GAZİOSMANPAŞA BİLİMSEL ARAŞTIRMA DERGİSİ (GBAD)
Gaziosmanpasa Journal of Scientific Research
ISSN: 2146-8168
http://dergipark.gov.tr/gbad
Araştırma Makalesi (Research Article)

Cilt/Volume : 12
Sayı/Number: 2
Yıl/Year: 2023
Sayfa/Pages: 42-56

***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 GÖKREM[2]

[1]Tokat Gaziosmanpaşa Üniversitesi, Lisansüstü Eğitim Enstitüsü, Mekatronik Mühendisliği, Tokat, Türkiye.
**Sorumlu yazar: mekatronik_00@hotmail.com*
[2]Tokat 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 içerisinden 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. Kişiye 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 değerin DLOS8 ağ geçidine iletilmesi akabinde, ağ geçidinden de kullanıcı arayüzü olan Cayanne 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

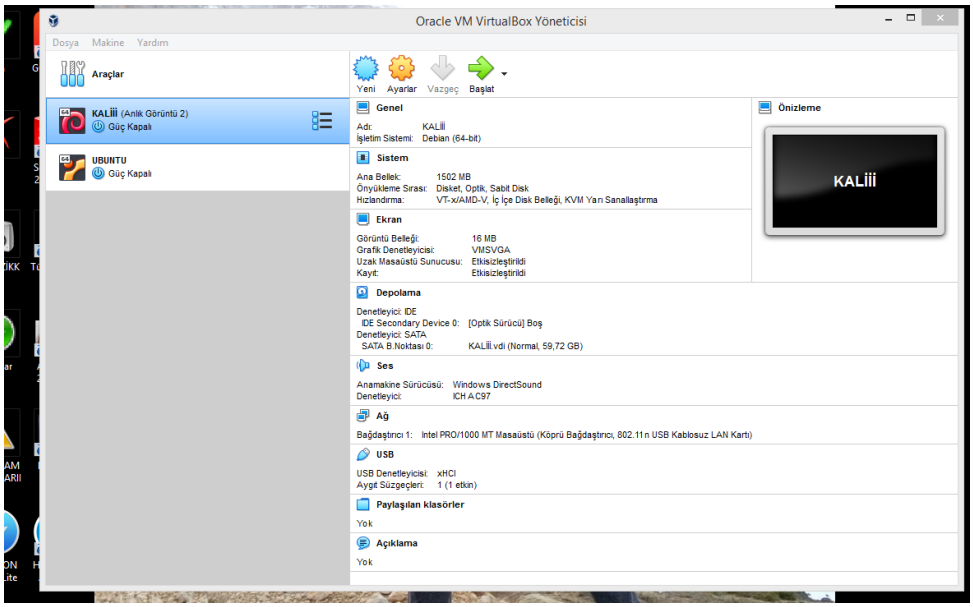
DLOS8 Ağ Geçidi: LHT65 sensörü tarafından gönderilen paketleri yakalayarak Cayanne MyDevices kullanıcı arayüzüne göndermektedir. Şekil 1'de ağ geçidi görseli ayrıntılı olarak verilmiştir.

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

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

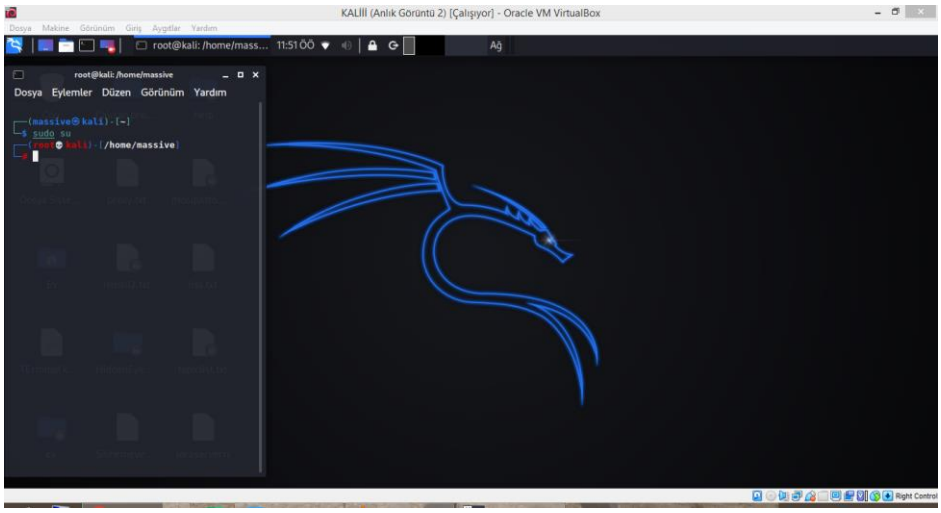
Şekil 2. LHT65 LoRaWAN sıcaklık ve nem sensörü
Figure 2. LHT65 LoRaWAN temperature and humidity sensor

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



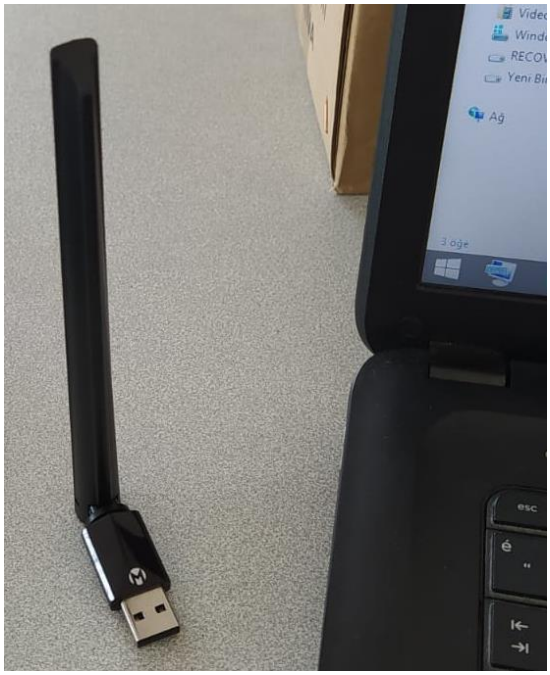
Şekil 3. Sanal Makine
Figure 3. Virtual Machine

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.

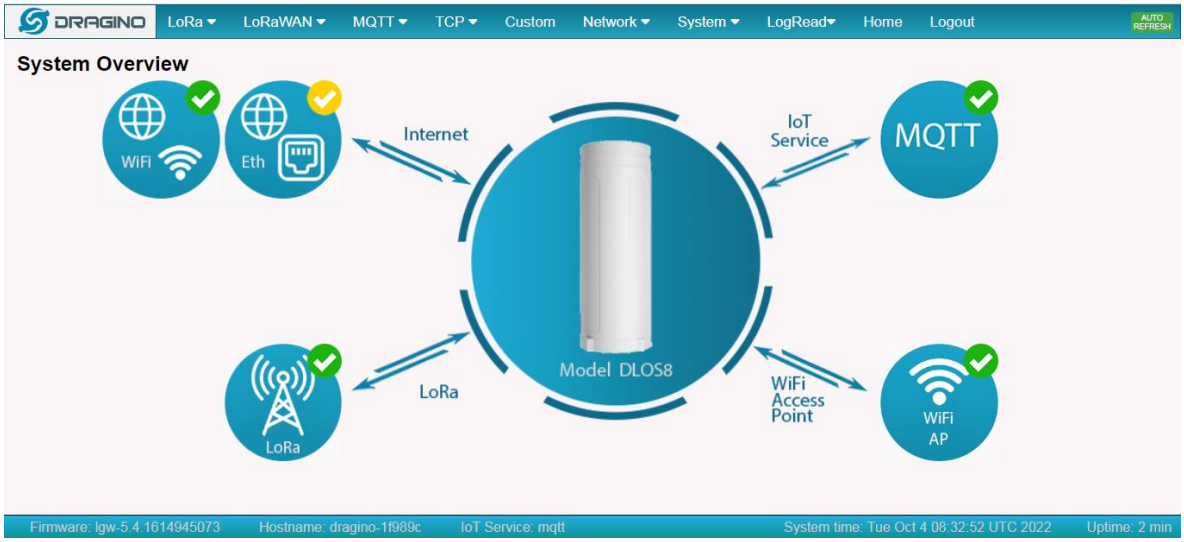


Şekil 5. Wi-fi Kartı
Figure 5. Wi-fi Card

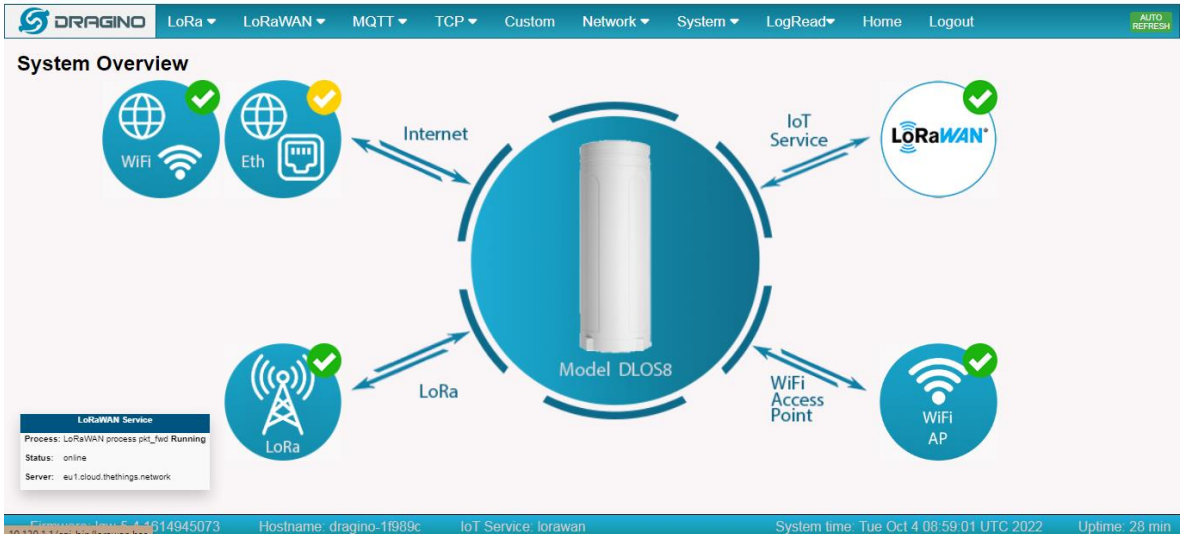
2.2. Yöntem

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 Cayanne myDevices

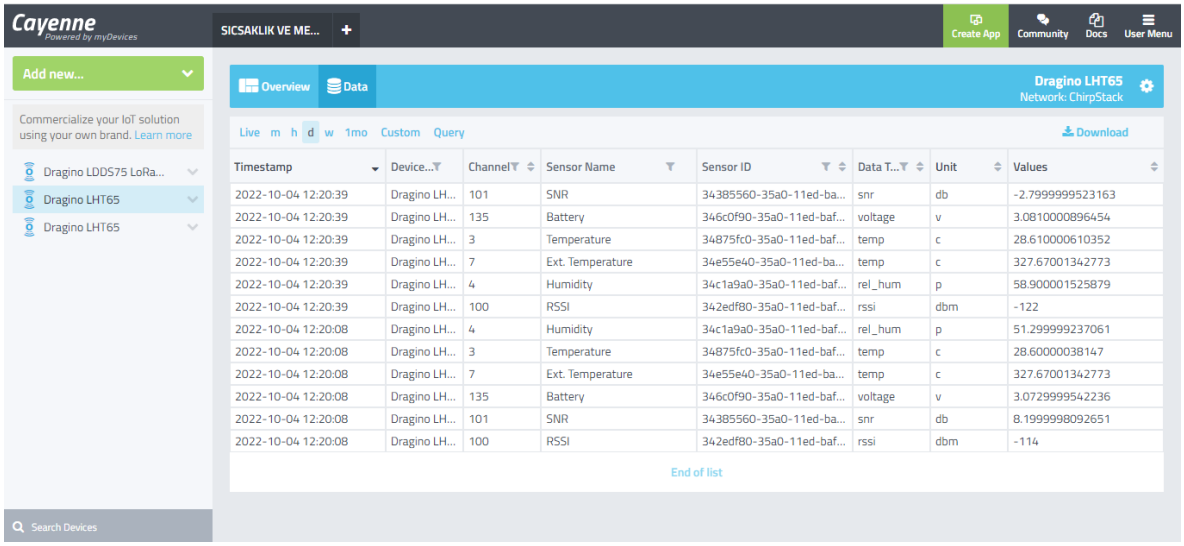
arayüzüne LHT65 sensöründen alınan paketler iletilmiştir. Alınan paketler Şekil 8 ve Şekil 9'da gösterilmektedir. Siber saldırı yapılacak uygulama sorunsuz çalışmaktadır.



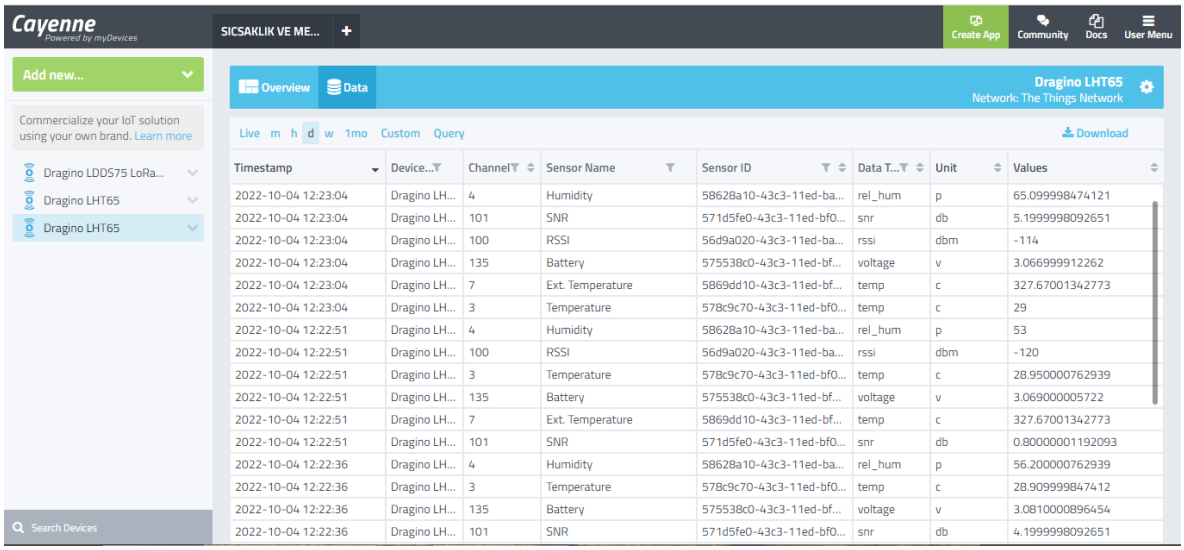
Şekil 6. MQTT Bağlantısı
Figure 6. MQTT Connection



Şekil 7. UDP Bağlantısı
Figure 7. UDP Connection

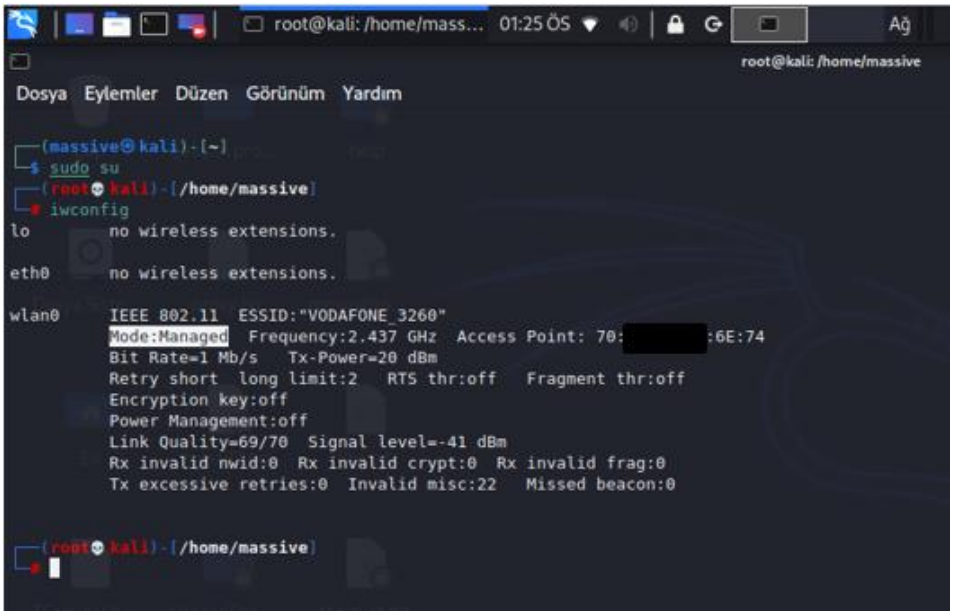


Şekil 8. MQTT Kullanarak Alınan Paketler
Figure 8. Packets Received Using MQTT

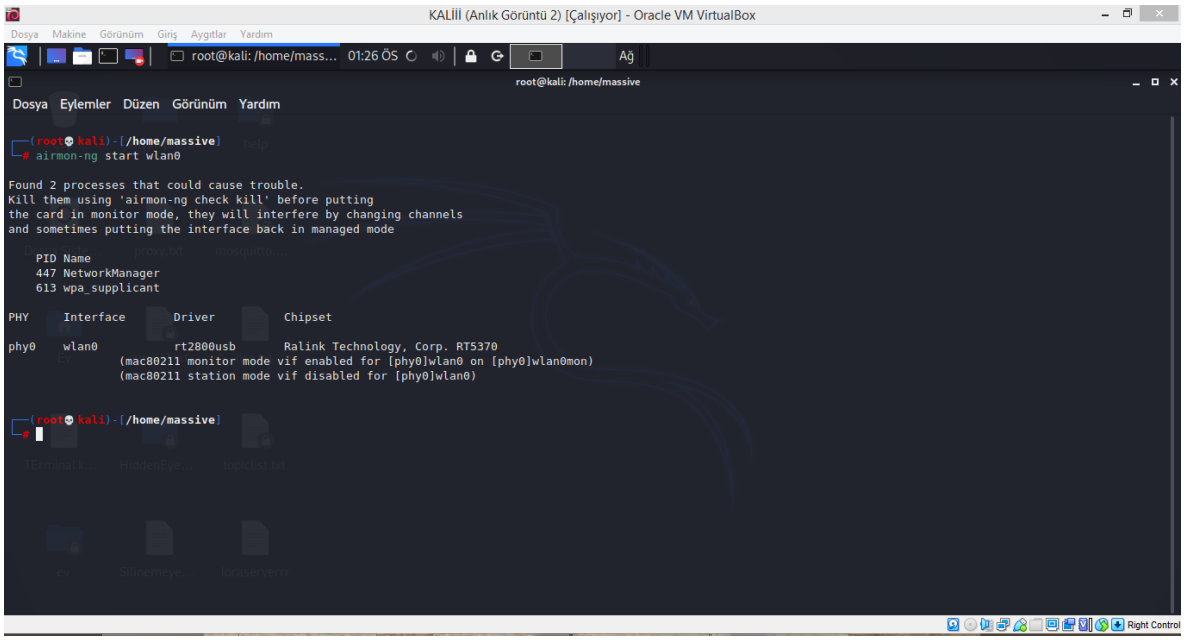


Şekil 9. UDP Kullanarak Alınan Paketler
Figure 9. Packets Received Using UDP

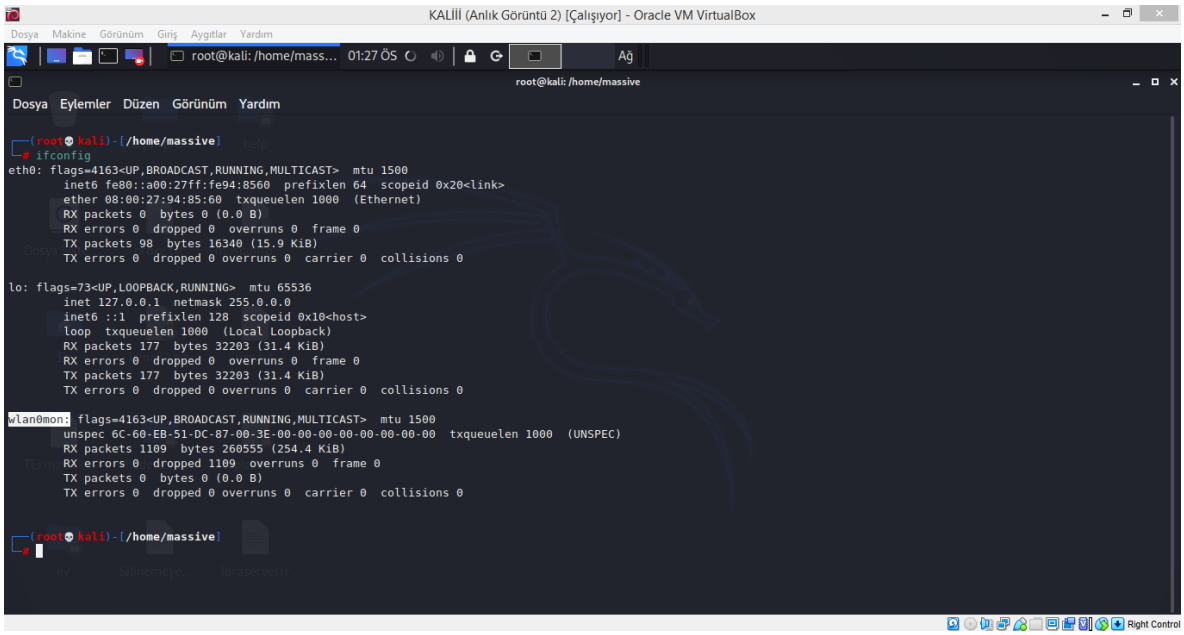
Siber Saldırı Sistemi Kurulumu: Şekil 10'da sistemin hangi modda çalıştığı kontrol edilmiştir. Daha sonra Şekil 11'de verildiği gibi ilk olarak saldırı işlemlerinin yapılabilmesi için terminale 'airmon-ng start wlan0' kodu girilerek sistem managed moddan monitör moda alınmıştır. Terminale 'ifconfig'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



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

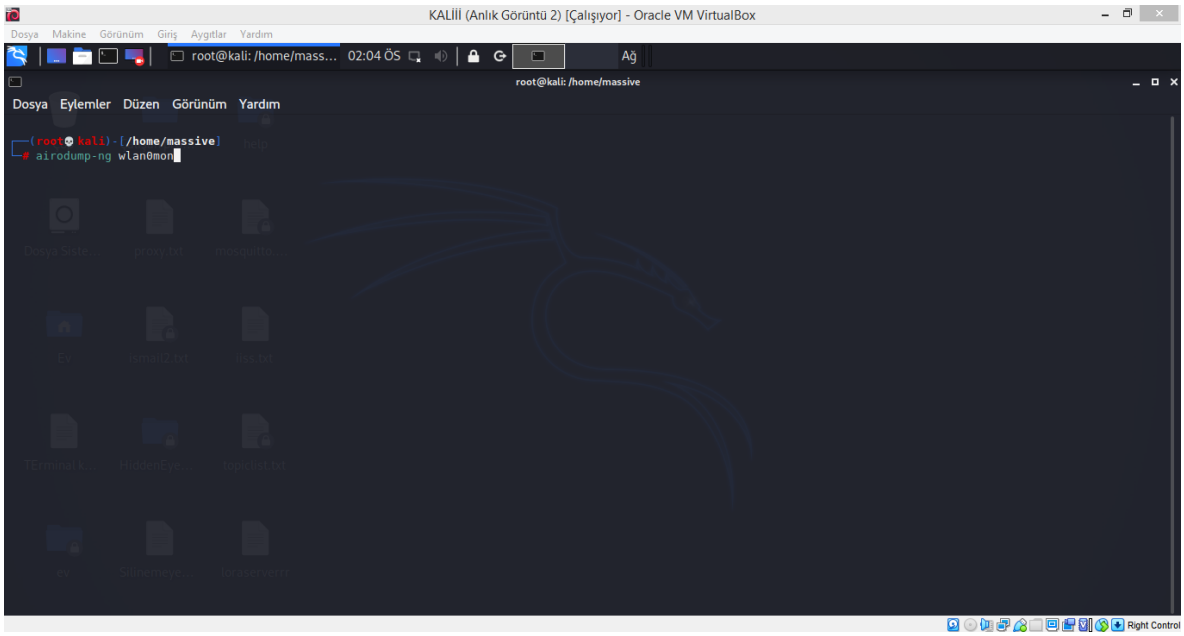


Şekil 11. Sistem Mod Değişimi
Figure 11. System Mode Change

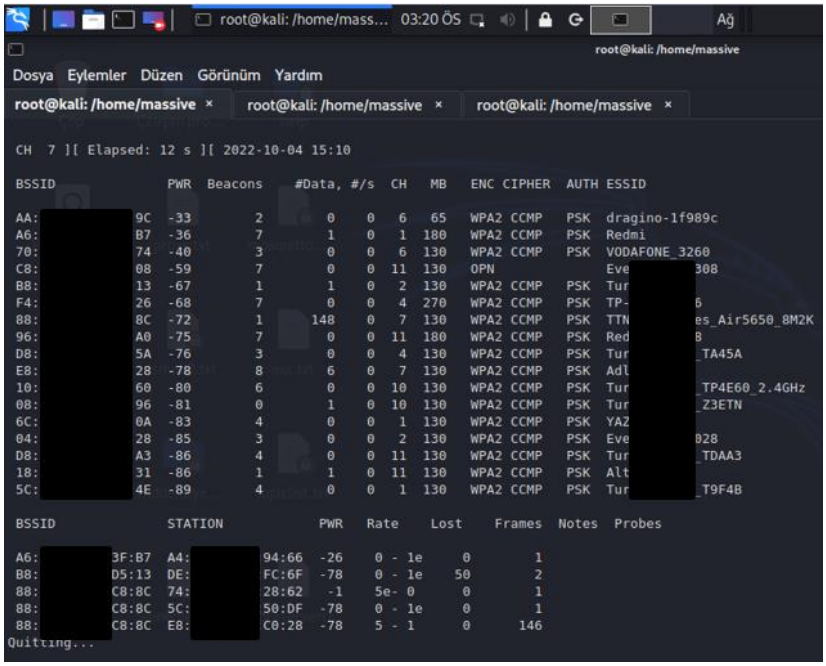


Şekil 12. Monitör Mod Kontrolü
Figure 12. Monitor Mode Control

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.

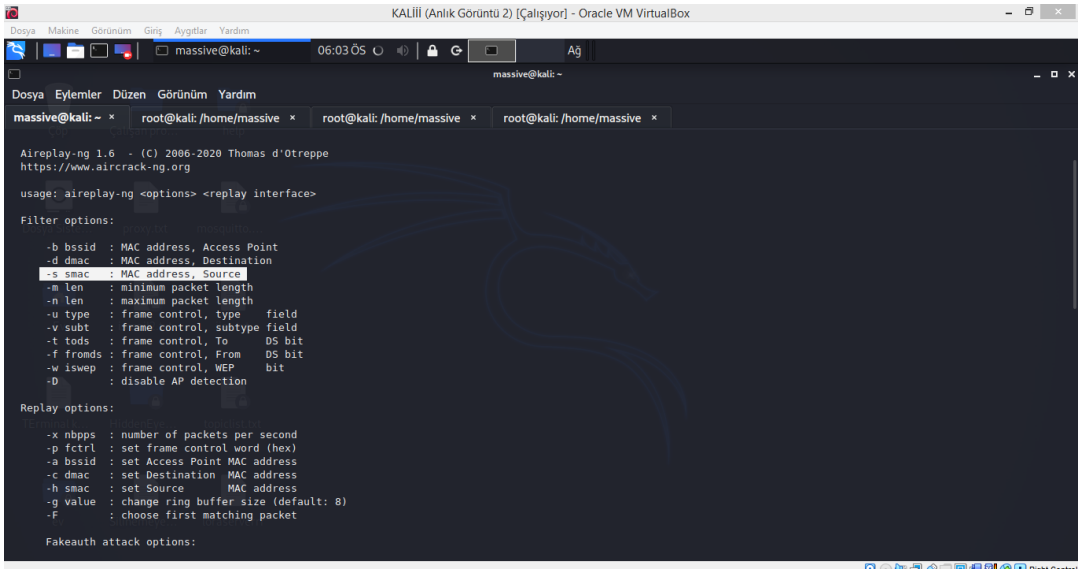


Şekil 13. Ağ Tarama Kodu
Figure 13. Network Scan Code

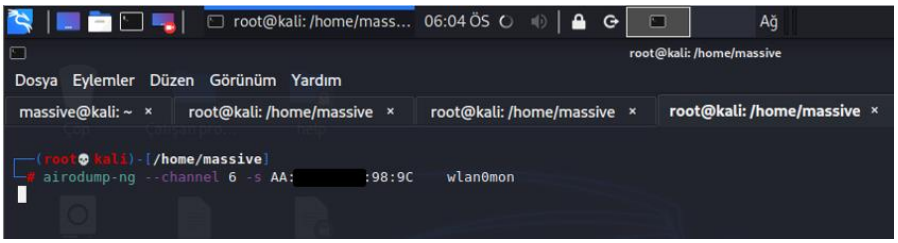


Şekil 14. Yakalanan Ağlar
Figure 14. Captured Networks

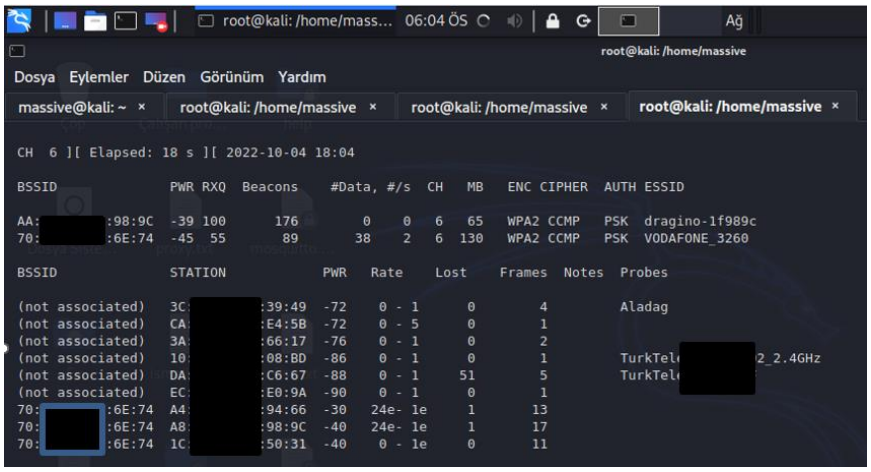
Yakalanan ağların içinde ESSID kısmında dragino-1f989c adlı bir wi-fi tespit edilmiştir. Şekil 15'de ağ geçidinin internet kaynağının MAC adresini öğrenebilmek için hangi parametrenin kullanılacağı verilmektedir. DLOS8 ağ geçidi internete bağlandığı zaman kendisi de bir kablosuz internet sağlayıcısı gibi kullanılabilmektedir. 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 gözükmektedir.



Şekil 15. Kod Seçenekleri
Figure 15. Code Options

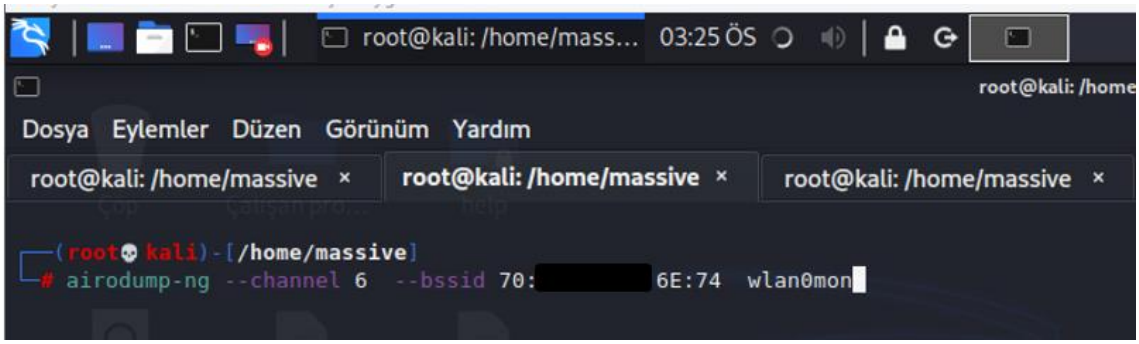


Şekil 16. Ağ Geçidinin İnternet Kaynağını Bulma Kodu
Figure 16. Gateway's İnternet Source Discovery Code

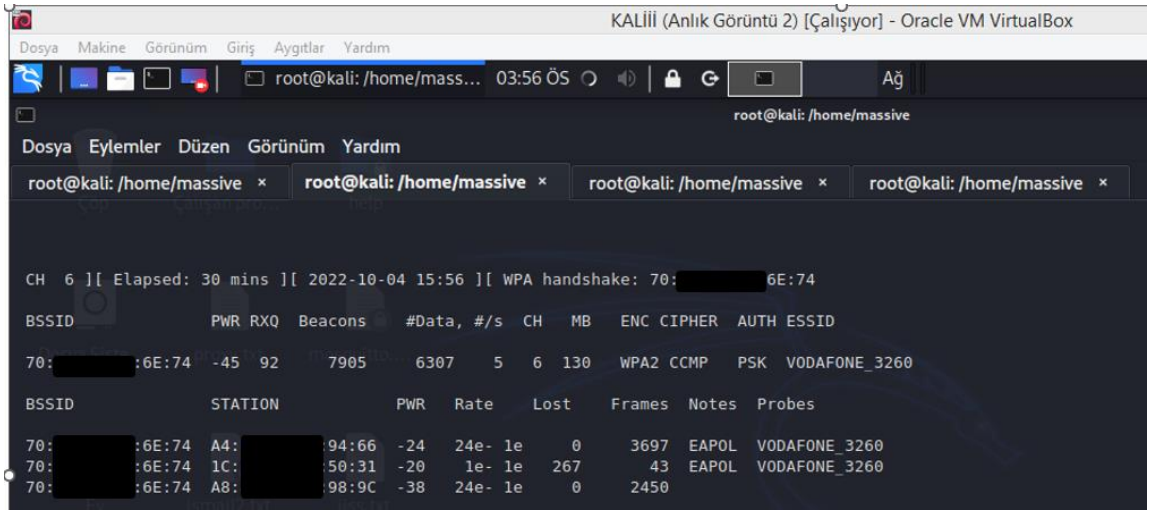


Şekil 17. Ağ Geçidinin İnternet Kaynağı
Figure 17. Gateway's İnternet Source

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 toplanılmıştır. 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.

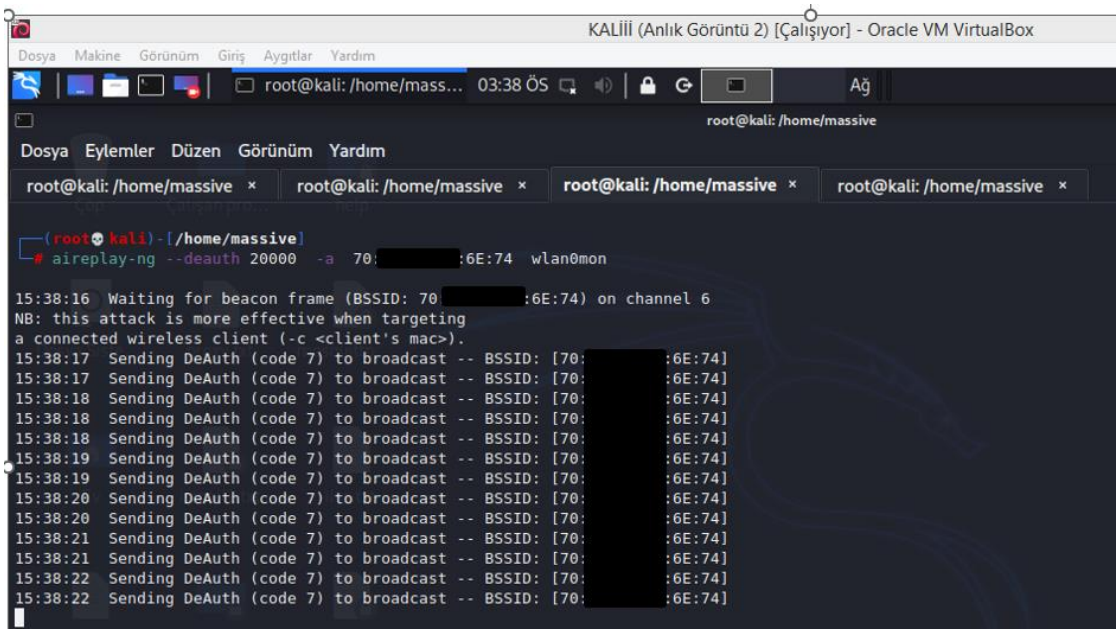


Şekil 18. Vodafone_3260 Kullanıcılarının Bulunması
Figure 18. Finding Vodafone_3260 Users

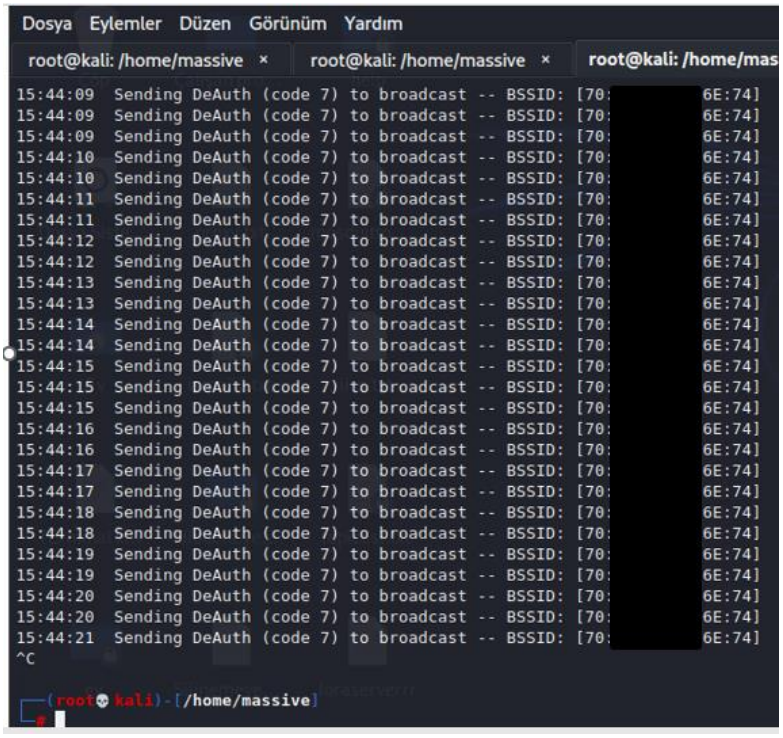


Şekil 19. Vodafone_3260 Kullanıcıları
Figure 19. Vodafone_3260 Users

Terminale yazılan ‘aireplay-ng --deauth saldırı sayısı -a wi-fi modemin 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.



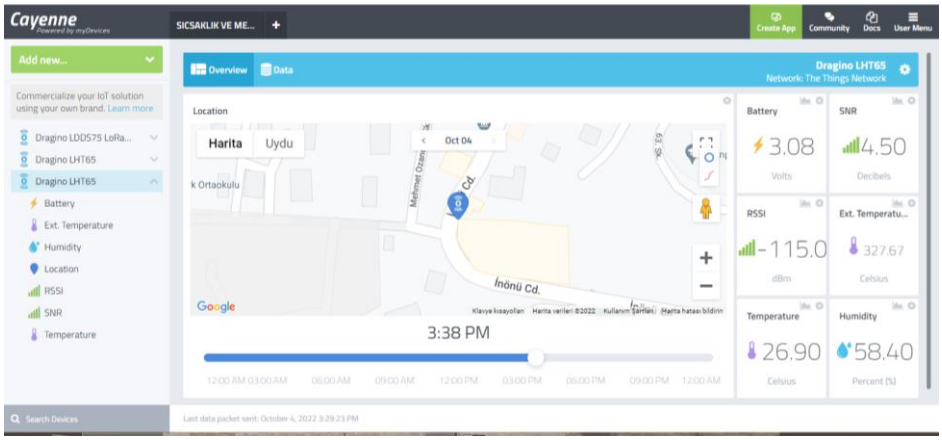
Şekil 20. Yetkisizleştirme Saldırısı
Figure 20. Deauthentication Attack



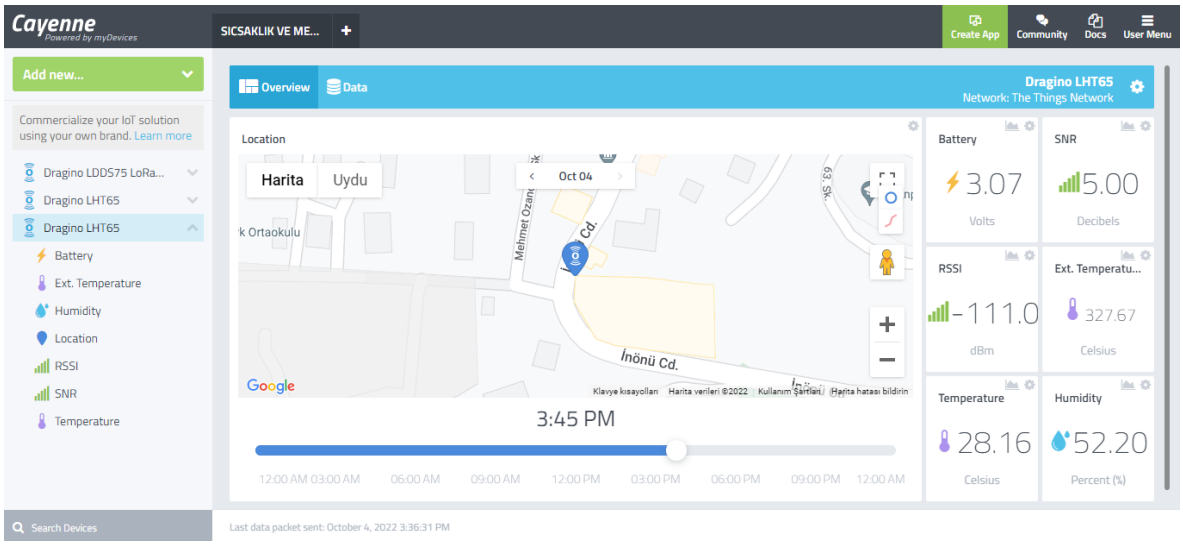
Şekil 21. Yetkisizleştirme Saldırısı Devamı
Figure 21. Deauthentication Attack Sequel

3. Bulgular ve Tartışma

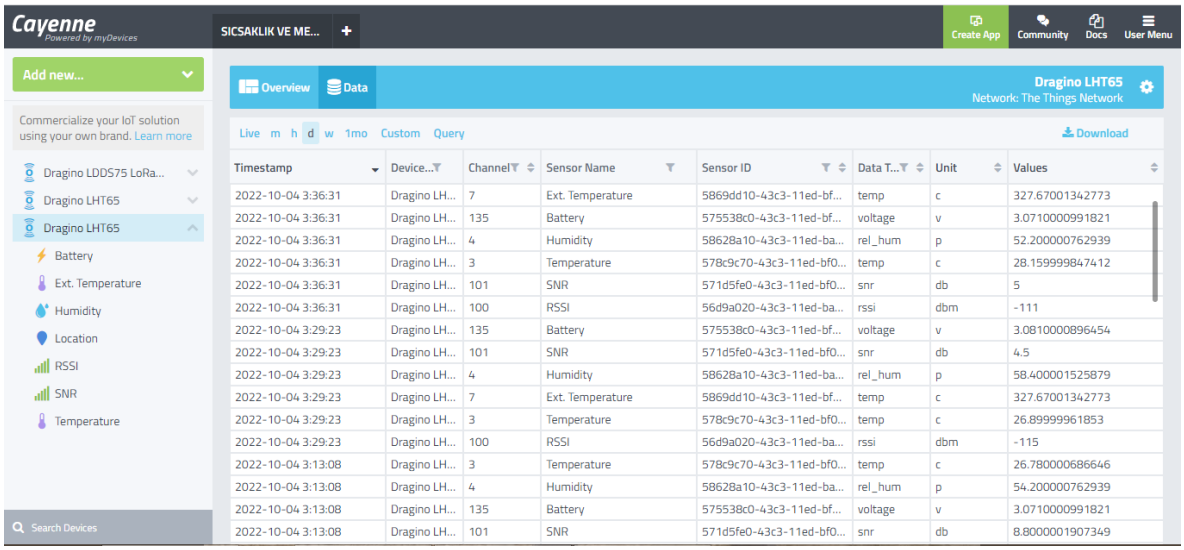
Yetkisizleştirme saldırısı yapılmadan önce LHT65 sensörü ile paket gönderimi Şekil 22'de görüldüğü gibi yapılmıştır. Daha sonra saldırı başlatılmış ve yaklaşık yedi dakika kadar süre içerisinde birçok kez LHT65 sensörü ile paket gönderimi yapılmıştır. Gönderilen paketler ağ geçidi tarafından alınmaktadır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



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 içerisinden, 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 iletilememiştir. 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 Saldırılar – 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 Saldırılar 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 Kablosuzu 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 Saldırılara 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 Saldırılar, Yüksek Lisan Tezi, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, Isparta, 202.