
GAZİ ÜNİVERSİTESİ
Gazi
1926

# GÖMÜLÜ SİSTEMLERDE SİBER GÜVENLİK

**Seda ŞANOĞLU**

**YÜKSEK LİSANS TEZİ**
**BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**TEMMUZ 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.

İmza
Seda ŞANOĞLU
...../……/……

GÖMÜLÜ SİSTEMLERDE SİBER GÜVENLİK

(Yüksek Lisans Tezi)

Seda ŞANOĞLU

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Temmuz 2021

## ÖZET

Kritik sektörler başta olmak üzere ulaşım, fabrika otomasyonu, ticaret ve finans, sağlık hizmetleri, akıllı ev, akıllı şehir ve diğer birçok alanda algılama, izleme, iletişim ve kontrol için yaygın olarak kullanılan gömülü sistemler hayatımızın ayrılmaz bir parçası haline gelmiştir. Bu sebeple bu sistemlerde yaşanacak beklenmedik davranışlar yaşamın günlük işleyişini etkilemekte ve büyük sorunlara neden olmaktadır. Özellikle Endüstriyel IoT gibi kritik altyapıların işletilmesinde de yaygın olarak kullanıldıkları dikkate alındığında, siber açıklıklarının istismar edilmesi sonucunda bu sistemlerde meydana gelecek bir aksaklık, kritik altyapıların en önemli güvenlik bileşeni olan işlerliğe önemli zararlar verebilecektir. Gömülü sistemlerin yaygın kullanımının artmasıyla nesnelerin internetine bağlantıları da artmaktadır. Birbirine bağlı cihaz sayısının artışı da beraberinde güvenlik sorunlarını getirmiştir. Gömülü cihazlarda güvenliğin önemine vurgu yapmak ve siber saldırıların cihazlar üzerindeki etkilerini incelemek maksadıyla bu çalışmada, oluşturulan sınama ortamında ağa bağlı bir gömülü sisteme DoS (Denial of Service), MitM (Man in the Middle) ve Process Öldürme saldırıları gerçekleştirilmiştir. Deney ortamında Raspberry Pi bilgisayarı ağa bağlı bir gömülü sistem cihazı olarak tasarlanmıştır. Ağda yer alan bir Windows bilgisayar ile veri alışverişi gerçekleştiren Raspberry Pi'ye kötü niyetli Kali makinesinden saldırılar gerçekleştirilmiştir. Cihaza yapılan saldırıların sisteme etkileri ve sonuçları analiz edilmiştir. Raspberry Pi özelinde gerçekleştirilen bu saldırıların diğer gömülü sistem cihazlarının güvenliğine ışık tutması amaçlanmaktadır.

| | | |
|---|---|---|
| Bilim Kodu | : | 92403 |
| Anahtar Kelimeler | : | Gömülü sistemler, siber güvenlik, siber saldırı, raspberry pi, nesnelerin interneti |
| Sayfa Adedi | : | 61 |
| Danışman | : | Prof. Dr. Ercan Nurcan YILMAZ |

CYBER SECURITY IN EMBEDDED SYSTEMS

(M. Sc. Thesis)

Seda ŞANOĞLU

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

July 2021

## ABSTRACT

Embedded systems, which are widely used for detection, monitoring, communication and control in critical sectors, especially in transportation, factory automation, trade and finance, healthcare, smart home, smart city and many other areas, have become an integral part of our lives. For this reason, unexpected behaviors to be experienced in these systems affect the daily functioning of life and cause serious problems. Considering that they are widely used in the operation of critical infrastructures such as Industrial IoT, a malfunction in these systems as a result of exploiting cyber vulnerabilities can cause significant damage to the operability, which is the most important security component of critical infrastructures. With the widespread use of embedded systems, their connections to the Internet of Things are also increasing. The increase in the number of connected devices also emerges new security problems. In this study, in order to emphasize the importance of security in embedded devices and to examine the effects of cyber attacks on devices, DoS (Denial of Service), MitM (Man in the Middle) and Process Kill attacks have been carried out on an embedded system connected to the network in the established testbed. In the experimental environment, Raspberry Pi is designed as an embedded system device connected to the network. Attacks have been carried out from the malicious system (Kali) to the Raspberry Pi that have exchanged data with a Windows computer on the network. The effects and results of the attacks on the device on the system have been analyzed. These attacks carried out specifically for Raspberry Pi are aimed to enlighten on the security of other embedded system devices.

| | | |
|---|---|---|
| Science Code | : | 92403 |
| Key Words | : | Embedded systems, cyber security, cyber attack, raspberry pi, internet of things |
| Page Number | : | 61 |
| Supervisor | : | Prof. Dr. Ercan Nurcan YILMAZ |

# TEŞEKKÜR

Tezin hazırlanma aşamasında değerli katkılarından dolayı danışmanım Sayın Prof. Dr. Ercan Nurcan YILMAZ'a, yüksek lisans çalışmam boyunca göstermiş olduğu sevgi ve anlayış ile bana destek olan çok değerli Eşim ile beni bugünlere getiren Babam ve Annem'e sonsuz teşekkürlerimi sunmayı borç bilirim.

# İÇİNDEKİLER

**Sayfa**

ÖZET ..... iv

ABSTRACT ..... v

TEŞEKKÜR ..... vi

İÇİNDEKİLER ..... vii

ÇİZELGELERİN LİSTESİ ..... x

ŞEKİLLERİN LİSTESİ ..... xi

SİMGELER VE KISALTMALAR ..... xiii

1. GİRİŞ ..... 1

2. LİTERATÜR TARAMASI ..... 3

3. GÖMÜLÜ SİSTEMLER ..... 11

3.1. Gömülü Sistemlere Genel Bakış ..... 11

3.2. Gömülü Sistem Çeşitleri ..... 13

3.2.1. Bağımsız gömülü sistemler ..... 13

3.2.2. Gerçek zamanlı gömülü sistemler ..... 13

3.2.3. Ağ bağlantılı gömülü sistemler ..... 13

3.2.4. Mobil gömülü sistemler ..... 13

3.3. Gömülü Sistemlerin Tarihçesi ..... 14

3.4. Gömülü Sistemlerde Siber Güvenlik ..... 16

3.5. Gömülü Sistem Güvenliğinde Karşılaşılan Zorluklar ..... 17

3.5.1. Zayıf güvenlik tasarımı ..... 18

3.5.2. Pazarlama süresi ..... 18

3.5.3. Güvenlik maliyeti ..... 18

3.5.4. Cihazların güncellenme zorluğu ..... 18

**Sayfa**

3.5.5. Sınırlı kaynaklar ..... 19
3.5.6. Standart olmayan işletim sistemleri ..... 19
3.6. Güvenlik Zafiyetleri ve Yapılan Saldırılar ..... 19
3.6.1. Enerji drenajı ..... 19
3.6.2. Fiziksel izinsiz giriş ..... 20
3.6.3. Ağa izinsiz giriş ..... 20
3.6.4. Bilgi hırsızlığı ..... 20
3.6.5. Sahte bilgilerin tanıtımı ..... 20
3.6.6. Termal olaylar ..... 20
3.6.7. Sistemlerin başka amaçlar için yeniden programlanması ..... 21
3.7. Gömülü Sistemlerde Güvenlik Gereksinimleri ..... 21
3.7.1. Kullanılabilirlik / Erişilebilirlik ..... 21
3.7.2. Bütünlük ..... 22
3.7.3. Gizlilik ..... 22
4. RASPBERRY PI ..... 25
4.1. Raspberry Pi'ye Genel Bakış ..... 25
4.2. Avantajlar ve Dezavantajlar ..... 25
4.3. Raspberry Pi'nin Gelişimi ..... 26
5. GÜVENLİK TESTİ METODOLOJİLERİ ..... 27
5.1. OWASP ..... 27
5.2. OSSTMM ..... 27
5.3. ISSAF ..... 28
5.4. NIST SP 800-115 ..... 28
5.5. PTES ..... 28

**Sayfa**

6. DENEY VE ANALİZ AŞAMASI ..... 29

6.1. Test Ortamının Hazırlanması ..... 29

6.2. Hizmet Dışı Bırakma Saldırısı (DoS) / Pseudo (Yalancı) DDoS ..... 33

6.3. MitM Saldırısı ..... 37

6.4. Süreç Öldürme Saldırısı ..... 40

6.5. Analiz Sonuçları ..... 48

7. SONUÇ VE ÖNERİLER ..... 51

KAYNAKLAR ..... 53

ÖZGEÇMİŞ ..... 61

# ÇİZELGELERİN LİSTESİ

**Çizelge** **Sayfa**

Çizelge 2.1. Raspberry Pi'nin siber güvenliği üzerine yapılan çalışmalar ..... 5

Çizelge 3.1. Gömülü sistemlerin kullanım alanları..... 11

Çizelge 3.2. Genel amaçlı bilgisayarlar ve gömülü sistemlerin karşılaştırılması ..... 12

Çizelge 3.3. Gömülü sistemlerin gelişim süreci ..... 14

Çizelge 6.1. Deney ortamında kullanılan cihaz bilgileri..... 30

Çizelge 6.2. Gerçekleştirilen saldırılar ve başarı durumları..... 49

# ŞEKİLLERİN LİSTESİ

**Şekil** **Sayfa**

Şekil 3.1. Bilgi güvenliği unsurları ..... 21

Şekil 6.1. Test topolojisi ..... 29

Şekil 6.2. Ledin yanıp sönmesini sağlayan python kodu ..... 31

Şekil 6.3. Ledin yandığı esnada alınan görüntüsü ..... 31

Şekil 6.4. Sunucu (Windows) tarafı soket programlama python kodu ..... 32

Şekil 6.5. İstemci (Raspberry Pi) tarafı soket programlama python kodu ..... 32

Şekil 6.6. Hizmet dışı bırakma daldırısı (DoS) akış diyagramı ..... 34

Şekil 6.7. Nmap aracı ile ağ taraması ..... 35

Şekil 6.8. Saldırı öncesi Raspberry Pi'nin durumu ..... 35

Şekil 6.9. Hping3 saldırısı ve wireshark ile gönderilen paketlerin görülmesi ..... 36

Şekil 6.10. Saldırı esnasında Raspberry Pi'nin durumu ..... 37

Şekil 6.11. MitM saldırısı akış diyagramı ..... 38

Şekil 6.12. Nmap aracı ile ağ taraması ..... 39

Şekil 6.13. Ettercap aracı ile hedeflerin ARP tablosunun zehirlenmesi ..... 39

Şekil 6.14. Led verisinin ele geçirilmesi ..... 40

Şekil 6.15. Süreç öldürme saldırısı akış diyagramı ..... 41

Şekil 6.16. Metasploit aracı ..... 42

Şekil 6.17. Metasploit aracında kullanılacak istismar modülünün seçilmesi ..... 43

Şekil 6.18. Metasploit aracında gerekli parametrelerin tanımlanması ..... 44

Şekil 6.19. Msfvenom aracı ile payload oluşturma ..... 45

Şekil 6.20. Raspberry Pi'de payload çalıştırılması ..... 45

Şekil 6.21. Kali ile Raspberry Pi arasındaki bağlantının kurulması ..... 46

Şekil 6.22. Raspberry Pi'nin bilgilerini görmek için sysinfo komutunu kullanma ..... 46

**Şekil** **Sayfa**

Şekil 6.23. Raspberry Pi üzerindeki dosya ve klasörlerin listelenmesi ..... 47

Şekil 6.24. Çalışan uygulamaların listelenmesi ve led2.py uygulamasının sonlandırılması ..... 47

Şekil 6.25. Raspberry Pi üzerinde uygulamanın sonlandığının görülmesi ..... 48

# SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

| Kısaltmalar | Açıklamalar |
|---|---|
| **ADC** | Analog Digital Converter |
| **ARP** | Address Resolution Protocol |
| **BIOS** | Basic Input Output System |
| **CPU** | Central Processsing Unit |
| **DDoS** | Distributed Denial of Service |
| **DEMA** | Differential Electromagnetic Analysis |
| **DoS** | Denial of Service |
| **GPIO** | General Purpose Input Output |
| **IoT** | Internet of Things |
| **ISSAF** | Information Systems Security Assesment Framework |
| **MAC** | Media Access Control |
| **MitM** | Man In The Middle |
| **NIST** | National Institute of Standards and Technology |
| **NTP** | Network Time Protocol |
| **OSSTM** | Open Source Security Testing Methodology |
| **OWASP** | Open Web Application Security Project |
| **PTES** | Penetration Testing Execution Standard |
| **RAM** | Random Access Memory |
| **ROM** | Read Only Memory |
| **RTC** | Real Time Clock |
| **TCP** | Transmission Control Protocol |
| **UDP** | User Datagram Protocol |

# 1. GİRİŞ

Gelişen teknoloji ile birlikte cihaz çeşitliliğinin artması ve bu cihazların nesnelerin interneti ile birbirine bağlanması bilginin en değerli varlık olduğu çağımızda gömülü sistemlerde güvenliğin önemini hızla artırmıştır. Birçok farklı marka ve modelde üretilen gömülü sistem kartlarının olması bu ürünlerin fiyatlarını da oldukça cazip hale getirmiştir. Kolayca erişilebilen bu kartların en yaygın kullanılanlarının başında Raspberry Pi ve Arduino gibi ürünler gelmektedir. Söz konusu tek kartlı bilgisayarlarla kolaylıkla gömülü sistem uygulamaları geliştirmek mümkün hale gelmiştir. Bu sistemlerin kullanımının artması ve sağladığı etkinlik, düşük maliyet, hız gibi faydalar insan hayatına önemli katkılar sağlamaktadır. Bu faydaların yanında, siber güvenlik açısından zafiyetlerinin var olması, üreticiler tarafından gerekli siber güvenlik testlerinin gerçekleştirilmemesi önemli bir eksikliktir.

Raspberry Pi, gelişiminden günümüze kadar akıllı ev çözümleri, robotik sistemler ve nesnelerin interneti alanlarında geniş çaplı projelerde kullanım alanı elde etmiştir. Maliyetinin düşük, boyutunun küçük ve erişilebilirliğinin kolay olması Raspberry Pi'nin gömülü sistem uygulamalarında kullanımını artırmıştır. Gömülü sistem uygulamalarında kullanımının artmasıyla birlikte, bu tek kartlı bilgisayar sisteminin zafiyetlerinden yararlanmak isteyen saldırganların sayısı artmıştır. Bu sebeple Raspberry Pi'nin gömülü sistemlere başarılı bir şekilde entegrasyonu için güvenlik boyutu çok önemlidir. Gömülü sistem güvenliği ise hala gelişmekte olan bir kavramdır. Yaşanan bu gelişmeler doğrultusunda öncelikle bu çalışmanın ikinci bölümünde bir literatür taraması gerçekleştirilmiştir. Bu bölümde, gömülü sistemlerin güvenliğine yönelik hangi araştırmaların yapıldığı incelenmiş ve gömülü sistem uygulamalarında kullanılan Raspberry Pi'nin hangi çalışmalara konu olduğuna değinilmiştir. Ayrıca Raspberry Pi'nin siber güvenlik kavramı etrafında hangi çalışmalarda ne amaçlarla kullanıldığına yönelik bir inceleme gerçekleştirilerek sonuçlar bir çizelgede kategorize edilmiştir.

Çalışmanın üçüncü bölümünde gömülü sistemlerin genel özellikleri, kullanım alanları ve gelişim süreci ele alınmış, sistemlerin güvenlik zafiyetlerinin neler olduğuna değinilmiştir. Çalışmanın dördüncü bölümünde Raspberry Pi'ye odaklanılmış, özelliklerinden ve gelişim sürecinden bahsedilmiştir. Çalışmanın beşinci bölümünde ise uluslararası güvenlik testi metodolojilerinden OWASP, OSSTMM, ISSAF, NIST SP 800-115 ve PTES'e değinilmiştir.

Son olarak çalışmanın altıncı bölümünde gömülü sistem uygulamalarında kullanılan Raspberry Pi bilgisayarına yönelik önemli saldırı türleri olan DoS, MitM ve Süreç Öldürme saldırıları gerçekleştirilmiştir. Oluşturulan deney ortamında Raspberry Pi'ye GPIO pinleri aracılığıyla led devresi bağlanmış olup bilgisayar gömülü sistem cihazı olarak tasarlanmıştır. Ağda yer alan bir Windows makineye sürekli olarak led verilerini gönderen Raspberry Pi, saldırgan Kali bilgisayarının DoS, MitM ve Süreç Öldürme saldırılarına maruz bırakılmıştır. Gerçekleştirilen söz konusu saldırılar analiz edilerek Raspberry Pi'nin bu saldırılara karşı davranışları ve sistem üzerindeki etkileri incelenmiştir. Çalışma Raspberry Pi özelinde gerçekleştirilmesine rağmen diğer gömülü sistemler içinde yol gösterici bir nitelik taşımaktadır.

# 2. LİTERATÜR TARAMASI

Genel amaçlı bilgisayarların ve yazılım uygulamalarının güvenliği konusunda çok sayıda araştırma yapılmış olmasına rağmen, donanım ve gömülü sistem güvenliği nispeten yeni ve gelişmekte olan bir araştırma alanıdır. Bu çalışma kapsamında yapılan literatür taraması neticesinde gömülü sistemlerde siber güvenlik çatısı altında yapılan bazı çalışmaların olduğu görülmüştür. Bu çalışmalar ise sistemlere yapılan saldırılar, sistemlerin zafiyetleri ve siber güvenliğinin incelenmesi kapsamında yoğunlaşmaktadır.

Örneğin, Çakır ve Özcanhan yaptıkları çalışmada gömülü sistemlere yapılan saldırıları incelemiş ve ağ bağlantılı gömülü sistemlerin güvenliğinin sağlanmasına yönelik bir standart geliştirmeye çalışmışlardır. IPsec standardının sadeleştirilerek, gömülü sistem içeren cihazların tümüne güvenlik özelliği kazandırılması amaçlanmıştır [1].

Chen ve arkadaşları ise gömülü sistemlerde ağ güvenliğine ve ağ saldırılarına yönelik bir çalışma yapmıştır. Gömülü sistemlerde ağ güvenliğinin iyileştirilmesine yönelik adımların ağ saldırılarının nasıl gerçekleştiğinin iyi bir şekilde anlaşılmasından geçtiğini ve bir güvenlik protokolü oluşturularak gömülü sistem ağlarının güvenliğinin güçlendirilmesi gerektiğini ifade etmişlerdir [2].

Diğer bir çalışmada ise yazarlar DoS ataklarının mobil robot düğümleri üzerindeki etkilerini incelenmiş ve hangi parametrelerin (CPU, RAM, Güç Tüketimi) saldırıdan etkilendiğinin tespit edilmesine yönelik bir deney gerçekleştirmişlerdir. Bu analiz, saldırıları tespit etmek için hangi parametrelerin değerlendirilmesinin uygun olduğunu anlamayı mümkün kılmıştır [3].

Literatürde Raspberry Pi özelinde yapılan çalışmalar incelendiğinde cihazın güvenlik kapsamları ele alınmadan genellikle basit bir gömülü sistem cihazı olarak kullanıldığı görülmektedir. Örneğin Vujovic ve Maksimovic yaptığı çalışmada ev otomasyonu sisteminde Raspberry Pi'yi binalarda yangın izleme ve tespit sistemi olarak tasarlamıştır [4]. Çalışma kapsamında ağa bağlı olan cihazın kötü niyetli saldırganlar tarafından ele geçirilme ihtimalini düşünmemiş cihazı bir etkileşim aracı olarak kullanmıştır. Diğer bir makalede Gupta ve diğerleri, Raspberry Pi kullanarak Elektrokardiyogram ve diğer hayati parametreleri sürekli olarak izlemek için bir sistem tasarlanmıştır [5]. Bu sistemin düşük güç

tüketimi ve çoklu görev kabiliyeti olan Raspberry Pi cihazı sayesinde tüm hastanelere kolaylıkla kurulabilir olduğuna değinilmiştir. Bu çalışmada da yazarlar cihaza güvenlik bakış açısıyla yaklaşmamış, cihazın maliyetinin uygun olması ve işlevselliğine vurgu yapmıştır.

Tüm bu araştırmalar kapsamda Raspberry Pi'nin siber güvenlik kavramı çerçevesinde literatürde hangi çalışmalara konu olduğuna yönelik bir literatür taraması gerçekleştirilmiştir. Yapılan çalışmalar değerlendirildiğinde cihazın daha çok bir siber güvenlik aracı olarak (saldırı tespit ve önleme sistemi, balküpü, trafik analizi) yapılandırılıp kullanıldığı görülmüştür. Ayrıca cihazın risk değerlendirmelerinin yapıldığı, güvenlik açıklıklarının incelendiği ve cihaza yapılan saldırıların olduğu birtakım çalışmalar da bulunmaktadır. Araştırma sonucunda incelenen çalışmalar ise alt kategorilere ayrılarak çalışmanın amacı, kullanılan yöntem ve uygulama ortamına göre Çizelge 2.1'de sınıflandırılmıştır.

Çizelge 2.1. Raspberry Pi'nin siber güvenliği üzerine yapılan çalışmalar

| Kategori | Alt Kategori | Yıl | Amaç/Odak | Kullanılan Araçlar/Yöntemler/Standartlar | Uygulama | Atıf |
|---|---|---|---|---|---|---|
| Risk Değerlendirmesi | Risk Değerlendirmesi | 2015 | Risk tahmini | NIST SP 800-30 ve NIST SP 800-37 Standartları | Raspberry Pi (Debian 7.0-Wheezy) üzerinde Kali Linux, DSL Modem kullanılarak yapıldı. | [6] |
| | Risk Yönetimi | 2018 | IoT Güvenlik Risk Yönetimi Referans Modeli Oluşturmak | SRM (Güvenlik Risk Yönetimi Modeli) | Raspberry Pi tarafından kontrol edilen bir akıllı ev sistemi üzerinde uygulanmıştır. | [7] |
| | Gömülü Sistemlere Yönelik Güvenlik Standardı Geliştirilmesi | 2011 | IPSec standardının sadeleştirilerek gömülü sistemlerde uygulanması | IPSec Standardı | Test Ortamı | [1] |
| | Dağıtık Güvenlik Açığı Değerlendirme Mimarisi | 2016 | Sızma testi ve güvenlik açığı değerlendirmesi için uygun fiyatlı çözüm sunmak | Raspberry Pi 2 Model B, OpenVASi Metasploit, Phyton ve PHP Betikleri | Test Ortamı | [8] |
| | Sızma Testi ve Güvenlik Açığı Değerlendirmesi | 2017 | Raspberry Pi'yi akıllı şehir kaynakları üzerinde penetrasyon testi yapmak için kullanmak | Raspberry Pi 3 Model B | Akıllı Şehirler Test Ortamı, Kali Linux, Nessus, Nmapi IBM AppScan | [9] |
| | Şifreleme Algoritmalarının Analizi | 2018 | Raspberry Pi'de en bilinen şifreleme algoritmalarının bir karşılaştırmasını sunmaktadır. | DES-64, 3DES-64, AES-128, AES-192, AES-256, MD5, SHA-1, SHA-256, SHA-512, RSA, DSA, ECDSA | Raspberry Pi 3 Model B | [10] |

Çizelge 2.1. (devam) Raspberry Pi'nin siber güvenliği üzerine yapılan çalışmalar

| Kategori | Alt Kategori | Yıl | Amaç/Odak | Kullanılan Araçlar/Yöntemler/Standartlar | Uygulama | Atıf |
|---|---|---|---|---|---|---|
| Saldırı | Yan Kanal Saldırısı | 2017 | Raspberry Pi üzerine uygulanan algoritmaların yan kanal saldırısına karşı güvenilirliği | Montgomery Güç Merdiveni Algoritması, Soldan Sağa Binary Yöntem, RSA | Raspberry Pi 3 Model B | [11] |
| | Yan Kanal Saldırısı | 2019 | Raspberry Pi üzerinde gerçeklenmiş bir AES algoritmasının yan kanal saldırısına karşı | AES Algoritması, DEMA Saldırısı | Raspberry Pi | [12] |
| | DDoS | 2016 | DDoS saldırısı yapan botnetlerin analizi ve değerlendirilmesi | UDP ve TCP Flood | Raspberry Pi | [13] |
| | DDoS | 2019 | Raspberry Pi üzerinde simüle edilen IoT cihazına Mirai saldırısını gerçekleştirmek | Mirai Kötücülü | Raspberry Pi Zero, Raspberry Pi 3 B+, Command and Control Server (C&C) | [14] |
| | DDoS | 2019 | İnternet üzerinden Raspberry Pi cihazlarına saldıran kötü amaçlı yazılımlara odaklanılmıştır. | UNIX_PIMINE Zararlısı | Raspberry Pi, Cowrie Honeypot | [15] |
| | DOS, SSH | 2017 | Saldırıların Raspberry Pi üzerindeki etkileri | Nmap,Angry,OpenVAS,Nessus, Armitage,Metasploit, hping3,CeWL, THC-Hydra, Wireshark,Netstat | Raspberry Pi B+ | [16] |
| | Dağıtılmış Yansıtıcı DoS Saldırısı (DRDoS) | 2018 | Saldırının uygulanan 4 cihaz üzerindeki etkileri | DRDoS saldırısının gerçekleştirilmesi | Akıllı ampuller, IP Kamera , Ağ yazıcısı, Raspberry Pi | [17] |

Çizelge 2.1. (devam) Raspberry Pi'nin siber güvenliği üzerine yapılan çalışmalar

| Kategori | Alt Kategori | Yıl | Amaç/Odak | Kullanılan Araçlar/Yöntemler/Standartlar | Uygulama | Atıf |
|---|---|---|---|---|---|---|
| IDS/IPS/Balküpü/ Paket Analizi | Saldırı Tespit Sistemi | 2015 | Düşük maliyetli IDS | Iperf, Sarf, Snort, Arc Linux ARM | Raspberry Pi Model B+, Raspberry Pi 2 Model B | [18] |
| | Balküpü | 2016 | Raspberry Pi'nin Balküpü olarak kullanılması | Dionaea, Glastopf, Kippo, Snort, Raspberry Pi | Test Ortamı | [19] |
| | Saldırı Tespit Sistemi | 2015 | Raspberry Pi üzerinde çalışan IDS performanslarının incelenmesi | Snort IDS, Bro IDS | Raspberry Pi 2 Model B | [20] |
| | IDS/Balküpü ve Paket Analiz Aracı | 2018 | Düşük maliyetli, taşınabilir IDS, Balküpü ve Paket Analiz Aracı | Snort, Barnyard2, Pulledpork, Cowrie, Tshark | Raspberry Pi 3 Model B | [21] |
| | Saldırı Tespit Sistemi | 2016 | Raspberry Pi'nin IoT için IDS olarak kullanılması | Snort, Raspberry Pi 2 Model B | Akıllı Ev Senaryosu | [22] |
| | Trafik Analizi | 2017 | Raspberry Pi ve Snort'un trafik analizi amacıyla kullanılması | Snort, Raspberry Pi | Küçük Ölçekli Bir Ağ | [23] |
| | Dağıtık Balküpü Geliştirilmesi | 2014 | Raspberry Pi'nin Dionaea Çalıştırarak Balküpü Sensörü Olarak Kullanılması | Dionaea, Raspberry Pi | Test Ortamı | [24] |
| | Saldırı Tespiti | 2019 | Router olarak yapılandırılmış Raspberry Pi kullanarak yönlendirici düzeyinde IoT güvenlik yöntemi önerilmesi | Raspberry Pi 3 Model B | Ev Ağı | [25] |

Çizelge 2.1. (devam) Raspberry Pi'nin siber güvenliği üzerine yapılan çalışmalar

| Kategori | Alt Kategori | Yıl | Amaç/Odak | Kullanılan Araçlar/Yöntemler/Standartlar | Uygulama | Atıf |
|---|---|---|---|---|---|---|
| Zaafiyetler | Güvenlik Açıkları | 2019 | Raspberry Pi'de bulunabilecek donanım ve yazılım güvenlik açıkları incelenmesi | NMAP, W3AF, Metasploit | Raspberry Pi | [26] |
| | Güvenlik Açıkları | 2017 | Raspberry Pi'de yer alan varsayılan ayarların ortaya çıkardığı güvenlik problemleri | *** | Raspberry Pi 2 Model B | [27] |
| | Güvenlik Açıkları | 2018 | SSH Protokolü Değişim Anahtarlarında Bulunan Güvenlik Açığının Sömürülmesi ve CRLF Enjeksiyonu | Windows 7(Putty), Fedora 20 (Saldırgan), Raspberry Pi Model B | Ev Ağı | [28] |

Çizelge 2.1’ de yer alan çalışmalardan birinde Sanada ve diğerleri, Raspberry Pi'ye soldan sağa ikili yöntem ve Montgomery'nin güç veren merdiven algoritması gibi iki modüler üstelleştirme algoritmasını uygulamış ve yan kanal saldırısına karşı güvenliklerini değerlendirmiştir. Bu iki algoritma arasında soldan sağa ikili yöntemin fiziksel saldırıya karşı çok güvenli olmadığı tespit edilmiştir [11].

Büyükkaya tarafından gerçekleştirilen çalışmada, Raspberry Pi üzerinde çalışan AES algoritmasına farksal yan kanal analizi yöntemlerinden birisi olan DEMA (Differential Electromagnetic Analysis) saldırısı uygulanmıştır. Raspberry Pi’nin bir bilgisayar görevi görmesi nedeniyle işletim sistemi aynı zamanda farklı görevlerde yerine getirmektedir. Bu durumun yan kanal analizi için bir önlem olup olmayacağı incelenmiş olup algoritmanın önlem alınmaksızın yan kanal analizi saldırısına karşı koyamadığı görülmüştür [12].

Farklı bir çalışmada ise Martin ve diğerleri kötü amaçlı yazılımların analizini ve internet üzerinden yeni cihazlara nasıl bulaştığını ele almıştır. Ayrıca Raspberry Pi tabanlı IoT cihazlarının yanlış yapılandırılmasının çok hızlı bir şekilde sömürülmesine yol açabileceğini ortaya koyulmuştur [15].

Yukarıda özetlenen literatür çalışmalarından açıkça görülebileceği gibi, kritik sistemlerde kullanılan ve kullanılması düşünülen Raspberry Pi’nin siber güvenliği son derece önemli olup bu konuda yaygın çalışmalar pek fazla bulunmamaktadır. Bu nedenle bu tez çalışmasında Raspberry Pi’ye yönelik oluşabilecek tehditler belirlenmiş ve deney ortamında bu tehditler cihaza uygulanmıştır.

# 3. GÖMÜLÜ SİSTEMLER

## 3.1. Gömülü Sistemlere Genel Bakış

Gömülü bir sistem, tek bir işlevi yerine getirmek için tasarlanmış donanım ve yazılım bileşenlerinden oluşan, büyük bir sistemin küçük parçasını oluşturan ve minimum insan etkileşimi sunan cihazlar olarak tanımlanmaktadır [29]. Daha anlaşılır bir şekilde ifade etmek gerekirse bir mikroişlemciyi standart bir bilgisayarın içine yerleştirmek yerine çamaşır makinesi, otomobil, klima gibi bilgisayarla ilgisi olmayan bir ürünün içine yerleştirip, bu ürün kontrol edilecek şekilde özelleştirildiğinde bir gömülü sistem elde etmiş olunur [30].

İlk kitlesel gömülü sistem üretiminin gerçekleştirilmesinden sonra birimlerin fiyatlarında yaşanan düşüş teknolojik ürün çeşitliliğini arttırmış ve fiyatlarını ucuzlatmıştır. Bu sebeple bu sistemler, tıbbi ekipmanlardan hava savunma sistemlerine, ev otomasyon ürünlerinden eğlence sektörüne, güvenlik sistemlerinden otomotiv sektörüne kadar geniş bir yelpazede kullanım alanı elde etmiştir. Gömülü sistemlerin kullanıldığı sektörler ve uygulama alanları Çizelge 3.1'de gösterilmiştir.

Çizelge 3.1. Gömülü sistemlerin kullanım alanları [31,32]

| Sektörler | Uygulamalar |
|---|---|
| Ofis Otomasyonu | Faks, Fotokopi Makinesi, Tarayıcı, Yazıcı Vb. |
| Ev Aletleri | Bulaşık Makinesi, Çamaşır Makinesi, Mikrodalga Fırın Vb. |
| Güvenlik | Yüz Tanıma Sistemi, Parmak İzi Tanıma, Göz Tanıma, Alarm Sistemleri Vb. |
| Akademik | Akıllı Tahtalar, Hesap Makinesi Vb. |
| Telekomünikasyon | Router, IP Telefon, Web Kamera, Hub Vb. |
| Otomotiv | Yakın Enjeksiyon Kontrolü, Hava Yastığı Sistemi, GPS, Seyir Kontrolü, Ateşleme Sistemleri, Farlar, Motor Kontrolü |
| Havacılık | Navigasyon Sistemleri, Otomatik İniş Sistemi, Uzay Robotiği |
| Endüstriyel Otomasyon | Montaj Hattı, Veri Toplama Sistemi, Voltaj, Sıcaklık Vb. |
| Tıbbi Malzeme | MR Cihazı, Kan Basıncı İzleme, Diyaliz Makineleri, Protez Cihazlar Vb. |

Gömülü sistemleri diğer sistemlerde ayıran belirli başlı özellikleri mevcuttur. Bunlar;

- Kullanım ömürleri boyunca sabit ve özel görevleri yerine getirmek üzere tasarlanmışlardır. Örneğin bir çamaşır makinesi sadece çamaşır yıkamakla görevlidir.
- Güç tüketiminde verimli, boyut ve ağırlık olarak küçük olup düşük maliyetlidirler [33].
- Gömülü sistemler, zor hava şartlarında çalışmak zorundadır.
- Bazı gömülü sistemler daha büyük bir sistemin bileşenlerini oluşturmakta olup daha büyük bir sistemin düzgün çalışması için birlikte çalışmak zorundadır. Örneğin bir otomobilin gösterge panosunu kontrol eden birçok gömülü sistem vardır. Otomobilin düzgün çalışması tüm sistemlerin birlikte sorunsuz çalışmasına bağlıdır.
- Gömülü sistemlerin güç kullanımı ve ısı yayılımı düşüktür [34]. Fazla ısı dağıtılırsa devreye soğutma fanları gibi ek ünitelerin eklenmesi gerekir. Daha fazla güç gerekiyorsa, daha yüksek güçte bir pil sisteme yerleştirilmelidir.

Gömülü sistemlerin bu karakteristik özellikleri Çizelge 3.2'de genel amaçlı bilgisayarların özellikleri ile karşılaştırılmıştır.

Çizelge 3.2. Genel amaçlı bilgisayarlar ve gömülü sistemlerin karşılaştırılması [35,36]

| Genel Amaçlı Bilgisayarlar | Gömülü Sistemler |
|---|---|
| Çeşitli uygulamaları yürütmek için genel bir donanım ve genel amaçlı bir işletim sisteminden oluşur. | Belirli bir dizi uygulamayı yürütmek için özel amaçlı bir donanım ve gömülü işletim sisteminin birleşiminden oluşur. |
| Son kullanıcı işletim sistemini kurabilir, uygulamaları ekleyip kaldırabilir. | Firmware önceden programlanmıştır ve son kullanıcı tarafından değiştirilemez. |
| Görevlerin belirli zaman içinde gerçekleşmesi kritik değildir. | Görevler zamanında yerine getirilmek zorundadır. |
| Performans en önemli faktördür. | Maliyet, hız, boyut, güç gereksinimi de önemlidir. |
| İşletim sistemi içerir. | İşletim sistemi olabilir veya olmayabilir. |

## 3.2. Gömülü Sistem Çeşitleri

Gömülü sistemler günlük hayatımızda bir dizi farklı görevi yerine getirmek için kullanılmaktadır. Bu sebeple gömülü sistemler performans ve işlevsel gereksinimlerine göre dört ana kategoride sınıflandırılır. Bunlar;

- Bağımsız gömülü sistemler
- Gerçek zamanlı gömülü sistemler
- Ağ bağlantılı gömülü sistemler
- Mobil gömülü sistemler

### 3.2.1. Bağımsız gömülü sistemler

Kendi başlarına çalışıp sadece girdi alıp çıktı üreten tepki süresinin önemli olmadığı sistemlerdir. Dijital veya analog verileri bağlantı noktalarından alır, işler ve elde edilen verileri çıkış noktasına verir [37].

### 3.2.2. Gerçek zamanlı gömülü sistemler

Belirli işlevleri belirli bir zamanda yerine getirmek zorunda olan, tepki süresinin hayati önem taşıdığı, kritik uygulamalarda kullanılan sistemlerdir. Kritik durumlara hızla yanıt verdikleri için askeri, tıbbi ve endüstriyel uygulamalarda kullanılmaktadır.

### 3.2.3. Ağ bağlantılı gömülü sistemler

Kaynaklara erişmek için ağ bağlantısı (Yerel Alan Ağı, Geniş Alan Ağı, İnternet) kullanan sistemlerdir. Bağlantılar kablolu veya kablosuz olabilir. Bu tür gömülü sistemler, TCP / IP veya UDP kullanılarak bir ağ üzerinden birbirine bağlanan sensörler, denetleyiciler, aktüatörler vb. çeşitli bileşenlerden oluşur [32].

### 3.2.4. Mobil gömülü sistemler

Cep telefonları, tabletler, dijital kameralar, akıllı telefonlar gibi taşınabilir gömülü cihazlarda kullanılır. Bellek kısıtlamaları, küçük boyut ve klavye bulunmaması ile iyi bir kullanıcı arayüzünün olmaması bu sistemlerin dezavantajlarıdır.

## 3.3. Gömülü Sistemlerin Tarihçesi

Gömülü sistemlerin gelişim süreci 1960'lara dayanmaktadır. Bu gelişim sürecinden maddeler halinde aşağıda bahsedilmiştir [38].

- İlk olarak Charles Stark Draper, Apollo Komuta Modülü ve Ay Modülü üzerine kurulu dijital sistem olan Apollo Rehberlik Bilgisayarının boyutunu ve ağırlığını azaltmak için 1961'de bir entegre devre geliştirdi.
- Ardından 1965 yılında Autonetics firması tarafından, Minuteman füze rehberlik sisteminde kullanılan D-17B geliştirilerek seri üretilen ilk gömülü sistem olmuştur.
- D-17B, 1966 yılında entegre devrelerin yüksek hacimli kullanımıyla bilinen NS-17 füze rehberlik sistemi ile değiştirildi.
- 1968 yılında ise Volkswagen 1600, elektronik yakıt enjeksiyon sistemini kontrol etmek için bir mikroişlemci kullanmasıyla birlikte araçlarda kullanılan ilk gömülü sistemi piyasaya sürmüş oldu.
- İlk mikro denetleyici ise 1971'de Texas Instruments tarafından geliştirildi. 1974'te ticari olarak satışa sunulan TMS 1000 serisi, 4 bitlik bir işlemci, ROM bellek ve RAM bellek içeriyordu ve maliyeti yaklaşık 2 dolardı.
- Ayrıca, 1971'de Intel, yaygın olarak piyasada bulunan ilk işlemci olan 4004'ü piyasaya sürdü. 4-bit mikroişlemci hesap makinelerinde ve küçük elektronik cihazlarda kullanılmak üzere tasarlandı.
- 1972'de piyasaya sürülen 8-bit Intel 8008, 16 KB belleğe sahipti.
- 1974 yılında 64 KB bellek ile Intel 8080 geliştirildi. 8080'in halefi x86 serisi, 1978'de piyasaya sürüldü ve bugün hala büyük ölçüde kullanılıyor.
- 1987'de ilk gömülü işletim sistemi olan gerçek zamanlı VxWorks, Wind River tarafından piyasaya sürüldü ve bunu 1996'da Microsoft'un Windows Embedded CE izledi.
- 1990'ların sonunda, ilk gömülü Linux ürünleri ortaya çıktı. Günümüzde ise Linux neredeyse tüm gömülü cihazlarda kullanılmaktadır.

Çizelge 3.3'de gömülü sistemlerin tarihçesi, günümüzde yaşanan gelişmeler ve gelecekteki durum hakkında bilgi verilmektedir.

Çizelge 3.3. Gömülü sistemlerin gelişim süreci [39]

| Nu. | Yıl | Geçmiş |
|---|---|---|
| 1 | 1960 | MIT Laboratuvarında geliştirilen Apollo Rehberlik Bilgisayarının boyutunu ve ağırlığını azaltmak için kullanılan entegre devreler.<br>(İlk Gömülü Sistem) |

Çizelge 3.3. (devam) Gömülü sistemlerin gelişim süreci [39]

| | | |
|---|---|---|
| 2 | 1961 | 1961 Minuteman füzesi için transistör mantığından yapılan Autonetics D-17 güdüm bilgisayarı.<br>(İlk Toplu Üretilen Gömülü Sistem) |
| 3 | 1965 | DEC'in 12 bit PDP-8 mini bilgisayarı.<br>(Ticari Ürünlerdeki İlk Gömülü Bilgisayar) |
| 4 | 1966 | D17'nin yerini alan Minutemen II.<br>(Entegre Devrelerin İlk Yüksek Hacimli Kullanımı) |
| 5 | 1968 | B.Noyce ve G.Moore, Entegre Elektronik'i kurdu.<br>(Intel'in Ortaya Çıkışı Başladı.) |
| 6 | 1969 | Wolksvagen 1600'ün yakıt enjeksiyonu mikroişlemci tarafından kontrol edildi.<br>(Arabalardaki İlk Gömülü Sistem) |
| 7 | 1971 | Intel 4004 mikroişlemci, Hesap Makineleri için tasarlandı .<br>(İlk 4-bit mikroişlemci) |
| 8 | 1974 | Intel 8008 ve 8080'i tasarladı.<br>Motorola, MC6800 Mikroişlemciyi tanıttı. (İlk 8 bit mikroişlemci) |
| 9 | 1974 | CLIP-4 aynı anda birden fazla hesaplama gerçekleştirdi.<br>(İlk Paralel Mimarili Bilgisayar) |
| 10 | 1975 | Bill Gates ve Paul Allen, MITS'e ilk BASIC derleyicisini ortaya çıkardı.<br>(Microsoft Doğdu.) |
| 11 | 1975 | ALTAIR 8800 piyasaya sürüldü.<br>(İlk Ev Bilgisayarı) |
| 12 | 1980 | Mikroişlemciler hız ve boyut için optimize edildi.<br>Mikrokontroller güç ve boyut için optimize edildi.<br>(Mikrokontrol tasarımı) |
| 13 | 1983 | Hewlett Packard'ın HP-150'si, parmak hareketini algılamak için monitörün ön tarafında bir Kızılötesi ışın kullandı.<br>(Dokunmatik ekran teknolojisine sahip ilk Ev bilgisayarı) |
| 14 | 1987 | VXWorks tarafından gömülü işletim sistemi geliştirildi. |
| 15 | 1989 | T.Berners-Lee, World Wide Web'i icat etti.<br>(İnternetin Doğuşu.) |
| 16 | 1989 | 1989 DOT matrix Yazıcı gibi Gömülü Sistem, güç kullanımı ve sıkı elektrik zamanlama kısıtlamaları nedeniyle 8 bit ile sınırlandırıldı.<br>Super Nintendo Entertainment System bilgisayarı, 80386 16-bit işleme ve Pentium 32-bit işleme kullanmaya başladı. |
| 17 | 1990 | Sistemin tasarımı ve özellikleri, bilgi işlem kaynağı olarak bir ağ kullanan dağıtık bilgi işlem teknolojisi ile geliştirilmiştir.<br>(World Wide Web ile Gömülü Sistem Tanıtıldı) |
| 18 | 1992 | 10 milyon telefon kullanılmaya başlandı.<br>(Gömülü Sistem Kablosuz Kullanım.) |
| 19 | 1993 | Apple, dokunmatik ekran teknolojisine sahip PDA'yı piyasaya sürdü.<br>(Dokunmatik Ekran Teknolojisi) |
| 20 | 1996 | 1996 Microsoft yerleşik pazara girdi.<br>(Windows Embedded CE1.0 Tasarlandı.) |
| 21 | 1998 | FSM Labs RTLINUX'da kullanılan yöntemin patentini aldı.<br>(RT'nin Doğuşu) |
| 22 | 1999 | Gömülü Linux ürünü pazarda piyasaya sürüldü. (İlk Gömülü Linux Ürünü) |

Çizelge 3.3. (devam) Gömülü sistemlerin gelişim süreci [39]

| | | |
|---|---|---|
| 23 | 2000 | Time Sys, LINUX'un ilk gerçek zamanlı sürümünü piyasaya sürdü. (İlk LINUX / RT1.0) |
| 24 | 2005 | ANDROID teknolojisi öne çıktı (Google, ANROID'i Satın Aldı.) |
| 25 | 2007 | Apple ilk iPhone'u piyasaya sürdü. (Hepsi Bir Arada Gömülü Mobil Cihaz) |
| 26 | 2008 | T-mobile G1, İlk ANROID telefonu piyasaya sürdü ve ANROID kodu açık kaynak olarak ilan edildi |
| Günümüz | | |
| 27 | Gömülü Sistem için elektronik çipler üretilmektedir. | |
| 28 | Otomobil, tren, traktör, vinçler, robotlar vb. tanıdık nesnelerin içine gizlenmiş gömülü sistemler yaygınlaştı. | |
| 29 | Saatler, kurutucular, fırınlar, buzdolabı, mikrodalgalar vb. nesnelerde gömülü sistemler yaygınlaştı. | |
| 30 | Tıbbi görüntüleme cihazlarında gömülü sistem kullanımı yaygınlaştı. | |
| Gelecek | | |
| 31 | Otonom gömülü sistem ağlarının olacağı öngörülmektedir. | |
| 32 | İnsan müdahalesi olmadan birbirleriyle etkileşime giren nesnelerin kullanımı artacak. | |
| 33 | Otomobiller birbirleriyle iletişim kuracak, yol kenarı ve şehir trafiği düzenlenecek. | |
| 34 | Sensörler nehir taşkınlarını, orman yangınlarını, bina yapısal sağlığını vb. tespit edebilir duruma gelecek. | |

### 3.4. Gömülü Sistemlerde Siber Güvenlik

Gömülü sistemlerin artan kullanımıyla birlikte kötü niyetli kişilerin bu sistemlerden yararlanmaya çalışmak istemeleri de olası bir durum haline gelmiştir. Özellikle finansal, endüstriyel ve nükleer tesislerde kullanılan gömülü sistemler, gerçekleştirdikleri işlevler nedeniyle daha fazla saldırı hedefi haline gelmektedir. 1990'lı yıllarda özellikle yan kanal saldırılarının akıllı kartlara karşı başarılı olduğu gösterildikten sonra gömülü sistem güvenliği önem kazanmış, ağa bağlı gömülü sistemlerin ortaya çıkması ile birlikte gömülü cihazların artık uzaktan saldırılara da maruz kalabileceği ortaya koyulmuştur [40]. Gömülü sistemlerin artan kullanımı ve siber uzayda yer alan sistemlere yapılan saldırıların arttığı göz önüne alındığında güvenlik bu cihazlar için önemli bir gerekliliktir. Fakat bu sistemlerde güvenlik her zaman sıkı bir şekilde uygulanmadığından, bu da onları bilinen ve bilinmeyen

birçok tehdide karşı savunmasız hale getirir [41]. Çok sayıda gömülü sistem, sınırlı donanımsal kaynakları ve artan karmaşık tasarımlarıyla daha savunmasız hale gelmiştir. Bunun yanı sıra ağa bağlantılarının artmasıyla birlikte saldırganlar için yeni saldırı vektörleri de ortaya çıkmıştır. Geçmişte gömülü sistemler kapalı ağlarda konumlandırılmakta ve diğer sistemlerle iletişim kurmadan görevlerini gerçekleştirmekteydiler. Fakat günümüzde internet ve diğer ağlar aracılığıyla farklı sistemlere ve cihazlara bağlanarak dış dünya ile iletişim kurar hale gelmişlerdir [42]. Ağa bağlantılarının artması ve kritik veriler barındırmaları sebebiyle gömülü sistemler saldırganların daha çok hedefi haline gelmiştir. Bu kapsamda ağ güvenliğinin önemi ise giderek artmaktadır.

Gömülü bir sistem eğer dışarıdan gelen saldırıların neden olduğu zararlara karşı korunuyorsa güvenlidir denebilir. Nesnelerin interneti ile birlikte sistemlerin birbirine bağlanması dışarıdan gelen saldırılarda artışlara sebep olmuştur. Bu bağlantılar işlerlik ve kullanılabilirlikte önemli avantajlar sağlarken daha fazla bileşeni bağlamak daha fazla saldırı ve hasar anlamına gelmektedir [43]. Bu kapsamda güvenli ve güvenilir bir sistem oluşturmak için, hem bileşenlere tasarım aşamalarında güvenlik sağlanması hem de gömülü sistemin yaşam döngüsü boyunca düzenli güvenlik denetimleri ve incelemeleri yapılması esastır [33]. Bununla birlikte bu sistemler, tasarım hedeflerini gerçekleştirebilmeli ve saldırı altındayken de belirli bir esneklikle çalışabilmelidir [44].

### 3.5. Gömülü Sistem Güvenliğinde Karşılaşılan Zorluklar

Gömülü sistemler, tıbbi cihazlar, uzay ve silah sistemleri, haberleşme sektörü, hava alanları gibi farklı sektörlerde kullanılmaktadır. Bu açıdan bakıldığında güvenlik, gömülü sistemlerin yaptıkları görevler ve kritik sistemlerdeki rolleri açısından önemli bir konudur. Geleneksel bilgi teknolojileri sistemleri ile karşılaştırıldığında, gömülü sistemlerde güvenliğin sağlanması kolay değildir. Burada karşılaşılan en önemli zorluklar şunlardır;

- Zayıf güvenlik tasarımı
- Pazarlama süresi
- Güvenlik maliyeti
- Cihazların güncellenme zorluğu
- Sınırlı Kaynaklar
- Standart Olmayan İşletim Sistemleri

### 3.5.1. Zayıf güvenlik tasarımı

Gömülü cihazlar tasarlanırken genellikle güvenlik ikinci plandadır. Toplu üretimi gerçekleştirilen bu sistemlerde, aynı versiyona sahip cihazlar aynı tasarıma sahip olduğundan bu cihazlardan birinin ele geçirilmesi, saldırının milyonlarca cihazda kolayca tekrar edilmesi anlamına gelmektedir.

### 3.5.2. Pazarlama süresi

Gömülü sistemler pazarı ürün çeşitliliğinin artmasıyla oldukça gelişmiştir. Bu sebeple pazara ilk ulaşan ürün kazanandır. Pazara sunma süresi, üreticileri güvenlik çözümlerinin uygulanmasını engellemeye zorlayan bir kriterdir. Pazara sunma süresinde gecikmeye neden olmayacak güvenlik çözümleri, üreticiler için çok önemli ve değerlidir [45].

### 3.5.3. Güvenlik maliyeti

Güvenlik faktörü, daha fazla yönetime ihtiyaç duyar. Bu da ürünün geliştirme aşamasında ve yönetim adımında ekstra maliyetine yol açmaktadır. Üreticiler mevcut işlevleri güvence altına almak yerine cihazlara daha fazla işlevsellik eklemeyi tercih etmektedir. Üreticilerin maliyetli çözümlerden kaçınmak istemesi nedeniyle ucuz güvenlik çözümlerinin geliştirilmesi, sistemleri daha güvenli hale getirecektir [45].

### 3.5.4. Cihazların güncellenme zorluğu

Gömülü sistemlerin çoğu, düzenli olarak güncellenmemektedir. Gömülü cihaz konumlandırıldıktan sonra, yıllarca üzerinde birlikte geldiği yazılım ile çalışmaya devam eder. Her şey düzgün çalışıyor gibi göründüğü sürece zaman alan, pahalı ve pratik olmayan bir yükseltmeden geçmek için yeterli bir sebep olmadığı görüşü hakimdir.

### 3.5.5. Sınırlı kaynaklar

Gömülü sistemler sınırlı kaynaklara sahiptir. Küçük bellekler ve ikincil depolama aygıtlarının olmayışı, virüs veya Truva atının bu kaynaklardan herhangi birini tüketerek DoS saldırısına neden olabileceğini göstermektedir.

### 3.5.6. Standart olmayan işletim sistemleri

Geleneksel BT sistemlerinde kullanılan bilgisayarlar genellikle popüler bir işlemci markası ve işletim sistemi kullanır. Oysa gömülü sistemler söz konusu olduğunda, işlemcilerde ve işletim sistemlerinde çok fazla çeşitlilik vardır. Bu da her bir sistem için farklı güvenlik mekanizmalarının geliştirilmesi gerektiği anlamına gelmektedir.

## 3.6. Güvenlik Zafiyetleri ve Yapılan Saldırılar

Gömülü sistemler, özel bilgileri çalmak, güç kaynağını boşaltmak, sistemi yok etmek veya sistemi amacı dışında kullanmak gibi birçok saldırıya karşı savunmasızdır. Gömülü sistemlerde yer alan güvenlik açıklıklarına yönelik yapılan saldırılar şunlardır [46]:

- Enerji drenajı
- Fiziksel izinsiz giriş
- Ağa izinsiz giriş
- Bilgi hırsızlığı
- Sahte bilgilerin tanıtımı
- Sensörün veya diğer çevre birimlerinin hasar görmesi
- Termal olaylar
- Sistemlerin başka amaçlar için yeniden programlanması

### 3.6.1. Enerji drenajı

Gömülü sistemlerdeki sınırlı pil gücü, kaynakları tüketen saldırılara karşı bu sistemlerin savunmasız hale gelmesine neden olur. Enerji drenajı, hesaplama yükünü artırarak uyku döngülerini azaltarak veya sensörlerin veya diğer çevre birimlerinin kullanımını artırarak sağlanabilir. Bu zafiyetler ile sistemlere tükenme saldırıları gerçekleştirilir.

### 3.6.2. Fiziksel izinsiz giriş

Sisteme içeriden yakın olan potansiyel bir saldırgan tarafından gerçekleştirilebilir. Sisteme fiziksel erişimin gerekli olduğu saldırılara karşı güvenlik açıkları oluşturur. Sistem veri yoluna yapılan güç analizi saldırıları buna örnektir.

### 3.6.3. Ağa izinsiz giriş

Gömülü sistemler ağa bağlanmasıyla birlikte diğer genel amaçlı bilgisayarlar veya sunucular gibi uzaktan müdahaleye açık hale gelmektedir. Arabellek taşması veya kötü amaçlı yazılımlarla ağa izinsiz girişler gerçekleştirilebilir.

### 3.6.4. Bilgi hırsızlığı

Güvenli olmayan bir ortamda konuşlandırılan gömülü bir sistemde depolanan veriler yetkisiz erişime açıktır. Korunması gereken bu verilere örnek olarak, kriptografik anahtarlar verilebilir. Bu zafiyetler neticesinde gizliliğe karşı saldırılar gerçekleştirilebilir.

### 3.6.5. Sahte bilgilerin tanıtımı

Gömülü cihazlar, sensörler aracılığıyla ya da doğrudan belleğe yazma yoluyla yanlış verilerin girilmesine ve kötü amaçlı kullanıma açıktır. Güvenlik kameralarında yanlış video beslemesi veya bir elektrik sayacındaki ölçüm verilerinin üzerine yazılması buna örnek olarak gösterilebilir.

### 3.6.6. Termal olaylar

Gömülü sistemlerin makul çevresel koşullarda çalışması gerekir. Gömülü sistemlere yapılacak saldırılarla soğutma sisteminde arıza meydana getirilebilir ve sistem aşırı ısınarak saldırganlar tarafından erişilebilir duruma gelmektedir.

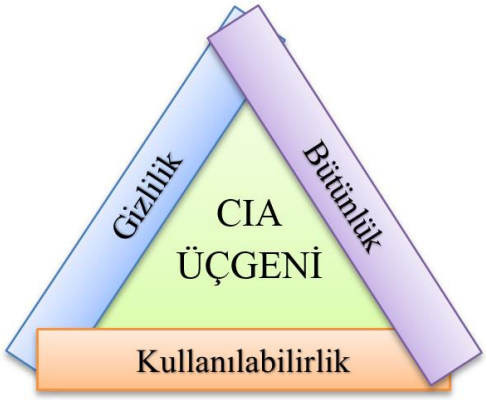
### 3.6.7. Sistemlerin başka amaçlar için yeniden programlanması

Birçok gömülü sistem genellikle belirli bir amaç için programlanıp kullanılmaktadır. Bu sistemler, kötü amaçlı kullanımlar için yeniden programlamaya karşı savunmasız olabilirler.

## 3.7. Gömülü Sistemlerde Güvenlik Gereksinimleri

Gömülü sistemlerdeki güvenlik hedefleri diğer bilgisayar sistemlerinin güvenlik unsurları ile aynıdır. CIA (Confidentiality, Integrity, Availability) olarak ifade edilen bu güvenlik üçlüsü bir varlığın korunması için gereken temel güvenlik ilkelerini içermektedir. Bu

üçlemede Gizlilik, Bütünlük ve Kullanılabilirlik unsurları yer almaktadır. Fakat bu unsurların önceliği gömülü cihazlarda farklılık taşımaktadır. Gömülü sistemlerde güvenlikten önce sistemlerin kullanılabilir olması ön plandadır. Bu sebeple Kullanılabilirlik, Gizlilik ve Bütünlük olarak önceliklendirme yapılmıştır.




Şekil 3.1. Bilgi güvenliği unsurları

### 3.7.1. Kullanılabilirlik / Erişilebilirlik

Saldırıların varlığına rağmen istenen sistem hizmetlerinin beklendiği anda kullanılabilir olmasını sağlar. Gömülü bir sistem için kullanılabilirliği sağlamaya yönelik en basit yaklaşım, gömülü sistemde herhangi bir değişikliğin meydana gelmesine asla izin vermemektir. Gömülü sistemlerdeki kullanılabilirlik mekanizmaları, DoS ve enerji açlığı saldırılarının yanı sıra kurcalama saldırılarıyla mücadele etmeye çalışır [47]. Gömülü bir sistemin erişilebilirliğinin sürekliliği için beyaz liste, izinsiz giriş koruması, yönetim ve karşı önlemler uygulamalarının gerçekleştirilmesi önerilmektedir [48].

### 3.7.2. Bütünlük

Verilerde yapılan değişikliklerin tespit edilebilir olmasını sağlayarak, hem kasıtlı değişiklik veya imha hem de kazara değişiklik veya kayıp dahil olmak üzere verileri yetkisiz değişikliklere karşı korur.

Bilgi ve sistemlerin doğruluğunun ve güvenilirliğinin muhafaza edildiğini ve herhangi bir yetkisiz değişikliğin önlendiğini garanti eder. Gömülü bir sistem içindeki veriler, işletim sistemini, uygulamaları ve konfigürasyon verilerini içerebilir. Bu verilerden herhangi biri

bozulursa, gömülü sistem amaçlanan işlevini yerine getirmez veya saldırganın gömülü sistemi kullanması için bir araç haline gelebilir [48].

Gömülü sistemdeki verilerin bütünlüğünün bozulması, bir konutun temelinin bozulması gibidir: üstündeki bileşenler zayıflatılır ve güvenilemez [49]. Bütünlüğü bozmaya odaklanan bir saldırgan, sahte bilgiler enjekte etmeye, mevcut verileri bozmaya veya sistemi başka şekilde aldatmaya çalışabilir.

### 3.7.3. Gizlilik

İletişim kuran taraflar arasında iletilen verilerin gizliliğinin korunmasını garanti eder. Yani meşru taraflar dışında hiç kimse mesajların içeriğini bilmemelidir. Pek çok gömülü sistemde, sistem içinde depolanan bilgilerin (ör. Güvenli anahtar) yetkisiz erişime karşı korunması çok önemlidir. Gizlilik ilkesi, bilgilerin yetkisiz kişilere, programlara veya işlemlere ifşa edilmediğine dair güvence sunarak veri işlemenin her bir noktasında gerekli gizlilik düzeyinin uygulanmasını sağlar ve yetkisiz ifşaları önler [49]. Bu nedenle, gizliliği bozmaya odaklanan bir saldırgan, bilmeye yetkili olmadığı hassas bilgileri (ör. Şifreler, finansal bilgiler veya ticari sırlar) öğrenmeye çalışır.

Yukarıda bahsedilen bilgi güvenliği gereksinimleri ile birlikte ele alınması gereken diğer ilkelerden aşağıda kısaca bahsedilmiştir.

Kimlik Doğrulama

Sistemi kullanmalarına izin verilmeden önce kullanıcıları doğrulama sürecini ifade eder.

Erişim Kontrolü

Sistemin yalnızca yetkili kullanıcılar için kullanılabilir olmasıdır.

Kurcalamaya Dayanıklılık

Gömülü bir sistem kötü niyetli kişilerin eline geçtiğinde bile bu güvenlik gereksinimlerini sürdürme arzusunu ifade eder.

Güvenilirlik

Gömülü sistemlerin genellikle yıllarca hatasız çalışması beklenir. Güvenilir bir şekilde işlevsellik sağlanması, sürekli hizmet ve vaat edilen hizmet kalitesinden ödün verilmemelidir. Bu nedenle gömülü bir sistem güvenilir olmalıdır [50].

Güvenlik

Sistemin kullanıcılar veya çevre için felaketle sonuçlanan olaylara yol açmayacağı anlamına gelir. Güvenlik görecelidir, olası tüm risklerin ortadan kaldırılması genellikle imkansızdır. Kullanılabilirlik ve güvenilirlik tüm arızaları önlerken, güvenlik yalnızca küçük bir alt küme olan felaketle sonuçlanan arızaları önler.

Tüm bu bileşenler incelendiğinde tek başına hiçbir güvenlik ilkesinin gömülü bir sistem için yüzde yüz koruma sağladığı söylenemez. Gömülü sistem için daha güçlü, çok yönlü koruma sağlayan ve tüm bu ilkelerin bir araya getirildiği mekanizmalar geliştirilmelidir.

# 4. RASPBERRY Pİ

## 4.1. Raspberry Pi'ye Genel Bakış

Raspberry Pi, bir bilgisayar monitörüne veya televizyona bağlanan, klavye ve fare ile kullanılabilen düşük maliyetli kredi kartı boyutunda bir bilgisayar olarak tanımlanır [51]. Dünya çapında özellikle Bilgisayar Bilimi, Elektronik ve Gömülü Sistemler alanındaki araştırmacılar başta olmak üzere herkes tarafından kullanılmaktadır. 2019 yılı itibariyle 30 milyon adet çeşitli Raspberry Pi modeli satılmıştır [52]. Raspberry Pi'nin geliştirilmesinin arkasındaki ana fikir ise bilgisayarların pahalı olduğu ve çocuklar arasında programlama uygulamasının İngiltere'deki çocukların ebeveynleri tarafından desteklenmediği dönemde çocuklara küçük ve uygun fiyatlı bilgisayar verme düşüncesi olmuştur [53]. Eben Upton liderliğinde çalışan ekip çeşitli prototipler ve versiyonlar geliştirdikten sonra son sürümü "Raspberry Pi" olarak adlandırmıştır [54].

Kredi kartı boyutunda tek kartlı bir bilgisayar olarak ifade edilen cihaz 35 ABD dolarından satışa sunulmaktadır [55]. Her türlü bilgi işlem görevini gerçekleştirmekte ve dış dünya ile etkileşim sunmaktadır. Raspberry Pi'nin çalışma prosedürü, genel amaçlı bilgisayarlara çok benzerdir ve işletim için klavye, fare, ekran ünitesi, güç kaynağı, işletim sistemi yüklü SD Kart gibi ek donanım gerektirir. Raspberry Pi ayrıca USB bağlantı noktaları içermektedir. Raspberry Pi Vakfı tarafından kamera gibi çeşitli donanım aksesuarları da kullanıcılar için piyasaya sürülmüştür [56].

## 4.2. Avantaj ve Dezavantajlar

Raspberry Pi kullanımının avantajları şunlardır [56,57]:

- Küçük, güçlü ve verimli bir kompakt formda bilgisayar olarak kabul edilir ve çok ucuzdur. Çeşitli küçük ölçekli firmalar, web sunucusu ve veritabanı sunucusu gibi küçük ve orta düzeydeki görevleri yapmak için Raspberry Pi'yi kullanabilir. Böylece, maliyet açısından tasarruf sağlanabilir.
- Kapsamlı programlama deneyimi için tek bir platform görevi görebilir. Pi tarafından çeşitli programlama dilleri desteklenir. Kullanılan ana programlama dili ise Python'dur.

- Ürün açık kaynaklı işletim sistemini ve açık kaynaklı uygulamaları desteklemektedir. Bu nedenle, çeşitli Linux sürümlerinde onlarca işletim sistemi ve bu Linux işletim sistemindeki milyonlarca uygulama Raspberry Pi'de kullanılabilir.
- Raspberry Pi, butonlar ve ledler gibi üçüncü taraf donanımın bağlanmasını kolaylaştıran ek donanımları destekler ve kullanıcı Pi üzerinde çeşitli işlemleri gerçekleştirebilir.
- Ürün enerji açısından verimlidir.
- Bir LAN adaptörü üzerinden ağ cihazlarıyla iletişim mümkündür.

Raspberry Pi kullanımının kısıtları ise şunlardır [56,57]:

- Ethernet bağlantı noktası ve işlemci çoklu görevleri işlemek için yeterince hızlı olmadığından tam donanımlı bir bilgisayar olarak kabul edilemez.
- Tam işlevsel Windows İşletim Sistemi ile uyumlu değildir.
- Pil yedeklemeli Gerçek Zamanlı Saat (RTC) yoktur. Zaman yalnızca NTP Sunucusu kullanılarak aşılabilir ve işletim sistemlerinin çoğu bu görevi otomatik olarak yapar.
- Bluetooth'u, kutudan çıktığı haliyle Wi-Fi'yi desteklemez ve hatta çeşitli USB Tabanlı donanım kilitleri de kablosuz bağlantı için desteklenmez.
- Dahili ADC Dönüştürücüsü yoktur. ADC amaçlı harici şarj cihazı kullanılmaktadır.
- BIOS'a sahip olmadığı için her zaman bir SD karttan önyükleme yapar.

### 4.3. Raspberry Pi'nin Gelişimi

Çocuklar için küçük ve ucuz bir bilgisayar geliştirme fikri, 2006 yılında Eben Upton, Rob Mullins, Jack Lang ve Alan Mycroft'un aralarında bulunduğu bir ekipten doğmuştur. Bu fikrin ortaya çıkma sebebi ise, Cambridge Üniversitesi'nde Bilgisayar Bilimleri okumak için başvuran öğrencilerin sayı ve beceri düzeylerinde düşüş gerçekleşmesiydi. Her akademik yılda 1990'larda başvuran çocukların çoğunun deneyimli hobi programcıları olarak görüşmeye geldiği bir durumdan, 2000'lerdeki manzara çok farklıydı. Artık başvuru yapan kişiler deneyimsiz kişilerden oluşmaktaydı. 2006 yılında Upton, Broadcom için çalışmaya başladı ve diğer zamanlarda düşük maliyetli bir bilgisayar geliştirme çalışmalarına devam etti. 2008 yılına kadar Eben Upton Raspberry Pi'nin birkaç prototipini geliştirerek orijinal dört yaratıcı, Pete Lomas ve David Braben ile birlikte Raspberry Pi Vakfı'nı kurdu ve üç yıl sonra seri olarak üretilen ilk Pi montaj hattından çıktı [58,59]. Pi ile Python kodlama diline, Raspberry adı ile Apple ve Tangerine gibi meyve ile isimlendirilen sistemlere atıfta bulunulmuştur [60].

# 5. GÜVENLİK TESTİ METODOLOJİLERİ

Gömülü sistemlere sızma testleri gerçekleştirmek, özellikle kritik altyapılarda kullanılan bu cihazların güvenlik ihtiyaçlarının sağlanması açısından önemli bir konudur. Bu testler yapılırken ise tüm sistemlere ya da cihazlara uygulanması gereken belirli adımlar vardır. Bu adımlar bilgi toplamak, keşif yapmak, zafiyetleri bulmak, zafiyetleri istismar etmek ve sistemi ele geçirmek olup bu aşamalar sızma testlerinin yaşam döngüsünü oluşturmaktadır [61]. Bu yaşam döngüsünü içinde barındıran uluslararası bazı standartlar ve metodolojiler yer almaktadır. Bunlardan en çok kullanılanları OWASP, OSSTMM, ISSAF, NIST SP 800-115 ve PTES olarak karşımıza çıkmaktadır.

## 5.1. OWASP

OWASP yazılım güvenliğini artırmak için çalışan kar amacı gütmeyen bir kuruluştur. Geliştiricilerin web uygulamalarını daha güvenli hale getirmek için kullandıkları bir kaynaktır. Bu kuruluş tarafından sunulan kılavuzlar, web uygulamalarının güvenliğinin test edilmesi amacıyla kullanılmaktadır. Dünya çapında yazılım güvenliğini geliştirmeye odaklanan kuruluşun misyonu, birey ve kuruluşların gerçek yazılım güvenlik riskleri hakkında bilinçli karar verebilmesi için yazılım güvenliğini öne çıkarmaktır [62, 63].

OWASP tarafından üreticilerin giderek daha güvensiz hale gelen bir dünyada güvenli cihazlar oluşturmaları için ayrıntılı teknik bilgiler sunan yol haritası niteliğinde Gömülü Uygulama Güvenliği Projesi geliştirilmiştir. Proje kapsamında oluşturulan belge, yalnızca üreticilerin güvenliği göz önünde bulundurarak gömülü cihazlar üretmelerine yardımcı olma amacı taşımaktadır [64].

## 5.2. OSSTMM (Open Source Security Testing Methodology Manual)

Açık Kaynak Güvenlik Testi Metodoloji Kılavuzu (OSSTMM), güvenlik riskleri, ölçümler ve açıklamanın yanı sıra farklı test türlerinin planlanması ve yürütülmesine ilişkin temel bilgileri içerir. Bununla birlikte, sızma testine odaklanan ayrıntılı bilgi içeren bir bölüm yoktur. Son versiyonu 2010 yılında yayımlanmıştır [65].

### 5.3. ISSAF (Information Systems Security Assesment Framework)

Bilgi Sistemleri Güvenlik Değerlendirme Çerçevesi (ISSAF) aktif bir topluluk olmamakla birlikte, sızma testleri için iyi bir referans kaynağıdır. Kapsamlı sızma testi teknik rehberliği sunar. Bilgi sistemi güvenlik değerlendirmesini çeşitli alanlara göre kategorize eden ve bu alanların her biri için özel değerlendirme veya test kriterlerini ayrıntılarıyla anlatan yapısal bir çerçevedir. ISSAF, öncelikle bir kuruluşun güvenlik değerlendirme gereksinimlerini karşılamak için kullanılmalıdır ve ayrıca diğer bilgi güvenliği ihtiyaçlarını karşılamak için bir referans olarak da kullanılabilir. ISSAF, güvenlik süreçlerinin önemli yönünü ve var olabilecek güvenlik açıklarının tam bir resmini elde etmek için bunların değerlendirilmesini ve sağlamlaştırılmasını içerir. Son versiyonu  Mayıs 2006 yılında yayımlanmıştır [66, 67].

### 5.4. NIST SP 800-115 (Bilgi Güvenliği Testi ve Değerlendirmesi için Teknik Kılavuz)

ABD Ulusal Standartlar ve Teknoloji Enstitüsü tarafından 2008 yılında yayımlanan bu belgenin amacı, kuruluşların teknik bilgi güvenliği testi ve değerlendirmelerini planlama, yürütme, bulguları analiz etme ve strateji geliştirme konusunda bir yöntem sağlamaktır. Bir sistem veya ağdaki güvenlik açıklarının bulunması gibi çeşitli amaçlarla kullanılabilen güvenlik testi, değerlendirme süreçleri ve prosedürleri ile ilgili teknik bilgilerin tasarlanması, uygulanması ve sürdürülmesi için pratik öneriler sunmaktadır [68].

### 5.5. PTES (Penetration Testing Execution Standard)

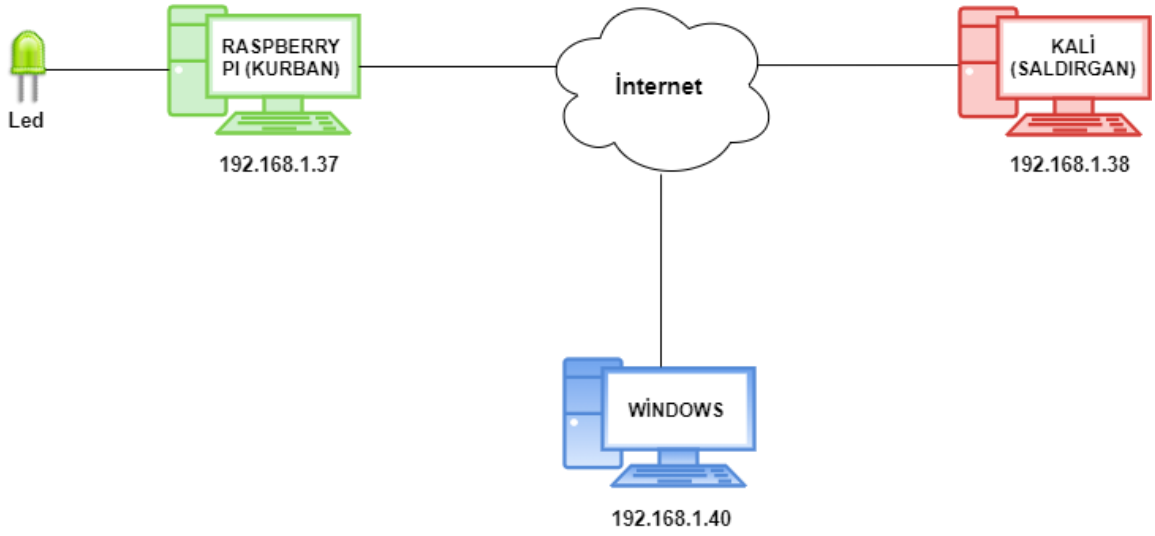
Penetrasyon Testi Uygulama Standardı (PTES) sızma testi yöntemini içeren bir standarttır. Sızma testinde eksiksiz ve güncel bir standarda olan ihtiyacı ele almak geliştirilmiştir. Güvenlik uzmanlarına rehberlik etmenin yanı sıra, işletmeleri bir sızma testinden ne beklemeleri gerektiği konusunda bilgilendirmeye ve onlara rehberlik etmeye çalışır. Ayrıca bu standart, gerçek bir sızma testinin nasıl gerçekleştirileceğine dair bir teknik kılavuzla birlikte sunulmaktadır [69].

# 6. DENEY VE ANALİZ AŞAMASI

Bu bölümde çalışma kapsamında oluşturulan test ortamında açıklık analizi saldırılarının gerçekleştirilmesi, tespiti ve sonuçları ele alınmıştır. Bu saldırıların hedefinde ise gömülü sistem ve nesnelerin interneti uygulamalarında yaygın olarak kullanılan Raspberry Pi cihazı yer almaktadır.

## 6.1. Test Ortamının Hazırlanması

Çalışmada, gömülü sistem uygulamalarında kullanılan Rasberry Pi cihazına yönelik DDoS MitM ve Süreç Öldürme saldırıları Kali işletim sisteminde yer alan Metasploit, Ettercap ve hping3 saldırı araçları ile Wireshark trafik analizi aracı kullanılarak Şekil 6.1'de belirtilen deneysel ağ topolojisi üzerinde gerçekleştirilmiştir.




Şekil 6.1. Test topolojisi

Test ortamında, bir adet Raspberry Pi kartı ve buna bağlı bir led, Raspberry Pi ile arasında veri trafiği olan bir Windows bilgisayar ve Kali Linux işletim sistemi kurulu bir adet saldırgan bilgisayar yer almaktadır. Cihazlar internet ağı üzerinden birbirlerine bağlıdır. Kullanılan saldırı araçları için Kali işletim sistemi, Vmware sanallaştırma yazılımı üzerine kurulmuştur. Kali, penetrasyon testleri için tasarlanmış açık kaynaklı bir işletim sistemidir. Raspberry Pi'ye bağlı led devresi için ekipman olarak devre tahtası, jumper kabloları, direnç ve kırmızı led kullanılmıştır. Bir led devresi tasarlanıp, ardından devreyi Raspberry Pi üzerindeki genel amaçlı giriş / çıkış (GPIO) pinlerine bağlayarak led devresi Raspberry

Pi'den kontrol edilebilir hale getirilmiştir. led devresi, bir led ve dirençten oluşmaktadır. Direnç, çekilen akımı sınırlamak için kullanılır ve buna akım sınırlayıcı direnç denir. Direnç olmadan led voltajın çok yüksek olduğu bir ortamda çalışacak ve bu da çok fazla akım çekilmesine neden olacak ve bu da anında ledi ve muhtemelen Raspberry Pi üzerindeki GPIO bağlantı noktasını yakacaktır [70]. Deney ortamında kullanılan cihazların bilgileri Çizelge 6.1'de belirtilmiştir.

Çizelge 6.1. Deney ortamında kullanılan cihaz bilgileri

| Cihazlar | IP Adresleri | MAC Adresleri | Rolü/Amacı |
|---|---|---|---|
| Raspberry Pi | 192.168.1.37 | b8:27:eb:08:86:07 | Kurban / İstemci |
| Windows Bilgisayar | 192.168.1.40 | fc:f8:ae:4e:c2:df | Sunucu |
| Kali Bilgisayar | 192.168.1.38 | 1c:bf:ce:1d:e4:c9 | Saldırgan |

Çalışmada, Raspberry Pi'ye bağlanan led devresinin sürekli yanıp sönmesi amaçlanmış ve topolojide yer alan Windows makinaya bu led bilgilerini göndermesi hedeflenmiştir. Böylelikle gerçek dünyada uzaktaki bir gömülü sistemden gelen verinin takip edilmesi senaryosu oluşturulmuştur.

Ledin yanıp sönmesi amacıyla yazılan python kodu Şekil 6.2'de yer almaktadır. Kod parçacığına, önce ilgili kütüphaneler olan GPIO ve time kütüphaneleri eklenmiştir. GPIO kütüphanesi GPIO pinlerini kontrol edebilmek için gereklidir. Ardından GPIO pinlerinden 12 numaralı pin kullanılmıştır. 12 numaralı pin çıkış pini olarak tanımlanmış ve başlangıçta kapalı olması gerektiği belirtilmiştir. Son olarak ledin 1 saniye aralıklarla sürekli yanıp sönmesi için tanımlama yapılmış ve ledin başarıyla yanıp söndüğü Şekil 6.3'te görülmüştür.

```
import RPi.GPIO as GPIO
import time

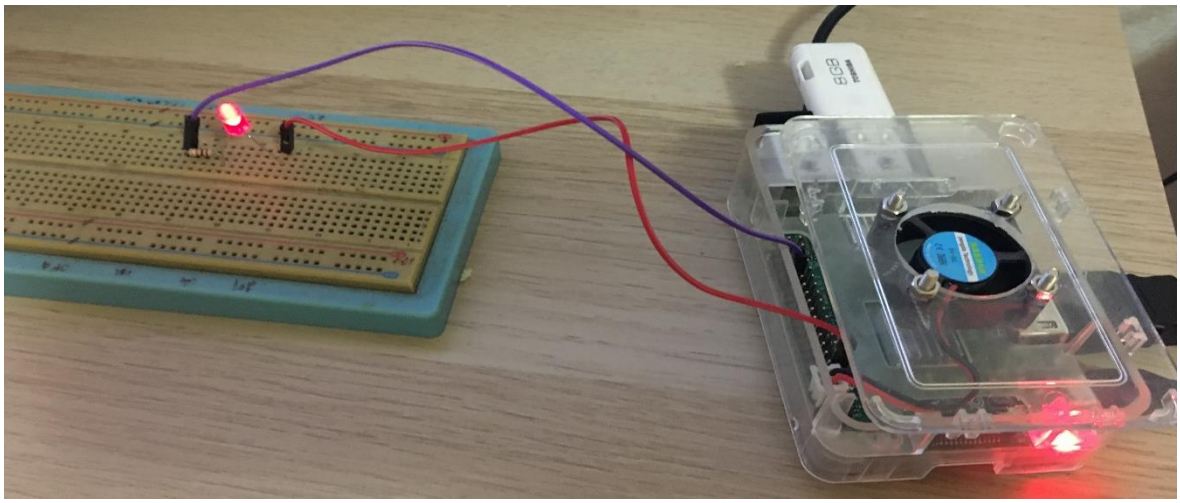
GPIO.setwarnings(False)

GPIO.setmode(GPIO.BOARD)

GPIO.setup(12, GPIO.OUT, initial=GPIO.LOW)

while True:
    GPIO.output(12, GPIO.HIGH)
    time.sleep(1)
    GPIO.output(12, GPIO.LOW)
    time.sleep(1)
```

Şekil 6.2. Ledin yanıp sönmesini sağlayan python kodu [71, 72]

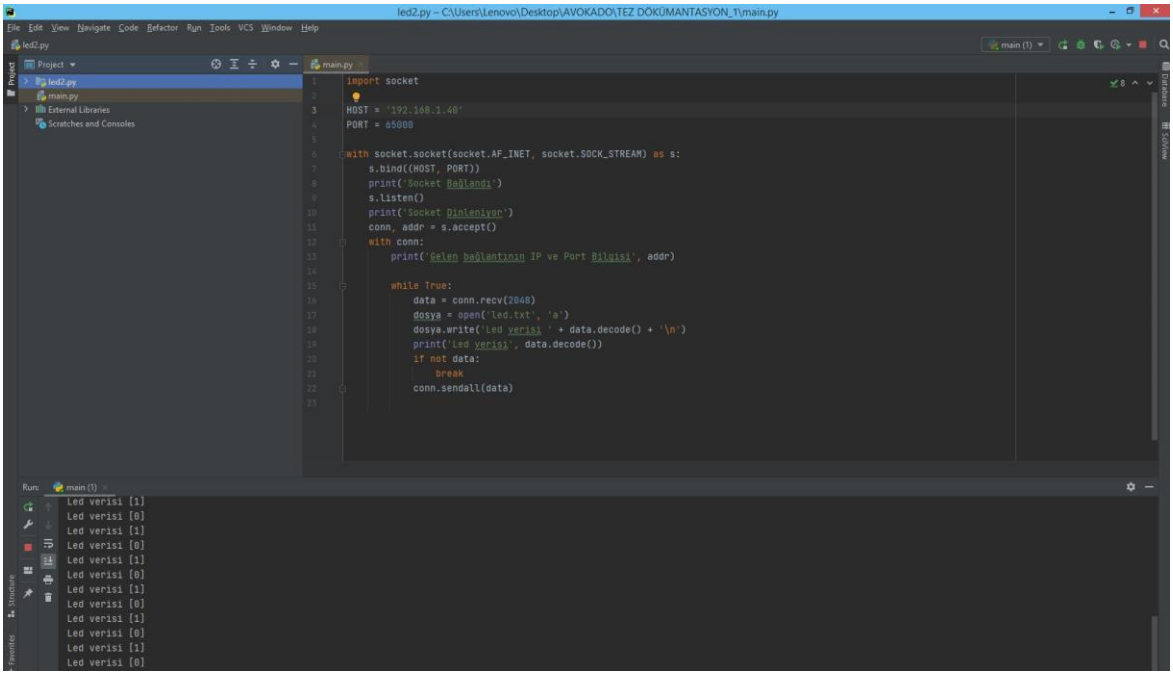


Şekil 6.3. Ledin yandığı esnada alınan görüntüsü

İkinci adım yanıp sönen led verilerinin (yandığında 1, söndüğünde 0) Windows makinaya gönderilmesi işlemidir. Bu maksatla soket programlama yöntemi kullanılmıştır. Soket programlama, TCP/IP protokolü aracılığıyla aynı ağda yer alan iki cihazın bir kanal yardımıyla haberleşmesi olarak tanımlanmaktadır [73].

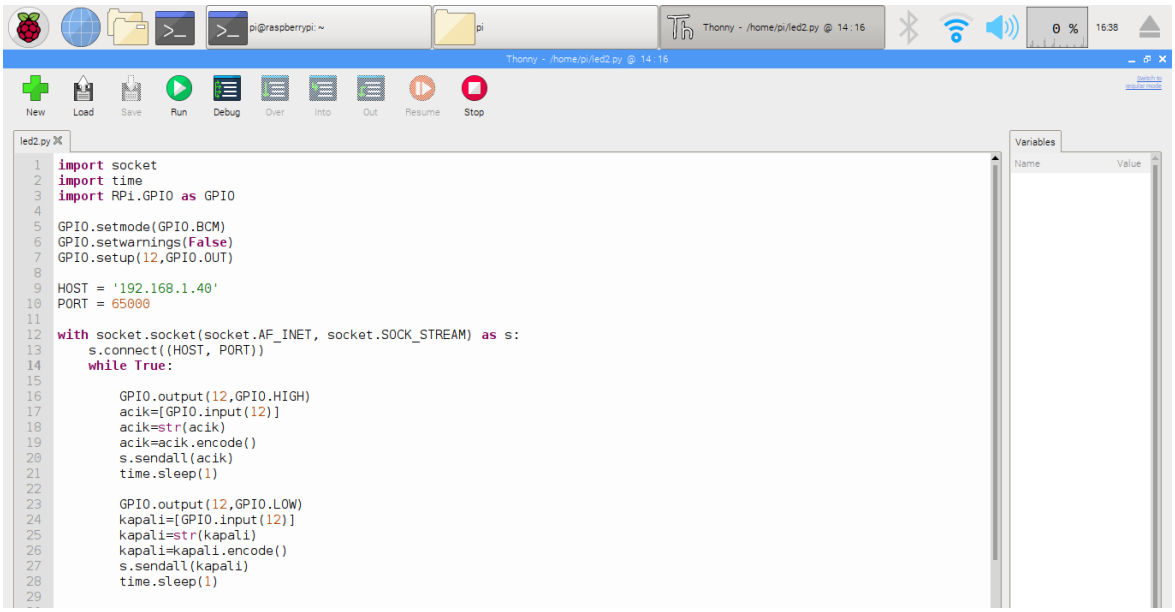
Soketler genellikle istemci ve sunucu etkileşimi için kullanılır. İstemciler sunucuya bağlanır, bilgi alışverişinde bulunur ve ardından bağlantıyı keser. Sunucu önce istemcilerin sunucuyu bulmak için kullanabileceği bir adres oluşturur. Adres belirlendiğinde, sunucu istemcilerin bir hizmet talep etmesini bekler. İstemciden sunucuya veri alışverişi, bir istemci bir soket aracılığıyla sunucuya bağlandığında gerçekleşir. Sunucu, istemcinin isteğini gerçekleştirir ve yanıtı istemciye geri gönderir [74].

Bu çalışmada python kullanılarak sunucu ve istemci için iki farklı kod parçacığı yazılmıştır. Sunucu tarafı kod bloğu Şekil 6.3'de, istemci tarafı kod bloğu Şekil 6.4'te yer almaktadır.




Şekil 6.4. Sunucu (Windows) tarafı soket programlama python kodu

İstemci tarafı için yazılan soket programlama kodu ile LED'in yanıp sönmesi için yazılan kod parçacığı birlikte yazılarak, yanıp sönen led verilerinin soket yardımıyla gönderilmesi amaçlanmıştır.

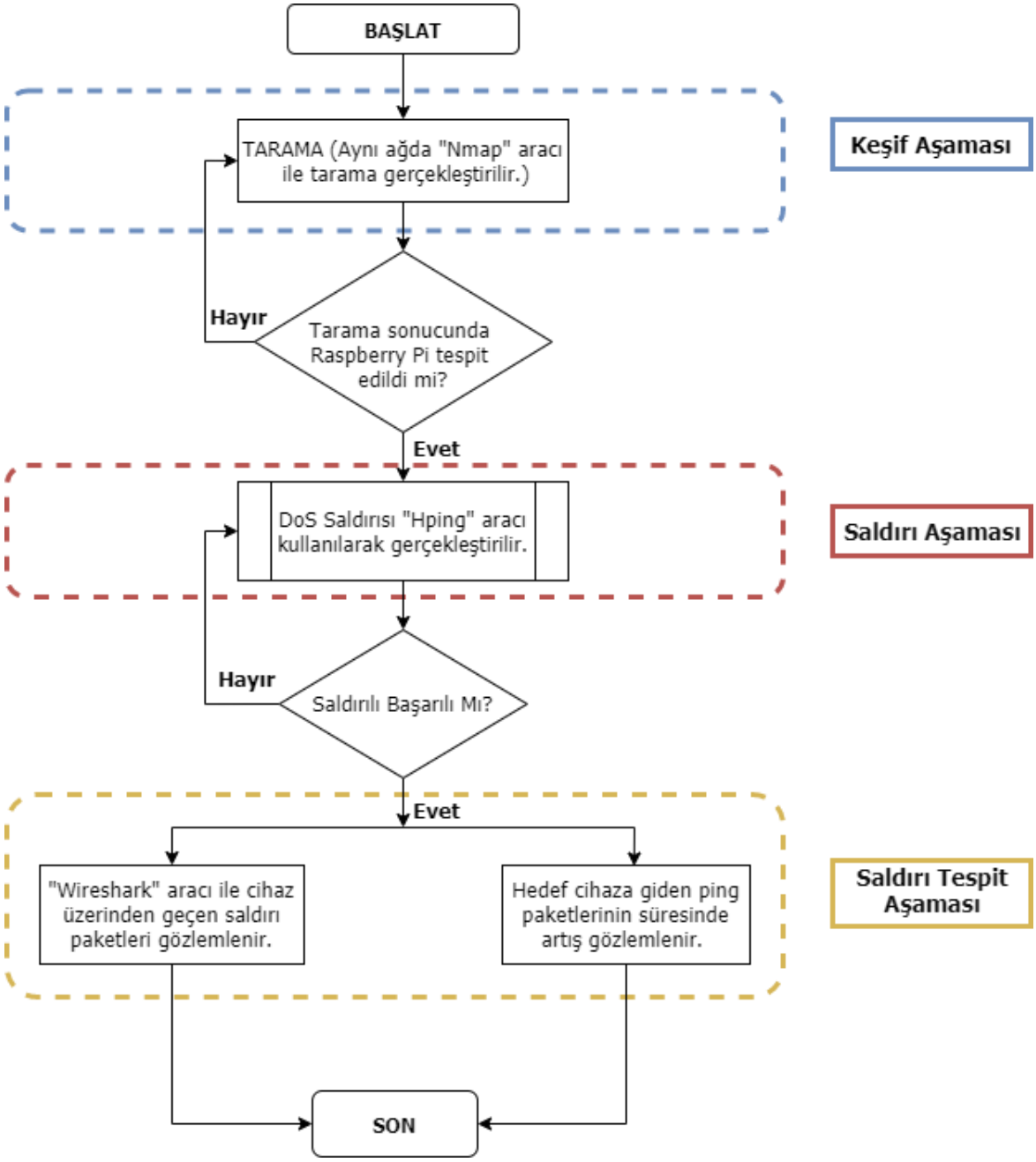



Şekil 6.5. İstemci (Raspberry Pi) tarafı soket programlama python kodu

Test ortamının hazırlanma süreci, topolojinin oluşturulması, ledin yanması ve led verilerinin iletilmesiyle tamamlanmıştır. Bundan sonraki adımlarda saldırı aşamasına geçilmiştir. İlk olarak hizmet dışı bırakma saldırısı, ardından ortadaki adam saldırısı ve son olarak süreç öldürme saldırısı gerçekleştirilmiştir. Bu saldırılar sızma testi metodolojileri adımları izlenerek yapılmıştır.

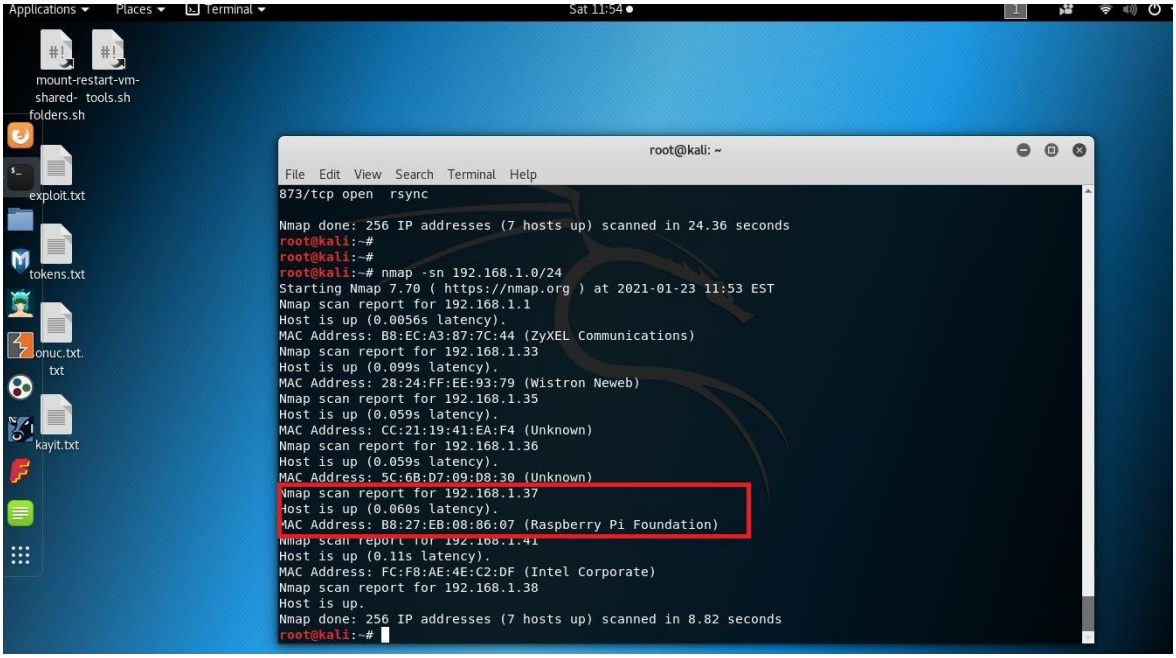
## 6.2. Hizmet Dışı Bırakma Saldırısı (DoS) / Pseudo (Yalancı) DDoS

DoS saldırısı, çalışan bir hizmeti engellemek veya aksatmak için yapılan saldırı olarak bilinir [75]. Tek bir kaynak kullanılarak gerçekleştirildiği için DoS olarak isimlendirilen bu saldırı, birden fazla dağıtılmış kaynak kullanılarak (botnet) gerçekleştirildiğinde DDoS olarak adlandırılır. DoS ve DDoS saldırılarının temel amacı, ağın, bilgisayar sistemlerinin ve donanımlarının bant genişliği, hafıza ve disk alanı gibi kaynaklarının kaldırabileceğinden daha fazla yük bindirilmesinin sağlanarak; sistemin kullanılamaz hale getirilmesidir [76]. Bu çalışmada oluşturulan topoloji kapsamında Raspberry Pi'ye DoS saldırısı gerçekleştirilmiş ve saldırı adımları Şekil 6.5'te ki akış şemasında gösterilmiştir.



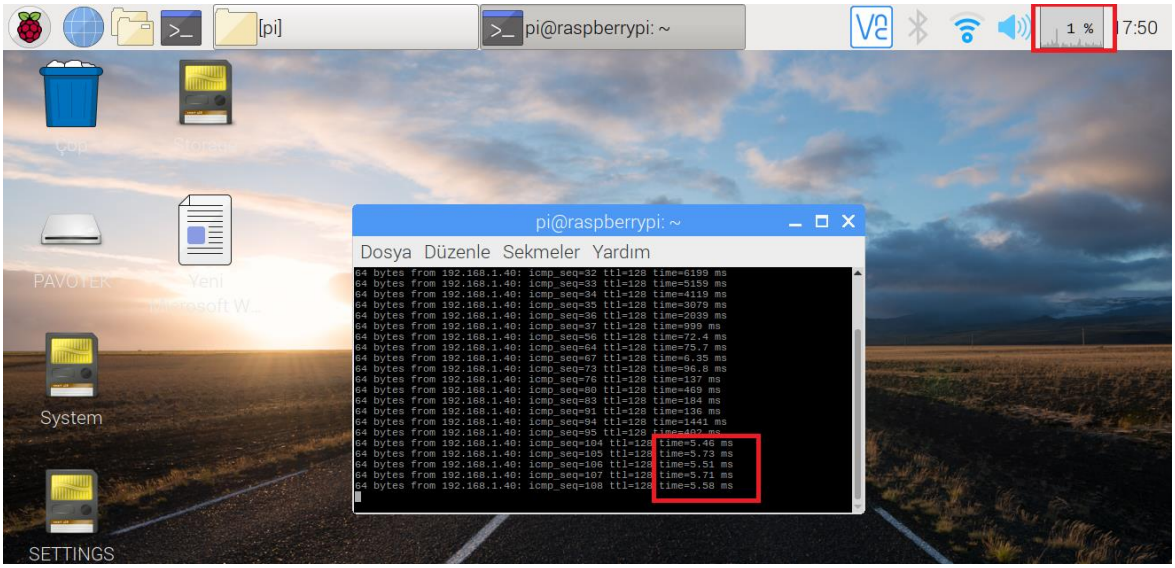

Şekil 6.6. Hizmet dışı bırakma daldırısı (DoS) akış diyagramı

Öncelikle saldırı yapılacak sistemle doğrudan iletişime geçmeden (pasif) veya iletişime geçerek (aktif) bilgi toplama işlemi gerçekleştirilir. Kali işletim sistemi üzerinde yer alan ve aktif bilgi toplama araçlarından olan nmap ile ağ taranarak hedef cihaz olan Raspberry Pi'nin IP adresi ve MAC adres bilgisi Şekil 6.6'da görüldüğü gibi elde edilmiştir. DoS saldırısı için ihtiyaç duyulan tek şey hedef makinanın IP adresi olduğu için Kali işletim sistemi üzerinde yer alan hping3 aracıyla saldırı başlatılmıştır.




Şekil 6.7. Nmap aracı ile ağ taraması

Şekil 6.7'de saldırı gerçekleştirilmeden önce Raspberry Pi'den Windows makinaya doğru gönderilen ping paketleri ve ping süreleri ile cihazın CPU değeri yer almaktadır . Burada ping sürelerinin kısa ve Raspberry Pi'nin CPU değerinin düşük olduğu görülmektedir.

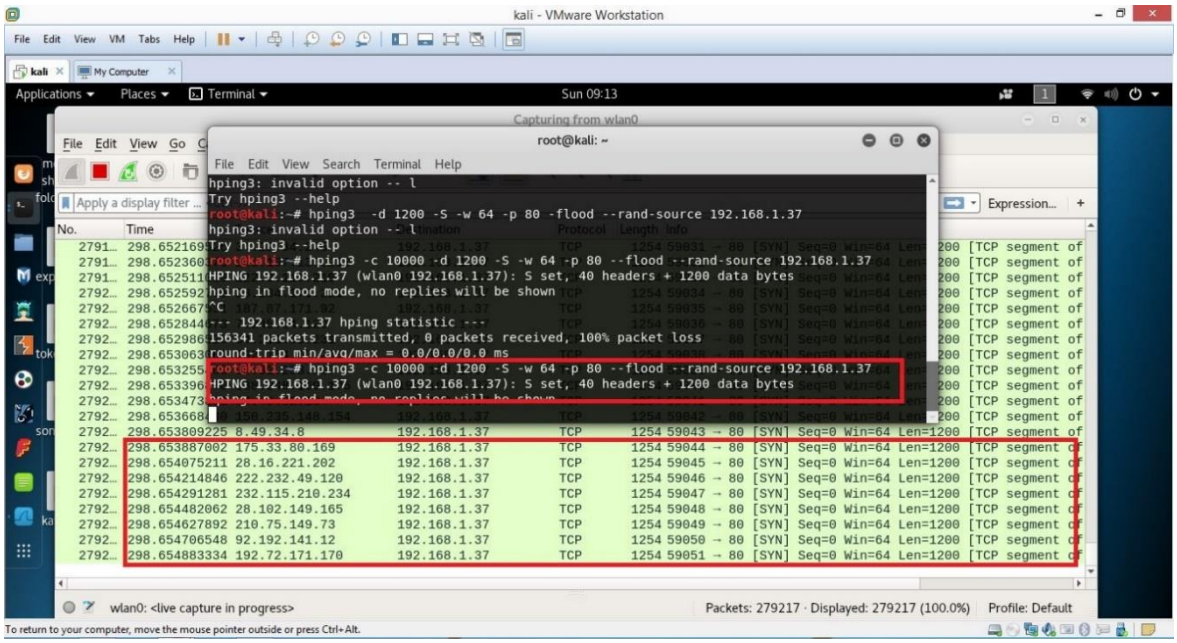



Şekil 6.8. Saldırı öncesi Raspberry Pi'nin durumu

Kali'de "hping3 -c 10000 -d 1200 -S -w 64 -p 80 --flood --rand-source 192.168.1.37" komutu çalıştırılmıştır. "-c 10000" gönderilecek paket sayısının 10000 olduğu, "-d 1200" hedef makineye gönderilen her paketin boyutunun 1200 bayt olduğu, "-S" yalnızca SYN

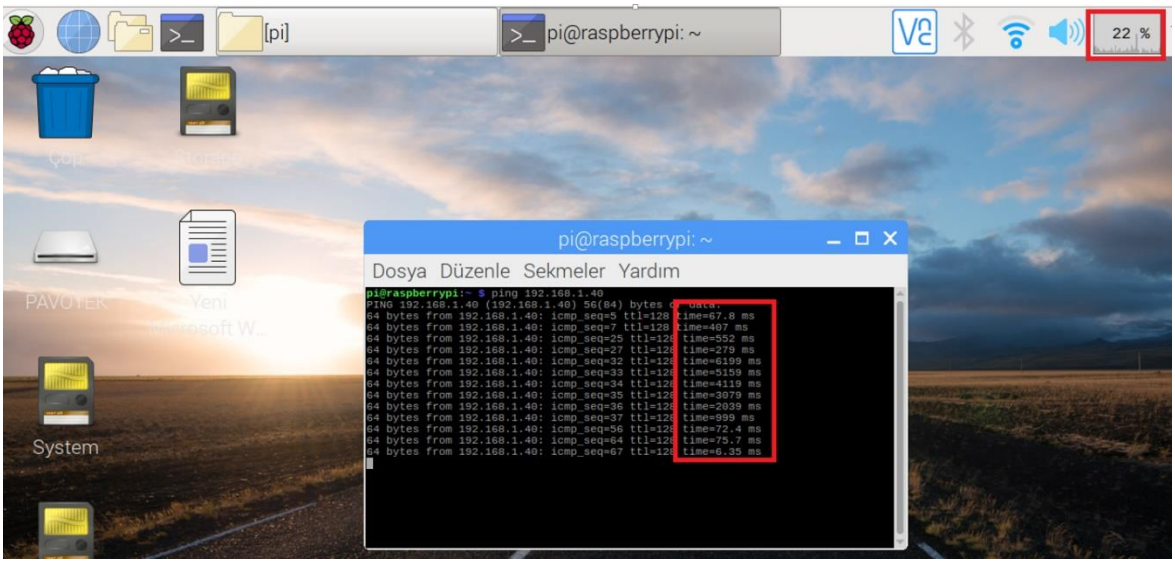
paketlerinin gönderileceği, "-w 64" TCP pencere boyutu, "-p 80" hedef bağlantı noktası, "--flood" gelen yanıtları göstermeye özen göstermeden paketlerin olabildiğince hızlı gönderileceği, "--rand-source " ise rastgele kaynak IP adresinin (bogon) kullanılacağı anlamına gelir. DoS saldırısı başlatıldıktan sonra, ping komutu ile Windows PC ve Raspberry Pi arasındaki bağlantı kontrol edilir.

Wireshark trafik analiz aracı ile saldırgan bilgisayardan kurbana giden TCP paketleri Şekil 6.8'de görülmektedir. Tek kaynaktan yapılan saldırılarda paketler genel olarak aynı IP adresinden gelmektedir. Fakat IP sahteciliği yapılarak farklı IP adreslerinden yapılan DoS saldırılarında ise saldırının hangi IP adresinden gerçekleştirildiğini tespit etmek çok zordur. Wireshark çıktısında görüldüğü üzere hping3 aracının IP sahteciliği özelliği ile Raspberry Pi'ye rastgele kaynaklardan (bogon IP) saldırılar gerçekleşmektedir. Bu sebeple bu saldırı Pseudo(yalancı/sözde) DDoS saldırısı olarak ifade edilir.




Şekil 6.9. Hping3 saldırısı ve Wireshark ile gönderilen paketlerin görülmesi

Saldırı esnasında Raspberry Pi üzerinden alınan ekran görüntüsü Şekil 6.9'da yer almaktadır. Saldırı oldukça kısa bir süre gerçekleştirildiği halde ping sürelerinde dalgalanmalar olduğu ve Raspberry Pi'nin CPU değerinin %22 değerine ulaştığı görülmüştür.



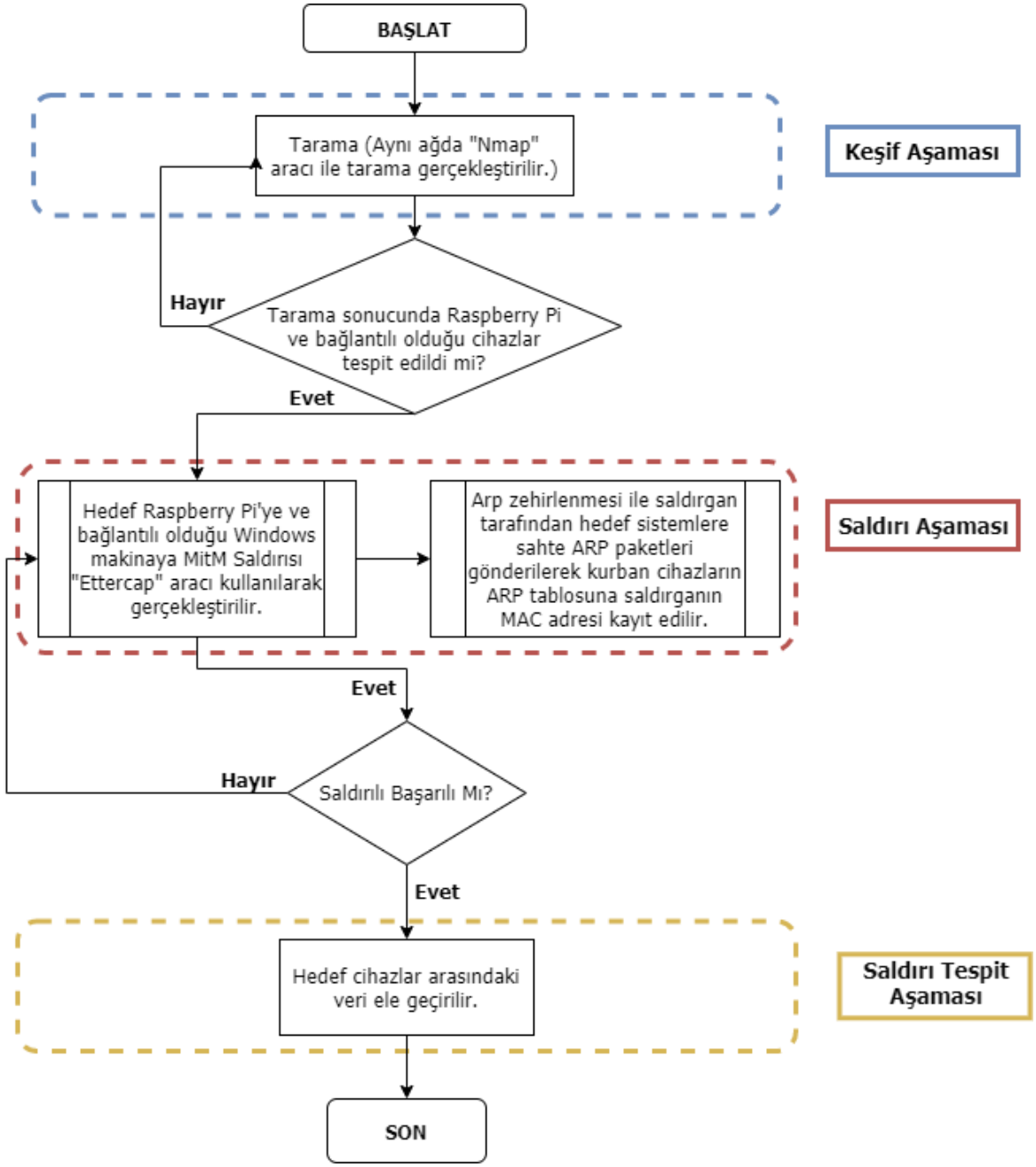

Şekil 6.10. Saldırı esnasında Raspberry Pi'nin durumu

### 6.3. Ortadaki Adam Saldırısı (MitM)

Ortadaki adam saldırısı, kötü niyetli saldırganın haberleşen iki sistem arasına girip iletişimi dinlediği, her iki tarafı taklit ettiği ve aradaki bilgilere ulaştığı bir saldırı türüdür. MitM saldırısı iletişimi gizlice dinleyerek gizliliğe, iletişimi durdurarak ve mesajları değiştirerek bütünlüğe, mesajları yok ederek veya taraflardan birinin sona ermesine neden olacak şekilde mesajları değiştirerek erişilebilirliğe zarar vermeyi amaçlar [77].

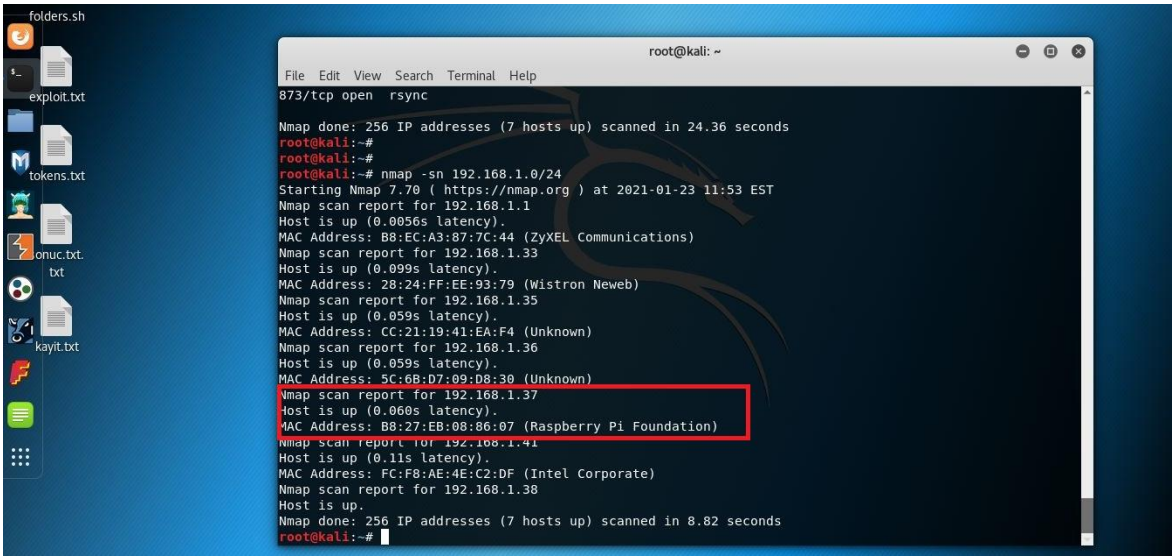
Bu saldırı türü genel olarak ARP (adres çözümleme protokolü) protokolündeki zafiyetler kullanılarak gerçekleştirilir. ARP, IP adresinin yerel ağdaki aygıtın MAC adresiyle eşlenmesine yardımcı olan protokoldür. Ağda iletişim kurmak isteyen tüm cihazlar, diğer makinelerin MAC adreslerini bulmak için sistemde ARP sorguları yayınlar. Bu protokoldeki açıklık kimlik doğrulama eksikliğidir. Protokol, ARP isteklerinin ve yanıtlarının doğru bilgisayarlardan gelip gelmediğini belirlemek için uygun bir kimlik doğrulama mekanizmasına sahip değildir. Bununla, bir saldırgan kurbanın cihazında bir ARP isteği veya yanıtı oluşturabilir ve meşru iletişim kuran ana bilgisayar gibi davranabilir. Cihazlar, isteklerin nereden geldiğini doğrulamadan kabul ederler [78].

Ortadaki adam saldırısının gerçekleştirilme adımları Şekil 6.10'da akış şemasında detaylı olarak anlatılmıştır.



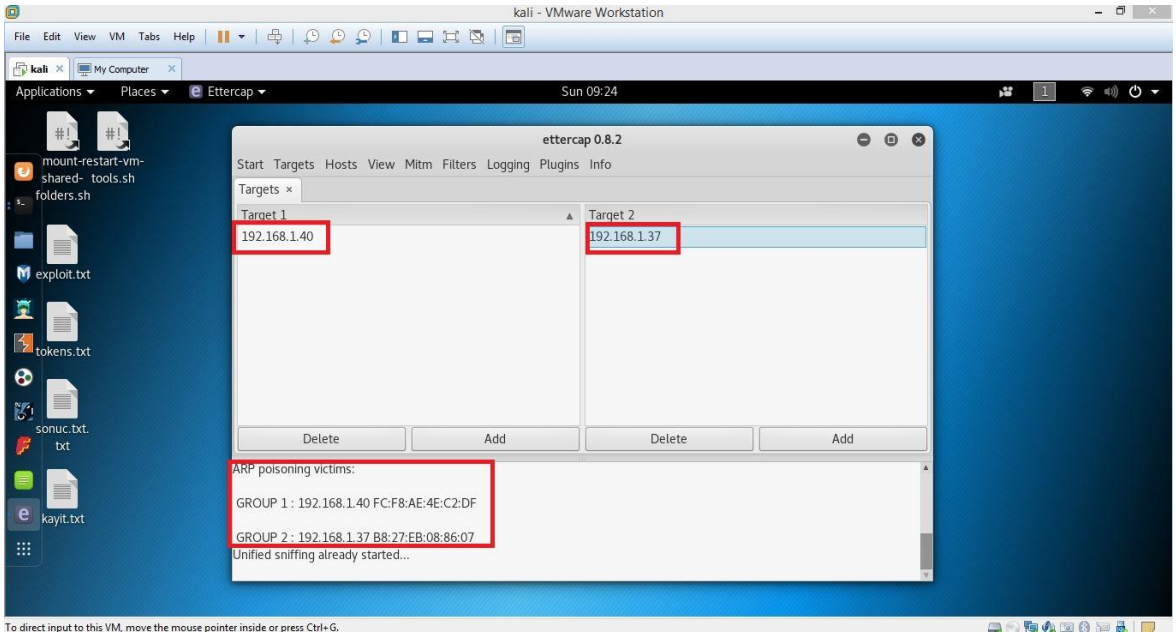

Şekil 6.11. MitM saldırısı akış diyagramı

Bu kapsamda, öncelikle Kali işletim sistemi üzerindeki nmap aracı ile ağ taranarak MitM saldırısının gerçekleştirilmesi için ARP zehirlenmesi yapılacak hedef ile haberleştiği sistem tespit edilmiştir. Şekil 6.11'de görüldüğü üzere tarama sonucunda elde edilen ağ adreslerinden 192.168.1.37 IP numarası Raspberry Pi bilgisayarına aittir. Daha sonra veri akışının gerçekleştiği Raspberry Pi ve Windows bilgisayarın arasına girilerek hassas bilgiler elde edilmiştir.



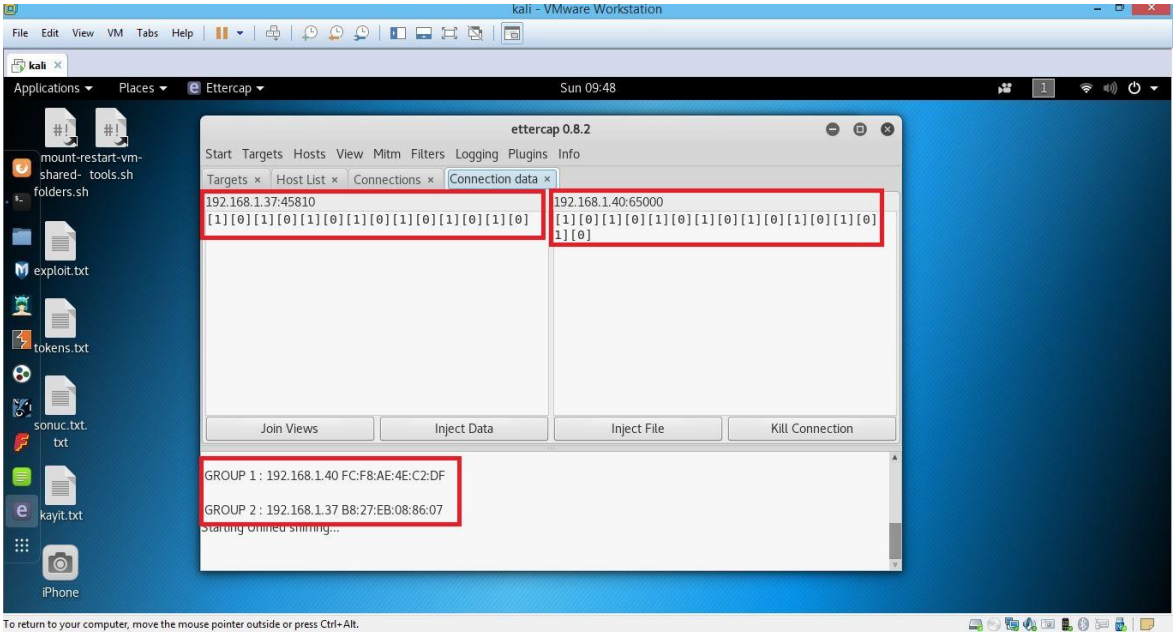

Şekil 6.12. Nmap ile ağ taraması

Kali işletim sistemi üzerinde yer alan ettercap aracı ile arp zehirlenmesi yapılarak iki kurban bilgisayar arasına girilerek ortadaki adam saldırısı gerçekleştirilmiştir. Saldırgan bilgisayar olan Kali, Raspberry Pi ve Windows makinaya sahte ARP paketleri göndererek kendisini diğer bilgisayar olarak tanıtır. Saldırı başarılı olduğunda ise her iki bilgisayarın ARP tablosu değişir tüm trafik saldırgan üzerinden iletilmeye başlar. Şekil 6.12'de tarama sonucu IP adresleri tespit edilen hedeflerin ettercap aracı ile arp tablosunun zehirlendiği görülmektedir.




Şekil 6.13. Ettercap aracı ile hedeflerin ARP tablosunun zehirlenmesi

Ettercap aracı ile arp tablosu zehirlenip araya girildikten sonra Şekil 6.13' de Raspberry Pi'den Windows makineye gönderilen led verisinin ele geçirildiği görülmektedir.

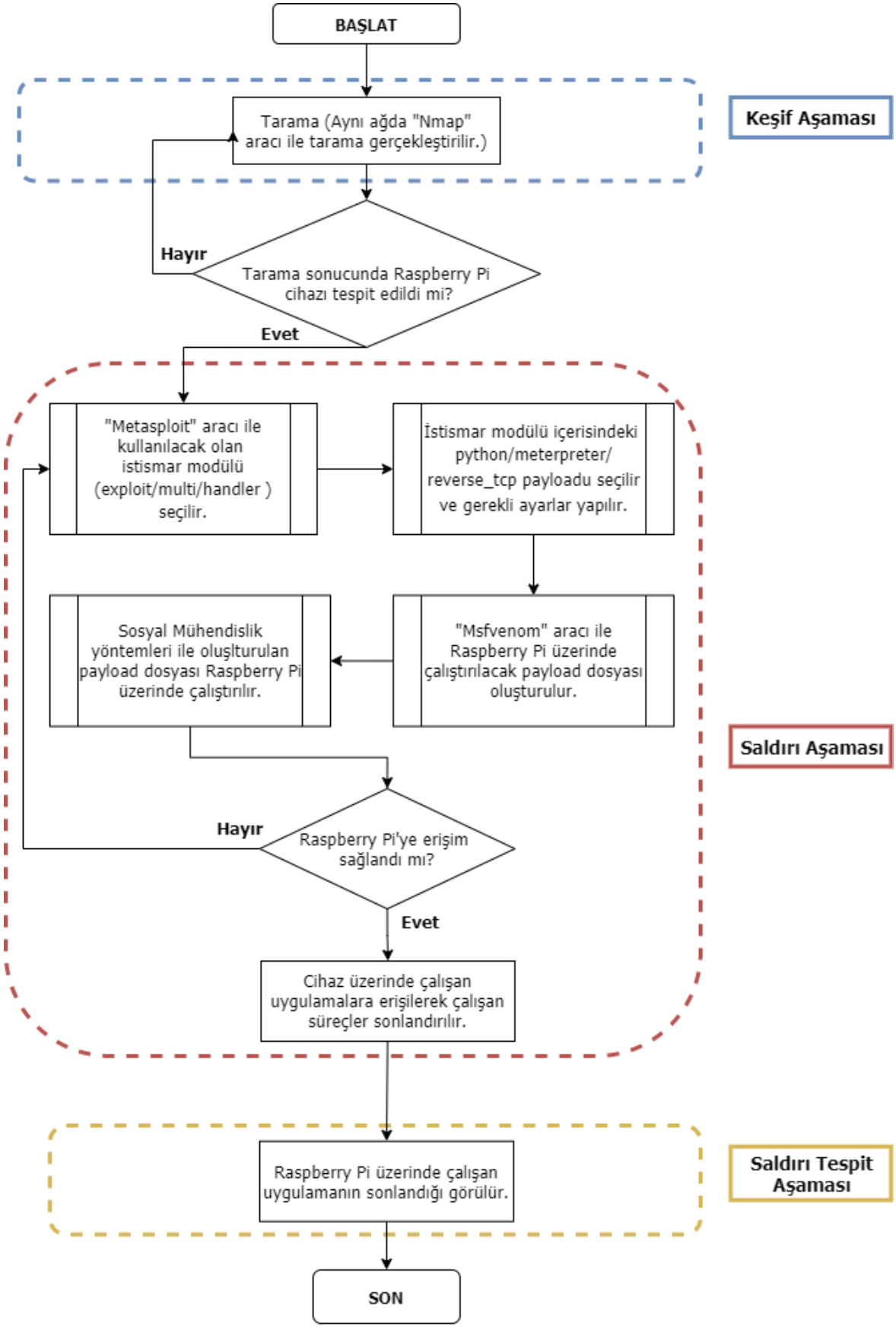



Şekil 6.14. Led verisinin ele geçirilmesi

### 6.4. Süreç Öldürme Saldırısı

Ters TCP (Reverse TCP) bağlantı saldırgan tarafta port açılması, karşı makinenin o porta bağlanarak veri aktarması mantığına dayanır. Bu bağlantı ile kurbanın makinesine meşru gibi görünen çalıştırılabilir bir dosya gönderilir. Eğer kurban dosyayı çalıştırırsa saldırganın sistemin uzaktan kontrolünü ele geçirmesine izin veren oturum kurulmuş olur. Kişinin dosyayı çalıştırmasının sağlanması sosyal mühendislik yöntemleri kullanılarak gerçekleştirilir. Kurban ele geçirildikten sonra saldırgan senkronizasyon paketlerini kurbana gönderir. Kurban sistem senkronizasyon paketlerini dinler ve arka kapıyı oluşturan istenen bağlantılara izin verir. Bağlantı kurban sistem tarafından başlatıldığından, sistemde güvenlik duvarı varsa bile bağlantıya izin verilir [79]. Güvenlik duvarları başta olmak üzere siber güvenlik sistemleri kurumsal ağın dışından gelen paketlere daha sıkı koruma, kısıtlama ve kontrol sağlarken, ağ içindeki trafiğe karşı aynı oranda koruma tedbirleri uygulamamaktadır [80]. Bu nedenle Reverse Shell kullanımı bağlantının devamlılığı için oldukça önemli bir avantaj sağlanmaktadır.

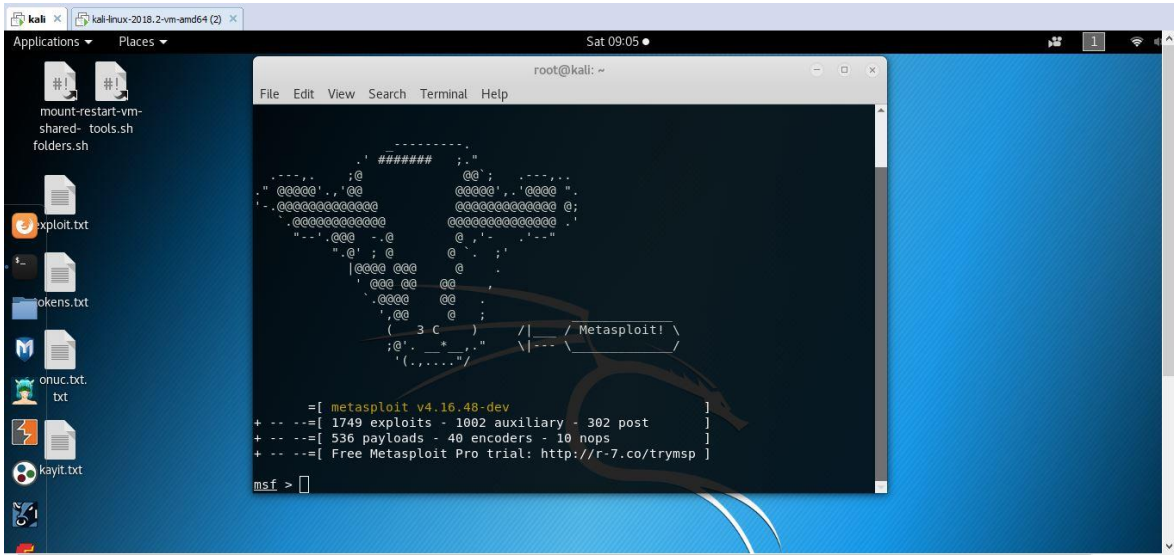
Saldırı adımları Şekil 6.15'de ki akış şemasında detaylı olarak belirtilmiştir.




Şekil 6.15. Süreç öldürme saldırısı akış diyagramı

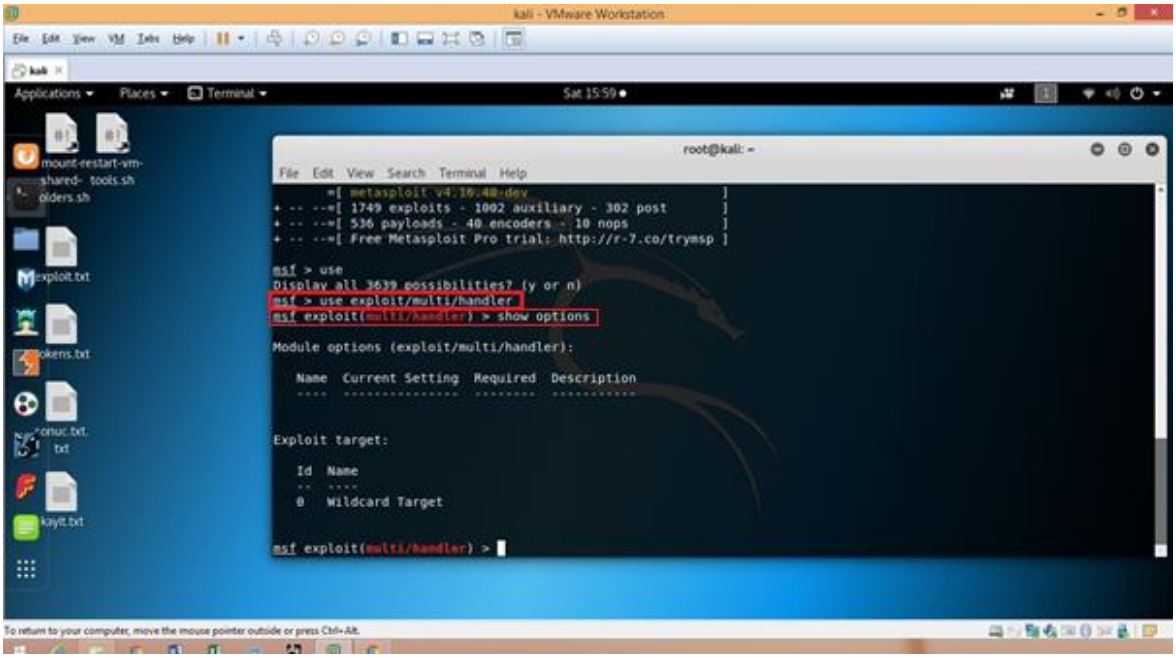
Bu saldırıyı gerçekleştirmek için bu çalışmada Kali işletim sistemi üzerinde yer alan Metasploit aracı kullanılmıştır. Metasploit sızma testi gerçekleştirmek amacıyla geliştirilmiş, içinde binlerce zararlı yazılım, araç ve payload barındıran bir platformdur. Metasploit de yer alan içerikler hedef sistemler üzerindeki zafiyetleri sömürmek amacıyla kullanılmaktadır.

Hedef makine olan Raspberry Pi'de bir Meterpreter shell açmak için Metasploit kullanılmıştır. Metasploit'in veritabanı ile etkileşim kurabilmesi için öncelikle ‘postgresql’ servisi aktif edilmiştir. Daha sonra ‘msfconsole’ komutu çalışıtırılarak Metasploit başlatılmıştır. Şekil 6.15’de Metasploit arayüzü görülmektedir.




Şekil 6.16. Metasploit aracı

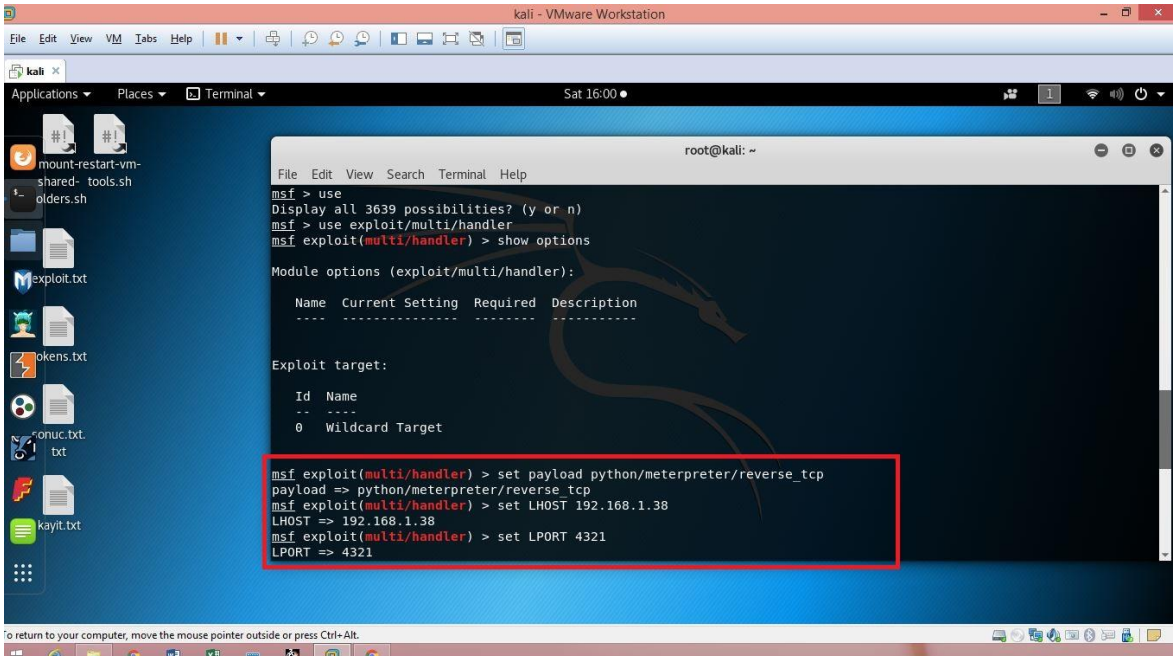
Metasploit başlatıldıktan sonra, bir exploit seçilmesi gerekir. Bu çalışmada exploit/multi/handler istismar modülü kullanılmıştır. Şekil 6.16’da modülün kullanılma komutları yer almaktadır. ‘use’ komutu exploit işlemlerinin gerçekleştirilmesi için gereken modülleri seçmemizi sağlamaktadır. ‘exploit’, kullandığımız modülün bir istismar modülü olduğunu belirtir.’multi’ ise bu istismarın işletim sistemlerinde çalıştığını belirtir. ’handler’, istismarın kurban makineden bazı verileri bekleyeceği ve ardından istismarın bu verileri kullanacağı anlamına gelir.




Şekil 6.17. Metasploit aracında kullanılacak istismar modülünün seçilmesi

Şekil 6.17'de görüldüğü gibi kullanılacak modül içerisindeki parametreler show options komutu ile görülebilmektedir. İlgili parametrelere atamalar ise set komutu ile gerçekleştirilmiştir. Yük için ise LHOST ve LPORT olmak üzere iki parametre mevcuttur. Bu seçeneklerin her ikisinin ayarlanması gerekir. LHOST, saldırgan makine IP adresini ifade eder. Bu çalışmada saldırgan makinemiz olan Kali'nin IP adresi 192.168.1.38'dir. LPORT ise yükün iletişim kurmasını istediğiniz bağlantı noktasını ifade eder. Çalışmada 4321 numaralı port kullanılmış olup bu herhangi bir port olabilir.

Kullandığımız istismar modülü içerisindeki payload (yük) ile metasploit belirtilen porttan dinleme yapmaya başlar ve oluşturduğumuz python payload u çalıştırıldığında oturum aktif hale gelir. python/meterpreter/reverse_tcp payloadu python platformunun desteklendiği sistemlerde kullanılmaktadır. Saldırgan, kurbanın son kullanıcının ağına uzaktan erişim sağlayabilmektedir. Bu saldırıda başarı büyük ölçüde sosyal mühendislik tekniklerine bağlıdır. 'python' komutu ile payload platformunun python olduğu belirtilmektedir. 'meterpreter' komutu ile payload un Meterpreter Shell açacağı belirtilir. 'reverse_tcp' komutu ise bağlantı türünü ifade eder.

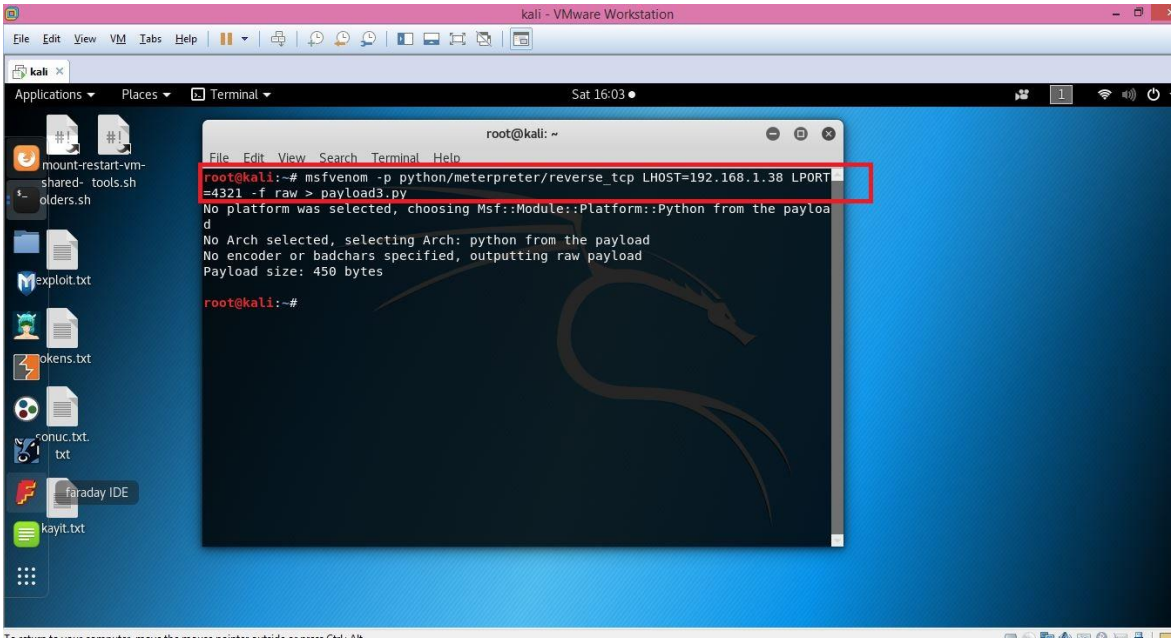



Şekil 6.18. Metasploit aracında gerekli parametrelerin tanımlanması

Metasploit üzerinde payload ayarları yapıldıktan sonra Meterpreter kabuğunu tetiklemek için Raspberry Pi üzerinde çalıştırılacak bir payload dosyası oluşturulmuştur. Yükü oluşturmak için msfvenom adlı bir araç kullanılmıştır. Msfvenom, bir girdi yükünden dosya ve kabuk kodu çıkarmak için kullanılan bir araçtır.

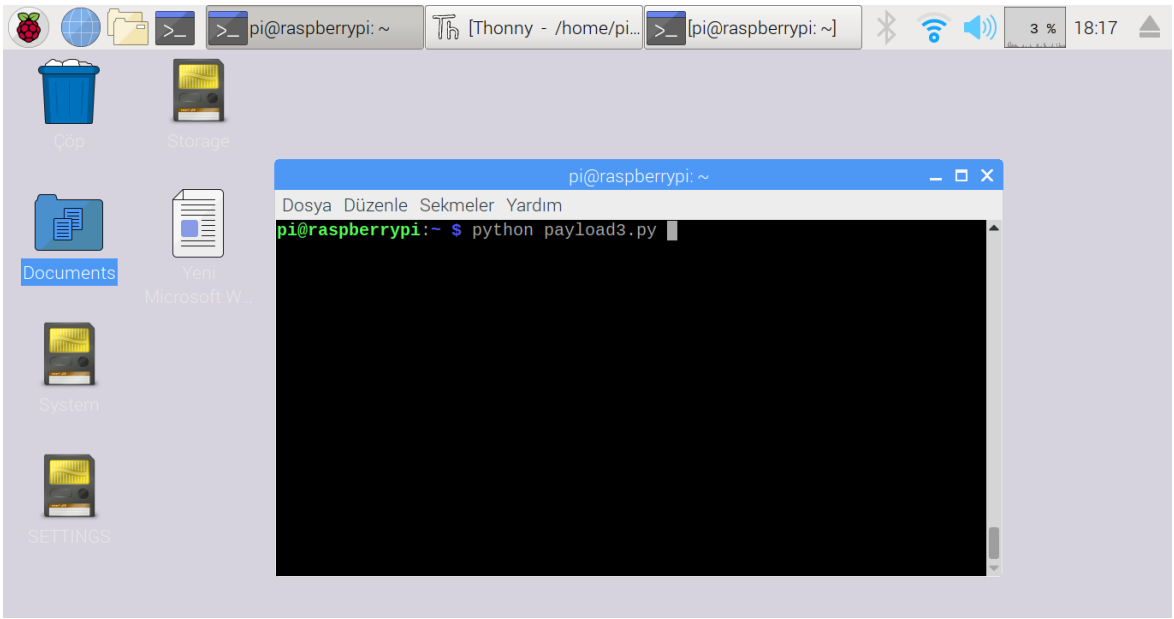
Şekil 6.18'de yük dosyasının msfvenom aracı ile oluşturulma komutu yer almaktadır. Bu komutta yer alan '-p' yükün python/meterpreter /reverse_tcp olduğunu tanımlar. LHOST saldırgan makine IP'si, LPORT ise yük tarafından kullanılan bağlantı noktasıdır. '-f ' değişkeni, yükün biçimini ayarlamamıza izin verir. Ham formatı kullanacağımızı belirttik. '>' parametresi ise yükü payload3.py adlı bir python dosyasına çıkartmak için kullanılmıştır.

Oluşturulan bu payload hedef makine olan Raspberry Pi'ye aktarılarak çalıştırılması sağlanmalıdır. Deney ortamında dosyayı hedef makineye göndermek için sosyal mühendislik yöntemleri kullanılmıştır. Sosyal mühendislik, belirli bilgilere erişim sağlamak veya belirli bir davranışı öğrenmek için kişi veya kişilerin manipüle edildiği bir dizi yöntemdir [81]. Sosyal mühendislik saldırıları yüz yüze etkileşimlerde, telefonlar, mektuplar, e-postalar, web siteleri, aracılığıyla gerçekleştirilebilir. Bu çalışmada ortalığa bırakılan bir USB bellek vasıtasıyla gerçekleştirilmiştir.



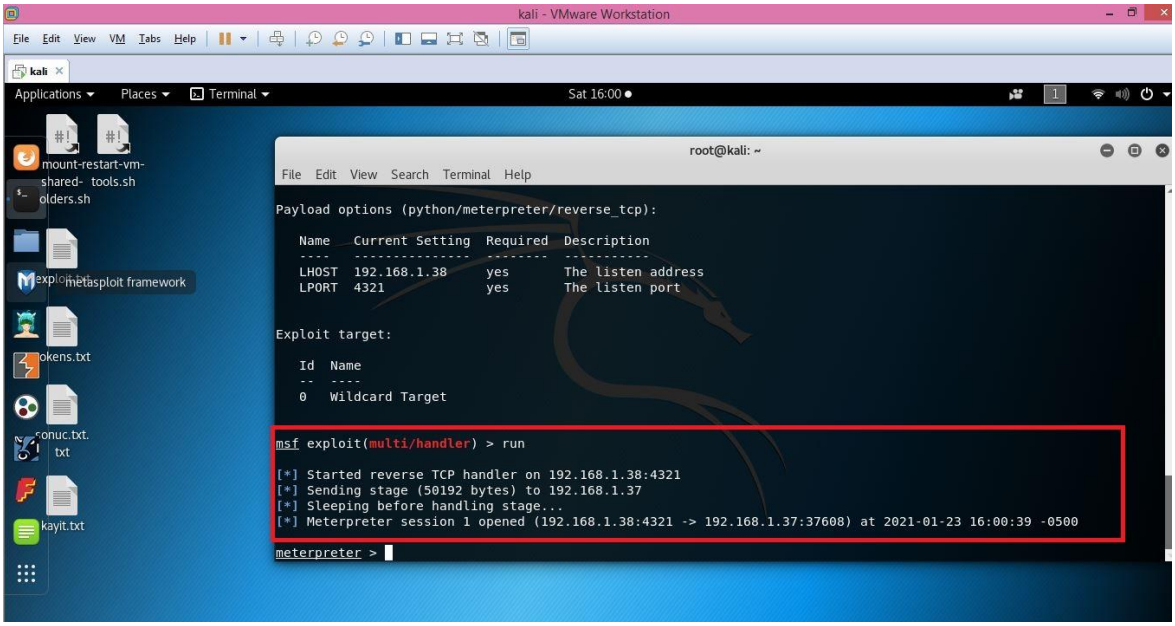

Şekil 6.19. Msfvenom aracı ile payload oluşturma

Payload bir usb belleğe kopyalanmıştır ve bu bellek ortalığa bırakılarak meraklı bir kullanıcı tarafından Raspberry Pi'ye takılarak Şekil 6.19'da görüldüğü gibi çalıştırılması sağlanmıştır.



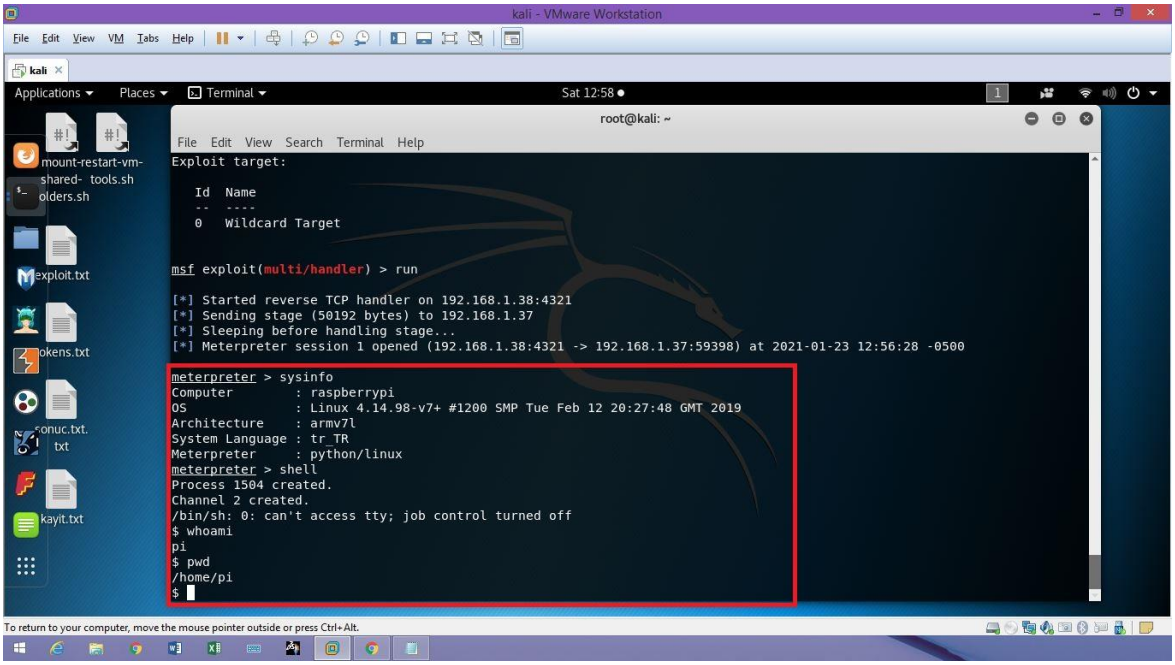

Şekil 6.20. Raspberry Pi'de payload çalıştırılması

Tüm bu aşamalardan sonra run komutu ile exploit çalıştırılmıştır ve Şekil 6.20'de bağlantının kurulduğunu gösteren ekran görüntüsü yer almaktadır. Bu noktada artık hedef sistem üzerinde neredeyse tam kontrole sahip olunmuştur.



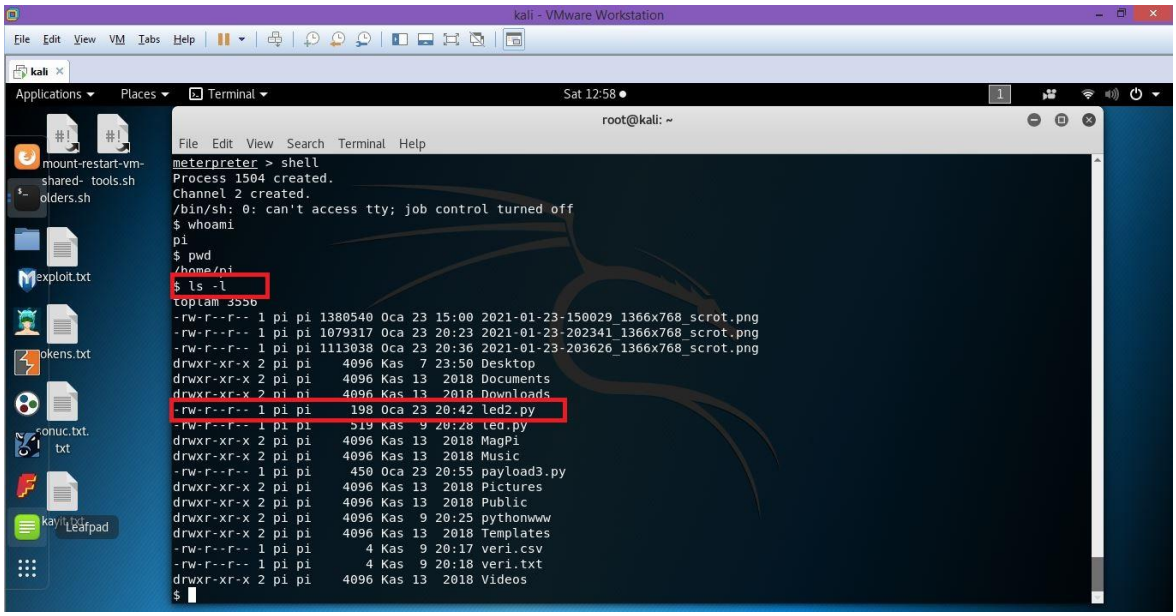

Şekil 6.21. Kali ile Raspberry Pi arasındaki bağlantının kurulması

Şekil 6.21'de görüldüğü gibi 'sysinfo' komutu çalıştırıldığında bilgisayarın Raspberry Pi olduğu görülmüştür. Ayrıca 'shell' komutu ile ele geçirilen sistemin komut satırına geçilerek istenilen işlemler buradan gerçekleştirilebilir. 'whoami' komutunu çalıştırdığımızda 'pi' cevabı, 'pwd' komutunu çalıştırdığımızda ise üzerinden çalışılan dizin olan '/home/pi' çıktısını yine Şekil 6.21'de görmekteyiz.



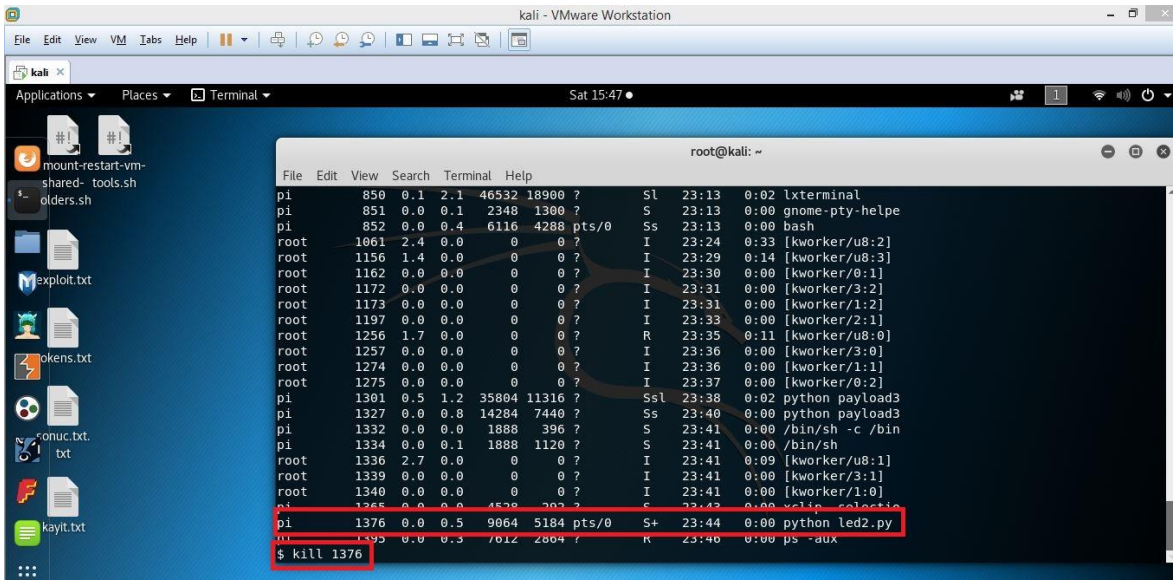

Şekil 6.22. Raspberry Pi'nin bilgilerini görmek için sysinfo komutunu kullanma

‘ls -l’ komutu ile ele geçirilen sistemdeki dosya ve klasörler listelenmiş ve led verilerinin aktarılmasını sağlayan led2.py isimli python dosyasının var olduğu Şekil 6.22’de görülmüştür.



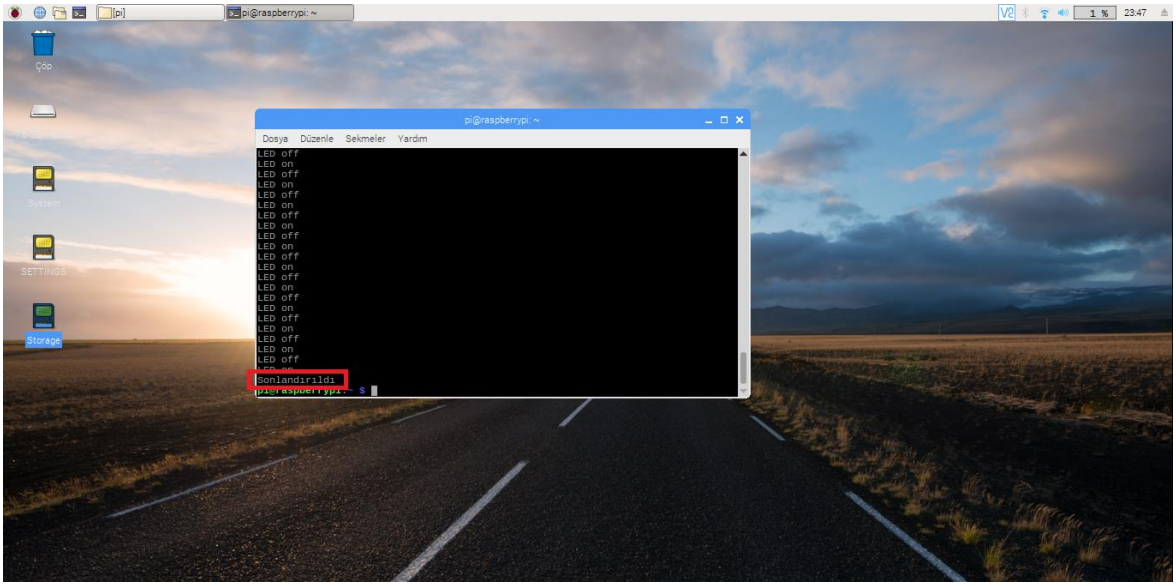

Şekil 6.23. Raspberry Pi üzerindeki dosya ve klasörlerin listelenmesi

‘ps –aux’ komutu ile hedef sistemde çalışan dosyalar Şekil 6.23’de listelenmiştir. Çalışan dosyalar listelendiğinde led2.py isimli python kodu da görülmektedir. Çalışan kod, kill komutu ile proses numarası girilerek sonlandırılmış, led verilerinin akışı durdurulmuştur.




Şekil 6.24. Çalışan uygulamaların listelenmesi ve led2.py uygulamasının sonlandırılması

Raspberry Pi üzerinde ledin çalışmasının durdurduğu Şekil 6.24'te 'sonlandırıldı' mesajının alınmasıyla tespit edilmiştir.




Şekil 6.25. Raspberry Pi üzerinde uygulamanın sonlandığının görülmesi

### 6.5. Analiz Sonuçları

Çalışmanın analiz sonuçları Kali Linux işletim sistemi üzerinde yer alan Wireshark ve Ettercap gibi ücretsiz programlar kullanılarak ve Raspberry Pi üzerinde saldırıların etkilerinin görülmesiyle elde edilmiştir.

İlk olarak Raspberry Pi'ye gerçekleştirilen DoS saldırısı analiz edildiğinde saldırının başarılı olduğu görülmüştür. Gerçekleştirilen DoS saldırısı ile sistemde yer alan Raspberry Pi'ye kısa bir süreliğine büyük miktarlarda paketler gönderilerek sistemin aşırı yük altında kalması sağlanmıştır. Cihaz üzerinden görüldüğü gibi CPU değeri kısa bir süre zarfında %1'den %22 değerine yükselmiştir. Ayrıca Raspberry Pi'den Windows makinaya gönderilen ping paketlerinin iletim süresinin 6199 milisaniyeye kadar çıktığı tespit edilmiştir.

Gerçekleştirilen MitM saldırısında Raspberry Pi ve Windows makine arasındaki verinin Ettercap aracı ile ele geçirilmesi planlanmış ve saldırının başarılı olduğu görülmüştür. Saldırgan Kali bilgisayarı sahte ARP istekleri ile kendisini hedef cihaz olarak göstermiştir. Böylece gerçek hedef olan Windows bilgisayara gidecek paketler saldırgan üzerinden

akmaya başlamıştır. Raspberry Pi üzerinde saldırının gerçekleştiğine yönelik bir tespit yapılamamıştır.

Son olarak süreç öldürme saldırısı ile sistemde çalışan ve Windows makinaya led verilerinin gönderilmesini sağlayan uygulamanın (kodun) durdurulması hedeflenmiştir. Başarılı bir şekilde gerçekleşen saldırı neticesinde sistemde çalışan uygulamalar arasından istenen uygulama bulunarak sonlandırılmıştır. Raspberry Pi üzerinde led bilgilerinin gönderilmediğini belirten "sonlandırıldı" mesajı görülerek saldırı gerçekleştiği tespit edilmiştir. Çizelge 6.2'de gerçekleştirilen saldırıların başarı durumları yer almaktadır.

Çizelge 6.2. Gerçekleştirilen saldırılar ve başarı durumları

| Saldırı Türü | Saldırı Araçları | Tespit Yöntemi | Başarı Durumu |
|---|---|---|---|
| DoS | Hping3 | • Raspberry Pi'nin CPU değerinin ve paket iletim süresinin artması<br>• Wireshark Aracı ile Bogon IP adreslerinin görülmesi | Başarılı |
| MitM | Ettercap | Tespit Edilemedi. | Başarılı |
| Süreç Öldürme | Metasploit ve Sosyal Mühendislik | Raspberry Pi üzerinde görülen "Sonlandırıldı" mesajı. | Başarılı |

Saldırıların sonuçları, Raspberry Pi özelinde diğer gömülü sistem cihazlarının bu saldırılara karşı savunmasız olduğunu ve bu gibi kritik cihazlar için gerekli önlemlerin alınmasının hayati öneme sahip olduğunu göstermiştir. Saldırıların tespit aşamasına yönelik sonuçlar ise gömülü sistemlerde gerçekleşen haberleşme trafiğinin sürekli izlenmesinin, gerçekleştirilebilecek muhtemel saldırıların tespit edilmesi ve önlem alınmasında önemli katkılar sağlayabileceğini göstermiştir.

# 7. SONUÇ VE ÖNERİLER

Endüstrilerde, otomobillerde, tüketici cihazlarında, ev otomasyonlarında, iş altyapısında ve askeri donanımlarda çeşitli ve karmaşık uygulamalarda her yerde mevcut ve yaygın kullanım alanı elde eden gömülü sistemler için güvenlik unsurunun önemi büyüktür. Gerçek zamanlı yanıt alma mekanizması ile kesintisiz ve sürekli çalışmak için tasarlanan gömülü sistemler, güvenlik fikrini ikinci plana attığından saldırganlar için verimli bir ortam sayılmaktadır. Bu sebeple çok çeşitli saldırılar gömülü sistem cihazlarına uygulanabilir. Bu kapsamda tez çalışmasında gerçekleştirilen saldırılar neticesinde ağa bağlı gömülü sistem uygulamalarında kullanılan Raspberry Pi bilgisayarının bir takım saldırılara maruz kalabileceği görülmüştür.

Bu çalışmadaki temel amaç gömülü cihazların kullanılmasıyla giderek daha fazla otomatik hale gelen dünyamızda bu sistemlerdeki güvenlik açıklarının fiziksel dünyada kesintiye ve yıkıma neden olmak için kullanılıp kullanılamayacağını tespit etmektir. Deney ortamında yapılan saldırılar neticesinde güvenlik açığı bulunan bu cihazların sömürülmesinin gerçek bir tehdit olarak algılanıp gömülü cihazların güvenliğinin ihlal edilebildiği görülmüştür. Sınama ortamında gömülü cihaz olarak Raspberry Pi tek kartlı bilgisayarı kullanılmıştır. Bunu sebebi uygun fiyatlı, erişilebilir ve popüler bir ürün olmasının yanı sıra literatürde cihazla ilgili güvenlik sorunlarına çok fazla değinilmediğinin görülmesidir. Bununla birlikte, benzer uygulamalar altıncı bölümde açıklanan saldırı, gözlem ve tespit aşamaları takip edilerek farklı marka ve model cihazlara da uygulanabilir.

Çalışmanın altıncı bölümünde gerçekleştirilen saldırılardan DoS saldırısı, internete bağlı bir gömülü cihazın sunduğu hizmetlerin engellenebileceği ve sistemin çalışamaz hale getirilebileceğinin tespit edilmesi açısından önem taşımaktadır. Hping3 aracı ile bogon IP'ler üzerinden TCP paketleri kullanılarak gerçekleştirilen bu saldırıda saldırganın tespit edilmesi neredeyse imkansızdır. Saldırı süresi kısa olmasına rağmen cihazın CPU kaynağının artmaya başladığı ve paket trafiğinde dalgalanmalar yaşandığı görülmüştür. İki cihazın arasındaki iletişimin dinlenmesi, verilerin ele geçirilmesi ve bu verilerde değişiklik yapılmasını kapsayan ortadaki adam saldırısı ile Raspberry Pi'den Windows bilgisayara gönderilen veri ele geçirilmiştir. Bu saldırı gömülü cihazlardaki kritik bilgilerin ele geçirilebileceğinin gösterilmesi açısından önemlidir. Son olarak metasploit aracı ile ters tcp bağlantı ve sosyal mühendislik yöntemi kullanılarak yapılan süreç öldürme saldırısı ile

gömülü cihazda çalışan kritik bir uygulamanın durdurulabileceği görülmüştür. Raspberry Pi'den Windows bilgisayara led bilgilerinin aktarılmasını sağlayan uygulama süreç öldürme saldırısı gerçekleştirilerek sonlandırılmıştır. Deney ortamında gerçekleştirilen bu saldırılar için alınması gereken tedbirlerden ise aşağıda bahsedilmiştir.

DoS/DDoS saldırılarının engellenmesi ve erken tespitine yönelik gömülü sistemlerin kurulu olduğu ağlarda öncelikle bir risk değerlendirmesi yapılmalı ve bu değerlendirme sonucunda ağda kullanılması gereken güvenlik ürünleri belirlenmelidir. Kritik sistemlerde kullanılan gömülü cihazların bu saldırılara maruz kalıp kalmayacağının tespiti için ise belirli zaman aralıklarında yük testi yapılmalı ve çıkan sonuçlar analiz edilerek gerekli önlemler alınmalıdır. Ağ altyapılarında kullanılan router, switch vb. ağ cihazlarının konfigürasyonlarında yaşanan hataların giderilmesi, ağa bağlı sistemlerde kullanılan güvenlik duvarı ürünlerinde gerekli ayarların yapılması, kullanılmayan servislerin kapatılması gibi uygulamalarda derinlemesine güvenlik için önemlidir.

Ağdaki bir istemcinin taklit edilmesine dayanan ve ARP zehirlenmesi yöntemi ile gerçekleştirilen ortadaki adam saldırısının tespit edilmesi için arpwatch gibi ARP trafiğini izleyen uygulamalar ile MAC ve IP adreslerindeki değişim takip edilmelidir. MAC ve IP eşleşmeleri değiştiği anda arpwatch yazılımı ile değişim tespit edilir ve belirlenen kriterler doğrultusunda log üretilebilir veya ilgili kişilere mail yoluyla bilgilendirme sağlanabilir.

Süreç öldürme saldırısı ile kritik sistemlerdeki uygulamaların sonlandırılabileceği görüldüğünden, çalışan uygulamaların 7/24 izlenmelidir. Sosyal mühendislik yöntemindeki başarı oranının saldırının gerçekleştirilmesindeki etkisi düşünüldüğünde kritik sektörlerde çalışan kişilerin farkındalığının artırılmasına yönelik çalışmalar yapılmalıdır. Kullanıcılara sıklıkla bilinçlendirici eğitimler verilmelidir.

Sağlam bir çözüm, güvenliği en başından ele alır ve güvenlik açıklarını tespit etmek için sistemin yaşam döngüsünü analiz eder. Güvenlik açıklarının kaynaklarını ve nedenlerini keşfettikten sonra, güvenlik önlemleri tasarım metodolojisine dahil edilmelidir. Şu anda, güvenlik sadece sonradan düşünülen bir konudur ve çoğu çözüm, belirli saldırıları engellemek içindir. Bununla birlikte, artan sayıda güvenlik ihlali, ortaya çıkan ekonomik kayıplar ve potansiyel tehlikelerin tümü, temel güvenlik çözümlerinin önemini vurgulamaktadır.

# KAYNAKLAR


1. Çakır, H. Ş., ve Özcanhan, M. H. (2011). *Gömülü Sistem Uygulamalarına Yapılan Saldırılar ve Ağ Bağlantılı Gömülü Sistemlerin Güvenliğinin Sağlanması*. Elektrik-Elektronik ve Bilgisayar Sempozyumu Bildiri Kitabı, 5-7.

2. Chen, J., Guo, H., and Hu, W. (2019). *Research on Improving Network Security of Embedded System*. In 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 136-138.

3. Basan, E., Medvedev, M., and Teterevyatnikov, S. (2018). *Analysis of the impact of denial of service attacks on the group of robots*. In 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 63-638.

4. Vujović, V., and Maksimović, M. (2015). Raspberry Pi as a Sensor Web node for home automation. *Computers & Electrical Engineering*, 44, 153-171.

5. Gupta, M. S. D. Patchava, V., and Menezes, V. (2015). *Healthcare based on iot using raspberry pi*. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 796-799.

6. Williams, M. (2018). *A Risk Assessment on Raspberry Pi Using NIST Standards*. Master's Thesis, Iowa State University Computer Engineering, Ames, Iowa, 1-12.

7. Raman, S. (2018). *Security Risk Management for the IoT Systems*, Master's Thesis, University of Tartu Institute of Computer Science, Tartu, Estonia, 6-12.

8. Hu, Y., Sulek, D., Carella, A., Cox, J., Frame, A., Cipriano, K., and Wang, H. X. (2016). *Employing miniaturized computers for distributed vulnerability assessment*. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 57-61.

9. Al Barghuthi, N. B., Saleh, M., Alsuwaidi, S., and Alhammadi, S. (2017). *Evaluation of portable penetration testing on smart cities applications using Raspberry Pi III*. In 2017 Fourth HCT Information Technology Trends (ITT), 67-72.

10. El-Haii, M., Chamoun, M., Fadlallah, A., and Serhrouchni, A. (2018). *Analysis of cryptographic algorithms on iot hardware platforms*. In 2018 2nd Cyber Security in Networking Conference (CSNet), 1-5.

11. Sanada, A., Nogami, Y., Iokibe, K., and Khandaker, M. A. A. (2017). *Security analysis of Raspberry Pi against Side-channel attack with RSA cryptography*. In 2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 287-288.

12. Hatun, E., Büyükkaya, E., and Evci, M. A. (2019). *Side Channel Analysis of Raspberry Pi with AES Algorithm and Measurement Improvement*. In 2019 27th Signal Processing and Communications Applications Conference (SIU), 1-4.

13. Bruning, M. (2016). An Analysis of the DDoS Potential of Single Board Computers: A Raspberry Pi Case Study. *The Netherlands in International Journal of Computer Science and Network Solutions (IJCSNS)*, 5(7), 47-55.

14. Ojeda Adan, M. F. (2019). *Designing an Internet of Things Attack Simulator*, Bachelor's Thesis, Metropolia University of Applied Sciences of Electronics, Helsinki, 21-37.

15. Martin, E. D., Kargaard, J., and Sutherland, I. (2019). *Raspberry Pi Malware: An Analysis of Cyberattacks Towards IoT Devices.* In 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT), 161-166.

16. Singh, U., Bharadjaw K.N., and Samajpati A. (2017). *Analysis, Detection and Mitigation of Cyber Attacks on IoT Platform*. In 2017 12th Annual Symposium on Information Assurance (ASIA '17), 45-53.

17. Huraj, L., Simon, M., and Horák, T. (2018). *IoT measuring of UDP-based distributed reflective DoS attack*. In 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY*)*, 209-214.

18. Aspernäs, A. and Simonsson, T. (2015). *IDS on Raspberry Pi: A Performance Evaluation*, Diploma Thesis, Linnaeus University Faculty of Technology Department of Computer Science.

19. Mahajan, S., Adagale, A. M., and Sahare, C. (2016). Intrusion detection system using raspberry pi honeypot in network security. *International Journal of Science and Computing IJESC*, *6*(3), 2792-2795.

20. Kyaw, A. K., Chen, Y., and Joseph, J. (2015). *Pi-IDS: evaluation of open-source intrusion detection systems on Raspberry Pi 2*. In 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), 165-170.

21. Tripathi, S., and Kumar, R. (2018). *Raspberry pi as an intrusion detection system, a honeypot and a packet analyzer*. In 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), 80-85.

22. Sforzin, A., Mármol, F. G., Conti, M., and Bohli, J. M. (2016). *Rpids: Raspberry pi ids—a fruitful intrusion detection system for iot*. In 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 440-448.

23. Coşar, M., ve Karasartova, S. (2017, Ekim). *Raspberry Pi ve Snort ile SOHO Networklerde Bir Güvenlik Duvarı Uygulaması*. 2nd International Conference on Computer Science and Engineering, 1000-1003.

24. Lim, C., Marcello, M., Japar, A., Tommy, J., and Kho, I. E. (2014). *Development of Distributed Honeypot Using Raspberry Pi*. In International Conference on Information, Communication Technology and System.

25. Nagy, L., and Coleşa, A. (2019). *Router-based IoT Security using Raspberry Pi*. In 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), 1-6.

26. Sainz-Raso, J., Martin, S., Diaz, G., and Castro, M. (2019). Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses. *IEEE Consumer Electronics Magazine*, *8*(6), 47-52.

27. Feng, X., Babatunde, O., and Liu, E. (2017). Cyber security investigation for Raspberry Pi devices. *International Refereed Journal of Engineering and Science*.

28. Alsaadi, H. H., Aldwairi, M., Al Taei, M., AlBuainain, M., and AlKubaisi, M. (2018). *Penetration and security of OpenSSH remote secure shell service on Raspberry Pi 2*. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1-5.

29. Jiménez, M., Palomera, R., and Couvertier, I. (2013). *Introduction to embedded systems*. New York: Springer, 3-9.

30. Toulson, R., and Wilmshurst, T. (2016). *Fast and effective embedded systems design: applying the ARM mbed*. Newnes, 3-38.

31. Molazem Tabrizi, F. (2017). *Security analysis and intrusion detection for embedded systems: a case study of smart meters*, Doctoral Dissertation, University of British Columbia, Vancouver, Canada, 1-8.

32. Qian, K., Den Haring, D., and Cao, L. (2009). *Embedded software development with C*. Springer, 1-37.

33. Sharma, S. (2013). *Embedded Systems--A Security Paradigm for Pervasive Computing*. In 2013 International Conference on Communication Systems and Network Technologies, 472-477.

34. Wang, X., Wang, Z., Huang, W., Wen, G. Q., and Zhang, S. L. (2017). *Summary of Embedded Systems Development*. In 2017 5th International Conference on Frontiers of Manufacturing Science and Measuring Technology (FMSMT 2017).

35. Shibu, K. V. (2009). *Introduction to embedded systems*. Tata McGraw-Hill Education, 5-60.

36. İnternet: Khadka, S. A Notebook on Embedded System Fundamentals. URL: https://www.scribd.com/document/494167280/A-Notebook-on-Embedded-System-Fundamentals, Son Erişim Tarihi: 12.06.2021.

37. Özcanhan, Mehmet Hilal (2011). *Security and reliability in embedded systems*. Doctoral Thesis. Dokuz Eylül University Graduate School Of Natural And Applied Sciences, İzmir.

38. Jiménez, M., Palomera, R. and Couvertier, I. (2013). *Introduction to embedded systems*, New York: Springer, 1-30.

39. Kavedia, M., and Bhide, A. (2018). *Introduction to Embedded Systems*, Mumbai: Himalaya Publishing, 1-10.

40. Farooq-i-Azam, M., and Ayyaz, M. N. (2012). Embedded Systems Security. In *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies*, IGI Global, 179-198.

41. Ott, K., and Mahapatra, R. (2019). *Continuous authentication of embedded software*. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE*)*, 128-135.

42. Larson, U. E., and Nilsson, D. K. (2008). *Securing vehicles against cyber attacks*. In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, 1-3.

43. Marwedel, P. (2017). *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things*, Dortmund:Springer, 1-25.

44. Vai, M., Nahill, B., Kramer, J., Geis, M., Utin, D., Whelihan, D., and Khazan, R. (2015). *Secure architecture for embedded systems*. In 2015 IEEE High Performance Extreme Computing Conference (HPEC), 1-5.

45. Mirjalili, S. H., and Lenstra, A. K. (2008). *Security observance throughout the life-cycle of embedded systems*. In Proceedings of the 2008 International Conference on Embedded Systems and Applications, 186-192.

46. Meshram, V. H., and Sasankar, A. B. (2016). *Security in Embedded Systems: Vulnerabilities, Pigeonholing of Attacks and Countermeasures*.

47. Khelladi, L., Challal, Y., Bouabdallah, A., and Badache, N. (2008). On security issues in embedded systems: challenges and solutions. *International Journal of Information and Computer Security, 2*(2), 140-174.

48. Baker, A. (2020). Wind River; A Survey of Informatıon Securıty Implementatıons For Embedded Systems, *White Paper,* Alameda, 3-16.

49. Vega, A., Bose, P., and Buyuktosunoglu, A. (2016). *Rugged Embedded Systems: Computing in Harsh Environments*. Cambridge: Elsevier, 149-203.

50. Mehmood, M. A., Khokhar, A. S., and Ali, M. (2011, November). Incorporating Security in Embedded System–A critical analysis. *International Journal of Computer Science Issues*, 8(6), 156-160.

51. İnternet: What is a Raspberry Pi. (2018) Web: https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/, Son Erişim Tarihi: 13.06.2021.

52. İnternet: Raspberry Pi Foundation Annual Review. (2019). Web: https://static.raspberrypi.org/files/about/RaspberryPiFoundationReview2019.pdf, Son Erişim Tarihi: 13.06.2021.

53. Kölling, M. (2016). Educational programming on the Raspberry Pi. *Electronics*, *5*(3), 33.

54. Nayyar, A., and Puri, V. (2015). Raspberry Pi-a small, powerful, cost effective and efficient form factor computer: a review. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(12), 720-737.

55. İnternet: Raspberry Pi 4. (2019) Web: https://www.raspberrypi.org/products/raspberry-pi-4-model-b/, Son Erişim Tarihi: 13.06.2021.

56. Maksimović, M., Vujović, V., Davidović, N., Milošević, V., and Perišić, B. (2014). *Raspberry Pi as Internet of things hardware: performances and constraints*. 1st International Conference on Electrical, Electronic and Computing Engineering, 3(8).

57. Chaudhari, H. (2015). Raspberry Pi technology: a review. *International Journal of Innovative and Emerging Research in Engineering*, *2*(3), 83-87.

58. Severance, C. (2013). Eben upton: raspberry pi. *Computer*, 46(10), 14-16.

59. Upton, E., Duntemann, J., Roberts, R., Mamtora, T., and Everard, B. (2016). *Learning computer architecture with Raspberry Pi*. Indianapolis: Wiley, 1-15.

60. Donat, W., & Krause, C. (2014). *Learn Raspberry Pi Programming with Python.* New York: Apress, 1-26.

61. Yiğit, T., Akyıldız, M. A., ve Bay, Ö. (2014). Sızma testleri için bir model ağ üzerinde siber saldırı senaryolarının değerlendirilmesi. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 18(1), 14-21.

62. İnternet: Who is the OWASP Foundation. (2021). Web: https://owasp.org/, Son Erişim Tarihi: 13.06.2021.

63. Aydoğdu, D., ve Gündüz, M. Web Uygulama Güvenliği Açıklıkları ve Güvenlik Çözümleri Üzerine Bir Araştırma. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2(1), 1-7.

64. İnternet: OWASP Embedded Application Security. (2021). Web: https://owasp.org/www-project-embedded-application-security/, Son Erişim Tarihi: 13.06.2021

65. İnternet: The Open Source Security Testing Methodology Manual. (2021). Web: https://www.isecom.org/OSSTMM.3.pdf, Son Erişim Tarihi: 13.06.2021

66. İnternet: Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B. (2021). Web: http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf, Son Erişim Tarihi: 13.06.2021.

67. Rathore, B., Brunner, M., Dilaj, M., Herrera, O., Brunati, P., Subramaniam, R., and Chavan, U. (2006). Information Systems Security Assessment Framework (ISSAF), 15-18.

68. Scarfone, K. A., Souppaya, M. P., Cody, A., and Orebaugh, A. D. (2008). *Technical guide to information security testing and assessment*, 1-80.

69. İnternet: PTES Technical Guidelines. (2012). Web: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines, Son Erişim Tarihi: 13.06.2021.

70. İnternet: Making a LED blink using Raspberry Pi and Python. (2018). Web: https://raspberrypihq.com/making-a-led-blink-using-the-raspberry-pi-and-python/, Son Erişim Tarihi: 13.06.2021.

71. İnternet: Physical Computing with Python. (2021). Web: https://projects.raspberrypi.org/en/projects/physical-computing, Son Erişim Tarihi: 13.06.2021.

72. İnternet: Raspberry Pi 3 ile LED Yakmak. (2017). Web: https://maker.robotistan.com/raspberry-pi-dersleri-4-gpio-ile-led-kontrolu/, Son Erişim Tarihi: 13.06.2021.

73. Kalita, L. (2014). Socket programming. *International Journal of Computer Science and Information Technologies*, *5*(3), 4802-4807.

74. İnternet: Socket Programming. (2010). Web: https://www.ibm.com/docs/en/ssw_ibm_i_71/rzab6/rzab6.pdf, Son Erişim Tarihi: 13.06.2021

75. Arış, A., Oktuğ, S. F., and Yalçın, S. B. Ö. (2015*). Internet-of-things security: Denial of service attacks*. In 2015 23nd Signal Processing and Communications Applications Conference (SIU), 903-906.

76. Gönen, S. (2018). PLC ile Kontrol Edilen Mikro Tip Akıllı Şebeke Sistemlerde Bilgi Güvenliğinin Sağlanması. Doktora Tezi, Gazi Üniversitesi, Ankara.

77. Conti, M., Dragoni, N., and Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3), 2027-2051.

78. Bavithra, R. MITM Attacks through ARP poisoning. *Anatolian Journal of Computer Science*, 4(2), 96-116.

79. Kolli, Y., Mohd, T. K., and Javaid, A. Y. (2018). *Remote desktop backdoor implementation with reverse tcp payload using open source tools for instructional use*. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 444-450.

80. Johnson, A., & Haddad, R. J. (2021, March). Evading Signature-Based Antivirus Software Using Custom Reverse Shell Exploit. In *SoutheastCon*, 1-6.

81. Greavu-Serban, V., and Serban, O. (2014). Social engineering a general approach. *Informatica Economica*, 18(2), 5.



*GAZİ GELECEKTİR...*