BİLİŞİM SUÇLARINA YÖNELİK IP TABANLI DELİL TESPİTİ

M. Zekeriya GÜNDÜZ

Yüksek Lisans Tezi
Elektronik ve Bilgisayar Eğitimi Anabilim Dalı
Danışman: Yrd. Doç. Dr. Resul DAŞ
OCAK-2013

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SUÇLARINA YÖNELİK IP TABANLI DELİL TESPİTİ

YÜKSEK LİSANS TEZİ

M. Zekeriya GÜNDÜZ

(Enstitü No: 101131108)

Tezin Enstitüye Verildiği Tarih : 06 Aralık 2012
Tezin Savunulduğu Tarih : 20 Aralık 2012

Tez Danışmanı : Yrd. Doç. Dr. Resul DAŞ (F.Ü)

Diğer Jüri Üyeleri : Doç. Dr. İbrahim TÜRKOĞLU (F.Ü)

Yrd. Doç. Dr. Ömür AYDOĞMUŞ (F.Ü)

OCAK-2013

TEŞEKKÜR

Bilişim alanında meydana gelen gelişmelerin takip edilmesi ve özellikle bilişim suçları konusunun yeni bir çalışma alanı oluşturduğunun farkına varılması konusunda bana yön gösteren ve bilişim suçları alanında yüksek lisans çalışmaları yapmam için bir yol gösterici olan başta sayın hocam Doç. Dr. İbrahim TÜRKOĞLU'na ve çalışmalarım konusunda uygulamalı olarak sahip olduğu tecrübeleri ile çalışmalarımda beni yönlendiren, akademik anlamda çalışma sistematiğini öğrenmem için gayretlerini esirgemeyen ve çalışmalarımla yakından ilgilenerek iyi bir temel üzerinde ilerlemem için gayretleriyle beraber zamanını da benden esirgemeyen sayın danışman hocam Yrd. Doç. Dr. Resul DAŞ'a ilgi, sabır ve anlayışlarından dolayı teşekkür ederim.

M. Zekeriya GÜNDÜZ

İÇİNDEKİLER

Sayfa No

KISALTMALAR

ABD : Amerika Birleşik Devletleri

ADSL : Asymetric Digital Subscriber Line (Asimetrik Sayısal Abone Hattı)

ARP : Address Resolution Protocol (Adres Çözümleme Protokolu)

BHO : Browser Helper Object (Tarayıcı Yardımcı Nesnesi)

CD-ROM : Compact Disk-Read Only Memory (Kompakt Disk-Salt Okunur Bellek)

CGI : Common Gateway Interface (Ortak Ağgeçidi Arayüzü)

CHP : Cumhuriyet Halk Partisi

CMK : Ceza Muhakemesi Kanunu

CPU : Central Processing Unit (Merkezi İşlem Birimi)

DDoS : Distributed Denial of Service (Dağıtık Hizmet Aksattırma Saldırıları)

DNA : Deoksiribo Nükleik Asit

DNS : Domain Name Server (Alan Adı Sistemi)

DoS : Denial of Service (Hizmet Aksattırma Saldırıları)

DVD-ROM : Digital Versatile Disk - Read Only Memory
(Sayısal Çok Yönlü Disk - Salt Okunur Bellek)

EGM : Emniyet Genel Müdürlüğü

GPL : General Public License (Halka Açık Lisans)

GPRS : General Packet Radio Service (Genel Paket Radyo Servisi)

GPS : Global Positioning System (Küresel Konumlama Sistemi)

HDD : Hard Disk Drive (Sabit Disk Sürücü)

HUMK : Hukuk Usulü Muhakemeleri Kanunu

HTML : HyperText Markup Language (İleri Metin İşaretleme Dili)

HTTP : HyperText Transfer Protocol (İleri Metin Aktarım Protokolü)

HTTPS : HyperText Transfer Protocol Secure (Güvenli İleri Metin Protokolü)

IDS : Intrusion Detection System (Saldırı Tespit Sistemi)

IEEE : Institue of Electrical and Electronics Engineers
(Uluslar Arası Elektrik Elektronik Mühendisleri Enstitüsü)

IP : Internet Protocol (İnternet Protokolü)

IPSEC : Internet Protocol SECurity

IRC : Internet Relay Chat (İnternet Aktarmalı Sohbet)

ISO : International Standards Organization
(Uluslararası Standartlar Örgütü)

LAN : Local Area Network (Yerel Alan Ağı)

MAC : Media Access Control (Ortam Erişim Denetimi)

MIT : Massachusetts Institute of Technology
(Massachusetts Teknoloji Enstitüsü)

NAT : Network Address Translation

NIC : Network Interface Card (Ağ Arayüz Kartı)

OEM : Orijinal Equipment Manufacturer (Orijinal Ürün Üreticisi)

OS : Operating System (İşletim Sistemi)

OSI : Open Systems Interconnection

P2P : Pear to Pear (Eşten Eşe)

PDA : Personal Digital Assistant (Kişisel Sayısal Asistan)

PING : Packet Internet Groper (Paket İnternet Yoklayıcı)

RAM : Random Access Memory (Rastgele Erişimli Bellek)

ROM : Read Only Memory (Sadece Okunabilir Bellek)

RAT : Remote Administration Tool (Uzaktan Yönetim Aracı)

SET : Secure Elektronic Transactions

SMB : Server Message Block

SSH : Secure SHell

SSL : Secure Socket Layer

TCK : Türk Ceza Kanunu

TCP : Transmission Control Protocol (İletim Denetim Protokolü)

TDK : Türk Dil Kurumu

TSE : Türk Standartları Enstitüsü

TTNET : Türk Telekom Net

UTP : Unshielded Twisted Pair (Kaplamasız Dolanmış Çift Kablo)

VPN : Virtual Private Network (Sanal Özel Ağ)

ŞEKİLLER LİSTESİ

Sayfa No

TABLOLAR LİSTESİ

Sayfa No

ÖZET

İnternet üzerinden işlenen bilginin miktarı ve değerinin artması, bütün dünya ile çok kısa bir sürede bağlantı kurulabilmesi, suçluların da ilgisini çekmiş ve internete yönelmelerini sağlamıştır. Bu yeni dünyaya çok hızlı adapte olan suçlular, kendilerini teknoloji alanında da hızlı bir şekilde geliştirmiş, normal yollar ile oldukça zor gerçekleşecek suçları, internet ortamından kolay bir şekilde yapabilmeye başlamışlardır. Bilişim suçları olarak adlandırılan bu suçlar, sanal ortamda kişi veya kişiler tarafından bir sisteme veya herhangi bir bilişim cihazına izinsiz girme veya saldırıda bulunmadır.

Hazırlanan bu tez çalışmasında bilişim suçları konusu detaylı olarak ele alınmış, konu ile alakalı henüz tam olarak sınırları belirlenmemiş kavramlar için sınırlar çizilmeye çalışılmış, gerçek hayatta yapılmış saldırı türleri incelenmiştir. Ayrıca, en büyük ağ sistemi olarak bilinen internet ortamındaki ağlarda ve yerel ağlarda bilgisayarlarlara yapılan saldırıların varlığının belirtilerinden bahsedilmiştir.

Yapılan çalışmalar ve literatür taraması sonucunda bilişim suçlarının tespitine yönelik yapılan çalışmalar incelenmiştir. Bilgisayar ağ sistemlerinde yapılan saldırıların, IP tabanlı delil tespitinin yapılması konusunda uygulamalar yapılarak, elde edilen sonuçlara göre; son kullanıcıları ve sistem yöneticilerini yakından ilgilendiren eksiklikler ve alınabilecek önlemler hakkında değerlendirmeler yapılmıştır.

Anahtar Kelimeler: Bilişim Suçları, Ağ Güvenliği, Kötücül Casus Yazılımlar, Ağ Saldırıları, Bilgi Güvenliği, IP Tabanlı Delil Tespiti

SUMMARY

IP-Based Evidence Detection

The rise of the quantity and value of the information committed via internet, establishing a connection with the whole world in a very short period of time has attracted the attention of criminals and made them lean to the internet. The criminals adapting to this new world quickly has also improved themselves in the technology area and started to commit crimes through the internet easily, which are very hard to commit in normal ways. These crimes called as cyber crimes are intruding or attacking to a system or any informatic device by the person or persons in virtual platform.

In this thesis work, cyber crimes have been discussed in detail, and it has been tried to demarcate the concepts relevant to the subject, which are not actually demarcated, and types of attacks made in real life has been examined. Furthermore, signs of the presence of attacks on computers in the internet media networks known as the largest network and local networks have been discussed.

As a result of the studies and review of the literature, the studies for the determination of cyber crimes have been examined. By performing applications about IP based recording of evidence of the attacks on computer network systems, according to the results, the evaluation has been made about the deficiencies and precautions involving end users and system administrators.

.

Key Words: Cyber Crimes, Network Security, Malware Spyware, Network Blitzs (Network Attacks), Information Security, IP-Based Evidence Detection (IP-Based Recording Of Evidence)

1. GİRİŞ

1.1. Tez Çalışmasının Amacı

Bilişim dünyasında bilgi ve bilgi varlıklarının öneminin gün geçtikçe artması, buna paralel olarak bilişim güvenliğinin öneminin de artmasını ortaya koymaktadır. Uluslar arası bir ağ sistemi olan internet ortamındaki verilerin veya bilgilerin korunması için donanımsal ve yazılımsal güvenlik tedbirleri alınmaktadır; ancak bu tedbirler sisteme veya bilişim cihazlarına yapılan saldırıları tamamen engelleyememektedir. Bu bağlamda bilişim suçlarının incelenmesi, saldırganların tespit edilmesi için birçok akademik ve ticari çalışmalar yapılmaktadır.

Bu tez çalışmasında da kapsamlı literatür taraması yapılarak bilişim suçları, bilgi ve bilgi güvenliği ile bilgisayar ağ güvenliği ve IP numaralarından yararlanarak saldırganların tespit edilmesi konuları detaylı olarak incelenmiştir. Ayrıca, bu konularda bilişim suçlarına örnek teşkil edecek saldırılar incelenmiştir.

1.2. Tez Çalışmasının Kapsamı

2. bölümde, bilişim suçları ile doğrudan ilişkili olan temel kavramlar açıklanmıştır. Bu kavramlarda bilişim suçları, işlenme nedenleri, saldırgan, bir bilişim suçu işlenirken bu suçu doğrudan veya dolaylı olarak ilgilendiren tanımlamalar gibi temel kavramlar verilmiş olup hukuksal açıdan kullanılması gereken dijital delillerin özelliklerinden bahsedilmiştir.

3. bölümde, bilgi ve bilgi güvenliği konusu ele alınarak, kötücül yazılımlar hakkında genel bilgiler ve bu kötücül yazılımlara karşı alınabilecek tedbirler incelenmiştir. Ayrıca bilgi güvenliğinin ülkemizdeki kurum ve kuruluşlarda standardize edilebilmesi için hazırlanan sertifikasyon işlemleri hakkında genel bilgiler verilmiştir.

4. bölümde, bilgisayar ağ ortamında teknik anlamda yapılan saldırılar ve belirtileri, ağ güvenliği için alınabilecek tedbirler ve ağı izlemek için kullanılabilecek güvenlik araçlarından bazıları hakkında bilgiler verilmiştir.

5. bölümde, ağ üzerinde bilgi çalmak üzere yapılan bir saldırı, uygulamalı olarak gösterilmiş ve bu saldırıyı gerçekleştiren saldırganın IP numarası üzerinden tespitinin nasıl gerçekleştirilebileceği adım adım gösterilmiştir.

6. bölümde ise tez çalışmasının genel anlamdaki sonuçlarından yola çıkarak değerlendirmeler yapılmış, öneriler ve ileriye dönük yapılabilecek akademik çalışmalar belirtilmiştir.

Hazırlanan bu tez çalışmasının, ülkemizde bilgi ve bilgisayar güvenliği ile ilgilenen kişi ve kurumlara ışık tutmasının ve konunun öneminin doğru bir şekilde kavranmasının sağlanması için ön bilgi olarak yardımcı olması ümit edilmektedir.

2. BİLİŞİM SUÇLARI

2.1. Giriş

Büyük bir ivme ile önemi artmakta olan bilgi güvenliği ve gün geçtikçe artan bilişim suçlarının adli olarak incelenmesi konuları büyük önem kazanmaktadır. Bu bölümde bilişim suçları ile ilgili olabilecek temel kavramlar ve önemli hususlar açıklanmaktadır.

Bilişim suçları son yüzyılda ortaya çıkan bir ifade olduğundan bazı kavramların birleşimi ile kendisine tanım bulmaya çalışmıştır. Bu kavramlar tanımlanarak bilişim suçu tanımı daha iyi anlaşılabilecektir.

Hukuki anlamda *suç*, bir toplumdaki hukuki kurumlar tarafından ceza veya güvenlik tedbiri yaptırımına bağlanmış fiildir [1]. Uygulamada ise suç; başka insanların veya tüzel kişiliklerin haklarına tecavüz etmek veya yanlış ya da zararlı olduğu için yasaklanan ve bazı durumlarda cezalandırılan davranış olarak tanımlanabilir [2]. Suçu gerçekleştiren kişiye *suçlu* denir. Hukuki anlamda bir kimsenin suçlu kabul edilebilmesi için suçun o kimse tarafından işlendiğinin hukuki süreçler sonucunda somut deliller ile ispatlanması gerekmektedir.

Bilişim, insanoğlunun kullandığı tüm telekomünikasyon araçları başta olmak üzere ağ haberleşme sistemleri, bilgisayarlar, uydu sistemleri gibi iletişim içeren ve insan hayatını kolaylaştırmaya yönelik tasarlanan sistemleri kapsar. Bilişim sistemlerinin insan hayatında vazgeçilmezler arasına girmesi, beraberinde bazı sorunları da getirmektedir. Bu sorunların en öne çıkanı sanal ortamdaki bilgi hırsızlığıdır. Bu sanal ortamdaki sorunlar ise bilişim suçu kavramını ortaya çıkarmıştır.

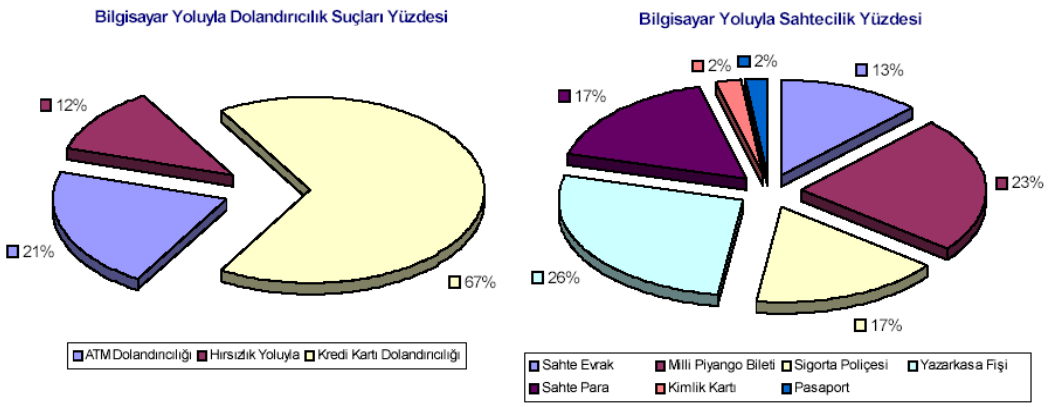
En genel tanımıyla bilişim alanında kullanılan araçlardan yararlanılarak işlenilen suçlar, *bilişim suçu* olarak tanımlanmaktadır. Bununla beraber bilişim suçları TCK'de bilişim sistemleri kullanılarak işlenen suçlar olarak tanımlanmaktadır [3]. Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması da, bilişim suçları olarak tanımlanmaktadır [4]. Bilişim suçları, klasik suçlar gibi değerlendirme sürecinde işlenme sebebinden başlanarak, mahkemelere intikal edecekleri süreye kadar dikkatli bir şekilde irdelenmelidir. Özellikle kolluk kuvvetlerinin ülkemizde konunun önemini anlayarak ciddi çalışmalar yaptıkları görülmektedir.

Günlük hayatın bir yansıması olarak görebileceğimiz sanal alem, aslında günlük hayattaki olayların benzerlerini bünyesinde barındırmaktadır. Normal bir suçu işlemek için en mantıklı cevap ne ise, aynı durum benzer şekilde sanal alemde işlenen bilişim suçları içinde geçerlidir. Örneğin; bir bankayı soymak için bankaya soygun amaçlı giren ve yakalanan ancak hapisten çıkınca tekrar banka soymak için bankaya soygun amaçlı saldıran saldırgana sorulan neden hep bankayı soymaya çalışıyorsun sorusuna "bana çok para lazım ve çok parada bankada bulunur" şeklinde verdiği cevap enteresandır [5].

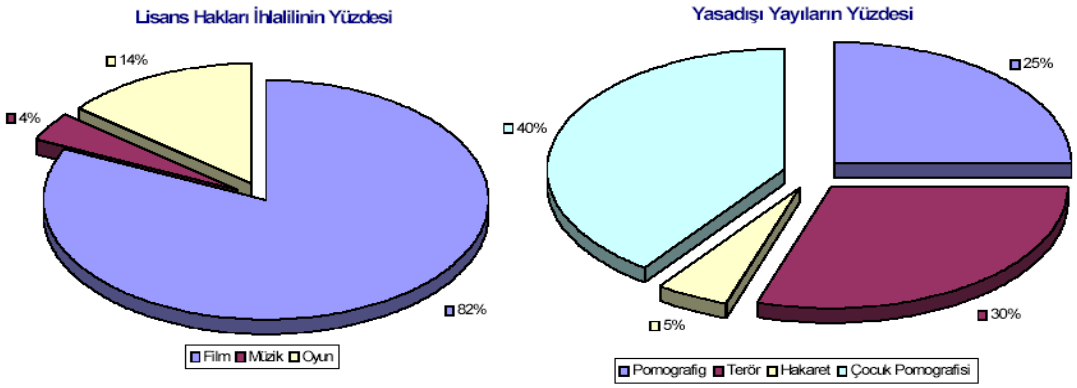
Buna paralel olarak sanal ortam düşünüldüğünde, geleneksel bir suçun işlenmesindeki sebeplerin benzerlerinin bilişim suçlarında da olduğunu görürüz. Bu sebepler maddi kazanç elde etmek, kişilerin itibarını sarsmak, intikam almak, sosyal hayatta insanlara aktaramadığını sanal ortamda gerçekleştirmek, karalamak veya yakalanma ihtimalinin zor olduğunu düşünerek zevk amaçlı saldırı yapmak gibi sebepler olarak ortaya çıkmaktadır. Sanal ortamda insanlar bu soyguncunun açık bir şekilde dile getirmiş olduğu ifadeyi kimseye hesap vermeme duygusu içinde işleyebilmektedirler.

2.2. Ülkemizde Bilişim Suçlarının Durumu ve Örnekler

2002'li yıllara kadar ülkemizde ciddi anlamda bilişim suçu işlenmemiş iken son on yıl içerisinde büyük bir ivme kazanarak bu suçların sayıları artmaktadır. Yakın bir zamanda EGM'nin yapmış olduğu bir araştırmada ülkemizde son zamanlarda işlenen bazı bilişim suçlarının oranları tespit edilmiştir. Bu tespitler Şekil 1 ve Şekil 2'de grafiksel olarak belirtilmiştir.



Şekil 1. Bilişim suçları işlenme oranları [6].



Şekil 2. Bilişim suçları işlenme alanları [6].

Ülkemizde meydana gelen bilişim suçlarına somut örnekler vermek de mümkündür. Özellikle Şekil 3'de gösterilen ve CHP eski genel başkanının şahsına yapılan ve sanal ortamda ülkemiz dışındaki bir sunucudan yayılan mahremiyete dair video görüntüleri bilişim suçlarının artık günümüzde her şekilde kullanılabileceğini göstermektedir.

Şekil 3. Bilişim suçu örneği [7].

Ülkemizde en çok karşılaşılan bilişim suçları örnekleri aşağıdaki şekilde sıralanabilir [8, 9]:

- Başkalarının adına e-mail göndererek özellikle ticari ve özel ilişkileri zedelemek,
- Başkalarının adına web sayfası hazırlayarak şahıs hakkında başta telefon ve e-mail adresi olmak üzere kişisel bilgileri vermek,
- Kişisel ya da kurumsal bilgisayarlara yetkisiz erişim ile bilgilerin çalınması ve karşılığında tehdit ederek maddi menfaat sağlamak,

- Şirketlere ait web sayfalarının alan adının izinsiz alınması ve bu alan adlarının karşılığında yüklü miktarlarda para talep etmek,
- Özellikle pornografik içerikli CD kopyalamak ve satmak,
- Sahte evrak basmak,
- Terörü destekler ve ahlaka aykırı içerikler bulunduran siteler yapmak ve yayınlamak,
- Lisans hakkı olan yazılımların lisans haklarına aykırı olarak kullanmak,
- Kişilerin mahremiyetine ait bilgileri sanal ortamda paylaşmak.

Bu ve benzeri bir bilişim suçuna maruz kaldığını düşünen şahısların Cumhuriyet Başsavcılığına başvurmaları neticesinde gerekli incelemeler kolluk kuvvetlerinin adli bilişim birimleri tarafından yapılmaktadır.

Bilişim suçları şu şekilde sınıflandırılabilir:

1. Bilgisayar sistemlerine ve servislerine yetkisiz erişim ve dinleme.
2. Bilgisayar sisteminin çalışmasını engellemek.
3. Bilgisayar yoluyla dolandırıcılık.
4. Bilgisayar yoluyla sahtecilik.
5. Kanunla korunmuş bir yazılımın izinsiz kullanılması.
6. Yasadışı yayınlar.

İnternetin yaygınlaşması ile bilişim suçu olarak tanımlayamayacağımız ancak millet menfaatine gibi görünen olaylarda mevcuttur. Bu olaylara somut bir örnek verilirse, mesai saatleri içerisinde bankada sıra bekleyerek işlemlerini tamamlamak isteyen müşterilerle ilgilenmeyen bir çalışanın, bilgisayarında oyun oynadığının görüntülenmesi ve görüntülerin internet ortamına aktarılması olayları da mevcuttur. Bu durum, suç kabul edilmeyip millet menfaatine gözüktüğünden görüntüyü internete aktaran kişi hakkında inceleme başlatılmamış olup, bilişim suçu kapsamına alınmamıştır. Bunun gibi binlerce örnekler verilebilir.

Ülkemizde artan bilişim suçlarının incelenmesi ve hukuki anlamda kontrolün sağlanması için çalışmalar yapıldığı görülmekte ancak uygulamada henüz istenen seviyeye ulaşılamadığı anlaşılmaktadır.

2.2.1.TCK' de Bilişim Suçları

Dünyada bilgisayar suçlarına yönelik ilk yasa *Bilgisayar Dolandırıcılığı ve İstismarı Yasası* 1986 yılında kabul edilmiştir. Ülkemizde ise konu ile alakalı kanunlar

2004 yılında yürürlüğe girmiştir [10]. Bilişim sistemlerine zarar verme ve bu sistemlerden veri çalmaya yönelik yapılan suçların kapsamı ve müeyyideleri TCK'nin şu maddelerinde belirtilmektedir:

Madde 243. Bilişim sistemine girme.

1. Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye iki yıla kadar hapis veya adli para cezası verilir.

2. Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

3. Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, iki yıldan dört yıla kadar hapis cezasına hükmolunur.

Madde 244. Sistemi engelleme, bozma, verileri yok etme veya değiştirme.

1. Bir bilişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka bir yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

2. Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

3. Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur.

Madde 245. Banka veya kredi kartlarının kötüye kullanılması.

1. Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adli para cezası ile cezalandırılır.

2. Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

Madde 246. Tüzel kişiler hakkında güvenlik tedbiri uygulanması.

1. Bu Bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur [11].

Bu maddelerle beraber TCK'de bilişim suçları vasıtası ile işlenen suçlar ve müeyyideleri ile ilgili maddeler şu şekildedir:

Madde 124. Haberleşmenin engellenmesi.

Madde 125. Hakaret.

Madde 132. Haberleşmenin gizliliğini ihlal.

Madde 133. Kişiler arası konuşmaların dinlenmesi ve kayda alınması.

Madde 135. Kişisel verilerin kaydedilmesi.

Madde 136. Verileri hukuka aykırı olarak verme veya ele geçirme.

Madde 142. Nitelikli hırsızlık.

Madde 158. Nitelikli dolandırıcılık.

Madde 226. Müstehcenlik.

2.3. Bilişim Suçlarında Kullanılan Dijital Deliller

İşlenen bir suçun aydınlatılabilmesi için suç ortamında bulunan kanıtların tespit edilip geçerliliğini kaybetmeden kullanılabilmesi başlı başına çalışılması gereken bir konudur. Bilişim dünyasındaki bu kanıtları ve özelliklerini iyi bilmek bilişim suçlarının aydınlatılmasında önemli bir etkendir.

Delil: İşlenen bir suç olayında fail/faillerin ortaya çıkarılabilmesi için ipuçları niteliğinde toplanan kaynaklar *delil* olarak tanımlanır. Bu deliller, aydınlatılması istenen olayın en önemli parçalarıdır. Bu elde edilen deliller bir araya getirilerek tüm resim görülmeye çalışılır. Böylece aydınlatılmak istenen olay bir çözüme kavuşturulmuş olur.

Delillendirme: Suçların tespiti ve yargılanmasındaki en önemli husus *delillendirme* olarak tanımlanmaktadır. *Delillendirme* kısaca, bir suç ile ilgili o suçun kim tarafından ve ne şekilde işlendiğini ispat edici nitelikte bilgiler elde edilmesi ve bunun adli mercilere sunulması şeklinde tanımlanabilir.

Dijital Delil: Sanal ortamda işlenen suçlardaki, suçluların tespit edilmesi için elde edilen kanıtlar *dijital delil* olarak isimlendirilmektedir. Shinder'e göre "bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere dijital delil" denilmektedir [12]. Chisum ise dijital delilleri "bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler" olarak tanımlamıştır [13]. Son olarak Casey'in tanımına göre dijital deliller "bir suçun işlendiğini gösteren veya

suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler" olarak karşımıza çıkmaktadır [14,15].

Bilişim suçları kapsamında dijital deliller çok büyük önem arz etmektedir. Dijital deliller yapı itibariyle çok hassas oldukları için toplanmasında, araştırılmasında, taşınmasında ve sunulmasında belirli prosedür ve süreçleri izlemek şarttır.

2.3.1.Dijital Delillerin Özellikleri

Sanal ortamda kullanılan dijital deliller genel olarak aşağıda belirtilen özelliklere sahiptirler.

- Dijital deliller, parmak izi veya DNA gibi gizli veriler olabilirler.
- Dijital deliller, kolaylıkla ve hızla sınırları aşabilirler.
- Dijital deliller, kolaylıkla değiştirilebilir, zarar verilebilir veya silinebilirler.
- Dijital deliller, bazen zaman ile sınırlı olabilirler.
- Dijital deliller, genellikle uçucu verilerdir.
- Dijital deliller, güvenliği sağlanmaz ise çok erken deformasyona uğrayabilirler.
- Dijital deliler, yapı itibariyle, fiziksel delillere göre daha hassas ve kolay bozulur niteliktedirler.

Dijital deliller, normal somut delillere göre yapı itibariyle bazı sıkıntıları barındırmaktadırlar. Bu sıkıntılar şu şekilde özetlenebilir:

- **Dijital Delillerin Bütünlüğü:** Dijital veriler üzerinde çok kolay bir şekilde değiştirme, silme ve yenisini oluşturma gibi işlemlerin yapılabilmesi bu delillerin bütünlüğünü sağlamayı zorlaştırmaktadır.
- **Dijital Delillerin Doğrulanması:** Bir kişiyi dijital delillerle birlikte yakaladıktan sonra mahkeme sürecinde o verilerin gerçekten o kişiye ait olduğunun ispatı gerekmektedir. Fakat delil olarak ele geçirilen verilerin aynısı her hangi bir kişi tarafından da oluşturulabilir. Hatta sanık bu verilerin daha sonra, polis tarafından bile oluşturulduğunu iddia edebilir.
- **Dijital Delillerin İnkar Edilememesi:** Dijital delillendirme işlemindeki dijital delilin sahibi, onu ele geçiren şahıslar (Ör: Kolluk kuvvetleri, polis), delilin alındığı medya, delilin ele geçirildiği zaman, delilin içeriği gibi bütün unsurların daha sonradan inkar edilememesi gerekmektedir.

- **Dijital Delillerin Doğruluğu:** Dijital delillerin ele geçirilmesi esnasında kullanılan teknikler ve kullanılan bilgilerin doğruluğunun ispatı gerekir. Örneğin, delilin ele geçirilme zamanını ispatlamak önemlidir.
- **Dijital Delillerin Daha Sonradan Ele Alınabilirliği:** Dijital deliller oluşturulduktan sonra, bu delilleri üçüncü bir şahıs inceleyebilmelidir [15,16].

Dijital deliller mahkemeye güvenli bir şekilde taşınabilirse delil olarak kullanılabilirler.

2.3.2.Dijital Delillerin Bulunduğu Yerler

Dijital delil kaynakları bilişim sistemleri açısından üç farklı grupta düşünülebilir.

1- Açık Bilgisayar Sistemleri: Harddisk, klavye, monitör gibi aygıtlardan oluşan (dizüstü, masaüstü, sunucu gibi) klasik bilgisayar sistemleri, dijital deliller yönünden oldukça zengin birer kaynak teşkil etmektedirler. Bu sistemler üzerinde basit olarak görünen bir dosyanın, oluşturulma zamanı, değiştirilme zamanı ve kim tarafından oluşturulduğu bilgileri bazen suça yönelik çok önemli deliller sağlayabilir.

2- İletişim Sistemleri: Geleneksel telefon sistemleri, kablosuz haberleşme sistemleri, internet ve bilgisayar ağları gibi birçok iletişim sistemi üzerinde, oldukça fazla dijital delile rastlamak mümkündür. Örneğin; internet üzerinden gönderilmiş bir e-posta mesajındaki gönderilme zamanı, kimin gönderdiği, mesajın içeriği gibi konular, delillere ulaşma noktasında oldukça büyük önem arz ederken, mesajın geçtiği sunucular, yönlendiriciler gibi aradaki sistemlerin üzerindeki kayıtlar da, ele geçirilen mesaj ile ilgili bazı hususları doğrulama noktasında, pekiştirici bilgi olarak kullanılabilmektedirler.

3- Gömülü Bilgisayar Sistemleri: Mobil telefonlar, PDA cihazları, akıllı kartlar gibi gömülü bilgisayar sistemlerinin birçoğu, dijital delillere kaynak teşkil edebilmektedirler. Örneğin GPRS, GPS gibi sistemler, araçların nerede olduğunun tespiti için kullanıldığı gibi, araçların üzerine yüklenecek gömülü bilgisayar sistemine sahip modüller sayesinde aracın hızı, frenlerin durumu, etkiden önceki 5 saniye içerisindeki işlevler gibi bir kaza esnasında oldukça yararlı ve kazayı aydınlatıcı bilgilere ulaşılabilmektedir. Günümüzde, gömülü bilgisayar sistemlerine sahip mikro dalga fırınlar, internet üzerinden bilgi alışverişi yapabilmekte ve bazı ev aygıtları, kablosuz ağ veya internet kullanılarak uzaktan kumanda edilebilmektedir. Teknolojinin bu seviyede olduğu bir ortamda, mikrodalga üzerinden elde edilecek veriler, bir kundakçılık olayında fırının belirli bir zamanda yangın çıkarmak için programlandığını ortaya çıkarabilmektedir [15,16].

Bilişim suçlarında dijital delillerin elde edildiği birçok kaynak olabilir. Bunlar genel olarak şu şekilde sıralanabilir:

- Bilgisayar sistemleri (masaüstü, dizüstü, sunucu vb.)
- Bilgisayar bileşenleri (HDD, memory v.b.)
- Erişim kontrol araçları (smart kartlar, biometrik tarayıcılar v.b.)
- Çağrı cihazları
- Dijital kameralar
- PDA ve PALM cihazları (el bilgisayarları)
- Harici harddiskler
- Hafıza kartları
- Network araçları (modem, yönlendirici, anahtar)
- Yazıcılar, tarayıcılar ve fotokopi makineleri
- Çıkarılabilir yedekleme üniteleri (disket, CD, DVD, kartuş, kaset ve teypler)
- Telefonlar
- Kredi kartı okuyucuları
- Dijital saatler
- GPS

Farklı çeşitlilikte bulunan dijital delillerin birçok farklı tipleri de mevcuttur. Bunlardan bazıları şu şekildedir:

- Veri dosyaları
- Kurtarılmış, silinmiş dosyalar
- Kayıp alanlardan kurtarılmış veriler
- Dijital fotoğraf ve videolar
- Sunucu kayıt dosyaları
- E-posta
- Sohbet (chat) kayıtları
- İnternet geçmişi
- Web sayfaları
- Erişim kayıtları veya kütükleri
- Abone kayıtları
- Ses kayıtları.

Dijital delillerin elde edildiği alanlardan en çok göze çarpanları şunlardır:

- Kuruluş kaynakları
- Geniş alan ağları
- Bilgisayarlar (masaüstü, dizüstü bilgisayar, PDA, sunucu, istemci)
- Elektronik aygıtlar
- Veri havuzları
- Bir sistemde yapılan işlemleri gösteren kayıtlar, geçmiş bilgileri, erişim listeleri
- Yedekleme üniteleri
- Yazılımlar
- E-postalar
- Çerezler gibi internet ile ilgili dosyalar, olarak belirtilebilir [15,16].

Bilgisayar ağları ile ilgili dijital delil kaynakları beş bölümde ele alınabilir:

1. İstemci Bilgisayar Sistemleri:

- İşletim sistemi kayıtları (Windows işletim sistemindeki olay görüntüleyicisi veya Unix işletim sistemlerindeki syslog mesajları gibi.)
- Bellek bilgileri (Özellikle olay anında alınacak bellek içeriğinden, çok değerli bilgiler elde edilebilir.)
- Çalışan aktif süreçlerdeki yazılımların kayıtları
- Ağ bağlantılarının durumu (dosya, klasör ya da aygıt paylaşımı gibi)
- Çalışan uygulamaların kayıtları (internet geçmişi, kayıtlı hesaplar, kişisel bilgiler)
- Kimlik kayıt bilgileri (kullanıcı, kütük bilgileri)

2. Sunucu Bilgisayar Sistemleri:

İstemci için belirtilen delil kaynakları, sunucu bilgisayar sistemleri için de geçerlidir. Ayrıca, ilaveten ek delil kaynakları da barındırmaktadır.

- Çalışan sunucu programının kayıt dosyaları (web sayfasına erişim kayıtları, e-posta sunucu kayıtları, gateway, NAT kayıtları vb.): Bu gibi sistemlerde özellikle hangi IP'nin hangi tarihte ne gibi bir işlem yaptığı bilgisi tutulur ve bu bilgiler çok önemlidir.
- Sistem kayıtları (login başarısızlığı ve syslog mesajları vb.): Birçok işletim sistemi başarısız login girişimlerini kayıt etmektedir.
- Durum tabloları (Geçit olarak kullanılan sunucu bilgileri gibi).

3. Güvenlik Sistemleri:

- Güvenlik sistemleri
- Doğrulama sistemleri (RADIUS, TACACS, VPN)
- Güvenlik duvarı sistemleri(Firewall, Proxy vb.)
- Saldırı tespit sistemleri
- Kayıt sistemleri (Audit systems, Ör: Proxy)
- Dinleme sistemleri (Sniffer)

4. Gömülü Sistemler:

Gömülü sistemler üzerinden elde edilebilecek deliller de çok önemlidir. Örneğin, GPRS, GPS gibi sistemler, araçların nerede olduğunun tespiti için kullanıldığı gibi, araçların üzerine yüklenecek gömülü bilgisayar sistemine sahip modüller sayesinde aracın hızı, frenlerin durumu, etkiden önceki 5 saniye içerisindeki işlevler gibi bir kaza esnasında oldukça yararlı ve kazayı aydınlatıcı bilgilere ulaşılabilmektedir.

5. Ağ Aktif Cihazları:

- Yönlendirici (kütük kayıtları, routing tabloları)
- Anahtar(IP-MAC bilgilendirme tabloları, kütük kayıtları)
- Ağ donanım elemanları (kütük kayıtları)

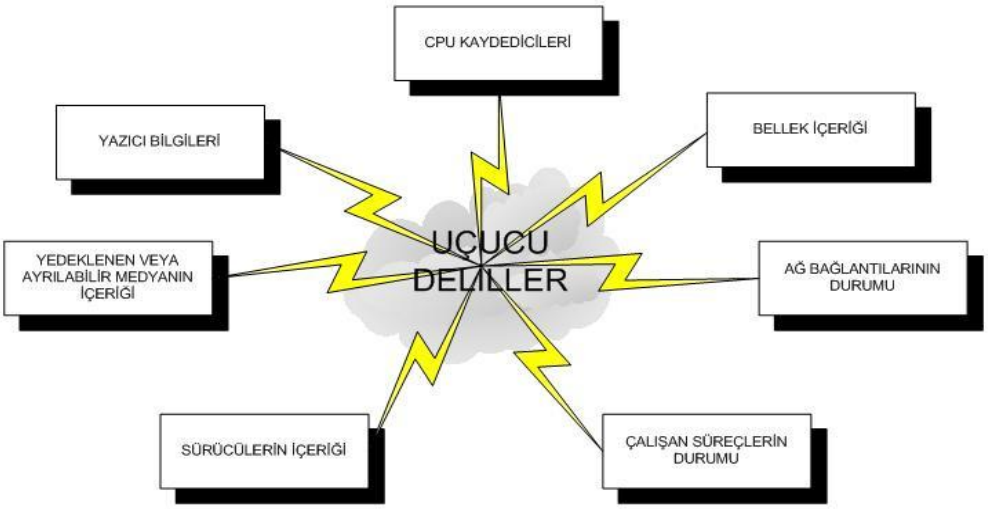
2.3.3. Dijital Delillerin Toplanması

Sanal bir suçun varlığından şüpheleniliyor ise söz konusu suç veya olay ile ilgili potansiyel delillerin toplanması gerekmektedir. Sürecin doğru bir şekilde işlemesi için öncelikle uygun prosedürleri ve gerekli hukuki şartları anlamak ve sağlamak büyük önem arz etmektedir. Deneyimli ve tecrübeli araştırmacılar için bu safhadaki amaç sanal veya fiziksel bütün delilleri toplamak değil, nelerin toplanıp nelerin toplanmayacağı konusunda mantıklı kararlar vermek, doküman oluşturmak ve ondan sonra eylemi gerçekleştirmektir. Dokümantasyon bütün basamaklarda yapılması gereken bir iştir ancak delillerin toplanması esnasında ayrı bir öneme sahiptir. Toplanan her bir delille ilgili ayrıntılı rapor tutmak, bunların doğrulanabilirliğini kolaylaştırıp, koruma zincirini başlatacaktır.

Geleneksel delil toplama, delillerin daha sonradan incelenmek üzere sahiplenilmesi anlamına gelmektedir. Fakat dijital delillerde durum biraz farklıdır. Delillerin doğrudan toplanması esnasında bazılarının kaybedilmesi, bozulması ile karşılaşılabilir. Özellikle

uçucu veriler (Ör: bellek, cpu kaydedicileri, çalışan süreçlerin durumu) dediğimiz elektrik kesildiğinde içeriği sıfırlanan ve tekrar kurtarılması mümkün olmayan delilleri barındıran bilgisayarlarda bazı ek işlemlerin gerçekleştirilmesi gerekmektedir [15,16].

Dijital delillerin uçucu diye tanımlanan elektrik kesildiğinde kaybolabilecek özellikte olanlarının, toplama aşamasında çok daha dikkatli toplanmasına önem gösterilmelidir. Şekil 4'de uçucu deliller gösterilmiştir.



Şekil 4. Uçucu deliller [16].

2.4. Dijital Saldırılar ve Dijital Saldırganlar

Günlük hayatta meydana gelen ve suç teşkil eden saldırganlık olayları, gerçek hayatın bir yansıması olan sanal ortamda da gerçekleşmektedir. Sanal ortamdaki bu fiiller ve bu fiilleri gerçekleştirenler de sanal dünyada kendilerine has bazı tanımlamalar ve özellikler bulmuşlardır.

Saldırı ifadesi en bilindik anlamda bir kimseye karşı yıpratmak amacıyla doğrudan doğruya silahlı veya silahsız bir eylemde bulunmadır. *Dijital saldırı* bir sistemin kullanılamaz hale getirilmesi için yapılan her türlü meşru veya gayri meşru hareketler olarak tanımlanabilir. Dijital saldırılardaki amaç, bilgiyi çalmak, bozmak, sızdırmak veya bilişim sistemindeki yazılım ve donanımlara zarar vermek olarak belirtilebilir. Dijital saldırıları aktif ve pasif saldırı olarak ikiye ayırmak mümkündür.

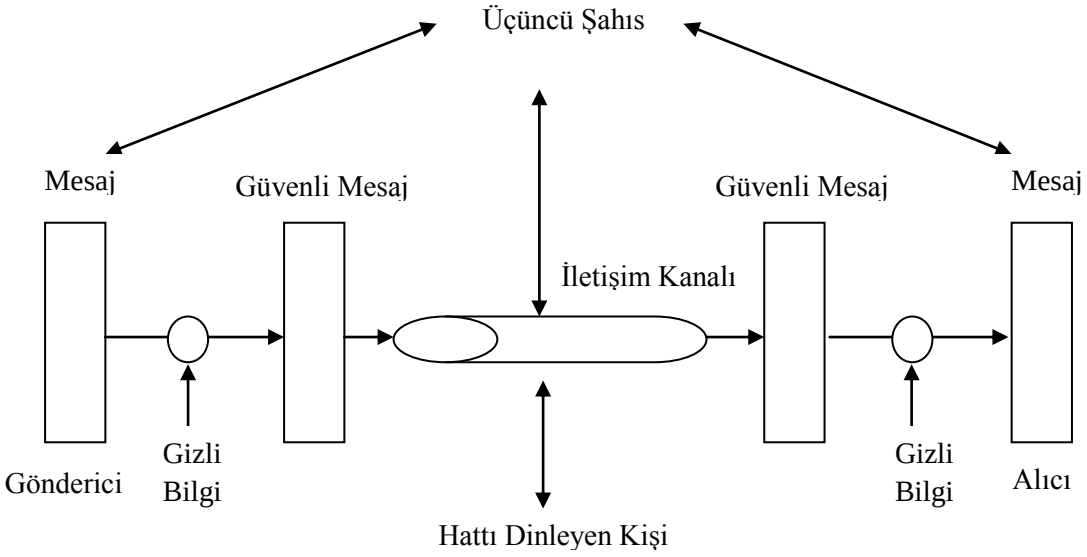
Pasif saldırıda, saldırgan taraf pasif davranmakta ve çoğu zaman sadece sistemi gözetlemekle yetinmektedir. Bu saldırı şeklindeki saldırganın yakalanması çoğu zaman

daha güç olmaktadır. Pasif saldırı yöntemlerine örnek olarak; mesajın içeriğini edinme, trafiğin akışını takip etme gibi yöntemler verilebilir.

Aktif saldırı yönteminde ise saldırgan aktif olarak rol oynar ve sistemin içerisine dahil olur. Sistemi savunan tarafın, saldırganı yakalama veya tespit etme ihtimali yüksektir. Aktif saldırı yöntemlerine örnek olarak olarak;

- Rol yapmak (Sniffer olayı, IP aldatmacası vb.)
- Eski mesajın tekrarlanması
- Aktarılan mesajı değiştirme
- Hizmet dışı bırakma/engelleme,

gibi yöntemler sayılabilir. Şekil 5'de görüldüğü gibi aktif veya pasif saldırı mesajın çıkış noktasından başlayarak varış noktasına kadar üçüncü şahıs olarak adlandırılan saldırgan tarafından herhangi bir bölgede gerçekleştirilebilir.



Şekil 5. Ağ güvenliği modeli

Hacker kavramı genel bir kavram olmasına rağmen genelde iyi niyetli hackerları ifade etmek için kullanılmaktadır. Bazı kaynaklarda hacker iyi niyetli profesyonelleri temsil ederken hackerların tam aksi uygulamaları yapanlar olarak ifade edilen *cracker* tanımlaması ise kötü niyetli profesyonelleri temsil etmektedir. Crackerlar özellikle şifre veya lisans numarası gerektiren program veya sistemlerin aşılmasında oldukça söz sahibidirler. Ayrıca crackerlar menfaat ve geliri için çalışan; sistemlere girme, veri çalma, zarar verme, işleyişi aksatma gibi olumsuzluklara da sebep olan kişilerdir.

Hackerlar, kültür ve bilgi düzeyi oldukça yüksek olan, en az bir işletim sisteminin yapısını tam olarak bilen, programcılık deneyimleri yüksek ve konusunda ileri eğitimler alarak uzun yıllarını bu işlere adamış kişilerdir [9]. Diğer bir tanımda ise işletim sistemlerini tam manası ile bilen, derinliklerine inen, bilgisayarla derinlemesine ilgilenen, programlamayı profesyonel düzeyde bilen bilgisayar uzmanlarıdırlar [8].

Hackerlar, bir yapı üzerindeki sistem hatası veya sistem açıklarını bulabilir, bu açıkların sebeplerini bilir, hiçbir zaman öğrendikleri ile yetinmez, daima daha fazlasını öğrenme çabası içerisinde olurlar.

Hackerların temel özellikleri şu şekilde tanımlanmaktadır: Temel olarak programlama mantığını ve en az bir programlama dilini iyi derecede bilirler, ingilizce bilgileri iyi düzeydedir, interneti kullanmayı ve HTML'yi iyi derecede bilirler, açık kaynak kodlu UNIX'lerden herhangi birini (Linux, Ubuntu, Redhat, vb.) iyi derecede bilirler [9].

Hacking olarak ifade edilen ve bir sisteme sızma ya da zarar verme anlamında yapılan saldırıların bir derlemesi Tablo 1'de sanal saldırganlar başlığı ile gösterilmektedir. Yapılan hacker tanımlamalarına bakılarak farklı niyette çalışan hackerler olduğu görülmektedir. Hackerlar; beyaz şapkalı hacker, siyah şapkalı hacker ve gri şapkalı hacker olarak sınıflandırılmaktadırlar.

Beyaz şapkalı hackerlar bilgi bakımından siyah şapkalılardan aşağı kalmamakla beraber; iyi niyetli, zarar vermeyen, amaçları bilgisayar güvenliğini sağlamak olan kişilerdir [8]. Siyah şapkalıların iyi niyetli olanlarıdırlar. Bazı kaynaklarda antihacker olarak da adlandırılmaktadır [17].

Tablo 1. Sanal saldırganlar

Saldırganlar	**Araçlar**	**Erişim**	**Sonuç**	**Amaç**
Bilgisayar Korsanları	Kullanıcı Komutları	Gerçekleme Zayıflıkları	Bilgi Bozma	Finansal Kazanç
Casuslar	Komut Dosyası veya Program	Tasarım Zayıflıkları	Bilgi Çalma yada Açığa Bilgi Çıkartma	Politik Kazanç
Teröristler	Araç Takımı	Yapılandırma Zayıflıkları	Hizmet Çalma	Sosyal Statüye Meydan Okuma
Meraklılar	Dağıtık Araçlar	İzinsiz Erişim	Hizmet Önleme	Zevk İçin
Profesyonel Suçlular	Veri Dinleyici Sistemler	-	-	-

Siyah şapkalı hacker kavramı ise tamamen kötü niyetli, sırf kazanç elde etmek ve karşıya zarar verme amacıyla sistemlere sızan, bilgi çalan, korsanlar için kullanılır. Bu grup hackerların amacı bilgi çalmak veya sisteme zarar vermektir [8]. Siyah şapkalı hackerlar bazı çalışmalarda korsan, saldırgan veya 3. şahıs olarak da adlandırılmaktadırlar.

Beyaz şapkalı ve siyah şapkalı grubun arasında kalan *gri şapkalı hacker* olarak adlandırılan bir grup vardır ki bunlar, yerine göre siyah, yerine göre de beyaz şapkalı hacker gibi hareket ederler.

Bilişim sistemlerine zarar vermek amaçlı çalışan kişiler genelde *cracker* tanımlamasına dahildirler. Örneğin; *phreaker* olarak adlandırılan ve telefon sistemlerindeki açıklardan yaralanmaya çalışan teknik anlamda donanımlı kişiler de aslında birer telefon crackerlarıdır.

Siyah şapkalı hackerlara nazaran daha zararsız olarak tanımlayabileceğimiz *Lamer* ifadesi genelde küçük yaşta ve hacker özentisi olan, birkaç hacker işlemini bilen ancak programlama bilgisi olmayan, herkesin yapabileceği işleri yaparak ün kazanmak isteyen kullanıcılardır. *Script Kiddie* ise genelde lise çağında olan, programlama bilgisi olmayan genellikle e-postalara saldırma işlemlerini öğrenen kişilerdir. Lamerlara göre fazla hacking bilgileri vardır [8]. *Newbie ise* Script Kiddie den bir adım daha yukarıda olan kişiler için çıkarılmış bir kelimedir. Bu kişiler sanal ortamda egolarını belli ölçüde tatmin etmiş ve öğrenmeyi hedeflemiş zararsız kesimdir [9].

2.4.1. Ünlü Dijital Saldırganlar ve Vukuatları

Dünyada yaptıkları ile ses getirmiş bazı ünlü hackerlar ve vukuatları şunlardır [8, 9, 18].

Jonathan James: Hacker suçlaması ile tutuklanan, yargılanan ve hüküm giyen ilk 18 yaş altı bilgisayar kullanıcısı olan James 16 yaşında tutuklanmıştır. ABD savunma bakanlığındaki bilgisayarlardan birine bir arka kapı (backdoor) programı yerleştirmiş, NASA bilgisayarlarından 1.7 milyon dolarlık yazılım çalmıştır.

*Adrian Lamo :"*Evsiz hacker" olarak adını duyuran Lamo'nun en çok ses getiren operasyonu New York Times ve Microsoft'un sistemlerine girmiş olmasıdır. Aynı zamanda Yahoo!, Bank of America, Citigroup ve Cingular sistemlerine de girmiş olabileceği tahmin edilmektedir.

Kevin Mitnick: Kendi deyimi ile "abartılmış olan ününün kurbanı" olan Mitnick adalet bakanlığı tarafından ABD tarihinde en çok aranan bilgisayar suçlusu olarak tanınmaktadır. Hakkında Freedom Downtime ve Takedown adlı iki film yapılmıştır. En ünlü aktivitesi telefon sistemlerini hacklemek ve Digital Equipment Corporation'ın bilgisayar ağına girip yazılım çalmaktır.

Kevin Poulsen: Kod adı Dark Dante olan Poulsen'in en ünlü aktivitesi LA radio radyo evinin KIIS-FM telefon hatlarına girerek kendisine çekilişle bir Porsche ve başka bir dizi ödül kazandırması olmuştur. Federal veritabanına girmek isterken yakalanmıştır**.**

Robert Tappan Morris: Dünyanın ilk solucan yazılımı olan Morris solucanının yaratıcısı olan Robert Tappan Morris bu programı aslında "internetin ne kadar büyük olduğunu test etmek için" yazdığını iddia etmekte olsa da programın çok büyük sayıda bilgisayara yayılıp ağları çalışmaz hale getirmesi sonucu yakalanmıştır.

Stephen Wozniak: Apple'ın "Woz" lakaplı yöneticisi bir beyaz hackerdır. Gençlik yıllarında telefon sistemlerini hackleyen ve bedava uzun mesafe telefon görüşmeleri yapan Wozniak, Steve Jobs ile beraber Apple'ı kurmuş ve bilgisayar dünyasında büyük bir devrim başlatmıştır.

Tim Berners-Lee: World Wide Web yani www konsepti Berners-Lee'nin icadıdır. Yine bir beyaz hacker olarak nitelendirilen Tim, üniversite yıllarında hacker suçlaması ile ceza almış ve bilgisayarları kullanması 3 yıl boyunca yasaklanmıştı. Üniversite yıllarında kendi bilgisayarını kendisi yapmış olan Lee, hypertext (http) sisteminin ilk geliştiren kişidir.

Richard Stallman: GNU projesinin babası olan Stallman okul yıllarında MIT'te kadrolu beyaz hacker olarak Emacs projesinde çalışıyorken her kurulan şifreli koruma sistemini kırıp öğrencilere açık hale getirmesi ile ünlenmiştir.

2.5. Siber Alan ve Siber Güvenlik

Siber kelimesi İngilizce "cyber" kelimesinden uyarlanıp kullanılmaya başlanan bir kelime olup bilgisayar ağlarına ait olan, internete ait olan, sanal gerçeklik manalarına gelmektedir. Soyut olarak iletişim kurulan sistemler *siber alan* olarak tanımlanmaktadır. Dünya üzerindeki en büyük iletişim sistemi olan interneti anlatan sanal alem ve siber alem

kavramlarının ikisi de doğru birer önermedir. Siber alanın yaygınlaşması bazı kavramlarında beraberinde ortaya çıkmasına sebep olmuştur.

2.5.1. Siber Zorbalık

Zorbalık denince sözlü veya fiziksel şiddet anlamları akla gelir. Teknolojinin kullanımının yaygınlaşması ile bu zorbalık sanal bir kılıfa da bürünmüştür. Siber zorbalık adını alan internet ortamındaki saldırı ve tehditler, kullanıcıları paranoyak olmaya hatta intihara bile sürükleyebilmektedir.

Bilgi ve iletişim teknolojilerinin en büyük ağı olan internet, artık insanların her geçen gün artan bilgiye; ulaşma, saklama ve paylaşma isteğini karşılayan bir mecradır. Bu durum bazen, imkanların sınırsız ve denetimsiz olması, avantajını dezavantaja dönüştürecek kapılar aralamaktadır. Her ne kadar bu imkânların olumsuz yanlarının başında internet bağımlılığı gelse de son beş yılda bilişim ve psikoloji literatürüne *Siber zorbalık* olarak adlandırılan yeni bir terim daha girmiş bulunmaktadır. Sanal ya da elektronik zorbalık olarak da bilinen bu tehdit türü, birey üzerindeki etkileri sebebiyle bağımlılıktan çok daha zararlı sorunlara yol açmaktadır.

Siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür. Elektronik zorbalık ve elektronik iletişim zorbalığı olmak üzere iki çeşit siber zorbalık mevcuttur.

Elektronik zorbalık, kişilerin şifrelerini ele geçirme, web sitelerini hackleme (bir sisteme izinsiz girmek), spam (zararlı virüs) içeren e-postalar gönderme gibi teknik olayları içermektedir. Bu tip saldırılar, bireylerin web siteleriyle sınırlı kalmayıp, kurumların ve devletlerin siteleri, yazılım ya da donanımlarını da olumsuz etkilemektedir.

Elektronik iletişim zorbalığı ise bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme (cyber-stalking), alay etme, isim takma, dedikodu yayma, hakaret ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içermektedir. Bu da direkt olarak insanın duygu ve psikolojisini etkilemektedir [19].

Siber zorbalık veya tehdidin en çok sosyal medya sitelerinde meydana geldiği görülmektedir. Genellikle fotoğraf ve video yayınlama tarzında gerçekleşen bu eylemler bazen sözlü alay ifadeleri ile mahremiyetlere zarar vermektedir.

2.5.2. Siber Saldırı

Bilgi sistemleri doğrultusunda elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinlikler *siber saldırı* olarak isimlendirilmektedir. Siber saldırılar genellikle internet üzerinden yapılan tecrübeli hackerların yapabildiği saldırı biçimidir.

2.5.3. Siber Savaş

21. yüzyılın en önemli güç kaynağı hiç şüphesiz bilgidir. Bilgiyi elinde tutan gücü de elinde tutmuş olmaktadır. Bilginin gücüyle teknolojik alandaki gelişmeler tüm yaşamımızı olumlu yönde etkilemektedir. İnternet, bilgisayar, uydular, cep telefonları sadece günlük yaşamımıza giren teknolojinin ürünlerinden bazılarıdır. Yine bilginin gücünü kullanarak aynı araçlar birer silaha dönüşebilmekte ve karşımıza siber savaş ve siber terör kavramları çıkmaktadır [1].

Terörizm; belirli bir siyasal hedefe ulaşmak veya siyasal bir davayı yüceltmek amacıyla ve genelde kurulu düzeni değiştirmeye veya söz konusu siyasal davaya boyun eğmeye mecbur etmek için başvurulan zorlayıcı ve şiddet içeren davranışlardır [20]. Bu tanıma paralel olarak *siber terörizm* ise belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır [21].

Siber terörizmi klasik anlamda terör eylemlerinin bilgisayar ve bilgisayar sistemleri kullanılarak icra edilmesi olarak tanımlamak da mümkündür. En genel anlamda siber terörizm "hükümeti etkilemek ya da toplumu korkutmak amacıyla elektronik sistemlerin içine izinsiz girmek veya bu sistemleri bozmak" olarak tanımlanmaktadır.

Siber terörde, saldırganların elektronik bir saldırı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir.

2.5.4. Siber Ordu

Ulusal bazda siber saldırılara karşı koymak için artık sadece eli silahlı kolluk kuvvetleri yeterli değildir. Hatta, artık eli silahlı kolluk kuvvetleri ikinci planda kalmaktadır. Çağımızın bilgi çağı olması sebebiyle devletlerde, ulusal dengeyi sanal alem üzerinden sarsmaya çalışan saldırganlara ve terörizm eylemlerine karşı sanal ordular kurarak savunma gerçekleştirmektedir.

Siber ordular ulusal güvenliği sanal ortamda sağlayan ordulardır. Siber orduların öneminin farkında olan Amerika Birleşik Devletleri gibi gelişmiş ülkeler sanal ortamda saldırı tespit yöntemleri oluşturmaya yönelik yarışmalar düzenleyerek konu hakkında yetenekli kişileri bu ordularına dahil etmektedirler. Pentagonun düzenlediği güvenlikle ilgili bir yarışmada birinci olan bir Türk öğrencinin Pentagon'dan davet mektubu alması buna bir örnektir [22].

2.5.5. Siber Etik

Bilişim dünyasında yeni bir kavram olarak yer bulmaya başlayan siber ahlak olarak da tanımlayabileceğimiz siber etik en genel anlamı ile gerçek hayatta iyi bir birey olmak için yapılan fiillerin sanal ortamda da yapılması olarak tanımlanmaktadır. Sanal alemde davranış kuralları konusunda özellikle genç kuşağın eğitilmesi gerekmektedir. Günlük yaşamında hırsızlık yapmayı ahlaki değerleriyle veya toplumsal statüsü ile bağdaştıramayan bir genç, web ortamında rahatlıkla hırsızlık yapabilmekte veya başkalarına zarar verebilmektedir. İnternet çağının gençlerinin, içine düştüğü sanal alem-gerçek alem çatışmasını eğitimle ortadan kaldırmak gereklidir. Gençler ilköğretimden başlayarak, bilişim dersleri veya medya okuryazarlığı derslerinde siber etik konusunda eğitilmelidir.

2.6. Adli Bilişim

Adli kelimesi TDK'nin sözlüklerinde adliye teşkilâtı ve hizmeti ile ilgili, adaletle ilgili olarak tanımlanmaktadır. Bu bağlamda adalete intikal etmesi gereken hadiselerin tamamına ise *adli vaka* veya *adli olay* denmektedir.

Sanal ortam kullanıcılarının artması ile bu ortamlarda da artık bazı adli olaylar gerçekleşmektedir. Bu olaylar yeni olmakla beraber hukuki anlamda da hızla gelişmekte olan adli bilişim kavramını ortaya çıkarmıştır.

Adli bilişim teriminin kökeni, ingilizce orijinal ismi ile *"Computer Forensics"* dir. Bu kavram, bilgisayar anlamındaki computer ile mahkemeye ait olan, adli anlamlarına gelen forensic kelimelerinden oluşmaktadır. Dilimize tam çevrildiğinde "adli bilgisayar" gibi bir anlam ortaya çıkmakla birlikte, ağırlıklı olarak adli bilişim terimi tercih edilmektedir. Adli bilişim yerine *bilgisayar kriminalistiği* de kullanılabilmektedir. Türkçedeki yaygın kullanım olan *adli bilişim* terimi ifadesi bu çalışmada tercih edilmiştir.

2.6.1. Adli Bilişim Çeşitleri

En sık telaffuz edilen adli bilişim alt başlıkları beş şekilde sıralanabilir:

1.Bilgisayar Adli Bilişimi (Computer Forensics) : Daha çok bir bilgisayar üzerinde yapılacak araştırmalarla ilgilenir.

2.Bilgisayar Ağlarına Yönelik Adli Bilişim (Network Forensics) : Ağ sistemleri ve iletişimine yönelik incelemeyi kapsar.

3.Bilgisayar Ağ Cihazlarına Yönelik Adli Bilişim (Network Device Forensics): Yönlendirici, switch gibi cihazlar üzerinde yapılacak incelemeyi kapsar.

4.İnternet Adli Bilişimi (Internet Forensics): Genel olarak internet kaynakları ve internet sistemleri üzerinde yapılan araştırmayı kapsar.

5.Bilgi Adli Bilişimi (Information Forensics): Bilgiyi içeren her türlü materyali barındıran sistemler üzerinde yapılan incelemeyi kapsar [23].

Aslında kavram karmaşasındaki en büyük nedenlerden birisi, sayılan bu alt başlıkların birbirinden kesin çizgilerle ayırt edilememesidir. Örneğin; bilgisayar ağlarına yönelik adli bilişim araştırması yaparken mecburen bilgisayar üzerinde, ağ aktif cihazları üzerinde ve internet üzerinde de araştırma yapılması gerekecektir [23].

2.6.2. Adli Bilişim Çalışma Alanları

Günümüzde bilişim sistemlerinin öneminin gittikçe artması ile adli bilişim de buna paralel olarak hızla gelişmekte, etki alanlarını genişletmektedir. Ülkemiz için henüz yeni sayılabilecek olan adli bilişim, bilgisayar endüstrisinin çok daha ileri olduğu ABD gibi ülkelerde çok çeşitli alanlarda kullanılmaktadır.

Adli bilişimin çalışma alanlarının genişlemesiyle adli bilişim analiz yöntemlerinin amacı yalnızca ceza davalarına delil sağlamak olmaktan çıkmış, hukuk uyuşmazlıklarında hatta şirketlerde de kullanılır olmuştur. Özellikle büyük şirketler, bugün veri kurtarma ya

da veri imha etme gibi esasen adli bilişimi yakından ilgilendiren konularda bu bilim dalına başvurmakta; adli bilişim uzmanlarını bünyelerinde çalıştırmaktadırlar.

Adli bilişimin çalışma alanlarından bazıları ana başlıklar halinde şöyle sıralanabilir:

- Veri kurtarma
- Veri imha etme
- Veri saklama
- Veri dönüştürme
- Şifreleme
- Şifre çözme
- Gizlenmiş dosya bulma
- IP numaralarından yararlanılarak suçluların tespit edilmesi.

2.6.3. Adli Bilişimin Faydaları

Adli bilişim, adli bilimler içerisinde yer almakta ve adaletin gerçekleşmesi amacına hizmet etmektedir. Bu hizmet, yargılamaya delil katkısı yaparak gerçekleşir. Ancak, bugün teknik gelişmelere bağlı olarak hızla gelişimini sürdüren adli bilişim, yalnızca yargı organlarına yardımcı olmanın daha ötesine geçmiştir. Bugün bazı şirketler ve kişiler de veri kurtarma, imha etme ya da diğer başka amaçlarla adli bilişime ihtiyaç duymaya başlamışlardır. Hatta büyük şirketler, bünyelerinde bir adli bilişim uzmanı görevlendirme ya da bu konuda hizmet veren firmalarla sürekli çalışma yolunu seçmektedirler.

Teknoloji, sanayi devriminden bu yana dünyayı şekillendiren, değiştiren bir olgu olarak mevcuttur. Ancak, son yıllarda bilgisayar sistemlerine bağlı olarak teknolojik gelişim süreci hız kazanmıştır. Hemen her gün insanlığın hizmetine yeni bir ürün sunulmakta, insanlar gitgide daha fazla teknolojik/sayısal aygıtla iç içe yaşar hale gelmektedir. Teknolojinin kullanımı, getirdiği sayısız kolaylıklar yanında birtakım olumsuz durumlar da yaratmaktadır. Hayatın her alanında var olan suç olgusu, teknolojiyi de araç olarak kullanmaktadır. Bu gelişmelere bağlı olarak geleneksel ve klasik suçların yapısı da değişmekte, bilişim ortamlarında giderek daha fazla suç işlenmektedir. Suçun bulunduğu her yerde cezalandırma, bunun için yargılama ve yargılama için de deliller vardır. İşte bu sebepten dolayı bilişim suçlarında delillerin toplanması konusu, adli bilişimi ilgilendirmektedir.

Adli bilişim, yalnızca bilişim suçlarına has bir delil toplama metodu değildir. Bilişim suçlarından başka, klasik suçlara ilişkin olarak da ihtiyaç duyulan deliller, yine elektronik aygıtlar içerisinde de yer alabilir. Örneğin, bir bilişim suçu olmayan bir hırsızlık olayında, soygun planı ve buna ilişkin haritalar bilgisayar ile hazırlanmış ve halen bilgisayarda mevcut olabilir. Bu bilgilere ulaşmada da yine adli bilişim devreye girecektir. Bu duruma en bariz örnek olarak; hala devam etmekte olan *Ergenekon* soruşturması ile alakalı bazı verilere, bilgisayar kayıtlarından ulaşılması gösterilebilir.

2.6.4. Adli Bilişim Uzmanlığı

Adli bilişim uzmanı, bilişim sistemleri ve güvenliği konusunda ileri derecede bilgi sahibi olan kimsedir. Bu bilgi, sürekli değişen teknolojiye bağlı olarak hep güncel kalmak durumundadır. Adli bilişim uzmanı, kendisini sürekli yenilemeye devam etmelidir. Adli bilişim uzmanları ile ilgili olarak CMK'nın bilirkişiliğe ilişkin hükümlerinin uygulanacağı, kanun tasarısında düzenlenmektedir. Ancak adli bilişim metotlarına hukuk yargılamalarında da başvurulabileceğinden; hukuk yargılamalarında da HUMK'nin bilirkişiliğe ilişkin hükümlerinin uygulanacağı haklı olarak belirtilmektedir.

Adli bilişim uzmanı kabul edilmek için birtakım sertifika programları mevcuttur. Bu programlardan birine devam ederek sertifika almak ve adli bilişim uzmanı sıfatına sahip olmak mümkündür. Bu sertifika programlarından en çok kabul edilenleri şunlardır: EnCase Certified Examiner (ENCE), Certified Computer Examiner (CCE), Certified Computer Crime Investigator (CCCI), Computer Forensic Computer Examiner (CFCE), Certified Information Forensics Investigator (CIFI), Professional Certified Investigator (PCI) [24]. Bireysel olarak adli bilişim uzmanlığı sertifikasına sahip olup çalışmalar yürüten ve mahkemelerde bilirkişilik yapan az sayıda uzman, özveriyle bu konularda çaba sarf etmektedir. Adli bilişim alanının, çalışmak üzere uzmanlarını beklediğini söylemek, haksız bir tespit olmayacaktır.

2.6.5. Adli Bilişimde Dijital Delillerin Kanıt Olarak Kullanılabilmesi

Elektronik/Sayısal delillerin klasik delillerden farklı özellikler taşıması, delillere ulaşma konusunda da bazı farklılıklar ortaya çıkarmaktadır. Örneğin, bir cinayet vakasında, olay mahallinde bulunan tabanca, kuvvetle muhtemeldir ki suça ilişkin bir delildir. Bu tabanca muhafaza altına alınarak, gerekli incelemelerin yapılması için

götürülür. Oysa ki dijital delillerde durum bundan çok farklıdır. Öncelikle, muhafaza altına alınan bir elektronik aygıt içerisinde suça ilişkin delil bulunup bulunmadığı belli değildir. Örneğin, suç mahallinde bulunan bir bilgisayarın suçta kullanılıp kullanılmadığı veyahut suça ilişkin bir delil ihtiva edip etmediği belli değildir. Şüphesiz ki, tabanca örneğinde de suça ilişkin kesin bir belirginlik yoktur. Ancak ortamda bulunan bilgisayar (yahut bir başka elektronik aygıt) konusunda bu belirsizlik çok daha fazladır.

Muhafaza altına alınarak incelenmeye başlanmış bir klasik delil, çeşitli analizlerden sonra çözülür ve nitelendirilir. Ancak elektronik delillerde bu işlem o kadar basit ve kolay olmamaktadır. Adli bilişimde delilin incelenmesi, nitelendirilmesi ve analizi klasik delillere kıyasla daha karmaşık, çok daha teknik ve oldukça pahalı bir işlemdir.

Adli bilişimde elektronik bulgunun, bir hukuki delile dönüştürülme süreci belli prosedürleri takip eder. Uygulanan bu prosedürlerden sonra dijital delil, kendisini bir hukuki delil olarak ortaya koyar. İşte bu prosedüre, *adli bilişim safhaları* denilmektedir. Adli bilişim safhaları, bazı yazarlarca dört tane olarak sayılırken; bazı yazarlar ise, bu aşamaları beşe ayırarak incelemektedir. Adli bilişimde dijital delillerin kanıt olarak kullanılabilmesi için incelenmesi gereken dört safha şu şekildedir [24]:

- Toplama (Collection)
- İnceleme (Examination)
- Çözümleme (Analysis)
- Raporlama (Reporting)

2.6.6. Ülkemizde Adli Bilişim

Adli bilişimin çalışma alanı, bilişim suçları üzerinden çalışmayı gerektirmektedir. Bilişim suçları kavramı, son yıllarda ülkemizde de gündemdeki yerini almıştır. Bu konuda yasal mevzuatın güncellenmesine rağmen, hukuki süreci destekleyecek teknik altyapı konusunda yeterli çalışma eş zamanlı olarak yapılamamıştır.

Bilişim suçları ile mücadele, sadece kolluk kuvvetiyle değil; kamu kurumları ile özel kurumlar ve üniversitelerle işbirliği içerisinde yapılması gereken kapsamlı bir çalışmadır. Bu noktada, siber çağın yöntemleriyle gerçekleştirilen suçların tespiti ve kanıtlanması sürecinde; yasal düzenlemeler ile uyumlu, standartları belirlenmiş, akredite uzman personeli olan, uluslararası sertifikalara sahip ve üniversitelerle işbirliği içerisindeki adli bilişim laboratuarlarının kurulması önem arz etmektedir [3]. Ülkemizde kolluk

kuvvetlerinden jandarmaya ait olan adli bilişim laboratuarları Ankara olmak üzere bazı merkezi illerde bulunurken, polis teşkilatına ait bazı adli bilişim laboratuarları da mevcut olup, bunlardan bir kısmı mobil adli bilişim laboratuarı olarak hizmet vermektedir. Konuyla alakalı özel adli bilişim laboratuarları da kurulmaktadır.

Ülkemizde adli bilişim uzmanlığı alanında büyük eksiklik bulunduğu bilinmektedir. Giderek artan bilişim suçları, adli bilişim uzmanlarına duyulan ihtiyacı da artırmaktadır. Ülkemizde de bu alanda büyük bir eksiklik olduğunu tespit eden ve yeni bir iş sahası olduğunun farkına varan bilişim güvenlik şirketleri bu alanlarda uzman personel yetiştirme sertifikasyon programları düzenlemektedir. Ancak adli bilişim uzmanı elemanlarının yetiştirilmesi konusunda üniversite ve kamu kuruluşlarının da ciddi anlamda çalışmalar yapmaları gerektiği görülmektedir. Özellikle üniversitelerde *adli bilişim mühendisliği bölümünün* mühendislik fakülteleri bünyesinde açılmasının gerekliliği görülmektedir.

3. BİLGİ VE BİLGİ GÜVENLİĞİ

Bilgiye sahip olmanın büyük bir güç olduğu bu asırda, bilgiye ulaşmanın yanında bu bilgilerin güvenliğinin sağlanması da başlı başına bir çalışma alanı haline gelmiştir. Bilginin paylaşıldıkça artacağının bilinen bir gerçek olmasının yanında, sadece şahısları veya kurumları ilgilendirecek bilgilerin mahremiyetinin sağlanması ise özellikle üzerinde durulması gereken bir konudur.

Bu bölümde bilginin tanımı, özellikleri, gelişiminin yanında teknik boyutlarda bilginin güvenliğini tehdit edecek bazı olaylar incelenmiş ve bazı çözüm önerileri sunulmuştur.

3.1. Bilgi

En basit tanımlaması ile bilgi kişi ya da kurumlar için kıymet teşkil eden ve para gibi korunması gereken kıymetli bir metadır [25]. Meta ifadesi ile eşya kast edilirken bunun yerine varlık ifadesi de kullanılmaktadır. Bilginin değerinin olması, bu değeri elde etmek için emek ve zamanın harcanması ve kazanılan bilginin fark oluşturması nedeniyle bilgi, korunması gereken bir varlık olarak görülmektedir. Bu açıdan bilginin korunmasına yönelik bilgi güvenliği konusu, dünya gündeminde önemi her geçen gün artarak karşımıza çıkmaya devam edecektir [26].

3.1.1. Bilginin Değeri

Bilginin yaşadığımız çağa damgasını vuran bir varlık olduğu bir gerçektir. Bu açıdan bakıldığında, çağımızın altın değerindeki hammaddesi olan bilgiyi tanımlamak, kavramak ve bilgi ile ilgili hususları incelemek, insanlığın başlangıcından itibaren geçen süreçte ileriye yönelik gelişimimizi şekillendirmenin en önemli anahtarıdır [10]. Günümüzde bilgi ön plana çıkmış gibi gözükse de, aslında bilgi; dünün ve bugünün anahtarları iken, geleceğin şekillenmesinde de her zaman anahtar rollere sahiptir.

Bilginin doğası ile ilgili aşağıda derlenen sözler, bilginin değerini ve boyutlarını bir kez daha gözler önüne sermek açısından faydalı olabilir [27]. Bilgi;

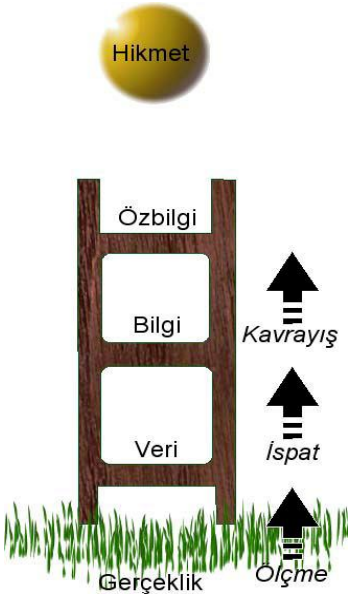
- Boşlukta ve zamanda yer kaplar.
- Gürültü çıkarmadan hareket edemez.
- Hareketi için enerji gerekir.
- Yaşam ve herhangi bir düzenli etkinlik için gereklidir.

- Hem maddesiz biçim, hem biçimsiz maddedir.
- Ağırlığa sahiptir. Bir gigabayt, bir parmak izinden daha az ağırlıktadır.
- Zaman içinde hareketli veya donmuş olabilir.
- Bir soruya tatmin edici, belki de rahatsızlık verici bir cevaptır.
- Katı hale sahiptir, donarak katılaşır (depolanma).
- Sıvı hale sahiptir, akar (iletişim).
- Bir yerlerde bilgi hareket eder.
- Maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.

3.1.2. Bilginin Gelişim Evreleri

Bilgi çağında ilerlemek, bir merdivenin basamaklarını kullanarak bir üst seviyeye çıkmaya benzetilebilir [28]. Şekil 6'da gerçeklik (reality) ile hikmet (wisdom) arasında gösterilen bu merdivenin basamakları, veri (data), bilgi (information), özbilgi (knowledge) basamaklarıdır. Çoğu durumda, her basamak, atlanmadan teker teker geçilir. Yukarıya çıktıkça elimizdeki şeyin miktarı azalırken, değeri artar. Yine yukarıya çıktıkça, bir sonraki basamağa adım atmak daha da zorlaşır veya daha çok çaba ister. Bu yüzden, merdivenin alt basamaklarında verinin ve bilginin paylaşımı daha kolay iken yahut insanlar veya çalışanlar elde ettikleri veri ve bilgileri paylaşmaya daha açık iken, daha yukarı çıkıldığında özbilginin paylaşımı için aynı şey söylenemez [29]. Genel olarak bilimin getirdiği yöntemlerden, ölçme ile eldeki gerçeklikten veriye, ispat ile veriden bilgiye ve kavrayış ile bilgiden özbilgiye ulaşılır. Özbilgiden hikmete ulaşma, sentezleme içeren bir düşünüş gerektirir. Bu düşünüş, fikirlerin öyle bir şekilde bir araya getirilmesidir ki ulaşılan bütün, parçalarının toplamından daha büyüktür. Bir başka gözlem de, merdivenin alt basamaklarında, daha algoritmik ve programlanabilir bir yaklaşıma ihtiyaç duyulurken, daha yukarı basamakların, algoritmik olmayan ve programlanamayan bir yapı arz etmesidir. Veri ve bilginin iletiminde bilişim teknolojileri kullanılabilirken, özbilgide buna ek olarak insan etkeni de işin içine girmektedir. Bir özbilginin gerçeklik haline dönüştürülmesi için yönetim biliminden yararlanılır [33].

Bilgi ve özbilgi kavramları veya basamakları, birbirine karıştırılmaması gereken kavramlardır. Bu kavramlar arasındaki farklar yukarıda anlatıldığı gibi Şekil 6'da gösterilmektedir.



Şekil 6. Bilgi basamakları [33].

Şekil 6'daki oluşumu, sırasına göre şu şekilde ifade etmek mümkündür:

İnsan bilincinden bağımsız olarak var olanlar veya hikmete ulaşmak için veri haline gelmeye hazır doğada bulunan her şey *gerçeklikdir*.

Verinin; İngilizce karşılığı olarak kullanılan "data", Latince "datum" kelimesinden (çoğul şekli "data" ve "vermeye cesaret etmek" fiilinin geçmiş zamanı, dolayısıyla "verilen şey") gelmektedir. Latince "data" (dedomena) kavramının M.Ö. 300 yıllarında Öklid'in bir çalışmasında geçtiği bildirilmektedir [34]. Dilimizde de "verilen şey" anlamında, "veri" olarak kullanılmaktadır. Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.

Bilgi; verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Bu aşamada, veri ve ilişkili olduğu konu, bilgi üretecek şekilde bir araya getirilir. Bilgi; işlenmiş veri olarak ve bir konu hakkında var olan belirsizliği azaltan bir kaynak olarak da tanımlanabilmektedir. Kısaca, veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s.) çıktısı, bilgi olarak ifade edilebilir.

Özbilgi; tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verilerin bir araya getirilip, işlenmesi bilgiyi oluştursa da özbilgi, kullanılan bilgilerin toplamından daha üstte bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç

haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir. Özbilgi, ne olduğunu (know-what), niçin olduğunu (know-why), nasıl olduğunu (know-how) ve kim olduğunu (know-who) bilmek şeklinde dört sınıftan oluşur. Ne olduğunu bilmek, gerçeklerin toplamıdır ve bilgiye en yakın olan sınıftır. Niçin olduğunu bilmek, teknolojik gelişmenin altında yatan ilke ve yasaların açıklandığı bilimsel özbilgidir. Nasıl olduğunu bilmek, bir şeyi yapabilme becerisidir. Kimin olduğunu bilmek, kimin neyi ve kimin neyi nasıl yapılacağını bildiğini bilmek olarak özetlenebilir [10].

Hikmet (wisdom), tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür. Hikmet, ayrıca, güvenilir yargıda bulunmak ve karar vermek için özbilginin nasıl kullanılacağını kavramak olarak da tanımlanmaktadır [36].

İnsanoğlu genellikle gerçeklikten özbilgiye kadar ulaşabilmektedir. Bilinmeyen gerçeklikten hikmete ulaşmak ise Yaratıcının ilmindedir. Örneğin; kültürümüzde insanların karşılaştıkları sıkıntılı durumlar karşısında kullandıkları, "Herşeyde bir hikmet vardır" veya "Hikmetinden sual olunmaz" tarzındaki ifadeler arka planda her şeyden haberdar olan birisinin varlığını göstermektedir. Asıl hikmet Yaratanın ilmi dahilinde iken insanoğlu genellikle özbilgi seviyesine ulaşabilmektedir. Bununla beraber insanoğlunda meleke haline gelen davranış, ileri görüşlülük (basiret) ve sezme yetisi (feraset) de hikmet olarak değerlendirilebilir.

3.2. Bilgi Güvenliği

Bilgi güvenliği; bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı, kişi ve kurumların sahip oldukları teknolojileri kullanırken, karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır.

Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikaları belirlenmeli ve uygulanmalıdır. Bu politikalar, faaliyetlerin sorgulanması, erişimlerin izlenmesi, değişikliklerin kayıtlarının tutulup değerlendirilmesi,

silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir. Bilgi güvenliği daha genel anlamda, güvenlik konularını detaylı olarak ele alan güvenlik mühendisliğinin bir alt alanı olarak görülmektedir.

Bilgi güvenliğinin sağlanması için kullanılabilecek birçok yöntem olmakla beraber yeni sayılabilecek biometrik alanda yapılan bilgi güvenliği çalışmaları da mevcuttur. Bu biometrik korunma yolları arasında parmak izi ile çalışan sistemler, el ve parmakların şekline göre çalışan sistemler, ses tanıma sistemleri, dijital imza, gözün retina ve iris tabakasından yararlanılarak çalışan sistemler mevcuttur. Buna örnek olarak Kuzey Carolina'daki uluslar arası havaalanında kullanılan iris ile çalışan güvenlik sistemi örnek olarak gösterilebilir [38].

3.2.1. Bilgi Güvenliği Sertifikasyonu

Bilgi güvenliği sertifikasyonu, büyüklüğü ne olursa olsun, ihtiyaç duyan tüm kurum veya kuruluşların bilgilerinin gizlilik, bütünlük ve erişebilirliklerini sağlamak amacı ile kurdukları bilgi güvenliği yönetim sistemini belgelendirmek ve bunu üçüncü taraflara kanıtlamak amacı ile aldıkları sertifikasyondur. Bağımsız belgelendirme kuruluşlarının, yaptıkları denetim sonucu düzenledikleri ve kurumdaki bilgilerin güvenliklerinin sağlanmasına yönelik sistematik bir uygulamanın olduğunun kanıtını sağlamak üzere; kurum adına düzenlenen sertifikaya veya belgeye TS ISO/IEC 27001 *Bilgi Güvenliği Yönetim Sistemi Belgesi* veya TS ISO/IEC 27001 *Bilgi Güvenliği Yönetim Sistemi Sertifikası* denir.

TS ISO/IEC 27001 belgesi için kurum ve kuruluşların öncelikle TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi standardına göre sistem kurmaları gerekmektedir. TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi standardına göre sistem kuran firmaların uluslar arası boyutta tanınan ve TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi hususunda akredite olmuş kuruluşlardan denetim yaptırması ve bu denetimlerden başarı ile geçmesi gerekmektedir.

Bilgi güvenliğine önem veren kurum veya kuruluşlar güvenlik sertifikasını belgelendirmek zorunda değildirler. Ancak, bilgi güvenliğine önem verdiğini ispatlamak için kurum ve kuruluşlar; TS ISO/IEC 27001 standardına göre TS ISO/IEC 27001 bilgi güvenliği yönetim sistemini kurmalıdırlar. Hiçbir sistemin ve uygulamanın, üçüncü taraftaki bir gözle kontrol edilmedikten ve denetlenmedikten sonra etkinliğinden

bahsedilemez. TS ISO/IEC 27001 bilgi güvenliği yönetim sistemlerini belgelendirmek isteyen kuruluşlar özellikle uluslar arası akreditasyon kuruluşlarından akredite olmuş belgelendirme kuruluşlarından TS ISO/IEC 27001 belgesini almalıdırlar. Akreditasyonsuz olarak verilen TS ISO/IEC 27001 belgesinin hiçbir geçerliliği yoktur.

TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi kurmak ve belgelendirmek bir firmaya, şirkete veya kuruluşa bilgi güvenliği kavramının temel ilkelerini sağlamaktadır. Bilgi güvenliği kavramının temel ilkeleri kısaca G-B-U kısaltması ile gösterilebilir. Bu kısaltmalar:

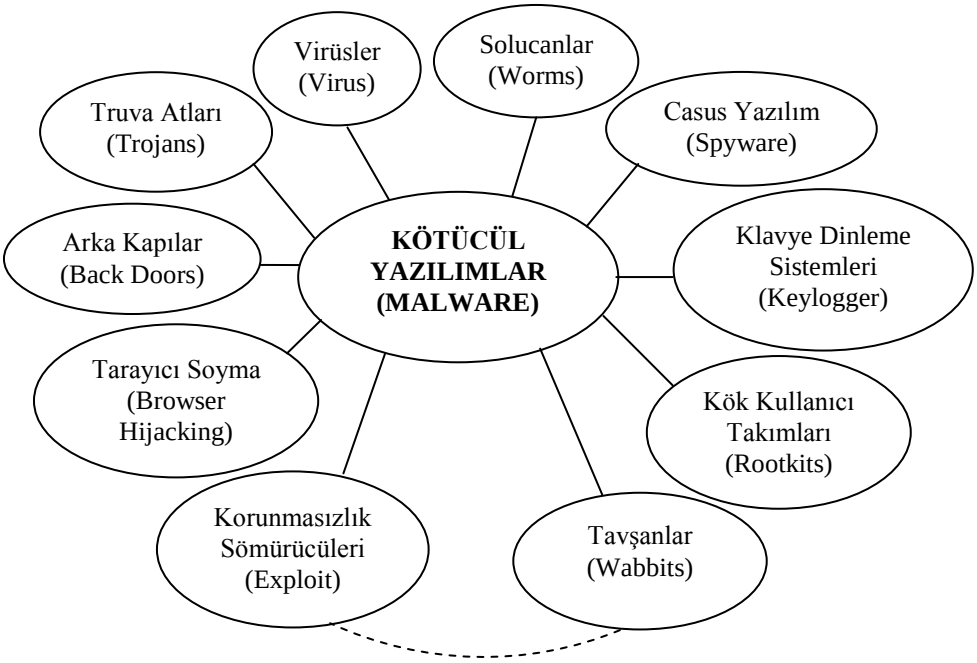
- Gizliliğin korunması (bilgiye ulaşımın, sadece yetki sahibi kişilerce olabildiğinin garanti altına alınması)
- Bütünlük (bilginin ve bilgi işleme yöntemlerinin, doğruluğunun ve eksiksizliğinin korunması)
- Ulaşılabilirlik (gereken durumlarda yetkili personelin, bilgiye ve ilgili varlıklara ulaşabilmesinin garanti edilmesi), şeklinde tanımlanır.

ISO 27000 standartları her geçen gün büyüyen ISO/IEC ISMS standartdı ailesinin bir parçasıdır. ISO 27000 standart serisi; (ISO 27001, ISO 27002, ISO 27003… vb.) bilgi teknolojisi, güvenlik teknikleri, bilgi güvenliği yönetimi sistemleri, genel bakış ve tanımlar başlıklarını kapsayan uluslararası standartları içeren bir standart ailedir [31].

3.3. Kötücül Casus Yazılımlar

Kötücül yazılım (malware, ingilizce “malicious software”in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır. Özellikle Türkçe kaynaklı literatür tarandığında 11 adet ana kötücül yazılımın varlığından bahsedilirken 38 adet yeni kötücül casus yazılımdan bahsedilmektedir [26].

Şekil 7’de şema şeklinde gösterilen virüsler (virus), solucanlar (worms), truva atları (trojan), casus yazılımlar (spyware), arka kapılar (backdoor), klavye dinleme sistemleri (keylogger), tarayıcı soyma (browser hijacking), telefon çeviriciler (dialer), kök kullanıcı takımları (rootkit), korunmasızlık sömürücüleri (exploit) ve tavşanlar (wabbit) en genel ana kötücül casus yazılımlardır. Kötücül casus yazılımlar için kullanılan başka bir ismin de scumware (kirli yazılım) olduğunu belirtmekte fayda vardır. Şekil 7’de gösterildiği gibi kötücül yazılım türleri gün geçtikçe artış göstermektedir.



Şekil 7. Kötücül yazılım ana türleri

Kötücül yazılımlardan en bilinen tür olan virüsler sanal ortamda fazlası ile bulunmaktadır. Bunlardan bir kısmı ile ilgili Tablo 2'de bazı bilgiler mevcuttur.

Tablo 2. En meşhur virüsler [30].

Virüs Adı	**Tipi**	**Karıştığı Olay Sayısı**	**Oranı (%)**
Win32/Ska	File	140	13.28
Laroux	Macro	124	11.76
Marker	Macro	122	11.57
Ethan	Macro	69	6.55
Class	Macro	59	5.60
Win32/Pretty	File	52	4.93
Win32/NewApt	File	48	4.55
Melissa	Macro	47	4.46
Tristate	Macro	44	4.17
Freelinks	Script	42	3.98
Win32/Babylonia	File	32	3.04
Cap	Macro	31	2.94
Win32/Fix	File	31	2.94
Thus	Macro	29	2.75
Win32/Explore.Zip	File	21	1.99
Win95/CIH	File	19	1.80

Literatürde bilinen yeni kötücül casus yazılımlar; reklâm yazılım(adware), parazit yazılım (parasiteware), hırsız yazılım (thiefware), püsküllü bela yazılım (pestware), tarayıcı yardımcı nesnesi (Browser Helper Object, BHO), uzaktan yönetim aracı (Remote Administration Tool (RAT)), ticari RAT (commercial RAT), bot ağı (botnet), ağ taşkını (flooder), saldırgan ActiveX (hostile ActiveX), saldırgan Java (hostile Java), saldırgan betik (hostile script), IRC ele geçirme savaşı (IRC takeover war), nuker, paketleyici (packer), ciltçi (binder), şifre yakalayıcılar/ soyguncular (password capture/ hijacker), şifre kırıcılar (password cracker), anahtar üreticiler (key generator), e-posta bombalayıcı (mail bomber), kitle postacısı (mass mailer), e-posta adres hasatçısı (E-mail harvester), web böcekleri (web bugs), aldatmaca (hoax), sazan avlama (phishing), web sahtekârlığı (web scam) ve dolandırıcılığı (fraud), telefon kırma (phreaking, phone breaking), port tarayıcılar (port scanner), sondaj aracı (probe tool), arama motoru soyguncusu (search hijacker), koklayıcı (sniffer), kandırıcı (spoofer), casus yazılım çerezleri (spyware cookie), iz sürme çerezleri (tracking cookie), turta (PIE), damlatıcı (trickler), savaş telefon çeviricileri (war dialer) ve tavşanları (wabbit) sayılmaktadır [10, 26, 36]. Bununla beraber daha birçok yeni kötücül yazılımın varlığından bahsedilmektedir.

3.3.1. Kötücül Casus Yazılımların Bulaşma Biçimleri

Casus yazılımların bir sisteme bulaşma yöntemleri veya bulaşma biçimleri için birçok farklı uygulamalar bulunmaktadır. En çok bilinen bu uygulamalar şu şekilde özetlenebilir.

- Farklı üreticilerden aldıkları parçaları bir araya getirerek bilgisayar yapan firmalar, bilgisayarlarını müşterilerine satmadan önce kurdukları yazılımlar arasında kasten veya bilmeden casus yazılım bulunabilir.
- Çoğunlukla ücretsiz dağıtılan uçtan uça dosya paylaşımı (P2P) programları, ekran koruyucular ve oyunlar içerisine casus yazılımların bohçalanması ile bulaşabilirler.
- Faydalı bir yazılım kurulumunun yanında; dosya, klasör ve sistem kütüğü isimlerini zararsız, bilindik veya sisteme ait isimler vererek saptanmasını ve sistemden kaldırılmasını zorlaştırarak sistemlere yerleşebilirler.
- Herhangi bir programın kurulumu sırasında, casus yazılım özelliği taşıyan başka yardımcı ve ek yazılımların kullanıcıya belirtilerek kurdurulabilirler.

- Kök kullanıcı takımları (rootkit) yardımıyla sisteme uzaktan giriş (login) sağlayarak klasör ve dosyalarını tamamen saklayarak sistemde çalışma yaparken bulaşabilirler.
- E-posta dosya eklentisi ile e-postada verilen bir web adresine gidildiğinde veya doğrudan HTML içerikli e-postaların okunması ile bulaşabilirler.
- İnternet tarayıcılarında bulunan korunmasızlık ve açıklardan yararlanarak kurulum yaparken sistemlere bulaşabilirler.
- Özellikle internet üzerinden, kullanıcıyı aldatan mesajlarla yanıltıp; herhangi bir casus yazılım kurulumunun başlatılması ile bulaşabilirler.
- Uç kullanıcı lisans sözleşmelerinde yanıltıcı veya eksik bildirim ile kullanıcının farkında olmadan zararlı bir yazılımın bilgisayarına kurdurulması ile bulaşabilirler.
- Çocukların ve bilinçsiz kullanıcıların zaafları dikkate alınarak aldatıcı taktikler kullanıp sistemlere bulaşabilirler.
- Çok çeşitli sosyal mühendislik ve insan hatası kaynaklı yöntemler kullanarak sistemlere bulaşabilirler [35].

3.3.2. Kötücül Casus Yazılımların Belirtileri

Casus yazılımlar, bir bilgisayar sistemine bulaştıktan sonra işlerini gizlice yapmaya çalışıp, ulaşacakları amaca sessizce erişmek isterler. Fakat çoğu kez, casus yazılım tanısını ortaya koymada, bazı önemli ve yaygın belirtiler dikkate alınarak kayda değer önemli deliller sunulabilir. Bu belirtiler şu şekilde kısaca özetlenebilir.

- Bilgisayarın mevcut başarımı ve performansında belirgin bir düşüş görülüyorsa,
- İnternet üzerinde tarayıcı ile sörf ederken istenmedik siteler açılıyorsa,
- İnternet tarayıcısındaki arama çubuğu bölümünde aranmak istenen anahtar kelime girildiğinde ayarlanmış olan arama motoru yerine başka bir arama motoru, arama sonuçlarını gösteriyorsa,
- İnternet tarayıcısındaki "*Sık Kullanılanlar Menüsü (Favorites)"* veya "*Yer İmi (Bookmark)"* bölümünde yabancı sitelere bağlantılar eklenmişse,
- İnternet tarayıcısının (browser) başlangıçta gösterdiği site olan "*Başlangıç Sayfası (Home Page)",* ayarlanandan başka bir siteyi gösteriyorsa ve bu ayar tekrar düzeltildiğinde yine farklı siteler açılışta ortaya çıkıyorsa,
- İnternet tarayıcısında daha önce olmayan araç çubukları varsa,
- *Sistem tepsisinde (system tray)* daha önce bilinmeyen bir simge varsa,

- İnternet erişimi olmadığı durumlarda bile, programlarda çalışırken sürekli olarak aralarda reklamlar (pop-up) görünüyorsa,
- İnternet sayfasında bazı tuşlar çalışmıyorsa (örneğin bir web formu doldururken bir sonraki yazım alanına geçmek için kullanılan sekme (tab) tuşu çalışmıyorsa),
- Bilgisayar ile faal olarak çalışılmadığı bir sırada bilgisayar kasasındaki sabit disk hareketini gösteren lamba sürekli yanıp sönüyorsa,
- İnternet'e erişim olmadığı sırada sistem tepsisindeki ağ bağlantısını gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren hareketler görülüyorsa,
- CD sürücüsü kendi kendine açılıp kapanıyorsa,
- Rastgele hata mesajları çıkıyorsa,
- İnternet bağlantısı modem ile gerçekleştirildiğinde büyük meblağlarda telefon faturası geliyorsa, sistemde çok büyük ihtimalle casus yazılım bulunmaktadır [10, 26, 36].

3.3.3. Kötücül Casus Yazılımlardan Korunma

Bilgi ve bilgisayar güvenliğinde, *karşı taraf*; kötü niyetli olarak nitelendirilen kişilerdir. Var olan bilgi ve bilgisayar güvenliği sistemini aşmak veya atlatmak, zafiyete uğratmak, kişileri doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemlerin işleyişini aksattırmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler *saldırı* veya *atak* olarak adlandırılmaktadır.

Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Saldırı türlerinin bilinmesi, doğru bir şekilde analiz edilmesi ve gereken önlemlerin belirlenmesi, bilgi güvenliği için büyük önem arz etmektedir. Alınabilecek bazı güvenlik önlemlerini gerçekleştirmek, bilgisayar güvenliği açısından iyi sonuçlar verecektir. Bu güvenlik tedbirleri aşağıdaki başlıklar halinde özetlenebilir.

1. Kötücül Yazılımlardan Korunma: Antivirüs programı bilgisayarda olmalı ve ulaşan her dosyayı kontrol etmek üzere her zaman çalışabilecek şekilde ayarlanmalı, düzenli olarak güncellemeler açık olmalıdır.

2. İşletim Sistemi Güncellemeleri: Bilgisayarın tüm güvenlik yamalarıyla sürekli güncel tutulması için işletim sistemi güncellemeleri otomatik olarak yapılmalıdır. Bu sayede işletim sistemi üreticilerinin tespit ettiği ve yamalarını oluşturduğu o anki eksiklikler otomatik olarak tamamlanacaktır.

3. Anti-Spyware (Casus Karşı Yazılım) Kullanımı: Kullanıcısının bilgisi dışında yazılım işlemleri gerçekleştiren, kullanıcının internet erişimini takip eden ve bu bilgiyi yine kullanıcının bilgisi dışında bir sunucuya gönderen, bilgisayardan kaldırıldığında bile bu işleri yerine getiren yazılım çeşididir. Bu yollarla kullanıcının bilgi ve onayı dışında detaylı profil bilgileri elde edilebilir ve bu bilgiler değişik amaçlar için kullanılabilir. Bu bilgilerin toplanması ve gönderilmesi sonucunda, hem kullanıcının bilgisayarındaki kaynaklar, hem de internet bant genişliği izinsiz olarak kullanılarak kişilerin özel, şahsi haklarına tecavüz edilmektedir.

Bir spyware yazılımının virüs olarak sınıflandırılmamasının tek sebebi, kendisini sistem içerisinde çoğaltmamasıdır. Ancak bilgisayarı karma

karışık eden bir yapısı vardır. Kullanıcının tüm web kayıtlarını tutar, her olayı izleyebilir, görülmek istenmeyen reklamların ekranda belirmesine sebep olur, webde ilk açılan (home page) sayfasını istenmeyen farklı bir sayfaya yönlendirir ve hatta kullanıcı şifrelerini çalabilir. Antispyware yazılımlar antivirüs yazılımlar ile kullanıldığında bunları belirli ölçüde engelleyecektir.

4. Host/Sunucu Bloklama: Kullanıcının web gezinmelerini takip eden, reklamlarla kullanıcıyı sinirlendiren, virüs ya da trojanları bilgisayarlara kurmaya çalışan kötü olarak bilinen web sitelerine bağlantıdan bilgisayarı korumanın kolay ve ücretsiz bir yoludur. Bloklama her şeye karşı tam bir koruma sağlamaz ama yine de karşı korunmanın kolay bir yoludur. TTNET'in sağladığı güvenlik aile paketleri de host bloklama olarak belirtilebilir.

5. E-Posta Kontrolü: Kullanılan e-posta programı da güvenlik açığı oluşturabilmektedir. Yaygın olarak kullanılmakta olan e-posta programları, dış saldırılara karşı büyük hedef olmaktadır. Bu yazılımların kendilerine özgü güvenlik seçenekleri olmasına rağmen bu yeterli olmamaktadır. Virüs yazılımıyla uğraşan insanların hedefinden uzaklaşmak için fazla revaçta olmayan e-posta yönetim programları kullanılabilir.

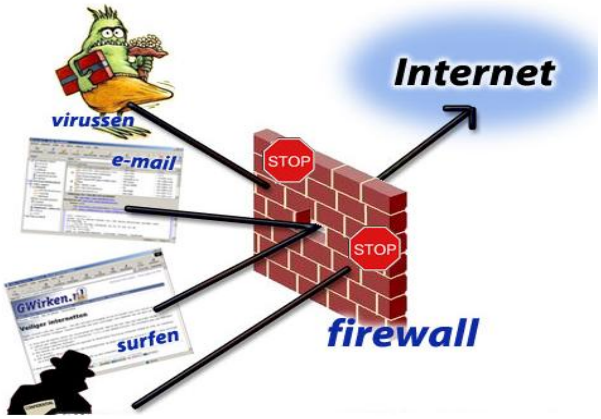
E-postalarla gelen eklentilerdeki çalıştırılabilir dosyalar asla çalıştırılmamalıdır. Özellikle gelen e-posta bilinen bir adresten gelmiyorsa, ya da e-posta gönderen kullanıcı bir dosya eklemediği halde gelen e-postanın ekinde bir dosya mevcut ise bu e-posta ve dosya asla açılmamalıdır. Solucan olarak adlandırılan yazılımlar, kişinin adres defterinden isimleri toplayıp, bu isimleri kullanarak sanki tanıdık birisinden geliyormuşçasına e-posta ve virüslü eklenti gönderebilmektedirler. Tanıdık olsa dahi eğer bir dosya beklenmiyorsa, e-

postadaki ekli dosya açılmadan, hemen silinmelidir. Karşı taraftan gelen e-postadaki dosyanın tipi, boyutu, ismi ve konu başlığını öğrenerek e-postayı açmak büyük olasılıkla kullanıcıyı zararlı yazılımların sisteme bulaşmasına karşı koruyacaktır.

6. Browser (İnternet Tarayıcısı) Kullanımı: İnternet kullanıcılarının birçoğu *internet explorer* ve varsayılan güvenlik ayarlarını kullanmaktadırlar. Bu yüzden zararlı yazılım yazan kişilerin ilgisini internet explorer daha fazla çekmektedir. Bu duruma karşı internet explorer kullanıcıları gerekli güncellemeleri Microsoft'un sitesinden takip etmelidirler. Ayrıca farklı tarayıcı programları kullanılarak internet ağında dolaşmak da bazı saldırılara karşı etkili bir çözüm olabilecektir.

7. Ofis Programları: Microsoft Office dokümanları içerisinde çeşitli makrolar oluşturulabilmektedir. Bu makrolar kötü niyetli kişiler için oldukça elverişli ortam oluşturmaktadır. Makro virüslerinden korunmak adına Open Office uygulamaları kullanmak faydalı olacaktır.

8. Güvenlik Duvarı (Firewall) Kullanımı: İnternete bağlanmak durumunda olan sistemler ve bilgisayarlar her an için saldırılara maruz kalabilirler. Şekil 8'de görüldüğü gibi internete çıkıldığı durumlarda dış etkenlerden korunmak için bir güvenlik duvarına ihtiyaç var demektir. İnternete bağlı olan bir bilgisayar veya sistem dakikada ortalama bir saldırıya maruz kalabilmektedir [37]. Güvenlik duvarı kullanıcının mahremiyetini korumak içindir. Bu yüzden kullanıcılar antivirüs programı dışında ayrıca bir güvenlik yazılımına gereksinim duyarlar.



Şekil 8. Firewall [37].

9. Yönlendirici (Router) ve Anahtar (Switch): Ağ sistemlerinde yönlendirici ve switch yaygın olarak kullanılan ağ aktif cihazlarıdır. Bu ekipmanların önemli ve temel özellikleri karşılaştırmalı olarak Tablo 3'de verilmiştir.

Tablo 3. Anahtar ve yönlendirici cihazlarının karşılaştırması

Anahtar Cihazının Özelliği	**Yönlendirici Cihazının Özelliği**
Tüm portlar aynı ağ adresini kullanır.	Her bir portun ağ adresi farklıdır.
Yönlendirme tablosu MAC adresine göre düzenlenir.	Yönlendirme tablosu IP adresine göre düzenlenir.
Trafik MAC adresi bilgisine göre filtrelenir.	Trafik ağ veya host bilgisine göre filtrelenir.
Broadcast trafiğini iletir.	Broadcast trafiğini iletmez.
Trafiği bilinmeyen adrese iletir.	Trafiği bilinmeyen adrese iletmez.
Güvenlik yüksek seviyede değildir.	Güvenlik yüksek seviyededir.
OSI referans modelinin üçüncü katmanında çalışır.	OSI referans modelinin ikinci katmanında çalışır.

En güvenilir firewall yazılımına veya antivirüs yazılımına sahip olmak tam güvenlik demek değildir. Eğer internete çıkıldığında kullanıcı ne yaptığını, nerede olduğunu ve ne gibi saldırılarla karşılaşacağının farkında değilse, virüs ve buna benzer tehlikelere karşı savunmasız demektir. Anlatılan bu tedbirlere uymak bile bazen kullanıcıya güvenlik açısından yeterli gelmeyecektir. Bu nedenle web ortamına çıkıldığında hiçbir şeye güvenmemek, girilen sitelerin ve gelen e-postaların güvenilirliğini tam kontrol ederek hareket etmek gerekmektedir [40].

4. AĞ GÜVENLİĞİ

4.1. Giriş

Son yıllarda internetin yaygın kullanımı ve e-ticaretin kullanımının artmasıyla, sanal ortamda oluşabilecek dijital saldırılarda buna paralel olarak artmaktadır. Bu saldırılar, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur. Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları bilgisayar ağları üzerinde hâlâ büyük bir tehlike oluşturmaktadır. Bununla beraber kurum ve kuruluşlar sanal dünyanın uçsuz bucaksız ortamında ağ saldırıları ve ağda yapılan aldatmacalara karşı güvenliklerini sağlamak için güvenlik politikaları da uygulamak zorunda kalmaktadırlar [32].

4.2. Ağ Saldırıları ve Ağda Yapılan Aldatmacalar

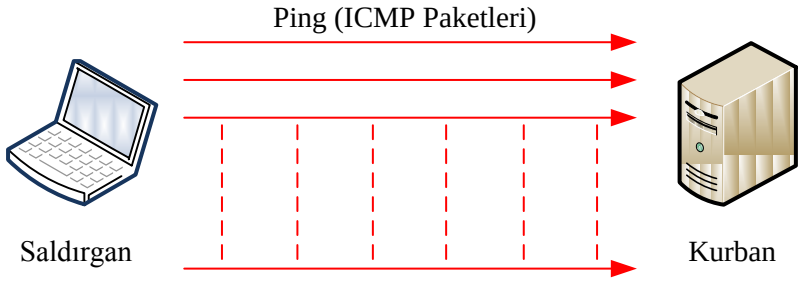
Bu bölümde, internet ortamında veya yerel ağ ortamlarında gerçekleştirilen önemli birkaç saldırı ve aldatmaca yöntemlerinden alt başlıklar halinde bahsedilmektedir.

4.2.1. DoS Saldırıları

Temel olarak tüm DoS (Denial of Services - Servis Dışı Bırakma) atak türleri sistem kaynaklarını veya bant genişliğini tüketerek servislerin hizmet dışı bırakılmasını amaçlamaktadır. DoS saldırıları farklı türlerde gerçekleştirilebilmektedir. Bu DoS ataklarını üç başlıkta toplamak mümkündür[39]:

1. DoS (Denial of Service): Paket direkt olarak hedef sisteme gönderilir. Asıl hedef web uygulamaları değil, sunuculardır. DoS saldırıları veri paketlerinin sunucuya/bilgisayara gönderilmesi ile çalışır. Yoğun bir şekilde gönderilen bu paketlere sunucunun/bilgisayarın cevap verememesi, sunucunun/bilgisayarın istemcilerin istek paketlerine cevap vermesine engel olur. Bu paketler işlemci, hafıza ve bant genişliği gibi sistem kaynaklarını tüketir. Bu tüketme sonucunda sistem çalışamaz duruma gelir. Şekil 9'da belirtildiği üzere, DoS saldırısı tek bir kaynaktan (saldırgan) tek bir hedefe (kurban) yöneliktir. Hedef bir sunucu veya bir bilgisayar olabilir. DoS atağında saldırgan bağlantı kurmak için birçok ICMP paketi (ping) yollar. Saldırganın buradaki amacı bağlantı kurmak değil bant genişliğini sömürerek sistemin çalışmasını engellemektir. Tek kaynaktan yapılan DoS saldırıları,

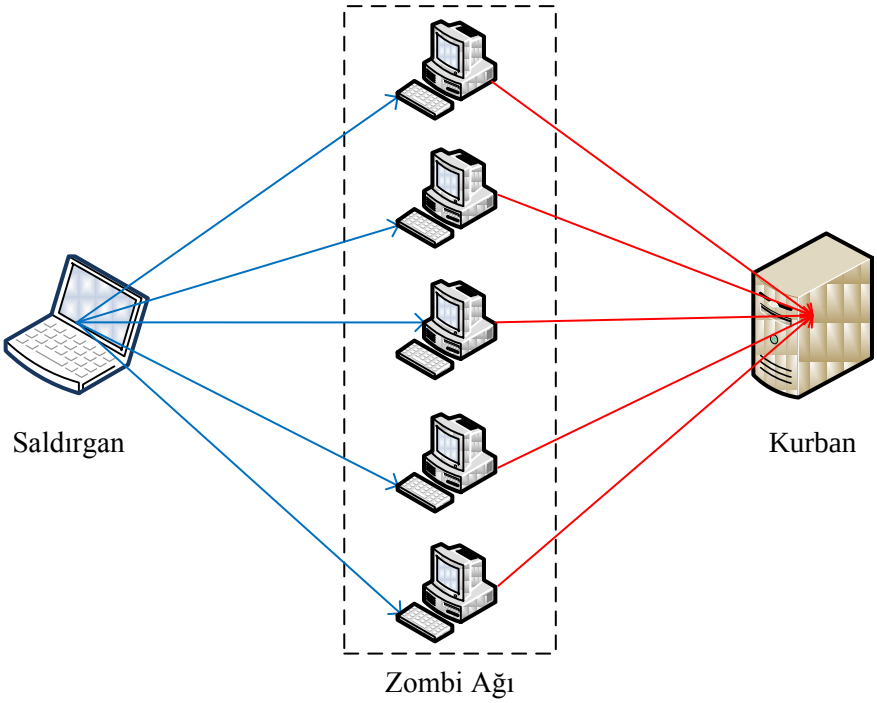
günümüzde bant genişlik oranları arttığından dolayı fazla kullanılmamaktadır. Bu yüzden DoS saldırısından bahsedildiğinde, genellikle DDoS saldırıları kastedilmektedir.



Şekil 9. DoS saldırı şeması

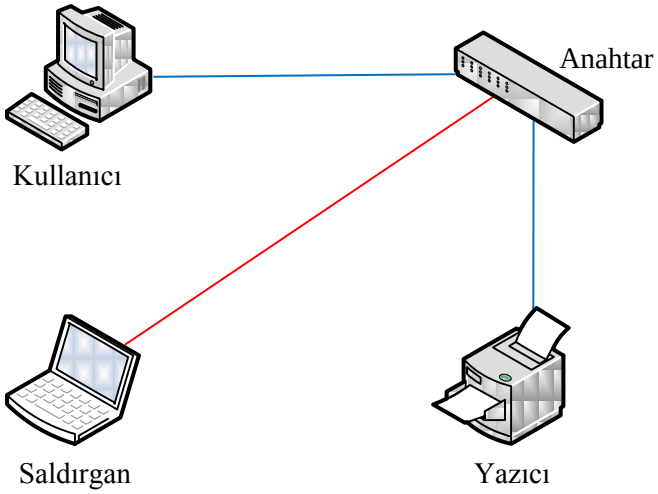
2. DDoS (Distributed Denial of Service): Çoğunlukla tek kaynağın, birden fazla bilgisayarı/sistemi yönlendirmesi ile yapılan saldırı türüdür. Şekil 10'da belirtildiği üzere, saldırganın bulunduğu bir bilgisayar, ağ sistemi içerisinde kontrol altına almış olduğu ağdaki diğer bilgisayarları kullanarak onlar üzerinden tek hedefe saldırı yapar. Bu saldırı sisteminde saldırgan kendisine bir *zombi ağı* oluşturur. Zombi ağındaki bilgisayarlar asıl saldırgan tarafından kullanılan ve kullanıldıklarının farkında bile olmayan masum bilgisayarlardır. Bu masum kaynaklardan tek bir hedefe çoklu ataklar yapılır. Anlık gönderilen paket sayısı zombilerin sayısı ile doğru orantılıdır. Çoğunlukla saldırıyı yapan kaynak tespit edilemez. Şekil 10'da belirtildiği üzere, korsanlar DDoS saldırılarını bu zombiler üzerinden yaparak hem aynı anda birçok bilgisayarın saldırmasını sağlar, hem de kendi kimliklerini ve IP numaralarını gizlerler. IP spoofing yöntemi kullanılarak gerçekleştiren bu saldırılarda IP numaraları gizlenebilir veya herhangi bir bilgisayarın IP numarası ile değiştirilebilir.

Korsan bilgisayar, zombi ağındaki bilgisayarları ele geçirme işlemini *zombi* adı verilen yazılımlar ile gerçekleştirir. Bu zombi yazılımları genellikle birer trojandır. DDoS saldırılarında, zombi ağı (saldırı ağı) genellikle IP Spoofing'e dayalı olarak Smurf, Fraggle, SYN Flood saldırları gibi yöntemleri kullanır. DoS ve DDoS'ta benzer saldırı tipleri kullanılmasına rağmen DDoS'u farklı kılan en önemli özellik, Şekil 10'da görüldüğü üzere, trafik yoğunluğunun daha fazla olmasıdır.



Şekil 10. DDoS saldırısı şeması

3. PDoS (Permanent Denial of Service): Bu saldırı sisteminde, saldırgan direkt sunucu veya uygulamaları hedef alma yerine Şekil 11'de bir örneği gösterildiği gibi yönlendirici, yazıcı, anahtar veya ağda çalışan farklı bir donanım elemanını hedef alır. Saldırılarda amaç, ilgili donanımın firmware yazılımını değiştirmek, bozmak veya silmektir.

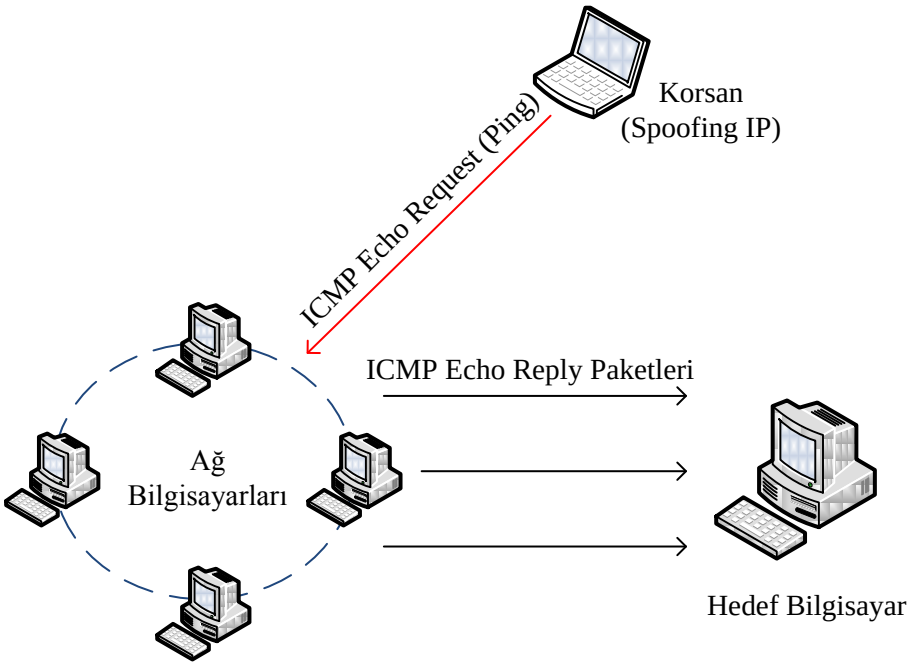


Şekil 11. PDoS saldırı örneği

DoS, DDoS, PDoS saldırılarından başka, ICMP paketlerinin farklı biçimlerde kullanımı ile gerçekleştirilen DoS saldırıları da bulunmaktadır.

ICMP paketleri, bilgisayarda geri bildirim mekanizması görevini gören bir protokoldür. Flood terimi ise, çok küçük zaman diliminde anlamlı veya anlamsız veri paketlerinin, cevap verilemeyecek şekilde gönderilmesidir. ICMP Flood, ICMP protokolünü kullanarak hedef bilgisayara DoS saldırısı yapılmasını sağlayan yöntemlerden biridir. Bu saldırı türünün farklı biçimleri vardır. En bilinenleri Smurf saldırıları, Fraggle saldırıları, Ping Flood, Ping of Death ve SYN Flood yöntemleridir. Bu yöntemlerin genel özellikleri alt başlıklar halinde anlatılmıştır.

Smurf: *Bu saldırı* yanlış konfigüre edilmiş *broadcast adresi* gibi ağ araçlarını sömürmeyi dikkate alarak çalışır. Bir ağ üzerinde broadcast adresi, aynı ağ üzerinde bulunan bilgisayarlara (hostlara) paket göndermeyi sağlar. Smurf saldırıda broadcast adresini kullanarak kaynağı gizlenmiş (spoof edilmiş) ping paketlerinin bilgisayarlara gönderilmesi amaçlanır. Bu saldırıda ICMP paketlerindeki kaynak adresi IP Spoofing yöntemi ile değiştirilir. Şekil 12'de gösterildiği gibi, ICMP paketleri zombilere gönderilir. Zombiler paketleri hedefe yollar. Hedef kendisinin göndermediği çok sayıda ICMP Echo Reply cevap mesajları aldığı için, bu mesajlara cevap veremez duruma gelir. Günümüzde pek etkili olmamakla, 1990'lı yıllarda internetin vebası olarak adlandırılıyordu.



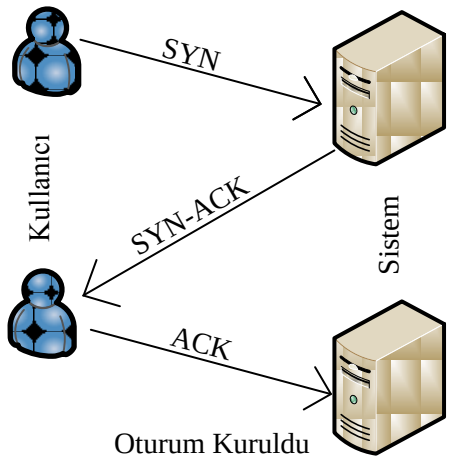
Şekil 12. Smurf saldırı şeması

Fraggle: Bu saldırı aslında *Smurf* saldırının bir varyantıdır. Aralarındaki tek fark, Smurf saldırıları TCP alt yapısını kullanırken, Fraggle saldırıları UDP altyapısını kullanır.

Ping Flood: Bu saldırı, direkt hedefe yöneltilen sonsuz sayıdaki ICMP Echo Request (Ping) paketleri ile yapılır. Gönderilecek paket sayısı belirlenebilir, bir saldırgan için çok fazla teknik bilgi gerektirmediğinden en basit saldırı yöntemlerindendir. Saldırılacak hedef sistemden daha hızlı bir bağlantıya ve bant genişliğine sahip olmak yeterlidir. DSL bağlantıya sahip olan korsan, Dial-up bağlantılı kurbanın bant genişliğini rahatlıkla doldurabilir. Ping flood saldırısı basit olmasına rağmen, eski ve tercih edilmeyen bir saldırı tipidir.

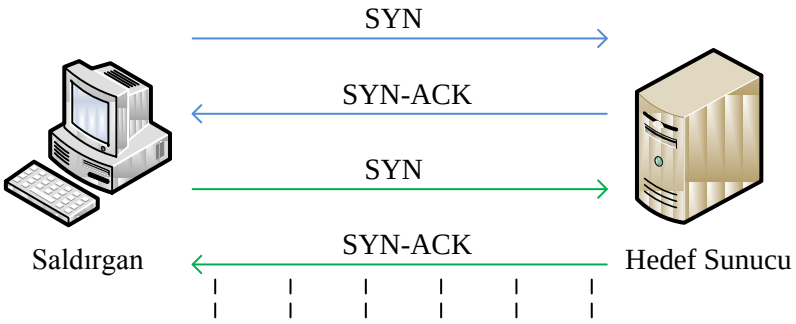
Ping of Death: Çok büyük boyuttaki ICMP paketleri (ping) direkt olarak hedefe gönderilir. Gönderilen paketin büyüklüğüne göre, sistem donabilir, çökebilir veya yeniden başlayabilir. Normal ping paketleri 32 byte iken bu saldırı tipindeki ping paketleri 65535 byte değerindedir.

TCP/SYN Saldırısı (SYN Flood Saldırısı): TCP bağlantı temelli bir protokoldür. Birbiriyle iletişim kuran iki bilgisayar, paketlerini önceden kurulmuş bir hat üzerinden aktarırlar. Bunun için iletişimin başlaması esnasında Şekil 13'de görüldüğü gibi 3 yönlü el sıkışma kuralıyla (handshake) hat kurulur. Bir TCP bağlantısının başında istekte bulunan uygulama, SYN paketi gönderir. Alıcı sistem/server SYN-ACK paketi göndererek isteği aldığını onaylar. Son olarak istekte bulunan uygulama ACK göndererek hattın kurulmasını sağlar.



Şekil 13. Normal TCP işleyişi

Flood saldırısı, kısa zamanda fazla sayıda bağlantı kurarak sisteme zarar vermek demektir. Bu saldırı türünde saldırgan, internet üzerinde kullanılmayan IP adreslerini kullanarak birçok SYN paketini hedef makineye yollar. Hedef makine, alınan her SYN paketi için kaynak ayırır ve bir onay paketini(SYN-ACK), SYN paketinin geldiği IP adresine yollar. Hedef makine, kullanılmayan IP adresinden yanıt alamayacağı için SYN-ACK paketini defalarca tekrarlar. Saldırgan bu yöntemi üst üste uyguladığında hedef makine ayırdığı kaynaklardan ötürü yeni bir bağlantıyı kaldıramaz duruma gelir ve bu sebepten makineye bağlanılamaz. Bu saldırıda TCP'nin 3 yollu handshake açığı kullanılır. Şekil 14'de gösterildiği gibi saldırgan SYN paketlerini hedefe/sunucuya gönderir (1. el sıkışma). Hedef SYN paketine SYN ACK olarak cevap verir (2. el sıkışma). Kaynak gelen pakete cevap vermeden yeni bir SYN paketi yollar ve hedef sürekli cevap bekler konumda kalır. TCP/SYN saldırıları genellikle sunucu kaynaklarına yapılan atak türlerinden olup TCP/IP servislerini devre dışı bırakmak için kullanılan bir saldırı türüdür.

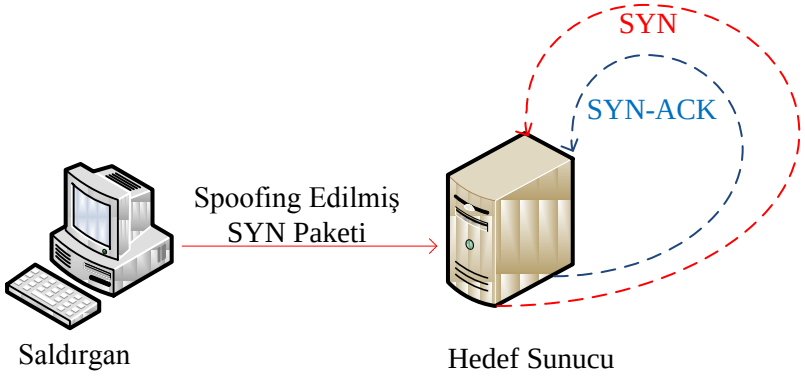


Şekil 14. SYN Flood saldırı şeması

Hizmet aksatma (DoS) saldırı tipleri sadece belirtmiş olduğumuz saldırı türleri ile sınırlı değildir. Ayrıca, Land Attack, Tear Drop ve Nuke gibi popülerliğini yitirmiş hizmet aksatma saldırıları da bulunmaktadır.

Land Attack: Saldırganın spoofing yaparak kaynak ve hedef adresi değiştirilmiş paketler ile sisteme saldırmasıdır. Paket içerisindeki kaynak ve hedef adresi, gönderilecek hedefin adresi olarak belirlenir. Paket hedefe ulaştığında hedef kendi paketini sürekli cevaplayacağından ve ACK cevap paketini alamayacağından sonsuz bir döngü içerisine girer ve çöker. Şekil 15'de gösterildiği gibi saldırgan SYN paketlerini hedefe/sunucuya gönderir. Hedef, SYN paketine, hedef ve kaynak adresi kendisini gösterdiğinden dolayı kendisine SYN ACK olarak cevap verir. Ancak ACK cevabını alamayacağından tekrar

SYN paketi yollar. Hedef bu şekilde sonsuz bir döngüye girer. Sonuçta ise sistem genellikle çöker.



Şekil 15. Land Attack saldırı şeması

Tear Drop: Parçalanmış UDP paketleri bozuk ofsetler ile hedefe gönderilir. Hedef paketleri tekrar birleştirmeye çalıştığında bozuk veya hatalı bir paket üretmiş olur ve sistem genellikle çöker.

Nuke: Windows NT makinelerde, NETBIOS'un bir açığından faydalanarak, 139. Porta paketler göndererek, sistemin mavi ekran hatası vermesidir [8].

DoS saldırılarından korunmak için; ağ trafiğinin izlenmesi, IDS/IPS sistemlerinin kurulması, bant genişliğinin artırılması, güncellemelerin yapılması, özellikle yönlendiriciler üzerinde doğru konfigürasyonların yapılması, firewall bulundurulması gibi temel önlemler alınabilir. Doğru konfigürasyon yapılması ile ilgili Cisco bir Router üzerinde DDoS saldırılarının engellenmesi adına aşağıdaki ayarlama yapılabilir.

```
Router(config-if)# no ip directed-broadcast
```

Bu konfigürasyon ile yönlendirici; gelen paketleri broadcast adresine yönlendirmeyecektir. Çünkü, ping (ICMP Echo Request) paketleri, yayın IP adresine (broadcast) gönderilir, bu adresten de ağ üzerindeki bilgisayara iletilmesi sağlanır, bu ayarlama ile bu engellenmiştir.

Sonuç olarak, DoS saldırıları ile ilgili temel bilgiler verilmiştir. Her saldırı türünün kendine özgü bir modellemesi vardır. Gün geçtikçe kimisi geçerliliğini yitirirken kimisi daha da güçlenmektedir. Günümüzde tüm DoS saldırılarının engellenmesi için geliştirilmiş kesin bir yöntem de mevcut değildir [29].

Literatürdeki kaynaklar incelendiğinde ağlarda yapılan saldırıların tam olarak bir sınıflama içerisinde olmadığı görülmektedir. Bunun en büyük sebebi ise, ağda yapılan bir

saldırının genellikle tek başına değil de, diğer saldırı türlerinin de kullanılması ile gerçekleşmesidir. Buna örnek olarak, DDoS saldırısında yapılacak saldırı sistemi için IP Spoofing yönteminin de kullanılması gösterilebilir. Bu yüzden bu tez çalışmasında da her saldırı türü ayrı bir alt başlık olarak incelenmiştir.
Ağ sistemlerine, sunuculara veya bilgisayarlara yapılan saldırılar sadece DoS saldırıları ile sınırlı değildir. DoS haricinde yapılan saldırılardan bir kısmı aşağıda belirtilmiştir.

4.2.2. Spoofing Saldırıları

Spoofing paketlerin bir bilgisayardan başka bir bilgisayara gönderilmesi sırasında kullanılan IP adresinin olduğundan farklı olarak gösterilmesidir. ICQ spoofing, DNS spoofing, IP spoofing, E-mail spoofing gibi birçok çeşitleri bulunmaktadır [9].

ICQ Spoofing: ICQ protokolünde gönderilen mesajların bir başkasından gönderiliyormuş gibi gösterilmesidir.

DNS Spoofing: Saldırganın yerel ağdaki DNS isteklerini izleyerek bu isteklere sahte cevaplar vermesine dayalı çalışan bir sistemdir. Saldırgan bir DNS çözümleme işlemine müdahale ederek, kullanıcıları farklı sistemlere yönlendirebilir. Saldırgan, anahtarlı ağlarda ARP zehirlemesi ile varsayılan ağ geçidini ele geçirir. Yani DNS sunucuların kandırılarak istenilen IP'nin olması gerektiğinden farklı bir şekilde gösterilmesi işlemidir.

IP Spoofing: İnternetin çalışmasını sağlayan TCP/IP protokol ailesi geliştirilirken güvenlik temel amaç olmadığı için olabildiğince esnek davranılmıştır. Bu esneklik IP adreslerinin aldatılabilir (spoofed) olmasına sebep olmuştur. IP Spoofing işlemi, IP paketlerinin yanlış kaynak adres kullanılarak gönderilmesidir. IP spoofing işlemi; saldırıda bulunan kişinin IP adresini gizlemesi, başka bir taraf ya da kişiyi saldırı yapan olarak göstermesi, güvenilir bir kullanıcı gibi görünmesi, network trafiğini dinleme/ele geçirme veya ortadaki adam saldırısı gibi saldırıları gerçekleştirmek için kullanılır. Spoofing saldırılarında en çok kullanılan IP spoofing yöntemidir. IP spoofing yöntemi saldırının bir aşamasıdır.

E-Mail Spoofing: Gönderilen mail kaynağının gizlenerek mailin nereden geldiğinin belirlenememesidir.

Spoofing olaylarına karşı genel korunma yöntemleri olarak; kaynak IP yanında hedef IP ve MAC kontrolünün yapılması, yönlendiricilerde kaynak yönlendirme

fonksiyonunun pasif hale alınması, iç ağın internete açıldığı yerde güvenlik duvarı kurulması, paket filtreleme, şifreleme yöntemleri sayılabilir.

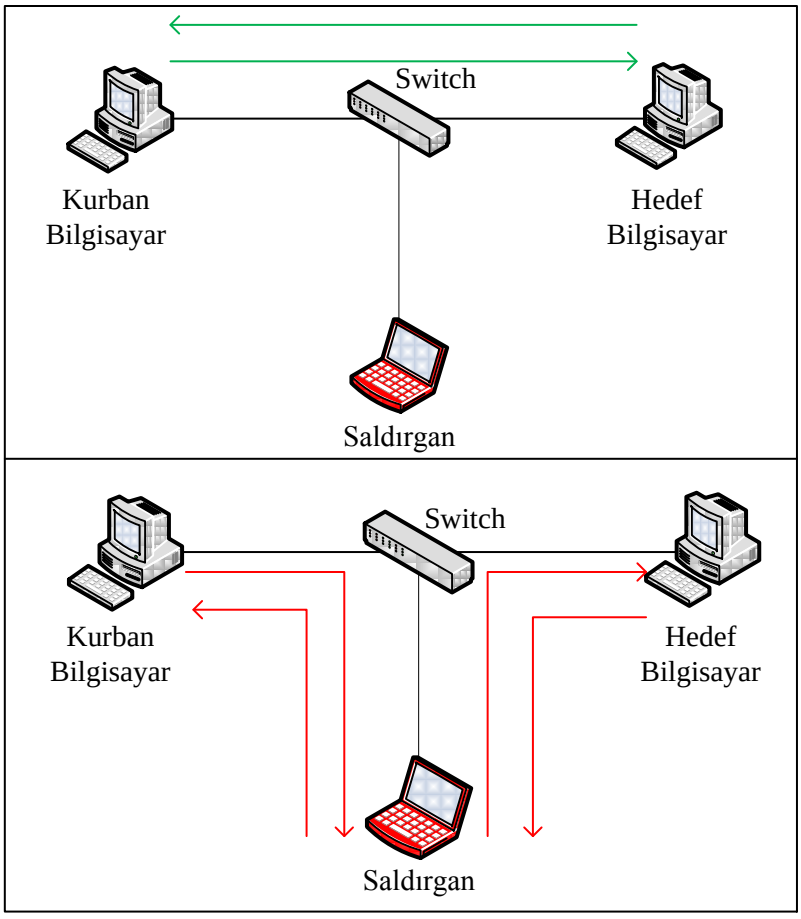
4.2.3. Diğer Saldırılar

SQL Injection: Web uygulamalarının kodlanma sürecinde yapılan hatalar ve dikkatsizlikler, uygulamalara yönelik komut saldırıları yapılmasına olanak sağlamaktadır. Bu hatalar, tanımlanmamış kodlar olabileceği gibi, filtrelenmemiş karakterler de olabilir. SQL injection, korsanın hedeflediği sisteme sızabilmek için kullanabileceği SQL komutları ve bazı karakterlerin ortak kullanımı ile oluşturulacak komut saldırılarıdır. Bu saldırı tipi veritabanları ile çalışan web uygulamalarına yöneliktir. Eğer, web veritabanı üzerinde gerekli önlemler önceden alınmamış ise, saldırgan SQL injection sayesinde veritabanında veri girme, silme, güncelleme gibi işlemleri gerçekleştirebilir. Veritabanı kullanan web siteleri için en büyük tehlikelerden biridir.
SSI injection, cross site scripting, reflected xss saldırıları, stored xss saldırıları, cross site request forgery saldırıları gibi direkt web uygulamalarına yönelik yapılan saldırılarda mevcuttur.

Sniffing: Sniffing temel olarak veriyi izlemek, koklamak olarak tabir edilebilir. Sniffing ile ağdaki paketler yakalanabilir, içerikleri okunabilir. Sniffing olayındaki amaç; şifreleri (E-Mail, WEB, SMB, FTP, TELNET, SQL), e-posta içeriğini, transfer edilen dosyaları (E-Mail, FTP, SMB) yakalamaktır. Snifferlar ağda olup biteni izleyen programlar oldukları için hem sistem yöneticileri hem de korsanlar için en önemli araçlardır. Sniffing metodu pasif sniffing ve aktif sniffing olarak ikiye ayrılır.
1. Pasif Sniffing: Hub kullanan sistemler için geçerlidir. Hub kullanan ağlarda paketler tüm bilgisayarlara iletilir. Ağdaki veri LAN üzerinden tüm bilgisayarlara gönderildiği için sniff etmek kolaydır.
2. Aktif Sniffing: Switch kullanan sistemler için geçerlidir. Switch, MAC adreslerine bakar ve veriyi sadece alması gereken bilgisayara gönderir. Saldırgan, switchi zehirlemeye çalışır, binlerce MAC adresi gönderip switchin bir hub gibi davranmasına neden olur ve verinin tüm portlardan çıkmasını sağlar.
Veri paketlerinin ağ içerisinde bulunan tüm bilgisayarlara iletilmesi, hub kullanılan ağlarda olur. Sniffing işlemleri genelde bu ağlarda direk olarak uygulanabilir. Ancak switch

kullanılan ağlar hub kullanılan ağlara göre daha güvenli olduğunda switch kullanılan ağlarda da ARP Poisoning saldırıları ile güvenlik atlatılabilmektedir [8].

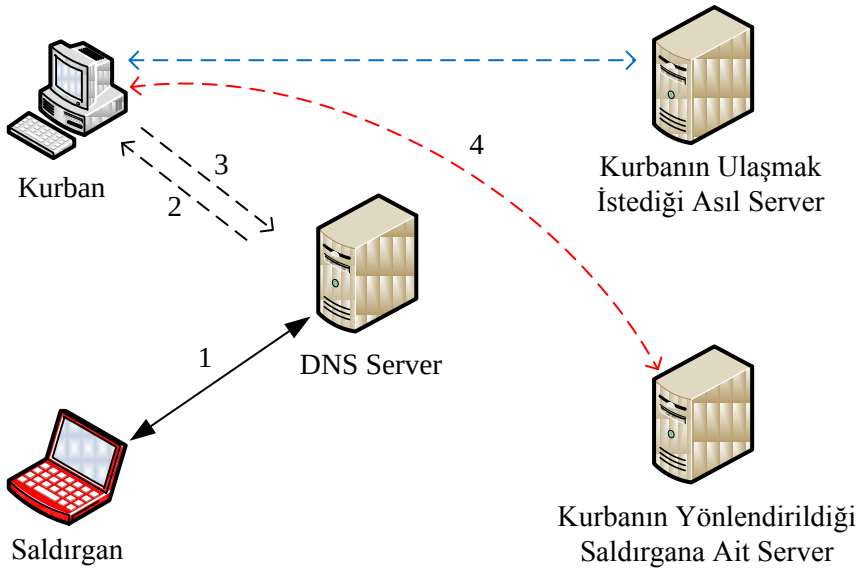
ARP Poisoning: ARP, veri göndermek için IP adresinin MAC adresini çözümlemeye yarayan protokoldür. ARP paketleri taklit edilerek saldırgan kendi makinesine verileri yönlendirebilir. Saldırgan ARP poisoning yaparak iki bilgisayar arasındaki trafiğin ortasına geçebilir. Gateway'e yapılacak flood ile verinin tüm portlara gönderilmesi sağlanarak sniff yapılabilir. Şekil 16'da üst kısım normal ağ trafik akışını gösterirken, alt kısım ise ARP poisoning olayının bulunduğu durumdaki ağ trafik akışını göstermektedir. Saldırgan IP adresini ve MAC adresini gatewaymiş gibi broadcast yaparak duyurur. Kurbanın ağ trafiği saldırgan üzerinden geçmeye başlar ve saldırgan kurbanın ağdaki tüm verilerini yakalar.



Şekil 16. ARP Poisoning saldırı şeması

DNS Poisoning: Yanlış DNS bilgileri birincil DNS sunucuya tanıtılır. Tüm istekler değiştirilmiş DNS sunucusuna yönlendirilir.

DNS Cache Poisoning: DNS isim çözümleme servisidir. İsmi, IP adresine, IP adresini, isme çevirir. DNS Cache Poisoning olayını Şekil 17'ye bakarak temsili olarak tanımlamak gerekirse; saldırgan DNS Server sistemindeki DNS eşleştirmelerinden bazılarını değiştirir. Bu yüzden kurban bilgisayar ulaşmak istediği sunucudan farklı bir sunucuya yönlendirilir.

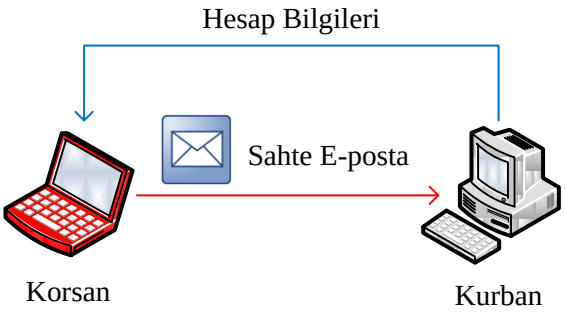


Şekil 17. DNS Cache Poisoning saldırı şeması

Phishing: Sahte e-postalar aracılığı ile genellikle şifre ve kredi kartı türündeki kişisel bilgilerin, sosyal mühendislik yöntemlerinin de eklenerek kullanıcıdan alınması olayı phishing olarak adlandırılır. Bu ifade dilimizde sazan avlama veya olta saldırısı olarak adlandırılır. Bazı e-posta içerikleri çok gerçekçi görünebilir. Eğer bir e-posta mesajı aşağıdaki cümlelerden birini içeriyorsa büyük ihtimalle bilgileri çalma amaçlı olta saldırısıdır.

- Hesap bilgilerinizi doğrulamanız gerekiyor!
- Eğer hemen cevaplamazsanız hesabınız iptal edilecek!
- Bilgilerinizi güncellemek için aşağıdaki bağlantı adresine tıklayın!

Phishing saldırılarında Şekil 18'de temsili olarak gösterildiği gibi korsan bilindik bir bankadan geliyormuş gibi bir sahte e-posta hazırlar ve bunu kullanıcıya gönderir. Sosyal mühendislik yöntemleri kullanılarak hazırlanan cümleler ile kullanıcıdan gerekli kişisel bilgiler ve şifreler elde edilmeye çalışılır. Eski bir yöntem olmasına rağmen popülerliğini hala devam ettirmekte olan bir saldırı türüdür.



Şekil 18. Phishing (sazan avlama)

Phishing saldırılarına karşı şu tedbirler alınabilir:

- Güvenilir kaynaklar, e-posta aracılığı ile şifre türü önemli bilgileri istemez.
- Bilinmedik adreslerden gelen e-postalar okunmadan silinmelidir.
- E-postalardaki IP numaraları üzerinden web sitelerine girilmemelidir.
- Banka ve online alışveriş işlemlerinde güvenli protokol (Https) kullanıldığından emin olunmalıdır.
- Hesap özetleri düzenli olarak kontrol edilmelidir.
- Bunlara rağmen bir phishing saldırısına maruz kalındı ise hemen savcılığa başvurulmalıdır.

Kullanıcıların olta saldırılarına inanmalarını engellemek, gelen e-postaların zararlı olup olmadıklarını tespit etmek için kullanıcıları uygulamalı olarak eğiten;
http://www.washingtonpost.com/wp-srv/technology/articles/phishingtest.html
http://www.sonicwall.com/phishing/
gibi web siteleri bile kurulmuştur. Yukarıdaki web adreslerinde, gelen e-postaların phishing amaçlı olup olmadıklarını tespit etmek için, son kullanıcıları bilinçlendirmeye yönelik uygulamalar mevcuttur.

Sosyal Mühendislik: Ağ sistemlerindeki saldırı türleri ile beraber, insan zafiyetlerinden yararlanmaya dayanan sosyal mühendislik konusu da saldırılara zemin hazırlamaktadır. Sıradan kullanıcı yetkileriyle, ilgili sistem hakkında elde edilemeyecek kritik bilgilerin; ikna etme, etkileme, aldatma gibi faktörler ile ele geçirilmesi *Sosyal Mühendislik* olarak adlandırılır. Sosyal mühendislik bazı kaynaklarda *toplum mühendisliği* olarak geçmektedir [17]. Sosyal mühendislik yöntemleri güvenlik sürecinde savunulması en zor saldırı yöntemi olarak sayılabilir. Çünkü, bu yöntemde hedef direkt olarak insan zafiyetlerinden

yararlanmaktır. Sosyal mühendislik yöntemleri olarak; yetkili personel gibi görünme, müşteri temsilcisi rolünde görünme, teknik personel gibi görünme, yardımsever görünme, minnet altında bırakma, zaaflardan yararlanma, hatta çöp sepetlerindeki bilgilerin toplanması vb. günlük insan hayatıyla ilgili senaryolar gösterilebilir.

Sosyal mühendislik kandırma sanatına dayandığından dolayı, kişinin muhatabı üzerinde bıraktığı etki ve ikna yeteneği önemli etkenler olarak öne çıkmaktadır. Sosyal mühendislik yoluyla muhatabını kandırmayı başaran kötü niyetli bir kullanıcı bir anda tüm yetkilere sahip olabilir. Sosyal mühendisliğin kurumsal ve kişisel zararlarından korunmak için kullanıcıların eğitimine önem verilmeli, fiziksel güvenlik sağlanmalı, şifreleme sistemleri dikkatli kullanılmalı, biometrik sistemler ile kullanıcı doğrulaması vb. tedbirler alınmalıdır.

Yukarıda belirtilen saldırı türlerine karşı, genel anlamda aşağıda belirtilen korunma yöntemleri uygulanmalıdır.

- Ağ kartlarına fiziksel ulaşımı engelleyerek sniffer yazılımlarının kurulması engellenmelidir.
- Statik IP adresleri kullanıp, ARP kayıtlarını statik olarak eklemelidir.
- Ağda sniffer yazılımı olup olmadığını denetlemek için ARP watch, promiscan, antisniff, prodetect, wireshark gibi yazılım araçları kullanılmalıdır.
- Ağ anahtarlarında port güvenliği sağlanmalıdır.
- Büyük ağa sahip kurum ve kuruluşların ağ sistemlerinde farklı VLAN'lar tanımlanmalıdır.
- Ağ hizmeti sunan kurum ve kuruluşların sistemlerinde saldırı tespit sistemlerinin (IDS/IPS) kullanılması sağlanmalıdır.

Ayrıca casus snifferlardan korunmanın en iyi yolu ağ trafiğini şifrelemektir. Bunun için ağ sisteminde; iyi bir yöntem olan SSH ve IPSEC kullanmak da, snifferların çalışmasını tam olarak engellemeyecek, fakat snifferların yakaladığı verilerin anlaşılma süresini uzatacaktır.

4.3. Veri Paketlerinin Ağda İletimi

Ağ ve bilgi sistemleri üzerinden iletişime geçebilmek için, posta sisteminde olduğu gibi bir adresleme mekanizmasına ihtiyaç duyulur. Bu mekanizmada iki önemli adres vardır. Bunlardan birisi fiziksel adres, diğeri de IP adresidir. Fiziksel adres, OSI referans modelinin ikinci katmanı olan veri bağı (data-link layer) katmanında ele alınır ve asıl

haberleşmede kullanılan adrestir. IP Adresi ise OSI referans modelinin üçüncü katmanı olan ağ katmanında ele alınır. Bilgisayar ağlarına yönelik adli bilişim kapsamında ağ üzerinden yapılan bir bilişim suçunda kaynağa ulaşabilmek için bu iki adresi iyi bir şekilde anlamak büyük önem taşımaktadır.

Günümüzde çoğu internet erişimi, önce yerel alan ağları üzerinden başlar. Bu tip ağlarda iletişim ortak bir kanal (broadcast kanalı) üzerinden gerçekleşir. Dolayısıyla ortak paylaşılan bir kanala gönderilen bir çerçeve (frame), bütün istemcilere (host) ulaşır ama asıl istenen ağdaki sadece belirli bir istemcinin bu çerçeveyi alıp, işleme koymasıdır. Bu yüzden veri bağı katmanındaki başlık alanında, hedef makineyi belirtecek bir adrese ihtiyaç duyulmaktadır. Bu adrese fiziksel adres denir.

Fiziksel adres; yerel alan ağı adresi, ethernet adresi, MAC adresi gibi değişik isimlerle de telaffuz edilmektedir. MAC adresi 6 bayt, yani 48 bitten oluşan ve onaltılık (hexadecimal) formatta "3C:5B:34:23:F4:A5" ifade edilir. Aslında yerel ağdaki her makinenin değil, makine üzerinde bulunan ağ bağdaştırıcı kartının bir fiziksel adresi vardır. Fiziksel adresler benzersizdir. Yani her kartın farklı bir fiziksel adresi vardır. Bu adresler ağ bağdaştırıcı kartının üreticisi tarafından kart üzerinde bulunan ROM'a yakılarak yazılırlar. Bu numaraları da IEEE düzenler.

IP adresi denilen ikinci bir adrese ihtiyaç duyulması; ise fiziksel adreslerin bir paketi, fiziksel olarak arasında bir bağ bulunan, bir düğümden başka bir düğüme iletmesi, IP adreslerinin ise paketleri hedef ağa iletmesindendir. IP adresleri hiyerarşik bir yapıda çalışırlar.

İletişimde dikkat edilmesi gereken en önemli husus, kaynak sistem ile hedef sistem arasında yer alan her düğüm, paketi alıp bir sonraki düğüme yönlendirirken veri bağı katmanında, kaynak fiziksel adresi silip kendi fiziksel adresini paket başlığına yerleştirmektedir. Fakat, üçüncü katmanda bulunan kaynak ve hedef IP adresi aynı kalmaktadır. Bu, paketin cevabının tekrar kaynağa gelebilmesi için gerekli olan bir mekanizmadır. Dolayısıyla dijital delil elde etme anlamında, hedefe gelen paketten kaynağa yönelik elde edilecek tek adres IP adresidir. Son paketten alınacak fiziksel adres, sadece ve sadece paketi en son gönderen düğümün adresi olacaktır.

4.4. Ağı İzlemede Kullanılabilecek Güvenlik Araçları

Bilgisayar sistemlerinin güvenliklerini sağlama amacıyla birçok çalışma yapılır. Bu çalışmalar genelde sisteme; güvenlik duvarları kurmak, saldırı tespit sistemleri kurmak, güvenli iletişim protokolleri sağlamak, zarar verici kodlara karşı yazılımlar kullanmak gibi çözümler olabilir. Fakat tüm bu yapılan çalışmalardan sonra bile sistemde saldırganların faydalanabileceği açıklar olabilir. Bu açıklar çeşitli güvenlik araçları kullanılarak tespit edilebilir ve gerekli önlemler alınabilir. Güvenlik araçları ayrıca sistemi izleme olanağı da sunarlar. Var olan güvenlik araçları genelde bilgisayar sistemlerine saldırı amacıyla geliştirilmiştir. Buradaki temel düşünce sistemin açıklarını saldırganlardan önce ortaya çıkarmak ve gerekli önlemleri almaktır [41].

Bu bölümde, ağ izlemede kullanılan önemli güvenlik araçları genel özellikleri ile tanıtılmaktadır.

Nmap: Nmap (Network mapper) ağ araştırmasında ve güvenlik denetlemelerinde kullanılan açık kaynak kodlu bir programdır. Geniş ölçekli ağları tarama amacıyla tasarlanmasının yanında tek bir konak üzerinde de verimli bir şekilde çalışabilir. IP paketleri göndererek ağ üzerinde aktif olan bilgisayarları gösterir. Ayrıca bu bilgisayarlar üzerindeki ağa sunulan uygulamaları tespit edebilir, bu bilgisayarların kullandığı işletim sistemleri ve güvenlik duvarlarını bulabilir. Nmap birçok işletim sistemi üzerinde çalışabilir ve GNU GPL lisansıyla dağıtılır. NMAP yazılımı Matrix Reloaded, Die Hard 4, The Bourne Ultimatum gibi birçok filmde hackerların bilgisayarlarında kullandıkları yazılımdır.

Nessus: Güçlü ve güncel bir uzaktan tarama aracıdır. Birçok UNIX türevi üzerinde ve Windows'ta çalışabilme özelliğine sahiptir. Nessus uyumlu ek yazılımları, ara yüzleri ile çok kullanışlı bir güvenlik aracıdır. 1200'ün üzerinde güvenlik açığını yakalayabilir ve bunlar hakkında çeşitli biçimlerde raporlar sunabilir (HTML, LaTeX, ASCII, vs.). Nessus'un önemli özelliklerinden biri olarak bilinen, kurallara bağlı olmadan tarama yapabilmesidir. Örneğin 1234 numaralı portta çalışan bir web sunucusunu tespit edebilir ve güvenlik taramasından geçirebilir. Bulduğu açıklar için kullanıcıya güvenlik çözümleri önerebilir.

Wireshark: UNIX ve Windows platformları için ücretsiz bir ağ protokolü analizcisidir. Canlı bir ağdan veya daha önceden diske kaydedilmiş bir ağ verisi üzerinde çalışarak ağ

incelemesi yapar. Kullanıcı, interaktif bir şekilde incelenen veri hakkında ayrıntılı bir bilgi alabilir. Bu bilgi tek bir paket için de söz konusudur. Güçlü özellikleri arasında zengin bir süzme diline sahip olması ve TCP oturumunu birleştirerek analiz imkanı sağlaması vardır. Wireshark programı *ethereal* olarak adlandırılan programın yenilenmiş versiyonudur. Wireshark 750 den fazla protokolü analiz etme özelliğine sahiptir. Belirli kriterlere göre filtreleme yapabilmesi de kullanımını kolaylaştırmaktadır. Diğer paket yakalama yazılımlarının dosyalarını da açabilmektedir.

Snort: IP ağları için gerçek zamanlı trafik analizi yapabilen ve paket kaydedebilen açık kaynak kodlu bir sızma belirleme sistemidir. Protokol analizi, içerik araştırması/eşlemesi dahil daha birçok inceleme yaparak saldırıları veya yoklamaları (tampon taşırma, gizli port taraması, CGI saldırıları, SMB yoklamaları, OS belirleme, vs.) tespit edebilir. Snort izin verilen/verilmeyen trafik tanımlanması için esnek bir kural yazma diline ve modüler bir tespit etme motoruna sahiptir. Ayrıca, çeşitli alarm mekanizmaları sayesinde herhangi bir saldırı tespitinden sonra kullanıcıyı uyarır.

Tcpdump: Ağ izleme ve veri inceleme yapmaya olanak veren en eski ve en çok sevilen ağ analiz (dinleme) programıdır. Ağ hareketlerini inceleme amacıyla kullanılır. Verilen deyimleri eşleyerek bir ağ ara yüzündeki paket bilgilerini gösterebilir. Nmap, Tcpdump'ın altyapısını oluşturan libpcap paket yakalama kütüphanesini kullanır. Günümüzde Tcpdump çok kullanılmamakla beraber ağ inceleme için genellikle wireshark kullanılmaktadır.

Dsniff: Ağ denetlemesi ve içeri sızma testleri yapmaya yarayan bir araçlar takımıdır. Dsniff; filesnarf, mailsnarf, msgsnarf, urlsnarf ve webspy gibi programlar içerir. Bu programlar pasif bir şekilde ağı dinleyerek ilgi çeken verinin (şifreler, epostalar, vs.) yakalanmasını sağlarlar. Arpspoof, dnsspoof, ve macof normalde bir saldırganın erişemeyeceği ağ trafiğine (2. katman) ulaşmasını sağlar. Sshmitm ve webmitm araçları da yönlendirilmiş HTTPS ve SSH bağlantıları için araya girme saldırılarında kullanılır.

GFI LANguard: Windows platformları için ücretli bir ağ güvenliği tarama aracıdır. LANguard ağı tarayarak her makine için çeşitli bilgiler sunar. Bu bilgiler makinelerin hangi servis paketlerini kullandığı, eksik güvenlik yamaları, herkese açık paylaşımları, açık portları, çalışan servisler/uygulamalar ve zayıf şifreler olabilir. Tarama sonuçları HTML formatında raporlanır ve sorgulanabilir. Web sayfasında deneme sürümü mevcuttur.

Ettercap: Ethernet ağlarında kullanılan terminal tabanlı bir koklama(sniff)/araya girme/kaydetme aracıdır. Aktif ve pasif olarak, şifreli olanlar dahil birçok protokolü izleyebilir ve araya girebilir. Kurulmuş bir bağlantıya veri enjeksiyonu yapma ve hızlı bir şekilde süzme yapma özellikleri vardır. Uyumlu ek yazılımları vardır. Anahtarlamalı ağda olduğunu anlayabilir ve işletim sistemi izlerini kullanarak ağ geometrisini çıkarabilir.

John The Ripper: John the Ripper çok güçlü bir şifre kırma aracıdır. Hızlı bir şekilde çalışma ve birden çok platform için şifre özü kırma özelliklerine sahiptir. UNIX'in neredeyse her versiyonu dahil DOS, Windows, BeOS ve OpenVMS'te çalışabilir.

Tripwire: Bütünlük kontrolü yapan araçların büyük babası olarak tanımlanan tripwire belirlenen dosya ve dizinlerin zaman içinde bütünlüklerinin bozulup bozulmadığını araştırır. Düzenli bir şekilde sistem dosyalarını kontrol ederek herhangi bir değişiklik halinde sistem yöneticisini uyarır. Linux için ücretsiz bir versiyonu olmakla birlikte diğer platformlar için ücretli bir yazılımdır.

Superscan: Windows tabanlı çalışan ve kapalı kaynak olan superscan yazılımı kullanışlı port tarama yazılımlarından olup IP aralığına dayalı port taraması yapar. Sadece TCP değil UDP taramalarını da yapabilmektedir.

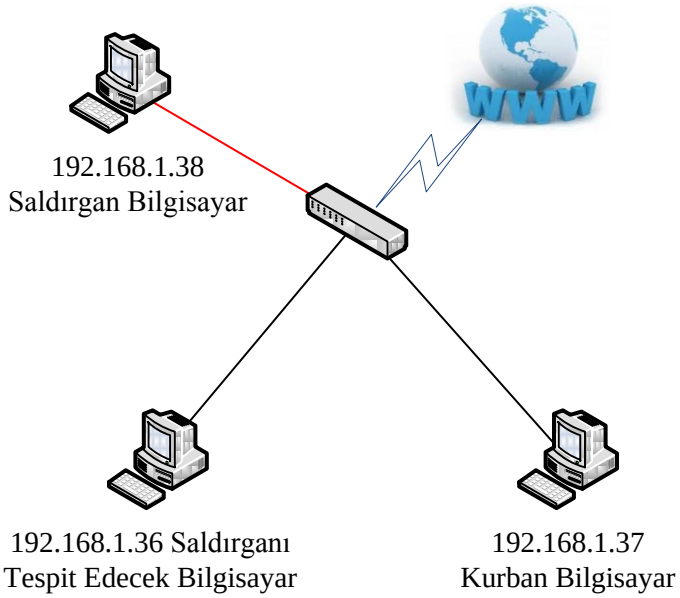
Cain & Abel: Ağ yöneticileri, güvenlik uzmanları, geliştiriciler için geliştirilmiş hedef ağda paket analizi yapma,ağdan şifre gibi bilgileri çekme, encrypt edilmiş şifreleri Brute Force ve Cryptanalysis metotları ile çözme gibi işlevlerinin yanında kötü niyetli kullanılmak ,istendiğinde tam bir silaha dönüşebilmektedir. ARP Poison alanında da en iyi sayılabilecek yazılımlardan biridir. Güvenli protokollerde bile ARP poison yaparak paket analizi yapabilir, şifrelenmiş veriyi okuyabilir. Ayrıca Cain & Abel Microsoft işletim sistemleri için bir password kırma aracı olarak da kullanılabilmektedir. Cain & Abel programının Linux sistemler için kullanılan formatı DSniff programıdır.

5. AĞ ÜZERİNDEKİ BİR SALDIRININ IP TABANLI DELİL TESPİTİ UYGULAMASI

5.1. Giriş

Bu bölümde, yerel bir ağ sisteminde gerekli önlemler alınmadığı takdirde bilgisayarlar üzerinde üçüncü kişiler tarafından sniffing (dinleme) işleminin ne kadar kolay gerçekleştirilebileceğini gösteren uygulamalar yapılmıştır. Ağda, istenilen kullanıcının web üzerinde girdiği siteler, kullanıcı adı, şifre bilgileri, girdiği sitelerdeki hesaplarının ele geçirilebileceği örnek bir uygulama ile gösterilmektedir.

Kapsamlı uygulamamızda, saldırı aşamasında kurban bilgisayarın dinlenmesi ve kurbana dair sniffing işlemi gerçekleştirilirken kullandığı kullanıcı hesaplarının nasıl ele geçirileceği gösterilmektedir. Kurban bilgisayarın dinlenmesinin sağlanması için Microsoft işletim sistemleri için bir password kırma aracı olarak da kullanılabilen *Cain & Able* aracı kullanılmıştır. Kurban bilgisayarın saldırgan tarafından dinlenmesi işlemi için, ağ üzerinde *ARP Poisining* saldırı yöntemi kullanılmıştır. Yapılan saldırının tespiti için *Wireshark* ağ dinleme aracı kullanılmıştır. Wireshark programı aracılığı ile ARP Poisining saldırısını gerçekleştiren saldırganın, ARP filtrelemesi yapılarak IP numarası üzerinden tespit edilmesi sağlanmıştır. Tespit edilen IP numarasının hangi kullanıcıya ait olduğu bilgisayar adının belirlenmesi ile anlaşılmıştır. Uygulama hem kablolu hem de kablosuz ağlar üzerinde gerçekleştirilmiştir. Şekil 19'da uygulamanın gerçekleştirildiği yerel ağ üzerinde bulunan bilgisayarlar ve görevleri gösterilmektedir.



Şekil 19. Yerel ağdaki saldırı şeması

Uygulamada kullanılan ARP Poisining saldırı yönteminin uygulanmasında kullanılan bilgisayarlar ve çalışmamıza yönelik özellikleri şu şekildedir:

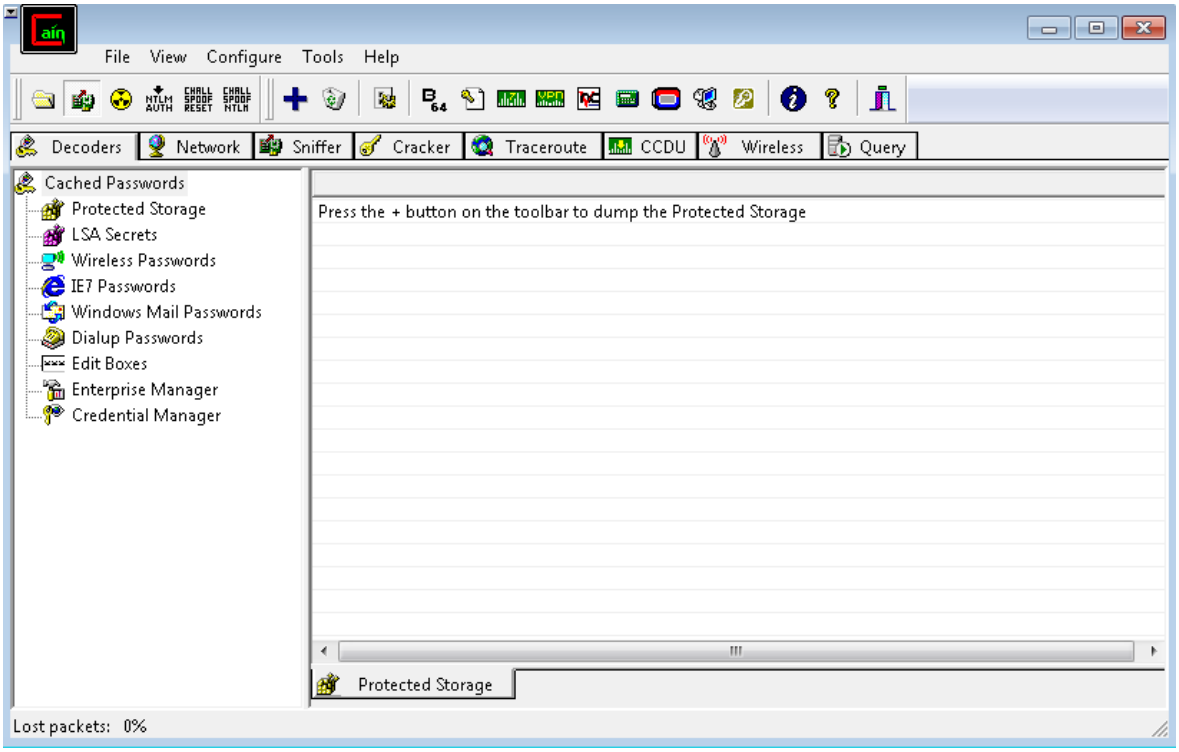
192.168.1.38 numaralı IP numarası sahibi olan bilgisayar Arp Poisining saldırısını gerçekleştirecek, üzerinde Cain & Able programı yüklü olan, saldırgana ait bilgisayardır.

192.168.1.37 numaralı IP numarası sahibi olan bilgisayar, Arp Poisining saldırısına maruz kalan, kurban bilgisayardır.

192.168.1.36 numaralı IP numarası sahibi olan bilgisayar, ağdaki saldırganı tespit edecek, üzerinde, protokol bazlı ağ dinleme yazılımı olan wireshark bulunan bilgisayardır.

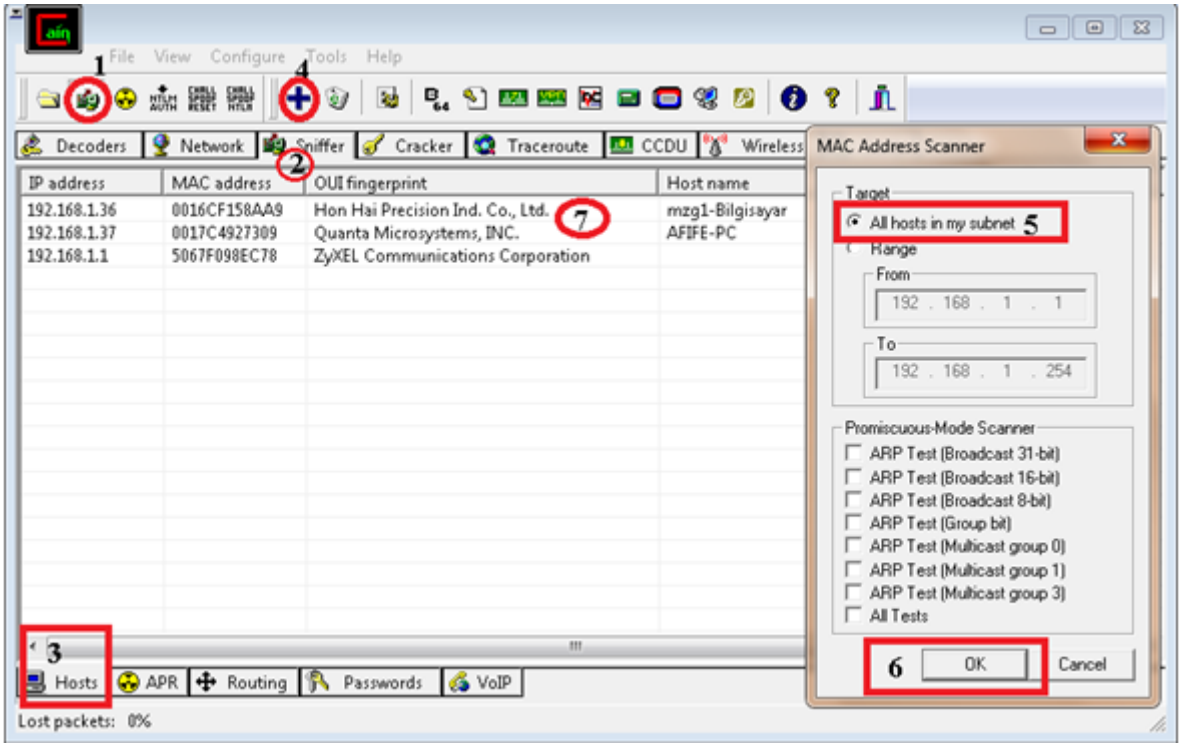
5.2.Yerel Ağ Üzerinde Saldırının Yapılması

İlk aşama olan kurban bilgisayarın Cain & Able programı ile ele geçirilmesi ve ağ üzerindeki faaliyetlerinin incelenmesi işlem sırasına göre ekran çıktıları ile beraber verilmiştir. Her bir işlem basamağı ile ilgili olaylar ve gerekli bilgiler ekran çıktılarıyla beraber belirtilmiştir. Yerel ağdaki sniffing için kullanılan Cain & Able programının arayüzü Şekil 20'de gösterilmektedir. Cain & Able programı kendi sitesinden ücretsiz olarak indirilebilen bir araçtır.



Şekil 20. Cain & Able programı arayüzü

Saldırı hazırlık aşamasında yapılan işlem adımları Şekil 21'de görüldüğü gibi şu şekildedir:



Şekil 21. Saldırı hazırlık aşaması-1

1. Adım: Kullanımda olan ethernet kartı aktif edilmektedir.

2. Adım: Sniff işleminin gerçekleştirilebilmesi için Sniffer sekmesine geçilmektedir.

3. Adım: Sniffer sekmesinden LAN'a bağlı olan cihazları görmek için Host sekmesi seçilmektedir.

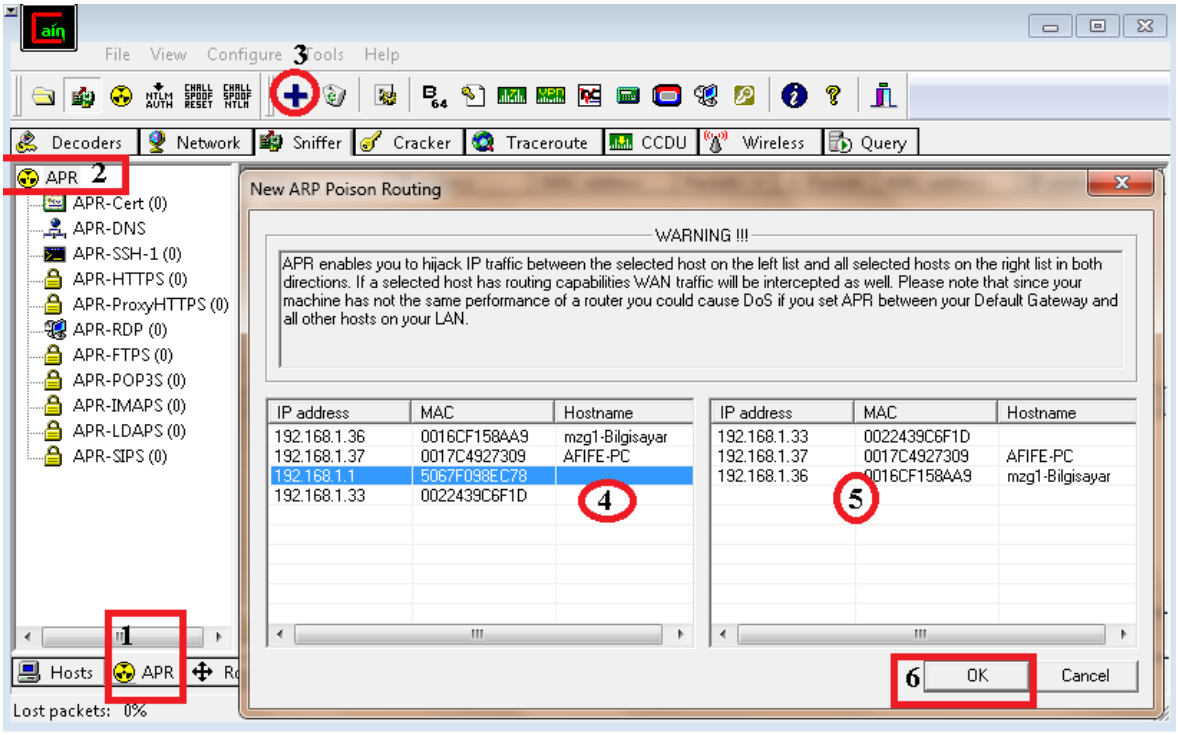
4. Adım: MAC'a dayalı adres taraması için Plus işareti tıklanmaktadır.

5. Adım: LAN'daki tüm cihazların tespit edilmesi sağlanmaktadır.

6. Adım: LAN'daki kablolu ve kablosuz tüm cihazların aranması sağlanmaktadır.

7. Adım: LAN'daki cihazlar IP numaraları ve adları ile liste olarak çıkarılmaktadır.

Şekil 22'de görülen saldırı hazırlık aşamasında ise saldırı için son hazırlık işlemleri gerçekleştirilmektedir. İşlem adımları şu şekildedir:



Şekil 22. Saldırı hazırlık aşaması-2

1. Adım: Gerekli işlemlerin yapılması için alt APR sekmesi seçili durumda bulunmaktadır.

2. *Adım:* Gerekli işlemlerin yapılması için üst APR sekmesi seçili durumda bulunmaktadır.

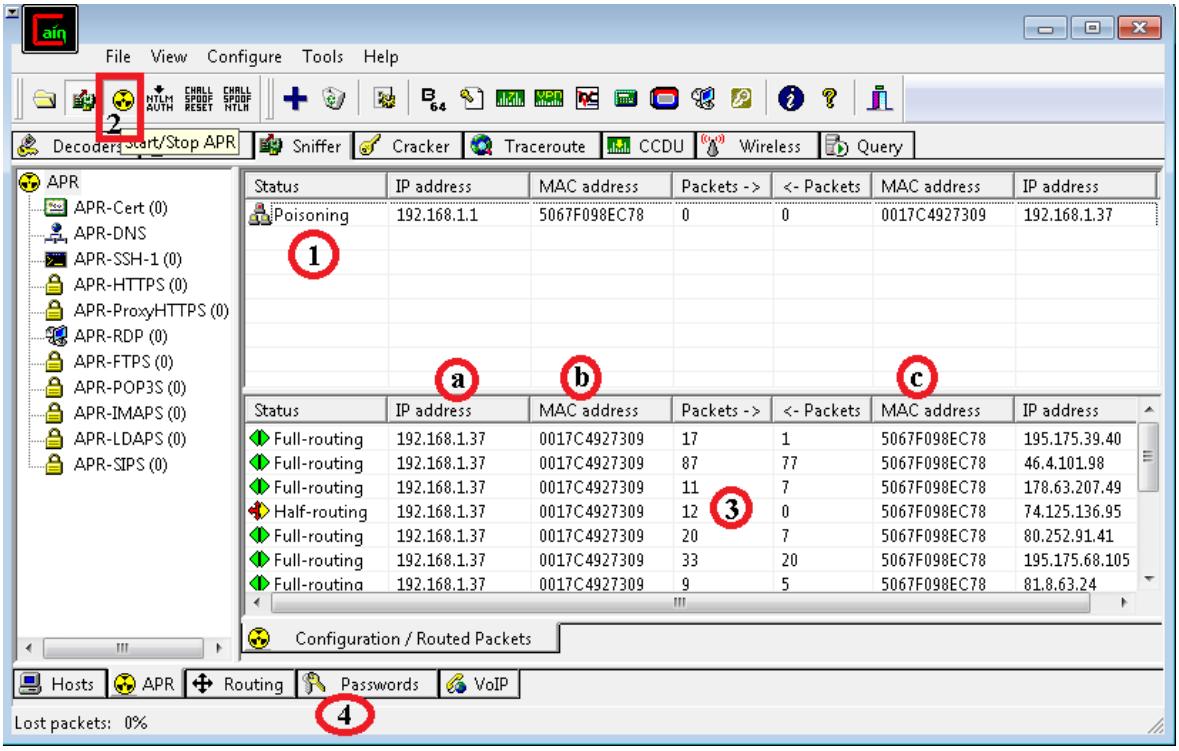
3. Adım: Plus simgesi aracılığı ile dinlenilmek istenilen cihazlar listesi çıkarılmaktadır,

4. Adım: Hangi cihaz üzerinden hangi cihazın ARP Poisining saldırısına maruz bırakılacağı belirtilmektedir.

5. Adım: Hangi cihaz üzerinden hangi cihazın ARP Poisining saldırısına maruz bırakılacağı belirtilmektedir.

6. Adım: Gerekli ayarlamalar onaylanmaktadır.

Şekil 23'de görülen saldırı aşamasında ise sırası ile şu işlem adımları uygulanmaktadır:



Şekil 23. Saldırı aşaması

1. Adım: ARP Poisining saldırısının başlatılacağı sanal bağlantı aktif edilmektedir.

2. Adım: ARP Poisining saldırısı başlatılmaktadır.

3. Adım: APR Poisining saldırısının çıktıları görülmektedir.

3.a bölgesindeki alan kurban bilgisayarın IP adresini göstermektedir.

3.b bölgesindeki alan kurban bilgisayarın MAC adresini göstermektedir.

3.c bölgesindeki alan ise yerel ağda bulunan gateway cihazına ait MAC adresini göstermektedir.

4. Adım: Kurban bilgisayarın çalışmaları incelenmek üzere Passwords sekmesine geçilmektedir.

Şekil 24'de Passwords alanına geçildikten sonra görüldüğü gibi bazı portallar ve siteler üzerinde dört farklı sonuç alınmaktadır. Bu sonuçlar şu şekilde belirtilebilir:

1. Kullanıcı adı ve şifrenin tespit edilemediği durumlar.

2. Kullanıcı adı ve şifrenin tespit edildiği durumlar.

3. Kullanıcı adının tespit edilip, şifrenin tespit edilemediği durumlar.

4. Kullanıcı adının tespit edilemeyip, şifrenin tespit edildiği durumlar.

Şekil-24'de;

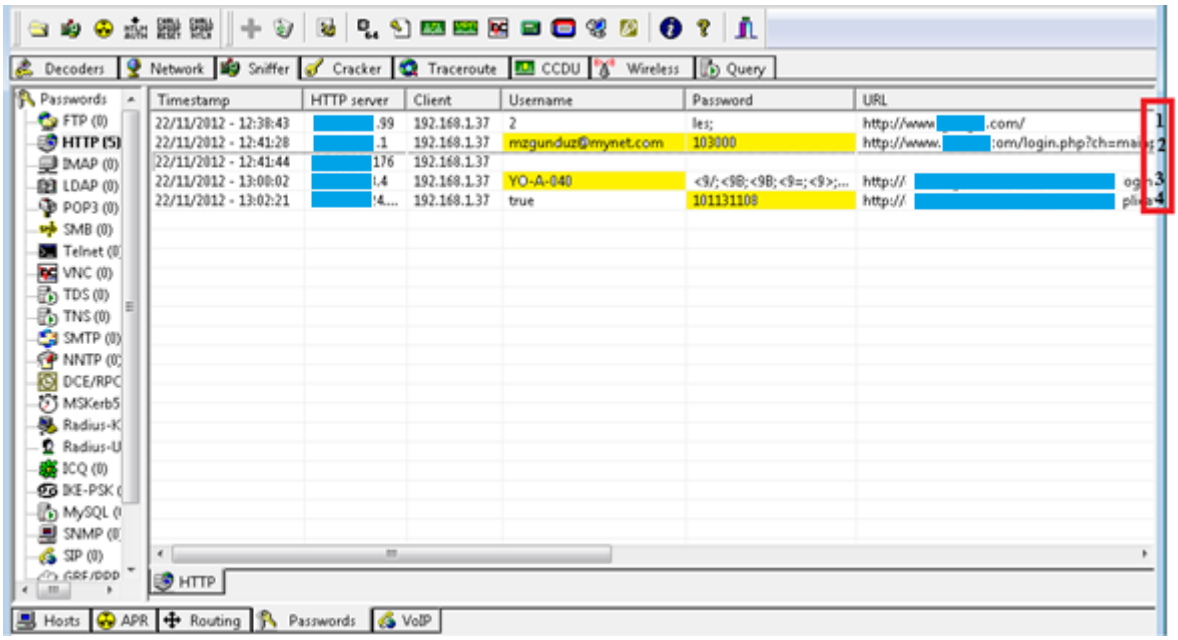
1. sonuçta hesaba dair bilgiler alınamamıştır.

2. sonuçta portaldan kullanıcı adı ve şifre bilgileri elde edilmiştir.

3. sonuçta password kriptolu olarak iletildiğinden ağ üzerinden elde edilememiştir.

4. sonuçta kullanıcı adı elde edilememiş, password elde edilmiştir. Username alanı boolean bir değer döndürmektedir. Bu değerin SQL Injection yöntemleri ile atlatılarak sisteme girilebileceği düşünülmektedir.

Şekil 24 üzerindeki sonuçlar gerçek uygulama sonuçları olduğu için bazı veriler kurum ve kuruluşların itibarını zedelememek adına gösterilmemiştir.



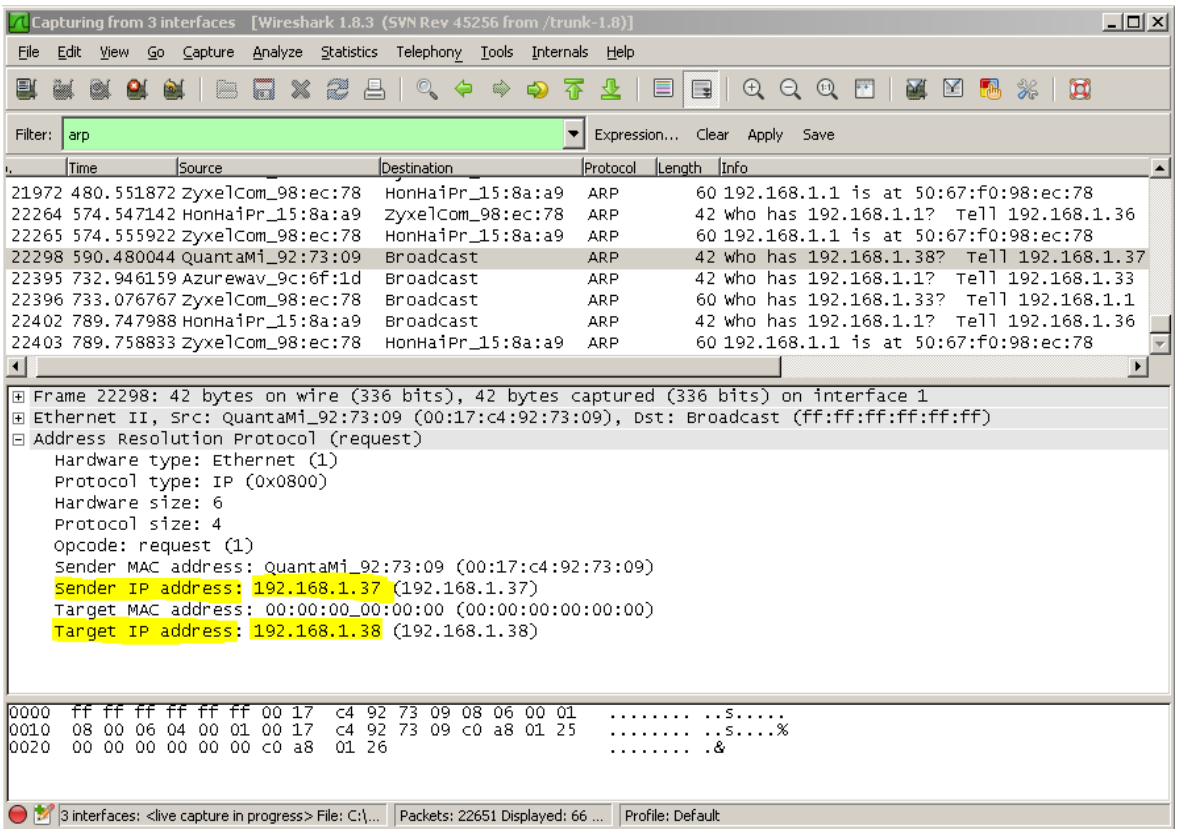
Şekil 24. Saldırı aşamasının sonuçları

5.3. Ağ Üzerindeki Saldırganın IP Adresinin Tespit Edilmesi

Saldırı hazırlık ve saldırı aşamalarından sonra saldırganın ele geçirdiği bilgiler, saldırgan tarafından kullanılabilecektir. En azından saldırgan istediği tüm bilgilere ulaşamasa bile yerel ağda elde ettiği bilgilerden yola çıkarak istediği kullanıcı üzerinde çeşitli sosyal mühendislik aldatmacaları ile istediği bilgilerin tamamına yakınını elde edebilecektir. Bununla ilgili olarak ağ ortamından şifresini tespit ettiği kullanıcının kullanıcı adını kurbanın bilgisayarı üzerinde "kullanıcı adımı anımsa" seçeneğini aktif hale getirerek kurbanın kullanıcı adını da ilerleyen süreçte ele geçirmesi örnek olarak

gösterilebilir. 4. bölümde anlatılan saldırı yöntemlerinin beraber kullanılması ile saldırganın daha fazla ve şüphe uyandırmadan, bilgileri elde edebileceği unutulmamalıdır.

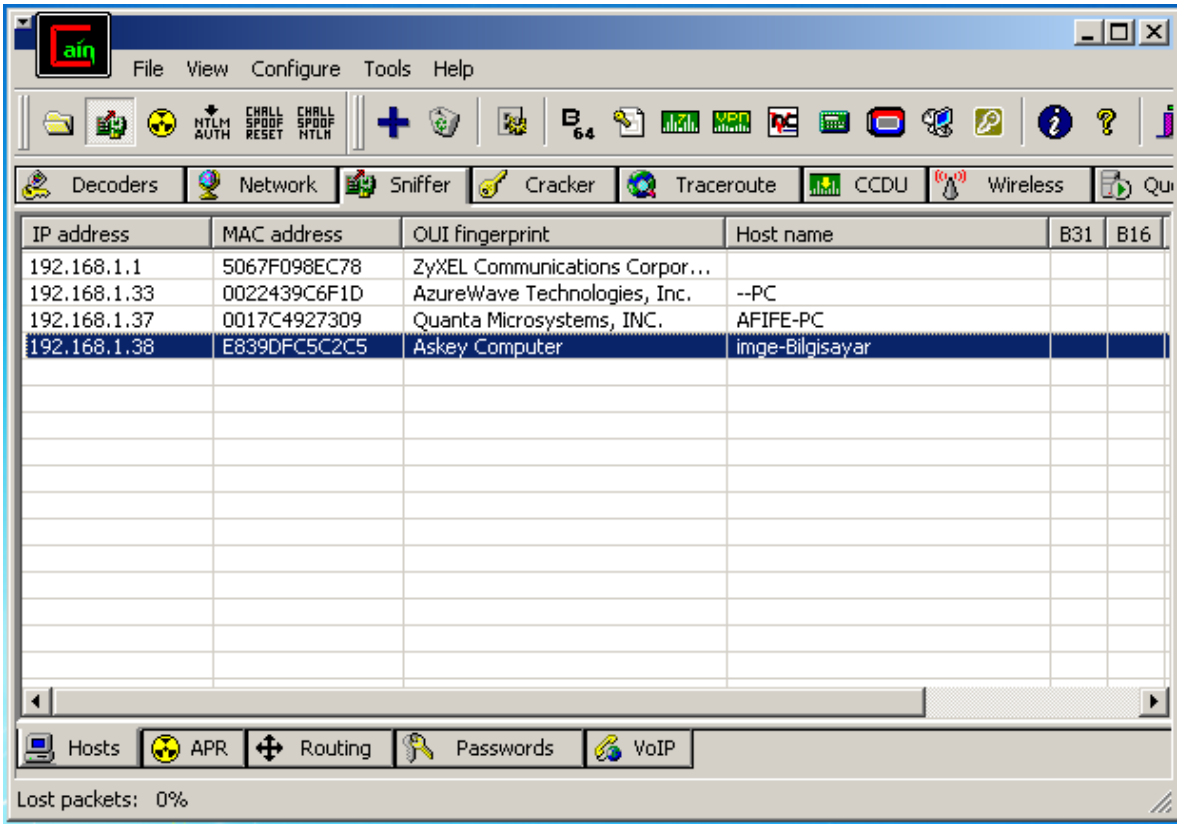
Bu tez çalışmasında, *ortadaki adam* (Man in the Middle) saldırılarından olan ARP Poisining saldırısının tespiti wireshark programı ile ARP filtresi üzerinden veri paketlerinin incelenmesi ile gerçekleştirilmiştir. Buna göre Şekil 25'de saldırı anında elde edilen wireshark çıktısı incelendiğinde; geçit yolunun (gateway) tüm bağlantı noktaları ile temas halinde olduğu görülmektedir. Ancak, saldırgan IP sinin kurban IP si ile de temas halinde olduğu tespit edilmiştir. Bu ilişkinin detayları incelendiğinde ise Şekil 24'ün alt tarafında görüldüğü gibi kurbanın verileri saldırganın IP adresine yönlendirilmiştir.



Şekil 25. Wireshark ile saldırganın IP adresinin tespit edilmesi

Şekil 26'da saldırganın yerel ağda tespit edilen IP numarasının ağdaki başka bir bilgisayardan, Cain & Able programı kullanılarak bilgisayar adı ve MAC adresi tespit edilmiştir. Saldırganımızın bilgisayarının adı "imge-Bilgisayar" olduğu görülmektedir.

Aynı şekilde kurban bilgisayarın IP adresi incelendiğinde bilgisayar adının AFIFE-PC olduğu görülmektedir.



Şekil 26. Saldırganın bilgisayar adının tespit edilmesi

5.4. Uygulama Sonuçları

Uygulama basamaklarındaki sonuçlar çizim modellemeleri ile gösterilmek yerine gerçek çıktıları ile gösterilmiştir. Buradaki amaç, hiçbir kurum ya da kuruluşun itibarını zedelemek değil, eğitim amaçlı ağ saldırılarının varlığını göstermektir. Ayrıca bu uygulamalar ile paylaşıldıkça artan bir nesne olarak da tanımlanan bilginin, korunumu ve güvenliği için alınacak tedbirlerin belirlenmesinde katkıda bulunmak amaçlanmıştır. Unutulmamalıdır ki bir saldırının nereden ve ne şekilde geleceği bilmek en iyi savunma sanatıdır. Uygulama sonucunda elde edilen bulgulara göre aşağıda belirtilen önemli çıkarımlar elde edilmiştir:

- Farklı LAN ağlarında yapılan uygulamalarda, kablosuz yayın yapan erişim noktalarının (access point) güvenliklerinin genellikle doğru yapılandırılmadığı tespit edilmiştir. Eğer gerekli güvenlik önlemleri alınmadı ise; basit bazı işlemler ile bu erişim noktalarının ağlarına dahil olunarak istenilen kullanıcılar izlenebilmekte, hatta yönetim paneli ele geçirilebilmektedir.

- Https protokolünü kullanan sitelerden veri çalınması http ve diğer protokolleri kullanan sitelere göre daha zordur.
- Wireshark gibi ağ paketleri üzerinde her türlü analizi yapabilen programlar kötü niyetli kullanıcılar elinde bir silaha dönüşebilir. Bu duruma; ağda MSN üzerinden görüşme yapan kullanıcıların konuşma metinlerinin ele geçirilmesi örnek olarak gösterilebilir.
- Kriptolamalı şifrelerin kırılması neredeyse imkânsızdır. Teorik olarak kırılması mümkün olsa bile, uygulamada kriptolu şifrenin elde edilmesi yıllar süreceğinden dolayı mümkün değildir.
- Cain & Able ile yapılan uygulamalarda güvenilirliğe önem veren sitelerden ilk denemede bilgiler çalınabildiği halde sonraki denemelerde başarılı olunamamıştır. Kurum ve kişilerin itibarını zedelememek açısından ekran çıktıları verilmemiştir.
- Saldırının varlığını tespit eden bazı sitelerin Şekil 27'de görüldüğü gibi sunucularına erişimi engelledikleri tespit edilmiştir.

Şekil 27. Güvenlik sertifikası

- Bazı sitelerin ise Şekil 28'de görüldüğü gibi kullanıcı adı ve şifre istenecek formlarında hemen https protokolüne geçtikleri görülmektedir

Şekil 28. Https protokolü

6.SONUÇ VE ÖNERİLER

Bilişim teknolojilerinin yaygınlaşması ile günlük hayatımızdaki iş ve işlemler elektronik ortamlarda artık daha hızlı yapılmaktadır. Bu durum bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir. Bu nedenle kullanıcılar yaptıkları iş ve işlemlerde bilginin öneminin farkında olup, bu konuda güvenlik unsurlarını, politikalarını ve güvenlik süreçlerini uygulamak zorundadırlar. Böylece belli oranda, karşılaşılabilecek sorunlar ve tehlikeler azaltılabilecek, işgücü, zaman ve parasal kayıplar önlenebilecektir. Aynı zamanda, internet üzerinden gelebilecek zararlı yazılımlara veya program parçacıklarına karşı kişisel ve kurumsal bilgi güvenliğinin sağlanmasına katkılar sağlanacaktır.

Bilgi güvenliği konusunda güvenlik açıklarının önlenebilmesi için kişilerin ve kurumların basitten en karmaşık güvenlik yöntemlerine kadar bir dizi önlemler alması gerekir. Ancak, tüm önlemler alınmış olsa da, sürekli geliştirilen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini %100 güvende hissetmemelidir. Saldırılar; kötü niyetli kişiler, arkadaşlarımız veya tanıdığımız kişilerden gelebilir. Alınması gereken en temel önlemler; muhtemel risklere ve bu çalışmada açıklanan saldırı tekniklerine karşı uyanık olmak, yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirgemek olarak belirtilebilir. Güvenliğin statik değil dinamik bir sürece sahip olduğu, koruma ve sağlamlaştırma ile başladığını, bir hazırlık işlemine ihtiyaç duyulduğu, saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gerektiği ve sistemde her zaman iyileştirme yapılması gerektiği unutulmamalıdır.

Yapılan uygulama ve araştırmalar sonucunda, ağ sistemlerinde var olan sunucu, switch, hub v.b. ağ cihazlarının veya bilgisayarların güvenliğinin artırılması için aşağıda belirtilen önemli temel unsurlar göz önüne alınmalıdır. Bilgi güvenliğinin sağlanması adına sistem veya ağ yöneticilerinin alabileceği önlemler şu şekilde sıralanabilir:

- Ağa veya sisteme gelebilecek fiziksel saldırılara karşı sunucuların bulunduğu sistem odasının fiziki giriş-çıkış kontrolü sağlanmalıdır.
- Ağ sisteminin güvenlik duvarı üzerindeki yönetim organizasyonu politikaları dikkatlice belirlenmelidir.
- Sunucu hizmetlerinin kullandığı portlar dışındaki diğer kullanılmayan portlar kapatılmalıdır.
- Ağ trafiğini kontrol etmek ve düzeltmek için VLAN yapıları oluşturulmalıdır.

- Sistem odasındaki sunucu ve ağ cihazlarının, şifre yönetimindeki güvenlik politikaları belirlenmelidir.
- Ağ sisteminde sniffing işlemlerinin tespiti için wireshark gibi ağ dinleme araçları kullanılmalıdır.
- Ağ sisteminde yazılımsal veya donanımsal olarak firewall kullanılmalıdır.
- Log analiz ve yönetim sistemi kullanılmalıdır.
- Ağda olası tehlikeleri saptamak için IDS/IPS otomatik açık tarama araçları kullanılmalıdır.
- Ağ ve bilgi güvenliği ile ilgili güncel konular ve bilgiler, özellikle ağ yöneticileri tarafından yakından takip edilmelidir.
- Hub kullanılan sistemlerde güvenliğin sağlanması adına switch, akıllı switch, router gibi cihazlar kullanılmalıdır.
- 65536 adet olan sanal portların kullanım durumları dışarıdan gelecek saldırıların engellenmesi için devamlı kontrol altında tutulmalıdır.
- Sistem için güvenlik politikaları oluşturarak bunların uygulanmasının ve takibinin yapılması sağlanmalıdır.
- Hizmet veren sunucuların işletim sistemlerinde güvenlik zafiyeti oluşturan servisler kapatılmalıdır.
- Bazı anahtarlar ve yönlendiriciler üzerindeki yönetim yetkilendirmelerine dikkat edilmelidir.
- Router ve firewall gibi ana cihazlar üzerinde erişim kısıtlamaları (access-list) oluşturarak kısıtlamalar getirilmelidir.
- Sunucu, router, firewall, switch vb. tüm ağ cihazları üzerinde güvenlik önlemleri en başından uzmanlarca yapılıp, herhangi bir güvenlik açığına meydan verilmemelidir.
- 5651 sayılı kanun gereğince ağ yöneticilerinin, ağ kullanıcılarının takibini yapmak zorunda olduğu unutulmamalıdır.
- VLAN ağında kullanıcıların yerinin tespit edilmesi için IP bazlı erişim kontrol listesi tekniği (IP adresinin erişim yapabileceği portun kenar switch üzerinde sabitlenmesi) kullanılmalı veya her MAC adresinin belli zaman aralığında hangi IP adresini kullandığının kayıt altında tutulmasının en kesin yöntemi olarak yönlendiricinin ARP tablosunun loglanması sağlanmalıdır.

- Yönlendiricilerin; erişim hakları, erişim protokolleri güvenliği, şifrelerin güvenliğinin sağlanması, gereksiz servislerin kapatılması vb. konfigürasyon (yapılandırma) ayarlamaları yapılmalıdır.

Ağ sisteminde yer alan son kullanıcılar şu hususlara dikkat etmelidir:

- Web ortamında şahsi bilgiler paylaşılmamalı ve şifre türü veriler kullanılmamalıdır.
- Sohbet ortamlarında saldırıların daha fazla olabileceği unutulmamalıdır.
- Kredi kartı bilgileri güvenilir siteler dışında kullanılmamalıdır.
- Web ortamında güvenliğin hiçbir zaman tam olarak sağlanamayacağı unutulmamalıdır.
- Güvenilir ve tanınır siteler haricindeki sitelerden dosyalar indirilmemelidir.
- E-ticaret yapılan sitelerde SSL, SET, SSH gibi güvenlik protokollerinin kullanılmış olmasına dikkat edilmelidir.
- Bilinmedik ve güvenilirliği şüphe uyandıran sitelere kişisel bilgiler verilmemelidir.
- Sosyal mühendislik yöntemleri incelendiğinden saldırıların insanın yakınındaki kişilerden de gelebileceği unutulmamalıdır.
- Kullanıcı internet ortamında kendini %100 güvende hissetmemelidir.
- İnternet ortamı, gerçek dünyanın, sanal âleme bir yansımasıdır. Bu yüzden sosyal paylaşım sitelerinde paylaşılacak bilgiler dikkatli seçilmelidir.
- Yapılan saldırı türlerinde çoğunlukla insanların bilgisizliğinden, tecrübesizliğinden ve zaaflarından yararlanıldığı unutulmamalıdır.
- Kişisel önemli parolalar düzenli bir şekilde değiştirilmelidir.
- İşletim sistemlerine ait güncellemeler düzenli olarak yapılmalıdır.
- Lisanslı yazılımlar kullanılmalıdır.
- Yasal ve güvenli olmayan sitelerden download yapılmamalıdır.
- İnternet kafe gibi halka açık ve güvenilirliği şüpheli olan ortamlarda online bankacılık ve e-ticaret işlemleri yapılmamalıdır. Yapılacak ise güvenlik esaslarına dikkat edilmelidir.
- Online alışverişlerde sanal kredi kartları kullanılmalı ve alışveriş süresince limitleri tanımlanmalıdır.
- Şüpheli görülen e-posta eklentileri okunmadan ve açılmadan silinmelidir.

Dünyada ve ülkemizde bilgi güvenliğine yönelik en önemli tehditlerden olan kötücül ve casus yazılımların, yaygın olarak kullanımda olduğu, fakat kullanıcıların bu tür

saldırı ve tehditlerden çoğunlukla haberdar olmadığı anlaşılmıştır. Herhangi bir zararla karşılaşılmaması için, konuya gereken önemin verilmesi, bilgi birikiminin arttırılması, bilgi güvenliğine yönelik hassasiyet gösterilmesi ve gereken önlemlerin alınması ile farkındalık oluşturulması gerekmektedir.

Yapılan literatür çalışmalarında, konuyla ilgili birçok çalışma mevcut olsa da "bilişim suçları ve güvenlik" konusunun ülkemiz için akademik ortamlarda yeterince tartışılmadığı ve konuya gereken ilginin yeterli düzeyde olmadığı görülmektedir. Konunun ülkemiz için bakir bir konu olması, magazin ve ticari bilgilerin dışında konunun akademik gündemde daha fazla yer bulması açısından, bu tez çalışmasının önemli olduğu düşünülmektedir. Ayrıca, bu tez çalışmasının konu ile alakalı olarak temel kavramsal bilgiler sunduğu ve uygulamaya yönelik yapılabilecek çalışmalar için fikirler oluşturabileceği düşünülmektedir.

Bu tez çalışmasında elde edilen bulgular ışığında bilginin korunmasına yönelik, akademik ve eğitim anlamında devlet politikası olarak aşağıdaki değerlendirmeler yapılarak öneri olarak sunulmaktadır:

- Bilgi ve bilgisayar güvenliğine yönelik ülkemizde, devlet, üniversite, kurum ve kuruluşların konuya gereken önemi vermesi için; bilgi ve bilişim güvenliğine yönelik yapılan çalışmaların özellikle akademik anlamda artırılması gerekmektedir.
- Gelişen teknolojinin hızla yükselen trendi olan bilgi güvenliği konusu son yüzyıla damgasını vurmaktadır. İnternet gibi devasa bir ağ sisteminde dünyanın adeta küçük bir köy haline gelmesi ve her türlü bilginin sürekli bir hareketlilik halinde olması, sanal bilgilerin bu ağ ortamında korunumunun gerçekleştirilmesi konusunda son kullanıcıların gerekli eğitimler ile eğitilmesini gerektirmektedir.
- Ülkemiz için hala tam olarak oluşturulamayan bilişim hukuku kanunlarının tam anlamı ile oluşturulabilmesi ve bilgininin korunmasının hukuki boyutta emniyet altına alınabilmesi için; konu ile ilgili hem hukuki boyutta hem de bilgisayar ağları konularında yetiştirilmiş uzman kişilerin, katkılarıyla bu süreç hızlandırılmalıdır. Konunun hem hukuki hem de teknik boyutu konusunda uzman olan bir kişinin bu kanunların düzenlenmesi noktasındaki katkılarının daha fazla olacağı düşünülmektedir.
- Üniversitelerin özellikle mühendislik bölümlerinde seçmeli veya zorunlu olarak bilgi ve bilgisayar güvenliği içerikli derslerin müfredata yerleştirilmesi gerekmektedir.
- Üniversitelerin mühendislik veya teknoloji fakültelerinde lisans düzeyinde, şu an için tek örneği Fırat Üniversitesi Teknoloji Fakültesinde bulunan "Adli Bilişim

Mühendisliği" bölümünün farklı üniversitelerimizde de açılmasının yeni nesil bilgisayar mühendislerinin ve bilgi savunma mühendislerinin yetiştirilmesinde çok büyük bir öneme sahip olacağı düşünülmektedir.

- Üniversitelerin hukuk fakültelerinde bilişim hukuku üzerine dersler verilerek hukukçuların bu alanda daha donanımlı bir alt yapıya sahip olması sağlanmalıdır.
- Bilgi ve bilgisayar güvenliği üzerine lisansüstü öğrencilerinin yetiştirilmesinin öneminin gün geçtikçe artacağı ve bu konuda uzman akademisyen ihtiyacının karşılanması için önemli adımlar atılmasının gerekli olduğu düşünülmektedir.

Tez çalışması sırasında akademik anlamda yapılan ulusal kaynak taramalarında soyut ifadelerin ve kavramların tanımlanması, bilişim güvenliği ile ilgili teorik birçok bilginin verilmiş olmasına rağmen uygulama alanlarına yönelik uygulama örneklerinin somut olarak nadir kullanıldığı görülmüştür. Ancak, bu tez çalışması ise hem teorik hem de uygulama ile desteklenmiştir. Ayrıca, bu tez çalışması güvenlik alanında daha farklı uygulamaların yapılabilmesi adına birçok fikir ve öneriler de sunmaktadır.

KAYNAKLAR

[1] **Örgün, F.,** 2001. Küresel Terör, Okumuş Adam Yayınları, İstanbul.

[2] http://tr.wikipedia.org/wiki/Suç, 16 Ekim 2012.

[3] **Çiçek, İ., Okatan, A.,** 2008. Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları, Ağ ve Bilgi Güvenliği Sempozyumu, Kuzey Kıbrıs Türk Cumhuriyeti / Girne.

[4] **Perry, R.L.,** 1986. Computer Crime, New York.

[5] **Özcan, M.,** 2001. Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu.

[6] http://dosyalar.hurriyet.com.tr/hacker/mozcan.asp, 10 Ekim 2012.

[7] http://www.habername.com/haber/baykal-metacafe-kaset-emniyet-39101.htm, 01 Ekim 2012.

[8] **Elbahadır, H.,** 2011. Hacking Interface, Kodlab Yayıncılık, İstanbul.

[9] **Güven, H.,** 2006. İnternette Güvenlik ve Hacker Cracker Meselesi, Seçkin Yayıncılık, Ankara.

[10] **Canbek, G.,** 2005. Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

[11] http://www.kemalsener.av.tr/bilisim-suclari/bilisim-suclari-ve-turk-ceza-kanunu.html, 15 Aralık 2012.

[12] **Shinder, D. L.,** 2002. Scene of Cybercrime – Computer Forensics Handbook, Syngress Publishing, USA.

[13] **Chisum, J. W.,** 1999. Crime Reconstruction and Evidence Dynamics, Presented at the Academy of Behavioral Profiling Annual Meeting, Monterey, CA.

[14] **Casey E.,** 2000. Digital Evidence and Computer Crime, Academic Press, London.

[15] **Uzunay, Y.,** 2005. Dijital Delil Araştırma Süreci, 2. Polis Bilişim Sempozyumu, Ankara.

[16] **Uzunay, Y., Koçak M.,** 2005. Bilişim Suçları Kapsamında Dijital Deliller, Akademik Bilişim Konferansı, Gaziantep.

[17] **Gelişken, U.,** 2009. 10 Adımda Bilgisayar Güvenliği, Kodlab Yayıncılık, İstanbul.

[18] http://www.chip.com.tr/galeri/Tum-zamanlarin-en-unlu-10-hacker-i_716_9.html, 27 Eylül 2012.

[19] http://teknoloji.samanyoluhaber.com/internet/735145/Zorbalik-sanal-alemde/, 23 Kasım 2012.

[20] **Ersoy, H.,** 2000. Ulusal Çıkar Aracı Olarak Uluslararası Politikada Terörizm, I. Milletlerarası Doğu ve Güneydoğu Anadolu'da Güvenlik ve Huzur Sempozyumu, Elazığ.

[21] Cybercrimes: Infrastructure Threats from Cyberterrorist, Cyberspace Lawyer, 4 No 2. Cyberspae Law 23.

[22] http://ekonomi.haberturk.com/teknoloji/haber/695683-bu-turk-dunyayi-solladi, 28 Ekim 2012.

[23] **Uzunay, Y.,** 2005. Bilgisayar Ağlarına Yönelik Adli Bilişim, Adli Bilişim Çalıştayı, İzmir.

[24] http://www.edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic/, 19 Kasım 2012.

[25] **Kuusisto, R., Helokunnas, T., Ahvenainen, S.,** 2003. Intellectual Capital and Time in information Superiority, Proceedings of the 2nd European Conference on Information Warfare and Security, UK.

[26] **Canbek, G., Sağıroğlu, Ş.,** 2007. Kötücül ve Casus Yazılımlar : Kapsamlı Bir Araştırma, Gazi Müh. Mim. Fak. Dergisi, Cilt 22, No: 1, Ankara.

[27] **Housman, E. M.,** 2000. The Nature of Information, Bulletin of the American Society for Information Science.

[28] **Schuler, A. J.,** 2003. How to Build Wisdom and Prosper in an Information Age, "What's Up, Doc?" e-Newsletter.

[29] **Tiwana, A.,** 2002. Knowledge Management Toolkit, The: Orchestrating IT, Strategy, and Knowledge Platforms, Prentice Hall PTR, 2nd Edition, Prentice Hall PTR.

[30] http://www.bilgisayardershanesi.com, 06 Aralık 2012.

[31] http://www.isokalitebelgesi.com/iso_belgeleri_egitim_danismanlik/ ISO_27001_ISO_27000_22057/bilgi_guvenligi_belgesi_1.php, 15 Aralık 2012.

[32] **Karaarslan E., Teke A., Şengonca H.,** 2003. Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması, İletişim Günleri, İzmir.

[33] **Canbek, G., Sağıroğlu, Ş.,** 2007. Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt 9, sayı:3, Ankara.

[34] “Data, Information, Knowledge and Knowledge Management”, 2005. The OR (Operational Research) Society, http://www.theorsociety.com/ about/ topic/ projects/notorious/2_2_Data_Info.htm, 27 Ekim 2012.

[35] **Canbek, G., Sağıroğlu, Ş.,** 2008. Casus Yazılımlar:Bulaşma Yöntemleri ve Önlemler, Gazi Müh. Mim. Fak. Dergisi, Cilt 23, No: 1, Ankara.

[36] **Canbek, G. ve Sağıroğlu, Ş.,** 2006. Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri, Grafiker Yayıncılık, Ankara.

[37] **Daş, R., Kara, Ş., Gündüz, M.Z.,** 2012. Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri, 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), ODTÜ, Ankara.

[38] **Mathew, A., Hajj, A., Ruqeishi, K.,** 2010. Cyber Crimes: Threads and Protection, International Conference on Networking and Information Technology.

[39] http://www.olympos.net/belgeler/servis-kullanimi-engelleme/temel-dos-ataklari-507458.html, 15 Kasım 2012.

[40] http://www.olympos.net/belgeler/guvenlik/kisisel-bilgisayar-guvenligi-4627833.html, 14 Ekim 2012.

[41] **Anuk, E.,** Güvenlik Araçları, İTÜ Bilişim Enstitüsü, İstanbul.

ÖZGEÇMİŞ

M. Zekeriya GÜNDÜZ, 1983 yılında Bakırköy'de doğdu. 2006 yılında Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar ve Elektronik Sistemleri Öğretmenliği bölümünü bitirdi. 2006-2010 yılları arasında Milli Eğitim Bakanlığına bağlı farklı Endüstri Meslek Liselerinde Bilişim Teknolojileri öğretmeni olarak görev yaptı. Halen Bingöl Üniversitesi Teknik Bilimler Meslek Yüksek Okulu, Bilgisayar Programcılığı bölümünde öğretim görevlisi olarak çalışmaktadır.