KTO KARATAY
ÜNİVERSİTESİ

T.C.

KTO Karatay Üniversitesi

Fen Bilimleri Enstitüsü

Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Programı

AĞ GÜVENLİĞİ SKORLAMA SİSTEMİ

Mustafa Sami KAÇAR

KONYA

Şubat, 2017

AĞ GÜVENLİĞİ SKORLAMA SİSTEMİ

Mustafa Sami KAÇAR

KTO Karatay Üniversitesi Fen Bilimleri Enstitüsü

Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Programı

Yüksek Lisans Tezi

KONYA

Şubat, 2017

Fen Bilimleri Enstitüsü Onayı

Prof. Dr. Hüseyin Bekir YILDIZ

Enstitü Müdürü

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

Yrd. Doç. Dr. Hüseyin Oktay ALTUN

Anabilim Dalı Başkanı

Mustafa Sami KAÇAR tarafından hazırlanan AĞ GÜVENLİĞİ SKORLAMA SİSTEMİ başlıklı bu çalışma 17.02.2017 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jüri tarafından tezli yüksek lisans tezi olarak kabul edilmiştir.

Yrd. Doç. Dr. Kasım ÖZTOPRAK

Tez Danışmanı

Tez Jüri Üyeleri

Başkan: Prof. Dr. Mehmet Reşit TOLUN.....

Üye: Yrd. Doç. Dr. H. Oktay ALTUN.....

Üye: Yrd. Doç. Dr. Kasım ÖZTOPRAK.....

TEZ BİLDİRİMİ

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

Mustafa Sami KAÇAR

ÖZET

AĞ GÜVENLİĞİ SKORLAMA SİSTEMİ

KAÇAR, Mustafa Sami

Elektrik ve Bilgisayar Mühendisliği Ana Bilim Dalı

Tez Danışmanı: Yrd. Doç. Dr. Kasım ÖZTOPRAK

Şubat, 2017

Ağ güvenliği, günümüz dünyasının en önemli meselelerinden biri haline gelmiştir. İnternetin yaygınlaşması ile beraber kurumlar ve şirketler, ağlar üzerinden önemli mahrem bilgiler paylaşmaktadırlar. Erişim izni olmayan üçüncü kişilerin eline geçmesi halinde ciddi zararlara yol açabilecek olan bu bilgilerin korunması oldukça kritiktir. Dahası, artan siber saldırılarla birlikte kurumsal veya özel ağlar ciddi tehdit altındadır. Özellikle kurumsal ağlar ulusal güvenlik açısından kritik önemde olduğu için, ağların güvenlik durumunun farkındalığı önemlidir. Bu tez çalışmasında, kullanıcı sayısının fazla olduğu ağların skorlanmasını sağlayan bir sistem önerilmektedir. Önerilen sistemde skorlama işlemi için kullanıcıların ağ üzerinden internete erişimiyle oluşan internet kayıt dosyaları kullanılmıştır. Bu veriler kullanılarak, kullanıcıların internet kullanım tercihleri, erişim sağladıkları cihazın işletim sistemi ve versiyonu, tercih ettikleri web tarayıcıları ve kullanıcıların DNS sunucu tercihleri göz önünde bulundurularak kullanıcıların güvenlik seviyesi skorlanmaktadır. Skorlama adımından sonra, kullanıcılar K means kümeleme ve Ağırlıklı ortalama hesaplama yöntemiyle hesaplanan skorlara göre sınıflandırılmaktadır. Ayrıca, incelenen ağın sahip olduğu ağ güvenlik ekipmanlarına göre de bir skor üretilmektedir. Kullanıcı skorları ile ağ güvenlik ekipmanları skorunun birleştirilmesi ile de ağ güvenlik skoru oluşturulmaktadır. Böylece ağ güvenliği skoruna göre ağın güvenlik seviyesi tespit edilmektedir. Sistem tarafından üretilen sonuçlar görsel grafik ve tablolarla gösterilmektedir.

Anahtar Kelimeler: Ağ güvenliği, güvenlik skorlama, ağ kullanıcı analizi, ağ bileşenleri analizi

ABSTRACT

NETWORK SECURITY SCORING SYSTEM

KAÇAR, Mustafa Sami

M.Sc. – Electrical and Computer Engineering

Thesis Consultant: Ass. Prof. Dr. Kasım ÖZTOPRAK

February, 2017

Network security has become one of the most significant concerns of today's world. With the widespreading of the internet, public and private organizations share personal information over the internet. Preservation of that information is pretty critical, while if it is captured by third party users there may arise serious damages. Therefore, with the rising of the cyber attacks, public and private networks are under serious threats. Especially recognization of network security conditions of public organizations is very important, while they are too critical points on national security. In this thesis, a system that handles to score networks where user numbers are high. To implement that process, internet log files which are created by users' internet connections over the network. Users usage and their devices', which are utilized by users while connecting to the internet, operating system, web browser and DNS server data is scoring utilizing from that log files. After the scoring parts, users are classified via K Means Clustering and Weighted Average Estimation methods. Otherwise, network security equipments are also scored by it is owned by inspected network or not. Combination of these scores creates network security score. Thus, network security level is determined according to network security score. Results, which are created by system, will be demonstrated by reports and graphics.

Keywords: Network security, security scoring, network user analysis, network components analysis

TEŞEKKÜR

Öncelikle, sadece bu tez çalışmasında değil tüm akademik çalışmalarımda bana yol gösteren tez danışmanım Yrd. Doç. Dr. Kasım ÖZTOPRAK' a şükranlarımı sunarım. Tez çalışmamın konusunun seçilmesinden ilerlemesine her adımda yardım aldım. Ayrıca, Amerika da gerçekleştirilen SCSN 2017 konferansına göndererek yayınladığımız bu çalışmayı duyurmamızı sağladığı için ayrıca minnettarım.

Bölüm başkanım Prof. Dr. Novruz ALLAHVERDİ hocama göstermiş olduğu ilgiden ve bana çalışmam için sağladığı kolaylıklardan dolayı teşekkür ederim. Oda arkadaşım, bölüm hocalarından Öğr. Gör. Semih YUMUŞAK hocama da tez yazımından, çalışmamdaki detaylara kadar sorularıma bıkmadan cevap verdiği için çok teşekkür ederim.

KTO Karatay Üniversitesi Mühendislik Fakültesi değerli asistanları, meslektaşlarıma da maddi, manevi ve bazen de benim yapmam gereken işleri kendileri üstelenerek yardımlarını eksik etmedikleri için teşekkürlerimi sunuyorum.

Son olarak değerli eşim Melek KAÇAR'a da vermiş olduğu tüm manevi destekleri, özellikle motive edici davranış ve konuşmaları için sonsuz şükranlarımı sunuyorum.

Mustafa Sami KAÇAR

Şubat-2017

İÇİNDEKİLER

ÇİZELGELER LİSTESİ

ŞEKİLLER LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Kısaltmalar	Açıklama
CERN	ConseilEuropeanpour la Recherche
CVSS	Common Vulnerabilities Scoring System
CSV	Comma Sperated Values
DOS	Denial of Services
DNS	Domain Name System
ICE	Internet Category Engine
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
NCSA	National Center for Supercomputing Applications
URL	Uniform Resource Locator
VPN	Virtual Private Network

1. GİRİŞ

1.1 Giriş

Bilgisayar ağları, iki veya daha fazla bilgisayar veya benzeri komut verilebilen, yorum yapabilen ve çıktı üreten akıllı cihazların etkileşimi için oluşturulan yapılardır. Dünya üzerindeki milyarlarca cihazın oluşturduğu bir ağ olan internet, günümüzün en önemli iletişim ortamı haline gelmiştir. 1961 yılında Leonard Kleinrock 'un çalışmasında [1] önerdiği fikirle doğduğu kabul edilen internet, 55 yılda çok sayıda kişi tarafından geliştirilerek yaşamımızın en önemli parçalarından biri haline gelmiştir. Hiçbir kütüphanenin alamayacağı kadar çok bilgi içeren, milyonlarca insanın aynı anda iletişim kurabildiği internet sayesinde bürokratik işlemler öncesine göre kat ve kat hızlanmıştır. Daha önce fiziksel ortamda tutulan yazılı, görsel hemen her tür bilgi internet ve ilgili teknolojilerle sanal ortamda, internetin olduğu her yerden ulaşılabilecek şekilde saklanmaktadır. Böylece bilginin korunması, tutarlılığı, kolay ulaşılabilirliği sağlanabilmektedir.

Üniversiteler, hastaneler, güvenlik ve haberleşme kurumları ülkenin ulusal güvenliği açısından kritik öneme sahip yerlerdir. Ülkenin iç ve dış tehditler açısından hassasiyeti olan bu kurumlara yapılabilecek saldırılar ülkeye ciddi zararlar verebilir. Bu yüzden, böyle kurumların güvenliği ülkenin öncelikli meselelerindendir. Devlete ya da vatandaşlara ait oldukça mahrem bilgiler bu kurumlarda, çoğunlukla bilgisayar ortamında, tutulmaktadır. Bu bilgilerin gizliliği de bahsedilen kurumların güvenliği açısından kilit öneme sahiptir. Kurumlar birbirleri ile bu bilgileri internet üzerinden paylaşmaktadır. 2008 yılından beri internet üzerinde hizmet veren E-Devlet [2]hizmeti ile de kurumlar vatandaşlarla bilgi etkileşimi kurmaktadır. Dolayısıyla kurumların bu bilgileri sakladığı, paylaştığı ağ güvenliği şüphesiz çok kritiktir. Bu ağlara yapılabilecek siber saldırılar[3] telafi edilmesi oldukça zor olacak zararlar verebilme potansiyeline sahiptir. Kurumlara düşen görev ise, ağ güvenlik seviyelerinin farkında olarak, durum ve şartlara uygun önlemler almaktır.

Bilişim dünyasındaki hızlı gelişim internetin imkân ve faydalarını günden güne artırmaktadır. Ancak buna paralel olarak, internetin artan yeteneklerinden faydalanan

kötü niyetli kullanıcılar da internet üzerinden yapılabilecek tehdit ve saldırı potansiyelini artırmaktadır. Bu alanda yetenekli kötü niyetli kullanıcılar, bilinen adlarıyla hackerler[4], kurumsal ağlara yasal olmayan yollarla iz dahi bırakmadan ulaşarak bilgi çalmakta, ağa kalıcı zararlar vermektedir. Bu bağlamda ağ güvenliği internetteki tüm zararlı içerikten ve kullanıcılardan ağı izole etmektir denilebilir. Kurumlar ağı tehdit eden böyle unsurlardan bu alanda ürünler üreten bilgisayar güvenlik firmalarından yazılım ve donanım desteği alarak ağlarını izole etmeye çalışmaktadır. Her yeni geliştirilen siber tehdit karşısında yeni bir önlem alınarak ağların sürekliliği ve tutarlılığı sağlanmaya çalışılmaktadır.

1.2 Tezin Amacı ve Kapsamı

Bu tez çalışmasında, devletlerin ulusal güvenliğinde kritik öneme sahip kurumların ağ güvenlik seviyelerini ve ağın genel durumunu; ağ üzerinden internete bağlanmak için ağı kullanan kullanıcıları, kullanıcıların ağı kullandıkları cihazların bazı bilgilerini ve ağın sahip olduğu güvenlik önlemlerini inceleyerek skorlayan, verilen skora göre de ağ güvenliğini derecelendiren bir sistem önerilmektedir. Önerilen bu sistemle ağ güvenliğinden mesul kişilerin ağın güvenlik durumunu gözlemleyebilmesi ve buna göre gerekli tedbirleri alması hedeflenmektedir. Özellikle üniversiteler, hastaneler gibi kişilerin özel bilgilerinin saklandığı, bakanlıklar, emniyet müdürlükleri gibi devletin mahrem bilgilerinin tutulduğu kurumların ağ güvenliğinin farkındalığının artırılarak varsa bu kurumların açıklarını gidermesi, kırılgan noktalarını güçlendirmesi amaçlanmaktadır. Ayrıca ağı kullanan kullanıcıların cihaz bilgilerine göre bazı kullanım eğilimlerinin incelenmesi ve kullanıcı tercihlerinin istatistiksel bilgi olarak grafiklerle gösterilmesi amaçlanmaktadır. Böylece kurumların ağları daha güvenli hale gelecek, bilgi sızması, bürokrasinin aksaması gibi durumlardan olabildiğince kaçınılacaktır. Kendi ağlarının durum ve şartlarının farkında olan kurumların kendilerine uygun ağ güvenlik yazılım ve donanım gereksinimlerini talep edebilir hale gelmelerine, bunun da bu alanlardaki yerli güvenlik ürünlerini teşvik etmesine bu çalışmanın yol açıcı olması da hedeflenmektedir. Yerli güvenlik ürünlerinin hem ülke güvenliğine hem de ülke ekonomisine önemli değerler katacağı şüphesizdir.

Bu tez çalışmasının temelini incelenen ağ üzerinden internete bağlanan kullanıcıların analizi oluşturmaktadır. Öncelikle kullanıcı internet erişim dosyaları (İngilizce adıyla Log Files) [5] ile tutulan kullanıcıların internet erişim geçmişleri, ağa bağlandıkları cihazın işletim sistemi, kullanılan tarayıcı vb. bilgilerin incelenmesiyle kullanıcılar hakkında analiz yapılmaktadır ve kullanıcılar sınıflandırılmaktadır. Ardından, ağın sahip olduğu ya da olmadığı güvenlik önlemlerine göre ağ incelenmektedir. Birinci ve ikinci adımdaki incelemelerin sonuçları birleştirilerek ağın güvenlik durumu resmedilir. Kullanıcılar ve cihazların incelenmesiyle ortaya çıkan istatistiksel bilgiler de kullanılan cihazlar ve özellikleri hakkında detaylı, kolay anlaşılabilir bilgiler sunmaktadır.

Tezde önerilen sistemde kullanıcı gizliliğini koruma adına kayıt dosyalarında yer alan kullanıcılar yerel ağda aldıkları yerel IP adresleri [6] olarak ifade edilmekte, ve yine bu adresler aracılığı ile birbirinden ayırt edilmektedir. Öncelikle ayırt edilen kullanıcıların ağ üzerinden erişim sağladıkları web sitelerine göre kullanıcıların kullanım skorları üretilmektedir. Kullanım skorları ağ üzerindeki kullanıcıların ağa zarar verme potansiyeli olup olmadığını göstermede en önemli aşamadır. Daha sonra kullanıcıların ağ üzerinden internete erişim sağladıkları cihazların işletim sistemi bilgileri incelenerek, kullanıcılar cihazlarında kullandıkları işletim sistemine göre skorlandırılmaktadır. Sonraki adımda cihazların web tarayıcı bilgileri incelenerek yine her kullanıcı için bir skor belirlenmektedir. Kullanıcı incelemesinin son adımında kullanıcıların internete erişim sağlarken tercih ettikleri ‘Alan Adı Sistemi (Domain Name System - DNS) [7] sunucusuna göre her kullanıcı için ayrı ayrı skor üretilmektedir. Bu dört adımda oluşan skorların yüzdesel değişimi ile kullanıcı skorunun ne kadar değiştiği incelenerek kullanıcı skoru dört skorun ağırlıklı ortalamaları hesaplanarak elde edilmektedir.

Sistemin ikinci aşamasında ağın daha önce sisteme tanımlanmış ağ güvenlik ürünlerine sahip olup olmadığı kontrol edilerek bir skor üretilmektedir. Bu skor sistemin kullanıcıdan bağımsız kendi güvenlik önlemlerini ne kadar aldığını, internet üzerinden gelebilecek saldırılara karşı ağın ne kadar dirençli olduğunu gösteren bir parametredir. Ağ güvenliğini güncel tutmada bu skorun bir gösterge olması

düşünülmektedir. Analizin sonunda detaylı istatistiksel veriler çıkarılmaktadır. Bu veriler kullanıcıların eğilimlerini görmede kolay anlaşılır bir kaynak sunacaktır. Bu çalışma kapsamında tüm bu sistemi uygulamak ve test etmek için bir simülatör programı geliştirilmiştir.

1.3 Tez Akışı

Tez çalışmasının akışı bu bölümde anlatılmıştır. İkinci bölümde, tez konusu ile ilişkilendirilen çalışmalar anlatılmaktadır. Özellikle ağ güvenliğinde kullanıcıların analizleri, internet erişim dosyaları ile kullanıcıların sınıflandırılması gibi uygulamalar anlatılmıştır. Ayrıca bazı skorlama sistemleri ile ilgili bazı çalışmalar da anlatılmıştır.

Üçüncü bölümde ağ güvenliği hakkında bilgiler yer almaktadır. Ağ ve internet kavramlarının doğuşundan itibaren gelişen süreç, günümüz ağlarına yapılan saldırılar ve bu saldırılara karşı geliştirilen güvenlik mekanizmaları anlatılmaktadır. Bu bölüm ile, ağ yapısı tanıtılarak var olan tehditlere karşı farkındalık oluşturmak, ağ güvenlik sistemlerine neden ihtiyaç duyulduğu açıklanmakta ve ağ güvenlik yazılım ve donanım araçları ile alınabilecek önlemler anlatılmaktadır.

Tez çalışmasında önerilen sistemin ayrıntıları dördüncü bölümde anlatılmaktadır. Sistemin yapısı detaylı olarak alt başlıklarda yer almaktadır. Her adımda hangi skorların üretildiği, skorların neye göre üretildiği, nasıl birleştirildiği, üretilen son skorların ne anlama geldiği bilgileri yer almaktadır. Ayrıca sistemi test etmek için üretilen ağ güvenlik simülatörü programının çalışma mantığı ve sözde kodu (pseudo code) ilgili bölümde yer almaktadır.

Deneysel sonuçlar beşinci bölümde gösterilmiştir. Kullanıcı kayıt dosyalarından üretilen sentetik veri setinin önerilen sisteme uygulanması ile elde edilen ağ güvenlik skoru, bu skorun anlamı ve diğer sonuçlar açıklanmıştır. En düşük kullanıcı skoruna sahip 10 kullanıcı, bu kullanıcıların detaylı skorları çizelge ile gösterilmiştir. Ayrıca, kullanıcı tercihleri grafiklerle deklare edilmiştir.

Son olarak sonuç bölümünde sistemin genel yapısı özetlenmiş ve gelecekte yapılması planlanan geliştirilmelerden bahsedilmiştir.

2. İLGİLİ ÇALIŞMALAR

Yaklaşık 50 yıldır ağ güvenliği üzerine yapılan çok sayıda çalışma literatüre geçmiştir. Yeni gelişen tehditlerin açıklandığı, bunlara karşı oluşturulan savunma sistemlerinin anlatıldığı, yeni ağ teknolojilerinin yer aldığı bu çalışmalar internetin ve teknolojinin hızlı gelişimine bağlı olarak hep kendilerini yenilemek durumunda kalmıştır. Kötü niyetli kullanıcılar ve kullandıkları yöntemlerin karmaşıklığı ağ güvenliğinin gelişiminde kilit rol oynamıştır. Bu tez çalışmasında sunulan yönteme literatürde rastlanamamıştır. Kullanıcı analizi ile ağ güvenliğinin bağdaştığı bazı çalışmalar mevcuttur ancak skorlama bu çalışmayı özgünleştirmektedir.

Yazarlar [8]' deki çalışmalarında ağ güvenlik açıklarını incelemişlerdir. Kurumların ağ trafiğinde zararlı olabilecek yazılımların yoğunluğunu incelemişler, saldırı yöntemlerine dikkat çekmişlerdir. Ağ trafiğini inceleme yöntemlerinden bahsedilmiş olup, bu tezdeki çalışmayla da ilgili olan kullanıcı davranış modellerinin ağ trafiğine bakılarak nasıl çıkarılabileceğine dair yenilikçi fikirler sunmuşlardır. [9]'da yazarlar web sitelerinden ve bu siteleri ziyaret eden kullanıcıların ziyaretleri ile oluşan verilerin incelenmesi anlamında kullanılan web madenciliği üzerine çalışma yapmışlardır. Çalışmada web madenciliği ve adımları hakkında detaylı bilgi verilmiş olup, web madenciliğinin kullanıcıların davranış biçimlerini ortaya çıkarmada nasıl kullanılabileceğini göstermişlerdir. Çoğu açık kaynaklı yazılım araçları ile kullanıcıların web erişim kayıtlarına bakarak kullanıcı davranış analizinin nasıl yapılacağına dair bilgiler yazarların [10] çalışmasında sunulmuştur. Ayrıca bu yazılım araçlarının bilgileri ve karşılaştırılması da yine bu çalışmada yer almıştır. [11] 'deki çalışmada yazar web kullanımında zarara en müsait grubun çocuklar olduğuna vurgu yaparak çocukların internet kullanım davranış biçimlerini incelemiştir. Çalışmanın davranış biçimlerini web sitelerini kategorize ederek sunması bu tezdeki çalışmayla benzerlik taşımaktadır. 'Common Vulnerability

Scoring System' (CVSS) [12] kar amacı gütmeyen bir organizasyon olan "Fisrt.Org.Inc." tarafından oluşturulan ve yönetilen, tüm yazılım ürünlerinin açıklarını inceleyen açık kaynak kodlu skorlama sistemidir. Bu sistem dünyada en çok kullanılan işletim sistemleri, web tarayıcıları, mobil uygulamalar gibi yazılım ürünlerini inceleyen bir metrik sunmaktadır. Bu metrik ile üretilebilecek bir yazılım aracı da ağ güvenliği gibi bir alanda kullanılıp, derecelendirme imkânı sağlayabilmektedir. Bu sistemde temel, geçici ve çevresel metrik gruplarıyla önerilen ana metrik oluşturulmaktadır. Sistemde incelenen yazılımsal ürüne yapılan ya da yapılması muhtemel saldırılar, ürünün açıkları, ürünün saldırıya verdiği tepki, ürünün saldırı sonrası durumu gibi metrik gruplarının alt başlıklarıyla detaylı inceleme yapılmaktadır. Sistemin skorlama üzerine kurulmuş olması, bu tezde sunulan ağ güvenliği skorlama görüşünü destekler niteliktedir. Ayrıca, tez içinde incelenen işletim sistemi, web tarayıcı ürünlerinin skorları CVSS ile ortaya çıkan skorlara paralel olarak oluşturulmuştur. [13]'te kayıt dosyalarının analizlerinde kullanılan sistemler, teknikler ve sonuçlar hakkında detaylı bilgi verilmiştir. Farklı meslek gruplarından kullanıcılar teste tabi tutulmuştur. Ancak bu çalışmada ve literatürde yer alan çoğu çalışmada bir web sitesinin kullanıcıları üzerine analiz yapılmış olup kullanıcıların o site ile etkileşimlerinden davranış paternleri ve kullanıcı sınıflandırmaları yapılmıştır. Yazarın [14] çalışması kullanıcılar internet kullanım karakteristiği ve davranışlarına göre birbirinden ayırt edilmesi üzerinedir. Çalışmada kullanıcıların erişim sağladıkları web sitelerinin 'İnternet Kategorizasyonu Motoru' (Internet Categorization Engine-ICE) tarafından kategorize edilmesi sonucu oluşan kategori bilgilerinden faydalanılmıştır. Hangi kullanıcının hangi kategorideki web sitelerine daha çok erişim sağladığı bilgisi ile kullanıcı eğilimlerinin hangi kategorilere doğru olduğu ortaya çıkarılmıştır. Kullanıcı sınıflandırmaları, kullanıcı ya da sistem skorlandırılması, skorlamanın kullanıcıların erişim sağladığı web sitelerinin kategorilerine göre skorlanması daha önce yapılan çalışmalarda yer alan başlıklardır. Ancak, bunların birlikte kullanımı ile ağ güvenliğinin skorlanması bu tezde sunulan özgün bir çalışmadır. Dünyanın en büyük bilgisayar ağ çözümleri şirketlerinden olan CISCO[15] siber savunma çözümleri üretiyor. Bu ürünlerden birisi olan "Lancope Stealth Watch System" ürünü bu tez çalışmasıyla benzerlikler taşımaktadır [16]. Ürünün temel amacı, ağ akış verisinin toplanarak normalize

edilmesi, ardından güvenlik analitikleri ile zararlı ve şüpheli ağ trafik paternlerinin ortaya çıkarılmasıdır. Yine bu ürünle ilişkili olan "Identity Services Engine" de ağda uç noktalardaki cihazları erişimleri ile tanımlamak için üretilmiş olup, cihaz özelliklerine ve erişimlere göre sınıflandırma yaparak kullanıcıları tanımlamayı hedeflemektedir.

3. AĞ GÜVENLİĞİ

3.1 Bilgisayar Ağları ve İnternet

Temel anlamda daha önce insanlar tarafından belirlenen komutlara göre bilgiyi yorumlayabilen elektronik cihazlara bilgisayar denilmektedir. Bilgisayarın yaygınlaşmasıyla birlikte bilgisayarların arasında gerçekleşecek iletişime ihtiyaç duyulmuştur. Bir bilgisayar tarafından yorumlanan bilginin diğerine aktarılması ya da bilgiyi yorumlamak için birden fazla bilgisayara ihtiyaç duyulması temel gereksinimlere örnek olarak sayılabilir. Tarihsel süreçte gelişip günlük yaşamın vazgeçilmez parçası haline gelen bilgisayar ağları ve bir tür bilgisayar ağı olan bugünkü internet de bu temel ihtiyaçla doğmuştur. 60'lı yıllarda Amerika tarafından geliştirilen 'ARPANET' [17] internetin ve gelişmiş bilgisayar ağlarının bilinen en eski örneği olarak kabul edilmektedir. Başlangıçta askeri alanda kullanılan ARPANET, askeri birimlerin ve bazı üniversitelerin bugünkü anlamıyla web sitelerinden oluşan bu ağ, bilgisayar dünyasında devrim niteliğindedir. 1989 yılında Avrupa Nükleer Araştırma Merkezi –CERN de çalışan Tim Berners-Lee tarafından geliştirilen 'World Wide Web' (WWW) günümüzdeki internetin doğuşunun ana faktörüdür. İnternetin gelişimi demek aslında geniş anlamda bilgisayar ağlarının gelişimi anlamına gelmektedir. İnterneti daha verimli kullanabilmek için üretilen tüm yazılım ve donanımlar, bilgisayarı ve bilgisayar ağlarını çok daha gelişmiş hale getirmiştir. İnternetin sunmuş olduğu mesafe tanımaksızın iletişim her gün geliştirilerek daha hızlı, daha hacimli ve daha güvenli hale gelmiştir.

Bugün internetin geldiği noktada milyonlarca insanın aynı anda sesli, görüntülü formlarda iletişime geçmeleri oldukça kolay hale gelmiştir. Sosyal medya platformlarından bir kullanıcının birden fazla kullanıcıya anlık görüntü aktarması

sıradan bir olgu olmuştur. Genç popülasyon tarafından talep gören çevrimiçi video oyunları geleceğin sporu olarak görülmektedir[18]. Gelişmiş ağ altyapılarına ihtiyaç duyan çevrimiçi video oyunları, bilgisayar ağlarının gelişmesini körükleyen başlıca etmenler arasındadır. Akıllı telefonların günlük hayatta yaygınlaşmasıyla birlikte ağ üzerinden yapılan iletişim oldukça fazla artmıştır. Mesajlaşma, içerik paylaşımı, navigasyon vb. çok farklı sebeplerle akıllı cihazlar tarafından kullanılan internet, mobil telefon servis sağlayıcılarını daha güvenli, daha gelişmiş ağ altyapılarına sahip olmaya itmektedir. Bilgisayar alanında yapılan yatırımların önemli bir kısmının bilgisayar ağları, internet, ağ güvenliği konularını kapsayan bilgi teknolojileri alanına yapılması da bunu göstermektedir [19].

Nesnelerin İnterneti 1990'lı yıllarından sonlarından itibaren kullanılan, tartışılan ve gelişim gösteren bir kavram olmuştur [20]. Günlük hayattaki tüm elektronik cihazların internete bağlanması düşüncesi merkezinde yoğunlaşan nesnelerin interneti, günlük hayatı oldukça kolaylaştıracak yenilikçi teknolojiler sunması beklenen bir konudur. Buzdolabının kapağına yapıştırılan bir restoran magnetinin üzerindeki bir tuşla yemek siparişi vermek, tek bir komutla evde kimse yokken evi süpüren bir süpürge gibi insanların günlük yaşantısını tamamen değiştirecek yenilikler nesnelerin interneti konusunda çalışan bilim insanlarının heyecan verici önerilerindendir. Tüm elektronik cihazları tek merkezli ve uzaktan yönetme, iş dünyasında işçi gereksinimini azaltarak insan kaynaklı hataları en aza indirmek nesnelerin interneti ile odaklanılan konulara örnek teşkil etmektedir. Tüm bu yeniliklerin yanında nesnelerin interneti konusu için de ağ güvenliği öncelikli meselelerdendir. Yukarıdaki örneklerden de görüleceği gibi insanların evlerindeki eşyalara kadar tüm elektronik cihazların bir ağa bağlanması ve bu ağa erişimin uzaktan sağlanması için internet üzerinden olması ciddi bir riski de beraberinde getirmektedir [21]. Kötü durum senaryolarında nesnelerin interneti ile kurulan bir ağ üzerinden yapılabilecek saldırıların maddi manevi oldukça yıkıcı zararlar verme olasılığı bulunmaktadır. Dahası evdeki bir eşya ya da arabanın kullanıcı kontrolünden çıkarak kötü amaçla kullanılmasıyla bireylere ve topluma yönelik saldırıların olabileceği düşüncesi bile korkutucudur. Tüm bunlar ağ güvenliğinin önemini tekrar vurgulamaktadır. Bireysel veya kurumsal olsun ağ güvenliği internet

erişimi olan tüm ağlarda üzerine düşülmesi gereken öncelikli meselelerdendir. Bir ülkenin güvenlik güçlerinin fiziksel dünyayı tehditlere karşı savunması gibi, bilgisayar ağları üzerinde çalışan bilim insanları, ağ yöneticileri, ağ güvenlik uzmanları ve bu alanlarda yazılım ve donanım üreten firmaların kötü kullanım ve kullanıcılara karşı siber savaş vermeleri insanları ve kurumları böyle tehditlerden korumak zorundadırlar.

3.2 Bilgisayar Ağlarına Yönelik Yapılan Siber Saldırılar

İnternetin gelişimi ile siber dünya suç mahallerinden biri haline gelmiştir. Kötü niyetli kullanıcılar kimlik veya para hırsızlığı, internet sitelerini ya da hizmetlerini etkisiz hale getirme gibi sebeplerle internet üzerinden saldırılar yapmaktadırlar. 1990'larda yaygınlaşan interneti kullanarak yapılan siber saldırıların kurum ve yöneticiler tarafından ciddiye alınması 1990'ların ortalarını bulmuştur. İnternetin en çok aranan ve en çok tanınan hackerı olduğu kabul edilen Kevin Mitnick Amerika tarihinin bilgisayarla yapılan en büyük suçunu işlediği düşünülmektedir [22]. Dünyaca bilinen dev şirketlere verdiği milyonlarca dolar zararın ardından 1995 yılında tutuklanmıştır. Bu olaydan sonra hükümetler ve elektronik devi şirketler ağ güvenliğini ve siber tehditlerin farkına varıp daha ciddi atılımlar göstermişlerdir [23]. Örneğin dönemin Amerikan başkanı Bill Clinton 1999 yılı için ağ güvenliği alanına 1.5 milyar dolarlık yatırım kararı almıştır [24]. O günden bugüne saldırıların çeşitliliği, büyüklüğü ve hedefleri ile saldırı yapan hackerların sayısı artarak devam etmiştir. Buna karşılık harcanın para ve güvenlik önlemleri de artmıştır. İnternet üzerinden yapılan en yaygın saldırı yöntemleri şunlardır:

3.2.1 Virüsler

Virüsler, dosyaların içine sızan ve iç güdümlü olarak çoğalıp, yayılmak için dosyaları kullanan, dosyanın açıldığı anda kendini aktive eden program ya da program parçası kötü amaçlı yazılımlardır. Virüsleri üretip yayılmasını sağlayan saldırganlar, çoğu zaman kullanıcıları yararlı yazılım gibi gösterdikleri program veya uygulamalarla tuzağa düşürürler. Kurbanın dosyayı açmasıyla virüsün dosyanın açıldığı cihaza yayılımı başlar ve kötü niyetli kullanıcıların virüsün yazılımında belirlediği

komutların tuzağa düşürülen cihazda çalışması başlar. Zamanla müdahale edilmezse virüsler tüm cihaza yayılabilir. Hatta cihazın erişim sağladığı diğer cihazlara da yayılabilir [25].

3.2.2 Solucanlar

Bilgisayar solucanları virüslere benzer şekilde çalışırlar. Kendi kendine çoğaltabilmeleri bunu gösterir. Ancak, solucanlar yayılmak için bir dosyaya ihtiyaç duymazlar. İki tür solucan vardır; e-posta yoluyla yayılan solucanlar ve ağ farkındalığı olan solucanlar. E- posta yoluyla yayılan solucanların aktif edilmesi halinde posta listesindeki tüm kullanıcılara yayılma tehlikesi vardır. Ağ farkındalığı olan solucanlar ise internet için daha büyük tehdittir [22]. Çünkü eğer bu solucanlar hedefini seçer ve sunucuya erişim sağlarsa sisteme ciddi zararlar verebilirler. Dünyada kendi ismiyle bilinen tarihe geçmiş solucan saldırıları mevcuttur. Melissa solucanı bunlardan biridir [26]. Melissa isimli bir bilgisayar kullanıcısının bilgisayarı üzerinden yayıldığı için bu ismi almıştır. 1999 yılında ortaya çıkan bu solucanın dünya çapında 1.1 milyar dolar zarar verdiği tahmin edilmektedir. Orijinal ismi 'I LoveYouWorm' olan başka bir solucanın ise daha yıkıcı olup 8.75 milyar dolarlık hasar verdiği düşünülmektedir.

3.2.3 Truva Atları

Tarihte Truva savaşında düşmanın hediye gibi göstererek ağaçtan atın içindeki düşman askerlerini Truva şehrine sızdırmasıyla bilinen ve adını da oradan alan Truva atından esinlenilmiş bir saldırı türüdür. Yararlı bir yazılım gibi görünen ancak gerçekte zararlı olan bu yazılımlar; solucanlar veya virüsler gibi yayılmaz ya da çoğalmazlar. İçine sızılan cihazda kullanıcı kontrolü dışında açıp kapanan pencerelerle kullanıcıyı zorlayan yada bilgi çalma, dosya silme gibi işlemlerde kullanılan Truva atları cihazda açık kapı bırakarak kötü niyetli yazılım ve kullanıcılara da sızmak için imkan sağlayabilmektedir [25].

3.2.4 Hizmet Engelleme – DOS Saldırıları

DOS saldırısı hizmet veren bir bilgisayar sunucusuna kapasitesinin üzerinde talep göndererek hizmet veremez hale getirme yöntemidir. Ağ üzerinden iletişim dünya çapında belirlenen bazı protokollere göre sağlanmaktadır [27]. Ağ topolojisi, ağ standartları ve sistemlerin güvenilirliği bu protokollerle teminat altına alınmaktadır. Bu protokollere uymak zorunda olan ağlar, ağa gelen isteklere cevap vermek durumundadır. Bu noktadan hareketle üretilen DOS saldırıları aynı anda farklı noktalardan gönderilen fazla sayıdaki taleplerle sunucuyu servis veremez hale getirirler [28]. Daha çok kötü niyetli kullanıcılar tarafından oluşturulan grupların üyelerinin toplu olarak saldırmasıyla veya yine kötü niyetli kullanıcılar tarafından daha önce ele geçirilmiş cihazlar, teknik adıyla 'Zombie Bilgisayarlar', ile bu saldırılar gerçekleştirilir. Yayınlanan raporlara göre, internet üzerinden saldırılarda en yaygın olarak kullanılan saldırı yöntemi Hizmet Engelleme saldırılarıdır [28].

Gizli dinleme, balıklama, IP adres kandırması, botlar da diğer en çok kullanılan saldırı yöntemlerindendir [28]. Tüm bu yöntemler kullanıcıları, kurumları ve internetin kendisini tehdit etmektedir. Böyle saldırılara karşı kullanıcıların farkındalığı artırılmalı, kurumların ağ yöneticileri kurum cihazlarını kullananlara gerekli eğitimi vermeli, ülkeler gerekirse savunma birimlerini kurarak siber saldırılara karşı önlem almalıdır.

3.3 Bilgisayar Ağlarında Kullanılan Güvenlik Önlemleri

Bilgisayar ağlarına yönelik yapılan tüm siber saldırılara karşılık yeni savunma sistemleri uzmanlar tarafından, tehditlerin oluştuğu günden beri, geliştirilmektedir. Maruz kalınan saldırılardan kaynaklanan maddi manevi kayıpların büyüklüğü nedeniyle devletler ve büyük şirketler bu sistemlere oldukça ciddi ücretler ödemektedirler [29]. Alınan bu önlemlerdeki amaç tümüyle saldırıları bertaraf etmek değil, ancak zararın en aza indirilmesini sağlayabilmektedir. Ağ güvenliği için doğru güvenlik araçlarını kullanmak da önem arz etmektedir. Ağın kullanıldığı kurumun, şirketin yapısı, ağ üzerinden interneti kimlerin ne amaçla kullandığı gibi soruların cevapları ile kullanılacak güvenlik araçları da belirlenebilmektedir. Kurum ve

şirketlerin ağ güvenliği için en çok kullanılan güvenlik araçlarından bazıları aşağıda açıklanmıştır.

3.3.1 Güvenlik Duvarı

Ağ güvenlik duvarları kullanıldıkları ağların dışarı ile bağlantı noktalarında kurulan, ön savunma sistemi olarak çalışan bir güvenlik sistemidir[30]. Ağlar üzerinden bilgiler paketler halinde taşınır. Bu paketler gerçek hayattaki posta sistemine benzemektedir. Gönderen ve alıcı kimlik bilgilerinin yer aldığı bu paketleme sistemi ile, ağların doğrulama sistemi çalıştırılmış olup, herhangi bir bağlantı kaybı sonrasında bilginin tümünün değil ilgili paketin yeniden alınmasıyla ağ trafiğine oluşan ilave trafik de ciddi oranda azaltılmış olur. Ağ güvenlik duvarları da gelen ve gönderilen bu paketleri filtreleme görevini üstlenir. Gönderenin doğrulanmadığı paketleri veya üzerinden bulunan sistemle zararlı olacağına karar verdiği paketleri engelleyerek saldırıları ya da saldırı tehlikelerini ağa gelmeden savuşturmuş olur. Bu güvenlik duvarları yazılım, donanım veya hem yazılım hem de donanım kullanılarak çalıştırılan bir sistemdir [28]. Kurulacağı ağın yapı ve ihtiyaçlarına göre uygun güvenlik duvarı ürünleri seçilmelidir. Günümüzde kurumlar ve şirketler için güvenlik duvarları olmazsa olmaz ağ savunma sistemleri arasındadır. İçerden ve dışardan gelebilecek tehditleri büyük oranda engeller [30].

3.3.2 Zararlı Yazılım Engelleyici Araçlar

Virüs, Truva atları, solucanlar gibi zararlı yazılımları tespit edip sistemden temizlemeye yarayan ve sistemi taramaya yarayan araçlara denir. Anti-virüs programları böyle yazılımlara örnektir. Genel olarak ağ güvenliği için değil ağ iletişiminde uç nokta olarak tabir edilen bilgisayar, akıllı telefonlar gibi elektronik cihazlarda kullanılır. Böyle güvenlik yazılımları bilinen tüm virüs, solucan gibi zararlı yazılımları tanımalı, yeni tehditlere karşı güncel olmalı ve kullanıcıyı uyarma konusunda kapsamlı olmalıdır [31].

3.3.3 Sanal Özel Ağlar

Fiziksel olarak bir ağa bağlı olmadan o ağa bağlıymış gibi hareket ettiren sistemlerdir. Bağlı olunan sanal ağ üzerinden internete erişim imkânı vererek çok kullanıcılı ağlarda kullanıcıyı koruyabilmektedir. İletişimde aktarılan veri şifreli olarak aktarıldığı için ağı görüntüleyen uzmanlar bile ağda şifreli veri aktarıldığını bilebilirler ancak verinin içeriğini çözemezler [32]. Bu yüzden, şifreleme mekanizmaları önemli kurumsal veya kişisel gizli bilgilerin, değerli bilgilerin iletildiği kurum ağlarında kullanılması gereken bir yöntemdir.

3.3.4 İzinsiz Giriş Tespit Sistemleri

İngilizce adı Intrusion Detection System (IDS) olan bu sistemler ağlara gelen tüm saldırıları tespit etmek için geliştirilmiştir. Bu sistemler ağ yöneticilerini uyarmak ve saldırılar hakkında detaylı bilgi vermek için geliştirilmiştir. İzinsiz Giriş Önleme Sistemleri (Intrusion Prevention System - IPS) de benzer yapıyla çalışır ancak tespit sistemlerinden fazla olarak saldırıları önlemeye de yarar [33]. Bu sistemlerin veri tabanlarında güncel saldırılarla ilgili bilgiler yer alır ve ortaya çıkan yeni saldırılarla bu veri tabanları sürekli güncellenir. Böylelikle, uçtaki cihazlara yapılan saldırılar için tüm cihazlara bakmak yerine ağ yöneticileri merkezden tüm tehlike ve saldırıları gözlemleyebilir ve engelleyebilirler.

Yukarıda bahsedilen bu sistemlere URL Filtreleme, Anti Spam Yazılımları, Güvenli Soket Katmanı gibi araçlar da eklenebilir [28]. Tüm bu yazılım ve donanım ürünleri ile ağları ve interneti tehdit eden, kurumlara ve kişilere zarar veren yazılımlar tespit edilip engellenmeye çalışılır. Kurumların ve kişilerin ağları bu sistemlerle tamamıyla korunamaz. Çünkü, ağlar için en büyük tehdit ağı kullanan kullanıcılardır. Bilinçsiz kullanıcılar ağın zayıf halkalarıdır. Açılmaması gereken bir e-posta, indirilmemesi gereken bir dosya yüzünden tüm ağ etkilenebilir ve ağın hizmet veremez hale gelmesine sebep olabilirler. Bu yüzden kullanıcıların analizi, ağa zarar verebilecek kullanıcı gruplarının ortaya çıkarılması kurum ağları gibi ağlar için önem arz etmektedir. Bu tez çalışması da böyle bir düşünceden hareketle yapılmıştır.

Kullanıcıları internet erişim davranışları ve kullandıkları uygulamalar incelenerek skorlayan bir sistemle belirli skorun altındaki kullanıcılara ağ yöneticilerinin dikkatini çekmek hedeflenmiştir.

4. AĞ GÜVENLİĞİ SKORLAMA SİSTEMİ

Bu bölümde tez çalışmasında önerilen sistemin çalışma mantığı, girdileri, çıktıları detaylı olarak yer almaktadır. Kullanıcılara verilen skorların neye göre verildiği deklare edilmiştir. Hangi durumların dikkat çekici olduğu, tehlikeli veya sorunsuz durumlardan bahsedilmiştir. Sistemin ağ yöneticilerini uyarma yönteminden bahsedilmiştir. Kullanıcı analizi ve ağ güvenlik ekipmanları analizi sistemin iki alt bileşenini oluşturmaktadır.

Çalışmada önerilen sistem ağ uzmanlarını uyarma üzerine tasarlanmıştır. Sisteminin temel mantığı, insanlara yapılan checkup gibi çalışmaktır. Nasıl ki sağlıklı bünyeye sahip bir insana verilecek tavsiye bu durumu koruması, belirli yiyecek ve içeceklerden uzak durması ise burada da verilen skorlarla ağ üzerinde bir tehlike görülmezse ağ yöneticilerinin durumu korumaları yönünde bilgilendirilecektir. Herhangi bir problem oluşması halinde ise durumun ciddiyetine göre ağa önlem alınması istenecektir. Ağın tehlike seviyesini de ağ güvenliği skorlama sistemi ile elde etmek mümkün olacaktır. Ağ güvenliği skorlama sistemi, kullanıcı skorlama ve ağ güvenlik ekipmanları skorlama olmak üzere ikiye ayrılmıştır. Bu iki alt sistemden üretilen skorlar birleştirilerek ağ güvenliği skorlanır ve derecelendirilir. Kullanıcı skoru da kullanım, işletim sistemi, tarayıcı ve DNS skorlama olarak dört ayrı skorla hesaplanır. Tüm alt skorlamaların toplam skorlara etkisi farklıdır. Kullanıcı skorunun ağ güvenliği skoruna etkisi ağ güvenlik ekipmanları skorundan fazladır. Kullanıcı skoru içinde de en yüksek skor kullanım (internet erişim karakteristiği) skoruna aittir, ardından sırası ile tarayıcı, işletim sistemi ve DNS skorları gelmektedir. Bu skorlar 1 ile 5 arasında değişmektedir. 5 sistemin en yüksek skorudur, böyle bir ağ doğada bulunmayan ancak laboratuvar ortamında üretilebilecek ideal gazlara benzetilebilir. Çünkü daha önce de bahsedildiği gibi, kullanılan tüm ağlar tehditlere açık haldedir ve her an bir yerinden açık verebilir. 1'e doğru skorun azalması ağ güvenliği tehlikesinin arttığını göstermektedir.

Ağ tehlike seviyeleri, sistemi kullanılarak elde edilen ağ güvenlik skoruna göre ölçülür. Ağ güvenlik skoru 1 ile 5 arasında belirlenen aralıklara göre farklı renkler verilerek, ağ tehlike seviyesi ölçülmektedir. Sistemde eşik değeri 3'tür. Hesaplanan

skorlarla kullanıcılar 6 farklı kümeye bölünmüştür. Buna göre, pembe, mor renk kümeler zararlı veya şüpheli olabilecek, 3'ten düşük kullanıcı skoruna sahip kullanıcıları işaret etmektedir ve sistemin genel amacı da bu kullanıcıları ortaya çıkarmaktır. Yeşil ve mavi renk grupları skoru 3 civarında olan, ara grup olarak nitelendirilebilecek gruplardır. Geçiş bölgesinde yer alan bu gruplar genel olarak güvenli sayılmaktadır ancak bu grupların incelenmesiyle varsa tehlikeli olabilecek kullanıcıların ortaya çıkarılması hedeflenmektedir. Sarı ve siyah renkteki kümeler ise zarar potansiyeli düşük, 3'ten yüksek kullanıcı skoruna sahip kullanıcıları barındırmaktadır.

Özellikle siyah ve sarı renk gruplarında yer alan kullanıcılar ağ üzerinde zararlı kullanımı olmayan, ağ üzerinden internete erişim sağlarken kullandıkları cihazların güvenilir web tarayıcı ve işletim sistemine sahip olduğunu ve DNS sunucu tercihlerinin güvenilir DNS sunuculardan yana olduğunu göstermektedir. İncelenecek ağın bu kullanıcılar yüzünden tehlikeli bir duruma düşme olasılığı düşük olacağı için bu grupların tespit edilip diğer gruplardan ayırt edilerek asıl tehlike gruplarının ortaya çıkarılması hedeflenmektedir. Mavi ve yeşil renk grupları ara gruplardır. Genel olarak kullanıcıların kullanımlarında ciddi problemlerin olmadığını, cihazlarındaki tercihlerin sistemde yüksek skorlara sahip, güvenli sayılan ürünlerden yana olduğunu göstermektedir. Ancak, yine de bu gruplarda az da olsa tehlike potansiyeli olan kullanıcıların varlığını sorgulamak gerekmektedir. Kullanıcıların kullanımından, web, tarayıcı, işletim sistemi veya DNS sunucu tercihlerinden kaynaklı almış olabilecekleri düşük skorların incelenerek ortaya çıkarılması hedeflenmektedir. Pembe ve mor kümeler en çok incelenecek gruplardır. Bu gruplarda yer alan kullanıcıların skorları 3'ün altında yer almaktadır. Kullanım veya DNS sunucu skorlarından kaynaklı düşük kullanıcı skoruna sahip olması beklenen bu kullanıcıların daha az güvenli işletim sistemi ve web tarayıcı kullanıyor olmaları da muhtemeldir. Ağ üzerinde tehlikeli bir duruma bu kullanıcıların neden olması beklenmektedir. Dolayısıyla, önerilen ağ güvenlik sisteminin temel amacı bu kullanıcıları ortaya çıkararak detaylı incelemek ve düşük skorun nedenine göre gerekli önlemlerin alınması için ağ yöneticilerini uyarmaktır. Ağ güvenlik

ürünlerinin incelenmesiyle birlikte, ağın sahip olduğu ürünlere göre kullanıcıların daha güvenli sayılan renk gruplarına doğru skorlarının yükselmesi hedeflenmektedir.

4.1 Kullanıcı Analizi

Kullanıcı analizi, bu tez çalışmasının en kritik aşamasıdır. Ağ üzerinden internete erişim sağlayan kullanıcıların detaylı incelemesi yer almaktadır. Bu analizi yapmak için yazarın [14] çalışmasında kullandığı veri seti kullanılmıştır. Bu veri setinde temizlenmiş ve Internet Categorization Engine (ICE) tarafından, 40 farklı kategori içine kategorize edilmiş URL kayıt dosyaları mevcuttur [34]. Kayıt dosyalarının içinde kullanıcının yerel ağda aldığı IP adresi, kullanıcının erişim sağladığı web sayfasının URL ve alan adı bilgileri, bu sayfanın kategorisi, bu sayfa ile gerçekleşen bağlantıdan üretilen verinin büyüklüğü bilgileri yer almaktadır. Bu tez çalışması için orijinal veri setinden yarı sentetik veri seti üretilmiştir. Yarı sentetik veri seti, aslına uygun olan, sistem testlerinde kullanılan, orijinaline göre içeriği değişebilen ancak formatı değişmeyen veri setlerine verilen isimdir. Orijinal veri setindeki bilgiler aynen korunmuş bunlara ek olarak yeni sütunlar eklenmiştir. Bunlar, işletim sistemi, tarayıcı ve DNS sunucu bilgileridir. En çok kullanılan 6 işletim sistemi, 5 tarayıcı ve 3 farklı tür DNS sunucusuna göre, bu ürünlerin [35] de yer alan kullanım istatistiklerine göre sistem tarafından kullanıcılara atanmıştır. Böylece, kullanıcının ziyaret ettiği web sayfası, kullandığı cihazın işletim sistemi, tarayıcı, DNS sunucu ve yerel ağda aldığı IP adresi bilgileri veri setinde ve bir dosya kayıt türü olan CSV (virgülle ayrıştırılmış değerler) formatında incelenmek üzere hazırlanmıştır. Kullanıcı analizi 4 alt grupta tanımlanmıştır. Bunlar; internet erişim analizi, işletim sistemi analizi, tarayıcı analizi ve DNS sunucu analizidir. En temelde, her analizden veri setindeki ilgili veriye dayanarak skorlar üretilmiştir. Üretilen bu skorlar analizlerle belirlenen ağırlık değerleri ile toplanmış ağırlıklı ortalama yöntemi ile kullanıcı skorları üretilmiştir ve bu skorlara göre kullanıcılar 6 farklı gruba ayrılmıştır. Ardından, literatürde en çok kullanılan kümeleme algoritmalarından olan K Means Kümeleme [36] yöntemi ile kullanıcılar kullanım, web tarayıcı, işletim sistemi ve DNS sunucu skorlarına göre 6 farklı kümeye bölünmüştür. Bu iki skor karşılaştırılarak artıları, eksileri belirtilmiş, zararlı veya tehlikeli kullanıcıları ayırt

etmede güçlü ve zayıf oldukları noktalar deklare edilmiştir. Alt analiz gruplarının çalışma şekilleri aşağıda açıklanmıştır.

4.1.1 İnternet Erişim Analizi

URL kayıt dosyalarında, kullanıcıların ağ üzerinde aldıkları yerel IP adresleri ile ayırt edilerek hangi sitelere erişim sağladıkları bilgisi mevcuttur. Bu bilgilere bakarak kullanıcıları analiz etmek mümkündür. Dahası bu çalışmada kullanılan verilerde yer alan web sitesi kategorileri, kullanıcı ve kullanım analizini kolaylaştırmış ve kapsamını artırmıştır. Kullanıcıların yoğun olarak kullandıkları sitelere ve kategorilerine bakarak kullanıcı eğilimlerini görmek de mümkündür. Böyle çıkarımlar internet üzerinden reklam ve pazarlama uygulamalarında sıkça yapılmaktadır [14]. Ulusal güvenlik alanında yapılacak böyle bir çalışma toplumların internet eğilimlerini ortaya çıkarmakta etkili olabilir. Bu tez çalışmasında kullanıcıların erişim sağladıkları web sitelere ve bu sitelerin kategorilerine göre, her kullanıcı için ayrı olmak üzere, kullanım skoru çıkarmak hedeflenmiştir. Kullanım skoru ağ güvenlik skorundaki en yüksek etkiye sahip skordur. Web sayfalarının kategorilerine göre her erişim sağlanan web sayfası için kullanıcıya ayrı ayrı 1 ile 3 arasında skor verilmesi, bu skorların toplanması ve ilgili kullanıcının tüm erişimleri skorlandığında bu skorun tüm erişime bölünerek ortalama kullanım skorunun kullanıcı için hesaplanması hedeflenmiştir.

Web sayfalarının skorları kategorilerine göre 1 ile 3 arasında değişmektedir. Sayfaların en yüksek skorun sistemin eşik değeri olan3 olmasının sebebi, herhangi bir web sayfasına girmenin sisteme olumlu bir katkısı olmayacağı düşüncesiyle kullanıcının ortalama kullanım skorunu yukarılara çekmemesi içindir. Örneğin, bir kullanıcı arama motoruna girdiği için skor olarak 4 almış olsa, kullanıcının arama motorunu kullanması ağ güvenlik skoruna olumlu katkı sağlıyor demek olur ki gerçekte böyle bir durum söz konusu değildir. Bir web sayfasına erişim sağlamak en iyi ihtimalle kullanıcı veya ağ güvenliği açısından tehlike arz etmiyor demektir. Diğer tüm durumlarda da zaten kullanıcı zararlı olabilecek bir web sayfasına erişim sağlamış demektir. Bu yüzden web sayfalarına en yüksek skor olarak ağ güvenlik sisteminin vasat skoru olan 3 verilmiştir. Kullanıcı erişimlerinin büyük bir kısmını

oluşturan, sistem tarafından zararsız olarak nitelendirilen kategorilere dahil olan web sayfalarına yapılan kullanıcı erişimleri sistemi olumlu ya da olumsuz etkilememiştir. Ağ güvenlik skorlama sisteminin hedef kategorileri zararlı olabilecek kategorilerdir. Bu kategorilere dahil olan web sayfalarına ziyaretlerin her birinden kullanıcılara 3'ün altında skor verilmiştir. Böylece tehlike arz eden web sayfalarına kullanıcılar tarafından yapılan her bir erişim kullanıcı skorunu düşürmüş dolayısıyla ağ güvenlik skorunu olumsuz etkilemiştir. 40 kategori içinden skoru 3'ün altında olan, zararlı olabilecek web sayfalarını içeren kategoriler aşağıdaki çizelgede verilmiştir.

Çizelge 4.1 Potansiyel Zararlı Kategoriler ve Sistem Skorları

Zararlı Olabilecek Kategoriler	**Skorları**
Zararlı Yazılım/Virüs	1
Potansiyel Tehlikeli	2
Pornografi	1
Kumar	2
Bilinmeyen	1
Reklam	2

Özetle kullanım skoru, kullanıcının erişim sağladığı web sayfasının kategori skoruna göre her erişim için ayrı ayrı skor alarak bu skorların toplanması, sonrasında toplam erişime bölünmesiyle elde edilmektedir. Örneğin, XYZ kullanıcısının incelenen ağ üzerinden erişim sağladığı web sayfalarının erişim sayıları ve kategorileri aşağıdaki gibi olsun;

- 2 defa Kumar
- 3 defa Bilinmeyen
- 4 defa Arama Motoru

XYZ'nin kullanıcı skoru = ((2 x 2) + (3x1) + (4x3)) / 9 şeklinde olur. Böylece bu bölümün sonunda her kullanıcı için kullanım skorları ve ortalama kullanım skoru bilgileri elde edilmiş olur. Bu bölüm için kullanım skorları hesaplanırken standart sapma yöntemi de denenmiştir fakat bu yöntemin etkili olmadığı görülmüştür. İstatistik alanında kullanılan standart sapma yöntemi ile incelenen verideki değişimlere bakarak önemli çıkarımlar yapmak mümkündür. Ancak, bu çalışmada sürekli zararlı web sayfalarına erişim sağlayan kullanıcıların standart sapmaları düşük olacağı halde zarar potansiyelleri yüksek olacaktır, böyle kullanıcıları ayırt etmekte etkili olmayacağı için standart sapma yöntemi kullanılmamıştır. Yine de daha sonra incelenmek üzere, standart sapmalar hesaplanarak, son rapora eklenmiştir.

4.1.2 İşletim Sistemi Analizi

İşletim sisteminde bulunan açıklar sayesinde kötü niyetli kullanıcılar bilgisayar sistemlerine zarar verebilmektedir [37]. İşletim sisteminin çalışma şekli, kullanıcı grupları, kullanım amaçları gibi sebepler saldırıların türünü, şeklini ve sıklığını değiştirmektedir. Elektronik cihazlardaki işlem yönetimi, dosya yönetimi gibi işletim sistemlerinin sorumluluğunda olan görevler üzerinden farklı formlarda tehdit ve tehlikeler mevcuttur [37]. Ağ üzerinden yapılan siber saldırıların büyük bir kısmı en çok kullanılan işletim sistemlerini hedef almaktadır. Daha fazla kullanıcıya zarar verme potansiyeli olduğu için saldırganlar böyle bir yol izlemektedirler. Özellikle mobil telefonların işletim sistemleri ve güvenlikleri ciddi tehdit altındadırlar[38]. Oldukça fazla kullanıcıya sahip olmaları, kullanıcıların günlük yaşantılarında oldukça sık kullanmaları, cihaza uygulama üretme ve yükleme yöntemlerinde yeterince denetlenmemesi, kullanıcıların uygulama tercihlerindeki bilinçsizlik mobil cihazların işletim sistemlerindeki tehditlerin önemli sebeplerindendir.

Çalışmada kullanılan veride yer alan işletim sistemleri [35]' de yer alan istatistiklere göre en çok kullanılan masaüstü ve mobil cihaz işletim sistemlerinin arasından 6 işletim sistemi olarak seçilmiştir. İşletim sistemlerine verilen skorlar sahip oldukları güvenlik açıklarına göre verilmiştir. Amerika merkezli 'Ulusal Veri Tabanı' [39] tarafından tespit edilen güvenlik açıkları üzerinden skorlama yapılmıştır. [40]' de yer

alan ve [39]'daki bilgileri kullanılarak oluşturulmuş, işletim sistemlerinin marka ve modellerine göre yapılan analizlerden faydalanılmıştır. Sadece sistem açıklarına bakılmasının ve buna göre skorlama yapılmasının nedeni, ağ üzerinden yapılan saldırıların hangi işletim sistemine ne kadar saldırı olduğunun metriğini çıkarmakta ki zorluk ve saldırıların asıl nedeninin işletim sistemi olmamasıdır. Çünkü, işletim sistemi tüm güvenlik önlemlerine sahip olsa, hiçbir sistem açığı olmasa dahi kullanıcı faktörü ile herhangi bir saldırı tehditti ile karşı karşıya gelebilir. Böylece, ağ güvenliği için işletim sistemi noktasında değiştirilecek çok parametre olmasa da ağ yöneticilerinin yapabilecekleri, kullanıcılara olanak sağlayarak anti virüs programlarının yaygınlaşmasını sağlamaktır [31]. Aşağıdaki çizelgede işletim sistemleri ve işletim sistemlerine atanan skorlar gösterilmiştir.

Çizelge 4.2 En Çok Kullanılan 6 İşletim Sistemi ve Sistem Skorları

İşletim sistemleri	**Skorları**
Linux	3,50
Windows 7	4,50
Android	3,30
IOS	4,00
Mac OS X	3,70
Windows 10	4,30

4.1.3 Web Tarayıcı Analizi

Web tarayıcıları kullanıcılar için bilgisayarlar, mobil telefonlar, tabletler gibi elektronik cihazların internete açılan yüzü olarak tanımlanabilir. İnternette yer alan bilgileri görülebilir, okunabilir, duyulabilir hale getiren, bir nevi internetin kullanıcı ara yüzü denilebilecek yardımcı programlardır. Ağ protokollerinin tümüyle uyumludur ve e-posta almadan, dosya indirip yüklemeye tüm işlemleri kullanıcının gerçekleştirmesine olanak sağlar. 'World Wide Web' in doğmasıyla birlikte kullanım

için bir tarayıcı ihtiyacı hasıl olmuş, böylece de 'Mosaic' isimli ilk tarayıcı üretilmiştir[41]. National Center for Supercomputing Applications (NCSA) [42] tarafından sunulan mosaic web sayfalarında görüntüleri gösterebilmekteydi. Netscape ürünü de ilk ticari tarayıcı olarak üretilmiştir [41].

Web tarayıcı güvenlik açıklarından faydalanılarak cihazlara ve sistemlere siber saldırılar düzenlemek mümkündür. Çapraz site saldırısı, oturum korsanlığı ismi verilen saldırılarla kullanıcıların cihazlarına sızma, hırsızlık gibi işlemler gerçekleştirilmektedir [43]. İşletim sistemi skorlama da olduğu gibi, bu adımda da web tarayıcılara skor ataması yapılmıştır. En çok kullanılan 5 tarayıcı seçilmiştir[35]. Skorlar yine işletim sisteminde olduğu gibi, [40]' daki çalışmada yer alan bilgilere göre web tarayıcı güvenlik açıkları baz alınarak verilmiştir . Bilinen tarayıcıları tercih etmek ağ güvenliği açısından önemlidir. Cihaz üzerinde çalışan ve internet üzerinde üretilen tüm veriye hakim olan web tarayıcılardan güvenli olanı tercih etmenin önemi şüphesizdir. Aşağıdaki çizelgede en çok kullanılan 5 web tarayıcısı ve sistem tarafından onlara verilen skorlar gösterilmiştir.

Çizelge 4.3 En Çok Tercih Edilen 5 Web Tarayıcı ve Sistem Skorları

Web Tarayıcıları	**Skorları**
Chrome	4,50
Internet Explorer	3,00
Firefox	5,00
Safari	3,50
Opera	4,00

4.1.4 DNS Sunucusu Analizi

Alan adı sistemi uygulama katmanında yer almasına rağmen internetin mimarisinin yapıtaşlarından biridir. İnternet hiyerarşisinde kritik bir görev üstlenmiştir. Alan adı

sistemi IP adresleri ile alan adları bağlantısını kuran sistemdir. IP, Türkçe manası İnternet İletişim Kuralları olan 'Internet Protocol' ün kısaltılmış halidir. IP adresleri internette web sitelerini ve kullanıcıları ayırt etmede kullanılan, numara bloklarından oluşan, belirli bir protokole dayanan, kimlik benzeri yapılardır. İnternetteki tüm web sayfalarının kendilerine has bir IP adresleri vardır ve internete bağlanan tüm kullanıcılara da IP adresi atanır. IPv4 ve IPv6 sırasıyla İnternet Protokol Versiyon 4 ve İnternet Protokol Versiyon 6 anlamına gelen, günümüzde kullanılan IP adresleme protokolleridir [27]. IPv6 sonradan önerilen protokol olmuştur, çalışma mantıkları benzerdir ancak IPv6 versiyon 4'ün geliştirilmiş formudur. İnsanların web sayfalarının IP adreslerini akıllarında tutamayacakları temel düşüncesi ile, web sayfaları içerik ve kullanım amaçlarına göre farklı uzantılı isimleri almak zorundadırlar. Böylece web sayfalarına tarayıcı üzerinden isim ve uzantısını girerek erişim sağlamak mümkün olmaktadır. İnternete bağlandığımız cihaz ile web sayfasını hizmete sunan cihaz arasındaki bağlantı IP adresleri ile sağlanmaktadır, fakat DNS sistemi sayesinde kullanıcılar sadece web sayfalarının isimleri ile muhatap olurlar. DNS sunucularının veri tabanlarında web sayfalarının alan adları, turkiye.gov.tr gibi ve bu adların temsil ettiği IP adresleri, 94.55.118.33 gibi, bulunmaktadır. DNS sunucuları gerekli eşleştirmeyi yaparak gelen talepleri cevaplandırmakta, kullanıcılara erişmek istedikleri alan adı ve bilgisayarın IP adres bilgisini sağlayarak, ilgili web sayfalarına erişimlerinde yardımcı olmaktadırlar [7].

DNS üzerinden yapılan saldırılar oldukça ciddi zararlar vermektedir. Alanlarında dünya devi şirketler de bu saldırılardan nasiplerini almaktadırlar. Örneğin, Amerika'nın en büyük bankalarından Bank of America, haber ajansı Al-Jazeera şirketleri DNS saldırılarının hedefi olmuşlar ve servis yapamaz hale gelmişlerdir [44]. DNS üzerinden yapılan saldırıların çoğunluğunu DDOS saldırıları oluşturmaktadır. DNS önbelleğini bozma, DNS sunucusu gibi davranarak kullanıcıyı zararlı sitelere yönlendirme diğer saldırılardandır. Kullanıcılar DNS sunucularını kullanarak onlara bilgilerini emanet etmektedir ve kendilerini yönlendirmelerine izin vermektedir. Bu yüzden güvenilmeyen bir DNS sunucusu kullanmak büyük bir risktir. Bu çalışmada DNS sunucuları 3 kısma ayrılmıştır.

- İnternet Servis Sağlayıcı DNS Sunucuları
- Bilinen DNS Sunucuları
- Bilinmeyen DNS Sunucuları

Ev ve işyerlerinde internet hizmeti aldığımız şirketlere İnternet Servis Sağlayıcı denmektedir. Kurulumundan yapılanmasına kadar tüm teknik detaylarından bu şirketler sorumludur. İnternete bağlanmak için kullanıcıya atanan IP adreslerini de servis sağlayıcılar kendileri için ayrılmış olan havuzdan sağlarlar. Tüm internet protokol işlemlerini sorumluluklarındadır. Genellikle kendi DNS sunucuları vardır. Sürekli denetim altında oldukları, hizmet verdikleri ülkenin yasalarına uyma zorunlulukları olduğu için, ticari bir yapı olarak müşteri güveni ve memnuniyetini esas alarak çalışma zorunluluklarına dayanarak en güvenli DNS sunucu internet servis sağlayıcı DNS sunucuları olarak belirlenmiştir. Cihazda tercih edilen DNS sunucusu otomatik seçeneğinde ise kullanılan DNS sunucusu servis sağlayıcı DNS sunucusudur. Bu sunucuya sistem tarafından atanan ve en yüksek DNS skoru olan '4.5' tir. Kullanıcı internet servis sağlayıcı DNS sunucusunu kullanması ağ güvenliği skoruna olumlu katkı sağlamaktadır.

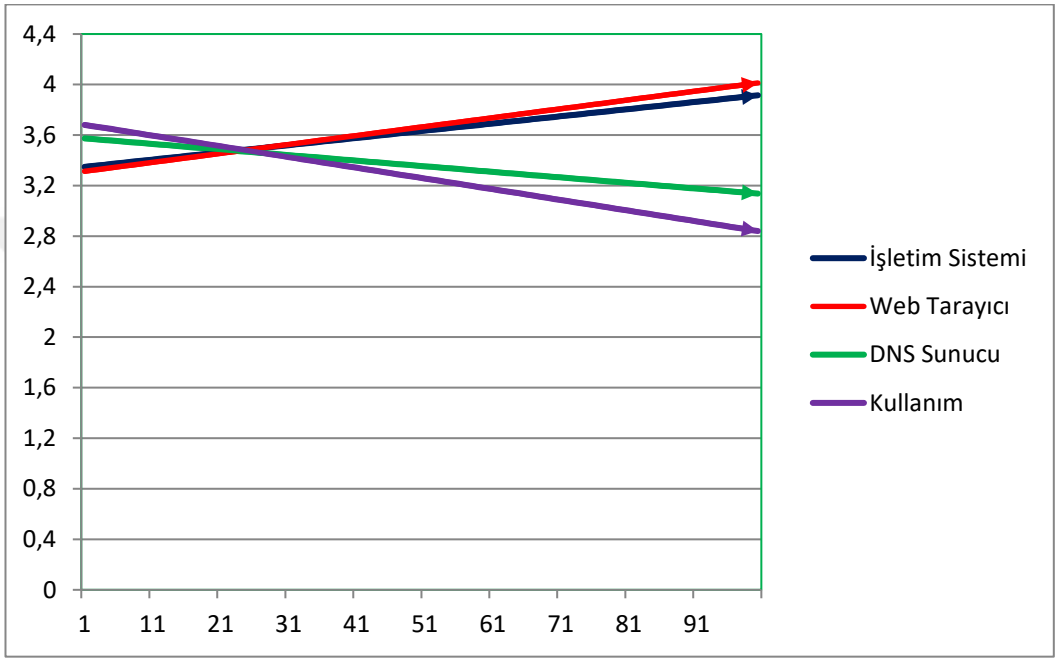
Bilinen DNS sunucuları, teknoloji ve internet alanında hizmet veren dünyaca ünlü şirketlerine ait sunuculardır. Büyük bir kısmı ücretsiz olmasına rağmen ücretli DNS sunucuları da mevcuttur. Google DNS [45], Open DNS [46], Norton DNS [47] internette en çok bilinen, ücretli ve ücretsiz DNS sunucu hizmeti ürünleridir. İnternet kullanıcılar DNS sunucularını genellikle yasaklı sitelere giriş imkânı olarak kullanılan bir araç olarak kullanmaktadır. Yukarıda belirtildiği gibi servis sağlayıcılar ülkenin mahkeme kararlarına uymak zorundadır, eğer bir web sayfasına erişim mahkeme kararı ile engelli ise servis sağlayıcı DNS sunucuları ile o sayfaya erişim sağlanamaz. Ancak, ücretsiz, halka açık DNS sunucuları yoluyla böyle sitelerin IP bilgisine erişerek bu sitelere girmek mümkündür, bu yüzden de kullanıcılar DNS tercihlerini mahkeme kararı ile yasaklanan sitelere girmek istedikleri zaman değiştirdikleri için DNS sunucularını yasak delici olarak görmektedirler. Güvenilir, tutarlı şirketlerin sunmuş olduğu bilinen DNS sunucularını kullanmak da güvenlidir [48]. Bu yüzden bilinen DNS sunucularının skoru '4' tür.

Bilinmeyen DNS sunucuları kullanıcılar için ciddi tehditler arz edilmektedir. Web sayfalarına kılavuzluk eden yardımcı bir birim gibi çalışan DNS'ler kullanıcıları talep ettikleri adrese yönlendirebileceği gibi yanlış yollara da saptırabilir. Kullanıcıları güvenlik açıkları ile karşı karşıya getirebilir [44]. Ağ üzerindeki kullanıcıların internet erişimlerinde bilinmeyen DNS sunucularını kullanmaları ağları da tehdit altında bırakmaktadır. Özellikle DNS üzerinden yapılacak DOS saldırıları ile ağı hizmet veremez hale getirmek en büyük tehlikedir. Bu yüzden bir kullanıcının bile bilinmeyen DNS sunucularından hizmet alması, ağ için kötü haberdir, ağ içeriden bir açık oluşmuş demektir. Bilinmeyen DNS sunucuların sistem skorları '1'dir. Bunun anlamı, bilinmeyen DNS sunucusundan hizmet alan bir kullanıcı kullanım ve ağ güvenlik skorunu ciddi oranda düşürmektedir. DNS sunucu skorlarının ağ güvenliği skoruna etkisi, işletim sistemi skorları ve tarayıcı skorlarının toplam etkisine eşittir. Yukarıda sayılan tehditlere ve DNS sunucularının tehlike potansiyeline bakılarak böyle bir skor ağırlığı belirlenmiştir. Kullanıcılara önerilecek en iyi tercih, servis sağlayıcının DNS sunucularını seçmeleridir. Eğer başka bir DNS sunucu kullanmaları gerekiyor ise de bilinen DNS sunucularını tercih etmeleri oldukça önemlidir.

4.1.5 Skorların Kullanıcı Skoruna Yüzdesel Etkisi

Bu aşamaya kadar kullanım, işletim sistemi, web tarayıcı ve DNS sunucu skorları ayrı ayrı incelenerek üretilmektedir. Bu skorların birleştirilmesi ile kullanıcı skoru çıkarım yöntemlerinden ilki olan ağırlıklı ortalamaların hesaplanması yöntemi ile kullanıcı skorları üretilmektedir. Her bir skor için kullanıcı skoruna yüzdesel etkisi incelenmektedir. Örneğin işletim sistemi skorunun yüzdesel etkisine başlangıç değeri olarak 0 verilmiştir. Diğer skorların yüzdeleri eşit verilerek, son kullanıcı skorları üretilmiştir. Bu adım işletim sistemi yüzdesel etkisi 100' e gelene kadar 100 defa tekrarlanmıştır, her adımda işletim sistemi skorunun yüzdesel etkisi artarken diğer 3 skorun yüzdeleri düşürülmüştür. Tüm kullanıcıların her yüzdedeki ortalama skorları hesaplanmıştır. İşletim sistemi yüzdesi 0 ve 100 de iken üretilen kullanıcı skorlarına bakılmıştır ve kullanıcı skorunun yüzdesel değişimi hesaplanmıştır. Bu adım diğer 3 skor için de tekrar edilmiştir. Skorların kullanıcı skoruna etkileri şekil [4.1] de

verilmiştir. Son olarak hesaplanan yüzdesel değişim değerleri dört skorlama adımı göz önünde tutularak toplam yüzdesel etkinin hesaplanabilmesi ve ağırlıklı ortalama kullanıcı skoru için ağırlıkların belirlenmesi için 100'e göre normalize edilmiştir.



Şekil 4.1 Skorlama Adımlarının Yüzdesel Değişimine Göre Kullanıcı Skorundaki Değişim

Şekil 4.1' deki grafiğe göre kullanım ve DNS skorları kullanıcı skorlarını azaltırken, işletim sistemi ve web tarayıcı skorları da artırmıştır. Yüzde 23 ile 3.4 skoru noktasında skorların kesiştiği görülmektedir. Bu noktadan sonra işletim sistemi ve web tarayıcı skorları kullanıcı skorunu 4 civarına çekerken, DNS sunucu ve kullanım skorları kullanıcı skorunu sistemin eşik değeri 3'ün altına doğru çekmektedir.

4.1.6 K Means Kümeleme ve Ağırlıklı Ortalama Hesaplama Yöntemleri ile Kullanıcıların Gruplandırılması

Kullanıcıların gruplandırılarak zararlı veya şüpheli kullanıcı gruplarının sonrasında ise bu gruplara dahil olan kullanıcıların tespit edilmesi hedeflenmektedir. Bunun için K Means kümeleme ve Ağırlıklı Ortalama Hesaplama yöntemleri kullanılmıştır.

K Means kümeleme yönteminde birbirine en çok benzeyen değerlerin aynı kümede yer alması ve kümelerin birbirine benzememesi hedeflenmektedir. Bunun için istenilen sayıdaki sınıfların merkezleri belirlenir, örnekler mesafelere göre sınıflandırılır, oluşan sınıfların merkezleri değerlere göre güncellenir ve istenilen sınıflar elde edilinceye kadar ikinci ve üçüncü adımlar tekrar edilir. Bu çalışmada K Means kümeleme yönteminin verilen değerlere göre kullanıcıları altı farklı sınıfa bölmesi amaçlanmaktadır. Böylece zararlı, şüpheli ve zararsız kullanıcılar sınıflandırılarak zararlı ve şüpheli kullanıcılar diğerlerinden ayırt edilebileceklerdir. Ağırlıklı Ortalama Hesaplama yönteminde ise kullanıcılar önceki adımlarda üretilen kullanım, işletim sistemi, web tarayıcı ve DNS sunucu skorları, bu skorların kullanıcı skoru üzerindeki yüzdesel değişim etkisi göz önünde bulundurularak birleştirilmesiyle kullanıcı skoru üretilmektedir. Buna göre:

- Kullanım %39.22
- İşletim Sistemi %19.19
- DNS sunucu %18.46
- Web Tarayıcı %23.11

Oranları ile çarpılarak kullanıcı skorları ortaya çıkartılmaktadır. Üretilen bu skorlara göre kullanıcılar K Means kümeleme yönteminde olduğu gibi kullanıcılar zararlı, şüpheli ve zararsız sınıflara ayrılmaktadır.

4.2 Ağ Güvenlik Ekipmanları Skorlama

Günümüzde, ağ güvenliğinde kritik rol oynayan yazılım ve donanım ürünleri bulunmaktadır. Ağların güvenilirliği, sürdürülebilirliği ve tutarlılığı böyle ürünlerin varlığına bağlıdır. Gün geçtikçe artan siber saldırılara karşı şirketler ve kurumlar bu güvenlik ürünleri ile maddi manevi kayıpları önlemeye çalışmaktadır. Kurumların ve şirketlerin güvenlik ürünlerine ödedikleri ücretler, saldırı olması durumunda uğrayacakları kayıpların yanında çok az bir miktarı teşkil etmektedir. Bu tez çalışmasında da ağ güvenliği için kullanımın yol açabileceği zararın önemi kadar ağ

güvenliği ekipmanlarının da faydaları ve ağ güvenliğine olan katkıları vurgulanmaktadır. Sisteme önceden tanımlanan ağ güvenlik ürünlerinin önemine göre skorlandırmalar yapılmış olup, tümünün varlığı halinde sistemin en yüksek skoru olan 5 ağ güvenliği ekipmanları skoruna verilecektir. Tanımlanan güvenlik ürünleri ve skorları aşağıdaki tabloda verilmiştir.

Çizelge 4.4 Sistemde Karşılaştırılan Ağ Güvenlik Ekipmanları ve Skorları

Ağ Güvenlik ekipmanları	**Skorlar**
Güvenlik Duvarı	2
Zararlı Yazılım Önleyici Araçlar	0.5
Sanal Özel Ağ – VPN	1
URL Filtreleme	0.5
Spam Engelleyici Yazılım	0.5
İzinsiz Giriş Tespit Sistemi	0.5

Sistem, ağ güvenlik ekipmanları skoru sisteme artı skor katmak üzere tasarlanmıştır. Özellikle ağı filtreleyen güvenlik duvarı ve dışarıdan ağa erişim sağlarken şifreli güvenli bir erişim yolu sağlayan VPN ürünlerinin günümüz ağlarında olmazsa olmaz ürünler olduğu gerçeğiyle skora katkıları %60 seçilmiştir. Yani, sadece bu iki ürüne sahip ağdaki ekipman skoru, ağ güvenlik skorunun vasat skoru olan 3'ü yakalamış oluyor. Diğer ürünler de önemli olmakla birlikte olmaları durumunda ağ güvenlik skorunu daha yüksek seviyelere taşımaktadır.

Tüm ortalama skorların bulunduğu bu bölümün sonunda ağ güvenlik skoru oluşturulmaktadır. Ağ güvenlik skoru üzerinde kullanıcı skorlarının %60, ağ güvenlik ekipmanları skorunun %40'lık ağırlıklı etkisi bulunmaktadır. Kullanıcı skorlarının düşüklüğüne göre ağ güvenlik ürünleri kullanılırsa, böylece gerekli

önlemlerin alınması ile ağın güvenliğinin sağlanacağı gerçeği bölümlerin ağ güvenlik skoruna etkileri ile vurgulanmaktadır.

4.3 Ağ Güvenliği Skorlama Simülatörü

Önceki bölümlerde anlatılan sistemin kurgulanması için ağ güvenlik skorlama simülatörü geliştirilmiştir. C# programlama dilinde geliştirilen simülatör raporları, grafikleri ve sonuçları çıkartmak üzere tasarlanmış bir ara yüz programıdır. Sistemi test etmek için üretilen sentetik veri seti de bu simülatör programı ile oluşturulmaktadır. Çalışma mantığını daha iyi açıklama adına, programın yalancı kodu aşağıda verilmiştir.

```
Start
      get input
      methodanalyze_user
            submethodanalyze_usage
            submethodanalyze_os
            submethodanalyze_brw
            submethodanalyze_dns
      methodanaylzetools
      extractten_users_by_usage
      extract_ten_users_by_total
      create scores
      plot diagrams
      create reports
End
```

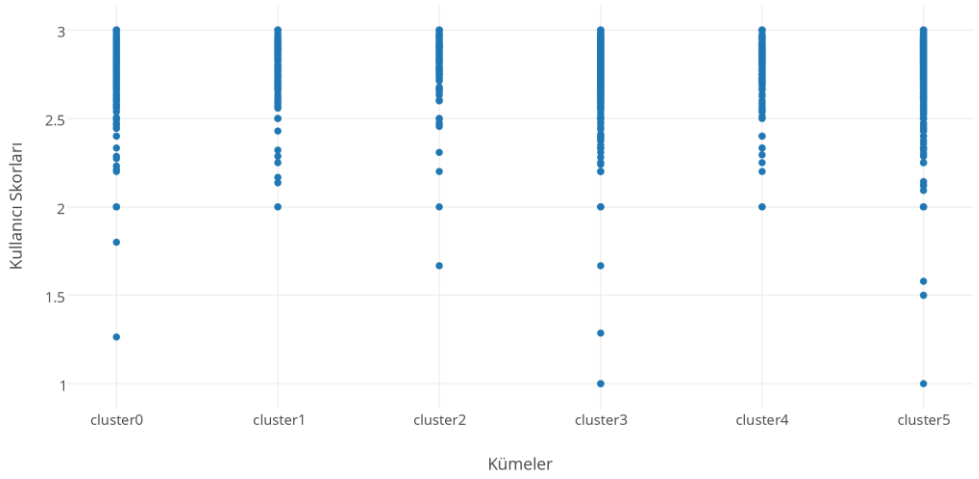
5. DENEYSEL SONUÇLAR

Bu bölümde, tez çalışmasında önerilen ağ güvenliği skorlama sistemine sentetik veri seti uygulanarak elde edilen sonuçlar açıklanmıştır. Ayrıca, kullanıcı eğilimleri de grafiklerle detaylı olarak açıklanmıştır. Sistem tarafından üretilen skorlar değerlendirilmiş ve yorumlanmıştır. Skorların iyileştirilmesi için yapılabilecekler de yine bu bölümde yer almaktadır. Ağ güvenlik skorlama sistemini test etmek amacı ile kullanılan sentetik veri seti ile 2697 farklı kullanıcı incelenmiştir. 40 farklı kategoriye ayrılan web siteleri, altı farklı işletim sistemi, beş farklı web tarayıcı ve üç farklı DNS sunucu incelenmiştir. Ağ güvenlik skoru ve diğer sonuçlar aşağıda açıklanmıştır.

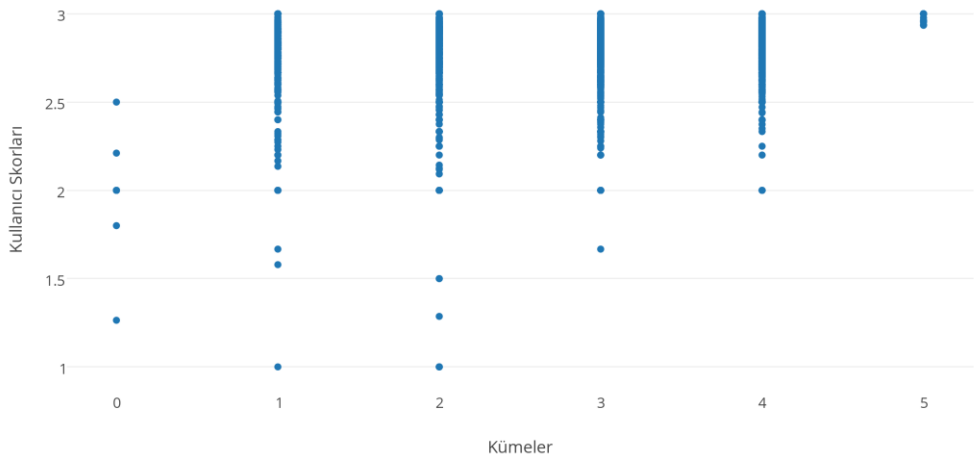
5.1 Kullanıcı Skoru Sonuçları

Sistemin temel amacı olan ağ güvenlik skoru kullanıcıların; internet erişim davranışı, kullandığı işletim sistemi, DNS sunucusu ve web tarayıcı puanlarının hesaplanması ve ağ güvenlik araçlarının puanlanması ile oluşturulmuştur. Öncelikle bunlara yukarıdaki çizelgelerde verilen puanlara göre puanlar atanmıştır. Örneğin, bir kullanıcının işletim sistemi tercihi Linux ise işletim sistemi skoru 3.5, web tarayıcı olarak Firefox kullanıyorsa web tarayıcı skoru 5, bilinen DNS sunuculardan birini tercih etmişse DNS sunucu skoru 4olur ve ağ üzerinden sadece arama motoru sitelerine erişim sağlamışsa kullanım skorundan da 3 almıştır. Her kullanıcı için bu işlem tekrar edilerek tüm kullanıcıların skorları hesaplanmıştır ve tutulmuştur. Sonraki adımda tutulan bu değerlerden ortalama kullanım skoru, ortalama işletim sistemi skoru, ortalama DNS sunucu skoru ve ortalama web tarayıcı skoru hesaplanmıştır. Sonraki adımda hesaplanan bu skorların kullanıcı skoruna yüzdesel etkileri hesaplanmıştır. Bu adımdan sonra ağırlıklı ortalama hesaplama yöntemi ile kullanıcı skorları çıkarılmış ve bu skorlara göre kullanıcılar 6 farklı sınıfa bölünmüştür. İlk dört adımda üretilen skorlar K Means kümeleme yöntemi ile de kullanıcılar 6 farklı sınıfa ayrılmıştır. Her iki hesaplama yöntemi için de 0 ve 1 numaralı gruplar zararlı, 2 ve 3 numaralı gruplar şüpheli son olarak da 4 ve 5 numaralı gruplar da zararsız kullanıcıların yoğun olduğu grupları temsil etmektedir. Ağırlıklı ortalama hesaplama yöntemi ile elde edilen sonuçlara göre, 0 ve 1 numaralı

gruplar tüm kullanıcıların %14'ünü, şüpheli kullanıcılar %53.3'ünü ve zararsız kullanıcılar %32.7'sini oluşturmaktadır. K Means kümeleme yönteminden elde edilen sonuçlara göre ise, tüm kullanıcıların, zararlı kullanıcılar %20.6'sını, şüpheli kullanıcılar %41.6'sını ve zararsız kullanıcılar %37.7'sini teşkil etmektedir. İncelenmesi gereken gruplar olan zararlı ve şüpheli kullanıcı grupları iki yöntem de de birbirine yakın çıkmıştır. Ağırlıklı ortalama hesaplama yönteminde elde edilen gruplarda zararlı kullanıcı grupları yüzdesel olarak K Means kümeleme yöntemi ile elde edilen gruplardan daha azdır. Ancak, şüpheli kullanıcı gruplarındaki kullanıcı yoğunluğu daha fazla olmuştur. Aşağıdaki şekillerde (Şekil 5.1 ve 5.2) her iki yöntem için de kullanıcıların skorlarına göre sınıf dağılımları gösterilmiştir.



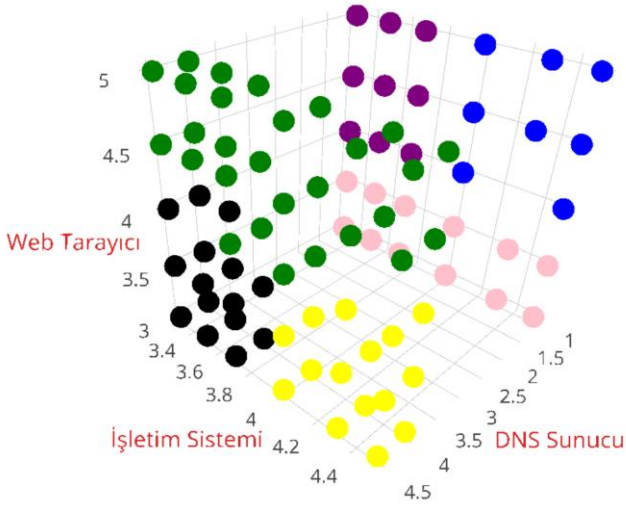
Şekil 5.1 K Means Kümeleme Yöntemi ile Kullanıcı Skoruna Göre Kullanıcı Yoğunluğu



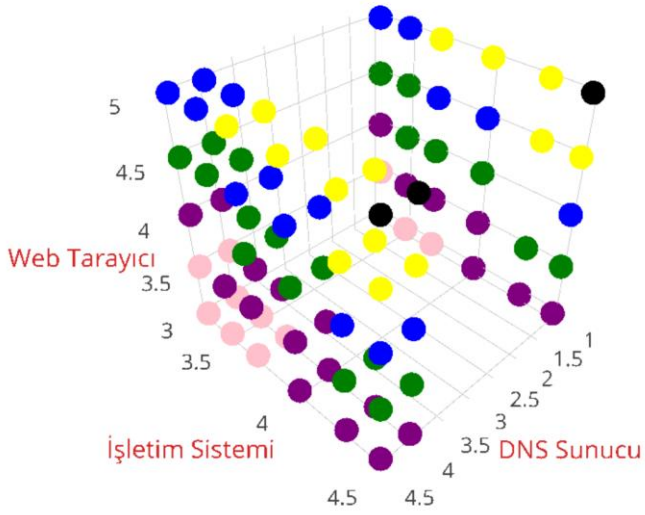
Şekil 5.2 Ağırlıklı Ortalama Hesaplama ile Kullanıcı Skoruna Göre Kullanıcı Yoğunluğu

Şekillere (Şekil 5.1 ve 5.2) bakıldığında, ağırlıklı ortalama hesabı ile elde edilen gruplardaki standart sapmaların düşük olduğu görülmektedir. Böylece, zararsız kullanıcı gruplarında zararlı kullanıcılara, zararlı gruplarda da zararsız kullanıcılara rastlama ihtimali düşüktür. Diğer yandan, K Means kümeleme yöntemi ile elde edilen grafiğe bakıldığında zararsız veya şüpheli kullanıcı gruplarında oldukça düşük skorların da yer aldığı görülmektedir. Bu bağlamda ağırlıklı ortalama skorunun zararlı ve zararsız kullanıcıları elde etme de daha etkili olduğu söylenebilir. Ancak, K Means kümeleme algoritması benzer kullanıcıları aynı gruplara atacağı için sistemde birbirine çok yakın kullanıcılar üzerinde ikilem yaşanma olasılığı düşüktür.

K Means kümeleme yöntemi ve Ağırlıklı Ortalama Hesaplama yöntemi ile elde edilen sınıflandırmalar farklı açılardan da karşılaştırılmıştır. Kullanıcıların ağ üzerinden erişim sağladığı web sayfalarına göre hesaplanan internet erişim skorları ayrı tutularak, işletim sistemi, web tarayıcı ve DNS sunucu skorları her iki yöntemle de sınıflandırılmıştır. Şekil 5.3 ve 5.4' de 3 boyutlu grafiklerle gösterilen bu sınıflandırılma işleminin sonuçları aşağıda verilmiştir.

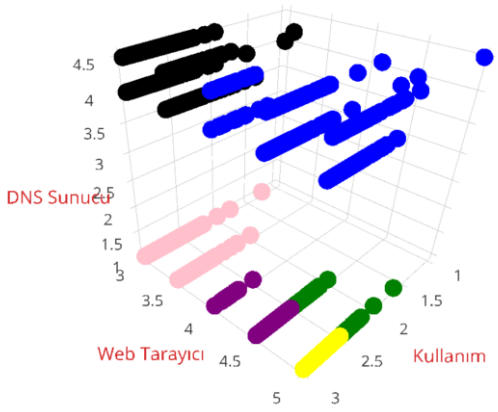


Şekil 5.3 Web Tarayıcı İşletim Sistemi ve DNS Skoru ile K Means Kümeleme Yöntemiyle Kullanıcı Sınıfları

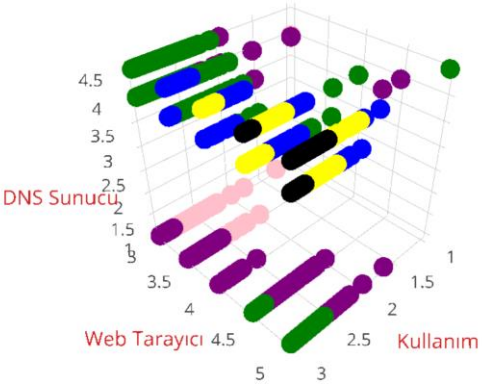


Şekil 5.4 Web Tarayıcı İşletim Sistemi ve DNS Skoru ile Ağırlıklı Ortalama Hesaplama Yöntemiyle Kullanıcı Sınıfları

Grafiklerde önceki bölümlerde olduğu gibi pembe ve mor renkler zararlı, yeşil ve mavi renkler şüpheli ve sarı ve siyah renkler de zararsız kullanıcıları temsil etmektedir. K Means kümeleme yönteminde zararlı kullanıcıları gösteren pembe ve mor renkler işletim sisteminden ve web tarayıcı skorundan bağımsız DNS sunucu skorlarının düşük olduğu bölgelerde yoğunlaştığı görülmektedir. Ağırlıklı ortalama hesaplama yöntemine göre ise pembe ve mor renkli zararlı kullanıcılar düşük web tarayıcı ve işletim sistemi skorunun olduğu bölgelerde yoğun olmakla beraber, mor renkli kullanıcılar düşük DNS sunucu bölgelerinde yoğun olarak yer almaktadır. Şüpheli kullanıcı gruplarından mavi renk grubu K Means kümeleme yöntemine göre düşük DNS sunucu skorunun olduğu bölgede yer almaktadır. Yeşil renk grupları da düşük işletim sistemi skorunun olduğu bölgelerde görülmektedir. İkinci yönteme göre şüpheli kullanıcı grupları mavi ve yeşiller grafiğin hemen her bölgesinde yer almaktadır. Buna göre, şüpheli kullanıcılar tek bir skordan ziyade her üç skorun da değişimine göre sınıflandırılmaktadır. Sarı ve siyah renk grupları da K Means kümeleme yönteminde yüksek DNS sunucu bölgelerinde, ağırlıklı ortalama hesabı yönteminde ise önceki gruplar gibi tüm grafik bölgelerine dağılmış durumdadır. Ağırlıklı ortalama hesabı ile yapılan sınıflandırma farklı skorlardaki kullanıcıları zararlı, şüpheli veya zararsız olarak tespit edebilme açısından, K Means kümeleme yöntemine göre yapılan sınıflandırma da her üç skordan birinin düşük olduğu bölgelerde zararsız, şüpheli veya zararlı kullanıcıları sınıflandırmasıyla bu skorların düşüklüğüne veya yüksekliğine dikkat çekmesi açısından daha verimli çalışmaktadır. Son olarak sistemdeki kullanıcıların cihazlarında tercih ettikleri işletim sisteminin tümü için aynı işletim sistemi olur ise sınıflandırmaların nasıl şekilleneceği test edilmiştir. Bu bağlamda yapılan sınıflandırmaların gösterildiği üç boyutlu grafikler (Şekil 5.5 ve 5.6) aşağıda verilmiştir.



Şekil 5.5 Web Tarayıcı İşletim Sistemi ve Kullanım Skorları ile K Means Kümeleme Yöntemiyle Kullanıcı Sınıfları



Şekil 5.6 Web Tarayıcı İşletim Sistemi ve Kullanım Skorları ile Ağırlıklı Ortalama Hesaplama Yöntemiyle Kullanıcı Sınıfları

Şekil 5.5 ve 5.6' da yer alan grafikler incelendiğinde, K Means kümeleme yönteminde zararsız kullanıcılar üç skordan ikisinin yüksek olduğu bölgelerde yoğunlaşmıştır. İkinci yöntemin grafiğinde ise üç skorun da yüksek olduğu bölgelerde zararsız kullanıcıların sınıfları olan sarı ve siyah renkler yoğunluktadır. Şüpheli kullanıcı grupları olan mavi ve yeşil renkler, K Means kümeleme yönteminde skorların yüksek olduğu bölgelerde de görülmektedir. Ağırlıklı ortalama hesabı yöntemindeki sınıflandırmada şüpheli kullanıcılar web tarayıcı skorlarının düşük olduğu bölgelerde yoğunlaşmaktadır. Zararlı kullanıcı sınıfları her iki yöntem

de de DNS sunucu skorunun düşük olduğu yerlerde yoğunlaşmaktadır. Ağırlıklı ortalama yönteminde zararlı kullanıcılar kullanım skorunun düşük olduğu bölgelerde de yüksek DNS sunucu skoruna rağmen, görülmektedir. Grafikler ve veriler incelendiğinde her iki yöntemin de kullanıcıları sınıflandırmada başarılı olduğu görülmektedir. Beklendiği üzere K Means kümeleme yönteminin sınıflandırmayı yakın skorlu kullanıcılar ile yaptığı, ağırlıklı ortalama hesabıyla yapılan sınıflandırmanın ise farklı skorlama adımlarından farklı skor alan kullanıcıları zararlı, şüpheli veya zararsız gruplarına attığı görülmektedir. Böylece, K Means kümeleme yöntemiyle ortaya çıkmayan zararlı kullanıcıların tespit edilmesinin ağırlıklı ortalama hesabıyla yapılan sınıflandırma ile mümkün olduğu görülmektedir.

Daha önce de bahsedildiği üzere, Ağırlıklı ortalama hesaplama yöntemiyle kullanıcıların ayrı ayrı skorları üretilmiştir. 2697 farklı kullanıcının analizi ile üretilen tüm kullanıcıların ortalama skoru ‘2.807661’ bulunmuştur. Bu skor, sistemin eşik değeri olan üç değerinden daha düşüktür. Skora göre sistemde, zararlı ve şüpheli kullanıcı grupları daha çok kullanıcıya sahiptir. Bu kullanıcıların analiz edilip düşük skorların nedenleri tespit edilmeli ve ağda gerekli tedbirler alınmalıdır. Ortalama skorun üçe yakın olması incelenen sistemin güvenilir bir ağ olduğuna da işarettir. Sistem skoru bire yaklaştıkça ağın tehlike seviyesi de artmaktadır. iki veya daha düşük skorlar ağdaki kullanıcıların zararlı web sayfalarına erişim sağladığına, erişim sağladıkları cihazların teknik özelliklerinin güvenlik açısından yeterli seviyede olmadığına işarettir. Böyle ağlar için, ağ yöneticileri acil önlem almalı, kişisel veya kurumsal verileri koruma altına almalıdır. Aşağıda sistemdeki skorlara göre en düşük kullanıcı skoruna sahip 10 kullanıcının skorları çizelge 5.1’de belirtilmiştir.

Çizelge 5.1 En Düşük 10 Kullanıcı Tüm Skorları

Kullanıcı Yerel IP Adresleri	Kullanıcı Analizi Skorları					Toplam Kullanıcı Skorları
	Kullanım Skorları	İşletim Sistemi Skorları	Web Tarayıcı Skorları	DNS Sunucu Skorları	Standart Sapma Skorları	
193.255.169.103	1	3,7	3	1	0	2,2
193.255.163.154	1	4	3	4	0	2,25
193.255.159.130	1,5	4,3	3	4,5	1,98	2,3
193.255.162.117	2	3,5	3	1	1,818	2,417
193.255.167.59	1,264	3,3	3,5	4,5	1,671	2,432
193.255.166.54	1,286	4,5	3	1	1,809	2,476
193.255.164.36	2	4	3	1	0	2,5
193.255.165.141	2	3,3	3,5	1	0	2,508
193.255.165.131	1	3,3	4,5	4	0	2,55
193.255.165.1	2,374	3,3	3	1	0,872	2,57

Çizelgeye göre, toplam kullanıcı skorları düşük olan tüm kullanıcıların kullanım skorları eşik değerinin altındadır. Yani, bu kullanıcılar zarar olabilecek web sayfalarına erişim sağlamıştır. Kullanım skorları 1 olan kullanıcılar ağ üzerinden sadece zararlı olabilecek web sayfalarına erişim sağlamıştır. Düşük skorlu kullanıcıların %60'ı bilinmeyen DNS sunucularını tercih etmeleri de toplam kullanıcı skorlarındaki düşüklüğün başlıca nedenlerindendir. İşletim sistemi ve web tarayıcı skorları toplam kullanıcı skorunu ciddi oranda etkilememiştir. Standart sapma skorları ile yorum yapabilmek zordur, çünkü standart sapma skorları 0 olan kullanıcılar vardır ve bu kullanıcıların kullanım skorları düşüktür. Tam tersi de mümkün olduğu için tutarlı bir yorum yapılamamaktadır. Kullanıcılar tarafından ağ üzerinden zararlı olabilecek kategorilerde yer alan web sayfalarına erişim sayıları aşağıda verilmiştir.

- 952 defa bilinmeyen kategorisindeki web sayfalarına
- 487 defa reklam kategorisindeki web sayfalarına
- 74 defa kumar kategorisindeki web sayfalarına
- 451 defa porno kategorisindeki web sayfalarına
- 2 defa virüs, potansiyel tehlikeli web sayfalarına

Bilinmeyen ve porno kategorileri en çok erişimin sağlandığı kategoriler olmuştur. Kimliği belirsiz web sayfalarına veya ahlak dışı içerikler içeren web sayfalarına kurum ağları gibi ağlardan erişim sağlamak yasak olduğu gibi ciddi de tehlikeler içermektedir. Özellikle porno kategorisindeki erişimlerin tespiti ağ güvenliğinin yanında incelenen kurum veya şirketler için sosyal güvenlik açısından da önemlidir.

5.2 Ağ Güvenlik Skoru Sonuçları

Önceki bölümde anlatıldığı gibi kullanıcılar skorlandıktan sonra sistemi skorlamak için ağ güvenlik araçları skorlanır. Ağ güvenlik araçları skorunun ağ güvenlik skoruna olumlu katkı sağlamak için temel gereksinim; ağın güvenlik duvarı ve VPN ürünlerine sahip olmasıdır. Özellikle güvenlik duvarı olmadan bir ağın güvenliğinden söz etmek pek mümkün görünmemektedir. Bu nedenle bir ağda tüm güvenlik ürünleri olsa ancak güvenlik duvarı olmasa, bu sistemden alacağı en yüksek skor üçü geçmeyecektir. Eğer ağda güvenlik duvarı ve VPN sistemleri kullanılıyor ise, kullanıcı skoru olan ‘2,807661’ ile birlikte ağ güvenlik araçları skorunun birleştirilmesiyle ağ güvenlik skoru ‘2,884596’ e yükselecektir. Böylece güvenli ağa daha da yaklaşmış olacaktır. Dahası, eğer ağ diğer güvenlik ürünleri olan; zararlı yazılım engelleyici araçlar, URL filtreleme, Spam engelleyici, IDS ürünlerine sahip ise skor ‘3,684596’ olacaktır. Bu skor sistemdeki analizlere göre güvenli bir ağı işaret etmektedir.

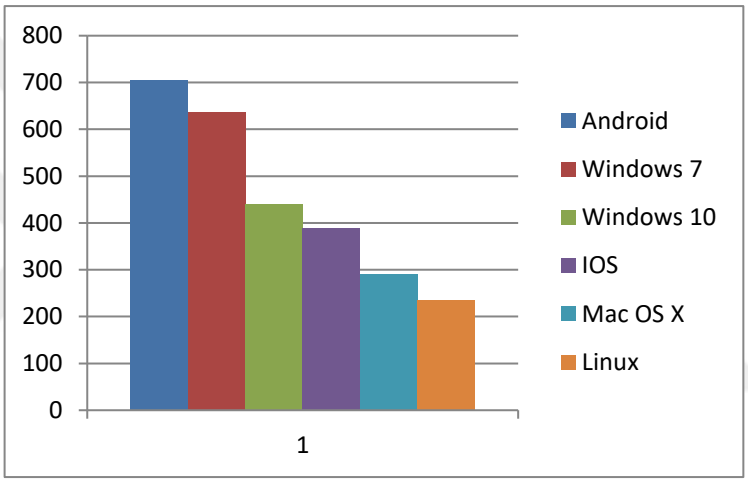
5.3 Kullanıcı Eğilimleri Sonuçları

Bu bölümde kullanıcı eğilimlerinin incelenmesiyle elde edilen istatistiksel bilgiler yer almaktadır. Bu bilgiler, incelenen ağ kullanıcılarını daha iyi profillemesi ile ağ için daha verimli güvenlik önlemleri için ve pazar araştırmaları için faydalı olacaktır.

Kullanıcıların sistem ve ürün tercihleri grafiklerle gösterilerek teknik detaylardan bağımsız kolay okunabilir sonuçlar üretilmiştir.

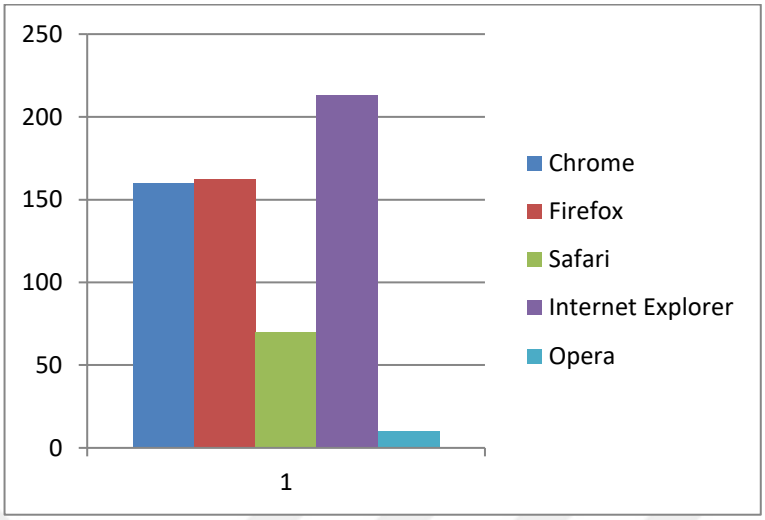
5.3.1 İşletim Sistemi Eğilimleri

Ağ üzerinden internete erişim sağlayan kullanıcıların kayıt dosyalarında yer alan bilgilere göre, kullanıcıların işletim sistemi eğilimleri çıkarılmıştır. Bilgilerin istatistiksel değerinin yanı sıra ağ güvenliğinde önlemlerinin en çok kullanılan işletim sistemlerine uygun alınmasına da olanak sağlayacaktır.

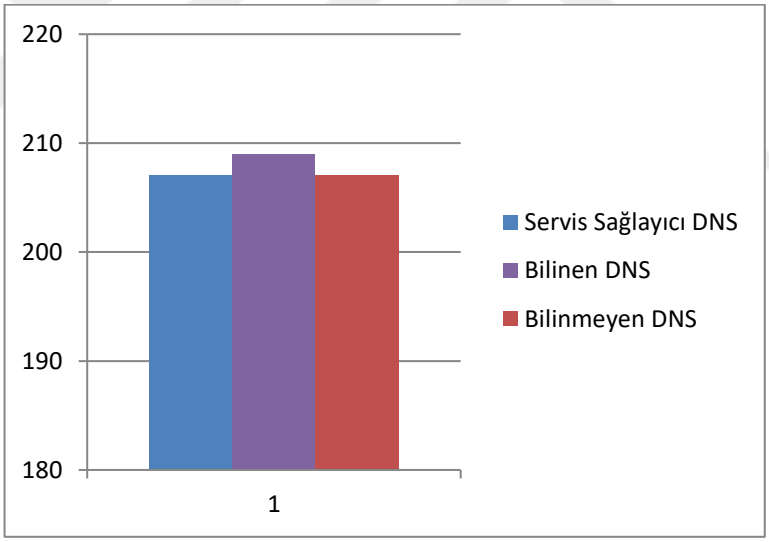


Şekil 5.7 İşletim Sistemlerinin Kullanıcılara Dağılımı Grafiği

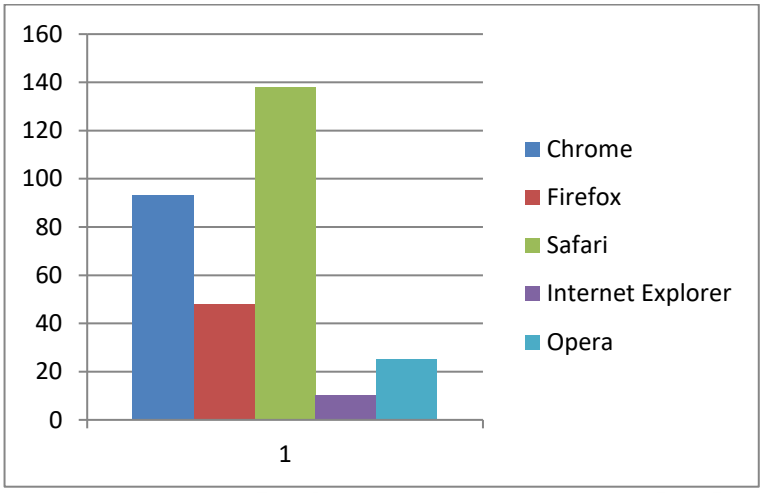
İşletim sistemlerinin kullanıcılara dağılımı yukarıda Şekil 5.7' de verilmiştir. Bu verilerin analizi sonrası mobil ve masaüstü kullanıcıları ayırt edilebilir, hangi marka hangi işletim sistemi daha çok tercih ediliyorsa tespit edilebilmesi mümkündür. Ağ kullanıcılarının ihtiyaçlarına göre ağ kurulumunu gerçekleştirmek de bu bilgilerin başka bir faydası olabilecektir. Örneğin mobil kullanıcıların yoğun olduğu bir ağ için kablosuz modemlerin sayısını yüksek tutmak kullanıcıların ağ kullanımını kolaylaştırır. Kullanıcıların işletim sistemi kullanımına göre, skorlama da diğer parametreler olan web tarayıcı ve DNS sunucu seçimleri de incelenmiştir. Mobil ve masaüstü kullanıcılarının hangi sistemleri veya ürünleri tercih ettikleri değerli istatistiksel bilgiler sunmaktadır. İşletim sistemlerinin ayrıntılı kullanım istatistiklerinin örnekleri aşağıda (Şekil 5.8-5.11) sunulmuştur.



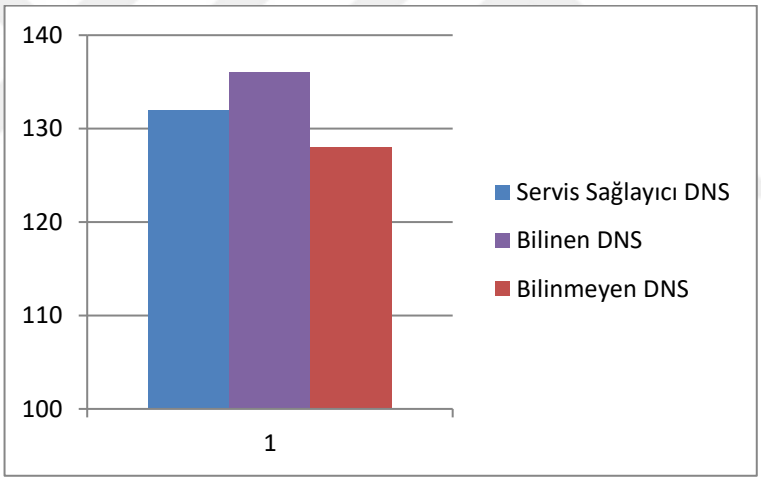
Şekil 5.8 Windows 7 İşletim Sistemini Kullanan Kullanıcıların Web Tarayıcı Tercihleri Grafiği



Şekil 5.9 Windows 7 İşletim sistemini Kullanan Kullanıcıların DNS Sunucu Tercihleri Grafiği



Şekil 5.10 IOS İşletim Sistemi Kullanan Kullanıcıların Web tarayıcı Tercihleri Grafiği

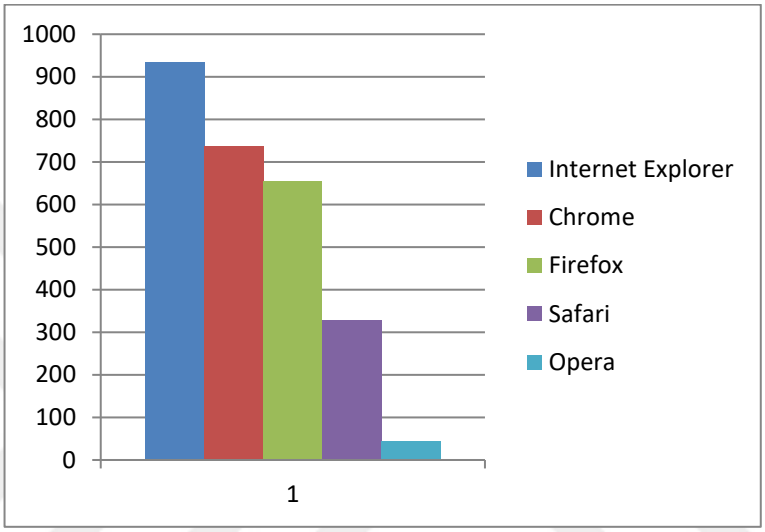


Şekil 5.11 IOS İşletim Sistemini Kullanan Kullanıcıların DNS Sunucu Tercihleri Grafiği

5.3.2 Web Tarayıcı Eğilimleri

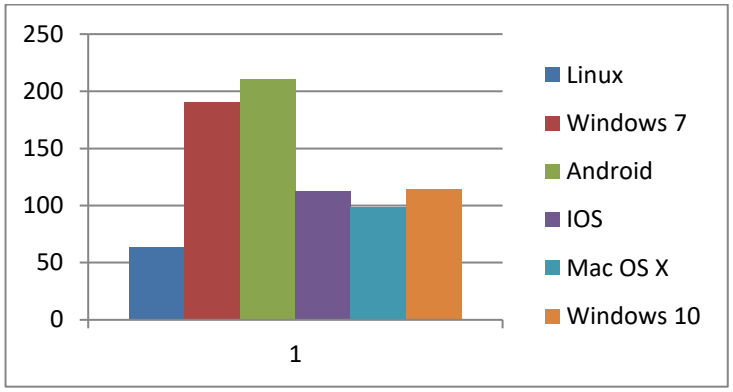
Ağ üzerinden internete erişim sağlayan kullanıcıların erişim kayıtlarında yer alan bilgilere göre, kullanıcıların web tarayıcı eğilimleri çıkarılmıştır. Kurumlar yazışmalarda, personel ve iş takibi gibi operasyonlarda belge yönetimi, kurum otomasyon sistemleri gibi sunucuları üzerinden hizmet veren yardımcı programları kullanmaktadırlar. Genellikle çoğu tarayıcı ile uyumlu çalışabilen bu programlar bazı tarayıcılarda düzgün çalışmamakta ya da tüm fonksiyonların kullanılmasına olanak

tanımamaktadır. En çok kullanılan web tarayıcıların bilinmesiyle kurumun işleyişi ile ilgili yardımcı programların bu tarayıcılara uyumlu biçimde tercih edilmesi hem zaman kayıplarını azaltacaktır hem de daha güvenli bir ağ için yardımcı olacaktır. Ayrıca kurumsal mail sunucuları ve web sayfalar da yine daha uyumlu tarayıcılar için tercih edilecektir.

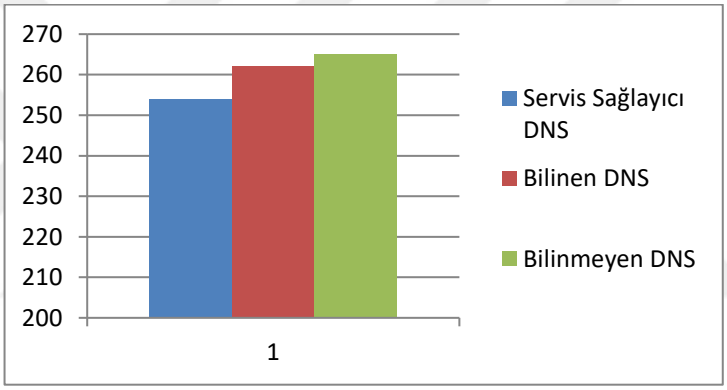


Şekil 5.12 Kullanıcıların Web Tarayıcı Tercihleri Grafiği

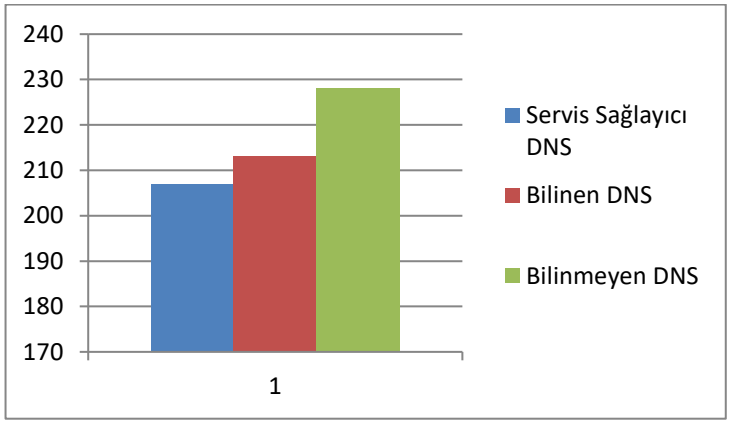
Şekil 5.12' de web tarayıcı ürünlerinin kullanıcı sayılarına göre dağılımı gösterilmiştir. Önceki bölümlerde bahsedildiği gibi, web tarayıcılar üzerinden siber saldırılar günümüzde oldukça yaygındır. Web tarayıcıların güvenlik açıkları bilinmektedir, ağ yöneticileri istatistiklere göre en çok kullanılan web tarayıcıların açıklarına göre önlem alırsa ağdaki saldırı olabilecek açıkları daha iyi kapatmış olurlar. İşletim sistemi bölümünde olduğu gibi bu bölümde web tarayıcı tercihlerine göre ayrıntılı istatistiksel bilgiler incelenmiştir. Buna göre ortaya çıkan sonuçların örnekleri aşağıda (Şekil 5.13-5.16) verilmiştir.



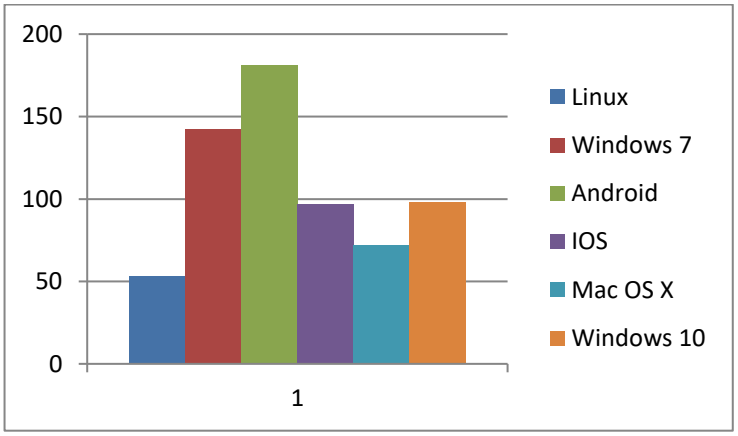
Şekil 5.13 Chrome Web Tarayıcısını Kullanan Kullanıcıların İşletim Sistemi Tercihleri Grafiği



Şekil 5.14 Chrome Web Tarayıcısını Kullanan Kullanıcıların DNS Sunucu Tercihleri Grafiği



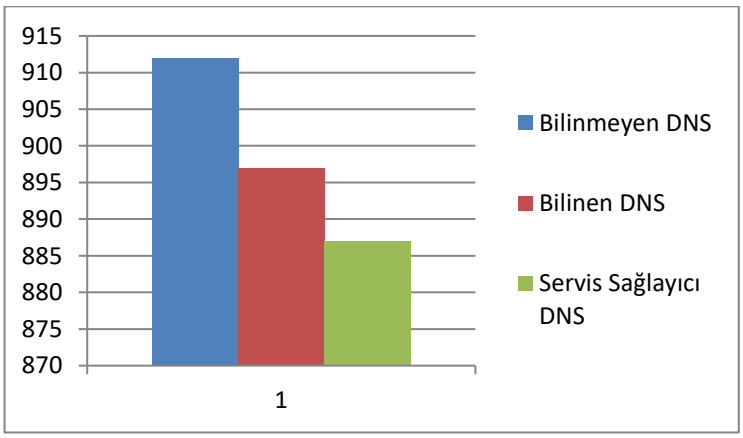
Şekil 5.15 Firefox Web Tarayıcısını Kullanan Kullanıcıların DNS Sunucu Tercihleri Grafiği



Şekil 5.16 Firefox Web Tarayıcısını Kullanan Kullanıcıların İşletim Sistemi Tercihleri Grafiği

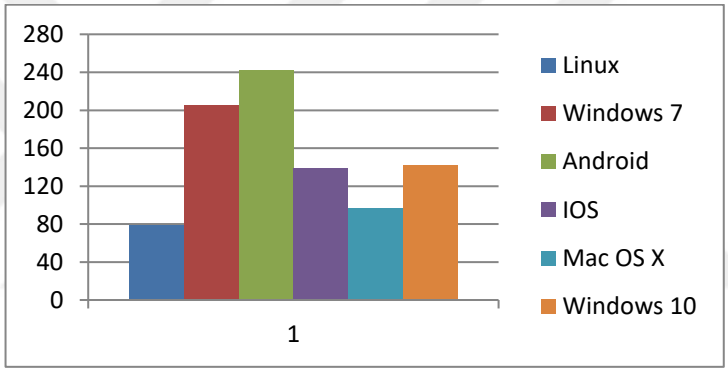
5.3.3 DNS Sunucu Eğilimleri

Ağ üzerinden internete erişim sağlayan kullanıcıların kayıt dosyalarında yer alan bilgilere göre, kullanıcıların DNS sunucu eğilimleri çıkarılmıştır. DNS sunucularda kullanıcıların seçimlerine göre değerlendirmeler yapmak mümkün olacaktır. Bazı DNS sunucuları zararlı amaçlar güderek kullanıcıları yanlış yönlendirmekte veya kullanıcıları saldırıya açık hale getirmektedir. Böyle DNS sunucularının ve tercih eden kullanıcıların ağ üzerinden erişimini engellemek ağ güvenliği için önemli bir geliştirme olacaktır. Kullanıcıların DNS sunucu tercihleri Şekil 5.17'de verilmiştir.

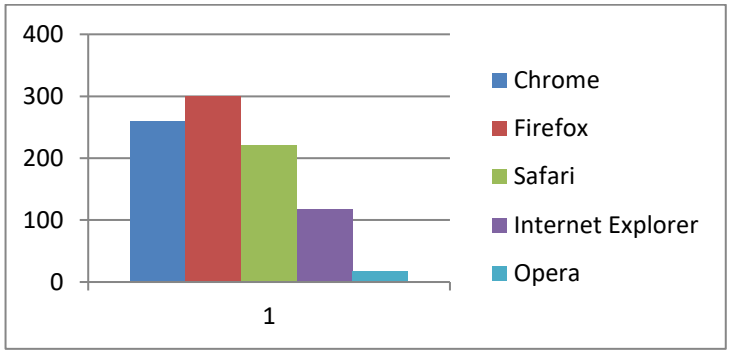


Şekil 5.17 Kullanıcıların DNS Sunucu Tercihleri Grafiği

Özellikle bilinmeyen DNS sunucuları ve bu sunucuları tercih eden kullanıcıların sayıları ağ güvenliği açısından kritik önem taşımaktadır. Güvenilmeyen bir DNS sunucu sistem için ciddi potansiyel tehlikedir. Bir kullanıcı ve DNS sunucu tercihi yüzünden tüm ağ tehdit altına alınabileceği için kullanıcıların tercihleri incelenmeli, gerekli kısıtlar getirilmeli veya uyarılar yapılmalıdır. Güvenilir de olsa Bilinen DNS sunucularını tercih eden kullanıcılar da bazı yasaklı sitelere erişim için bu sunucuları tercih etmektedir. Servis Sağlayıcının sunmuş olduğu DNS sunucuları değil de diğer sunucuları tercih eden kullanıcıların sayıları bu noktada önemlidir. Önceki bölümlerde olduğu gibi bu bölümde de ayrıntılı DNS sunucu istatistikleri çıkarılmıştır. Bu istatistiklerin örnekleri aşağıda verilmiştir.



Şekil 5.18 Bilinen DNS Sunucusunu Kullanan Kullanıcıların İşletim Sistemi Tercihleri Grafiği



Şekil 5.19 Bilinen DNS Sunucusunu Kullanan Kullanıcıların Web Tarayıcı Tercihleri Grafiği

6. SONUÇ

Önceki bölümlerde ağ güvenliği ve bu tez çalışmasında önerilen ağ güvenlik skorlama sistemi açıklanmıştır. Bu bölümde, yapılan çalışma, çalışmanın katkıları ve çalışmanın sonuçları müzakere edilmektedir. Böyle bir çalışmanın gerekliliği ile ortaya çıkan sonuçlar değerlendirilmiştir. Ayrıca bölümün sonunda gelecekte bu tez çalışmasına konu olan ağ güvenliği skorlaması üzerine yapılması planlanan geliştirmelerden bahsedilmiştir.

6.1 Tez Çalışmasına Genel Bakış

Üçüncü bölümde ağ güvenliği üzerine genel bilgiler verilmiştir. Bilgisayar ağlarının ve internetin tanımları yapılarak, ortaya çıktıkları günden bugüne geldikleri nokta ilişkilendirilerek açıklanmıştır. Günümüzde bilgisayar ağlarının kullanım biçimleri ile bilgisayar biliminde sıcak gündem maddelerinden olan nesnelerin interneti kavramı üzerinde durulmuştur. Bilgisayar ağlarına yönelik yapılan siber saldırılardan bahsedilmiştir. En çok bilinen, kişi ve kurumlara oldukça ciddi maddi manevi zararlar veren siber saldırılar ve uygulanma yöntemleri incelenmiştir. Kötü niyetli kullanıcılara ve yazılımlara karşı ağların korunma yöntemlerinden bahsedilmiştir. Günümüzde, özellikle kurum ve şirket ağları gibi çok kullanıcılı ağlarda olması gereken ağ güvenlik ürünleri detaylı olarak açıklanmıştır. Böylece ağ kavramı, ağ güvenliğine neden ihtiyaç duyulduğu ve alınabilecek güvenlik önlemleri açıklanmıştır.

Dördüncü bölümde bu tez çalışmasında önerilen ağ güvenlik skorlama sistemi detaylı olarak açıklanmıştır. Verinin oluşum sürecinden test ortamının oluşturulmasına kadar tüm adımlar açıklanmıştır. Ayrı ayrı hesaplanan kullanıcı ve güvenlik ekipmanları skorlarının adımlarından bahsedilmiştir. Kullanıcıların skorlanmasında kullanılan parametreler; kullanım, işletim sistemi, web tarayıcı ve DNS skorları ve bunların sistem tarafından neye dayanarak skorlandığı incelenmiştir. Kullanıcıların almış oldukları skorların ne anlama geldiği, ağ güvenlik uzmanlarının kullanıcılardan elde edilen skorların bantlarına göre neler yapabilecekleri, hangi durumun aciliyet taşıdığı, hangi durumun sağlıklı bir ağı gösterdiği anlatılmıştır. Ağ

güvenlik ekipmanlarının nelerden oluşması gerektiği ve var olan ekipmanla alınacak skorlardan bahsedilmiştir. Son olarak da ağ güvenlik skorunu simüle etmek için geliştirilen program hakkında bilgiler verilmiş olup, programın sözde kodu ile çalışma mantığı anlatılmıştır.

Beşinci bölümde ağ güvenlik sistemi, önceki bölümlerde bahsedilen sentetik veri setinin uygulanması ile elde edilen sonuçlar yer almaktadır. Ağ güvenlik skoru ve bu skorun elde edilmesi için üretilen kullanıcı ve ağ ekipmanları skorları verilmiştir. Kullanıcı skorlarına göre en az skoru alan 10 kullanıcının skorları Çizelge 5.1 de gösterilmiştir. Çizelgede bu 10 kullanıcının yerel IP adres bilgisi, kullanım skoru, işletim sistemi skoru, web tarayıcı skoru, DNS skoru, standart sapma ve toplam skoru yer almaktadır. Ayrıca kullanıcıların tercih ettikleri web tarayıcı, işletim sistemi ve DNS sunucu bilgilerine göre; ürünlerin kullanıcı sayılarına göre dağılımı gösterilmiştir. Elde edilen verilerle ortaya çıkan ve daha detaylı bilgiler sunan, kullanıcıların işletim sistemi tercihlerine göre web tarayıcı ve DNS sunucu tercihleri, web tarayıcı tercihlerine göre işletim sistemi ve DNS sunucu tercihleri ve DNS sunucu tercihlerine göre işletim sistemi ve web tarayıcı tercihleri her tercih için seçilen örneklerle gösterilmiştir. Örneğin işletim sistemi olarak Windows 7 ürününü tercih eden kullanıcıların tercih ettiği web tarayıcılarının kullanıcı sayılarına göre dağılımı Şekil 5.2 de gösterilmiştir.

Özetle, bu çalışmada bilgisayar ağları için ağ güvenliğini sorgulayarak skorlayan bir sistem önerilmiştir. Skorlama için kullanıcıların ağ üzerinden internete erişim sağlarken ağda bıraktıkları izlerden oluşan kayıt dosyaları ile yapılmaktadır. Log kayıtlarında yer alan kullanıcıların yerel ağda kullandıkları IP adresler, kullanıcıların erişim sağladıkları web sayfalarının alan adları, kullandıkları cihazın işletim sistemi ve web tarayıcı bilgileri ile DNS sunucu tercihi bilgileri incelenip, her kullanıcı için kullanım, işletim sistemi, web tarayıcı ve DNS sunucu tercihleri skorlanmaktadır. Üretilen skorlar istatistiksel çalışmalarda sıkça kullanılan K Means kümeleme ve Ağırlıklı Ortalama Hesaplama yöntemleri ile 6 ayrı sınıf içinde sınıflandırılmaktadır. Bu iki yöntem farklı metriklerle kıyaslanmıştır ve her iki yöntemin de eksik ve artı yönleri vurgulanmıştır. Son olarak da ağ güvenlik ürünlerinin varlığına göre bir skor

verilmiştir ve ağ güvenlik skoru oluşturulmuştur. Log kayıtlarının analizi, ağ analizi, ağdaki kullanıcıların sınıflandırılması daha önce yapılan çalışmalarda mevcuttur. Ancak, ağdaki kullanıcıların skorlanması, iki farklı yöntemle sınıflandırılması ve ağ güvenlik skorunun üretilmesi bu tez çalışmasında önerilen yeniliklerdir.

6.2 Gelecekte Yapılması Planlanan İşler

Bu tez çalışmasında önerilen ağ güvenliği skorlama sistemi ile ağ yöneticilerinin ağlarının güvenliğine dikkat çekmek hedeflenmiştir. Bu skorlama sistemi geliştirilerek tüm ağlar için genel bir metrik haline gelmesi, dolayısıyla tüm kurumsal ve özel ağların güvenilirliklerine göre skorlanması bu çalışmanın nihai hedefidir. Böylece, devletler ulusal düzeyde siber güvenliklerinin de farkına varabileceklerdir. Birçok uzmanın siber savaşlara dikkatini çektiği günümüz dünyasında da bu alandaki eksikleri, zayıf noktaları görmek de ulusal güvenlik açısından devlet politikalarında önemli bir yer teşkil edecektir. Bu çalışmada önerilen sistem ağ güvenlik uzmanları tarafından uygulanması gereken bir prosedür olarak sunulmaktadır. Yani, uzmanlar ağlarındaki kullanıcıların kayıt dosyaları ile bu çalışmada önerilen metriklerle kullanıcılarını skorlayarak ağ güvenlik skorunu elde edebileceklerdir. Gelecekte, ağ güvenlik skorlama sistemi otomatize edilerek kurumların veya şirketlerin ağlarını belirli aralıklarla, hatta genellikle gerçek zamanlı olarak, kontrol eden ve iç güdümlü olarak skorlama yapabilen bir sistemin tasarlanması hedeflenmektedir.

Ağ güvenlik skorlama sistemi, tüm bileşenlerin skorlanarak nihai skorun üretilmesi felsefesi üzerine oturtulmuştur. En önemli ayağı kullanıcıların analiz edilerek skorlanması olan bu sistemde, kullanıcıların skorlandıkları parametreler olan kullanım, işletim sistemi, web tarayıcı ve DNS sunucuları ayrı ayrı skorlanmaktadır. Bu adımların daha geniş kapsamlı analizlerle skorlanması gelecekte yapılması planlanan başka bir işlemdir. Şu anki sistemde işletim sistemleri ve web tarayıcılar sistem açıklarına göre, DNS sunucular güvenile bilirliklerine göre ve kullanıcı kullanımı da erişim sağlanan web sayfalarına göre skorlanmaktadır. İşletim sistemi, web tarayıcı ve DNS sunucu skorlanırken kullanıcı deneyimleri, marka değerleri, maruz kaldıkları saldırı sayıları gibi yeni parametreler eklenerek skorlanmaları hedeflenmektedir. Kullanıcıların kullanım yoğunluğunun da tehlike potansiyeli

olması sebebiyle kullanıcı kullanım yoğunluğu skoru da sisteme eklenecektir. Ağ güvenlik ekipmanlarının skorlanmasında da ağ güvenlik skorlama sisteminde tanımlı güvenlik ekipmanlarının sayısının artması ve incelenen ağda var olan güvenlik ekipmanlarının otomatik tespit edilmesi ile bu adımın da iyileştirilmesi gelecek için hedeflenmektedir. Örneğin, davranış analizi yapan antivirüs benzeri programların da sistemde varlığı sorgulanacaktır. Son olarak da bu tez çalışmasında önerilen sistemin, devlet kurumlarının ağlarının incelenmesi ile illerin, bölgelerin ve son olarak ülkenin kurumsal olarak ağ güvenlik durumu hakkında bilgiler verebilecek bir sisteme genişletilmesi nihai hedef olarak belirlenmiştir.

KAYNAKÇA

[1] L. Kleinrock, “Information flow in large communication nets,” *RLE Quarterly Progress Report*. 1961.

[2] “E-Devlet,” 2008. [Online]. Erişim İçin: https://www.turkiye.gov.tr/bilgilendirme?konu=sikcaSorulanlar.

[3] GFI, “Targeted Cyber Attacks; the dangers faced by your corporate network, GFI white paper,” *GFI white Pap.*, pp. 1–16, 2014.

[4] B. Harvey, “What is a Hacker,” *ACM Select Panel on Hacking*, 1985. [Online]. Erişim İçin: https://people.eecs.berkeley.edu/~bh/hacker.html.

[5] “Wikipedia,” 2016. [Online]. Erişim İçin: https://en.wikipedia.org/wiki/Logfile.

[6] “IP adresleri,” 2016. [Online]. Erişim İçin: https://tr.wikipedia.org/wiki/IP_adresi.

[7] IEEE Computer Society., “IT professional,” vol. 548414707, no. February, pp. 1–6, 1999.

[8] A. Badea, V. Croitoru, S. Member, and D. Gheorghic, “Computer Network Vulnerabilities and Monitoring,” pp. 49–54, 2015.

[9] V. Anitha, “A Survey on Predicting User Behavior Based on Web Server Log Files in a Web Usage Mining,” 2016.

[10] N. Goel, “Analyzing Users Behavior from Web Access Logs using Automated Log Analyzer Tool,” *Int. J. Comput. Appl.*, vol. 62, no. 2, pp. 29–33, 2013.

[11] N. Anand, “Effective Prediction of Kid ’ s Behaviour Based on Internet Use,” vol. 4, no. 2, pp. 183–188, 2014.

[12] FIRST, “Common Vulnerability Scoring System v3.0: Specification Document,” 2015.

[13] S. Alspaugh, B. Chen, J. Lin, A. Ganapathi, M. Hearst, and R. Katz, “Analyzing Log Analysis: An Empirical Study of User Log Mining,” *28th Large Install. Syst. Adm. Conf.*, pp. 62–77, 2014.

[14] K. Oztoprak, “Profiling subscribers according to their internet usage characteristics and behaviors,” *Proc. - 2015 IEEE Int. Conf. Big Data, IEEE Big Data 2015*, pp. 1492–1499, 2015.

[15] CISCO, “CISCO,” 2017. [Online]. Erişim İçin: http://www.cisco.com/.

[16] Cisco Systems, “Cisco Cyber Threat Defense Solution: Delivering Visibility into Stealthy, Advanced Network Threats,” 2012.

[17] R. Hauben, “Chapter 8 The Birth and Development of the ARPANET,” pp. 1–10, 1962.

[18] L. Rai and G. Yan, “Future perspectives on next generation e-sports infrastructure and exploring their benefits,” *Int. J. Sport. Sci. …*, vol. 3, no. 1, pp. 27–33, 2009.

[19] “Gartners IT Forecast.” [Online]. Erişim İçin: http://www.gartner.com/technology/research/it-spending-forecast/.

[20] K. Rose, S. Eldridge, and C. Lyman, “The internet of things: an overview,” *Internet Soc.*, no. October, p. 53, 2015.

[21] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, “Privacy in the internet of things: Threats and challenges,” *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[22] B. Daya, “Network Security : History , Importance , and Future.”

[23] C. Sweigart, “Interested in learning more ? In sti tu te , A ut ho ins ll r igh,” no. Security 401, 2003.
[24] “Bill Clinton,” 2017. [Online]. Erişim İçin: https://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history.
[25] Cisco, “What Is the Difference: Viruses, Worms, Trojans, and Bots?”
[26] C. Fosnock, “Computer Worms : Past , Present , and Future,” 2005.
[27] A. Aksu, “Ağ Protokolleri,” 2011.
[28] D. Bansal and M. Godara, “Internet Security and Privacy,” *Int. J. Res.*, vol. 1, no. 11, pp. 232–241, 2014.
[29] Paul Janes, “Interested in learning SANS Institute InfoSec Reading Room,” *Inf. Assur. Secur. Integr. Proj. People, Process. Technol. Impact Inf. Data Loss*, 2012.
[30] H. Abie, “An Overview of Firewall Technologies,” *Telektronikk*, pp. 1–9, 2000.
[31] C. Science and S. Engineering, “How Anti-virus Software Works ??,” vol. 3, no. 4, pp. 483–484, 2013.
[32] HKSAR, “VPN Security,” 2008.
[33] N. Chakraborty, “International Journal of Computing and Business Research (IJCBR) INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM : A COMPARATIVE STUDY Nilotpal Chakraborty,” *Int. J. Comput. Bus. Res.*, vol. 4, no. 2, 2013.
[34] K. Oztoprak, “Veri Seti,” 2016. [Online]. Erişim İçin: https://drive.google.com/open?id=0BwKD8MfB9H2MaEFRU2NUYl9yeWM.
[35] “Market Share Statistics for Internet Technologies.” [Online]. Erişim İçin: https://www.netmarketshare.com/.
[36] K. Alsabti, S. Ranka, and V. Singh, “An efficient k-means Clustering algorithm,” 1997.
[37] O. Alhazmi, Y. Malaiya, and I. Ray, “Security vulnerabilities in software systems: A quantitative perspective,” *Lect. Notes Comput. Sci.*, vol. 3654, pp. 281–294, 2005.
[38] K. Singh, “Mobile Phone Operating Systems :,” vol. 5, no. 3, pp. 610–613, 2014.
[39] DHS/NCCIC/US-CEC, “NVD,” 2017.
[40] “The Ultimate Security Vulnerability Datasource.” [Online]. Erişim İçin: http://www.cvedetails.com/.
[41] J. Gube, “The history of web browsers,” *Useful Inf. Web Dev. Des.*, vol. 2009, no. 30 September, p. 3, 2009.
[42] University of Illinois, “NCSA,” 2017. [Online]. Erişim İçin: http://www.ncsa.illinois.edu/.
[43] M. Silic, J. Krolo, and G. Delac, “Security vulnerabilities in modern web browser architecture,” *MIPRO 2010 Proc. 33rd Int. Conv.*, pp. 1240–1245, 2010.
[44] Infoblox, “Top Five DNS Security Attack Risks and How to Avoid Them,” 2013.
[45] Google, “Google DNS.” [Online]. Erişim İçin: https://developers.google.com/speed/public-dns/.

[46] Opendns, “OpenDNS.” [Online]. Erişim İçin: https://www.opendns.com/home-internet-security/.
[47] Norton, “NOrton DNS.”
[48] S. A. Kulkarni and H. S. Kshirsagar, “Taxonomical study of the rumen protozoan ciliate Entodinium ciculum (Dehority, 1979), from stomach of Indian cattle (Bos indicus),” *Asian J. Microbiol. Biotechnol. Environ. Sci.*, vol. 8, no. 1, pp. 41–43, 2006.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	**:**	Kaçar, Mustafa Sami
Uyruğu	**:**	T.C.
Doğum Tarihi ve Yeri	**:**	04.11.1990 ISPARTA
e-mail	**:**	msami.kacar@karatay.edu.tr

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	Çankaya Üniversitesi / Bilgisayar Mühendisliği	19.08.2013

İş Deneyimi

Yıl	**Yer**	**Görev**
2014 -	KTO Karatay Üniversitesi / Bilgisayar Mühendisliği	Araştırma Görevlisi

Yabancı Dil

İngilizce