T.C.
KONYA TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KABLOSUZ AĞDAN DÜŞÜRME SALDIRILARINA KARŞI KORUNMAK İÇİN SİNYAL İZLEME TEMELLİ ANOMALİLERİN ALGILANMASI VE ENGELLEMESİ

Yusuf TAŞ

YÜKSEK LİSANS TEZİ

Elektrik Elektronik Mühendisliği Anabilim Dalı

Mayıs-2024
KONYA

TEZ KABUL VE ONAYI

YUSUF TAŞ tarafından hazırlanan "Kablosuz Ağlarda Ağdan Düşürme Saldırılarına Karşı Korunmak İçin Sinyal İzleme Temelli Anomalilerin Algılanması ve Engellemesi" adlı tez çalışması 15/05/2024 tarihinde aşağıdaki jüri tarafından oy birliği ile Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Elektrik Elektronik Mühendisliği Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Danışman	
Prof. Dr. Levent SEYFİ	……..
Üye	
Doç. Dr. Ömer Kaan BAYKAN	……..
Üye	
Doç.Dr. Muhammed Fahri ÜNLERŞEN	……..

Yukarıdaki sonucu onaylarım.

Prof. Dr. Mevlüt Uyan
Enstitü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Yusuf TAŞ
18.04.2024

ÖZET

YÜKSEK LİSANS TEZİ

KABLOSUZ AĞLARDA AĞDAN DÜŞÜRME SALDIRILARINA KARŞI KORUNMAK İÇİN SİNYAL İZLEME TEMELLİ ANOMALİLERİN ALGILANMASI VE ENGELLEMESİ

Yusuf TAŞ

Konya Teknik Üniversitesi
Lisansüstü Eğitim Enstitüsü
Elektrik Elektronik Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Levent SEYFİ

2024, 67 Sayfa

Jüri
Prof. Dr. Levent SEYFİ
Doç. Dr. Ömer Kaan BAYKAN
Doç. Dr. Muhammed Fahri ÜNLERŞEN

Günümüzde internet kullanım oranı o kadar artmıştır ki; 2021 verilerine göre dünyadaki insanların %59.5'i internet kullanmaktadır. İnternet kullanımının bu kadar yaygınlaşmasında kablosuz ağ teknolojileri büyük rol almaktadır. Bu durum güvenlik sorunlarını da beraberinde getirmektedir. Kablosuz ağlarda iletişim güvenliği konusunda birçok potansiyel tehdit bulunmaktadır. Bilgisayar korsanları, kablosuz ağa bağlı olan kullanıcıların ağ trafiğini izleyebilir, değiştirebilir ve kişisel bilgilerini ifşa edebilirler. Kolay uygulanabilir olması ve diğer birçok güvenlik sorununa kapı aralaması nedeniyle ağdan düşürme saldırıları en tehlikeli saldırı yöntemi olarak kabul edilmektedir. Bu yöntemde kablosuz ağ iletişim protokollerindeki güvenlik zafiyetlerinden yararlanılarak kullanıcıların bağlantısı sonlandırılır. Bu aşamadan sonra bilgisayar korsanları amaçlarına göre farklı saldırı tekniklerini uygulayabilmektedir.

Bu tez çalışmasında, kablosuz ağlarda gerçekleştirilen ağdan düşürme saldırılarını tespit etmek ve önlemek için bir yazılımın geliştirilmesi amaçlanmıştır. Bu yazılımda Python programlama dili, Scapy kütüphanesi ve kullanıcı dostu bir arayüz GUI (Graphical User Interface) kullanılmıştır.

İlk etapta Wi-Fi alıcı kartıyla ortamdaki ağlar taranır. Sonrasında tespit ve uyarı yazılımından korunması istenilen ağ seçilerek koruma altına alınır. Saldırı gerçekleştirildiğinde tespit ve uyarı yazılımı sesli ikaz verir. Bu ikaz sayesinde bir anormalliğin olduğu anlaşılarak ağdan düşürme saldırısından korunmak amacıyla bağlı olduğumuz ağdan bağlantımızı sonlandırırız.

Anahtar Kelimeler: Kablosuz Ağ, Ağdan Düşürme Saldırısı, Monitör Mod, Kali Linux, Wireshark, Aircrack-ng, Scapy, Tkinter

ABSTRACT

MS THESIS

DETECTION AND PREVENTION OF ANOMALIES BASED ON SIGNAL MONITORING TO PROTECT AGAINST DEAUTHENTICATION ATTACKS IN WIRELESS NETWORKS

Yusuf TAŞ

Konya Technical University
Institute of Graduate Studies
Department of Electrical Electronics Engineering

Advisor: Prof.Dr. Levent SEYFİ

2024, 67 Pages

Jury
Prof.Dr. Levent SEYFİ
Assoc.Prof.Dr. Ömer Kaan BAYKAN
Assoc.Prof.Dr. Muhammed Fahri ÜNLERŞEN

The use of the internet has increased so much in today's world that, according to 2021 data, 59.5% of the world's population uses the internet. Wireless network technologies play a significant role in the widespread use of the internet. In this case also bring along security issues. There are numerous potential threats to communication security in wireless networks. Hackers can monitor, modify, and disclose the network traffic of users connected to wireless networks. Due to its ease of execution and its potential to open the door to many other security problems, deauthentication attacks are considered the most dangerous attack method. In this method, the attackers exploit security vulnerabilities in wireless network communication protocols to terminate the users' connections. After this stage, hackers can implement various attack techniques according to their objectives.

The aim of this thesis is to develop a software to detect and prevent deauthentication attacks in wireless networks. In this software, the Python programming language, the Scapy library, and a user-friendly graphical user interface (GUI) are used.

In the first stage, networks in the environment are scanned with the Wi-Fi receiver card. Afterwards, the network that is required to be protected from the detection and warning software is selected for protection. When an attack is carried out, the detection and warning software gives an audible alert. Upon receiving the alert, we disconnect our connection from the network to prevent ourselves deauthentication attacks, which exploit anomalies.

Keywords: Wireless Network, Deauthentication Attack, Monitor Mode, Kali Linux, Wireshark, Aircrack-ng, Scapy, Tkinter

ÖNSÖZ

Bu yüksek lisans tezinin hazırlanmasında başta manevi desteklerini esirgemeyen, hayatım boyunca yanımda duran, ilerlediğim yolda nasıl hareket etmem gerektiğini gösteren, her zaman ve her koşulda bana güvenen, inanan değerli ailem; Annem, Babam, Ağabey'im, Kız Kardeşim, Yengem ve diğer TAŞ ailesi bireyleri iyiki varsınız.

Ayrıca bu süreçte benimle her türlü bilgi birikimini paylaşan, beni sabırla dinleyen, beni doğru yönlendiren ve yazılımsal anlamda desteklerini hiçbir zaman esirgemeyen değerli arkadaşım İlkcan DOĞAN'a, Yüksek Lisansa başlamamda en büyük desteği veren başta değerli komutanlarım Muhabere Albay Serdar TÜRK ve Muhabere Binbaşı İsmail AKCURA olmak üzere diğer değerli komutanlarım ve kurum arkadaşlarıma desteklerinden ötürü teşekkürü borç bilirim.

Değerli danışmanım Sn. Prof. Dr. Levent SEYFİ 'ye Yüksek Lisans sürecim boyunca bana kattıklarından, olumlu tutumundan, hoşgörüsünden, anlayışından ve tez süresince yol haritamı çizmeme vesile olan uzmanlığından ve engin tecrübelerinden dolayı teşekkür eder sevgi ve saygılarımı sunarım.

Yusuf TAŞ
KONYA-2024

İÇİNDEKİLER

KISALTMALAR

AAA : Authentication, Authorization Accounting (Kimlik Doğrulama, Yetkilendirme Muhasebesi)
AES : Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
AP : Access Point (Erişim Noktası)
ASCII : American Standard Code for Information Interchange
ATM : Asynchronous Transfer Mode (Asenkron İletim Modu)
BSSID : Basic Service Set Identifier (Temel Hizmet Seti Tanımlayıcı)
CCMP : Counter Mode with Cipher Block Chaining Mode Protocol (Şifre Blok Zinciri Bağlama İleti Doğrulama Kodu Protokolü)
DeAuth : Deauthentication (Ağdan Düşürme)
DES : Data Encryption Standard (Veri Şifreleme Standardı)
DHCP : Dynamic Host Configuration Protocol (Dinamik Ana Bilgisayar Yapılandırma Protokolü)
DKE : Dynamic Key Exchange (Dinamik Anahtar Değişimi)
DNS : Domain Name System (Alan Adı Sistemi)
DNSmasq : Domain Name System Mass Query (Alan Adı Sistemi Kütle Sorgusu)
DoS : Denial of Service (Hizmet Reddi)
DSSS : Direct Sequence Spread Spectrum (Doğrudan Dizi Yayılı Spektrum)
FHSS : Frequency Hopping Spread Spectrum (Frekans Atlama Yayılı Spektrum)
FIPS : Federal Information Processing Standards (Federal Bilgi İşleme Standartları)
GHz : Gigahertz
GUI : Graphical User Interface (Kullanıcı dostu Arayüz)
HTML : Hypertext Markup Language (Hipermetin İşaretleme Dili)
ICV : Integrity Check Value (Bütünlük Kontrol Değeri)
IDE : Integrated Development Environment (Entegre Geliştirme Ortamı)
IEEE : Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
ISO : International Organization for Standardization (Uluslararası Standartlar Örgütü)
IoT : Internet of Things (Nesnelerin İnterneti)

IP	: Internet Protocol (İnternet Protokolü)
IV	: Initialization Vector (Başlangıç Vektörü)
KRACK	: Key Reinstallation Attack (Anahtar Yeniden Kurulum Saldırısı)
LLC	: Logical Link Control (Mantıksal Bağlantı Kontrolü)
MAC	: Media Access Control (Ortam Erişim Kontrolü)
MB	: Megabyte
Mbps	: Megabit per second
MHz	: Megahertz
OSI	: Open Systems Interconnection (Açık Sistem Bağlantısı)
OSINT	: Open Source Intelligence (Açık Kaynak İstihbaratı)
PHP	: Hypertext Preprocessor (Hipermetin Önişlemcisi)
PRNG	: Pseudo Ramdom Number Generator (Soyut Rastgele Sayı Üreteci)
RC4	: Rivest Cipher 4 Algoritması
SSID	: Service Set Identifier (Hizmet Seti Tanımlayıcı)
TKIP	: Temporal Key Integrity Protocol (Geçici Anahtar Bütünlüğü Protokolü)
VsCode	: Visual Studio Code (Görsel Studio Kodu)
WEP	: Wired Equivalent Privacy (Kabloluya Eşdeğer Gizlilik)
Wi-Fi	: Wireless Fidelity (Kablosuz Bağlantı)
WLAN	: Wireless Local Area Network (Kablosuz Yerel Alan Ağı)
WPA	: Wi-Fi Protected Access (Wi-Fi Korumalı Erişim)
XML	: Extensible Markup Language (Genişletilebilir İşaretleme Dili)
XOR	: Exclusive OR (Özel Veya)

1. GİRİŞ

Günümüzde kablosuz ağların kullanımı hızla artmaktadır ve bu ağlar, evlerden ofislere, kampüslerden havaalanlarına kadar her yerde yaygın olarak kullanılmaktadır. Şekil 1.1'de örnek bir kablosuz ağ donanımı görülmektedir. Wi-Fi teknolojileri kullanıcılara sunduğu bu deneyimin yanında, 4 milyar satış hacmiyle (Anonymous, 2021) beraber 2023 yılında tahmini olarak 13.1 milyar cihaza yayılan etki alanıyla dünya internet trafiğinin yarısından fazlasını taşımaktadır (Anonymous, 2020).

Şekil 1.1. Kablosuz ağ donanımı.

Kablosuz teknolojilerle paralel olarak yeteneklerini arttıran ağ teknolojileri, neredeyse dünyadaki tüm ağ noktalarının birbirleriyle iletişim kurabileceği kompakt bir ağ modeline sahiptir. Bu kompakt ağ modeli, siber saldırıların neden olacağı potansiyel hasarı gün geçtikçe daha yıkıcı ve tolere etmesi zor hale getirmektedir. Kablosuz ağların dünya internet trafiğin önemli bir kısmını taşıdığı düşünülünce, kablosuz ağlarda siber güvenliğin önemi iyice artmaktadır (Yüksel, 2021). Çünkü bu ağlar güvenlik açıklarıyla karşı karşıyadır (Taş ve ark, 2021). Kablosuz ağlara bağlı cihazlar, ağdan düşürme saldırıları gibi daha birçok saldırı türüne maruz kalabilirler, bu durumda kablosuz ağa erişim engellenebilir ve ardından veri güvenliğinin aşılması söz konusu olabilir (Yüksel,

2021). Literatürde Kali Linux işletim sistemi kullanılarak ağdan düşürme saldırılarıyla alakalı çalışmalar bulunmaktadır. Bu çalışmalar kullanılan akıllı cihazlar, beyaz eşyalar hatta otomobiller bile olabilmektedir.

Örneğin Android temelli araç içi multimedya sistemlerindeki güvenlik zafiyetlerinin tespiti amacıyla otomobil içerisindeki multimedya cihazı üzerinde sızma testleri yapılabilir. Sızma testleri linux çekirdeğine sahip Debian tabanlı Kali işletim sistemi kullanılarak gerçekleştirilmiştir. Sisteme önce ağdan düşürme saldırısı gerçekleştirilerek bağlantısı sonlandırılmaya çalışılmıştır. Sonrasında ise kablosuz ağ üzerinden sızma işlemi gerçekleştirilerek zafiyetlerin nasıl tespit ve istismar edilebildiği somut bir araç üzerinde doğrulanmıştır (Kancura, 2022).

Bu çalışmaların yanında, eğitim ve test amaçlı çok sayıda açık kaynak kodlu araç ve yazılımla desteklenen çalışmalar da bulunmaktadır (Kancura, 2022). Ancak yapılan çalışmaların derlenmesi sonucunda kablosuz ağ güvenliği konusunda gelişime açık alanlar olduğu görülmüştür.

Anlatılan bilgiler doğrultusunda tez çalışması beş ana bölüme ayrılmıştır. İlk bölümde kablosuz ağlar ve güvenliği konusunda temel kavramlar ayrıntılı olarak açıklanmıştır. Ayrıca kablosuz ağların çalışma prensibi, önemli ağ paketleri ve yapıları gösterilmektedir.

Tezin ikinci bölümü kablosuz ağlarda ağdan düşürme saldırılarını konu almaktadır. Ağdan düşürme saldırılarının temel sebebi ve saldırıda kullanılan araçlar anlatılmış, ardından örnek saldırı senaryosu ile saldırı ve sonuçları gösterilmiştir.

Tezin üçüncü bölümü kablosuz ağlarda ağdan düşürme saldırılarında sinyal temelli anomali tespit algoritması oluşturulmuş ve saldırı tespit yazılımı geliştirilmiştir.

Tezin dördüncü bölümünde araştırma sonuçları ve senaryo aşamalarından bahsedilmektedir. Materyal ve yöntemleri açıklanan sistemler kullanılarak bir deney ortamı kurulmuştur. Deney ortamı kurulurken kullanılan sistemlerdeki donanım ve yazılım araştırmaları, kurulumları, denemeleri ve uygulamaları yapılmıştır.

Tezin beşinci bölümünde ise yapılan çalışmanın sonuç ve önerilerinden bahsedilmektedir. Sonuç olarak kablosuz ağlara yönelik gerçekleştirilen ağdan düşürme saldırılarını tespit etmesi için geliştirilen yazılım günün farklı zamanlarında aynı anda 10 adete kadar erişim noktasının aktif olduğu ev ortamında denenmiş ve saldırının ardından 0,5-2 saniye arasında bir algılama süresiyle sesli ve yazılı ikaz vererek ağ güvenliğini sağlamıştır.

1.1. Tezin Amacı

Yapılan literatür taramaları sonucunda ağdan düşürme saldırılarının anlatıldığı görülmüş, ancak aynı veya benzer saldırı türüne yönelik bir yazılım geliştirilmediği gözlemlenmiştir. Bu tez çalışması kablosuz ağlarda bulunan ağdan düşürme saldırılarının tanımlanması ve önlenmesi amacıyla bir yazılım geliştirmeyi hedeflemektedir. Kablosuz ağlar, günümüzün bilgi iletişiminde kritik bir rol oynamaktadır. Ancak, bu ağlara yönelik güvenlik tehditleri de giderek artmaktadır. Bu tez çalışması, kablosuz ağ güvenliği alanında bir açığı ele alarak, ağdan düşürme saldırılarını tespit etme ve engelleme konularına odaklanmaktadır.

Geliştirilen yazılımda, kablosuz ağ trafiğini analiz etmek için çeşitli teknikler kullanılmış ve ağdan düşürme saldırılarına karşı etkili savunma mekanizmaları oluşturulmuştur. Bu mekanizmalar, ağdaki anormallikleri izlemek, saldırı işaretlerini tanımlamak ve hızla müdahale etmek için tasarlanmıştır. Kullanıcıların ağdaki potansiyel tehditlere karşı daha iyi korunmalarını sağlamak için geliştirilen yazılım ağdan düşürme saldırılarının tespit edilmesi durumunda kullanıcılara anında bildirimlerde bulunarak saldırının fark edilmesini sağlamaktadır.

Bu tez çalışması, kablosuz ağların güvenliğini artırmak ve ağdan düşürme saldırılarına karşı daha etkili bir koruma sağlamak amacıyla kablosuz ağ güvenliği alanında önemli bir katkı sunmayı amaçlamaktadır. Kablosuz ağ güvenliği alanındaki bu gelişme, endüstriyel ve kişisel kullanımlar için kablosuz iletişimdeki güvenilirliği artırarak bilgi güvenliği risklerini azaltmaktadır. Ayrıca, kablosuz ağlarda kullanılan diğer güvenlik açıklarının tespit edilmesi ve önlenmesi konusunda da örnek teşkil edebileceği düşünülmektedir. Bu tez çalışması, kablosuz ağ güvenliği konusunda yapılan araştırmalara da katkı sağlayarak bu alandaki bilgi birikimini de artırmayı hedeflemektedir.

2. KAYNAK ARAŞTIRMASI

Yüksel, 2021 yılında yaptığı tez çalışmasında, kablosuz teknolojilerin kullanımın artmasıyla beraber konumlandırıldıkları ağlarda siber saldırılara maruz kalma riskleri ve bu risklerin potansiyel etkilerinin arttığından bahsederek potansiyel saldırı senaryolarını ve ilgili korunma yaklaşımlarını ele almıştır. Ayrıca kablosuz örgü ağlarında tanımlı sahte kimlik doğrulama, yol saptırma ve karadelik saldırıları özelinde oluşturulmuş yazılım mimarisi kullanmıştır.

Gezgin ve Buluş, 2012 yılında yayımladıkları makalede, kablosuz ağlarda kullanılmaya başlanılan ve ağ protokollerinin temelinde yatan açıklardan faydalanarak gerçekleştirilen en önemli saldırı çeşitlerinden biri olan DoS saldırılarını incelemişlerdir. Ayrıca Kabloluya Eşdeğer Gizlilik (WEP) ve Wi-Fi Korumalı Erişim (WPA), MAC adres filtreleme gibi WPA2 öncesi güvenlik standartları saldırılara karşı zayıf kaldığından saldırıları engellemek için AES algoritması kullanan WPA2 şifrelemesi kullanılmaya başlanıldığından bahsetmiştir.

Kancura, 2022 yılında yaptığı tez çalışmasında, Android temelli araç içi multimedya sistemlerindeki güvenlik zafiyetlerinin tespiti amacıyla otomobil içerisindeki multimedya cihazı üzerinde sızma testleri yapmıştır. Sızma testleri linux çekirdeğine sahip Debian tabanlı Kali işletim sistemi kullanılarak gerçekleştirilmiştir. Sisteme kablosuz ağ üzerinden sızma işlemi gerçekleştirilerek zafiyetlerin nasıl tespit ve istismar edilebildiği somut bir araç üzerinde doğrulanmıştır.

Sontowski, 2022 yılında yaptığı tez çalışmasında, çeşitli siber fiziksel sistemlere DoS saldırıları gerçekleştirerek mevcut zayıflıkları ortaya çıkarmayı amaçlamıştır.

Taş ve Kiani, 2021 yılında yayımladıkları makalede, nesnelerin interneti (IoT) cihazlarının güvenliğini tehdit eden saldırıları inceleyerek ağ katmanlarına göre detaylı şekilde sınıflandırılmış ve savunma tekniklerini önermişlerdir.

Kösem, 2016 yılında yaptığı tez çalışmasında kablosuz ağ standartlarını karşılaştırmıştır. Ayrıca tezde, 802.1x standardı ile kablosuz ağ güvenliği tasarımı gerçekleştirmiştir.

Altınok, 2017 yılında yayımladığı bir kitapta, kablosuz ağlar ve bu ağlara bağlı cihazlara yapılabilecek saldırıları, kablosuz ağlarda alınan güvenlik önlemlerini ve bu önlemlerin saldırganlar tarafından nasıl atlatılabileceğini incelemiştir.

Anıl, 2020 yılında online olarak yaptığı çalışmasında ağdan düşürme saldırı çeşitlerinden, saldırıların hangi amaçlarla yapıldığından ve bu saldırılara karşı korunma yöntemlerinden bahsetmiştir.

Ozztech Bilgi Güvenliği ve Yazılım Limited Şirketi, 2021 yılında yaptıkları çalışmada ağdan düşürme saldırı çeşitlerinden, saldırıların nasıl ve hangi amaçlarla yapıldığından ve bu saldırılara karşı korunma yöntemlerinden bahsetmiştir.

Söğüt ve Erdem, 2020 endüstriyel kontrol sistem (SCADA) protokolüne yönelik Command Injection, Reconnaissance and DoS (Denial of Service) yöntemleri içine alan farklı sınıflarda ataklar gerçekleştirerek atak uygulanan sistem ile uygulanmayan sistemlerin davranışlarının incelenmesi ve değerlendirmesini sağlamışlardır. Amaçları siber terör atak davranışlarını tespit edilmesini kolaylaştırmaya çalışmaktır. Veriler analiz için hazırlama da sınıflandırma, regresyon, kümeleme, birleşme kuralları madenciliği yöntemlerinden faydalanılmıştır. Atakların tespitinde Decision Stump, Hoeffding Tree, J48, Rastgele orman (Random Forest) ve REP Tree karar ağaçları algoritmaları kullanılmıştır.

Angin, 2020, bir askeri otonom ağ sistemine yönlendirilen veri bütünlüğünü bozma, ortadaki adam saldırısı (man-in-the middle), kimlik denetimini yanıltma, gizli mesaj saldırılarının blokzincir tabanlı bir iletişim mimarisi ile tespiti ve engellenmesi üzerine bir çalışma gerçekleştirmiştir. Önerilen iletişim mimarisinin veri bütünlüğü bozma ve kimlik denetimini yanıltma saldırılarına karşı koruma sağladığı gözlemlenmiştir.

3. MATERYAL VE YÖNTEM

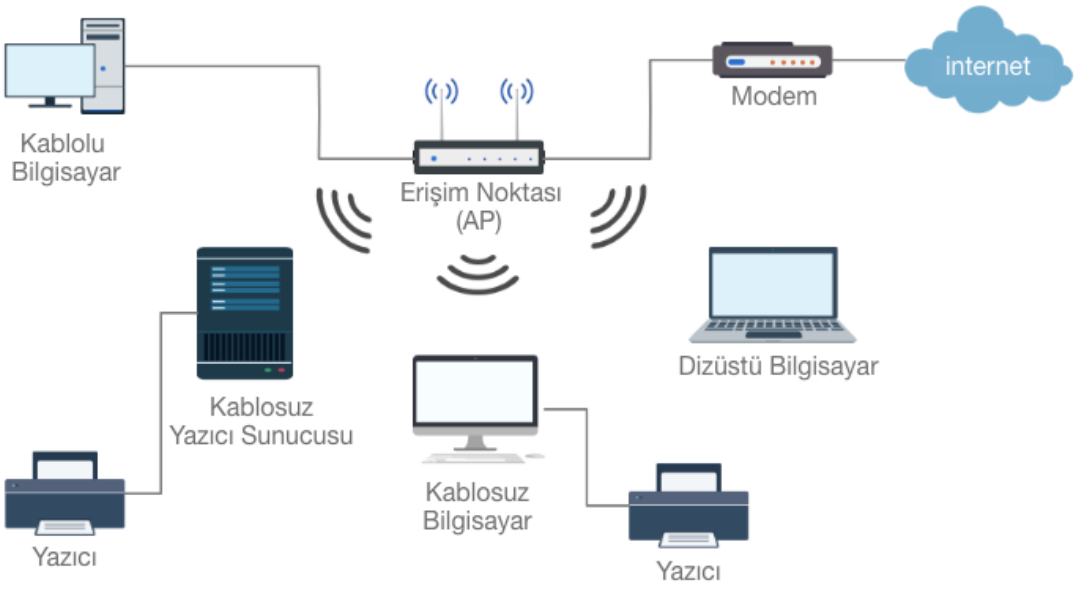
3.1. Kablosuz Ağlar

Kablosuz ağlar sağladıkları avantajlar bakımından kısa zamanda yaygınlaşmıştır. Kablosuz bir iletişim sağladığı için taşınabilir cihazlarda bu şekilde rahatça kullanılmaya başlanmıştır. Kullanımın bu derece yaygınlaşması ile beraber insanlara hizmet veren kafe gibi ortamlarda ücretsiz internet hizmeti sağlamaya başladılar. Bu sayede saldırganlar hedefledikleri kullanıcılar ile aynı ağda olmaya başladılar (Altınok, 2017). Ancak riskler, kablosuz ağların ayrılmaz bir parçasıdır. Bu risklerden bazısı kablolu ağlardaki risklerle aynıdır, bazısı da yenidir. Kablosuz ağlarda riskin kaynağı iletim ortamının hava olmasıdır. Yetkili olmayan kullanıcıların sisteme ve bilgilere girmesi, sistem bilgilerinin bozulmasına, ağ bant genişliğinin azalmasına, ağ performansının düşmesine neden olmaktadır (Erkınay, 2005). Bu nedenle kablosuz ağların güvenliği büyük önem taşımaktadır.

3.1.1 Temel kavramlar

3.1.1.1 AP (Access Point)

Erişim noktası olarak tanımlanabilir. Kablolu ağları kablosuz ağlara çevirmek için kullanılan veya kablosuz ağları daha uzak mesafelerden bağlantı kurulabilmesi için etki alanını genişleten donanımlardır. Şekil 3.1’de bir erişim noktasının istemci cihazlarla iletişimi görülmektedir.



Şekil 3.1. Erişim noktası ve istemci cihazlarla iletişimi.

Bu donanımlar genellikle 2.4 GHz veya 5 GHz bant genişliğinde çalışmaktadır (Kösem, 2016). Çok daha uzak mesafelere ve yüksek bant genişliğinde internet bağlantısı sağlamak için çeşitli türleri bulunmaktadır.

3.1.1.2 SSID

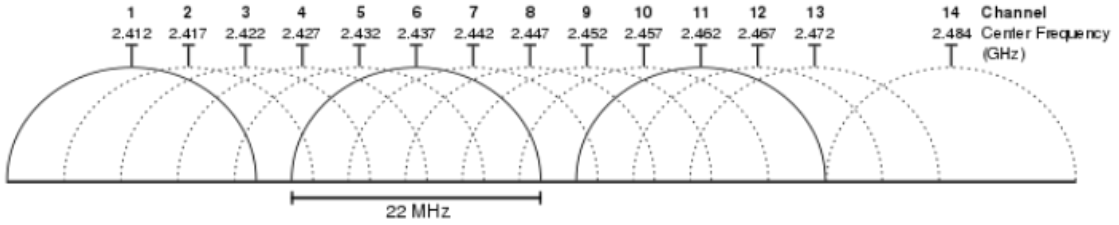
Hizmet Kümesi Tanımlayıcı (SSID), kısaca kablosuz ağların adıdır. Ağ kimliği anlamına da gelen SSID, tüm cihazların görüntüleyebileceği adlardır. "TP-Link_E45TWS" ve "cufcuf_0606" gibi isimler SSID yani kablosuz ağ adlarına örnektir.

Kablosuz ağlarda ağın güvenliğini sağlamak amacıyla SSID gizlenebilmektedir (Altınok, 2017). Örneğin IP kameralar, IoT cihazlar ve bazı kablosuz ağ kullanan donanımlar için güvenlik amaçlı SSID bilgileri gizlenerek meraklı gözlerden uzak tutulabilir. Bu durumda SSID bilgisi gizli olan ağlar Wi-Fi alıcısının listesinde görünmezler. Bu ağlara bağlanmak için SSID ve diğer bağlantı bilgileri (şifreleme türü, ağ şifresi vb.) manuel olarak girilerek bağlantı kurulabilmektedir.

SSID gizlemek tam bir koruma sağlamamaktadır. Adı gizli olan ağa bağlantı kuran cihazların tekrardan bağlantı isteği yapması halinde kötü niyetli kişiler tarafından bu istek paketi elektromanyetik olarak kopyalanabilir ve içerisindeki ağ adı bilgisi ifşa edilebilmektedir (Akbaş, 2015).

3.1.1.3 Kablosuz ağlarda kanal numaraları

Wi-Fi ağlarında kablosuz iletişimde kullanılan radyo frekans bantlarına bölünmüş kanallar bulunmaktadır. Bu kanallar kablosuz ağların yayın esnasında birbirleri ile çakışmaması ve daha iyi performans alınması için kullanılmaktadır. Kanal numaraları Şekil 3.2'de detaylı olarak görülmektedir.



Şekil 3.2. Kablosuz ağ kanal numaraları.

Kanal numarası, 1-14 arasındaki değerler ile tanımlanır. Erişim noktalarının birbirine yakın kanal numaralarında çalışmaları bazı problemleri de meydana getirebilmektedir. Bu nedenle her kanal arasında 5 MHz'lik bir aralık bulunmaktadır. (Altınok, 2017). Her erişim noktası sadece bir kanalda çalışabilir ve bağlantı kurulabilmesi için istemci ile erişim noktasının aynı kanalda bulunması gerekir (Kancura, 2022). Çizelge 3.1'de kanal numaraları ve hangi ülkelerde kullanıldıkları verilmiştir.

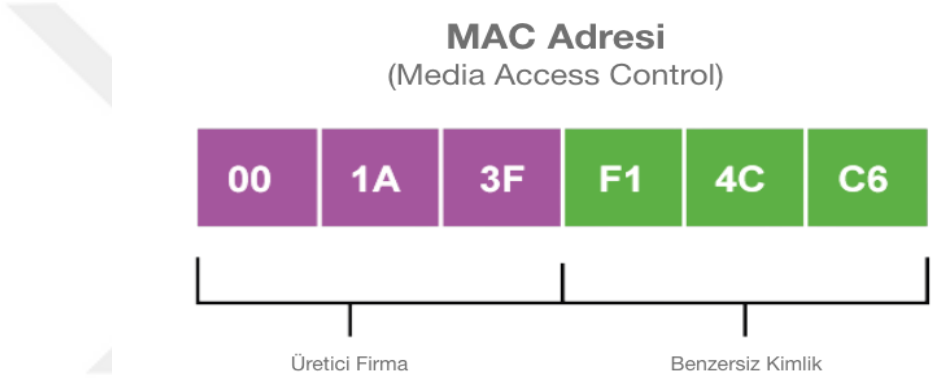
Çizelge 3.1. Kanal numaraları ve kullanıldıkları ülkeler (Altınok, 2017).

Kanal Numarası	Frekans (MHz)	Kuzey Amerika	Japonya	Diğer Ülkeler
1	2412	✓	✓	✓
2	2417	✓	✓	✓
3	2422	✓	✓	✓
4	2427	✓	✓	✓
5	2432	✓	✓	✓
6	2437	✓	✓	✓
7	2442	✓	✓	✓
8	2447	✓	✓	✓
9	2452	✓	✓	✓
10	2457	✓	✓	✓
11	2462	✓	✓	✓
12	2467	X	✓	✓
13	2472	X	✓	✓
14	2484	X	Sadece 802.11b standartları	X

3.1.1.4 MAC adresi

Ortam Erişim Kontrolü (MAC) adresi kablolu ve kablosuz ağ donanımlarının benzersiz kimliğidir. MAC adresi, ağ donanımını üreten firma tarafından oluşturulur ve her ağ cihazı için benzersizdir. Bu adresler yerel ağlarda ağ güvenliği ve yönetimi için kullanılmaktadır.

MAC adresleri 6 byte uzunluğundadır ve iki haneli onaltılık (hexadecimal) sayılarla ifade edilmektedir. İlk 3 byte ağ kartının üreticisini temsil eder ve son 3 byte ise üretici firma tarafından ağ kartına atanan benzersiz kimliktir. Genellikle iki nokta üst üste (:) veya tire (-) işaretiyle ayrılmış olarak yazılır (Altınok, 2017). Şekil 3.3'de MAC adresinin yapısı görülmektedir.



Şekil 3.3. MAC adresi yapısı.

MAC adresleri ağ kartındaki çiplerde bulunurlar ve değiştirilemezler. Ancak bazı yazılımlar ile ağ kartından alınan veriler kötü niyetli kişiler tarafından işletim sistemine farklı gösterilebilir ve kablosuz ağlardaki MAC adresine dayalı güvenlik önlemleri atlatılabilir (Akbaş, 2015).

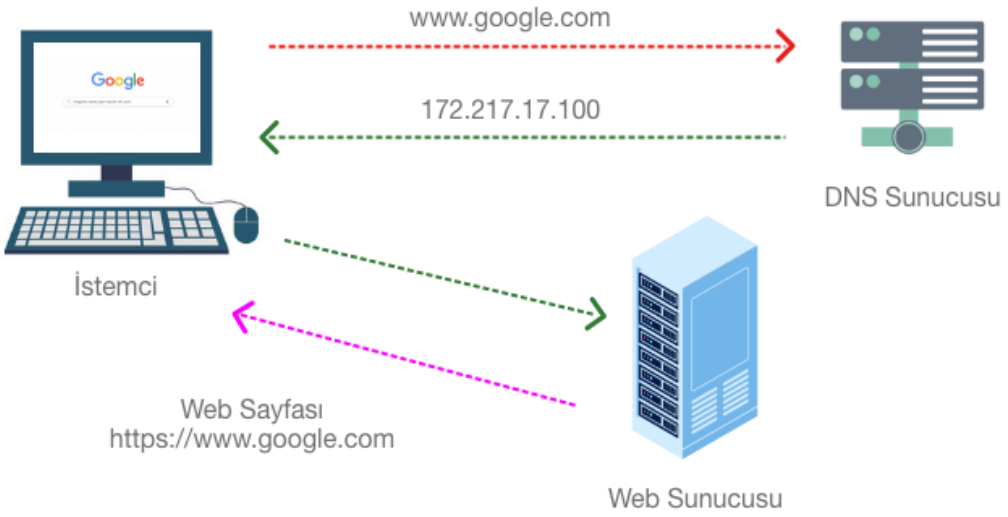
3.1.1.5 BSSID

Temel Hizmet Seti Tanımlayıcı (BSSID) MAC adresi formatında ifade edilir ve her kablosuz erişim noktasının benzersiz donanım kimliğini temsil eder. BSSID, kablosuz ağlarda tanımlama ve yönlendirme için kullanılır (Altınok, 2017).

3.1.1.6 DNS

Alan Adı Sistemi (DNS), WEB sunucuya domain ismiyle erişebilmek için kullanılan bir sistemdir. TCP/IP uygulamaları tarafından bilgisayar isimlerini IP

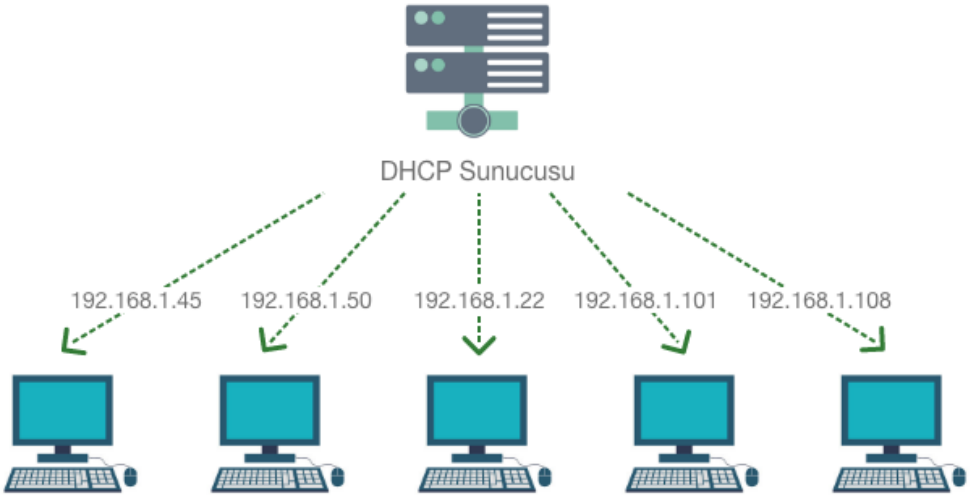
adreslerine eşleyen, erişim için yol bilgisini sağlayan bir veri tabanıdır. Bir TCP/IP networkündeki tüm bilgisayarlar IP adresleriyle tanımlanır. Fakat IP adreslerini hatırlamak kullanıcılar açısından zor olacağından, IP adreslerini kolay anlaşılan isimlere dönüştürmek için DNS'ten yararlanılır (Anonim, 2009). Şekil 3.4'te DNS'in yapısı görülmektedir.



Şekil 3.4. DNS'in yapısı.

3.1.1.7 DHCP

Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP), ağ üzerinde istemci/sunucu (client/server) mimarisi ile çalışır. Bu sebepten dolayı ağ ortamında DHCP hizmetinin verilebilmesi için bir sunucu bileşenine ve bir de istemci bileşenine ihtiyaç vardır. Dinamik IP adresi ve yapılandırması kullanan bir bilgisayara DHCP istemcisi denir. DHCP sunucusu, IP adresleri ve ilgili yapılandırma bilgileri hakkında bir veri tabanı oluşturma işinden sorumludur. İstemci DHCP sunucudan bir IP adresi aldığında, atanan IP adresini kiraladığı söylenebilir. Kira deyimi, bu atama işlemi kalıcı olmadığı için kullanılmaktadır. Bir bilgisayarın DHCP istemcisi olarak çalışması için otomatik IP alacak şekilde ayarlanması gerekir (Anonim, 2014). Şekil 3.5'te DHCP'nin yapısı görülmektedir.



Şekil 3.5. DHCP'nin yapısı.

3.1.2 Kablosuz ağ çalışma modları

3.1.2.1 Client ve master mode

Wi-Fi ağ kartları, temelde istemci modu (client) ve erişim noktası modu (master mode) olarak çalışırlar. Master modda çalışan bir kablosuz ağ kartı erişim noktası veya yönlendirici olarak hareket eder (Altınok, 2017). Master modda çalışan bir kablosuz ağ kartı kablosuz ağlar oluşturulmasında kullanılır. Client modda çalışan bir kablosuz ağ kartı ise bu ağlara bağlanmak için kullanılır.

3.1.2.2 Manage mode

Yönetim Modu (Manage Mode), kablosuz ağ kartlarının yapılandırılması için kullanılır. SSID, şifreleme yöntemleri, kanal seçimi ve diğer ayarları uygulamak için kullanılır (Altınok, 2017).

3.1.2.3 Monitor mode

İzleme Modu (Monitor Mode), bir kablosuz ağda verileri izlemek, kaydetmek ve ağ sorunlarını çözmek için kullanılır. Bu mod ağ sorunlarının çözülmesi için oluşturulmuş olsa da Wi-Fi iletişim yapısında kullanılmadığı için her kablosuz ağ kartında bulunmaz.

Bu mod, bir erişim noktasına bağlı olmadan havada başı boş gezinen ağ paketlerini dinleyebilme ve manipüle etme olanağı sağlar (Altınok, 2017). Öte yandan

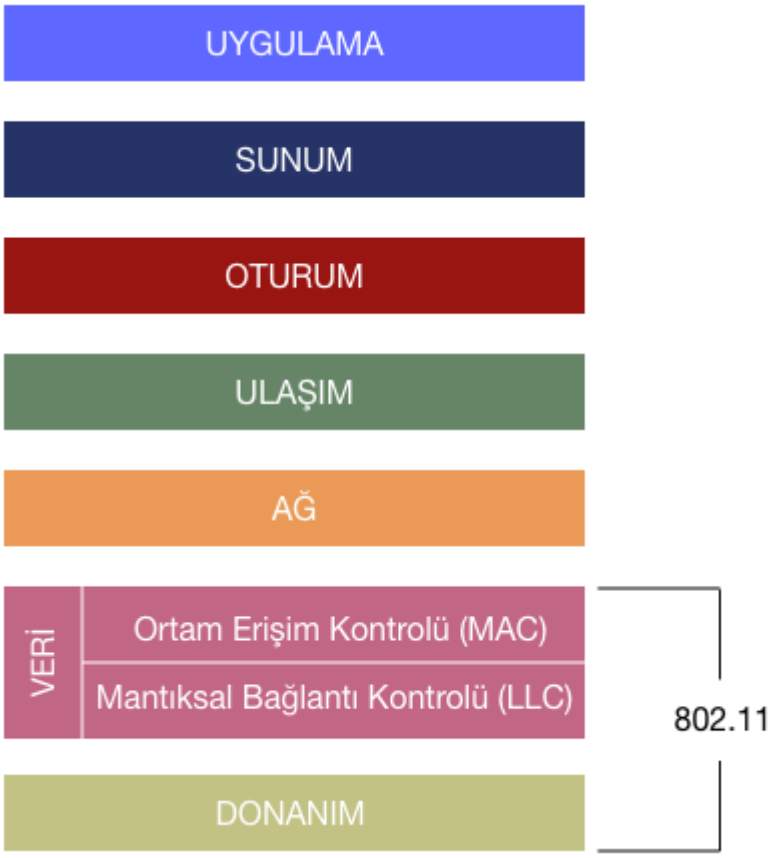
kötü niyetli kişiler, monitör mod destekli kablosuz ağ kartları kullanarak erişim noktaları hakkında bilgi edinebilir ve ağa sızma girişiminde bulunabilirler. Her ne kadar ağ sorunlarını çözmeye yardımcı olsa da güvenlik konusunda sorun oluşturması nedeniyle günümüzde piyasaya sunulan yeni nesil kablosuz ağ kartlarında monitör mod desteği bulunmamaktadır.

3.1.2.4 Promiscuous mode

Gözetim Modu (Promiscuous Mode), ağdaki tüm paketlerin dinlemesini sağlayan bir işletim modudur. Bu modun çalışabilmesi için ağa dahil olunması gerekir ve sadece bağlı olunan ağdaki cihazların paketleri dinlenebilir. Gözetim modu ile monitör mod arasındaki fark bu modda ağa dâhil olunması gerekmektedir.

3.1.3 Kablosuz ağ standartları

Kablosuz ağ standartları, farklı cihazların kablosuz iletişim kurması için belirlenmiş teknik protokollerdir. Bu standartlar, belirli frekans bantları üzerinde iletişim kurmak için kullanılan protokoller, veri aktarım hızları, güvenlik özellikleri ve diğer iletişim parametrelerini tanımlamaktadır. Ağ kavramının ortaya çıkmasıyla beraber daha çok bilgisayar donanımı üreten firmalar tarafından birçok protokol geliştirilmiştir. Fakat bu protokoller bir standarda göre değil, üreticinin kendi ürettiği ürüne uygun olarak geliştirilmiştir. Bu durumda farklı üreticiler tarafından üretilen donanımlar arasında iletişim sorunu yani beraber çalışamama sorununu ortaya çıkmıştır. Bu sebeple ISO (International Organization for Standardization/Uluslararası Standartlar Örgütü) tarafından donanım ve ağ altyapısı bağımsız olarak geliştirilen OSI modeli ortaya konulmuştur. Şekil 3.6’da OSI referans modeli ve katmanları görülmektedir.



Şekil 3.6. OSI referans modeli.

Veri katmanı, iki alt katmana ayrılmıştır. Bu iki katman veri iletimini düzenler ve üst katman cihazlarının (bilgisayar, mobil cihazlar, sunucular vb.) farklı ağ tipleriyle uyumlu olmalarını sağlar. Örneğin, bir bilgisayarın internete kablolu veya kablosuz bağlantı üzerinden erişebilmesi için aynı mantıksal arabirimi kullanması gerekir. Sonuç olarak OSI referans modelinde ağ cihazları farklı ağ tiplerinde çalışabilir ve iletişim kurabilirler.

802.11, 1997 yılında IEEE tarafından kablosuz ağlar için geliştirilmiş bir standarttır. İlk geliştirilen standart olan 802.11, 2.4 GHz frekansında, saniyede 1 MB veya 2 MB veri transferine izin vermektedir. Bu standardın fiziksel katmanda, Frekans Atlama Yayılma Spektrumu (FHSS) ve Direkt Sıralı Yayılı Spektrum (DSSS) olmak üzere kullandığı iki farklı modülasyon yöntemi bulunmaktadır. FHSS ile elverişli ortamlarda 2 Mbps, sinyal gürültüsü olan ortamlarda ise DSSS ile 1 Mbps veri iletim hızlarına ulaşılabilmektedir. Günümüzde 802.11a, 802.11b, 802.11g ve 802.11n standartları kullanılmaktadır (Abdulkareem, 2012).

3.1.3.1 IEEE 802.11a standardı

802.11 standardının gelişen teknoloji ile belirli özellikleri karşılayamamaya başlamış ve 1999 yılında IEEE 802.1a Sürümü yayınlanmıştır. Bu standart temeli 802.11 olmasına karşın yayın bandını 5 GHz frekansında çalıştırmaktadır ve 54 Mbps gibi bir veri iletim hızına ulaşılmış bu standart, açık alanlarda ise 100 metreye kadar kapsama desteğinde bulunmaktadır (Kösem, 2016).

3.1.3.2 IEEE 802.11b standardı

802.11b standardı 802.11a ile birlikte 1999 yılında yayınlanmıştır. 802.11b, 802.11 gibi 2.4 GHz frekans bandında çalışmakta ve 11 Mbps veri iletimi hızına ulaşabilmektedir. İlk yayına girdiği sürede sağladığı veri hızı ve 2.4 GHz'de yayın yapabilmesi nedeni ile kablolu ağ teknolojilerine rakip hale gelmiş ve kablosuz ağ kullanımının yaygınlaşmasında büyük rol oynamıştır (Kösem, 2016).

3.1.3.3 IEEE 802.11g standardı

Kablosuz ağ kullanımının yaygınlaşmaya başlaması ile 2003 yılında IEEE tarafından kablosuz ağ standartlarında geliştirilen 3. nesil teknoloji ve 2.4 GHz frekansında çalışmaktadır (Kösem, 2016).

Video uygulamalarında hızı ve kapsadığı alan genişliği nedeniyle tercih edilmektedir. Ayrıca 802.11b ile çalışan cihazlarla uyum sorunu bulunmaktadır (Abdulkareem, 2012).

3.1.4 Kablosuz ağlarda güvenlik anahtarı

Kablolu bir ağda, kullanıcı yetkilendirmesinin ilk yolu ağa giriş yapabilmeleri için fiziksel engeller uygulamaktır. Fiziksel engeller, sinyalleri bir binanın duvarlarının ötesine taşıyan kablosuz ağlar için uygun değildir (Abdulkareem, 2012). Kablosuz ağlardaki güvenlik 802.11 standartlarında belirlenmiştir. 802.11'in ilk güvenlik mekanizması olan Kabloluya Eşdeğer Gizlilik'i (WEP) kırmak oldukça kolaydır (Altınok, 2017). WEP protokolü, 802.11'in orijinal güvenlik mekanizmasıdır. WEP algoritmasının zayıf noktaları sebebiyle, genellikle şifreleme için nadiren tercih edilmektedir. Bu sebeplerden ötürü, Wi-Fi İttifakı, WEP'in yerini alan Wi-Fi Korunaklı Erişim (WPA) adında bir ara güvenlik çözümü geliştirmiştir. Güvenlik anahtarı, yetkisiz

kullanımı önlemek ve kablosuz ağda iletilen verilerin güvenliğini sağlamak için kullanılır.

ASCII, Amerikan Karakter Kodlama Sistemi anlamına gelmektedir. ASCII sisteminde 128 farklı karakter bulunmaktadır. Bu karakterlerden 33 tanesi yazılmaz (denetim karakterleri) ve 95 tanesi yazılabilir (A-Z, a-z, 0-9 ve özel semboller). Bu yazılabilir karakterler, kablosuz ağlarda güçlü ve karmaşık güvenlik anahtarları oluşturmak için tercih edilir (Abdulkareem, 2012).

3.1.4.1 Kabloluya eşdeğer gizlilik (WEP)

Kabloluya Eşdeğer Gizlilik, kablosuz ağlardaki veri gizliliğini sağlamak amacıyla geliştirilmiş bir güvenlik protokolüdür. Bu protokol, 802.11'de bulunan temel güvenlik standartlarından biridir. WEP, verinin kablosuz ağın iletişim hattında taşınırken güvende olmasını sağlamak için geliştirilmiştir.

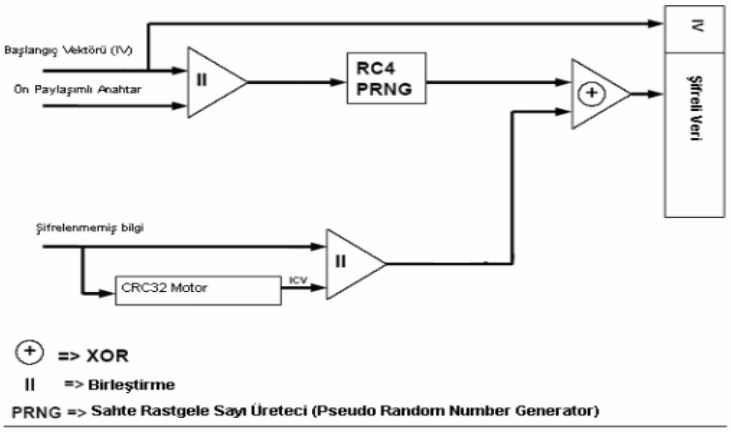
WEP, veri şifreleme işlemi için Ron Rivest tarafından geliştirilen RC4 (Rivest Cipher) şifreleme algoritmasına dayanır. RC4, gizli bir anahtar kullanarak rastgele sayıları üreten bir şifreleme algoritmasıdır. Kabloluya Eşdeğer Gizlilik protokolü, iletilmesi gereken veriyi bu algoritma ile şifrelemektedir. İstemci tarafında da aynı anahtar kullanılarak şifrelenmiş veri çözülür.

Ancak WEP, bazı güvenlik açıkları ve zayıflıkları içerir. Özellikle WEP erişim noktasının ötesindeki güvenliği sağlama konusunda oldukça zayıftır. Yani bilgisayar korsanları havadaki sinyalleri okuyarak WEP'i çözebilir (Altınok, 2017).

WEP algoritmasının çalışma şekli aşağıda listelenmiştir:

1. İletilecek veri, veri bütünlüğünü sağlamak amacıyla bir doğrulama algoritmasından geçirilir. Bu işlem sonucunda doğrulama bitleri (ICV) elde edilir.
2. Elde edilen doğrulama bitleri verinin sonuna eklenir, verinin değişmediğini ve bütünlüğünün korunduğunu garanti eder.
3. 24 bitlik başlatma vektörü (IV), statik anahtarın başına eklenerek 64 bitlik bir paket oluşturulur.
4. 64 bitlik paket, statik anahtar kullanılarak RC4 algoritması ile şifrelenir ve verinin gizliliği korunur.
5. İkinci adımda elde edilen veri ile dördüncü adımda elde edilen veri arasında XOR işlemi uygulanır. Bu, verinin daha fazla güvende olmasını sağlar.

6. Elde edilen verinin başına IV tekrar eklenir ve verinin güvenli bir şekilde iletilmesi için veri erişim noktası ve istemci cihazın MAC adresleri eklenir. Böylece veri iletilmek için hazırdır.
7. İstemci, şifrelenmiş veriyi aynı işlemlerin tersini uygulayarak gerçek veriyi elde eder. Böylece iletim sırasında verinin gizliliği ve bütünlüğü korunmuş olur. Bu şifreleme mekanizması şekil 3.7'de gösterilmiştir.



Şekil 3.7. İletim için WEP şifreleme süreci (Hammand ve ark., 2003).

WEP algoritmasının zayıflıkları aşağıda listelenmiştir.

- WEP algoritması, aynı mesajın defalarca gönderilmesine izin verir ve istemci tarafından dikkate alınmaması için bir mekanizma bulunmaz. Bu durum bilgisayar korsanlarının ağdaki veriyi yetkisiz şekilde ele geçirmesine veya yanıltıcı işlemler yapmalarına olanak sağlar.
- WEP algoritmasında kullanılan ICV, lineer bir yöntemle oluşturulur ve asıl verinin sonuna eklenir. Bilgisayar korsanları bu durumu kullanarak şifrelenmiş veride bit değiştirerek istemciyi yanıltabilir.
- WEP, 24 bitlik IV kullanır. Bu durumda yaklaşık 17 milyon farklı IV oluşturulabilir. 802.11b standardına göre tekrarlanmadan birer artırarak kullanıldığında yaklaşık 7 saate tüm IV'ler kullanılmış olacaktır. Ancak IV'lerin tekrar kullanılması bilgisayar korsanlarının şifreyi kısa bir sürede kırmalarına yol açmaktadır.
- RC4 algoritmasının anahtar üretim algoritması güçlü ve karmaşık anahtarlar üretmez. Bu zayıflık, bilgisayar korsanlarının şifrelenmiş veriden statik anahtarı elde edebilmesine olanak sağlar.

3.1.4.2 Dinamik anahtar değişimi (Dynamic Key Exchange- DKE)

DKE; birçok kuruluşun WEP'deki otomatik anahtarlama yönetiminin eksikliğinin üstesinden gelmek için, kablosuz güvenliği geliştirmek adına ilgilendiği bir çalışmadır. DKE için iki temel olumsuzluk vardır: Birlikte işlerlik yoktur ve bütün uyarlamalar AAA (Authentication, Authorization Accounting) hizmet sağlayıcısı gerektirir. Bunun anlamı; küçük bölgeler ve SOHO (Small Office Home Office) ağlar için bir çözüm sağlamaz. Birlikte çalışabilirliğin önemli olmadığı ve sadece AAA hizmet sağlayıcısının olduğu durumlarda DKE kullanılabilir (Erkınay, 2005).

3.1.4.3 Wi-Fi korumalı erişim (WPA)

Wi-Fi Protected Access (WPA), WEP'in zayıflıklarını gidermek amacıyla 2003 yılında Wi-Fi Alliance tarafından geliştirilmiştir. Wi-Fi Korumalı Erişim, TKIP algoritmasını kullanarak WEP'de var olan şifreleme zayıflıklarını güçlendirir ve şifreleme anahtarlarını otomatik olarak üretmek ve dağıtmak için bir yöntem sunar. Kuruluş düzeyinde kullanıcı kimlik doğrulamasını geliştirmek için, Wi – Fi korumalı erişim ağdaki her kullanıcının kimliğini doğrular ve bu kullanıcıların aldatıcı ağlara katılmalarını engeller. WPA var olan teknolojileri temel alıp, 802.11i ile ileri doğru uyumluluk ve var olan 802.11 çözümleriyle geriye doğru uyumluluk sunarak, WEP ile ilgili zayıflıklara pratik bir çözüm sağlar (Abdulkareem, 2012).

WPA'nın WEP'e göre sağladığı yararlar aşağıda listelenmiştir.

- WEP'den daha iyi güvenlik sağlar.
- Eski kablosuz ağ donanımlarında yazılımsal güncelleme ile kullanılabilir.
- WEP tabanlı istemcilerde karıştırılmış (WEP/WPA) ağ iletişimine izin verir.

3.1.4.4 Geçici anahtar bütünlüğü protokolü (TKIP)

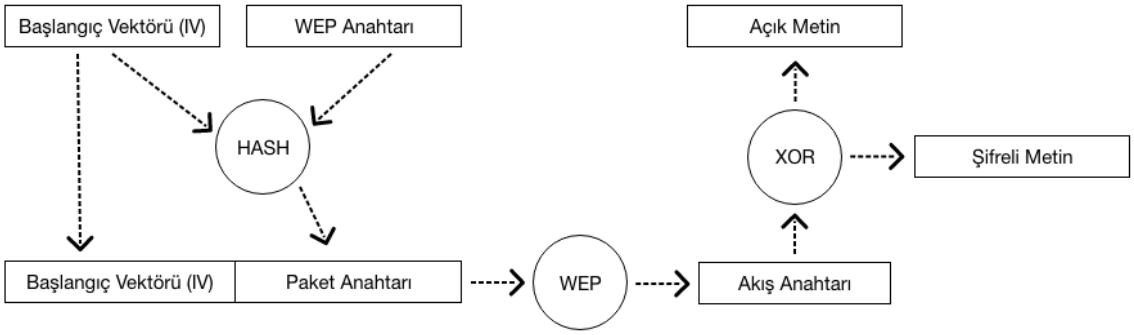
TKIP, WEP'in güvenlik açıklarını gidermek ve mevcut donanımı kullanarak daha güvenli bir şifreleme katmanı oluşturmak amacıyla geliştirilmiştir. TKIP, WEP'in zayıf yönlerini ele alarak ağ güvenliğini artırır. Bu protokol, güvenlik önlemlerini güçlendirme ve kablosuz ağı saldırılara karşı daha dayanıklı hale getirmek için geliştirilmiştir.

TKIP'nin özellikleri aşağıda listelenmiştir.

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

- Anahtarları yenileme mekanizması.

TKIP'de başlangıç vektörü 48 bit'e çıkarılmıştır. Başlangıç vektörü, hem paketlere sıra numarası vermek hem de her paket için tek kullanımlık anahtar üretiminde kullanılır. Paketlere sıra numarası vermek tekrar saldırılarını önlemek içindir. Ayrıca sırasız gelen paketler alıcı tarafından atılmaktadır (Abdulkareem, 2012). Şekil 3.8'de TKIP'nin yapısı gösterilmiştir.



Şekil 3.8. TKIP'nin yapısı.

3.1.4.5 Wi-Fi korumalı erişim 2 (WPA2)

WPA2, WPA ile benzer yöntemler kullanır. Ancak farklı bir şifreleme algoritması kullanarak güvenliği artırır. WPA ile WPA2 arasındaki temel fark şifreleme algoritmasıdır. WPA, RC4 şifreleme algoritmasını kullanırken, WPA2 daha güçlü bir şifreleme algoritması olan Gelişmiş Şifreleme Standardı (AES) kullanır. WPA2, AES şifreleme algoritması ile şifreleme yapar ve günümüzde güçlü ve yüksek güvenlik sağlayan şifreleme algoritması olarak kabul edilir. WPA2, güvenliği sağlamak için CCMP protokolünü kullanır. Bu protokol, verilerin şifrelenmesi ve bütünlüğünün korunması için kullanılır (Altınok, 2017).

3.1.4.6 Gelişmiş şifreleme standardı (AES)

Bu standart; şimdiki Federal Information Processing Standart (FIPS) Şifreleme tanımlaması olan, DES'in (Data Encryption Standart) yerine tasarlanmıştır. AES; şimdiye kadar bilinen bir kusuru olmayan ve bütün şifre çözücülere karşı direnen çok güçlü bir şifreleme algoritmasıdır. (Kula, 2009).

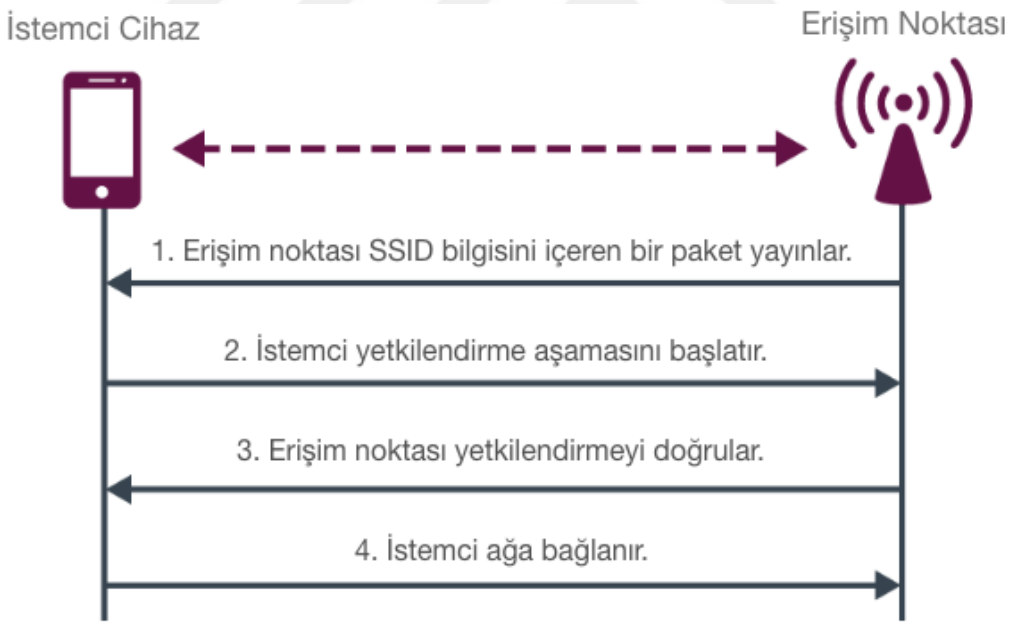
3.1.4.7 Wi-Fi korumalı erişim 3 (WPA3)

WPA3, 2018'de Wi-Fi İttifakı tarafından tanıtılan bir güvenlik standardıdır ve kapalı bir Wi-Fi ağına parola kullanarak bağlandığınızda gerçekleşen süreçleri yönetmek için kullanılır. En son Wi-Fi güvenlik protokolü olan WPA3, kişisel ağlardaki siber güvenliği artırmak için yeni yetenekler sunar. Wi-Fi ağını güvence altına almak amacıyla parolaların daha güvenli bir şekilde şifrelenmesini ve kaba kuvvet saldırılarına karşı artırılmış koruma sağlamaktadır (Anonim, 2024).

3.1.5 Kablosuz ağlarda iletişim ve önemli ağ paketleri

3.1.5.1 İletişim

Kablosuz ağlarda, erişim noktası ve istemci cihaz arasındaki bağlantı 4 aşamada gerçekleşir. Şekil 3.9'da erişim noktası ve istemci cihaz arasındaki bağlantı temsili olarak görülmektedir.



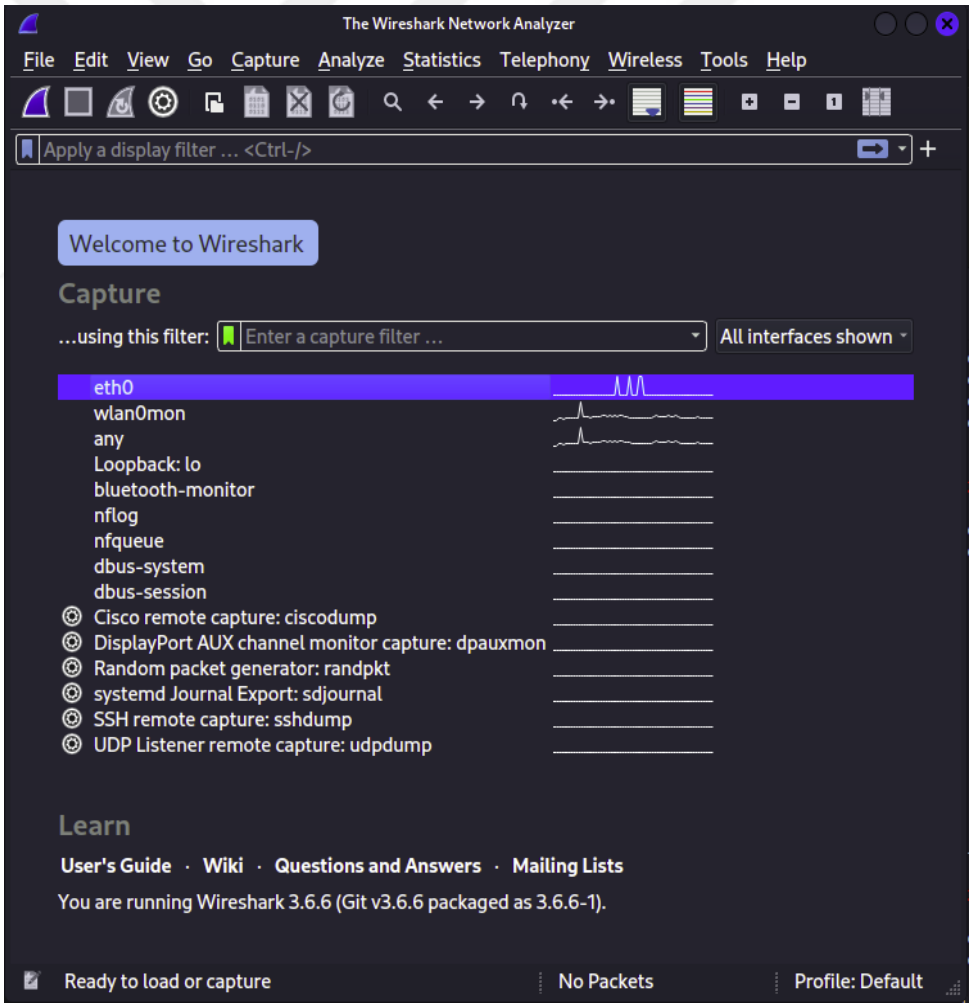
Şekil 3.9. Erişim noktası ve istemci cihaz bağlantısı.

İlk aşamada erişim noktası, Hizmet Seti Tanımlayıcısı (SSID) bilgisini içeren bir paketi yayınlar ve çevredeki istemcilere varlığını gösterir. Bu durum, istemcilerin erişim noktasının varlığını ve adının algılanmasını sağlar. İstemci SSID bilgisinin bulunduğu paketi alarak çevresindeki kablosuz ağları kullanıcıya listeler. İkinci aşamada istemci kablosuz ağlardan birine bağlanmak için yetkilendirme aşamasını başlatır. Bu süreçte

istemci, kablosuz ağda bir güvenlik koruması (WPA/WPA2) varsa erişim noktasının güvenlik anahtarını girmek zorundadır. Üçüncü aşamada erişim noktası, güvenlik anahtarı geçerli ise yetkilendirme aşaması tamamlanmış olur. Ancak güvenlik anahtarı geçersiz ise ikinci aşamaya geri döner. Son aşama olarak erişim noktası yetkilendirme aşamasını tamamlayan istemcilere otomatik veya istemci tarafından talep edilen IP adresi gibi bilgileri iletir ve bağlantı sağlanmış olur (Yüksel, 2021).

3.1.5.2 Wireshark hakkında temel bilgiler

Wireshark ağ trafiğini izlemek, analiz etmek ve kaydetmek için kullanılan açık kaynak ağ analiz yazılımıdır. Genellikle ağ sorunlarını çözmek ve penetrasyon (sızma testi) için kullanılabilir (Sontowski, 2022). Şekil 3.10'da Wireshark yazılımının örnek ekran görüntüsü verilmiştir.



Şekil 3.10. Wireshark ekran görüntüsü.

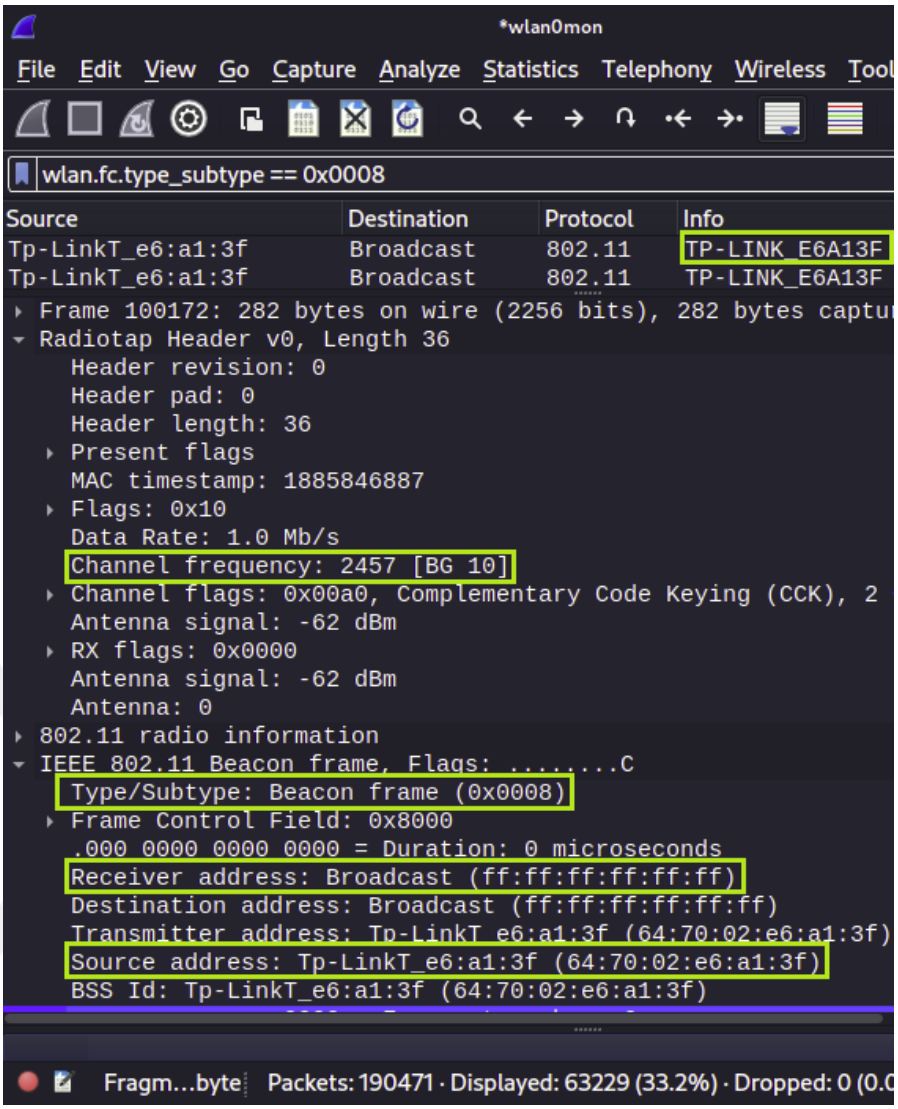
Wireshark yazılımının bazı temel özellikleri aşağıda listelenmiştir (Altınok, 2017):

- Bir ağ arayüzü (ethernet, wlan, bluetooth vb.), üzerinden gelen ve giden ağ trafiğini istenilen formatta kaydedebilir ve içerisinde bulunan çeşitli modüller ile hızlı bir şekilde analiz edebilir.
- Daha önceden kaydedilmiş veya anlık olarak tespit edilen ağ paketlerini özelliklerine göre filtreleyebilir.
- Geniş bir protokol desteğiyle paket analizini gerçekleştirebilir ve ücretsiz kullanılabilir.
- Kullanıcı dostu grafiksel arayüzü ile bir uzmana gerek duymadan analizlerin gerçekleştirilmesine imkân sağlar.

3.1.5.3 Önemli kablosuz ağ paketleri

3.1.5.3.1 Beacon frame

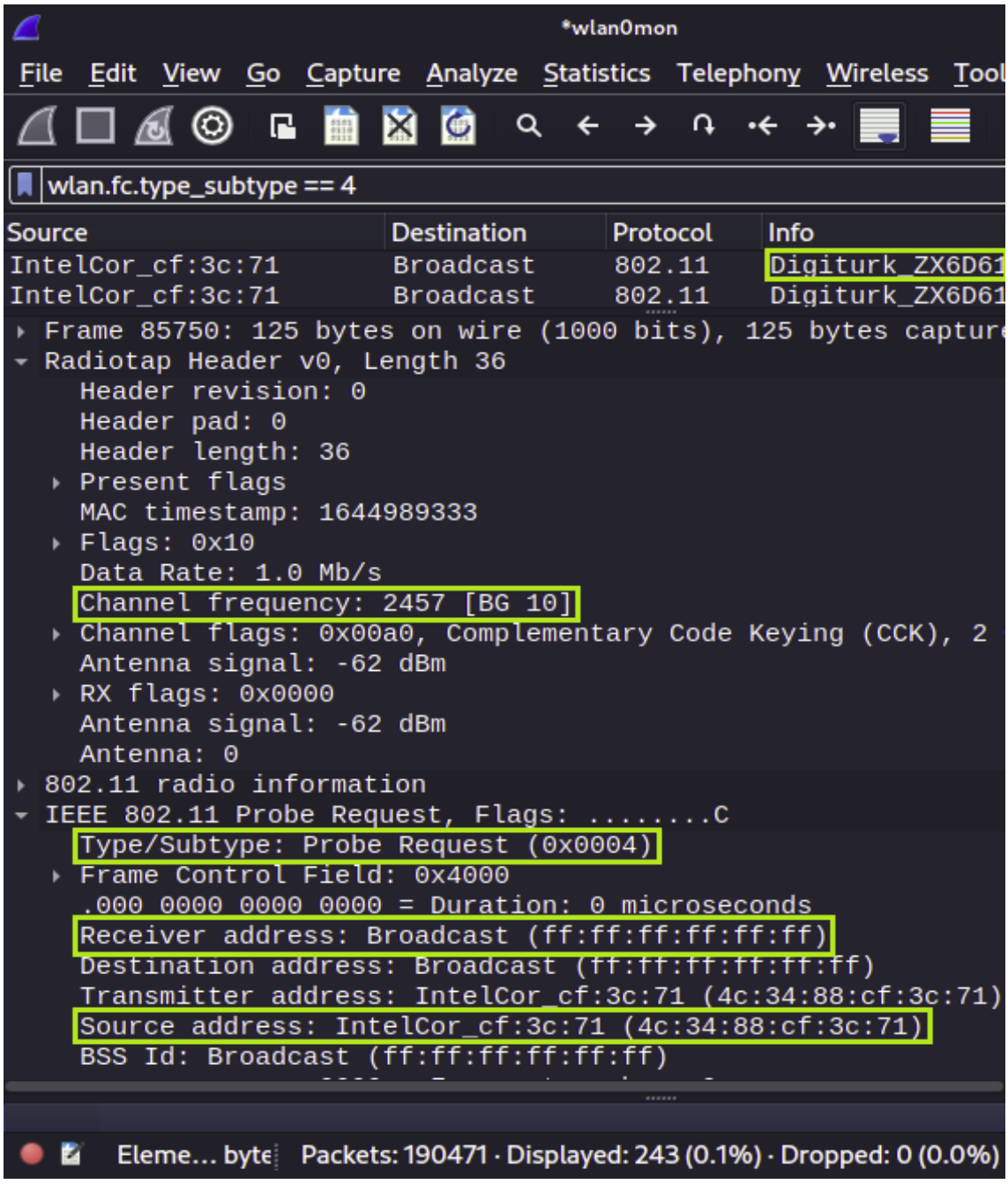
Beacon Frame, içerisinde erişim noktasına ait SSID ve diğer bilgileri (frekans, tip, MAC adresi vb.) barındıran bir kablosuz ağ paketidir. Erişim noktaları sürekli olarak beacon frame yayınlarlar ve böylece istemciler kablosuz ağları görebilirler. Şekil 3.11'de Wireshark programıyla incelenen Beacon Frame paketi görülmektedir.



Şekil 3.11. Wireshark ile incelenen Beacon Frame ekran görüntüsü.

3.1.5.3.2 Probe request

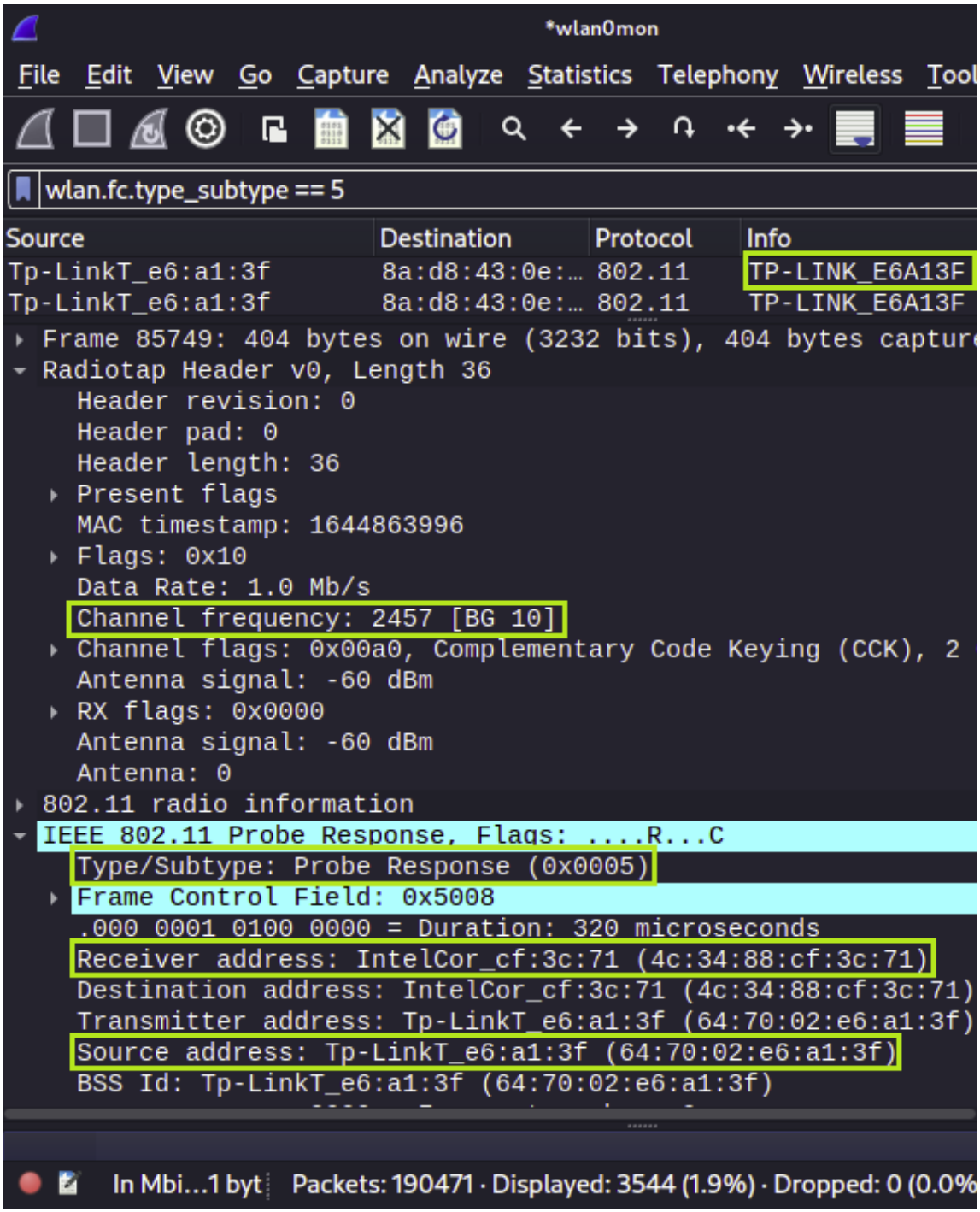
Bağlantı Talebi (Probe Request), kablosuz iletişimde istemcinin erişim noktasına bağlanma isteğidir. Bu paket ağa bağlanmak isteyen istemci tarafından düzenli aralıklarla gönderilir. Ayrıca istemci cihazın kablosuz ağ kartı özelliklerini, desteklediği güvenlik protokollerini ve diğer iletişim bilgilerini içerir. Şekil 3.12'de Wireshark programıyla incelenen probe request paketi görülmektedir.



Şekil 3.12. Wireshark ile incelenen probe request ekran görüntüsü.

3.1.5.3.3 Probe response

İstemci tarafından gönderilen erişim talebi paketine karşılık erişim noktası tarafından gönderilen pakettir. Şekil 3.13'te Wireshark programıyla incelenen probe response paketi görülmektedir.

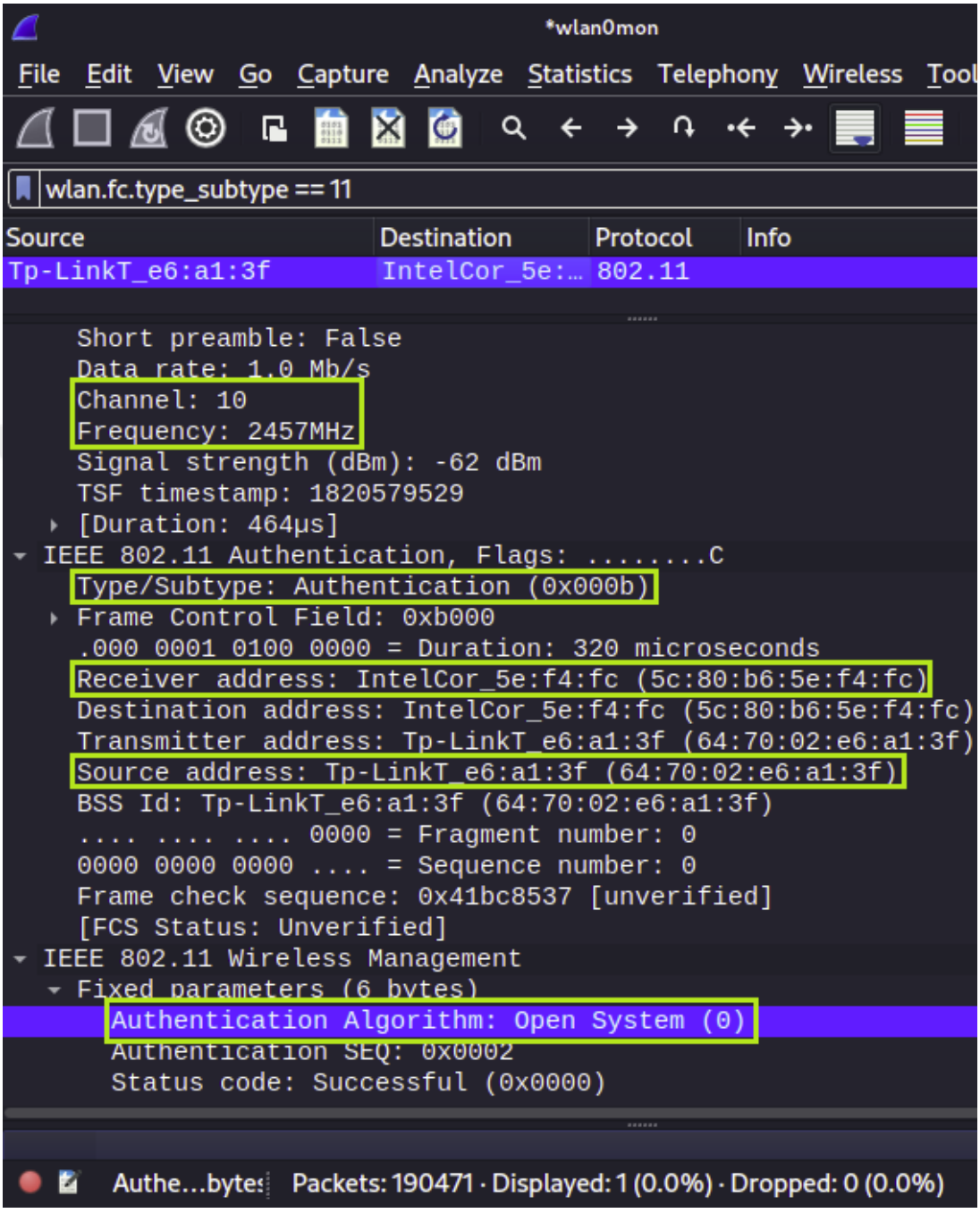


Şekil 3.13. Wireshark ile incelenen probe response ekran görüntüsü.

3.1.5.3.4 Authentication frame

Erişim noktası ve istemci arasındaki Probe Request ve Probe Response aşaması tamamlandıktan sonra ağa bağlanmak isteyen istemci cihazın yetkilendirme aşamasında gönderilen pakettir. Bu paket içerisinde ağın kullanıldığı şifreleme algoritması da tespit

edilebilir. Şekil 3.14'te Wireshark programıyla incelenen authentication paketi ve erişim noktasının şifresiz olduğu görülmektedir.

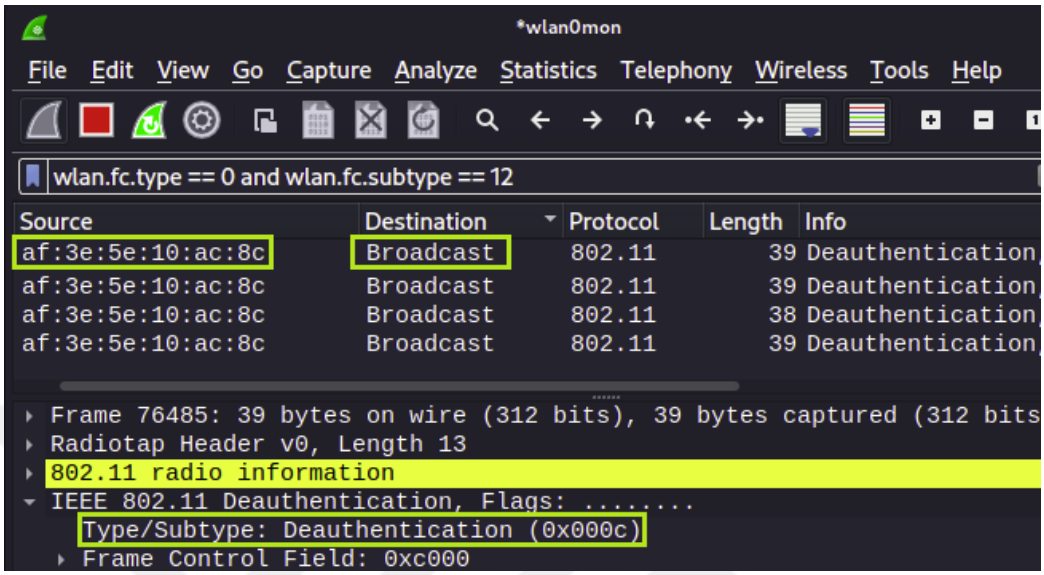


Şekil 3.14. Wireshark ile incelenen authentication paketi ekran görüntüsü.

3.1.5.3.5 Deauthentication frame

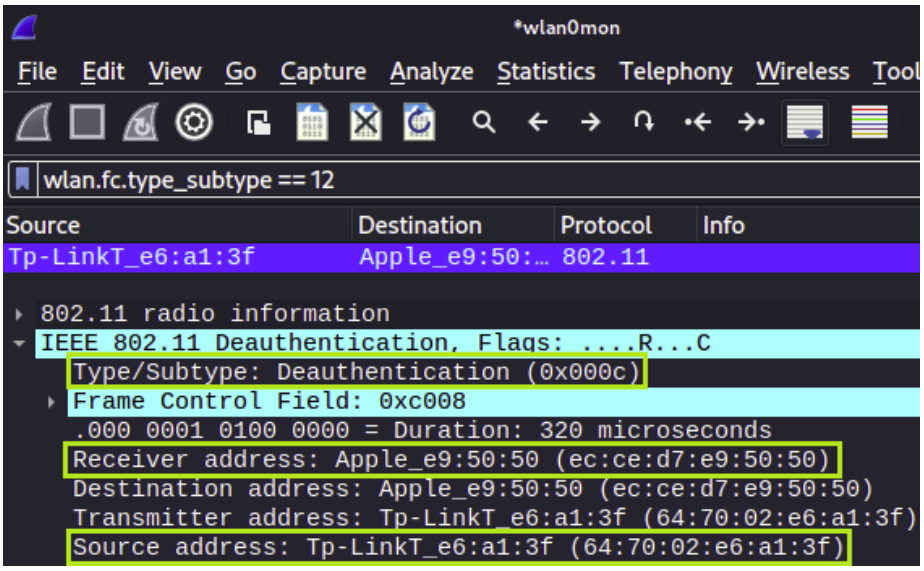
Erişim noktaları, normal şartlar altında ağ sorunlarını gidermek veya ağ üzerinde yapılan konfigürasyonlar nedeniyle bağlı bulunan istemci cihazları ağdan düşürmek için genel veya istemciye özel bir deauthentication paketi yayınlayabilir ve bu bir saldırı

değildir. Erişim noktaları bu amaçlar dışında deauthentication paketlerini yayımlamamaktadır. Şekil 3.15'te Wireshark programıyla incelenen erişim noktasının tüm istemcilere (broadcast) gönderdiği deauthentication paketi görülmektedir.



Şekil 3.15. Wireshark ile incelenen deauthentication paketi ekran görüntüsü.

Erişim noktası kendisine bağlı bulunan tüm istemcilere deauth paketi gönderebileceği gibi tek bir istemcinin de bağlantısını sonlandırabilir. Diğer istemcilerin deauth paketinden etkilenmemesi için bağlantısını sonlandırmak istediği istemcinin MAC adresini kullanır. Şekil 3.16'da Wireshark programıyla incelenen erişim noktasının tek bir istemciye gönderdiği deauthentication paketi görülmektedir.



Şekil 3.16. Wireshark ile incelenen deauthentication paketi ekran görüntüsü.

3.2. Kablosuz Ağlara Yönelik Ağdan Düşürme (Deauthentication) Saldırısı

3.2.1 Ağdan düşürme saldırılarının temel nedeni

Kablosuz ağlarda Deauthentication paketleri, genellikle erişim noktası tarafından istemcinin otomatik olarak bağlantısını kesmek veya istemcinin bağlantıyı tekrar başlatmasını tetiklemek için kullanılır. Erişim noktası tarafından sadece bir istemciye veya tüm bağlı istemcilere gönderilebilir.

Deauthentication paketinin zayıf noktası tekrarlanabilir olmasıdır. Ayrıca üçüncü kişiler tarafından sahte paketler oluşturulabilir ve erişim noktası ile istemci cihaz arasındaki bağlantı kolayca sonlandırılabilir. Kablosuz erişim noktası veya istemci bu paketlerin gerçek olup olmadığını doğrulayamaz. Deauthentication paketleri bu özellikleri nedeniyle bilgisayar korsanları tarafından kablosuz ağlarda ağdan düşürme saldırısı gerçekleştirmek için sıkça kullanılmaktadır (Anonymous, 2022).

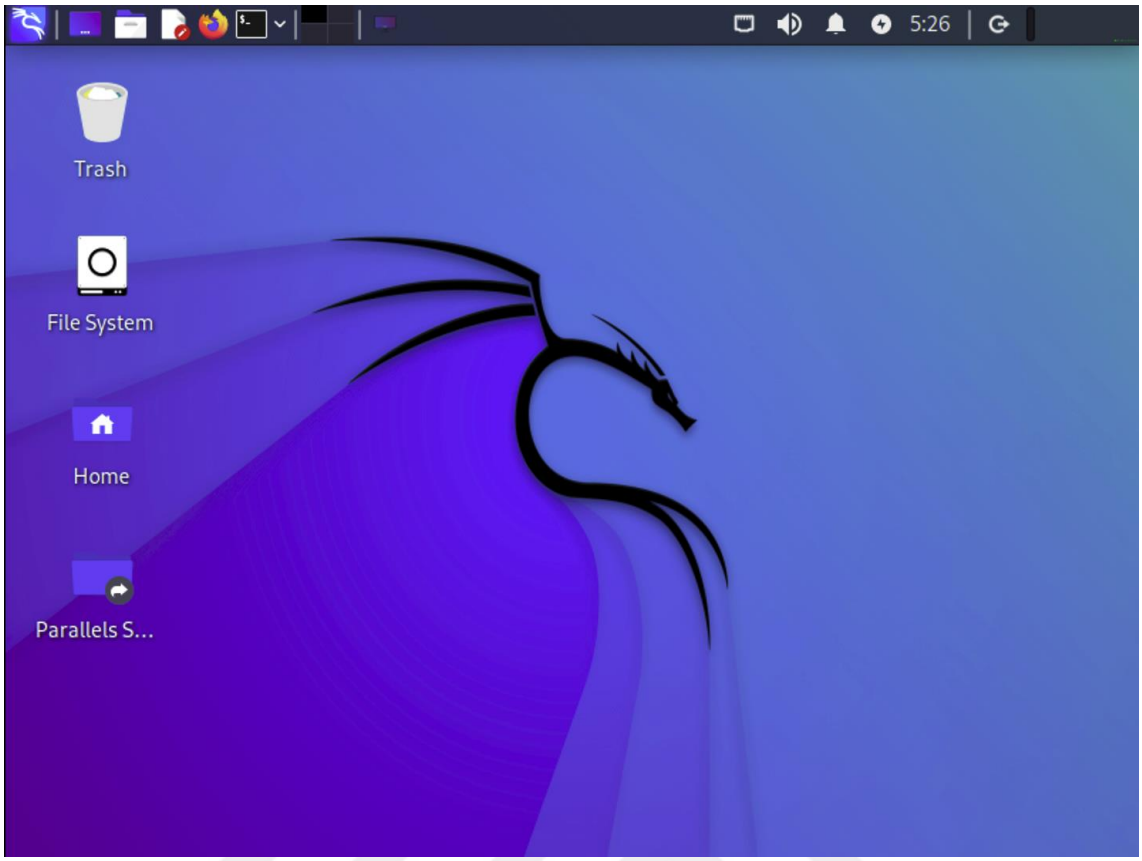
Ağdan düşürme saldırısı, kablosuz ağlar üzerinde gerçekleştirilebilecek birçok atak vektörünün ilk adımıdır. Bilgisayar korsanları bu adımdan sonra sahte erişim noktaları oluşturabilir ve istemcinin tüm ağ trafiğini sahte erişim noktası üzerinden yönlendirebilirler. Böylece bilgisayar korsanları çeşitli yazılımlar ile istemcinin ağ trafiğini dinleyebilir ve gizli bilgileri ifşa edebilirler. (Altınok, 2017)

3.2.2 Saldırıda kullanılan araçlar

3.2.2.1 Kali Linux işletim sistemi

Kali Linux, içerisinde 600'den fazla sızma testi aracı bulunduran ve etik hackerlık ile güvenlik denetimleri uygulamalarının tek bir sistem üzerinden gerçekleştirilmesini amaçlayan bir işletim sistemidir. Kali Linux, Offensive Security tarafından Linux işletim sisteminin bir dağıtımı olan Debian'ın standartlarına göre geliştirilmiş, ücretsiz ve birçok dil seçeneğine sahip açık kaynaklı bir işletim sistemidir (Dilben, 2020).

Bu işletim sistemi, siber güvenlik uzmanları, hackerlar ve ağ güvenliği uzmanları tarafından kullanılması için geliştirilmiştir. Kali Linux, siber güvenlik testleri yapmak, ağ zafiyetlerini ortaya çıkarmak, sistem güvenliğini değerlendirmek ve sistem açıklarını kapatmak amacıyla kullanılır. Şekil 3.17'de Kali Linux işletim sisteminin örnek bir ekran görüntüsü bulunmaktadır. İndirme linki EK-1 A'da verilmiştir.

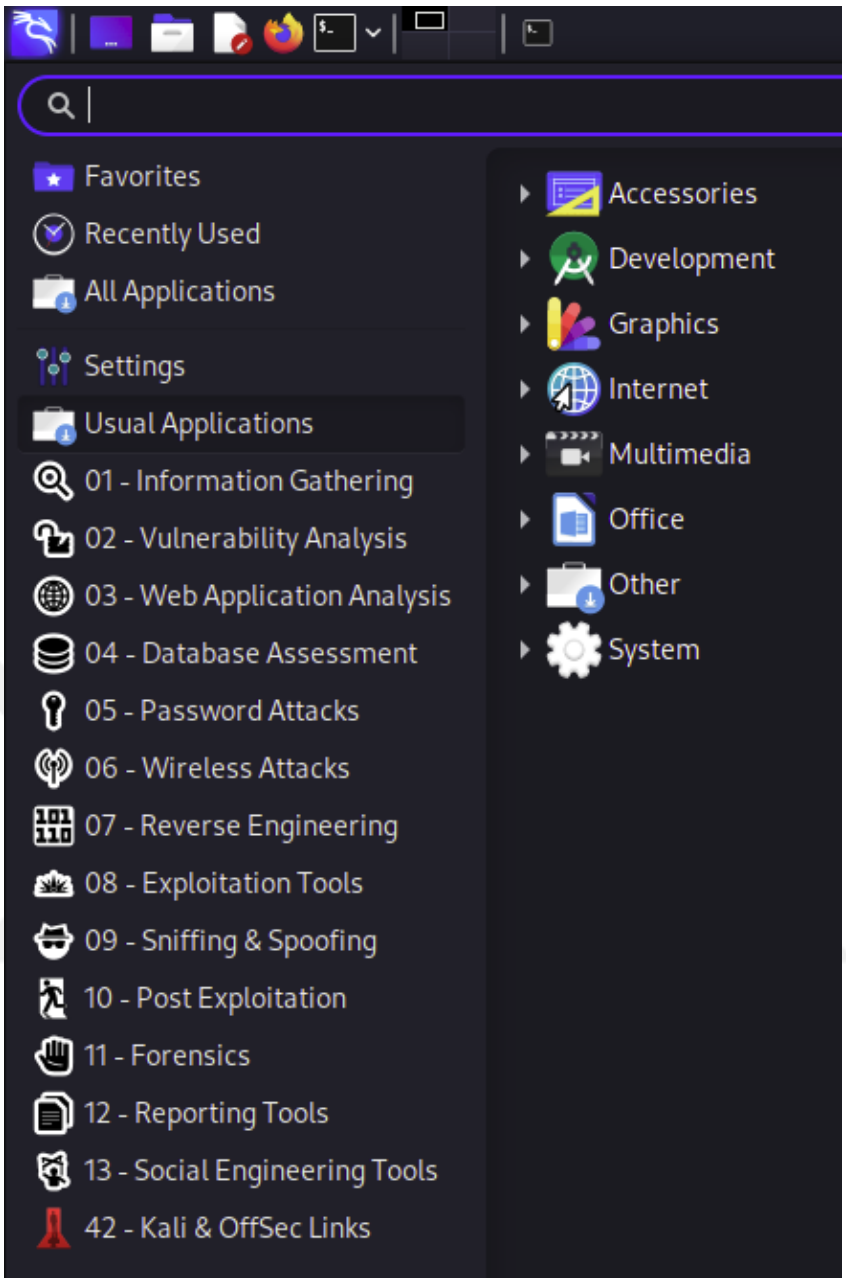


Şekil 3.17. Kali linux ekran görüntüsü.

Kali Linux işletim sistemin bazı özellikleri aşağıda listelenmiştir.

1. Siber güvenlik uzmanlarının ihtiyaç duyduğu onlarca açık kaynak yazılımlar ile donatılmıştır. Bu yazılımlar, ağ tarama, güvenlik açıkları tespiti, parola kırma, saldırı simülasyonu ve diğer birçok siber güvenlik testleri için kullanılır.
2. Birçok farklı donanım altyapısında çalışabilir. Bu durum farklı cihazlar ve sistemler üzerinde siber güvenlik testleri yapmak için esneklik sağlar.
3. Siber güvenlik eğitimleri ve sertifikasyon programları için de sıkça tercih edilir. Öğrenciler ve profesyoneller, Kali Linux'ı kullanarak siber güvenlik becerilerini geliştirebilirler.
4. Açık kaynaklı bir işletim sistemidir. Bu durum kodunun herkes tarafından incelenebilir ve geliştirilebilir olmasını sağlar.

Kali Linux, siber güvenlik uzmanlarının ve araştırmacılarının ihtiyaç duyduğu yüzlerce zafiyet tespit aracını içerisinde barındırmaktadır. Bu araçlar işletim sisteminde kategorize edilmişlerdir. Toplam 13 kategori bulunmaktadır. Şekil 3.18'de Kali Linux işletim sistemi içerisinde kategorize edilmiş araçlar menüsü görülmektedir.



Şekil 3.18. Kali Linux ekran görüntüsü.

Kali Linux içerisinde bulunan popüler güvenlik kategoriler ve açıklamaları aşağıda listelenmiştir.

- Information Gathering (Bilgi Toplama): Hedef sistem hakkında bilgi toplamak için gerekli araçları içerir. Bu araçlar ile hedef sistem üzerinde güvenlik duvarı tespiti, erişime açık portlar gibi bilgiler elde edilebilir. Ayrıca açık kaynak istihbaratı (OSINT) araçları bulunmaktadır.
- Vulnerability Analysis (Zafiyet Analizi): Sistemlerdeki potansiyel zafiyetleri tespit etmek için gerekli araçları içerir.

- Web Applications (Web Uygulamaları): Bu kategorideki araçlar ile web uygulamalarındaki zafiyetlerin tespiti gerçekleştirilir. Ayrıca içerisinde günümüzde sıkça kullanılan Wordpress tabanlı web uygulamalarındaki zafiyetleri tespit etmek için bir araç bulunur.
- Password Attacks (Parola Saldırıları): Bu kategori, parola saldırıları ve parola güvenliğini test etmek için gerekli araçları içerir.
- Wireless Attacks (Kablosuz Saldırılar): Kablosuz ağları hedef alan saldırıları gerçekleştirmek için kullanılan araçları barındırır. Tez kapsamında bahsedilen Aircrack-ng araç kiti bu kategoride bulunur.
- Exploitation Tools (Sömürü Araçları): Keşfedilen zafiyetleri kullanarak sistemlere erişmeyi amaçlayan araçları barındırır.
- Forensics Tools (Adli Bilişim Araçları): Adli bilişimde kullanılan araçları içerir. Bu araçlar ile sistem imajı alınabilir ve sonuçlar raporlanabilir.
- Social Engineering Tools (Sosyal Mühendislik Araçları): Hedef kullanıcıları üzerinde oltalama saldırıları gerçekleştirmek ve Trojan virüsleri oluşturmak için gerekli araçları içerir.

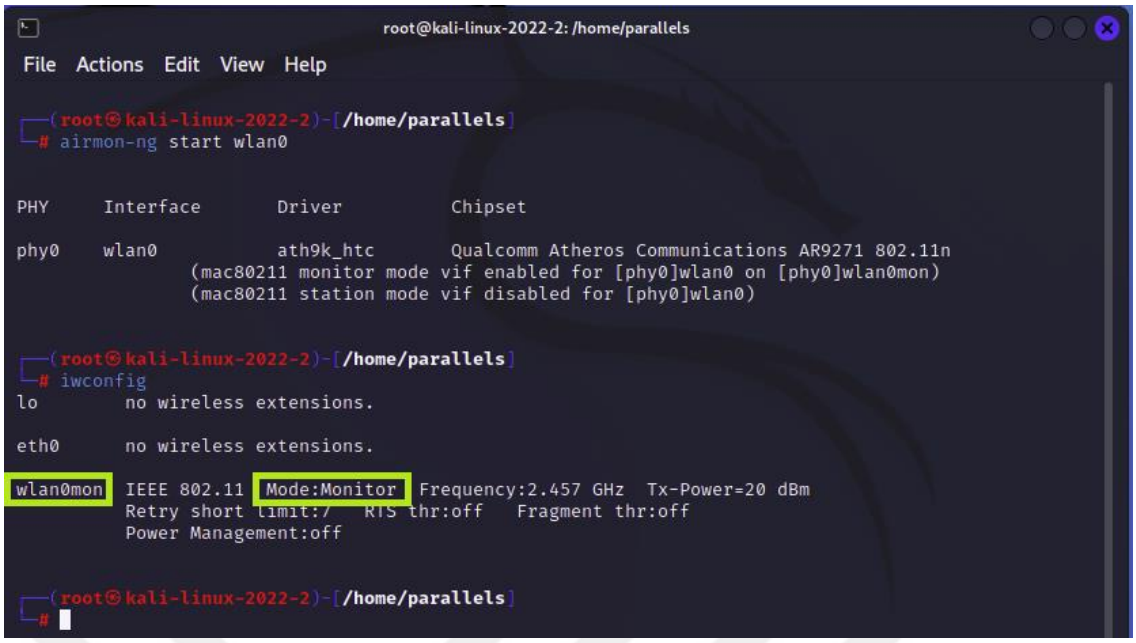
3.2.2.2 Aircrack-ng araç kiti

3.2.2.2.1 Aircrack-ng araç kiti hakkında

Aircrack-ng, kablosuz ağ güvenliği ve penetrasyon testi alanında kullanılan birçok açık kaynaklı yazılımı içerisinde barındıran bir araç kitidir. Aircrack-ng araç kiti, kablosuz ağlardaki güvenlik açıklarını tespit etmek, ağ şifrelerini kırmak ve ağ güvenliği testlerini yapmak için kullanılır (Sontowski, 2022). Kali linux işletim sisteminde hazır gelen ve Aircrack-ng ailesinden olan Airmon-ng, Airodump-ng, Aireplay-ng ve Airbase-ng araçları kablosuz ağlarda ağdan düşürme saldırılarında sıklıkla kullanılır (Altınok, 2017).

3.2.2.2.2 Airmon-ng

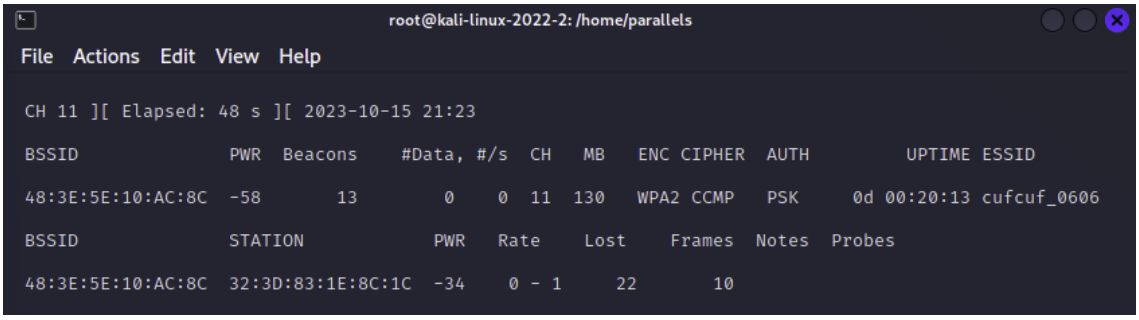
Kablosuz ağ kartını monitör moda almak ve ağ trafiğini izlemek için kullanılır. Şekil 3.19'da airmon-ng aracının kullanımı ve "iwconfig" komutu ile mod durumu görülmektedir. Bazı kablosuz ağ kartlarında bu komut çalıştırıldıktan sonra ağ kartı adının yanına monitör moda alındığını ifade etmek için "mon" takısı eklenir (Altınok, 2017).



Şekil 3.19. Airmon-ng aracı terminal ekran görüntüsü.

3.2.2.2.3 Airodump-ng

Kablosuz ağları taramak ve bu ağlar hakkında bilgi toplamak için kullanılır. Aracı kullanabilmek için ağ kartının monitör moda alınması gerekmektedir (Akbaş, 2015). Şekil 3.20'de airodump-ng aracının kullanımı ve çıktısı görülmektedir. Airodump-ng aracının kullanılabilir parametreleri, filtreleri ve çıktının nasıl yorumlandığı EK-2'de verilmiştir.



Şekil 3.20. Airodump-ng aracı terminal ekran görüntüsü.

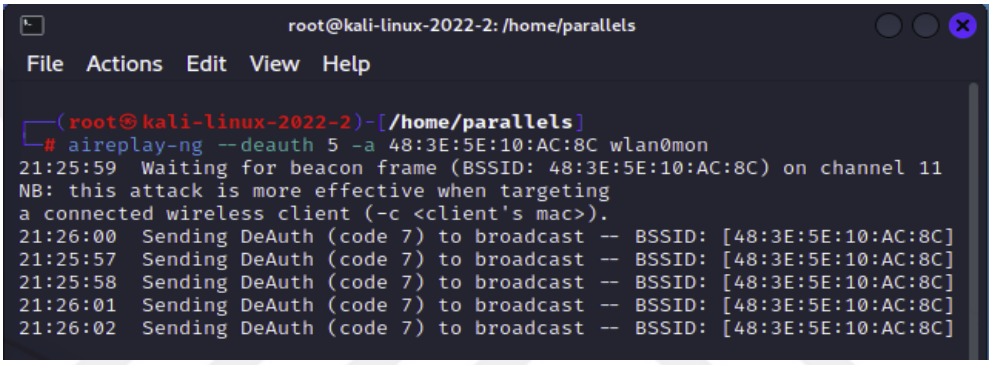
Airmon-ng aracı ile kablosuz ağlar hakkında elde edilebilecek bilgiler aşağıda listelenmiştir.

1. SSID
2. Yetkilendirme türü
3. Ağa bağlı bulunan istemciler

4. Erişim noktasının ne kadar süredir açık olduğu
5. Şifreleme türü
6. Kanal Numarası

3.2.2.2.4 Aireplay-ng

Kablosuz ağlara yönelik ağdan düşürme saldırılarını gerçekleştirmek, parolaları kırmak ve sahte trafik üretmek gibi birçok saldırı yöntemini destekleyen bir araçtır (Yüksel, 2021). Şekil 3.21'de aireplay-ng aracının kullanımı ve çıktısı görülmektedir. Aireplay-ng aracının kullanılabilir parametreleri ve saldırı modları EK-3'te verilmiştir.



Şekil 3.21. Aireplay-ng aracı terminal ekran görüntüsü.

3.2.2.2.5 Airbase-ng

Sahte kablosuz ağlar oluşturmak için kullanılan araçtır. Çalıştırıldığında monitör moda alınmış kablosuz ağ kartı üzerinden at(x) adlı sanal bir ağ kartı oluşturur ve erişim noktası olarak yayın yapar (Altınok, 2017). Şekil 3.22'de airbase-ng aracının kullanımı ve çıktısı görülmektedir. Airbase-ng aracının kullanılabilir parametreleri EK-4'te verilmiştir.

Şekil 3.22. Airbase-ng aracı terminal ekran görüntüsü.

3.2.2.2 Dnsmasq

Dnsmasq, DNS ve DHCP sunucusu olarak kullanılabilen basit bir yazılımdır. Genellikle erişim noktası olarak tasarlanmamış istemci cihazların erişim noktası olarak kullanılabilmesi için DNS ve DHCP sunucuları oluşturur. İçerisinde bulunan birçok yapılandırma seçeneği ile hızlı bir şekilde erişim noktası oluşturulmasını sağlar (Kelly, 2001).

3.2.3 Örnek ağdan düşürme saldırısı

3.2.3.1 Saldırı senaryosu ve aşamaları

Kablosuz ağlarda ağdan düşürme saldırıları sonrasında uygulanabilecek birçok saldırı vektörü bulunmaktadır (Gezgin ve ark, 2012). Bu saldırı vektörleri, erişim noktası şifresinin ele geçirilmesi ve ağ trafiğinin izlenerek gizi bilgilerin (hesap şifreleri vb.) ifşa edilmesi olarak iki ana başlık altında toplanabilir.

İstemci cihazlar erişim noktasına bağlanmak için yetkilendirme aşamasında kablosuz ağ şifresinin de içinde olduğu ve bir kez oluşturulan paketi (handshake) erişim noktasına gönderirler. Bilgisayar korsanları ağdan düşürme saldırılarını kullanarak sürekli olarak istemcinin tekrardan bağlantı kurmasını sağlayarak erişim noktasının şifresinin içinde olduğu paketi yakalamaya çalışırlar.

Ancak paketin içerisinde kablosuz ağ şifresi açık olarak yer almamaktadır. Bu nedenle bazı kelime listeleri ve araçlar kullanarak brute force (kaba kuvvet saldırısı) yöntemiyle paketi deşifre etmeye çalışırlar (Yüksel, 2021). Bilgisayar korsanları brute force yöntemi ile kablosuz ağ şifresini kırmanın çok uzun süreceğini bildiklerinden genellikle sahte kablosuz ağlar oluşturularak son derece gerçekçi görünen sahte captive portal (kısıtlama portalı) saldırısı yapmayı tercih ederler.

3.2.3.1.1 Captive portal saldırısı

Captive portal, genellikle halka açık yerlerde bulunan kablosuz ağlarda kullanılan bir kimlik doğrulama mekanizmasıdır. Kullanıcılar, bu ağlara bağlandıklarında öncelikle tarayıcılarında bir captive portal penceresi ile karşılaşırlar. Kimlik doğrulaması başarılı olan kullanıcılara internet erişimi sağlanır (Kancura, 2022). Bu sayede, ağ sahipleri istemcilerin ağı kullanmadan önce belirli bir kimlik doğrulama işlemi tamamlamalarını sağlarlar.

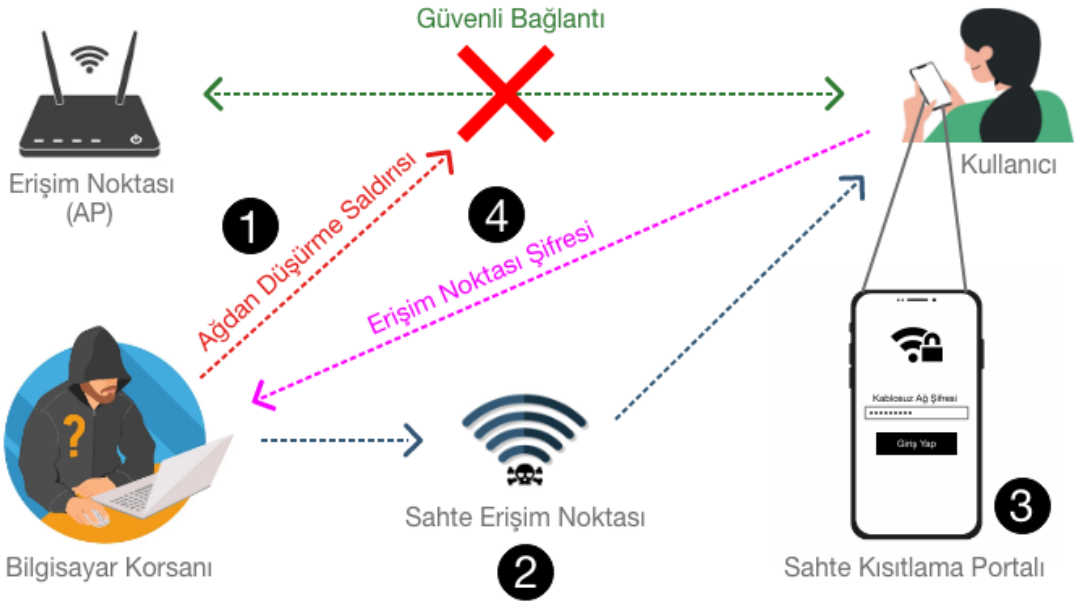
Captive portal, istemci cihazlar bağlandıktan sonra otomatik olarak açılır ve kullanıcılardan gerekli kimlik bilgilerini girmelerini veya kullanım koşullarını kabul etmelerini isteyebilir. Kimlik doğrulanması tamamlandığında, istemciler internete erişebilirler. Captive portal, kablosuz ağların güvenliğini artırır ve ağ sahiplerine kullanıcı aktivitelerini izleme ve ağ erişimini yönetme olanağı sağlar.

Captive portal penceresinin otomatik olarak açılmasının nedeni, işletim sistemlerinin internet erişimini kontrol etmek için belirli adreslere istek göndermeleridir. Eğer erişim noktasında bir captive portal kurulu ise işletim sistemlerinin internet erişimi için yaptığı isteklere karşılık olarak captive portalın çalıştığı adres bilgisi gönderilir. Bu sayede kullanıcılar, önce captive portal penceresinde kimlik doğrulama veya kullanım koşullarını kabul etme gibi işlemleri tamamlarlar ve ardından internet erişimine sahip olurlar.

Bilgisayar korsanları, hedef erişim noktası ile aynı SSID ve kanal bilgisine sahip ancak şifresiz sahte bir erişim noktası oluştururlar. Oluşturdukları sahte erişim noktası üzerine kullanıcılardan hedef erişim noktasına ait şifreyi talep ettikleri özel bir captive portal kurulumu yaparlar. Ardından hedef erişim noktasına ağdan düşürme saldırısını başlatırlar. Ağdan düşen istemciler, gerçek erişim noktasının şifresiz olarak yayın yaptığını zannederek sahte erişim noktasına otomatik olarak bağlanırlar.

Bilgisayar korsanları, captive portal penceresinin otomatik olarak açılma özelliğinden faydalanarak istemcilerden kablosuz ağ şifresini talep ederek kandırmaya çalışırlar.

Kullanıcılar captive portal penceresinde kablosuz ağ şifresini girdiklerinde bilgisayar korsanları sahte erişim noktasını kapatır ve hedef erişim noktasına başlattıkları ağdan düşürme saldırısını durdururlar. İstemciler otomatik olarak yeniden gerçek erişim noktasına bağlanırlar ve erişim noktasının şifresinin çalındığını anlamazlar. Bu sayede bilgisayar korsanları kolayca şifreyi elde etmiş olurlar. Şekil 3.23’te örnek saldırı senaryosunun nasıl gerçekleştiği temsili olarak görülmektedir.

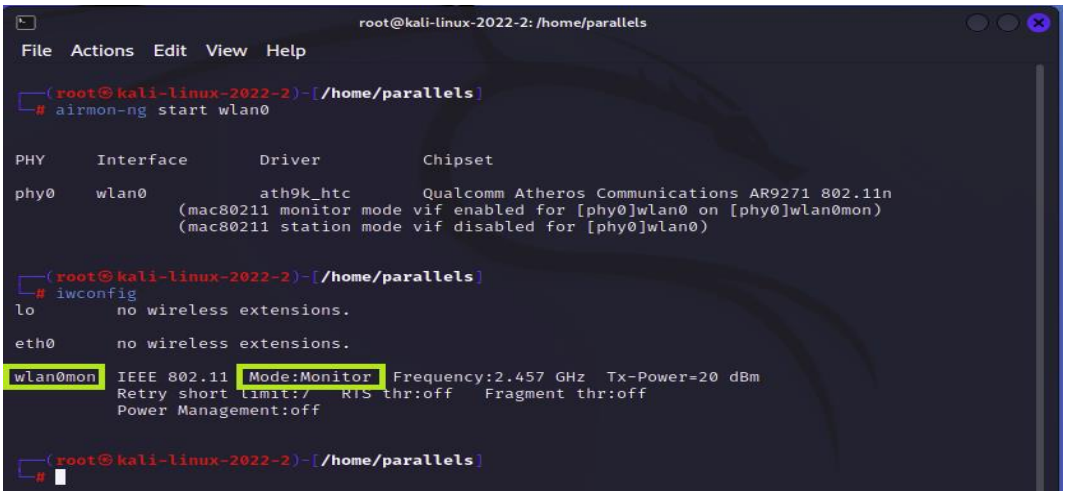


Şekil 3.23. Captive portal saldırısı.

3.2.3.1.2 Saldırı senaryosunun uygulanması

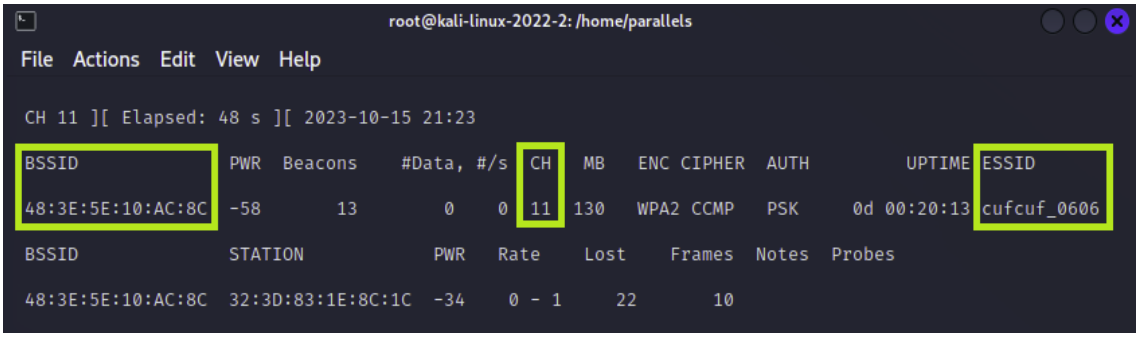
Keşif aşamasında, hedef erişim noktasına ait önemli bilgiler olan SSID, BSSID ve bağlı istemci cihazlar gibi verileri elde etmek kritik bir adımdır.

Bu bilgilere ulaşmak için "airodump-ng" aracı kullanılmıştır. Ancak airodump-ng'nin kullanılabilmesi için öncelikle kablosuz ağ kartının "airmon-ng" aracıyla monitör moda alınması gerekmektedir. Şekil 3.24'te, kablosuz ağ kartının "iwconfig" komutu ile monitör moda alındığının kontrolü yapılmıştır (Anonim, 2021).



Şekil 3.24. Kablosuz ağ kartının monitör moda alınması.

Kablosuz ağ kartının monitör moda alınmasının ardından airodump-ng aracı ile hedef erişim noktasına ait bilgiler Şekil 3.25'te görülmektedir.



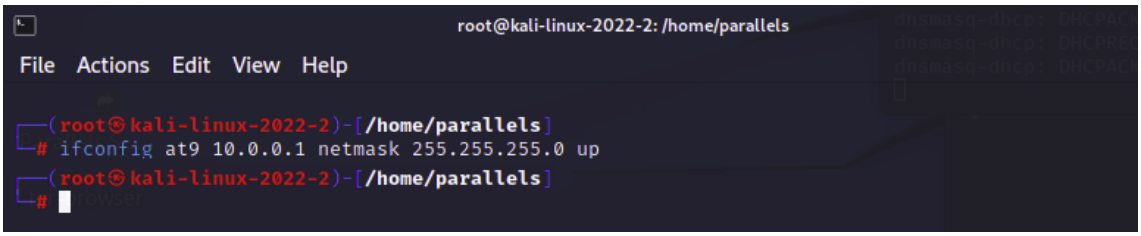
Şekil 3.25. Hedef erişim noktasına ait bilgiler.

Hedef erişim noktasına ağdan düşürme saldırısı başlatıldıktan sonra istemci cihazların bağlanabileceği sahte erişim noktası oluşturmak için airbase-ng aracı kullanılmıştır. Şekil 3.26'da airbase-ng aracı ile oluşturulan sahte erişim noktası görülmektedir.

Şekil 3.26. Sahte erişim noktasının oluşturulması.

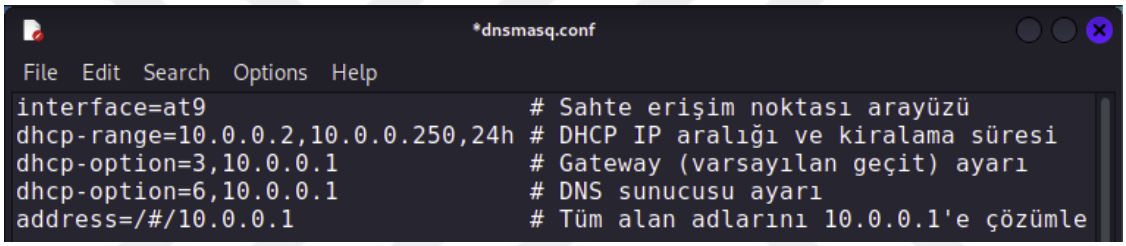
İstemci cihazların sahte erişim noktasına otomatik olarak bağlanabilmeleri için SSID ile kanal bilgisi aynı olması ve şifresinin olmaması gerekir. Airbase-ng aracı, sahte erişim noktası oluşturabilmek için monitör moda alınmış kablosuz ağ kartı üzerinden at(x) isimli bir sanal ağ arayüzü oluşturur ve yayın yapar.

Airbase-ng aracı ile oluşturulan sahte erişim noktasının ağ arayüzünün kullanabileceği IP adresi aralığının tanımlanması gerekir. Şekil 3.27'de "at9" adlı arayüze tanımlanan IP adresi aralığı görülmektedir.



Şekil 3.27. Ağ arayüzüne ip aralığının tanımlanması.

Airbase-ng aracı DHCP ve DNS hizmetlerini içermez. Bu nedenle sahte erişim noktasına istemci cihazların bağlanabilmeleri ve gerekli ağ yapılandırma bilgilerini alabilmeleri için Dnsmasq aracı kullanılmıştır. Şekil 3.28'de airbase-ng ile oluşturulan sahte erişim noktasına entegre edilecek DHCP ve DNS hizmeti sağlayan Dnsmasq aracının ayarları görülmektedir. Airbase-ng ile oluşturulan sanal ağ arayüzünün adı da ayarlara eklenerek, dnsmasq aracı sahte erişim noktasına entegre edilmiştir.

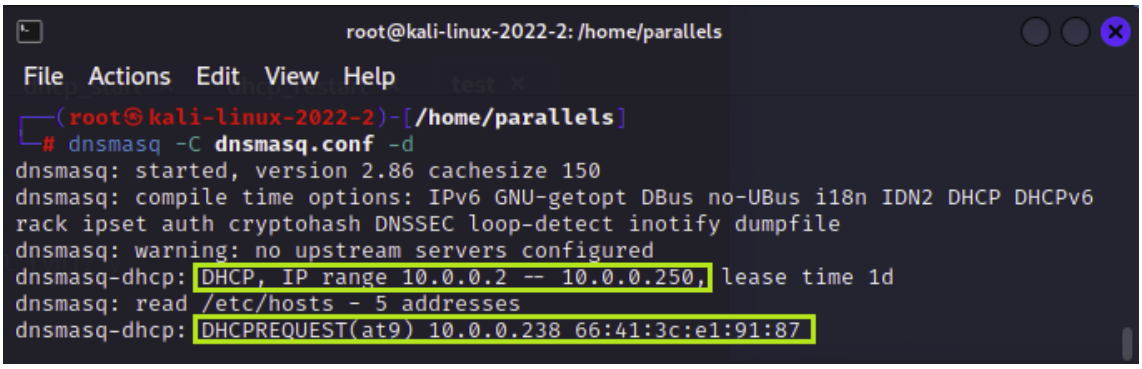


Şekil 3.28. Dnmasq aracının ayarları.

Dnsmasq ayarlarının açıklamaları aşağıda listelenmiştir.

1. Interface: Erişim noktasının ağ arayüzü adını ifade eder.
2. Dhcp-range: İstemci cihazlara verilecek yerel IP adresi aralığını ifade eder.
3. Address: DNS sunucusunun IP adresini ifade eder. Bu adres, genellikle Dnmasq aracının üzerinde çalıştığı işletim sisteminin IP adresidir. Erişim noktası üzerinden gelen tüm DNS istekleri bu adres üzerinden işlenir ve yanıtlanır.

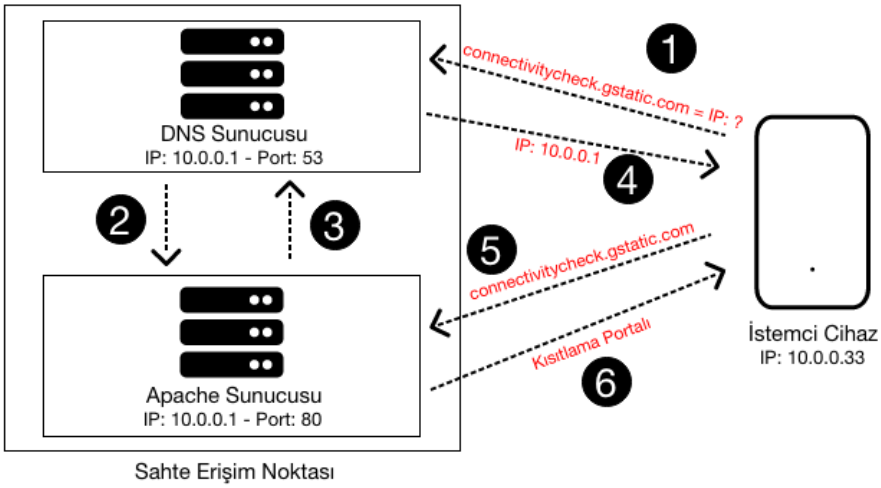
Dnsmasq aracı, çalıştırıldıktan sonra sahte erişim noktasına bağlanan istemci cihazlara yapılandırma bilgilerini iletmek üzere bekler. Şekil 3.29'da dnmasq aracı görülmektedir.



Şekil 3.29. Dnmasq aracı ekran görüntüsü.

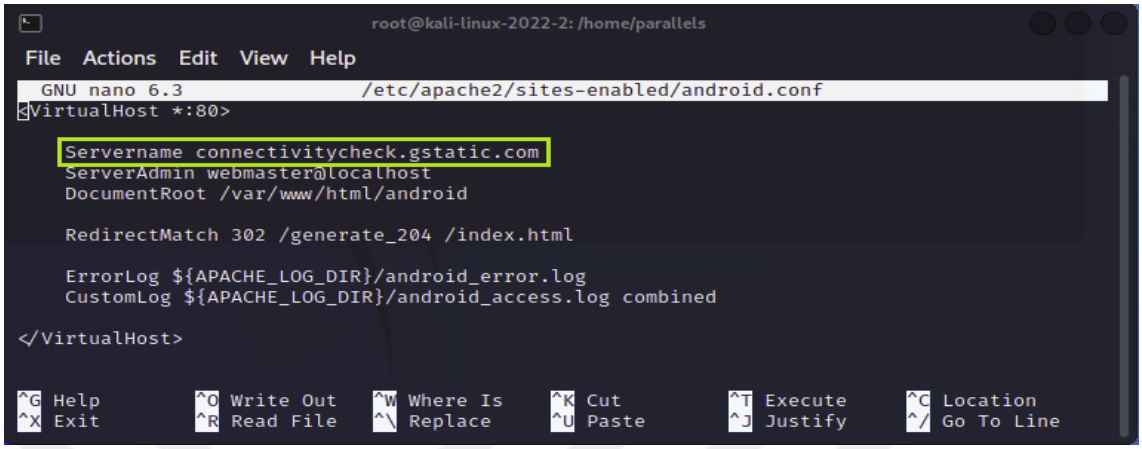
İstemci cihazlar, sahte erişim noktasına bağlandıktan sonra internet erişimini kontrol etmek için "connectivitycheck.gstatic.com" gibi adreslere istek gönderirler. Dnsmasq aracı ile oluşturulan DNS sunucusu bu istekleri işletim sisteminin IP adresini verir.

İstemci cihazlarda captive portal penceresinin görüntülenebilmesi için işletim sisteminin IP adresi üzerinde bir captive portal hizmeti sunulması gereklidir. Captive portallar, bir web sitesi şeklinde çalışırlar. Bu nedenle, Kali Linux işletim sistemi üzerinde bulunan Apache sunucusu kullanılarak captive portal hizmeti oluşturulacaktır. Şekil 3.30'da DNS sunucusuna gönderilen isteklerin Apache sunucusu ile ilişkisi görülmektedir.



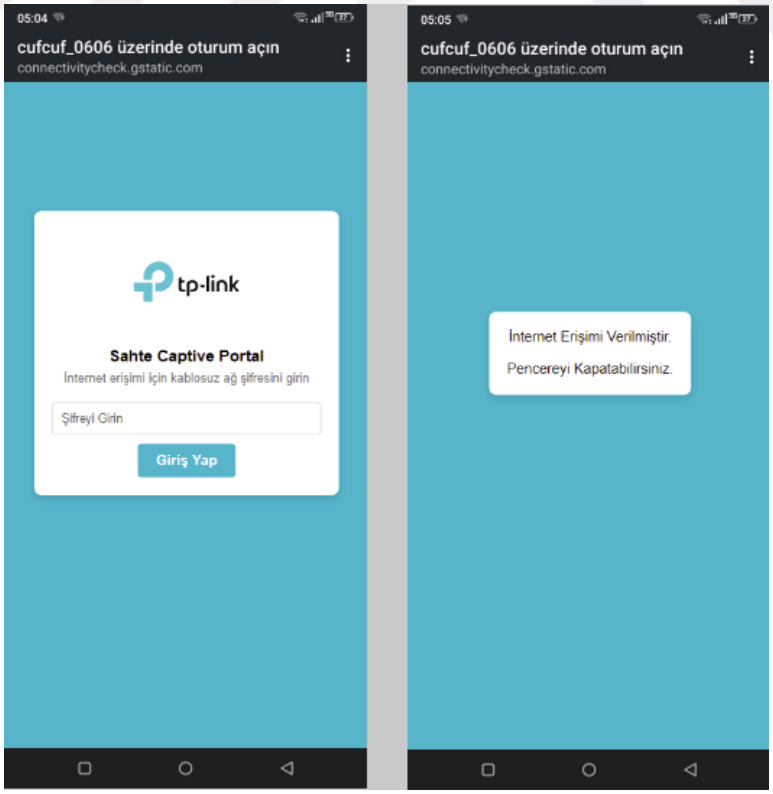
Şekil 3.30. DNS ve apache sunucusu ilişkisi.

DNS sunucusunun internet erişimi için gelen isteklere işletim sisteminin IP adresini çözümleyebilmesi ya da verebilmesi için Apache sunucusu üzerindeki yapılandırma ayarları Şekil 3.31'de görülmektedir.



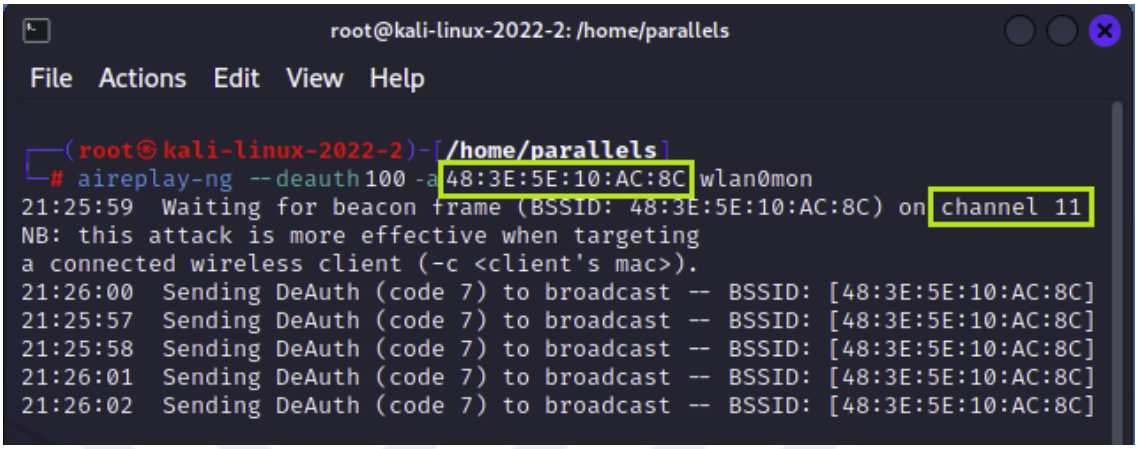
Şekil 3.31. Apache yapılandırma ayarları.

İstemci cihazda görüntülenecek olan captive portal, Apache sunucusunun desteklediği PHP programlama dili kullanılarak geliştirilmiştir. Şekil 3.32'de captive portalın ekran görüntüleri verilmiştir.



Şekil 3.32. Captive portal ekran görüntüleri

İstemci cihazlarda açılan captive portal ekranında ağ şifresinin girilebilmesi için metin kutusu ve buton kullanılmıştır. Captive portal girilen ağ şifresini password.txt adlı metin belgesine kaydedilmiştir. Aireplay-ng aracı ile ağdan düşürme saldırısı başlatılmıştır. Şekil 3.33'te ağdan düşürme saldırısı görülmektedir.



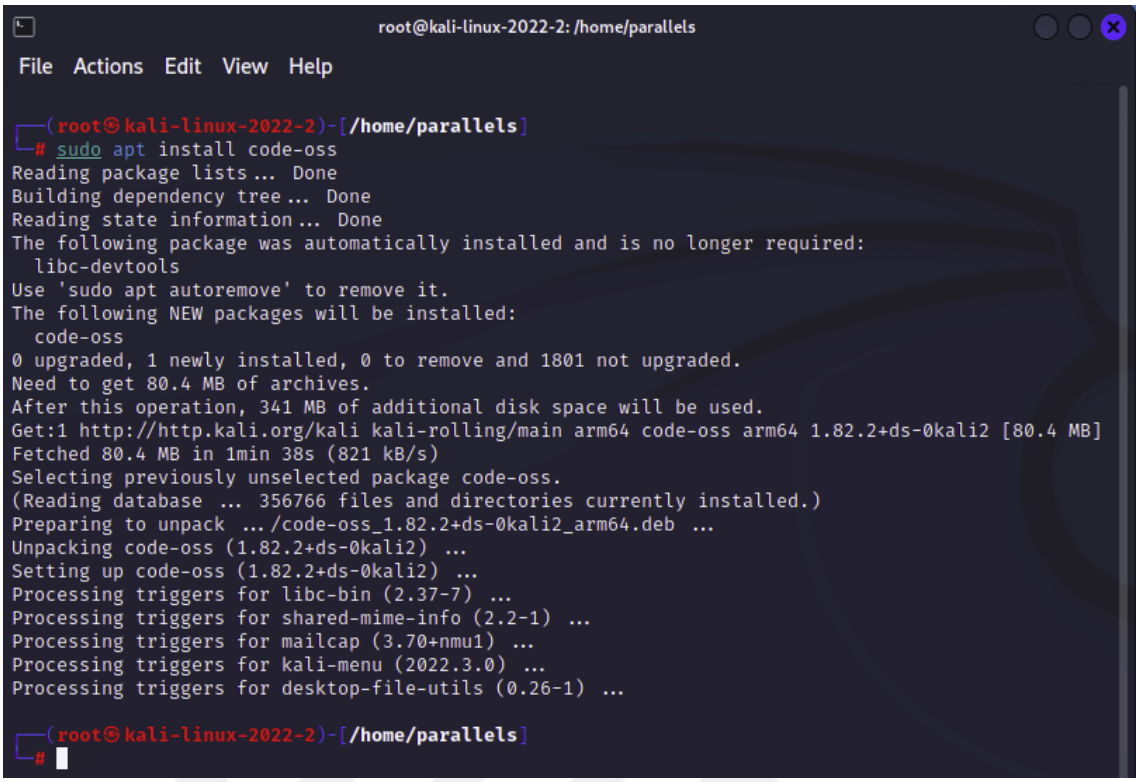
Şekil 3.33. Aireplay-ng ile ağdan düşürme saldırısı.

Sonuç olarak istemci cihazların gerçek erişim noktası ile bağlantısı koparılmış ve sahte erişim noktasına bağlanmaları sağlanmıştır. İstemci cihazlarda açılan captive portal ile ağ şifresi ele geçirilmiş ve ağdan düşürme saldırısı sonlandırılmıştır.

3.3 Ağdan Düşürme Saldırılarına Karşı Tespit ve Uyarı Yazılımın Geliştirilmesi

3.3.1 Code-OSS editör kurulumu

Visual Studio Code kısaca VsCode olarak adlandırılan, Microsoft tarafından geliştirilen, yaygın olarak kullanılan bir metin düzenleyici ve entegre geliştirme ortamı (IDE) yazılımıdır. Bu yazılım geliştirme ortamı, birçok programlama dili için destek sunar ve açık kaynaklı bir yazılımdır. Visual Studio Code, birçok platformda çalışabilen basit ve çok yönlü bir yazılım geliştirme aracıdır. Yazılım geliştirme ortamı olarak Visual Studio Code editörünün Kali Linux işletim sistemi için özelleştirilmiş Code-Oss editörü tespit ve uyarı yazılımı geliştirmek için kullanılmıştır. Şekil 3.34'te Code-Oss editörünün kurulumu ve çıktısı görülmektedir.

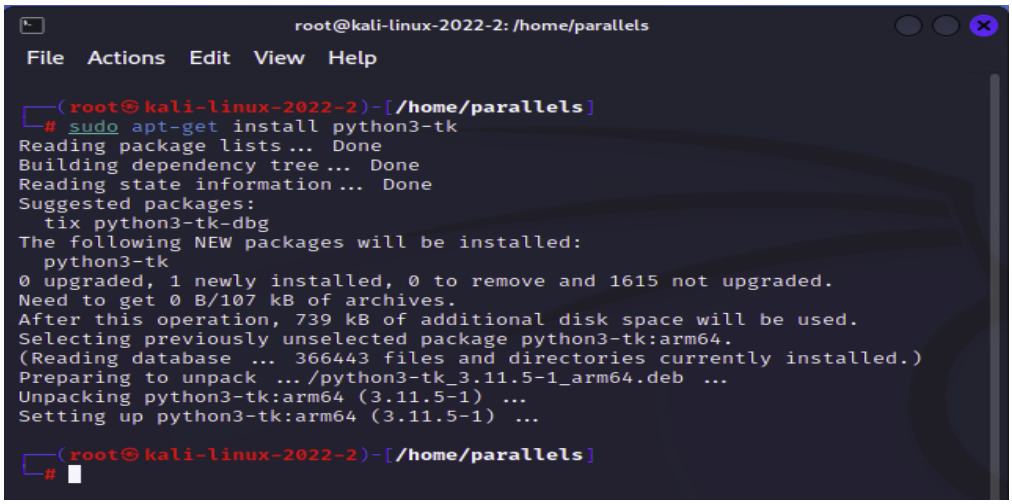


Şekil 3.34. Code-Oss kurulumu.

3.3.2 Tkinter kütüphanesi ve kurulumu

Tkinter, Python için standart GUI (Graphical User Interface – Grafiksel Kullanıcı Arayüzü) kütüphanesidir. Python, Tkinter ile birlikte kullanıldığında GUI uygulamaları hızlı ve kolay bir şekilde oluşturulur. Tkinter, Tk GUI araç setine güçlü bir nesne yönelimli arayüz sağlar (Uzun, 2024).

Bu kütüphane sayesinde buton, pencere, metin kutusu, menüler, renklendirmeler ve diğer arayüz öğeleri oluşturulur. Saldırı tespit ve uyarı yazılımın kullanıcı arayüzü bu kütüphane ile geliştirilecektir. Şekil 3.35'te Tkinter kütüphanesinin kurulumu ve çıktısı görülmektedir.



Şekil 3.35. Tkinter kütüphanesinin kurulumu.

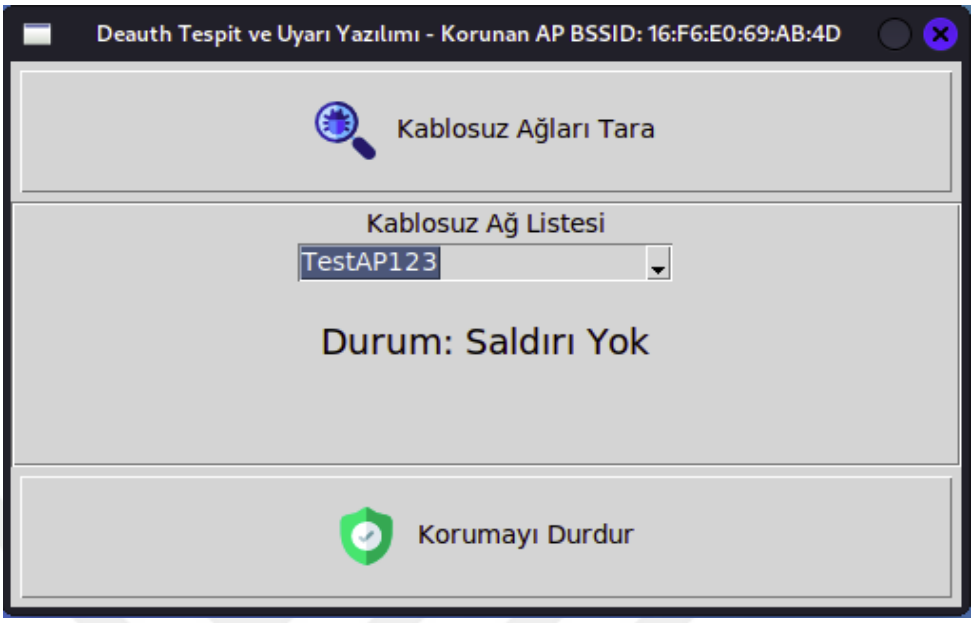
3.3.3 Scapy kütüphanesi

Scapy, ağ paketlerini gönderme, izleme ve doğalarını anlama yeteneğine sahiptir. Bu program, ağları araştırmak ve hatta saldırmak için araçlar oluşturmayı kolaylaştırabilir. Scapy, farklı program türlerine ait paketleri anlayabilir, ağa gönderebilir, yakalayabilir ve bunlarla iletişim kurabilir. Scapy iz sürme, birim testleri, keşif, tarama, ağ keşfi veya saldırılar gibi çeşitli görevleri kolaylıkla yerine getirebilir (Hamzah, 2017). Ağ trafiğinde her paketin tip (type) ve alt tip (subtype) numarası bulunmaktadır. Deauthentication paketlerinin tip numarası 0 ve alt tip numarası ise 12'dir (Altınok, 2017). Ağ trafiğini dinleyebilmek için, kablosuz ağ kartı monitör moda alınmış ve Scapy kütüphanesi koda dâhil edilmiştir. Ardından scapy kütüphanesi fonksiyonları kullanılarak deauthentication paketi tespit edilmiş ve paket bilgileri ekrana yazdırılmıştır. Bu işlem için yazılmış python kodu Ek-5'te verilmiştir.

3.3.4 Arayüz tasarımı ve yazılımın geliştirilmesi

Kablosuz ağlarda ağdan düşürme saldırılarına karşı tespit ve uyarı yazılımı python programlama dili kullanılarak geliştirilmiştir. Python, açık kaynak bir programlama dilidir ve geniş bir topluluk tarafından desteklenmektedir. Ayrıca python, zengin bir kütüphane ekosistemi sunar ve bu durum yazılım geliştirme sürecini hızlandırmamıza ve kaynakları daha verimli bir şekilde kullanmamıza olanak sağlar.

Tez çalışmasında sistem kurgusunu ifade edip deney ortamında gösterilmek üzere yeterli olan kullanıcı arayüzü tasarım Şekil 3.36'da gösterilmiştir.

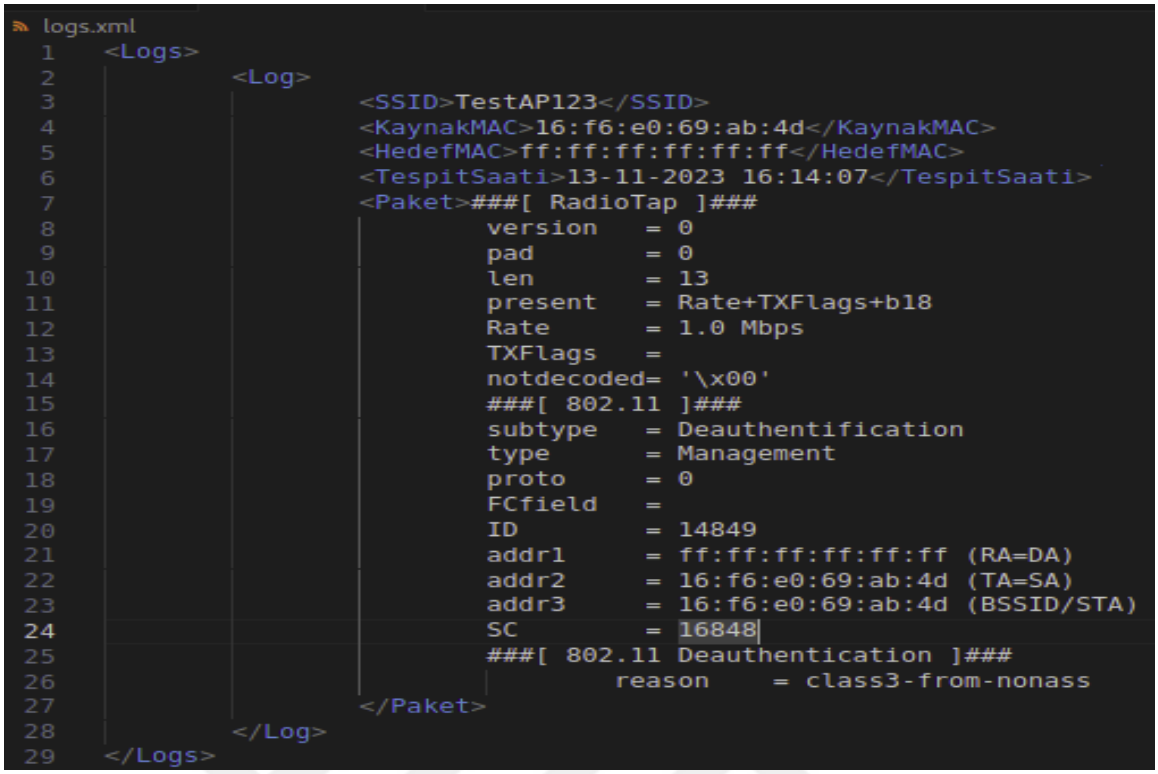


Şekil 3.36. Kullanıcı arayüzü.

Bu tasarımda, deney ortamında saldırı tespiti gerçekleştirilerek kablosuz ağ sahiplerine bilgi verilmesi amaçlanmıştır. Geliştirilen program arayüzünde "Kablosuz Ağ Listesi" sekmesinde listelenen ağlardan biri seçilerek "Korumayı Başlat" butonu ile saldırı tespiti için yazılım çalıştırılmıştır. Bu senaryolar bölüm 4'te açıklanmıştır.

Saldırı tespiti ve uyarı yazılımında, saldırı tespitini gerçekleştirmek için scapy kütüphanesi kullanılmıştır. Kullanıcı arayüzünde listelenen kablosuz ağlar arasından seçilen hedef kablosuz ağın benzersiz kimlik numarası olan BSSID bilgisini kullanarak, scapy kütüphanesi yardımıyla deauthentication paketleri tespit edilmektedir. Saldırgan sayısı fark etmeksizin tespit edilen deauthentication paketlerinin yayınlanma sıklıkları incelenmekte ve belirli bir sıklığın üstüne çıkılması durumunda, bu durum bir anomali olarak değerlendirilmektedir. Ardından kullanıcıya yazılı ve sesli olarak uyarı mesajı verilmektedir.

Saldırı tespit ve uyarı yazılımı, saldırı tespitini gerçekleştirdikten XML formatında sonra log (günlük) dosyası oluşturarak saldırı sonrası analizleri kolaylaştırmaktadır. Bu log dosyasının içerisinde saldırının hangi erişim noktasına yapıldığı gibi bilgiler ve meta veriler bulunmaktadır. Şekil 3.37'de log dosyasının içeriği görülmektedir.



Şekil 3.37. Log kayıt dosyası içeriği.

3.3.5 Harici Kablosuz Ağ Kartı Kullanılması

Kablosuz ağlara yönelik ağdan düşürme saldırıları uzmanlık bilgisi gerektirmeyen ve açık kaynak kodlu yardımcı yazılımlar ile basitleştirilmiş olmasından dolayı oldukça tehlikelidir. Ayrıca bu saldırıların gerçekleştirilebilmesi için kablosuz ağ kartının monitör mod destekli olması gerekmektedir. Bu nedenle günümüzde kablosuz ağ kartı üretici firmaları bilgisayarlarda yerleşik olan kablosuz ağ kartlarında monitör mod desteğini kaldırmışlardır. Ancak bazı eski kablosuz ağ kartlarında ve bu iş için özel olarak tasarlanmış kablosuz ağ kartlarında monitör mod desteği bulunmaktadır. Bu nedenle ağdan düşürme saldırıları güncelliğini korumaktadır. Saldırıların simüle edilebilmesi ve tespitinin gerçekleştirilebilmesi için monitör mod destekli kablosuz ağ kartı kullanılmıştır. Şekil 3.38'de deney ortamında kullanılan TP-Link marka ve TL-WN722N model monitör mod destekli kablosuz ağ kartı görülmektedir.

Şekil 3.38. TP-Link TL-WN722N kablosuz ağ kartı.

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Tez çalışmasında materyal ve yöntemleri açıklanan sistemler kullanılarak bir deney ortamı kurulmuştur. Deney ortamı kurulurken kullanılan sistemlerdeki donanım ve yazılım araştırmaları, kurulumları, denemeleri ve uygulamaları yapılmıştır. Araştırması yapılan ve uygulanabilir sonucuna varılan Ağdan Düşürme Saldırılarına Karşı Tespit ve Uyarı Yazılımına ait kaynak kodları EK-5 ve EK-6'da verilmiştir.

Gerçekleştirilen deney sistemine göre yapılanlar aşağıda listelenmiştir:

1. Deney düzeneğinde hedef erişim noktasını temsil eden ve gerçek kullanıcıların olmadığı bir kablosuz ağ donanımı kullanılmıştır.
2. Hedef erişim noktasına Android işletim sistemine sahip bir mobil cihaz bağlanmıştır.
3. Bir dizüstü bilgisayar ağdan düşürme saldırısını simüle etmek için ayarlanmıştır.
4. Başka bir dizüstü bilgisayar ise geliştirilen saldırı tespit ve uyarı yazılımının çalışması için ayarlanmıştır.
5. Genel olarak yukarıdaki kontrollerin haricinde tez projesinin amaçlarını yerine getirecek birtakım senaryolar oluşturularak denenmiştir. Bunlar;
    - Hedef erişim noktasına düzenlenen ağdan düşürme saldırısının tespitinin gerçekleştirilmesi ve ağ sahiplerine bilgi verilmesi,
    - Hedef erişim noktasına benzer sahte erişim noktasının oluşturulması ve istemci cihazın sahte erişim noktasına bağlanmalarının sağlanması,
    - Sahte erişim noktası üzerine hedef erişim noktasının ağ şifresini talep eden captive portal kurulması örnek uygulamaları yapılmıştır.

Gerçekleştirilen deney ortamı Şekil 4.1'de görülmektedir.

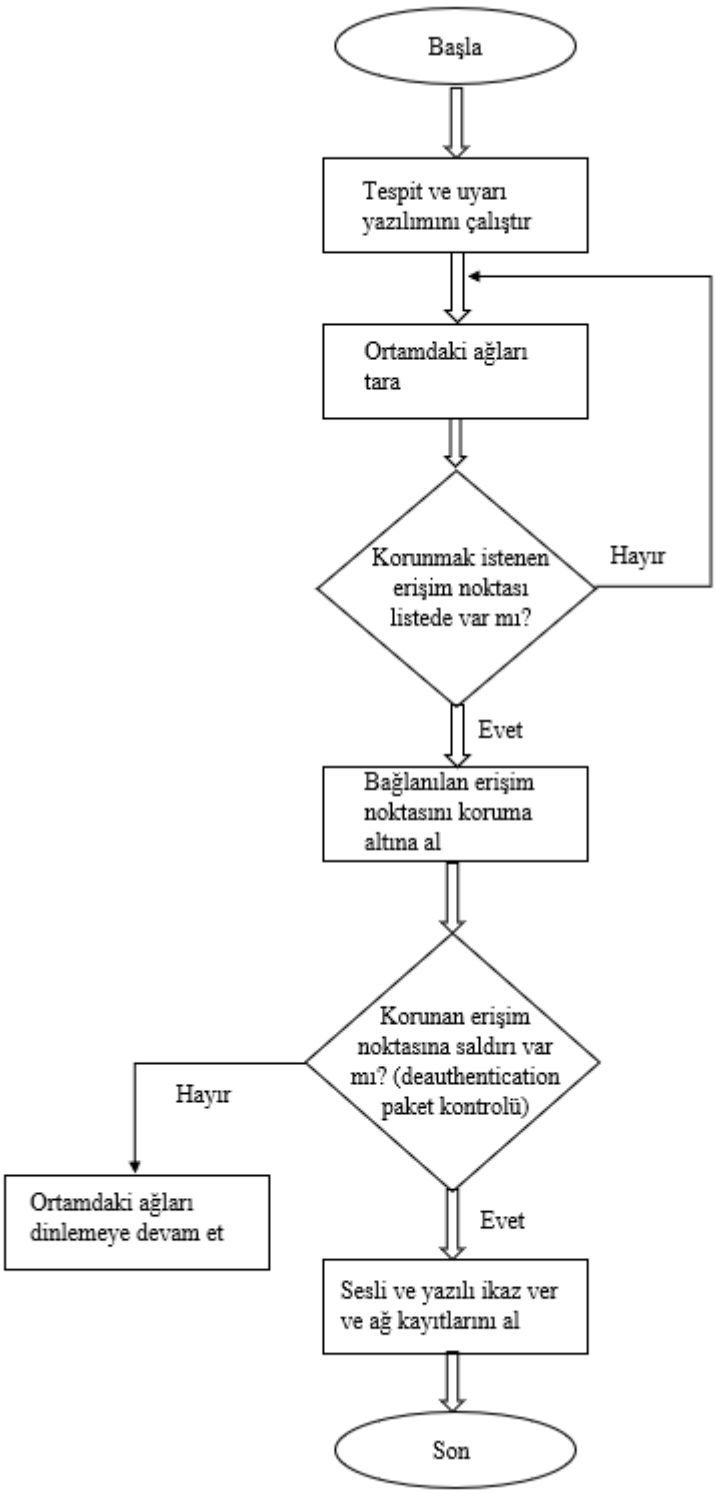
Şekil 4.1. Projenin ilk testlerinin yapılması.

Ağdan düşürme saldırısını gerçekleştirmek amacıyla izlenen adımlar Şekil 4.2'de gösterilmiştir. Algoritması verilen saldırı mekanizmasının araçları ve yöntemi üçüncü bölümde anlatılmaktadır.

Şekil 4.2. Ağdan düşürme saldırı algoritması.

Saldırı deney ortamında kullanılan dizüstü bilgisayardan biriyle yapılmaktadır. Sonrasında ise deney ortamında kullanılan ikinci dizüstü bilgisayardan tespit ve uyarı yazılımı çalıştırılarak bağlanmak istediğimiz ağ koruma altına alınır. Tespit ve uyarı

yazılımına ait algoritma Şekil 4.3'te verilmiştir. Algoritması verilen koruma mekanizmasının araçları ve yöntemi üçüncü bölümde anlatılmaktadır.



Şekil 4.3. Tespit ve uyarı yazılımı algoritması.

Deauthentication işlemi, ağ cihazlarının otomatik olarak ve yöneticilerin ağ üzerindeki değişiklikleri sonucunda uygulanan bir pakettir. Fakat günümüzde kullanılan 802.11x Wi-Fi protokollerinin güvenlik açısından yetersiz yani zafiyetlerinin olmasından dolayı bu saldırı hedef kablosuz ağa dâhil olmadan, yalnızca hedef sistemin MAC adresini bilerek gerçekleştirilebilir.

Saldırı tespit ve uyarı yazılımı arayüzünde çevredeki tüm erişim noktaları listelenerek koruma altına alınmak istenen kablosuz ağ bu listeden seçilir. Seçilen erişim noktasına gönderilen deauthentication paketleri belirli bir süre içerisinde sık olarak geliyorsa geliştirilen yazılım, bu durumu anormal bir durum olarak değerlendirerek yazılı ve sesli olarak seçilen erişim noktasına saldırı olduğu uyarısını yapmaktadır. Bu durumda bilgisayar korsanları amaçlarına ulaşamadan saldırının fark edilmesi sağlanır.

Geliştirilen tespit ve uyarı yazılımıyla saldırıların önüne geçebilir ve sonraki saldırı yöntemleri engellenebilir. Sinyal izleme tabanlı anomalilerin algılanması, kablosuz ağlardan düşürme saldırılarına karşı etkili bir önlem olarak öne çıkmaktadır. Anomalilerin tespit edilmesi ve engellenmesi, kablosuz ağların güvenliğinin sağlanması için hayati bir adımdır. Kablosuz ağlardaki düşürme saldırılarına karşı korunma, sinyal izleme temelli yöntemlerin hassasiyeti ve hızıyla doğrudan ilişkilidir. Geliştirilen bu yazılım, günün farklı zamanlarında aynı anda 10 adete kadar erişim noktasının aktif olduğu ev ortamında denenmiş ve yaklaşık 0,5-2 saniye arasında bir algılama süresinde sesli ve yazılı ikaz vererek tespit ve uyarı yazılımının kullanıcı dostu olduğu gözlemlenmiştir.

Kablosuz ağlar için geliştirilen WEP, WPA, WPA2 ve WPA3 gibi farklı güvenlik mekanizmalarına rağmen saldırı için birçok yol vardır. Bilgisayar korsanları bu güvenlik açıklarından yararlanılarak kablosuz ağlara saldırılar yapmaktadır. Kablosuz ağlarda zayıflıklar, sistemin tasarımı esnasında gözden kaçan sistem tasarımının bir parçası olan donanım veya yazılım kusurlarını kapsamaktadır. Yapılan bu tez çalışmasında siber güvenliğin ne kadar önemli olduğunu vurgulamak ve alınabilecek tedbirlere yönelik bir farkındalık oluşturmak amaçlanmıştır. Günümüzde kablosuz ağlara olan talebin artması sonucu onları daha güvenli hale getirmek için bilimsel araştırmalar devam etmektedir. Bu saldırıları gerçekleştirmek için birçok yöntem ve araç mevcuttur.

4.1 Kali Linux Kullanmanın Avantajları

Kali Linux işletim sistemi, kablosuz ağlara yönelik ağdan düşürme saldırıları yapmak ve yönetmek için çeşitli yazılımlarla donatılmıştır. Kablosuz ağ kartını monitör moda olmak, sahte erişim noktaları oluşturmak ve diğer saldırı yöntemlerini simüle etmek gibi oldukça karmaşık ve zorlu görevleri basitleştirmiştir. Ağdan Düşürme Saldırılarına Karşı Tespit ve Uyarı Yazılımın geliştirilmesi için kullanılan Python kütüphanelerinin yüklü olması yazılım geliştirme sürecini hızlandırmıştır. Ayrıca içerisinde barındırdığı airmon-ng saldırı kiti ve ağ yönetimi yazılımları ile saldırı simülasyonu oluşturmayı daha kolay hale getirmiştir.

5. SONUÇLAR VE ÖNERİLER

Siber saldırılar bugün tartışmasız çok önemli bir konudur ve önümüzdeki yıllarda da zorlu bir sorun olmaya devam edecektir. Kullanıcıları ve geliştiricileri, teknolojilerin güvenliği konusunda eğitmek önemlidir. Siber alemdeki kullanıcıların hem siber savunma yetenekleri hem de siber saldırı yetenekleri hakkında sağlam bir anlayışa sahip olması gerekir. Bir siber saldırının etkisi, kademeli olarak büyük yankılara sahip olabilir. Günümüzde teknolojiye bu kadar çok güven duyulduğu için, toplumun her kesimi etkili bir şekilde tehlikeli koşullara girebilir. Finansal kurumlar, sağlık hizmetleri, eğitim kurumları devlet hizmetleri, enerji hizmetleri ve çok daha fazlası bir ağa bağlı- küresel erişimli bir ağ bağlantılıdır. Yaşamsal hizmetlerini korumak ve korunmak için sürekli olarak siber saldırılar hakkında kullanıcıların eğitilmesi zorunluluk haline gelmiştir. İnternetin kullanımının genişlemesi, teknolojinin gelişmeye devam etmesi, kişisel ve hassas bilgilere sızan bilgisayar korsanları, toplumun her kesiminde, işletmelerde ve hatta devlet kurumlarında endişe oluşturmaktadır. Siber saldırılar, dünyanın dört bir yanındaki ülkelerde her gün aralıksız olarak gerçekleşmektedir. Siber tehditlere karşı koruma sağlamak için; yasalar oluşturmak ve güvenlikli ağ mimarileri tasarlamak, tüm kullanıcılar için eğitim ve öğretime kadar birden fazla eşzamanlı boyutta çok önemlidir (Hatipoğlu ve Tunacan, 2021).

Bu çalışmada kablosuz ağ kartı ile hedef erişim noktasına ait trafiği izleyip, işleyip ve ağdan düşürme saldırılarının tespit edilebileceği anlatılmıştır. Siber güvenlik dünyasını doğrudan ilgilendiren bir konu olduğu için hiçbir zaman önemini yitirmeyeceği ve gelişen teknoloji ile birlikte oluşan zafiyetlerin sömürülmesine karşı tespit ve savunma araçlarının geliştirilmesinin önemi görülmektedir.

Kablosuz ağlarda kullanılan güvenlik anahtarları adından da anlaşılacağı üzere ağa dahil olmak isteyen yetkisiz kişileri engellemek amacıyla kullanılmaktadır. Bu nedenle deauthentication saldırısı için bir koruma sağlamazlar.

Güvenlik duvarları kablolu ve kablosuz ağa dahil olan istemci cihazların ağ paketlerini filtrelemek üzere geliştirilmiş yazılımlar olması nedeniyle deauthentication saldırılarına karşı bir önlem olarak kullanılamazlar. Çünkü deauthentication saldırıları ağa dahil olmadan yapılmaktadır.

Antivirüs yazılımları istemci cihazların işletim sistemi üzerinde çalışan güvenlik yazılımları olması nedeniyle deauthentication saldırısına karşı bir koruma sağlamazlar.

Çünkü deauthentication saldırıları ağa dahil olmadan ve işletim sistemi üzerinde herhangi bir çalıştırılabilir zararlı yazılım kullanılmadan yapılmaktadır.

Bu uygulama çalışması, kablosuz ağ güvenliği çalışmalarına önemli bir katkı sağlamak amacıyla gerçekleştirilmiştir. Ayrıca siber güvenlik araştırmalarında sıkça kullanılan Kali Linux işletim sistemi ve güvenlik araçlarının geliştirilmesinde önemli bir role sahip olan Python programlama dili anlatılarak bu konularda çalışacaklara önemli bir kaynak oluşturulmuştur. Kablosuz ağlara yönelik ağdan düşürme saldırılarını tespit eden ve saldırıyı fark ederek engellemek için uyarılarda bulunan yazılım başarıyla gerçekleştirilmiştir.

Geliştirilen tespit ve uyarı yazılımıyla saldırıların önüne geçilebilir ve sonraki saldırı adımları engellenebilir. Yazılım sayesinde sivil ve askeri alanlardaki ağlarda veri sızıntıları engellenebilir. Kablosuz ağ cihazlarına entegre edilebilir, harici saldırı tespit donanımları geliştirilebilir ve saldırıların raporlanması sağlanabilir. Kablosuz ağ yöneticileri bilgilendirilerek dolandırıcılık faaliyetlerinin önüne geçilebilir. İnternet kullanıcılarının bu konularda bilgilendirilmesine imkan oluşturabilmek adına bu çalışmada olduğu gibi korunmayı amaçlayan yazılımların geliştirildiği akademik çalışmaların sayısı artırılmalıdır.

KAYNAKLAR

Abdulkareem, M., 2012, IEEE 802.11 Kablosuz Ağlarda Güvenlik, Yüksek Lisans Tezi, *Bilişim Enstitüsü*, Ankara Gazi Üniversitesi, Bilgisayar Bilimleri Anabilim Dalı.

Akbaş, E., 2015, Penetrasyon Çalışmalarında Kablosuz Ağ Güvenlik Testleri, https://www.bgasecurity.com/makale/penetrasyon-calismalarinda-kablosuz-ag-guvenlik-testleri/, [Son erişim 26.10.2023].

Altınok, B., 2017, Kablosuz Ağ Güvenliği, *Abaküs Yayın Dağıtım Hizmetleri*, İstanbul, 2- 78.

Angin, P., 2020, Blockchain-Based data security in military autonomous systems. *Avrupa Bilim ve Teknoloji Dergisi*, Özel Sayı, 362-368.

Anonim, 2024, https://www.tp-link.com/tr/wpa3/ [Son Erişim 07.06.2024].

Anonim, 2021, Ozztech Bilgi Güvenliği ve Yazılım Limited Şirketi, https://www.ozztech.net/siber-guvenlik/deauth-attack-nedir/ [Son erişim 26.10.2023].

Anonim, 2023, Turknet, https://turk.net/blog/kablosuz-aglara-yapilabilen-siber-saldirilar-nelerdir/, [Son erişim 17.05.2024].

Anonim, 2009, Endüstriyel Otomasyon Teknolojileri, Sunucu Servisleri 2, T.C. Millî Eğitim Bakanlığı, Ankara, 3.

Anonim, 2014, Bilişim Teknolojileri, Ağ Hizmetlerinin Yönetimi, T.C. Millî Eğitim Bakanlığı, Ankara, 3-5.

Anonymous, 2021, Annual Report 2020, https://www.wi-fi.org/system/files/Wi-Fi_Alliance_2020_Annual_Report.pdf, [Son erişim 26.10.2023]

Anonymous, 2020, Annual Internet Report 2018-2023, https://www.cisco.com/content/en/us/solutions/collateral/executive perspectives/annual-internet-report/white-paper-c11-741490.pdf, [Son erişim 26.10.2023].

Anonymous, 2022, Airodump-ng, https://aircrack-ng.org/doku.php?id=airodump-ng, [Son erişim 26.10.2023].

Anonymous, 2022/a, Aireplay-ng, https://aircrack-ng.org/doku.php?id=aireplay-ng, [Son erişim 26.10.2023].

Anonymous, 2022/b, Airbase-ng, https://aircrack-ng.org/doku.php?id=airbase-ng, [Son erişim 26.10.2023].

Anonymous, 2022, Deauth Attack Nedir, https://www.ozztech.net/siber-guvenlik/deauth-attack-nedir/, [Son erişim 26.10.2023].

Dilben, A. E., 2020, https://ahmetemindilben.com.tr/kali-linux-nedir-temel-kali-linux-kullanimi-2020-2/, [Son erişim 04.06.2024].

Erkınay, Z. M., 2005, Kablosuz Ağlar (Wireless Networks) ve Kablosuz Ağlarda Güvenlik, Yüksek Lisans Tezi, *Fen Bilimleri Enstitüsü*, Yüzüncü Yıl Üniversitesi, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Van.

Gezgin, D. M., Buluş E., 2012, Kablosuz Ağların Güvenlik Açıklarının Eğitim Amaçlı İncelenmesi İçin Uygulama Tasarımı, *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, Cilt 2 Sayı 1 (127-135), Trakya Üniversitesi, Edirne.

Hamzah M., 2017, Developing A Method To Protect Attacks In Wireless Networks, Yüksek Lisans Tezi, *Fen Bilimleri Enstitüsü*, Erciyes Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı.

Hatipoğlu ve Tunacan, 2021, Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması, *BŞEÜ Fen Bilimleri Dergisi*, 8(1), 430-445.

Hammand, J., Kessler, B., Rivero, J., Skinner, C., Sweeney, T., 2003. Wireless Hotspot Deployment Guide, *Mobile Platfroms Group-WVP*: 32-49.

Kancura, N., 2022, Otomobillerdeki Android Temelli Multimedya Cihazlarının Güvenlik Zafiyetleri, Yüksek Lisans Tezi, *Fen Bilimleri Enstitüsü*, Sakarya Üniversitesi, Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı.

Kelley, S., 2001, Dnsmasq, https://thekelleys.org.uk/dnsmasq/doc.html, [Son erişim 26.10.2023]

Kösem, M., 2016, Kablosuz Ağ Standartlarının Karşılaştırılması ve 802.1x Standardı İle Bir üniversitede Kablosuz Ağ güvenliği Tasarımı, Yüksek Lisans Tezi, *Fen Bilimleri Enstitüsü*, İstanbul Aydın Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı.

Kula, G. Ç., 2009, Gelişmiş Şifreleme Standardı Blok Şifreleme Algoritmasının Bir Mikroişlemci Üzerinde Gerçeklemesine Yan Kanal Saldırısı, Yüksek Lisans Tezi, *Fen Bilimleri Enstitüsü*, İstanbul Teknik Üniversitesi, Elektronik ve Haberleşme Mühendisliği Ana Bilim Dalı.

Sontowski, S., 2022, Exploratıon And Detectıon Of Denıal-Of-Servıce Attacks On Cyber-Physıcal Systems, Degree Master Of Science, Tennessee Technological University.

Söğüt, E. & Erdem, O.A., 2020, Endüstriyel kontrol sistemlerine (SCADA) yönelik siber terör saldırı analizi, *Journal of Polytechnic*, 23(2), 557-566.

Taş, O. ve Kiani, F., 2021, Nesnelerin İnterneti (Iot) ve Kablosuz Algılayıcı Ağların Güvenliğine Yapılan Saldırıların Tespit Edilmesi ve Önlenmesi, *Politeknik Dergisi*, 24 (1): 219-235.

Uzun E., 2024, https://erdincuzun.com/ileri-python/tkinter-gui, [Son erişim 04.06.2024]

Yüksel, O., 2021, 802.11AC Ortamında Makine Öğrenmesi Yaklaşımları ile Donanım Tabanlı Saldırı Tespit Sistemi ve 802.11S Örgü Ağlarına Yönelik Saldırı Gerçeklemeleri, Yüksek Lisans Tezi, *Fen Bilimleri Enstitüsü*, TOBB Ekonomi ve Teknoloji Üniversitesi, Elektrik-Elektronik Mühendisliği Anabilim Dalı.

EKLER

EK-1
4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA Başlığı Linkleri

- A : https://archive.kali.org/kali-images/kali-2023.2/kali-linux-2023.2a-installer-amd64.iso

EK-2
Airodump-ng Aracı Parametreleri

A) Kullanılabilir Parametreler

Parametre	Açıklama
-i	Kullanılacak ağ kartını tanımlamak için kullanılır.
-w	Yakalanan paketleri kaydetmek amacı ile kullanılır.
-f [zaman]	Kanallar arasında geçiş yaparken geçecek süre belirtilir.
--manufacturer	OUI veritabanı kontrol edilerek üretici firmalar gösterilir.
--uptime	Erişim noktasının aktif olduğu süreyi verir.
--output-format	Toplanan verileri daha sonra kullanmak veya incelemek amacıyla izin verilen formatlarda (pcap, csv, kistmet, netxml) bir dosyaya yazar.

Kaynak: (Anonymous, 2022)

B) Kullanılabilir Filtreler

Filtre	Açıklama
--wps	WPS korumalı ağları listeler.
--encrypt	Şifreleme tipine göre listeler.
--bssid	Belirli bir erişim noktası için bilgi toplar.
--essid-regex [regex]	Kablosuz ağ isimlerinde belirtilen kritere uyan erişim noktalarını gösterir.
--essid [ssid]	Kablosuz ağ ismine göre bilgi toplar.
-a	İlişkilendirmeyi tamamlayan istemcileri filtreler.
--channel	Belirli bir kanal numarasına göre bilgi toplar.
-C	Belirli bir frekans numarasına göre bilgi toplar.

Kaynak: (Anonymous, 2022)

C) Çıktıların Yorumlanması

Alan	Açıklama
Probe	Aynı satırdaki STATION kolonundaki cihazın bağlanmak için probe request paketi gönderdiği ağı gösterir.
BSSID	Erişim noktasının MAC adresini ifade eder.
STATION	Erişim noktasına bağlı istemcinin MAC adresini ifade eder.
Beacons	Erişim noktaları tarafından yayılan toplam paket sayısını gösterir.
CH	Erişim noktasının yayın için kullandığı kanal numarasıdır.
CIPHER	Ağdaki verileri şifrelemek için kullanılan algoritmadır.
AUTH	Ağa bağlanmak için kullanılan kimlik doğrulama tipini gösterir.
ESSID	Yayın yapan erişim noktasının adıdır.
ENC	Kullanılan 802.11 güvenlik standardını ifade eder.
Packets	İstemci tarafından gönderilen data paketlerinin sayısını gösterir.

Kaynak: (Anonymous, 2022)

EK-3
Aireplay-ng Aracı Parametreleri

A) Kullanılabilir Filtreler

Filtre	Açıklamalar
-d	Hedef MAC adresi.
-s	Kaynak MAC adresi.
-m	Minimum paket boyutu.
-n	Maksimum paket boyutu.
-b	Erişim noktasının MAC adresi.
-c	Erişim noktasına bağlı istemcinin MAC adresi.
-h	Saldırı yaparken görünecek MAC adresi.
-e	Erişim noktasının SSID bilgisi.
-x	Saniyede gönderilecek paket sayısı.

Kaynak: (Anonymous, 2022/a)

B) Saldırı Modları

Saldırı Tipi	Saldırı Modu	Açıklama
--deauth	-0	Deauthentication saldırısı.
--fakeauth	-1	Sahte Authentication saldırısı.
--interactive	-2	Interactive Packet Replay.
--arpreplay	-3	ARP Request Replay saldırısı.
--chopchop	-4	KoreK chopchop saldırısı.
--fragment	-5	Fragmentation saldırısı.
--caffe-latte	-6	Cafe-Latte saldırısı.
--cfrag	-7	Client-oriented Fragmentitation saldırısı.
--migmode	-8	WPA Migration Mode.
--test	-9	Injection test.

Kaynak: (Anonymous, 2022/a)

EK-4
Airbase-ng Aracı Parametreleri

A) Kullanılabilir Parametreler

Parametre	Açıklama
-a	Oluşturulacak erişim noktasının MAC adresi.
-i	Kullanılacak kablosuz ağ artını ifade eder.
-w	Oluşturulan WEP korumalı kablosuz ağlar için bir WEP şifresi tanımlanır.
-h	Kaynak MAC adresi.
-q	Ekranda herhangi bir istatistik göstermez.
-v	Ekrana daha fazla bilgi basmak için kullanılır
-c	Erişim noktası için kanal numarası tanımlanır.
-X	Gizli SSID tanımlamak için kullanılır.
-L	Cafe-Latte saldırıları için kullanılır.
-N	Cfraf (Hirte) saldırısı için kullanılır.
-z	Oluşturulacak erişim noktasının şifreleme standardını ifade eder (1=WEP40, 2=TKIP, 3=WRAP, 4=CCMP, 5=WEP104)
-Z	WPA2 ağlar için kullanılır.
-F [dosya ismi]	Gelen giden paketlerin kayıt altında tutulacağı bir dosya tanımlanır. Sahte erişim noktası için tüm aktiviteler kaydedilir.
-I	Oluşturulacak erişim noktalarının Beacon paketi yayma aralığı belirlenir.
-P	Gönderilen Probe isteklerinin hepsine cevap verir.
-C	Probe paketlerine kaç saniyede cevap verileceği belirlenir.

Kaynak: (Anonymous, 2022/b)

EK-5
Scapy Deauthentication Paket Yakalama ve Analiz Kodları

```
# Gerekli modülü içe aktar
from scapy.all import *

def deauth_paket_yakala(packet):
    if packet.haslayer(Dot11):
        # Sadece yönetim çerçevelerini yakala
        if packet.type == 0:
            # Yalnızca Deauth çerçevelerini yakala
            if packet.subtype == 12:
                source_mac = packet.addr2
                target_mac = packet.addr1
                print(f"Deauth Paketi Yakalandı")
                print(f"Kaynak MAC Adresi: {source_mac}")
                print(f"Hedef MAC Adresi: {target_mac}")

# Ağ trafiğini dinlemek için kullanılacak ağ arayüzü
interface = "wlan0mon"

# Paket yakalama işlemini başlat
sniff(iface=interface, prn=deauth_paket_yakala)
```

EK-6
Saldırı Tespit ve Uyarı Yazılımı Kodları

```
# Python gerekli modüller.
from tkinter import *
from tkinter import messagebox
import tkinter.ttk as ttk
import subprocess
from pygame import mixer
from scapy.all import *
import xml.etree.ElementTree as ET
from datetime import datetime

# Default başlık ve buton metinleri
rootDefaultTitle = "Deauth Tespit ve Uyarı Yazılımı"

protectButtonDefaultTitle = "Korumayı Başlat"

# Ana pencereyi oluştur
root = Tk()

# Pencere boyutu ve yeniden boyutlandırılabilirliği ayarla
root.geometry("500x300")

root.resizable(FALSE, FALSE)

root.title(rootDefaultTitle)

# Global değişkenler

# Tarama sonucunda bulunan kablosuz ağ listesi
apList = []

# Sniffing işleminin devam edip etmediğini kontrol etmek için
sniffingRun = False

# Deauthentication paket sayısını tutmak için
deauthPacketCount = 0

# Alarm ayarları
mixer.init()

mixer.music.load("./beep.mp3")
```

```
def LogXML(sourceMAC, targetMAC, captureTime, packetContent):
    # Dosyanın zaten var olup olmadığını kontrol et
    if os.path.exists("logs.xml"):
        # Eğer dosya varsa, onu aç ve root elementini al
        tree = ET.parse("logs.xml")
        root = tree.getroot()
    else:
        # Eğer dosya yoksa, yeni bir root elementi oluştur
        root = ET.Element("Logs")
        tree = ET.ElementTree(root)

    # Yeni log girişi oluştur
    log = ET.Element("Log")

    childAP = ET.SubElement(log, "SSID")
    childAP.text = combobox.get()

    childSourceMAC = ET.SubElement(log, "KaynakMAC")
    childSourceMAC.text = sourceMAC

    childTargetMAC = ET.SubElement(log, "HedefMAC")
    childTargetMAC.text = targetMAC

    childCaptureTime = ET.SubElement(log, "TespitSaati")
    childCaptureTime.text = captureTime

    childPacketContent = ET.SubElement(log, "Paket")
    childPacketContent.text = packetContent

    # Yeni log girişini root'a ekle
    root.append(log)

    # Değiştirilmiş XML dosyasını kaydet
    tree.write("logs.xml")

    print("[+] Log Kaydedildi.")

# Monitor modunu etkinleştiren fonksiyon
def EnableMonitorMode():
    try:
        subprocess.run([
            "airmon-ng",
            "start",
            "wlan0"
        ], check=True)

        print("[+] Kablosuz arayüz başarıyla monitör moduna alındı.")

    except subprocess.CalledProcessError as error:
```

```
        print(f"[-] EnableMonitorMode Function: {error}")

# Kablosuz ağları taramak için fonksiyon
def ScanAP():
    global apList

    EnableMonitorMode()

    packets = sniff(
        iface="wlan0mon",
        timeout=10,
        filter="type mgt subtype beacon"
    )

    for packet in packets:
        if packet.haslayer(Dot11Beacon):
            bssid = packet[Dot11].addr3

            ssid = packet[Dot11Elt].info.decode("utf-8")

            apInfo = {
                "SSID": ssid,
                "BSSID": bssid
            }

            if apInfo not in apList:
                apList.append(apInfo)

    ssidList = ""

    for ap in apList:
        ssid = ap["SSID"]

        ssidList = ssidList + " " + ssid

    combobox["values"] = ssidList

    messagebox.showinfo("Bilgi", "Tarama Tamamlandı.")

# Seçilen kablosuz ağın BSSID'sini almak için fonksiyon
def GetSelectedApBSSID():
    global apList

    selectedApSSID = combobox.get()
    for ap in apList:
        if ap["SSID"] == selectedApSSID:
            return (ap["BSSID"]).upper()

# Deauthentication paketlerini tespit etmek için fonksiyon
def DetectDeautPacket(pkt):
```

```
    global deauthPacketCount

    try:
        if pkt.haslayer(Dot11):
            if pkt.type == 0 and pkt.subtype == 12:
                if (pkt.addr2).upper() == GetSelectedApBSSID():
                    deauthPacketCount = deauthPacketCount + 1

                    statusText["text"] = "Durum: Saldırı Tespit Edildi!"

                    if deauthPacketCount == 1:
                        # Alarmı Başlat
                        mixer.music.play(loops=-1)

                        # Kaynak ve hedef MAC adreslerini al
                        sourceMAC = pkt.addr2
                        targetMAC = pkt.addr1

                        # Yakalama zamanını al
                        captureTime = datetime.fromtimestamp(pkt.time).strftime('%d-%m-%Y
%H:%M:%S')

                        # Paketin içeriğini hex formatında al
                        packetContent = pkt.show(dump=True)

                        # Saldırıyı Kaydet
                        LogXML(
                            sourceMAC,
                            targetMAC,
                            captureTime,
                            packetContent
                        )


    except Exception as error:
        print(f"[-] DetectDeautPacket Function: {error}")

# Sniffing işlemini başlatmak için fonksiyon
def SniffStart():
    sniff(
        iface="wlan0mon",
        prn=DetectDeautPacket,
        stop_filter=lambda x: not sniffingRun
    )

# Kablosuz ağı korumak için fonksiyon
def ProtectStart():
    global ThSniff
    global sniffingRun
```

```
    selectedApBSSID = GetSelectedApBSSID()

    if selectedApBSSID != None:
        protectButton["text"] = "Korumayı Durdur"
        protectButton["command"] = ProtectStop

        root.title(rootDefaultTitle + " - Korunan AP BSSID: " + selectedApBSSID)

        statusText["text"] = "Durum: Saldırı Yok"

        print("[+] AP Koruma Başladı. BSSID: " + selectedApBSSID)

        sniffingRun = True
        ThSniff = Thread(target=SniffStart)
        ThSniff.start()
    else:
        messagebox.showerror("Hata", "Lütfen bir kablosuz ağ seçin.")

# Korumayı durdurmak için fonksiyon
def ProtectStop():
    global sniffingRun
    global deauthPacketCount

    sniffingRun = False
    deauthPacketCount = 0

    ThSniff.join()

    mixer.music.stop()

    statusText["text"] = ""

    protectButton["text"] = protectButtonDefaultTitle

    protectButton["command"] = ProtectStart

    root.title(rootDefaultTitle)

    print("[+] AP Koruma Durduruldu.")

# İkonları yükle
malwareIcon = PhotoImage(file=r"malware.png")

protectIcon = PhotoImage(file=r"protect.png")

# Kablosuz ağları tarayan buton
scanButton = Button(
    compound=LEFT,
    text="Kablosuz Ağları Tara",
    height="55",
```

```
    width="20",
    image=malwareIcon,
    command=ScanAP
)

scanButton.grid(
    row=3,
    column=3,
    columnspan=2
)

scanButton.place(
    relx=0.5,
    rely=0.5,
    anchor=CENTER
)

scanButton.pack(
    side="top",
    fill="both",
    padx=4,
    pady=4
)

# Etiket çerçevesi
labelFrame = LabelFrame(text="")

labelFrame.pack(
    fill="both",
    expand="yes"
)

# Combobox başlığı
comboboxTitle = Label(
    labelFrame,
    text="Kablosuz Ağ Listesi"
)
comboboxTitle.pack()

# Combobox
combobox = ttk.Combobox(
    labelFrame,
    state="readonly"
)

combobox.set("Seçiniz")

combobox.pack()

# Saldırı bilgi metni
```

```
statusText = Label(
    labelFrame,
    text="",
    font=(
        "Verdana",
        14
    )
)

statusText.pack(
    side=TOP,
    pady=20
)

# Koruma butonu
protectButton = Button(
    compound=LEFT,
    text=protectButtonDefaultTitle,
    height="55",
    width="20",
    image=protectIcon,
    command=ProtectStart
)

protectButton.pack(
    side="top",
    fill="both",
    padx=4,
    pady=4
)

def WindowCloseRequest():
    global sniffingRun

    result = messagebox.askquestion("Uyarı", "Pencereyi kapatmak istiyor musunuz?")
    if result == 'yes':
        if sniffingRun == True:
            ProtectStop()

        root.destroy()


root.protocol("WM_DELETE_WINDOW", WindowCloseRequest)

# Pencere döngüsünü başlat
mainloop()
```