T.C.
KTO Karatay Üniversitesi
Fen Bilimleri Enstitüsü

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI TEZLİ YÜKSEK LİSANS PROGRAMI

KURUMLAR İÇİN SİBER GÜVENLİK LABORATUVARI ALTYAPISININ OLUŞTURULMASI

Arif Emre ADIR

KONYA

HAZİRAN 2019

KURUMLAR İÇİN SİBER GÜVENLİK LABORATUVARI ALTYAPISININ OLUŞTURULMASI

Arif Emre ADIR

KTO Karatay Üniversitesi Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Ana Bilim Dalı Yüksek Lisans Programı

Yüksek Lisans Tezi

KONYA

Haziran, 2019

Fen Bilimleri Enstitü Onayı

Prof. Dr. Hüseyin Bekir YILDIZ
Fen Bilimleri Enstitüsü Müdürü

Bu tezli yüksek lisans tezinin yapılması gereken bütün gerekliliklerinin yerine getirdiğini onaylıyorum.

Prof. Dr. Novruz ALLAHVERDİ
Anabilim Dalı Başkanı

Arif Emre ADIR tarafından hazırlanan KURUMLAR İÇİN SİBER GÜVENLİK LABORATUVARI ALTYAPISININ OLUŞTURULMASI başlıklı bu çalışma 01.07.2019 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jüri tarafından tezli yüksek lisans tezi olarak kabul edilmiştir.

Dr. Öğr. Üyesi Ali ÖZTÜRK
Tez Danışmanı

Jüri Üyeleri

Başkan: Prof. Dr. Harun UĞUZ

Üye: Dr. Öğr. Üyesi H. Oktay Altun

Üye: Dr. Öğr. Üyesi Ali Öztürk

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu bildirir aksi bir durumda aleyhime doğabilecek tüm hak ve kayıplarını kabullendiğimi beyan ederim.

10.06.2019

Arif Emre ADIR

ÖZET

KURUMLAR İÇİN SİBER GÜVENLİK LABORATUVARI ALTYAPISININ OLUŞTURULMASI

ADIR, Arif Emre

Yüksek Lisans- Adli Bilişim Mühendisliği Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Ali ÖZTÜRK

Haziran 2019

Bu çalışma, hassas ve gizli verilerin saklandığı ve işlendiği kritik bilişim sistemlerinin maruz kaldığı güncel siber tehditlere karşı yüksek seviyede güvenliğin sağlanabilmesi için ilgili kurumlar tarafından yapılması gerekenleri belirlemektedir. Bu amaçla, Symantec firması tarafından 2017 yılında hazırlanan internet tehditleri raporu, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliği ile gerçekleştirilen siber güvenlik tatbikatları araştırılmıştır. Ayrıca Avrupa Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA) 2018 Tehdit Durum Raporu'nda değerlendirilen 15 siber tehdit türü ile siber güvenliğe ilişkin çok sayıda kaynak incelenmiştir. Sonuç olarak, hassas verilerin saklandığı ve işlendiği kritik sistemlerin siber tehditlere karşı korunması için kurumlara kapsamlı bir siber güvenlik laboratuvarı kurulması tavsiye edilmiştir. Bu laboratuvar, söz konusu sistemler üzerindeki güvenlik açıklıklarının, ağdaki olağan dışı şüpheli davranışların, tehditlerin ve bunların bıraktıkları izlerin çeşitli analiz ve test yöntemleri ile tespit edilmesini ve güvenlik riskini en aza indirgemeyi sağlayacaktır.

Anahtar Kelimeler: Bilgi Güvenliği, Sızma Testleri, Ağ Güvenliği, Siber Güvenlik Laboratuvarı, Adli Bilişim.

ABSTRACT

CYBER SECURITY LABORATORY INFRASTRUCTURE IMPLEMENTATION FOR INSTITUTIONS

ADIR, Arif Emre

M.Sc. Forensic Science Engineering

Asst. Prof. Dr. Ali ÖZTÜRK

June 2019

This work aims to advise the relevant institutions by identifying the necessary efforts to ensure the high level of security against the current cyber threats that critical information systems, where sensitive and confidential data are stored and processed. For this purpose, the internet threat report prepared by Symantec in 2017, the cyber security exercises performed in cooperation with the Scientific and Technological Research Council of Turkey (TUBITAK) and the Information and Communication Technologies Authority (ICTA) have been investigated. Furthermore, the 15 cyber threat types evaluated in the 2018 Threat Status Report of the European Network and Information Security Agency (ENISA), and many resources on cyber security in the literature was investigated. As a result, it was recommended that a cyber security laboratory has to be established in the institutions in order to protect the critical systems where sensitive data is stored and processed against cyber threats. This laboratory will enable the institutions to make comprehensive analysis for detecting security gaps, unusual suspicious behaviors, threats, traces left on the systems by means of various analysis and test methods to minimize security risks.

Keywords: Information Security, Penetration Tests, Network Security, Cyber Security Laboratory, Forensic Informatics.

TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Dr. Öğretim Üyesi Ali ÖZTÜRK'e, araştırma ve yazım süresince yardımlarını esirgemeyen KTO Karatay Üniversitesi Adli Bilişim Mühendisliği Bölümü hocalarıma ve araştırma boyunca manevi desteklerini esirgemeyen eşim Ayşegül ADIR ve çocuklarım Azra ADIR ile Eymen ADIR'a teşekkür ederim.

Arif Emre ADIR

Haziran-2019

İÇİNDEKİLER

ÖZET iii

ABSTRACT iv

TEŞEKKÜR v

İÇİNDEKİLER vi

ÇİZELGELERİN LİSTESİ viii

ŞEKİLLERİN LİSTESİ ix

KISALTMALAR x

1. GİRİŞ 1

2. LİTERATÜR TARAMASI 2

3. GENEL BİLGİLER 5

3.1. Siber Kavramlar 5

3.2. Bilişim Kavramları 8

3.3. Web Kavramları 9

4. SİBER TEHDİTLER 12

4.1. Siber Tehditlerin Amaçları 12

4.2. Tehditlerin Hedefindeki Değerler 13

4.3. Tehditlerin Etkilediği Sistemler 13

4.4. Tehditlerin Özellikleri 13

4.5. Tehdidin Tarafları 14

4.6. Siber Tehdit Türleri 18

4.7. Siber Saldırılara Karşı Mevcut Durum 37

4.8. Türkiye'de Siber Güvenlik Çalışmaları 38

4.9. Kurumlarımızda Sınır Güvenliği Sistemleri 41

4.10.Zafiyet Analizi ve Sızma Testleri 44

4.11.Bilişim Suçlarının Tespiti ve Dijital Delillerin İncelenmesi 48

5. LABORATUVAR ALTYAPISININ OLUŞTURULMASI 50

5.1. Adli Bilişim Araçları (Forensics Tools) 52

5.2. Sızma Testi Laboratuvarı 60

6. SONUÇLAR VE TARTIŞMA 72

KAYNAKLAR 79

ÖZGEÇMİŞ 86

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 4.1 Trustwave Global Security Raporu - Kimlik avı saldırısı temaları 30
Çizelge 4.2 Tehditlerin hedefindeki değerler 38
Çizelge 4.3 Kuruluşlara yönelik en büyük on (10) siber tehdit 38
Çizelge 5.1 Adli Bilişim Araçları 59
Çizelge 5.2 Sızma Testi Araçları 70

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 4.1 Botnet Necus virüsüne ait spam aktiviteleri 32

KISALTMALAR

Kısaltmalar	Açıklamalar
ABD	Amerika Birleşik Devletleri (USA)
API	Uygulama Programlama Arayüzü (Application Programming Interface)
ASP	Aktif Sunucusu Sayfaları (Active Server Pages)
ACK	Onay Mesajı (Acknowledge)
ARPA	Gelişmiş Araştırma Projeleri Dairesi (Advanced Research Project Agency)
BT	Bilişim Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
BGYS	Bilgi Güvenliği Yönetim Sistemi
CMS	İçerik Yönetim Sistemi (Content Management System)
CPU	Merkezi İşlem Birimi (Central Processing Unit)
CORS	Sürekli Çalışan Referans İstasyonları (Continuously Operating GPS Reference Stations)
COBIT	Bilgi ve İlgili Teknoloji İçin Kontrol Hedefleri (Control Objectives for Information and Related Technology)
CSS	Basamaklanmış Stil Katmanları (Cascading Style Sheets)
CVE	Bilinen Güvenlik Zafiyetleri (Common Vulnerabilities and Exposures)
DDOS	Dağıtılmış Hizmet Reddi Saldırıları (Distrubuted Denial of Service Attack)
DOM	Belge Nesnesi Modeli (Document Object Model)
DTD	Belge Türü Tanımı (Document Type Definition)
DoS	Hizmet Reddi Saldırıları (Denial of Service)
FBI	Federal Araştırma Bürosu (Federal Bureau of Investigation)
FTP	Dosya Aktarım Protokolü (File Transfer Protocol)
GWT	Google Web Araç Takımı (Google Web Toolkit)
HTTP	Hipermetin Aktarma İletişim Protokolü (Hypertext Transfer Protocol)
HTML	Hypertext Markup Language, Hipermetin İsaret Dili
ICMP	Internet Control Message Protokol (Ġnternet Mesaj Kontrol Protokolü)
IDPS	Saldırı Tespit ve Önleme Sistemleri (Intrusion Detection and Prevention Systems)
IEC	Uluslararası Elektroteknik Komisyonu (International Electrotechnical Organization)
IP	İnternet Protokolü (Internet Protocol)
IPS	Saldırı Önleme Sistemi (Intrusion Prevention System)
ISO	Uluslararası Standartlar Teşkilatı (International Organization for Standardization)
ITU	Uluslarası Telekomünikasyon Birliği (International Telecommunication Union)

ITU-T	Uluslarası Telekomünikasyon Birliği Standardizasyon Sektörü (International Telecommunication Union Standardization Sector)
IDS	Saldırı Tespit Sistemi (Intrusion Detection System)
ISSAF	Bilgi Sistemleri Güvenlik Değerlendirme Sistemi (Information Systems Security Assessment Framework)
JWT	JSON Web JSON Özellikleri (JSON Web Tokens)
LDAP	Kolay Dizin Erişim Protokolü (Lightweight Directory Access Protocol)
loT	Nesnelerin İnterneti (Internet of Things)
MTU	Maksimum Transfer Ünitesi (Maximum Transfer Unit)
NIST	National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
NSS	Ağ Simülasyon Sistemi (Network Simulation System)
ORM	Nesne-İlişkisel Haritalama (Object Relational Mapping)
OOP	Nesneye Dayalı Programlama (Object - Oriented Programming)
OSSTMM	Açık Kaynak Kodlu Güvenlik Test Metodolojisi El Kitabı (The Open Source Security Testing Methodology Manual)
OWASP	Açık Web Uygulaması Güvenliği Projesi (Open Web Application Security Project)
PHP	Hipermetin Ön İşlemcisi (Hypertext Preprocessor)
PIM	Ayrıcalıklı Kimlik Yöntemi (Privileged Identity Management)
PPTP	Noktadan Noktaya Tünel Protokolü (Point-to-Point Tunneling Protocol)
SQL	Yapısal Sorgulama Dili (Structured Query Language)
SAST	Statik Uygulama Güvenliği Testi (Static Application Security Testing)
SFP	Takılabilir küçük form faktörü (Small Form-factor Pluggable)
SOP	Aynı Kök Politikası (Same Origin Policy)
SSD	Katı Hal Sürücüsü (Solid-State Drive)
SSL	Güvenli Soket Katmanı (Secure Socket Layer)
SSTP	Güvenli Yuva Tünel Protokolü (Secure Socket Tunneling Protocol)
SSO	Tek Oturum Açma (Single Sign On)
SOAP	Basit Nesne Erişim Protokolü (Simple Object Access Protocol)
SOC	Güvenlik Operasyon Merkezi (Security Operation Center)
SYN	Senkronizasyon (Syncronization)
TTL	Yaşam Süresi (Time to Live)
TSE	Türk Standartları Enstitüsü
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TLS	Taşıma Katmanı Güvenliği (Transport Layer Security)
TCP	İletişim Protokolü (Transmission Control Protocol)
UDP	Kullanıcı Veribloğu İletişim Kuralları (User Datagram Protocol)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
UTM	Birleşik Tehdit Yönetimi (Unified Threat Managament)
URL	Tekdüzen Kaynak Bulucu (Uniform Resource Locator)
USB	Evrensel Seri Veriyolu (Universal Serial Bus)
VPN	Sanal Özel Ağ (Virtual Private Network)

WASC	Web Uygulaması Güvenlik Konsorsiyumu (Western Association of Schools and Colleges)
WAF	Web Uygulaması Güvenlik Duvarı (Web Application Firewall)
WHID	Web Hacking Olayları Veritabanı (Web Hacking Incidents Database Project)
XEE	XML Dış Varlıklar (XML External Entities)
XML	Genişletilebilir İşaretleme Dili (Extensible Markup Language)
XHTML	Genişletilebilir Büyütülmüş Metin İşaretleme Dili (Extensible Hypertext Markup Language)
XSS	Siteler Arası Betik Çalıştırma (Cross Site Script)

1. GİRİŞ

Tüm dünyada siber güvenliğin önemi her geçen gün daha fazla artmakta, ulusal güvenliğin en yeni sorunu olarak gündemde yerini almıştır. Uluslararası platformlarda bilgi ve iletişim teknolojileri casusluk, saldırı ve savunma aracı olarak kullanılmaya başladı. Siber güvenlik, şirketler, organizasyonlar ve hükümetler için önemli konu haline gelmiştir. Hassas ve gizli verilerin saklandığı ve işlendiği kritik sistemler üzerindeki zafiyetlerin, yeni güvenlik açıklıklarının, hukuki boşlukların keşfedilmesi ve bu açıklıkların içeriden veya dışarıdan birtakım saldırgan kişi veya gruplar tarafından istismar edilmesi, kurumları ve şirketleri maddi, manevi, güven ve itibar kaybına maruz bırakmaktadır.

Hassas ve gizli verilerin saklandığı ve işlendiği kritik bilişim sistemlerinin, maruz kaldığı siber tehditlere karşı yüksek seviyede güvenliğin sağlanmasına yönelik yapılan çalışma kapsamında, literatür taramasının ardından üçüncü bölümde; siber güvenlik terimlerinin tanıtılması, dördüncü bölümde; siber tehditler, beşinci bölümde; laboratuvar altyapısının oluşturulması ve tasarlanması, altıncı bölümde konuya ilişkin olarak görüş ve tavsiyeler belirtilmiştir.

Bu tez çalışmasında, kurumların bilişim alt yapıları ve sistemleri üzerindeki güvenlik açıklarını olası saldırılardan önce tespit ve analiz etmeleri ve karşılaştıkları bir bilişim olayı sonrasında her türlü delili toplayarak analiz etmeleri ve ilgili makamlara rapor olarak sunmaları için kendi organizasyonları içerisinde siber güvenlik laboratuvarı altyapılarını oluşturmaları tavsiye edilmiş ve rehber niteliğinde bir kaynak hazırlanmıştır.

2. LİTERATÜR TARAMASI

Eric Francis Dazet çalışmasında otomatik sızma test araçlarının manuel testler kadar esnek olmadığını, bazı güvenlik açıklıklarını tespit edemediğini ve bu nedenle otomatik sızma araçlarının geliştirilmesi gerektiğini ifade etmiştir. Çalışmasındaki temel amaç, az kullanıcı ile etkili bir güvenlik değerlendirme çözümü sunarak açık kaynak kodlu programlara dayalı otomatik araçların kullanılmasını önermektir. Bunun için otomatik sızma testi aracı olan ANEX aracı ile bir bilgisayardan diğer hedef bilgisayara şebeke sömürüsü haritasını sunmuştur [1].

Romuald Thion çalışmasında; sızma testi ve izinsiz giriş tespit tekniklerinin güvenlik değerlendirmesinde önemli olduğunu vurgulayarak ağ tabanlı bilgi toplama işlemleri gerçekleştirmiştir [2].

M. Alparslan Akyıldız tarafından yapılan çalışmada; zafiyet taraması ve sızma testi araçları, Linux komutları, Linux işletim sistemi üzerinde çalışan servisler ve uygulama laboratuvarı altyapısının oluşturulması konularında gerçek uygulamalar üzerinde çeşitli bilgiler verilmiştir [3].

Benjamin Livshits tarafından yapılan doktora tez çalışmasında; web güvenlik açıklıklarının giderilmesinde çalışma süresi bir alternatif çözüm olarak tanımlanmıştır. Web tabanlı Java uygulamaları üzerinde çalışma gerçekleştirilmiştir. Kod denetim araçları ve Java dili ile derlenen kodlar denetlenmiş ve raporlanmıştır. Çalışmada on bir (11) ayrı test uygulaması gerçekleştirilerek doksan sekiz (98) güvenlik zafiyeti tespit edilmiş ve bulunan zafiyetler üzerinde tartışılmıştır [4].

Gürol Canbek ve Şeref Sağıroğlu tarafından yapılan çalışmada; bilgisayarlara yapılan saldırılar incelenmiş, saldırı ile saldırgan arasındaki bağ değerlendirilmiş, saldırganların ortak karakteristik özelikleri belirlenmiş, meydana gelmiş saldırıların gelişimi araştırılmış ve temel saldırı türleri gözden geçirilerek saldırılarda kullanılan yöntem, metodoloji ve zafiyetlerin giderilmesinde saldırgan profilinin de mutlaka dikkate alınmasının faydalı olacağı değerlendirilmiştir [5].

Adem Tekerek ve arkadaşları tarafından yapılan çalışmada; imza ve anormal tabanlı denetimlerle web tabanlı tehditleri engellemek için yeni bir hibrit modeli önerilmiştir. Bazı tehditlerin imza tabanlı denetimlerinde alfa numerik karakter, harf frekans ve istek uzunluğu öznitelikleri kullanılarak bayes sınıflandırma algoritması ile anormal tabanlı denetim yapılmıştır. Anormal tabanlı denetim sonucu tespit edilen anormal istekler ve imza tabanlı denetim listesi güncellenerek sistem yeni saldırılara karşı dayanıklı hale getirilmiştir. Bu çalışmada önerilen model, örnek web uygulaması veri kümesi, CSIC 2010 ve ECML-PKDD 2007 veri kümeleri kullanılarak test edilmiştir. Test sonuçları benzer fakat farklı çalışmalar ile karşılaştırılmıştır. Karşılaştırma sonucuna göre önerilen modelin mevcut çalışmalara göre daha yüksek denetim performansı gösterdiği ve düşük yanlış-pozitif oranına sahip olduğu görülmüştür [6].

Tuncay Yiğit ve Muhammed Alparslan Akyıldız tarafından yapılan çalışmada; gerekli servis ve sunucu kurulumları tamamlanarak sunucu sanallaştırmaları ve ağ kurulumları yapılmış ve bir model ağ üzerinde saldırı senaryoları değerlendirilerek sızma testlerinin önemi vurgulanmıştır [7].

Yılmaz Vural tarafından yapılan çalışmada; bilgi güvenliği için risk teşkil eden tehditler incelenmiş, web ortamlarında büyük tehdit oluşturan SQL enjeksiyon açıklıkları, sızma testleri genel olarak gözden geçirilmiş ve alınması gereken önlemler sunulmuştur. Bilgi güvenliğini sağlamaya yönelik gerçekleştirilen sızma testlerinin insan faktörü ve teknoloji üzerindeki etkisi araştırılmış, çözüm önerileri sunulmuştur [8].

Birhanu Eshete ve arkadaşları tarafından yapılan çalışmada; web alanındaki en tehlikeli tehdidin zararlı web sayfalarının olduğu, mevcut tekniklerin belirli saldırılara odaklandığı ve saldırganların harmanlanmış teknikleri kullandıkları ifade edilmiştir.

Statik analiz ve minimalist kombinasyonunu kullanan Binspect isimli deneysel değerlendirme işlemi ile denetimli öğrenme tekniklerini kullanarak düşük yanlış sinyallerle iyi ve zararlı web sayfalarını ayırt ederken %97 oranında doğruluk elde ettiler. 3-5 saniye aralığında tek bir web sayfasını analiz etmiştir [9].

Hwee-Joo Kam ve Joshua J. Pauli tarafından yapılan çalışmada; öğrencilerin saldırı tekniklerini öğrenerek sistemleri saldırgan bakış açısı ile savunabilecekleri ifade edilmiştir. Ayrıca web uygulama güvenliğine ilişkin güvenli kod geliştirme eğitimlerinin dışında sızma testi eğitimlerinin de verilmesinin önemli olduğu belirtilmiştir [10].

3. GENEL BİLGİLER

3.1. Siber Kavramlar

Siber**,** oluşturulan, depolanan ve paylaşılan sayısallaştırılmış verilerden oluşan bir bilgi ortamıdır. Siber kelimesi tüm dijital ağları kapsayan geniş bir terimdir. "Siber" kelimesi İngilizce "Cyber" kelimesinden uyarlanıp kullanılmaya başlayan bir kelime olup "Bilgisayar ağlarına ait olan", "İnternete ait olan", "Sanal gerçeklik" manalarına gelmektedir. İnternet ile ilgili her şey siber kategorisine girer [11].

Siber uzay, 2016-2019 Ulusal Siber Stratejisi dokümanında bütün dünyaya ve uzaya yayılmış durumda olan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamı ifade eder.

Siber varlık, siber ortamda bulunan her türlü bilgi, araç, doküman, yazılım, donanım, sunucu, Veritabanı veya internete bağlı sistemlerin her biri siber ortamdaki varlıklardır.

Siber risk, tehditlerin bir veya birden çok bilgi varlığındaki açıklığı kullanarak zarar yaratma potansiyelini ifade eder. Risk kelime anlamı olarak tehlikeli bir olayın gerçekleşme olasılığıdır.

Siber tehditler, belirli bir amaç doğrultusunda bilgisayar ağ yapıları kullanılarak bilişim sistemlerine yönelik gerçekleştirilen saldırılardır. Tehdit kavramı bilgi güvenliğini oluşturan gizlilik, bütünlük ve erişebilirlik özelliklerinden bir veya birkaçını sistem zafiyetlerinden faydalanarak bozma olasılığı bulunan etken olarak ifade edilmiştir [12].

Siber olay, siber ortamda bulunan yazılım, donanım, sistem, cihaz gibi her türlü varlığın zarar gördüğü, etkilendiği durumdur. Siber Olaylara Müdahale Ekiplerinin (SOME) kuruluş, görev ve çalışmalarına ilişkin usul ve esasları hakkındaki tebliğde Siber Olay: “Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını” ifade eder şeklinde tanımlanmıştır [13].

Siber savaş, devletlerin rakibi ve düşmanı oldukları gizli bilgi ve teknolojilerini çalmak için yaptıkları saldırı ve girişimleri ifade eder. Son yıllarda ülkeler siber ortamda başka devletlere ait hizmetlerini durdurmak, varlıklarına zarar vermek, yok etmek veya menfaatleri doğrultusunda kullanmak üzere operasyon düzenlemektedirler. Siber savaş, Birleşmiş Milletler Terim sözlüğünde, bilgi savaşı ile birlikte aynı anlamda tanımlanmıştır ve bu tanıma göre; ”Bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etmek maksadı ile kullanıldığı savaş tipidir” şeklinde ifade edilmiştir [14]. Bir başka sözlük tanımında ise siber savaş; ”Askeri veya politik amaçlara ulaşmak için bilgisayar teknolojisinin bir ülke tarafından diğerine karşı kullanılması” olarak tanımlanmıştır [15].

Siber terörizm, siyasi ve sosyal kurum ve kişilere gözdağı vermek, baskı oluşturmak amacıyla içeriden veya dışarıdan devletin kritik altyapılarına, güvenlik birimlerine ve hükümet temsilciliklerine yönelik gerçekleştirilen saldırılardır. Siber terörizm eylemleri, devletlerin kritik altyapılarını, bilgisayar ağlarını, sunucu ve bilgisayarlarını hedef alan hukuki olmayan eylemlerdir. Bu eylemlerin amacı istihbarı bilgi toplamak, ekonomik nedenler, haksız rekabet, sosyal, dinsel, ekonomik ve kültürel yönden psikolojik çöküntü yaratmak, düşmanı zayıflatmak, casusluk faaliyetlerinde bulunmak, ego tatmini, güç ve gövde gösterisi gibi nedenlerdir. FBI; siber terörizmi, “planlı ve politik amaçlara hizmet etmek amacıyla planlı olarak kimliği belirsiz kişiler tarafından gerçekleştirilen, barışçıl kişileri hedef alan, verilere, bilgisayar sistemlerine, bilgisayar programlarına ve platformlara yapılan saldırılar” olarak tanımlamaktadır [16]. Son yıllarda özellikle enerji (elektrik, su, doğalgaz ve petrol vb.) sektörlerinin modern bilgi teknolojileri daha fazla kullanması nedeni ile terörist ve terörist gruplarının hedefi haline dönüşmüştür. Saldırı sonrasında ağ sistemleri çalışamaz hale getirilmekte, sır niteliği taşıyan gizli bilgiler çalınarak fikri mülkiyet hakları çiğnenmekte ve devletlerin kritik altyapıları büyük zarar görmektedir [17]. Dolayısıyla kritik altyapı sistemlerine yönelik güvenliğin sağlanması devletler için çok önemli bir hale gelmiştir. Bu sistemlere yönelik saldırılar sonrasında büyük can ve mal kayıpları yaşanabilir, kamu düzeninin bozulmasına neden olabilecek büyük problemler meydana gelebilir.

Siber silah, dijital ortamda kişisel veya ulusal maksatlarla, hırsızlık, istihbarat, casusluk, saldırı ve savunma için kullanılan yazılım ve araçlar olarak ifade edebiliriz. Silah karşınızdakine zarar vermek veya korunmak için kullanılır. Siber savaşlarda kullanılan en büyük güç olan silah bilgidir. Bilgiyi elde etmek için kullanılan silahlara zararlı yazılımlar (Virüsler, Solucanlar, Truva atı, Mantık Bombası, Arka Kapı), hizmet dışı bırakma saldırıları, sosyal mühendislik saldırıları, yapay zekâ, arama motorları birkaç örnek olarak verilebilir.

Siber Casusluk, ticari, politik ve askeri kazanç elde etme düşüncesi olan yetkisiz kişilerce rakip devletlerin sistemlerine sızılması, gizli sır bilgi ve düşüncelerin çalınması için yürütülen faaliyetlerin tümü olarak tanımlanabilir. 5237 sayılı Türk Ceza Kanunu'nda (TCK) devletin güvenliği veya iç ve dış siyasal yararları bakımından gizli kalan bilgileri askeri veya siyasi amaçlarla elde eden kimselerin casusluk suçunu işledikleri ve cezalandırılacakları belirtilmektedir. Merriam-Webster'a göre, casusluk "özellikle yabancı bir hükümetin veya rakip bir şirketin planları ve faaliyetleri hakkında bilgi edinmek için casusluk veya casusluk uygulaması" şeklinde ifade edilmiştir [18].

Symantec tarafından hazırlanan İnternet Güvenliği Tehdit Raporu'nda, Regin ve Turla isimli iki farklı casus yazılım türünü ortaya çıkarılarak, bu yazılımların uzaktan ekran görüntüsü alma, takip, dosya atma veya silme vb. gibi işlemler yapabildiğini belirtilmiştir [19]. Siber istihbarat faaliyetleri bilgi edinmenin dışında devletlerin e-devlet altyapılarının hizmet dışı bırakılması, web sitelerine erişimin engellenmesi, ekonomik zarar vermek amacı ile yapılabilmektedir [20]. Bu tanımlamalar ışığında siber casusluğu, kişi ve devletler hedef devletlerin niteliği itibari ile gizli bilgilerini casusluk amacı ile siber silahları kullanarak çalması veya ekonomik kazanç elde etmek düşüncesi ile siber silahlar kullanarak diğer devletlere karşı zarar verici hareketleri olarak ifade edebiliriz.

Siber suç, bilgisayar ve ağ ile ilgili suç eylemlerini kapsar. Ayrıca siber suç, internet üzerinden yürütülen nefret suçlarını, telefonla pazarlama ve internet sahtekârlığını, kimlik hırsızlığı ve kredi kartı hesap hırsızlığını, yasadışı faaliyetlerin bilgisayar veya internet yoluyla yapılmasını kapsamaktadır [11].

Siber güvenlik, kişisel bilgilerin, kritik altyapı ve bilgi sistemlerinin saldırı ve tehditlere karşı korunması anlamına gelir [21]. Siber güvenlik, bilişim sistemlerinin ve işlenen bilgilerin gizlilik, bütünlük veya erişebilirliğinin güvence altına alınması, siber saldırıların tespit edilmesi ve bu tespitlere karşı tepki mekanizmalarının devreye alınması olarak da ifade edilmektedir. Siber âlemde kurum kuruluş ve kullanıcıların mağduriyetini, imajını, özel gizli bilgilerin çalınmasını, ele geçirilmesini veya saldırıya uğramasını korumak için kullanılan güvenlik prosedürleri, risk analizleri, kontrol mekanizmaları, fiziksel ve çevresel güvenlik vb. uygulamaların tamamıdır [22].

Zafiyet, yazılım veya donanımda, programlama hatası nedeniyle bulunan ve bilgisayarın kötü niyetli kişiler tarafından kullanılmasına sebep olan hatalardır. Açıklıklar, kötü niyetli kişiler tarafından bilgi sistemlerinde bulunan bilgileri silmek, çalmak, değiştirmek veya diğer sistemlere saldırı düzenlemek amacıyla istismar edilmektedir.

Metasploit, sistemlerde bulunan açıklıkların tespit edilmesi ve ispatlanması için yazılmış programlardır. Zafiyetlerden yararlanılarak hedef sistemler üzerinde yetki yükseltme, yetkisiz erişim elde etme, hizmet dışı bırakma gibi eylemler için kullanılan betiklere istismar kodu (exploit) denir.

3.2. Bilişim Kavramları

Bilişim, insanların; teknik, finans ve toplumsal alanlardaki iletişimlerinde kullandıkları, bilginin, dijital cihazlar aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimidir.

Adli bilişim, adli vakaların belirlenmesi ve ortaya çıkarılması için, olay mahallinden, dijital veri saklama ve iletme özelliğine sahip cihazların toplanması, cihazlarda bulunan elektronik delillerin tespit edilmesi ve adli mercilere dijital delillerin raporlanması süreci içerisinde gerçekleştirilen faaliyetlerin tamamıdır.

Dijital delil, bilişim teknolojilerinin veya veri kaydetme özelliğine sahip elektronik cihazlarda bulunan ve suçun aydınlatılmasında önemli rol oynayacak verilere verilen genel isimdir.

Bilişim sistemleri, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda; "Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemleri" olarak tanımlanmıştır.

Kamu bilişim sistemleri, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda; "Türkiye Cumhuriyeti kamu kurum ve kuruluşlarına ait olan veya işletilen bilişim sistemleri" olarak ifade edilmiştir.

Kritik altyapılar, toplumsal ve kamusal düzenin sağlıklı, sürdürülebilir bir şekilde işlemesi için gerekli devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri kritik altyapıların en başta gelen kritik altyapılar olarak sıralanabilir.

3.3. Web Kavramları

Web uygulaması, internet ağı ile ulaşılabilen kullanıcı etkileşimli veya veriye dayalı web tabanlı yazılımlardır. Web uygulamaları herhangi bir program kurma ve yükleme işlemi yapmadan kullanılabilmektedir. Web uygulamaları sunucu, orta ve arka uç katman olmak üzere üç (3) farklı katmandan oluşur. Son kullanıcıların bulunduğu taraf istemci tarafını, uygulamaların barındığı web sunucuları sunucu tarafını, uygulama sunucularının bulunduğu orta katmanı, veri tabanının olduğu katmanda arka uç katmanı ifade eder.

HTML, internet dokümanlarını oluşturmaya yarayan bir dildir**.** Fakat programlama dili değil, internet sayfasının kullanıcıya nasıl gösterilmesi gerektiğini belirlemek, web sayfaları oluşturmak için kullanılan bir işaretleme dilidir. HTML belgelerindeki tag'lar (HTML kodları) "<" ve ">" işaretleri arasına yazılırlar. Yeni bir tag başlatacağımızda

kodunuzu <...> işaretleri arasına yazarız ve kodun kullanımını bitirmek istediğimiz zaman da </...> şeklinde kodumuzu sonlandırırız. Web tarayıcılarının yazı, link ve görsel verilerini sunması ve bunların ilişkilerini sağlaması için kullanılır. Html'in yapısı aşağıdaki şekilde görüldüğü gibidir.

İnternet üzerinde bilgi erişimi için "www" kullanılır. İnternet üzerinde yayınlanan birbirleriyle bağlantılı üst metin (hypertext) dokümanlarından oluşan bir bilgi sistemidir. Bu dokümanlara web sayfası adı verilir ve bu sayfalara web tarayıcısı aracılığıyla erişilir.

URL, Türkçe 'de "Standart Kaynak Bulucu" anlamına gelir. İnternet dünyasında bir kaynağa rastgelen standart bir formata uygun bir karakter tertibidir. Webde bulunan dokümanlara ve diğer kaynaklara ulaşılmasını sağlayan adresleme standardıdır. URL'ler, bilgisayarların sunucularla iletişim kurabilmek için kullandıkları sayıları (IP adreslerini) değiştirir ve kullanıcıların okuyabilmesi için birer metin haline getirir. Bileşenleri arasında protokol, alan adı, domain uzantısı, ülke uzantısı ve dosya uzantısı yer alır.

Http, web üzerinde dokümanları transfer etmek için kullanılan bir protokoldür. http ve tcp bağlantıları üzerinde çalışmaktadır. İstek ve yanıt (request ve response) şeklinde iki çeşit http mesaj içeriği bulunmaktadır. Get metodu, sunucuya, istek yapılan url kısmındaki veriyi yorumlaması için gönderilen anahtar kelimedir. Get metodunu gören sunucu, gerçekleştireceği işlemlerde parametre olarak kabul edeceği verileri url'den gelenler olarak bilir. Post, sunucuya yapılan isteğin gövde (body) kısmında bulunan veriyi yorumlaması için gönderilen metottur. Get isteği, sunucudan bir veri almak istendiğinde kullanılır, Post ise sunucuya veri göndererek bu verilerle bir dosya yaratmak için kullanılır. Get metodunda alınan parametreler ve içlerindeki bilgiler adres satırında görülür, yapılan işlemlere doğrudan erişilebilir aksine Post metodunda ise bilgiler adres satırında görülmediği gibi yapılan işlemlere de direk erişilemez. Kısacası veri, get metodu ile url içinde, post metodu ile ise sadece http isteği içinde gider. Proxy, istemci ile sunucu arasına giren uygulamalardır. Bunlardan http vekilleri, tarayıcı ile sunucu arasına girecek olan uygulamalardır. Kullanıcı bir ağa erişmek istediğinde Proxy kullanırsa vekil sunucuya bağlanır. Proxy öncelikle isteği

alır ve ilgili sayfaya bağlanır, içeriği alır. Daha sonra bu içeriği tarayıcıya gönderir. Kullanıcılar bir web sitesine erişeceklerinde bağlantıyı kullanıcıların yerine Proxy kurar.

JWT, taraflar arasında güvenli bir şekilde veri transferi için kendisine göre bir yol tanımlayan açık standarttır ve bu veriler dijital olarak imzalandığı için doğrulanabilir ve güvenilirdir [10]. .Haberleşen iki veya daha fazla sistem arasında kullanıcı doğrulama, kullanıcı tanıma, veri bütünlüğü ve bilgi güvenliğini koruma gibi noktalarda kullanılmaktadır.

SOP, tarayıcılarda Ajax istekleri, cookie yönetimi vs. birçok uygulamada kullanılan bir güvenlik mekanizmasıdır ve kaynakların aynı olması gerekir bunun için de protokol, domain, port bilgilerinin de aynı olması gerekir [8]. Örneğin, kullanıcı bir kez giriş yaptıktan sonra yapılan her istek bu standardı içerecek ve kullanıcının izin verilen servis ve kaynaklara erişimi sağlanacaktır. İmza işlemi imza başlığı ve yüklü olan bilgi kullanılarak hesaplandığı için içeriğin değişmediği de doğrulanabilir. Bu standart başlık, taşıma kapasitesi ve imza olmak üzere birbirinden nokta (.) ile ayrılmış üç (3) farklı bölümden oluşur. Bu standardın JSON kullanması, URL üzerinde taşınabilmesi, web çerezleri kullanma zorunluluğu olmaması, hızlı doğrulama yapabilmesi ve veri bütünlüğünü sağlaması gibi avantajları yönleri vardır.

ORM, nesne kodunu ilişkisel bir veritabanına bağlamak için kullanılan bir programlama tekniğidir ve nesne kodu, Java veya C# gibi nesne yönelimli programlama dillerinde yazılmıştır [12].

DOM, html, genişletilebilir köprü metni biçimlendirme dili olan XHTML ve genişletilebilir işaretleme dili olan XML gibi belgelerin diğer programlama dilleri ve programlama dilleriyle iletişim kurabilmesini sağlamak için geliştirilmiş bir arabirimdir [12]. Captcha, Carnegie Mellon Bilgisayar Bilimleri Okulu tarafından geliştirilen bir projedir. Form girişinin otomatize araçlar tarafından yapılmasını engellemek için sunucu tarafında rastgele üretilen ve resim içerisine gömülen karakterlerin forma giriş yapan kullanıcılar tarafından algılanıp tekrar sunucuya gönderilmesinden oluşan yöntemdir.

4. SİBER TEHDİTLER

Tehdit, sistem açıklıklarının istismar edilerek sistem üzerindeki bilgi varlıkları açıklıklarını kullanarak varlığa kısmen veya tamamen zarar veren unsurlara tehdit denilmektedir. Teknolojinin gelişimine paralel olarak tehditlerin hacmi, şiddeti ve karmaşıklığı gün geçtikçe artmaktadır. Önceleri bilgi kâğıt üzerinde klasörlerde saklanırken bugün elektronik ortamlarda muhafaza edilmektedir. Dolayısıyla saldırgan gruplarda bu alanlara yönelmişlerdir. Saldırganlar kötü niyetli eylemlerini gerçekleştirebilmek için bilişim sistemlerini hukuka aykırı olarak kullanırlar.

4.1. Siber Tehditlerin Amaçları

Kurumların, devletlerin ve kişilerin hassas verilerini yasal olmayan yollarla ele geçirmek, çalmak, başkaları ile paylaşmak veya yok etmek, bu verilerin saklandığı ve işlendiği sistemleri çalışamaz hale getirmek siber tehditlerin birincil amaçları arasında yer almaktadır.

Sisteme erişim yetkisi olmayan kişiler firewall, IPS, IDS vb. gibi saldırı engelleme sistemlerini kırma, bu sistemler üzerindeki güvenlik açıklıklarını istismar etme veya şifre, parola gibi sisteme giriş parametrelerini ve kullanıcı hesaplarını ele geçirerek sisteme izinsiz erişim sağlama gibi eylemleri bulunurlar. Bu eylem türü, Türk Ceza Kanunu'nun Bilişim Alanında Suçlar kısmında 243. Madde ile: "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimse cezalandırılır" şeklinde suç olarak tanımlanmıştır. Saldırganlar bilgilere zarar verme girişimlerinin dışında, hedef sisteme kaldıramayacağı kadar çok istek göndererek hizmet veremez ve çalışamaz hale getirirler. Sistemin işlemesinin engellenmesi sistemin somut unsurlarına yönelik eylemlerle yapılabileceği gibi, sisteme zararlı bir yazılımın bulaştırılması veya farklı bir şifrenin sisteme yerleştirilmesi gibi eylemlerle de yapılabilir [23]. Hizmetin engellenmesi, verilerin ele geçirilmesi, değiştirilmesi, ifşa edilmesi veya yok edilmesi Türk Ceza Kanunu'nun Bilişim Alanında Suçlar kısmında 244. Madde ile suç olarak tanımlanmıştır. Kredi ve banka kartlarının kötüye kullanılması, zararlı yazılım ve yasak cihazların kullanılması da bilişim suçları başlığı altında düzenlenmiştir. Ayrıca Bilişim Suçları başlığı altında olmayan bilişim sistemlerinin araç olarak kullanılması ile dolandırıcılık, müstehcenlik,

hakaret, cinsel taciz, tehdit ve şantaj suçu, yasa dışı yayın, yasa dışı ürünlerin satılması, fikri mülkiyet ihlali, özel hayatın gizliliğini ve haberleşmenin gizliliğini ihlal suçları düzenlenmiştir. Bu suçlar genel olarak internet yoluyla ve sosyal medya yoluyla işlenmektedir.

Bilgi ifşası kapsamına girebilecek eylemlere; kurumun varlıklarını çalmak, rüşvet vermek veya almak, kuruma ait kritik ve gizli bilgileri şahsi çıkar sağlamak maksadıyla kurum dışına çıkartmak, kara para aklamak, denetim konusunda ihmali davranmak, kaynakları boşa harcamak ve kişisel çıkarları için bulunduğu pozisyonu kullanmak vb. gibi unsurlar örnek olarak verilebilir[24].

4.2. Tehditlerin Hedefindeki Değerler

Kurum kimliği, güvenilirliği, sahip olduğu hassas ve gizli bilgileri, politika ve iş devamlılığını sağlayan süreçleri, üçüncü kişiler tarafından emanet edilen bilgileri, adli ve ticari sırları saldırıların hedefindeki değerlerdir. Bu değerlerin istismar edilmesi ile kişisel veya kurumsal imaj kaybı, mahremiyet, rekabet ortamı, kaynakların tüketimi, kamu güvenliği ve düzeni, ülke ekonomisi olumsuz yönde etkilenecektir.

4.3. Tehditlerin Etkilediği Sistemler

Tehditler, kuruma ait gizli ve hassas bilgilerin ifşa edilmesine, yazılım, servis ve sistemlerin çalışamaz hale gelmesine, rekabetin ve politik gücün zayıflamasına [25], kişiler nezdinde güven ve itibar kaybı gibi birçok maddi ve manevi kayıpların oluşmasına neden olur.

Bilgi sistemlerine ve kritik altyapılara yönelik olası bir saldırı, ülkelerin devlete ait önem arz eden tüm bilgilerin saklandığı sunucuları, nükleer tesisleri, enerji hatlarını, elektronik hizmetleri, sinyalizasyon ve uydu sistemlerini, su, sağlık, ulaşım, bankacılık ve finans, baraj sistemleri ve benzeri her türlü internet hizmetlerine zarar verebilir.

4.4. Tehditlerin Özellikleri

Daha önceki tarihlerde ülkeler arası savaşlar cephede ve meydanlarda gerçekleşirken, teknolojinin gelişimi ile savaş metotları da değişmiştir. İnternet teknolojileri üzerinden psikolojik savaş, algı operasyonları, yönlendirmeler profesyonel olarak

uygulanmaktadır. Tehditler özellikle kamu hizmeti veren kuruluşların web sitelerine, veritabanı ve kritik altyapılarına yönelik gerçekleşmektedir. Birtakım aktörler rakibi ve düşmanı oldukları devletler, şirketler veya kişiler hakkında siyasi, ekonomik, bilimsel, teknolojik, coğrafi ve askeri bilgiler elde edebilmek, bu devletlerin hizmetlerini kesintiye uğratmak, milli savunma ve güvenliğine zarar vermek, ekonomik kazanç elde etmek vb. gibi amaçlarla kritik sistemlerine saldırırlar.

4.5. Tehdidin Tarafları

Tehditler, siber uzayda bulunan yazılım, donanım ve altyapıları hedef alırlar. Amaçları, saldırı yöntemleri ve motivasyonları farklı aktörler vardır ve bu aktörler merak, hırs, intikam almak, ekonomik kazanç elde etmek, siyasi ve politik düşünce, ideolojik ve dini inanç ve benzeri sebeplerle motive olurlar.

Amaçları hedef sistemlere zarar vermek veya çalışmaz hale getirmek, psikolojik baskı kurmak, kötü propaganda yapmak ve bu sistemler üzerinde işlenen ve saklanan hassas verileri ele geçirerek tahrip etmek veya yok etmektir. Tehditler çalışanlar, genç ve tecrübesiz kişiler, Bot-Net Operatörleri, suç örgütleri, zararlı yazılım yayıncıları, siber suçlular, siber casuslar, rakip kurum ve firmalar, organize suç örgütleri, hackerlar, devlet veya istihbarat örgütleri, terörist gruplar, doğal afetler ve devletler tarafından yapılabilmektedir [26].

4.5.1. Çalışanlar

Yaşanan tehditlerin çoğunluğunun kaynağı insan faktörü olarak karşımıza çıkmaktadır. Kasıtlı veya farkında olmadan kritik sistemler üzerinde riskli işlemler yapabilirler. İç aktörler, iyi niyetli bilinçsiz çalışanalar olabileceği gibi kötü niyet besleyen mutsuz, işten ayrılmış, emekli olmuş veya başkasına adına ajan olarak istihdam edilmiş çalışanlarda olabilir. Çalışanlar, dış aktörlerden farklı olarak sahip oldukları ayrıcalıklı erişim yetkileri nedeni ile kurumlarına çok daha büyük zararlar verebilirler. Güvenliğin en zayıf halkası olan insan, ekonomik kazanç elde etmek, haksız rekabet üstünlüğü sağlamak, intikam almak veya casusluk yapmak gibi amaçlarla birer iç tehdide dönüşebilmektedirler [27]. Dışarıdan kurumu tehdit eden kişiler genellikle kurum içindeki bilinçsiz ve eğitimsiz kişileri yanıltarak, kandırarak veya ikna ederek

her türlü parola, şifre ve benzeri gizli bilgileri elde ederler. Ayrıca kurum çalışanları tarafından kullanılan lisansız programlar ve işletim sistemleri, güvenlik koruması bulunmayan cihazlar, zayıf şifre ve parolalar, sosyal medya platformlarında dikkatsiz ve bilinçsizce paylaşılan kurumsal gizli bilgiler kurumlar için birer tehdit unsurudur.

4.5.2. Genç ve Tecrübesiz Kişiler

Daha çok genç yaştaki özenti kişilerin oluşturduğu gruptur. Bu gruptaki kişilerin hacker becerileri yoktur ve bilmeden hackerlar tarafından geliştirilen kötü amaçlı araç, yazılım veya uygulamaları kullanırlar. Kendilerini ispatlamak, yeteneklerini göstermek ve eğlenmek için motive olurlar.

4.5.3. Bot-Net Operatörleri

Botnet, büyük bir zombi bilgisayar ağı olarak ifade edilebilir. Farklı noktalardan yönetilebilen ve kötü amaçlı yazılım bulaşmış çok sayıda bilgisayarın oluşturduğu ağı tanımlar. Bu bilgisayarlar üzerinden hedefe saldırılar yönlendirilir. Ağ üzerindeki yüzlerce zombi bilgisayarlar, kullanıcılarının haberi olmadan gönderilen direktifleri takip ederler. Bu bilgisayarlar kullanıcılarının haberi olmadan çeşitli suçların işlenmesinde kullanılabilirler. Güvenlik duvarı koruması olmayan bilgisayarların botnet tuzağına düşmeleri daha kolaydır. Zombi bilgisayar ağları çoğunlukta dağıtık servis dışı bırakma saldırılarında kullanılırken, istenmeyen e-posta gönderimi, oltalama saldırıları, casusluk, bilgi hırsızlığı vb. gibi işler içinde kullanılmaktadır [28]. Saldırganlar kontrolü altındaki binlerce zombi bilgisayardan oluşan ağı maddi kazanç sağlamak için genellikle üçüncü kişilere kiralarlar.

4.5.4. Zararlı Yazılım Yayıncıları

Kötü niyetli saldırganlara hizmet eden, türlerine göre farklı şekillerde yayılan zararlı programlara virüs, Truva atı, solucan, fidye yazılımı, casus yazılımlar örnek verilebilir.

4.5.5. Siber Suçlular

Şiddet karşıtı ve maddi kazanç sağlama eğiliminde olan daha genç yaştaki kişilerin hedef kişi ve kurumlara yönelik bazen hukuka aykırı olmadığını düşündükleri zafiyet taraması, güvenlik zafiyetlerini istismar etme, kullanıcı bilgilerini çalma, şantaj,

lisansız yazılım kullanma, veri trafiğini ve ağı izleme vb. gibi eylemlerini özel yazılımlar kullanarak gerçekleştirirler. Yeteneklerini geliştirmek için kolektif hareket eder bilgi paylaşımında bulunurlar.

4.5.6. Siber Casuslar

Devletler, diğer devletlerin kurumsal, askeri veya devlet sırlarını elde edebilmek için istihbarat faaliyetleri yürütürler. Haksız rekabet içine giren şirketler rakiplerine ait yeni buluş, icat vb. gibi eserleri hak sahibinin izni olmadan kullanmak, çoğaltmak vb. amaçlarla fikri mülkiyet ihlalleri yaparlar, zarara uğratacak sabotajlar gerçekleştirirler [29].

4.5.7. Rakip Kurum ve Firmalar

Rakip kurum ve firmalar, rekabet üstünlüğü elde edebilmek için siber tehditleri kullanarak rakip oldukları firmalara ait yatırım planı, proje, taslak, çizim, strateji ve müşterilerini hukuka aykırı bir şekilde ele geçirmek için hareket ederler. Rakibi oldukları firmalar hakkında sosyal medya hesaplarında kamuoyunu yanıltacak kara propaganda, yalan yanlış bilgileri kullanarak duyguları istismar etmek suretiyle halkın kendi çıkarları doğrultusunda düşünmesini ve hareket etmesini sağlayacak eylemler yaparlar. Rakip kuruluşların e-hizmetlerini, web sitesini, servislerini veya sistemlerini çalışamaz hale getirerek itibarını zedeler, haksız rekabet ortamı yaratırlar.

4.5.8. Organize Suç Örgütleri

Maddi çıkar ve güç elde etmek üzere bir araya gelir, sistem açıklarından faydalanarak aldatma, yönlendirme, oltalama, fidye isteme, bilgi hırsızlığı vb. gibi eylemlerde bulunurlar. Bireyleri ve toplumları tehdit ettiği gibi ulusal ve uluslararası güvenliği de tehdit eden bir hale gelmiştir. Toplu olarak hareket edebilme kabiliyetine sahiptirler.

4.5.9. Bilgisayar Korsanı (Hacker)

Hacker, İngilizce kökenli bir kelime olup Türkçe karşılığı Bilgisayar Korsanıdır. Genellikle ağ ve sistemlere yetkisiz erişim sağlamak için çeşitli yöntemleri deneyen, yeteneklerini kullanan kişiler olarak tanımlanır. Maddi kazanç arayışı, heyecan, eğlence, öfke, intikam, hırs, duygusal ve politik nedenler, cinsel dürtüler, psikolojik

bozukluklar ve kendilerini ispatlamak, isimlerini duyurmak amacı ile hareket ederler**.** İstihbarat örgütleri tarafından en kolay kullanılabilen kendilerine özgü sloganları, markaları ve yöntemleri olan gruptur [30]. Hacker türleri arasında en yaygın olanları Hactivists, Yazılım Korsanı, Siyah Şapkalı, Beyaz Şapkalı ve Gri Şapkalı Hacker'lar vardır.

Hactivistler, politik veya siyasi amaçlarla hareket ederler. Bu grupta yer alan bilgisayar korsanlarının bir amacı ve ideolojisi vardır. Bu gruplara Anonymous, LulzSec, Suriye Elektronik Ordusu örnek verilebilir. Pınar Demirkıran'a göre; Hactivizm, bilişim teknolojilerinin toplumsal problemlere yönelik tepki, protesto etmek amaçlı kullanılması, Alexandra Samuel'e göre; "Hack ve Aktivizm kelimelerinin portmantosu ve yasal açıdan belirsiz araçların politik sonuçlar peşinden sessiz bir şekilde kullanılması" olarak tanımlanmıştır [31].

Siyah Şapkalı Hacker, bilgisayar korsanları arasında en tehlikeli ve deneyimli olan kişilerdir. Hedefleri sistem üzerindeki güvenlik açılıklarından yararlanarak gizli bilgileri ele geçirmek, sistemi çalışamaz hale getirmek veya kurum ve kişilerin itibarına zarar verecek şekilde eylemlerde bulunmaktır.

Beyaz Şapkalı Hacker, bilgisayar korsanlarına karşı alternatif çözümler üretir, sistem üzerindeki açıklıkları bulur, kurum içinde bu açıklıkların kapatılması ve gerekli önlemlerin alınması için çalışırlar. Siyah şapkalılar kadar bilgi sahibi olurlar ve devlet kurumlarında veya şirketlerde güvenlik uzmanı olarak çalışırlar.

Gri Şapkalı Hacker ise, bir yandan iyi eylemler yaparken diğer yandan suç sayılabilecek eylemler de bulunabilirler. Sistem açıklıklarını bulur sistemleri kontrol ederler fakat genellikle bilgi çalmaz ve zarar vermezler. Bazen sistemdeki açıklıkları sistem yöneticilerine veya rakip sistemlere para karşılığında bildirirler.

Yazılım Korsanları (Cracker), temelde ücretli yazılımları kırarak ücretsiz kullanılmasını sağlayan kişilerdir. Doğrudan programı kırmaz program üzerinde değişiklik yaparak tema, dil, ücretsiz kullanım gibi özellikleri program üzerine kurarlar.

4.5.10. Devlet veya İstihbarat Örgütleri

Rakibi veya düşmanı oldukları devlet ve kurumlar hakkında siyasi, politik, askeri, ekonomik, coğrafi ve stratejik önemli bilgiler elde edebilmek için siber güvenlik açıklıklarını ve çeşitli siber saldırı yöntemlerini kullanarak faaliyet gösterirler.

Devlet ve istihbarat örgütleri, rakipleri ve düşmanları hakkında istihbarat toplamak için teknik, insan kaynaklı ve açık kaynak istihbarat toplama tekniklerinden yararlanmaktadırlar. İstihbarat teşkilatlarının büyük bir kısmı istihbarı bilgilerin çoğunluğunu sosyal medya hesaplarından, internetten, açık kaynaklardan elde etmektedirler. İstihbarat örgütleri istihbari faaliyetlerde bulunmak için kurumsal ağ ve sistemlere izleme programları yüklerler ve kurum içerisine casus yerleştirirler. Devletin bekası, ülkenin ve vatandaşların korunması, milli ve ekonomik çıkarları göz önünde bulundurarak belirli hedeflere yönelik saldırı gerçekleştirir ve savunma sistemi geliştirirler. Günümüzde artık devletler birbirleri arasındaki mücadele ve rekabeti bilgi teknolojileri üzerinden yürütmekte ve askeri yatırımların büyük bir bölümünü siber savaşlar için yapmaktadırlar [20].

4.5.11. Terörist Gruplar

Terörist gruplar, hedef kurumların bilgi altyapısını yok etmek için kurumların kritik sistemlerini hedef alırlar ve kötü niyetli yazılım enjekte ederler. Kurum içerisine ayrıcalıklı erişim hakkı tanınan pozisyonlara casus kişileri yerleştirirler. Teröristler, Hactivist'lerden farklı olarak hedeflerine yönelik doğrudan zarar verici eylemlerde bulunurlar. Devletler, sürekli olarak rakiplerinden önemli bilgileri çalmak için çeşitli operasyonlar düzenlemektedir.

4.5.12. Doğal Afetler

Birtakım aktörlerin yanı sıra beklenmedik yangın, sel, deprem, kasırga gibi doğal afetler de bilişim sistemlerine ciddi zarar verirler.

4.6. Siber Tehdit Türleri

Kurumların savunma beceri ve kabiliyetlerini ölçmek için ülkemizde çeşitli ulusal denetim ve tatbikatlar yapılmakta ve bu sayede meydana gelebilecek riskler

belirlenerek gelebilecek siber tehditlere karşı daha etkin savunma geliştirilmesi hedeflenmektedir [32]. Avrupa Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA) 2018 yılında hazırladığı tehdit durum raporunda değerlendirilen başlıca on beş (15) siber tehdit türü şu şekildedir [33];

4.6.1. Kötü Amaçlı Yazılımlar

Sistem üzerindeki açıklıkları bularak hedeflenen verileri elde etmek için kullanılan yazılımlardır. Bu yazılımların hedefleri ve yöntemleri göz önüne alındığında virüs, solucan, istismar kodları, sahte antivirüs yazılımları, kök kullanıcı takımları, fidye yazılımı, indirme (downloader), tarayıcı soyma, reklam yazılımları, bukalemun, mantık bombaları, Truva Atı, arka kapı, trojen ve tuş kaydedici olarak sınıflandırılabilir.

Bilgisayar virüsleri, bilgisayar belleğine yerleşir ve kendi kendilerine diğer yazılımları tetikleyerek veya bozarak çoğalan kötü amaçlı yazılım türüdür. Genellikle elektronik posta iletileri içinde dikkat çekici, ilginç, komik resim, ses veya görüntü dosyaları gibi ekler şeklinde kendilerini gizleyerek yayılırlar. Anlık mesajlaşma esnasında veya internetten yükleme yoluyla da bulaşabilirler. Bu kötücül yazılımlar yayılma yöntemine, yapısına ve amacına göre ayrılırlar. Virüs türleri arasında yazılım bombaları, Truva atları, sömürme ve casus yazılımları, reklam, ekran-kayıt, arka kapı, tarayıcı ele geçirme gibi farklı virüs çeşitleri bulunmaktadır [34].

Bilgisayar solucanı, ana bilgisayarlara saldıran ve ağ aracılığıyla yayılan kötü amaçlı kod içeren, çoğalması ve çalışması için virüsler gibi etkinleştirilmesi ya da insanın müdahale etmesi gerekmeyen, kendi kendilerine çoğalabilen, ağ üzerinde haberleşme kanallarının kapasitesini düşüren, kalitesini bozan ve trafiği olumsuz yönde etkileyen programlardır. CPU kaynaklarını olumsuz yönde etkileyerek bilgisayarın, programların yavaş çalışmasına ve düzgün çalışamamasına neden olurlar.

İstismar kodları, sistemler üzerindeki güvenlik açıklıklarına saldırmak ve kötücül programları bulaştırmak için kullanılan bir araçtır. Web trafiğini yönlendirmek, güvenlik açığı bulunan tarayıcı tabanlı uygulamaları tespit etmek ve zararlı yazılımları çalıştırmak için daha güvenli web sitelerini kullanan otomatik tehditlerdir. İstismar

kodu ile ilk saldırı örneğine 2012 yılında rastlanmıştır. Saldırganlar binlerce bilgisayarın kontrolünü ele geçirerek ekranları dondurmuş ve mağdurlara tekrar bilgisayar ve dosyalarına erişebilmeleri için belli bir miktar para ödemeleri gerektiğini ve bilgisayarlarında bir virüsün kurulduğunu belirten mesaj duyurmuşlardır [35].

Sahte anti virüs yazılımları, genellikle bilgisayarınızda çok fazla virüs tespit edildiğini ve bunları temizlemek için uygun olan bir yazılım indirmeniz gerektiğini belirten mesajlarla bulaşır veya e-posta ile sahte ücretsiz anti virüs yazılımı linki göndererek yüklenmesini sağlarlar. Son yıllarda lisanslı yazılımların kullanılması için yasal çalışmalar yapılıyor; fakat ülkemizde çok fazla lisansız yazılım kullanılmaktadır.

Kök kullanıcı takımları (Rootkit), bilgisayara bulaşan ve çalışan işlemler arasında kendini gizleyen, uzaktan erişim ve kontrolü sağlayan virüs türevi bilgisayar programlarıdır. Genel anlamda, çekirdek, kütüphane ve uygulama seviyelerinde, işletim sistemi ayırt etmeksizin çalışabilirler. İlk kez UNIX sistemlerinde ortaya çıkmıştır ve herşeyi yapma yetkisine sahip en kuvvetli kullanıcı olan "rot" ve bir dizi program olan "kit" terimlerinden gelmiş Rootkitler, zararsız olsalar da kötü niyetli kullanıcılar tarafından zararlı hale getirilebilmektedir [36].

Fidye yazılımı (Ransomware), kullanıcıların bilgisayarını kilitler veya dosyalarını şifreleyerek kullanıcıdan dosyaları kurtarması veya kilitlediği bilgisayarı açması karşılığında belli bir miktar para talep eden zararlı yazılım saldırısıdır. Genellikle ilgi çekici bir konu, önemli bir evrak veya fatura gibi görünen e-posta ekleri ile bulaşırlar. Güncel olmayan işletim sistemi veya kullanılan tarayıcı ve benzeri yazılımlar üzerindeki güvenlik zafiyetlerini istismar ederler.

Downloader, sadece diğer kötü amaçlı yazılımları ve kod parçalarını indirmek için kullanılan zararlı program türüdür. Bu tür programlar ağ kaynaklarından çeşitli içerikleri gizlice indirirler. Kötü amaçlı program değildir. Kötü niyetli kişiler sisteme ilk eriştiklerinde bu programı kurarlar. Bu program sayesinde ilave zararlı yazılımları yükleyebileceklerdir.

Tarayıcı Soyma (Browser Hijacking), kullanıcının izni olmadan web tarayıcısının ayarlarını değiştiren bir saldırı çeşididir. Genellikle web tarayıcısı eklentisi şeklinde

olur ve başlangıç sayfası, varsayılan arama motoru ve yeni sekme sayfasını değiştirerek eylemlerine başlarlar. Korsanlar tarafından ayarlanan giriş sayfaları genellikle arama motoru sayfalarıdır ve bu programların çoğu casus yazılımlarıdır. Örneğin, Google Web Araç Takımı (GWT) çerçevesindeki CVE-2007-2378, kişisel verileri hukuka aykırı olarak takip eden bir JavaScript kaçırma saldırısıdır [37]. Tarayıcı korsanları, arama terimlerini, ziyaret edilen sayfaları, yüklenilen dosyaları, IP bilgilerini, girilen bilgileri toplarlar. Sistemlere bulaştıktan sonra ciddi performans kayıplarına, ana sayfa ve sık kullanılanlar listesinin değişmesine neden olabilirler.

Reklam Yazılımları (Adware), arka planda çalışırlar. Bilgisayarın performansını önemli ölçüde etkilerler. Arama isteklerini reklam sitelerine yeniden yönlendiren, ziyaret edilen web sitelerinin türleri hakkında bilgileri toplamak vb. gibi amaçlar için tasarlanmış programlardır. Reklam yazılımları ücretsiz veya paylaşılan yazılımlar ve virüs içeren web siteleri vasıtasıyla bilgisayarlara bulaşır [38] ve diğerlerine göre daha az tehlikelidir.

Bukalemun, diğer programlardan farksız çalışma şekli olan, aldatıcı ve hileler içeren bir yazılımdır. Bir başka programmış gibi davranabilir. Çok kullanıcılı bir sisteme giren bütün kullanıcıların adlarını ve şifrelerini gizli dosyaya kaydeder. Sonra bakım için sistemin bir süreliğine kapatılacağını duyurur. Saldırgan kaydedilen isim ve şifreleri alır ve kendi amaçları için istediği gibi kullanır.

Mantık Bombaları, genellikle bilişim sistemlerini servis dışı bırakmak için kullanılan, herhangi bir program içerisine yerleştirilen virüs programlardır. Şartlar oluştuğu zaman patlayarak sisteme zarar verirler. Örneğin; NASA ve ABD donanmasına bileşenler üreten Omega Engineering Firması'nın sistemine zaman ayarlı mantık bombası kodu yerleştirilerek 10 milyon dolarlık üretim verileri silinmiştir [39].

Casus yazılımlar, tarama geçmişini ve izlerini kaydeden, kullanıcı izni gerektirmeksizin kendi kendini yükleyebilen kötü amaçlı programlardır. Bilgisayarlara tuzak yazılımların kurdurulması ile bilgilerin aktarılması sağlanır [40]. Casus yazılımlar aşağıdaki gibi Truva Atı, arka kapı, tuş kaydedici olarak gruplandırılabilir [41]. Arka kapı, kimlik doğrulaması olmadan sisteme erişmesini ve sistemde komut

çalıştırmasını sağlayan zararlı bir yazılımdır. Arka kapı birtakım teknikler kullanılarak oluşturulabildiği gibi sistem ve yazılım geliştiren kişilerce de kasıtlı veya istenmeden oluşturulabilir.

4.6.2. Web Tabanlı Saldırılar (Web Based Attacks)

İnternetten verilen hizmetlerin sayısındaki artış nedeniyle web uygulamalarına yönelik saldırıların ve türlerinin sayısı da her geçen gün artmaktadır. İnternetin yaygınlaşması ile beraber güvenlik riskleri de aynı ölçüde artmıştır. Web tabanlı saldırılar arasında özel saldırı vektörleri, sürücü indirmeleri, kötü niyetli web sayfaları, Water-holing ve içerik yönetim sisteminde uzlaşma saldırıları yer almaktadır. Bunlar;

Özel saldırı vektörleri, kullanıcıların haberi olmadan ayarları değiştirerek tarayıcı güvenliğini ihlal etmek amacıyla işletim sistemi ve yazılımdaki bir güvenlik açığından yararlanan kötü amaçlı kodlardır [42]. Bu zararlı kodlar HTML, ActiveX, JavaScript, Flash vb. gibi teknolojilerden yararlanabilir ve tarayıcının gelişi güzel kod çalıştırmasına neden olabilirler.

Sürücü indirmeleri saldırısında, saldırganlar PHP veya HTTP kodları içine kötü amaçlı komut dosyası yerleştirmek için güvensiz web sitelerini ararlar. Komut dosyaları sayfayı ziyaret eden birinin bilgisayarına kötü amaçlı yazılım yükleyebilir veya kontrolü ele geçirilmiş bir siteye yönlendirme yapılabilir. Diğer saldırılarda olduğu gibi e-posta ekininin açılması veya bir linke tıklanması gerekmez. Bir web sitesini ziyaret ederken veya bir e-posta hesabını görüntülerken farkında olmadan indirme işlemleri gerçekleştirilebilir. Bu yöntemle yapılan saldırılar gizlidir ve etkisi daha büyüktür.

Kötü niyetli web sayfaları (URL), genellikle kullanıcıları aldatıcı niteliktedir ve yaygın olarak istenmeyen e-posta, kimlik avı içerirler. Ziyaret edildiğinde saldırıyı başlatmak için tarayıcının güvenlik zafiyetlerinden yararlanan sayfalardır. Aldatma, yanıltma, yönlendirme, sosyal mühendislik ve zararlı yazılım yükleme şeklinde atak yaparlar [43].

Water-holing, kullanıcıları cezbeden oltalama saldırısında olduğu gibi e-posta kampanyaları, reklam gibi unsurları kullanmak yerine savunmasız sitelere zararlı yazılımları enjekte eder ve sonrasında kullanıcıları bu sitelere yönlendirirler.

İçerik yönetim sistemi (CMS), web sitesine ait içerikleri yönetmek için tasarlanmış bir sistemdir. Sistem içerisinde bulunan içerikler içerik yönetim sistemi ile kontrol edilebilir, düzeltilebilir, değiştirilebilir ve tamamen silinebilir. Güvenlik açıklıklarını kullanan saldırıcı aracıdır. Saldırganlar kimliği doğrulanmış ve ayrıcalıklı alanlara uzaktan erişim sağlamak için web sunucusuna kötü amaçlı yazılım yüklerler.

4.6.3. Web Uygulaması Saldırıları

Web sunucularının dış dünyaya açık ve erişilebilir olmaları tehditleri daha fazla üzerlerine çekmelerine neden olmaktadır. ASP, HTML, JavaScript ve PHP gibi diller kullanılarak geliştirilen web uygulamaları hatalı kodlama veya eksikliklerden dolayı güvenlik zafiyetleri barındırmaktadır. Bu zafiyetler istismar edilerek hedef sunucuların giriş sayfaları değiştirilebilmekte, veri tabanından veriler silinebilmekte, arka kapı yazılımları yüklenebilmekte ve son kullanıcıların çerez bilgileri çalınabilmektedir. Genellikle saldırılar, uygulama katmanı üzerinde gerçekleşmektedir. Güvensiz yazılımların meydana getireceği sorunlara karşı mücadele etmek amacıyla 2014 tarihinde ABD'de OWASP Vakfı kurulmuştur [42]. Bağlı olduğu bir kurum veya kuruluş yoktur. OWASP'a ait dokümanlar ve araçlar herkese açıktır. Tüm web açıklarını belli bir puan sistemine göre sıralar ve en popüler olan ilk on (10) web güvenliği riskleri listesini önerileri ile birlikte yayınlar. 2017 yılında güncellenen top on (10) web açıklıkları listesi başlıklar halinde aşağıda belirtilmiştir.

4.6.3.1. Enjeksiyon Kusurları

Enjeksiyon saldırıları, tehlikeli saldırılara neden olabilecek güvenlik açığı kategorilerini oluşturur. Bu tür saldırıda saldırgan, uzaktan komutları çalıştırabilmek için bilgisayara zararlı kod enjekte ederek veritabanındaki verileri değiştirebilir. Bu saldırı türleri arasında SQL enjeksiyonu, işletim sistemi komut enjeksiyonu ve LDAP enjeksiyonu dâhildir. Saldırganların bir SQL deyimine web sayfası girişi yoluyla SQL komutları ekleyebildiği bir tekniktir [44].

Enjeksiyon tehdidinden korunmak için, veriler komut ve sorgulardan ayrı tutulmalıdır. Yorumlayıcının kullanımını engelleyen ve veri tabanını bir harita olarak gösteren ORM aracı kullanılmalıdır. Pozitif veya 'beyaz liste' sunucu tarafı giriş doğrulaması kullanılmalıdır. Dinamik sorgular için özel karakterlerden kaçınılmalıdır. SQL enjeksiyon durumunda kayıtların toplu olarak ifşa edilmesini önlemek için sorgu içinde limit koyulmalı ve diğer SQL kontrolleri kullanılmalıdır.

4.6.3.2. Bozuk Kimlik Doğrulama (Broken Authentication)

Kimlik doğrulama, uygulamayı kullanacak kişilerin geçerli ve tanımlı başka kullanıcı olup olmadığının kontrol edilmesi işlemidir. İnternet üzerinden işlemler gerçekleştirildiği için bu sistemler üzerinden kişi ve kurumlara ait kullanıcı adı, parola ve şifre gibi gizli veriler çalınabilmektedir. Bu zafiyet genellikle "kimlik doğrulama veya oturum yönetimi" ile ilgili işlemlerin hatalı yapılması sonucunda ortaya çıkar. Saldırganlar parolaları, oturum belirtecini (session token) ele geçirebilirler. Yetkisi olmayan kişilerin sisteme girişimini engellemek için her ortamda kimlik doğrulamasına ihtiyaç duyulur. Kullanıcı bilgileri önceden uygulama içerisinde tanımlanır ve erişmek istediğinde kullanıcı uygulamaya kendisini tanıtır. Kimlik doğrulama metodolojisinde üç (3) farklı faktör bulunmaktadır, bunlar;

- Kullanıcının bildikleri (kullanıcı adı, parola vb.)
- Kullanıcının sahip oldukları (telefon, OTP Cihazı vb.)
- Kullanıcının varlığına ait (retina, avuç içi, parmak izi, yüz tanıma vb.)

Bozuk kimlik doğrulama tehdidinden korunmak için; çok faktörlü kimlik doğrulaması yapılması, genel verilerin dışındaki diğer verilerin default olarak engellenmesi, yönetici kimliği ile veri gönderilmemesi, zayıf şifre kontrollerinin uygulanması, başarısız giriş deneme sayısının sınırlandırılması ve sunucu taraflı kimlik doğrulamasının yapılması gerekir. Herhangi bir saldırı algılandığında tüm hatalar günlüğe kaydedilmeli ve yöneticiler uyarlılmalıdır. Oturum kimlikleri, oturum esnasında, sonlandırıldığında veya zaman aşımına uğradığında URL'de bulunmamalı ve güvenli yerde saklanmalıdır. Hatalı giriş denemeleri kayıt (log) altına alınmalı ve incelenmelidir [44].

4.6.3.3. Hassas Veriyi Açıkta Bırakma (Sensitive Data Exposure)

Hassas veri riskinde saldırganlar parola saldırısı yerine anahtarı ele geçirerek ortadaki adam saldırısı gerçekleştirir veya sunucudan veri aktarımı esnasında açık metinleri çalarlar. Oturum kimliği, finans ve müşteri vb. gibi hassas verilerin şifrelenmeden saklanması veya taşınmasından dolayı bu tür tehditler meydana gelmektedir [43]. Parola kullanılan uygulamalarda ise zayıf algoritma, protokol ve şifre kullanımı, zayıf anahtar üretimi en yaygın yapılan hatalardır.

Hassas veri riski tehdidini önlemek için; işlenen, transfer edilen ve saklanan veriler, risk seviyelerine göre sınıflandırılmalı ve gerekli olmayanları imha edilmelidir. Güncel ve güçlü algoritma, protokol ve anahtar kullanılmalıdır. Hassas veriler TLS ve SSL protokolü ile taşınmalıdır.

4.6.3.4. XML Dış Varlıklar (External Entities)

HTML sayfası tasarlanırken önceden belirlenmiş taglar kullanılır. XML sayfası tasarlanırken belli kurallara göre taglar tasarlanabilir. XML, yapısının esnekliği sayesinde birbirine uyumlu olmayan sistemler arasında veri alışverişi kolay gerçekleştirmektedir. Her sistemde çalışabilir olması, kolay öğrenilmesi, verilere erişimin kolay olması XML'i avantajlı kılar. XML dokümanları veri yapısını tanımlar ancak verinin nasıl işleyeceğini tanımlamaz. Bu da XML'i dezavantajlı kılar. Web uygulaması veya web servisi güvensiz kaynaklardan gelen XML girdisine ve yüklemelerine direk müsaade ediyorsa veya bu veriyi XML dokümanına ekliyorsa saldırıya açıktır. Ayrıca herhangi bir XML sayfası veya web servisleri doküman tipi tanımlarına (DTD) izin veriyorsa, tek oturum açmaya (SSO) olanak tanıyan XML tabanlı bir kimlik standardı kullanılıyorsa hizmet reddi ve diğer saldırılara karşı savunmasızdır. XML Dış Varlık Zafiyetine Bug Bounty' kapsamında yapılan bir çalışma ile çeşitli yöntemler ve kodlar kullanılarak Cisco Firması'na ait Webex Konferans yazılımı üzerinde bulunan kritik güvenlik açığı örnek olarak verilebilir [45]. Bu zafiyet ile sistemin log kaydına, dosyalarına, kullanıcı parolası bilgilerine, görüntü kayıtlarına ve birçok kritik bilgiye erişim sağlanmıştır.

Bu zafiyet türünden korunmak için; okuyup yazılabilmesi kolay, XML'e göre daha hızlı, daha küçük boyutlarda verilerle işlem gerçekleştirilebilen JavaScript uygulamaları için oluşturulmuş veri formatı olan JSON dili tercih edilmelidir. Web uygulaması ve işletim sistemi tarafından kullanılan en kritik XML uygulama ve işletim sistemlerinin yama yönetimi düzenli olarak yapılmalı ve XML formatında olan ve HTML formatında gönderilen SOAP (Simple Access Protocol) protokolünün son sürümleri kullanılmalıdır. Bütün verilerin doğrulandığından emin olunmalı, HTML form alanları, REST çağırımları, sorgu parametreleri, http başlıkları, çerezler ve benzeri girdi içeren alanlar içerisindeki zararlı girdileri önlemek için sunucu tarafında pozitif ('beyaz liste') doğrulaması, filtreleme veya temizleme işlemi yapılmalıdır.

4.6.3.5. Eksik Erişim Kontrolü (Broken Access Control)

Saldırganlar, saldırılarında erişim kontrollerini kullanır ve güvenlik açıklıklarını tespit edebilmek için kod çalıştırmadan bilinen güvenlik açıklıklarını ve derlenmiş bir kodun detaylı bir modelini çıkartarak beyaz kutu testi olan SAST testini gerçekleştirirler. Böylece erişim kontrolünün yokluğu tespit edebilir veya işlevsel olup olmadığını anlarlar.

Eksik erişim kontrolü tehdidini önlemek için; sunucu üzerinde JWT belirteci, oturum kapatıldıktan sonra geçersiz kılınmalıdır. API ve kontrol erişimi sınırlandırılmalı, sunucu dizin listesi devre dışı bırakılmalı, başarısız erişim kontrolleri günlüğe kaydedilmeli ve gerektiğinde yöneticiler uyarılmalıdır. Uygulama boyunca erişim kontrol mekanizmaları bir kez uygulanmalı ve CORS kullanımını en aza indirgemek için yeniden kullanılmalıdır.

4.6.3.6. Yanlış Güvenlik Yapılandırması (Security Misconfiguration)

Uygulamalar, çerçeveler ve sunucu vb. gibi tüm bileşenler için güvenlik gereksinimleri bulunmalı, güvenlik yapılandırması tanımlanmalı ve uygulanmalıdır. Saldırganlar, genellikle yama eksikliğinden yararlanmak veya sistemde yetkisiz erişim elde edebilmek için varsayılan hesaplara, kullanılmayan sayfalara, korunmayan dosyalara ve dizinlere erişmeyi denerler. Uygulama yığını veya bulut hizmetleri üzerinde uygun güvenlik ve doğru yapılandırmanın bulunmaması, gerekli özelliklerin

etkinleştirilmemesi veya yüklenmemesi, varsayılan hesapların ve şifrelerin değiştirilmemesi, yükseltilmiş sistemler için güvenlik özelliklerinin devre dışı bırakılması, yazılımların güncel olmaması bu tür saldırılara karşı savunmasız kılmaktadır.

Yanlış güvenlik yapılandırması tehdidini önlemek için; yazılım geliştirme ve çalışma platformlarında farklı kimlik bilgileri kullanılmalı, kullanılmayan gereksiz özellikler, bileşenler, belgeler ve örnekler yüklenmemeli ve kaldırılmalıdır. Veri tabanı güncellemeleri ve yama kontrolleri düzenli olarak yapılmalıdır.

4.6.3.7. Siteler Arası Betik Çalıştırması (XSS Cross-Site Scripting)

Siteler arası betik çalıştırması, OWASP Top On (10) listesinde yerini koruyan en yaygın görülen saldırı türüdür. XSS zafiyeti; HTTP, CSS, JavaScript vb. ile kod parçacıklarının hedef kullanıcının istemcisinde izinsiz olarak çalıştırılmasından meydana gelir. Saldırganların istemcinin tarayıcısında çalıştırılacak kötü amaçlı kodlar eklemesine izin veren bir güvenlik açığıdır. Güvenlik zafiyeti türüne bağlı olarak tehlikeli kodu web sitesine yükleyebilir veya zararlı kod içeren bir bağlantı oluşturabilir. Phishing yöntemi ile kullanıcın bu kodu çalıştırmasını sağlar. Bu sayede oturum ele geçirilebilir, farklı saldırı türlerinin başlatılmasına izin verilebilir. Bu zafiyet türü kendi içerisinde yansıtılmış, depolanmış ve DOM tabanlı XSS olmak üzere üçe ayrılır.

Yansıtılmış XSS; uygulamaya ait girdi noktalarında kontrol ve filtreleme yoksa bu girdi noktalarına girilen zararlı JavaScript vb. Script kodları sayfaya çıktı olarak yansıtılıyorsa bu yol kullanılarak istenilen değerlerin sayfaya yansıtılması işlemidir [46]. Kısaca özetlersek; girilen zararlı kodun sunucuya gittikten sonra sunucuda depolanmadan geri döndüğü saldırıdır. Bunlardan;

Depolanmış XSS, en tehlikeli XSS saldırı türüdür. Bu saldırıda kullanıcıdan gelen girdiler ekrana yazdırılmaz ve öncelikle veritabanına tutulur. Gönderilen zararlı kod uygulama tarafından veritabanına veya dosya sistemine kayıt edilir. Örneğin; kaydedilen veri kullanıcıya gönderilen özel mesaj alanında ise bu mesaj tek bir kişi tarafından görüntülenir şayet bütün yorum sayfasına eklendiyse o zaman herkes bu

saldırının kurbanı olacaktır. DOM tabanlı XSS saldırıları, DOM açıklamasını değiştirerek, içeriğin farklı ve kötü amaçlı oluşturulmasını sağlayarak çalışır. XSS güvenlik açıklıklarını kontrol altına almak için güvensiz yerlere veri eklenmemeli, girdi ve çıktı denetimi yapılmalı ve her girdi kontrol edilerek içeri alınmalıdır [47].

4.6.3.8. Güvensiz Ters Serileştirme (Insecure Deserialization)

Bu tehdit ölçülebilir değildir. Endüstri anketine dayanarak OWASP Top On (10) listesinde yer almıştır. Serileştirme (Serilization), .NET üzerinde işlem yapıldığı zaman bir nesnenin, bir sınıfın saklanmak istenilen ya da gönderilmek istenilen formata dönüştürülmesi işlemidir. Bu şekilde nesneler kalıcı veya geçici olarak saklanabilir. Ters Serileştirme (Deserialization) ise, uygulanmış olan nesne, verinin tekrar okunabilir hale getirilmedir. Düzgün erişim kontrolü olmayan uygulamalara yönelik gerçekleşen bir kusurdur ve bu kusur dizilerin, dosyaların, anahtarların görüntülenmesine veya kullanılmasına neden olur [43].

4.6.3.9. Bilinen Açıklık Bileşenlerini Kullanma (Using Components with Known Vulnerabilities)

Bu tehdit türü, zafiyet bulunan servis, uygulama ve eklentilerin, eski ve bilindik istismar kodu içeren sürümlerin kullanılması sonucu oluşmaktadır. Saldırganlar bu servislerin sürümlerini bulduktan sonra bilindik istismar kodu kullanıp uygulamayı/sunucuyu ele geçirebilirler. İşletim sistemi, veritabanı, uygulama, servis, API ve tüm bileşenler güncel değilse, düzenli zafiyet taramasından geçirilmiyorsa, güncel yama ve güvenlik bültenleri düzenlik takip edilmiyorsa bu tehdide karşı savunma sağlanamayacaktır [42].

Bu zafiyet türünden korunmak için; gereksiz özellikler, dosyalar, belgeler vb. gibi unsurlar kaldırılmalıdır. Sunucu tarafındaki bileşenlerin ve sürümlerinin envanteri düzenli olarak çıkarılmalıdır. CVE ve NVD gibi kaynaklar takip edilmelidir.

4.6.3.10. Yetersiz Kayıt ve İzleme (Insufficient Logging & Monitoring)

Olası siber saldırı esnasında müdahale sürecinin iyi yönetilmemesi ve saldırılara karşı sistemler üzerinde anormalliklerin ve değişikliklerin yeterince izlenmemesi bu tür saldırılara karşı savunmasız kılar. Başarılı veya başarısız giriş denemeleri ve riskli

işlemlerin kayıt (log) altına alınmaması, hatalı durumlarda uyarı ve mesaj alınmaması, uygulama ve API'lerin şüpheli hareketlerine ait kayıtların (logların) izlenmemesi, sızma testlerinin alarm üretmemesi, günlük kaydının yapılmaması vb. gibi eksiklikler zafiyet oluşturmaktadır.

4.6.4. Kimlik Avı Saldırıları (Phishing)

Sosyal mühendisliğe dayanan bir saldırı çeşidi olan kimlik avı saldırıları birden fazla biçimde gerçekleşebilir. Saldırganlar kendilerini hedefindeki kişilere polis, savcı veya otorite sahibiymiş gibi göstererek ve güven duymalarını sağlayarak onlardan kişisel bilgilerini, banka bilgilerini paylaşmalarını isteyebilirler. Kimlik avı genellikle e-posta ya da reklam üzerinden veya hâlihazırda kullandığınız sitelere benzeyen siteler aracılığıyla yapılır. Örneğin, müşterisi olduğunuz bankanızdan veya bilinen bir web sitesinden geliyor gibi görünen e-postalardır. Kimlik avı siteleri genellikle kimlik numarası, kullanıcı adı ve şifre, banka hesap numarası, anne kızlık soyadı, doğum tarihi gibi bilgileri isterler.

Kimlik avı saldırılarını önlemek için; kaynağı belli olmayan veya bilinmeyen e-posta ekine ve içerisinde bulunan linkle etkileşime girilmemeli, kaynağı bilinmeyen web sitelerinin güvenliği kontrol edilmeli ve yönlendirme yapılarak doldurulması doldurulması istenen şifre, banka kartı ve benzeri kişisel bilgiler kesinlikle yazılmamalıdır. Sayısal rakam içeren adresler dikkatli bir şekilde kontrol edilmeli, güvenlik yamaları yüklenmeli ve anti virüs yazılımları düzenli olarak güncellenmelidir. Güvenli sitelerin beyaz listesinin tutulması, güvenli iletişim kanallarının oluşturulması ve ağ trafiğini izlenmesi güvenlik açıklıklarını azaltmaya yardımcı olur.

Saldırıların türü ve türüne göre şiddeti, yaygınlığı yıldan yıla değişim göstermektedir. Trustwave Global Security'nin raporunda; kimlik avı saldırılarının 2017 yılında güçlü olduğu belirtmiştir ve çizelge 4.1'de kimlik avı saldırılarına ait ana temalar verilmiştir [48].

Çizelge 4. 1 Trustwave Global Security Raporu - Kimlik avı saldırısı temaları.

CVE Referans	**Ürün**
Banka	Çevrimiçi bankacılık bilgilerinin toplandığı sahte açılış sayfası
Amazon	Çeşitli açılış sayfaları, zararlı kimlik bilgileri ve önemsiz ürünler içeren sahte Amazon makbuzu.
Courier	Sahte paket teslimatları ve nakliye şirketinden gelen makbuz. Fidye yazılımı veya bankacılık Truva atları gibi kötü amaçlı yazılımların yüklenmesine yol açar.
Apple	Sahte Apple Mağazası makbuzları ve 'reset' parolaları ile kimlik bilgileri toplanır.
Kamu Hizmeti Kuruluşu	Sahte enerji veya telekomünikasyon kuruluşlarından geliyormuş izlenimi veren ve fidye veya Truva atı zararlı yazılımlarını içeren sahte fatura bağlantıları.
Finans Yazılımı	Görünüşte MYOB, Quickbooks, Xero veya Intuit gibi görünen sahte e-postaları
Vergi İadesi	IRS'den gelen Java tabanlı uzaktan Trojen erişimli bir mesaj
E-posta Kotası	Kullanıcının domain giriş bilgilerini almak için sahte e-posta kotası veya hatırlatıcı şifreler.

4.6.5. Hizmet Reddi Saldırıları (DoS - Denial of Service)

Bir bilgisayar veya ağın, kaynaklarını kullanılmaz hale getirecek şekilde aşırı kaynak kullanılmasını sağlayarak gerçekleşen saldırılardır. Hizmet reddi saldırısında mağdurun paylaşılan kaynaklarında bozulmalar olur ve mağdur kullanıcıların bu kaynaklara erişimi engellenir. Bu saldırı, bilgisayar sisteminin belli bir kısmını, tamamını, belli bir ağ altyapısını ve tüm altyapısını hedef alabilir. Bu tür saldırılar güvenlik yazılımları veya işletim sistemleri marifetiyle tam olarak engellenemez. Ancak sistemin en baştan tasarım aşamasından başlanarak önlemlerin alınması gerekir. Birden fazla bilgisayar üzerinden saldırı yapılırsa dağıtılmış hizmet reddi saldırısı (DDoS) yapılmış olur.

Dağıtılmış ağ saldırıları, genellikle "Dağıtılmış Hizmet Reddi (DDoS) Saldırıları" adıyla bilinir. Bu tür saldırılar, kurumun web sitesi altyapısı ve geçerli olan belirli kapasite sınırlarından faydalanır. Saldırıya uğrayan web kaynağına otomatize yazılımlarla veya zombi bilgisayarlar ile birden çok istek göndererek sistemi çalışamaz hale getirir veya kilitlerler [49]. Zombi bilgisayarlar, birden fazla kişinin sanal olarak

karşılıklı görüşmesini sağlayan çevrim içi sohbet sistemlerini kullanarak birbirileri ile iletişim kurar ve komut gönderirler [50]. Bu yöntem ile zombi bilgisayarlar fark edilmeden kendi aralarında daha güvenli ve garantili etkileşim sağlarlar.

Hizmet reddi saldırılarını önlemek için; saldırıların önceden tespit edilmesi ve engellenmesi gerekir. Bunun için anti virüs sistemleri, yama yönetimi, güvenlik duvarı, zararlı yazılımların taranması ve sensörlerle protokollerin korunması için önleyici mekanizmaların kullanılması önemlidir [51].

Nexusguard Q2 araştırma raporuna göre [52]; 2018 yılının ikinci çeyreğinde ağ ve kritik hizmetlere yönelik DDoS saldırılarından nesnelerin interneti IoT zombi bilgisayarlarının büyük ölçüde sorumlu olduğu görüşü desteklenmiştir. Mirai kötü amaçlı programının bir türevi olan Satori, bazı ev ağ cihazlarındaki sıfırıncı gün güvenlik açıklarından yararlanarak UDP, TCP SYN ve TCP ACK paketlerine yönelik saldırılar yapmak için tasarlanmıştır. Saldırganların daha çok vur kaç taktikleri üzerine odaklandıkları ve gelir getiren hedeflere yönelik zamanlanmış saldırı başlattıkları ifade edilmiştir. Sırası ile 4.07 saldırının %31.56'sı UDP, 1.997 saldırının %18.50'si TCP SYN ve 1.006 atağın %9.32'sinin ICMP vektörü ile yapıldığı ve toplam atakların % 35.87'sinin 10 Gbps'den büyük, % 64'nün 10 Gbps'den küçük olduğu belirtilmiştir.

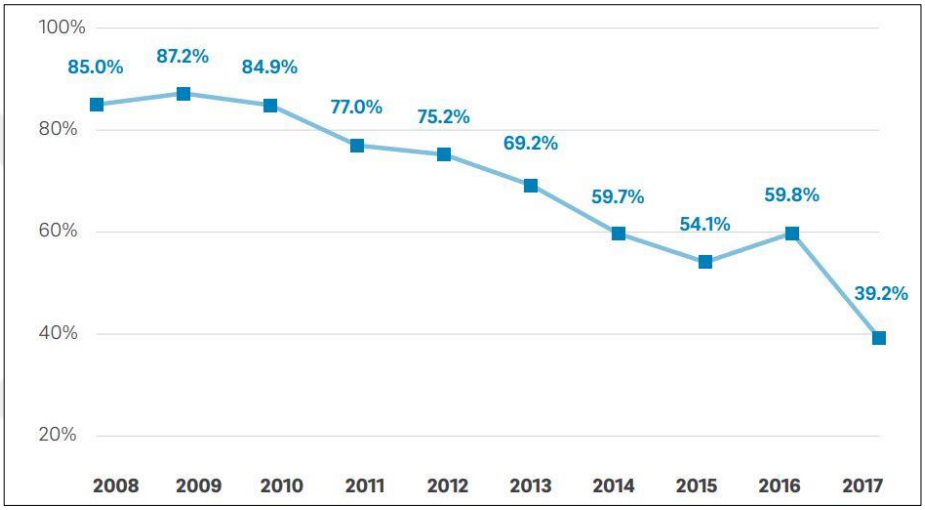
4.6.6. İstem Dışı Alınan Elektronik İletiler (Spam)

Spam, kullanıcılar tarafından istenmeyen e-posta ve mesajlaşma teknolojilerinin kötüye kullanılmasıdır. İstem dışı alınan elektronik iletiler genellikle ticari reklam şeklinde olur. Spam gönderimi küçük maliyetlerle yapılabilirken alan taraflar için büyük maliyetlere neden olmaktadır.

Kaspersky Lab tarafından hazırlanan Q1 2019 yılı Spam ve Kimlik Avı Saldırısı başlıklı raporunda, istem dışı alınan e-postaların en yüksek görüldüğü ilk 10 ülke belirtilmiştir [53]. Sırasıyla en çok Çin %15,82, ABD % 12,64, Rusya % 6,98, Brezilya %6,95, Almanya % 5,86, Fransa % 4.26, Arjantin % 3.42, Polonya % 3.36, Hindistan % 2.58 ve Vietnam % 2.18 oranla yer almaktadır.

İstenmeyen e-posta saldırılarına maruz kalmamak için anti spam yazılımlarının kullanılması, istenmeyen iletilerin servis sağlayıcılara bildirilmesi, kaynağı bilinmeyen ticari reklam veya benzeri dikkat çeken mesajların açılmaması ve yanıtlanmaması gibi kişisel tedbirler alınmalıdır.

Trustwave Global Security Raporun'da yaklaşık 6 milyon bot ile bilinen en yaygın botnet virüslerinden olan Necurs'un yıldan yıla istenmeyen e-posta aktivitelerindeki düşüş grafik olarak şekil 4.1'de gösterilmiştir [48].



Şekil 4. 1 Botnet Necus virüsüne ait spam aktiviteleri

Bot, bilişim dünyasında "robot" anlamında kullanılan yaygın bir terimdir. En temel anlamıyla verilen görevi yerine getiren programlara verilen isimdir. İnternet üzerinde çalışan otomatik bir programdır. Botların bazıları otomatik bazıları ise belirli bir giriş aldıklarında komutları çalıştırır. Farklı türlerde bot vardır. Solucan, virüs vb. gibi kötücül yazılımların sebep olduğu arka kapıları kullanarak yayılabilir. Ana cihazlar ile iletişim kurmak için bu yazılımlar genellikle kişilerin birbirileri ile çevrimiçi sohbet etmelerini sağlayan bir hizmet olan "Internet Relay Chat" protokolünü kullanırlar [54]. Botnet, kötü amaçlı programların bilgisayarlarda yayılıp bu programları kullanan bilgisayarlara çeşitli görev ve talimat vermeye yarayan saldırı yazılımlarıdır. Daha çok DDoS saldırılarında kullanılır. Çeşitli cihaz ve güvenli olmayan bilgisayarlarında botnet ağına dâhil olması bu saldırılara karşı savunmayı daha da zorlaştırmaktadır. Milyonlarca cihazı kontrol altına alabilen, IP aldatması vb. gibi çeşitli yöntemler

kullanarak kendilerini ve çıkış noktalarını gizleyen bu ağların sahiplerinin takip edilmesi zor olduğu için ağ üzerindeki bu cihazların erişiminin engellenmesi de bir o kadar imkânsızdır.

4.6.7. Veri İhlalleri (Data Breaches)

Veri ihlallerinde, SQL enjeksiyon ve kimlik avı saldırılarıyla kritik bilgilere erişim sağlarlar. Veri ihlalleri, kurumsal kaynakların her türlü yetkisiz ve kötü amaçlı kullanımını içerir. ENISA ve diğer güvenlik raporlarında, ayrıcalıklı yetkilere sahip veya diğer çalışanların veri ihlallerinde büyük rol oynadıkları ifade edilmektedir. Sosyal mühendislik veya doğrudan fiziksel saldırılar nedeniyle veri kayıpları kasıtlı veya kasıtsız olabilir.

Veri ihlallerini önlemek için; büyük veri transferinde ve usb cihazlarının kullanımında veri kaybı önleme çözümleri uygulanmalıdır. Hassas veriler şifrelenerek saklanmalı, verilere erişim sınırlandırılmalı ve tüm cihazlar için güvenlik çözümleri uygulanmalıdır. Kimlik doğrulaması iki faktörlü yapılmalı ve güçlü parola politikası geliştirilmelidir. Farkındalık eğitimleri düzenlenerek veri ihlalleri konularında çalışanlar bilinçlendirilmelidir.

4.6.8. İçeriden Gelen Tehditler (Insider Threat)

Daha öncede bahsettiğimiz üzere kurum içinden kötü niyetli bilerek hareket eden, ihmalkâr, dikkatsiz, güvenlik politika ve talimatlarına riayet etmeyen veya istemeden hareket eden kişiler birer tehdit unsurudur. Kurum içinde güvenilir ve erişim yetkisi olan kullanıcıların ne zaman zarar verebileceklerini kestirmek zordur. CA Teknoloji Firması tarafından hazırlanan İçeriden Gelen Tehditler Raporunda (Insider Threat Report 2018) tehditlere ilişkin sonuçlar aşağıda maddeler halinde verilmiştir [55];

1) Kuruluşların % 90'ının içeriden gelen saldırılara karşı kendilerini savunmasız hissettikleri,
2) Risk faktörleri arasında kurumlarda % 37 oranında aşırı erişim yetkilerine sahip kişilerin olduğunu, hassas verilere erişebilen cihaz sayısının % 36 oranında olduğu,

3) Son bir yıl içerisinde kurumların % 53'ü içeriden gelen saldırıların daha sık yaşandığı,
4) Kurumların iç tehditlerin tespitine % 64, caydırıcılık yöntemlerine % 58, analiz ve ihlal sonrası adli tıpa %49 oranında odaklandıkları,
5) İçeriden gelen tehditleri caydırmak için en popüler teknolojilerin Veri Kaybını Önleme (DLP), şifreleme, kimlik erişim ve yönetim çözümlerinin olduğu,
6) Kurumların içeriden gelen tehditleri tespit etmek için Saldırı Tespit ve Önleme Sistemleri'ni (IDS), log yönetimi ve SIEM platformlarını kullandıkları,
7) % 30'un altında kurumun içeriden gelen saldırılara karşı savunma için resmi bir programa sahip olduklarını, % 50'sinin programları geliştirmeye odaklandıkları,
8) % 51 oranında yanlışlıkla / kasıtsız veri ihlalleri ve % 47 oranında kasten kötü niyetli ihmal edilmiş ve tehlikeye atılmış kimlik bilgilerinin olduğu,
9) İç tehditlere karşı % 50 veri tabanı, % 46 dosya sunucuları, % 39 bulut uygulamaları, % 32 ağ, % 25 mobil cihaz ve benzeri BT varlıklarının savunmasız olduğu,
10) Kazara içeriden gelen tehditlerin kaynağının % 56 zayıf / tekrar kullanılan şifrelerin, % 44 kilitsiz cihazların, % 44 kötü şifre paylaşımı uygulamasının ve % 32 güvenli olmayan kablosuz ağların olduğu raporda ifade edilmiştir.

İçeriden gelen tehditleri önlemek için; veri kaybı engelleme yazılımları kullanılmalıdır. Bu yazılımlar sayesinde sistem üzerindeki çalışanlara ait aktiviteler ve davranışlar izlenebilir. Çok faktörlü kimlik doğrulama politikaları uygulanmalı ve çalışanların rol ve sorumlulukları net bir şekilde belirlenmeli ve tanımlanmış rollere göre kimlik erişim yönetimi çözümleri kullanılmalıdır.

4.6.9. Fiziksel Manipülasyon / Hasar / Hırsızlık / Kayıp

Yangın, sel vb. gibi doğa olaylarından kaynaklı tehditler, çeşitli etkenler nedeni ile meydana gelebilecek hasarlar, içeriden veya dışarıdan kaynaklanabilecek veri ve cihaz hırsızlığı olaylarıdır.

Bu tür saldırılardan korunmak için; uç noktalardaki cihazlar, ağlar, bulut hizmetleri vb. verilerin muhafaza edildiği ve kullanıldığı sistemler şifre ile korunmalıdır. Hassas

verilerin işlendiği ve saklandığı sistemlerin bulunduğu ortamlara erişim sınırlandırılmalıdır.

4.6.10. Bilgi Sızıntısı (Information Leakage)

Bilgi sızıntısı en önemli siber tehditlerden biridir. Veri sızıntısı/kaybı usb bellekler, ekran görüntüsü alma, ağ üzerinden veriyi taşıma, şifreli yollarla başka sitelere aktarma ve e-posta ile yollama girişimi gibi daha birçok yöntemle yapılabilmektedir. İnsan hataları, teknik yetersizlikler, hatalı sistem yapılandırmaları, kod hataları, güvenlik açıklıkları birer tehdit unsurudur ve saldırganlar bu kusurlardan yararlanırlar.

Bilgi sızıntısını engellemek için; çalışanlara farkındalık eğitimleri verilmeli, güvenlik politikası hazırlanmalı, riskler önceden belirlenmeli ve politikalar veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir. Güncel olmayan veriler imha politikalarına uygun yok edilmelidir. Veri sorumluları ile veri işleyenler arasında sözleşme yapılmalıdır. İstemeyen verinin dışarı çıkmaması için son kullanıcı sistemleri üzerinde ve ağ giriş/çıkış noktalarında veri kaybı/sızıntısı önleme (DLP) çözümü, anti virüs, anti-spam, güvenlik duvarı ve ağ geçidi kullanılması önemlidir. Yazılım güncellemeleri ve yama yönetimi düzenli olarak yapılmalı, güçlü şifre ve politika kullanılmalı, güvenlik zafiyetleri tespit edilmeli ve tüm kullanıcıların sistem üzerindeki işlem hareketlerinin düzenli olarak kayıt (log) altına alınmalıdır. David McCandless tarafından kurulan “Information is beautiful” veri ihlalleri istatistiğinde; 2016 yılında en az 500 milyon kullanıcı hesabının veri ihlalinden etkilendiği ve üç (3) milyar Yahoo hesabının etkilenerek tarihteki en büyük veri ihlali olarak kayıtlara geçtiği ifade edilmiştir [56].

4.6.11. Kimlik Hırsızlığı (Identity Theft)

Kimlik hırsızlığı, kişisel ve hassas bilgileri ele geçirmek için saldırganların kullanıcıları aldatması suçudur. Kimlik hırsızları daha çok kimlik numarası, banka kartı bilgileri, sosyal güvenlik numaraları gibi kişisel bilgileri ele geçirir ve bu bilgileri yasa dışı olarak kullanırlar. Kimlik hırsızlığı saldırılarında genellikle sosyal mühendislik yöntemleri kullanılır. Çevrim içi ortamlarda, sosyal ağlarda saldırganlar kurbanları hakkında bilgi toplarlar. 2017 yılında Javelin Strateji ve Araştırma

tarafından yapılan kimlik sahtekârlığı çalışmasında 15,4 milyon tüketici 16 milyar dolar zararla karşı karşıya kalmıştır[57].

Kimlik hırsızlığı saldırılarından korunmak için; güvenliğinden emin olunmayan web sitelerinde kişisel bilgiler kullanılmamalı, kaynağı bilinmeyen e-postalar açılmamalı, farklı hesaplarda farklı parola kullanılmalı ve sosyal medya hesaplarında kişisel bilgiler paylaşılmamalıdır.

4.6.12. Kripto Para Madenciliği (Cryptojacking)

Kripto para madenciliği, etkilenen cihazın gizlice para kazanmasını sağlayan kötü niyetli bir yazılımdır ve fark edilmeden uzun süreler hedef sistemin işlemci gücünü ve bant genişliğini sömürür [58].

4.6.13. Fidye Yazılımı (Ransomware)

Fidye yazılımı, cihazları kilitleyen, ekranını engelleyen veya diskte saklanan verileri şifreleyen kötü amaçlı programlardır. Kullanıcılara ekrandan ödeme detayları ile fidye talebi görüntülenir. Belirli bir miktar para ödenene kadar cihaza erişimi engellerler. Fidye yazılımlarının farklı çalışma teknikleri vardır. Fidye yazılımlarından bazıları tüm diski şifreleyerek kullanıcıların sisteme erişmesini, bazıları grafiksel ara yüzün kontrolünü ele geçirerek ekran görüntüsüne, bazıları ise diskte saklanan verileri şifreleyerek erişimi engellerler. Bu yazılımlar sıklıkla kimlik avı e-postaları aracılığıyla [59] gönderilerek güvenlik açıklıklarını istismar ederler. 2018 Sonicwall Siber Tehdit Raporunda, 2017 yılının en etkili Fidye Yazılım saldırıları arasında WannaCry, Petya & NotPetya, BadRabbit, Cerber ve Nemucod saldırılarının olduğu belirtilmiştir [60]. Bu saldırılardan WannaCry fidye yazılım saldırısı, 12 Mayıs tarihinde, Türkiye'nin de aralarında olduğu 150'ye yakın ülkede binlerce bilgisayara bulaşarak verileri şifreledikten sonra şifreyi çözmek için fidye talep etmiştir.

4.6.14. Siber Casusluk (Cyber Espionage)

Siber Casusluk, kavramlar kısmında daha detaylı tanımlandığı üzere; ticari, politik ve askeri kazanç elde etme düşüncesi olan yetkisiz kişilerce rakip devletlerin sistemlerine sızılması, gizli sır bilgi ve düşüncelerin çalınması için yürütülen faaliyetlerin tümü olarak tanımlanabilir.

4.7. Siber Saldırılara Karşı Mevcut Durum

Çalışma kapsamında farklı kurumlar tarafından uygulanmış siber güvenlik raporları, anketleri incelenmiş ve siber güvenliğin sağlanması konusunda önerilere yer verilmiştir. Cyber Security Breaches Survey 2016 Raporu'na göre, kurum yöneticilerinin %69'nda siber güvenlik fakındalığının olduğu ve sadece % 51'nin önlem aldığı, kurumların %29'nda güvenlik politikasının bulunduğu ve %10'nunda da kaza yönetim planının olduğu ifade edilmiştir. Kurumlarda saldırıların %68'inin virüs ve kötücül yazılımlardan, %32'inin ise kötü niyetli kurum çalışanlarından kaynaklandığını söylemektedir [61].

On bin kişiden fazla kişinin katılımı ile PwC tarafından gerçekleştirilen The Global State of Information Security Survey 2017 anketinde; internetten erişilebilen cihaz ve uygulamalar hakkında kurumsal güvenlik politikalarına uygun çalışma gerçekleştirilmesi ve kurum çalışanlarının eğitilmesi gerektiği ifade edilmiştir [62].

Global EY Şirketi tarafından gerçekleştirilen, 1400'den fazla katılımcının yer aldığı 21. EY Küresel Bilgi Güvenliği Anketine göre kurumların siber tehditlere karşı mevcut durumları raporlanmıştır. Anket sonuçlarında, tehditlerin belirlenerek savunma sistemlerinin geliştirilmesi gerektiği, kurumlarda güvenlik harcamalarının arttığı ve sıkça DDoS ve kimlik avı saldırıları ile karşı karşıya kaldıkları belirtilmiştir [63]. Ayrıca kurumlardaki tehditlere karşı en büyük savunmasızlıkların bilinçsiz çalışanlar, hatalı erişim yetkileri ve eksik güvenlik denetimlerinin olduğu belirtilmiştir. Ankette katılımcılardan %75'i kurumlarında siber güvenlik bilincinin oluşmadığını, %12'si saldırı tespit sistemlerinin bulunmadığını, %38'i de yeteri düzeyde kimlik denetimlerinin olmadığını ve katılımcıların %43'ü de olası bir saldırı durumunda bir iletişim stratejisi ve planına sahip olmadıklarını belirtmişlerdir. Ankete göre tehditlerin hedefindeki değerler çizelge 4.2'de ve kuruluşlara yönelik en büyük on (10) siber tehdit türü çizelge 4.3'de belirtilmiştir.

Çizelge 4. 2 Tehditlerin hedefindeki değerler.

Tehditler	**Oranları %**
Müşteri Bilgileri	17
Finansal Bilgileri	12
Stratejik Planlar	12
Yönetim Kurulu üyesi bilgileri	11
Müşteri Parolaları	11
Ar-Ge Bilgileri	9
M&A bilgisi	8
Fikri Mülkiyet	6
Patentsiz IP	5
Tedarikçi Bilgileri	5

Çizelge 4. 3 Kuruluşlara yönelik en büyük on (10) siber tehdit.

En Büyük 10 Siber Tehdit	**Oranları %**
Kimlik Avı (Phishing) Saldırısı	22
Malware	20
Siber Saldırılar (Bozma amaçlı)	13
Siber Saldırılar (Para Çalma)	12
Dolandırıcılık	10
Siber Saldırılar (IP Çalınması)	8
Spam	6
İç Saldırılar	5
Doğal Afetler	2
Casusluk	2

4.8. Türkiye'de Siber Güvenlik Çalışmaları

Son yıllarda meydana gelen ve sürekli şekil değiştiren siber saldırılar kurumları, şirketleri ve bilgisayar kullanıcılarını ciddi olarak tehdit etmektedir. Kişisel ve hassas verilerin gizlilik, bütünlük ve erişebilirliğinin güvence altına alınması, tehditlerin önceden tespit edilmesi ve bu tespitlere karşı önlem ve tedbirlerin alınması çok önemli hale gelmiştir. Siber güvenliğe ilişkin küresel çapta yürütülen faaliyetlerin dışında ülkemizde birçok çalışma yapılmış ve yapılmaya devam etmektedir.

4.8.1. Siber Güvenlik Kurulu

Ulusal Siber Güvenlik Çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar 2012 yılında yayımlanarak yürürlüğe girmiştir. Bu karar gereğince; Siber Güvenlik Kurulu oluşturularak Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiştir. Siber Güvenlik Kurulu'nun çalışma usul ve esasları Başbakanlık tarafından çıkartılacak yönetmelikle belirlenir.

Siber Güvenlik Kurulu'nun görevleri arasında; siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak ve kanunlarla verilen diğer görevleri yapmak yer almaktadır.

4.8.2. Siber Güvenlik Kurulu Toplantıları

Siber Güvenlik Kurulu'nun ilk toplantısı 21.12.2012 tarihinde yapılarak "Siber Güvenlik Kurulu'nun görevleri, çalışma usul ve esasları yönergesi" ve "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilmiştir. İkinci toplantısında 20.06.2013 tarihinde yapılan toplantıda Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) kurulduğu ve 15 Mayıs 2013 tarihi itibarıyla USOM'un faaliyet göstermeye başladığı bildirilmiştir.

4.8.3. Siber Güvenlik Stratejisi ve Eylem Planı

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" Siber Güvenlik Kurulu tarafından 21.12.2012 tarihli toplantıda kabul edilmiş ve Bakanlar Kurulu'nun 20.06.2013 tarihli ve 28683 sayılı kararı ile Resmi Gazetede yayımlanmıştır [64]. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amaçları arasında, kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet sunumunda kullanılan sistemlerin ve kritik sistemlerinin güvenliğinin sağlanması ve oluşan suçların adli makam ve kolluk kuvvetleri tarafından daha etkin araştırılmasının ve soruşturulmasının sağlanmasına yönelik bir altyapı oluşturulması yer almaktadır.

4.8.4. USOM ve Kurumsal Siber Olaylara Müdahale Ekibi

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı uyarınca ülkemizde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması

adına Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur. USOM, siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri yapmakta, kritik sektörlere yönelik siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlamaktadır.

Kurumsal SOME'lerin görevleri arasında; kurumlarına yönelik olası siber saldırılara karşı önlem alma veya aldırma, farkındalık çalışmaları düzenleme, savunma mekanizmaları kurma ve siber güvenliğe ilişkin teknik ve idari tedbirler konusunda öneri sunma vb. gibi faaliyetler yer almaktadır [65].

4.8.5. Siber Güvenlik Tatbikatları

Devlet kurum ve kuruluşlarının siber tehditlere karşı veya siber saldırılara maruz kalma durumlarında savunma yeteneklerinin ve aldıkları önlemlerin ne ölçüde yeterli olduğunu tespit etmek amacıyla siber güvenlik tatbikatları gerçekleştirilmektedir. Tatbikatlar sayesinde kurumlar güvenlik zafiyeti ve meydana gelebilecek riskleri tespit etme ve bu tehditlere karşı koordineli olarak karşı koyma, önlem alma gibi kabiliyet ve yeteneklerini birleştirme ve güçlendirme fırsatı bulurlar. Kurumlarımızın siber tehditlere karşı hazırlıklı olması, savunma yeteneklerinin tespit edilmesi, farkındalığın arttırılması amacı ile ülkemizde Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliğiyle (belirli aralıklarla) ulusal siber güvenlik tatbikatları düzenlenmektedir. Tatbikatlara bugüne kadar çok sayıda kurum katılmıştır. Bu tatbikatlar neticesinde elde edilen bulgular aşağıda listelenmiştir [32].

1) Bilgi Güvenliği Yönetim Sistemi (BGYS) eksikliği.
2) Sistem yöneticilerinin teknik konularda yetersizliği.
3) Saldırı tespit sistem ve süreçlerinin yetersizliği.
4) Sosyal mühendislik saldırılarına yönelik bilinç yetersizliği.
5) Güncel olmayan antivirüs programları.
6) Sistem yöneticilerinin güvenlik boyutunda yetersiz olmaları.
7) Kurum içi koordinasyon konusunda eksikliklerin olması.
8) Erişim kontrol politikasının bulunmaması.
9) Sistem planlama aşamasında güvenliğin göz ardı edilmesi.

10) Kablosuz ağlardan kaynaklanan risklerin bulunması.
11) İş sürekliliği planlarının eksikliği.
12) Port tarama saldırılarının tespit edilememesi.
13) Dağıtık Servis Dışı Bırakma saldırılarının (DDOS) olumsuz sonuçlar vermesi.
14) Web uygulamalarında açıklıkların bulunması.
15) Kayıt dosyalarının analizinin tam olarak gerçekleştirilememesi.
16) Yasal mevzuata ilişkin bilgi eksikliğinin bulunması.

4.8.6. Projeler

Uluslararası Telekomünikasyon Birliği'nin (ITU) ülkemizde temsilen üyesi olan Bilgi Teknolojileri ve İletişim Kurulu tarafından siber güvenliğin sağlanmasına yönelik çalışmalar yürütülmektedir. Uluslararası Telekomünikasyon Birliği, Telekomünikasyon Standardizasyon Sektörü (ITU-T) Çalışma Grubu 17'nin (SG17) birinci ve ikinci toplantısı 2013 yılının nisan ayı ile Ağustos ve Eylül ayları arasında, üçüncü toplantısı ise 2014 tarihinde İsviçre'nin Cenevre kentinde yapılmıştır [66].

4.8.7. ISO 27001 Standardı: Bilgi Güvenliği Yönetim Sistemi

Uluslarası denetlenebilir ve kurumun genel iş riskleri kapsamında etkinliği belirlemeyi, izlemeyi, iyileştirmeyi, gözden geçirmeyi, ihtiyaçları belirlemeyi amaçlayan ve ticari veya devlet kurumları tarafından kullanılmak üzere esnek yapıda tasarlanmış bir standarttır [67]. Üst yönetim tarafından desteklenen ISO 27001 Bilgi Güvenliği Yönetim Sistemi sayesinde bilgi varlıklarına erişim ve kurumsal saygınlık korunur, rekabet avantajı, iş sürekliliği ve farkındalık sağlanır, gereksiz iş yükü ve zaman kaybı azaltılır. ISO 27001, bilişim sektöründe faaliyet gösteren, uydu haberleşme ve altyapı işletmeciliği hizmeti veren, internet servis sağlayıcıları gibi sektörleri ilgilendirir. Petrol, elektrik, doğalgaz ve e-fatura verecek şirket ve birçok kuruluş ISO 27001 belgesi almak zorundadır.

4.9. Kurumlarımızda Sınır Güvenliği Sistemleri

Değişen tehdit karakteristiklerine, ihtiyaçlara uyum sağlayacak şekilde bilgi yönetimi, koruma, tespit /teşhis/takip, test, izleme, kayıt ve yeniden oynatma gibi özellikleri olan sistemlerdir.

4.9.1. Güvenlik Duvarı (Firewall)

Güvenlik duvarı, bilgisayar ağlarında, önceden tanımlanmış veya kurallar ve ilkelere dayanarak ağ üzerinde gelen ve giden trafiğini kontrol eden, oluşturulan filtreleme politikalarına göre veri transferine izin veren veya engelleyen yazılımsal veya donanımsal sistemlere denir. Bu araçlar iç ağ ile güvenilmeyen dış ağ arasında bir güvenlik duvarı oluşturur. Güvenlik duvarı ile güvenilir olmayan servislerin filtrelenmesi, sisteme kontrollü erişimin sağlanması, güvenlik zafiyetleri olan servislerin ağa girmesinin ve çıkmasının önlenmesi gibi birçok önleyici işlemler yapılabilir. Güvenlik duvarı teknolojileri, kurumların ağlarını dışarıdan saldırılara karşı korumak için sürekli gelişmektedir. Yapılarına göre donanımsal ve yazılımsal olmak üzere iki farklı firewall türü vardır. Yazılım tabanlı olanlar genelde istemci veya sunucu üzerindeki işletim sistemlerine kurulurlar. Donanım tabanlı olan güvenlik duvarı cihazları ise, özel donanımlar üzerinde çalışırlar.

4.9.1.1. Bütünleşik Güvenlik Cihazı (Unified Threat Management –UTM)

Anti-virüs, içerik filtreleme, saldırı tespit sistemi ve spam filtreleme kullanan çoklu sistemler yerine, günümüzde daha çok tüm özellikleri barındıran UTM cihazları yaygın olarak kullanılmaktadır. Bu cihazlar çoklu tehditlere karşı daha kapsamlı güvenlik sağlayabilmektedir.

4.9.1.2. Saldırı Önleme Sistemi (Intrusion Prevention System - IPS)

Saldırı önleme sistemleri (IPS), ağ trafiğini sunuculara gelmeden önce üzerlerinden geçirip inceleyen, denetleyen ve gerektiğinde saldırıları engellemeye yarayan sistemlerdir [68]. IPS, kaynak ve hedef arasındaki doğrudan iletişim yoluna yerleştirilir. Trafik üzerinde daha önce oluşturulmuş saldırı imzalarına uyan trafiği ararlar ve bulduklarında, paketi engeller, TCP bağlantısını sonlandırma gibi işlemler yaparlar.

4.9.1.3. Saldırı Tespit Sistemleri (Intrusion Detection Systems - IDS)

IDS, ağ trafiğini izler, analiz eder ve istenmeyen bir paket, zafiyet veya saldırı tespit ederse bunları kayıt altına alarak alarm üreterek yöneticiye bildirirler. IDS'ler, adli araç olarak geliştirilmiş yazılımsal ve donanımsal sistemlerdir. Genellikle güvenlik

duvarının hemen arkasında bulunur. Saldırı tespit sistemlerinin saldırı anında yöneticiye uyarı gönderme, zararlı paketleri bırakma, trafiği engelleme, bağlantıyı yenileme gibi birçok özelliği mevcuttur. IDPS teknolojilerinin bilgi toplama, kaydetme, algılama ve önleme farklı yetenekleri vardır. IDS sistemler host tabanlı ve ağ tabanlı olmak üzere iki türlüdür.

Özetle IDS, saldırıları tespit etmek için, IPS ise saldırıları önleme, durdurma üzerine geliştirilmiş yazılımsal veya donanımsal güvenlik sistemleridir [69]. Bu iki sistem bir arada kullanıldığında IDPS olarak tanımlama yapılmaktadır. IDPS sistemlerinin alarm/uyarı üretme, önem seviyesi belirleme, beyaz ve kara liste oluşturma vb. gibi özellikleri vardır [70].

4.9.1.4. Anti-Virüs / Anti-Malware / Anti-Spyware

Anti-virüs, Truva atı, tehlikeli web siteleri, fidye yazılımları gibi zararlı yazılımlara karşı koruma sağlar. Gelişmiş Anti-virüs mekanizmaları, ağ geçidindeki çok sayıda saldırıya karşı koruma sağlar. SMTP, POP3, IMAP, FTP ve HTTP gibi önemli protokolleri inceler. Virüslerin en çok yayıldığı e-mail, http ve ftp trafikleri antivirüs ağ geçidine yönlendirilir ve tarama işleminden sonra gerekli yerlere yönlendirilme yapılır. Bu sistemle dışarıdan gelecek olan virüsler engellenmiş olur. Sunucu bilgisayarları üzerine kurulacak virüs koruma yazılımları ve çalışanların sistemlerini kontrol edecek yazılımlarla kurumsal antivirüs çözümü sağlanmış olur. Bu sistemlerle istem dışı mailleri engellemek, içerdiği kelimelere ya da eklerine göre silme/arşivleme vb. işlemler yapılabilmekte kısaca mail yönetimi sağlanabilmektedir.

4.9.1.5. Uygulama Kontrolü

Uygulama kontrolü ile kullanıcıların kullanabilecekleri uygulamalar sınırlandırılabilmektedir. İnternet üzerinden kullanılacak servisler veya indirilecek dosyalar kontrol edilebilir. Kullanıcı bazlı engellemeler yapılabilir.

4.9.1.6. Web Filtreleme Çözümleri (URL)

URL filtreleme yöntemleri, kullanıcıların ve kurum çalışanlarının siber tehditlerden ve aynı zamanda zararlı yazılım ve oltalama saldırıları içeren sitelerden korunmasını sağlar. Kullanıcıların internet erişimlerinin güvenli bir şekilde yapılabilmesi için vekil

sunucu görevini üstlenir. Sahip oldukları üstün inceleme ve tespit motorları, raporlama arabirimleri ve bildirimleri sayesinde, anlık olarak kullanıcı erişimleri denetlenebilmektedir. Bant genişliği kontrolü, uygulama kontrolü, anti virüs kontrolü, SSL sonlandırma gibi çeşitli kontroller yapılabilmektedir.

4.9.2. VPN

VPN, İngilizce Virtual Private Network' ün kısaltmış şekli ve Türkçe olarak Sanal Özel Ağ anlamına gelmektedir. Yetkilendirilmiş uzak kullanıcıların yerel ağa güvenli bir şekilde bağlanmasını sağlayabilir. Kurum ve işletmeler güvenlik duvarı üzerinde uzak erişim VPN yapılandırılarak mobil kullanıcılar için güvenli erişim sağlarlar [70].

4.9.3. Veri Sızıntısı Engelleme Sistemleri (DLP)

DLP, birbirlerinin yerine de kullanılabilen "data loss" prevention ya da "data leak" prevention sözcüklerinin kısaltması olup veri sızıntısı önleme, veri kaybı önleme anlamlarına gelmektedir. Mobil çalışanlar, kurum içi yetkili kullanıcılar, Hacker ve diğer dış aktörlerin kötü niyetli veya kazara sebep olduğu veri sızıntılarını önlemek için kullanılan sistemlerdir. Hassas verilerin yetkisiz kullanımı, iletiminin izlenmesini ve korunmasını amaçlar. Birtakım kurallar ile ağ trafiğini gözetler, eposta sunucusuyla entegre çalışır ve kullanıcı bilgisayarında kurallar çerçevesinin dışına çıkılmamasını denetler.

4.9.4. Sayısal İmza

Sayısal İmza kavramı Türkiye'de 15.01.2004 tarihli 5070 sayılı Elektronik İmza Kanunu ile Elektronik İmza (E-İmza) olarak isimlendirilmiş ve bu adla hukuki statü kazanmıştır. Bir kullanıcı, sunucu ya da hosttan gönderilen bilgilerin kesinlikle o kuruma veya kişiye ait olduğunu doğrulayarak, verinin başkası tarafından yollanmadığını garanti eden dijital sertifikadır.

4.10. Zafiyet Analizi ve Sızma Testleri

Zafiyet analizi, sistemler üzerindeki güvenlik açıklarının belirlenmesi için gözden geçirilme süreci olarak tanımlanabilmektedir.

Sızma testleri, teknik olarak saldırganların istismar etmek için yararlanabileceği zafiyetleri ve açıklıkları bulmak için “içeriden” veya ”dışarıdan” detaylı bir şekilde bilgi varlıklarının analiz edilmesi ve incelenmesidir [72]. Sızma testleri ile güvenlik kusurları, zafiyetler ve ihlaller tespit edilerek kurumların mevcut güvenlik durumu belirlenir. Böylece zayıf noktalara yönelik doğru güvenlik yatırımlarının yapılmasına imkân sağlar. Sızma testleri ile kritik sistemler üzerindeki yanlış yapılanmalar bulunur, IEC/ISO 27001, PCI DSS, COBIT vb. gibi bilgi güvenliği sertifikaları ve politikalarının gereksinimleri test edilir.

4.10.1. Test Kılavuzları

OSSTMM, OWASP, ISSAF, NIST ve PTES olmak üzere kabul görmüş uluslararası test kılavuzları vardır. Bunlardan; OSSTMM (The Open Source Security Testing Methodology Manual) kılavuzu, uluslararası kabul görmüş açık kaynaklı güvenlik test metodoloji kılavuzudur. Gerçek güvenlik doğrulaması için tasarlanmış olan bu kılavuz, her denetim türüne uygulanabilir testler, etik saldırılar, güvenlik değerlendirmeleri, güvenlik açığı değerlendirilmeleri, kırmızı takım vb. gibi detaylar içerir [73]. OSSTMM, fiziksel güvenlik, kablosuz güvenlik, telekomünikasyon ve veri ağları testlerini, uyum yönetmeliği, STAR ile raporlama bölümlerini içeren bir kılavuzdur [74].

OWASP (Open Web Application Security Project), web uygulama açıklıkları için alınabilecek önlem ve iyileştirmeler konusunda rehberlik hizmeti veren test kılavuzudur. Uygulama güvenliği konusunda yazılım araçları ve bilgi tabanlı belgeler sunmaktadır.

ISSAF (Information Systems Security Assessment Framework), OWASP gibi aktif bir topluluk değildir fakat kapsamlı sızma testi kaynağıdır. ISSAF, kaynak kod denetimi, sosyal mühendislik, kayıt izleme ve denetim, proje yönetimi, teknik kontrol, risk değerlendirme metodolojisi, şifre güvenliği, şifre kırma stratejileri, güvenlik duvarı, antivirüs, kablosuz güvenlik, saldırı tespit sistemi ve VPN güvenlik değerlendirmesi, sızma test laboratuvarı tasarımı vb. benzeri alanları kapsamaktadır [74].

NIST, ABD ekonomisini ve kamu refahını destekleyen bir kılavuzdur. Ulusal Standartlar ve Teknoloji Enstitüsü'ndeki (NIST) tarafından yayınlanan NIST SP800-115 (Bilgi Güvenliği Test ve Değerlendirme Teknik Kılavuzu), teknik anlamda bilgi güvenliğini test ve yöntemlerini planlama, yürütme, analiz stratejileri geliştirme, gözden geçirme teknikleri, güvenlik açıklığı değerlendirmeleri gibi konularında kurumlara yardımcı olacak önemli referans kaynaklarındandır [72].

PTES, öz sözleşme, istihbarat toplama, tehdit modelleme, zafiyet analizi, istismar süreci, sömürme ve raporlama gibi 7 ana bölümden oluşan açık kaynak proje sızma testi yürütmek için hazırlanmış bir rehberdir [75].

4.10.2. Sızma Testi Türleri

Sızma testini yapmadan / yaptırmadan türü belirlenmelidir. Hedef sistem hakkındaki bilginin çeşitliliğine göre sızma testleri siyah kutu, beyaz kutu ve gri kutu testleri olmak üzere üçe ayrılır.

Siyah kutu testinde testi gerçekleştirecek olan kişiler hedef sistem hakkında önceden herhangi bir bilgiye sahip olmazlar. Kara kutu testine uzaktan penetrasyon testide denir. Testi gerçekleştiren kişi güvenlik açıklıklarını ortaya çıkarabilmek için saldırganların kullandığı tekniklere benzer şekilde yöntemler kullanırlar.

Beyaz Kutu testinde, ağ hakkında gereken bilgiler verilerek içeriden bir kişinin sistemdeki açıkları kullanması sonucunda nelerin yapılabileceği görülür. Teste tabi tutulacak IP aralıkları, ağ topolojisi, sunucular, servisler, sunucu üzerinde tanımlı kullanıcı adı ve parolaları vb. gibi bilgiler test yapacak kişiye verilir. İç tehdit aktörlerinin (çalışan, emekli, işten ayrılmış vb.) sahip oldukları şifre, parola, ağ yapısı gibi bilgileri ile kurumu hedef alması durumunda neden olabilecekleri zararın tespit edilmesi için beyaz kutu testleri gerçekleştirilmektedir.

Gri kutu sızma testleri, beyaz kutu sızma testleri ile siyah kutu sızma testleri arasında yer alan bir sızma metodudur. Beyaz kutu ve siyah kutu test türleri birlikte kullanıldığında daha güçlü bir bakış açısı sağlar ve testçilerin kamuya açık bilgileri

daha hızlı elde etmeleri için tercih edilen bir yöntemdir [76]. Testi gerçekleştirecek olan kişi sistem hakkında bilgilendirilir fakat bu bilgi detaylı değil yüzeyseldir.

4.10.3. Sızma Testi Aşamaları

Sızma testini bir standarda kavuşturmak için 2010 yılında oluşturulan Penetration Testing Execution Standard (PTES) standardında sızma testleri yedi (7) ana aşama olarak belirlenmiştir.

1) Katılım Öncesi Etkileşim (Pre-engagement Interactions)

Teste tabi tutulacak sızma testi türü, IP aralıkları, sistemlerin tipi gibi detaylar belirlenir. İşin kapsamı, testin türü, testin gerçekleştirileceği sistemlere ait IP, domain vb. gibi bilgiler, test tarihi ve saati gibi bilgilerin belirlenmesi gerekir.

2) İstihbarat Toplama (Intelligence Gathering)

Hedef sistem hakkında domain, IP aralıkları, kullanıcı profilleri, domain ve subdomain alan adları, servisler, ağ yapısı gibi bilgiler için web üzerinden bilgi toplanır. Beyaz kutu testlerinde bilgi toplamaya ihtiyaç duyulmaz çünkü gerekli olan tüm bilgiler güvenlik uzmanına verilir. Aktif ve pasif bilgi toplama işlemleri ile hedef sistem hakkında detaylı bilgilere ulaşılır. Pasif bilgi toplama işleminde, teste tabi tutulan kurum hakkında internet üzerinde yer alan bilgilere erişilmeye çalışılır. Bu işlem gerçekleştirilirken herhangi bir sisteme veya sunucuya ulaşılmasına gerek yoktur. Aktif bilgi toplamı işleminde ise, teste tabi tutulan kuruma ait IP adresleri elde edilebilmektedir. Özel metotlar ve araçlar kullanılarak IP adresleri üzerinden çeşitli bilgi elde edilebilmektedir.

3) Tehdit Modelleme (Intelligence Gathering)

Ağ ve sistem alt yapısındaki cihazların açık portlarının ve açık servislerinin tespit edilmesi için yapılan bilgi toplama ve tarama aşamasıdır. Bazı kaynaklarda "Ağ Haritalama" olarak ta ifade edilmektedir. VPN, firewall, IPS cihazlarının belirlenmesi, işletim sistemlerinin belirlenmesi, versiyonlarının belirlenmesi ve ağ haritasının çıkarılması gibi işlemleri kapsar.

4) Zafiyet Analizi (Vulnerability Analysis)

Çeşitli zafiyet tarama araçları veya manuel olarak kritik sistemler üzerindeki güvenlik açıklıklarının ortaya çıkarılması aşamasıdır. Bu süreçte hedef sisteme zarar vermeyecek taramalar gerçekleştirilir.

5) İstismar (Exploitation)

Penetrasyon sürecidir. Çeşitli metot ve zafiyet tarama araçları ile elde edilen güvenlik açıklıklarının istismar edilmesi sürecidir. Açıklık için uygun tarama aracı yok ise sıfırdan Exploit yazılır.

6) İstismar Sonrası (Post Exploitation)

Açıklıklar istismar edilerek sistem üzerinde bir şekilde yetkisiz erişim hakkı elde edilir. Daha sonra sızılan sistem üzerinde kalıcı hale gelme ve yetki yükseltme gibi işlemler gerçekleştirilir. Yetki yükseltme işlemi basit bir ifadeyle, standart bir kullanıcı hesabının root, administrator gibi tam yetkili bir kullanıcı moduna yükseltilmesi işlemidir. Bunun için çeşitli exploit denemeleri yapılır.

7) Raporlama (Reporting)

Yönetici raporu, kritik güvenlik açıklıkları ve alınması gereken tedbirler konusunda tavsiyeleri içeren dokümanlardır. Raporda, test ekibi, kontrol eden kişi, testin gerçekleştirildiği erişim noktaları, testin türü ve test işlemleri, risk seviyelerine göre tespit edilen açıklıklar ve alınması gereken önlemleri içeren bölümler yer alır. Doküman şifreli bir şekilde kuruma teslim edilir.

4.11. Bilişim Suçlarının Tespiti ve Dijital Delillerin İncelenmesi

Adli Bilişim, bilişim suçlarında kullanılan veya suçun hedefi olan bilişim sistemlerimin incelenmesi ve raporlanması işlemleridir. Adli bilişimin amacı; olay mahallinde delillerin zarar görmeden eksiksiz ve sağlam toplanmasını sağlayıp, daha sonra bu delilleri yazılım ve donanımları kullanarak inceleme, analiz ve raporlama yaparak adli makamlara sunmaktır. Bilgisayar sistemlerine yetkisiz erişim, sistemi bozma, bilgisayar sabotajı, dolandırıcılık, sahtecilik, hakaret, sosyal medya

hesaplarının ele geçirilmesi veya dinlenmesi, zararlı yazılımların bulaştırılması, yazılımların izinsiz kullanımı ve kurum içi yolsuzluk vb. gibi birçok suçta kullanılan delillerin bulunarak ilgili adli makamlara verilmek üzere raporlanması işlemlerini de kapsar. Hukuki mevzuat açısından Türk Ceza Kanunu'nda madde 243 ile yetkisiz erişim ve sisteme girme, madde 244 ile verileri engelleme, bozma, değiştirme ve yok etme ve madde 245 ile kredi ve banka kartlarının kötüye kullanılması suç olarak düzenlenmiştir.

4.11.1. Dijital Delil Olabilecek Bulgular

Bilişim sistemlerinden elde edilebilecek ve delik oluşturabilecek bulgular arasında silinmiş dosyalar, görüntülü veya sesli görüşme kayıtları geçmişi, zararlı programlar, gizli ve şifreli dosyalar, fotoğraflar, video görüntüleri, kamera kayıtları, ziyaret edilen internet siteleri, haritalar, Word, Excel vb. gibi dosyalar yer almaktadır.

4.11.2. Dijital Delillerin Bulunduğu Yerler

Bilgisayarlar, yazıcı, tarayıcı, akıllı telefon, dijital kamera ve avuç içi bilgisayarlar, CD/DVD'ler, sabit ve taşınabilir diskler, hard disk ve ram vb. gibi bilgisayara bağlı donanımlar, SIM, smart ve hafıza kartları, video kaydediciler, dijital kamera ve fotoğraf makineleri, firewall, dongle, modem ve telesekreter vb. gibi yerlerde bulunurlar.

4.11.3. Adli Bilişim Süreci ve Yöntemler

Elektronik bulguların bir hukuki delile dönüştürülme süreci belli prosedürleri takip eder. Sırası ile delillerin korunması, elde edilmesi, incelenmesi, analizi ve raporlanması safhaları vardır. Laboratuvar çalışması safhalarında yazılımsal ve donanımsal imaj alma işlemleri, disk yazma ve koruma işlemleri, hash işlemi ve analiz işlemleri, gizlenme yöntemleri ve veri kurtarma işlemleri gerçekleştirilir. Delillere müdahalede ise imaj işlemleri için plan yapılması, kullanılacak donanım ve yazılımların hazırlanması, personel ve olay yeri güvenliği, imaj alınacak ortamın sağlanması, yapılan her işlemin fotoğraf ve video kayıt ile görüntü kaydının yapılması ve tüm işlemlerin detaylı bir şekilde tutanak tutulması sırası ile yapılacak müdahale önceliklerdir.

5. LABORATUVAR ALTYAPISININ OLUŞTURULMASI

Tüm dünyada siber güvenliğin önemi her geçen gün daha fazla artmakta, ulusal güvenliğin en yeni sorunu olarak gündemde yerini almıştır. Uluslarası platformlarda bilgi ve iletişim teknolojileri casusluk, saldırı ve savunma aracı olarak kullanılmaya başladı. Siber güvenlik, şirketler, organizasyonlar ve hükümetler için önemli konu haline gelmiştir. Hassas ve gizli verilerin saklandığı ve işlendiği kritik sistemler üzerindeki zafiyetlerin, yeni güvenlik açıklıklarının, hukuki boşlukların keşfedilmesi ve bu açıklıkların içeriden veya dışarıdan birtakım saldırgan kişi veya gruplar tarafından istismar edilmesi, kurumları ve şirketleri maddi, manevi, güven ve itibar kaybına maruz bırakmaktadır.

Günümüz koşullarında siber tehditlere karşı kurumlarımız kritik altyapılarını korumak amacıyla ağ yapıları üzerinde meydana gelen trafiği denetlemek, zararlı aktiviteleri tespit etmek için firewall sistemlerine büyük bütçeler ayırmaktadırlar. Güvenlik duvarı, internet bağlantılı birkaç uçtan oluşan ağa sahip kurumlar için çok önemlidir. Fakat güvenlik duvarı ağın en başında düzgün şekilde ayarlanmamışsa, birden fazla giriş noktası oluşturulmuş olur ve bazı tehditler tespit edilemez. Ayrıca üretici firma veya tecrübesiz BT çalışanlarının yanlış yönlendirmeleri yüzünden birçok kez hatalı yatırımlar yapılabilmekte ve neticesinde yazılımsal, sistemsel ve fiziksel güvenlik açıklıkları ortaya çıkabilmektedir. Yine birçok doğru yapılan güvenlik yatırımlarında da firewall üzerinde oluşturulan kurallardaki hata, eksiklik, yanlış yapılandırma, performans tabanlı sorunlar, yanlış güvenlik topolojisi, WAF/IPS sistemlerinin kontrol edilmemesi gibi hatalar sistemlere doğru istenmeyen bağlantıların yapılmasına yol açmaktadır.

Kurumlara yönelik gerçekleştirilen güvenlik denetimlerinde güvenlik açıklıklarına sıkça neden olan unsurlar arasında güncelleştirme problemleri, zayıf veya parolasız kullanılan ağ bileşenleri, domain politikalarının yetersizliği, firewall, IDS, IPS vb. gibi güvenlik cihazlarının yönetimindeki yetersizlikler, uygulamalardaki tasarım ve kodlama eksiklikleri, ağ tasarımındaki eksiklikleri yer almaktadır [77].

Bilişim sistemlerini kötü amaçlı kullanımlardan korumak, başarılı başarısız giriş denemelerini görmek için kurumlar standart saldırı önleme sistemleri kullanırlar. Fakat IDS'ler, üzerlerinden geçen her paketi denetledikleri için aşırı trafiğin artmasına neden olurlar ve eşik değeri aşıldığında sistem üzerinden geçen paketleri denetleyemez duruma gelirler. Günlük kayıtlarının ve uyarıların fazlalığı nedeni ile sistem yöneticileri incelemeye zaman bulamazlar. Dolayısıyla gerçek saldırıları da göremezler. Uyarıların sayısının düşürülmesi için kötü niyetli aktivitelerin listesinin doğru yapılması, risk seviyelerinin belirlenmesi ve ona göre uyarı ayarlarının doğru oluşturulması gerekir. Tehlikeli trafiğin ağ üzerinden geçişine ve zararlı web sayfalarının erişimine izin vermeyen güvenlik duvarlarının çoğu kez güvenli web sayfalarını da tehlikeli zannederek yanlışlıkla engellediği görülmektedir. Ağa giren ve çıkan tüm veri paketlerini kontrol ettiği için çok fazla işlem gücü kullanmaktadır ve bu nedenle çoğu kurum güvenlik duvarı üzerindeki çoğu güvenlik özelliğini devre dışı bırakarak filtrelerin yoğunluğunu düşürürler. Fakat çok fazla filtre özelliği devre dışı bırakılır veya devreye alınırsa ya kritik sistemler tehditlere karşı savunmasız kalır ya da uygunsuz şekilde engellenen içeriklerle karşılaşılır. Özetle, güvenlik duvarı filtrelerinin seviyesi, filtre yoğunluğu, risk seviyeleri, uyarı kriterleri gibi birçok ayarlama sistem yöneticileri veya kişisel kullanıcılar tarafından yapılandırıldığı için güvenlik mekanizmaları üzerinde çeşitli güvenlik açıklıkları çıkmaktadır.

Dolayısıyla güncel tehditlere karşı yüksek seviyede güvenliğin sağlanabilmesi için yazılımsal veya sistemsel güvenlik açıklıklarının ve zafiyetlerinin sızma testleri ile saldırganlardan önce tespit edilerek gerekli önlemlerin alınması ve adli bilişim analizleri ile meydana gelmiş suçlarla ilgili suça ait dellilerin toplanması, korunması, analiz edilmesi, raporlanması ve hukuki boyutunun değerlendirilmesi açısından kurumlar için siber güvenlik laboratuvarı altyapısının oluşturulması çok önemlidir.

Bu çalışmada belirtilen testlerinin güvenlik çalışanları tarafından kurumlarında gerçek sistemlere zarar vermeden uygulanabilmesi için öncelikle sanal makineler üzerinde belirtilen test yazılımları kurularak tecrübe kazanılmalıdır. Teorik olarak öğrenilen bilgiler sanal makine üzerinde pratiğe dönüştürülüp belli bir tecrübe kazanıldıktan kısa bir süre sonra gerçek sistemler üzerinde uygulanması daha yararlı olacaktır.

Bu bağlamda; laboratuvarda işletim sistemlerinin sanallaştırılması için VMware Workstation, CISCO imajlarının sanallaştırılması için GNS3, ağ içerisinde kullanılacak ağ anahtarlarının sanallaştırılması için WMware Workstation yazılımında bulunan sanal ağ anahtarları kullanılabilir.

VMware Workstation üzerinde oluşturulan sanal makineler üzerinde ağ bağlantıları yapılandırılarak IP aralıkları belirlenmelidir. Daha sonra hedef sistemlere yönelik çeşitli tehdit denemelerinin uygulanabilmesi için Backtrack, Kali Linux vb. gibi farklı işletim sistemleri olan farklı birkaç saldırı makinesi kurulmalıdır. Bu işletim sistemlerinin kurulumu, "iso" veya ".vm" uzantılı imajlar aracılığı ile gerçekleştirilebilmektedir. VMware sanallaştırma yazılımları ile kurulan sanal makineler GNS3 ile ağa dâhil edilebilir. Dış ağdan gerçekleştirilecek olan test senaryolarında kullanılmak üzere yönlendirici sanal makine yani ağ cihazı kurulmalıdır. Bu makine üzerine de Windows 7 ve benzeri bir işletim sistemi kurulabilir. İşletim sistemi kurulduktan sonra karmaşık ağları simule etmek, Cisco yönlendirici imajını sanallaştırmak için açık kaynak kodlu GNS3 veya benzeri grafiksel ağ yazılım emülatörü kullanılmalıdır.

Sanal ağ içerisinde OWASP, Metasploitable vb. gibi dağıtımlar web sunucusu olarak, Freebsd, Pfsense ve Smoothwall gibi açık kaynak kodlu dağıtımlar güvenlik duvarı sanallaştırmak için, SQL Server, Oracle gibi veritabanı yönetim sistemleri, saldırı tespit sistemi (IDS) olarak ta Snort ve benzeri güvenlik mekanizmaları kurularak kullanılabilir.

Adli bilişim ve sızma testi laboratuvarı, en az hard disk kapasitesi 500 GB ile 1 TB arasında, işlemci tipi I5 veya I7, sistem belleği 16 GB ile 32 GB arasında teknik özelliklere sahip bilgisayarlardan oluşmalıdır. Her bilgisayarda, Windows ve Linux tabanlı sistemler için adli bilişim incelemelerinde ve sızma testlerinde kullanılan lisanslı ve açık kaynaklı yazılımlar kurulu durumda olmalıdır.

5.1. Adli Bilişim Araçları (Forensics Tools)

Laboratuvarda adli inceleme kiti, veri depolama aygıtı, SIM kart okuyucu, sinyal kesici kılıf, sabit disk, flash bellek, sim kart adaptörü vb. gibi donanımlar dışında disk,

bilgisayar, mobil cihaz, delil imajları, web tarayıcılar, sosyal medya takibi vb. delil niteliğinde olacak cihazları inceleme yazılımları, imaj alma yazılımları bulunmalıdır. Laboratuvarda, dijital deliller toplandıktan sonra incelenerek elde edilen bulguların derlenmesi ve raporlanma işlemleri gerçekleştirilecektir. Bazı açık kaynak kodlu ve ticari adli bilişim araçları aşağıda incelenmiştir. Bunlar;

5.1.1. Sans-Sift

Ücretsiz olarak kullanıma sunulmuş adli inceleme aracıdır. SIFT Unix tabanlı işletim sistemi üzerinde çalışmaktadır. SIFT yazılımı ile: Windows, MAC, Solaris ve Linux tabanlı sistemler üzerinde inceleme yapmayı desteklemektedir. E01, dd ve AFF formatında sıkıştırılmış adli kopyalar üzerinde çalışabilmektedir. Şifre kırma/bulma, Malware analizi, ağ analizi, antivirüs taraması, ağ bağlantılarına ait paketlerin toplanması, geri dönüşüm kutusunun incelenmesi ve dosya kurtarma gibi birçok inceleme yapılabilmektedir. Ayrıca Phone, Blackberry ve Android cihazları üzerinde inceleme yapılabilmektedir. SIFT Workstation sürümüne https://digital-forensics.sans.org/community/downloads adresi üzerinden ulaşılabilir.

5.1.2. The Sleuth Kit (TSK) ve Autopsy

The Sleuth Kit yazılımı açık kaynak kodlu ve ücretsiz bir yazılımdır. Komut satırı üzerinden inceleme gerçekleştirilir. Disk görüntülerinin analizini ve dosya kurtarma işlemlerini yapmaya yarayan ve C kütüphanesinden oluşan bir koleksiyondur. Bu program içerisinde Autopsy isimli grafiksel arayüz bulunmaktadır.

Autopsy, akıllı telefon ve sabit diskleri analiz eden adli bir araçtır. Kolluk kuvvetleri, ordu ve firmalar tarafından bilgisayar sistemi üzerinden araştırma yapmak için kullanılır. Arayüz üzerinden komutlar kullanılmaktadır. Autopsy ile e-delil yönetimi, adli kopya bütünlüğü kontrol, kelime araması, web tarayıcılarından yer imleri, çerez ve geçmişi çıkarma vb. gibi uygulamalar kullanılabilmektedir.

Bu iki yazılım ile dd, EnCase ve AFF formatında adli kopyalar üzerinde inceleme yapılabilmektedir. NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, HFS ve ISO 9660 ve bunların türü olan dosya sitemlerini desteklemektedir. Kelime ve karakter araması, elektronik deliller üzerinden hash hesaplaması, zaman çizelgesi çıkarılması ve

steganography kontrolü yapılabilmektedir. Bu araç ile DOS bölümleri, BSD ve MAC bölümleri, Sun slice ve GPT diskleri incelenebilmektedir. Mac OS X, Solaris, FreeBSD, Cygwin, Windows ve Linux platformlarında çalışabilmektedir. The Sleuth Kit sürümüne http://www.sleuthkit.org adresinden ulaşabilir.

5.1.3. Oxygen Forensic

Oxygen programı ticari bir yazılımdır. Cep telefonlarından kanıt toplanmasına yardımcı olan bu yazılımdır. Oxygen yazılımı ile seri numarası, IMEI, OS vb. gibi cihaza ait tüm bilgiler toplanarak cep telefonlarındaki rehber, mesajlar, arama kayıtları, takvim, rehber ve rehberdeki fotoğraflar, belgeler, video, telefon kamerası kayıtları kurtarılabilmektedir.

Harita özelliği ile, tüm check-in'leri, harita aramalarını, ziyaret edilen web sitelerini ve bu durumda incelenen tüm cihazların coğrafi konum meta verilerini içeren mesajları bulur. Şifrelenmiş yedeklerin ve görüntülerin şifrelerini bulur, Android işletim sistemlerinde cihazların ekran kilidini atlar, dronlardan konum geçmişini ve medya dosyasını edinir. Ücretli olan sürümlerinde daha fazla özellik kullanıma sunulmuştur.

Android, Bada, Blackberry, IOS, MTK, Symbian, Preadtrum ve Qualcomm chipset sahip telefonlar, Windows Mobile 5/6, Windows 8 ve diğer akıllı telefonlardaki işletim sistemlerini desteklemektedir. Program Windows 7, Windows 8 veya Windows 10 işletim sistemlerinin 32-bit veya 64-bit versiyonlarında çalışabilmektedir. Oxygen Forensic programı USB dongle lisansı ve elektronik lisansı olmak üzere iki tür lisansa sahiptir. Detaylı bilgiye https://www.oxygen-forensic.com/en/ adresinden ulaşabilirsiniz. Adli görüntüleme araçları, disk görüntülerini en ince ayrıntısına kadar analiz etmek için kullanılan araçlardır.

5.1.4. FTK

FTK Imager, ücretsiz olarak sunulan bilgisayar kriminalistiği yazılımıdır. Bu yazılım, okunabilir şekilde delilleri toplayarak analiz yapılmasına izin verir. Yazılımın ana amacı veri depolama birimlerinin içeriğini görüntülemek ve birebir kopyasını almaktır. Diğer bir özelliği de erişilebilen medyaların MD5 veya SHA hash değerlerini üretebilmesidir. FTK Imager yazılımı ile ham halde (dd), E01 (Expert Witness,

Encase) ve AFF biçimlerinde birebir kopyalar alınabilmektedir. FTK Imager, FAT, NTFS, ext2, ext3 gibi dosyalama formatlarını desteklemektedir. Windows, Mac IOS, Linux, Unix, iphone, Blackberry ve Android platformlarında çalışabilmektedir. Bu yazılım sayesinde elektronik medyalar içerisinde bulunan dosyaların birebir ön izlemesi yapılabilir, kopyası alınabilir veya görüntülenebilir. Çöp kutusuna atılmış ve silinmiş dosyaları görüntülemek mümkündür.

5.1.5. Linux "dd"

Linux dd, çoğu Linux dağıtımında (Fedora, Ubuntu) varsayılan olarak yüklenen güçlü bir araçtır. dd aracı, cd, disket, sabit disk, zip, tape sürücü imajı alabilmeye yarar. Bir bölümü veya tüm sürücüyü yedekleme ve geri yükleme, veri formatlarını dönüştürme, sabit boyutlu dosyaları oluşturma ve disk üzerindeki verilerin imhası gibi fonksiyonları vardır. Linux platformlarında yüklü olarak gelir. dd, hem Linux hem de Windows işletim sistemlerinde kullanılabilmektedir.

5.1.6. IXImager

Linux tabanlı ve ücretsiz bilgisayar kriminalistiği yazılımıdır. Cihazın fiziksel olarak ön yüklemesini yapma, dosya sistemini yeniden yapılandırma ve bilgisayar sistemini yakalama gibi özellikleri vardır. Sadece belli şartları taşıyan kolluk kuvveti, ordu ve adli kurumların kullanımına sunulmuştur. NIST tarafından test edilmiştir. IXImager yazılımına https://www.xtremeforensics.com/solutions/e-forensics/iximager adresi üzerinden ulaşılabilir.

5.1.7. WireShark

Ağ trafiğinin, bir grafik arayüz üzerinden izlenmesini sağlayan, ücretsiz ağ adli analiz aracıdır. Uygulamanın kurulu olduğu bilgisayar üzerinden anlık network trafiği izlenebileceği gibi, Wireshark daha önce kaydedilmiş dosyaların incelenmesi amacı ile de kullanılabilir. Ağ üzerindeki tüm aktiviteleri incelemek için kullanılır. Kamu kurumları ve şirketler tarafından yaygın olarak kullanılmaktadır. Çevrim içi ve çevrim dışı analiz etme imkanı vardır. Kerberos, ISAKMP, IPsec, SSL / TLS, WPA / WPA2 ve WEP dahil olmak üzere çeşitli protokoller için şifre çözme işlemini destekler. Elde edilen veriler CSV, XML formatında dışa aktarılabilir. Windows, Solaris, Linux,

FreeBSD, Mac OS ve NetBSD ve platformlarını destekler. WireShark sürümleri, https://www.wireshark.org/#download adresi üzerinden indirilebilir.

5.1.8. Network Miner

Ağ trafiğini yakalayan, saldırı bilgisayarlarını araştıran ve yakalanan trafikteki dosyaları toplayan ve ayıklayan ücretli ve ücretsiz ağ adli analiz aracıdır. Ana bilgisayar adlarını, oturumları, açık portları ve işletim sistemlerini tespit etmek için ağ üzerinde trafik oluşturmadan paketleri yakalayan pasif bir ağ dinleyicisi olarak çalışır. PCAP dosyalarını ayrıştırarak çevrim dışı analiz yapılmasına olanak sağlar. Windows 7/8/10, Linux, Mac OS X ve FreeBSD platformlarını desteklemektedir. Network Miner sürümlerine https://www.netresec.com/?page=networkminer adresinden erişilebilir.

5.1.9. Xplico

Uygulama trafiğini internet trafiğinden çıkarabilen açık kaynak kodlu, ücretsiz ağ adli analiz aracıdır. http, Imap, Pop, Sip, Smtp, Udp ve Ipv6 protokollerini destekler. Verileri Mysql veya SqLite veri tabanı olarak verir. Birden fazla kullanıcı tarafından aynı anda erişime izin verir. Kali Linux, Back Track ve BackBox vb. gibi dağıtımlarda kurulur. 32 ve 64 bit versiyonu https://www.xplico.org/download adresi üzerinden indirilebilir.

5.1.10. Magnet Ram Capture

Magnet Forensic tarafından sağlanan bilgisayarların fiziksel hafızasını yakalayabilen ücretsiz bir araçtır. Elde edilen veriler Raw formatında dışa aktarılabilir. RAM kanıtlarını, ağ bağlantılarını, kayıt defteri bilgilerini, şifresi çözülmüş anahtar ve dosyaları, kullanıcı adlarını ve şifrelerini içerir. Windows XP/Vista/7/8/10 ve diğer 2003/2008/2012 platformlarını desteklemektedir. Magnet Ram Capture sürümlerine https://www.magnetforensics.com/resources/?cat=Free%20Tool adresi üzerinden erilebilir.

5.1.11. Memoryze

Disk üzerindeki Rootkit tarafından yüklenenlerde dâhil olmak üzere tüm yüklenen ve kötü niyetli aktiviteleri keşfetmeye yarayan bir araçtır. Bellekten görüntüleri alabilir ve analiz edebilir. Sistem belleğinin görüntüsünü oluşturma, bellekteki sürücülerin görüntüsünü diske oluşturma ve belleğe yüklenen sürücüleri belirleme gibi anahtar özellikleri mevcuttur. Windows 8/Server 2012 platformlarını desteklemektedir.

5.1.12. FAW

Web siteleri üzerinden sayfaları almaya yarayan tarayıcıdır. Bilgisayar dosyalarını görüntüleme ve düzenleme, ses/video çekimi, IP adresini alma ve görüntülenmekte olan web sayfalarındaki resim dosyalarını çıkarma gibi özelliklere sahiptir. Zararlı yazılımların tespitinde web sitesi üzerindeki JavaScript ve CSS vb. gibi dosyaları yakalayabilir. Windows 7/8/8.1 ve 10 platformlarını destekler. FAW tarayıcısı https://en.fawproject.com/download/ adresi üzerinden indirilebilir.

5.1.13. Volatility

Volatility, açık kaynak kodlu ücretsiz adli bilişim yazılımıdır. Uçucu bellek (RAM) adli analizi için geliştirilmiş ve RAM'da bulunan delilleri ve Malware analizi yapmayı sağlar. RAM bellek dökümlerini almak, dijital bulguları analiz etmek için kullanılır ve işlem listelerini, ağ bağlantılarını, açık portları, önbelleğe alınmış anahtarları ve RAM'de tutulan daha birçok veriyi listeler. 32 ve 64 bit Windows 7/8/10 ve Vista, Windows Server 2012 (64 bit), Linux ve Mac OSX platformlarını desteklemektedir. Volatility sürümüne https://www.volatilityfoundation.org/releases adresi üzerinden ulaşılabilir.

5.1.14. EnCase

Windows tabanlı ücretli bir yazılımdır. EnCase, çoğu dosya sistemlerini tanıyan, birçok imaj formatı ile uyumlu ve RAID sistemlerini desteklemektedir. EnCase yazılımı, birebir kopya alma ve saklama fonksiyonlarından anahtar sözcük arama ve basit anlamda veri kurtarma fonksiyonlarına kadar sabit disk içerisinde byte seviyesinde birçok analiz işlemi yerine getirebilmektedir. Genellikle hard disk, taşınabilir medya, akıllı telefonlar, tabletler vb. aygıtlar için inceleme çözümleri sunar.

Yereldeki sabit disk, hafıza kartı ve hafızanın anlık görüntüsünü sunar ve imajlarının alınmasına imkân tanır. Sayısal delil toplanması, görüntüleme, analiz ve kanıtların raporlanması için kullanılmaktadır.

EnCase yazılımı ile imaj alınması esnasında delillerin imaj dosyalarına herhangi bir müdahale yapılmaz. Yazılımın E01, Ex01, L01 ve Lx01 olmak üzere farklı sıkıştırılmış imaj formatları bulunmaktadır. İmaj dosyaları ham şekilde RAW formatındadır. Genellikle adli incelemelerde hızlı imaj alabilmek için RAW formatı tercih edilir ve sonrasında saklanmak üzere daha az yer kaplaması için FTK Imager ve benzeri yazılımlar ile sıkıştırılmış E01 formatına dönüştürülebilir. FAT, NTFS, ext3, ReiserFS, UFS ve JFS gibi dosya sistemi formatlarını okuyabilme, raw (dd), Vmware, EnCase (.EO1) ve Safeback gibi disk görüntü dosyalarını okuyabilme ve farklı dosya formatlarını görüntüleme özellikleri bulunmaktadır.

İncelemelerin kaydedildiği dosya olan case dosyası içerisinde delillerin işletim sistemi içindeki yeri, Bookmark bilgileri, adli incelemeye ait bilgiler, arama sonuçları, sınıflandırmalar, hash değeri analizleri, dosya imza sonuçları vb. gibi çeşitli bilgiler yer alır.

5.1.15. Forensic Explorer

Forensic Explorer ticari adli analiz aracıdır. Gizli sistem dosyaları, silinmiş dosyalar, disk boşluğu vb. gibi mevcut tüm verilere erişebilmektedir. Windows 7/8/8.1 veya 10 işletim sistemlerini destekler. Apple DMG, DD veya RAW, E01, L01, ISO ve Vmware gibi formatları desteklemektedir. Forensic Explorer sürümüne http://www.forensicexplorer.com/ adresi üzerinden ulaşılabilir.

5.1.16. Helix 3 Pro

Adli incelemeler için geliştirilmiş ticari bir üründür. İnternet altyapısı, veri paylaşımı ve taciz gibi zararlı faaliyetleri açığa çıkaran bir programdır. İnternet kullanımını gözden geçirme, tüm ağı inceleme, ekran görüntüsü yakalama, anahtar kaydı ve raporlama özellikleri vardır. Windows, Linux ve Mac OSX platformlarını desteklemektedir. Helix 3 Pro sürümüne http://www.e-fense.com/contact-us.php adresi üzerinden ulaşılabilir.

Yukarıda belirtilen adli bilişim araçları, kullanım durumuna, desteklediği işletim sistemine, inceleme alanına ve özelliklerine göre çizelge 5.1'de kategorilendirilmiştir.

Çizelge 5.1 Adli Bilişim Araçları

Araçlar	**Kullanımı**	**İşletim Sistemi**	**İnceleme Alanı**	**Özellikleri**
Sans-Sift	Ücretsiz	Linux	Windows, MAC, Solaris ve Linux tabanlı sistemler.	Şifre kırma, ağ ve malware analizi, anti virüs taraması, ger dönüşüm kutularını inceleme vb.
The Sleuth Kit and Autopsy	Ücretsiz	Linux, Windows, Mac OS X, Solaris, FreeBSD ve Cygwin	Akıllı telefonlar ve sabit diskler. DOS, BSD ve MAC bölümleri	Kelime ve karakter araması, hash hesaplaması, zaman çizelgesi çıkarılması, steganography kontrolü vb.
Oxygen Forensic	Ücretli Ücretsiz	Windows 7,8 ve 10.	Mobil cihaz ve bileşenleri.	Cep telefonundaki rehber, telefon kamerası kayıtları ve fotoğraflar vb. gibi verilerin elde edilmesi.
FTK	Ücretsiz	Linux, Windows, Mac IOS, Unix, iphone, Android	Sabit disk, ağ sürücüsü, CD/DVD	Disk görüntülerini mikroskobik düzeyde analiz etmek.
Linux"dd"	Ücretsiz	Linux ve Windows.	Cd, disket, sabit disk ve zip vb.	Sürücü yedekleme, geri yükleme, veri format dönüştürme, disk üzerindeki verilerin imha edilmesi vb.
IXImager	Ücretsiz	Linux.	Bilgisayar ve bağlı sistemler.	Cihazların fiziksel olarak ön yüklemesi ve dosya sisteminin yeniden yapılandırılması vb.
WireShark	Ücretsiz	Linux, Windows, Mac OS, FreeBSD, ve NetBSD.	Ağ sistemleri ve kaydedilmiş dosyalar vb.	Anlık ağ trafiğinin izlenmesi, ağ üzerindeki aktivitelerin ve daha önce kaydedilmiş dosyaların incelenmesi vb.
Network Miner	Ücretli Ücretsiz	Linux, FreeBSD, Windows 7/8/10 ve Mac OS X.	Ağ sistemleri.	Ağ trafiğini yakalama, yakalanan trafikteki dosyaları toplama ve ayıklama, açık port ve işletim sistemlerini tespit etme vb.
Xplico	Ücretsiz	Kali Linux, Back Track ve BackBox dağıtımları.	Ağ sistemleri.	Uygulama trafiğini internet trafiğinden çıkarma ve elde edilen verileri MYSQL veya SQLITE veri tabanı olarak verme.
Magnet Ram Capture	Ücretsiz	Windows XP, Vista/7/8/10 ve Server 2003/2008/2012	Bilgisayarların fiziksel hafızaları, RAM vb.	Bilgisayarların fiziksel hafızasını, RAM kanıtlarını, ağ bağlantılarını, kayıt defteri bilgilerini, kullanıcı adları ve şifrelerini yakalar.
Memoryze	Ücretsiz	Windows 8/Server 2012	Disk, sistem belleği.	Disk üzerindeki tüm yüklenen zararlı aktiviteleri keşfetmek ve bellekten görüntü almak vb.
FAW	Ücretsiz	Windows 7/8/8.1 ve 10	Web siteleri, bilgisayar dosyaları	Web siteleri üzerinden sayfa alma, bilgisayar dosyalarını görüntüleme ve düzenleme, ses/video çekimi ve IP adresi alma vb.
Volatility	Ücretsiz	Linux, Mac OS X, Windows 7/8/10 ve Vista ve Server 2012	RAM.	RAM analizi, malware analizi, RAM bellek dökümlerini almak ve dijital bulguları analiz etmek.
EnCase	Ücretli	Windows.	Sabit disk, hard disk, akıllı telefon, tablet ve hafıza kartları vb.	Yereldeki sabit disk, hafıza kartı ve hafızanın anlık görüntüsünü alma, hızlı imaj alma ve farklı dosya formatlarını görüntüleyebilme vb.
Forensic Explorer	Ücretli	Windows 7/8/8.1 ve Windows 10.	Sistem dosyaları, disk.	Gizli sistem dosyaları, silinmiş dosyalar, disk boşluğu vb. gibi mevcut tüm verilere erişebilmektedir.
Helix 3 Pro	Ücretli	Linux, Windows ve Mac OS.	Ağ sistemleri, ekran görüntüleri.	İnternet altyapısı, veri paylaşımı ve taciz vb. gibi zararlı faaliyetleri tespit etme, tüm ağı inceleme, ekran görüntüsü yakalama ve raporlama vb.

5.2. Sızma Testi Laboratuvarı

Sızma testleri ve güvenlik denetimi için gerek duyulabilecek araçlarla donatılmış, Debian tabanlı ve açık kaynak olarak geliştirilmiş ücretsiz Linux işletim sistemi dağıtımıdır. GNU Lisansı ile dağıtılmaktadır. Kali Linux, içerisinde sonradan kurulmaya ihtiyaç olmadan birçok sızma testi aracı ile hazır olarak gelir. Kali linux Offensive Security şirketi tarafından desteklenmektedir. Kişiselleştirilebilir yapıda çoklu dil ve Türkçe desteğine sahiptir. Kali Linux üzerinde yaklaşık altı yüzden (600) fazla sızma testi aracı mevcuttur. Bilgi toplama, zafiyet analizi, kablosuz ataklar, web uygulama saldırıları, sömürme araçları, stres testi, parola atakları, erişim bakımı, tersine mühendislik, donanım saldırısı ve raporlama araçları bulunmaktadır. Kali Linux dağıtımlarına https://www.kali.org/downloads/ adresi üzerinden ulaşılabilir. Kali Linux üzerindeki araçların listesi kategorilerine göre aşağıda listelenmiştir. Bunlardan;

5.2.1. Bilgi Toplama Araçları

5.2.1.1. Arp-scan

ARP Tarama Aracı alt ağdaki her aktif IPv4 cihazını gösteren çok hızlı bir ARP paket tarayıcısıdır. ARP tarayıcı türü yalnızca yerel LAN üzerinde çalışır. ARP Tarama Aracı, güvenlik duvarları olsa bile tüm etkin cihazları gösterir. Aygıtlar, Ping'den gizleyebilecekleri gibi ARP paketlerinden gizlenemez. Linux, FreeBSD, OpenBSD, Mac OS X, Solarix vb. gibi platformlarını destekler. Linux arp-scan aracı ile IP aralıkları inceleme, ağ tarama ve gizli cihazları tespit etme işlemleri gerçekleştirilir.

5.2.1.2. Dmitry

Dmitry, C dilinde kodlanmış UNIX/Linux komut satırı programıdır. Hedef sunucu veya bilgisayar hakkında basit bir hedeften uptime raporlarına ve Tcp portuna kadar basit bir arama ile bilgi toplamaya yarayan bir araçtır. Açık kaynak kod olan bu program ile etki alanı whois (w) taraması, IP whois (i) taraması, Netcraft bilgileri (n) subdomain taraması, e-posta adresi araması, tcp bağlantı noktası taraması gerçekleştirilir. Kullanıcı tarafından belirlenen modüllere izin veren modüler yapıda bir programdır. Linux LFS 6.1, FreeBSD 4, 5 ve 6.0, OpenBSD 3.8, MacOSX 10 ve

SuSE Linux 8 platformlarını destekler. Dmitry aracı https://github.com/jaygreig86/dmitry/ adresinden indirilebilmektedir.

5.2.1.3. Hping3

Hping, bir TCP/IP paket analizörü test aracıdır. TCP, ICMP, UDP ve RAW-IP protokollerini destekler. Güvenlik duvarı testi, gelişmiş port taraması, ağ testi, MTU keşfi,uzaktan parmak izi ve çalışma süresi tahmini, TCP/IP denetimi özellikleri vardır. Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X ve Windows platformlarında çalışır. Hping aracı https://github.com/antirez/hping adresinden indirilebilmektedir.

5.2.1.4. Maltego Aracı

Bilgi toplamak için kullanılan araçlardan bir tanesidir. DNS kayıtları, whois kayıtları, arama motorları, sosyal ağlar, çevrim içi API'ler gibi kaynakları sorgulayarak kullanıcılar, e-mail adresleri, takma adlar, organizasyonlar, web siteleri, dns isimleri, IP adresleri, bağlantılar, belgeler bulunur [80]. Ücretsiz olan sürümü Kali Linux ile birlikte varsayılan olarak yüklü olarak gelir. Ticari olan ücretli sürümlerinde daha fazla grafik oluşturma ve daha fazla biçimde dışarı aktarma özelliği mevcuttur. Maltego aracı ile, insan grupları, şirketler, organizasyonlar, web siteleri, etki alanları, dns adları, IP adresleri, ifadeler, belge ve benzeri varlıklar hakkında bilgi toplanır. Windows, Mac ve Linux platformlarında çalışabilmektedir. Ticari olan Maltego ürün modellerinin fiyatları 999 ile 1999 ABD doları arasında değişmektedir. Ticari sürümü http:// https://paterva.com/index.php adresinden temin edilebilir.

5.2.1.5. Nikto

Açık kaynak web sunucusu tarayıcısı olan Nikto, web uygulaması hakkında bilgi toplama ve zafiyet analizi yapma işlemlerinde kullanılan bir programdır. Güvenli olmayan dosyaları, yapılandırmaları ve programları bulmak için tasarlanmış bir araçtır. Yanlış yapılandırılan sunucu ve yazılımları, eski program ve sunucuları, güvensiz dosya ve programları vb. gibi güvenlik açıklıklarına neden olan sorunları bulmaya yarar. Ayrıca çerez, yönlendirme, kimlik doğrulaması gerektiren URL' yönlendirmeleri, hata ayıklama çıktıları ve https hataları hakkında bilgi edinebilmek

için kullanılır. Perl ortamına sahip Linux platformlarında çalışabilir. Nikto aracı https://github.com/sullo/nikto adresinden indirilebilmektedir.

5.2.1.6. TheHarvester

Açık kaynaklı istihbarat toplama aracı olarak kullanılır. Arama motoru, PGP anahtar sunucuları be SHODAN veritabanı vb. gibi farklı kamu kaynaklarından gelen e-posta, alan adları, IP, URL, subdomain ve açık port bilgilerini toplar. TheHarvester aracı https://github.com/laramies/theHarvester adresinden indirilebilmektedir.

5.2.1.7. Wireshark

Yaygın olarak kullanılan açık kaynaklı tamamen ücretsiz ağ protokolü analiz yazılımıdır. Wireshark network trafiğinin, bir grafik arayüz üzerinden izlenmesini sağlayan bir araçtır. Ağ üzerindeki aktiviteleri mikroskobik düzeyde inceleme imkânı sağlar. Bilgisayar ağında çalışan trafiği tarayıp yakalar. IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP ve WPA / WPA2 dâhil olmak üzere birçok protokol için şifre çözme desteği vardır. Canlı veriler Ethernet, IEEE, PPP/HDCL, ATM, bluetooth, usb, token ring, frame relay ve diğerlerinden okunabilir. 750'den fazla protokolü analiz etme özelliğine sahip, yüzlerce protokolü ve medya türünü destekleyen Wireshark aracı, belli kriterlere göre filtreleme yapabilmektedir [81]. Filtreleme özelliği ile belirli kriterlere uygun paketler yakalanabilir veya gösterilebilir. Linux, Mac OS X, BSD, ve Solaris ile Microsoft Windows platformlarında çalışabilir. Unix ve Windows platformları için ücretsizdir. Aracı indirmek için wireshark.org sitesinden yararlanabilirsiniz.

5.2.2. Güvenlik Açığı Analizi

5.2.2.1. Nmap

Ağ keşfi ve güvenlik denetimi için ücretsiz ve açık kaynaklı Fyodor Firması tarafından üretilmiş bilgi toplama için kullanılan bir programdır. Bilinen bütün port tarama tiplerini destekler. Grafik arabirimine sahiptir. IDS/IPS atlatma seçeneklerine sahiptir. Nmap aracı, port tarama, ağ tarama, işletim sistemi belirleme, zafiyet tarama gibi işlevlere sahip olan Nmap aracı, ağda hangi ana bilgisayarların kullanılabilir olduğunu, hangi ana bilgisayarların sunduğunu hangi hizmetlerin hangi işletim

sistemlerini çalıştırdığını, ne tür paket filtreleri / güvenlik duvarları kullandığını belirlemek için kullanılır. Bu program ile taranan ağın haritasını çıkarabilir, açık durumda olan portlar, bu portları kullanmakta olan servisler ve servislerin versiyon bilgileri, kullanılan işletim sistemleri gibi birçok bilgi elde edilebilir. Temel TCP taraması yapmanın dışında daha detaylı bilgi toplamak için daha farklı TCP Syn Scan, TCP Connect Scan, UDP Scan, TCP Null Scan, TCP Fin Scan, XMAS Scan, TCP ACK Scan, IP Protocol Scan gibi Nmap tarama parametreleri vardır [83]. Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga ve diğerleri dahil olmak üzere çoğu işletim sisteminde kullanılabilir. Nmap sürümleri https://nmap.org/download.html adresinden indirilebilmektedir.

5.2.2.2. OpenVAS

Open Vulnerability Assessment System (OpenVAS), Kali üzerinde varsayılan olarak paketleri bulunan, açık kaynaklı, popüler zafiyet tarama ve denetim araçlarının başında gelir. Çoğu bileşeni Genel Kamu Lisansı (GNU GPL) kapsamında açık kaynak olarak kullanılmaktadır. Kali Linux üzerinde varsayılan olarak paketleri bulunan, açık kaynaklı, popüler zafiyet tarama ve denetim araçlarının başında gelir. Gerçek zamanlı açıkları test edebilme, aynı anda birden çok sistemi test edebilme, SQL açıklarını test edebilme, sistem hakkında detaylı raporlama gibi birçok özelliği mevcuttur. Kaynak kodları https://gitlab.com/kalilinux/packages/openvas adresinden indirilebilir.

5.2.2.3. SQLMAP

SQL enjeksiyon hatalarını tespit etmek ve veri tabanı sunucularını devralma işlemini otomatikleştiren açık kaynaklı bir test aracıdır. Veri tabanı parmak izi alma, veri tabanından veri alma, temel dosya sistemine erişme ve işletim sistemi üzerinden komutları çalıştırma işlemlerine kadar birçok işlem yapılabilmektedir. MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, HSQLDB ve H2 veritabanı yönetim sistemlerini destekler. Sql tabanlı sitelerin güvenliğini denetlemek için kullanılır. Linux ve Windows platformlarında çalışabilir. Kali Linux ve Backbox benzeri sızma testi dağıtımlarında yüklü olarak gelir. Sqlmap aracı https://github.com/sqlmapproject/sqlmap adresinden indirilebilir.

5.2.3. Kablosuz Saldırıları

Kablosuz ağ analiz ve test işlemlerinde kullanılan Aircrack-ng ve Kismet araçları incelenmiştir.

5.2.3.1. Aircrack-ng

Kablosuz manuel testlerinde kullanılan bir araçtır. Güvenlik açığı olan kablosuz bağlantıları keser. WPA ve WPA 2 şifreleme anahtarları tarafından desteklenmektedir. Paket yakalama ve verilerin metin dosyalarına aktarılması, kimlik doğrulama, Wi-Fi kartlarını ve sürücü yeteneklerini kontrol etme işlevleri vardır. Linux, OS X, FreeBSD, OpenBSD, NetBSD, Solaris ve benzeri platformlarda çalışabilmektedir.

5.2.3.2. Kismet

Kablosuz ağ detektörü algılayıcı ve izinsiz giriş algılama sistemidir. Kismet açık kaynak kodlu kablosuz ağ analiz programıdır ve wi-fi ve Bluetooth arabirimleri, bazı SDR donanımları ve diğer özel yakalama donanımları ile çalışır. En önemli özelliklerinden biri pasif olarak kablosuz ağ keşif yapabilmesi ve keşif esnasında iz bırakmamasıdır. Linux, Unix ve Windows platformlarında çalışır. Kismet programı https://www.kismetwireless.net/downloads/ adresinden indirilebilmektedir.

5.2.4. İnternet Uygulamaları

Web uygulamaları güvenlik açıklıklarını tespit etmek ve web uygulama güvenliğini sağlamak için kullanılan araçlardan Arachni, Burp Suite, Maltego, Nikto, Sqlmap ve w3af programları incelenmiştir. Maltego, Nikto ve Sqlmap araçları daha önce güvenlik açığı analizi ve bilgi toplama araçları başlığı altında anlatılmıştır.

5.2.4.1. Arachni

Arachni, açık kaynak kodlu web uygulama güvenliğinde kullanılan test aracıdır. Windows, Mac OS X ve Linux platformlarında çalışabilir. JavaScript, HTML5, DOM manipülasyonu ve Ajax gibi teknolojileri kullanan web uygulamalarını destekler. Arachni aracı https://www.arachni-scanner.com/features/framework/crawl-coverage-vulnerability-detection/ adresinden indirilebilmektedir.

5.2.4.2. Burp Suite

Web uygulamalarının güvenliğini test etmek için kullanılan bir platformdur. Burp aracı ile bir uygulamanın saldırı yüzeyinin ilk haritalandırılması ve analiz edilmesinden güvenlik açıklıklarının bulunarak sömürülmesine kadar tüm test işlemleri gerçekleştirilebilmektedir. Tarayıcı ile uygulama arasındaki trafiğin incelenmesi için Proxy engelleme, içerik ve işlevleri taramak için uygulama bulan örümcek, taramaları otomatik hale getirmek için gelişmiş web uygulama tarayıcısı gibi bileşenleri içermektedir. Kali üzerinde Burp Suite'in ücretsiz sürümü yüklü olarak gelir. Haricen https://portswigger.net/burp adresinden indirilebilir.

5.2.4.3. w3af

Web uygulama açıklıklarını bulmaya yarayan ve Python dili ile geliştirilmiş GPLv2.0 altında lisanslanan, ücretsiz güçlü penetrasyon araçlarından biridir. Otomatik tarama özelliklerinin dışında grafik arayüzü üzerinden özelleştirilebilir araçlar sunar. SQL enjeksiyonu, siteler arası komut dosyası çalıştırma (XSS), uzaktan dosya ekleme vb. gibi birçok eklentiye sahiptir. Linux, BSD ve Mac OS platformlarını desteklemektedir. Bazı eski sürümleri Windows platformlarında çalışabilmektedir. w3af aracı https://github.com/andresriancho/w3af adresinden indirilebilmektedir.

5.2.5. Sömürme Araçları

Zafiyet sömürme işlemleri gerçekleştirmek için kullanılan araçlardan Armigate, Exploitdb, Maltego, Metasploit-framework, Sqlmap ve Yersinia programları incelenmiştir. Maltego ve Sqlmap araçları daha önce güvenlik açığı analizi ve bilgi toplama araçları başlığı altında incelenmiştir.

5.2.5.1. Armigate

Metasploit işlevini basitleştirmek ve kolaylaştırmak için kullanılan grafiksel bir arabirimdir. Sistemlere sızabilmeye yarayan görsel etkileşimli bir programdır. Uzaktan sömürme imkanı sağlayan bu araç ile hedefte bulunan açık portlar üzerinde çalışan servisler, işletim sistemi ve cihazlar tespit edilir. Armigate aracı Metasploit veritabanını kullanmaktadır. İstemci veya sunucu olarak çalışabilmektedir. Armigate programı Windows, Linux ve Mac OS üzerinde

kullanılabilmektedir. Fakat tüm bileşenleri Windows platformları üzerinde kurmak mümkün olmamaktadır. Armigate programı Kali Linux işletim sistemi üzerinde mevcuttur. Bu aracı Kali Linux işletim sisteminde kullanabilmek için postgreSQL ve Metasploit servislerinin aktif edilmesi gerekmektedir.

5.2.5.2. Exploitdb

Exploit veritabanı, Offensive Security tarafından kamu hizmeti olarak sunulan kar amacı gütmeyen bir projedir. Penetrasyon test uzmanları tarafından kullanılmak üzere geliştirilen, kamu yararına ve ilgili hassas yazılımlara karşı CVE uyumlu bir arşivdir.

5.2.5.3. Metasploit-framework

Güvenlik açıklıklarını bulmak, kullanmak ve doğrulamak için kullanılan sızma testi platformudur. Ruby dili ile kodlanmıştır ve 1000'in üzerinde exploit ve birçok parametre ile modül barındırmaktadır [84]. Bu araç ile web güvenlik testleri ve işletim sistemlerine yönelik testler gerçekleştirilebilir. Exploitler, sisteme erişim sağlamak için sistemde veya uygulamada bulunan güvenlik açıklıklarını hedef alan arabellek taşması, backdoor, kod enjeksiyonu veya bilgi sızdıracak kodlar içerirler [85]. .

Hedef sisteme erişim sağlayabilmek için Nmap ağ tarama aracı ile versiyonlar belirlendikten sonra Nessus ve OpenVAS ile zafiyetler tespit edilerek bu zafiyetlere uygun exploit kodlarının bulunması gerekir.

Windows, Linux ve Mac gibi farklı platformları destekleyen Metasploit, Kali Linux ve Backtrack Linux dağıtımlarında yüklü olarak gelir. Ticari olan sürümlerinde kullanıcılarına sosyal mühendislik, kaba kuvvet saldırıları gibi kötü eylemleri otomatikleştirmeyi ve kolaylaştırmayı hedefleyen özellikleri bulmak mümkündür. Metasploit Framework veya Metasploit Pro sürümlerini metasploit.com adresinden indirilebilir.

5.2.5.4. Yersinia

Layer 2 katmanı (Data Link) üzerinde gerçekleştirilen saldırılar için kullanılan bir araçtır. Farklı ağ protokolleri üzerindeki zafiyetlerden yararlanılmak üzere tasarlanmıştır. STP, CDP, DTP, DHCP, HSRP, ISL ve VLAN Protokollerine yönelik

saldırılar gerçekleştirilebilir. Yersinia aracı açık kaynak kodlu olup https://github.com/tomac/yersinia adresinden indirilebilir.

5.2.6. Stres Testi

Web tabanlı uygulamalara yönelik yük testleri, uygulamaların farklı senaryolar ve kullanıcı yükleri altında nasıl davrandığını görmek ve mevcut alt yapının kaldırabileceği maksimum ve optimum performans değerlerini ortaya çıkaran araçlardır. Web uygulamalarında performans testlerinin yapılmasındaki amaç, belirlenen kısıtlar ölçüsünde uygulanan yük altında, sistemde ortaya çıkabilecek darboğazları ortaya çıkarmaktır. Yük testi aslında Performans testlerini bir türevi olarak kabul edilebilir. Yük testleri, yük miktarının belirli oranlarda arttırılarak hangi seviyede sorun çıktığının araştırılması şekliyle uygulanıyor. Yine, performans testlerinde olduğu gibi otomatize araçlar kullanılıyor.

5.2.6.1. DHCPig

DHCP tükenme saldırısı aracıdır. LAN üzerindeki tüm IP'leri tüketir, yeni kullanıcıların IP almalarını engelleyecek, kullanılan IP adreslerini serbest bırakacak saldırılar gerçekleştirilebilir. IP ve MAC adreslerini bulma ve DHCP isteklerini dinleme gibi özelliklere sahiptir. Kali Linux stres testi aracıdır. DHCPig, https://github.com/kamorin/DHCPig adresinden indirilebilir.

5.2.6.2. mdk3

Protokol zayıflıklarından yararlanmak için kullanılan bir araçtır. Mdk3, verileri kablosuz ağlara "enjekte eden" bir araçtır ve kablosuz bağlantılara ait geçerli ve geçersiz paketler göndermek için kullanılır. Kali Linux üzerinde stres testi için kullanılan bir araçtır. Mdk3 aracına https://github.com/charlesxsh/mdk3-master adresinden indirilebilir.

5.2.6.3. Apache JMeter

Web uygulamalarında performans ve yük testlerini gerçekleştirmeye yarayan Java tabanlı ve açık kaynak kodlu bir araçtır. Gücü test etmek veya farklı yük tipleri altında

performansı analiz etmek için sunucu, ağ veya nesne üzerindeki yükleri simule etmek için kullanılabilir.

5.2.7. Parola Atakları

5.2.7.1. Hydra

Şifre kırmaya yarayan esnek yapıda bir Kali aracıdır. Birçok cihaz kilidini açma, güvenlik kodunu sıfırlama ve kodları okuma gibi özellikleri vardır. HTTP (s)-get, HTTP Proxy, IMAP, IRC, NFS, FTP, CVS, Cisco, Oracle SID ve SNMP protokollerini destekler. Hydra aracı, https://tools.kali.org/password-attacks/hydra adresi üzerinden indirilebilir.

5.2.7.2. John The Ripper

John The Ripper, Unix, Mac OS, Windows, BeOS ve OpenVMS için kullanılan Kali şifre kırma aracıdır. DES tabanlı "bigcrypt", BSDI DES tabanlı, FreeBSD MD5 tabanlı ve OpenBSD Blowfish tabanlı dağıtımlarda kullanılmaktadır. John The Ripper sürümleri https://www.openwall.com/john/ adresi üzerinden indirilebilir.

5.2.7.3. Ncrack

Bilgisayarları ve ağ aygıtlarını zayıf parolalar için test etmeye yarayan ağ kimlik doğrulama test aracıdır. SSH, RDP, FTP, Telnet, HTTP(S), POP3(S), IMAP, SMB, VNC, SIP, Redis, PostgreSQL, MySQL, MSSQL, MongoDB, Cassandra, WinRM and OWA protokollerini desteklemektedir. Ncrack, Linux, BSD, Windows ve Mac OS X platformlarını desteklemektedir. Ncrack sürümlerine https://nmap.org/ncrack/ adresi üzerinden erişilebilmektedir.

5.2.8. Tersine Mühendislik

5.2.8.1. Apktool

Android uygulamaları için kullanılan 3.parti bir araçtır. Android uygulamalarının apk dosyalarını smali koda dönüştürür. Uygulama analizi için de kullanılabilir. Java 8 ve üzeri sürümlerde apktool aracı kullanılmaktadır. Kaynakların orijinal forma dönüştürülmesi ve yeniden oluşturulması işlemleri gerçekleştirilir. Apktool aracına https://github.com/iBotPeaches/Apktool adresi üzerinden erişebilir.

5.2.8.2. Yara

Kötü amaçlı yazılım örneklerini tanımlama ve sınıflandırma konusunda yardımcı olan bir araçtır. Bu araç ile metinsel ve ikili desenlere dayanarak zararlı yazılımlara ait açıklamalar oluşturulabilir. Windows, Linux ve Mac OS X platformlarında çalışabilir. Yara aracına https://github.com/virustotal/yara/releases/tag/v3.10.0 adresinden erişilebilir.

5.2.9. Raporlama Araçları

5.2.9.1. CaseFile

CaseFile, Maltego aracının küçük kardeşi olarak ifade edilmektedir. Verileri hızlı bir şekilde ekleme, bağlama ve analiz etme özellikleri olan grafik uygulamasıdır. Çevrimdışı veriler elde ederek grafik oluşturulabilir. Maltego'daki yerleşik grafikler için ücretsiz bir grafik görüntüleyici olarak kullanılabilmektedir. Csv, Xls ve Xlsx formatlarında saklanan verileri görselleştirme yeteneğine sahiptir. Windows, Mac ve Linux platformlarında çalışabilmektedir. CaseFile sürümleri, https://paterva.com/downloads.php#tab-4 adresi üzerinden indirilebilir.

Yukarıda belirtilen sızma testi araçları, kullanım durumuna, desteklediği işletim sistemine, inceleme alanına ve özelliklerine göre çizelge 5.2'de kategorilendirilmiştir.

Çizelge 5.2 Sızma Testi Araçları

	Araçlar	Kullanımı	İşletim Sistemi	İnceleme Alanı	Özellikleri
Bilgi Toplama Araçları	Arp-scan	Açık Kaynaklı	Linux, FreeBSD, OpenBSD, Mac OS X, Solarix.	Yerel LAN üzerinde	Ağdaki aktif IPv4 cihazlarını gösterme, IP aralıklarını inceleme, ağ tarama ve gizli cihazları tespit etme.
	Dmitry	Açık Kaynaklı	Linux, FreeBSD, Linux 8, ve MacOSX 10	Sunucu ve bilgisayar.	Whois, IP, subdomain ve TCP bağlant noktası taraması, e-posta adresi araması vb.
	Hping3	Ticari Açık Kaynaklı	Linux, Windows FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X ve	Bilgisayar TCP/IP.	Güvenlik duvarı ve ağ testi, gelişmiş port taraması, MTU keşfi, e-posta adresi araması, tcp bağlantı noktası taraması, uzaktan parmak izi ve çalışma süresi tahmini, TCP/IP denetimi
	Maltego Maltego Pro	Ticari Açık Kaynaklı	Linux, Windows ve Mac IOS.	DNS kayıtları, arama motoru, sosyal ağlar,	Maltego aracı ile, insan grupları, şirketler, organizasyonlar, web siteleri, etki alanları, dns adları, IP adresleri, ifadeler, belge ve benzeri varlıklar hakkında bilgi toplanır.
	Nikto	Açık Kaynaklı	Linux.	Web sunucusu.	Web uygulaması hakkında bilgi toplama ve zafiyet analizi yapma aracı.
	TheHarvester	Açık Kaynaklı	Linux.	Bilgisayar ve bağlı sistemler.	Pasif olarak Google, Bing vb. gibi arama motorlarından, Linkedin, Shodan vb. gibi platformlardan kullanıcı profilleri, mail adresleri, sanal hostlar tespit edilebilir.
	Wireshark	Açık Kaynaklı	Linux, Windows, Mac OS, FreeBSD, ve NetBSD.	Ağ sistemleri ve kaydedilmiş dosyalar vb.	Ağ üzerindeki aktiviteleri mikroskobik düzeyde inceleme imkânı sağlar. Bilgisayar ağında çalışan trafiği tarayıp yakalar.
Güvenlik Açığı Analizi	Nmap	Açık Kaynaklı	Linux, Windows, OpenBSD, Sun OS, Mac OS X.	Ağ sistemleri.	Ağ keşfi, port tarama, ağ tarama, işletim sistemi belirleme, güvenlik duvarı tespiti ve zafiyet tarama vb.
	Openvas	Açık Kaynaklı	Linux ve Windows.	Web, sunucu vb.	SQL açıklarını test etme, zafiyet tarama ve sistem hakkında detaylı raporlama vb.
	Sqlmap	Açık Kaynaklı	Linux ve Windows.	SQL tabanlı web siteleri.	Kali Linux üzerinde yüklü olarak gelir. SQL enjeksiyon hatalarını tespit etme, veri tabanı sunucularını devralma ve temel dosya sistemine erişme vb. gibi işlemler.
Kablosuz Saldırıları	Aircrack-ng	Açık Kaynaklı	Kali Tools	Kablosuz ağ ve bileşenleri.	Kali aracıdır. Güvenlik açığı olan kablosuz bağlantıları keser. Paket yakalama, kimlik doğrulama vb.
	Kismet	Açık Kaynaklı	Linux, Unix, OSX, Windows 10 ve üzeri.	Kablosuz ağ ve bileşenleri.	Kali aracıdır. Kablosuz ağ analiz programıdır. En önemli özelliği pasif olarak kablosuz ağ keşfi yapmasıdır. Keşif esnasında iz bırakmaz.
İnternet Uygulamaları	Arachni	Açık Kaynaklı	Linux, Windows ve Mac OS X.	Web uygulamaları.	Kali aracıdır. Web uygulama güvenliği test aracıdır.
	Burp-Suite	Açık Kaynaklı (Kali üzerinde)	Linux.	Web uygulamaları	Kali üzerinde ücretsiz sürümü yüklü gelir. Web uygulama güvenliği test aracıdır. Proxy engelleme, içerik ve işlevleri tarama, taramaları otomatik hale getirme
	W3af	Açık Kaynaklı	Linux, Mac OS, BSD ve bazı eski Windows sürümü.	Web uygulamaları.	Sızma testi aracıdır. Otomatik tarama özelliği vardır. Grafik arayüzü üzerinden özelleştirilebilir araçlar sunar. SQL enjeksiyonu, XSS ve uzaktan dosya ekleme vb. gibi özellikleri vardır.

Sömürme Araçları	Armigate	Açık Kaynaklı	Linux, Windows ve Mac OS.	İşletim sistemleri ve web uygulamaları.	Kali sömürme aracıdır. İstemci ve sunucu olarak çalışır. Uzaktan sömürme, açık portlar üzerinde çalışan servis, işletim sistemi ve cihazları tespit etme vb.
	Metasploit Framework	Ticari ve Açık Kaynaklı	Linux, Windows ve Mac OS.	İşletim sistemleri ve web uygulamaları.	Kali sömürme aracıdır. Kali üzerinde yüklü olarak gelir. Bu araç ile web güvenlik testleri ve işletim sistemlerine yönelik testler gerçekleştirilebilir.
	Yersinia	Açık Kaynaklı	Linux, Windows ve Mac IOS.	Ağ Sistemleri.	Kali sömürme aracıdır. STP, CDP, DTP, DHCP, HSRP, ISL ve VLAN protokollerine yönelik saldırılar gerçekleştirilebilir.
Stres Testi	DHCPig	Açık Kaynaklı	Linux.	Ağ sistemleri.	Kali stres testi aracıdır. LAN üzerindeki tüm IP'leri tüketebilir, serbest bırakabilir, IP/MAC adreslerini bulabilir ve DHCP isteklerini dinleyebilir.
	Mdk3	Açık Kaynaklı	Linux.	Kablosuz ağlar.	Kali stres testi aracıdır. Protokol zayıflıklarından yararlanmak için kullanılan bir araçtır. Verileri kablosuz ağlara enjekte eder.
	Apache JMeter	Açık Kaynaklı	Linux.	Web uygulamaları.	Gücü test etmek veya farklı yük tipleri altında performansı analiz etmek için sunucu, ağ veya nesne üzerindeki yükleri simule etmek için kullanılabilir.
Parola Atakları	Hydra	Açık Kaynaklı	Linux.	Bilgisayarları ve ağ aygıtları.	Kali şifre kırma aracıdır. Birçok cihaz kilidini açma, güvenlik kodunu sıfırlama ve kodları okuma özelliği vardır.
	John The Ripper	Açık Kaynaklı	Linux, Unix, Windows, OpenVMS, BeOS.	Bilgisayarları ve ağ aygıtları.	Kali şifre kırma aracıdır. **.** DES tabanlı "bigcrypt", BSDI DES tabanlı, FreeBSD MD5 tabanlı ve OpenBSD Blowfish tabanlı dağıtımlarda kullanılmaktadır.
	Ncrack	Açık Kaynaklı	Linux, BSD, Windows ve Mac OS X.	Bilgisayarları ve ağ aygıtları.	Kimlik doğrulama test aracıdır. Zayıf parolaları test eder.
Tersine Mühendislik	Apktool	Açık Kaynaklı	Linux.	Android uygulamaları.	Kali tersine mühendislik aracıdır. Android uygulamalarının apk dosyalarını smali koda dönüştürür.
	Yara	Açık Kaynaklı	Windows, Linux ve Mac OS X.	Yazılımlar.	Kali tersine mühendislik aracıdır. Kötü amaçlı yazılımları tanımlama ve sınıflandırma konusunda yardımcı bir programdır.
Raporlama Aracı	CaseFile	Açık Kaynaklı	Windows, Linux ve Mac OS X.	CSV, XLS ve XLSX dosyaları.	Kali raporlama aracıdır. Verileri hızlı ekleme, bağlama ve analiz etme özelliği olan grafik uygulamasıdır.

6. SONUÇLAR VE TARTIŞMA

Ağ sistemleri ve bilişim teknolojilerinin gelişmesi ile birlikte devletler, tüm kamu kurumlarının hizmetlerini dijitalleştirerek bilgisayar ortamına taşıdı. Kurumların tüm kayıtlarını bilgisayar ortamına taşıması bazı güvenlik risklerini de beraberinde getirmektedir. Bu kayıtların internet üzerinden tüm dünyaya erişilebilir hale geldiği çağımızda kamu düzeni ve güvenliği, kamu hizmetlerinin sürdürebilirliği açısından kritik altyapıların korunması büyük önem arz etmektedir.

Uluslarası platformlarda bilgi, ağ ve iletişim teknolojileri; amaçları, saldırı yöntemleri ve motivasyonları farklı aktörler tarafından intikam, hırs, maddi çıkar ve güç elde etmek, askeri, siyasi, stratejik ve benzeri devlet sırlarını çalmak, hizmeti engellemek, verileri yok etmek, doğrudan cana kast eden eylemlerde bulunmak gibi sebeplerle casusluk, saldırı ve savunma aracı olarak kullanılmaya başlamıştır.

Günümüz koşullarında kurumsal bilgi güvenliğini sağlamada kurumlarımız saldırı tespit ve engelleme sistemleri, güvenlik duvarı, sanal ağ, web filtreleme, log ve izleme çözümlerine yönelik çeşitli güvenlik yatırımı yapmaktadırlar. Ancak bu yatırımlara rağmen yazılımların tamamının güncel olmaması, güncelliğin takip edilmemesi, çıkan yama/eksiklerin zamanında uygulanmaması, güvenlik duvarı ve sistemleri üzerinde oluşturulan kuralların, yapılandırmaların eksik veya hatalı yapılması, kritik varlık envanterinin çıkarılmaması, performans tabanlı sorunlar ve gerçek ihtiyaçlar belirlenmeden gereğinden fazla veya yanlış yapılan yatırımlar vb. gibi hatalar sistemlere doğru istenmeyen bağlantıların yapılmasına yol açmaktadır. Güvenlik yatırımları içerisinde en yaygın olarak kullanılan güvenlik duvarı sistemleri, üzerlerinden geçen her paketi denetledikleri için aşırı trafiğin artmasına ve çok fazla işlem gücü kullanılması ile sistemin yavaşlamasına neden olurlar ve eşik değeri aşıldığında sistem üzerinden geçen paketleri bir süre sonra denetleyemez duruma gelirler. Ayrıca günlük kayıtlarının ve uyarıların fazlalığı nedeni ile sistem yöneticileri incelemeye zaman bulamazlar. Bu sebeplerle güvenlik mekanizmaları üzerinde birçok önemli filtre özelliği devre dışı bırakılmakta ve bu durum kritik güvenlik zafiyetlerine neden olmaktadır.

Ülkemizde kurumların kritik altyapılarının korunmasına ilişkin hukuki düzenlemeler, yasal çalışmalar yapılmakta ve kurumların siber savunma yeteneklerini ölçmek ve yeterli olup olmadıklarını tespit etmek amacıyla siber güvenlik tatbikatları gerçekleştirilmektedir.

Bu çalışmada; öncellikle Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliğiyle gerçekleştirilen ulusal siber güvenlik tatbikatı sonucunda elde edilen bulgular incelenmiştir. Bugüne kadar yapılan tatbikatlara çok sayıda kurum katılmıştır. Elde bulgular arasında; sistem yöneticilerinin teknik yetersizlikleri, saldırı tespit sistemlerinin ve süreçlerinin yetersizliği, güncel olmayan anti virüs programları, sistem planlama aşamasında güvenliğin göz ardı edilmesi, erişim kontrol politikalarının olmaması, web uygulamalarındaki güvenlik açıklıkları, yasal mevzuata ilişkin bilgi eksikliği gibi başlıklar yer almıştır.

Daha sonra kurumları hedef alan siber tehdit türlerini ortaya koymak için Avrupa Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA) 2018 yılında hazırladığı tehdit durum raporu incelenerek raporda belirtilen 15 farklı siber tehdit türü hakkında kapsamlı bilgi verilmiştir. Belirtilen siber tehdit türleri arasında; kimlik avı, fidye, botnet, hizmet reddi ve web tabanlı saldırılar, kötü amaçlı yazılımlar, veri ihlalleri, bilgi sızıntısı, kimlik hırsızlığı, iç tehditler, istem dışı alınan elektronik iletiler, kripto para madenciliği ve yaygın olarak görülen web uygulaması saldırıları yer almaktadır.

Yaygın olarak görülen web uygulaması saldırıları hakkında Uluslarası bir organizasyon olan Açık Web Uygulama Güvenliği Projesi olan OWASP Kuruluşu tarafından hazırlanan belli bir puan sistemine göre sıralanmış en popüler web açıklıkları ve alınması gereken önlemleri içeren 2017- OWASP Top 10 listesi incelenmiştir. Listede yer alan web uygulaması tehditleri arasında; Enjeksiyon Saldırısı, Bozuk Kimlik Doğrulama, Hassas Veri Riski, XML Dış Varlık Enjeksiyonu, Eksik Erişim Kontrolü, Yanlış Güvenlik Yapılandırması, Siteler Arası Betik Çalıştırılması, Güvensiz Seri Kaldırma, Bilinen Güvenlik Açıklıkları olan Bileşenleri Kullanma Tehdidi ve Yetersiz Kayıt ve İzleme Riskleri bulunmaktadır.

Çalışma kapsamında farklı kurumlar tarafından uygulanmış Siber Güvenlik Raporları ve anketleri incelenmiş ve Siber Güvenliğin sağlanması ve siber farkındalık konusunda önerilere yer verilmiştir. Bunlardan;

DDoS saldırı vektörlerinin dağılımına ilişkin 2018 Nexusguard Q2 Araştırma Raporu incelenmiştir. Raporda; sırası ile 4.07 saldırının %31.56'sı UDP, 1.997 saldırının %18.50'si TCP SYN ve 1.006 atağın %9.32'sinin ICMP vektörü ile yapıldığı ve toplam atakların % 35.87'sinin 10 Gbps'den büyük, % 64'nün 10 Gbps'den küçük olduğu belirtilmiştir.

Kaspersky Lab tarafından hazırlanan Q1 2019 yılı Spam ve Kimlik Avı Saldırısı başlıklı raporu incelenmiştir. İstem dışı alınan e-postaların (Spam) en yüksek görüldüğü ilk 10 ülke sırasıyla en çok Çin %15,82, ABD % 12,64, Rusya % 6,98, Brezilya %6,95, Almanya % 5,86, Fransa % 4.26, Arjantin % 3.42, Polonya % 3.36, Hindistan % 2.58 ve Vietnam % 2.18 oranla takip etmektedir. [53].

CA Teknoloji firması tarafından hazırlanan İçeriden Gelen Tehditler (Insider Threat) raporu incelenmiştir. Başlıca sonuçlar arasında; kuruluşların %90'ının içeriden gelen saldırılara karşı kendilerini savunmasız hissettikleri, %53'nün son bir yıl içerisinde içeriden gelen saldırılara maruz kaldıkları, %51'nin içeriden kazara ve %47'sinin kasıtlı olarak veri ihlallerine neden oldukları vb. gibi maddeler yer almaktadır.

Cyber Security Breaches Survey tarafından 2016 yılında düzenlenen rapor incelenmiştir. Rapora göre, kurum yöneticilerinin %69'nda siber güvenlik fakındalığının olduğu fakat sadece % 51'nin önlem aldığı, %29'nda güvenlik politikasının bulunduğu, %10'nunun da kaza yönetim planının olduğu belirtilmiştir.

On bin kişiden fazla kişinin katılımı ile PwC tarafından gerçekleştirilen The Global State of Information Security Survey 2017 anketi incelenmiştir. Ankete göre, internetten erişilebilen cihaz ve uygulamalar hakkında kurumsal güvenlik politikalarına uygun çalışma gerçekleştirilmesi ve kurum çalışanlarının eğitilmesi gerektiği ifade edilmiştir [62].

Global EY Şirketi tarafından gerçekleştirilen 21. EY Küresel Bilgi Güvenliği Anketine göre; kurumların siber tehditlere karşı mevcut durumları raporlanmıştır ve bu rapora göre; kurumların siber tehditlere karşı korumak istedikleri en önemli bilgileri aşağıda verilmiştir. Bu bilgiler arasında; kuruluşlara yönelik en büyük tehditlerin müşteri, finans, ar-ge, tedarikçi ve yönetim kurulu üyesi bilgileri ile stratejik plan, M&A bilgisi, patentsiz IP, fikri mülkiyet olduğu ifade edilmiştir. Ayrıca kuruluşlara yönelik en büyük 10 siber tehdit türü olarak; kimlik avı, para çalma, bozma, IP hırsızlığı, Spam, içeriden gelen tehdit, casusluk ve doğal afetler belirtilmiştir.

Ayrıca yapılan ankette; katılımcıların %75'i kurumlarında siber güvenlik bilincinin tam olarak oluşmadığını, %12'si saldırı tespit sisteminin olmadığını, %38'i yeteri düzeyde erişim ve kimlik denetimlerinin olmadığını ifade etmişlerdir. Çıkan siber saldırılara karşı katılımcıların %63'ü IT departmanı içerisinde raporlama işlevlerini yaptıklarını, %89'uda bu işlevlerin tam olarak ihtiyaçlarını karşılamadığını söylemişlerdir. Son olarak ta %43 katılımcı olası bir saldırı durumunda bir iletişim stratejisi ve planına sahip olmadıklarını belirtmişlerdir.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliğiyle (belirli aralıklarla) çok sayıda kurumun katıldığı ulusal siber güvenlik tatbikatları incelenmiştir. Bu tatbikatlar neticesinde elde edilen bulgular aşağıda listelenmiştir.

1) Bilgi Güvenliği Yönetim Sistemi (BGYS) eksikliği.
2) Sistem yöneticilerinin teknik konularda yetersizliği.
3) Saldırı tespit sistem ve süreçlerinin yetersizliği.
4) Sosyal mühendislik saldırılarına yönelik bilinç yetersizliği.
5) Güncel olmayan antivirüs programları.
6) Sistem yöneticilerinin güvenlik boyutunda yetersiz olmaları.
7) Kurum içi koordinasyon konusunda eksikliklerin olması.
8) Erişim kontrol politikasının bulunmaması.
9) Sistem planlama aşamasında güvenliğin göz ardı edilmesi.
10) Kablosuz ağlardan kaynaklanan risklerin bulunması.
11) İş sürekliliği planlarının eksikliği.

12) Port tarama saldırılarının tespit edilememesi.
13) Dağıtık Servis Dışı Bırakma saldırılarının (DDOS) olumsuz sonuçlar vermesi.
14) Web uygulamalarında açıklıkların bulunması.
15) Kayıt dosyalarının analizinin tam olarak gerçekleştirilememesi.
16) Yasal mevzuata ilişkin bilgi eksikliğinin bulunması

Özetle kurumların karşılaştıkları en büyük sorunların merkezinde siber güvenlik zafiyetleri ve çalışanların sebep oldukları sorunlar yer almaktadır. Bu sebeple güncel tehditlere karşı yüksek seviyede güvenliğin sağlanabilmesi için kurumların sahip olduğu karmaşık Bilgi Teknolojileri altyapılarının düzenli olarak denetlenmesi ve saldırı simülasyonları ile güncel tehditlere karşı ne kadar hazır olduğunun belirlenmesi, saldırganlardan önce tehditlerin, tehditlerin kaynağının, oluşma şekillerinin, etkilerinin, bıraktıkları izlerinin birtakım yöntemler, analiz ve test teknikleri ile tespit edilmesi gerekmektedir. Ayrıca meydana gelmiş siber saldırılar ile ilgili suça ait delilleri toplayabilmeleri, analiz edebilmeleri, raporlayabilmeleri ve hukuki boyutunu değerlendirebilmeleri için adli bilişim analizlerinin yapılması gerekmektedir.

Bu çalışmada, siber saldırı sonrasında kurumların olay mahallinde delilleri toplama, inceleme, analiz ve raporlama vb. işlemleri gerçekleştirebilmeleri için laboratuvarda kullanılabilecek bazı adli bilişim araçları aşağıda listelenmiştir. Bunlar;

1) Adli analiz işlemleri için; Sans-Sift, The Sleuth Kit (TSK), Oxygen Forensic,

2) Adli görüntüleme işlemleri için; FTK, Linux “dd”, IXImager,

3) Ağ görüntüleme işlemleri için; Wireshark, Network Miner, Xplico,

4) Bilgisayarların fiziksel hafızalarını okumak, silinmiş ve diğer gizli dosyalara erişmek, kötü aktiviteleri tespit etmek ve imaj dosyasını oluşturmak için; Magnet Ram Capture, Memoryze, FAW, Volility, EnCase, Forensic Explorer ve Helix 3 Pro araçları incelenmiştir.

Kurumların olası siber saldırı öncesinde karşı karşıya kaldıkları siber riskleri görebilmeleri ve önlem alabilmeleri için laboratuvar ortamında kullanacakları bazı sızma testi araçları aşağıda listelenmiştir. Bunlar;

1) İstihbarat ve bilgi toplama toplamak için; Arp-scan, Dmitry, Hping3, Maltego, Nikto, TheHarvester ve Wireshark araçları,

2) Ağ keşfi ve güvenlik açığı analizleri için; Nmap, OpenVas ve Sqlmap araçları,

3) Kablosuz saldırılar için; Aircrack-ng ve Kismet araçları,

4) İnternet uygulamaları ve web uygulamaları güvenlik açıklıklarını tespit etmek için; Aranchi, Burp Suite, Maltego, Nikto, Sqlmap ve W3af araçları,

5) Zafiyet sömürme işlemler için; Armigate, Exploitdb, Maltego, Metasploit-framework, Sqlmap ve Yersinia araçları,

6) Web uygulamalarına yönelik stres yük testi için; DHCPig, Mdk3 ve Apache JMeter araçları,

7) Parola atakları için; Hydra, John The Ripper ve Ncrack araçları,

8) Tersine mühendislik için; Apktool ve Yara araçları,

9) Raporlama işlemleri için; CaseFile aracı incelenmiştir.

Söz konusu test türlerinin güvenlik çalışanları tarafından kurumlarında gerçek sistemlere zarar vermeden uygulanabilmesi için öncelikle sanal ortamlar üzerinde belirtilen test yazılımları kurularak tecrübe kazanılması önerilmiştir. Bu kapsamda; kurum ağı içerisinde yer alan temel bileşenler WMware Workstation ve GNS3 yazılımları kullanarak sanallaştırılabilir. Saldırı denemeleri için Kali Linux, Backtrack ve benzeri işletim sistemleri, web sunucusu olarak OWASP, , Metasploitable ve benzeri dağıtımlar, yönlendirici makineler için Windows 7, güvenlik duvarı sanallaştırması için Freebsd, Pfsense, Smoothwall vb. gibi yazılımlar, saldırı tespit sistemi (IDS) olarak ta SNORT ve benzeri güvenlik mekanizmaları kullanılmalıdır.

Siber tehditlerin ve hatta siber savaşların çok sık yaşandığı siber dünyaya her gün daha da bağımlı hale geliyoruz. Bu da birçok riski beraberinde getiriyor. Kurumların kendi siber güvenlik laboratuvarı altyapılarını oluşturmaları siber riskleri fark etmelerini, engellemelerini ve kendilerini siber saldırılara karşı korumalarını sağlayacaktır. Bu çalışmanın siber güvenliğin sağlanmasına ilişkin yürütülen faaliyetlerde, kurumlara önemli ölçüde katkı sağlayacağı düşünülmektedir.

KAYNAKLAR

[1] Dazet, E. F., 2016, Anex: Automated Network Exploitation Through Penetration Testing, *Master Thesis, California Polytechnic State University.* Department of Computer Science, USA.

[2]"Network-Based Passive Information Gathering" erişim adresi: https://perso.liris.cnrs.fr/romuald.thion/files/RT_Papers/Thion07:Cyber:Network.pdf, erişim tarihi: 15 Eylül 2017.

[3] Akyıldız, M.A., Uygulamalarla Siber Güvenliğe Giriş, *Gazi Kitapevi*, Beşevler, Ankara, 2016.

[4] Livshits, B., 2006, Improving Software Security With Precise Static And Runtime Analysis, *Doctoral Thesis, Stanford University.* Department of Computer Science and The Committee On Graduate Studies, USA.

[5] Canbek, G., Sağıroğlu, Ş., Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23, 1-12, 2007.

[6] Tekerek, A., Gemci, C. ve Bay, Ö., Web Tabanlı Saldırı Önleme Sistemi Tasarımı ve Gerçekleştirilmesi: Yeni Bir Hibrit Model, Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 31 (3), 0-0, 2016.

[7] Yiğit, T., Akyıldız, M.A., ve Bay, Ö., Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 18 (1), 14-21, 2014.

[8] Vural, Y., 2007, Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri, *Yüksek Lisans Tezi, Gazi Üniversitesi.* Fen Bilimleri Enstitüsü, Ankara.

[9] Eshete, B., Villafiorita, A. and Weldemariam, K.., BINSPECT: Holisitic Analysis and Detecion of Malicious Web Pages, In International Conference on Security and Privacy in Communication Networks (SECURECOMM2012), Trento, Italy, Jan 2012.

[10] Kam, H. J., Pauli J.J., Work in Progress - Web Penetration Testing: Effectiveness of Student Learning in Web Application Security, Frontiers in Education Conference (FIE), *IEE,* Rapid City, USA, 2011.

[11] "Cyber Crime" erişim adresi: https://www.webopedia.com/TERM/C/cyber_crime.html, erişim tarihi: 15 Şubat 2019.

[12] "cyber security", URL: https://www.techopedia.com/definition/, erişim tarihi:15 Ekim 2018.

[13] " Siber Olaylara Müdahale Ekipleri'nin Kuruluş, Görev ve Çalışmalarına İlişkin Usul ve Esasları Hakkında Tebliğ " erişim adresi: http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=9.5.19004&MevzuatIliski=0&sourceXmlSearch=Siber%20Olaylara%20M%C3%BCdahale%20Ekiplerinin, erişim tarihi: 11 Şubat 2019.

[14] Yayla, M., Hukuki Bir Terim Olarak Siber Savaş, Türkiye Barolar Birliği (TBB Dergisi), 104, 177-202, 2013.

[15] "Macnillan Dictionary" erişim adresi: http://www.macmillandictionary.com/dictionary/american / cyberwar, erişim tarihi: 07 Şubat 2019.

[16] Sağıroğlu, Ş. vd., Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık, *Grafiker Yayınları*, Ankara, 2018.

[17] Güntay, V., Uluslarası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu: Siber Savaş Örneği, Güvenlik Bilimleri Dergisi, 6(2), 81-108, 2017.

[18] "What is Cyber Espionage" erişim adresi: https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/, erişim tarihi: 07 Şubat 2019.

[19] "Internet Security Threat Report" erişim adresi: https://www.symantec.com/content/dam/symantec/docs/reports/istr-20-2015-en.pdf, erişim tarihi: 07 Şubat 2019.

[20] Keleştemur, S.A., 2018, Siber İstihbaratın Kamu Güvenliği için Rolü ve Önemi, *Yüksek Lisans Tezi, İstanbul Gedik Üniversitesi* Sosyal Bilimleri Enstitüsü, İstanbul.

[21] Fumudoh, S., Viswanathan, U., Exploring the Relationship between Online Privacy on Cyber Security, *Yüksek Lisans Tezi, Lulea University of Technology*. Department of Computer Science, Electrical and Space Engineering, *Sweden*.

[22] Ercan, M., Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri, *Yüksek Lisans Tezi, Gebze Teknik Üniversitesi.* Sosyal Bilimleri Enstitüsü, Gebze.

[23] İnternetin Getirdiği Fırsat ve Faydalar erişim adresi: http://internet.btk.gov.tr/internetin-getirdigi-firsat-ve-faydalar-detay-60.html, erişim tarihi: 08.Haziran 2019.

[24] Uyar, S., Yelgen, E., Bilgi İfşası ve Denetim, Yönetim ve Ekonomi Araştırmaları Dergisi, 13(1), 86-88, 2015. Retrieved from: https://dergipark.org.tr/download/article-file/203308

[25] Şahinaslan, Ö., 2013, Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma, *Doktora Tezi, Trakya Üniversitesi.* Fen Bilimleri Enstitüsü, Edirne.

[26] Başaran, A., Siber Savaş Cephesinden Notlar, *Arıon Yayınevi*, İstanbul, 2017.

[27] "Data Breach Investigations Report (2016)" erişim adresi: https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/2b_Verizon_Data-Breach-Investigations-Report_2016_Report_en_xg.pdf, erişim tarihi: 09 Nisan 2019.

[28] Zou, C.C., 2010, The Next Generation Botnet Attacks and Defenses, *Doctoral Thesis, University of Central Florida Orlando*, Engineering and Computer Science, Florida.

[29] Fritzvold, E., 2017, Cyber Security in Organizations, *Master's Thesis, University of Stavanger,* Faculty of Science and Technology, Norway.

[30] Güngör, M., 2015, Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, *Uzmanlık Tezi, T.C.Kalkınma Bakanlığı.* Bilgi Toplumu Dairesi Başkanlığı, Ankara.

[31] Keleş, A.R., Sal, Y., Hack Kültürü ve Hacktivizm, *Alternatif Bilişim* , İstanbul, 2013.

[32] Yasar, H., 2014, Kurumsal Siber Güvenliğe Yönelik Tehditler ve Mücadele Yöntemleri: Eylem Planı Örneği, *Yüksek Lisans Tezi, Gazi Üniversitesi.* Bilişim Enstitüsü, Ankara.

[33] "ENISA Threat Landscape Report 2018", https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, erişim tarihi:30 Nisan 2019.

[34] Goertzel, K.M., Tools Report on Anti-Malware, *Defense Technical Information Center*, Fort Belvoir, Washington, 2009.

[35] Stamatis, K., 2017, Exploit Kit Traffic Analysis, *Master's Thesis, University of Pıraeus.* Department of Digital Systems, Piraeus.

[36] Flatley, B.N., 2013, Rotkit Detection Using A Cross-View Clean Boot Method, *Master Thesis, Air University.* Air Force Institute of Technology, *United States of America*.

[37] Junjie, W., 2018, Detection and Analysis of Web-based Malware and Vulnerability, *Doctoral Thesis, Nanyang Technological University.* School of Computer Science and Engineering, Singapore.

[38] "Reklam Yazılımı Nedir?", https://www.kaspersky.com.tr/resource-center/threats/adware, erişim tarihi: 16 Nisan 2019.

[39] Ergin, T.E., Küpheli, B.G., Siber Kırılma, *Altıkırkbeş Yayınları* , İstanbul, 2018.

[40] F, Cohen., "Computer Viruses: Theory and Experiments", *IEE,* New Orleans, 1988.

[41] Turhan, O., 2006, A Comparison of Ballistic Behavior of Steel and Laminated Composite Armors, *Doktora Tezi, O.D.T.Ü.* Fen Bilimleri Enstitüsü, Ankara.

[42] "OWASP Top 10 – 2017 The Ten Most Critical Application Security Risks" erişim adresi: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf, erişim tarihi: 07 Mayıs 2019.

[43] Gıannını, N.J., 2015, Vulnerable , *Master's Thesis, University of Rhode Island.* Computer Science and Statistics, Island.

[44] "Oturum Açma Giriş Sınırlandırma Eklentisi" erişim adresi: https://webinyo.com/wordpress-oturum-acma-giris-sinirlandirma-eklentisi-limit-login-attempts.html, erişim tarihi: 15 Mart 2019.

[45] Ardıç, A., Cisco Webex XEE Zafiyeti, Cezeri Siber Güvelik Akademisi Yayın Kurulu, 1, 2017.

[46] AbuSeada, W., 2017, Alternative Approach to Automate Detection of DOM-XSS Vulnerabilities , *Master's Thesis, University of Tartu.* Institute of Computer Science, Statistics, Tartu.

[47] Nahari, H., Krutz, R.L., Web Commerce Security Design and Development: Threats and Attacks, *Wiley Publishing, Inc.*, Indianapolis, Indiana, 2011.

[48] "Trustwave Global Security Report: Spam As a Percentage of Total Inbound Mail" erişim adresi: https://trustwave.azureedge.net/media/15350/2018-trustwave-global-security-report-prt.pdf?, erişim tarihi: 15 Mayıs 2019.

[49] Rani, P., Attack Prevention Methods for DDoS Attacks in Manets, Asian Journal Of Computer Science And Information Technology, 1, 18-21, 2011.

[50] Rani, C., Gowda, V., 2015, System Security, Threat Detection and Prevention Measures of Autonomous Systems , *Master's Thesis, University of Texas At Arlington.* Science in Electrical Engineering, Arlington, Texas.

[51] Bhuyan, M.H., Kashyap H.J., Bhattacharyya, D.K. and Kalita, J.K., Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions, y Oxford University Press on behalf of The British Computer Society, 1, 18-21, 2013.

[52] "Threat Report: Distributed Denial of Service (DDoS)" erişim adresi: https://www.nexusguard.com/hubfs/Threat%20Report%20Q2%202018/Nexusguard_DDoS_Threat_Report_Q2_2018_EN.pdf, erişim tarihi: 15 Mart 2019.

[53] "Spam and phishing Report: Sources of spam by country" erişim adresi: https://securelist.com/spam-and-phishing-in-q1-2019/90795/, erişim tarihi: 15 Mart 2019.

[54] Pirscoveanu, R.S., 2015, Clustering Analysis of Malware Behavior, *Master Thesis, Aalborg University.* Institute of Electronic Systems, *Niels Jernes Vej*.

[55] "Insider Threat 2018 Report: It Assets at Risk" erişim adresi: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, erişim tarihi: 17 Mayıs 2019.

[56] "Number of compromised data records in selected data breaches as of November 2018 (in milllions)", erişim adresi: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/, erişim tarihi: 19 Mart 2019.

[57] "Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study" erişim adresi: https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new, erişim tarihi: 22 Mayıs 2019.

[58] Narain, P., 2018, Ransomware - Rising Menace to an Unsuspecting Cyber Audience, *Master's Thesis, University of Houston.* Information System Security, Calhoun Rd, Houston.

[59] "Ransomware", https://www.us-cert.gov/security-publications/Ransomware, erişim tarihi: 29 Nisan 2019.

[60] "2018 Sonicwall Siber Tehdit Raporu", http://www.m2s.com.tr/bulten/2018_Sonicwall_siber_tehdit_raporu-TR.pdf, erişim tarihi: 29 Nisan 2019.

[61] "Cyber Security Breaches Survey 2016", Social Research Institute & Institute for Criminal Justice Studies, University of Portsmouth, Erişim adresi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf, erişim tarihi: 27 Aralık 2018.

[62] Yıldırım, E.Y., Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması, Mesleki Bilimler Dergisi (MBD), 7(2), 24-33, 2018. Retrieved from: http://dergipark.gov.tr/mbd/issue/40281/442848

[63] "EY Global Information Security Survey 2018-19", Is Cybersecurity about more than protection, Erişim adresi: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf, erişim tarihi: 27 Aralık 2018.

[64] "T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, erişim tarihi: 11 Nisan 2019.

[65] Yıldız, M., 2014, Siber Suçlar ve Kurum Güvenliği, *Denizcilik Uzmanlık Tezi, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı*, Ankara.

[66] Sheikhpour, R., Modiri, N., An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls, International Journal of Security, 6(2), 18-21, 2012.

[67] Mariani, M.E., 2001, Firewall Strategies using network processors, *Master's Thesis, University of Rochester*. Rochester Institute of Technology, 252 Elmwood Ave., Rochester, NY.

[68] Cannady, J., Artificial neural networks for misuse detection, In National information systems security conference, 1998.

[69] Mukhopadhyay, I., Chakraborty, M. and Chakrabarti, S., A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems, Journal of Information Security, 2, 28-38, 2011.

[70] Scarfone, K., Mell, P., "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication, 800-94 February 2007.

[71] Valburg, S.V., 2018, Fuzzing OpenVPN, *Master's Thesis, Radboud University*. Computer Science, Nijgemen.

[72] Shrestha, N., 2012, Security Assessment via Penetration Testing: A Network and System Administrator's Approach, *Master's Thesis, University of Oslo.* Department of Informatics, P.O. Box 1072 Blindern 0316 Oslo.

[73] Herzog, P., "The Open Source Security Testing Methodology Manual" erişim adresi: http://www.isecom.org/mirror/OSSTMM.3.pdf, erişim tarihi: 28 Mayıs 2019.

[74] Şahinaslan, Ö., 2013, Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma, *Doktora Tezi, Trakya Üniversitesi.* Fen Bilimleri Enstitüsü, Edirne

[75] "High Level Organization of the Standard", http://www.pentest-standard.org/index.php/Main_Page, erişim tarihi: 25 Mayıs 2019.

[76] Appiah, K.A., 2014, Network and Systems Security Assessment using penetration testing, *Master's Thesis, Kwame Nkrumah University of Science and Technology*. Department of Information Technology, Kumasi, Ghana.

[78] Muharremoğlu, G., 2013, Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı ve Savunma Ögelerinin İncelenmesi, Yüksek Lisans Tezi, İstanbul Üniversitesi. Fen Bilimleri Enstitüsü, İstanbul.

[78] "Shodan Search Engine" erişim adresi: https://www.shodan.io/, erişim tarihi: 28 Mayıs 2019.

[79] "Free online network tools" erişim adresi: https://centralops.net/co/, erişim tarihi: 28 Mayıs 2019.

[80] "Maltego" erişim adresi: https://docs.maltego.com/support/home, erişim tarihi: 01 Haziran 2019

[81] Baykara, M., Daş, R. ve Karadoğan, İ., Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, 1st International Symposium on Digital Forensic and Security (ISDF'13), 231-239, Elazığ, Türkiye, Mayıs 2013.

[82] "Definition – What does Tcpdump mean? erişim adresi: https://tools.kali.org/maintaining-access/sbd, erişim tarihi: 29 Mayıs 2019

[83] Altuntaş, A., E.U., Metasploit ve Penetrasyon Testleri, *Kodlab Yayıncılık,* Bağcılar, İstanbul, 2016.

[84] Yalçınkaya, M.A. ve Küçüksille, E.U., Uygulamalı Sızma Testleri, *Abaküs Yayıncılık*, Kadıköy, İstanbul, 2016.

[85] Beecroft, A.J., 2009, Passive Fingerprinting of Computer Network Reconnaissance Tools, *Master Thesis, Naval PostGraduate School.* Science in Information Warfare Systems Engineering, *Montery, California.*

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: Adır, Arif Emre
Uyruğu	: Türkiye
Doğum tarihi ve yeri	: 11.03.1981 Konya
Medeni hali	: Evli
Telefon	: 05321639009
e-mail	: a.emreadir@gmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet tarihi**
Lisans	Lefke Avrupa Üniversitesi/ Bilgisayar Mühendisliği	2011

İş Deneyimi

Yıl	**Yer**	**Görev**
2011-2019	Konya Büyükşehir Belediyesi	Bilgisayar Mühendisi

Yabancı Dil

İngilizce