T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

KABLOSUZ AĞ GÜVENLİK PROTOKOLLERİNİN İNCELENMESİ VE PERFORMANS KARŞILAŞTIRMASI

Hassan ABDI MOHAMED

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Danışman

Yrd. Doç. Dr. Derya YILTAŞ KAPLAN

Haziran, 2015

İSTANBUL

Bu çalışma 11/06/2015 tarihinde aşağıdaki jüri tarafından Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği programında Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Jürisi:

Yrd.Doç.Dr. Derya YILTAŞ KAPLAN (Danışman)
İstanbul Üniversitesi
Mühendislik Fakültesi

Prof.Dr. Ahmet SERTBAŞ
İstanbul Üniversitesi
Mühendislik Fakültesi

Prof.Dr. A. Halim ZAİM
İstanbul Ticaret Üniversitesi
Mühendislik ve Tasarım Fakültesi

Doç.Dr. Hakan DOĞAN
İstanbul Üniversitesi
Mühendislik Fakültesi

Yrd.Doç.Dr. G. Zeynep GÜRKAŞ AYDIN
İstanbul Üniversitesi
Mühendislik Fakültesi

ÖNSÖZ

Her şeyden önce, bu tezi tamamlamak için gerekli olan sağlık ve sıhhati bana bahşeden Yüce Allah'a şükrediyorum. Ayrıca danışmanım Yard. Doç. Dr. Derya YILTAŞ KAPLAN'a gönülden teşekkürlerimi sunuyorum. Değerli görüş ve yorumları, rehberliği ve desteği için kendisine çok müteşekkir ve minnettarım. Bu tez çalışmam boyunca doğrudan ya da dolaylı olarak yardımlarını esirgemeyen herkese minnettar olduğumu belirtmek isterim.

Yüksek mühendislik çalışmalarımda benden yardımlarını esirgemeyen ve hayatım boyunca benim için fedakârlıkta bulunmaktan çekinmeyen aileme en içten teşekkür ve minnetlerimi sunuyorum.

Bu çalışmayı aileme ve arkadaşlarıma ithaf eder ve kendilerine teşekkürlerimi sunarım.

Haziran, 2015 Hassan ABDI MOHAMED

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

KISALTMALAR

IEEE	Institute of Electrical and Electronics Engineering
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network
WEP	Wired Equivalent Privacy
WPA	WiFi Protocted Access
WPA-2	WiFi Protected Access -2
AP	Access Point
irDA	InfraRed Data Association
MAC	Media Access Control
PHY	Physical Layer
BSS	Basic Service Set
STAs	Stations
IBSS	Independent Basic Service Set
ESS	Extended Service Set
SOHO	Small Offices, Home Offices
OFDM	Orthogonal Frequency-Division Multiplexing
QPSK	Quadrature Phase Shift Keying
CCK	Complementary Code Keying
MIMO	Multiple Input, Multiple Output
ISM	Industrial Science and Medical
SSID	Service Set Identifier
RC4	Rivest Chipher 4
PRGA	Pseudo-Random Generation Algorithm
ICV	Integrity Check Value
IV	Initialization Vector
RADIUS	Remote Authentication Dial In User Service

TKIP	Temporary Key Integrity Protocol
MIC	Message Integrity Code
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code
WPA-PSK	Wi-Fi Protected Access-Pre-shared Key
WPA2-PSK	WiFi Protected Access 2-Pre-shared Key
DOS	Denail Of Service
ARP	Address Resolution Protocol
CRC-32	Cyclic Redundancy Code
PTW	Physhkin Tews Weinmann
FMS	Fluhrer Mantin and Shamir
CBC-MAC	Chipher Block Chaining –Message Authentication Code
AES	Advanced Standard Encryption
EAP	Extention Authentication Protocol
NAS	Network Access Server
AS	Authentication Server
PMK	Pairwise Master Key
SSL	Secure Sockets Layer
TLS	Transport Layer Security

ÖZET

YÜKSEK LİSANS TEZİ

KABLOSUZ AĞ GÜVENLİK PROTOKOLLERİNİN İNCELENMESİ VE PERFORMANS KARŞILAŞTIRMASI

Hassan ABDI MOHAMED

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Yrd.Doç.Dr. Derya YILTAŞ KAPLAN

Günümüz dünyasında teknoloji günlük hayatımızın önemli bir parçasını oluşturmaktadır; ayrıca günlük hayatımızda Ethernet'ten kablosuz ağlara kadar uzanan yelpazede taşınabilirlik ve esneklik için sürekli artan bir talep bulunmaktadır. Kablosuz ağ kavramı ilk olarak 20 yıldan uzun bir süre önce önerilmiş olsa da Kablosuz Yerel Alan Ağı (WLAN) teknolojilerinin ilk ortaya çıkışı 1990'ların sonlarıdır.

Bu çalışma temel olarak IEEE 802.11a/b/g /n/ac spesifikasyonları ve özellikle IEEE 802.11n standardına dayalı WLAN için bulunan güvenlik protokollerinin analizi üzerine odaklanmaktadır. Mevcut hücresel ağlarla karşılaştırıldığı zaman bir WLAN sistemi çok daha yüksek iletim oranlarına ve daha düşük iletim mesafesine sahiptir.

Bu tezde kablosuz güvenlik protokollerinin performansını analiz ettik ve WEP 64bit, WEP 128bit, WPA-PSK/WPA2-PSK gibi farklı kablosuz güvenlik protokollerinin şifre kırma testlerini açıkladık.

Bu çalışmanın ilk bölümlerinde konunun genel bakışına ve literatür araştırmasına odaklandık. İkinci bölümde, ilk ikisi WEP 64 /128 bit ve WPA-PSK/WPA2-PSK güvenlik protokollerinin şifre kırma süreçlerini gösteren üç uygulamayı gerçekledik. İlk iki uygulama boyunca tüm kablosuz güvenlik protokollerinin kırılabilir olduğuna değindik ve son uygulama ile değişik kablosuz güvenlik protokollerinin ağ performansı üzerine etkisini, TCP veya UDP protokollerinin yerel Ethernet kablosu veya IEEE802.11n kablosuz bağlantısı kullandıkları durumlara göre ölçüm yaptık. Sonuç olarak, kendi ağımızı daha güvenli mekanizmalara uygulayarak ağ yükünün düştüğünü elde ettik.

Haziran 2015, 76.

Anahtar kelimeler: Kablosuz güvenlik protokolleri, kablosuz güvenlik protokollerinin karşılaştırılması, şifre kırma süreçleri, WEP 64/128, WPA-PSK/WPA2-PSK, WLAN güvenlik protokollerinin performans analizi.

SUMMARY

MASTER OF SCIENCE THESIS

ANALYSIS AND PERFORMANCE COMPARISON OF SECURITY PROTOCOLS FOR WIRELESS NETWORKS

Hassan ABDI MOHAMED

İstanbul University

Institute of Graduate Studies in Science and Engineering

Computer Engineering

Supervisor: Assist.Prof.Dr. Derya YILTAŞ KAPLAN

In the current world, technology has become a vital part to our daily lives; moreover, there is an increased demand for mobility and flexibility in our daily life that leads the development from Ethernet to wireless networks. Although the concept of a wireless network was firstly proposed more than two decades ago, but in late 1990 Wireless Local Area Network (WLAN) technologies emerged.

This study mainly focus on the analysis of security protocols for WLAN based on IEEE 802.11a/b/g /n/ac specifications especially the IEEE 802.11n standard. Compared with the current cellular networks, a WLAN system has much higher transmission rates and shorter transmission range.

In this dissertation we analyzed the performance of wireless security protocols and also described the cracking tests for different wireless security protocols such WEP 64bit, WEP 128bit, WPA-PSK/WPA2-PSK.

In the first sections of this study we focused on the general overview and literature review of the topic. In the second section, we performed three applications in which the first two demonstrates the cracking processes of WEP 64 /128 bit and WPA-PSK/WPA2-PSK security protocols. During the first two applications we noticed that all wireless security protocols are breakable. The last application measures impact of different wireless security protocols on the network performance in case of TCP protocol or UDP protocol while using local Ethernet cable or IEEE802.11n wireless connection. Consequently, we obtained that the network throughput decreased as we implemented our network to more secure mechanisms.

June 2015, 76.

Keywords: Wireless security protocols, comparisons of wireless security protocols, cracking processes, WEP 64/128, WPA-PSK/WPA2-PSK, performance analysis of WLAN security protocols.

1. GİRİŞ

1.1. KABLOSUZ AĞLARA DUYULAN İHTİYAÇ

Günümüz dünyasında teknoloji gündelik yaşamımızın önemli bir parçası haline gelmiştir, üstelik gündelik yaşamımızda artan taşınabilirlik ve esneklik talepleri ethernetten kablosuz ağlara doğru gelişimin önünü açmıştır. Ayrıca, küresel ağa erişim ilk radyo ve telefondan cep telefonu, dizüstü bilgisayar gibi mevcut cihazlara geldikçe hayatımızın değişmez bir parçası haline gelmiştir. Bu nedenle, bireylerin ve işverenlerin dizüstü bilgisayarlara sahip olduğunu ve daha fazla boş zaman geçirdiğini görüyoruz.

1.2. KABLOSUZ TÜRLERİ VE STANDARTLARI

Bu bölümde kablosuz türlerini ve bunların mevcut kablosuz veri iletişimi standartlarını kısaca anlatacağız.

Kablosuz ağ fikri, ilk olarak 20 yıldan fazla bir süre önce ortaya atılmış olsa da, kablosuz yerel alan ağı teknolojileri ilk kez 1990'ların sonunda kullanılabilir hale gelmiştir. Bu dönemde farklı üreticiler 900 MHz frekans aralığında çalışan ürünleri tanıtmaya başlamışlardır.

Aşağıda en yaygın kablosuz ağ türleri verilmiştir.

- Kablosuz Kişisel Alan Ağları (WPAN)

Bluetooth ve Kızılötesi Veri Birliği (IrDA), kablosuz kişisel alan ağları için iki ana teknoloji olup, IEEE 802.15 standardına dayanır. Bunlar, yaklaşık 10 metrelik (30 feet) bir alan içinde kişisel cihazların bağlantısını sağlar.

- Kablosuz Yerel Alan Ağları (WLAN)

Bu tür kablosuz ağlar kullanıcıların üniversite yerleşkesi ya da kütüphanelerde bir ağ kurmasını ya da internete erişmesini sağlar. Bir erişim noktasına (AP) gerek olmadan

küçük bir bilgisayar grubuyla geçici bir ağ oluşturulabilir, bu kablosuz ağlar IEEE 802.11 ve HiperLan/2 standartlarını kullanır.

- Kablosuz Metropolitan Alan Ağları (WMAN)

Bu tür kablosuz ağlar bir şehir içinde birden fazla farklı binanın bağlantısını sağlar. Bu ağlar IEEE 802.16 standardını kullanır.

- Kablosuz Geniş Alan Ağları (WWAN)

Bu ağ türü, şehir ya da ülkeler gibi geniş alanlar arasında çoklu uydu sistemleri ya da bir Internet servis sağlayıcı tarafından kontrol edilen anten sistemleri aracılığıyla kurulabilir.

1.3. WLAN'A GENEL BAKIŞ

Kablo altyapısı kullanan kablolu ağların aksine, WLAN radyo dalgalarını kullanarak iş istasyonları arasında konumdan bağımsız ağ erişimi sağlayan bir veri aktarım sistemidir.

WLAN'ın gelişim sürecinde, Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) 1997'de ilk 802.11 ölçüsünü WLAN standardı olarak kabul etmiştir.

Kablolu ve kablosuz ağ arasındaki temel fark iki şekilde kendisini gösterir.

Birincisi, kablolu ve kablosuz ağların kullandığı veri aktarım aracıdır; örneğin, kablolu ağlar (Ethernet) veri aktarımı için bakır kablo ya da başka fiziksel araç kullanırken, WLAN aktarım için havayı araç olarak kullanır. Ethernet ağı kullanıcıları esnekliğe sahip olmadığı için kullanıcılar bir konumda sabit olmalıdır.

İkincisi ise kullanıcıların ağa nasıl eriştiğidir. Kablolu yerel alan ağına erişen kullanıcılar fiziksel bir ethernet kablosuna ihtiyaç duyarken, WLAN'a erişen kullanıcıların yalnızca kablosuz sinyalin alanı içinde bulunmaları gerekmektedir ve bu alan içinde bir yerden diğerine hareket etme esneklikleri vardır.

Kısacası, Ethernet ağı (kablolu) ve kablosuz ağ arasındaki temel fark, birinin fiziksel kablo kullanması (bakır kablo, çift bükümlü, fiber kablo) diğerinin ise radyo frekanslarını kullanmasıdır. [1]

Bilindiği üzere kablosuz ağlar ortaya çıkışlarından itibaren kablolu ağlara göre pek çok avantaja sahip olmuştur ve bu avantajların en önemlisi taşınabilirlik olup sizi Ethernet kablosu kullanma zorunluluğundan kurtarır.

Bununla birlikte, kablosuz ağlar kablolu ağlara göre başka avantajlara da sahip olup bu avantajlar esneklik, kurulum hızı ve kolaylığı ve kurulum maliyetidir.

WLAN için en yaygın teknolojiler hizmet amaçlarına göre farklı kategorilere ayrılabilir. Dünyada, telekomünikasyon şirketleri hücresel ağları üzerinden ses ve veri aktarımında önemli ilerleme kaydetmektedir.

- Bluetooth (IEEE 802.15), kişisel bir alanda (genelde 10 metreden az) taşınabilir cihazlar için düşük maliyetli ve kısa mesafeli bağlantı sunar.
- Wi-Fi (IEEE 802.11): Wi-Fi; yerel bir alan ağında, bir şirket ya da yerleşke binası içinde kullanıcıların kablosuz bağlantılar kurmalarını sağlayan, IEEE 802.11 WLAN standartlarının Wi-Fi Birliği tarafından sertifikalanmış, birlikte çalışabilir uygulamaları anlamına gelir.
- WiMAX (IEEE 802.16): WiMAX; bir metropol alan ağında, kullanıcılara yüksek hızlı geniş bant internet erişimi sağlayan, WiMAX Forumu tarafından kabul edilmiş, IEEE 802.16 kablosuz ağ standartları ailesinin birlikte çalışabilir uygulamaları anlamına gelir.

Bu tez, IEEE 802.11a/b/g/n/ac ve özellikle IEEE 802.11n standardını temel alan WLAN güvenlik protokollerinin analizi üzerinde duracaktır. Mevcut hücresel ağlarla karşılaştırıldığında, WLAN sistemi çok daha yüksek aktarım hızına ve daha kısa aktarım mesafesine sahiptir.

Ancak, WLAN'ın yaygınlaşmasıyla birlikte, kablosuz aracının belirli bir mesafe içinde genel erişime açık olması nedeniyle güvenlik önemli bir konu haline gelmiştir.

1.4. TEZİN AMACI

Günümüzde, kablosuz ağ bağlantısı kullanıcıları giderek artmaktadır ve kablosuz ağlarda güvenlik ciddi bir konu haline gelmiştir. Güvenlik amacıyla WEP, WPA, WPA2 ve IEEE 802.11i gibi farklı protokoller geliştirilmiş ve uygulanmıştır.

Bu çalışmanın genel amacı kullanımdaki mevcut kablosuz ağ yapılarını ve kablosuz ağ standartlarını kısaca açıklamak ve WLAN standartlarını ve güvenlik mekanizmalarını detaylı bir biçimde incelemektir. Bu çalışmanın ilerleyen bölümlerinde, WEP ve WPA-PSK temelli kablosuz ağların kırılması, kablosuz güvenlik protokollerinin performanslarının değerlendirilmesi ve şifreleme algoritmalarının bu performansı nasıl etkilediği anlatılacaktır.

Bu tez, WLAN'ların güvenlik sorunlarını inceleyecek, mevcut kablosuz ağ güvenliği yöntemlerini ve bu yöntemlerin zayıf noktalarını karşılaştıracak ve en iyi kablosuz güvenlik protokolleri için önerilerde bulunacaktır.

1.5. TEZİN SINIRLANDIRILMASI

Bu tez, WLAN'ların ilk kez kullanıma sunulduğu 1990 yılından tezin yazıldığı Haziran 2015'e kadar yapılan çalışma ve kaynak incelemelerinin bir kısmıyla sınırlıdır.

2. GENEL KISIMLAR

2.1. IEEE 802.11 WLAN MİMARİSİ VE STANDARTLARI

2.1.1. 802.11 WLAN Mimarisi

Bu tezde WLAN ile kastettiğimiz şey, uygulamalarda ortam erişim denetimi (MAC) ve fiziksel katman (PHY) standartlarını oluşturan spesifikasyonlar dizisi olan IEEE 802.11'dir.

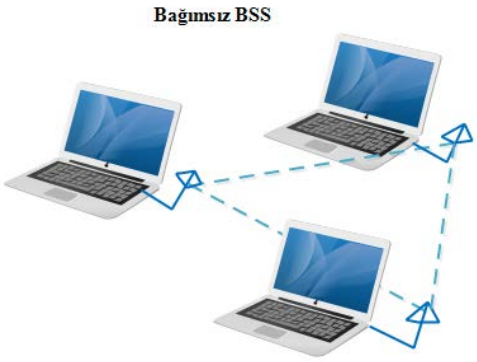
Wi-Fi ağında; taşınabilir ya da sabit olduğuna bakılmaksızın tüm cihazlara kablosuz istasyonlar (STA'lar) adı verilir ve bu cihazlar PC, dizüstü bilgisayar ya da başka cihazlar olabilir. Böylece iki veya daha fazla STA kablosuz olarak birbirine bağlanmış olur ve BSS (temel hizmet seti) adı verilen Wi-Fi ağının temel yapı taşını oluşturur. [2]

Bu BSS kapsamı, mantıksal bir işlev olan tek bir koordinasyon işlevi aracılığıyla yönetilir ve bu koordinasyon işlevi STA'lar arasındaki veri aktarımını, örneğin bir STA veri gönderdiğinde ya da aldığında tespit eder.

Aşağıdaki bölümde IEEE 802.11 standardında belirtilen iki çalışma mimarisini tartışacağız. Tüm STA'ların bir Wi-Fi ağı oluşturmadan ya da bir ağa bağlanmadan önce bir çalışma modu seçmesi gerekir.

2.1.1.1. Ad-hoc Modu (IBSS)

Bu mimaride, eşler arası bağlantı oluşturmak için her istemci bir diğeriyle doğrudan iletişime geçer, bu nedenle bu mod sadece aynı aktarım alanı içindeki istemcilere yöneliktir. Bir istemcinin hücre dışındaki başka bir istemciyle iletişime geçmek istemesi durumunda, alan içindeki istemcinin bir ana kapı ya da yönlendirme testi olarak çalışması gerekir. Bu mod en basit Wi-Fi ağı türüdür, STA'lar ad-hoc çalışma modunu kullanarak birbirleriyle doğrudan iletişime geçer.



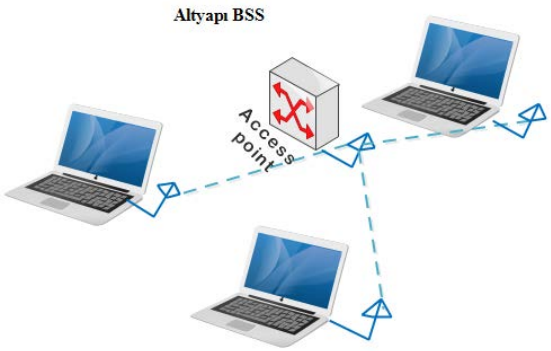
Şekil 2.1: Bağımsız BSS [3]

Bu ağ, tipik olarak kısa süreliğine az sayıda STA içerir ve genellikle bir konferans odasındaki tek bir toplantıyı destekleme gibi kısa süreli bir ağ kurulumunda kullanılır.

2.1.1.2. Altyapı Modu (ESS)

Altyapı modunda kablosuz ağ tüm bilgisayarların bağlı olduğu bir merkezi AP'ye sahiptir, yani ağın, kablolu ağ altyapısına bağlı en az bir AP ve kablosuz son kullanıcıları olması gerekir.

Altyapı modunda BSS ek işlevlere sahip en az bir kablosuz AP'ye sahiptir, böylece AP Ethernet ağı erişimini kablosuz ağ istasyonlarına açar.



Şekil 2.2: Altyapı BSS [3]

2.1.2. IEEE 802.11 WLAN / Wi-Fi Standartları

WLAN teknolojileri ilk olarak 1990'da, bazı kablosuz ağ aygıtı üreticilerinin 900 MHz radyo frekansında çalışan ürünler tanıtmaya başlamasıyla kullanılabilir hale gelmiştir.

IEEE, 1997'de günümüzde kullanımdan kalkmış olan ilk WLAN standardını tanıtmış ve bu standardı 802.11 olarak adlandırmıştır. 802.11 WLAN standartları, fiziksel katman ve veri bağlantısı katmanları olan OSI ağ modelinin en düşük katmanını oluşturmakta olup bu standartları belirlemenin amacı fiziksel katmana farklı yaklaşımlar, örneğin; farklı frekanslar, farklı kodlama yöntemleri ve aynı yüksek katmanların paylaşılması gibi, getirmektir.

Maalesef 802.11 başlangıçta, çoğu uygulama için çok yavaş olan 2 Mbps maksimum ağ bant genişliğini desteklemiştir.

Kısacası, 802.11'i kablosuz ağ aktarım yöntemlerini denetleyen bir IEEE standartlar dizisi olarak tanımlayabiliriz ve günümüzde SOHO (küçük ofisler ve ev ofisler)'larda, işletmelerde ve kuruluşlarda kablosuz bağlantı sağlaması amacıyla kullanımda olan en yaygın kablosuz standartları 802.11a, 802.11b, 802.11g, 802.11n ve 802.11ac dir.

Gelecek bölümlerden itibaren, günümüzde kullanımda olan en yaygın kablosuz standartlarını ayrıntılandıracak ve bu standartları karşılaştıracağız.

2.1.2.1. IEEE 802.11a

IEEE, 1999 yılında 5 GHz bandında veri aktarımı sağlayan ve 54 Mbps maksimum teorik veri hızına sahip olan IEEE 802.11a standardını onaylamıştır. Bu hız IEEE 802.11g standardının veri hızıyla aynıdır. Bu standart büyük ölçekli kurumsal işyerlerinde uygulamaya konulmuştur. Bu standart, etkili bir kodlama tekniği olan Dikey Frekans Bölmeli Çoklama (OFDM)'yı kullanır. Bu teknik, radyo sinyalleri alıcıya ulaşmadan önce onları birkaç alt sinyale ayırır bundan dolayı OFDM kodlama tekniğinin kullanılması sayesinde bu standartta sinyaller arasında daha az radyo paraziti oluşur. [4] [5]

Bu standartta, güçyitirim halinde -frekanstaki yüksek parazitten ya da cihazlar arasındaki yüksek binalar gibi engellerden dolayı sinyal gücünün zayıflaması anlamına gelir- iş istasyonu ve AP gibi kablosuz ağ cihazları arasındaki bağlantının sürdürülmesi için veri hızı otomatik olarak daha düşük hızlara (54/48/36/24/12/9/6 Mbps) ayarlanır.

2.1.2.2. IEEE 802.11b

Bu standart da IEEE tarafından IEEE 802.11a standardıyla aynı zamanda kabul edilmiştir, ancak bunda IEEE 802.11a standardında kullanılan kodlama tekniğinden farklı bir kodlama tekniği kullanmaktadır. Bu standart, 64 adet 8 bit sözcük ve QPSK (Dörtlü Faz Kaydırmalı Anahtarlama) modülasyon tekniğinden oluşan gelişmiş bir kodlama tekniği olan Tamamlayıcı Kod Anahtarı (CCK) kullanır. [4] [5]

IEEE 802.11b işletme ve kurumsal kablosuz ağlarında lider olarak görülse de IEEE 802.11b'nin de bazı eksiklikleri vardır, bu da bu standardın ses cihazlarında multimedya içeriği ve birlikte çalışabilirlik için servis kalitesi (QoS) sunmamasıdır.

2.1.2.3. IEEE 802.11g

IEEE 802.11g standardı Haziran 2013'te kabul edilmiştir. Bu standart IEEE 802.11a ve IEEE 802.11b standartlarını birleştirmekte olup, bu da bu standardın 2.4 GHz ISM bandında çalıştığı (IEEE 802.11b gibi) ve IEEE 802.11a da kullanılan OFDM aktarım şemasını kullandığı anlamına gelir. Bu standart, önceki standart ile (IEEE 802.11b) geriye uyumludur. [4] [5]

İş istasyonu ve AP gibi kablosuz ağ cihazları arasındaki artan mesafe nedeniyle sinyal kaybı oluşarak güçyitirim adı verilen bir sorun meydana gelebilir, bu sorun frekanstaki yüksek parazit ya da cihazlar arasındaki yüksek bina gibi engeller nedeniyle sinyal gücünün zayıflamasıyla meydana gelir. Bu durumda, bağlantının sürdürülebilmesi için veri hızı otomatik olarak daha düşük hızlara (54/48/36/24/12/9/6 Mbps) ayarlanır.

2.1.2.4. IEEE 802.11n

Bazen 802.11n-2009 olarak da yazılan bu kablosuz ağ standardı, IEEE 802.11-2007 kablosuz ağ standardı üzerinde yapılan bir değişikliktir. IEEE 802.11-2007, 8 değişikliği (IEEE 802.11a, IEEE 802.11b, IEEE 802.11d, IEEE 802.11e, IEEE 802.11g, IEEE 802.11h, IEEE 802.11i) birleştiren tek bir dökümandır ve 8 Mart 2007'de kabul edilmiştir. IEEE 802.11n, IEEE 802.11g'nin yerine geçmiştir.

Bu standart önceki IEEE 802.11 standardına dayalı olup Çoklu Giriş Çoklu Çıkış (MIMO) teknolojisini eklemiştir. Bu teknoloji tek anten yerine daha fazla bilgiyi çözümlemek için birden fazla anten, PHY (fiziksel katman)'lerde 40 MHz kanalları -

veri aktarımında önceki 802.11 PHY'lerinde kullanılan 20 MHz kanal genişliğini ikiye katlar- ve MAC katmanında çerçeve toplamını kullanır.

Bu WLAN standardı; Sınai, Bilimsel ve Tıbbi Cihaz (ISM) frekans bantları olan IEEE 802.11b (2.4 GHz) ve IEEE 802.11a (5 GHz) frekans bantlarında çalışır.

2.1.2.5. IEEE 802.11ac

IEEE 802.11ac, IEEE 802.11 ailesindeki en yeni kablosuz ağ standardı olup 5 GHz frekans bandında çalışan WLAN yüksek veri hacmi sağlar. Bu standardın gelişim süreci 2011'den 2013'ün sonuna kadar sürmüş ve standart Ocak 2014'te kabul edilmiştir.

Tablo 2.1: En yaygın IEEE 802.11 WLAN standartlarının karşılaştırılması [4]

Parametreler	**IEEE 802.11a**	**IEEE 802.11b**	**IEEE 802.11g**	**IEEE 802.11n**	**IEEE 802.11ac**
Frekans Bandı	5 GHz	2.4 GHz	2.4 GHz	2.4 – 5 GHz	5.0 GHz
Veri hacmi	23 Mbit/s	4.3 Mbit/s	19 Mbit/s	74 Mbit/s	1 Gbit/s
Hız	54 Mbps	11 Mbps	54 Mbps	248 Mbps	500 Mbps – 1000 Mbps
İç mekan Alanı	35 mt	38 mt	38 mt	70 mt	12 - 35 mt
Dış mekan Alanı	120 mt	140 mt	140 mt	250 mt	--

2.1.2.6. Diğer standartlar

IEEE 802.11 WLAN standartları ailesinde, yukarıda bahsettiğimiz yaygın kullanımdaki standartların hatalarını düzelten, güvenlik sorunlarını çözen ve güvenlik zaaflarını güçlendiren yaygın olmayan başka standartlar bulunmaktadır ve bunlar daha önceki standartların spesifikasyonları üzerinde yapılan hizmet değişiklikleri, eklentileri ya da düzeltmeleridir. Aşağıdaki tabloda IEEE 802.11 standardı için tüm kablosuz standartlar işlevleri ve yayınlanma tarihleriyle birlikte görülmektedir. [4] [5]

Aşağıdaki tablo mevcut ve önceden planlanmış olup gelecekte uygulamaya geçirilecek olan tüm IEEE 802.11 WLAN standartlarını göstermektedir.

Tablo 2.2: Mevcut ve Gelecekteki WLAN/ Wi-Fi IEEE Standartları [5]

Seri No	**IEEE 802.11 Standardı**	**Yayınlanma Yılı**	**Yorumlar**
1	IEEE 802.11a	1999	54 Mbps hız ve 5 GHz bandı
2	IEEE 802.11b	1999	5.5 ve 11 Mbps hızları desteklemesi için 802.11'de yapılan geliştirmeler
3	IEEE 802.11c	2001	Köprü çalışma prosedürleri; IEEE 802.11d standart 4'e dâhildir
4	IEEE 802.11d	2001	Uluslararası (ülkeden ülkeye) dolaşım eklentileri
5	IEEE 802.11e	2005	Geliştirmeler: QoS, veri genişlemesi dâhil
6	IEEE 802.11f	2003	AP'ler Arası Protokol, Şubat 2006'da geri çekildi
7	IEEE 802.11g	2003	54 Mbps, 2.4 GHz standardı (IEEE 802.11b ile geriye uyumlu)
8	IEEE 802.11h	2004	Avrupa uyumluluğu için Spektrum Kontrollü 802.11a (5 GHz)
9	IEEE 802.11i	2004	Arttırılmış güvenlik
10	IEEE 802.11j	2004	Japonya için eklentiler
11	IEEE 802.11k	2008	Radyo kaynağı ölçümü geliştirmeleri
12	IEEE 802.11n	2009	MIMO kullanılarak yüksek veri hacmi iyileştirmeleri
13	IEEE 802.11p	2010	WAVE - Taşıt Ortamına Kablosuz Erişim
14	IEEE 802.11r	2008	Hızlı BSS geçişi (FT)
15	IEEE 802.11s	Temmuz 2011	Örgüsel Ağ, Gelişmiş Hizmet Kümesi (ESS)
16	IEEE 802.11u	Şubat 2011	Genel Alanlarla ve istemcilerin 3. taraf yetkilendirmesiyle ilgili iyileştirmeler, örneğin hücresel ağ boşaltımı

Tablo 2.2 (devam): Mevcut ve Gelecekteki WLAN/ Wi-Fi IEEE Standartları [5]

17	IEEE 802.11v	Şubat 2011	Kablosuz ağ yönetimi
18	IEEE 802.11w	Eylül 2009	Korumalı Yönetim Çerçeveleri
19	IEEE 802.11x	-	Güvenliğin arttırılması için genişletilebilir kimlik doğrulama ağı
20	IEEE 802.11y	2008	ABD'de 3650-3700 MHz'de çalışma
21	IEEE 802.11z	Eylül 2010	Doğrudan Link Kurulumu (DLS) eklentileri (Eylül 2010)
22	IEEE 802.11aa	Haziran 2012	Ses Görüntü Taşıma Akışlarının güçlü akışı
23	IEEE 802.11ad	Aralık 2012	60 GHz Çok Yüksek Veri Hacmi
24	IEEE 802.11ae	Mart 2012	Yönetim Çerçevelerinin Önceliklendirilmesi
25	IEEE 802. 11ac	Şubat 2014	6 GHz Çok Yüksek Veri Hacmi, 802.11n'ye yapılan önemli iyileştirmeler; daha iyi modülasyon şeması (%10 civarı veri hacmi artışı bekleniyor), daha geniş kanallar (gelecekte 80 ile 160 MHz arasında olması bekleniyor), birden çok kullanıcılı MIMO
26	IEEE 802.11af:	Haziran 2014	TV Aralıklama Karakteri ()
27	IEEE 802.11ah:	Ocak 2016	1 GHz altı sensör ağı, akıllı ölçüm
28	IEEE 802.11ai:	Şubat 2015	Hızlı İlk Link Kurulumu
29	IEEE 802.11mc:	Mart 2015	Standardın bakımı
30	IEEE 802.11aj:	Ekim 2016	Çin Milimetre Dalgası
31	IEEE 802.11aq	Mayıs 2015	İlişkilendirme öncesi Keşif
32	IEEE 802.11ak	-	Genel Link

2.2. WLAN GÜVENLİK PROTOKOLLERİ VE ŞİFRELEME ALGORİTMALARI

Kablosuz ağların ilk dönemlerinde, güvenlik; işletmeler, kuruluşlar hatta ev kullanıcıları için önemli bir endişe konusu olmuştur. Ancak WLAN kullanımının artışıyla birlikte, işletmeler ve kuruluşlar iç ağlarını korumaya daha fazla önem göstermiştir.

Günümüzde kullanılan WLAN ürünleri çoğunlukla IEEE 802.11 standartlarını kullanmaktadır. IEEE 802.11'de, WLAN'daki veri güvenliğini sağlamak için farklı teknolojiler ve protokoller bulunmaktadır.

Gelecek bölümlerde hava dalgaları üzerinden iletilen verilerin dışarıdan dinleyenlere karşı güvenliğinin sağlanması için IEEE 802.11 standardında kullanılan bazı teknoloji ve protokolleri tartışacağız.

2.2.1. Hizmet Seti Tanımlayıcısı (SSID)

Her AP için SSID'ler belirlenerek farklı kullanıcı gruplarına WLAN'a erişim izni verilebilir ve değişken erişim olanakları sağlanabilir. Bu şekilde, kablosuz iş istasyonları ya da devreler doğru SSID'yi vermeden AP'ye erişemez. SSID teknolojisi yetkisiz ya da lisanssız kullanıcıların WLAN'a erişmesini önler. [1]

2.2.2. Ortam Erişim Denetimi (MAC)

MAC, kablosuz ağların güvenliği için IEEE 802.11 standardında geliştirilen güvenlik mekanizmalarından biridir. MAC, ağ kartındaki 48 bitten oluşan çift dizilimdir. MAC adresi her ağ kartını belirlemek için kullanılır, çünkü her kablosuz iş istasyonu benzersiz bir MAC adresine sahiptir.

MAC teknolojisi bir WLAN'a uygulanırken, WLAN'ın her AP'sine devrelerin MAC adres listesi yerleştirilir, böylece bir devre WLAN'a bağlanmak istediğinde AP bu devrenin MAC adres listesinde bulunup bulunmadığını kontrol eder ve eğer devre listede yoksa ağa erişim isteğini reddeder.

Bu teknolojinin tanımından anlayacağımız üzere AP'nin sürekli güncellenmesi gerekir, bundan dolayı MAC listesinin ölçeklenebilirliği zayıftır ve teorik olarak MAC adresleri kolayca taklit edilebilir. Ancak MAC teknolojisi kablosuz ağ iletişimlerinin güvenliğini sağlamada son çözüm değildir.

2.2.3. WEP (Kablolu Eşdeğer Gizlilik)

WEP 1997 yılında IEEE 802.11b çalışma kolu tarafından kablosuz ağların güvenliğini sağlamak ve kablolu ağların güvenlik mekanizmasına eşdeğer bir mekanizma sunmak için geliştirilmiş bir ağ güvenliği protokolüdür. WEP ayrıca kablosuz ağlarda kullanılan ilk şifreleme protokolüdür. [6] [7] [8]

Bu protokol, zaaflarının ve güvenlik açıklarının bulunmasından önce kablosuz bağlantıları bilgisayar korsanlarından korumak, bilgisayar korsanlarının aktarım halindeki verileri izlemesine engel olmak ve kablosuz ağlara yetkisiz erişimi engellemek için kullanılmıştır. WEP 64 bit ya da 128 bit boyutlarında anahtardan oluşan bir şifreleme algoritmasıdır. Bu anahtar, şifreli metnin çözülmesi amacıyla alıcı taraftan istendiği için ortak anahtar da denilen 24 bit başlangıç vektörü (IV) ve 40 bit özel/paylaşımlı anahtar içerir, böylece IV kablosuz iletişim ağı üzerinde aktarılan paket veriye şifrelenmemiş olarak eklenir.

2.2.3.1. RC4 Kesintisiz Şifreleme

Bu kesintisiz şifreleme 1987'de RSA ortak anahtar şifreleme algoritmasının mucitlerinden biri ve RSA Security, Inc. şirketinin kurucu ortaklarından olan Ron Rivest tarafından tasarlanmıştır. Ticari sır olarak saklanan bu kesintisiz şifreleme 1994'te sızdırılmış ve tanımlamaları pek çok web sitesinde yayınlanmıştır.

RC4; WEP, WPA, SSL ya da TSL gibi yaygın pek çok standart ve protokolde kullanılmıştır ancak ne yazık ki bu kesintisiz şifrelemenin bazı zaafları bulunmakta olup artık modern protokollerde kullanılmamaktadır.

WEP, şifreleme ve şifre çözme için RC4 kullandığı için RC4 kesintisiz şifreleme algoritmalarının iki ana bölümüne değinmek önemlidir.

- **Anahtar zamanlama algoritması**

Bu algoritma RC4 algoritmasının iki ana bölümünden biri olup {0,… N-1}'nin S permütasyonunu almak için kullanılır. Bu permütasyon da pseudo random ilk durumu oluşturmak için gizli anahtarı kullanır.
Anahtar zamanlama algoritmasına ilişkin pseudo kodu aşağıdaki gibidir: [9]

```
For i = 0 to N-1     // (where N =256)
        S[i] = i
End
j = 0
For i =0 to N-1      // (where N =256)
        j = (j + S[i] + key [i mod key length]) mod 256
        S[i] ve S[j] değerlerini değiştir
End
```

Yukarıda, anahtar zamanlama algoritmasının pseudo kodundan anlaşılacağı üzere iki döngü vardır: birincisi S dizisini başlatırken, ikincisi diziyi permütasyon dizisi haline getirmek için anahtarı kullanarak diziyi karıştırır.

Permütasyon dizisi oluşturulduktan sonra, anahtar akışını oluşturmak RC4'ün sonraki bölümü devreye girer.

- **Pseudo random oluşturma algoritması**

Bu algoritma RC4 algoritmasının ikinci bölümüdür ve şifrelenecek mesaj boyutunun anahtar akışını oluşturmada kullanılır.
Anahtar akışı oluşturma işlemi iki indeksin 0'a ilklendirilmesiyle yapılır ve şifrelenecek mesajın boyutuna ulaşana kadar tek seferde bir bayt olacak şekilde anahtar akışı başlatılır.

Pseudo random oluşturma algoritmasına ilişkin pseudo kodu aşağıda görülmektedir: [9] [10]

```
i = 0
j = 0
```

While GeneratingOutput

i = (i + 1) mod 256

j= (j + S[i]) mod 256

S[i] ve S[j] değerlerini değiştir

K = S [(S[i] + S[j]) mod 256]

Çıktı K

End while

2.2.3.2. Veri şifrelemesi ve tamlığın korunması

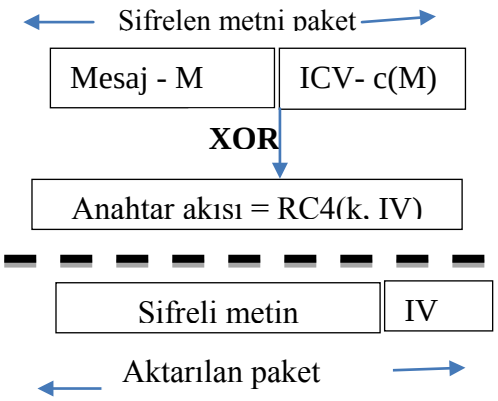
WEP korumalı bir ağda, hat kesintisi iletisi gibi veri olmayan çerçeveler ve korunmayan onay çerçeveleri dışında her veri çerçevesi alıcıya gönderilmeden önce şifrelenir ve tamlığı korunur.

Aşağıda, bir istasyonun veri şifrelemesi için alıcıya bir paket göndermesi sırasındaki adımlar bulunmaktadır.

1. Göndericide, sağlama değeri ya da bütünlük kontrol değeri (ICV) gönderilecek mesajdan hesaplanır ve bu sağlama değeri aktarım sırasında verinin değiştirilmemesi için kullanılır. Böylece hem şifresiz metin hem de ICV birleştirilir; örneğin M'nin şifresiz metin ya da mesaj olduğunu varsayarsak, P'nin sağlama değeri ya da ICV'si CRC 32 algoritmasından elde edilen c(M)'dir. Bu nedenle, P= M + c (M)'dir.
2. Şifreleme anahtarı ya da kesintisiz anahtar oluşturulur. Kesintisiz anahtar RC4 algoritması kullanılarak oluşturulur ve iki alana dayanır: ilk ağ yapılandırmasında doğrudan kodlanmış ve ağın tüm iş istasyonları ve sunucuları tarafından paylaşılan k isimli gizli bir anahtar ve ortak bir anahtar ya da IV. [11] [12]

   yani anahtar akışı = RC4 (k, IV)

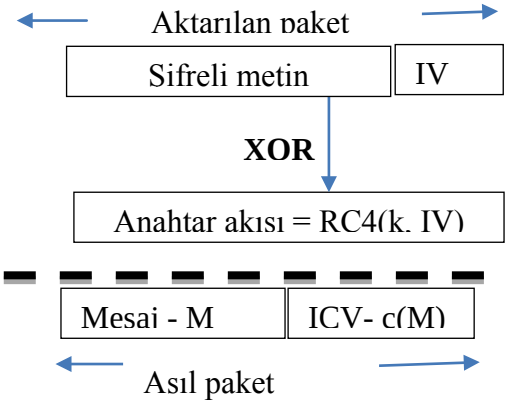
3. Şifreli metin XOR tarafından alınır -yani 2. adımın sonucuyla birlikte 1. adımın sonucu, IV şifreli metnin başına eklenir. C=P +RC4(k,IV);



Şekil 2.3: WEP Şifrelemesi

Yukarıdaki grafikte gördüğümüz üzere şifreli metin, alıcıya ulaşan şifrelenmiş bir veridir ve şifreli metnin yanı sıra pakete eklenen bir ortak anahtar ya da IV de bulunmaktadır, çünkü bu anahtar bu şifreli metnin çözümü için alıcı tarafa lazımdır. Bu ortak anahtar paylaşımlı anahtardan farklıdır ve bunun çözülebilmesi için saldırgan tarafından kırılması gerekir.

Alıcı, şifreli metni elde ettikten sonra şifreli metni şifrelenmemiş metne dönüştürmek için yine aynı işlemi yapar. Ardından verinin aktarım sırasında değiştirilip değiştirilmediğini öğrenmek için verinin tamlığını kontrol eder. Alıcı, verinin tamlığını öğrenmek için önce paylaşımlı anahtarı daha sonra da RC4 algoritmasını kullanarak şifreli metnin başına eklenen anahtar akışını ve IV değerlerini elde eder. Daha sonra XOR'lar oluşturulur. Aktarılan şifreli metin, şifreleme işleminde kullanılan anahtar akışını etkisiz hale getirecektir ve sonuç asıl şifresiz metin olacaktır.



Şekil 2.4: WEP şifre çözümü

Alıcı, tamlığın korunması için şifresi çözülmüş verinin sağlama değerini tekrar hesaplayarak veri tamlığını kontrol eder. Ardından da yeni hesaplanmış sağlama değerini daha önceki sağlama değeriyle karşılaştırır, dolayısıyla iki sağlama değeri aynı değilse alınan veri tam değildir.

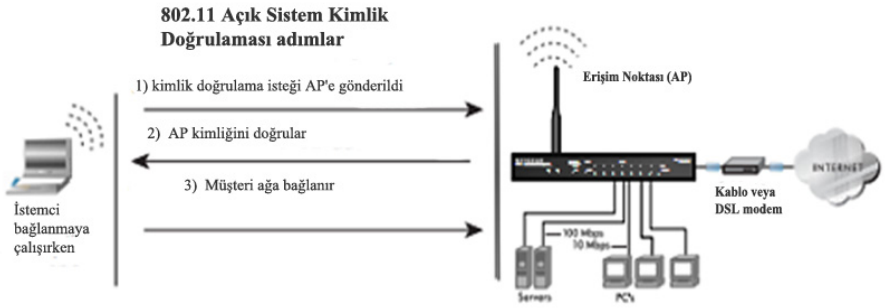
2.2.3.3. Kimlik Doğrulama Yöntemleri

IEEE 802.11 standardı, bir Wi-Fi ağına bağlanmaya çalışırken iki farklı kimlik doğrulama yöntemi belirlemiştir: Açık Sistem ve Paylaşımlı Anahtar Kimlik Doğrulaması.

- WEP Açık Sistem Kimlik Doğrulaması

  Bu açık sistem adından anlaşılacağı üzere SSID'si, AP SSID'siyle eşleşen ve kimlik doğrulama isteğinde bulunan her STA (istasyon)'nın kimliğini doğrular. Bu kimlik doğrulama, istasyon kimliğini içeren basit bir kimlik doğrulama isteği ve başarılı/başarısız verisi içeren bir kimlik doğrulama cevabından oluşur.

  Açık Sistem Kimlik Doğrulaması aşağıda gösterilmektedir [13]:

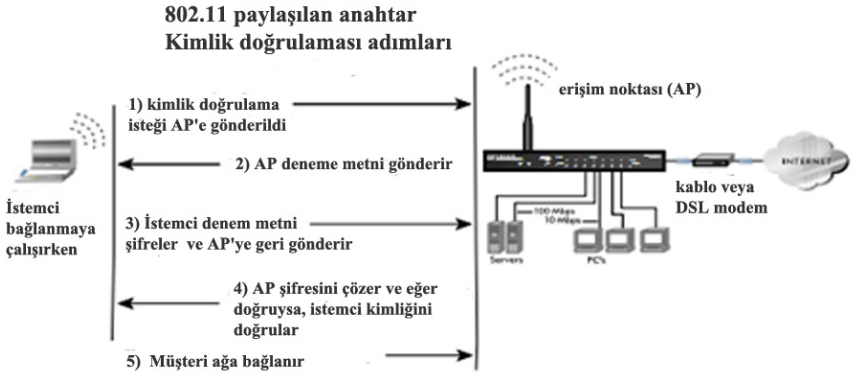


Şekil 2. 5: WEP Açık Sistem Kimlik Doğrulaması

- WEP Paylaşımlı Anahtar Kimlik Doğrulaması

  Paylaşımlı anahtar kimlik doğrulaması, doğrulama için WEP ve paylaşımlı anahtar kullanan standart bir kimlik sorgulama ve cevaplama mekanizmasıdır. Bu yolla AP, istemciye şifrelenmemiş kimlik sorgusu gönderir ve istemci de şifreli kimlik sorgusu metnini onaylanması için AP'ye gönderir. AP aynı kimlik sorgusu metninin şifresini çözerse kimlik doğrulama başarılı olur.

  WEP paylaşımlı anahtar kimlik doğrulaması aşağıdaki şekilde gösterilmektedir[13]:



Şekil 2.6: WEP Paylaşımlı Anahtar Kimlik Doğrulaması.

2.2.3.4. WEP Protokolündeki Güvenlik Açıkları

WEP, mekanizmasındaki açıklar nedeniyle Wi-Fi ağının güvenlik gereksinimini karşılayamaz ve IEEE 802.11 standardındaki kimlik doğrulama, şifreleme ve bütünlük işlemlerini gerçekleştiremez.

WEP Protokolündeki bazı temel açıkları aşağıda inceleyecek ve tartışacağız.

- RC4 Algoritması

WEP, şifreleme ve şifre çözme işlemleri için RC4 algoritması kullanmaktadır ve bazı araştırmalara göre RC4 algoritması her 256 ya da daha az anahtarın bir zayıf anahtar oluşturması nedeniyle zayıftır. Buna değişimsizlik zaafı ismi verilmiş olup bu zayıf anahtarlarla şifrelenmiş veriler bilgisayar korsanlarınca kırılabilir. [14]

- Anahtar yönetimi

WEP, veri paketlerinin şifrelenmesinde her kablosuz cihaz için gizli paylaşımlı bir anahtar kullansa da herhangi bir anahtar yönetimi mekanizması belirtmemiştir. Bağlantı üzerinden ulaştırılan her çerçeve aynı paylaşımlı anahtarı kullanır, bu da bilgisayar korsanlarının WEP şifrelemesini kırma işini kolaylaştırır.

Öte yandan statik WEP anahtarlarının kullanılması -bir kablosuz ağdaki ağ kullanıcılarının potansiyel olarak aynı anahtarı uzun bir süre boyunca paylaşması- iyi bilinen bir güvenlik açığıdır. WEP'te anahtarın oluşturulması ve yenilenmesi için bir mekanizma bulunmamaktadır. [15] [14]

- Anahtar akışının tekrar kullanılması

WEP'te IV ya da ortak anahtar, alıcıya şifresiz metin içerisinde iletilen 24 bit ikili dizilimdir. Bu IV 16777216 olası sonuca sahip olabilir, ancak bahsedildiği gibi anahtar boyutu çok küçüktür ve anahtar akışı kolayca tekrar kullanılabilir. Üstelik WEP'te IV ya da ortak anahtarın tekrar kullanımını önleyecek bir mekanizma da bulunmamaktadır.

Örneğin, ağ trafiğinin IEEE 802.11b'de olduğu gibi 11 Mbps olduğunu varsayalım. 1500B paket göndermek için IV yaklaşık 5 saat içinde tekrar kullanılacaktır. IEEE 802.11g ya da daha yeni bir kablosuz ağ olsa bile IV 1 saat içinde tekrar kullanılacaktır. [12]

$$54\text{mbps} \div (1500\text{byte/paket} \times 8\text{bit})$$
$$= 4500 \text{ paket/sn.}$$
$$= 16777216 \div 4500 = 3728.27\text{sn}$$
$$= 1.04 \text{ saat}$$

Bu nedenle, WEP protokolünde anahtarın tekrar kullanımı açığından dolayı saldırganlarda aynı anahtar akışıyla şifrelenmiş iki şifreli metin bulunabilir.

- Kimlik doğrulama mekanizması

Güvenlik standardı olarak WEP kullanan WLAN'da kimlik doğrulama yöntemi tek yönlüdür, bu da AP'nin yalnızca istemciyi doğrulaması, fakat AP'nin istemci aracılığıyla doğrulanmasının mümkün olmaması anlamına gelir. Ayrıca AP ve istemci arasındaki bu tek yönlü kimlik doğrulama, ağ iletişimi üzerinden şifresiz metin olarak iletilen paylaşımlı bir anahtara dayanır, bu nedenle bu sorun Hizmeti Engelleme (DoS)'ye yol açabilir. [15]

- Zayıf mesaj bütünlük mekanizması

WEP, şifrelenmiş paket yükünün bir parçası olan bütünlük sağlama alanını kullanmakta olup bu alan aktarım sırasında verinin değiştirilmediğini denetlemek için kullanılır. Ancak bu bütünlük mekanizması lineer bir sağlama olan CRC-232'yi kullanır, bu da iki CRC arasındaki bit farkının alındıkları mesajların bit farkına göre hesaplanabileceği anlamına gelir. [12]

2.2.4. WPA VE WPA2 (IEEE 802.11i)

Kablolu Eşdeğer Gizlilik (WEP)'teki ciddi güvenlik açıkları ve zaafları, WEP'teki sorunların çözümü için WPA güvenlik standardının geliştirilmesine yol açmıştır.
WPA, WEP'teki güvenlik açıkları için geçici ve hızlı bir yol olmuş ve ileriye uyumluluğu sürdürmüştür. Şifresinin kırılabilmesine karşın WPA; paket sahteciliği, eklerin yeniden oynatılması ve RC4'ün yanlış bir biçimde kullanılması gibi WEP protokolündeki bazı güvenlik açıklarını çözmüştür. WPA yalnızca IEEE 802.11i taslağının bir alt kümesi olarak uygulanıp Wi-Fi Birliği tarafından 2003'te kabul edilmiş, ancak daha sonra 2006'da yerini WPA2'ye bırakmıştır.

Öte yandan WPA ile WPA2 arasındaki en belirgin fark veri şifrelemesi için WPA2'de, WPA'da kullanılan Geçici Anahtar Bütünlük Protokolü (TKIP) yerine Gelişmiş Şifreleme Standardının kullanılmasıdır. AES ise WEP ve WPA'da kullanılan RC4'ün aksine blok şifre temelli bir algoritmadır.

Güvenlik açıklarının ve zaaflarının giderilmesi adına WPA'nın WEP üzerine yaptığı en önemli geliştirmeler TKIP ile yapılan iyileştirilmiş veri şifrelemesi, 2004'te yayınlanan ve ortak anahtar şifrelemesi kullanan Genişletilebilir Kimlik Doğrulama Protokolü

(EAP) ile yapılan kullanıcı kimlik doğrulaması -RFC 3748'de belirtildiği [16] ve RFC 5247 ve 7057 ile güncellendiği üzere- ve TKIP için Michael isimli yeni bir algoritmayla yeni bir mesaj bütünlük kodu (MIC) ile sağlanan bütünlük olmuştur.

2.2.4.1. WPA ve WPA2'nin Kimlik Doğrulama Yöntemleri

WPA ve WPA2 protokollerinin kimlik doğrulama yöntemleri iki sürüme ayrılabilir: önceden paylaştırılan anahtar kimlik doğrulaması (PSK) olan kişisel sürüm ve EAP kullanan kuruluş sürümü. Bu iki model kısaca açıklanacaktır.

- Kişisel Mod (Önceden Paylaştırılan Anahtar modu)

  Bu modda iş istasyonlarının kablosuz ağa erişiminde kimlik doğrulaması, 8-63 ASCII karakteri ya da 64 onaltılık sayı uzunluğundan oluşan anahtar parolası ile yapılır.

  PSK modu ayrıca verilen bir şifreden ana anahtarı türetmek için bir anahtar türev fonksiyonunu kullanır.

- Kuruluş Modu ya da 802.1x Kimlik Doğrulama Sunucusu

  Bu mod, kimlik doğrulama işlemi için kimlik doğrulama sunucusunu (AS) kullanır. Kablosuz kullanıcısının yanlışlıkla sahte bir ağa bağlanmaması için EAP ile birlikte ortak bir kimlik doğrulama kullanır. Bu kimlik doğrulama mekanizması kuruluş ağları içindir. Bu modda, kablosuz ağ trafiği için çok iyi güvenlik sunan Arayan Kullanıcı Kimliğini Uzaktan Doğrulama Hizmeti (RADIUS) sunucusu gereklidir.

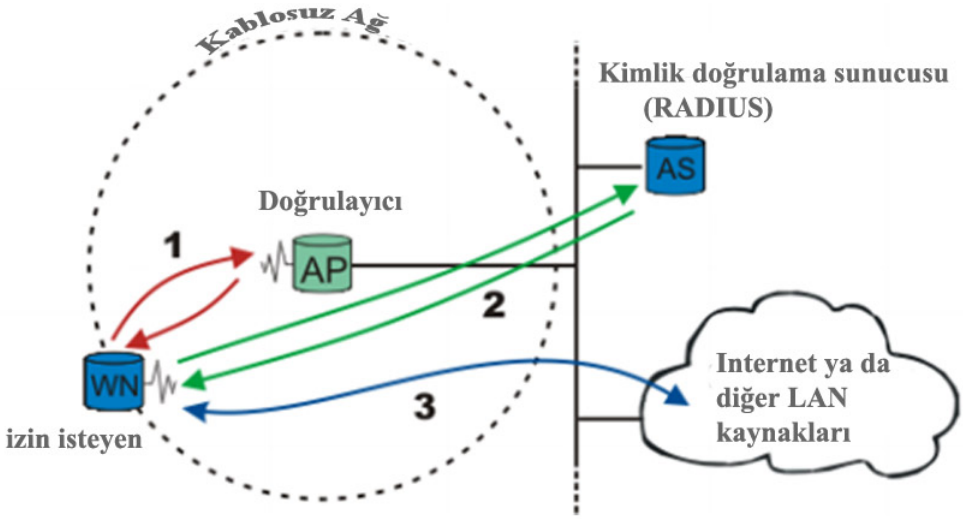
  Ancak EAP tam bir kimlik doğrulama mekanizması olmaktan çok, yaygın işlevleri ve istenilen kimlik doğrulama mekanizmasında uzlaşılmasını sağlayan bir kimlik doğrulama şemasıdır.

Kuruluş modu aşağıdaki prensipler doğrultusunda çalışır:

1. AS kullanıcının kimlik bilgilerini alır.
2. AS benzersiz bir ana anahtar oluşturmak için 802.1x çerçevesini ve EAP'ı kullanır.
3. 802.1x, anahtarı AP ve istemciye paylaştırır.

4. TKIP, ana anahtarı kullanarak bir anahtar hiyerarşisi ve yönetimi sistemi kurar.

Aşağıdaki şekilde RADIUS sunucusu kullanan 802.1x kimlik doğrulama mekanizması gösterilmektedir:



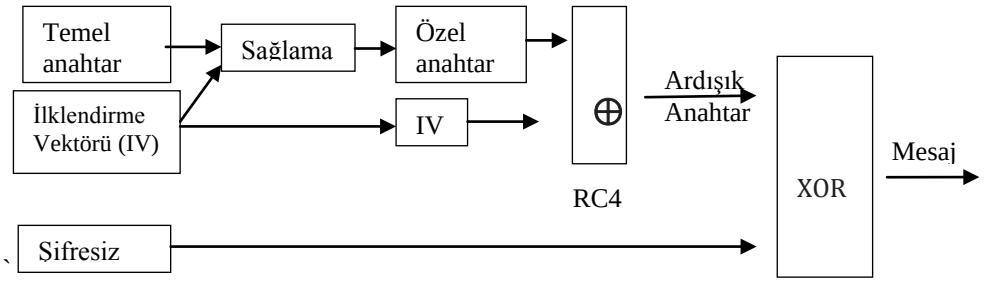
Şekil 2.7: 802.1x kimlik doğrulamaları[17]

2.2.4.2. TKIP

Bu güvenlik protokolü geçici bir protokoldür ve WEP'in zaaflarını çözmek için tasarlanmıştır, WEP protokolünün ana zaaflarından biri, protokolün saldırgan tarafından ele geçirilip tekrar oynatılan bir paketi tespit etme becerisinin olmamasıdır. Bu sorun TSC (TKIP sıra sayacı) isimli bir sayacın kullanılmasıyla çözülmüştür.

TKIP, anahtarları karıştıran karma bir algoritma kullanır. Ayrıca, veri ya da anahtarların alıcıya aktarım sırasında değiştirilmemesini sağlayan, MIC adı verilen bir bütünlük denetimi işlevi de kullanır. TKIP RC4 kesintisiz şifrelemesini kullansa da kablosuz ağdaki tüm istasyonların aynı gizli anahtarı paylaşması gerekir. Bu anahtar da WEP'te kullanılan 40 bit uzunluğundaki anahtardan çok daha uzundur. Ancak ağ ile ilişkisi olan tüm taraflar farklı bir RC4 anahtar akışı oluşturur. TKIP paket başına anahtar olarak da bilinmekte olup bu da oluşturulan her paket için çarpışmaları önlemek amacıyla yeni bir anahtar oluşturulduğu anlamına gelir.

Aşağıdaki şekilde TKIP şifreleme algoritmasının nasıl çalıştığı gösterilmiştir:



Şekil 2.8: TKIP Şifreleme Algoritması[8]

2.2.4.3. AES-CCM Protokolü

WPA2, Gelişmiş Şifreleme Standardı (AES)'nın AES-CCM protokolü (CCMP) olarak bilinen özel bir modunu kullanmakta olup, bu mod sayaç modunda AES kullanır. Böylece veri gizliliği (şifrelemesi) ve bütünlüğü sağlanır. Genellikle gizlilik ve kimlik doğrulamasını vermek için iki farklı şifreleme algoritması kullanılır, ancak AES-CCM algoritması bu iki güvenlik hizmetini aynı algoritmayla sağlar.

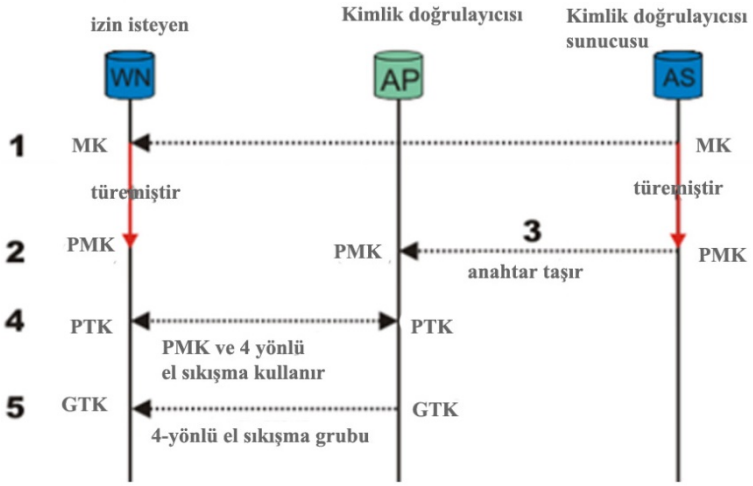
2.2.4.4. Anahtar yönetimi ve paylaşımı

İstasyon (STA) ve AS arasında başarılı bir kimlik doğrulaması gerçekleştirildikten sonra ana anahtar oluşturulur ve bu anahtar kimlik doğrulama işleminin başarıyla gerçekleştirilmesinden sonra AS'ye gönderilir. Bu anahtarı yalnızca STA ve AS bilir.

Hem istasyon hem de AS, mevcut bir pseudo random fonksiyonu kullanarak ana anahtardan (MK) İkili Ana Anahtar (PMK) türetir.

Bu şekilde AS PMK'yı STA'ya gönderir böylece AP, WPA ve WPA2'de bulunan anahtar yönetimi mekanizmasının temel bir parçası olan 4 yönlü el sıkışmayı gerçekleştirmiş olur.

Aşağıdaki şekilde, WPA ve WPA2'de anahtar yönetimi ve paylaşımı gösterilmektedir:



Şekil 2.9: 802.11i'de anahtar yönetimi ve paylaşımı[18].

2.2.4.5. EAP Yöntemleri

Önceki bölümlerde belirtildiği gibi EAP tam bir kimlik doğrulama mekanizması olmaktan çok, yaygın işlevleri ve istenilen kimlik doğrulama mekanizmasında uzlaşılmasını sağlayan bir kimlik doğrulama çerçevesidir. Bu bölümde EAP yöntemleri incelenecektir.

EAP'ın temel bileşenleri; erişim istemcileri, AP ya da ağ erişimi sunucusundan (NAS) oluşan EAP kimlik doğrulayıcısı ve belirli bir EAP yönteminin belirli bir EAP erişim istemcisiyle uyuşmasını sağlayan AS'den oluşur.

Tablo 2.3: En yaygın EAP yöntemleri ve bu yöntemlerin ağ erişimi türleri[19]

Protokol / EAP yöntemi	Açıklama	Ağ erişimi türü
Hafif EAP (LEAP)	Cisco mülkiyetinde - MS-CHAP'ın değiştirilmiş bir sürümüdür.	-
EAP-TLS	İletim katmanı güvenliği (PKI)'ne dayanır.	VPN, çevirmeli uzaktan erişim
EAP-PSK	Önceden paylaştırılan anahtara dayanır.	WPA-PSK, WPA2-PSK
EAP-TTLS	Tünelli iletim katmanı güvenliğine dayanır (En yaygın kullanılan).	Kablosuz AP için 802.1x kimlik doğrulaması
EAP-MD5	MD5 sağlamasına dayanır.	Çevirmeli uzaktan erişim
PEAPv0/EAP-MSCAHPv2	Tasarım olarak EAP-TTLS'ye benzer - yalnızca sunucu tarafında PKI sertifikası gerektirir.	Kimlik doğrulayan anahtar için 802.1x kimlik doğrulaması

2.2.5. WLAN Güvenlik Protokollerinin Karşılaştırılmasının Özeti

Aşağıdaki tabloda WLAN'lardaki güvenlik protokollerinin özeti gösterilmektedir:

Tablo 2.4: WLAN Güvenlik Protokollerinin Karşılaştırılması WEP, WPA ve WPA2[20]

	WEP	WPA	WPA2
Amaç	Kablolu ağlara eşdeğer güvenlik Sağlama	Yeni donanıma gerek kalmadan WEP'in eksikliklerini giderme, IEEE 802.11i standardının çoğuna uygulanmıştır.	IEEE 802.11i standardının tamamına uygulanmıştır ve WPA'ya yapılan bir geliştirmedir.
Veri Gizliliği (Şifreleme)	Rivest Cipher 4 (RC4)	TKIP	Gelişmiş Şifreleme Standardı (AES) kullanılan blok şifre Zincirleme Mesaj Doğrulama Kodu Protokolü (CCMP)'yle Sayaç Modu
Kimlik doğrulama	WEP-Açık ve WEP-Paylaşımlı	WPA-PSK ve WPA-Kuruluş	WPA2-Kişisel ve WPA2-Kuruluş
Veri Tamlığı	CRC-32	Michael (MIC oluşturur.)	Blok şifre zincirleme mesaj doğrulama kod (CBC-MAC)
Anahtar Yönetimi	Anahtar yönetimi eksikliği	Güçlü bir anahtar yönetimi sağlar ve anahtarlar dört yönlü el sıkışma ile oluşturulur.	Güçlü bir anahtar yönetimi sağlar ve anahtarlar dört yönlü el sıkışma ile oluşturulur.
Donanım Uyumluluk	Mevcut donanımda Çalışır	NIC'e yapılacak yazılım güncellemeleriyle mevcut donanımda çalışır.	2006'dan bu yana sertifikalanmış Wi-Fi cihazlarında desteklenmektedir, daha eski NIC ile çalışmaz.
Saldırılar/ Açıklar	Chopchop, Bittau's fragmentasyonu, FMS ve PTW saldırısı, DoS saldırıları	Chopchop, Ohigashi-Morii, WPA-PSK, Beck-Tews ve Michael Sıfırlama Saldırısı ve Hole 196 açığı, DoS saldırıları.	Hole 196 açığı, şifrelenmemiş yönetim ve kontrol çerçevelerinden kaynaklanan DoS saldırıları, kimlik doğrulamanın devre dışı kalmasından kaynaklanan MAC adresi yanılta sinyalleri, WPA2-Kişisel'deki çevrimdışı sözlük saldırıları
Dağıtım Karmaşıklığı	Kolay kurulum ve yapılandırılma	WPA-kuruluş için gerekli karmaşık kurulum.	WPA2-kuruluş için gerekli karmaşık kurulum
Yeniden oynatma saldırısına karşı koruma	Yeniden oynatma saldırılarına karşı koruma yok.	Yeniden oynatma koruması için sıra sayacını kullanır.	48 bit paket numarası yeniden oynatma saldırılarını önler.

2.3. WI-FI GÜVENLİK PROTOKOLLERİNE YAPILAN SALDIRI VE TEHDİTLER

Önceki bölümlerde bahsettiğimiz gibi 802.11 WLAN endüstrileri çok hızlı bir şekilde gelişmektedir ve şu anda ciddi bir ilerleme kaydetmiş durumdadır. Dünya üzerinde yaşayan insanların yaklaşık %17'sinin Wi-Fi kullandığı tahmin edilmektedir.

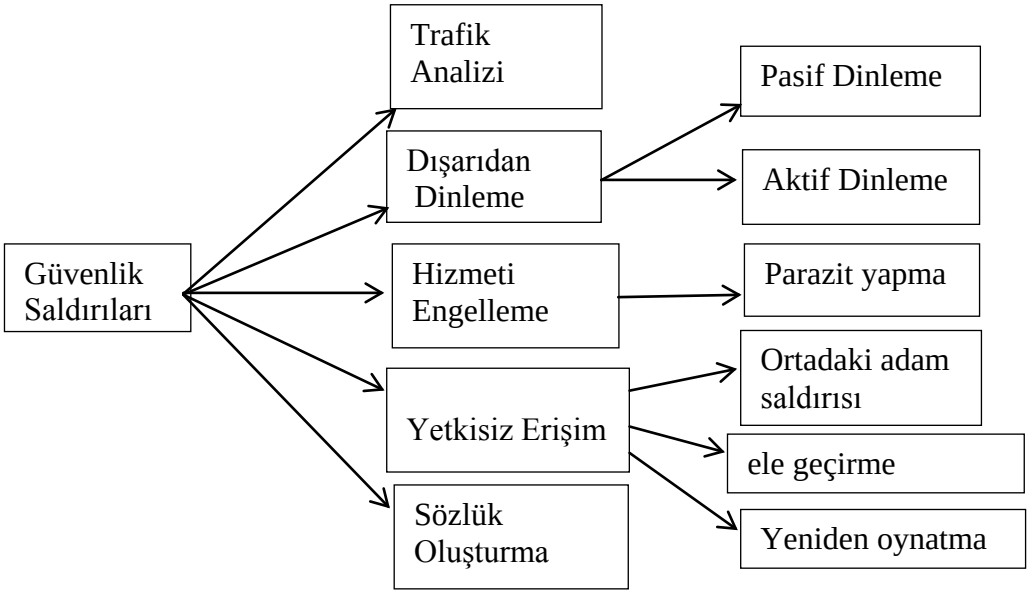
Kablosuz ağların; bilgi kaynağına yüksek erişilebilirlik, kurulum kolaylığı, daha hızlı ve ucuz olması gibi avantajları olsa da WLAN hakkındaki her şey olumlu değildir. WLAN'ların hemen her türlü ortama yerleştirilmesiyle birlikte kablosuz ağlara yapılacak saldırı riski artmaktadır ve bu nedenle 802.11'e yapılan ve kuruluşları güvenlik risklerine maruz bırakan saldırıları tanımlayan birçok rapor ve makale yayınlanmıştır.

2.3.1. Wi-Fi Tehditleri

Kablosuz ağlara dışarıdan gerçekleştirilen saldırılar temelde şu şekilde özetlenebilmektedir:

- Hizmeti Engelleme
- Sahte AP'ler/Ad-Hoc Ağları
- Pasif Ele Geçirme
- Yapılandırma Sorunları

Kuruluşların ve kullanıcıların kablosuz ağlara yapılan saldırılardan bazılarını anlamasına yardımcı olmak için güvenlik saldırıları sınıflandırılarak Şekil 2.10'da gösterilmiştir [21] [22]. Burada gördüğümüz gibi, bunlar WLAN'larda bulunan ana tehditlerdir.



Şekil 2.10: WLAN Güvenlik Saldırılarının Sınıflandırılması

2.3.2. WEP'E Yapılan Saldırılar

- **FMS Saldırısı**

Fluhrer ve arkadaşları tarafından 2001 yılında yayınlanmış olan bu saldırı, WEP'e yapılan istatistiksel temelli bir saldırıdır. [14] WEP, kriptografi ya da güvenlik uzmanlarınca geliştirilen bir protokol olmadığından, WEP protokolüne ilişkin RC4 açığı ünlü FMS makalesi yayınlanmadan dört yıl önce David Wanger tarafından kolayca ortaya çıkarılabilir hale gelmiştir. FMS; **F**luhrer, **M**antin ve **S**hamir isimlerinin kısaltması olup, bunlar RC4 şifreleme algoritmasındaki şu iki açığı gösteren ünlü makaleyi yayınlayan kişilerdir: değişimsizlik zaafı ve bilinen IV saldırıları.

Bu saldırı, RC4'teki açıkları ve zaafları kullanmaktadır. Ayrıca, saldırgan paket başına anahtar IV'sinin üç baytını bilmektedir. Böylece saldırgan RC4'ü değiştirerek anahtarın bir baytını %5 olasılıkla tahmin etme olanağı elde eder. Ayrıca saldırgan, bir oylama sistemi kullanarak olası bir anahtarı tahmini ve testi yapabilir. Anahtar doğru değilse, saldırgan başka bir olası doğru anahtarı deneyecek ve ardından tekrar tahmin etmeye çalışacaktır. Bu saldırıda bu yolla %50 başarı oranına ulaşabilmek için, 6,000,000'a yakın paket gerekir.

- **KoreK Saldırısı**

WEP'e yapılan çeşitli saldırılardan biri olan KoreK, NetStumbler.org güvenlik forumundaki anonim bir katılımcı tarafından geliştirilmiştir ve bu katılımcı saldırısını 17 saldırıyı tanımlayan bir kod halinde NetStumbler forumunda sunmuştur. Katılımcının ilk saldırısı FMS saldırısı temeline dayanmakta olup saldırganın anahtarı daha hızlı bulmasını sağlamaktadır. KoreK, anahtar alanını azaltarak saldırgana anahtarı daha hızlı bulma olanağı sağlayan A-neg isimli bir saldırı yayınlamıştır.

- **Chopchop Saldırısı**

Bu saldırı da KoreK tarafından keşfedilmiştir ve RC4 algoritmasındaki açığı kullanmaktan çok bizzat WEP protokolünün tasarım açıklarını ve zaaflarını kullanır. WEP protokolünün temel tasarım açıkları ise, yeniden oynatma korumasının olmaması ve **CRC32** sağlamasının zaafıdır. [23]

Bu saldırı saldırganın anahtarı bilmeden paketi çözebilmesini sağlar. Ancak bu saldırı hızlı olmamasından dolayı bir paketi izleme, çözme, değiştirme ve daha fazla trafik elde etmek için paketi tekrar ağa yerleştirme ile sınırlıdır, böylece PTW gibi tam bir anahtarı çözme saldırısı yapmak için gerekli bilgiyi verir. Bu saldırı şifreli metindeki bir bitin çevrilmesine dayalıdır ve şifrelenmiş CRC32 değerindeki bit değeri hesaplanarak değiştirilmelidir, böylelikle paketin hala geçerli olması sağlanır. Bu saldırı bir paketin son baytını alarak değerini tahmin etme yöntemiyle çalışır [20].

- **PTW Saldırısı**

Bu saldırı 2007'de Pyshkin Tews Weinmann (PTW) tarafından yayınlanmıştır ve iki yeni kapsam geliştirmiştir. İlki, Jenkins istatistiklerinin bağıntısına dayanır. İkincisi ise saldırı için yeni bir yapı oluşturan bir kapsamdır. Saldırı, anahtarı bayt bayt tahmin etmeye çalışmak yerine birden çok baytın bağıntısıyla çalışır.

Bu saldırı için yapılan testler, %50 başarı olasılığı elde etmek için yalnızca 35,000 - 40,000 civarı paket gerektiğini göstermiştir. [23] [24]

Tablo 2.5: Anahtar çözme saldırılarının özeti

Ad	Tür	Yıl	Paket	Oran
FMS	İstatistiksel	2001	6,000,000 (64 bit WEP)	86
KoreK	İstatistiksel	2004	200,000 (64 bit WEP)	3
PTW	İstatistiksel	2007	70,000 (64 bit WEP)	1

2.3.3. WPA-PSK'YA Yapılan Saldırılar

- **Beck-Tews Saldırısı**

Bu saldırı WPA'ya yapılan RC4 temelli gelişmiş bir saldırı olup Martin Beck ve Erik Tews'in 2008'de yayınladıkları makalede ayrıntılarıyla anlatılmıştır. [25]

Bu saldırı, TKIP'nin WEP protokolünün bir uzantısı olması ve şifreleme mekanizması olarak RC4'ü kullanmasından dolayı TKIP'deki açıkları ve zaafları kullanır. Bu saldırı, WEP chop-chop saldırısının da bir uzantısıdır, çünkü WEP kriptografik açıdan güvenli olmayan bir sağlama mekanizması (CRC32) kullanmaktadır. Bu da saldırganın ARP paketlerini çözmesini ve ağa trafik yerleştirmesini sağlayarak saldırgana bir paketin tekil baytlarını tahmin etme olanağı tanır ve kablosuz AP de bu tahminin doğru olduğunu onaylar ya da reddeder. Eğer tahmin doğruysa, saldırgan tahminin doğru olduğunu saptayabilir ve paketin diğer baytlarını tahmin etmeye devam eder. Ayrıca bu durum saldırgana DoS (hizmeti engelleme) saldırısı ya da ARP zehirlenmesi yapma olanağı sağlayabilir. [24]

- **Ohigashi-Morii Saldırısı**

Bu saldırı WPA-TKIP'ye yapılan Beck-Tews saldırısının bir uzantısıdır. Gerçekten de sahte bir paket yerleştirme süresi en iyi koşulda 15 dakikadan 1 dakikaya düşürülmüştür. Bu saldırı için, saldırıyı gerçekleştirme süresini azaltacak ipuçlarıyla birlikte iki bağlantı noktası arasındaki bağlantıyı izinsiz izleme saldırısıyla Beck Tews saldırısı üst üste bindirilir. [23] [24]

- **El sıkışmaya yapılan sözlük saldırısı**

Bu saldırı, anahtarın sözlükten bir sözcük olduğu durumlarda WPA-PSK'ya yapılan anahtar çözme saldırısıdır. Bu saldırıda saldırganın en önemli noktası kablosuz AP ve istasyon arasındaki el sıkışmayı elde geçirmesidir. Ağ iletişiminin dinlenmesiyle bu el sıkışma ele geçirilebilir,

Çünkü AP ve istemci arasındaki hash anahtarlar istemci bağlantıyı başlattığı anda değiş tokuş edilir. Böylece saldırgan bekleyebilir ya da izin isteyene karşı bir yetkisiz kılma saldırısı başlatabilir.

Saldırgan, AP ve iş istasyonu arasındaki el sıkışmadan hash anahtarını elde ettikten sonra kablosuz ağı kolayca kırabilir ve bir sözlük saldırısı ya da mevcut başka saldırılarla anahtarı bulmaya çalışabilir. [23] [24]

- **Hole196 açığı**

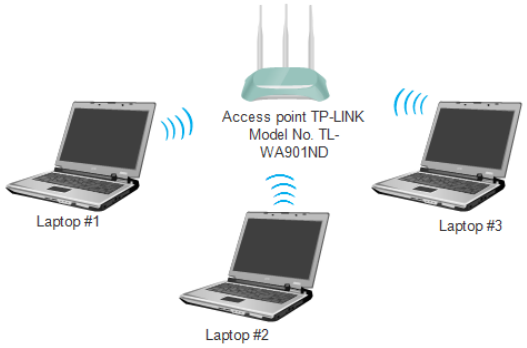
Hole196, 2010'da Sohail Ahmad tarafından WPA2 protokolünde bulunmuş bir açık olup paylaşımlı grup geçici anahtarını kullanır. Numaranın da gösterdiği üzere bu açık, adını 802.11 protokolleriyle ilgili standart belgenin 196'ncı sayfasından alır.
Bu saldırı anahtar çözme saldırısı değildir, ama iki bağlantı noktası arasındaki bağlantıyı izinsiz izleme ve hizmeti engelleme saldırıları gerçekleştirmek için kullanılabilir. [20]

3. MALZEME VE YÖNTEM

bu bölüm, üç uygulamayı ve bunlardan elde edilen bulguları içermektedir. Hazırlanacak üç uygulama şunlardır:

- WEP Şifre Kırma Testi
- WPA-PSK/WPA2-PSK Şifre Kırma Testi
- WLAN'ın Performans Ölçümü

Deneysel uygulamamızda kullandığımız WLAN'ın genel şekli aşağıda gösterilmektedir:



Şekil 3.1: Kullanılan WLAN'ın genel şekli

3.1. HEDEFLER

Yukarıda bahsedildiği gibi bu kısım 3 bölümden oluşmaktadır. Bunların ilk iki tanesi WLAN'lardaki güvenlik protokollerinin şifre kırma testlerinin gösterimlerine dayanmaktadır. Güvenlik protokollerinin şifrelerinin kırılmasıyla ilgili daha önceden çalışmalar mevcut olsa da bu çalışmada farklı metotlar düşünülerek ortalama şifre kırma süreleri tahmini olarak ölçülmektedir. Bununla birlikte deneylerin ana hedefi günümüzdeki WLAN'larda kullandığımız güvenlik protokollerinin içerisindeki zayıflıkları belirlemektir.

WLAN'ların kullanımıyla bağlantılı uygulamaların sürekli olarak artması, beraberinde yavaş cevaplama sürelerini veya düşük yük miktarlarını getirmektedir. Böylece

güvenlik protokollerinin kimlik doğrulama ve şifreleme kavramlarının her ikisine göre WLAN trafiğini nasıl etkilediğini göstermek oldukça önem kazanmaktadır. Bu amaçla 3. test bu konuyu ele alacaktır. Bu uygulama WLAN performans ölçümüne bağlı tüm konuları direk olarak göstermese de bu araştırmamın, güvenlik kavramının ağ performans çeşitleri üzerinde oluşturacağı etkilerin doğru anlaşılmasına katkıda bulunmayı hedeflemekteyim. Bununla birlikte bu tez çalışması, günümüzde kulllanılan güvenlik protokollerine genel bir bakış sunmayı ve cevaplama süresi, gecikme süresi ve yük miktarı gibi parametreler çerçevesinde birbirleriyle nasıl karşılaştırılabileceğini amaçlamaktadır.

3.2. DONANIM PARÇALARI

Uygulamalar için kullanılan donanım parçalarına ait özellikler ve ağ bileşenleri Tablo 3.1 ve Tablo 3.2'de gösterilmektedir.

Tablo 3.1: Kullanılan dizüstü bilgisayar özellikleri

Makine	**Laptop #1**	**Laptop #2**	**Laptop #3**
Marka/Model	HP Pavilion dv4	HP 2000 Notebook PC	HP Pavilion Sleekbook 14
İşlemci	Intel Core 2 Duo T6500-2100.0 MHz	Intel® Core ™ i3 - 2328M CPU @2.20GHz	Intel® Core™ i3-2375 M CPU @1.50GHz (4 CPUs)
Bellek	4 GB	4 GB	6 GB
Ağ Adaptörü	Broadcom 802.11b/g WLAN	Ralink RT5390R 802.11b/g/n Wifi adaptör	Intel® Centrino ® Wireless N

Tablo 3.2: Kullanılan ağ bileşenlerinin gereksinimleri

Makine	**Model**	**Açıklama**
Kablosuz Erişim Noktası	TP-LINK 300 Mbs Wireless N Erişim noktası	Tüm güvenlik standartlarını destekler (WEP,WPA/WPA2, WPA-PSK/WPA2-PSK, MAC filtreleme)
USB Kablosuz Adaptör	300 MBbps Mini USB Kablosuz Adaptör (IUWA-300 N)	Inca –IUWA-300N USB kablosuz adaptor, Backtrack -3 – cracking destekli

3.3. YAZILIM ELEMANLARI

- **Kali Linux**

Kali Linux Mart 2013'de ortaya çıkan Debian tabanlı bir Linux dağıtımıdır ve ileri seviyeli nüfuz test (penetration testing) işlemini hedeflemektedir. Offensive Security Ltd. tarafından korunup fonlanmaktadır. Kali Linux, Backtrack Linux'un tamamen düzenlenmiş halidir ve Offensive Security firmasından Mati Aharoni ve Devon Kearns tarafından geliştirilmiştir [26] [27]

Bu tez için gerçekleştirilen Kali Linux kurulumu Ek A'da ayrıntılı olarak yer almaktadır. Bu program çeşitli nüfuz test programlarıyla birlikte kurulmaktadır. Bu programlar arasında Wireshark (paket analizcisi) ve Aircrack-ng (WLAN'ların nüfuz testleri için kullanılan bir yazılım parçası) yer almaktadır.

- **Aircrack-ng Aracı**

Aircrack-ng 2008 yılında Thomas d'Otreppe tarafından geliştirilen bir ağ yazılım parçasıdır ve paket koklayıcı, WEP ve WPA/WPA2-PSK şifre kırma ve analiz aracı gibi çeşitli araçları içermektedir [28].

Bu uygulamada WEP/WPA-PSK/WPA2-PSK şifresini kırmak ve bulmak için Kali Linux dağıtım sisteminin içinde önceden kurulmuş olan Aircrack-ng takımı kablosuz şifre kırma aracı olarak seçilmiştir.

- **Airodump-ng**:

Aircrack-ng takımının içinde bulunan kablosuz koklama aracıdır. Bu araç, WEP/WPA/WPA2-PSK-destekli ağların şifrelerini çözmek için gerekli tüm bilginin elde edilmesi amacıyla kullanılmaktadır.

- **Aireplay-ng Aracı**

Bu araç, seçili paketleri çok hızlı bir şekilde ve tekrarlı biçimde yeniden göndermesi için kablosuz ağı zorlayarak ağ trafiğini arttırmak için kullanılan bir enjeksiyon aracıdır. Bu sayede kısa süre içinde çok sayıda başlangıç vektörü (IV) ele geçirilmektedir.

4. BULGULAR

4.1. TEST #1: WEP ŞİFRESİNİ KIRMA

WLAN güvenlik protokolleri ve şifreleme algoritması bölümünde bahsettiğimiz gibi WEP şifrelemesinin kablosuz ağları güvenli hale getirdiği inanılıyordu ancak WEP şifrelemesinde farklı güvenlik açıkları bulunmuştur. Böylece yeterli sayıda IV başlığı elde edildikten sonar WEP'in şifresinin kırılması mümkün olmaktadır.

Bu tezde, kablosuz paketlerin başlangıç vektörlerindeki zayıflıkları avantaj olarak ele alınarak WEP güvenlikli bir kablosuz ağın şifresi kırılmakta ve böylece WEP güvenlik protokolünün güvenli olmayan durumu gösterilmektedir. Bu bölümdeki deneyde aircrack-ng tool, airreplay-ng ve airodump-ng gibi mevcut kablosuz şifre kırma araçları kullanılmaktadır. WEP-güvenlikli kablosuz bir ağı kırmak için Linux ortamıyla ilgili sınırlı bir bilgi ile Kali Linux sistemine gereksinim duyulmaktadır.

Literatürdeki Kali Linux komutlarıyla ilgili kaynaklarda belirtilen adımlar başka bir yüksek lisans tezinde de kullanılmıştır [29]. Bizim çalışmamızın bu tezden farkı WEP şifresini kırarken yeterli sayıda IV'nin yakalanması sırasında süreci hızlandıran ARP-enjeksiyon işlemi için aireplay-ng aracını kullanmamız, WEP 64 bit ve WEP 128 bit anahtar şifrelerini ayrı ayrı kırmak için her birinde 50 test yapmamız ve daha sonra bu değerlerin ortalamalarını analiz etmemizdir. Bunun dışında [29] kaynağındaki tezde WPA/WPA2 şifre kırma işlemleri sırasında yalnızca Airodump-ng ve Aircrack-ng araçları kullanılmakta iken bizim tezimizde Wifite kullanımının dışında Aireplay-ng aracına Deauthentication atağının uygulanması, Pyrit veritabanının kullanılarak anahtarın kırılması gibi ayrıntılar yer almaktadır. Bölüm 4.3'de gösterilen JPerf ile ağın performansının ölçülmesi ise bizim tezimize özgü önemli bir uygulamadır.

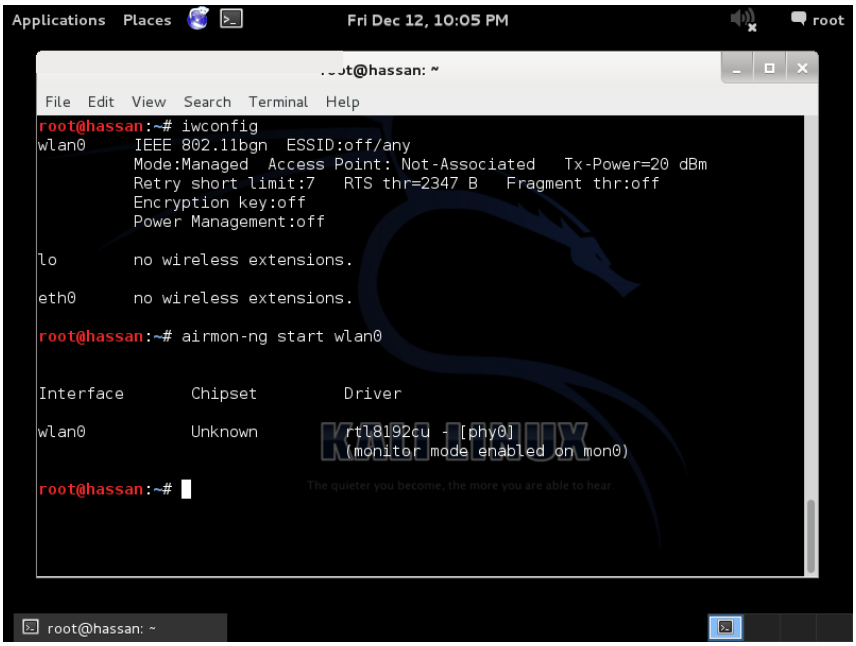
4.1.1. Kablosuz adaptör kontrolü ve [monitör modu]na geçiş

Prosedüre başlarken öncelikle kablosuz kartımızın monitör modunu destekleyip desteklemediğini kontrol ediyoruz. Terminale Airmon-ng komutunu yazarak kablosuz

kart kontrolünü sağlıyoruz. Aşağıdaki ekranda görüldüğü gibi wlan0 monitör modunu (enjeksiyon değil) destekleyen kablosuz adaptördür.

Şekil 4.1: Airmon-ng çıktısının görüntüsü

Terminale ***airmon-ng start wlan0*** yazarak kablosuz kartı monitor mod tipine getiriyoruz.



Şekil 4.2: Airmon-ng start wlan0 çıktısının görüntüsü

4.1.2. Şifresi kırılacak ağın bulunması

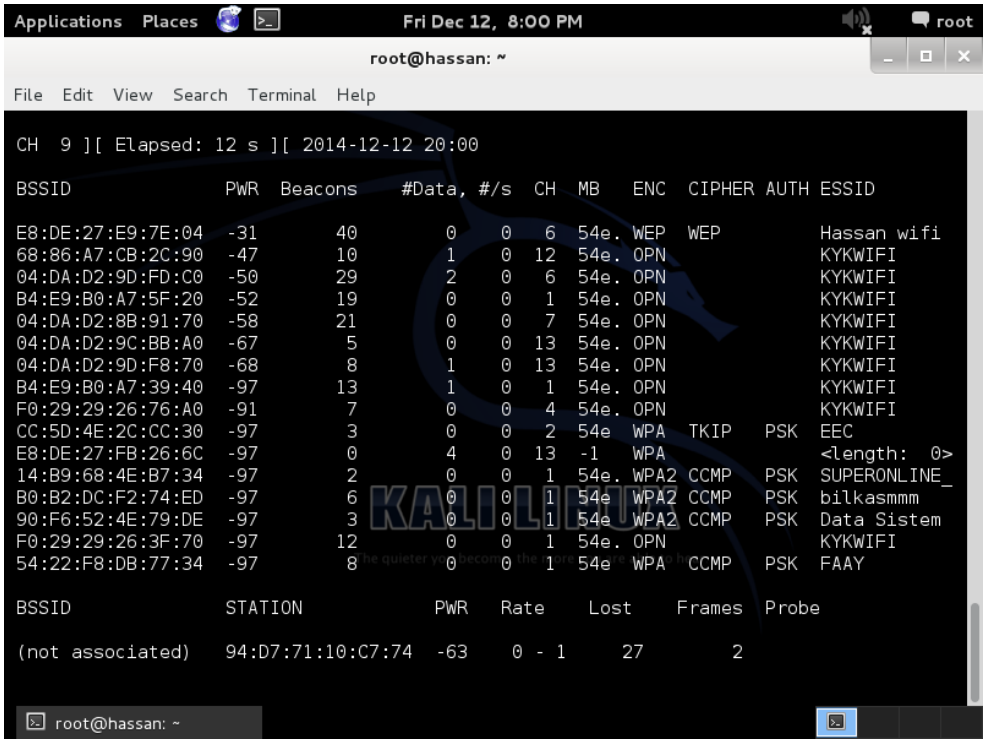
Bu prosedürün ilk adımında şifresi kırılacak ağı bulmamız gerekmektedir. Kabuk (Shell) terminali açıldıktan sonra Airodump-ng aracı kullanılarak AP için koklama başlatılacaktır. Bu araç, çevredeki ağlar hakkında bütün önemli bilgileri ortaya çıkarmaktadır.

WEP şifresini kırmak için elde etmemiz gereken en önemli bilgi hedef ağımızda kullanılan şifreleme tipini, kablosuz ağın ismini (ESSID), AP'nin MAC adresini (BSSID), kablosuz ağın kanalını ve kablosuz terminallerin MAC adreslerini belirlemektir.

- **IV'lerin yakalanması için terminal komutu**

```
root@engkafi:~# airodump-ng mon0
```

Aşağıdaki ekran çevremizde bulunan kablosuz ağları göstermektedir. Şifresini kırmak istediğimiz ağ ise **Hassan wifi** isimli olan ve denemeler için kendi kurduğumuz ağdır.

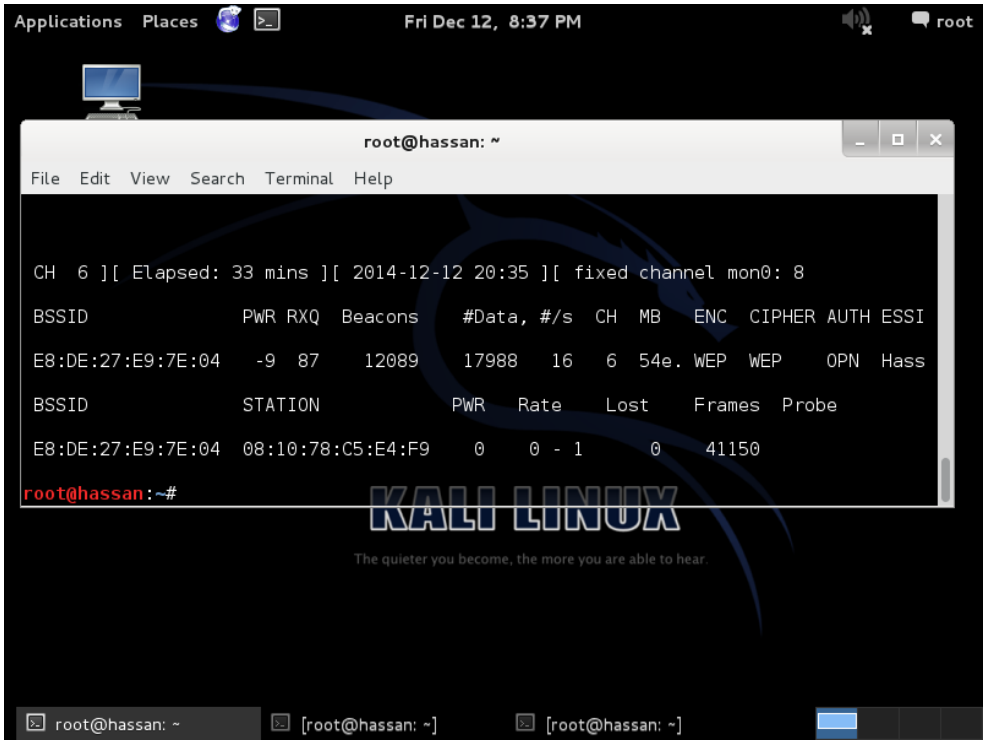


Şekil 4.3: Yakındaki tüm kablosuz ağları tarama ekranı

4.1.3. IV'leri yakalamak

Yukarıdaki bölümde IV paketlerini yakalamak için gerekli olan bütün bilgileri topladık; bu adımda ise IV paketlerini yakalamak için bu bilgileri kullanma adımına geçiyoruz. Bunu yapmak için **aircrack-ng takımındaki** en önemli araçlardan biri **airodump-ng**'dir. Çünkü bu komut şifre kırma işlemi devrede olduğu sürece tüm IV'lerin sürekli sayısını tutar ve yeni yakalanmış IV'leri bulduğunda **aircrack-ng**'yi otomatik olarak günceller.

```
root@engkafi:~# airodump-ng –c 6 –w wep --bssid E8:DE:27:E9:7E:04 mon0
```



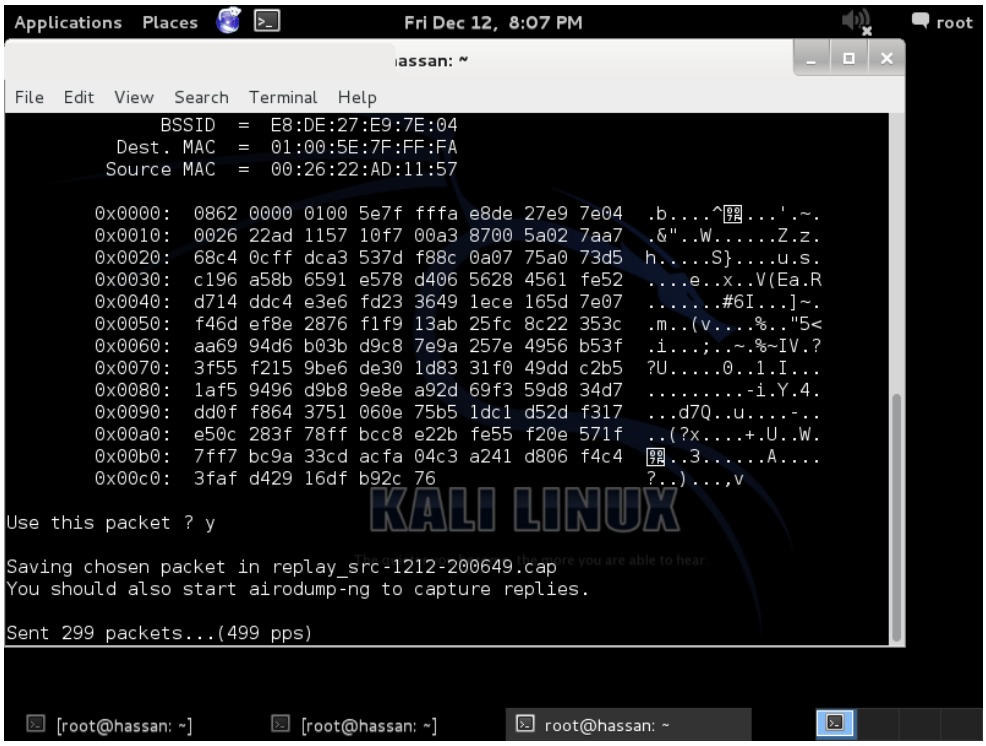
Şekil 4.4: Airodump-ng çalıştırma ekranı.

4.1.4. ARP istek/cevap modunda aireplay-ng'nin başlatılması

Yukarıda bahsedildiği gibi bir WLAN'ın WEP şifresini kırmak için çok sayıda IV'yi yakalamamız gerekir. Normal ağ trafiği bu IV'leri çok hızlı bir şekilde oluşturmazlar. Bu nedenle sabırlı bir şekilde ağ trafiği dinlenerek yeterli sayıda IV'nin yakalanabilir ve biriktirilebilir. Bununla birlikte bu tezde süreci hızlandırmak için enjeksiyon denilen bir yöntemi kullanacağız. Bu amaçla trafiği arttırmak için aireplay-ng isimli enjeksiyon aracını kullanarak AP'nin seçilmiş paketleri sürekli bir şekilde tekrarlı olarak ve çok hızlı yollamasını sağlarız. Bu sayede kısa zamanda çok sayıda IV yakalanabilmektedir. Bu yakalanan IV'ler WEP anahtarını bulmak için kullanılacaktır.

Bu süreç için başka bir konsol oturumu açıp aşağıdaki komutu yazarız.

```
root@engkafi:~# aireplay-ng -3 -b E8:DE:27:E9:7E:04 -h 08:10:78:C5:E4:F9 mon0
```

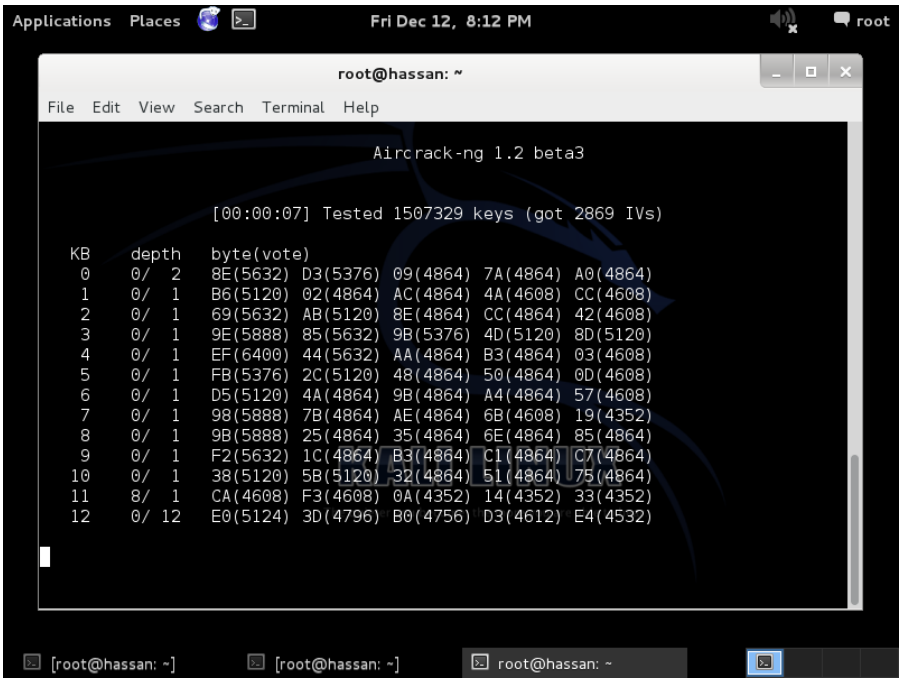


Şekil 4.5: Süreci hızlandırmak için ARP-enjeksiyon görüntüsü

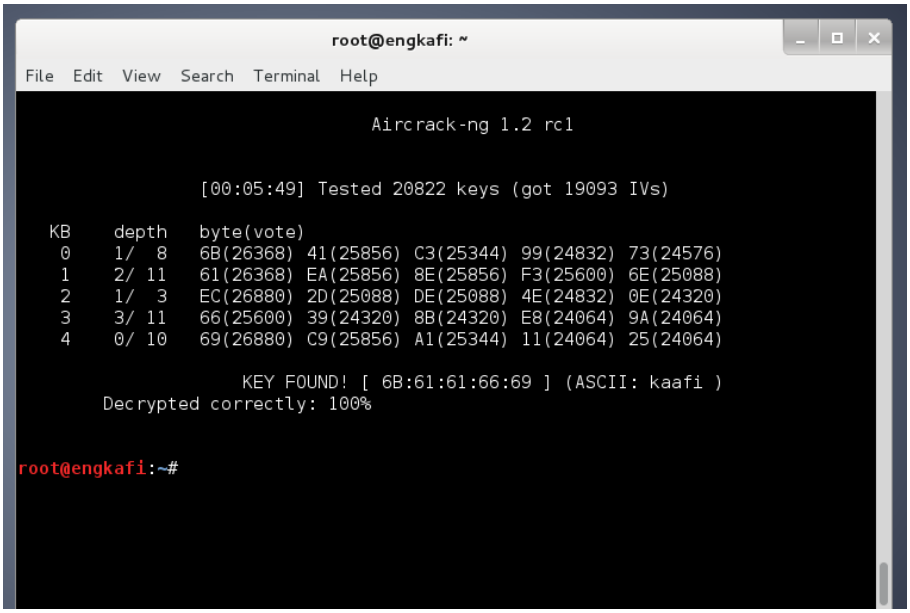
4.1.5. Anahtarın şifresini çözmek için IV'lerin kullanılması

Hedeflediğimiz kablosuz ağ için yeterli sayıda IV elde ettikten sonra hedef ağın paylaşılan şifresini kırabiliriz. Bunun için yeni bir Kabuk terminalini açarız (airodump'ın IV'leri yakalamasını durdurmadan, bu komut yeni IV'ler bulunduğunda otomatik güncelleme yapar) ve şifre kırma prosesine başlarız. Yeni terminale aşağıdaki komut yazılır.

```
root@engkafi:~# aircrack-ng  wep*.cp
```



Şekil 4.6: aircrack-ng çalıştırma ekranı.



Şekil 4.7: aircrack-ng çıktı ekranı

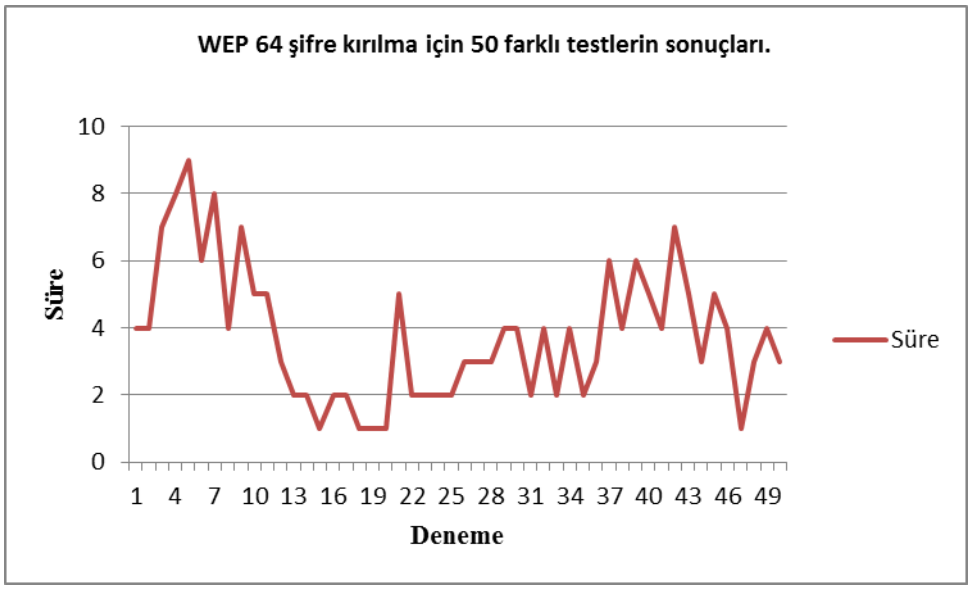
Tablo 4.1 : WEP 64 bit anahtar şifresini kırmak için gerçekleştirilen 50 teste ait sonuçlar

Deneme	Süre	#Anahtar	#IV
1	04:16	24	14569
2	04:15	37	13185
3	07:05	205130	19436
4	07:52	21856	15314
5	09:41	44800	19116
6	05:52	127177	15900
7	08:36	610	19589
8	04:32	100914	14175
9	07:34	96395	15240
10	05:49	20822	19093
11	05:00	81452	15771
12	03:45	162030	14437
13	02:40	1498	19515
14	01:51	1321	16319
15	01:08	22838	9799
16	02:23	4568	19705
17	02:49	12	19784
18	01:11	65793	5698
19	01:08	17	10293
20	01:11	69713	6267
21	05:17	6632	24811
22	02:06	19226	9936
23	02:10	56464	9913
24	02:33	3602	14897
25	01:59	204546	9945
26	02:59	818	14888
27	03:00	13203	14892
28	03:17	277204	14880
29	04:18	49357	19851
30	04:31	75420	19853
31	02:02	2840	9871
32	04:08	10842	16337
33	02:04	73427	9898
34	04:22	15031	19856
35	02:25	2744	10886
36	02:51	90810	11457
37	06:16	10964	20482
38	03:50	364	15288
39	04:51	70584	20241
40	04:53	7366	20577

Tablo 4.1 (devam): WEP 64 bit anahtar şifresini kırmak için gerçekleştirilen 50 teste ait sonuçlar.

41	03:59	80030	15439
42	07:09	2956	26949
43	05:28	36659	4940
44	03:25	465697	2991
45	04:51	70584	20241
46	04:11	1586	15585
47	01:23	60790	6190
48	03:05	115754	9716
49	04:00	81452	15771
50	03:45	162030	14437

Tablo 4.1'de görüldüğü gibi WEP 64 için ortalama şifre kırma süresi yaklaşık 4 dakikadır.



Şekil 4.8: Zamana göre WEP 64 şifre kırılmasını gösteren 50 deneme

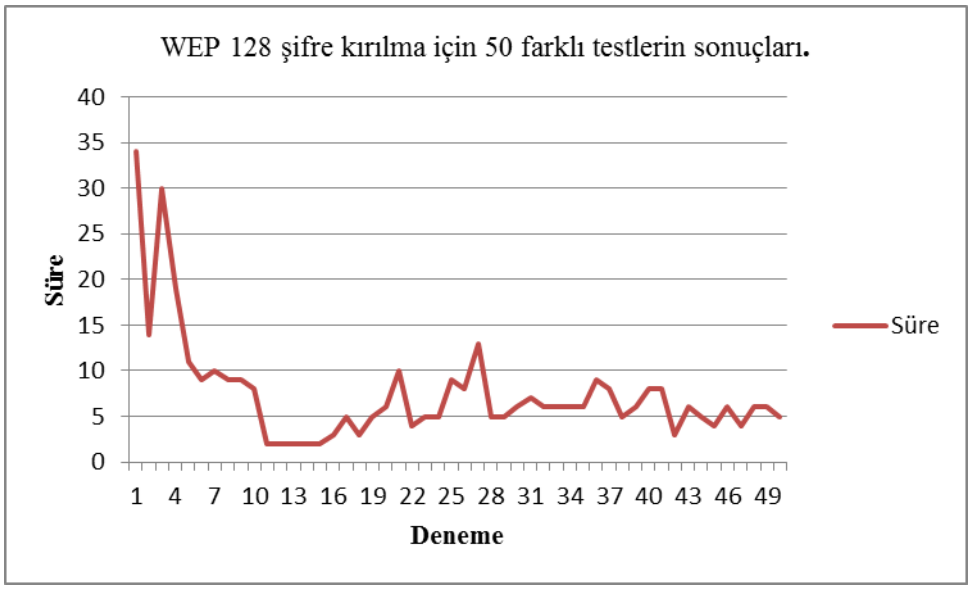
Tablo 4.2: WEP 128 bit anahtar şifresini kırmak için gerçekleştirilen 50 teste ait sonuçlar

Deneme	Süre	#Anahtar	#IV
1	0:34:14	694	65255
2	0:14:26	12596	33820
3	0:30:15	209204	40406
4	0:19:35	733492	28523
5	0:11:38	274740	44013
6	0:08:54	577	31225
7	0:10:01	767	46851
8	0:08:58	602420	42219
9	0:09:18	811	44465
10	0:08:40	143668	44551
11	0:02:39	340276	47193
12	0:02:21	864564	42455
13	0:02:28	156262	49725
14	0:02:35	793	50534
15	0:02:04	143668	37963
16	0:03:09	681	40370
17	0:05:14	641	77649
18	0:03:04	793	47726
19	0:05:33	759	47027
20	0:06:26	864564	48948
21	0:09:52	877	53889
22	0:03:54	819	31939
23	0:04:55	156263	40552
24	0:05:27	209204	49331
25	0:09:08	787	74866
26	0:07:56	758	44178
27	0:13:33	1061172	43198
28	0:05:21	691	43526
29	0:05:25	667956	37042
30	0:06:07	605	41676
31	0:07:13	601	46469
32	0:06:26	817	34115
33	0:06:30	12596	45127
34	0:06:03	78132	49236
35	0:05:56	687	44352
36	0:09:34	667956	58534
37	0:07:58	799028	59712
38	0:05:30	589	44358
39	0:06:33	601	44166

Tablo 4.2 (devam): WEP 128 bit anahtar şifresini kırmak için gerçekleştirilen 50 teste ait sonuçlar

40	0:08:13	625	54048
41	0:08:45	209204	53882
42	0:03:05	673	25855
43	0:06:13	577	49362
44	0:05:19	739	36972
45	0:04:11	143668	24741
46	0:05:50	822	41973
47	0:04:28	697	35869
48	0:06:41	615	51963
49	0:06:03	78132	49236
50	0:05:25	667956	37042

Tablo 4.2'de görüldüğü gibi WEP 128 için ortalama şifre kırma süresi yaklaşık 8 dakikadır.



Şekil 4.9: Zamana göre WEP 128 şifre kırılmasını gösteren 50 deneme

4.2 TEST #2: WPA-PSK/WPA2-PSK ŞİFRESİNİ KIRMA

Bu çalışmanın ikinci testi WPA/WPA2 PSK şifresinin kırılmasını göstermektedir. Bu işlem iki temel adımı içermektedir, birincisi parolanın hash halini içeren el sıkışmasının (handshake) bulunmasıdır, ikincisi ise parolanın bu hash halini kırmaktır.

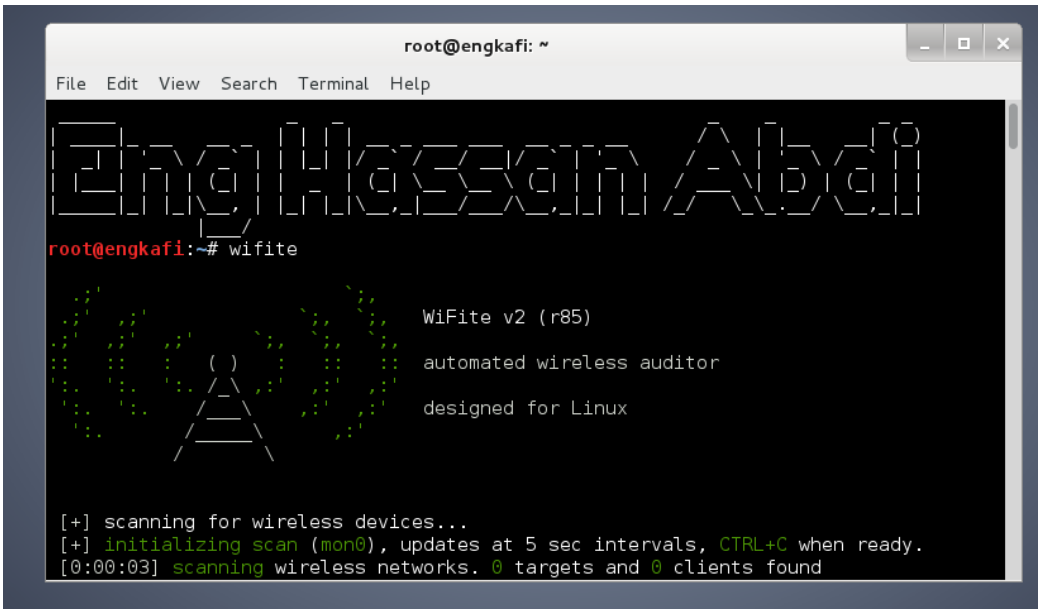
4.2.1. El sıkışmasını gerçekleştirme süreci

El sıkışması bilgisini elde etmek için iki yol izleyebiliriz: Wifite veya aireplay-ng'li Airodump-ng kullanmak.

1. **Wifite kullanmak**

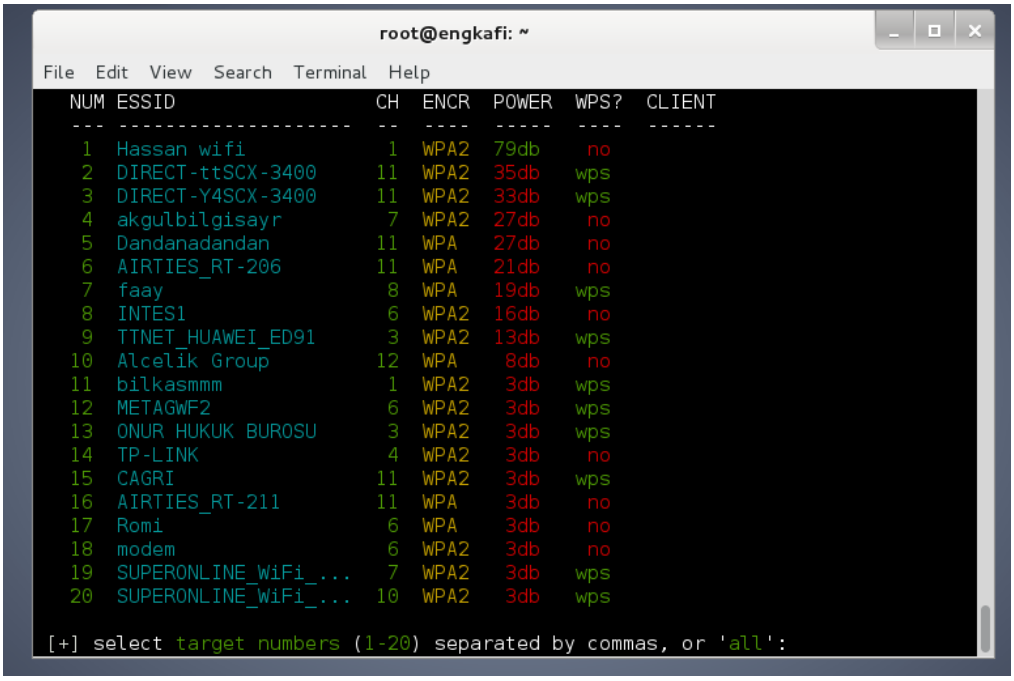
Terminal Kabuk kısmına **Wifite** komutu yazılır.

```
root@engkafi:~#wifite
```



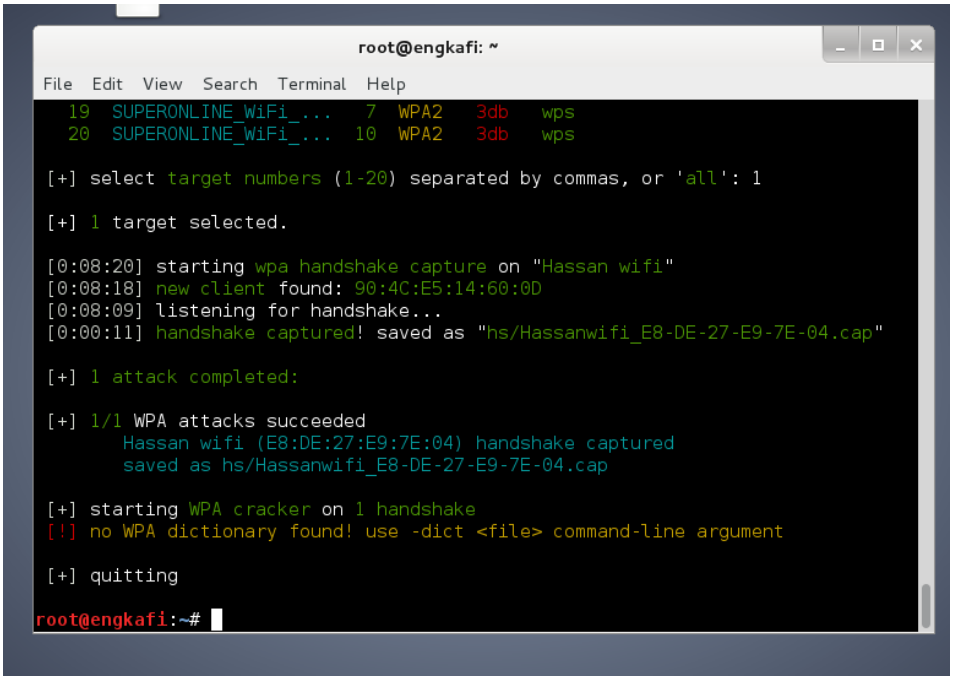
Şekil 4.10: Kablosuz aygıtların taranması (Wifite ile)

Aşağıdaki şekilde görüldüğü gibi yakındaki tüm WLAN'lar gösterilmektedir. Burada "**hassan wifi"** isimli ağ hedef ağımızdır ve birinci satırda yer almaktadır.



Şekil 4.11: Wifite kullanarak yakındaki tüm WLAN'ların bulunması

Aşağıdaki ekran WPA el sıkışmasının yakalandığını ve "**hs/hassanwifi_E8-DE-27-E9-7E-04.cap**" olarak kaydedildiğini göstermektedir.

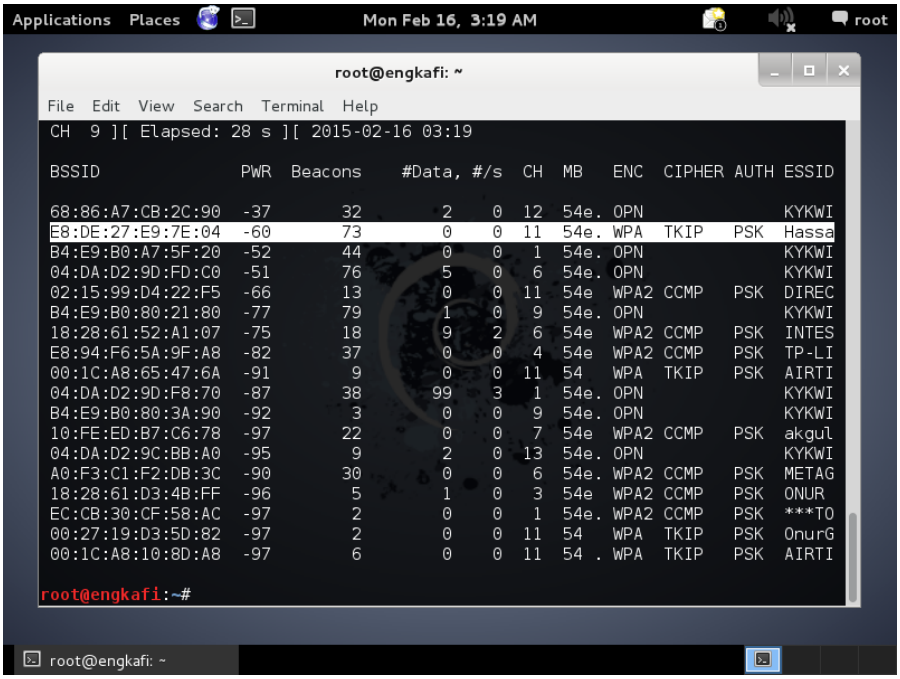


Şekil 4.12: Wifite kullanarak el sıkışmasının yakalanması

2. Airodump-ng komutlu ile Aireplay-ng kullanmak

- **Yakındaki tüm ağları taramak**

```
root@engkafi:~#airodump-ng mon0
```

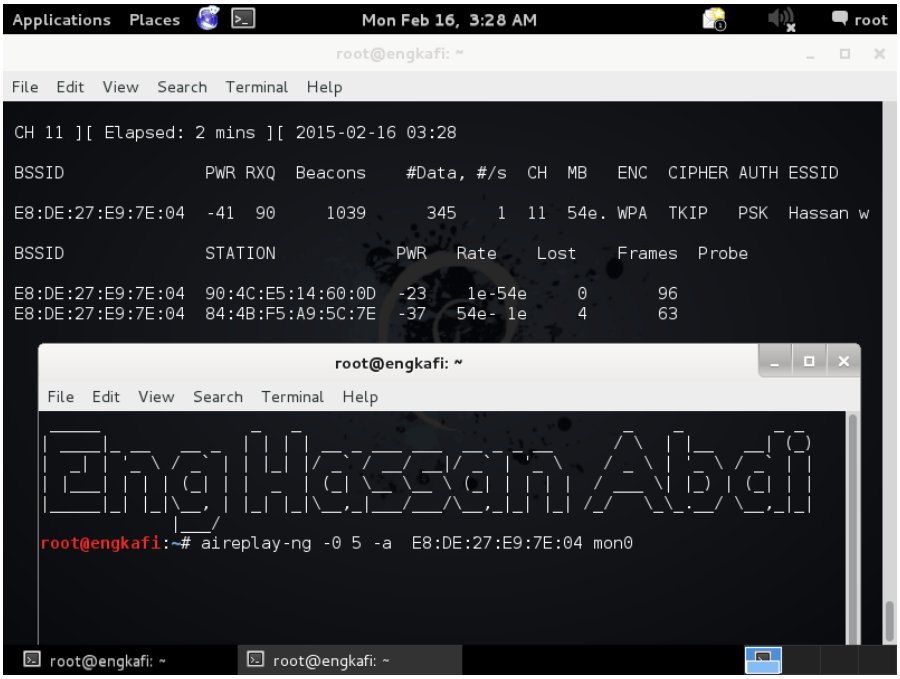


Şekil 4.13: WPA şifre kırılması için tüm yakın kablosuz ağların taranması

Aşağıdaki ektan görüntülerinde görüldüğü gibi kimlik doğrulamadan vazgeçme (Deauthentication) atağı kullanılarak AP'ye bağlı tüm istemcilere ilgisiz paketler gönderilir. Bu türdeki diğer ataklar gibi bu atağın amacı da WPA el sıkışma verisini yakalamak için kimlik doğrulamayı devre dışı bırakmaya neden olabilmektir. Normalde istemcileri ağdan koparma işlemi, WPA/WPA2 el sıkışmalarını göstermek veya yakalamak istediğimiz gizli ağ ismini elde etmek için yapılır. Bu atağı gerçekleştirmek için hedef ağ için bağlantılı kablosuz istemcilerin olması gerekmektedir. Bu nedenle "**Hassan wifi**" isimli WLAN'ımızda aşağıdaki şekilde görüldüğü gibi kablosuz bağlantılı iki bilgisayar kullanmaktayız.

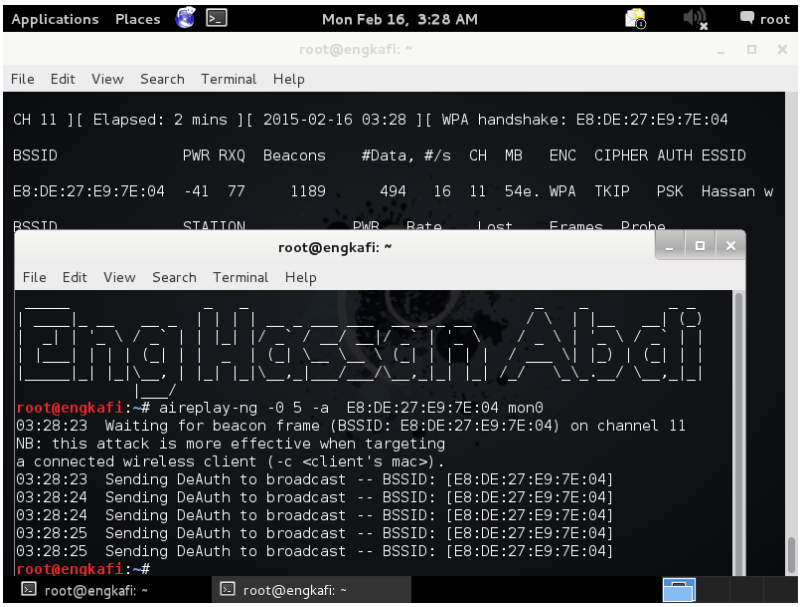
Enjeksiyon komutu:

```
root@engkafi:~#aireplay-ng  -0 5 -a E8:DE:27:E9:7E:04 mon0
```



Şekil 4.14: Deauthentication atağını gerçekleştirme ekranı

Deauthentication atağı gerçekleştirildikten sonar süreç doğru işlemişse el sıkışma airodump-ng kabuğunun sağ üst köşesinde belirmelidir. Aşağıdaki ekranda yakalanmış olan WPA el sıkışması görülmektedir.



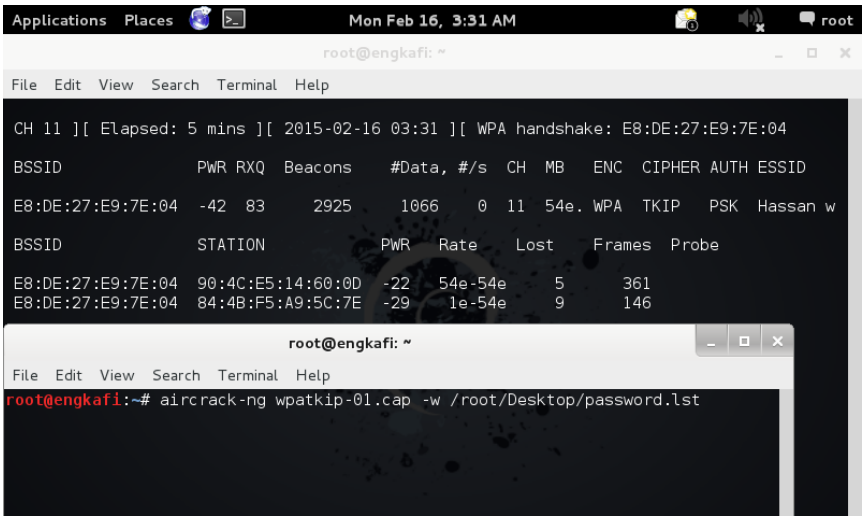
Şekil 4.15: Yakalanmış WPA el sıkışması ekranı

4.2.2. WPA/WPA2 anahtarının kırılması

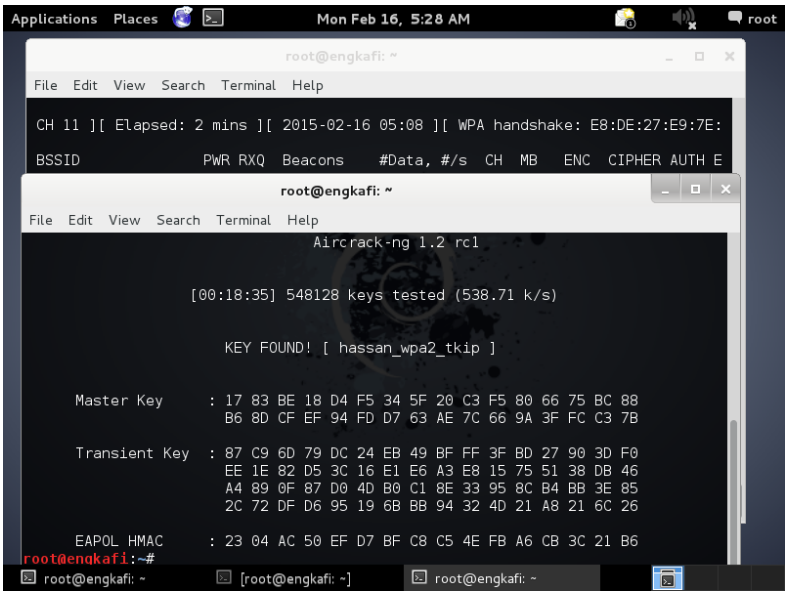
1. Aircrack-ng ile el sıkışma anahtarını kırmak

Dört yollu el sıkışması yakalandıktan sonar airodump-ng kabuğunu durdururuz ve anahtarı bulmak için aircrack-ng komutunu kullanarak bir Dictionary (Sözlük) veya Brute Force atağını başlatırız.

```
root@engkafi:~#aircrack-ng  wpatkip-01.cap  -w  /root/Desktop/password.lst
```



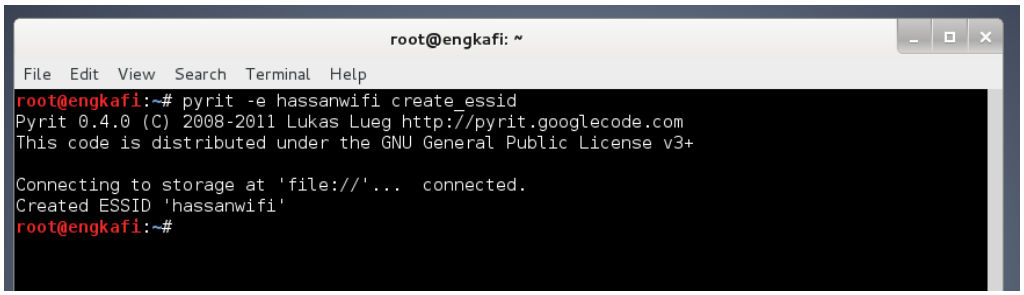
Şekil 4.16: WPA şifre kırma işleminin gerçekleştirilmesi



Şekil 4.17: aircrack-ng kullanarak PSK anahtarının bulunma ekranı

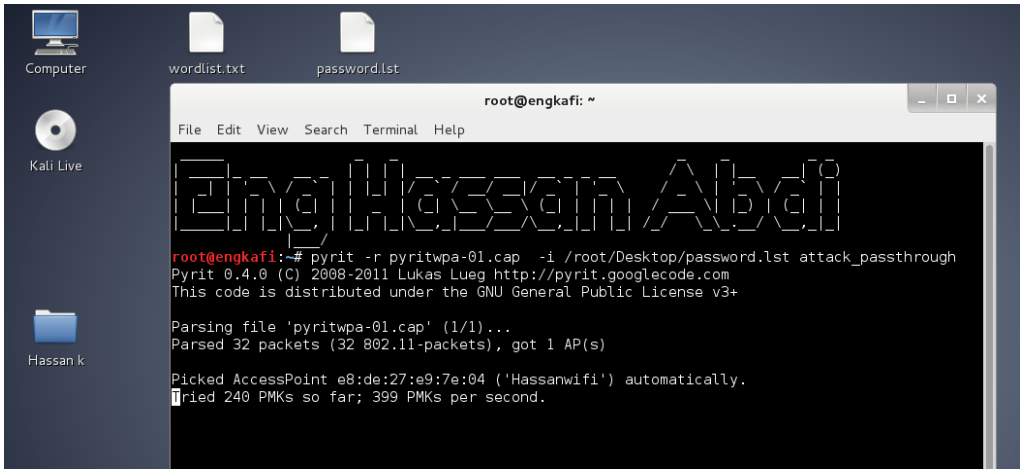
2. Pyrit veritabanını kullanarak el sıkışma anahtarını kırmak

```
root@engkafi:~#pyrit –e hassanwifi create_essid
```

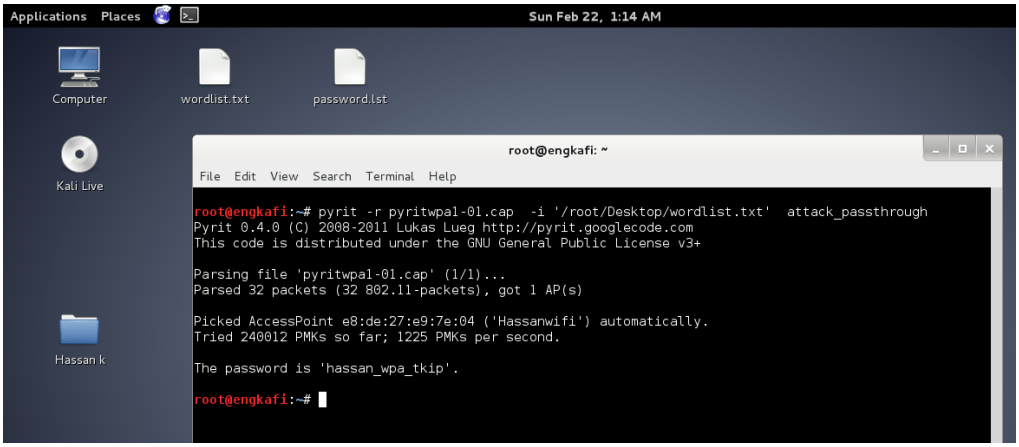


Şekil 4.18: Veritabanındaki hedef için ESSID oluşturma

```
root@engkafi:~#pyrit –r pyritwpa-01.cap –i /root/Desktop/password.lst
attack_passthrough
```



Şekil 4.19: Pyrit programıyla WPA-PSK şifresinin kırılması



Şekil 4.20: Pyrit program kullanarak PSK anahtarının bulunma ekranı

Sonuç olarak yukarıdaki sayfalardaki WEP 64/WEP128 şifre kırma kısımlarında değindiğimiz gibi ortalama işlem süreleri sırasıyla 6 ile 15 dakika sürmektedir. Ancak WPA-PSK /WPA-2 PSK kısmına geldiğimizde işlem süresinin bundan çok daha fazla olduğu görülmektedir. Brute Force atağıyla 8 karışık karakterden oluşmuş bir şifrenin ne kadar sürede çözüldüğünü gözlemleyerek bu sonuç görülebilir. WPA –PSK parolasının Brute Force veya Dictionary atakları ile kırılması için gereken süre parolanın uzunluğuna ve kullanılan karakter kümesine bağlıdır. Atağın yalnızca bir bilgisayarda yapıldığı ve Brute Force hızının saniyede 500 000 parola olduğu varsayılsın. Bu durumda gereken süre, yalnızca küçük harflerden oluşan karakter kümesi için 4 gün, küçük harf ve rakamlar birlikte olduğunda 65 gün, küçük ve büyük harflerin her ikisi de varsa 3 yıl, tüm yazılabilir ASCII karakterleri olduğunda da 463 yıl olmaktadır [30].

Bölüm 4.1 ve 4.2 testlerinde denemeleri gösterilen ve daha önceki bölümlerde de ayrıntısı verilen WEP, WPA, WPA2 protokolleriyle ilgili bazı sonuç ve bilgiler [31] kaynağında raporlanmaktadır.

4.3. TEST #3 WLAN'IN PERFORMANS ÖLÇÜMÜ

Bu kısımda ağ performansıyla ilgili çeşitli metrikler (ölçütler) kullanılmaktadır ve bunların anlaşılması oldukça önemlidir. Kablosuz ağ performansı ölçülürken kullanılan araç ve metotlar aşağıda açıklanmaktadır.

4.3.1. Metrik Tanımları

Normalde ağ mühendisleri ağ konfigürasyonlarını analiz etmek ve ağ problemlerini çözmek için çok sayıda metric kullanmaktadır. Bunlar arasında en yaygın kullanılan iki tanesi yük miktarı (throughput) ve gecikme süresidir (latency). Bunların dışında ağın içinde bulunduğu ortama bağlı olan başka metrikler de vardır. En çok kullanılan bazı performans metrikleri aşağıda açıklanmaktadır:

• **Yük**

Ağ kavramı olarak yük, tahsis edilen zaman içinde bir haberleşme linki üzerinden yollanan veri oranının ölçüsüdür. Bu iletim oranı merkezi işlem birimi, disk preformansı ve birçok diğer çevresel faktörlerden etkilenebilmektedir. Bu metriğin birimi bps şeklindedir (saniye başına bit, bits per second), bazen saniye başına paket (packets per second) olarak da hesaplanabilir [29].

• **Gecikme süresi**

Ağ kavramı olarak gecikme süresi, bir ağ kanalı üzerinden, kaynaktan hedefe doğru tek yönlü veya gidiş-dönüşlü olarak veri iletimi için geçen süredir. Bu birçok nedenden kaynaklanmaktadır. Örneğin link üzerinde verinin yolcululuğundan kaynaklanan yayılım gecikmesi; ağ üzerinde verinin taşınması için gerçek zamanı gösteren iletim gecikmesi; veri kapsüllenmesi ve yol kurulumu için gerekli işlem gecikmesi gibi kısımları vardır [29].

• **Cevap süresi**

Bir istek gönderip alınacak cevabı beklemekle geçen zaman miktarını göstermektedir. Cevaplama süresi böylece gecikme süresi ile işlem süresinin toplamına eşittir. Yük miktarı gibi ağın performansını gösteren bir kavramdır.

• **Bant genişliği**

Ağ kavramı olarak bant genişliği, bir haberleşme kanalının etkin şekilde taşıyabileceği maksimum frekans kapasitesi demektir. Kanalın ilettiği veya aldığı maksimum frekans

olarak düşünülür. Bant genişliği ve yük miktarı aynı gibi düşünülse de aradaki fark şöyle bir örnekle açıklanabilir: bir boru olarak ağ kablosu ele alındığında bant genişliği bu borunun çapına, yük miktarı ise bu boru içerisinden geçen su miktarına eşdeğerdir. İletim oranı elektronik ağ cihazlarına bağlıdır.

4.3.2. Performans Ölçüm Yazılımı

Denemeler için kullanılacak işletim sistemine ve yük testi yazılımına karar vermek oldukça zordur. Çünkü IEEE 802.11 standardıyla uyumluluk problemleri ve her uygulamayı desteklemeyen bilgisayar cihazlarından kaynaklanan diğer problemler vardır.

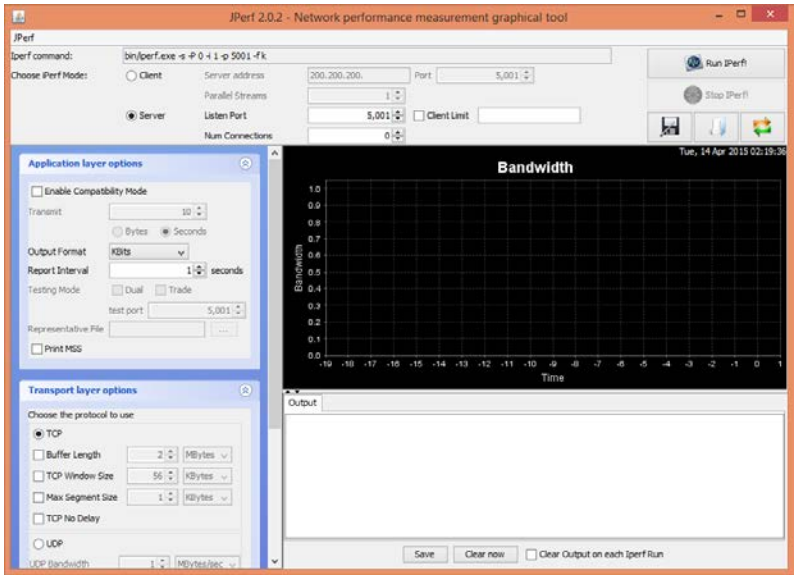
Bu nedenle bu tezdeki deneylerde Microsoft Windows işletim sistemi tercih edilmektedir. Yük testiyle ilgili yazılım konusunda birçok çeşit test edildikten sonra en çok uyumlu olan ve belirlenmiş ağ konfigürasyonu için en iyi sonuçları veren yazılım kararlaştırılmıştır. Bu araştırma çerçevesinde kablosuz ağ performansını ölçmede kullanılacak metrikler yük miktarı ve cevaplama süresi olarak belirlenmektedir. Kendi "**hassanwifi**" isimli kablosuz ağımıza uygulanan çeşitli güvenlik seviyelerini karşılaştırmak için bu metrikler kullanılacaktır. Bu ölçümlerin yapılması sürecinde yazılım olarak **Jperf** kullanılacaktır. Bu yazılım sayesinde farklı şifreleme mekanizmalarının yük miktarını nasıl etkilediği ve farklı protokollerle kimlik denetimi yapmak için ne kadarlık zaman gerektiği ölçülebilmektedir. İlgili yazılımın genel açıklaması aşağıda verilmektedir:

- **Jperf 2.0.2**

Jperf hem TCP, hem UDP trafiğinde yük miktarını ölçmek için kullanılan güçlü ve basit bir ağ performans aracıdır. Jperf ile ağda iletilen verinin çeşitli durumları gözlenir ve değiştirilir. Bu yazılım aracılığıyla UDP bağlantılarıyla ilişkilendirilmiş olan pencere ölçüsü ve bant genişliği gibi metrikleri ayarlama tercihleri yapılmaktadır.

Jperf yazılımının çalışması için hem sunucu, hem istemci üzerinde uygulamanın görev yapması gerekmektedir. Sunucu üzerindeki seçenekler ayarlandıktan sonra ilgili zaman

aralığında istemci bir transfer başlatabilir. İşlem tamamlanınca sunucu ve istemci taraflarının her ikisi de ölçümlerini istemci ve sunucu pencerelerinde raporlarlar.



Şekil 4.21: Jperf uygulama ekranı

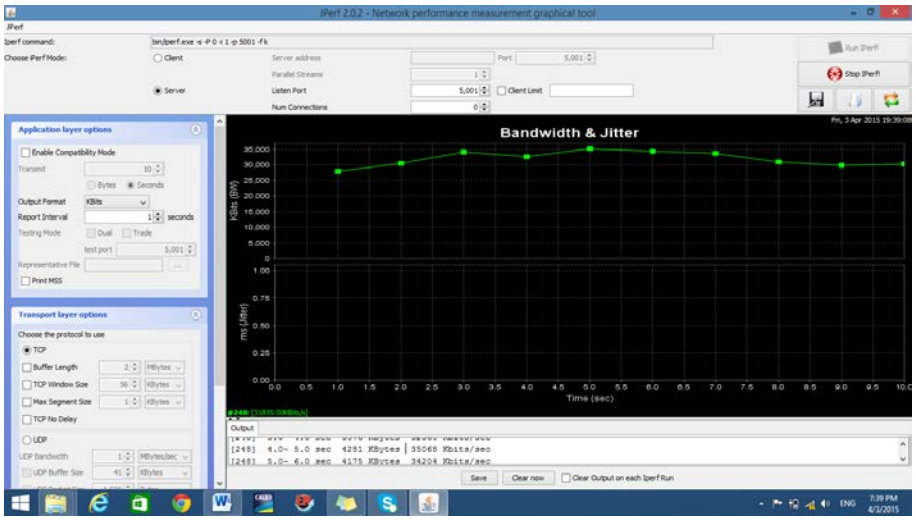
4.3.3. Deneylerin sonuçları

Birinci TCP Testi: Sunucu (150 mbps) WLAN Güvenlik Protokolü: AES şifreleme metoduna sahip WPA2

bin/iperf.exe -s -P 0 -i 1 -p 5001 -f k

Server listening on TCP port 5001
TCP window size: 64.0 KByte (default)
---
[248] local 200.200.200.100 port 5001 connected with 200.200.200.101 port 49160

[ID] Interval	Transfer	Bandwidth
[248] 0.0- 1.0 sec	3395 KBytes	27810 Kbits/sec
[248] 1.0- 2.0 sec	3726 KBytes	30524 Kbits/sec
[248] 2.0- 3.0 sec	4152 KBytes	34010 Kbits/sec
[248] 3.0- 4.0 sec	3976 KBytes	32569 Kbits/sec
[248] 4.0- 5.0 sec	4281 KBytes	35068 Kbits/sec
[248] 5.0- 6.0 sec	4175 KBytes	34204 Kbits/sec
[248] 6.0- 7.0 sec	4097 KBytes	33562 Kbits/sec
[248] 7.0- 8.0 sec	3768 KBytes	30865 Kbits/sec
[248] 8.0- 9.0 sec	3632 KBytes	29750 Kbits/sec
[248] 9.0-10.0 sec	3680 KBytes	30145 Kbits/sec
[248] 0.0-10.0 sec	39016 KBytes	31835 Kbits/sec



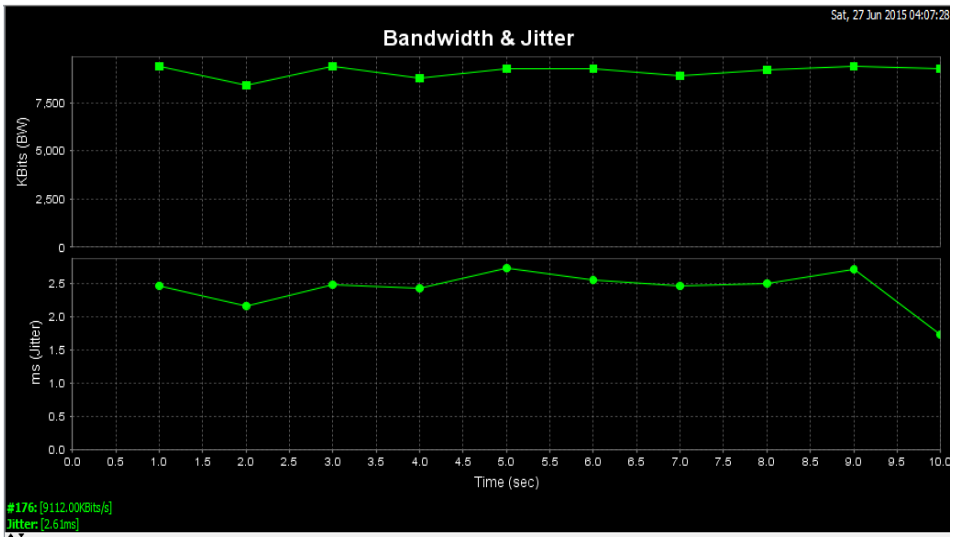
Şekil 4.22: Birinci TCP Testi: Sunucu (150 mbps) WLAN Güvenlik Protokolü: AES şifreleme metoduna sahip WPA2

Birinci UDP Testi: Sunucu (150 mbps) WLAN Güvenlik Protokolü: AES şifreleme metoduna sahip WPA2

bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -f k

Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
---
[176] local 200.200.200.101 port 5001 connected with 200.200.200.100 port 59884

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[176] 0.0- 1.0 sec	1147 KBytes	9396 Kbits/sec	2.462 ms	1229344594/ 799 (1.5e+008%)
[176] 1.0- 2.0 sec	1024 KBytes	8385 Kbits/sec	2.162 ms	0/ 713 (0%)
[176] 2.0- 3.0 sec	1143 KBytes	9361 Kbits/sec	2.475 ms	0/ 796 (0%)
[176] 3.0- 4.0 sec	1074 KBytes	8796 Kbits/sec	2.422 ms	0/ 748 (0%)
[176] 4.0- 5.0 sec	1128 KBytes	9243 Kbits/sec	2.723 ms	0/ 786 (0%)
[176] 5.0- 6.0 sec	1128 KBytes	9243 Kbits/sec	2.542 ms	0/ 786 (0%)
[176] 6.0- 7.0 sec	1088 KBytes	8914 Kbits/sec	2.453 ms	0/ 758 (0%)
[176] 7.0- 8.0 sec	1120 KBytes	9173 Kbits/sec	2.499 ms	0/ 780 (0%)
[176] 8.0- 9.0 sec	1147 KBytes	9396 Kbits/sec	2.707 ms	0/ 799 (0%)
[176] 9.0-10.0 sec	1127 KBytes	9232 Kbits/sec	1.724 ms	0/ 785 (0%)
[176] 0.0-10.0 sec	11128 KBytes	9112 Kbits/sec	2.613 ms	0/ 7752 (0%)

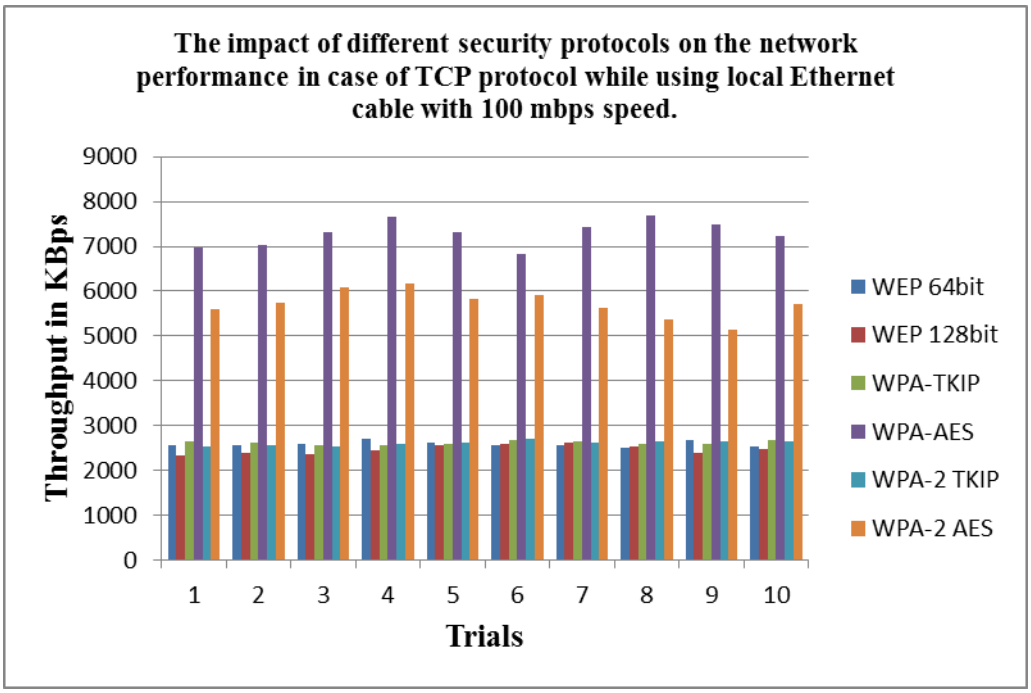


Şekil 4.23: Birinci UDP Testi: Sunucu (150 mbps) WLAN Güvenlik Protokolü: AES şifreleme metoduna sahip WPA2

TCP protokolünün 100 mbps hızında yerel Ethernet kullandığı durumda farklı güvenlik protokollerinin ağ performansı üzerindeki etkisi.

Tablo 4.3: TCP kullanan farklı güvenlik protokolleri için varsayılan pencere ölçüsünün (64k) yük miktarları (Kilobyte/Saniye)

Deneme	**WEP 64bit**	**WEP 128bit**	**WPA-TKIP**	**WPA-AES**	**WPA-2 TKIP**	**WPA-2 AES**
1	2562	2336	2649	6987	2538	5610
2	2567	2400	2608	7033	2567	5753
3	2585	2361	2559	7324	2520	6097
4	2718	2450	2575	7672	2576	6158
5	2632	2558	2600	7316	2608	5816
6	2568	2591	2675	6821	2698	5903
7	2554	2608	2645	7440	2621	5639
8	2503	2529	2584	7691	2642	5377
9	2663	2400	2592	7485	2641	5151
10	2545	2463	2672	7224	2646	5719

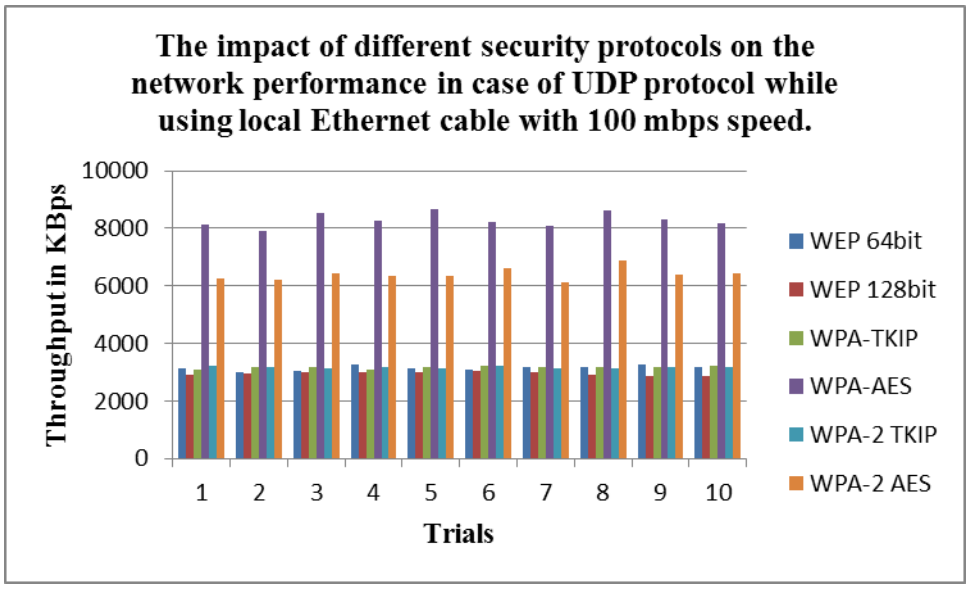


Şekil 4.24: 100 mbps hızındaki Etherneti kullanan TCP içerikli WLAN'da protokollerin yük miktarına etkileri

UDP protokolünün 100 mbps hızında yerel Ethernet kullandığı durumda farklı güvenlik protokollerinin ağ performansı üzerindeki etkisi.

Tablo 4.4: UDP kullanan farklı güvenlik protokolleri için varsayılan pencere ölçüsünün (64k) yük miktarları (Kilobyte/Saniye)

Deneme	WEP 64bit	WEP 128bit	WPA-TKIP	WPA-AES	WPA-2 TKIP	WPA-2 AES
1	3128	2894	3089	8137	3214	6272
2	3009	2970	3184	7930	3157	6194
3	3052	2997	3168	8547	3138	6441
4	3263	3009	3109	8276	3190	6325
5	3154	3020	3160	8665	3128	6337
6	3095	3046	3239	8234	3233	6605
7	3163	2979	3177	8105	3122	6141
8	3167	2918	3171	8632	3135	6873
9	3256	2861	3170	8326	3158	6400
10	3181	2874	3216	8160	3173	6436

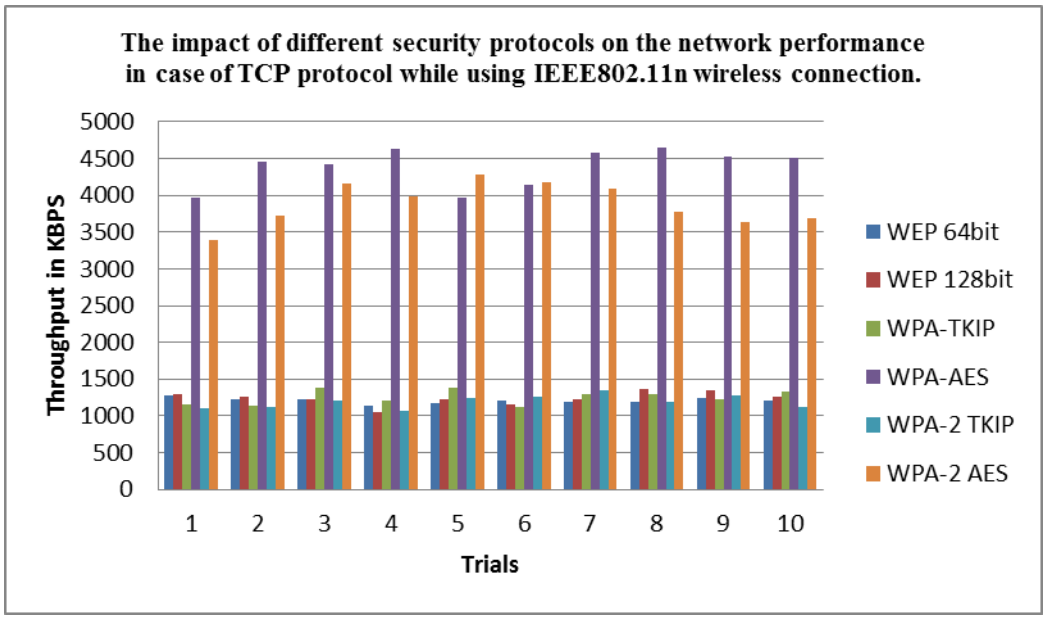


Şekil 4.25: 100 mbps hızındaki Etherneti kullanan UDP içerikli WLAN'da protokollerin yük miktarına etkileri

TCP protokolünün IEEE802.11n bağlantısını kullandığı durumda farklı güvenlik protokollerinin ağ performansı üzerindeki etkisi.

Tablo 4.5: IEEE802.11n bağlantılı TCP kullanan farklı güvenlik protokolleri için varsayılan pencere ölçüsünün (64k) yük miktarları (Kilobyte/Saniye)

Deneme	WEP 64bit	WEP 128bit	WPA-TKIP	WPA-AES	WPA-2 TKIP	WPA-2 AES
1	1280	1288	1153	3961	1097	3395
2	1224	1265	1144	4464	1127	3726
3	1232	1231	1383	4417	1217	4152
4	1144	1056	1201	4638	1072	3976
5	1176	1218	1375	3972	1248	4281
6	1200	1159	1120	4149	1264	4175
7	1184	1234	1304	4584	1352	4097
8	1184	1366	1296	4656	1193	3768
9	1240	1345	1224	4520	1279	3632
10	1208	1264	1336	4505	1120	3680



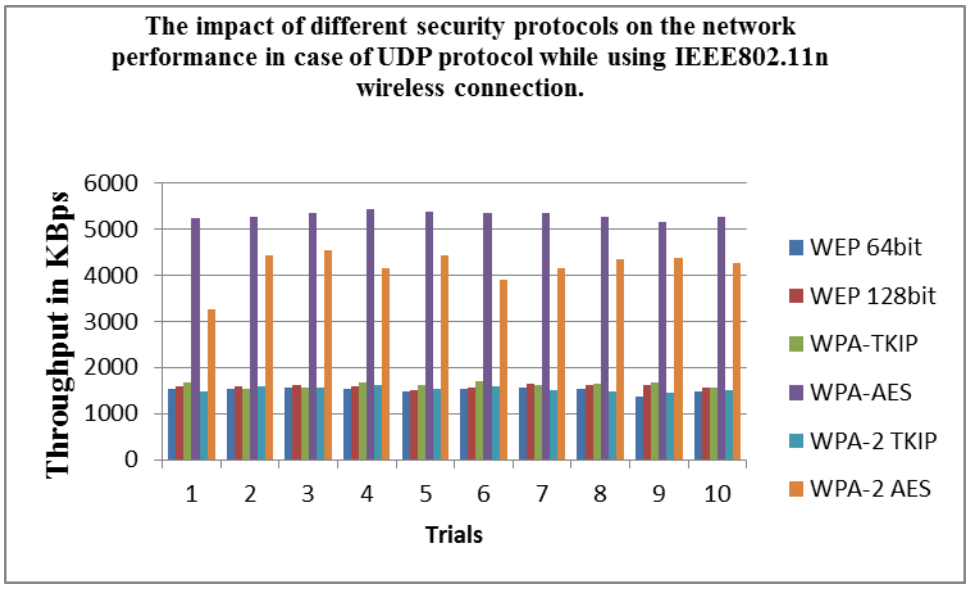
Şekil 4.26: Çeşitli güvenlik protokollerinin IEEE802.11n bağlantılı TCP performansları için yük miktarı gösterimleri

UDP protokolünün IEEE802.11n bağlantısını kullandığı durumda farklı güvenlik protokollerinin ağ performansı üzerindeki etkisi.

Tablo 4.6: UDP kullanan farklı güvenlik protokolleri için varsayılan pencere ölçüsünün (64k) yük miktarları (Kilobyte/Saniye)

Deneme	WEP 64bit	WEP 128bit	WPA-TKIP	WPA-AES	WPA-2 TKIP	WPA-2 AES
1	1542	1593	1661	5248	1476	3274
2	1542	1596	1533	5263	1599	4442
3	1570	1625	1565	5355	1560	4551
4	1540	1598	1685	5434	1616	4156
5	1489	1494	1609	5376	1545	4432
6	1542	1576	1714	5356	1589	3899
7	1558	1637	1618	5356	1499	4144
8	1527	1619	1648	5261	1469	4350
9	1371	1619	1685	5169	1459	4380
10	1469	1552	1569	5263	1506	4259

Tablo 4.6'deki değerlerin grafiksel gösterimi aşağıdadır:



Şekil 4.27: Çeşitli güvenlik protokollerinin IEEE802.11n bağlantılı UDP performansları için yük miktarı gösterimleri

Bu bölüm içerisinde WEP, WPA, WPA-2 gibi çeşitli güvenlik protokollerinin ağ performansı üzerine etkileri incelenmiştir. Deneylerde Ethernet kablosu veya IEEE802.11n kablosuz bağlantısı bulunduran TCP protokolü veya UDP protokolü örnekleri ele alınmıştır. Elde edilen sonuçlardan görüldüğü gibi ağımızı ne kadar güvenli hale getirirsek ağdaki yük miktarını da o kadar düşürmüş oluruz.

Farklı bir yazılım olan IP Traffic kullanılarak TCP ve UDP protokollerine göre ağdaki yük ve cevap süresi ölçümleri [32] kaynağında yer almaktadır.

5. TARTIŞMA VE SONUÇ

Günümüzde teknoloji oldukça önemli bir konumda bulunmaktadır. Bilgisayar uygulamalarının her alanda kullanıldığı bir dünyada Ethernet ortamından kablosuz ağ ortamlarına kadar geniş bir alan söz konusudur. Taşınabilirlik ve esnekliğin önem kazanmasıyla birlikte kablosuz ağlar da gittikçe yaygınlaşmaktadır.

Bu tez kapsamında IEEE 802.11a/b/g /n/ac spesifikasyonları ve özellikle IEEE 802.11n standardına dayalı WLAN'lar için bulunan güvenlik protokollerinin analizi ele alınmıştır. Hücresel ağlara göre daha avantajlı olan WLAN'lar özellikle yüksek iletim oranları ve düşük iletim mesafeleriyle kullanım kolaylığı sunmaktadır. Tez boyunca WEP 64bit, WEP 128bit, WPA-PSK/WPA2-PSK güvenlik protokollerinin şifre kırma süreçlerinin yanısıra ağ ortamında trafik metrikleriyle ilgili ölçümler yapılmıştır. Bütün bu aşamaları gerçekleştirmek için üç farklı uygulama hazırlanmıştır. Ağ performansı ölçümlerinde özellikle TCP ve UDP protokollerinin kullanılması ile birlikte Ethernet kablosuz veya IEEE802.11n kablosuz bağlantısı kullanma durumları analiz edilmiştir. Böylelikle çeşitli güvenlik protokollerinin ağ yükü sonuçları gösterilmiştir.

Sonuç olarak bu çalışmadaki üç uygulamanın genel çıktısı şunlardır:

Test #1 aracılığıyla ilk kablosuz güvenlik protokolü olan WEP protokolünün bir ağı saldırganlardan korumak için elverişli olmadığı ve Aircrack-ng araçları ile Kali Linux kullanıldığında şifrelerin ortalama olarak 3 ve 7 dakika gibi sürelerde kırılabildiği görülmektedir.

Test #2'de WPA-PSK /WPA2-PSK şifrelemelerine kırma testi uygulanmaktadır ve bu protokollerin ağ üzerinde WEP'e göre daha güçlü bir güvenlik sağladığı ortaya analiz edilmektedir. Böyle bir düzenekte saldırgan kolay kolay başarılı olamamaktadır.

Test #3 ile daha güvenli mekanizmalar kullanıldığında ağ yükünün azaldığı görülmektedir.

Kablosuz ağ konusunda gün geçtikçe yeni çalışmalar yapılarak farklı algoritmalar geliştirilmektedir. Bu çalışmanın ileriki aşamaları için daha farklı güvenlik algoritmaları kullanılarak bunların test karşılaştırmaları yapılabilir. Çok sayıdaki kablosuz ağ protokolünün teorik kısımları incelenerek bunların heterojen şekilleri elde edilebilir. Heterojen yapılarda farklı algoritmaların farklı avantajları birleştirilince sonuçlar değişebilmektedir. Bunların dışında farklı araştırmacıların uygulamaları ile bu tez kapsamında tasarlanan uygulamalar, çalışma süresi ve bellek kullanımı gibi çeşitli performans parametreleri açısından karşılaştırılarak en etkin yöntem ortaya çıkarılabilir.

KAYNAKLAR

[1] Feng, P., 2012, Wireless LAN Security Issues And Solutions, 2012 IEEE Symposium On Robotics and Applications (ISRA), Changzhou Institute of Light Industry Technology, Changzhou,China, ISBN: 978-1-4673-2207-2/12, 921-924.

[2] Digi International Inc., 2008, An Introduction to Wi-Fi®, ISBN: 019-0170 - 090409-B.

[3] Gast, M., 2005, 802.11 (®) Wireless Networks The Definitive Guide, 2nd ed., Sebastopol: O'Reilly, Nisan 2005, p. 630, ISBN : 0-596-10052-3.

[4] Singh A.K., and Mishra B., 2012, Comparatıve Study On Wıreless Local Area Network Standards, International Journal of Applied Engineering and Technology, 2(3), 1-4.

[5] Boban B., 2014, Comparative Analysis In IEEE 802.11 Standards, Lovely Faculty of Technology and Sciences, Lovely Professional University, Phagwara, 1-7.

[6] Li J., and Garuba M., 2008, Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities, in Fifth International Conference on Information Technology: New Generations, Howard University - DC 20059, USA, 557 -562.

[7] Lashkari, A.H., Towhidi, F., Hosseini, R.S., 2009, Wired Equivalent Privacy (WEP), 2009 International Conference on Future Computer and Communication (ICFCC 2009), ISBN: 978-0-7695-3591-3/09, 492- 495.

[8] Lashkari, A.H., Mansoori, M., Danesh A.S., 2009, Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA), 2009 International Conference on Signal Processing Systems, IEEE Xplore., ISBN: 978-0-7695-3654-5/09, 445-449.

[9] Galvane, Q. And Uzel, B., 2012, Cryptography - RC4 Algorithm, Undergraduate Project Team 4, Rochester Institute of Technology- Department of Computer Science.

[10] Halvorsen, F.M., Haugen, O., 2009, Cryptanalysis of IEEE 802.11i TKIP, Master of Science in Communication Technology, Norwegian University of Science and Technology-Department of Telematics.

[11] Lashkari, A.H., Danesh, M.M.S., Samadi, B. 2009, A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i), IEEE , ISBN: 978-1-4244-4520, 48-52.

[12] Wang, M., Dai, G., Hu, H., Pen, L., 2008, Security Analysis for IEEE802.11, IEEE, ISBN: 978-1-4244-2108-4/08

[13] NETGEAR Inc, 2005, Wireless Networking Basics, 4500 Great America Parkway, Santa Clara, CA 95054 USA.

[14] Fluhrer, S., Mantin, I., Shamir, A., 2001, Weaknesses in the Key Scheduling Algorithm of RC4, 1-23.

[15] Rahman, M., Hassan Riyad, M. A., Sinha M. I. And Fazlul, A. 2011, Security Enhancement of WEP Protocol IEEE802.11b with Dynamic Key Management," Proceedings of the World Congress on Engineering and Computer Science 2011 (WCECS 2011), San Francisco, USA, 2011, ISBN: 978-988-18210-9-6.

[16] IEE, 2004, Extensible Authentication Protocol (EAP), The Internet Society.

[17] Zhao, S. Shoniregun, CH.A. and Imafidon, CH.,2008, Addressing the vulnerability of the 4-way handshake of 802.11i, Third International Conference on Digital Information Management (ICDIM), ISBN: 978-1-4244-2917-2/08, 351-356.

[18] Ananthoj R. et.al., 2007, CMPE 209 Network Security, San Jose State University, Thesis.

[19] Sotillo, S., 2007, Extensible Authentication Protocol (EAP) Security Issues.

[20] Sukhija, S. And Gupta S., 2012, Wireless Network Security Protocols A Comparative Study, International Journal of Emerging Technology and Advanced Engineering, 2(1), ISSN 2250-2459, 357-364.

[21] Karygiannis, T. and Owens, L., 2002, Wireless Network Security 802.11, Bluetooth and Handheld Devices, National Institute of Standards and Technology, Gaithersburg, NIST Special Publication 800-48, 3-19- 2-24.

[22] Kumar, U. and Gambhir, S., 2014, A Literature Review of Security Threats to Wireless Networks, International Journal of Future Generation Communication and Networking, 7(4), 25-34.

[23] Wang, Y., Jin, Z., and Zhao, X., 2010, Practical Defence against WEP and WPA-PSK Attack for WLAN, 6th International Conference on Wireless Communications Networking And Mobile Computing (wicom), Chengdu, ISBN: 978-1-4244-3709-2/10.

[24] M. Caneill and J.-L. Gilis, "Attacks against the wifi protocols WEP and WPA," 2010.

[25] M. Beck, E. Tews, Practical attacks against WEP and WPA, http://dl.aircrack-ng.org/breakingwepandwpa.pdf, November 8, 2008. [Son Erişim 21 Haziran 2015].

[26] "Kali Linux," [Online]. Available: https://www.kali.org/downloads/. [Son Erişim 4 Mayıs 2015].

[27] "iperf," [Online]. Available: http://iperf.sourceforge.net/. [Son Erişim 4 Mayıs 2015].

[28] "jperf 2.0.2," [Online]. Available: https://code.google.com/p/xjperf/. [Son Erişim 4 Mayıs 2015].

[29] Georgios G., 2014, Wifi Security and Testbed Implementation for WEP/WPA Cracking Demonstration, Thesis (Master), Master of Science in Networking and Data Communications, Kingston University, London, 1-78.

[30] Lastbit.com, 1997, Last Bit Sofware, . [Online]. Available: http://lastbit.com/password-recovery-methods.asp#Brute Force Attack. [Son Erişim 23 Nisan 2015].

[31] Abdi Mohamed, H. and Yiltas-Kaplan, D., 2015, Cracking Tests on WLAN Security Protocols, International Conference on Communication Information Technology and Robotics, Dubai, United Arab Emirates, 13-15 Ağustos 2015 (Kabul Edildi).

[32] Gürkaş, G.Z., Danışman:Zaim, A.H., 2005, Kablosuz Güvenlik Protokollerinin Karşılaştırmalı Analizi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi.

[33] "JAVA SE," [Online]. Available: http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html. [Son Erişim 4 Mayıs 2015].

[34] "wikipedia.org," [Online]. Available: http://en.wikipedia.org/wiki/Kali_Linux. [Son Erişim 5 Mayıs 2015].

[35] "docs.kali.org," [Online]. Available: http://docs.kali.org/introduction/what-is-kali-linux. [Son Erişim 5 Mayıs 2015].

[36] Aircrack-ng Tool, 2015, [Online]. Available: http://en.wikipedia.org/wiki/Aircrack-ng. [Son Erişim 5 Mayıs 2015].

[37] Dyson , P., 1999, Dictionary of Networking, 3rd edition ed., ISBN: 1-58720-045-7.

[38] Barnett, D., Groth, D. and Mcbee, J., 2004, Cabling: The Complete Guide to Network Wiring,3rd ed, San Francisco , London: SYBEX Inc , ISBN: 002-5211443316.

[39] Bouvette, Th.D., 802.11 WEP and WPA-PSK keys cracking program , http://www.aircrack-ng.org, 05-02-2015. [Online].

[40] "wikipedia," [Online]. Available: http://en.wikipedia.org/wiki/vmware_Workstation. [Son Erişim 4 Mayıs 2015].

EKLER

Bu tez çalışması boyunca kullanılan yazılımlarla ve yöntemlerle ilgili yardımcı kaynaklar [33]-[40] arasında belirtilmiştir.

EK A

VMware Workstation 11 Kurulumu

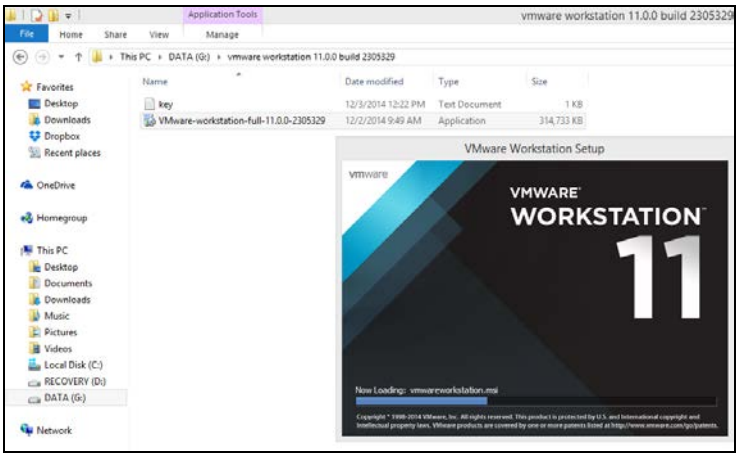
- **VMware Workstation'a Kısa Bir Bakış**

VMware Workstation 32 ve 64 bit bilgisayarlarda çalışan bir bilgisayar yazılımı olup, kullanıcıların tek bir fiziksel ana bilgisayarda bir ya da daha fazla sanal makine (VM) oluşturmasını ve kurmasını sağlar.

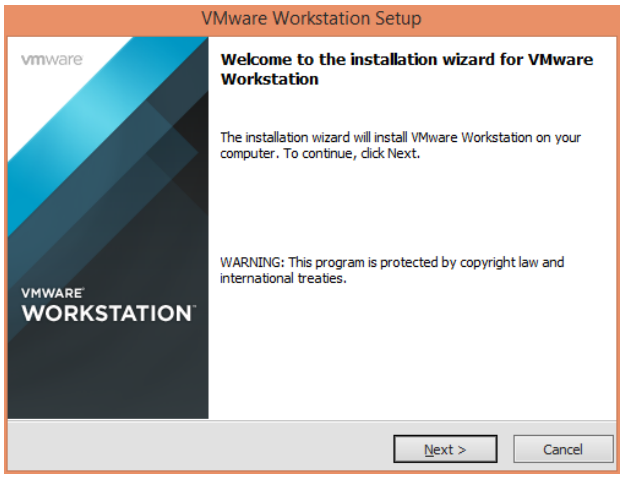
Tüm bu sanal makineler Microsoft Windows gibi kendi işletim sistemleriyle birbirinden bağımsız olarak çalışır.

VMware Workstation, EMC Corporation'un bağlı bir kuruluşu olan VMware, Inc. tarafından geliştirilmiştir ve satılmaktadır. [40]

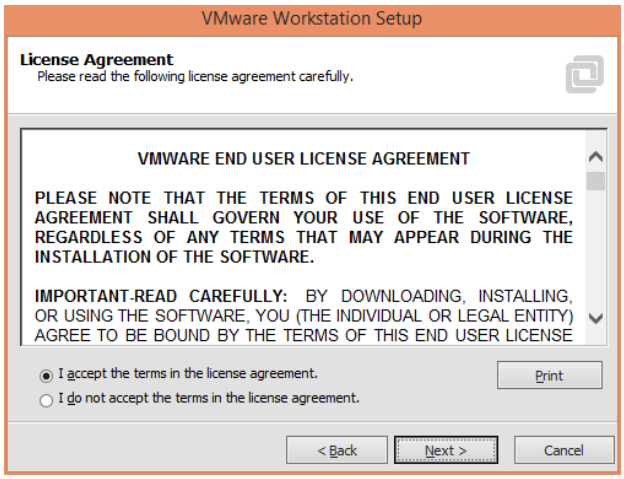
- **VMware Workstation v. 11 Kurulum ekranları**



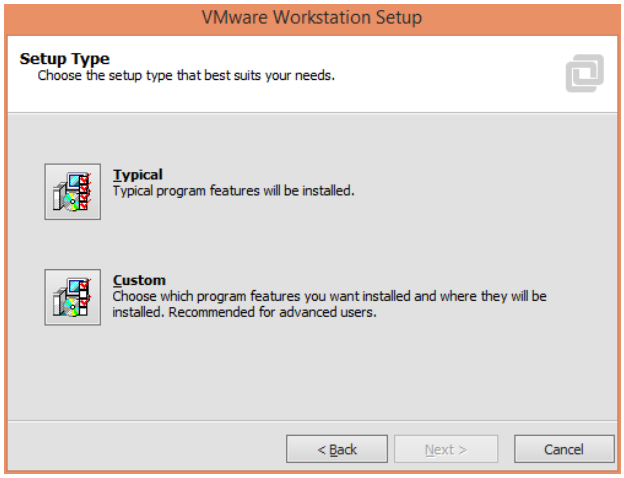
Şekil A.1: Uygulama dosyası çalıştırıldıktan sonraki yükleme işlemi sayfasını göstermektedir



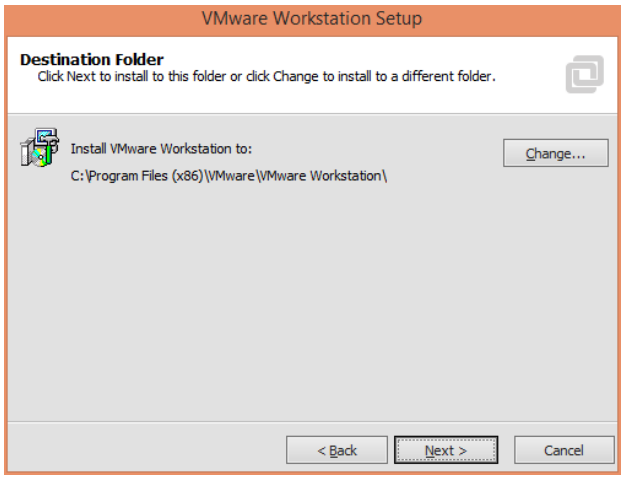
Şekil A.2: Bu, kuruluma hazırlığın ilk ekranıdır



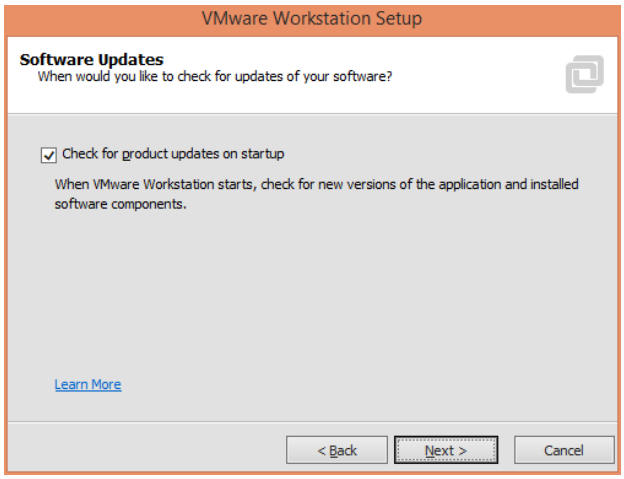
Şekil A.3: Lisans Sözleşmesi sayfası



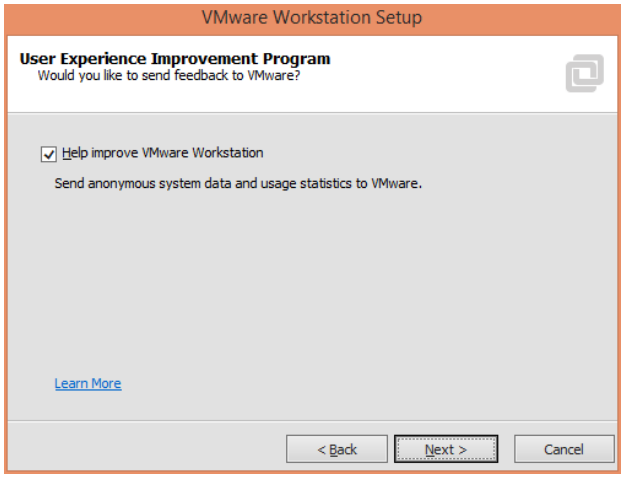
Şekil A.4: Kurulum tipi seçimi ekranı



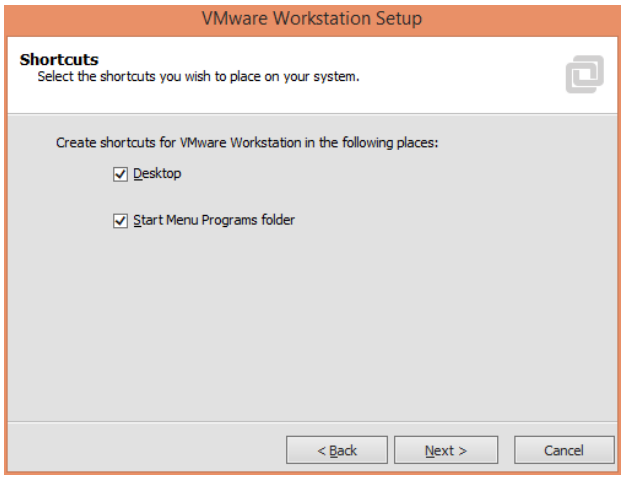
Şekil A.5: Hedef klasör seçimi ekranı



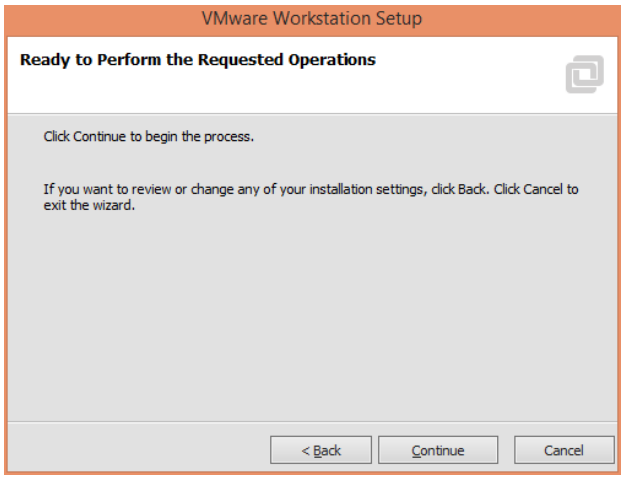
Şekil A.6: Yazılım güncellemeleri kontrolü ekranı



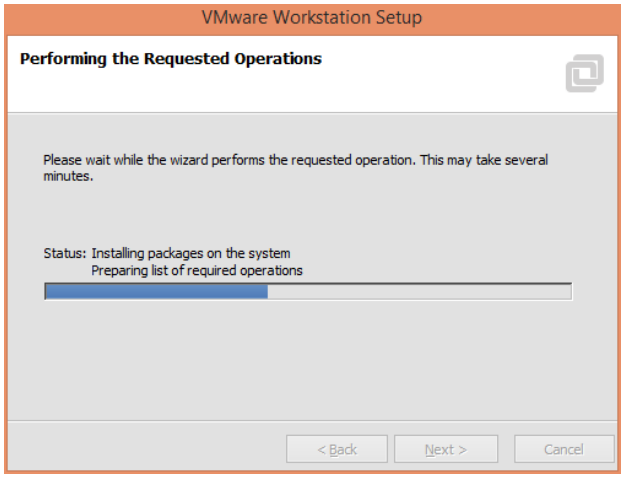
Şekil A.7: Kullanıcı Deneyimi Geliştirme ekranı



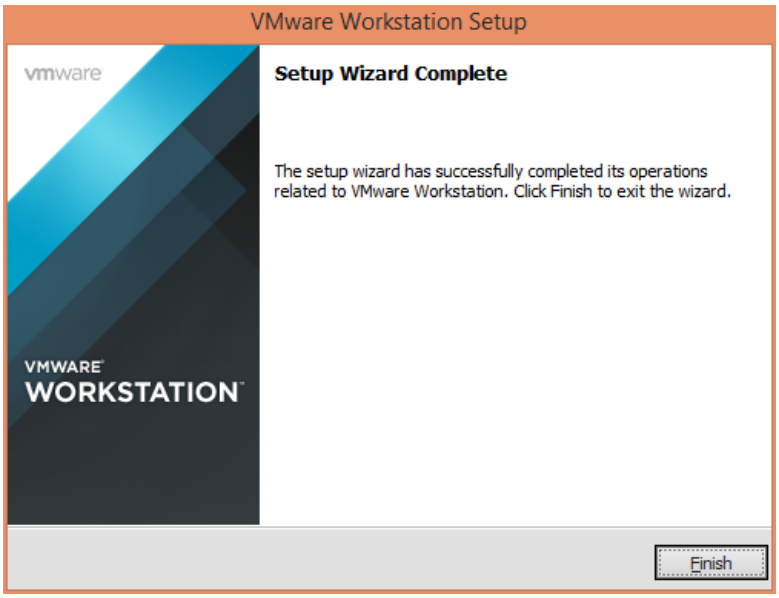
Şekil A.8: Kısayolların yerleşimi seçimi ekranı



Şekil A.9: Kurulumu başlatmaya hazır



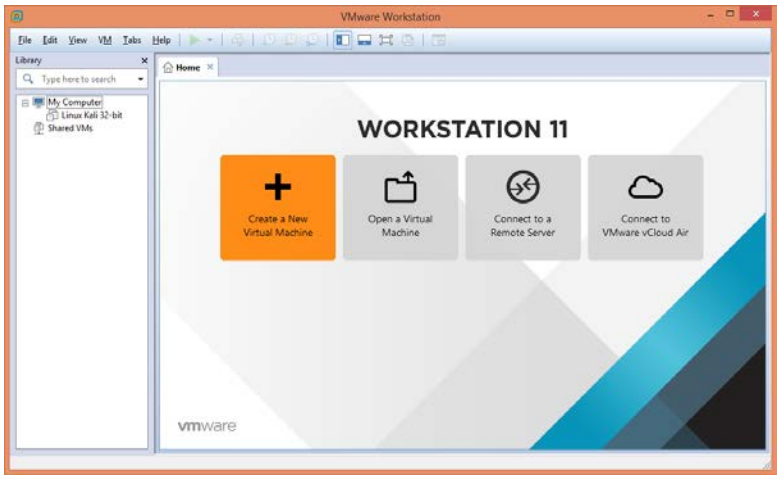
Şekil A.10: Bilgisayara kuruluyor



Şekil A.11: VMware kurulumu tamamlama sihirbazı

- **VMware Workstation v.11'i Çalıştırma ve Kali Linux Kurulumu**

Bu bölümde Kali Linux'ın en son ISO imaj sürümünü indirmemiz gerekmektedir, bunu Kali Linux web sayfasından indirebilirsiniz [26]

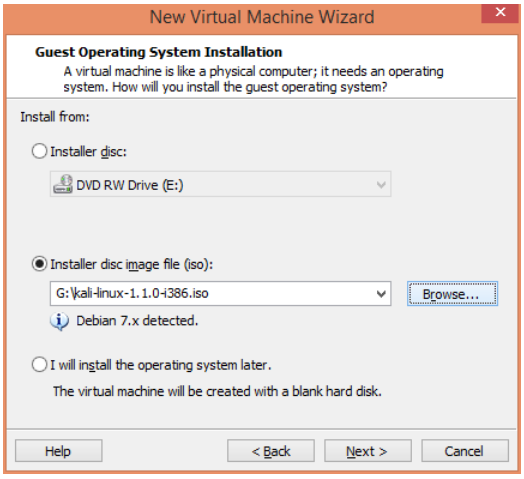


Şekil A.12: Başlangıç VMware Workstation 11 penceresi

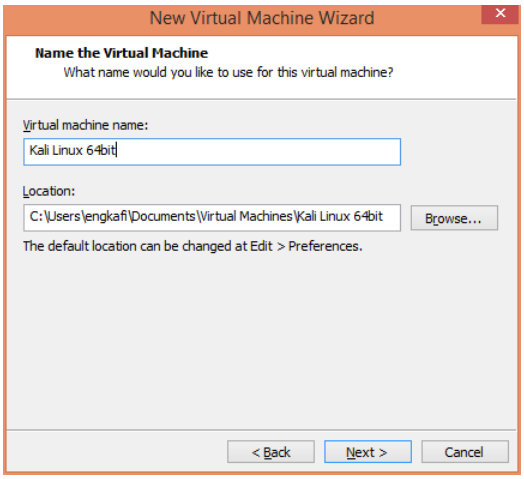
Masaüstündeki VMware Workstation v11 kısayolu çalıştırıldıktan sonra yukarıdaki pencere ekranı görünür.

Yeni sanal makine oluşturmak için artı (+) simgesine tıklayın ve aşağıdaki ekranlara devam edin

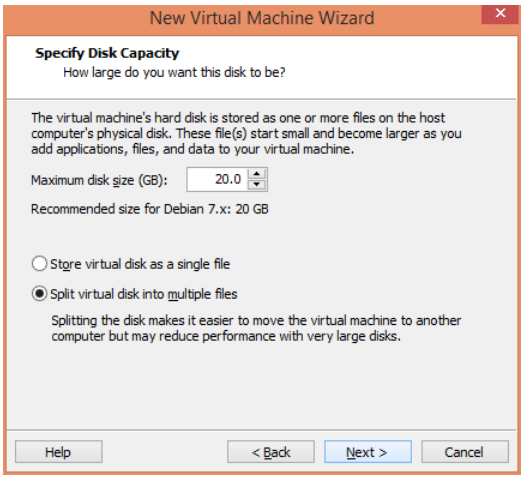
Şekil A.13: Yeni sanal makine sihirbazı



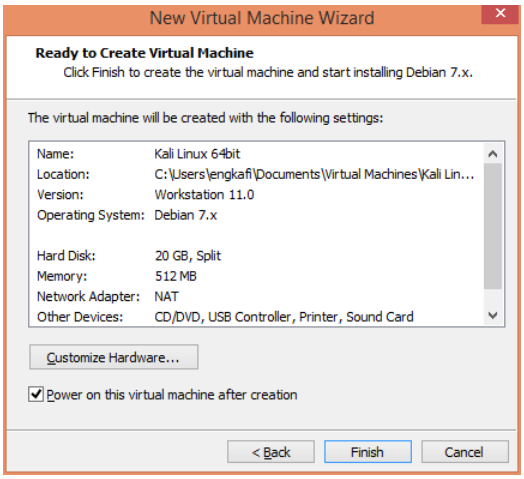
Şekil A.14: Konuk İşletim Sistemi kurulumu



Şekil A.15: Sanal Bilgisayarı Adlandırma



Şekil A.16: VM Disk Kapasitesini belirleme ekranı

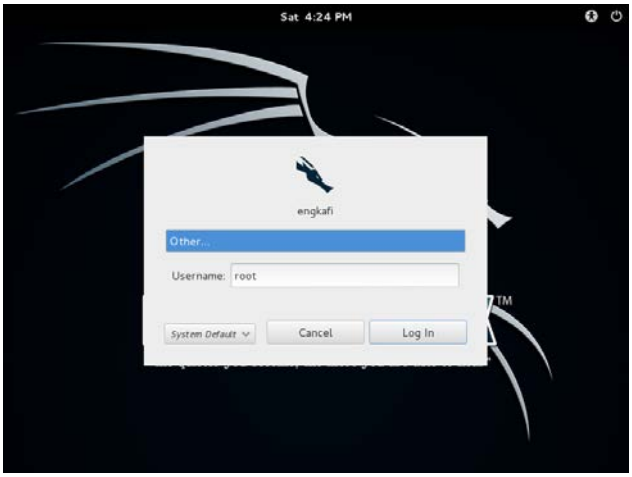


Şekil A.17: Özet ekranı

VM kurulum işlemi tamamlandıktan sonra işletim sisteminin kurulumu otomatik olarak başlar.

Şekil A.18: Kali Linux ilk kurulum ekranı

Bundan sonraki tüm ekranlar, dil, tarih, bilgisayar adı vb. ayarları gibi düz ve basittir ekranlardır



Şekil A.19: Kali Linux'ta oturum açma ekranı

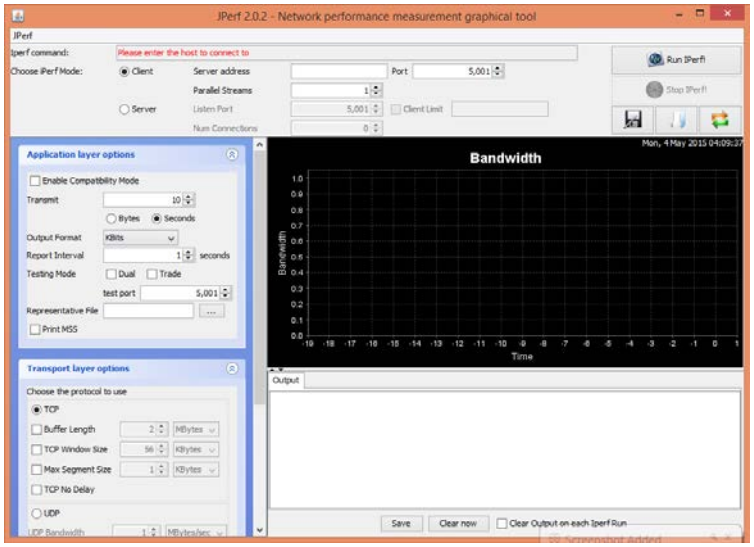
Şekil A.20: Kali Linux için varsayılan ana ekran

EK B

JPerf 2.0.2'nin Çalıştırılması

Deneysel çalışmada bahsettiğimiz üzere JPerf, iperf temelli ağ bant genişliği ölçüm aracıdır [27] ve Google code'dan indirilebilir. [28] Yalnız JPerf 2.0.2 için ön gereksinim olarak JAVA SE gerekir, JAVA SE'yi de Oracle'ın web sitesinden indirebilirsiniz [33].

JPerf 2.0.2 çalıştırabilir dosyalar portalıdır ve kurulum işlemlerinin yapılandırılması gerekmez.



Şekil B.1: JPerf 2.0.2'nin başlangıç ekranı

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı	Hassan ABDI MOHAMED
Uyruğu	SOMALI
Doğum tarihi, Yeri	1985, MOGADISHU
Telefon	05533090904
E-mail	Kaafi2002@gmail.com
Web adres	Enghassam.wordpress.com

Eğitim

Derece	Kurum/Anabilim Dalı/Programı	Yılı
Yüksek Lisans	İ.Ü. Fen Bilimleri Enstitüsü/ Bilgisayar Mühendisliği / Bilgisayar Mühendisliği Programı	2015
Lisans	Mogadishu University/Faculty of Computer Science and IT/Computer Science	2009
Lise	Al-khalil Primary and Secondary School	2004