldırganın sahip olmadığı tek şey önceden paylaşılmış olan anahtardır. O zaman önceden paylaşılmış olan anahtar nasıl yaratılmaktadır? Bu, kullanıcı tarafından SSID ile birlikte sağlanan WPA-PSK parolası kullanılarak oluşturulmaktadır. Bu ikisinin bir kombinasyonu şifre bazlı anahtar oluşturma fonksiyonu (PBKDF2) ye gönderilir ve bu fonksiyon da 256 bitlik bir paylaşımlı anahtar oluşturur.



Şekil 4.16. WPA/WPA2 PSK' nın çalışma şeklini göstermektedir

4.7.1. Sözlük (dictionary) saldırısı

Sözlük saldırısı (dictionary attack), şifre temelli güvenlik sistemlerini, yaygın kullanılan ifade ve kelimeleri deneyerek kırma yöntemi olarak tanımlanır. Örneğin, şehir ve insan isimleri, meşhur deyişler, doğum tarihleri, önemli günler gibi kolay hatırlanır her şey sözlük saldırılarında kullanılan elverişli malzemelerdir. Bu nedenle, sözlük saldırılarında dil ve kültür farklılığı önemli rol oynar.

Genel olarak, sözlük saldırılarına kelime ve tarihleri tek tek kullanmakla başlanılır. Ancak, zaman geçtikçe kelimelerin ve tarihlerin kombinasyonu alınmaya başlanır. Sözlük saldırısı, zahmetli olmakla beraber çoğu zaman işe yarayan bir yöntemdir.

Saldırı adımları

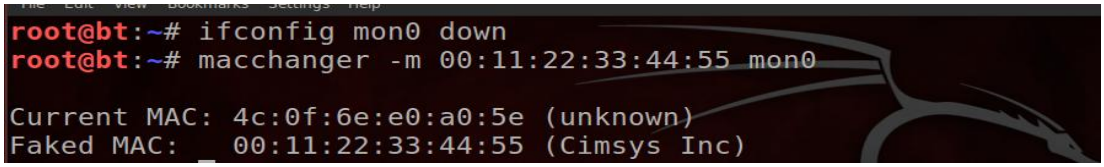
Bir kablosuz ağa bir kaç saldırı modeli olabilir ancak en çok yapılmak istenilen şey bu ağa izinsiz bağlantı kazanabilmek ve paketleri dinleyebilmektir.
Kablosuz ağa izinsiz giriş şu şekilde ilerler;

1. Kablosuz Ağları tespit etme
2. Paket Toplama
3. Şifreyi Kırma

WPA ve WPA2 şifresi, WEP gibi sınırlı bir kombinasyona sahip değil. Aklınıza gelen her karakteri WPA2 şifresinde kullanabilirsiniz. Şifrenin uzunluğu da standart değildir. Ayrıca şifreleme yönteminde WEP'teki gibi yakalayacağımız IV`ler de bulunmamaktadır. Bu yüzden WPA2 şifresini kırmak çok da kolay değil. Ama eğer kullanılan WPA2 şifresi "abcd1234″ gibi basit bir diziyse, kırma işlemi sadece 10-15 dakika kadar sürede tamamlanabilir. şifrede güçlü bir kombinasyon kullanılmışsa kırma işlemi gerçekten çok güçlü olabilir.

Komut 1 : ifconfig , macchanger

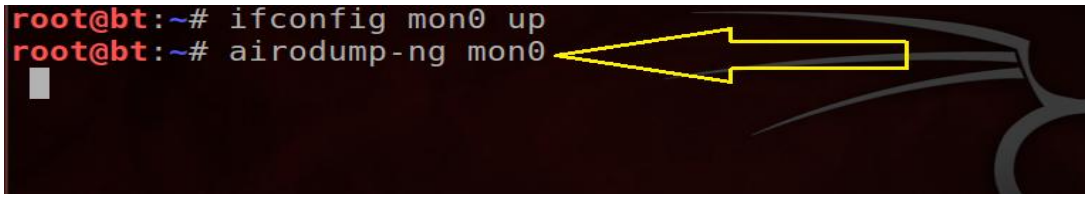
MAC Adresini *macchanger* komutu ile değiştirmek için *ifconfig* down komutuyla, kullandığımız wlan arayüzü üzerinde sistem, mesaj transferi durdurulmaktadır.



Şekil 4.17. MAC adresinin değiştirilmesi

Komut 2 : airodump - ng mon0

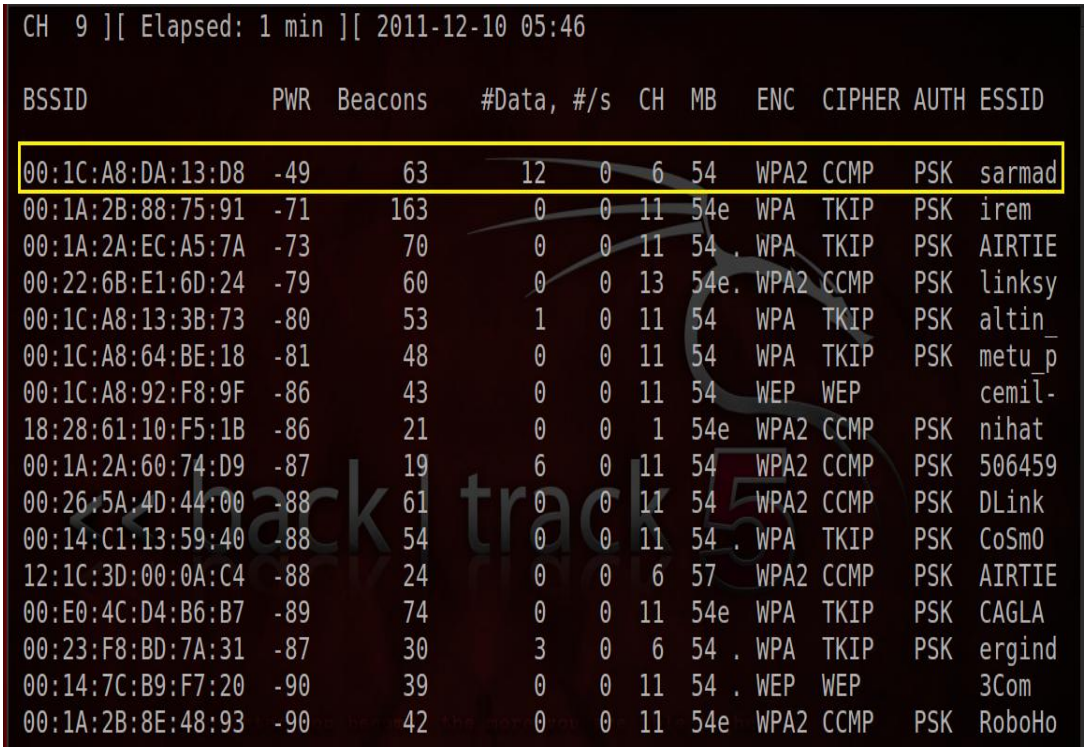
Dinleme Modu Bu komut ile WPA2 şifrelenmiş (Encrypt) verileri Wlan0 olan ağ kart ile dinlemeye alınmaktadır.



Şekil 4.18. Ağ kartının dinlemeye alınması

Kablosuz ağlarla ilgili yapılacak her işlem "dinleme" ile başlar. Yani havada dolaşan kablosuz sinyalleri yakalamak.

Kurbanın bilgileri
ESSID: Kurbanın ağ ismi
BSSID: Kurbanın MAC Adresi
STATION: Modemin MAC adresi
CHANNEL: Kurbanın yayın yaptığı kanal



```
CH  9 ][ Elapsed: 1 min ][ 2011-12-10 05:46

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

00:1C:A8:DA:13:D8  -49       63       12    0   6  54   WPA2 CCMP   PSK  sarmad
00:1A:2B:88:75:91  -71      163        0    0  11  54e  WPA  TKIP   PSK  irem
00:1A:2A:EC:A5:7A  -73       70        0    0  11  54 . WPA  TKIP   PSK  AIRTIE
00:22:6B:E1:6D:24  -79       60        0    0  13  54e. WPA2 CCMP   PSK  linksy
00:1C:A8:13:3B:73  -80       53        1    0  11  54   WPA  TKIP   PSK  altin_
00:1C:A8:64:BE:18  -81       48        0    0  11  54   WPA  TKIP   PSK  metu_p
00:1C:A8:92:F8:9F  -86       43        0    0  11  54   WEP  WEP         cemil-
18:28:61:10:F5:1B  -86       21        0    0   1  54e  WPA2 CCMP   PSK  nihat
00:1A:2A:60:74:D9  -87       19        6    0  11  54   WPA2 CCMP   PSK  506459
00:26:5A:4D:44:00  -88       61        0    0  11  54   WPA2 CCMP   PSK  DLink
00:14:C1:13:59:40  -88       54        0    0  11  54 . WPA  TKIP   PSK  CoSmO
12:1C:3D:00:0A:C4  -88       24        0    0   6  57   WPA2 CCMP   PSK  AIRTIE
00:E0:4C:D4:B6:B7  -89       74        0    0  11  54e  WPA  TKIP   PSK  CAGLA
00:23:F8:BD:7A:31  -87       30        3    0   6  54 . WPA  TKIP   PSK  ergind
00:14:7C:B9:F7:20  -90       39        0    0  11  54 . WEP  WEP         3Com
00:1A:2B:8E:48:93  -90       42        0    0  11  54e  WPA2 CCMP   PSK  RoboHo
```

Şekil 4.19. Ağ kartı ile ortamın dinlenmesi ve hedef tespiti

ESSID

Herhangi bir kablosuz ağı bulduğunuzda size ağın SSID' sini verir yani özetle erişim noktasının ismini. Eğer bir erişim noktasında SSID Broadcast açık ise genelde saniyede 10 defa olmak üzere yayın yaptığı kanalda kendisinin orada olduğunu belirten bir şekilde sinyal gönderir.

BSSID

Kablosuz interneti dağıtan modemin ya da access point'in MAC adresi.

Kanallar (CH)

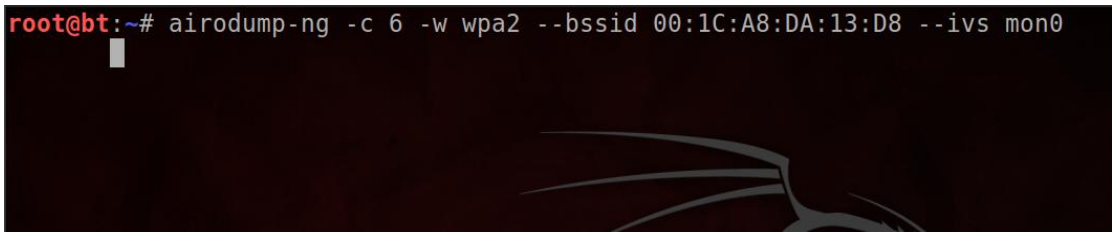
Farklı frekanslarda 1-14 arası yayın kanalı vardır, AP(erişim noktası) ve STA(İstasyon, yani Kablosuz Ağ İstemcisi) bir kanaldan iletişim kurar. Örnek olarak AP 12. kanalda yayın yapıyorsa STA' da o kanaldan bağlanır. Aynı şekilde AP ve

STA' in yaptığı broadcast (genel) isteklerde her kanal için ayrı yapılmalıdır. Amerika' da 11 kanal kullanılmaktadır. Kanada, Avrupa ve Ülkemizde 13 kanal kullanılır. Kanal GHz spektrum' u 2.412' den başlayıp her kanalda 0.005 GHz yükselerek ilerler. Yani Kanal 13 frekansı 2.472 GHz' dir.

Komut 3: airodump-ng -c 6 -w wpa2 --bssid 00:1C:A8:DA:13:D8 --ivs mon0

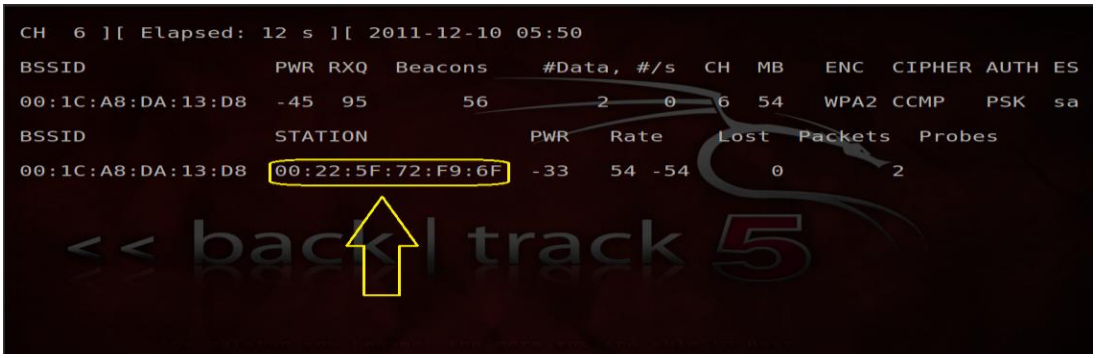
Bu komut yayın yapan (6) numaralı kanal (BSSID) hedefin MAC adresi şifrelenmiş WPA2 dinler. Bu komutta yapılmak istenen işlem şudur: 6. kanaldaki yayınları wlan0 arayüzündeki kablosuz ağ cihazı ile yakalayıp yakalanan verileri wpa2.01.ivs isimli bir dosyanın içine kaydetmek.

-w: Handshake yakalamak için biz paket dinlerken modeme başkasının bağlantı kurması gerekir. Böylece o sırada yollanan handshake paketi yakalanabilir. Eğer dinlediğimiz ağda kimse yoksa sadece birisinin bağlanması beklenecektir. Biz ağı dinlemeye başladığımızda zaten birileri varsa bu kişilerin bağlantısını kopartıp tekrar bağlanmalarını sağlayacağız.



Şekil 4.20. Hedefin MAC adresi ile şifrelenmiş WPA2 dinlenmesi

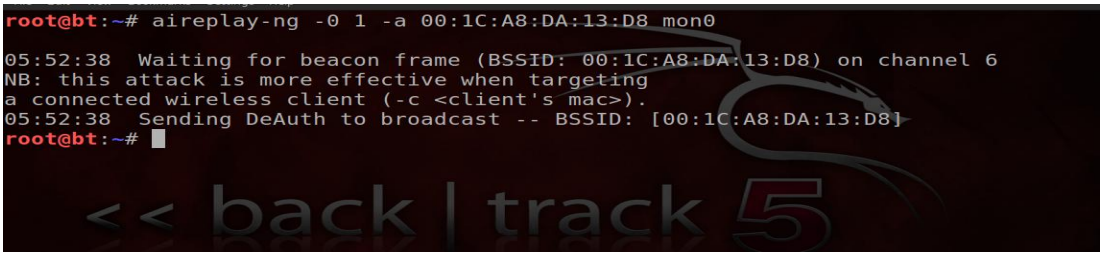
Böylece tekrar şifreli paket göndermeleri gerekecek. Airodump IV dosyalarını çalıştığı klasöre kaydedecektir. Network yoğunluğuna göre gerekebilir, bunun için "***Aireplay***" kullanabilirsiniz. Toplama hızınız değişebilir. Bu hızı yükseltmek için ağda ekstra trafik yapmanız gerekmektedir.



Şekil 4.21. Airodump'dan paket toplama

Komut 4 : aireplay-ng -0 1 -a 00:1C:A8:DA:13:D8 mon0

Bu komut hem trafiği hızlandırmak hem de Handshake yakalamak için (-0 1) parametreleri modem trafiği hızlandırmak içindir.
-a: WPA2 şifresi kırılacağını belirtiyor.

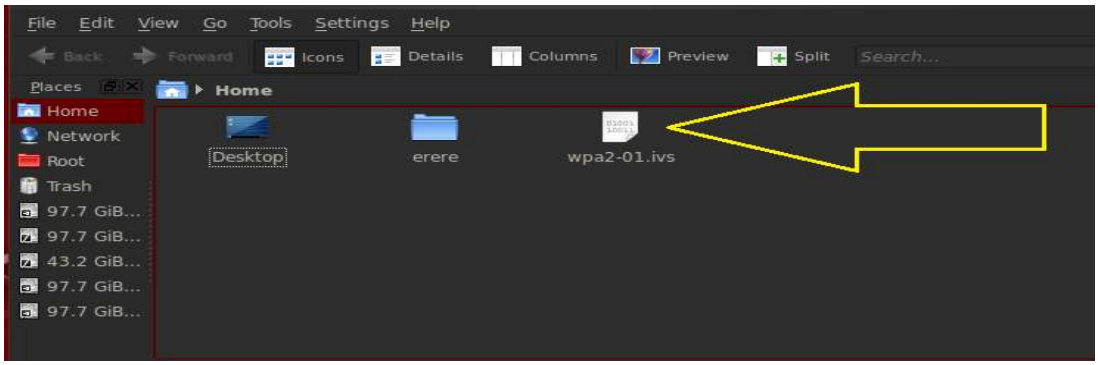


Şekil 4.22. Handshake yakalamanın başlatılması

Handshake: WPA2 şifrelemesinde bilgisayarların ağa giriş yaparken kullandığı doğrulama işlemi. Handshake elde etmek için bir kullanıcının ağa bağlı olması gerekmektedir

Şekil 4.23. Handshake durumunun yakalanması

WPA2-01.ivs : Paketleri topladığımız dosya



Şekil 4.24. Paketlerin toplandığı dosya

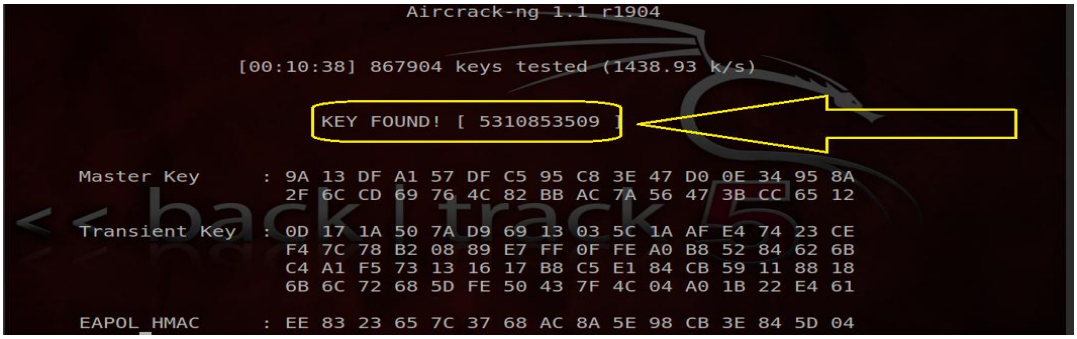
Komut 5 : aircrack-ng -w /root/darkc0de.lst/root/wpa2.01.ivs

Aircrack paket toplama için kullandığımız "airodump" ın geliştiricisinden, çok kısa bir sürede ve az paketle sonuca ulaşabiliyor. Bu komut yakalanan Handshake ile elimizdeki sözlük olan Wordlist.txt kombinasyonlarla karışılaştırıp sonuca ulaşmasını sağlar.

-w /root/darkc0de.lst : Şifrelerin olduğu liste dosyası

Şekil 4.25. Yakalanan handshake ile mevcut wordlist. txt karşılaştırılması

Eğer tek bir sonuç çıkarsa aircrack otomatik olarak kırma ekranına geçecektir.



Şekil 4.26. WPA2 için elde edilen şifre

WPA2 Şifresini Çözmek; WPA2 protokolü kullanan bir ağda şifre kırmak için teoride ne yapacağımızı anlatalım. Önce her zaman olduğu gibi kıracağımız kablosuz ağı belirleyip, kanal bilgisini ve BSSID`sini bulacağız. Daha sonra bu ağdaki trafiği dinleyerek, şifreli paketleri kaydedilecektir. Ardından bu paketlerin içerisinden bir "handshake" yakalamaya çalışacağız. Handshake olarak tabir ettiğimiz, herhangi bir kullanıcının WPA2 şifresini kullanarak ağa dahil olması, yani ağa kabul edilmesidir. Ya da kendimiz bir handshake yaratmak için Deauthentication atağı yapmayı deneyeceğiz. Bu atak yönteminde en basit anlatımıyla ağa bağlı olan kullanıcıyı ağdan düşürmeye çalışacağız ki, o yeniden bağlanmaya çalışırken biz bir handshake yakalayalım. İşin buraya kadar olan kısmı imkansız değil. Günler boyu ağı dinleyerek sonunda handshake yakalanabilir. Ancak bundan sonrası biraz tesadüflere bağlı. Elimizdeki sözlük listesini kullanarak Sözlük (Dictionary) Saldırısı uygulayacağız.

4.8.2. WPS destekli kablosuz ağların WPA/WPA2 saldırısı

Wi-Fi teknolojisine sahip bilgisayar, telefon, kişisel el bilgisayarları gibi cihazların kullanmış olduğu kablosuz ağ ortamı için ağ ayarlamaları ve güvenlik gereksinimleri daha önemlidir. WPS destekli güvenli bir kablosuz ağ ortamı kurulumu resmi olarak 8 Ocak 2007'de yapılmıştır [50].

WPS hem 2.4 GHz (802.11b/g) hem de 5 GHz (802.11a) kablosuz ağ teknolojilerinde Wi-Fi sertifikalı cihaz olarak çalışabilmektedir. IEEE 802.11i bir kablosuz ağ alanı içerisindeki kablosuz veri ve sistem güvenliği için gerekli olan anahtar yönetim stratejileri, kimlik denetimi, kriptolama gibi güvenlik standartlarını belirler. İki tane veri gizlilik protokolü mevcuttur (TKIP ve AES-CCMP). Bunlar, uygun gizlilik protokolünün seçimi için anlaşma işlemi ve her trafik tipi için bir anahtar sisteminin belirlenmesidir. TKIP Mesaj Tanımlama Kontrolü (MIC) ve Paket Başına Anahtarlama (PPK) içerir [51].

Son yıllarda, kablosuz ağ güvenlik alanında Wi-Fi destekli iki güvenlik protokolü geliştirilmiştir. Bunlar, 2003 yılında Wi-Fi korumalı erişim (WPA) ve 2004 yılında Wi-fi korumalı erişim II (WPA2) protokolleridir. Bu teknolojilerden daha önce kullanılan sistem WEP teknolojisidir. Fakat bu sistemde oldukça ciddi güvenlik açıkları mevcuttur [52]. Kablosuz ağlara erişimi arttırmak için bir anahtar dağıtım sistemi IEEE 802.11i tarafından uygulanmıştır. IEEE 802.11 tekli ve herkese yayınının trafik tipini ayrı ayrı ele almıştır. Çünkü bu trafik tiplerinin oluşturduğu güvenlik açıkları farklılıklar göstermektedir. Çeşitli veri gizlilik protokolleri ve anahtar dağıtımlarıyla, IEEE 802.11 uygun gizlilik protokolünün seçimi için anlaşma işlemi ve her trafik tipi için anahtar sisteminin uygulanması şeklinde iki yapıdan oluşur [52].

Wi – Fi Korumalı Kurulum (WPS- Wi – Fi Protected Setup)

IEEE 802.11i çalışma grubunun asıl amacı IEEE 802.1X ağlarının güvenliği arttırmak ve kontrol etmektir. Diğer taraftan, WPS protokolü kablosuz ağlardaki güvenlik için gerekli olan ayarlamalarının yapılması işlemini basitleştirmektedir. Bu protokol kablosuz ağ güvenliğini çok az bilen ev kullanıcılarına hali hazırda mevcut güvenlik teknolojilerinden yararlanarak (WPA) güvenli bir şekilde kablosuz internet kullanabilme imkanı sağlar.

WPS'in bazı avantajları aşağıda sıralanmıştır [53,54,58]

- Kablosuz ağların otomatik olarak ayarlamalarını yapar.
- Kablosuz ağ adının (SSID) ve güvenlik anahtarının bilinmesine gerek yoktur.
- Güvenlik anahtarı rastgele üretilir. Böylece, güvenlik anahtarının tahmin edilebilme ihtimali azalır ve ağa sızma işlemi zorlaşır.
- WPS gerekli olan sistem şifresini karmaşık olarak üretir.
- WPS Genişletilebilir Kimlik Denetim Protokolü (EAP) içinde barındırır.

WPS ’in bazı dezavantajları aşağıda sıralanmıştır.

- WPS sertifikası olmayan cihazlar, WPS’in sunduğu geliştirilmiş güvenlik avantajlarından yararlanamaz.
- WPS desteği olmayan cihazların WPS’li bir ağa dahil olabilmesi için uzun olan hexadecimal şifrenin kullanıcı tarafından girilmesi gerekmektedir.
- WPS Ad Hoc iletişimi desteklemez. Ad Hoc, kullanıcılara birbirleri üzerinden sıçrayarak internete erişimi sağlayan bir teknolojidir.
- Tüm iletişim, erişim noktaları aracılığı ile olmalıdır.
- WPS teknolojisi oldukça yenidir. Bu yüzden şuan kullanılan cihazların tümü tarafından desteklenmemektedir.

WPS kurulumun yapılabilmesi için ilk olarak, WPS destekli cihazın üzerinde Şekil 4.27’ deki gibi WPS düğmesine basılır.

Şekil 4.27. Yönlendirici ve ya AP üzerindeki WPS düğmesi

WPS’in en yaygın kullanım modu hem kablosuz yönlendirici ve ya adaptörü üzerindeki (PBC) düğmesine basılması hem de kullanıcının cihazında bulunan WPS işlemini gerçekleştiren düğmeye basılması ile ağa dahil olunması işlemidir.

Şekil 4.28. AP üzerindeki PBC düğmesi

Wi-Fi’ın 2.28 ve sonrası versiyonu için getirdiği bir özelliktir. Örneğin, RN-131, RN-171 serileri WPS desteklidir [53]. Yönlendirici veya AP üzerinde

kullanılabilecek olan diğer bir methods ise Kişisel Bilgi Numarasıdır (PIN). PIN numarası cihaz üzerindeki etiketin üzerinde olabildiği gibi cihazın ayarlamalı için bağlanıldığı ekrandan da elde edilebilir.

Şekil 4.29 bir AP'nin arkasındaki etikette bulunan PIN numarasını göstermektedir.

Şekil 4.29. Kablosuz cihazlardaki PIN etiketi

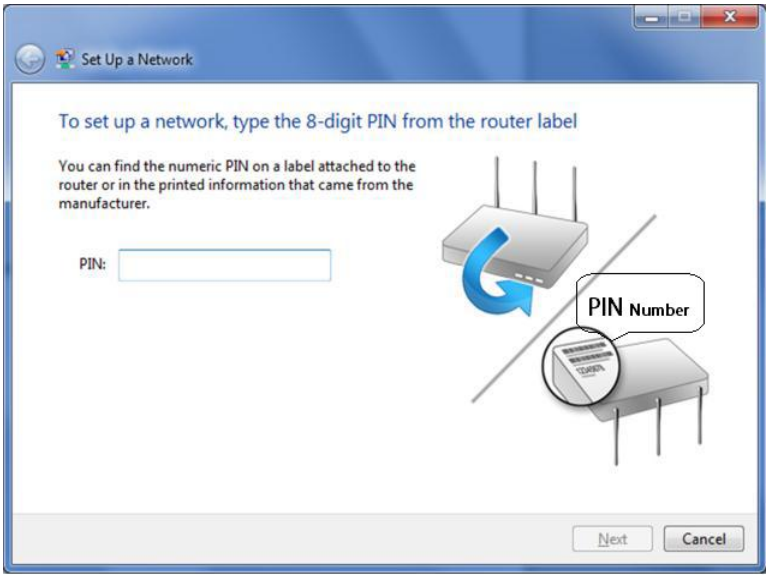
PBC metodunda, kullanıcı yönlendirici yada AP üzerindeki PBC düğmesine basmalıdır. Bir kaç dakika sonra kablosuz ağ içerisindeki WPS ayarlanmış olacaktır. WPS PIN metodunda, cihaz üzerindeki PIN numarası okunur ve ağ içerisindeki bu hizmetten yararlanacak olan cihazlara girilir. İki metot arasındaki temel fark, PIN metodunda istemcinin cihazına PIN numarasının girilmesi iken PBC'de böyle bir durum söz konusu değildir [55].

PIN metodu, dahili kayıt modu ve harici kayıt modu olmak üzere iki model içerir. Dahili kayıt modunda, Kullanıcı AP üzerindeki PIN numarasını doğrudan kendi kullandığı bilgisayara yada el bilgisayarına girer. Şekil 4.30'da WPS PIN modunun PIN numarasının girildiği durum gözükmektedir.

Şekil 4.30. PIN dahili modunun kayıt işlemi

Bu mod AP'nin PIN numarasına erişebilir olduğu durumlarda istemci tarafından PIN numarasının alınabilmesi gibi durumlarda kullanılır. Kullanıcı PIN numarasını kendi bilgisayarına Şekil 4.30'daki gibi ilgili alana girerek register düğmesine basmalıdır. AP veya istemci ayarlandıktan sonra, daha fazla detay bilgi için Ok düğmesine basılmalıdır.

WPS ayarlamalarında PIN metodunun harici modu üç adımdan oluşur. Üçüncü mod istemci cihazı yönlendiricinin PIN numarasını istediği zaman uygulanır. Kullanıcı yönlendiricinin arkasındaki etikette yazan PIN numarasını girmelidir. Daha sonra detay bilgilere erişmek istenirse Ok butonuna basılmalıdır. Sonraki şekil harici kayıt olma durumunu göstermektedir (Windows 7 dikkate alınmıştır).



Şekil 4.31. Harici PIN Kayıttı

Aslında, harici kayıt olma seçeneği PIN'in sağladığından başka kimlik doğrulama şekline ihtiyaç duymaz. Bu durum kaba kuvvet ataklarına karşı potansiyel bir açıklıktır [56,55]. Yönlendirici veya erişim noktası üreten üreticilerden bazıları Cisco, Linksys, D-Link, Belkin, Buffalo ve ZyXEL'dir. Örneğin, IEEE 802.11n teknoloji standardını kullanan Kablosuz N600 çift bantlı bulut yönlendiricisi (2.4 GHz, 2x2 + 5 GHz 2x2) tüm bilgisayarların ve mobil cihazların geniş bantlı internet

bağlantısı ile bağlantı sağlayan yüksek hızda bir ağ oluşturur ve Şekil 4.32'de gösterildiği gibi WPA&WPA2 WPS PIN/PBC desteği sunar.

Şekil 4.32. Kablosuz N600 çift bantlı gigabit bulut yönlendirici

Aşağıdaki çizelge WPS seçeneklerini ve kimlik doğrulama modlarını göstermektedir.

Çizelge 4.1. WPS Seçenekleri ve Kimlik doğrulamaları

Seçenek/Kimlik doğrulama	**Fiziksel Erişim**	**Web Arayüzü**	**PIN**
PBC	✓		
PIN-Dahili Kayıt		✓	
PIN- Harici Kayıt			✓

Yönlendirici yada AP üzerindeki PIN numaraları çizelge 4.2'de görüldüğü gibi yedi tane sayıdan oluşur. Son sekizinci Kısım ise hata kontrolü için bırakılmıştır.

Çizelge 4.2.Yönlendirici üzerindeki PIN numarasının görünüşü

1	2	3	4	5	6	7	0 (Kontrol kısmı)
PIN numarasının 1^{inci} Kısmı				PIN numarasının 2^{inci} kısmı			

Eğer WPS kimlik denetimi başarısız olursa, AP isteği yapan istemciye bir EAP-NACK mesajı gönderecektir. WPS sadece yönlendiricinin veya AP'nin PIN'ine ihtiyaç duyan harici kayıt olarak bilinen bir kimlik denetleme metodu içerir. EAP-NACK mesajları saldırganın PIN'in ilk yarısının doğru olup olmadığına karar verebilecek şekilde gönderilir. Ayrıca, PIN'in son sayısal alanı hata kontrol için

kullanılır. Bu tasarım PIN'i elde etmek için gerekli olan kaba kuvvet denemelerin sayısı oldukça azaltır.

Viehbock üreticilere yanlış şifre denemelerinden sonra kaba kuvvet ataklarını uygulanamaz hala getiren yeterli uzunluğa sahip bir kilitleme süresi önermiştir. Son kullanıcılar için, WPS'i kapatmalarını ve eğer mevcut ise daha güvenli bir sürüme yazılımlarını güncellemesini önermektedir. En uygunu olarak, WPA2 şifreleme algoritması ile güçlü bir şifre kullanılması ve sadece güvenli olduğu bilinen istemcilerin erişimini sağlamak için MAC adres tabanlı güvenlik sağlamayı önermiştir [58].

Çizelge 4.3. PIN harici kayıt işlemindeki IEEE kimlik denetim modlarını göstermektedir.

IEEE 802.11		
İstek yapan -> AP	Kimlik denetimi isteği	802.11 Kimlik denetimi
İstek yapan -> AP	Kimlik denetim yanıtı	
İstek yapan -> AP	Kimlik denetimi isteği	802.11 İlişkisi
İstek yapan -> AP	Kimlik denetim yanıtı	
IEEE 802.11/EAP (Extensible Authentication Protocol)		
İstek yapan -> AP	EAPOL-Başla	EAP Başlaması
İstek yapan -> AP	EAP-Kimlik İsteği	
İstek yapan -> AP	EAP-Kimlik İsteği (Kimlik:"WFA-Simple Config-Register-1-0")	

IEEE 802 ile EAP kapsülleme 802.1X'in içinde tanımlanır ve LAN ya da EAPOL ile EAP olarak bilinir. EAPOL aslında 802.1x-2001 içinde 802.3 ethernet teknolojisi için tasarlanmıştır. Fakat 802.11 kablosuz ve 802.1X-2004 içerisinde Fiber Dağıtımlı Veri Arayüzü gibi diğer IEEE 802 LAN teknolojileri ile uyumlu olarak ortaya çıkmıştır [59].

EAP kablosuz ağlarda veya SOHO ortamında ve noktadan noktaya bağlantılarda uygulanan kimlik doğrulama sistemidir. EAP'ın kulanım alanı oldukça geniştir. Örneğin, IEEE 802.11 (Wi-Fi) içerisinde WPA ve WPA 2 standartları beş tane EAP tipiyle IEEE 802.1X olarak kabul edilmiştir. AP bir EAP-NACK mesajı gönderdiği zaman, saldırgan AP'nin ya da yönlendiricinin cevabından PIN numarasının ilgili kısımları hakkında bilgi edinebilir. Eğer saldırgan M4 gönderdikten sonra bir EAP-NACK mesajı alırsa, PIN numarasının ilk kısmının yanlış olduğu anlamaktadır. Eğer saldırgan M6 gönderdikten sonra bir EAP-NACK alırsa, PIN numarasının ikinci kısmının yanlış olduğunu anlamaktadır [58]. Çizelge 4.4'te M1...M8 aralığının tanımlamaları yapılmıştır.

Kullanılan terminoloji aşağıda istenmektedir.

- Kayıt olma, kablosuz ağa erişmek isteyen yeni bir cihazı ifade etmektedir.
- Kayıttı yapma, kayıt olma işlemi için gerekli olan kablosuz ağ ayarlarını temin eder.
- Erişim noktası, kablosuz sunucu imkanı sağlar ve kayıt olma ile kayıt yapma arasındaki mesaj değişimi için vekil görevi yapar [58].

Çizelge 4.4. IEEE 802.11/EAP tipleri

IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: Simple Config (0x01)			
M1	Enrollee-> Register	N1‖ Description ‖ PK_E	
M2	Enrollee<- Register	N1‖N2‖Description‖PK_R‖Authenticator	Diffie-Hellman Key Exhchange
M3	Enrollee-> Register	N2‖E-Hash1‖E-Hash2‖Authenticator	
M4	Enrollee<- Register	N1‖R-Hash‖R-Hash 2‖ $E_{KevWrapKev}$(R-S1)‖ Authenticator	Proove Posession of 1st half of PIN
M5	Enrollee-> Register	N2‖$E_{KeyWrapKey}$(E-S1)‖Authenticator	Proove Posession of 1st half of PIN
M6	Enrollee<- Register	N1‖$E_{KeyWrapKey}$(R-S2)‖Authenticator	Proove Posession of 2nd half of PIN
M7	Enrollee-> Register	N1‖$E_{KeyWrapKey}$(E-S2‖ConFigData)‖ Authenticator	Proove Posession of 2nd half of PIN, send AP configuration
M8	Enrollee<- Register	N1‖$E_{KeyWrapKey}$(ConFigData)‖ Authenticator	Set AP configuration

IEEE 802.11/EAP geliştirilmiş türünde, M1 yeni bir cihazın kayıt olma ve ağa bağlanma isteğini ifade eder. M2, Diffie-Hellman anahtar değişimi ile yeni bir cihaza kablosuz ağ ayarları sunar. M3 yeni bir cihazın ağa bağlanmak istediği zaman, M4 yeni bir cihazın kayıt edilme işlemi olduğu zaman ve PIN'in ilk yarısı ile ilgili işlem yapılacağı oluşur. M5 yeni bir cihaz kayıt olmak istediği zaman ve PIN'in ikinci yarısı ile ilgili işlem yapılacağı oluşur. M6 yeni bir cihaz kayıt olması ve PIN'in ikinci yarısı ile ilgili işlem yapılacağı zaman oluşur. M7 yeni bir cihaz kayıt olmak istediği ve PIN'in ikinci yarısı ile ilgili işlem yapılacağı zaman oluşur ve sonunda AP'nin ayarlamalarını gönderir. M8'de yeni cihazlar yukarıdaki sıra düzenine göre kayıt edilir ve AP ayarlamaları tamamlanır [58].

Çizelge 4.4 deki kısaltılmış ifade ve tanımlamalar Çizelge 4.5'te verilmiştir.

Çizelge 4.5. IEEE 802.11/EAP tiplerini kısaltmalarının açıklamaları

Enrollee=AP	PSK1=first 128 bits of $HMAC_{AuthKey}$(1st half of PIN)
Register= Supplicant=Client/Attacker	PSK2=first 128 bits of $HMAC_{AuthKey}$(2nd half of PIN)
Pk_E=Diffie-Hellman Public Key Enrollee	E-S1= 128 random bits
PK_R=Diffie-Hellman Public Key Register	E-S2= 128 random bits
AuthKey and KeyWrapKey are Derived from Diffie-Hellman Shared key.	E-Hash1=$HMAC_{AuthKey}$(E-S1‖PSK1‖PK_E‖PK_R)
Authenticator= HMACAuthKey (last message‖Current message)	E-Hash2=$HMAC_{AuthKey}$(E-S1‖PSK1‖PK_E‖PK_R)
EKeyWrapKey=Stuff encrypted with KeyWrapKey(AES-CBC)	R-S1= 128 random bits
	R-S2= 128 random bits
	R-Hash2=$HMAC_{AuthKey}$(E-S1‖PSK1‖PK_E‖PK_R)
	R-Hash2=$HMAC_{AuthKey}$(E-S1‖PSK1‖PK_E‖PK_R)

Kimlik denetleme işlemi daha karmaşık bir işlemdir. Çünkü, WPS'in bu işlemi çözmesi için yapması gereken bir çok şey vardır [59].

- Tekrar ataklarını durdurma
- Ortak kimlik denetimi sağlama
- AP ve istemci arasında şifrelenmiş bir kanal yaratma
- Çevrim dışı ataklara karşı sağlam olma

Saldırgan tarafından PIN numarasının tahmin edilebilmesi için, takip seçenekleri vardır. Güvenlik sebebiyle doğru PIN numarasını girmek için maksimum bir kimlik doğrulama sayısı vardır. Kimlik doğrulamanın bu şekli mümkün olan maksimum kimlik denetim denemesini oldukça azaltacaktır.

PIN'in olması saldırgana ağ ortamına tam yetki ile erişme imkanı tanır. Ayrıca, PIN çoğu cihaz üzerinde değiştirilemeyen bir şeydir. Bu sebeple, PIN'in bilinmesi saldırgana yönetici ağa erişim şifresini ya da SSID'yi değiştirse bile ağa bağlanma imkânı sağlar. WPS saldırı desteği WPA ve WPA2 ye göre bazı avantajlar sağlar [60]:

- WPS PIN'in oluşturulması oldukça hızlıdır.
- PIN'in bilinmesi yönetici şifreyi değiştirse dahi, anında şifreyi tekrar elde etme imkan sağlar.
- Çok radyolu erişim noktası (2.4/5 GHz) çoklu WPA anahtarı ile yapılandırılabilir. Radyolar aynı WPS PIN'i kullandığı için, PIN'in bilinmesi saldırgana tekrar şifreyi elde etme imkanı sağlar.

Saldırgan tarafından PIN numarasının tahmin edilebilmesi için, takip seçenekleri vardır. Güvenlik sebebiyle doğru PIN numarasını girmek için maksimum bir kimlik doğrulama sayısı vardır. Kimlik doğrulamanın bu şekli mümkün olan maksimum kimlik denetim denemesini oldukça azaltacaktır. PIN'in sekiz hanesi her zaman hane bir ile hane yedinin sağlama toplamı olduğundan, doğru PIN'i bulmak için gereken girişim en fazla $10^4 + 10^3 = 11.000$'dir.

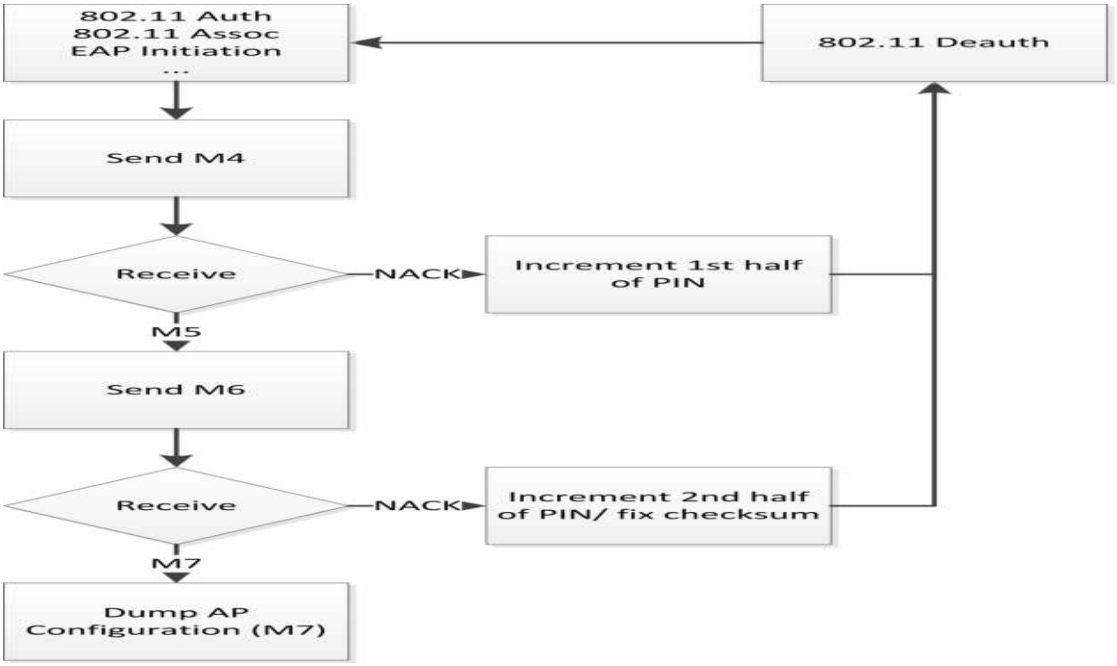
WPS güvenliği, 8 haneli güvenlik kodunu 4 haneli 2 gruba ayırmaktadır. 4 hane ise toplamda 10.000 olası kombinasyon anlamına gelmektedir. Diğer üç hane ise 1000 olası kombinasyondur son rakamsa Kontrol kısmı için kullanmaktadır. Dolayısıyla 4 yıllık süre sadece 1 güne düşürmektedir

Kısacası özel yazılımlar sayesinde (WLAN modemin PIN numarasını deneme / yanılma ile tespit eden araçlar) rastgele kombinasyon yöntemleri ile birkaç saat içinde tespit edilebiliyor. Eğer bütün halinde 8 rakam kombinasyonu olsaydı. Bu süreç günlerce inmesine sebep olmakta. İlk 4 hane tespit edildikten sonra modem karşı tarafa ilk dört rakamın doğru olduğu onayını alıyor ve diğer 4 rakam için denemelere başlıyor.

WLAN Şifresinin kırılması da PIN kodun bilinmesine bağlı. Modemin PIN kodu kırıldıktan sonra WLAN sinyalleri sniffer edilerek şifre ne kadar zor olursa olsun, ne kadar uzun bir şifre olursa olsun birkaç saat hatta birkaç dakika içerisinde kırılabilmektedir [60].

Kaba Kuvvet Saldırısı

Kaba kuvvet atağı PIN şifresini bulmak için çok büyük miktarlarda denemeler yaparak şifrenin elde edilmesini amaçlayan bir metottur. Kaba kuvvet saldırısının akış şeması Şekil 6'de gösterilmiştir. 802.11 iletişimi başladığı zaman, kaba kuvvet algoritması AP'nin doğru PIN numarasını kontrol etmeye başlar [62].



Şekil 4.33. Kaba kuvvet saldırısı akış şeması

AP bir EAP-NACK mesajı gönderdiği zaman, AP'nin cevabından PIN numarasının iki kısmının doğruluğu ile ilgili bilgiyi saldırgan ele geçirir. Şekil 6' daki algoritmaya göre, AP bir EAP-NACK mesajı gönderdiği zaman, saldırgan AP'nin yada yönlendiricinin cevabından PIN numarasının ilgili kısımları hakkında bilgi edinebilir. Eğer saldırgan M4 gönderdikten sonra bir EAP-NACK mesajı alırsa, PIN numarasının ilk kısmının yanlış olduğu anlamaktadır. Eğer saldırgan M6 gönderdikten sonra bir EAP-NACK alırsa, PIN numarasının ikinci kısmının yanlış olduğunu anlamaktadır. Saldırgan PIN numarasının birinci kısmının yanlış olduğu bilirse, PIN numarasının birinci kısmı için algoritmanın çalışmasını arttırır. Aynı şekilde, Saldırgan PIN numarasının ikinci kısmının yanlış olduğu bilirse, PIN numarasının ikinci kısmı için algoritmanın çalışmasını arttırır. Sonunda saldırgan M7 değerini alırsa PIN numarasını bulmuş olur. Bu durum saldırgana yaklaşık 10 saatten daha az bir süre içeresinde olası tüm kombinasyonları deneme imkanı sunar [58].

Reaver komut satırının saldırı adımları

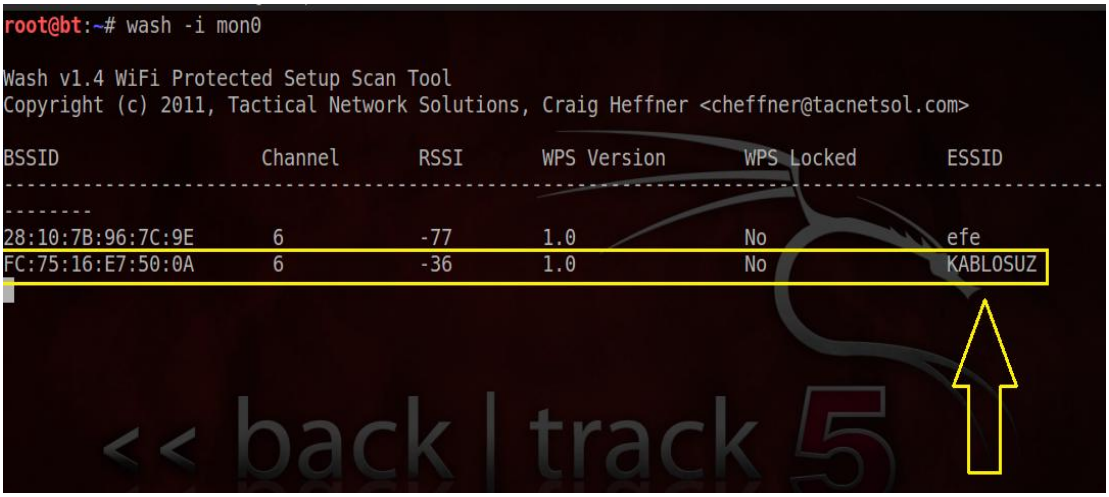
WPS; PIN'i, kaba kuvvet saldırıya müsaittir. PIN kimlik doğrulaması için WPS şartnamesindeki tasarım çatlağı, önemli ölçüde tüm PIN'e kaba kuvvet için gereken süreyi kısaltır.

Reaver adındaki bir alet, aynı konuyu bağımsız bir şekilde takip eden ikinci bir araştırmacı tarafından piyasaya sürülmüştür. Reaver, WPS'deki protokol tasarım çatlağını kötüye kullanan Tactical Network Solution tarafından geliştirilen bir saldırı aletidir. Bu saldırıya açıklık, ağı güvenli hale getirmek için kullanılan Pre-Shared Key (PSK) önceden paylaşılmış anahtarın çıkarılmasına izin veren Kablosuz Korumalı Erişime WPA karşı yan kanal saldırısını ortaya çıkarır. İyi seçilmiş PSK ile WPA ve WPA2 güvenlik protokolleri, 802.11 güvenlik topluluğunun büyük bölümü tarafından güvenli olarak sayılmaktadır.

Saldırının aracı, WPS etkin cihazların PIN'i almaları için piyasaya sürülmüştür ve geniş biz dizi WPS uygulamasına karşı test edilmiştir. Neredeyse tüm büyük yönlendirici ve erişim noktası satıcıları WPS belgeli cihazlara sahip olduğundan, birçok cihaz bu tür saldırılara açıktır. WPS genelde, varsayılan olarak etkinleştirilir ve bu saldırıya açıklığı daha da kötüleştiren kaba kuvvet saldırılarını önlemek için herhangi engelleme mekanizması olmaksızın uygulanır.

Reaver, bir saldırıya başlamak için iki girdiye ihtiyaç duyar: başlamak için kullanılan arayüz ve hedefin MAC adresi. Kablosuz adaptöre doğrudan eriştiği için, dizin kökü olarak çalıştırılması gerekir.

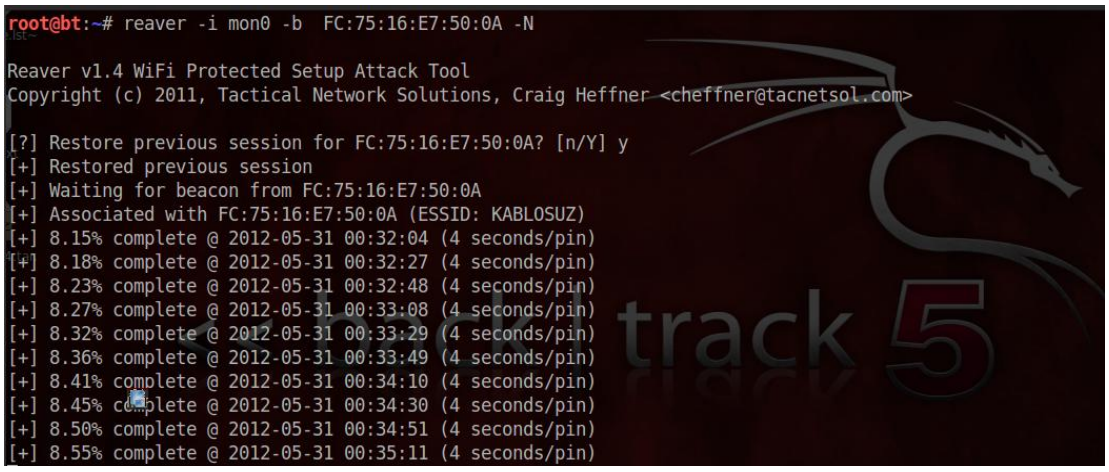
Komut 1: wash –i mon0
WPA anahtarını ele geçirmek için saldırgan öncelikle monitör modu destekleyen bir kart ile mevcut kablosuz ağ ortamları taranmaktadır. Tarama işlemi sonucunda bulunan WLAN ağlarını tespit edip saldırı moduna geçilebilir. Bunun içinde **wash -i** kullanılmaktadır.



Şekil 4.34.wash –i komutu kullanarak hedef tespiti

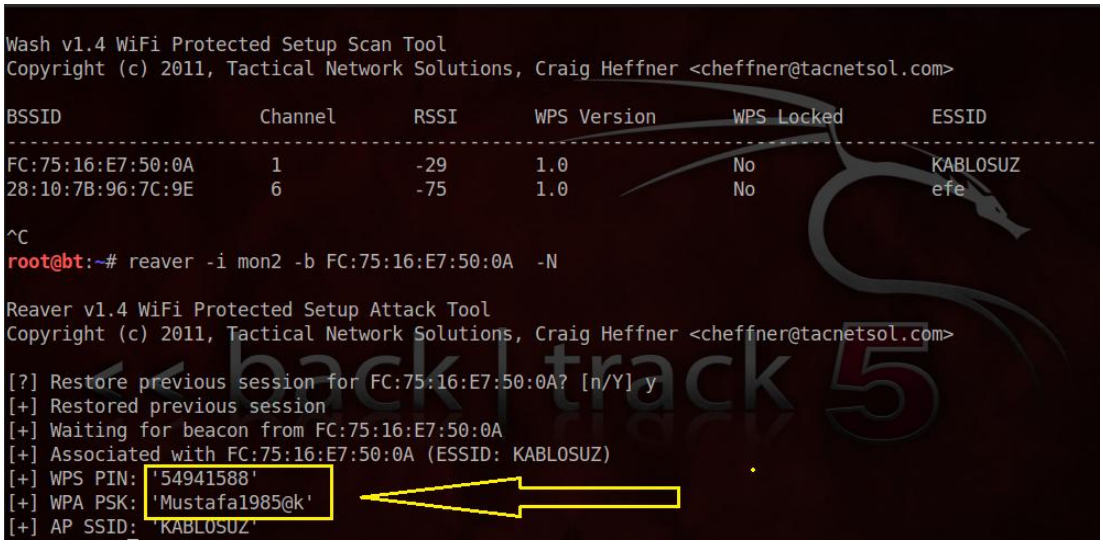
Komut 2 : reaver – i mon0 –b FC:75:16:E7:50:0A -N

Reaver komutu BackTrack'in 5 R1 versiyonunda kurulu gelmemektedir. Bu yüzden, kullanılacak olan bu paketin kurulması gerekmektedir. Paket internetten indirilerek BackTrack üzerine el ile kurulmalıdır. Kurulma işlemi bittikten sonra reaver komutu kullanılabilir. Saldırgan hedef ağın BSSID değerini ve yayın yaptığı kanalları not alarak diğer bir araç ile PIN numarasını Brute Force (rastgele denemeler) atak kullanarak kırılmaktadır.



Şekil 4.35. Reaver – i kullanarak WPS'ye saldırısının gerçekleştirilmesi

Modemin WPS özelliği kapalı bile olsa saldırı başarılı olabilmektedir. WPS PIN numarasını tespit edilmesi maksimum 10 saat kadar sürmektedir.



Şekil 4.36.Saldırı sonunda bulunan WPA2 şifresi ve PIN numarası

Reaver paketi ile yapılan bu saldırının en büyük avantajlarından biri ise, saldırının gerçekleştirilmesi ile başlanan sürecin bitene kadar sonlandırılmaması gibi bir zorunluluğunun olmamasıdır. Saldırıya başlandıktan sonra istenildiği anda saldırı el ile sonlandırılıp, tekrardan saldırı işlemine kalınan yerden devam edilebilir. Bu durum saldırgana zaman açısından esneklik sağlar.

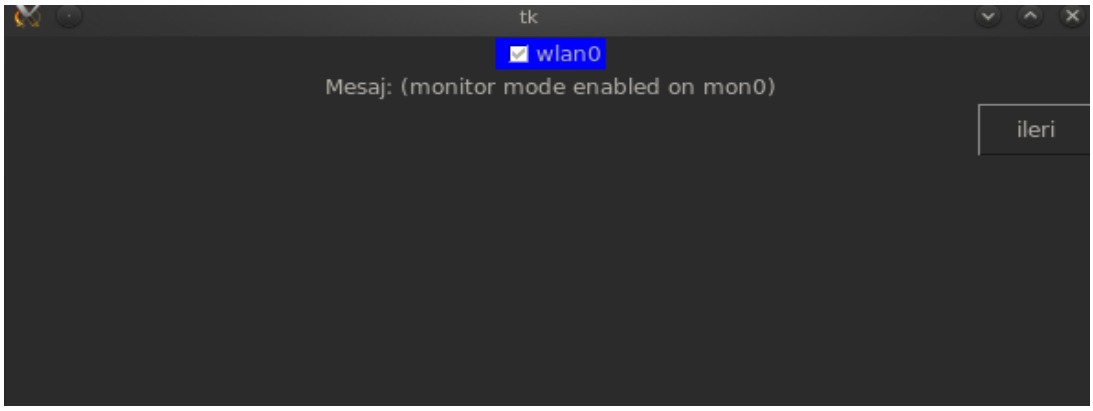
Hedef sisteme yapılan saldırı sonrasında PIN numarası elde edildikten sonra, kurban olan sistem şifreleme algoritmasını ya da şifresini değiştirse bile bunun tespit edilerek yeni şifrenin bulunması sadece saniyeler almaktadır. Gerekli olan ön koşul sadece bir kez PIN numarasının tespit edilmesidir. PIN numarası değiştirilemeyen ve her cihaz için tek olan bir numaradır.

Reaver görselin saldırı adımları

Reaver açık kaynak versiyonu komut satırını kullanmaktadır; Reaver, bir saldırıya başlamak için iki girdiye ihtiyaç duyar: Saldırı yapmak için kullanılan arayüz ve hedefin fiziksel (MAC) adresi. Dikkat edilmesi gereken nokta kablosuz adaptöre doğrudan eriştiği için, dizin kökü (root) olarak çalıştırılması gerekir. Reaver görselin amacı akılda tutulması zor olan komutların yerine daha kullanışlı bir arayüz sağlayarak kullanım kolaylığı sağlamaktır. Bunu yanı sıra arayüzde yapmak istediğiniz işlemleri seçip taramayı başlat dediğiniz anda size arka planda çalışan kodları göstermesidir.

Reaver'e daha fazla özellikler katmak için bir arayüz tasarlanmıştır, bunlar ;

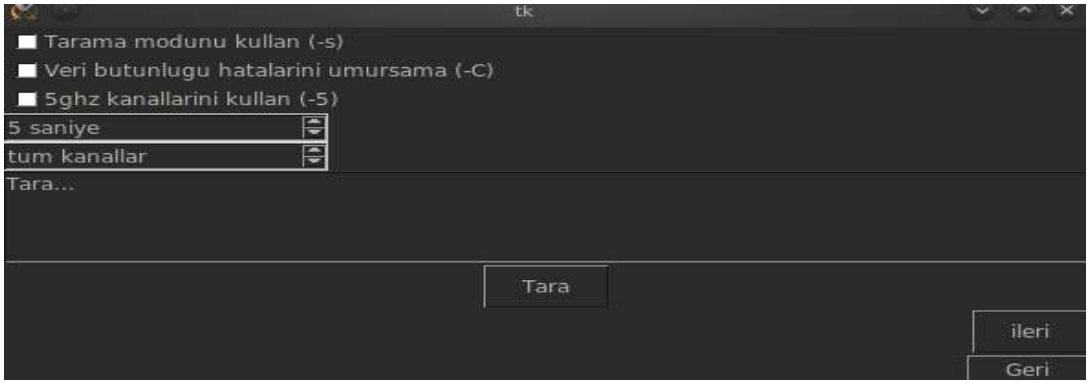
1. Kablosuz ağ kartını otomatik olarak aktif moda getirmek. Reaver Görsel çalıştırıldığında otomatik olarak görüntüleme modu arayüzü aktif hale getiriliyor. Artık airmon_ng komutunu yazmadan program çalıştırıldığı andan itibaren monitör 0 'dan monitör 15'a kadar bütün monitör modlarını izliyor. Arayüz her yeniden başlatıldığında monitör modu bir diğerine geçiyor. Bunun bize getirdiği fayda , izlemesi yapılacak olan kablosuz ağ kartının seçiminde yaşanan karmaşıklığı gidermesidir. Kablosuz ağ kartını otomatik olarak kendi seçerek bizi bu karmaşıklıktan kurtarıyor.



Şekil 4.37. Kablosuz ağ kartı monitör modunda aktif durumda

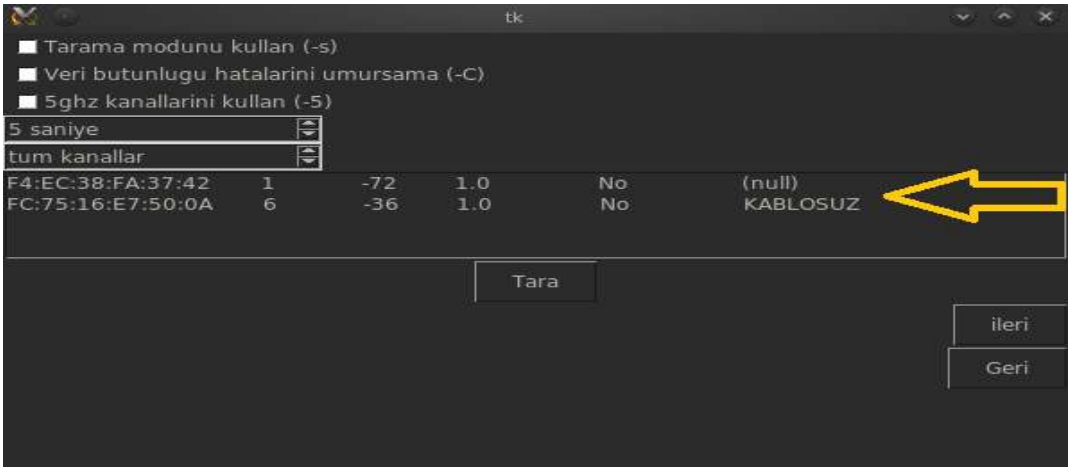
2. İzlenmesi gerekli olan kablosuz ağ kartını seçtikten sonra, kablosuz kartın kapsama alanında bulunan WPS destekli kablosuz ağları bulmak ve ekstra

özellikleri eklemek için kullanılan Wash -i komutunu yazmadan, sadece arka planda çalıştırarak onun yerine görsel bir şekilde tarama işlemleri gerçekleşmektedir .(Daha fazla seçenekler; 5 Ghz kanallarda tarama yapmak veri bütünlüğü hatalarını umursamamak, 1 saniyeden 15 dakikaya kadar tarama süresi, tüm kanallarda ve ayrıca 1-14 arasında seçilebilecek olan istenilen kanallarda tarama yapmak)



Şekil 4.38. Reaver görselin tarama özelliklerinin belirlenmesi

3. Kablosuz ağ kartının kapsama alanında bulunan erişim noktalarını tespit ettikten sonra saldırı yapılmak istenen WLAN(Wireless Local Area Network-Kablosuz yerel alan ağı) seçimi. Bu aşama diğer aşamalara oranla çok daha karmaşıktır çünkü burada saldırı yapılabilecek olan WLAN'ların SSID si, RSSI değeri dediğimiz elektro manyetik girişime neden olabilecek dalgalara karşı koyma gücü (RSSI sıfırın altında değerler alır sıfıra yakın olan her zaman daha iyidir.), saldırı yapılacak olan erişim noktasının BSSID'si (MAC adresi). Bunların hepsini seçimini komut satırı arayüzünü kullanmadan Reaver görselden işaretlemek şartıyla seçilebilmektedir.

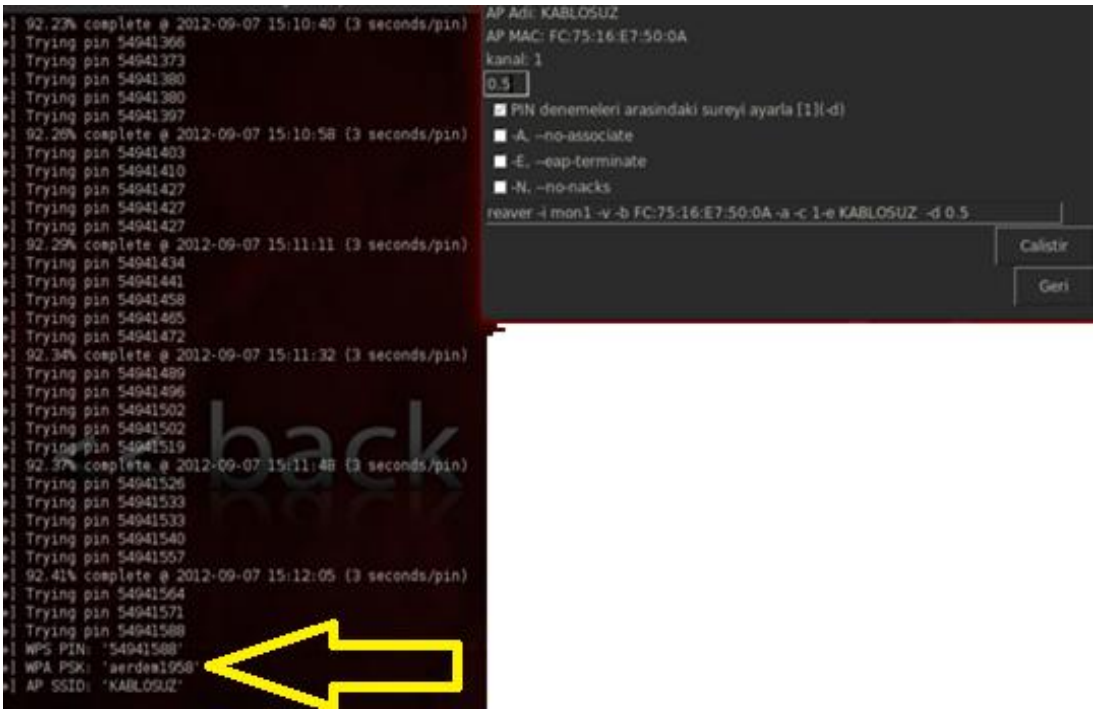


Şekil 4.39. Reaver görsel kullanarak hedef tespiti

4. İşlemin son sırasında ise Reaver komutunu çağırmak için kullanılan arayüz bulunmaktadır. (Burada erişim noktası adı, fiziksel adresi (MAC) ve yayın yapılan kanal numarasını vermektedir. PIN denemeleri arasındaki süreyi ayarlamak mesela (0.5 ,1,2) gibi rakamlar verilebilir ve alttaki şekilde göründüğü üzere –A ,başka bir uygulamanın ilişkilendirme yapma isteğini yok sayma, -E ,EAP paketlerinde oluşabilecek bir hata sonucunda her WPS oturumunu kapatmak ,-N yanlış olan paketler için not acknowledge paketlerini gönderme gibi seçenekler kullanabilmektedir ve sadece çalıştır düğmesine basarak WPS saldırısı gerçekleştirilmektedir).
5.

Şekil 4.40. Reaver görsel kullanarak WPS özellikli erişim noktasına saldırının başlatılması

6. Tüm bu yapılan işlemler sonucunda yaklaşık olarak 6-10 saatlik bir süre zarfında şifre elde edilir. Her ne kadar WPA2(AES/PSK) kullanılsa bile istemcinin PIN numarasını bulması durumunda erişim noktası şifresini istemciye yollar ve şifre böylelikle elde edilir.



Şekil 4.41. Reaver görsel kullanarak şifrenin elde edilmesi

Bu saldırının faydalandığı açıklık sadece donanım yazılımı güncellemesi ile yararlanabileceği için, aşağıdaki çözümlerden birinin uygulanması önerilir:

- WPS cihazınız tarafından izin verilirse, WEB yönetim ara yüzünüzü kullanarak WPS özelliğini devre dışı bırakılmalıdır ve sonrasında kablosuz bağlantı manuel olarak ayarlanmalıdır.
- Bu saldırıya açıklıktan bahseden güncellenmiş donanım yazılımı için WPS cihazın üreticisinin destek web sitesinin kontrol edilmesi önerilir.

Yönlendiricide WPS varsa, koruması için iki yolu vardır:

1. Yönlendirici üzerindeki web ara yüzü ile WPS devre dışı bırakılabilir. Bazı durumlarda, hatta WPS'yi kapatıldığında bile, yönlendirici dinlemez. WPS'nin gerçekten kapandığından emin olmak için şunları yapın: Kablosuz bir Windows 7 makine bulun ve makineden mevcut kablosuz bağlı ağı kaldırın ve yeniden bağlanmaya çalışın. Eğer WPS PIN için sizi harekete

geçirirse, WPS halen etkindir. WPS şifresi için sizi harekete geçiriyorsa, bu durumda WPS başarılı bir şekilde devre dışı bırakılmıştır.

2. Donanım yazılımı güncellemesi. Bu WPS konusunu beraber doğrulamak, yönlendiriciye bir donanım yazılımı güncellemesi gerektirecektir. Ayarlamak gerçekten kolay bir şey olmalıdır, böylelikle yönlendirici üreticileri kısa sürede yönlendirici güncellemelerini piyasaya sürmelidirler.

Reaver Source kod

1. İnit.c

İlk önce : WPS konfigürasyonu olup olmadığını denetlemektedir.

```
wpsconf = malloc(sizeof(struct wps_config));
if(!wpsconf)
{
        perror("malloc");
        goto end
}
```

Sonra WPS - register konfigürasyonu denetlemektedir

```
reg_conf = malloc(sizeof(struct wps_registrar_config));
if(!reg_conf)
{
        perror("malloc");
        goto end;
}
```

Windows 7 ve WPS kullanılmışsa aşağıdaki bilgileri elde edilir .

```
wps->wps->dev.device_name = WPS_DEVICE_NAME;    cihaz ismi
wps->wps->dev.manufacturer = WPS_MANUFACTURER;  üretim şirket ismi
wps->wps->dev.model_name = WPS_MODEL_NAME;      model adı
wps->wps->dev.model_number = WPS_MODEL_NUMBER;   model numarası
```

2. PINS.c

Genellikle bu programın amacı anahtar tablodan uluşturmaktadır PIN bulmak için iki parça P1&P2 olarak aramaktadır ilk P1'de meşhur kullanımı erişim noktalarında PIN değerlerini denemektedir

PIN 'nin ilk yarsını bulmak için kullanılan işlem

```
if(!get_static_p1())
{
        /*
         * Look for P1 keys marked as priority. These are pins that have been
         * reported to be commonly used on some APs and should be tried
first.
         */
        for(index=0, i=0; i<P1_SIZE; i++)
        {
                if(k1[i].priority == 1)
                {
                        set_p1(index, k1[i].key);
                        index++;
                }
        }
```

İkinci PIN P2'in değerini bulmak için erişim noktalarında çok kullanılan PIN değerlerini aramaktadır sonra rasgele değerleri denemektedir.

PIN 'nin ikinci yarsını bulmak için kullanılan işlem

```
if(!get_static_p2())
{
        /*
         * Look for P2 keys statically marked as priority. These are pins that
have been
         * reported to be commonly used on some APs and should be tried
first.
         */
```

```
                for(index=0, i=0; i<P2_SIZE; i++)
                {
                        if(k2[i].priority == 1)
                        {
                                set_p2(index, k2[i].key);
                                index++;
                        }
                }

for(i=0; index < P2_SIZE; i++)
        {
                if(!k2[i].priority)
                {
                    set_p2(index, k2[i].key);
                    index++;
                        }
           }
      }
        else
        {
                /* If the second half of the pin was specified by the user, only use that
*/
                for(index=0; index<P2_SIZE; index++)
                {
                        set_p2(index, get_static_p2());
                }
        }
```

3. Keys.c

PIN'nin ilk parçası olan P1 için anahtar endeks tablosu oluşturmaktadır

$10^4 = 10000$

```
struct key k1[P1_SIZE] = {
        { "1234", 1 },      1: öncelik değeridir örnek
        { "0000", 1 },      1234 ve 9999 ve 0000 gibi
        { "0001", 0 },      değerleri önce denenmektedir.
        { "0002", 0 },
```

Sonra PIN'nin ikinci parçası olan P2 için bu deva üç basamaklı anahtar endeks tablosu oluşturmaktadır.

$10^3 = 1000$

```
struct key k2[P2_SIZE] = {
        { "567", 1 },
        { "000", 1 },
        { "001", 0 },
        { "002", 0 },
        { "003", 0 },
        { "004", 0 },
        { "005", 0 },
```

5. SONUÇLAR VE ÖNERİLER

Ağlar öncelikle kablolu şekliyle karşımıza çıkmıştır, ancak isteklerin artması ve teknolojinin gelişmesiyle, kablosuz ağlar da yaşantımızda yerini almaya başlamıştır. Kablosuz ağların ortaya çıkmasından beri bu alandaki teknolojik ilerlemesi çok hızlı olmuştur. Ancak bu hızlı ilerlemeyle birlikte güvenlik açıkları da ortaya çıkmıştır. İlk nesil kablosuz ağlar güvenliği seçenekli olarak tanımlamıştır, yeni nesil güvenlik protokolleri ise kablosuz ağlara girişte doğrulamayı zorunlu hale getirmiştir.

Bu çalışmada 802.11 kablosuz ağlarında güvenlik konusu ele alınmıştır, geliştirilen güvenlik mekanizmaları incelenmiş farklı güvenlik mekanizmaları sonucunda görülmüştür ki; WEP ve WPA şifreleme teknikleri kablosuz ağlarda güvenliği temin etmemektedir. Güvenli bir kablosuz ağ oluşturmak için WPA2 standardının kullanılması gerekmektedir. Bu standart ile daha güçlü bir şifreleme algoritması olan AES ve kullanıcı ile erişim noktası arasında karşılıklı bir kimlik doğrulaması gerektiren yöntemi kullanılmaktadır.

İlk olarak geliştirilen WEP, RC4 (Rivest Cipher) şifreleme algoritmasındaki yapısal (Xor gibi) eksikliklerden dolayı zorunlu ihtiyaçlar nedeniyle güvenlik açıkları kapatılarak WPA'ya geçilmiştir. Aslında WPA yeni bir denetim sistemi olmaktan çok acele ile çıkarılan WEP'in geliştirilmiş halidir. Sadece RC4 şifreleme algoritmasının boşlukları doldurularak aynı temel üzerine TKIP şifreleme algoritması ve bir kaç yapısal değişikliğe gidilmiştir. Yani binanın temelleri güçlendirilmiştir. Geçici bir süre güvenlik ihtiyaçlarını karşılayan WPA artık yerini neredeyse tamamen farklı veri denetim mekanizması olan WPA2'ye devretmiştir. WPA2'yi WPA'dan ayıran en önemli özelliği şifreleme teknolojisi olan AES kullanması. WPA2 günümüzün en güvenilir kablosuz ağ iletişim denetim mekanizmasıdır. WEP basit araçlarla 10-15 dakikada kırılabilmektedir yani güvenli değildir. WPA ve sonrasında geliştirilen WPA2 ise yeterli güvenlik gücüne sahiptir.

Bu çalışmada, kablosuz ağların güvenliği üzerine detaylı olarak incelemeler yapılmıştır. Laboratuvar ortamı kurularak günümüzde mevcut olan kablosuz ağ şifreleme algoritmaları ile şifrelenmiş ağların şifrelerinin kırılma işlemi gerçekleştirilmiştir. Yapılan çalışma sonucunda, WEP şifreleme algoritmasının dakikalar içinde kırılabildiği görülmüştür. WPA ve WPA2 şifreleme algoritmaları ise sözlük saldırısı ile, kullanılan sözlüğün kalitesine bağlı olarak kırılabilme ihtimalinin olduğu sonucuna ulaşılmıştır. Son dönem erişim noktalarına getirilen WPS teknolojisine sahip olan cihazlarda ise şifreleme algoritması her ne olursa olsun en fazla 10 saat içerisinde kırılabildiği sonucuna ulaşılmıştır.

Bu çalışmada, WPS teknolojisi kullanılarak yapılandırılan WPA2 şifreleme algoritmasının açıklarından yararlanılarak şifre kırma işlemi gerçekleştirilmiştir. Bu işlemi gerçekleştirebilmek için komut satırı tabanlı reaver isimli araçtan esinlenilmiştir. Reaver aracının kullanım zorluğunu ortadan kaldırabilmek için, açık kaynak kodlu ortam üzerinde python dili kullanılarak bir arayüz hazırlanmıştır. Ayrıca, sunulan bu arayüz sayesinde, istenildiği kadar monitör arayüz sayısı belirlenebilmektedir. Bu sayede, saldırı için tek bir monitör arayüze bağımlı olma durumu ortadan kaldırılarak saldırıya başlangıç aşaması çok daha esnek bir hala getirilmiştir. Geliştirilen arayüz ile saldırının gerçekleştirilmesi, sonuçların alınması ve alınan sonuçların yorumlanması çok daha kolay bir hale getirilmiştir.

Elde edilen bu bilgiler ışığında, kablosuz ağlar her ne kadar kolaylık sağlasa da, güvenliğin önemli olduğu durumlarda kullanımı için gerekli olan tüm önlemlerin alınması ve saldırı tespit sistemleri kullanılarak izlenmesi gerekmektedir. Genel kablosuz internet kullanıcıları için ise, kablosuz ağ güvenlik farkındalığı oluşturulmalı ve kullanıcılar bu yönde bilgilendirilmelidir.

KAYNAKLAR

1. Cache, J., Wright, J., Liu, V., "Hacking Exposed Wireless: Wireless Security Secrets & Solutions, Second Edition 2nd ed.", ***McGraw-Hill***, United States of America, 8-23, 2010.

2. Kizza, J, M., "Computer network security and cyber ethics 3rd ed.", ***McFarland & company***, North Carolina, 87-135, 2011.

3. Kocak, T., Jagetia, M., "A WEP post-processing algorithm for a Robust 802.11 WLAN implementation", ***Computer Communications***, 31 (14), 3405–3409, 2008.

4. Beaver, K. Davis, P., "Hacking Wireless Networks For Dummies", ***Wiley Publishing, Inc***, Canada, 259-267, 2005.

5. Beaver, K. McClure, S., "Hacing For Dummies 3rd ed.", ***Wiley Publishing, Inc***, Canada, 159-168, 2010.

6. Tews, E. Weinmann, R. Pyshkin, A., "Breaking 104 bit WEP in less than 60 seconds", ***TU Darmstadt, FB Informatik Hochschulstrasse***, 10-64289, 2007.

7. Bittau, A. Handley, M. Lackey J., "The final nail in WEP's coffin. In IEEE Symposium on Security and Privacy", ***IEEE Computer Society*** , 386-400 , 2006.

8. Bradbury, D., "Hacking wifi theeasy way", ***Network Security*** , 2011(2), 9-12, 2011.

9. Beck, M. Tews, E., "Practical attacks against WEP and WPA", ***TU-Dresden*** , 2008.

10. Gold, S., "Craking Wireless Networks", ***Network Security*** ,2011(11), 14-18, 2011.

11. Kindervag, J., "The five Myths of Wireless Security", ***Information Systems Security***, 15(4), 7-16, 2006.

12. Tanenbaum, A., Wetherall, D ., "Computer Networks. 5th ed", ***Prentice Hall,*** United States of America, 8-11, 2011.

13. Makki, S.A.M., Pissinou, N, Daroux, P., "Mobile and Wireless Internet Access", ***Computer Communications***, 26(7) , 734-746, 2003.

14. Kima, H., Chan Park, E., Kyu Lee, S., Hu, C., "Fast Performance Assessment of IEEE 802.11-Based Wireless Networks", ***Mathematical and Computer Modelling*** , 53(11-12), 2173-2191, 2011.

15. Lehr, W., Chapin, J., "On The Convergence of Wired and Wireless Access Network Architectures", ***Information Economics and Policy***, 22(1), 33-41, 2010.

16. Hung, K., Bensaou, B., "Throughput Analysis and Bandwidth Allocation for IEEE 802.11 WLAN with Hidden Terminals", ***Journal of Parallel and Distributed Computing***, 71(9) , 1201-1214, 2010.

17. Bayilmis, C., Erturk, I., Ceken, C., Ozcelik, I., "A Can/IEEE 802.11b Wireless Lan Local Bridge Design", ***Computer Standards & Interfaces*** , 30(3), 200-212, 2008.

18. Boulmal, M., Barka E., Lakas A , "Analysis of The Effect of Security on Data and Voice Traffic in WLAN.", ***Computer Communications***, 30(11-12), 2468-2477, 2007.

19. Barbeau, M., "Mobile Wireless Network Security", ***Handbook on Securing Cyber-Physical Critical Infrastructure***, United States of America, 103‑112, 2012.

20. Rowan, T., "Negotiating WiFi Security", ***Network Security*** 2010(2), 8-12, 2010

21. Zukerman, "Speed Addicts Push The Wireless Boundaries Beyond Wi-Fi", ***The New Scientist***, 205(2749), 20-21, 2010.

22. *Kocak, T., Jagetia, M., "A WEP post-processing algorithm for a Robust 802.11 WLAN implementation",* **Computer Communications***, 31(14), 3405-3409, 2008.*

23. Katz, F., "WPA vs. WPA2: Is WPA2 Really an Improvement on WPA", ***Computer Security Conference***, Coastal Carolina University, 2010.

24. Gold, S., "Why WPA Standards Won't Protect your Network", ***Infosecurity***, 7(1), 28-31, 2010.

25. Arbaugh, W., Edney, J., "Real 802.11 security: Wi-fi protected access and 802.11i",***Wesley professional***, 169-185, 2003.

26. Dantu, R., Clothier G., Atri, A., "EAP methods for wireless networks", ***Computer Standards & Interfaces***, 29(3) , 289-301, 2007

27. Kula, G., "Gelişmiş Şifreleme Standardı Blok Şifreleme Algoritmasının Bir Mikroişlemci Üzerinde Gerçeklemesine Yan Kanal Saldırısı", Yüksek Lisans Tezi, ***İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 29-32, 2009.

28. Hori, Y., Sakurai, K., "Security Analysis of MIS Protocolon Wireless LAN comparison with IEEE802.11i", ***Mobility Conference***, Thailand, 2006.

29. Chen, Y., Yang, J., "Defending Against Identity-Based Attacks in Wireless Networks", ***Handbook on Securing Cyber-Physical Critical Infrastructure***, United States of America, 191-222, 2012.

30. Chen, Y., Yang, J., Trappe, W., Martin ,R., "Detection and Localizing Identitu-Based Attacks in Wireless and sensor Network", ***IEEE Trans vehicular technol***, 59(5), 2418-2434, 2010.

31. Konorski, J., "A Station Strategy to Deter Backoff Attacks in IEEE 802.11 LANs", Journal of Discrete Algorithms, 5(3), 436-454, 2007

32. Beitollahi, H., Deconinck, G., "Analyzing Well-Known Countermeasures Against Distributed Denial of Service Attacks", 35(11), 1312-1332, 2012.

33. Bicakci, K., Tavli ,B., "Denial-of-Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks", ***Computer Standards & Interfaces*** 31 (5), 931–941, 2009.

34. Krishnan, N., Saravanan, V., "Defending Denial of Service: State Overload Attacks", ***Int. J. Advanced Networking and Applications***, 2(3), 719-722, 2010.

35. Wang, F., Wang, H., Wang, X., Su, J,. "A New Multistage Approach to Detect Subtle DDoS Attacks", ***Mathematical and Computer Modelling***, 55(1-2), 198-213, 2012.

36. Gupta, B., Joshi, R., Mirsa, M., "Ann Based Scheme to Predict Number of Zombies in DDoS Attack", ***International Journal of Network Security*** 14(1), 35-46, 2012.

37. Prowell, S., Kraus, R., Borkin, M., "Password Replay", ***Seven Deadliest Network Attacks***, United States of America, 121-137, 2010

38. Zhu Lu, J., Zhou, J., "Preventing Delegation-Based Mobile Authentications From Man-In-The-Middle Attacks", ***Computer Standards & Interfaces***, 34(3), 314-326, 2012

39. Prowell, S., Kraus, R., Borkin, M., "Man-In-The-Middle", ***Seven Deadliest Network Attacks***, United States of America, 101-120 , 2010

40. Khan, L.A., Baig M.S., Hassan, A., "Crypt Analysis of Two Time Pads in Case of Compressed Speech", Computers & Electrical Engineering, 37(4), 559-569, 2011

41. Hancke, G.P., Mayes K.E., Markantonakis, K., "Confidence in Smart Token Proximity: Relay Attacks Revisited", ***Computers & Security***, 28(7), 615-627, 2009

42. Gold, S., "Cracking Wireless Networks" ***Network Security***, 2011(11), 14-18, 2011

43. Seop, Park, C., "Two-way Handshake Protocol for Improved Security in IEEE 802.11 Wireless LANs", ***Computer Communications***, 33(9), 1133-1140, 2010.

44. Nose, P., "Security Weaknesses of Authenticated Key Agreement Protocols", ***Information Processing Letters***, 111(14), 687-696, 2011

45. Haines, B., "Bad Encryption", ***Seven Deadliest Wireless Technologies Attacks***, 89-102, 2010.

46. Feitelson, D., "Perpetual Development: A model of The Linux Kernel Life Cycle", ***Journal of Systems and Software***, 85(4), 859-875, 2012

47. Ali, S., Heriyanto, T., "BackTrack4 Assuring Security by Penetration Testing" ***Packt Publishing Ltd***, Birmingham, 9-15, 2011.

48. Wilhelm, T., "Vulnerability Identification", Professional Penetration Testing − Creating and Operating a Formal Hacking Lab, 259-284, 2010

49. İnternet : Wikipedia "BackTrack", http://en.wikipedia.org/wiki/BackTrack, (2012)

50. Lashkari, A, H., Mansoori, M., "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)", International Conference on Signal Processing Systems, 445-449, 2009.

51. Beck, M., Dresden, T. "Practical Attacks against WEP and WPA", November, 1-12, 2008.

52. İnternet: "IEEE 802.11i and Wireless Security", http://www.eetimes.com/ discussion/other/ 4025006/IEEE-802-11i-and-wireless-security.

53. İnternet: Wi-Fi Protected Setup, http://kb.netgear.com/app/answers/detail/a_id/96/~/what-is-wi-fi-protected-setup-(wps)-or-netgear's-push-'n'-connect%3F, (2012).

54. İnternet: Wi-Fi Protected Setup , http://linksys-de.custhelp.com/app/answers/detail/a_id/17334/~/wi-fi-protected-setup-(wps), (2009).

55. İnternet: Wikipedia "Wi-Fi Protected Setup", http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup, (2012).

56. Anil, S, K., Bharat, M., "WLAN Security Active Attack of WLAN Secure Network (Identity Theft)", ***International Journal of Computer Science,*** 8(3) 555-559, 2011.

57. Nazmus, S., "Security Improvement of WPA 2 (Wi-Fi Protected Access 2)", ***International Journal of Engineering Science and Technology***, 3(1), 0975-5462, 2011.

58. İnternet: Viehböck, S., "Brute Forcing Wi-Fi Protected Setup", http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf, (2011).

59. İnternet: WiFly The Most Convenient Wi-Fi Network Service, http://www.wifly.com.tw/Wifly7/en/, (2011).

60. İnternet: Heffner, C., "Cracking Wi-Fi Protected Setup with Reaver", http://www.tacnetsol.com/news/cracking-wi-fi-protected-setup-with reaver.html, (2011).

61. İnternet: Jared, A., "Vulnerability Note VU#723755 WiFi Protected Setup (WPS) PIN brute force vulnerability", http://www.kb.cert.org/vuls/id/723755, (2011).

62. İnternet: Sean, G., "Hands-on: Hacking WiFi Protected Setup with Reaver" http://arstechnica.com/business/2012/01/hands-on-hacking-wifi-protected-setup-with-reaver, (2012).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : ABDULKAREEM, Mustafa

Uyruğu : Irak

Doğum tarihi ve yeri : 08.10.1985, Kerkük

Medeni hali : Bekar

Telefon : 05392501440

e-mail : mustafa_menaf@yahoo.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	Kerkük Üniversitesi / Bilgisayar Bilimleri	2008
Lise	Kerkük Lisesi	2004

Yabancı Dil

İngilizce, Arapça