T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

OTOMOBİLLERDEKİ ANDROID TEMELLİ MULTİMEDYA CİHAZLARININ GÜVENLİK ZAFİYETLERİ

YÜKSEK LİSANS TEZİ

Nasrullah KANCURA

Enstitü Anabilim Dalı	**:**	**BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Dr.Öğr.Üyesi Murat İSKEFİYELİ**

Ağustos 2022

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

OTOMOBİLLERDEKİ ANDROID TEMELLİ MULTİMEDYA CİHAZLARININ GÜVENLİK ZAFİYETLERİ

YÜKSEK LİSANS TEZİ

Nasrullah KANCURA

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ

Bu tez / /2022 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Yönetici **Jüri Üyesi** **Jüri Üyesi**

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Nasrullah KANCURA

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren çok değerli danışman hocam Dr.Öğr.Üyesi Murat İSKEFİYELİ'ye teşekkürlerimi sunarım.

Ayrıca benim için hiçbir fedakarlıktan kaçınmayan eşime, her daim heyecan ve enerjisiyle beni motive eden biricik oğlum Selim'e en derin şükranlarımı sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

5G	: Fifth-Generation
BSSID	: Basic Service Set Identifier
DHCP	: Dynamic Host Configuration Protocol
DOS	: Denial of Service
ESSID	: Extended Service Set Identifier
GPS	: Global Positining System
IVI	: In-Vehicle Infotainmet
MAC	: Media Access Control
NAT	: Network Adress Translation
NIST	: National Institute of Standards and Technology
OHA	: Open Handset Alliance
OEM	: Original Equipment Manufacturer
USB	: Universel Serial Bus
Wi-Fi	: Wireless Fidelity

ŞEKİLLER LİSTESİ

ÖZET

Anahtar kelimeler: Android, otomobil, multimedya, sızma testi, Kali Linux, Metasploit

Günümüz otomobillerinde araç içi multimedya cihazları yaygın bir şekilde kullanılmaya başlanmıştır. Üreticiler araç içi multimedya cihazlarında Android işletim sistemini çokça tercih etmektedirler. Android işletim sisteminde bulunan zafiyetler güncellemeler ile azaltılsa da halen devam etmektedir. Bu sistemler Bluetooth, Wi-Fi, 5G, USB gibi birçok kablolu ve kablosuz bağlantı seçeneği de sunmaktadır. Ancak sunulan bu bağlantı seçenekleri beraberinde birçok güvenlik zafiyeti getirmektedir. Bu zafiyetler Android işletim sisteminin zafiyetleri ile birleştiğinde otomobil kullanıcılarını ciddi riskler beklemektedir.

Bu çalışmada Android temelli araç içi multimedya sistemlerindeki güvenlik zafiyetlerinin tespiti amacıyla otomobil içerisindeki multimedya cihazı üzerinde sızma testleri yapılmıştır. Sızma testleri Linux çekirdeğine sahip Debian tabanlı Kali işletim sistemi kullanılarak gerçekleştirilmiştir. Sisteme kablosuz ağ üzerinden sızma işlemi gerçekleştirilerek zafiyetlerin nasıl tespit ve istismar edilebildiği somut bir araç üzerinde gerçeklenmiştir. Elde edilen sonuçlar detaylarıyla sunulmuştur. Ayrıca bu tür siber saldırılara karşı çözüm önerileri getirilmiştir.

SECURITY VULNERABILITIES OF ANDROID-BASED MULTIMEDIA DEVICES IN CARS

SUMMARY

Keywords: Android, automobile, multimedia, penetration testing, Kali Linux, Metasploit

In-car multimedia devices are widely used in today's cars. Manufacturers mostly prefer the Android operating system in in-car multimedia devices. Although the vulnerabilities in the Android operating system are reduced with updates, they still continue. These systems also offer many wired and wireless connection options such as Bluetooth, Wi-Fi, 5G, USB. However, these offered connection options bring many security vulnerabilities. When these vulnerabilities are combined with the vulnerabilities of the Android operating system, serious risks await car users.

In this study, penetration tests were carried out on the multimedia device in the car in order to detect the security vulnerabilities in the Android-based in-car multimedia systems. Penetration tests were carried out using the Debian-based Kali operating system with a Linux kernel. How vulnerabilities can be detected and exploited by penetrating the system over the wireless network has been implemented on a real car. Obtained results are presented in detail. In addition, solutions have been proposed against such cyber-attacks.

BÖLÜM 1. GİRİŞ

Otomobillerin siber güvenliği insanoğlunun şu ana kadar karşılaştığı en önemli güvenlik sorunlarından biridir. Günümüz otomobilleri taşıdıkları elektronik bileşenler ve yazılımlarla hareketli ve ağır birer bilgisayar gibi düşünülebilir. Ancak ne var ki bu hareketli bilgisayarlar insan canı taşıdığı için potansiyel güvenlik açıkları ciddi birer tehdittir.

Modern otomobiller doğrudan ya da dolaylı olarak internet bağlantılı cihazlar içermektedirler. Bu cihazlardan birinin yetkilerinin ele geçirilmesi durumunda araç dışardan gelecek tehditlere karşı savunmasız kalmaktadır [1].

Bu modern otomobillerde dokunmatik ekranlı multimedya cihazları gitgide daha çok talep görmektedir. Bu cihazlar müzik çalma, telefon araması yapma, mesaj gönderme ve GPS navigasyonu gibi özelliklere sahip olması bu talebin en önemli nedenlerindendir. Bu cihazlarda kullanılan Android Auto platformu 3. parti uygulamaların bu cihazlarda kullanılmasına imkân tanımıştır. Birçok otomobilde Android Auto dışında Apple CarPlay desteği de bulunmaktadır [2].

Bu çalışmada Android temelli araç içi multimedya cihazlarındaki güvenlik zafiyetlerinin tespiti amaçlanmıştır. Bu amaçla somut bir otomobildeki multimedya cihazı üzerinde sızma testleri yapılmıştır. Sızma testleri Linux çekirdeğine sahip Debian tabanlı Kali işletim sistemi kullanılarak gerçekleştirilmiştir [3].

Araç içerisindeki multimedya cihazlarının internete bağlanabilmesi için en çok tercih edilen yöntem akıllı telefonlar üzerinden bir hot spot ağı oluşturulmasıdır. Cihaza kablosuz ağ üzerinde sızabilmek için öncelikle bu ağın bir ikizi oluşturulmuştur. Bir

ağın ikiz olabilmesi için aynı ESSID yani erişim noktası adı ve aynı BSSID yani erişim noktasının MAC adresi aynı olmalıdır [4].

Cihazın gerçek ağ ile bağlantısının kesilebilmesi için Deauthentication yani ağdan düşürme saldırıları düzenlenmiştir. Bu saldırı bir çeşit DOS (Denial of Service) olarak düşünülebilir. Bu saldırıda erişim noktasına (Acces Point) bağlı olan cihazlara Deauthentication Frame yani ağ bağlantısının sonlanmasını sağlayan paketler gönderilir. Normalde bu paketler sadece erişim noktası ya da istemci bağlantıyı sonlandırmak istediği zaman kullanılsa da bu paketler kopyalanarak ve tekrarlanarak bu tür saldırılarda kullanılmaktadır [5].

Cihaz ağdan düştükten sonra aynı ESSID ve BSSID ye sahip ikiz ağa bağlanana kadar bu saldırı devam etmiştir. Cihaz ikiz ağa bağlandıktan sonra captive portal yani kısıtlama portalı ile daha önce hazırlanan sahte bir web sayfasına yönlendirilir. Captive portal cihaza internet çıkışı vermeden önce cihazı belirli bir web sayfasına girmeye mecbur bırakır. Kullanıcı bu özel web sayfasından istenen verileri girene kadar internete giremez [6].

Kullanıcı bu sahte web sayfasına girdiğinde kendisinden Wi-Fi şifresini talep eden bir sayfa ile karşılaşır. Kullanıcı bu şifreyi web sayfasına girene kadar internete giremediği için şifreyi girmek durumunda kalır. Kullanıcı şifreyi girdiğinde wifiphisher açık kaynak kodlu yazılımı ile şifre yakalanır. Deauthentication yani ağdan düşürme saldırıları, ikiz ağ ve captive portal oluşturulurken açık kaynak kodlu wifiphisher yazılımından faydalanılmıştır [7].

Kullanıcının wi-fi şifresini elde ettikten sonra multimedya cihazına gönderilecek zararlı yazılım oluşturulur. Bunun için Kali İşletim Sistemi üzerinde mevcut bulunan Metasploit platformu kullanılmıştır [8]. Metasploit, Ruby yazılım dili ile geliştirilmiş açık kaynak koldu bir sızma test aracıdır [9].

Metasploit Rapid7 firması tarafından geliştirilmiş olup kullanıcının exploitleri çalıştırabileceği ve üzerinde birçok ağ tespit ve saldırı modülleri barındıran gelişmiş

bir platformdur. Exploit sızma testi uzmanlarının ya da saldırganların hedef sisteme girmek ve buradaki zafiyetlerden istifade etmek için kullanılan programdır. Exploitler payloadların hedef sisteme iletilmesini sağlarlar [9]. Payload ise exploit çalıştırıldıktan sonra hedef sistemin belleğine yerleşerek sisteme sızmaya, geriye dönük bağlantının oluşturulması ve mikrofon açma, ekran görüntüsü alma gibi istenen işleri yapmayı sağlayan bileşenlerdir [9] [10] [11].

Zararlı yazılım Metasploit üzerindeki Msfvenom modülü ile oluşturulmuştur [12]. Msfvenom Msfpayload ve Msfencode araçlarının yaptığı işleri tek başına ve daha hızlı yapabilen ve bu araçların birleştirilmiş halidir [13]. Msfvenom ile herhangi bir uygulama ya da zararlı yazılıma payload yüklenerek kullanıcıya gönderilir ve kullanıcın bunu çalıştırması beklenir [14]. Burada Msfvenom hedef cihazdan reverse (geri) bağlantı alınmasını ve cihaza sızmayı sağlar [15]. Oluşturulan bu zararlı yazılım önemli bir güncelleme dosyası şeklinde Wifiphisher yazılımı ile captive portal aracılığıyla kullanıcıya iletilmiştir. Kullanıcı zararlı yazılımı kurup çalıştırdığında Metasploit platformundaki Multi-Handler modülü ile cihaza başarılı bir şekilde sızılmıştır. Multi-Handler, hedef cihazdan saldırıyı yapan cihaza gelen bağlantıları yakalamak için kullanılan istismar modülüdür [16].

BÖLÜM 2. MULTİMEDYA CİHAZLARI

2.1. Multimedya Nedir?

Multimedya ya da diğer adıyla çoklu ortam eski dönemlerde kullanılan sadece yazılı bilgi ya da ses veren ve hiç etkileşimin olmadığı ya da çok az olduğu iletişim araçlarının aksine ses, metin, animasyon, resim ve video gibi çeşitli içerikleri bir araya getiren iletişim biçimidir. Animasyonlu videolar, podcastler ve sesli slayt gösterileri buna örnek olarak gösterilebilir. Multimedya, bilgisayarlar, telefonlar ve buna benzer akıllı cihazlar ile gerçek zamanlı olarak kaydedilebilir [17].

Multimedyayı oluşturan donanımsal ve yazılımsal bileşenler Şekil 2.1.'de gösterilmiştir.

Şekil 2.1. Multimedya bileşenleri [18]

2.2. Multimedya Cihazı Nedir?

Multimedya cihazı, metin, ses ve video gibi çeşitli biçimlerdeki medyaları çalıştırmaya yarayan elektronik cihazlardır. Multimedya cihazları kullanıcının farklı medyalarla aynı anda etkileşime girmesini sağlamaktadır. Ayrıca bu farklı medyalar için ayrı birer cihaz gerekliliğini de ortadan kaldırmaktadır. Bu cihazlara örnek olarak tablet bilgisayarlar, mp3 oynatıcılar ve araç yol bilgisayarı diye tabir edilen multimedya cihazları verilebilir. Multimedya cihazları kullanıcının çok çeşitli işlemleri yerine getirmesini sağlar. Mesela bir sunum hazırlayabilir, fotoğraf veya video çekebilir ve bunları daha sonra erişebilmek için kaydedebiliriz. Oluşturduğumuz bu içerikleri başka bir multimedya cihazına aktarabilir ya da başka biriyle paylaşabiliriz. Bu cihazların bütünleşik olması ve kullanım kolaylığı sağlaması amaçlandığından tüketiciler taşınabilir küçük multimedya cihazlarını daha çok tercih etmektedirler. Buna en iyi örnek akıllı telefonlardır. Her yeni sürümle birlikte bu cihazların medya yetenekleri de artma eğilimindedir [19].

Şekil 2.2. Multimedya cihazları, ayrı cihazlara olan ihtiyacı ortadan kaldırır [19].

2.3. Multimedya Cihazı Kullanım Alanları

Multimedya cihaz kullanımın en popüler olduğu alanlardan biri eğitimdir. Özellikle öğrencilerin çalışma materyalleri üretmek ve çeşitli konulara hakimiyetini artırmak için bu cihazlardan istifade edilmektedir. Ayrıca bu cihazlar öğrencilere eğlenirken öğrenmelerini de sağlamaktadır [20].

Şekil 2.3. Eğitimde multimedya kullanımı [21]

Eğlence sektörü de multimedya cihazlarının en sık kullanıldığı alanlardan biridir. Multimedya eğlence alanında en çok müzik ve video uygulamaları ile ön plana çıkmıştır. Bu cihazların filmlerde kullanımı benzersiz bir görsel ve işitsel izlenim sağlar. Yine bu cihazlar ile oyun sektöründe interaktif video oyunları mümkün hale gelmiş ve bu oyunlar ses ve görsel efektler sayesinde daha ilgi çekici bir hal almıştır [20].

Şekil 2.4. Eğlence sektöründe multimedya cihazı kullanımı [22]

Bu cihazların kullanıldığı bir diğer alan ise işletmelerdir. Firmalar reklam, pazarlama ve ürün sunumları gibi birçok alanda multimedya uygulamalarından istifade ederler. Müşterilerin dikkatini çekmek, ürünlerini daha iyi tanıtmak ve satışlarını artırmak amacıyla multimedya cihazlarını kullanırlar. Ayrıca basit ve etkili sunumlar yapmak ve ürünler hakkında etkili bilgiler verebilmek amacıyla da kullanılmaktadır [20].

Şekil 2.5. İşletmelerde multimedya kullanımı [23]

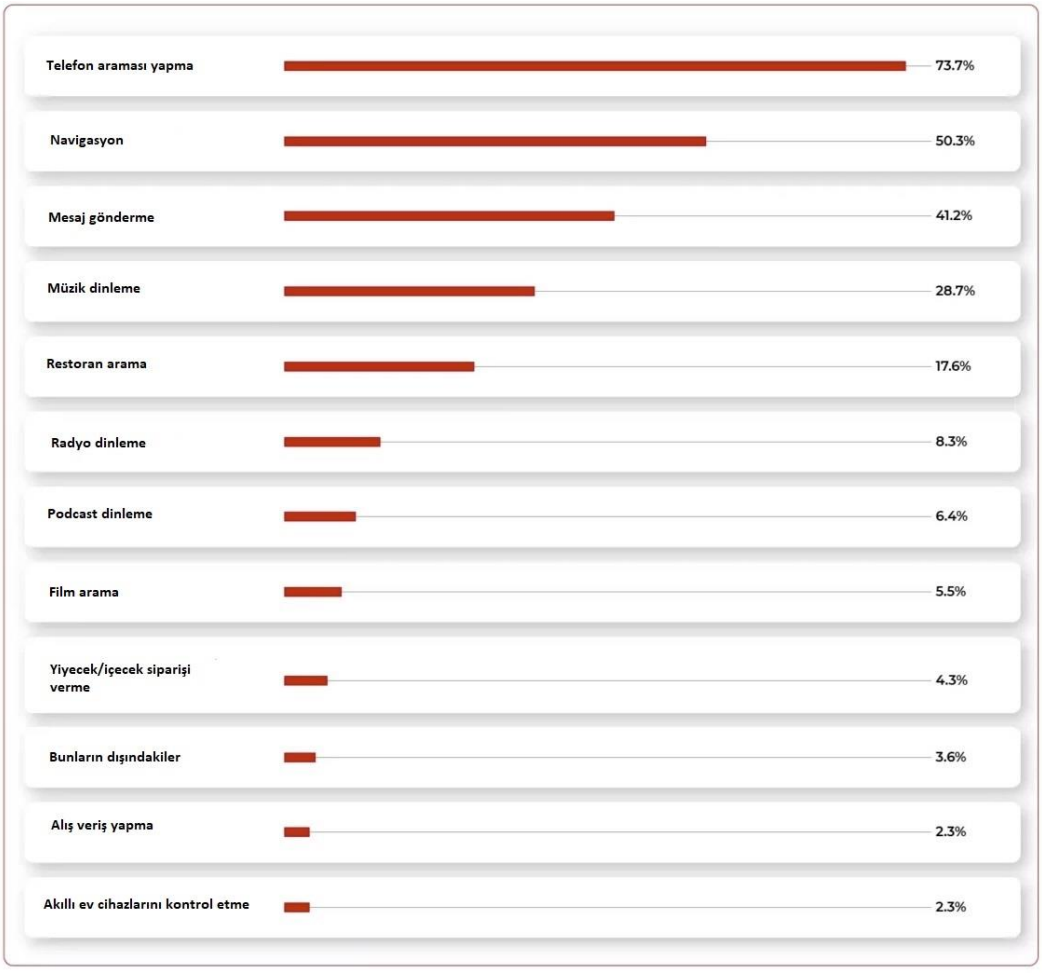
Bilim ve teknoloji alanında da multimedya cihazlarından istifade edilmektedir. Multimedya sayesinde bir yerden başka bir yere canlı yayın mümkün hale gelmektedir. Yine bu alanda masraf ve sorunların azaltılarak verimliliğin artırılmasına katkı sağlamaktadır [20].

Şekil 2.6. Otomobillerde multimedya cihazı kullanımı [24]

Bu alanların dışında özellikle son yıllarda multimedya cihazları neredeyse bütün otomobillerde kendine yer bulmuştur. Özellikle navigasyon, geri görüş kamerası, eller serbest telefon görüşmesi, internet bağlantısı, televizyon gibi birçok faydalı özelliği bir arada sunması sayesinde otomobillerde vazgeçilmez bir cihaz olmuştur. Ayrıca sahip oldukları büyük ve renkli ekranları sayesinde araç içerisine daha modern bir görünüm katması da bu talebi artırmıştır [25].

2.4. Otomobillerde Kullanılan Multimedya Cihazları

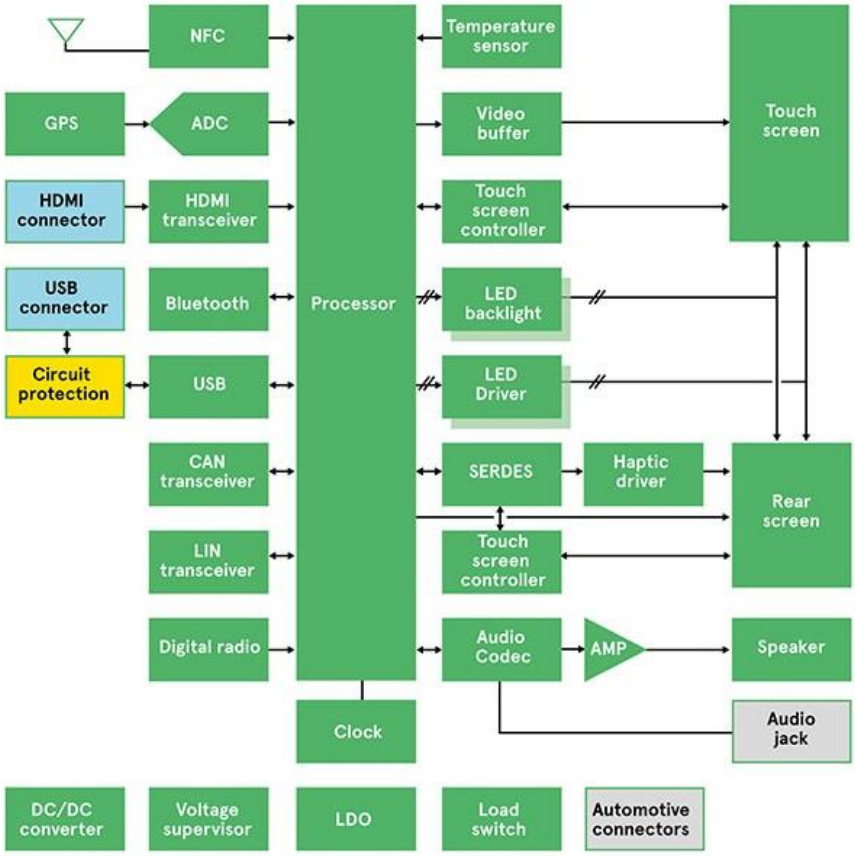
Otomobillerde kullanılan multimedya cihazları, görüntü ve ses arabirimleri, dokunmatik ekran, panel tuşları ve sesli komutlar gibi kontrol öğeleri ile sürücü ve yolculara bilgi ve eğlence sağladığı için araç içi bilgi-eğlence sistemi (IVI) olarak adlandırılmaktadır [26].



Şekil 2.7. IVI kullanım amaç ve oranları [27]

IVI sistemleri arasında farklılıklar olsa de genel olarak bu cihazlar sesli içeriklerin oynatılması ve yönetilmesi, istediğimiz konuma gidebilmek için navigasyonun kullanılması, oyunlar, filmler ve sosyal ağlar gibi eğlencelerin sunulması, sms metin mesajlarının sesli olarak dinlenilmesi ya da sesle metin mesajı gönderme, telefon araması yapma, dahili ya da harici internet bağlantısı sayesinde canlı trafik bilgisine ulaşma ve hava durumu tahminlerini öğrenme gibi görevleri yerine getirirler [28].

IVI mimarisi modüler olma eğilimindedir. Bu sayede araç içerisindeki kullanılabilir alandan en verimli şekilde faydalanılmasını sağlar. Standart bir IVI sistemi tüm sistem elemanlarının kablolu ya da kablosuz bağlandığı bir işlemci sistemi etrafında toplanmaktadır. Dokunmatik ekran sürücünün kolayca erişebilmesi için ön panelin ortasına yerleştirilmektedir. Bazı IVI sistemlerinde ses kontrolü için fiziksel düğmeler mevcutken eğilim düğmesiz tam ekranlara doğrudur [29].

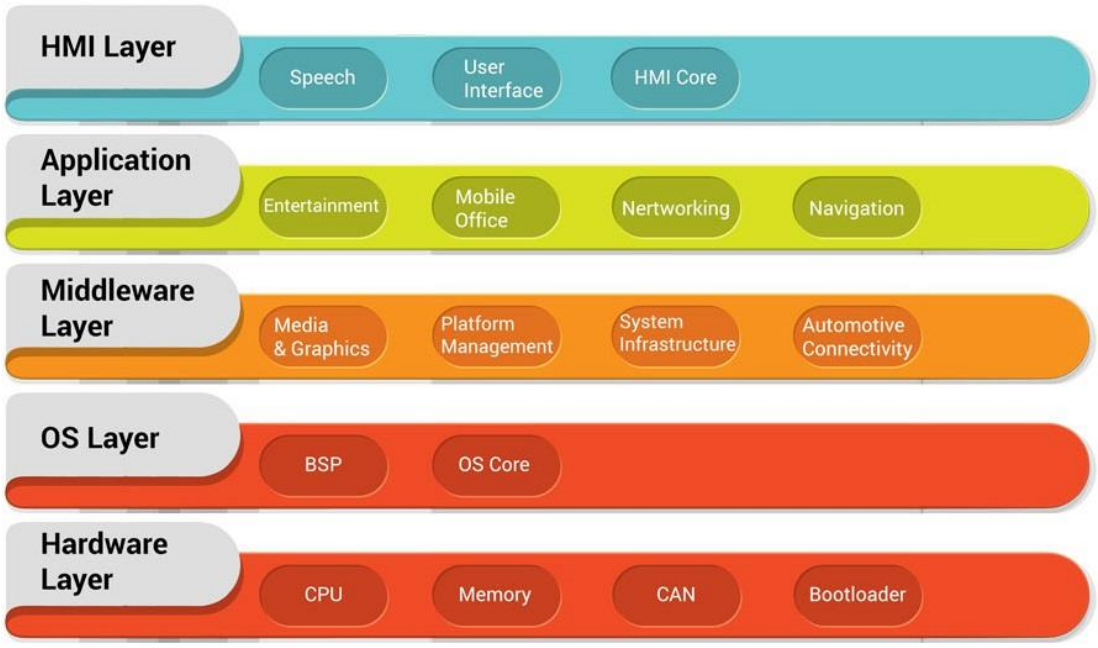


Şekil 2.8. IVI blok diyagramı [29]

Otomobillerde kullanılan multimedya cihazları, sisteme yeni fonksiyonlar katabilmek için bağlantı seçenekleri ve indirilebilir yazılım uygulamalarını destekleyen işletim sistemi gerektirmektedir. Bu cihazlarda Android, QNX, Linux ve Windows önde gelen işletim sistemleridir [26]. Şekil 2.9.'da Anroid Auto'ya ait ekran görünümü paylaşılmıştır.

Şekil 2.9. Android Auto ekran görünümü [31]

Araç içi bilgi eğlence sistemlerindeki (IVI) elektronik bileşenler kontrolör alan ağı (CAN) gibi standartlaşmış iletişim protokolleriyle birbirlerine bağlıdırlar. CAN ya da herhangi bir ağ protokolü, cihazların ve mikrodenetleyicilerin ana bir bilgisayar olmadan uygulamalarda birbirleriyle haberleşmesini sağlar. Şekil 2.10.'da IVI sistem mimarisi gösterilmiştir [26].



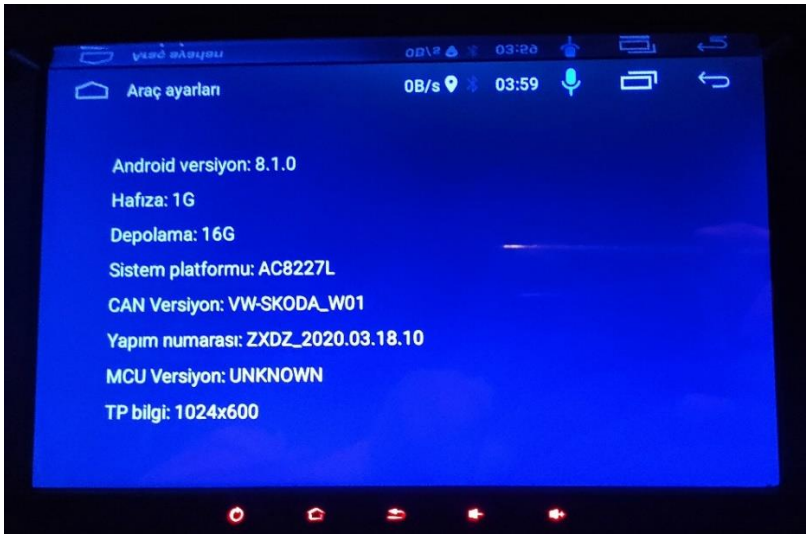
Şekil 2.10. IVI sistem mimarisi [26]

Apple CarPlay ve Anroid Auto platformları kullanıcının akıllı telefonunu aracın bilgi-eğlence sistemiyle entegre edilmesine imkân tanır. Android Auto android tabanlı herhangi bir telefon vasıtasıyla Google uygulamalarını (Google play music, Google maps vb.) desteklerken Apple CarPlay ise App Store'daki IOS tabanlı uygulamaları destekler [26]. Şekil 2.11.'de Apple CarPlay'e ait ekran görünümleri paylaşılmıştır.

Şekil 2.11. Apple CarPlay ekran görünümü [30]

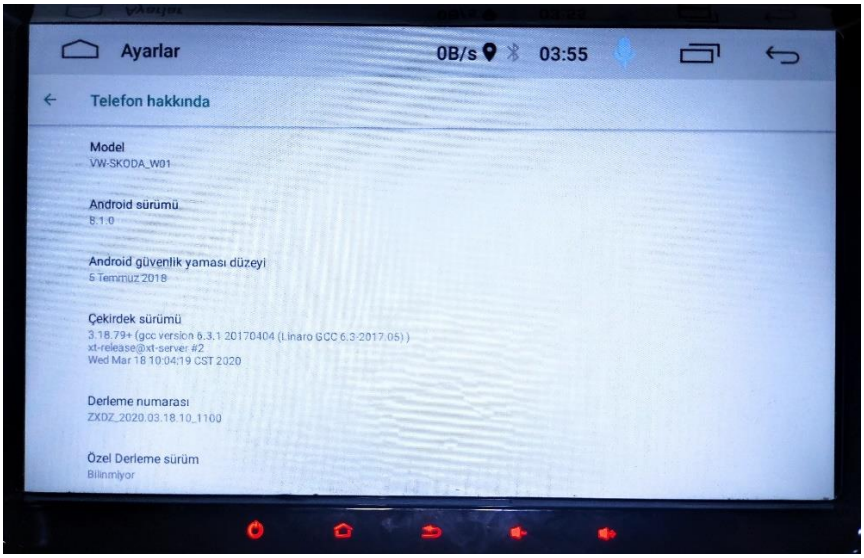
2.5. Çalışmada Kullanılan Multimedya Cihazı

Bu çalışmada Volkswagen Marka Golf 2005 model araca sonradan takılmış Android 8.1.0 sürümü bulunan 1 GB ram ve 16 GB depolama alanını sahip AC8227L model oem bir multimedya cihazı kullanılmıştır. Cihaz bilgileri Şekil 2.12.'de gösterilmiştir.



Şekil 2.12. Çalışmada kullanılan multimedya cihazı bilgileri

Android 8.1.0 sürümünü kullanan bu cihaz en son aldığı güvenlik yaması 5 Temmuz 2018 tarihli olup, Linux çekirdeği 3.18.79 sürümüdür. Bu bilgiler Şekil 2.13.'te gösterilmiştir.



Şekil 2.13. Çalışmada kullanılan multimedya cihazı yazılım bilgileri

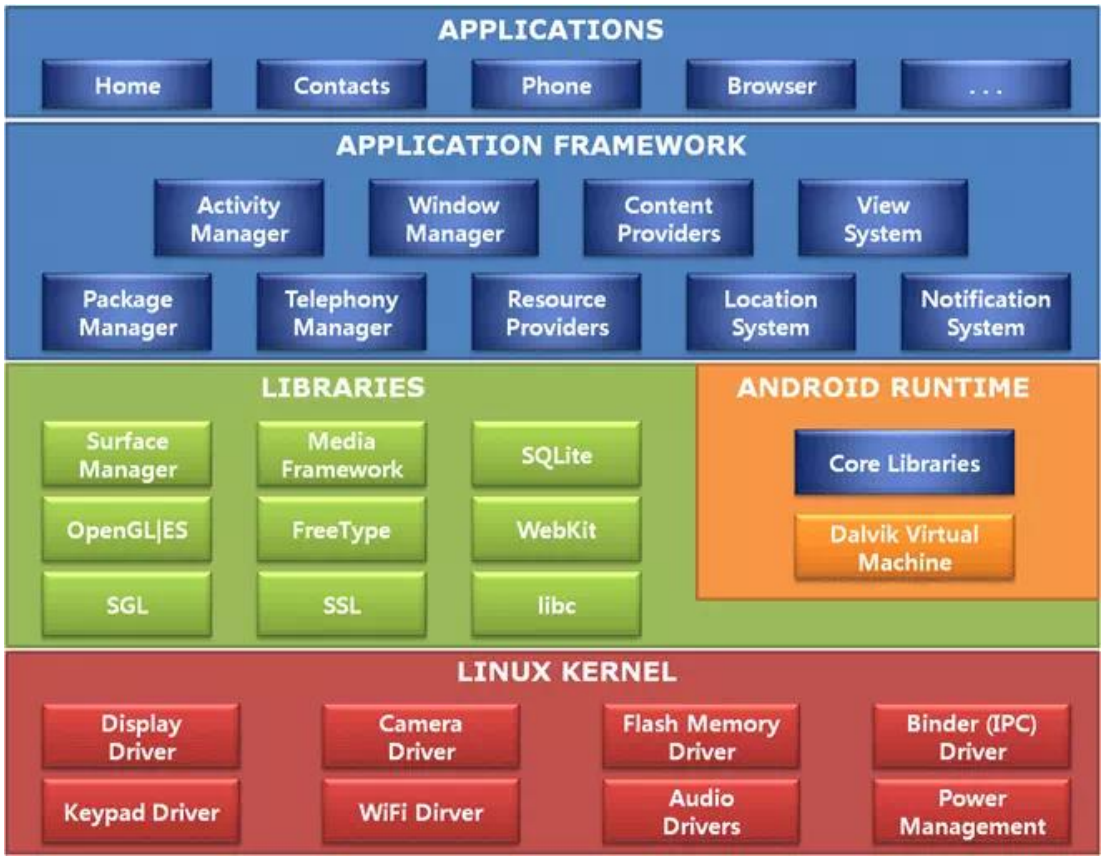
BÖLÜM 3. KAYNAK ARAŞTIRMASI

3.1. Android İşletim Sistemi

Android işletim sistemi sıradan bir işletim sisteminden çok daha fazlasını sunmaktadır. Android mimarisi Linux çekirdeğini temel alarak inşa edilmiştir. Android Google firması tarafından başlatılan bir proje olmayıp, Google firmasının yönettiği Open Handset Alliance (OHA) tarafından geliştirilmiş olup 2005 yılında Google tarafından satın alınmıştır. Google 86 şirketi bir araya getirerek OHA'yı kurmuştur. HTC, LG, Motorola, Qualcomm gibi telekomünikasyon firmaları OHA'nın üyeleri arasında yer almıştır. Mobil cihazlar için açık standartların oluşturulmasında bu ekip ciddi bir çaba sarf etmiştir [32]. Şekil 3.1.'de OHA üyelerinden bazıları gösterilmiştir.

Şekil 3.1. OHA üyeleri [33]

Android mimarisi temel olarak 4 katman üzerine kurulmuştur. Bu katmanlar Linux çekirdeği (kernel), Android kütüphaneleri (libraries), Anrdoid yazılım çerçevesi (framework) ve uygulama katmanıdır. Şekil 3.2.'de bu katmanlar ve içerikleri gösterilmiştir.



Şekil 3.2. Android katmanları [34]

Android sadece kullanıcılar için değil gerek şirketler gerekse geliştiriciler için kısa sürede en çok tercih edilen mobil işletim sistemi olmuştur. Android'e gelen bu yüksek talep ile kötü niyetli siber saldırganlar da bu platforma yönelmişlerdir [35].

Android platformu çok parçalı bir yapıya sahip olması nedeniyle işletim sistemi güvenliği bakımından nispeten zayıftır. Android platformunda en az dört etkin ana sürüm mevcut olup Google bilinen güvenlik zafiyetlerini düzeltmek için sadece her ay en son Android sürümü için güvenlik güncellemeleri çıkarmayı taahhüt edebilir. Bu güncellemeler her ay çıksa dahi OEM üreticileri hızlı güncelleme yapamadığından kullanıcılardan birçoğunun cihazı zamanında güncellenemediği gibi hatta bazı cihazlar hiç güncellenemeden piyasaya sürülmektedir. Bu durum birçok kullanıcının Android sistem güvenliğinin Apple hatta Microsoft'un işletim sistemleri kadar iyi olmadığı düşüncesine neden olmuştur. Ayrıca bazı üreticilerin Android üzerinde yaptığı değişiklikler güvenlik zafiyetlerine neden olmuştur [36].

Amerika Birleşik Devleri Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) güvenlik açığı veri tabanından elde edilen verilere göre son 20 yılda ücretsiz bir işletim sistemi olan Debian Linux bildirilen 3067 teknik güvenlik açığı ile toplamda ilk sırada yer almıştır. İlgili web sitesine göre Debian Linux kullanıcıları çok duyarlı olduklarından bu açıklıklar çoğu zaman birkaç gün içinde düzeltilmektedir. Android 2019 yılında 414 güvenlik açığıyla Debian Linux'ü geçerek birinci sıraya yerleşmiştir. Bunun sebebi olarak Android cihazlarda yüklü gelen üçüncü taraf uygulamalar ve bunların kullanıcıları tespit edilemeyen hatalara maruz bırakması gösterilebilir. Şekil 3.3.'te NIST güvenlik açığı veri tabanından elde edilen verilere göre hazırlana işletim sistemlerinin 1999-2019 arası ve 2019 yılına ait güvenlik açığı sayıları ve sıralaması gösterilmiştir [37].

1999–2019	
Debian Linux	3,067
Android	2,563
Linux kernel	2,357
Mac OS X	2,212
Ubuntu	2,007
Mozilla Firefox	1,873
Google Chrome	1,858
iPhone iOS	1,655
Windows Server 2008	1,421
Windows 7	1,283
Adobe Acrobat Reader DC	1,182
Adobe Acrobat DC	1,182
Windows 10	1,111
Adobe Flash Player	1,078
Windows Server 2012	1,050

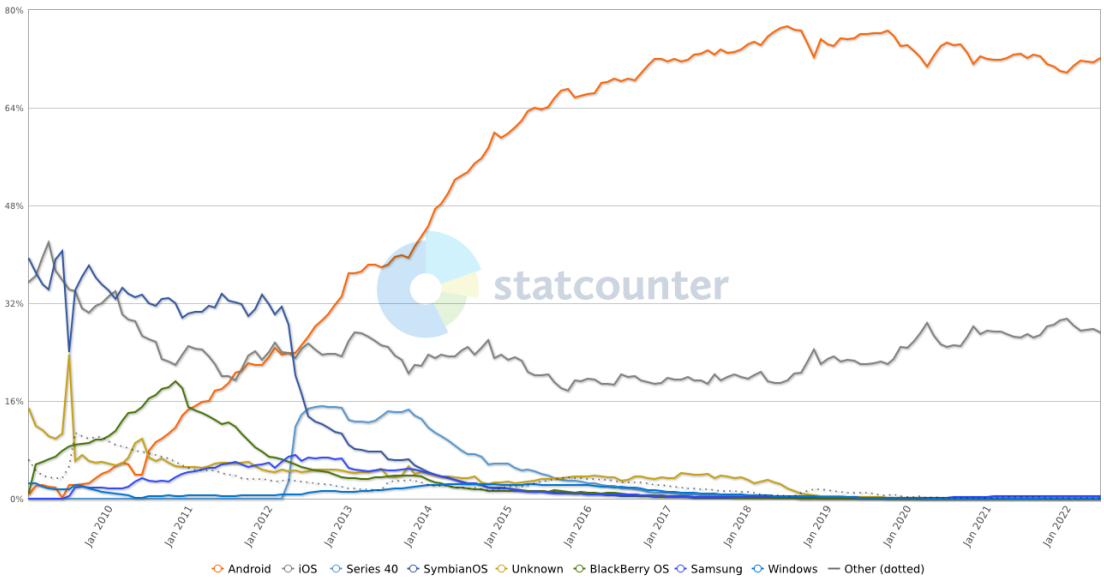
2019	
Android	414
Debian Linux	360
Windows Server 2016	357
Windows 10	357
Windows Server 2019	351
Adobe Acrobat Reader DC	342
Adobe Acrobat DC	342
cPanel	321
Windows 7	250
Windows Server 2008	248
Windows Server 2012	246
Windows 8.1	242
Windows RT 8.1	235
Ubuntu	190
Fedora	184

Şekil 3.3. İşletim sistemlerinin güvenlik açığı sayıları [37]

3.2. Android Cihazlar

Android ekosistemi her geçen gün daha da büyümektedir. Üreticiler her gün yeni ve farklı cihazlarını tanıtmakta. Her gün bir milyondan fazla cihaz tüketiciler tarafından alınıp etkinleştirilmektedir. Android 2005 yılında Google tarafından satın alındıktan üç yıl sonra HTC Dream Android kullanan ilk telefon olarak tüketicilerin beğenisine sundu. 2011 yılına gelindiğinde Google tablet ve televizyonlarda ilk defa Android kullanımına başladı. Bu Android'e olan ilgiyi daha da arttırdı. Android artık dizüstü bilgisayarlardan kol saatlerine ve otomobillerdeki multimedya cihazlarına kadar yayıldı [38].

Android cihaz oranının ne kadar arttığını görmek için Statcounter web sitesi üzerinden 2009-2022 yılları arasındaki Dünya geneli mobil işletim sistemleri pazar payları sorgulanmış ve Şekil 3.4.'teki grafik elde edilmiştir. Grafikten anlaşılacağı üzere Android diğer mobil işletim sistemlerini ciddi bir fark atmış olup açık ara en çok tercih edilen mobil işletim sistemi olmuştur.



Şekil 3.4. Dünya geneli mobil işletim sistemleri pazar payları [39]

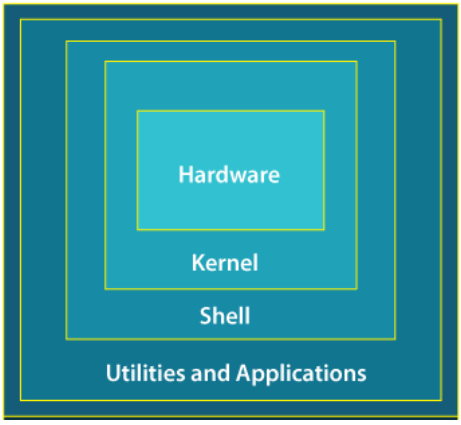
3.3. Unix İşletim Sistemi

Unix ilk olarak Dennis Ritchie ve Ken Thompson tarafından 1970 yılında AT&T Bell laboratuvarlarında geliştirilen bir işletim sistemidir. Esneklik, çoklu görev ve birçok özelliği sayesinde mühendislik, bilim ve akademik kurumlar arasında yaygın olarak kullanılmıştır. Unix dosya sistemi kullanıcının dosyaları kullanarak veri depolayabildiği ve alabildiği hiyerarşik bir dizin ve dosya yapısı şeklinde oluşturulmuştur [40].

Unix işletim sisteminin belli başlı özellikleri arasında çoklu görev (multitasking), çoklu kullanıcı (multi-user), taşınabilirlik, dosya güvenliği ve koruması, komut yapısı, iletişim, açık kaynak, hesap oluşturma, Unix araç ve yardımcı programları gösterilebilir [40].

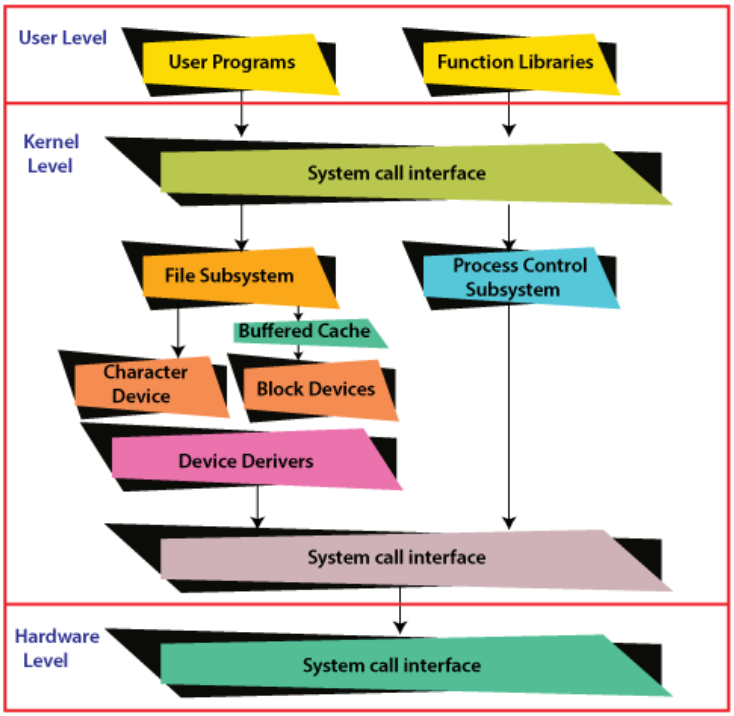
Şekil 3.5. Unix'in özellikleri [40]

Unix ile çalışırken bu sistemin bazı katmanları donanım ile kullanıcı arasında etkileşim sağlamaktadır. Unix donanım, çekirdek (kernel), kabuk (shell), uygulama programları katmanı olmak üzere toplam dört katmandan oluşmakta olup bu katmanlar Şekil 3.6.'da gösterilmiştir.



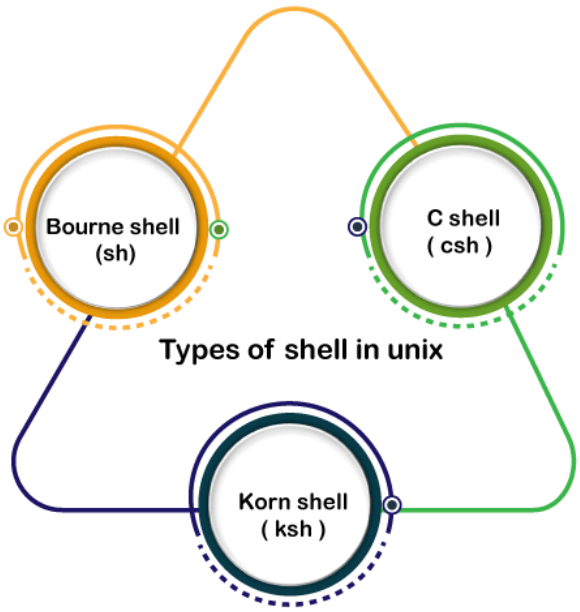
Şekil 3.6. Unix'in katmanları [40]

Çekirdek (kernel) işletim sisteminin tam işlevsel olarak çalışmasını sağlar. Unix çekirdeği belirli donanımlarla çalışır ve etkin bir şekilde donanımla etkileşime girer. Çekirdek ayrıca aygıt yöneticisi gibi çalışır ve çevresel aygıtları aygıt sürücüleri aracılığıyla kontrol eder. Bunun dışında çekirdek belleği de yönetir. Çekirdek ana belleğin etkin kullanılması ve her işlem için gerekli miktarda bellek ayırmak için takas (swapping), sayfalama (paging) ve sanal depolama gibi teknikler kullanır. Unix çekirdek mimarisi Şekil 3.7.'de gösterilmiştir [40].



Şekil 3.7. Unix çekirdek mimarisi [40]

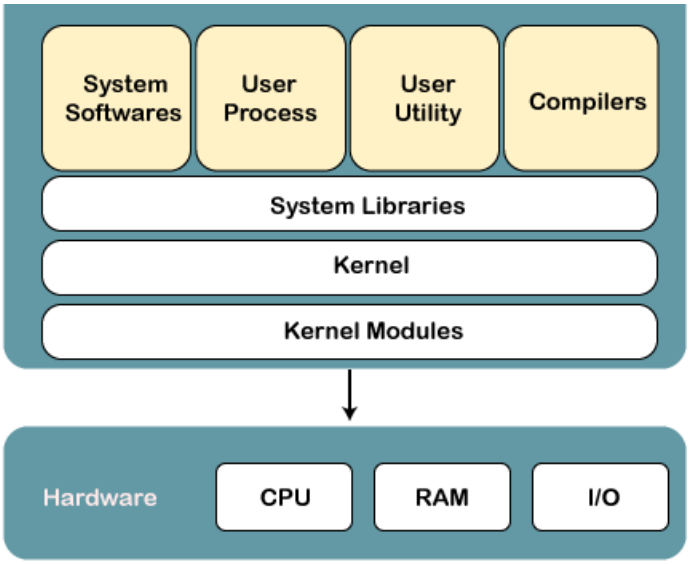
Kabuk (shell) kullanıcının terminale gönderdiği komutu yorumlayıp sadece istenen programı çağıran bir yorumlayıcıdır. Ayrıca yazılan komutların listesinin geçmişlerini de tutarak daha sonra listede yukarı ya da aşağı kaydırarak bu komutu tekrar çağırabiliriz. Bourne kabuğu, C kabuğu ve Korn kabuğu olmak üzere üç çeşit kabuk vardır. Bourne kabuğu Unix için oluşturulan ilk kabuktur. Unix'te hala en yaygın olarak bulunan kabuktur. C kabuğu da yaygın kullanılmakta olup Bourne kabuğundaki eksiklikler giderilmiştir. Korn kabuğu ise C kabuğundaki komut dosyası eksikliklerini gidermek için oluşturulmuştur [40].



Şekil 3.8. Unix kabuk çeşitleri [40]

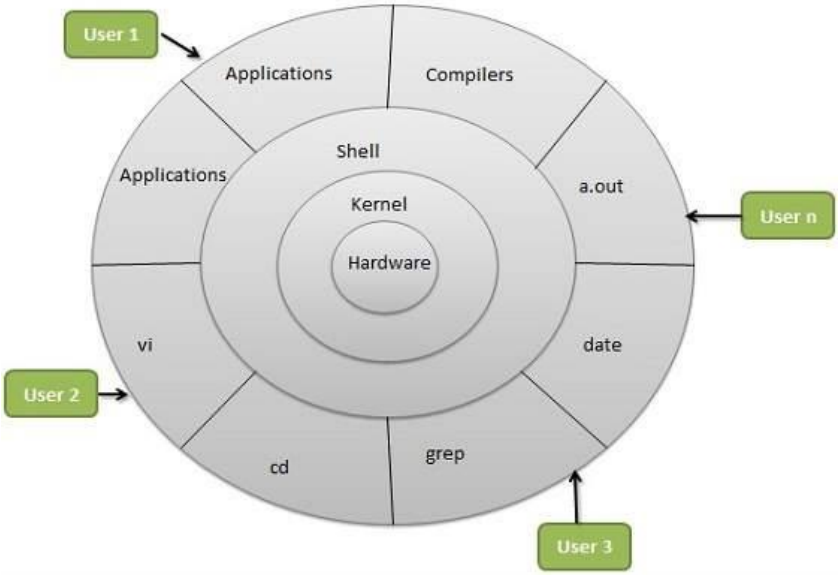
3.4. Linux İşletim Sistemi

Linux, Unix işletim sisteminin en popüler sürümüdür. Açık kaynak kodlu olup kaynak kodu ve kullanımı ücretsizdir. Linux, Unix ile uyumlu tasarlanmış olup işlevsellik olarak Unix'e çok benzer. Linux işletim sisteminin temel olarak çekirdek (kernel), sistem kitaplığı (system library) ve sistem yardımcı programlar olmak üzere üç bileşeni mevcuttur. Linux işletim sisteminin yapısı Şekil 3.9.'da gösterilmiştir [41].



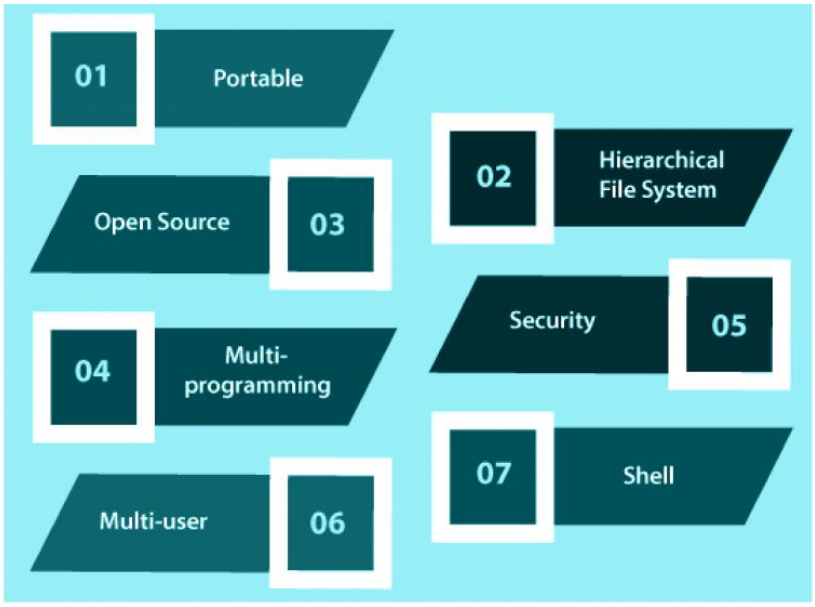
Şekil 3.9. Linux İşletim Sistemi'nin yapısı [42]

Linux mimarisi Unix mimarisine benzer şekilde toplam dört katmandan oluşmaktadır. Bunlar donanım katmanı, çekirdek, kabuk ve yardımcı programlardır. Donanım katmanı işlemci, sabit disk ve geçici bellek gibi çevresel aygıtlardan oluşur. Çekirdek işletim sisteminin temel bileşeni olup direkt donanımla etkileşime girer. Kabuk çekirdeğe bir arayüz sağlayarak kullanıcıdan komutlar alır ve çekirdeğin fonksiyonlarını yürütürler. Yardımcı programlar ise işletim sisteminin işlevlerinin çoğunu sağlarlar. Linux mimarisi Şekil 3.10.'da gösterilmiştir [41].



Şekil 3.10. Linux mimarisi [41]

Linux'un özellikleri arasında taşınabilir, hiyerarşik dosya sistemi, açık kaynak kodlu, çoklu uygulama, güvenlik, çoklu kullanıcı ve kabuk yapısı sayılabilir [43].



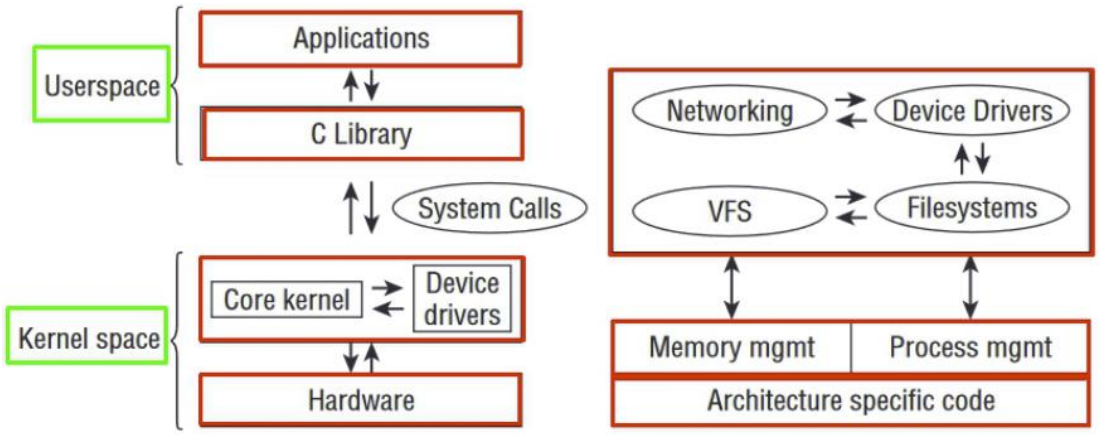
Şekil 3.11. Linux'ün özellikleri [43]

3.5. Kali Linux İşletim Sistemi

Kali Linux, Debian Linux temelli güvenlik testlerinin yapılabildiği kurumsal kullanım için hazır bir Linux dağıtımıdır. Kali, bilgi güvenliği uzman ve yöneticilerine yönelik hazırlanmıştır. Kali ile gelişmiş sızma testleri, adli inceleme ve güvenlik denetimi yapılabilir [44].

Kali Linux, BackTrack Linux'un Debian geliştirme standartlarına bağlı kalarak yeniden yazılması ile 2013 yılında piyasaya sürülmüştür. Kali'de 600'den fazla sızma testi aracı mevcuttur. Bu araçlar ile ilgili bilgilere www.kali.org/tools/ sayfasından ulaşılabilmektedir. Kali tamamen ücretsiz bir işletim sistemidir. Açık kaynak geliştirme modeline sahip olup geliştirme ağacı (devoleopment tree) herkes tarafından görülebilmektedir. Kali Linux kullanıcılarının destek dosyaları (support files), kitaplıkları (libraries) ve buna benzer dosyaları kolaylıkla bulabilmesini sağlayan sistem hiyerarşisi standartlarına bağlı kalmaktadır [45].

Kali İşletim Sistemi mimarisi Şekil 3.12.'de gösterilmiştir [46].



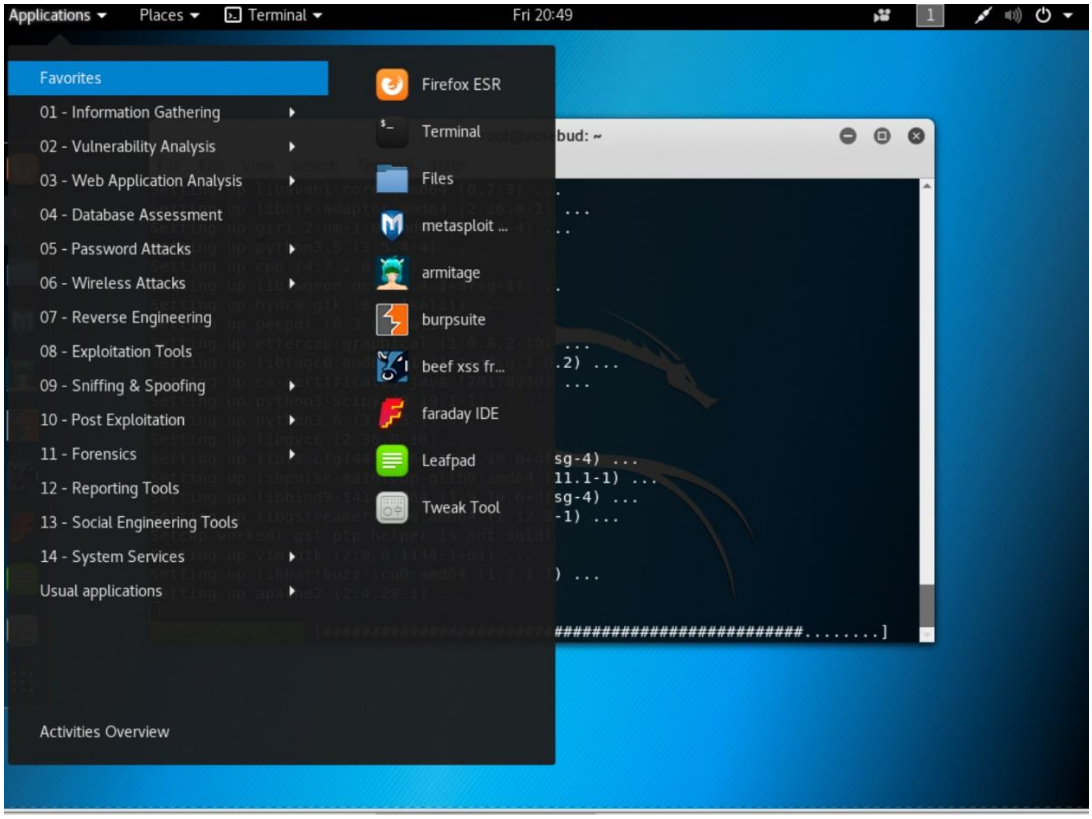
Şekil 3.12. Kali sistem mimarisi [46]

Kali ayrıca geniş kapsamlı kablosuz cihaz desteği de sunmaktadır. Mümkün olduğunca en fazla sayıda kablosuz cihazı desteklemekte ve çok çeşitli donanımlarla düzgün çalışacak ve sayısız usb ve diğer kablosuz cihazlarla uyumlu olacak şekilde kurulmuştur. Kali'de her paket onu yazan ve taahhüt eden geliştiricisi tarafından imzalanır. Sızma testi araçları genelde İngilizce yazılmış olsa da Kali çok dilli desteği sayesinde kullanıcının kendi ana dilinde çalışabilmesine, iş için ihtiyaç duyduğu araçları bulabilmesine imkân tanır. Kali tamamen özelleştirebilir. Kullanıcı Kali'yi çekirdeğe kadar kendine göre özelleştirebilir. Kali'nin Armel ve Armhf desteği de mevcuttur. Raspberry Pi gibi Arm tabanlı tek kartlı sistemler her geçen gün giderek daha ucuz ve yaygın hale geldiğinden hem Armhf hem Armel sistemleri için tamamen çalışan kurulumlar oluşturulmuştur [45].

Kali'nin BackTrack'te de bulunan özelliklerden biri de canlı önyükleme (live boot) özelliğidir. Kali önyükleme ortamı indirildiğinde bu bilgisayara yüklenebilir ya da canlı başlatabilir. Bu ortam DVD ya da taşınabilir bellekten çalıştırılabilir veya sabit sürücüye yüklenebilir. Bilgi depolanması için yazılabilir ortam yoksa her açılışta sıfırdan başlanır. Şekil 3.13.'te önyükleme seçenekleri gösterilmiştir [47].

Şekil 3.13. Kali önyükleme ekranı [47]

Kali kurulduğunda tıpkı Windows'ta olduğu gibi yüklü programların kısayollarını içeren bir uygulama menüsüyle karşılaşırız. Kali bu programları yazılımcısına veya program adına göre değil işlevselliğe göre gruplandırmıştır. Uygulama menüsünde bilgi toplama, güvenlik açığı analizi, web uygulama analizi, veri tabanı değerlendirmesi, şifre saldırıları, kablosuz saldırılar, tersine mühendislik, sömürü araçları, koklama ve sahtekarlık (sniffing & spoofing), sömürü sonrası, adli araçlar, raporlama araçları ve sosyal mühendislik araçları mevcuttur. Şekil 3.14.'te uygulama menüsü gösterilmiştir [47].

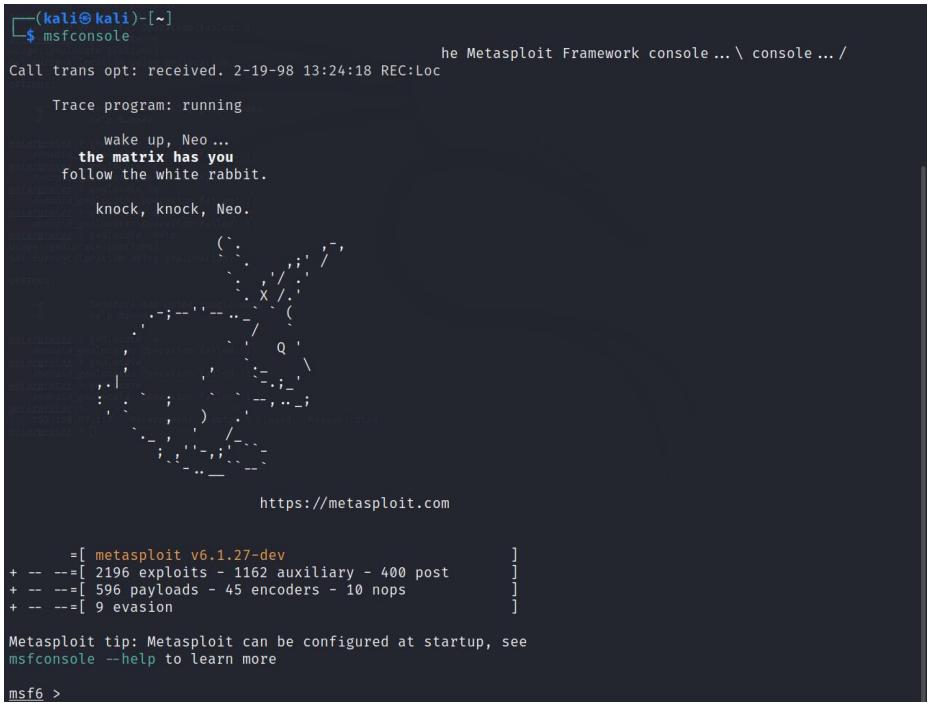


Şekil 3.14. Kali uygulama menüsü [47]

3.6. Metasploit

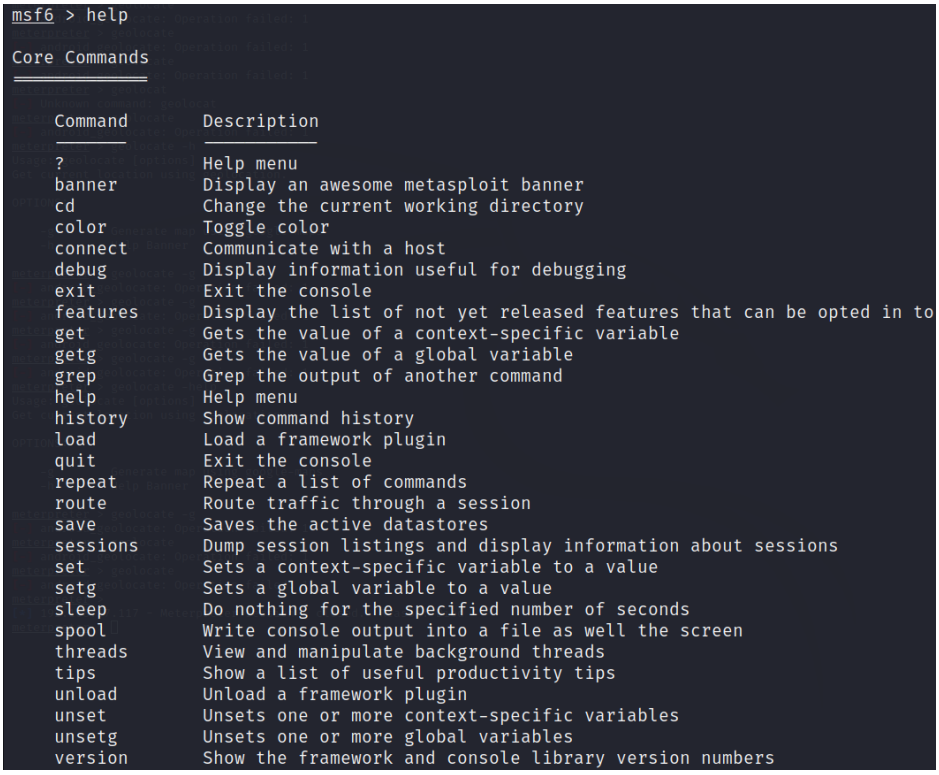
Metasploit dünyada en çok tercih edilen sızma testi aracı olup bu alanda ve bilgi güvenliği alanında en geniş açık kaynaklı projedir. Metasploit güvenlik testlerinin yapılmasında yeni bir çığır açmıştır. Metasploit projesinin bu kadar tercih edilmesindeki en önemli nedeni sistemlerin güvenliğinin sağlanması için gereken sızma testlerinin kolaylıkla yapılabilmesini sağlamasıdır. Metasploit yaygın tüm işletim sistemlerinde kullanılabilmektedir. Tüm işletim sistemlerinde de benzer süreçte çalışır. Metasploit Kali üzerinde hazır kurulu olarak gelmektedir [48].

Metasploit'i kullanmanın en çok tercih edilen yolu Metasploit'in kendi etkileşimli kabuğu (shell) olan msfconsole'dur [49]. Kali işletim sisteminde msfconsole komutu çalıştırıldığında gelen Metasploit etkileşimli arayüzü Şekil 3.15.'de gösterilmiştir.



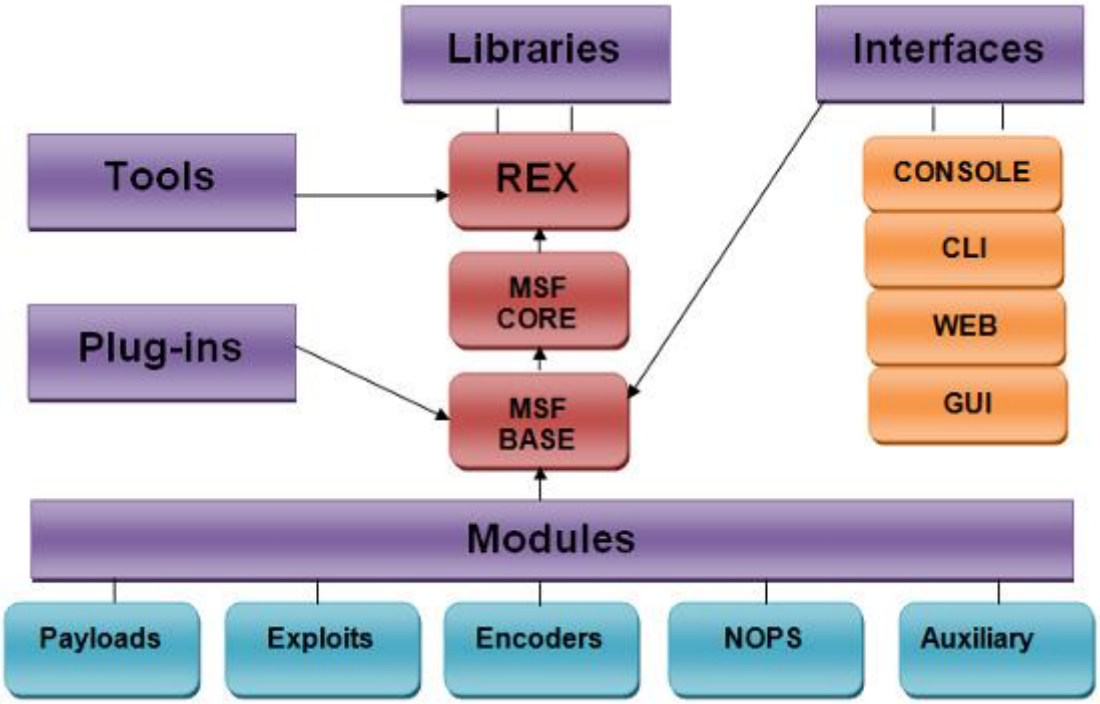
Şekil 3.15. Metasploit msfconsole arayüzü

Metasploit komutları ve açıklamalarının bir listesi help komutu kullanılarak konsol ekranına Şekil 3.16.'da gösterildiği gibi getirilmektedir.



Şekil 3.16. Metasploit komutları ve açıklamaları

Metasploit önemli modüller, kitaplıklar, eklentiler ve araçlar gibi birçok bileşen içerir. Metasploit mimarisinin şematik görünümü Şekil 3.17.'de gösterilmiştir [50].

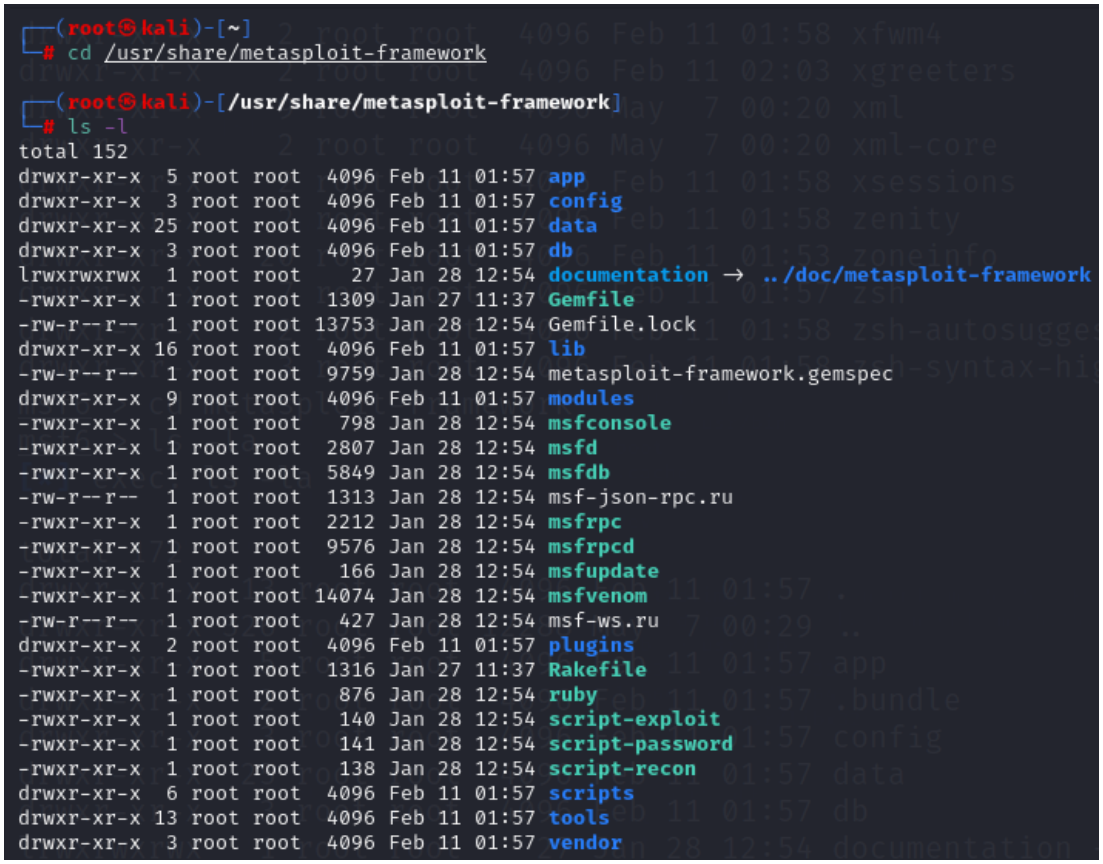


Şekil 3.17. Metasploit mimarisi [50]

Bir saldırganın ya da sızma testi uzmanının sisteme girmesine veya sistem güvenliğini tehlikeye atmasına izin veren zayıflıklara güvenlik açığı (vulnerability) denir. Bu zayıflık, uygulama yazılımlarında, işletim sisteminde hatta ağ protokollerinde bile görülebilir. Metasploit ile bu zayıflıklardan istifade edilir. Yine bir saldırganın ya da sızma testi uzmanının güvenlik açığı bulunan bir sistemden yararlanmasına ve güvenliğini tehlikeye atmasına izin veren kod parçaları exploit (istismar) olarak adlandırılmaktadır. Her güvenlik açığı için buna karşılık gelen bir exploit mevcuttur. Metasploit platformunda 2000'den daha fazla exploit mevcuttur. Bir sitemin güvenlik açığı ilgili exploit ile sömürüldükten sonra sistem üzerinde çalışan ve asıl işi yapan kodlara payload (yük) denilir. Genelde saldırgan ya da sızma testi uzmanı ile hedef cihaz arasında bağlantı kurmak için kullanılır. Metasploit üzerinde 500'den fazla payload mevcuttur [48].

Metasploit modüllerindeki Auxilary (yardımcı fonksiyonlar) ek araç ve komutlar içerir. Encoders (kodlayıcılar) kod ya da bilgiyi dönüştürmek için kullanılır. Nops (işlem yok) ise payloadın olağan dışı sonlanmasını önleyen talimatlardır [51].

Metasploit mimarisi Bash kabuğundaki (Bash shell) komut satırından da görülebilir. Bunun için Metasploit'in Kali'deki dizinine girildiğinde ve dizin içeriği listelendiğinde Şekil 3.18.'deki gibi görünmektedir [52].



Şekil 3.18. Metasploit mimarisine ait dizinler

Burada modules dizinine girildiğinde Şekil 3.19.'da görüleceği üzere Metasploit modüllerine ait dizinler mevcuttur. Bu dizin her biri ayrı bir modül tipi içeren altı alt dizin içermektedir [52].

```
┌──(root㉿kali)-[/usr/share/metasploit-framework]
└─# cd modules

┌──(root㉿kali)-[/usr/share/metasploit-framework/modules]
└─# ls -la
total 36
drwxr-xr-x  9 root root 4096 Feb 11 01:57 .
drwxr-xr-x 13 root root 4096 Feb 11 01:57 ..
drwxr-xr-x 22 root root 4096 Feb 11 01:57 auxiliary
drwxr-xr-x 12 root root 4096 Feb 11 01:57 encoders
drwxr-xr-x  3 root root 4096 Feb 11 01:57 evasion
drwxr-xr-x 22 root root 4096 Feb 11 01:57 exploits
drwxr-xr-x 11 root root 4096 Feb 11 01:57 nops
drwxr-xr-x  5 root root 4096 Feb 11 01:57 payloads
drwxr-xr-x 14 root root 4096 Feb 11 01:57 post
```

Şekil 3.19. Metasploit modülleri

Exploit dizinine girildiğinde bir sistemdeki kusur veya güvenlik açığından istifade etmek veya sömürmek için geliştirilmiş exploit kodlarına ait dizinler Şekil 3.20.'de gösterilmiştir [52].

```
┌──(root㉿kali)-[/usr/share/metasploit-framework/modules]
└─# cd exploits

┌──(root㉿kali)-[/usr/share/metasploit-framework/modules/exploits]
└─# ls -la
total 112
drwxr-xr-x 22 root root 4096 Feb 11 01:57 .
drwxr-xr-x  9 root root 4096 Feb 11 01:57 ..
drwxr-xr-x  3 root root 4096 Feb 11 01:57 aix
drwxr-xr-x  6 root root 4096 Feb 11 01:57 android
drwxr-xr-x  5 root root 4096 Feb 11 01:57 apple_ios
drwxr-xr-x  3 root root 4096 Feb 11 01:57 bsd
drwxr-xr-x  3 root root 4096 Feb 11 01:57 bsdi
drwxr-xr-x  3 root root 4096 Feb 11 01:57 dialup
-rw-r--r--  1 root root 6373 Jan 27 11:37 example_linux_priv_esc.rb
-rwxr-xr-x  1 root root 1819 Jan 27 11:37 example.py
-rw-r--r--  1 root root 2886 Jan 27 11:37 example.rb
-rw-r--r--  1 root root 7501 Jan 27 11:37 example_webapp.rb
drwxr-xr-x  3 root root 4096 Feb 11 01:57 firefox
drwxr-xr-x 10 root root 4096 Feb 11 01:57 freebsd
drwxr-xr-x  3 root root 4096 Feb 11 01:57 hpux
drwxr-xr-x  3 root root 4096 Feb 11 01:57 irix
drwxr-xr-x 23 root root 4096 Feb 11 01:57 linux
drwxr-xr-x  3 root root 4096 Feb 11 01:57 mainframe
drwxr-xr-x 28 root root 4096 Feb 11 01:57 multi
drwxr-xr-x  4 root root 4096 Feb 11 01:57 netware
drwxr-xr-x  3 root root 4096 Feb 11 01:57 openbsd
drwxr-xr-x 13 root root 4096 Feb 11 01:57 osx
drwxr-xr-x  4 root root 4096 Feb 11 01:57 qnx
drwxr-xr-x  9 root root 4096 Feb 11 01:57 solaris
drwxr-xr-x 14 root root 4096 Feb 11 01:57 unix
drwxr-xr-x 54 root root 4096 Feb 11 01:57 windows
```

Şekil 3.20. Exploit dizinleri

3.7. Wifiphisher

Wifiphisher, Man in the Middle (ortadaki adam) saldırılarında ve Evil Twin (Şeytani İkiz) saldırılarında kullanılan otomatikleştirilmiş bir sosyal mühendislik saldırı aracıdır. Bu saldırı aracı erişim noktasına bağlı cihazları ağdan düşürmek için deauthentication frameleri gönderir, erişim noktasının kopyasını çıkarır ve aynı zamanda bir NAT/DHCP sunucu kurarak hedef cihazın ikiz ağa bağlanmasını sağlar [53].

Wifiphisher wi-fi güvenlik testleri için de kullanılan sahte bir erişim noktasıdır. Wifiphisher kullanarak sızma testleri ve ortadaki adam saldırıları düzenlenilebilir. Wifiphisher ayrıca şifreleri yakalamak veya hedef cihaza zararlı yazılım bulaştırmak için kullanılabilir. Wifiphisher esnek bir uygulama olup düzinelerce argüman destekler. Wifiphisher'ın bir diğer özelliği ise modüler olmasıdır. Kullanıcılar hedef odaklı saldırılarda aracın işlevselliğini artırmak veya yeni senaryolar oluşturmak için Python'da modüller yazabilir. Kullanımı kolaydır. Etkileşimli metin kullanıcı arayüzü sayesinde kullanıcıya saldırının oluşturulmasında rehberlik eder. İleri düze kullanıcılar ise Wifiphisher'ın sunduğu zengin özelliklerden istifade eder. Geniş bir geliştirici ve kullanıcı topluluğu tarafından destek görmektedir. Tam kaynak koduyla ücretsiz olarak sunulmaktadır [54].

Wi-fi oltalama saldırıları iki adımdan oluşur. İlk adımda wi-fi istemcileri arasında ortadaki adam (MITM) pozisyonu alma süreçlerini kapsar. Wifiphisher bunun üstesinden gelebilmek için bir dizi farklı teknikler kullanır. Wifiphisher gerçek bir ağa benzeyen sahte ikiz ağlar oluşturur. Wi-fi istemcileri tarafından aranan halka açı bir ağ gibi görünen ağlar da oluşturabilir. Bu uygulama aynı zamanda istemcilerin bağlantılarını düşürmek ve kendi ağına çekmek için yetkisizleştirme (deauthenticate) ve ilişkilendirmeyi kaldır (disassociate) paketleri oluşturmaya devam eder. Bu durum Şekil 3.21.'de gösterilmiştir [55].

Şekil 3.21. Wifiphisher saldırı mantığı [55]

Sızma testi yapan kişi Wiphisher ile ortadaki adam saldırısı yapmak istediğinde bunun için birkaç teknik vardır. Mesela testi yapan veri koklama (sniffing) gerçekleştirebilir veya hedef cihazın güvenlik açıklarını tarayabilir. Wifiphisher ile hem hedef ortamdan hem de hedef kullanıcıdan veri toplayarak gelişmiş bir web oltalama saldırısı yapmak mümkündür. Örneğin Şekil 3.20.'de Wifiphisher Windows ağ yöneticisinin web tabanlı bir taklidini görüntüleyerek önceden paylaşılan anahtarı (pre-shared key) yakalamak için yayınlanan işaret çerçevelerinden (beacon fremes) ve http kullanıcı aracısı başlığından (user-agent) bilgi almaya çalışmaktadır [55].

Şekil 3.22. Wifiphisher ile önceden paylaşılan anahtarı yakalama [55]

3.8. İlgili Çalışmalar

Otomobillerde kullanılan multimedya cihazları üzerine yapılan çalışmalar incelendiğinde, Takahashi ve arkadaşları bu cihazlarda sistemin güvenlik açıklarından faydalanarak oluşabilecek güvenlik tehditlerini incelemiştir. Çalışmalarında araçların uzaktan kontrol servisleri üzerinde güvenlik analizleri yapmışlardır. Ayrıca araç içi ağ hizmetinin DOS (hizmet engelleme) saldırısı açısından analizini yapmışlardır [56].

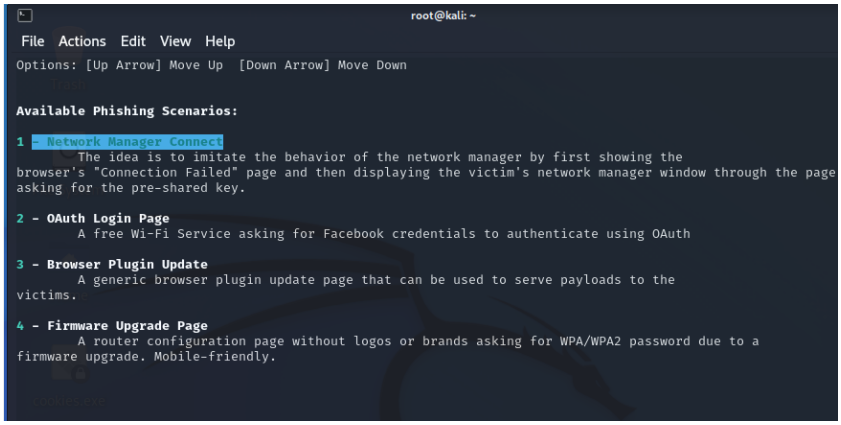
Mazloom ve arkadaşlarının yaptığı çalışmada ise araç kullanıcısının telefonunun kontrolünü ele geçiren bir saldırganın Mirorlink protokolü ve multimedya cihazındaki zafiyetler sayesinde aracın CAN veri yoluna zararlı mesajlar gönderilebileceği uygulamalı bir şekilde gösterilmeye çalışılmıştır [1].

Josephlal ve Adepu'nun yaptığı çalışmada bir test ortamı oluşturarak multimedya cihazının Wi-Fi yeteneklerindeki güvenlik açıklıkları port taraması yapan Nmap ve güvenlik açığı taraması yapan Nessus uygulamaları ile tespit edilmeye çalışılmış ve cihazla ilgili hassas bilgilere ulaşıldığı gösterilmiştir. Cihazın Android işletim sistemine zararlı bir yazılım yüklenerek cihazın dosya sistemine ulaşıldığı ifade edilmiştir. Ayrıca cihazın bağlı olduğu kablosuz ağa ağdan düşürme (deauthentication) paketleri gönderilerek DOS saldırısı gerçekleştirilmiştir [57].

BÖLÜM 4. UYGULAMA VE SONUÇLARI

4.1. Kullanıcının Wi-Fi Şifresinin Elde Edilmesi

Araç içerisindeki multimedya cihazlarının internete bağlanabilmesi için en çok tercih edilen yöntem akıllı telefon üzerinden bir hot spot ağı oluşturulmasıdır. Burada öncelikle multimedya cihazının bağlı olduğu ya da bağlanmaya çalıştığı erişim noktası tespit edilmiştir. Bu erişim noktası Kismet, Airodump-ng gibi herhangi bir ağ algılayıcısı kullanılarak tespit edilebilir. Bu ağa sızabilmek için öncelikle bu erişim noktasının ikizi oluşturulmuştur. Bu amaçla açık kaynak kodlu Wifiphisher yazılımından istifade edilmiştir. Erişim noktasının ikizi oluşturulduktan sonra captive portal (kısıtlama portalı) üzerinden yapılacak phishing (oltalama) saldırısı için sahte bir ağ bağlantı yöneticisi senaryosu Şekil 4.1.'de gösterildiği gibi hazırlanmaya başlanmıştır.

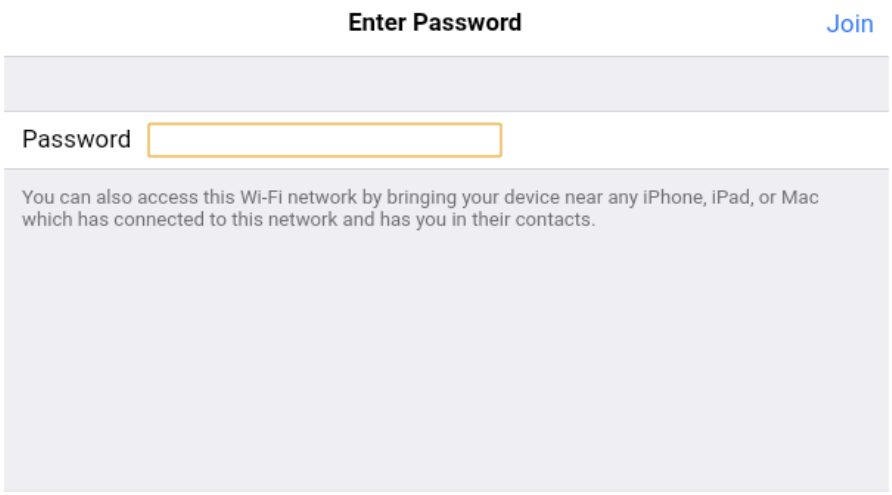


Şekil 4.1. Oltalama saldırısı senaryoları

Söz konusu multimedya cihazının bağlı olduğu ağdan düşürülerek ikiz ağa bağlanması için deauthentication yani ağdan düşürme saldırıları yapılmıştır. Bu saldırı bir çeşit DOS (Denial of Service) olarak düşünülebilir. Bu saldırıda erişim noktasına (Acces Point) bağlı olan cihazlara Deauthentication Frame yani ağ bağlantısının sonlanmasını

sağlayan paketler gönderilmiştir. Bu paketler Aireplay-ng veya benzeri bir paket üreticisi tarafından üretilebilir. Cihaz bağlı olduğu ağdan düşüp sahte ikiz ağa bağlanana kadar bu saldırı devam etmiştir.

Cihaz ikiz ağa bağlandıktan sonra seçilen bu senaryo ile Şekil 4.2.'de gösterildiği gibi captive portal üzerinden sahte bir web sayfasına yönlendirilerek kullanıcının wi-fi şifresi girmesi beklenmiştir. Bu sayfa kullanıcının gireceği şifreyi alarak bilgisayarımıza iletecektir.



Şekil 4.2. Sahte web sayfası

Kullanıcı wi-fi şifresini girdiğinde bu sahte web sayfası ile iletilen şifre Şekil 4.3.'te gösterildiği gibi yakalanmıştır.

Şekil 4.3. Yakalanan wi-fi şifresi

4.2. Zararlı Yazılımın Oluşturulması

Captive portal üzerinden sahte web sayfası ile gönderilecek zararlı yazılım Metasploit platformu üzerindeki Msfvenom modülü kullanılarak Şekil 4.4.'te gösterildiği şekilde oluşturulmuştur. Zararlı yazılım kullanıcıya bir güncelleme dosyası gibi gönderileceğinden bu yazılım "update" adıyla oluşturulmuştur.

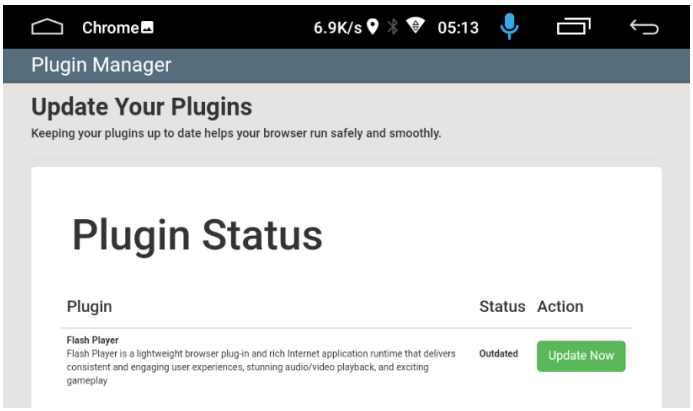
Şekil 4.4. Zararlı yazılımın oluşturulması

4.3. Zararlı Yazılımın Multimedya Cihazına Gönderilmesi

Cihazın tekrar deauthentication saldırıları ile bağlı olduğu ağdan düşürülerek ikiz ağa bağlanması sağlanmıştır. Cihaz ikiz ağa bağlandığında captive portal üzerinden Şekil 4.5.'te gösterildiği gibi zararlı yazılım kullanıcıya gönderilmiştir.

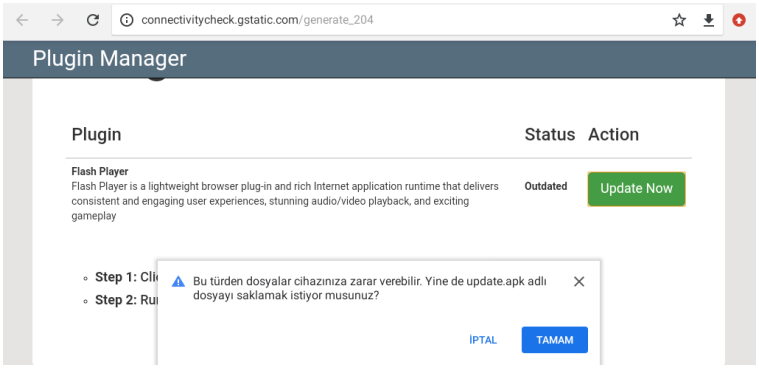
Şekil 4.5. Zararlı yazılımın gönderilmesi

Bu zararlı yazılım captive portal aracılığıyla Şekil 4.6.'da görüleceği şekilde sahte bir güncelleme sayfası şeklinde kullanıcının indirmesi sağlanmaktadır.



Şekil 4.6. Sahte güncelleme sayfası

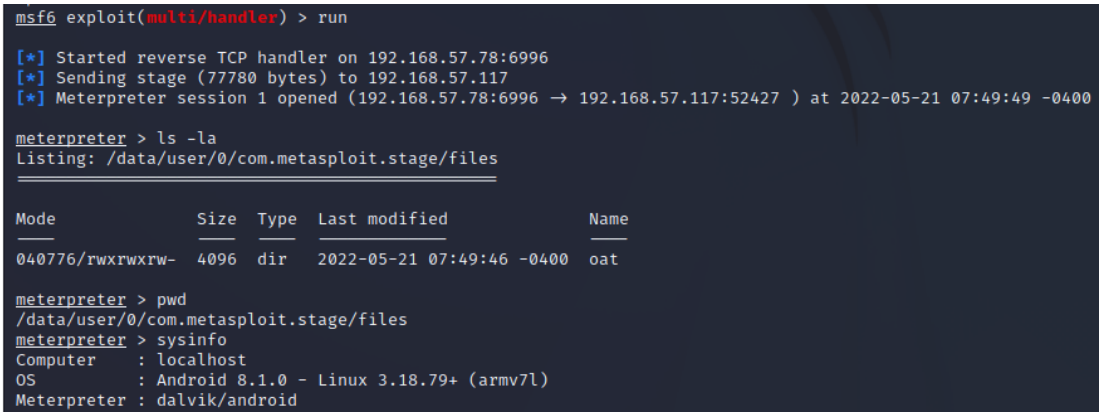
Kullanıcı güncelleme sandığı zararlı yazılımı indirmeye çalıştığında Android işletim sistemi tarafından Şekil 4.7.'de görüldüğü şekilde uyarılmıştır.



Şekil 4.7. Sistem uyarısı

4.4. Multimedya Cihazına Bağlanma

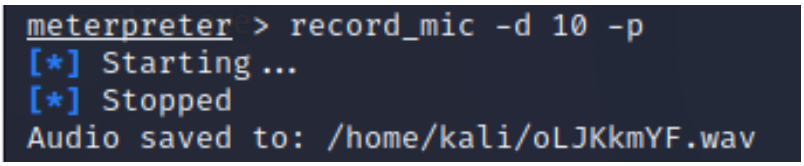
Kullanıcı güncelleme sandığı zararlı yazılımı kurduğunda Metasploit projesindeki multi-handler modülü ile multimedya cihazına Şekil 4.8.'de gösterildiği şekilde bağlanılmıştır. Burada sysinfo komutu ile multimedya cihazında kurulu olan işletim sistemi versiyonu ve Linux çekirdek versiyonu tespit edilmiştir.



Şekil 4.8. Multimedya cihazına bağlanma

4.5. Kullanıcının Sesini Kaydetme

Araç içerisindeki multimedya cihazına bağlandıktan sonra araç içerisindeki tüm konuşma ve sesler Şekil 4.9.'da gösterildiği şekilde bir süre kaydedilmiş ve daha sonra dinlenilmiştir.

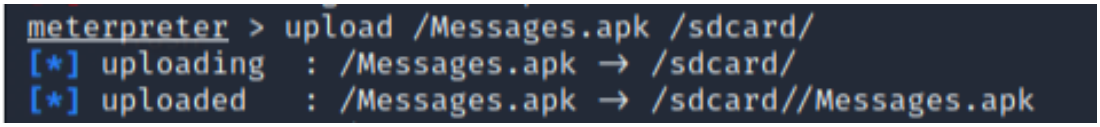


Şekil 4.9. Kullanıcının sesini kaydetme

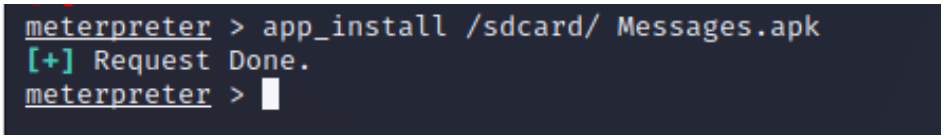
4.6. Kullanıcıya Mesaj Gönderme

Araç içerindeki kullanıcıya mesaj gönderebilmek için öncelikle mesaj uygulaması aracın multimedya cihazına Şekil 4.10.'da gösterildiği şekilde gönderilmiş ve kurulum işlemi Sekil 4.11.'deki gibi başlatılmıştır. Bu sayede multimedya cihazında paket

yükleyici açılmıştır. Kullanıcı istenen izinlere onay verdikten ve yüklemeyi kabul ettikten sonra uygulama başarılı bir şekilde cihaza kurulmuştur.

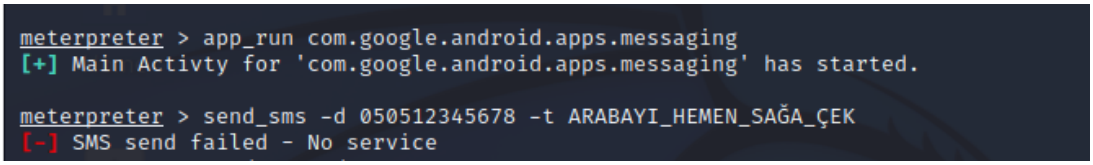


Şekil 4.10. Dosya gönderme



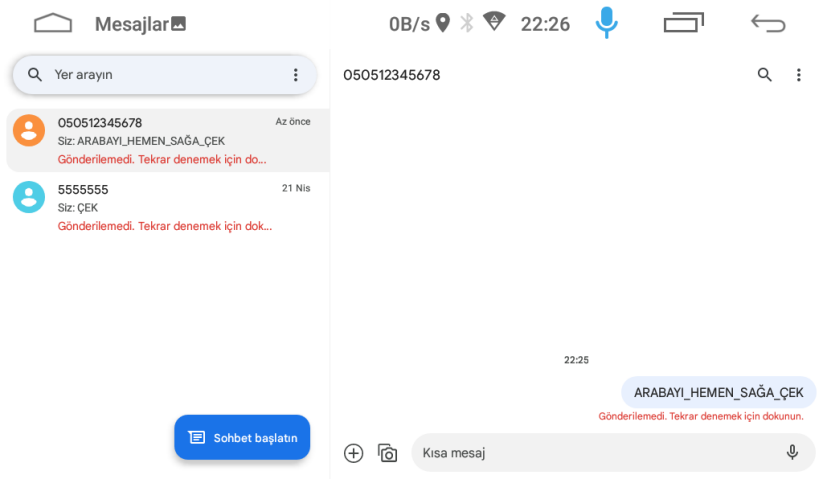
Şekil 4.11. Uygulama Yükleme

Mesaj uygulaması cihaza kurulduktan sonra Şekil 4.12.'de gösterildiği şekilde çalıştırılmış ve araç kullanıcısına mesaj gönderilmiştir.



Şekil 4.12. Mesaj gönderme

Şekil 4.12.'de bir hata mesajı görülmüş olsa da Şekil 4.13.'te görüleceği üzere mesaj kullanıcıya başarılı bir şekilde iletilmiştir.



Şekil 4.13. Gelen mesajlar

BÖLÜM 5. SONUÇ VE ÖNERİLER

Bu çalışmada otomobil içerisindeki multimedya cihazına başarılı bir şekilde sızılarak, kullanıcı verilerine ulaşılmış, kullanıcının haberi olmadan cihaza dosya gönderilmiş, araç içerisindeki sesler kaydedilmiş, daha da ileri gidilerek kullanıcı ile mesaj yoluyla iletişime geçilerek kullanıcı için ciddi bir tehdit oluşturulmuştur. Bu çalışmada kullanıcının standart bir kullanıcı olduğu ve internete bağlanabilmek için istenen tüm izinlere onay verdiği ve uygulamaları yüklediği kabul edilmiştir.

Bu çalışmada bazı aşamaların geçildiği kabul edilmiş ve bu aşmalarla uğraşılmamıştır. Bu aşamalar farklı tekniklerle geçilebilir. Bu çalışmada geçildikten sonra neler yapılabildiği üzerinde durulmuştur. Kullanmış olduğumuz multimedya cihazı ile yapılabilen işlemler bunlardır. Araçların kendi orijinal multimedya cihazları CAN BUS ile haberleşir ve bu sayede aracın bilgilerini çekerler. Araç yol bilgisayarı diye tabir edilen araçtan bilgi çağırma ve aracın bazı ayarlarını değiştirme gibi özellikler bu orijinal cihazlarla daha mümkündür. Bu sayede aracın lastik basıncı gibi önemli bilgilere ulaşılabilir ya da aracın hız sınırı ayarlanabilir. Bu multimedya sistemlerinde CAN ağına müdahale edildiğinde örneğin hız sınırı kullanıcı bilgisi dışında değiştirilebilir veya lastik basıncı olduğundan düşük ya da yüksek gösterilebilir ve buna benzer tehditler oluşturulabilir. Hatta park asistanı ya da otonom sürüş yeteneğine sahip bir araçta bu ağa ulaşıldığında aracın gaz, fren ve direksiyonuna hükmedilip ciddi riskler oluşturulabilir.

Bu tür siber saldırılardan korunmak için işletim sistemi tarafından belirtilen uyarılar dikkate alınmalı ve sistemin tüm izinlerini isteyen şüpheli uygulamalar kurulmamalıdır. Özellikle otomobillerdeki multimedya cihazlarında web sayfası üzerinden şifre girmekten kaçınılmalıdır.

KAYNAKLAR

[1] Mazloom, S., Rezaeirad M., Hunter, A., McCoy, D., A Security Analysis of an In Vehicle Infotainment and App Platform. Proceedings of the 10th Usenix Conference on Offensive Technologies, WOOT'16, 2016

[2] Palm, A., Gafvelin, B., Ethical Hacking of Android Auto in the Context of Road Safety. Examensarbete Inom Datateknik, Grundniva, 15 HP, Stockholm, Sverige, 1-3, 2021.

[3] Lu, H.J., Yu, Y., Research on WiFi Penetration Testing with Kali Linux. Hindawi, Complexity, Volume 2021

[4] Modi, V., Chandresh, P., Rogue Access Point Based DoS Attacks against 802.11 WLANs. International Journal of Advanced Research in Computer Science, 774, 2017.

[5] Liu, C., Yu, J., Detection & Analysis of Evil Twin Attack in Wireless Network. The Fourth Advanced International Conference on Telecommunications, IEEE, 2008.

[6] Chen, W.L., Wu, Q., A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal. Proceedings of the Asia-Pacific Advanced Network, 2010

[7] https://github.com/wifiphisher/wifiphisher, Erişim Tarihi: 22.05.2022.

[8] https://www.kali.org/tools/metasploit-framework, Erişim Tarihi: 22.05.2022.

[9] Valea, O., Oprisa, C., Towards Pentesting Automation Using the Metasploit Framework. 16th International Conference on Intelligent Computer Communication and Processing (ICCP), IEEE, 2020

[10] Kolli, Y., Mohd, T.K., Javaid, A.Y., Remote Desktop Backdoor Implementation with Reverse TCP Payload using Open Source Tools for Instructional Use. IEEE, 250, 2018.

[11] https://www.siberguvenlik.web.tr/index.php/2019/09/16/metasploit-framework-nedir-nasil-kullanilir, Erişim Tarihi: 23.05.2022.

[12] https://www.hackers-arise.com/post/2018/07/06/Metasploit-Basics-Part-13-Exploiting-Android-Mobile-Devices, Erişim Tarihi: 22.05.2022.

[13] https://www.offensive-security.com/metasploit-unleashed/msfvenom, Erişim Tarihi: 23.05.2022.

[14] https://www.hackers-arise.com/post/2017/07/31/metasploit-basics-part-9-using-msfvenom-to-create-custom-payloads, Erişim Tarihi: 23.05.2022.

[15] https://www.kursatoguzhanakinci.com/2015/07/msfvenom-kullanm-detayl.html, Erişim Tarihi: 23.05.2022.

[16] https://www.siberportal.org/red-team/penetration-testing/handling-connections-with-msf-multi-handler-exploit-module, Erişim Tarihi: 23.05.2022.

[17] Li, Z.N., Drew, M.S., Liu, J., Fundamentals of Multimedia, Springer, 3, 2021.

[18] https://www.tutorialspoint.com/multimedia/multimedia_introduction.htm, Erişim Tarihi: 13.06.2022.

[19] https://www.easytechjunkie.com/what-is-a-multimedia-device.htm, Erişim Tarihi: 14.06.2022.

[20] https://www.geeksforgeeks.org/what-is-multimedia, Erişim Tarihi: 15.06.2022.

[21] https://www.observerbd.com/details.php?id=166576, Erişim Tarihi: 15.06.2022.

[22] https://www.webtekno.com/htc-5g-vr-film-oyun-aciklamasi-h77174.html, Erişim Tarihi: 15.06.2022

[23] https://www.mindtree.com/insights/resources/how-leading-multimedia-software-company-uses-shotclasses-microlearning-train, Erişim Tarihi: 15.06.2022.

[24] https://www.otostil.com/multimedya-sistemleri/, Erişim Tarihi: 15.06.2022.

[25] https://navigasyonstore.com/neden-oto-multimedya-cihazi-almaliyim, Erişim Tarihi: 15.06.2022.

[26] https://www.einfochips.com/blog/everything-you-need-to-know-about-in-vehicle-infotainment-system, Erişim Tarihi: 15.06.2022.

[27] https://grapeup.com/blog/beyond-spotify-and-netflix-the-future-of-in-vehicle-infotainment-systems-in-connected-cars, Erişim Tarihi: 20.06.2022.

[28] https://www.webopedia.com/definitions/in-vehicle-infotainment-ivi, Erişim Tarihi: 15.06.2022.

[29] https://www.avnet.com/wps/portal/abacus/solutions/markets/automotive-and-transportation/automotive/comfort-infotainment-and-safety/automotive-infotainment, Erişim Tarihi: 15.06.2022.

[30] https://tr.motor1.com/news/590437/apple-yeni-nesil-carplay-sistemi, Erişim Tarihi: 20.06.2022.

[31] https://solutionmade.net/tr/honda-2022den-itibaren-otomobillerinde-android-auto-isletim-sistemini-standart-hale-getirmek-icin-google-ile-isbirligi-yapiyor, Erişim Tarihi: 20.06.2022.

[32] Dubey, A., Misra, A., Android Security Attack and Defenses, CRC Press, 11, 2013.

[33] http://techurosity.blogspot.com/2015/12/android-technology.html, Erişim Tarihi: 21.06.2022.

[34] https://www.dev2qa.com/android-architecture-components-introduction/, Erişim Tarihi: 20.06.2022.

[35] Makan, K., Alexandar-Bown, S., Android Security Cookbook, Packt Publishing, 1, 2013.

[36] https://meterpreter.org/android-becomes-the-most-vulnerable-operating-system-in-2019, Erişim Tarihi: 20.06.2022.

[37] https://thebestvpn.com/vulnerability-alerts/, Erişim Tarihi: 21.06.2022.

[38] Sessa, C., 50 Android Hacks, Manning Publications, xvii, 2013.

[39] https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-200901-202206, Erişim Tarihi: 20.06.2022.

[40] https://www.javatpoint.com/unix-operating-system, Erişim Tarihi: 20.06.2022.

[41] https://www.tutorialspoint.com/operating_system/os_linux.htm, Erişim Tarihi: 26.06.2022.

[42] https://www.javatpoint.com/what-is-linux, Erişim Tarihi: 26.06.2022.

[43] https://www.interviewbit.com/blog/linux-architecture/, Erişim Tarihi: 26.06.2022.

[44] Hertzog, R., O'Gorman, J., Aharoni, M., Kali Linux Revealed, Offsec Press, 2, 2017

[45] https://www.kali.org/features/, Erişim Tarihi: 28.06.2022.

[46] https://selflearning.io/study-material/website-penetration-testing/website-penetration-testing/chapter-7-linux-hacking/system-architecture-of-kali-linux, Erişim Tarihi: 28.06.2022.

[47] https://www.oreilly.com/library/view/learning-kali-linux/9781492028680/ch01.html, Erişim Tarihi: 28.06.2022.

[48] Teixeira, D., Singh, A., Agarwal, M., Metasploit Penteration Testing Cookbook, Packt Publishing, Third Editon, 8, 2018

[49] https://www.hackers-arise.com/post/2017/01/25/metasploit-part-1-getting-started-with-metasploit, Erişim Tarihi: 29.06.2022.

[50] https://hydrasky.com/network-security/metasploit-for-pentest-web-application, Erişim Tarihi: 29.06.2022.

[51] https://www.varonis.com/blog/what-is-metasploit, Erişim Tarihi: 29.06.2022.

[52] https://www.hackers-arise.com/post/2017/01/30/metasploit-part-2-metasploit-module-types, Erişim Tarihi: 29.06.2022.

[53] https://www.trazer.org/2017/04/kali-linux-wifiphisher.html, Erişim Tarihi: 23.05.2022.

[54] https://github.com/wifiphisher/wifiphisher, Erişim Tarihi: 29.06.2022.

[55] https://gitlab.com/kalilinux/packages/wifiphisher, Erişim Tarihi: 29.06.2022.

[56] Takahashi, J., Iwamura, M., Tanaka M., Security Threat Analysis of Automotive Infotainment Systems. IEEE 92nd Vehicular Technology Conference , 2020

[57] Josephlal, E. F. M., & Adepu, S., Vulnerability Analysis of an Automotive Infotainment System's WIFI Capability, IEEE 19th International Symposium on High Assurance Systems Engineering (HASE), 2019.

ÖZGEÇMİŞ

Adı Soyadı **:** Nasrullah Kancura

ÖĞRENİM DURUMU

Derece	Eğitim Birimi	Mezuniyet Yılı
Yüksek Lisans	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı/ Siber Güvenlik Pr.	Devam ediyor
Lisans	Sakarya Üniversitesi / Bilgisayar ve Bilişim Bilimleri Fakültesi / Bilgisayar Mühendisliği	2015
Lisans	Süleyman Demirel Üniversitesi / Mühendislik Fakültesi / Elektronik ve Haberleşme Mühendisliği	2011

İŞ DENEYİMİ

Yıl	Yer	Görev
2011-Halen	Türk Standardları Enstitüsü	Mühendis

YABANCI DİL

İngilizce