WEB TABANLI UZAKTAN EĞİTİM SİSTEMLERİNDE BİLGİ GÜVENLİĞİNİN SAĞLANMASI

YÜKSEK LİSANS TEZİ

Yaşar ARSLAN

DANIŞMAN
Yrd. Doç. Dr. Uçman ERGÜN

BİLGİSAYAR ANABİLİM DALI

ŞUBAT 2009

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

WEB TABANLI UZAKTAN EĞİTİM SİSTEMLERİNDE BİLGİ GÜVENLİĞİNİN SAĞLANMASI

Yaşar ARSLAN

DANIŞMAN
Yrd. Doç. Dr. Uçman ERGÜN

BİLGİSAYAR ANABİLİM DALI

ŞUBAT 2009

ONAY SAYFASI

Yrd. Doç. Dr. Uçman ERGÜN danışmanlığında,
Yaşar ARSLAN tarafından hazırlanan
"Web Tabanlı Uzaktan Eğitim Sistemleri'nde Bilgi Güvenliğinin Sağlanması" başlıklı bu çalışma, lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca
…../…../2009
tarihinde aşağıdaki jüri tarafından Bilgisayar Anabilim Dalında
Yüksek Lisans tezi olarak oybirliği / oy çokluğu ile kabul edilmiştir.

Ünvanı, Adı, Soyadı		İmza
Başkan	Doç.Dr.Muhammet YÜRÜSOY	
Üye	Yrd.Doç.Dr.Ömer DEPERLİOĞLU	
Üye	Yrd.Doç.Dr.Uçman ERGÜN	

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

Doç. Dr. Zehra BOZKURT
Enstitü Müdürü

İÇİNDEKİLER

ÖZET

Yüksek Lisans Tezi

Web Tabanlı Uzaktan Eğitim Sistemlerinde Bilgi Güvenliğinin Sağlanması

Yaşar ARSLAN

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar

Danışman: Yrd. Doç. Dr. Uçman ERGÜN

Günümüz Uzaktan Eğitim Sistemleri, güçlü teknolojik altyapı ile desteklenmiş yazılımlardan oluşmaktadır. Dünya genelinde internet kullanımının yaygınlaşması ile yazılımlar web tabanlı oluşturulmaya başlanmıştır. Bu gelişme ile birlikte, Uzaktan Eğitim Sistemleri web tabanlı yazılımlar olarak tasarlanmaktadır. Web Tabanlı Uzaktan Eğitim Sistemleri dışardan gelebilecek saldırılara karşı tehdit altında kalan sistemlerdir. Bu nedenle bilgi güvenliği çalışmalarının titizlikle yapılması gerekmektedir.

Bu tez çalışmasının birinci bölümünde Uzaktan Eğitim, Web Tabanlı Uzaktan Eğitim Sistemleri, bilgi güvenliği, bilişim teknolojileri ve sunucu güvenliği kavramları doğru zemine oturtulmaya çalışılarak ilişkilendirilmiştir.

Sonraki kısımda Afyon Kocatepe Üniversitesi Web Tabanlı Uzaktan Eğitim Sistemi olarak tasarlanan WELANIMAL projesi için bilgi güvenliği çalışmaları yapılmıştır. Sistem kullanıma açılmadan önce bilgi güvenliği testleri yapılmış ve gerekli düzenlemelere gidilmiştir. Bilgi güvenliği çalışmaları, ağ güvenliği, sunucu sistem güvenliği ve yazılım güvenliği şeklinde uygulamalı olarak yapılmıştır.

2009, 110

Anahtar Kelimeler: Uzaktan Eğitim, Web Tabanlı Uzaktan Eğitim Sistemleri, Bilgi Güvenliği, Sunucu Güvenliği, Bilişim Teknolojileri, Web Tabanlı Uygulama

ABSTRACT

MSc. Thesis

Ensuring Data Security for Web based Distance Learning Systems

Yaşar ARSLAN

Afyon Kocatepe Üniversity

Gradute School of Natural and Applied Science

Computer

Supervisor: Assoc. Prof. Uçman ERGÜN

Modern Distance Learning Systems cover software systems supported by powerful technologic infrastructure. Software programs are now created with web based technologies because of the increase in internet usage. With this development, Distance Learning Systems are started to be designed with web based software. Web Based Distance Learning Systems are open to external threats and for this reason, it is necessary to work meticulously on data security.

In the first the concepts of Distance Learning Web Based Distance Learning Systems, data security, information science and server security have been clarified.

In the following two parts, data security studies have been carried out on WELANIMAL project which is designed as a Web Based Distance Learning System for Afyon Kocatepe University. The system has been controlled via data security tests and necessary arrangements have been done before putting it into service. Data security studies have been applied in terms of network security, server system security and software security.

2009, 110

Key Words: Distance Learning, Web Based Distance Learning Systems, Data Security, Server Security, Information Technologies, Web Based Application

TEŞEKKÜR

Bu çalışmanın ortaya çıkmasında her zaman yakın ilgi ve desteğini gördüğüm, çalışmanın başlangıcından sonuna kadar aynı ilgiyi devam ettiren danışmanım Yrd.Doç.Dr. Uçman ERGÜN'e, düşünceleri ile bu çalışmanın gerçekleşmesinde desteklerini esirgemeyen Bilgi İşlem Daire Başkanlığındaki değerli mesai arkadaşlarıma ve aileme teşekkürü bir borç bilirim.

Yaşar ARSLAN

AFYONKARAHİSAR, 12 Ocak 2009

SİMGELER ve KISALTMALAR DİZİNİ

ACL	Access List (Erişim Kontrol Listesi)
ATM	Asynchronous Transmission Mode (Eşzamanlı Olmayan Aktarım Modu)
DHCP	Dynamic Host Configuration Protocol (Dinamik İstemci Yapılandırma Protokolü)
FTP	File Transfer Protocol (Dosya Transfer Protokolü)
HTML	HyperText Markup Language (Hareketli Metin İşleme Dili)
HTTP	Hyper Text Transfer Protokol (Hiper Metin Transfer Protokolü)
ICMP	Internet Control Message Protocol (İnternet Kontrol Mesaj Protokolü)
IIS	Internet Information Server (İnternet Bilgi Servisi)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevention Systems (Saldırı Tespit ve Önleme Sistemleri)
LAN	Local Area Network (Yerel Alan Ağı)
MAC	Media Access Control (Ortam Erişim Yönetimi)
MSSQL	Microsoft Structured Query Language (Microsoft Yapılandırılmış Sorgu Dili)
NAT	Network Address Translation (Ağ Adres Dönüşümü)
OWASP	Open Web Application Security Platform (Web Uygulamaları Güvenlik Platformu)
QoS	Quality of Service (Hizmet Kalitesi)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SSL	Secure Socket Layer (Güvenli Yuva Katmanı)
WTUES	Web Tabanlı Uzaktan Eğitim Sistemi

VLAN	Virtual Local Area Network (Sanal Yerel Alan Ağı)
VRF	Virtual Route Forwarding (Sanal Yönlendirme İletimi)
XML	Extensible Markup Language (Uzatılabilir Metin İşleme Dili)

ŞEKİLLER DİZİNİ

RESİMLER DİZİNİ

1. UZAKTAN EĞİTİM

1.1. Uzaktan Eğitim Geçmişi

Uzaktan Eğitim uygulamaları 1850'li yıllardan sonra ortaya çıkmış ve çağın iletişim araçlarına göre şekillenerek günümüzdeki halini almıştır. Uzaktan Eğitim'in tarihsel gelişimi dört ayrı kuşak olarak ele alınmaktadır. Birinci kuşak, ilk defa 1856 yılında Berlin'de yabancı dil eğitimi için kurulan bir okul ile "Mektupla Eğitim" adlı eğitim modelinin kullanılmasıyla başlamıştır. İkinci kuşak "Çoklu Ortam Modeli", üçüncü kuşak "Tele Öğrenme Modeli" ve dördüncü kuşak ise "Esnek Öğrenme Modeli" adıyla, eğitsel teknolojilerde kullanılmaya başlanmıştır (Mclendon 1999).

Eş zamanlı olmayan (asekron) eğitim adı verilen ilk kuşakta, tek bir teknolojinin (basılı materyal) kullanımı söz konusudur. Bu tür eğitimde öğrenci ile eğitici arasında doğrudan bir etkileşim yoktur. Bir gazetenin dağıtılması gibi tek taraflı etkileşimle eğitim ve öğrenim gerçekleşmektedir. Mektupla Öğretim bu ilk kuşağa örnek olarak verilebilir.

İkinci kuşakta ise; uzaktaki öğrencinin çalışması için öğretim materyallerinin özellikle eğitimi alacak öğrenci modeline göre tasarlandığı ancak iki yönlü iletişimin üçüncü bir kişi tarafından sağlandığı ortamlardır ve çoklu ortama geçişi ifade etmektedir. Bu üçüncü kişi öğretim materyallerinin oluşturulma işleminden ziyade, daha çok eğitime rehberlik etmektedir. Teknoloji ve haberleşmedeki gelişmelerin henüz ortaya çıktığı dönemlerde, bağımsız olarak uzaktan eğitim sunan üniversite ve fakültelerin kurulmasını, bu kuşağa örnek olarak verebiliriz. Bu kuşağın ortaya çıkmasıyla, daha önce Uzaktan Eğitim kuramcıları tarafından dikkate alınmayan Uzaktan Eğitim'in uzak sınıf biçimi önem kazanmaya başlamıştır (Daniel 1996). Ülkemizde 1982-83 öğretim yılında, Anadolu Üniversitesi Açıköğretim Fakültesi'nin Uzaktan Eğitim Sistemi ile eğitim veren ilk fakülte olarak hizmete başlaması, bu kuşağa verilebilecek örneklerdendir.

Eş zamanlı (sekron) adı ile yapılan eğitime geçiş üçüncü kuşakla birlikte ortaya çıkmıştır. Uzaktaki öğrenciyle öğretmen arasında doğrudan etkileşime izin veren ortamlar oluşturulmaya başlanmıştır. Uzaktaki öğrenciler ya bireysel ya da grup olarak eğitime katılarak etkileşimli bir ortam oluşturmaktadırlar. Bu yüzden hem bireysel, hem de bilgisayar

ve haberleşme sistemleriyle zenginleştirilmiş ortamlar ortaya çıkmaktadır. Bu oluşumdaki teknolojiler, öğretmen-öğrenci ve öğrencilerin kendileri arasında, diğer kuşaklarda yaşanandan çok daha eşit bir iletişim ağı sağlamaktadır (Bates 1995). Bu kuşağa örnek olarak, endüstri devrimin etkisinde bulunan endüstriyel kurumların sahip olduğu üniversiteler gösterilebilir. Özel üniversiteler olarak adlandırabileceğimiz bu eğitim kurumlarına örnek olarak, John Daniel'in "Mega Üniversiteler" olarak adlandırdığı, 100.000'den fazla öğrenciye sahip, özerk, açık üniversiteler verilebilir. İngiltere'deki Open University ve yine ülkemizde uzaktan eğitim veren Anadolu Üniversitesi mega üniversiteler arasında bulunmaktadır (Daniel 1996).

Günümüzü temsil eden dördüncü kuşak ise Esnek Öğrenme Modelidir. Bu kuşakta öğrencinin öğrenme ortamı açısından esnekliği korunur ve bununla birlikte öğrenme etkileşimi, günümüz teknolojileriyle üst düzeyde sağlanmaktadır. Bu kuşağa örnek olaraktan, küresel değişim ve gelişime açık, daha esnek yönetime sahip "Endüstri Sonrası (Post-Fordist)" kurumlardır (Bates 2000). Bu kurumlar sunumlarında ve eğitimlerinde yeni teknolojiyi kullanarak daha esnek ve etkileşimli eğitim sunmaktadırlar. Günümüzde gerek kuruluşlar, gerekse öğrenciler, internet üzerinden web sayfaları aracılığı ile interaktif eğitimlerini sağlamaktadırlar. Bu kuşakta, web sayfaları aracılığı ile senkron ve asenkron eğitim sağlanabilmektedir. Asekron yönü ile öğrencilerin bilgiye erişiminde daha esnek bir yapı sağlanmakta, sekron yönü ile de öğrenci ve eğitmen arasında bir etkileşim sağlanmaktadır.

1.2. Günümüz Uzaktan Eğitim Sistemleri

Günümüz Uzaktan Eğitim Sistemleri'nin temelinde teknolojik araçlar kullanılmaktadır. Eğitim ve teknolojinin birlikte kullanımı toplum içerisinde "Eğitim Teknolojisi" kavramını ortaya çıkarmıştır. Eğitim teknolojisi kısaca; eğitim alanında teknolojik ürünleri kullanarak çeşitli hizmetlerden yararlanılmasıdır. Öğrenme-öğretme süreçleri için uygun teknolojilerin geliştirilmesi ve kullanılmasıdır (Neville 1977). "Eğitim teknolojisi; insanlar için öğrenmeyi iyileştirmek, sistemleri, yöntemleri ve araçları geliştirmek, uygulamak ve değerlendirmektir" (Mitchell 1978).

Uzaktan Eğitim Sistemleri'nin gelişimi, iletişim teknolojilerinin gelişmesiyle paralel ilerlemekte ve eğitim tamamen teknoloji odaklı gerçekleşmektedir. Uzaktan Eğitim

Sistemi'nin büyük bir çoğunluğu hareketli, görsel ve işitsel öğelerden oluşmaktadır. Yeni nesil yazılımlarla birlikte hızlı haberleşme ve iletişim altyapısı sayesinde daha akıcı ve etkileşimli görsel öğeler rahatlıkla kullanılabilir hale gelmiştir.

Bilgisayar okuryazarlığının artması ile birlikte bilgisayar teknolojileri eğitimin vazgeçilmez öğesi haline gelmiştir. Bu bağlamda sistem tasarımı ve görsel öğelerdeki hareketlilik ve eğitim içerikleri ayrı bir önem kazanmıştır. Sadece öğrenciye yönelik olmayan Uzaktan Eğitim Sistemi'nde, eğitim içeriklerinin hazırlanmasında eğitmenler için, kullanımı kolay araçlar tasarlanmakta ve kullanıma sunulmaktadır.

1.3. Uzaktan Eğitim Sistemi'nde Bilgi

1.3.1. Uzaktan Eğitim Sistemi'nde Bilginin Önemi

Bilgiyi kısaca; öğrenme, araştırma ve gözlemleme sonucu elde edilen ilkelerin bütünüdür, şeklinde tanımlayabiliriz. Uzaktan Eğitim Sistemleri ise; bilginin etkin araçlarla kaynağından alınıp, ihtiyaç sahiplerine ulaştırıldığı bir birimdir. Bilgiyi toplayan, depolayan ve istenildiğinde bu isteklere cevap verebilen bir sistem tasarımıdır. İhtiyaç sahipleri ise; belirli eğitim hedefleri olan ve ihtisas yapmak isteyen öğrenciler, özel konularda bilgi gereksinimleri olan tüzel guruplar veya herhangi bir konuda küçükte olsa bilgi ihtiyacı olan kimselerdir. Bilgiye erişim sağlama konusunda kişiler veya gruplar için bir takım kısıtlamalar ve özel izinler tanımlanarak, herkesin her türlü bilgiye erişimi sağlanmaz. Uzaktan Eğitim Sistemi'nde bilgi farklı işlemlerden geçerek ihtiyaç sahiplerine eriştirilir.

- Bilginin elde edilmesi: Kullanılacak bilginin elde edilme safhasıdır. Uzaktan Eğitim sisteminde bilgi, eğitim metaryellerinin hazırlanarak dosyalar halinde veya kitap, dergi ve yazılı materyallerin taranarak elektronik ortama aktarılması ile oluşturulur. Elektronik ortamlara aktarılan bilgi maliyet yönünden daha hesaplı olmaktadır.
- Bilginin işlenmesi: Bilginin işlenmesi ihtiyaç sahiplerinin ve bilginin türüne göre amacına ulaşır hale getirilmesidir. Yani bilginin belirli bir formata dönüştürülmesi ve ihtiyaç sahibine göre şekillendirilmesi işlemidir.

- Bilginin stoklanması: Bilginin saklanması ve ihtiyaç halinde tekrar ulaştırılabilir halde saklanması işlemidir. Uzaktan Eğitim Sistemi sürekli bilgi ihtiyacına cevap verebilen bir sistem olmalıdır. Bu açıdan bakıldığında, elde edilmiş ve işlenmiş bilgilerin titizlikle korunması ve erişime hazır halde tutulması gerekmektedir.
- Bilginin gözden geçirilmesi: Uzaktan Eğitim Sistemleri'nde bilgi akışı çok hızlı çalışmalı ve bilginin güncelliği her zaman canlı tutulmalıdır. Bundan dolayı bilgiyi elde etme ve işleme aşamaları çok hızlı bir yapıda tasarlanması gerekmektedir. Bilginin bu aşamalardan sonra ihtiyaç sahiplerine ulaştırılmadan önce mutlaka kontrol edilmesi ve gerekirse yeniden düzeltmelere gidilmesi gerekir. Gözden geçirme titiz bir çalışma olmalıdır, bunun aksi bir durumda ise veri bütünlüğü riski söz konusudur. Neticesinde ise ihtiyaç sahibinin yanlış bilgilendirmesi ve sistem içerisinde kritik hataların oluşması söz konusudur.
- Bilginin iletilmesi: Bilginin ihtiyaç sahibine ulaştırılması safhasıdır. Elektronik ortama aktarılan bilginin iletim işlemi, Uzaktan Eğitim Sistemi'nin sorumluluğu altındadır. Günümüz teknolojilerinde bilgi iletimi, elektronik ortamlarda kolay ve hızlı bir şekilde sağlanmaktadır. Ayrıca günümüz sistemlerinde sadece bilgi iletimi yapılmaz, aynı zamanda farklı noktalardan bilgi toplama işlemi de gerçekleştirilir.

Yapılan bu evrelerin kısa bir özeti olarak Uzaktan Eğitim Sistemi'nde bilgi, ihtiyaç sahipleri için faklı kaynaklardan elde edilerek işlenir ve uygun formata dönüştürülür. Her zaman erişilebilir konumda saklanır. Güncelliği ve gözden geçirme işlemleri sağlanarak hedefe iletilir. Bu evrelerden sonra sistemin görevi; tüm aşamaları otomasyon halinde sürekli işler halde çalıştırmaktır.

1.3.2. Uzaktan Eğitim Sistemi'nde Bilgiyi Oluşturan Öğeler

Uzaktan Eğitim Sistemi'nde bilgi yönünden en çok kullanılan öğe ders içerikleridir. Eğitimcinin bilgiyi işleyip uygun formata getirmiş halidir ve kullanıcıya bu şekilde iletilir. Günümüz Uzaktan Eğitim Sistemleri'nde bilgi sadece ders içeriklerinden oluşmamaktadır. Sistemi tüm yapısıyla ele aldığımız zaman, teknolojik altyapı ile çalışan tamamen elektronik bir sistem karşımıza çıkmaktadır. Sistem bir web sayfası aracılığı ile farklı tür kullanıcılara bilgilendirme hizmeti sunmaktadır. Bu sistemde bilgi 2 farklı gurupta sıralanabilir.

- Sistem yönetim bilgileri: Her bir üye için kullanıcı bilgileri, kullanıcı yetkileri, sistem içerisinde kullanıcı hareket bilgileri, sistem genelindeki mesajlaşma bilgileri, sistem duyuru bilgileri, sistem dönem ve ders bilgileri, sistem için kullanıcıları bilgilendirecek yardım bilgileri, üye veya misafir kullanıcılar için sistem ve eğitimler hakkındaki bilgi içerikleri, sistem yönetimi ve işleyişi açısından önemli bilgilerdir.
- Üye kullanıcı bilgileri: Üye kişisel bilgileri, forum sayfaları, anketler, anket sonuçları, sorular, soru bankaları, sınavlar, deneme sınavları, sınav sonuçları, başarı istatistikleri, mesajlar, içerik hazırlamada kullanılacak yardımcı bilgiler, kişisel notlar, sohbet, ders notları, ders içerikleri ve yardımcı belgeler, sistemden faydalanan kullanıcıların tümü için gerekli bilgileri içerir.

1.3.3. Uzaktan Eğitim Sistemi'nde Bilgi Güvenliği ve Gizliliği

Son 10 yıl içerisinde internetin dünya çapında hızla büyümesi ile birlikte, web tabanlı uzaktan eğitim sistemlerinin sayısı hızla artmaya başlamıştır. Bunda en büyük pay eğitim kurumları olan üniversitelerdir. Üniversitelerin internete erişim yönünden zengin altyapılara sahip olması, sürekli eğitim kadrosu ve sistem tasarım ekibinin olması uzaktan eğitim sistemi hazırlanmasını daha çekici hale getirmiştir. Nitekim ülkemizde yapılan ilk uzaktan eğitim uygulamaları üniversiteler tarafından gerçekleştirilmiştir. Sakarya Üniversitesi'nin 2000'li yılların başlarında gerçekleştirdiği uzaktan eğitim sistemi buna verebileceğimiz bir örnektir.
Web tabanlı uzaktan eğitim sistemlerinin çoğalmasındaki büyük etkenlerden birisi de böyle bir sisteme olan ihtiyacın bilişim teknolojilerinin gelişmesine paralel olarak artmasıdır. Günümüzde internete bağlı herhangi bir noktadan bilgiye erişimin mümkün olması sebebi ile uzaktan eğitimle birlikte meslek edinme ve bilgi sahibi olma ihtiyacı doğmuştur. ABD'de Teknoloji ve Yetişkinlerin Öğrenimi Komisyonu'nun (The Commission on Technology and Adult Learning) hazırlamış olduğu rapora göre e-öğrenim, insanların ailelerinden veya bulundukları ortamlardan ayrılmadan kariyerlerinde ilerleme kaydedebilecekleri veya daha üretken olabilmek için bilgi ve becerilerini geliştirebilecekleri, teknolojik bileşenlerinden oluşan bir eğitim modeli olarak ifade edilmektedir (Bonk 2000). Diğer yandan uzaktan öğrenim, geleneksel öğretme-öğrenme yöntemlerinin sınırlılıkları nedeniyle sınıf içi etkinlikleri yürütme olanağının bulunmadığı durumlarda, eğitim etkinliklerini planlayanlar ve uygulayıcılar ile öğrenciler arasında iletişim ve etkileşimin, özel olarak hazırlanmış öğretim

üniteleri ve çeşitli ortamlar yoluyla sağlandığı bir öğretim merkezi şeklinde ifade edilmektedir (Alkan 1981).

İnternet üzerinden bilgi paylaşımının yapılması, bilgisayar uygulamalarında bilgi güvenliği çalışmalarının yapılmasını vazgeçilmez hale getirmiştir. Web tabanlı uzaktan eğitim sisteminde tüm bilgilerin ağ üzerinden yapılması neticesi ile bilgi güvenliğinin hem ağ katmanlarında hem de uygulama katmanlarında yapılmasını gerekli kılar. Web tabanlı uzaktan eğitim sistemlerinde bilgi güvenliği incelemeleri yaklaşık olarak bilişim güvenliğinin tümünü kapsamaktadır. Bu bağlamda web tabanlı uzaktan eğitim sistemlerinde bilgi güvenliği konusu bilişim güvenliğine benzer özellikleri barındırmaktadır.

Bilişim güvenliği, bilişim ürünleri veya cihazları ile bu cihazlarda işlenmekte olan verilerin gizliliğini, bütünlüğünü ve sürekliliğini korumayı amaçlayan çalışmaların tümüne verilen isimdir. Bilişim güvenliği temel olarak gizlilik, veri bütünlüğü, süreklilik şeklinde üç prensip ve bunlara eklenebilecek izlenebilirlik (kayıt altına alma), kimlik sınaması, güvenilirlik, inkâr edememe prensipleri ile ifade edilebilir. Bu prensipleri kısaca açıklamak gerekirse;

- Gizlilik: Bu prensip bilginin yetkisiz kişilerin eline geçmesini engellemeyi amaçlar. Bilgi bilgisayar sistemlerinde, disk, disket, CD, DVD gibi saklama ortamlarında veya ağ üzerinde gönderici ve alıcı arasında taşınırken yetkisiz erişimlerden korunmalıdır. Sisteme saldırmayı amaçlayan kişi, bir yapılandırma veya yazılım hatasını istismar ederek veya sosyal mühendislik teknikleri ile yetkili insanların hatalarını istismar ederek bilgilere izinsiz olarak erişebilir. Parola dosyalarının çalınması, ağ üzerindeki trafiğin gözetlenmesi ve kaydedilmesi, yetkili kullanıcının fark ettirilmeden gözetlenmesi ile kullanıcıya ait kullanıcı adı ve parola gibi özel bilgilerin alınması, sisteme giriş yapan kullanıcının bilgisayarını saldırganın izinsiz kullanması gibi durumlar gizlilik prensibi kapsamında değerlendirilir.
- Veri bütünlüğü: Bu prensibin amacı veriyi olması gerektiği şekilde tutmak ve korumaktır. Saklanan bilginin bozulmasını, değiştirilmesini, yeni veriler eklenmesini, bilginin bir kısmının veya tamamının silinmesini engellemeyi hedefler. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır.
- Süreklilik: Bilginin her an ulaşılabilir ve kullanılabilir olmasını amaçlayan prensiptir. Bilişim sistemlerinin kendilerinden beklenen işi sürekli bir şekilde tam ve eksiksiz

olarak yapmasını amaçlamaktadır. Süreklilik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek ve kurumun çalışmalarını engelleyebilecek tehditlere karşı korumayı hedefler. Süreklilik hizmeti sayesinde, kullanıcılar, erişim yetkileri dâhilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilirler. Sistem sürekliliği sadece bir saldırı sonucu zedelenmez, yanlış, bilinçsiz ve dikkatsiz kullanım gibi kullanıcı hataları, yazılım hataları sonucu yazılımların çökmesi gibi yazılım hataları veya donanım sorunları, yangın, su basması, yıldırım düşmesi gibi ortam şartlarındaki olumsuz değişiklikler bu prensip kapsamındadır.

- İzlenebilirlik (Kayıt Altına Alma) : Bu prensip sistemde gelişen her türlü olayın daha sonra incelenmesine olanak sağlayacak şekilde kayıt altına alınmasını kapsar. Kullanıcıların sisteme giriş yapmaları, e-posta alıp göndermeleri, çeşitli servislerin ve yazılımların çalıştırılması veya durdurulması gibi bilgisayar sistemi veya ağ üzerinde meydana gelen her türlü etkinlik olay kapsamına girmektedir. Toplanan kayıtlar incelenmek sureti ile bilinen saldırı türlerine ait kayıtların varlığı veya yeni bir saldırıyı işaret eden sıra dışı kayıtların olup olmadığı kontrol edilerek sistem yöneticilerini uyaracak alarm mesajları üretilebilir.
- Kimlik Sınaması: Kimlik sınaması alıcının, göndericinin veya kayıtlı kullanıcının iddia ettiği kişi olduğundan emin olunmasıdır. En basit şekli ile bilgisayar sistemine giriş yaparken parola girilmesi bir kimlik sınamasıdır.
- Güvenilirlik: Sistemin öngörülen ve beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Sistemin kendisinden beklenen şeyi eksiksiz ve değiştirilmemiş olarak her çalıştırıldığında tutarlı bir şekilde yapması olarak tanımlanabilir.
- İnkâr Edememe: Bu prensip verinin iletildiği gönderici ve alıcı arasında ortaya çıkabilecek iletişim sorunları ve anlaşmazlıkları en aza indirmeyi amaçlar. İki sistem arasında bir bilgi aktarımı yapılmışsa ne gönderen veriyi gönderdiğini, nede alıcı veriyi aldığını inkâr edememelidir.

Bilişim güvenliğinde olması gereken maddelerin belirtilmesinden sonra üzerinde durulması gereken husus, bilişim güvenliğini tehdit eden unsurların gözden geçirilmesidir. Tehdit kavramı; bir sistemin veya kurumun zarar görmesine neden olan istenmeyen olayın arkasındaki gizli neden olarak tanımlanabilir. Her tehdidin bir kaynağı ve bu kaynağın

sistemden yararlandığı bir güvenlik boşluğu vardır. Tehditler nereden geldiklerine bağlı olarak iki şekilde değerlendirilebilirler.

- İç Tehditler: Bu tür tehditlerde güvenliği zedeleyecek davranış kurum içerisinde yer alan bir saldırgan tarafından gerçekleştirilir.
- Dış Tehditler: Kurum dışından bir saldırganın kuruma karşı oluşturduğu tehditler dış tehditlerdir.

Tehditler insan kaynaklı tehditler ve doğa kaynaklı tehditler olmak üzere iki temel guruba ayrılır.

- İnsan Kaynaklı Tehditler: Kötü niyetli olan ve olmayan şeklinde iki kısımda incelenir. Kötü niyetli tehditler; sisteme zarar vermek amacı ile sisteme yapılacak tüm müdahaleler bu başlık altında değerlendirilir. Bu tehdit kaynağı sistemdeki güvenlik boşluklarından yararlanarak, sistemin güvenliğini zedelemeye çalışacaktır. Kızgın eski bir personelin kayıtları silmeye çalışması, dışarıdan bir başkasının ticari sırları çalmak için bilişim sistemine erişmesi gibi tehditler bu kapsamda değerlendirilir.

  Kötü niyetli olmayan tehditler; Eğitimsiz, bilinçsiz, dikkatsiz veya ihmalkâr kullanıcıların hatalarına bağlı olarak ortaya çıkma ihtimali bulunan sorunlardır. Dikkatsiz bir personelin veritabanına zarar vermesi, temizlik personelin farkında olmadan ağ kablolarını yerinden çıkarması gibi kötü niyet olmayan ancak bilişim sistemin güvenliğini zedeleyen bir durumdur.
- Doğa Kaynaklı Tehditler: Deprem, sel, su baskını, yangın, toprak kayması, çığ düşmesi gibi büyük ihtimalle önceden bilinemeyen ve engellenemeyen tehditlerdir. Bu gibi tehditler ciddi şekilde güvenliği zedelemektedir bu yüzden bilişim güvenliği kapsamında yer alırlar (İnt.Kyn.1).

2. WEB TABANLI UZAKTAN EĞİTİM SİSTEMİ (WTUES)

Günümüz internet altyapısının gelişmesi ile artan internet kullanımı, yazılımların web tabanlı hale gelmesine ve bu şekilde hizmet vermesine başlamıştır. Uzaktan Eğitim Sistemleri'de internet ağını kullanarak eğitimlerini, elektronik kitap, elektronik posta, tele konferans görüşmeleri gibi metodlarla yapmaya başlamışlardır. Bu metodların artması ve sürekli geliştirilmesi ile birlikte tüm sistemi kapsayan yapıya Web Tabanlı Uzaktan Eğitim Sistemi (WTUES) adı verilmiştir.

WTUES'nin en önemli avantajlarından birisi, sanal bir kampüs oluşturabilmesi ve eşzamansız (asynchronous) eğitime imkan sağlayabilmesidir. Öğrenciler, eğitmenler tarafından sisteme aktarılan eğitim içeriklerine istedikleri zaman erişebilmekte ve bu kaynaklardan faydalanabilmektedirler. Oluşan bu esneklik ve sistemin maliyet avantajı WTUES'nin oluşmasına imkan sağlamıştır (Carswell and Venkatesh 2002).

WTUES'in günümüzde sayılarının hızla artması ve öğrenci ve eğitimciler tarafından kabul görmesinin en önemli nedeni zamandan ve mekandan bağımsız bir yapı ile çalışıyor olmasıdır. Bundan dolayı iş hayatı nedeniyle zaman sıkıntısı çeken veya eğitimin verildiği yerde bulunamayan kişiler için önemli bir tercih nedeni olmuştur (Aslantürk 2002).

2.1. WTUES'nin Tasarlanması

WTUES farklı bilgisayar alanlarını içinde barındıran bir sistemdir. WTUES'i sadece yazılım olarak düşünmek yanlıştır. Çünkü sistem içerisinde yazılımla birlikte tasarlanması gereken sunucu donanımı, sunucu sistemi, ağ altyapısı ve ağ içerisinde kullanılacak donanım göz önüne alınmalıdır. Farklı bilgisayar alanlarını barındıran bu sistem, bilgi güvenliği konusunda ancak çok titiz bir çalışma ile korunabilir. İnternet ağının tüm dünyaya açık olması ve WTUES'nin sürekli çalışması gerektiğinden dolayı bilgi güvenliği daha çok önem arzetmektedir. Sistem yöneticilerinin sürekli bu sistemin başında bulunmaları ve gözetlemeleri çok zordur. Sistem tasarlanırken WTUES'nin kendi güvenliğini belli bir noktaya kadar kendi yapısı ile sağlayabilecek şekilde tasarlanması gerekmektedir.

2.1.1. Bilgi Güvenliği Stratejisinin Oluşturulması

Bilgi güvenliği stratejisinin oluşturulmasındaki en önemli konu uzman bir takımın oluşturulmasıdır. Bu takımın yöneticisi, yani proje koordinatörü bilgi güvenliğini üst düzeyde değerlendirmeli ve tüm aşamalarda bunun kontrolünü elinde bulundurmalıdır.

WTUES'nin tasarlanmasında düşünülen güvenlik çalışmaları; ağ güvenliği, sunucu güvenliği, yazılım güvenliği, bilginin saklanması ve bilginin düzenli yedeklenmesi şeklinde tespit edilmelidir. Yazılım işlemine geçilmeden önce, tüm sistem ve ağ topolojisi çıkartılarak, hangi noktalarda ne tür iyileştirmeler ve yeni düzenlemeler yapılacağı saptanmalıdır. Bu bağlamda ağ iletişim cihazları ve sunucuları, donanımsal olarak tespit edilmelidir. Ayrıca bu donanımlarda çalışacak güvenli ve performanslı işletim sistemi belirlenmeli, yazılım olarak hangi platformda uygulama yazılacağı kararlaştırılmalıdır. WTUES'nin tasarlanmasında görev alacak takım için, gerek donanım gerekse yazılım olarak özel kuruluşlardan birtakım eğitimler alınabilir. Bu eğitimler donanım ve sunucu alımlarında firma desteği ile oluşturulan eğitimler veya yazılım eğitimi veren özel firmalar aracılığı ile sağlanabilir.

Son olarak takım çalışanları için görevlendirme ve zaman takvimi ortaya çıkarılmalıdır. Bilgi güvenliğini sağlamada herkesin yetkileri belirlenmeli, sunucu, sistem ve yazılım çalışmalarında hassas olarak durulması gerekli noktalar yazılı olarak ortaya çıkarılmalı ve takım çalışanlarına sunulmalıdır. Bilgi güvenliği stratejisinin oluşturulmasındaki aşamalar şu şekilde gerçekleştirilmelidir.

- Proje takımının oluşturulması
- Projede yapılacak güvenlik çalışmalarının tespiti
- Proje takımının bilgi güvenliği hususunda eğitilmesi
- Projedeki güvenlik çalışmalarının görev dağılımının yapılması

2.1.2. Oluşturulan Stratejiye Göre WTUES Tasarımı

Uzaktan Eğitim Sistemi tasarlanmadan önce sistemin performans ve güvenliği açısından ne tür donanım, yazılım ve veritabanı üzerinde çalıştırılacağı belirlenmelidir. Sistem web tabanlı bir sistem olacağı için platformlar incelenmeli ve tasarlanmalıdır

Platform seçimi, önce sunucu üzerine kurulacak işletim sistemi ve bu işletim sistemi üzerinde performanslı çalışacak yazılım ve veritabanı seçimi şeklinde olmalıdır. Ayrıca sunucu donanımı alınırken, alınacak donanımın seçilen platforma uygunluğu ve uzun süre teknik desteğinin olması göz önünde bulundurulmalıdır.

WTUES'nin ağ yapısı, iç ağdan başlayarak dış ağa kadar sunucu trafiğini denetleyen mekanizmalarla desteklenmelidir. Bu mekanizmalar donanım veya yazılım tabanlı güvenlik duvarları, omurga switch ve diğer denetleme yazılımları olabilir. WTUES'nin ağ trafiğini yoğun olarak kullanacağı düşünülerek dış çıkış ucu yani internete bağlantı hızı yüksek kapasitede olmalıdır. Günümüz internet altyapı bağlantılarından en hızlı ve kolay kurulumu olan yapı Metro Ethernet yapısıdır. Bu teknolojiye göre internet bağlantısı sağlanmalı ve yüksek kapasitede bir hız tercih edilmelidir. WTUES için minimum hız 10Mbit şeklinde olmalıdır. WTUES'nin daha güvenli bir ortamda çalışabilmesi için, tüm sistemin korumaya alınması tasarlanmalıdır. Güvenlik duvarları ve ağ donanımlarının dışında virus koruması sağlanmalı, sistemlerin otomatik güncellenmelerini sağlayacak bir yapı tasarlanmalıdır.

Ayrıca WTUES içerisinde bulunan tüm bilgiler güvenli ortamlara yedeklenmeli ve bu yedekleme işlemi otomatik olarak belirli zaman periyotları halinde düzenli devam etmelidir. Bilgilerin daha güvenli ortamlarda saklanabilmesi amacıyla yedekleme üniteleri sisteme dahil edilmelidir. Günümüz Uzaktan Eğitim Sistemi için gerekli içerik ve bilgiler oldukça geniş yer kaplamaktadır. Bu yüzden artık gigabyte kapasitesine sahip alanlar yetersiz kalmakta ve terabyte kapasitesine sahip disk üniteleri gerekmektedir.

2.2. WTUES Ağ Güvenliği

2.2.1. Ana Çıkış Bağlantısı

Bir Uzaktan Eğitim Sistemi'nin verimli çalışmasındaki en büyük etkenlerden birisi de tahsis edilen hattın bant genişliğidir. Web tabanlı öğretimde; sohbet kanalları, görsel veya işitsel içerikler ve tele konferans gibi gerçek zamanlı eğitimler ile birlikte, elektronik posta, forumlar, mesajlaşma işlemleri gibi farklı zamanlarda kullanıcıların girip kullanabildikleri yapılar bulunmaktadır. Üniversite gibi eğitim kurumlarında bugün en çok kullanılan yapı ATM (Asynchronous Transmission Mode) bağlantısıdır. WTUES'nin zamanla büyümesi kaçınılmazdır, büyüyen sistemin en büyük ihtiyaçlarından birisi internet bağlantısında gerekli hız artırımının yapılmasıdır. Ancak Uzaktan Eğitim Sistemi için hız artırımı yapmaya çalışan bir kurum, ATM bağlantısında sorunlar yaşayabilmektedir. Bunun nedeni ise ATM bağlantısında hız artırımlarının donanımsal yönden yüksek maliyetler gerektirmesi ve değişen teknolojiye ayak uydurmasında sıkıntıların olmasıdır. Bundan dolayı günümüzde bu bağlantı sistemi yerini Metro Ethernet bağlantısına bırakmaktadır. Metro Ethernet bağlantısı ise yeni kurulum esnasında veya hız artırımında kolay ve basit yapılandırma ile yüksek hız sağlayabilmektedir. Metro Ethernet sisteminin bilgi güvenliğindeki rolü ise, sistem güvenlik yapılandırma çalışmalarında cihaz içerisinde güvenlik kurallarının daha kolay ve geniş çerçevede yapılabilmesidir. Ayrıca kullanılan teknolojinin yeni olması nedeniyle daha akılcı ve hızlı bir iletişim sağlamaktadır. Herhangi bir iletişim kopukluğunda veya cihaz arızasında onarımı daha kısa sürede tamamlanabilmektedir.

2.2.2. Metro Etherenet Yapılandırması

Metro Ethernet, Metropolitan ağlarda yüksek hızda ethernet paketlerinin uçtan uca taşınmasını sağlayan bir teknolojidir (M. Huynh and P. Mohapatra 2007). Günümüzde yerel ağlarda Ethernet protokolü ile iletişim sağlanmaktadır. Metro Ethernet sistemi de Ethernet mantığı ile çalışır ve bu taşıma kapasitesini Metropolitan ağlarda yüksek hızlarda gerçekleştirir. Yerel ağlarda iletişim 1 Gbit hızlarında çalışmakta ve Metro Ethernet teknolojisi ile bu hızlar Metropolitan ağlarda da başarıyla uygulanabilmektedir. Metro Ethernet teknolojisinde hız artışları kesintiye neden olmaz.

Yüksek hız nedeniyle karşılaştırma yapılabilecek bir teknoloji olan ATM teknolojisinde hız artışında yaşanan port sıkıntısı, Metro Ethernet teknolojisinde yaşanmaz. Günümüzde erişim hızı çok yüksek olan Ethernet teknolojisi yönetimi kolay bir teknolojidir. ATM ise daha karmaşık, yönetimi ve kurulumu zor bir teknolojidir. Ethernet teknolojisinde ağ paketlerinin yapısındaki farklılık, ATM teknolojisine göre daha efektif link kullanımı sağlar. Metro Ethernet bağlantılarında fiber kablo kullanıldığından, bakım işletme sorunları yaşanmamakta, arızaların tespiti ve onarımı daha hızlı olmaktadır. Fiber hatlarda son kullanıcının merkez santraline olan uzaklığı önemli değildir. Metro Ethernet sistemi 50 km üzerindeki mesafelerde de sorunsuz çalışmaktadır. Bakır hatlarda bu mesafe maksimum 10 km dir. Ethernet teknolojisi sürekli geliştiğinden teknoloji eskimesi gibi bir problem yaşanmayacaktır. Metro Ethernet tarifeleri şu anda diğer teknolojilere göre çok daha ucuz bir sistemdir.

Metro Ethernet VLAN yapısı üzerine kurulu bir teknolojidir. VLAN fiziksel olarak aynı ortamı paylaşan veya aynı kablo üzerinden iletişim yapan yerel ağa bağlı kullanıcıları sanki farklı noktalardaymış gibi yapılandıran yönteme verilen isimdir. VLAN sayesinde kullanıcılar fiziksel bölgesinden bağımsız olarak gruplanabilir ve farklı ağlarda çalışıyormuş gibi bir yapılandırma yapılabilir. Bir LAN (Local Area Network) ağını, farklı VLAN'lar olarak ayırmak ve yapılandırmak tek başına bir güvenlik önlemi sayılmamakla beraber, güvenlik çalışmalarında yapılması gereken önemli bir adımı teşkil etmektedir. VLAN'lar tamamen yazılımsal bir işlemdir ve genellikle switch cihazları üzerinde yapılandırılırlar ve bunun neticesinde daha esnek ve kullanışlı bir yapı sunarlar (Dennis M. Seymour 2004).

2.2.3. Uzak Yerleşke Bağlantıları

Bazı bölgeler hala ATM teknolojisi ile internet bağlantılarını sağlamaktadırlar. Bunlar özellikle, Uzaktan Eğitim hizmeti veren birime bağlı ancak fiziksel olarak o birimden uzak yerleşkelerdir. Uzak yerleşkelerde ağ alt yapısı herzaman gelişmiş teknolojiye imkan vermez. Böyle yapıda olan uzak yerleşkelerin internet bağlantılarında sıkıntı yaşamamaları için bağlantıları merkez bağlantıya alınmalıdır. Yani internet bağlantıları önce merkeze kadar ATM sistemi ile sağlanmalı, merkezde ise Metro Ethernet ağına dahil edilmelidir. Böylece tüm uzak yerleşke bağlantıları Uzaktan Eğitim hizmeti veren merkez birime yerel ağ ile

birbirine bağlanmış ve Metro Ethernet bağlantısı ile internete erişimleri sağlanmış olmaktadır.

ATM sisteminde router cihazları seri bağlantı ile haberleşerek farklı iki ağın haberleşmesini gerçekleştirir. Seri bağlantıda ise router cihazları tek başlarına işlemi gerçekleştiremezler. Bundan dolayı hattın uç noktalarında sisteme uygun modem cihazları konulmaktadır. Birime bağlı tüm uzak yerleşkelerin bu şekilde yapılandırıldığı düşünülürse, tüm yerleşkeler için bir güvenlik sorunu söz konusu olmaktadır. Ancak bu yerleşkelerde güvenliği üst düzeyde tutmak amacıyla birtakım iyileştirmeler gerçekleştirilmelidir. Tüm yerleşkeler merkez LAN ağının birer parçasıymış gibi merkez ağa dâhil edilmeli ve bu şekilde güvenlik politikaları, yerleşkelere uygulanarak internet ağına erişim sağlanmalıdır.

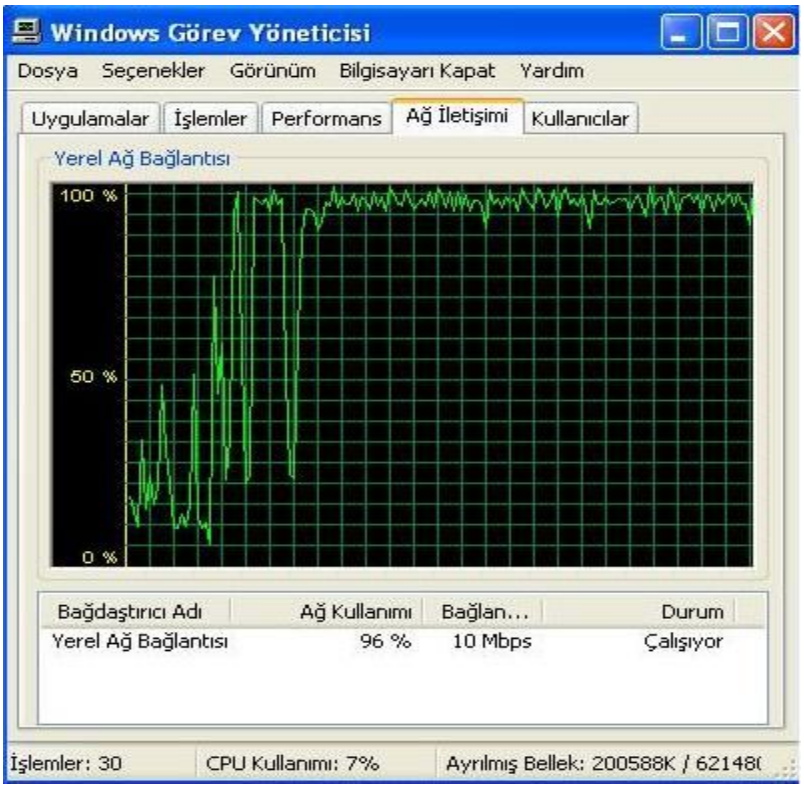
Uzak yerleşkeler güvenlik zafiyetlerinden dolayı çok sık saldırılara maruz kalabilmekte ve bu saldırılardan dolayı ana merkezde bulunan sunucu ve cihazlar sıkıntı çekebilmektedirler. Bu yüzden tüm yapılandırmalar hem yerleşkede bulunan router cihazı üzerinde, hem de ana merkezde bulunan router cihazı üzerinde gerçekleştirilmelidir.

2.2.4. İç Ağ Bağlantıları

internet bağlantısı ve uzak yerleşke bağlantılarının yapılandırılmasından sonra, yapılması gereken sunucu ve iç ağ bağlantılarının yapılandırılmasıdır. İç ağ üzerinde, eğitmenlerin kullandıkları sistemler ile sunucu sistemleri bulunmaktadır. Böyle bir yapı için gerekli olan sağlıklı LAN (Local Area Network) yapılandırma işlemidir. Uzak yerleşke bağlantılarınında aynı yerel ağa bağlanacağı düşünüldüğünde, ağ üzerindeki yoğunluk artacaktır. Tüm bu bağlantılar için gelişmiş özelliklere sahip switch kullanılmalıdır. Buradaki amaç, iç ağı tek bir LAN şeklinde değil, birkaç farklı yerel ağ olarak tanımlamaktır. LAN üzerindeki bu tanımlamaya sanal LAN anlamında (Virtual LAN-VLAN) adı verilmektedir. Böylece ağlar arasında oluşabilecek güvenlik sorunları ve virus saldırıları en aza indirilmiş olacaktır. Ayrıca sunucu VLAN ağı için, farklı konfigrasyonlar tanımlanarak güvenliği artırılmalıdır.

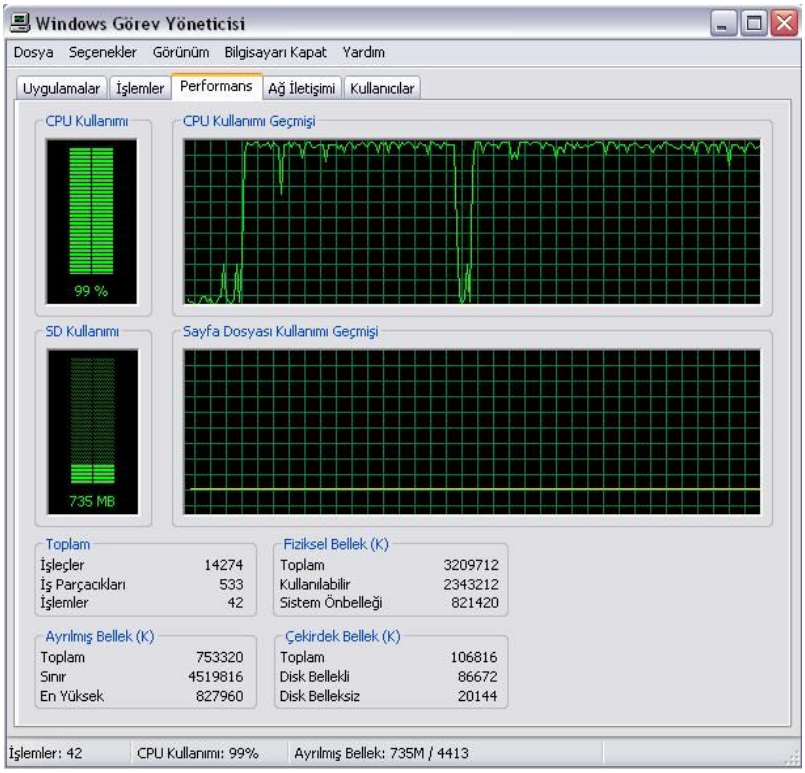
2.2.4.1. VLAN Yapılandırma İşlemi

Ağ güvenliğinin korunması amacıyla VLAN yapılandırmasının gerektirdiği en büyük etkenlerinden birisi şüphesiz virüs ve worm saldırılarıdır. Ağ tek bir LAN olarak yapılandırıldığında, herhangi bir noktadan başlayan ataklar veya rastgele ağa gönderilen paketler tüm sistemi ve kaynakları yormaktadır. Diğer yandan hem sunucu güvenliğini tehdit etmekte hem de diğer kullanıcı bilgisayarlarına rahatlıkla bulaşabilmektedir. Bunun neticesinde ağ yönetimi için çözümü zor süreçler başlamaktadır. Tüm ağ farklı LAN'lara bölünerek VLAN olarak tasarlandığı durumda ise, ilgili paketler sadece o VLAN üzerindeki adreslerde dolaşacağı için herhangi bir atak veya paket saldırılarından sadece ilgili VLAN etkilenecektir. Yönetici için sorunlu kullanıcıyı tespit etmek zor olmayacak ve kısa sürede sorunlar giderilecektir. Resim 2.1 üzerinde virüslü bir bilgisayarın ağ üzerinde saldırıya başladıktan sonraki durumu gösterilmektedir. Normal bir bilgisayarda ağ kullanımı %0-1 arasında olduğu halde, burada %96-100 gibi değerlere tırmanmıştır. Bu bilgisayar ağdaki diğer kaynakları ve cihazları kısa bir süre sonra iletişim yapamaz hele getirmektedir.



Resim 2.1 Virüslü bir bilgisayarın ağ iletişiminin yoğunluğu

Resim 2.2 de farklı bir virüsün, kendini aktif ettikten sonra işlemci üzerinde nasıl bir etki yaptığı görülebiliyor. Virüsün çalıştırmış olduğu işlem kapatıldıktan sonra bile tekrar devreye girmesi ve işlemciyi %100 gibi değerlerde, kullanıcının farkında olmadan çok farklı işlemler yapması muhtemeldir.



Resim 2.2 Virüslü bir bilgisayarın işlemci yoğunluğu

2.2.4.2. Switch Üzerinde VLAN Yapılandırma İşlemi

Tüm ağı besleyen cihazların başında kenar switch ve hub aygıtları gelir. Ancak hızlı ağlar ve daha güvenli bir yapı oluşturmak için üzerinde gelişmiş yazılımı olan switch cihazları kullanılmalıdır. Sunucu ağını besleyen switch GigaBit hızında olursa haberleşme daha verimli çalışır, ancak GigaBit hızıyla çalışabilmesi için sunucu ağ kartlarınında aynı hızı destekliyor olması gerekmektedir. Eğer iç ağdaki haberleşme çok yoğun ve switch sayısı çok fazla ise tüm switch cihazlarını bir araya getirmek gerekir. Bu ise omurga switch adı verilen daha kapsamlı bir ağ iletişim cihazının ağ üzerine entegre edilmesi ile mümkündür. Tüm ağ trafiği

bu şekilde rahatlıkla kontrol edilebilir. Ayrıca VLAN uygulamaları ve güvenlik kuralları daha etkileşimli bir şekilde gerçekleştirilebilir.

VLAN yapılandırılmasına geçilmeden önce fiziksel olarak ilgili ağ kablolarının omurga üzerinde hangi uçta takılı olduğunun belirlenmesi ve o porta göre yapılandırılması gerekmektedir. Eğer çok sistemli bir yapı oluşturulacaksa tüm VLAN planı, omurga cihazı üzerindeki portlara gore belirlenmelidir. İç ağ kablolarının hangi portlara takılacağı yazılı bir plan haline getirildikten sonra işleme tabi tutulmalıdır.

Omurga switch üzerinde toplanan tüm iç ağ, farklı ağlarla iletişime gereksinim duyacaktır. Ağ üzerindeki iç ağ trafiği omurga switch tarafından kolalıkla sağlanır ancak başka bir ağa bağlantı gerektiğinde durum farklıdır. Bu nedenle farklı ağlara bağlantı için ağ çıkış noktası olarak ağ geçidi (default gateway) oluşturulmalıdır. Her bir VLAN için ilgili IP aralığına bağlı bir ağ geçidi tanımlanmalıdır.

Ağ geçidi tanımı yapılırken ağ geçidinin hangi noktaya erişim sağlayacağı belirtilmelidir. Bu erişim, farklı ağa bağlı bir firewall veya router cihazının IP numarası olabilir. Ağ üzerinden dış ağa giden paketler ağ geçidi ile bağlantısı sağlanırken, gelen paketlerinde bu ağa erişimi sağlanmalıdır. Aksi halde tüm sistem kendi arasında haberleşmesine rağmen diğer ağlara erişemeyecek veya internete bağlanamayacaktır. Bu yüzden gelen paketler için yönlendirme satırı tanımlanmalıdır.

2.2.4.3. VLAN Yapısı için DHCP Sunucu Yapılandırma İşlemi

İç ağ üzerindeki bilgisayarın IP yapılandırmaları eğer DHCP (Dynamic Host Configuration Protocol) sunucusu tarafından otomatik olarak yapılıyorsa, VLAN yapısı için sunucu ayarlarının tekrar düzenlenmesi gerekmektedir. Çünkü DHCP sunucusu, tüm LAN için IP numarası dağıtırken, VLAN yapısına geçilmesinden sonra her VLAN için farklı guruplarda ve belirlenen aralıklarda IP numarası dağıtması gerekmektedir. Sunucunun bu şekilde yapılandırılması ile birlikte bu yapıyı omurga switch üzerinde tanımlamak gerekmektedir. Oluşturulan her VLAN IP aralığının düzenli çalışması için omurga switch üzerinde VLAN tanımlamaları bölümünde DHCP sunucu tanımlaması yapılmalıdır.

2.2.4.4. Omurga Switch Üzerinde Hat Kalitesinin Artırılması (QoS)

Hizmet Kalitesi (QoS-Quality of Service) isminden de anlaşılacağı üzere ağ içinde sunulan hizmet kalitesi demektir ancak burada yapılan çalışma hizmet kalitesinden ziyade veri akışının denetlenmesi şeklindedir. Günümüz internet teknolojileri çok fazla multimedya içeriği barındırmaktadır. Ancak bu içeriklerin ağ üzerinde taşınmasını garanti eden bir servis mevcut değildir. Hangi teknoloji kullanılırsa kullanılsın verimliliği artırıcı çalışmalar yapılmadığı müddetçe, kullanılan teknoloji çok ilerde bile olsa sıkıntılar çıkacaktır. Uzaktan Eğitim Sistemleri'nde multimedya içeriklerinin etkin bir şekilde kullanılması gerekmektedir. İçerikler ağ üzerinde çok fazla yoğunluk yaşatırlar. Bu yoğunluğa rağmen, ağ üzerinde multimedya trafiğinin verimli bir şekilde çalışması garanti altına alınmalıdır. Bu trafiğin düzenlenmesindeki en verimli yapılandırmalardan birisi QoS tekniğinin kullanılmasıdır. Özellikle farklı uygulamalar için bant genişliğinin belirlenmesi sağlanarak ağ verimliliğinin uygulamalara ve protokollere göre düzenlenerek artırılması sağlanabilmektedir (Guillauma Jourjon 2007). QoS tekniği omurga switch üzerinde gerçekleştirilmiştir. Cihazın QoS yapılandırmasındaki en önemli nokta Access List kavramıdır.

2.2.4.5. Access List Kavramı

ACL (Access List) cihaz üzerine gelen paketleri yönlendirmek ya da silmek üzere inceleyen yazılımsal bir yapıdır. ACL karar mekanizması; kaynak IP adresi, hedef IP adresi, 3. katman protokolü (ICMP ya da IP) ve üst katman port numaralarından oluşur. ACL oluşturulurken her bir kural satır şeklinde sırayla listeye tanımlanır. Bir koşul sağlandığında duruma göre pakete izin verilir ya da geri çevrilir (permit, deny). Tanımlama yaparken; her bir protokol için, her bir yön için (in, out) ve her bir uç için ayrı komut satırları uygulanır. Ağ sisteminin VLAN yapısından oluşması farklı portların ve farklı gurupların oluşturulabilmesine imkân tanır. Guruplar arası güvenlik yönetimi ve veri iletişim yapılandırmaları en verimli ACL kullanımı ile sağlanmaktadır (Ido Dubrawsky 2007).

2.2.5. Üst Düzey Güvenlik İçin IPS Cihazı

IPS (Intrusion Prevention Systems-Saldırı Tespit ve Önleme Sistemleri) donanımsal çalışan güçlü bir ağ güvenlik teknolojisidir. Bu teknoloji tamamen donanımsal bir yapı olmakla birlikte, kendini internet ortamında sürekli güncelleyen bir yazılım teknolojisini de barındırır. Ağ üzerinde firewall veya ağın giriş çıkış uç noktalarına takılabilir. Ağ üzerinde paketler IPS cihazından geçerken yasallığı ve güvenliği kontrol edilmesi için her açıdan denetlenir. Bu anlık koruma sistemi hedeflenmiş tüm saldırıları en etkin biçimde amacına ulaşmadan bertaraf etmenizi sağlar. TippingPoint IPS teknolojisi performans güvenliği ve altyapı güvenliği konularında gigabit hızında paket denetimi yapabilmektedir. Paketlerin tüm katmanlarını detaylı bir şekilde inceler. Üstün uygulama koruma kapasitesi sayesinde dâhili ve harici saldırılara hızlı, kesin ve güvenilir müdahale imkânı sağlamaktadır (İnt.Kyn.2).

2.2.5.1. IPS Cihazının Özellikleri

- IPS cihazı sadece paket taraması yapmaz, ayrıca sistem içerisindeki tüm protokoller ve portlar için bant genişliği yapılandırma yapılabilmesine olanak sağlar. Örneğin FTP (File Transfer Protocol) kullanımı 4 Mbit ile sınırlandırılabilir veya video iletişimi 2 Mbit olarak belirtilebilir. Bunun neticesinde QoS hizmeti burada da gerçekleştirilebilir.
- Diğer önemli özelliklerinden birisi de sadece saldırı tespiti değil, virüs, trojan veya birtakım casus yazılımların içerisindeki kötü amaçlı paketleri inceleyerek ağa girişine izin vermez. Böylelikle iç ağda virüs koruması olmayan bilgisayarlar veya sunucular korunmuş olur.
- Msn tarzı mesajlaşma programları için yine engellemeler veya kısıtlamalar konulabilir.
- Farklı gruplar veya IP aralığı belirtilerek sadece VLAN veya ilgili ağa özel iletişim kuralları veya kısıtlamalar uygulanabilir.
- Günlük veya aylık sistem saldırıları loglar halinde tutulur ve daha sonra sorgulanabilir. Gerekli analizler grafiksel olarak görüntülenebilir.

2.2.5.2. IPS Cihazının Kullanımı

Cihazın tüm yönetimi kendi içerisinde bulunan program arayüzü tarafından sağlanmaktadır. Cihazın yönetim aşamasında kısaca işlevler ve özellikleri anlatılmaktadır.

- Profil Oluşturma: Bu kısımda, ağ için bant genişliği limitlerini belirtmek, sorunlu paketleri durdurmak veya bazı özel durumlar için izin vermek gibi tanımlamalar gerçekleştirilmektedir.
- Ağ üzerinde çalışan uygulamalara, oluşturulan profiller atanarak kısıtlama, izin veya kesme işlemleri yapılmaktadır.
- İç ağdan veya dışarıdan gelen saldırı ve engellemeler bu arayüz vasıtasıyla görüntülenebilmektedir. Belirli zaman dilimleri olarak veya güvenlikte oluşturduğu duruma göre izlenimler ve raporlar alınabilmektedir. Güvenlik tehdidi algılanıyorsa sistem bunu durduracak ve e-posta göndererek uyaracaktır.

2.3. Sunucu Güvenliği

İnternetin yaygınlaşması ve kurumların iç ağlarını global ağa bağlaması sonucunda bilgi güvenliği tehlikeleri artmaya başlamıştır. Sunucu güvenliği, diğer güvenlik çalışmaları gibi ciddiyet gerektiren bir iştir. Sunucular için güvenlik çalışmasına başlamadan önce hangi sunucuda ne tür yazılımlar ve servisler çalışacağı belirlenmeli ve sistem şematik olarak tasarlanmalıdır. Sunucunun ne amaçlı kullanılacağı bir çizelge üzerinde belirlenmeli ve temel işlevi dışında hiçbir yazılımın kurulmasına izin verilmemelidir. Sunucu üzerinde işlem yapacak yetkiler daha önceden belirlenmeli ve özellikle sunucu yöneticisinin, bu konulara çok hassas yaklaşan kişilerden seçilmesine özen gösterilmelidir. Sunucuyu sadece bir defaya mahsus yapılandırmak kesinlikle yetmez, önemli olan sunucunun hem donanımsal hem de yazılımsal bakım ve güncellemelerinin yapılması gerekir. Diğer önemli hususlardan birisi ise, makinenin sürekli çalışacak olması, durması veya güvenliğinin tehlikeye girmesi durumunda çok ağır neticeler verecek olmasıdır. Kaybedilen bilgi ve zamanın insan hayatında telafisi mümkün değildir.

2.3.1. Firewall Sunucusu

Bilgi güvenliği yapılandırması için, sistem içerisindeki ağ iletişimine çok iyi hâkim olunması gereklidir. Firewall burada trafik polisi vazifesini görür ve her türlü denetimi gerçekleştirir. Firewall sunucusu ağ üzerinde birtakım kuralları çalıştırarak bu denetlemeyi gerçekleştirir. Ayrıca oluşan trafiğin takibi ve ağ paketlerinin kayıt altına alınması maksadıyla kullanılabilir. Ağ üzerinde ne tür kuralların çalışması gerektiği ise, tamamen kurulan sistemle ve alınmak istenen güvenlik önlemleriyle alakalıdır. Ağ üzerindeki yeri çok önemlidir ve ağ trafiğine hâkimiyeti gerektirir. Sunucu üzerine ağ trafiğini denetlemesi açısından birden fazla Ethernet kartı takılabilir. Bu kartlara ilgili ağa bağlı olarak IP yapılandırması yapılarak Firewall kuralları tanımlanabilir.

Günümüzde farklı tip Firewall yazılımları mevcuttur, bunlar işletim sistemlerine göre farklılık göstermektedir. Özel ticari yazılım veya açık kaynak kodlu yazılımlar olarak kullanılabilmektedir. Örnek olarak Linux işletim sistemi üzerinde çalışan açık kaynak kodlu Iptable yazılımı incelenmiştir.

2.3.1.1. Iptable paketi

Iptable: Ağ iletişimi üzerinde çalıştırılması düşünülen kuralları uygulayan servistir. Kendi formatında kurallar yazılır ve kaydedilir. Kurallar sistem açılışında devreye girer ve uygulanmaya başlar. Iptable üzerinde uygulanacak kurallarda kullanılan bazı terimler ve açıklamaları şu şekildedir (İnt.Kyn.3).

Zincir: Iptables işlemleri için INPUT, OUTPUT, FORWARD gibi temel kural zincirleri (chain) kullanılabildiği gibi kişisel zincirler de oluşturulabilir. Her zincir altında o zincire ait kurallar tanımlanır.

- INPUT: Sunucuya gelen paketlerin kontrolüdür. Bir paket sunucuya geldiğinde bu kural zinciri tarafından incelenir ve yorumlanır.
- OUTPUT: Sunucudan çıkan paketleri inceleyen ve zincirdeki kurallara göre yorumlayan kuraldır.
- FORWARD: Sunucu üzerinden geçen paketlerin yönlendirilmesi işlemini yürüten kuraldır.

Zincir yönetiminde kullanılan parametreler:

- -N: Yeni zincir ekleme
- -X: Boş zincir silme
- -P: Temel zincirdeki kuralı (policy) değiştirme
- -F: Zincirdeki kuralları boşaltma
- -Z: Zincirdeki paket ve byte sayacını sıfırlama

Zincirlere kural tanımlama parametreleri:

- -A: Zincire yeni kural ekleme
- -I: Zincirde herhangi bir konuma kural ekleme
- -R: Zincirde herhangi bir konumdaki kuralı değiştirme
- -D: Zincirdeki herhangi bir kuralı silme

Zincirdeki kuralların yönetiminde kullanılan parametreler:

- -p: Protokol (tcp, udp, icmp ve all)
- -m: Protokol içerisinde daha detaylı işlem için modül seçimi
- -s: Kaynak makine (IP numarası / ağ maskesi)
- -d: Hedef makine (IP numarası / ağ maskesi)
- -i: Giriş (INPUT) işleminde kullanılacak arabirim
- -j: Uygulanacak kural
- -o: Çıkış (OUTPUT) işleminde kullanılacak arabirim
- -t: Kullanılacak zincir
- --sport: Kullanılacak kaynak port
- --dport: Kullanılacak hedef port
- ! : olmayan manasında kullanılır

Kuralın davranış şekilleri:

- ACCEPT: Bir zincirdeki varsayılan seçenek olarak algılanır.
- DROP: Zincir kuralının uygulanması halinde paketin engelleneceğini gösterir.
- REJECT: DROP gibi paketi engeller fakat sonucunda geriye reject sinyali döndürür.
- RETURN: ACCEPT gibi paketi kabul eder sonucunda geriye return sinyalini döndürür.

NAT (Network Address Translation-Ağ Adres Dönüşümü): NAT işlemi sistem için gerekli bir işlemdir ve internet bağlantısını paylaştırmak, sunucu yükünü paylaştırmak ve yapılandırılan squid proxy işlemini düzgün yürütmek amacıyla kullanılır. NAT özelliği temel olarak iki bölümden oluşur. Kaynak NAT (SNAT) ve Hedef NAT (DNAT).

SNAT (POSTROUTING): Kaynak adres üzerinde bir değişiklik yapılmak isteniyorsa kullanılır. Maskeleme (Masquerading) işlemi SNAT ile yapılır. İç ağdan gelen paket SNAT işlemi sonucunda, dış ağa, sanki firewall sunucusunun IP adresinden geliyormuş gibi iletilir ve karşı bilgisayardan gelen sonuç ise yine sunucu tarafından istek yapan IP' ye iletilir.

DNAT (PREROUTING): Hedef adres üzerinde bir değişiklik yapılmak isteniyorsa kullanılır. Örneğin herhangi bir bilgisayara gelen paketi, iç/dış ağdaki başka bir bilgisayara yönlendirilmek isteniyorsa DNAT kuralı ile işlem yapılır. Paket sunucuya gelir, fakat bu işlem sonucunda, paket hedef adresi değiştirilmiş olarak yoluna devam eder. Transparent proxy, port yönlendirme, yük paylaşımı (load sharing) gibi işlemlerde bu kural kullanılır.
Bu işlemler için -t nat parametresi ile belirlenen iptable kuralının NAT ile ilgili komutu kullanılır. Bu yüzden nat işlemlerini kullanmak için, ilk olarak -t nat parametresinin kullanılması gerekiyor. Daha sonra ise yapılacak işlemlere göre -A parametresinden sonra POSTROUTING ya da PREROUTING kuralı kullanılır. Fakat burada dikkat edilmesi gereken nokta PREROUTING işleminde sadece giriş parametrelerinin, POSTROUTING işleminde ise sadece çıkış parametrelerinin kullanılması gerektiğidir.

- PREROUTING komutu: -j [DNAT,REDIRECT] pakete uygulanacak işlemi belirler.
- DNAT komutu: Paketin hedef adresini değiştirir ve yollar.
- REDIRECT komutu: Paketi hedef adresini değiştirmeden başka bir adrese iletir. (Transparent proxy işlemleri)
- POSTROUTING komutu: -j [SNAT, MASQUERADE] pakete uygulanacak işlemi belirler.
- SNAT komutu: Paketin kaynak adresini değiştirme işlemini gerçekleştirir.
- MASQUERADE komutu: Pakete maskeleme işlemini uygular. Bu işlem sonucunda paketin kaynak adresi ve kaynak portu, sunucu adresi ve boş bir port ile eşlenerek hedefe yollanır.

2.3.1.2. Squid Paketi

Squid: Proxy görevini yapan bir yazılımdır. Ancak bilgi güvenliğinde kullanılma amacı, sisteme yapılan her işlemi kayıt altında tutmak ve saklamaktır. Squid bu amaca göre yapılandırılabilir ve log adı verilen kayıt tutma işlevini yapmak üzere görevlendirilebilir. Squid yazılımının tutmuş olduğu logları incelemek için yine bir yazılıma gerek duyulmaktadır. Ntop isimli yazılımı kullanarak, tüm sistem üzerinde yapılan işlemler ve trafik görüntülenebilmektedir. Eğer herhangi bir güvenlik ihlali yapan bilgisayar IP si tespit edilirse bu IP firewall üzerine yazılacak kurallarla engellenebilir. Ayrıca yine squid üzerinde transparent proxy oluşturarak iç ağdan internete bağlanan kullanıcıların daha verimli sayfa taraması ve ağda fazla yük oluşturmadan işlem yapabilmelerini sağlayacak bir yapı oluşturulacaktır. Transparent Proxy olması, internet tarayıcı ile bağlanırken herhangi bir ayar gerektirmeden yani kullanıcıya hissettirmeden çalışıyor olması demektir. Bu işlem, ağ üzerindeki kullanıcılar bir sayfaya bağlanırken, bağlanılan bu sayfaları, kendine ayrılan diskte saklar. Diğer kullanıcıların aynı yöne bağlantı istekleri durumunda, kendi sakladığı içerikleri kullanıcıya sunar. Her seferinde ilgili adrese gidilmemesini sağlar ve verimliliği artırır.

Squid yapılandırması squid.conf dosyası üzerindeki ayarları düzenlemekle yapılabilmektedir. Dosya içersine girildiğinde birtakım ayarlar ve açıklamalar yer almaktadır. Sistem için tasarlanan yöntem Transparent Proxy oluşturmaktır.

2.3.1.3. Squid Kullanımı ve Ntop Yazılımı

Squid işlemi çalıştırıldıktan sonra arka planda ilgili dosyalara yazma işlemini başlatır. Ancak sistem yöneticisinin ağ takibini yapabilmesinde bu dosyalardan bakarak takip etmeye çalışması oldukça zordur. Bundan dolayı Squid log dosyalarını okuyan ve analiz çıkartan farklı yazılımlar mevcuttur. Sağlıklı ağ takibi yapabilmek amacıyla Ntop isimli bir yazılımı firewall sunucusu üzerine entegre edilebilir. Kurulumu çok basit olan yazılımın en büyük özelliği ise ağ istatistiğini çıkarması ve hangi bilgisayarların ne kadar ağ kaynaklarını harcadığını göstermesidir. Ayrıca IP bazlı olarak bir bilgisayarın ne zaman hangi sitelere bağlandığı veya hangi IP adresleri ile iletişime geçtikleri gibi sonuçları sistem yöneticisine bildirebilmektedir.

2.3.2. Web ve Veritabanı Sunucuları

Web tabanlı yazılım geliştirmek için programcılar açısından çok fazla platform bulunmamaktadır. Bunun yanında hızlı, esnek ve görsel program geliştirmek, Uzaktan Eğitim Sistemleri'nde büyük önem arz etmektedir. WTUES'inde sunucu modeli olarak Microsoft işletim sistemleri örnek olarak seçilmiştir. Uygun yazılım geliştirme aracı olarak Microsoft ürün ailesinden Visual Studio 2005 yazılımı ve bununla birlikte veritabanı sistemi Microsoft SQL Server 2005 seçilmiştir. Tüm bu sistemlerin düzenli çalışabileceği sunucu ortamı ise Microsoft sunucu ailesine ait bir işletim sistemidir. Bundan dolayı işletim sistemi olarak Microsoft Server 2003 sistemi incelenmiştir.

2.3.2.1. Windows 2003 Server

Windows Server 2003 ürün ailesi, bilişim teknolojileri verimliliğinin ve yazılım üretiminin sağlıklı bir şekilde artması için ölçeklenebilir altyapı oluşturan sunuculardan oluşmaktadır. Windows 2000 sunucu teknolojisinin en iyi özelliklerini baz alarak geliştirilmiş hizmetlere sahiptir. Bu hizmetlerin yanı sıra Microsoft .NET desteğine sahiptir ve .NET vizyonunun teknolojik altyapısını oluşturan .NET Framework, Windows Server 2003 ile birlikte yüklü gelmektedir.

Windows Server 2003, çok amaçlı bir işletim sistemidir. Merkezi ya da dağıtık olarak ihtiyaçlar doğrultusunda çok çeşitli roller üstlenebilir. Windows Server 2003 ile birlikte IIS (Internet Information Services-Microsoft Web Sunucusu) 6.0 sürümüyle gelmektedir. IIS 6.0, daha önceki 5.0 ve 5.1 sürümlerine göre güvenlik geliştirmelerine sahiptir. Aynı zamanda IIS hizmeti Windows Server 2003'ü kurulduğunda varsayılan olarak güvenlik nedeniyle kapalıdır. Buradaki amaç, sistem yöneticisinin hangi hizmete ihtiyacı varsa, bilinçli ve kontrollü bir şekilde ilgili hizmeti başlatmasını sağlamaktır (İnt.Kyn.4).

2.3.2.2. Web Sunucusu IIS 6.0

Windows Server 2003 içerisinde gelen web sunucu yazılımını yapılandırmadan önce Framework sistemini de gözden geçirmek gerekir. Framework .NET ortamında hazırlanan

yazılımı bilgisayar alt dillerine dönüştüren bir sistemdir ve sunucu ile birlikte gelir. Eski versiyonu 1.0 olan sistem, Server 2003 üzerinde 2.0 ile birlikte gelmektedir. Bu yüzden IIS, sürüm farklılığından dolayı üzerinde sorunlar olabilmektedir. Kodlama Framework 2.0 sürümüne göre hazırlanmışsa IIS sistem sürümü de Framework 2.0 olarak ayarlanmalıdır. Bazı sistemlerde ise IIS, 2.0 olmasına rağmen Framework başka bir sürüme göre ayarlı kalabiliyor, bunu düzenlemek için; Framework'ün yüklü olduğu dizinde yer alan "aspnet_regiis.exe" isimli dosyayı "-i" parametresi ile komut satırında çalıştırmak gerekir.

IIS üzerinde güvenlik ayarları basit ama çok önemlidir. Yapılan küçük bir hata bazı dosyalara yetkisiz kişiler için müdahale hakkı oluşturabilir. IIS yapılandırması ile birlikte, sistemin bilgi güvenliği açısından bir sertifika ile desteklenmiş olması bilgi güvenliğini artırıcı bir işlemdir. SSL (Secure Socket Layer- Güvenli Yuva Katmanı) sertifikaları, sunucu ile iletişim yapmak isteyen diğer bilgisayarlar arasında karşılıklı kimlik doğrulama işlemini gerçekleştirirler. Bu işlem ağ üzerinde kimlik oluştururken kullanılan bilgileri içerir. Geleneksel kimlik formlarına benzeyen sertifikalar, bir bağlantı kurulmadan önce birbirlerinin kimliklerini denetlemeleri için Web sunucularını ve kullanıcıları etkinleştirir.

Sunucu sertifikaları, önemli bilgileri paylaşmadan önce istemcinin sunucuyu tanımasını sağlayan bilgilerdir. İstemci sertifikaları, siteye erişim isteyen istemcilere izin vermeden önce onları tanımayı sağlayan kişisel bilgiler içerir.

2.3.2.3. Veritabanı Sunucusu MSSQL Server 2005

Veritabanı sunucusu olarak önemli güvenlik çalışmalarının yapılması gerekmektedir. Çünkü veritabanı sunucularının da kendilerine ait kullanıcıları ve bu kullanıcılara ait farklı erişim tipleri bulunmaktadır. Ayrıca kullanıcı için daha özel izinler ve haklar belirlenebilmektedir. MSSQL sisteminin güvenliği 4 aşamadan oluşmaktadır. MSSQL Server Kimlik Doğrulama Kipleri, Sunucu Oturumları, Roller ve İzinler şeklinde belirlenmektedir.

MSSQL Server Kimlik Doğrulama Kipleri: MSSQL Server üzerinde iki tür kimlik doğrulama kipi vardır.

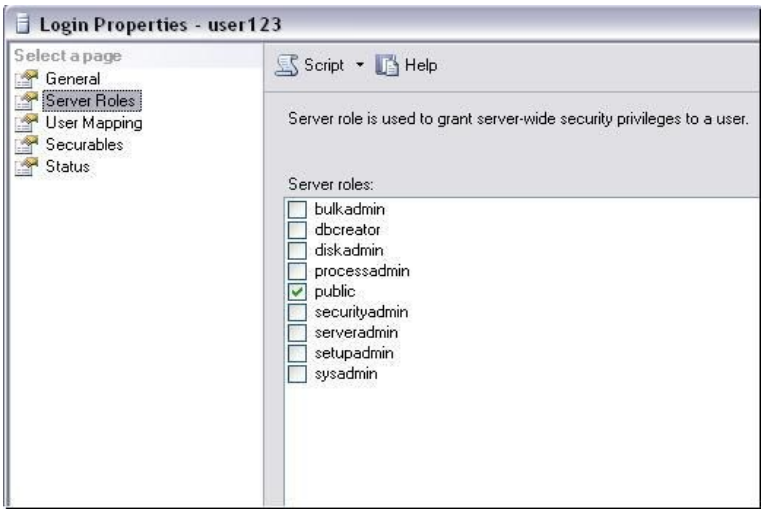
- Windows Authentication Only: Windows etki alanında bulunan kullanıcı ve grup hesaplarının kullanımı ile yapılan girişlerdir. Bir Domain (etki alanı) hesabına kayıtlı

kullanıcılar veya sunucu bilgisayarın kendi kullanıcıları, hakları doğrultusunda MSSQL Server için ayrıca kullanıcı adı ve şifre tanımlanmadan veritabanlarına erişim yapılabilirler.

- Karma Güvenlik: Veritabanlarına farklı sunucu veya sistemlerden bağlantılar oluyorsa Karma Güvenlik kipi ile erişim sağlanılabilir. Bunun için MSSQL Server üzerinde farklı kullanıcı adları ve şifreler tanımlanarak her kullanıcı için ayrı hesap oturumları oluşturulur.

Sunucu Oturumları: İki tür kimlik doğrulama kipi bulunduğu gibi yine iki tür sunucu oturumu mevcuttur. Etki alanın oturumlarını etki alanında, yerel kullanıcı hesabını yerel grup hesaplarında, evrensel veya genel etki alanı grup hesapları olabilen, etki alanı hesapları oluşturulabilir.

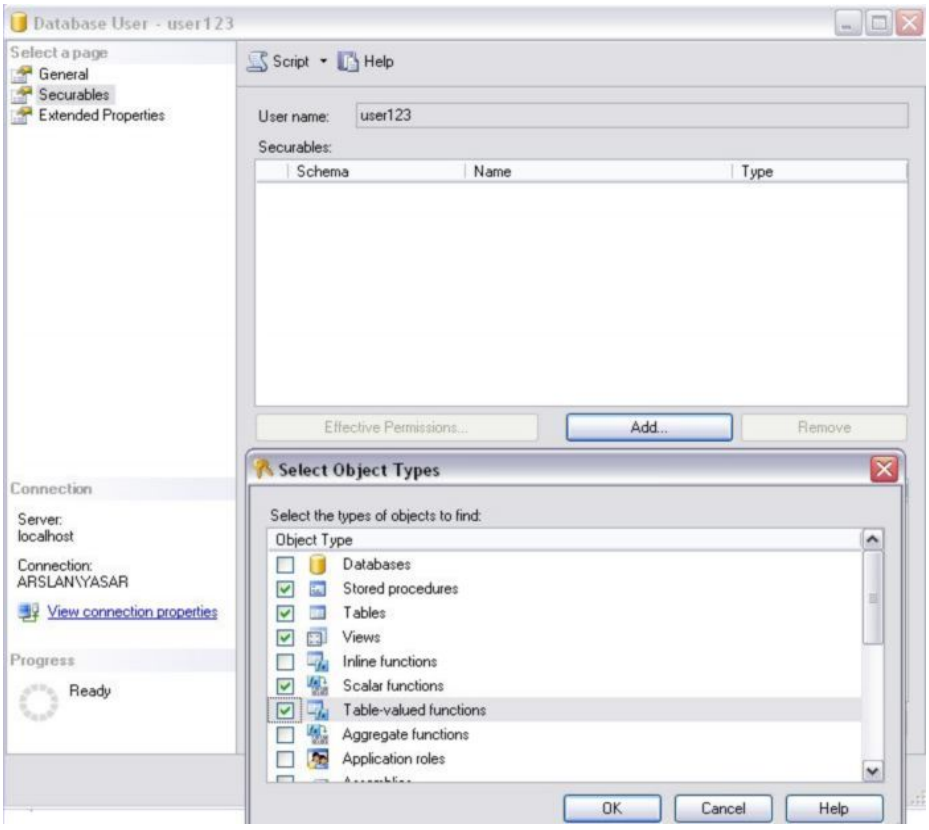
Roller: Yeni bir hesap açıldıktan sonra bununla ilgili bir takım yetkilendirme işlemi gereklidir. MSSQL Server üzerinde sistem tarafından atanmış belirli değiştirilemez kullanıcı gurupları mevcuttur. Yetkiler bu guruptan seçilerek de atanabilir. Resim 2.3 üzerinde bu guruplar listelenmektedir. Eğer kullanıcıya özel yetkiler verilecekse public olarak belirtilmelidir. Tüm haklar için, yani bir yönetici yetkisi verilecekse sysadmin olarak tanımlanabilir. Eğer sisteme, yapılan yazılım bağlantı kuracak ve sadece veri okuma veya yazma işlemi yapacaksa kesinlikle yönetici yetkisi verilmemelidir.



Resim 2.3 Sunucu üzerindeki genel kullanıcı tipleri

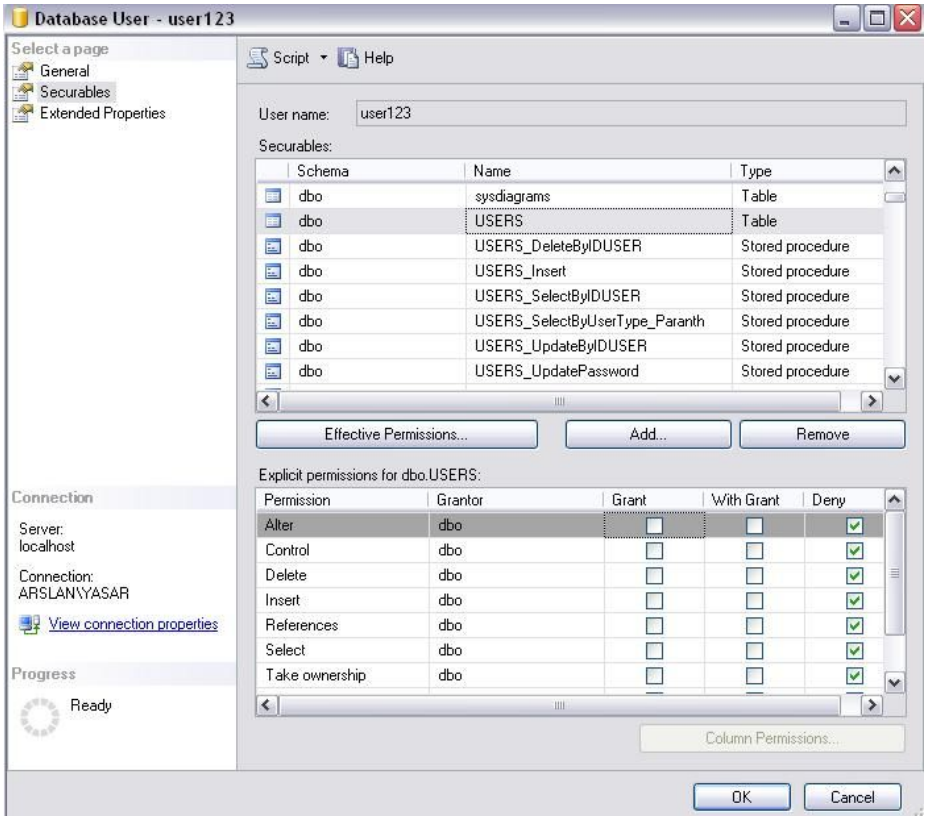
İzinler: Oturum rolünün belirlenmesinden sonra kullanıcı için özel yetkiler mutlaka tanımlanmalıdır. Yazılımının bağlantı kurup işlem yapacağı kullanıcı tanımlanarak, kullanıcı için okuma yazma gibi yetkileri verilmelidir. Böylece kullanıcı, yetkisinin dışında farklı bir işlem yapamayacaktır.

İzinler, yetkilerden daha üst düzey güvenlik için düşünülmüş bir yapılandırmadır. Bunun için MSSQL Server genel kullanıcı hesaplarında oluşturulan yeni kullanıcı izinlerini, bu pencereden düzenlenmesine izin vermez. Bu düzenlemeyi yapmak için hangi veritabanına ait özel izinler verilecekse, ilgili veritabanına yönelerek yapılandırma işlemi gerçekleştirilir. Özel izinler, bir veritabanında bulunan tablo veya fonksiyon gibi öğelerin kullanımına ait özelliklerinin yapılandırılması işlemini kapsamaktadır. İzinler için ilgili veritabanı sekmesi tıklanarak güvenlik sekmesi açılır, sonra kullanıcılar bölümüne girilerek bu veritabanı için yetki almış kullanıcılar listelenir. İlgili kullanıcı özelliklerine girilerek nesnelere özel erişim hakkı verilir. Bunun için veritabanında mevcut tüm nesneler listelenir ve oradan seçimler yapılarak izinler düzenlenir. Resim 2.4 üzerinde özel izinler için veritabanındaki mevcut öğeler seçiliyor.



Resim 2.4 Özel izinler için mevcut öğelerin seçimi

Resim 2.5 üzerinde ise bazı tablolara erişim ve işlem yetkisi kaldırılıyor. Örneğin normal bir kullanıcı belirli tablolarda işlem yapmaktadır. Ancak sistemle ilgi bazı tabloları görmesi gerekmez. Bundan dolayı resim üzerinde, site kullanıcı isimleri ve yetkilerinin bulunduğu USERS tablosu, bu kullanıcı için erişilemez hale getiriliyor. Ancak yapılan projede yazılıma ait kullanıcının bu tabloyu kullanması gerekiyor ise yetki verilmelidir. Aksi halde yazılım işlemi sırasında "Bu işlemi yapamazsınız, yetkiniz yoktur" şeklinde hata verecektir.



Resim 2.5 Bazı öğeler için, özel izinler ve kısıtlamaların belirlenmesi

2.4. Yazılım Güvenliği

Bir Uzaktan Eğitim Sistemi'nde, bilgi güvenliği olarak yapılması gereken çalışmalar sadece sistem ve ağ yapılandırmaları değildir. En önemli noktalardan birisi de yazılım hususunda güvenliğin ön plana alınmasıdır. Yapılan yazılımdaki yanlışlıklar veya programcının bazı senaryoları eksik algılaması ve gereken hassasiyeti göstermemesi, bugün birçok sistemin güvenlik açıklarını oluşturmaktadır. Hatta sadece yapılan yazılımın değil, kullanılan işletim

sistemindeki güvenlik açıkları bile ciddi riskler içermektedir. Dolayısıyla işletim sistemi üreticileri sürekli sistemleri için güncelleme yaparlar ve bunu yayınlarlar. Hiçbir sistem veya yazılım yüzde yüz güvenli olduğunu garanti edemez. Ancak sistemde ve ağda yapılan çalışmalardan sonra yazılımda sürekli gözetim altında tutulması gerekmektedir. Aynı şekilde sunucu işletim sistemlerinin de düzenli güncellenmesi gerekmektedir. Bilgi güvenliği çalışmaları, yazılım hususunda daha kodlamaya başlamadan önce düşünülmesi ve tasarlanması gereken bir aşamadır. Bu yüzden daha analiz çalışmalarından itibaren yazılımda kullanılacak güvenlik metotları ve saldırıdan korunma önlemleri detaylı olarak tasarlanmalıdır. Yazılım bitmiş bile olsa bilgi güvenliği çalışmalarından taviz verilmemelidir. Çünkü değişen sistemler ve gelişen teknoloji, sistem ve yazılımdaki eski yapılandırmaların kolayca kırılmasına sebep olabilmektedir. Uzaktan Eğitim Sistemi yazılım aşamasında gerekli görülen bilgi güvenliği çalışma ve içerikleri sırayla belirtilmektedir.

2.4.1. Yazılım Analizi

Yazılım geliştirme işlemi kod yazmak ve tasarım yapmaktan ziyade, yazılım yapılmasını gerekli kılan problemi, temel parçalarına ayırarak, daha sonra parçaları ve aralarındaki ilişkileri tanımlayarak çözüme gitme yoludur. Bu yüzden kodlamaya başlamadan once, tüm parçaların doğru bir şekilde tanımlanması ve genel hatlarıyla tasarlanması gerekir.

Yazılım geliştirmede ilk aşama problemin genel bir kapsamının çıkartılmasıdır. Bu kapsamla birlikte yazlımın çalışacağı platform, sistem, ağ kaynakları ve donanım bileşenlerini kapsayacak şekilde bir analiz çalışmasının yapılması gereklidir. WTUES'nde tüm yapı, tamamen veri transferine dayalı bir sistem olduğundan dolayı, analizin her aşamasında bilgi güvenliği konusunda daha detaylı bir çalışmaya gerek duyulmaktadır.

2.4.2. Veritabanı Tasarımı

Veritabanı tasarımı, analiz çalışmaları sürecinde defalarca gözden geçirilerek yapılan detaylı bir çalışmadır. Analiz çalışmalarındaki herhangi bir modülde olması gereken tablo ve bu tablolara ait alanlar ile alan özellikleri tasarlanarak, aynı şekilde veritabanı üzerinde uygulanır. Analiz içerisinde, farklı tablolardan bilgi filtrelemesi veya bilgi girişi gibi işlemler

olması durumunda, veritabanı tümleşik bir yapıda, ilişkilendirilerek hazırlanmalıdır. Analizin her aşamasında kurulan bu ilişkisel veritabanının bozulmamasına özen gösterilmelidir. İlişkilerden doğabilecek herhangi bir aksaklık, bilgi bütünlüğünü bozacağı gibi, bilgi güvenliğinde riske atmaktadır. Uzaktan Eğitim Sistemi'nin veritabanı, ilişkisel ve karmaşık bir yapıyı temsil eder. Sistemde farklı kullanıcı ve yetkilerin olması, her yetkiye göre sistemde davranış kurallarının olması ve bu yetkiler çerçevesinde bilgi paylaşımının olması ilişkisel veritabanını gerekli kılmaktadır. Örneğin sisteme bir üye eklenecekse, bu üyeye ait veritabanında kullanacağı alanlar üyenin tipine göre otomatik oluşturulmalıdır. Uzaktan Eğitim Sistemi'nde bir üyeye ait farklı bilgiler, farklı tablolar halinde; sınavlar, kişisel bilgiler, dersler gibi tablolarda tutulur. Üyenin sisteme eklenmesi ile birlikte bu alanların otomatik oluşturulacağı bir ilişkisel veritabanı tasarımı gerekmektedir. Yine benzer şekilde eğer üye sistemden tamamen kaldırılacaksa, bu sefer ilişkili tablolardan üye kullanıcıya ait ilgili kayıtlar sistemden otomatik olarak silinmelidir.

2.4.3. Yazılımın Kodlanması

Analizi tamamlanan yazılım modülü kodlanmaya başlamadan önce bir algoritması oluşturulur. Bu algoritma üzerinden ilgili kodlar yazılmaya başlanır. Yazılımlardaki güvenlik açıkları genellikle, yanlış yapılan algoritmalar veya titizlikle test edilmeyen kodlardan meydana gelmektedir. Özellikle web tabanlı çok kullanıcılı uygulamalarda, her kullanıcı yetkisine göre çalışacak iş parçacıklarının olması ve bunların birbiri arasında farklılıklar içermesi nedeniyle yazılım kodlama işleminin önemli güvenlik süzgeçlerinden geçirilmesi ve test edilmesi gereklidir. Ancak projenin büyüklüğü ve karmaşıklığı bu işlemlerin kontrollü bir şekilde gerçekleştirilmesini zorlaştırır.

OWASP (Web Uygulamaları Güvenlik Platformu) tarafından açıklanmış olan güvenlik açıklarında yer verilen kodlamada yapılabilecek güvenlik hataları şu şekilde anlatılmaktadır.

- Kontrol edilmemiş girdi: Web uygulamalarında kullanıcıdan alınan verinin kontrol edilmeden işleme alınması. Örneğin, rakam girilmesi gereken kutucuğa, kullanıcının farklı karakter girmesi halinde sistemin bu işleme izin vermesi durumudur.
- Ezilmiş erişim kontrolü: Yetkilendirilmiş kullanıcıların sistemde neler yapabileceği uygun şekilde belirtilmediği durumlarda, başka kullanıcı haklarının kullanılması veya yetkisiz olduğu halde bilgilere erişebilme olanağının olması durumudur.

- Ezilmiş yetkilendirme ve oturum yönetimi: Hesabın önemli verileri veya kimlik denetim anahtar veya şifrelerinin ele geçirilmesi durumudur.
- Çapraz site betikleri: Web yazılımının kullanıcı bilgisayarında, bir atak aracı olarak kullanılması durumudur.
- Tampon taşması: Kontrolü ele almak üzere tamponların, yani sistem hafızasındaki işlemlerin şişirilerek taşırılması olayıdır.
- Sokuşturma açıkları: Yazılım kodlarında kullanılan birtakım parametrelerin yazılım dışından verilebiliyor olması durumu. Bu durumda sokuşturma yapılabilir. Örneğin SQL kodlarına dışarıdan farklı kodlarla müdahale edilmesi durumudur.
- Uygunsuz hata yönetimi: Yazılım hata ve uyarılarının son kullanıcıya açık olması durumu. Bu durum bu hataların oluşması esnasında kullanıcıya sistem ile ilgili bilgiler verebilir.
- Güvensiz Saklama: Verilerin saklandıkları yerden kullanıcıya verilmeleri sırasında kullanılan verilerin çözümleme sırasındaki parçaları iyi kodlanmaması ya da verilerin şifrelenmeden saklanması durumudur.
- Servis Reddi: Servisi performans ya da kısıtlamaları yönünden zorlayıp doğru hizmet vermelerini engelleme olayıdır.
- Güvensiz Ayar Yönetimi: Sunucu tarafındaki sistem ayarlarının, yazılımla birlikte güvenli çalışmasının yapılmaması veya eksik yapılması durumudur.

Buradaki problemler web tabanlı uygulamalarda çok sık göz ardı edilen ve günlük hayatta karşılaşılan sorunlardır. Fakat bu sorunlar kodlama işlemindeki hassasiyetlerle birlikte uygun denetimler sonucunda ortadan kaldırılabilmektedir. Bu denetimleri uygulamak için öngörülen yöntemler şu şekilde sağlanabilir.

- Yazılım kodlama esnasında kodlamaların takım çalışması halinde yapılmasıdır.
- Tüm takım çalışanlarının ortak bir planda hareket ederek kodlama işlemini gerçekleştirmesi ve uygun bir formatın ortaya çıkmasıdır. Bu format sayesinde, takım elemanın yaptığı bir uygulama diğer takım çalışanları tarafından kolaylıkla anlaşılabilir, yokluğunda bu uygulama üzerinde gerekli düzenlemeler yapılabilir.
- Takım içerisindeki bazı kişilere denetleme sorumluluğu verilerek, bu formatların dışında kodlamaya izin verilmemesi ve ilgili güvenlik önlemlerini sürekli denetlenmesi gerekmektedir. Bundan dolayı proje içerisinde bir denetleme mekanizması oluşturulur ve ilgili denetim planı hazırlanır.

- Denetleme mekanizması ile denetimlerde inceleme yapacak birimler gruplara ayrılır ve sorumlulukları verilir.
- Analiz-Tasarım süreci sonunda bir dizi denetim grubu projeye uygulanır. Bunlar daha çok mimari seçimi, modül ilişkileri, veri tutma stratejileri gibi birimleri sorgulayan denetimler olacaktır.
- Kodlamanın başlamasının ardından, belli grup denetimler, yatay hiyerarşide her bir parçacığın bitiminde gerçekleştirilir. Bunlar kodlama yöntemleri denetimleri gibi koda özel denetimler olacaktır.
- Modüllerin tamamlanmasının ardından da, geçiş öncesi, bir diğer grup denetimler yapılır. Bunlar parçacıklar halinde bir anlamı olmayan ancak sistemin genel bütününde gözlenebilecek denetimlerdir (İnt.Kyn.5).

2.4.4. Yazılım Geliştirme Platformu

WTUES'nde sunucu sistemi platformu seçimine benzer bir seçim yazılım platformu içinde gerekmektedir. Uygulamanın web tabanlı olmasından dolayı yazılım platformu seçiminde çok fazla seçenek yoktur. Günümüzde en yaygın olanları Microsot .NET, Linux tabanlı sistemlerde yaygın kullanılan PHP ve Java gibi yazılım geliştirme araçlarıdır. Bu tez çalışmasında geliştirilen Uzaktan Eğitim Sistemi'nin uygulandığı WELANIMAL projesi .NET platformunda hazırlanmıştır. Yazılım .NET ortamında ASP.NET ve C# kodlaması kullanılarak geliştirilmiştir. NET ortamında bir web uygulaması geliştirilirken yeni bir form arayüzü oluşturulmak istenildiğinde yazılım aracı tarafından, aynı isimde ancak farklı uzantılarda iki dosya oluşturulur. Bu dosyalar "aspx" ve "cs" uzantılı dosyalardır. Form üzerinde oluşturulan her bir araç için, arka planda "aspx" uzantılı dosyaya yazılım aracı tarafından kodlama yapılır. İstenildiğinde programcı buraya müdahale eder ve form görünümünü kodlama yöntemi ile değiştirebilir. Bu kısımda yapılan değiştirme ve kodlama ortamına ASP.NET adı verilir. Programsal mantık ve algoritmaların uygulandığı katman C# kodlarının kullanıldığı "cs" uzantılı dosyadır. Kullanıcının tepkilerine göre sistemin nasıl davranması gerektiği bu dosya üzerinde kodlanarak gerçekleştirilir. Döngüler, sınıflar veya veritabanı işlemleri bu sayfada kodlanarak uygulama geliştirilir. Web tabanlı uygulama geliştirme işleminde .NET ortamının en önemli özelliklerinden biriside web.config dosyasının oluşturulması işlemidir. Yeni bir uygulama ilk çalıştırılmaya başlanacağı zaman yazılım aracı

tarafından otomatik oluşturulur. Bu dosya web uygulamasının güvenlik ve birtakım bağlantı ayarlarının saklandığı geniş özellikleri olan bir dosyadır. Sistem tarafından ziyaretçilere kapalı tutulan bu dosya, programcı tarafından ayarlanarak web sayfasının davranışlarını kontrol altında tutar.

2.4.5. Çok Kullanıcılı Kimlik Denetimi

Web tabanlı çok kullanıcılı uygulamalarda, her kullanıcının yetkilerine göre sistem içerisinde ne tür davranışlar sergilemesi gerektiği bir erişim denetimi mekanizması ile sağlanmaktadır. Erişim denetimi özetle; yapılan sisteme hangi kullanıcının, hangi haklarla erişebileceğinin ve bu sistem üzerinde hangi işlemleri yapmaya yetkin olduğunun belirlenmesi ve yönetilmesidir. Erişim denetiminin uygulanması sayesinde, yalnızca yeterli yetkiye sahip olan kullanıcıların sisteme ve üzerindeki veriye erişmesi sağlanır. Erişim denetimi ilkeleri belirlenirken iki temel gereksinim dikkate alınmalıdır:

- Görevlerin ayrılması: Sistem içerisinde belli işlemleri gerçekleştirmek üzere birden çok kullanıcı görevlendirilir. Görevlerin ayrılması işleminde uygulanması gereken ilk husus, yapılması gereken işlemlerin, hangi kullanıcı grupları tarafından yapılması gerektiğinin belirlenmesidir. Bu ilkenin uygulanması ile bir sürecin baştan sona kontrolünün, farklı kullanıcılar tarafından sistematik bir yapıda çalışması sağlanır. Bu sayede yetkiler bir tek kişide değil, farklı kullanıcı guruplarında ve aynı guruba ait benzer yetkilere sahip birden fazla kişilerde toplanır. Görevlerin ayrılması ile oluşturulmuş sistem birden fazla kişinin işbirliği ile çalışmasına devam eder.
- Mümkün olan en az yetki: Bu çerçevede sistemde bulunan süreçler ve kullanıcılar, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetkiye sahiptirler. Örneğin sistemde sadece raporlama amacıyla işlem yapan bir kullanıcının, sisteme sadece raporu oluşturacak olan formlara veya araçlara bağlanarak işlem yapmak üzere bağlanması yeterlidir.

2.4.6. Çok Kullanıcılı Kimlik Denetimi Uygulaması

Kullanıcı yetki seviyeleri, yani rollerine göre gerçekleştirebileceği işlemler denetlenebilmeli, yetkisi olmayan kullanıcılar ise engellenebilmelidir. ASP.NET teknolojisinde güvenlik iki kısımdan oluşmaktadır, bunlar gerçekliğin doğrulanması (authentication) ve yetki kontrolü (authorization) teknikleridir. Gerçekliğin doğrulanması işlemi, kullanıcı adı ve şifre bilgilerinin doğru olup olmadığının ilgili kullanıcı bilgilerini saklayan yapının denetlenerek bulunmasıdır. Gerçekliğin doğrulanması işlemi başarı ile sonuçlanırsa, yetki kontrol işlemi aracılığı ile kullanıcının ilgili kaynaklara erişip erişemeyeceğine karar verilmektedir. ASP.NET kodu içerisinde de kullanıcı kimliğini kullanarak yetkiye göre davranış sergileyebilmektedir. Buna kişileştirme denilmektedir. Özetlemek gerekirse ASP.NET uygulamasında güvenlik üç adımdan oluşmaktadır: Kullanıcı Gerçekliğinin Doğrulanması, Kullanıcı Yetkilerinin Kontrolü ve Kullanıcı Kişiselleştirme işlemleridir.

2.4.6.1. Kullanıcı Gerçekliğinin Doğrulanması

Üyelerin kullanıcı adı ve şifreleri ile sisteme giriş yapmaları işlemidir. Bilgiler doğru ise kullanıcı kimlik doğrulaması onaylanarak sisteme alınıyor. ASP.NET teknolojisinde gerçekliğin doğrulanması işlemi üç farklı yapı içerisinde sağlanabilmektedir. Bu yapılar;

- Form Tabanlı Kimlik Denetimi (Form-Based Authentication)
- Windows Sistemi Kimlik Denetimi (Windows Authentication)
- Giriş İzinli Kimlik Denetimi (Passport Authentication).

Web Tabanlı Uzaktan Eğitim Sistemi üzerinde kullanılan kimlik denetimi form tabanlı kimlik denetimi (Form-Based Authentication) tipinde hazırlanmalıdır. Bunun sebebi, yukarıdaki üç yaklaşım arasından en esneği olmasından dolayıdır. Form tabanlı kimlik denetimi, yapısında gerçekliğin doğrulanması işlemi için çerezler (cookie) kullanılmaktadır. Çerez, web sunucusunun, kullanıcının sayfayı ziyareti esnasında, kullanıcı bilgisayarında birtakım bilgileri saklayan dosyalara verilen isimdir. Çerezler; kullanıcının daha önce siteyi ziyaret ettiğini, ziyaret tarihini, hangi sayfalara erişildiğini, son ziyarette kullanılan birtakım parametreleri içerir.

Gerçekliğin doğrulanması işlemini gerektiren isteklerde bulunulduğunda (Örneğin öğrenci uzaktan eğitim sistemine bağlanıp ders almak istediğinde kendine has ilgili dersleri alabilmesi durumu) kullanıcı Sisteme Giriş (Login) formuna yönlendirilmektedir. Kullanıcı adı ve şifre bilgileri girildikten sonra bu bilgilerin doğru olup olmadığı sistem tarafından ilgili kaynakların (kullanıcı bilgilerinin saklandığı veritabanı veya XML dosya veya web.config dosyası) taranması aracılığı ile tespit edilmektedir. Bilgilerin doğru olması durumunda kullanıcı kimliğini belirten bir cookie yaratılmaktadır. Daha sonraki istekler için bu cookie kontrol edilmektedir. Gerçekliğin doğrulanması işleminin aktif hale getirilmesi için web.config dosyası içerisinde, <security> bölümü altındaki <authentication> öğesi biçimlendirilmelidir.

```
<authentication mode="Forms">
</authentication>
```

Bu işlem kimlik denetiminin form tabanlı bir metodla yapılacağı ve kullanıcı tipine göre ilgili formlara erişebileceğini belirlemektedir.

2.4.6.2. Kullanıcı Yetkilerinin Kontrolü

Kullanıcı sisteme girdiği zaman kendi yetki bilgileri, veritabanındaki ilgili alanlardan getirilerek, kullanıcının sistem içerisinde hangi yöne gideceği belirlenir. Gerçekliğin doğrulanması işleminin ardından kullanıcının erişim kontrolleri yine web.config dosyası kullanılarak denetlenebilmektedir. ASP.NET kullanıcı tipine göre rol tabanlı güvenliği (Role Based Security) desteklemektedir.

2.4.6.3. Kullanıcı Kişiselleştirme

Kullanıcının yetkilerinin belirlenmesi işleminden sonra kullanıcının tüm davranışları, bu kullanıcı için sürekli işletilir halde tutulur. Giriş işlemlerinden sonra kullanıcının tüm formlarda kendine has bilgilerini görebilmesi gerekir. Uzaktan Eğitim Sistemi'ne öğrenci olarak giriş yapıldığında; derslerim, sınavlarım, notlarım, raporlarım, mesajlarım gibi öğrenciye has bilgiler her forma girişte o öğrenci bilgilerine göre şekillenmesi gerekir. Bunun için formlar arası kullanıcı bilgilerinin bellekte saklanması ve uygulama kapatılıncaya kadar

devam etmesi gereklidir. Bunu gerçekleştirmek için Session adı verilen bir metot kullanılmaktadır. Session, sunucu tarafında oluşturulan oturum olarak tanımlanabilir. Herhangi bir ziyaretçi sisteme ilk girdiği anda, onunla ilgili session başlatılmış olur. Ziyaretçi, sayfalar arasında dolaştığında session bilgileri oturum sona erene kadar sistem tarafından tutulur. Kullanıcı sisteme kullanıcı adı ve şifresiyle giriş yaptıktan sonra, diğer sayfalarda kullanılabilecek kullanıcı bilgileri session olarak saklanmaya başlar ve oturum kapatılıncaya kadar sistemde canlı tutulur. Yani, session değişkenlerini sayfalar arasında taşımaya gerek yoktur, onlar ziyaretçi sitede kaldığı sürece veya oturum sona erme zamanı ile belirtilen dakika boyunca aktif kalırlar. Ziyaretçi sayfaları dolaşırken oluşturulan session nesnesi, ya programcının belirlediği ya da önceden sunucu tarafından belirlenen zaman aşıldığında sona erer. Ayrıca, ziyaretçi sistemi terk ettiği zaman da onunla ilgili oturum sona erer.

Bazı durumlarda kullanıcı uzun süre sistem üzerinde işlem yapmadığı zaman timeout işlemi gerçekleştirilir ve kullanıcının session tanımlamaları yok edilir. Fakat kullanıcı bu durumun farkına varmaz ve işlem yapmak ister. Bu durumda hem güvenliği güçlendirmek hem de oluşabilecek hataların önüne geçmek üzere, sistemden hatasız çıkışı sağlayan kod bloğu, formların açılış kısımlarına uygulanabilir.

2.4.7. Kimlik Denetiminde Şifreleme

Kullanıcın sisteme girişi esnasında kullanıcı adı ve şifresi veritabanından kontrol edilerek kimlik denetimi yapılır ve eğer uygunsa sisteme girişi kabul edilir. Veritabanındaki kullanıcı bilgilerini içeren tabloda, şifrelerin olduğu gibi tüm karakterleriyle saklanması birtakım güvenlik sorunlarını da beraberinde getirir. Herhangi bir şekilde veritabanındaki bu alanların ele geçirilmesi durumunda kullanıcıların kişisel bilgileri de tehlikeye atılmış olabilir. Kullanıcı bu şekilde başka sistemler içinde benzer şifreyi vermiş olabilir. Kullanıcı adı ve şifresi çalınan bir kişinin diğer uygulamalarda da verilerinin çalınması durumu ile karşı karşıya kalınabilir. Bu durumu önlemek için, kullanıcı şifreleri çözümlenemeyecek bir algoritma ile şifrelenerek veritabanında saklanır. Yazılımcı kendi algoritmasını oluşturarak da bu işlem amacıyla kullanabilir. Ancak .NET teknolojisi ile birlikte gelen şifreleme algoritmaları mevcuttur. Bunlar SHA1, SHA2 ve MD5 gibi algoritmalardır.

2.4.8. Dosya Alışveriş İşlemi

Uzaktan Eğitim Sistemleri'nin en önemli noktalardan birisi şüphesiz dosya transfer işlemleridir. Dosya transfer işlemleri yerel bilgisayarlardan sunucu bilgisayara veri transfer (Upload) işlemi ile sunucu bilgisayarından yerel bilgisayarlara veri transfer (Download) işlemi ile gerçekleştirilmektedir. Her iki dosya transfer işleminde sunucu üzerinde bu hizmeti sağlayacak bir servisin hizmet vermesi gereklidir. Sunucu tarafında dosya transferi için FTP veya HTTP servisleri ile iletişim gerçekleştirilebilir. Ancak web uygulamalarında HTTP servisi, uygulamaya hizmet eden servistir ve sürekli açıktır. Bundan dolayı ikinci bir servis ile sunucu üzerinde servis açmak gereksizdir.

Günümüz web uygulamalarında dosyalar iki türlü ortamda saklanmakta ve kullanıcıya sunulmaktadır. Bu metotlar; dosyaların doğrudan sunucu üzerindeki klasörler içerisinde saklanması ve dosyaların veritabanı üzerinde saklanması işlemleridir.

Dosyaların doğrudan sunucu üzerindeki klasörler içerisinde saklanması: Web uygulamasında, uygulama üzerinde kullanılması düşünülen, resim, müzik veya birtakım dokümanlar dosyalar halinde belirli klasörler içerisinde saklanır. Ancak bu klasöre uygulamanın dışında herhangi bir sistemin ya da kullanıcının erişmesi engellenmelidir. Bu klasörün içeriğinin görüntülenmesi klasör içerisindeki diğer dosyalarında paylaşıldığı anlamına gelir. Bu işlem uygulamanın dışında gerçekleştirilmiş olur ve bilgi güvenliğini tehdit eden bir unsur ortaya çıkar. Benzer şekilde yine, kullanıcılar tarafından sunucu üzerine bir upload işlemi yapılacaksa, bu işlemi sadece uygulama yapmalıdır. Uygulama üzerinde programcı, dosya kontrolü yaptırır ve dosyanın saklanacağı klasörlerin yerlerini ayarlayarak, uygun yerde saklanmasını temin eder. Kullanıcıların farklı klasörlere veri atmasının önüne geçer. Ancak bu işlem uygulamanın dışında kullanıcıya bırakılırsa, bilgi güvenliğini tehdit edebilecek dosyalar sisteme transfer edilebilir. Ayrıca dosya yerlerinde herhangi bir karışıklık oluşabilir ve bunun sonucunda bilgi tutarsızlıkları ile karşılaşılabilir. Tasarlanan Uzaktan Eğitim Sistemi üzerinde genellikle içerik hazırlama sırasında kullanılacak, resim veya müzik dosyaları gibi görsel ve işitsel dokümanlar bu şekilde saklanmaktadır. Bu dosyalar içeriklerde kullanıldığından dolayı kullanıcı bilgisayarlara gönderilen dosyaları teşkil ederler.

Dosyaların veritabanında saklanması: Bu metot dosyaların doğrudan veritabanında saklanmasını temin eder. Veritabanı üzerindeki tablolar üzerine eklenecek alanlar ile dosya

saklama bölümleri oluşturulabilir. Diğer metoda göre daha güvenlidir. WTUES üzerinde daha çok gizliliği olan dosyalar veritabanında tutulmaktadır. Sistem üzerinde; kullanıcılar arasında mesajlaşma işlemlerinde dosya gönderme seçeneği veya kullanıcıların kendilerine has kişisel dosyalarını saklama istekleri gibi dosyalama işlemleri mevcuttur. Bu yüzden her kullanıcının kendi kişisel dosyalarının saklanması gerektiğinden dolayı veritabanı üzerinde saklanarak, daha sağlıklı ve güvenli çalışması sağlanabilir.

2.4.9. İçeriklerin Saklanması ve Gösterimi

Ders içeriklerinin hazırlanması veya hazırlanmış ders içeriklerinin web ortamından kullanıcılara sunulması uzaktan eğitim sistemlerinin temelini oluşturan esas yapıdır. Eğitmenin uzaktan eğitim sisteminde en çok görevlendirildiği nokta içerik hazırlama kısmıdır. Çünkü eğitmen, öğrencinin ilgisini çekebilecek görsel, hareketli ve ayrıca eğitim yönünden zengin içerikler hazırlamalıdır. İçerik, öğrenci tarafından rahatlıkla anlaşılabilecek bir çerçeve içerisinde ilginç örnekler içermelidir. Eğitmenlerin verecekleri eğitimin kalitesi, kullanmayı planladıkları öğretim materyallerinin görsel tasarım ve akıcı anlatımına bağlıdır. Görsel tasarım öğeleri ise çizgi, alan, şekil, doku ve renklerden meydana gelmektedir. İlgi çekici ve etkili bir görsel içerik için bütünlük, denge ve vurgu gibi bazı tasarım ilkeleri dikkate alınmalıdır (Özen 2001).

Web tabanlı eğitim materyali içerisinde sık kullanıldığı için ses ve görüntü kullanımında bazı hususlara dikkat edilmesi gerekir. Bu hususlar aşağıdaki gibi sıralanabilir (Yiğit ve Özden 2000).

- Web sayfası tasarımı, kullanıcı ilgili bağa tıkladığında ilgili dosyanın gelebileceği biçimde yapılmalıdır. Kullanıcı herhangi bir istekte bulunmadan otomatik olarak yüklenmemelidir. Kullanıcıya dosyanın büyüklüğü ve transfer süresi ile ilgili bilgi verilmelidir. Dosya transfer hızı bilgisayar ağlarının bant genişliği ve doluluk oranına bağlı olarak değiştiği için kullanıcıya dosyanın transfer süresi ile ilgili bilgi verilmesi, kullanıcının kendi kararını verebilmesi açısından önemlidir.
- Görüntü ve ses dosyaları yalnızca gerektiğinde kullanılmalıdır. Bir hareketi göstermek veya gerçek bir uygulamayı farklı bir perspektiften sunabilmek gibi amaçlar için Web tabanlı eğitim materyali içerisinde görüntü kullanılabilir.

- Görüntü ve ses dosyaları hazırlanırken büyüklüklerine dikkat edilmelidir. Dosyalar mümkün olduğunca küçük boyutlara indirgenerek sunulmalıdır.
- Görüntü ve ses dosyaları, tüm platformlara uyum sağlayabilmeleri açısından standart bir formatta sunulmalı ve ilgili sayfada dosyanın hangi platformda veya platformlarda çalışabileceğine ilişkin bilgi yer almalıdır.
- Web tabanlı eğitim materyali içerisine görüntü yerleştirilirken, görüntü sayfa içerisine yerleştirilebilir veya yeni bir pencere içerisinde görüntülenmesi sağlanabilir.

2.4.10. Sistem Hata Denetimleri

Gerek web uygulamaları, gerekse Windows uygulamalarında, sistemde oluşabilecek herhangi bir hatada ne yapılması gerektiği, programcı tarafından belirlenmelidir. Buradaki amaç; program üzerinde normal işlevlerin dışında herhangi bir işlem söz konusu olmuşsa hata tespit edilmeli ve gerekli önlemler alınmalıdır. Örneğin; Uzaktan Eğitim Sistemi üzerinden tüm eğitmenlere kritik bir elektronik posta gönderilmek isteniyor. Ancak bu sırada elektronik posta servisinde bir problem var ve gönderen kişi bunun farkında değildir. Böyle bir durumda, eğer programcı bu durumun olabileceğini tahmin etmiş ve hata risklerine göre kodlarını düzenlemiş ise, sistem e-posta gönderen kişiye; "Şuanda elektronik posta servisi çalışmıyor daha sonra tekrar deneyiniz veya sistem yöneticinizle görüşünüz" türünde bir hata mesajı verecektir. Aksi durumda ise bir hata ile karşılaşılacak ancak hatanın içeriği yabancı dilde veya daha teknik, anlaşılması zor bir mesaj olacaktır. Ayrıca kullanıcının sistemdeki oturumunun sonlandırılması riski doğacaktır. Bu durumda e-posta atan kişinin ne yapması gerektiği belirsizdir. Tüm bunların düzenlenmesi için uygun hata mesajı kodlamaları programcı takımı tarafından düzenlenmelidir. .Net ortamındaki hata olaylarının tespiti try-catch blokları ile tespit edilmektedir ve aşağıdaki kod bloğu üzerinde görülmektedir. Buradaki çalışmada; eğitmen göndereceği mesaja bir dosya eklemek istiyor ve bunun için seçtiği dosya veritabanında saklanacaktır. Ancak bu esnada; dosya açık kalmış olabilir veya dosya silinmiştir yerinde olmayabilir. Kullanıcı bunun farkında değildir ve göndermek istediğinde, uygun hatanın kullanıcıya gösterilmesi gerekir. Programcı isterse kendi hata mesajını veya sistemin kendi mesajını kullanıcıya bildirir. Buradaki örnekte sistem hata mesajı kullanıcıya iletilmektedir.

```
try
{
      HttpPostedFile postedFile = fileInput.PostedFile;
      if (postedFile != null && postedFile.ContentLength > 0)
      {
         string serverPath = Server.MapPath(".");
         string filePath = postedFile.FileName;
         FileInfo clientFileInfo = new FileInfo(filePath);
         string filename = clientFileInfo.Name;
         string yeniPath = serverPath + "\\Dosyalar\\" + filename;
         postedFile.SaveAs(yeniPath);
         FileInfo serverFileInfo = new FileInfo(yeniPath);
         FileStream stream = new FileStream(serverFileInfo.FullName,
         FileMode.Open, FileAccess.Read);
         byte[] buffer = new byte[stream.Length];
         stream.Read(buffer, 0, (int)stream.Length);
         stream.Close();
         lblStatus.Text = "File was updated";
       }
       else
         lblStatus.Text = "File was not updated";
}
catch (Exception ex)
{
         lblStatus.Text = ex.Message.ToString();
}
```

Uzaktan Eğitim Sistemi uygulamasında sadece uygulama içerisinde hatalar oluşmamakta, veritabanı sisteminde de hatalar oluşabilmektedir. Veritabanındaki hataların başlıca sebepleri: Veritabanı bağlantı hataları, tablodaki alanlara program tarafından yanlış formatta bilgi gönderilmesi, yanlış SQL sorgularının gönderilmesi, uygun olmayan ölçekte verilerin alana girilmeye çalışılması veya ilişkisel veritabanında ilişkiye aykırı verilerde değişiklik yapılmaya çalışılması gibi durumlardır. Bu durumlarda veritabanı sistemi, programa veri olarak hata mesajı döndürecektir. Ancak programcı bu hata mesajını doğrudan kullanıcının görmesini sağlarsa, veritabanı sistemi hakkında bazı ipuçlarını kullanıcıya vermiş olur. Bunu engellemek için, programcı tarafından kendi dilinde uygun bir hata mesajını verdirmesi daha mantıklıdır.
Veritabanı hatalarının denetiminde diğer bir yöntem ise hataların veritabanı sisteminde Store Procedure yapısı içerisinde kontrol edilmesidir. Böyle bir yapıda yine programcı hata oluşması durumuna göre Stored Procedure yapısı içerisinde try-catch bloğunu kullanır.

Veritabanı hata denetimlerinde diğer bir önemli husus ise işlemlerin yarıda kalması durumudur. Özellikle geri dönüşümü olmayan kritik işlemlerde kullanılması sistem içerisindeki veri bütünlüğünü korumaktadır. Bu özellik Transaction işlemidir. Bu özellik sayesinde eğer işlem esnasında bir hata ile karşılaşılmışsa yapılan işlemler geriye alınarak veriler eski haline getirilir. Geri alma işlemine ise Rollback adı verilir.

2.4.11 Güvenlik İçin Ek Modüllerin Oluşturulması

Bir web uygulamasında bilgi güvenliğini sağlamanın gerekli görüldüğü noktalardan birisi de, uygulama içerisine kontrol mekanizmalarının oluşturulmasıdır. Bu bağlamda, uygulama içerisinde kullanılan önemli noktalara işlem kayıtlarını tutmak amacıyla mekanizmalar yerleştirilir. Bu mekanizmalar işlemleri kayıt altına alan (loglama yapan) ve gerektiğinde kontrol amaçlı kullanılan yapılardır. Tasarlanması düşünülen Uzaktan Eğitim Sistemi üzerinde bu amaçla birçok kontrol mekanizması geliştirilmeli ve uygulama içerisinde önemli noktalarda kullanılmalıdır.

2.5. Bilginin Saklanması

Uygulama ve sistemler üzerinde yapılan bilgi güvenliğini koruma çalışmaları, olabilecek saldırı veya problemlerden sistemi korumayı amaçlar. Ancak şimdiye kadar ortaya çıkmamış bir problem veya doğa afetleri gibi durumlar için, bilgi güvenliği tedbirlerinin alınması gerekmektedir. Bu gibi durumlarda yapılması gereken; bilgiyi, uygun araçlarla, veri bütünlüğünü koruyacak şekilde, güvenli ortamlarda saklamaktır. Bilginin veri bütünlüğünün korunarak alınmasındaki en büyük etken, bilginin en son haliyle saklanması ve gerekli durumlarda tekrar sisteme adapte edilebilmesidir. Bunun için sistemlerde, sürekli yedekleme ve saklama ünitelerinin devrede olması gerekmektedir. Bilginin önem durumuna göre yedek alma işlemleri zaman bakımından kısaltılabilir. Ayrıca güvenliği sağlanmış uzak noktalara da tekrar ikincil bir yedekleme ünitesi kurularak bilgiler daha güvenli ortamlara taşınabilir.
Sistemin yedeğinin alınmasındaki önemli bir husus; bilgi bakımından hangi verilerin yedeklerinin alınması ve saklanmasıdır.

2.5.1. Bilgi Yedekleme ve Geri Dönüşüm

Bir Uzaktan Eğitim Sistemi'nde, yedeği alınması gereken veriler iki türdür. Sistemin işleyişini devam ettiren bilgiler bunlar: Sunucu sistemi, uygulama yazılımı ve genel sistem ayarlarıdır. Diğeri ise veritabanı bilgileri: Uygulama yazılımına bağlı çalışan ve eğitimde kullanılan tüm bilgileri içeren veritabanıdır.

Sistem bilgileri sürekli değişen bir yapı değildir. Tüm ayarları ve testleri yapılmış bir sistemin yedeği alınarak daha sonra kullanılmak üzere saklanabilir. Ancak veritabanı bilgileri sürekli değişen bir yapı olduğu için, yedekleme işlemi ne kadar çok sık yapılırsa, geri dönüşüm işleminde fazla problem yaşanmayacaktır. Ancak veritabanı yedekleme işlemi, sistemin genel performansını düşürecek şekilde tasarlanmamalıdır. Yedekleme işleminde yapılması gereken hususlar aşağıda belirtilmiştir.

- Sistemdeki her verinin yedeği alınmamalıdır. Sürekli aynı bilgilerin yedeklenmesi yedekleme işlemini uzatacak performans ve yedekleme ortamında kayıplara neden olacaktır.
- Verilerin önem durumu ve yedeklerinin alınmasındaki öncelik durumu tespit edilerek öncelik sırası düzenlenmelidir.
- Yedeği alınacak verilerle birlikte, yedek alma sıklığı tespit edilmelidir.
- Yedekleme süreci, sistemin günlük işleyişini en az şekilde etkileyecek biçimde düzenlenmelidir.
- Özellikle doğal afetlere karşı, yedekler farklı bir coğrafi bölgede saklanmalıdır.
- Yedekler elektronik cihaz ortamlarında saklanabileceği gibi, periyodik olarak da CD, DVD gibi ortamlarda saklanmalıdır.
- Veritabanı yedekleme işlemi; periyodik ayarlamalarla otomatik olarak diğer ortamlara aktarılmalıdır.
- Veritabanı yedekleme işleminde ikinci bir yedekleme işlemi çalışarak anlık değişikliklerin yedeklerini almalıdır. Bu işlem sistemin zarar görmesi durumunda, bilginin son haliyle tekrar geri dönüşümüne olanak sağlar.

Bazı uygulamalarda kısa bir süre dahi olsa sistem kesintileri, kullanıcı ve sistem yöneticilerini sıkıntıya sokmaktadır. Örneğin uzaktan eğitim uygulamasında çevrimiçi bir sınavın yapılması esnasında problem yaşanması ve sistemin susması, büyük sorunların ortaya çıkmasına neden

olacaktır. Anlık yedekler alınmış dahi olsa, bu işlemin tekrar eski haline dönmesi belirli bir süre kaybına mal olacaktır ve sınav esnasında bunun olması kabul edilemez bir durumdur. Bu durumda işlemlerin sekteye uğramadan gerçekleşmesini sağlayacak bir teknik mevcuttur. Bu teknik uygulamanın küme (cluster) yapısında çalıştırılmasıdır. Cluster; uygulamaya hizmet veren servis noktalarının (node) sayısını artırarak, bu servislerin bir araya getirilerek çalıştırılmasını sağlayan bir servistir. Yani birden fazla sunucu makine üzerinde uygulama çalıştırılır ve bu çalışan servisler tek bir noktadan hizmet veriyormuş gibi yapılandırılır. Bunun neticesinde; sunucuların birisinin arızalanması durumunda, diğer sunucu yoluna devam edecek ve servis hizmetinde aksama olmayacaktır. Arızalanan sunucunun arıza durumu atlatıldığında tekrar devreye alınsa bile sistemin kapanmasına gerek kalmayacaktır. Yenilenen sunucu devreye alınır alınmaz, kendini diğer sunucu bilgisayarla eşdeğer şekilde güncelleyerek yoluna devam edecektir. Ayrıca cluster yapısında sunucular arasında yük dağılımı gerçekleştirilerek, sistemin performansında artış sağlamak mümkündür. Yük dağılımı, servise gelen istekleri sunucular arasında paylaştırarak daha etkin ve verimli bir çalışma amacıyla dağıtım yapar.

2.5.2. Disk Depolama Ünitesinin Sisteme Entegrasyonu

Disk depolama (Disk Storage) ünitesi fiber kablolar aracılığı ile sunucu bilgisayarlara hizmet verebilen donanımsal bir yapıdır. Sunucu bilgisayarların disk alanlarının yetersiz olması durumunda veya sunucunun hizmet verdiği bazı servislerin çok fazla disk alanına ihtiyaç duyması gibi durumlardaki ihtiyaçları giderme amacıyla kullanılırlar. Bu ünite kendi üzerinde yüksek kapasiteli diskleri barındırır. Disk sayıları cihazın marka ve modeline göre değişkenlik gösterir. Ayrıca üzerindeki diskler normal bilgisayar diskleri olmayıp genelde sunucu teknolojisinde kullanılan hızlı ve yüksek kapasiteli disklerdir. Cihazın özelliğine göre disk sayısı ve her bir diskin kapasitesi ile birlikte terabyte ölçüsünde veri kapasitesine sahip olabilmektedirler.

Cihaz üzerinde sunucular ile iletişimi sağlamak üzere fiber portlar bulunmaktadır. Fiber portlara fiber modüller eklenerek fiber kablo ile çalışabilmesi sağlanır. Sunucu tarafında ise disk depolama birimine bağlantı için geliştirilmiş donanım kartlarının takılması gerekmektedir. Bu kartlar fiber kablo bağlantı yuvaları ile birlikte gelmekte ve sunucu üzerine herhangi bir donanım gibi takılabilmektedir. Daha sonra her bir sunucu ve disk ünitesi için

fiber kablo tesisatı çekilerek donanımsal yapı tamamlanmalıdır. Disk depolama ünitesi sunucuya bağlı herhangi bir bilgisayar üzerinden kontrol edilebilir. Donanımla birlikte gelen yazılımla, hangi sunucu için ne kadar disk alanına ihtiyaç duyulduğu belirtilir. Yazılım farklı işletim sistemleriyle uyumlu çalışabilmektedir.

Uzaktan Eğitim Sistemleri'nde ders içerikleri görüntü, ses, resim ve diğer dosya formatlarını barındıran ve fazla disk alanı gerektiren dosyalardan oluşmaktadır. Ayrıca her eğitimcinin veya öğrencinin kendine has bilgilerini saklayabilecekleri ve dosyalarını istedikleri zaman sunucu üzerine gönderip alabilecekleri disk alanlarının olması gerekmektedir. Bazı özel durumlarda ise verilen konferansların video formatında saklanması ve gerektiğinde kullanıcılara sunulması gerekebilir. Buna benzer durumlarda sunucunun kendi disk alanları yetersiz kalacaktır ve sunucu üzerine acil disk takviyesi gerekir. Bu tür problemlerin ortadan kaldırılmasında disk ünitesinin kullanılması tavsiye edilmektedir. Sistem üzerine disk depolama ünitesi dâhil edilmesinin avantajları şu şekilde açıklanabilir.

- Sunucu bünyesindeki diskler üzerinde herhangi bir değişiklik yapılmadan, mevcut sunucu sistemi ve donanımı üzerine kurulum yapılabilir.
- Fiber bağlantı ile çalıştıkları için herhangi bir yavaşlık hissedilmez.
- Ünite üzerindeki diskler, sunucu üzerindeki disklerden farksız çalışır.
- Sunucular, ünite üzerindeki diskleri kendi sistemindeki diskler gibi dâhili olarak kabul ederler.
- Sunucu üzerinde oluşabilecek herhangi bir problemde bu diskler farklı bir ünitede korunduğu için bilgi kaybına neden olmazlar.
- Ünite üzerinde, sunucu için yapılandırılmış disk alanları herhangi bilgi kaybına neden olmaksızın değiştirilebilirler.
- Maliyet açısından pahalı gibi görünmesine karşı, daha sonra kendini amorti edebilecek bir yapıya sahiptir. Sunucularda disk alanları sınırlıdır, ihtiyaç karşısında sunucunun tüm disklerinin değişmesi gerekebilir, ancak üniteden beslenen bir sunucu için yapılması gereken sadece program üzerinden sunucuya disk alanı tahsis etmektir.
- Ünite satın alınırken eğer bütçe kısıtlıysa disk sayıları azaltılabilir. Sunucuların ihtiyaçlarına göre daha sonra takviye edilerek genişletilebilir.

Disk ünitesinin bazı dezavantajları vardır. Bunlardan en önemlisi, sunuculara ait çok fazla verinin tek bir cihaz üzerinde toplanmasıdır. Ancak donanımsal arızalara karşı cihaz üzerinde

güçlü bir yapı mevcuttur. Fanları ve elektrik beslemeleri gibi donanımları yedekli çalışmaktadır. Herhangi bir arıza durumunda diğer yedek donanım görevi otomatik olarak devralmaktadır.

2.5.3. Teyp Depolama Ünitesinin Sisteme Entegrasyonu

Teyp Depolama (Tape Backup) ünitesi disk ünitesinden farklı bir amaçta kullanılan bir depolama aracıdır. Buradaki amaç; çalışan sistemlerin yedeklerini manyetik ortama taşıyarak farklı bölgelerde koruma altına almak ve ihtiyaç duyulduğunda kısa zaman içerisinde kolayca sunucuya tekrar yükleyebilmektir. Teyp depolama ünitesinin bağlantısı için herhangi özel bir kablo tesisatına gerek yoktur. Ünitenin sunucu ağına bağlı olması yeterlidir. Benzer şekilde yine yazılımla yönetilen bu araç, farklı sistemler üzerindeki sunucuların bilgilerini teyp kasetlerine kopyalar. Kullanılan modellere göre farklılık gösteren bu araç üzerinde, diskler yerine kasetler bulunmakta ve kasetler otomatik olarak işletilmektedir.

Uzaktan Eğitim Sistemi'nde donanımsal olarak yaşanabilecek herhangi bir sorun ciddi problemlerin ve risklerin yaşanmasına sebep olacaktır. Uzaktan Eğitim Sistemi, hem bilgi güvenliği yönünden korunması hem de bilginin saklanması konusunda titizliği üst seviyede tutulması gereken bir sistemdir. Oluşabilecek bilgi kaybında geri dönüşümün hatasız ve zaman kaybı olmadan yapılması gerekmektedir. Teyp üniteleri farklı tarihte alınan yedeklerin kolayca geri dönüşümünü garanti eden bir sistemdir. Yönetilen yazılım üzerinde iş süreçleri belirlenerek, sistemlerin belirli zaman aralıklarında sürekli yedeklerinin alınması sağlanır. İstenildiğinde yedekler üzerinden hareket edilerek istenilen tarihe ait bilgiler sunucu üzerine aktarılabilir.

2.6. Sistemin Test Edilmesi

WTUES'nin hayata geçirilmesinden önce yapılması gereken en önemli noktalardan birisi de güvenlik ve performans bakımından test edilmesidir. Güvenlik sorunlarını gidermek için yapılan her çalışmanın sistem performansını engellememiş olması gerekmektedir. Ağ üzerinde hedef noktaya ulaşmaya çalışan paketlerin, farklı cihazlar ve sistemler üzerinden geçirilmesi ve cihazlar üzerinde herhangi bir uyumsuzluk sorunun ortaya çıkması durumunda

ciddi performans sıkıntıları yaşanabilir. Sunucu sistemlerde kullanılan farklı işletim sistemleri ve sistemde kullanılan herhangi bir programla çakışması durumu da yine performansı etkileyen sebeplerden birisidir. Bu sebeplerden dolayı sistem performansı takip edilmiş, ağ üzerinde paket taramaları yapılmış ve son olarak da yazılım güvenliği test edilmiştir.

2.6.1. Performans Testi

Performans testlerinin asıl amacı yazılımın performans gereksinimlerine ulaşıp ulaşmadığını tespit etmektir. Test ile elde edilecek analizler sonucunda sistemin iyileştirilmesinde rol oynamaktadır. Web tabanlı yazılım performans testi, belirli sayıda kullanıcıların aynı anda benzer işlemleri sürekli gerçekleştirmeye çalışmaları ile ölçülebilir. Bu işlem sırasında yazılımın cevap süreleri, veritabanın cevap süreleri gibi kriterler değerlendirmeye alınır. Arzu edilen performansın sistem tarafından sağlanamaması durumunda gerekli iyileştirmelerin yapılması ve tekrar teste tabi tutulması gerekmektedir. Bununla birlikte test otomasyon araçları kullanılarak, sistem performans testlerine tabi tutulabilir. Bu tür araçlar sayesinde yazılımın nasıl tepki verdiği analiz edilebilmektedir (İnt.Kyn.6).

2.6.2. Ağ ve Güvenlik Taramaları

Ağ trafiği, omurga switch ve diğer uç noktalardaki ağ donanımları üzerinde yapılan çalışmalarla test edilmiştir. Ağ donanım cihazları haberleşme işlemlerini TCP/IP protokolünün fiziksel katmanında devam ettirmektedirler. Bu fiziksel katman, ağa bağlı cihazların fiziksel adreslerine göre çalışmaktadır. Fiziksel adres donanımların ağ kartlarında bulunmakta ve MAC (Media Access Control) adresi olarak adlandırılmaktadırlar. Ağ donanımı üzerinde testler fiziksel katman değerlendirilerek yapılmıştır. Testler sırasında laboratuar içerisinde bazı bilgisayarların sistemin işleyişini büyük oranda kestiği görülmüştür, bunun en büyük nedeni ise anti virüs yazılımını güncellemeyen bir bilgisayarın ağ üzerinde yaptığı virüs ataklarıdır. Bu virüs bilgisayara ait ağ geçidi cihazının MAC adresini kendine kopyalamakta ve böylece tüm trafiğin kesilmesine neden olmaktadır. Hatta ağ üzerindeki bilgisayarların MAC adreslerini de kendine tanımlamaktadır. Böylece ağ üzerindeki paket trafiğini tamamen durdurmaktadır.

Ağ üzerinde test işlemi olarak yapılması gereken bir diğer nokta ise ağ paketlerinin dinlenmesidir. Buna sniffer adı verilir. Ağ trafiğindeki tüm paketlerin dinlenmesi donanımsal olarak hub adı verilen küçük cihazlarla mümkündür, çünkü bu cihaz, üzerindeki bir porta gelen tüm veriyi diğer portlara da göndermektedir. Uygun geçiş noktalarına bu cihaz konarak dinleme yapılabilir ancak bu eski bir metottur. Bunun yerine switch üzerinde port-mirroring adı verilen bir metot kullanılır. Bu metot ile ağ üzerinde, ağ geçidi olarak ayarlanmış bir port, cihaz üzerindeki boş bir porta eş zamanlı olarak yönlendirilmiş olur. Böylelikle aynı veriler aynı anda iki porta da aktarılmış olur. Boş olan porta bir bilgisayar takılarak ağ trafiği dinlemeye alınabilir.

3. WTUES ve ÖRNEK BİR UYGULAMA WELANIMAL

Bu tez çalışmasında, tasarlanmış olan WTUES'nin uygulaması, üniversitemizin bir projesi olan WELANIMAL kapsamında gerçekleştirilmiştir. Bu amaçla özellikle bilgi güvenliği konusunda yapılması gereken çalışmalar ve alınması gereken önlemler WELANIMAL projesi ile uygulamaya dönüştürülmüştür. Afyon Kocatepe Üniversitesi Veteriner Fakültesi'nin Avrupa Birliği Leonardo Da Vinci projesi olarak kabul edilen WELANIMAL projesi, bu tez çalışması ile birlikte, daha güvenli bir sistem haline getirilmiştir.

Projenin amacı kısaca: "Hayvan yetiştiriciliği ve hayvan refahı gibi konularda dünya genelinde bir uzaktan eğitim sisteminin oluşturulması" şeklinde adlandırılmaktadır. Afyon Kocatepe Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından geliştirilen Uzaktan Eğitim Sistemi'nde; bilgi güvenliği özellikle dikkate alınmış ve tüm sistem bu doğrultuda planlanarak hazırlanmıştır. Yazılım, donanım, sistem ve ağ çalışmaları olmak üzere; bilginin güvenliği, bilginin elektronik ortama aktarılması, bilginin yayınlanması, iletimi ve saklanması gibi konular tasarlanmış, kodlanmış ve uygulamaya geçirilmiştir.

3.1. Sistemin Tasarlanması

3.1.1. Bilgi Güvenliği Stratejisinin Oluşturulması

Takım yönetimi Yaşar Arslan tarafından sağlanmış yazılım ve sistem konusunda tecrübeli 3 uzman kişi çalışmalarda görevlendirilmiştir. Proje takımı için, gerek donanım gerekse yazılım olarak özel kuruluşlardan birtakım eğitimler alınmıştır. Bu eğitimler donanım ve sunucu alımlarında firma desteği ile oluşturulan eğitimler ve yazılım eğitimi veren özel firmalar aracılığı ile sağlanmıştır. Daha sonraki aşamada ise, takım çalışanları için görevlendirme ve zaman takvimi ortaya çıkarılmıştır. Bilgi güvenliğini korumada herkesin yetkileri belirlenmiş, sunucu, sistem ve yazılım çalışmalarında hassas olarak durulması gerekli noktalar yazılı olarak ortaya çıkarılmış ve takım çalışanlarına sunulmuştur.

3.1.2. Oluşturulan Stratejiye Göre WTUES Tasarımı

Uygulanan WTUES için platformlar incelenerek sistemin tasarımı şu şekilde gerçekleştirilmiştir. WTUES için 2 adet HP DL380 sunucu, işletim sistemi olarak Microsoft Server 2003 seçilmiştir. Yazılım platformu Microsoft Visual Studio 2005 olmakla birlikte programlama dili C# dilidir.Kullanılacak veritabanı ise Microsoft SQLSERVER 2005 olarak tespit edilmiştir. Sunucuların biri web sunucusu, diğeri ise veritabanı sunucusu olarak tasarlanmıştır. Ayrıca normal bir masaüstü bilgisayarı test amaçlı kullanım için devreye sokulmuştur.

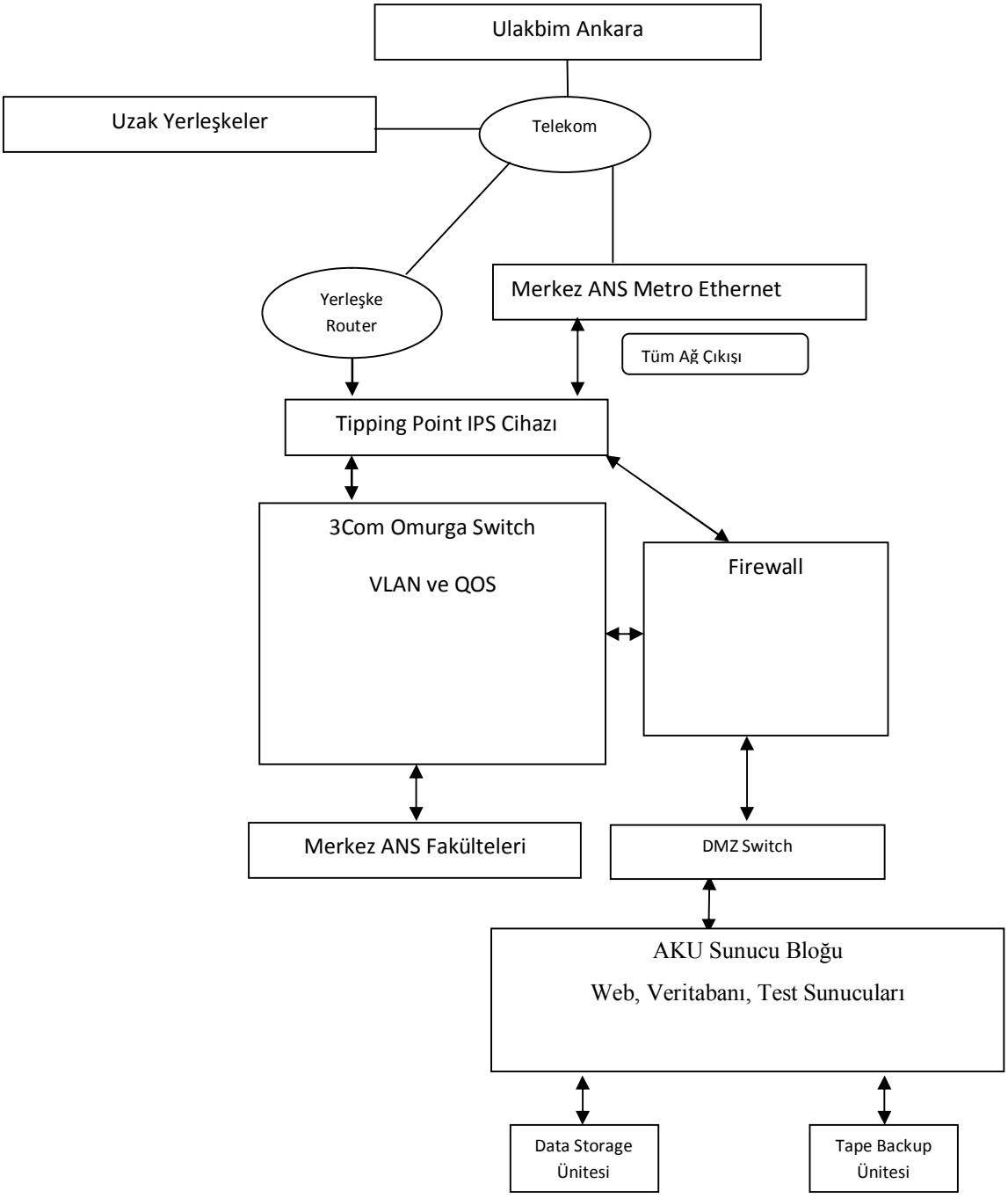
Sistemin ağ yapısında ise; ana çıkış kapasitesini artırmak için Metro Ethernet bağlantısı sağlanmıştır. Ayrıca iç ağ için güvenli VLAN yapısı kurularak omurga switch üzerinde tanımlamaları yapılmıştır. Proje, Afyon Kocatepe Üniversitesi dâhilindeki öğretim elemanları, görevli personel ve öğrencileri kapsayacağı için, üniversiteye bağlı diğer uzak yerleşke bağlantılarında iyileştirme çalışmaları yapılmıştır. Sistemin bir VLAN yapısı üzerinde toplanması, bilgi güvenliği açısından çok önemlidir. Böylece tüm sistem tek noktadan VLAN yapısı ve omurga switch aracılığı ile yönetilebilir hale getirilmiştir.

Tasarlanan WTUES'nin daha güvenli bir ortamda çalışabilmesi için, tüm sistemi koruma planı ortaya çıkarılmıştır. Bunun için sunucuların dışında bir sunucu, firewall olarak kullanılmak üzere yapılandırılmıştır. Ayrıca Tipping Point adı altında donanımsal güvenlik cihazı ile sistemin işleyişinde önemli güvenlik açıklarını kapatacak bir sistem yapısı kurulmuştur. Sistemin sürekli yedeklenmesi, bilgi kaybının önlenmesi ve daha fazla disk alanına ihtiyaç duyulması düşünülerek 3 terabyte kapasiteli veri depolama ünitesi entegre edilmiştir. Ayrıca yedeklerin daha güvenli ortamlarda saklanabilmesi amacıyla yedekleme ünitesi sisteme dâhil edilmiştir.

3.1.3. Sistem İçin Gerekli Donanımsal Altyapının Sağlanması

Projede kullanılması düşünülen tüm donanımsal yapı Afyon Kocatepe Üniversitesi Bilgi İşlem Dairesi Başkanlığı'nın imkânları bünyesinde sağlanmıştır. Ayrıca tüm donanımın ve veri yedeklerinin bilgi güvenliği açısından güvenli bir ortamda saklanması gerekmektedir. Bu önemli nokta için bilgi işlem merkezinin sistem odası düşünülmüştür. Tüm donanım burada

klimalı ve yangın korumalı bir sistemde saklanmaktadır. Sadece yetkili kişilerin girişine izin verilen odada tüm cihazların elektriği güvenli güç kaynakları ile beslenerek, sürekli çalışır halde, işlevlerine devam etmesi sağlanmaktadır. Projenin ağ ve donanımsal tasarımı şeması Şekil 3.1 de gösterilmektedir. Afyon Kocatepe Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yapılandırılan sistem Ankara Ulakbim kurumuna bağlanmaktedır. Bağlantı Türk Telekom şirketinin altyapı ve fiber bağlantıları ile sağlanmaktadır.



Şekil 3.1.Sistemin ağ ve donanımsal yapısı

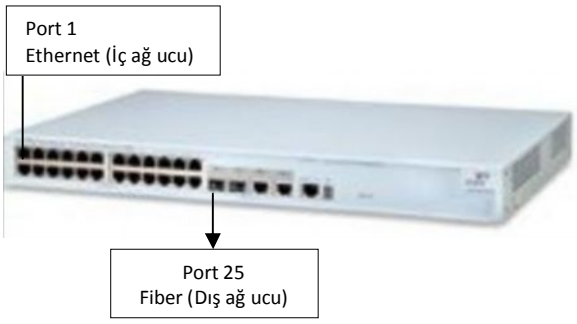
3.2. Ağ Güvenliği

3.2.1. Ana Çıkış Bağlantısı

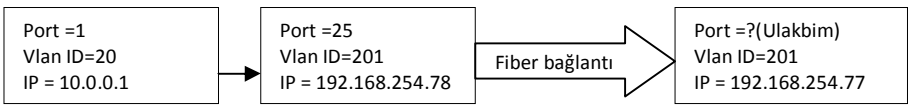
Afyon Kocatepe Üniversitesi'nin kullandığı mevcut hat WTUES için yetersiz bulunmuş ve hız artırım çalışmaları yapılmıştır. Kullanılan sistem Afyon Kocatepe Üniversitesi ile Ankara Ulakbim arasındaki ATM (Asynchronous Transmission Mode) bağlantısıdır ve hızı 34 Mbit'dir. Yapılan hız artırımı çalışmasında bu hız 50 Mbit'e çıkartılmış ve artık ATM protokolü devreden çıkartılmıştır. Bunun yerine bağlantısı, yapılandırması ve bakımı daha kolay olan Metro Ethernet sistemi uygulanmıştır.

3.2.2. Metro Etherenet Yapılandırması

WTUES için yapılan Metro Ethernet çalışması şu şekilde gerçekleştirilmiştir. Telekomünikasyon şirketi ile Ankara Ulakbim Kurumu ve Afyon Kocatepe Üniversitesi arasında 50Mbit hat sözleşmesi yapılmış ve bu doğrultuda bir adet 3Com 4500 fiber modüllü switch bu iş için tahsis edilmiştir. Şekil 3.2 ve Şekil 3.3 üzerinde bağlantı şeması verilmiştir ayrıca cihazın yapılandırma aşamaları ve açıklamaları aşağıda gösterilmiştir.



Şekil 3.2 Metro Ethernet sisteminde switch üzerinde yapılan bağlantı noktaları



Şekil 3.3 Metro Ethernet sisteminde, switch bağlantı yapılandırması

Metro Ethernet sisteminin switch üzerindeki yapılandırma ayarları:

1.Adım: Metro Ethernet işleminde ilk öncelik VLAN tanımlamalarıdır. VLAN sistemleri tanımlanırken her yeni bir VLAN için, bir VLAN numarası belirtilmelidir. Bundan dolayı Ankara bağlantısı için 1 adet VLAN ID şirket tarafından belirlenmiştir. Bu VLAN numarası dış bağlantı içindir. Aynı zamanda bu dış bağlantıya üniversite sistemi bağlanacaktır. Üniversite iç bağlantısının etkin olabilmesi için ise farklı bir VLAN numarası kurum içi çalışanlar tarafından tanımlanabilir. Bu VLAN iç ağa bakan kısımdır. Kurulacak sistemin ethernet protokolü ile çalışabilmesi için, telekomünikasyon şirketinin merkez sistemi ile üniversite dış ağ ucu, aynı VLAN içerisinde olması gerekmektedir. Telekomünikasyon şirketi üniversite arasındaki bağlantı ve üniversite iç ağ bağlantısı için VLAN numaraları belirlenmiştir ve bunlar switch üzerinde yapılandırılmaktadırlar.

- `vlan 20` (Üniversite ağı için VLAN ID tanımlanıyor)
- `vlan 201` (Üniversite dış ağı ve telekomünikasyon şirketi için VLAN ID tanımlanıyor.)

2.Adım: VLAN ID tanımlamalarından sonraki adım, her bir VLAN için sanal uçların yani VLAN uç bağlantı noktalarının tanımlanması aşamasıdır. Buradaki amaç IP adreslerini yapılandırmaktır. Bu yapılandırmada iki adet fiziksel bağlantı ucuna ihtiyaç vardır. Birisi karşı bağlantı yani dış ağa bakan, diğeri ise üniversite iç ağına bakan uçtur.

- `interface vlan-interface20` (vlan-interface20 adında uç tanımlaması. Bu üniversite iç ağına bakan uçtur ve iç ağ için ağ geçidi olacaktır.)
- `ip address 10.0.0.1 255.255.255.224` (Bu uca ait IP tanımı yapılandırması)
- `interface vlan-interface201` (vlan-interface201 adında uç tanımlaması. Üniversitenin Ankara ağına bağlantı kurmak için kullanacağı uçtur.)
- `ip address 192.168.254.78 255.255.255.252` (Bu uca ait IP tanımı yapıldı.)

3.Adım: Sonraki adım ise oluşturulan bu ayarların hangi portlara aktarılacağı kısımlardır. Switch üzerinde bir fiber modül telekomünikasyon şirketine yani Ankara bağlantı noktasına, diğeri ise normal ethernet bağlantı ucu olarak yerel ağa takılacaktır.

- `interface gigabit 1/0/25` (25. Port fiber portudur, yapılandırılmak üzere bu komut çalıştırılıyor.)

- `port trunk permit vlan 20 201` (Bu işlem portun hangi VLAN içerisinde çalışacağı belirleniyor. Port trunk komutu paket içerisinde VLAN ID bilgisinin yer almasını sağlar, diğer bir deyişle tagged olarak adlandırılır. Bunun neticesinde Metro Ethernette farklı VLAN'lar bulunduğundan dolayı bu port trunk komutu ile yapılandırılmalıdır. Burada daha önce tanımlanan VLAN ağlarının bu uç üzerinde görev yapması atanıyor.)
- `quit` (interface gigabit 1/0/25 yapılandırmasından çıkartılır.)
- `interface Ethernet 1/0/1` (Switch üzerindeki ethernet portların birincisidir ve yapılandırmak üzere yazılıyor.)
- `port Access vlan 20` (Bu portun 20 numaralı VLAN ID ile bu VLAN ağına hizmet vereceği tanımlanıyor.)
- `quit` (interface Ethernet 1/0/1 yapılandırmasından çıkartılır.)

4.Adım: Son aşama bir yönlendirme satırının yazılmasıdır. Buradaki amaç, aynı router cihazlarda olduğu gibi trafiğin yönlendirilmesidir.

- `ip route-static 0.0.0.0 0.0.0.0 192.168.254.77 preference 60` (Tüm paketleri; adresi ve ağ maskesi adresi ne olursa olsun 192.168.254.77 adresine yönlendir manasında kullanılmaktadır. Bu adres Ulakbim Kurumu içerisindeki sistemin IP numarasıdır.)

3.2.3. Uzak Yerleşke Bağlantıları

Afyon Kocatepe Üniversitesi'ne ait uzak yerleşke bağlantıları ATM sistemi ile haberleşmelerine devam etmektedir. ATM sisteminde router cihazları seri bağlantı ile haberleşerek farklı iki ağın haberleşmesini gerçekleştirir. Seri bağlantıda ise router cihazları tek başlarına işlemi gerçekleştiremezler, bundan dolayı hattın uç noktalarında sisteme uygun modem cihazlar konulmaktadır. Diğer uzak yerleşkeler de bu şekilde yapılandırıldığından dolayı, tüm yerleşkeler için bir güvenlik sorunu söz konusudur. Ancak bu yerleşkelerde güvenliği üst düzeyde tutmak amacıyla birtakım iyileştirmeler gerçekleştirilmiştir. Daha önce her bir yerleşke kendi içinde bir LAN olmakta ve gerçek IP ile güvenlikten uzak bir şekilde Ankara Ulakbim Kurumu'na bağlanmaktaydı. Yapılan iyileştirmelerle tüm yerleşkeler üniversite merkez LAN ağının birer parçasıymış gibi bu ağa dâhil edilmişler ve bu şekilde

güvenlik politikaları, yerleşkelere uygulanarak internet ağına erişmeye başlamışlardır. Uzak yerleşkeler daha önce güvenlik zafiyetlerinden dolayı çok sık saldırılara maruz kalmakta ve bu saldırılardan dolayı ana merkezde bulunan sunucu ve cihazlar sıkıntı çekmekteydiler. Buradaki tüm yapılandırmalar hem yerleşkede bulunan router cihazı üzerinde, hem de ana merkezde bulunan router cihazı üzerinde gerçekleştirilmiştir. Başka hiçbir cihaza gerek duyulmamıştır. Örnek olarak bir meslek yüksek okulu yerleşkesinin yapılandırması anlatılmıştır. Yapılandırmalar yerleşke ve ana merkez üzerindeki router cihazları üzerinde yapılmıştır.

Yerleşke 1.Adım: Ethernet ve Serial bağlantı uçları ve IP tanımları gerçekleştiriliyor

- `interface Ethernet0` (İç ağa yönelik ethernet ucu tanımlanıyor)
  - `ip address 172.22.1.1 255.255.255.0` (IP si veriliyor.)
  - `quit`
- `interface Serial0` (Router üzerinde Seri bağlantı özellikleri tanımlanıyor)
  - `clock DTECLK1`
  - `link-protocol fr`
  - `fr lmi type ansi`
  - `quit`
- `interface Serial0.1 Point-to-Point` (Seri bağlantı için uç tanımlanıyor)
  - `ip address 192.168.3.2 255.255.255.252` (Bu uca ait IP adresi)
  - `fr dlci 42` (pvc numarası, diğer bir deyişle dlci numarası)
  - `quit`

Yerleşke 2.Adım: Yönlendirme satırı yazılıyor.

- `ip route-static 0.0.0.0 0.0.0.0 Serial 0.1 preference 60` (Tüm ağ trafiği seri bağlantıya yönlendiriliyor.)
- `quit`

Ana Merkez 1.Adım: Benzer şekilde uçlar tanımlanıp yönlendirme yapılacak ancak farklı olarak VRF (Virtual Route Forwarding) işlemi yapılacaktır. VRF Ağ güvenliğini sağlayan bir protokoldür ve paketleri, sanal bir tablo oluşturarak yönlendirme veya aktarma işlemlerinde kullanılır (İnt.Kyn.7).

- `ip vrf A` (A isimli yeni bir VRF tablosu oluşturuluyor.)
- `interface FastEthernet0/0` (Router üzerinde iç ağa bağlı olan ethernet ucu tanımlanıyor.)

- `ip vrf forwarding A` (A VRF' i üzerinde olacağı belirtiliyor.)
- `ip address 192.168.254.1 255.255.255.252` (IP adresi tanımlanıyor.)

- `interface ATM4/0.4 point-to-point` (Yerleşke için seri haberleşme noktası oluşturuluyor.)
  - `description Afyon_MYO` (İsim tanımı yapılıyor)
  - `ip vrf forwarding A` (A VRF' i üzerinde olacağı belirtiliyor.)
  - `ip address 192.168.3.1 255.255.255.252` (IP adresi)
  - `pvc 0/42` (pvc numarası belirleniyor.)
  - `protocol ip 192.168.3.2 broadcast` (Karşı iletişim noktası belirtiliyor)

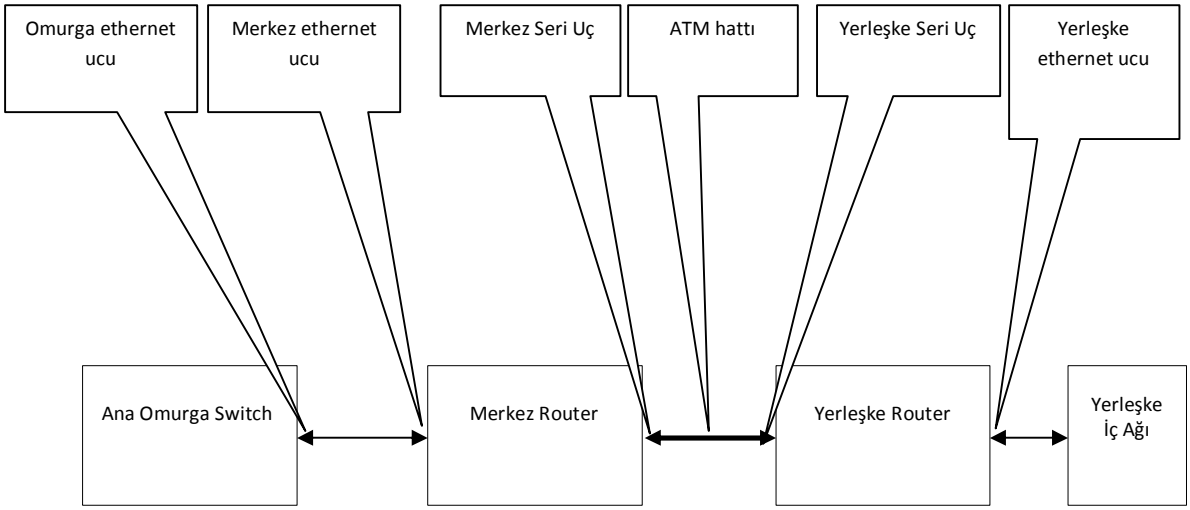
Ana Merkez 2.Adım: Bu yerleşke için yönlendirme satırı eklenmesi gerekiyor.

- `ip route vrf A 172.22.1.0 255.255.255.0 ATM4/0.4` (172.22.1.0 ağını ATM4/0.4 ucuna yönlendiriliyor.)

Ana Merkez 3.Adım: Router üzerindeki önemli husus ise, 1. adımda tanımlanan ethernet ucunun omurga switch üzerine bağlanmasıdır. Bunun nedeni ise daha önce belirtildiği gibi tüm uzak yerleşkelerin bu şekilde yerel ağa aktarılmış olması ve güvenlik politikalarından geçerek güvenli hale gelmesinin sağlanmasıdır. Bu nedenden dolayı router cihazı ile omurga switch cihazının haberleşmesinin sağlanması gerekmektedir. Cihazlar üzerindeki iki uç aynı ağ üzerine alınarak IP yapılandırmaları sağlanır, yani bu iki uç kendi aralarında başka bir LAN oluştururlar. Ethernet protokolü ile haberleşerek, iletişimi sağlarlar. Omurga üzerine 192.168.254.3 ve router üzerine 192.168.2.254.2 IP numaraları atanmıştır. Router üzerinde tüm paketlerin omurga switch'e yönlendirmesini yapmak için aşağıdaki satırı eklenmektedir.

- `ip route vrf A 0.0.0.0 0.0.0.0 192.168.254.2`

Yapılan işlemlerin şeması Şekil 3.4 üzerinde verilmiştir.



Şekil 3.4 Yerleşke ile merkez bağlantısının şematik gösterimi

3.2.4. İç Ağ Bağlantıları

Afyon Kocatepe Üniversitesi'nin dış bağlantıları olan, uzak yerleşke ile Ankara bağlantılarından sonra, diğer önemli çalışma ise iç ağ üzerine yapılmıştır. İç ağ üzerinde; merkez fakülteler, rektörlük, kütüphane gibi idari binalar fiber kablo ile bağlanmış durumdadır. Ayrıca uzak yerleşkeler yine iç ağa dâhil edilmişlerdir. Tüm bu bağlantılar 3Com 7700 omurga switch üzerinde toplanmakta ve üniversitenin yerel ağ yapısını oluşturmaktadır. Güvenlik çalışmalarının belirli bir kısmı omurga switch üzerinde yapılandırılan çeşitli ayarlar ile sağlanmıştır.

3.2.4.1. VLAN Yapılandırma İşlemi

Tasarlanan WTUES'nin ağ üzerindeki zararlı paketlerden etkilenmemesi amacıyla Afyon Kocatepe Üniversitesi iç ağ bağlantıları tamamen bir VLAN yapısı haline dönüştürülmüştür. Tüm akademik ve idari birim ağları kendi aralarında birar VLAN şekline getirilmiştir. Tüm bu yapılandırmalar omurga switch üzerinde yapılmıştır.

3.2.4.2. 3Com 7700 Omurga Switch Üzerinde VLAN Yapılandırılması

VLAN yapılandırılmasına geçmeden önce fiziksel olarak ilgili kablonun omurga üzerinde hangi uçta takılı olduğunun belirlenmesi ve o porta göre yapılandırılması gerekiyor. Eğer çok sistemli bir yapı oluşturulacaksa tüm VLAN planı, omurga portlarına hangi hatların takıldığı yazılı bir doküman haline getirildikten sonra işleme tabi tutulmasında fayda vardır. Örnek olarak sadece Fen Edebiyat Fakültesi' ne ait yapılandırma anlatılmaktadır. Fakülte fiber kablo aracılığı ile omurga üzerindeki fiber modüllü GigabitEthernet2/0/14 portuna bağlı durumdadır.

1.Adım: Afyon Kocatepe Üniversitesi'nin bulunduğu ağ içerisinde IP yapılandırmasını otomatik sağlayan bir DHCP (Dynamic Host Configuration Protocol) sunucusu bulunmaktadır. Bu sunucu daha önce tüm LAN için IP numarası dağıtırken, VLAN yapısına geçilmesinden sonra her VLAN için farklı ağlarda IP numarası dağıtmaktadır. Omurga switch üzerinde yapılması gereken DHCP sunucusunu tanımlamak ve uçlar tanımlanırken bu tanımlamayı o kısma eklemektir. Omurga üzerinde oluşturulan VLAN yapısı, daha önce bahsedilen Metro Ethernet VLAN yapısına benzer bir şekilde gerçekleştirilmektedir.

- `dhcp-server 1 ip 172.17.0.10` (DHCP sunucusu tanımlanıyor)

2.Adım: Yeni bir VLAN tanımlanarak açıklaması yazılıyor

- `Vlan 10` (Fakülte için Vlan, ID numarası verilerek oluşturuluyor.)
  - `description Fen_Edebiyat` (İsim tanımı yapılıyor)
- `interface Vlan-interface10` (Fakülte için VLAN noktası oluşturuluyor.)
  - `ip address 172.20.10.1 255.255.254.0` (IP adresi ve ağ maskesi belirtiliyor)
  - `dhcp-server 1` (Hangi DHCP sunucusu ile çalışacağı belirleniyor. Yukarda tanımlanmıştır.)
- `interface GigabitEthernet2/0/14` (Fakülte için VLAN bağlantı noktası oluşturuluyor.)
  - `port Access vlan 10` (port atanıyor.)

3.Adım: Son adımda omurgaya gelen tüm iç ağın çıkış noktası (default gateway-varsayılan ağ geçidi) oluşturuluyor. Bunun için bir yönlendirme satırı eklenerek tüm ağ paketlerinin çıkış

noktası olarak firewall sunucusuna yönlendiriliyor. Aksi halde tüm sistem kendi arasında haberleşmesine rağmen diğer sunuculara erişemeyecek ve internete bağlanamayacaktır.

- `ip route-static 0.0.0.0 0.0.0.0 172.17.0.9 preference 60` (Tüm ağ, firewall sunucusunun IP'sine yönlendiriliyor.)

3.2.4.3. VLAN Yapısı için DHCP Sunucu Yapılandırma İşlemi

Sisteme kurulan DHCP sunucusu, Suse Linux işletim sisteminin DHCP paketinden oluşmaktadır. Bu paketin kullanımı çok basit olmakla birlikte yapılması gereken VLAN yapısına göre, her VLAN için ilgili konfigürasyon (conf) dosyasına bu değerlerin uygun formatta belirtilmesi gerekmektedir. Örnek olarak daha önce oluşturulan VLAN için dhcpd.conf dosyasında uygulanış şekli verilmektedir.

```
shared-network subnet-10 {
subnet 172.20.10.0 netmask 255.255.254.0 {
        option routers 172.20.10.1;
        option subnet-mask 255.255.254.0;
        option domain-name-servers 172.17.0.8;
        range 172.20.10.20 172.20.11.254;}}
```

Buradaki ayrıntılar sırasıyla; VLAN ID numarası, ağ IP aralığı, ağ geçidi, ağ maskesi, DNS Domain Name System) sunucunun IP numarası ve hangi aralıklarda VLAN için otomatik IP dağıtması gerektiği tanımlamaları yapılıyor. Bu şekilde hem omurga hem de DHCP sunucu üzerinde VLAN tanımlamaları yapılmıştır.

3.2.4.4. Omurga Switch Üzerinde Hat Kalitesinin Artırılması (QoS)

Ağ güvenliği için gerekli görülen QoS uygulaması 3Com 7700 omurga switch üzerinde yapılmış ve yapılan çalışmalar aşağıda anlatılmıştır.

1.Adım: Önce yeni bir ACL oluşturulmakta ve ardından kurallar satırlar halinde sırayla tanımlanmaktadır.

- `Acl number 3007` (3007 numaralı yeni bir ACL oluşturuluyor.)

- `rule 0 permit tcp destination-port eq www` (www 80.port demektir, port numarası da yazılabilir. permit komutu ile tcp protokolü 80.porttan iletişime izin veriliyor)
- `rule 1 permit tcp destination-port eq 443` (Tcp Port 443 e izin veriliyor)
- `rule 2 permit udp destination-port eq dns` (Udp Dns portuna izin veriliyor.)
- `rule 3 permit udp destination-port eq bootps` (Udp bootps yani dhcp sunucudan otomatik ip almasına izin veriliyor)
- `rule 4 permit udp destination-port eq bootpc` (Yukardaki ile benzer işlevi taşıyor)
- `rule 5 permit tcp source 172.20.1.30 0 destination-port eq ftp` (Kaynağı 172.20.1.30 IP si olan makine ftp iletişimi yapabilsin)
- `rule 6 permit tcp source 172.16.1.30 0 destination-port eq ftp-data` (yukardaki satır ile benzer işlem için tanımlanıyor)
- `rule 7 deny ip` (Tüm iletişime izin verilmesin şeklinde tanımlama yapılıyor, bunun nedeni ise yukarda verilen kurallar geçerli olacak, ama bunların dışında kalanlar, iletişim yapamayacaklardır.)

Burada yapılan çalışmaların özeti şu şekildedir. İletişim yaparken sadece web kullanıma izin verilsin ancak diğer özel işlemlere izin verilmesin. Ağın web dışında farklı işlemlerden dolayı meşgul edilmesi engellensin. Uzaktan Eğitim Sistemi'nde bunların dışında farklı bir iletişime gerek duyulmaz, sadece burada bir bilgisayara FTP erişimi verilmiştir. Bu bilgisayara veya buna benzer diğer özel izinler için farklı izinler verilebilir. Buradaki amaç o kişilerin yönetici gibi dosya alma, dosya gönderme gibi farklı yetkilerinin olması ve bu işlemlere ihtiyaç duymalarıdır.

2.Adım: ACL oluşturma işleminden sonra yapılması gereken bu kuralların nerelerde uygulanma ihtiyacının olduğudur. Cihaz üzerine gelen uçlardan hangi nokta için bu işlemin gerçekleştirilmesi isteniyorsa o uçla ilgili yapılandırma kısmına girilir ve tanımlama gerçekleştirilir.

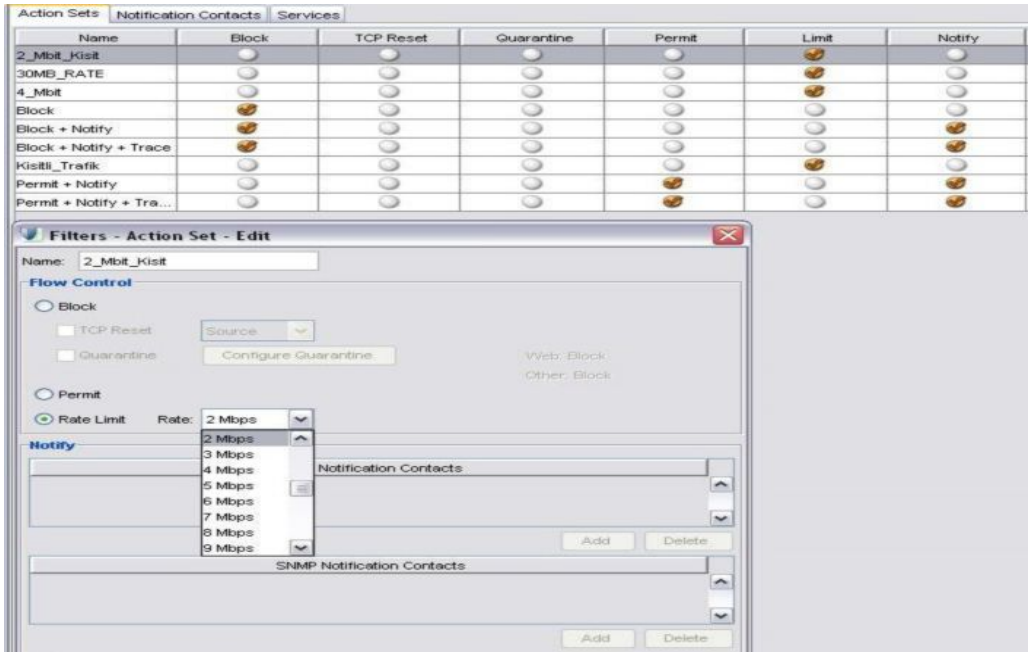
- `interface GigabitEthernet6/0/10` (Daha önce tanımlanan VLAN kısmına yapılandırılmak üzere giriş yapılıyor)
- `qos` (QoS yapılandırması için bu komut yazılıyor)
- `packet-filter inbound ip-group 3007` (3007 numaralı ACL bu VLAN'a atanıyor)

- `traffic-limit inbound ip-group 3007 rule 5 kbps 1024 exceed drop` (Bu kod ACL üzerindeki bazı kurallar için özel olarak band genişliğini belirtme amaçlı kullanılmıştır. ACL 'in 5. kuralı 1024 kbps den fazla hat hızını geçemez.)

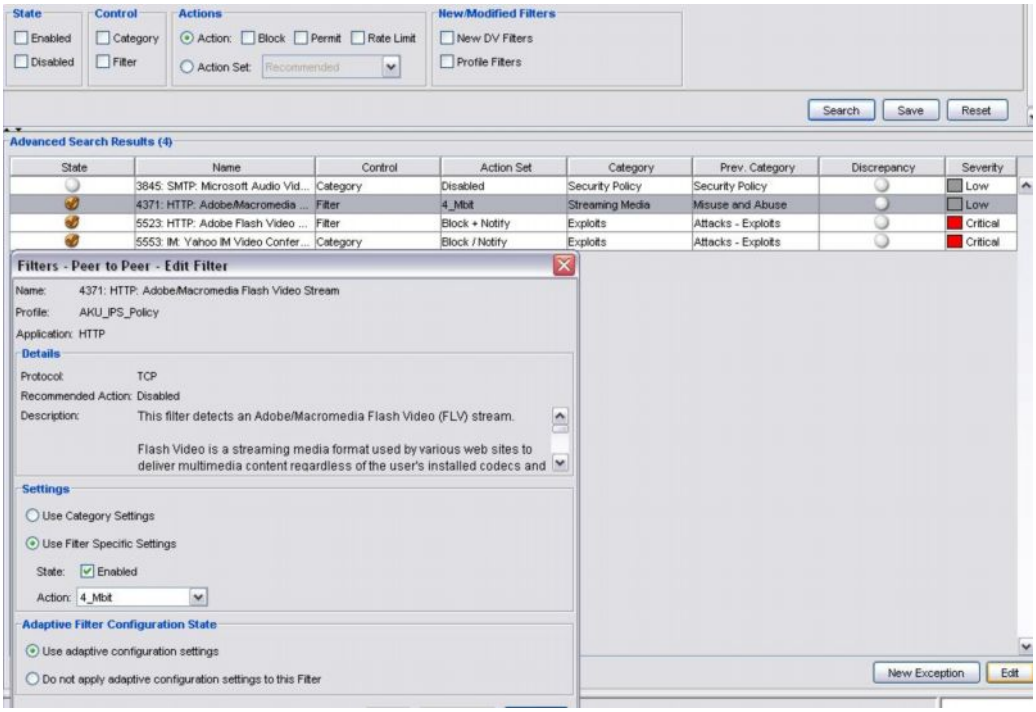
3.2.5. Üst Düzey Güvenlik İçin IPS Cihazının Kullanımı

WTUES'ni koruma ve güvenliğini sağlama amaçlı olarak 3Com Tıpping Point adı altında IPS cihazı, iç ve dış ağ noktalarına entegre edilmiştir. Cihaz üzerinde gelen 6 Ethernet portu ile birlikte 3 farklı ağ noktasının kontrolü yapılabilmektedir. Cihaz ile birlikte gelen yazılımı sayesinde ağ üzerindeki paketlerin kontrolü ve birtakım güvenlik uygulamaları yapılabilmektedir. Örnek kullanımı aşağıda açıklanmaktadır.

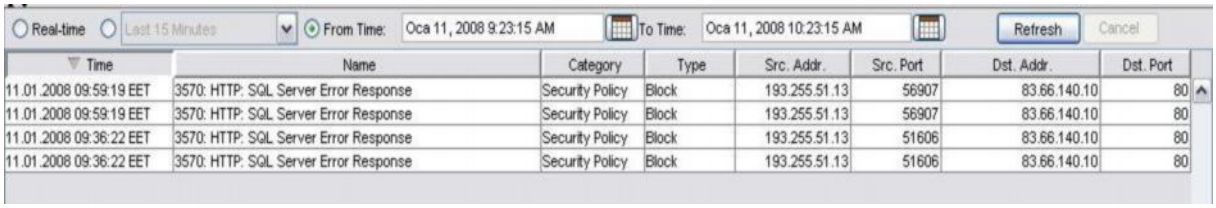
- Profil Oluşturma: Bu kısımda, ağ için bant genişliği limitlerini belirtmek, sorunlu paketleri durdurmak veya bazı özel durumlar için izin vermek gibi tanımlamalar gerçekleştirilmektedir. Resim 3.1 üzerinde 2Mbit kısıtlı yeni bir profil oluşturuluyor.
- Ağ üzerinde çalışan uygulamalara, oluşturulan profiller atanarak kısıtlama, izin veya kesme işlemleri yapılmaktadır. Resim 3.2 üzerinde Macromedia Flash uygulamalarında ağda oluşan trafiğe 4Mb gibi bir kısıt konulmaktadır. Aynı tabloda yine bazı video işlemleri engellenmektedir.
- İç ağdan veya dışarıdan gelen saldırı ve engellemeler bu arayüz vasıtasıyla görüntülenebilmektedir. Belirli zaman dilimleri olarak veya güvenlikte oluşturduğu duruma göre izlenimler ve raporlar alınabilmektedir. Güvenlik tehdidi algılanıyorsa sistem bunu durduracak ve e-posta göndererek uyaracaktır. Resim 3.3 ve Resim 3.4 üzerinde yapılmış saldırıların engellenişi (Block-Bloke edilişi) görülmektedir.



Resim 3.1 IPS Cihazı üzerinde kısıtlı trafik için yeni profil oluşturma

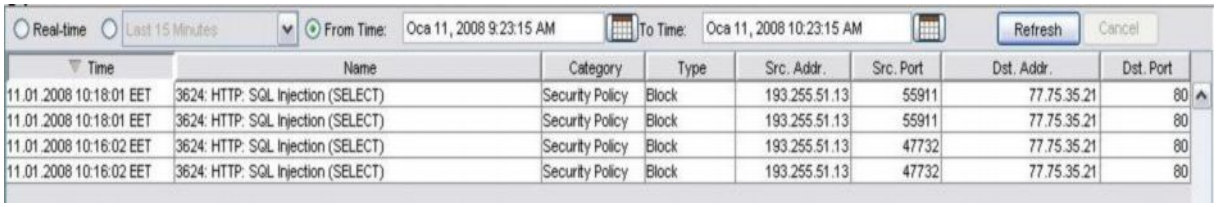


Resim 3.2 Bazı uygulamalara hazırlanmış profillerin atanması


Real-time | Last 15 Minutes | From Time: Oca 11, 2008 9:23:15 AM | To Time: Oca 11, 2008 10:23:15 AM | Refresh | Cancel

Time	Name	Category	Type	Src. Addr.	Src. Port	Dst. Addr.	Dst. Port
11.01.2008 09:59:19 EET	3570: HTTP: SQL Server Error Response	Security Policy	Block	193.255.51.13	56907	83.66.140.10	80
11.01.2008 09:59:19 EET	3570: HTTP: SQL Server Error Response	Security Policy	Block	193.255.51.13	56907	83.66.140.10	80
11.01.2008 09:36:22 EET	3570: HTTP: SQL Server Error Response	Security Policy	Block	193.255.51.13	51606	83.66.140.10	80
11.01.2008 09:36:22 EET	3570: HTTP: SQL Server Error Response	Security Policy	Block	193.255.51.13	51606	83.66.140.10	80

Resim 3.3 Sistemdeki sunucu için yapılan bir saldırının IPS tarafından engellenişi


Real-time | Last 15 Minutes | From Time: Oca 11, 2008 9:23:15 AM | To Time: Oca 11, 2008 10:23:15 AM | Refresh | Cancel

Time	Name	Category	Type	Src. Addr.	Src. Port	Dst. Addr.	Dst. Port
11.01.2008 10:18:01 EET	3624: HTTP: SQL Injection (SELECT)	Security Policy	Block	193.255.51.13	55911	77.75.35.21	80
11.01.2008 10:18:01 EET	3624: HTTP: SQL Injection (SELECT)	Security Policy	Block	193.255.51.13	55911	77.75.35.21	80
11.01.2008 10:16:02 EET	3624: HTTP: SQL Injection (SELECT)	Security Policy	Block	193.255.51.13	47732	77.75.35.21	80
11.01.2008 10:16:02 EET	3624: HTTP: SQL Injection (SELECT)	Security Policy	Block	193.255.51.13	47732	77.75.35.21	80

Resim 3.4 Sistem SQL sunucusuna, SQL Injection saldırısının IPS tarafından engellenmesi

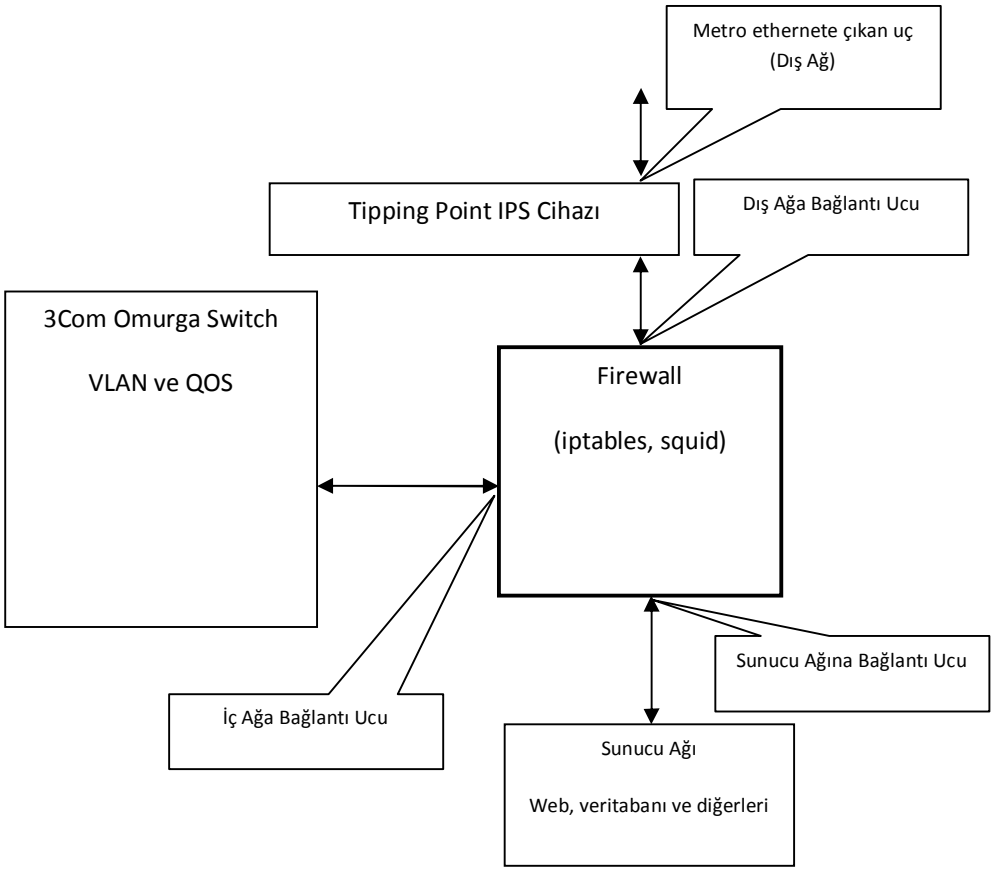
3.3. Sunucu Güvenliği

Tasarlanan WTUES için kullanılan sunucular firewall, web ve veritabanı olmak üzere 3 ana sunucudan oluşmaktadır. Bunun yanında sistemde e-posta, dhcp, dns, anti virüs gibi proje ile birlikte kullanılan sunucular bulunmaktadır. Ayrıca deneme ve test amaçlı bir test bilgisayarı yine sistem dâhilinde kullanılmaktadır. Web ve veritabanı sunucuları Microsoft Windows 2003, diğer sunucular ise Linux işletim sistemleri ile yapılandırılmışlardır. Linux, kararlı çekirdeği, ağ yazılımlarının çeşitliliği ve kalitesi, performans/maliyet eğrisindeki konumu nedeni ile günümüzün en çok tercih edilen ağ işletim sistemlerinden olmuştur. Yazılım platformunun Microsoft tabanlı olması, yazılım sistemlerinde geniş dokümantasyon ve ileri teknolojiye sahip olmasından dolayı web ve veritabanı sunucularında Microsoft Windows işletim sistemi tercih edilmiştir.

3.3.1. Firewall Sunucusu Yapılandırması

Firewall sunucusu 3 ayrı ağ üzerinde konumlandırıldığından dolayı 3 Ethernet kartı ile desteklenmiştir. Dolayısı ile 3 yönlü trafiği yönetmekle yükümlüdür. Bu trafik; iç ağ, dış ağ

ve sunucu ağı olmak üzere Şekil 3.5 üzerinde belirtilmektedir. Üç ethernet bağlantısının olması sebebiyle her uç için ilgili IP numaraları verilmiştir.



Şekil 3.5 Firewall sunucusunun sistem içerisinde şematik gösterimi

Firewall sunucusu olarak tasarlanan sistem Linux tabanlı Suse 10.3 işletim sistemidir. Sistem üzerinde yapılan bilgi güvenliğini sağlama amacıyla kurulan paketler ve bu paketler üzerinde yapılan çalışmalar aşağıda anlatılmaktadır.

3.3.1.1. Iptable paketi

Iptable kurulan sunucunun işletim sistemi ile birlikte gelen bir yazılım paketidir. Ağ kurallarının işletilmesini ve yönetilmesini sağlar. Tasarlanan WTUES'ni olabilecek saldırılardan koruma amacıyla işletilen kurallar şu şekildedir. Burada tüm kurallar anlatılmamış sadece uygulamdan çeşitli örnekler aktarılmıştır.

Kaynak ve hedef portu 80 olan tüm tcp giriş paketlerini kabul et bunların dışında kalanları durdur.

- `iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT`
- `iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT`
- `iptables -A INPUT -j DROP`

Üzerinden ICMP protokolü işleyen paketlerden 172.22.1.30 makinesine izin ver bunların dışındakileri durdur.

- `iptables -A FORWARD -s 172.22.1.30 -p ICMP -j RETURN`
- `iptables -A FORWARD -s 0.0.0.0/0.0.0.0 -p ICMP -j DROP`

Üzerinden geçen TCP 25.port (e-posta alıp-gönderme) işlemleri için 193.255.48.101 (e-posta sunucusu) için izin ver ancak 172.22.0.0 ağındaki makinelerinden hiçbirine izin verme durdur.

- `iptables -A FORWARD -s 193.255.48.101/32 -m tcp -p tcp --dport 25 -j ACCEPT`
- `iptables -A FORWARD -s 172.22.0.0/16 -m tcp -p tcp --dport 25 -j DROP`

Hedef adresi 193.255.48.124 olan ve ethernet0 ucundan gelen TCP paketlerini DNAT yaparak 172.22.0.28 hedefine gönder.

- `iptables -t nat -A PREROUTING -d 193.255.48.124 -i eth0 -p tcp -m tcp -j DNAT --to-destination 172.22.0.28`

Hedef adresi 193.255.48.123 olan, ethernet0 ucundan gelen ve hedef portu 5003 olan TCP paketlerini DNAT yaparak 172.22.0.22 hedefinin 5003 numaralı portuna gönder.

- `iptables -t nat -A PREROUTING -d 193.255.48.123 -i eth0 -p tcp -m tcp --dport 5003 -j DNAT --to-destination 172.22.0.22:5003`

Kaynak adresi 172.22.0.0 ağına ait tüm paketleri ethernet0 çıkışından SNAT yaparak 193.255.48.11 adresinden çıkıyormuş gibi çıkart (Burada belirtilen ağa ait tüm makinelerin çıkış IP si 193.255.48.11 adresinden gidiyormuş gibi hedefe ulaşır.)

- `iptables -t nat -A POSTROUTING -s 172.22.0.0/16 -o eth0 -j SNAT --to-source 193.255.48.11`

MSSQL isminde yeni bir zincir oluşturuluyor. Bu zincire hedef adresi 193.255.48.15 (veritabanı sunucusu) olan ve üzerinden gecen paketleri göz önüne alacağı bir kural belirleniyor. Belirtilen bu kural; hedef portu 1433 olan 193.255.48.14 (web sunucusu) kaynaklı ise kabul et. Bunun dışındaki iletişime izin verme. Buradaki maksat web sunucusu sadece veritabanı sunucusundan sorgulama yapabilsin, bunun haricindekiler ulaşamasın. 1433 portu MSSQL sunucuya erişim ve sorgulama portudur. Eğer bu kural uygulanmaz ise farklı kişiler dışarıdan veya içerden bilgilere erişim için sistemi yoklayacak ve kırmaya çalışacaklardır.

- `iptables -N MSSQL`
- `iptables -A FORWARD -d 193.255.48.15 -j MSSQL`
- `iptables -A MSSQL -p tcp -m tcp -s 193.255.48.14/32 --dport 1433 -j RETURN`
- `iptables -A MSSQL -p tcp -m tcp -j DROP`

Squid sisteminin çalışması için aşağıdaki kural işletiliyor. Önce tüm 3128 hedefli girişler kabul ediliyor, sonrasında ise 172.22.0.0 ağına ait 80.port (HTTP) istekleri 3128 port numarasına (Squid dinleme portu) yönlendiriliyor.

- `iptables -A INPUT -p tcp -m tcp --dport 3128 -j ACCEPT`
- `iptables -t nat -A PREROUTING -s 172.22.0.0/16 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3128`

3.3.1.2. Squid Paketi

Squid yapılandırması squid.conf dosyası üzerindeki ayarları düzenlemekle yapılabilmektedir. Dosya içersine girildiğinde birtakım ayarlar ve açıklamalar yer almaktadır. Sistem için tasarlanan yöntem Transparent Proxy oluşturmaktır. Bunun için gerekli ayarlar şu şekildedir.

Squid'in Transparent Proxy olarak 3128. porttan çalışacağı belirtiliyor.

```
http_port 3128 transparent
```

Sonraki aşamada kullanıcıların sayfalara bağlandıkları zaman ilgili sayfa içeriklerinin nerede depolanması gerektiği belirtiliyor. Kullanıcıların ziyaret ettiği sayfaların içerikleri tutulur ve başka bir kullanıcı, aynı sayfayı ziyaret etmek istediğinde ana sayfaya gönderilmez ve sakladığı sayfayı göndererek ve performans artışı sağlar.

- `cache_dir ufs /cache1 100 16 256`
- `cache_dir ufs /cache2 100 16 256`

Bağlantı ve içerik loglarının sürekli yazıldığı log dosyalarının nerede saklanacağı belirleniyor.

- `access_log /var/log/squid/access.log squid`
- `cache_store_log /var/log/squid/store.log`

ACL tanımlamaları yapılıyor, tanımlanan her bir ACL için kaynak IP adresi veya IP adreslerinin listesinin bulunduğu bir dosya ismi belirtiliyor. Örneğin Yasak_Siteler kısmında iç ağ üzerinden dışarıya erişilmesi istenmeyen adresler belirtilmiştir. Bu adresler genelde video, müzik siteleri veya dosya paylaşım siteleri olmaktadır. Yasak_Ipler kısmında ise tamamen hiçbir yerle iletişim kurmasını istemediğimiz IP'lerdir. Bu kişiler sistem kaynaklarını çok tüketen veya virüs worm atakları yapan sorunlu makineler olabilir. Izinli_Ipler_Full kısmında ise heryere erişim hakkı bulunan özel kullanıcıların IP numaraları belirtilmiştir.

- `acl localhost src 127.0.0.1/255.255.255.255`
- `acl kampus src 172.22.0.0/255.255.0.0`
- `acl saglikmyo src 172.23.1.0/255.255.255.0`
- `acl Yasak_Siteler  dstdomain "/etc/squid/Yasak_Siteler"`
- `acl Yasak_IP src "/etc/squid/Yasak_IP"`
- `acl Izinli_IP src "/etc/squid/Izinli_IP"`

Yasak_IP ve Yasak_Siteler tanımları deny komutu kullanılarak sistemden geçişleri yasaklanıyor.

- `http_access deny  Yasak_IP`
- `http_access deny  Yasak_Siteler`

Burda ise ACL tanımlarına allow komutu kullanılarak sistemden geçişlerine izin veriliyor.

- `http_access allow Izinli_IP`
- `http_access allow localhost`
- `http_access allow kampus`
- `http_access allow afyonsaglik`

Uygulanan tüm ACL'lerin dışında kalan her şey deny all komutu kullanılarak iletişimleri yasaklanıyor.

- `http_access deny all`

Squid.conf dosyasının yapılandırılmasından sonra kayıt edilir ve tekrar çalıştırılır. İlgili dosyalardaki herhangi bir değişiklikten sonra yapılan işlemin geçerli olabilmesi için tekrar kapatılıp çalıştırılması gerekmektedir.

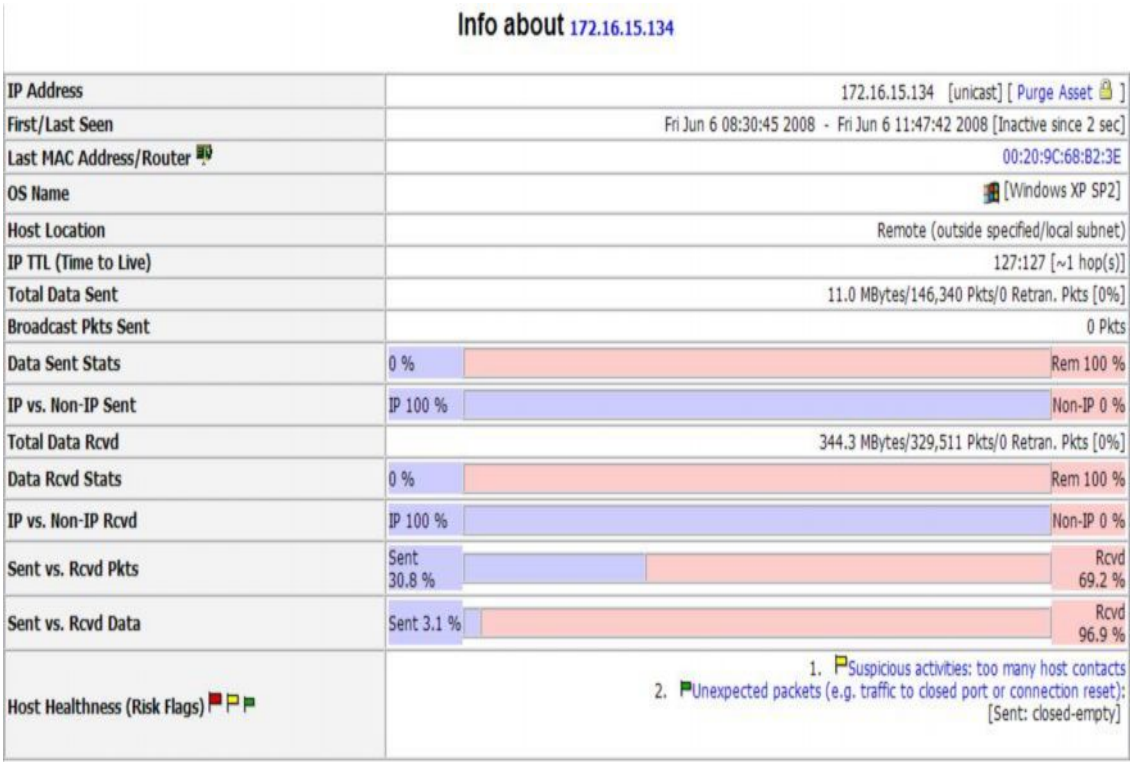
3.3.1.3. Squid Kullanımı ve Ntop Yazılımı

WTUES projesinde kullanmak ve sağlıklı ağ takibi yapabilmek amacıyla NTOP isimli bir yazılımı firewall sunucusu üzerine entegre edilmiştir. Kurulumu çok basit olan yazılımın en büyük özelliği ise ağ istatistiğini çıkarması ve hangi bilgisayarların ne kadar ağ kaynaklarını harcadığını göstermesidir. Ayrıca IP bazlı olarak bir bilgisayarın ne zaman hangi sitelere bağlandığı veya hangi IP adresleri ile iletişime geçtikleri gibi sonuçları sistem yöneticisine bildirebilmektedir. Resim 3.5 üzerinde yaklaşık 12 saatlik bir ağ trafiği çıkartılmıştır. Hangi bilgisayarların ne kadar ağ trafiği yaptıkları sıralanmıştır.

Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail
172.17.2.24		6.7 GBytes	15.3 %	16.2 KBytes	18.9 MBytes	236	0	0	11.2 KBytes
akudemi		2.2 GBytes	4.9 %	0	2.1 GBytes	0	0	7.3 KBytes	1.7 KBytes
www.aku.edu.tr		1.8 GBytes	4.0 %	139.8 KBytes	1.0 GBytes	0	0	11.5 KBytes	3.3 KBytes
radyo		1.5 GBytes	3.4 %	0	37.7 KBytes	0	0	9.3 KBytes	0
172.16.71.203		1.1 GBytes	2.6 %	2.2 MBytes	22.6 MBytes	3.4 KBytes	0	0	0
172.16.31.199		871.5 MBytes	1.9 %	0	7.9 MBytes	5.0 KBytes	0	0	40.7 KBytes
172.16.42.76		753.1 MBytes	1.7 %	4.1 KBytes	8.2 MBytes	9.1 KBytes	0	0	24.1 KBytes
172.16.0.6		698.2 MBytes	1.6 %	2.0 MBytes	668.0 MBytes	17.6 MBytes	60	4.8 KBytes	8.9 KBytes
crawl-66-249-72-232.googlebot.com		661.8 MBytes	1.5 %	0	661.8 MBytes	0	0	0	0
www.hurriyet.com.tr		544.4 MBytes	1.2 %	0	544.4 MBytes	0	0	0	0
172.16.1.217		503.2 MBytes	1.1 %	0	493.2 MBytes	34.6 KBytes	0	54.5 KBytes	0
212.156.63.102		499.6 MBytes	1.1 %	0	188.6 MBytes	0	0	0	0
www.milliyet.com.tr		468.6 MBytes	1.0 %	0	468.6 MBytes	0	0	0	0
172.17.4.27		423.2 MBytes	0.9 %	0	12.0 MBytes	3.7 KBytes	0	0	244

Resim 3.5 Ntop yazılımı ile belirli zaman aralığında ağ iletişimi yapan bilgisayarların bir kısmı harcadıkları bant genişliğine göre sıralanmışlardır.

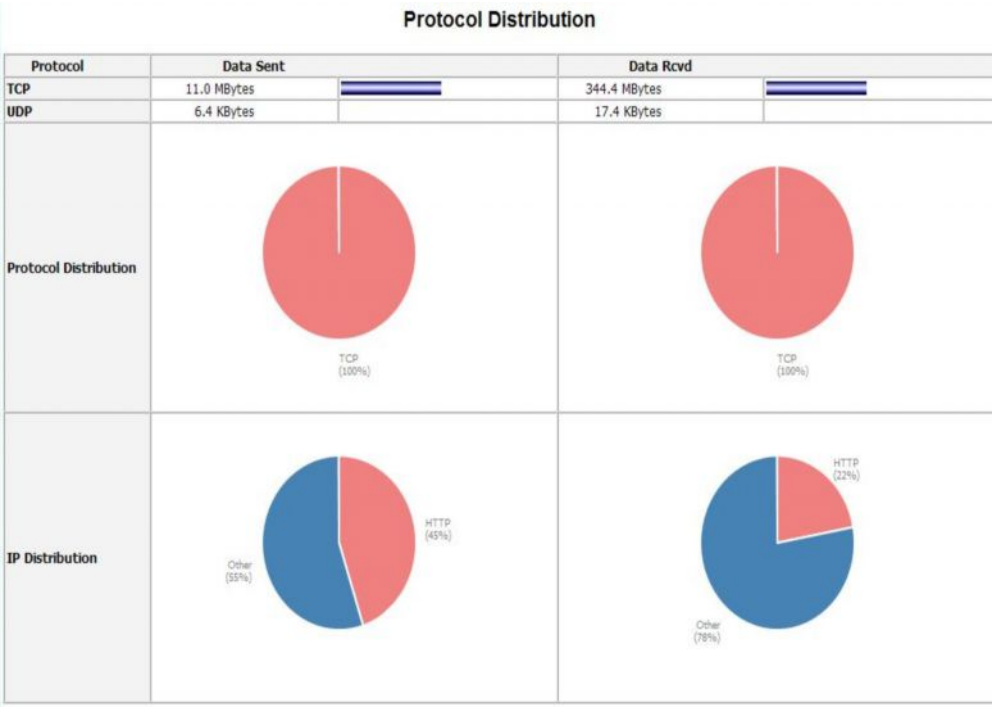
Ayrıntılı inceleme amaçlı olarak bir bilgisayarın yaptığı ağ istatistiği ve bağlantıları çıkartılıyor. Resim 3.6 üzerinde bayrak ikonları ile bu bilgisayarın içerdiği riskler bildirilmektedir. Resim 3.7 üzerinde grafiksel olarak ağ istatistiği çıkartılmış ve Resim 3.8 üzerinde ise hangi bilgisayarlar ile iletişim kurduğu detaylı olarak listelenmiştir.



Info about 172.16.15.134

IP Address	172.16.15.134 [unicast] [Purge Asset]
First/Last Seen	Fri Jun 6 08:30:45 2008 - Fri Jun 6 11:47:42 2008 [Inactive since 2 sec]
Last MAC Address/Router	00:20:9C:68:B2:3E
OS Name	[Windows XP SP2]
Host Location	Remote (outside specified/local subnet)
IP TTL (Time to Live)	127:127 [~1 hop(s)]
Total Data Sent	11.0 MBytes/146,340 Pkts/0 Retran. Pkts [0%]
Broadcast Pkts Sent	0 Pkts
Data Sent Stats	0 % Rem 100 %
IP vs. Non-IP Sent	IP 100 % Non-IP 0 %
Total Data Rcvd	344.3 MBytes/329,511 Pkts/0 Retran. Pkts [0%]
Data Rcvd Stats	0 % Rem 100 %
IP vs. Non-IP Rcvd	IP 100 % Non-IP 0 %
Sent vs. Rcvd Pkts	Sent 30.8 % Rcvd 69.2 %
Sent vs. Rcvd Data	Sent 3.1 % Rcvd 96.9 %
Host Healthness (Risk Flags)	1. Suspicious activities: too many host contacts 2. Unexpected packets (e.g. traffic to closed port or connection reset): [Sent: closed-empty]

Resim 3.6 172.16.15.134 IP numaralı bilgisayarın ilgili zaman diliminde yapmış olduğu bağlantı oranları gösterilmektedir.



Resim 3.7 Grafiksel olarak bilgisayarın yapmış olduğu ağ trafiği iletişim protokollerine göre değerlendirilmiştir.

Last Contacted Peers

Sent To	IP Address
istatistik.milliyet.com.tr	213.243.28.197
msnmercustacqprod.112.2o7.net	128.241.21.163
a.rad.live.com	65.55.197.114
yorum.milliyet.com.tr	213.243.28.122
.	67.159.30.212
by2msg1063001.gateway.edge.messenger.live.com	207.46.110.138
adsrv.adgroupm.com	213.144.108.197
cubics.com	216.21.215.14
Total Contacts	1475

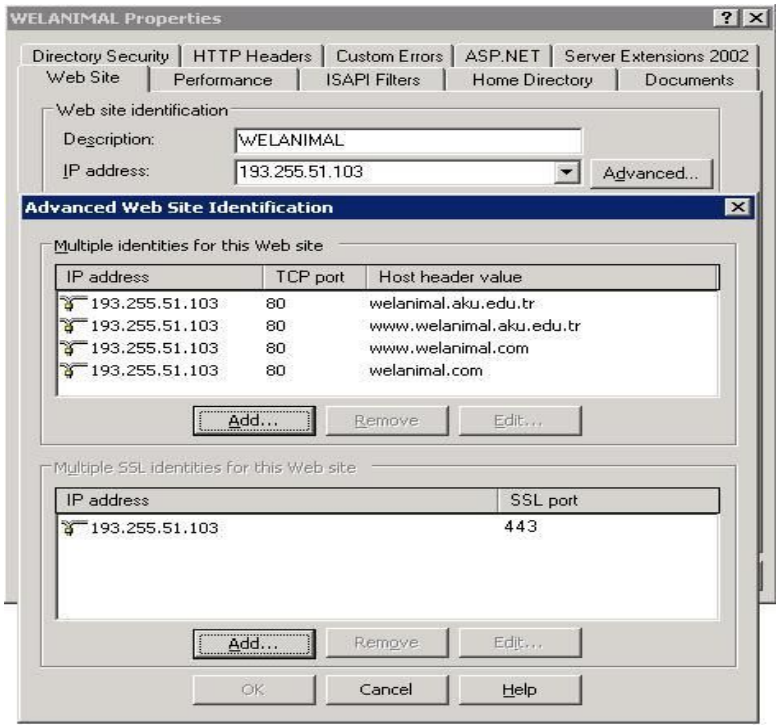
Received From	IP Address
msnmercustacqprod.112.2o7.net	128.241.21.163
a.rad.live.com	65.55.197.114
yorum.milliyet.com.tr	213.243.28.122
hp.msn.com	207.123.33.124
by2msg1063001.gateway.edge.messenger.live.com	207.46.110.138
.	67.159.30.212
adsrv.adgroupm.com	213.144.108.197
cubics.com	216.21.215.14
Total Contacts	1262

Resim 3.8 Bilgisayarın yapmış olduğu bağlantılar ve IP numaraları, ilgili noktalara tıklandığı zaman bu noktalara bağlanan diğer bilgisayarların listesi görüntülenebilmektedir.

3.3.2. Web Sunucusu (IIS 6.0) Yapılandırması

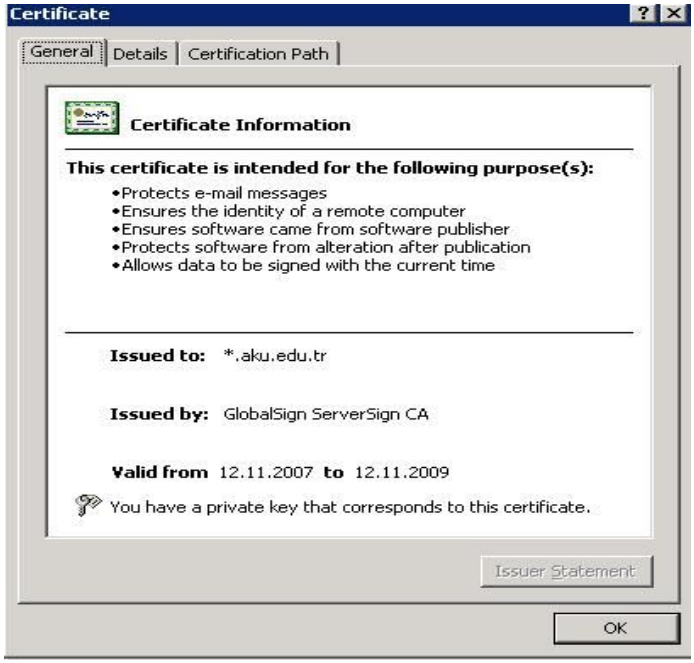
WTUES için Web sunucusu üzerinde güvenlik çalışmaları yapılmalıdır. Bu çalışmalar, sisteme yetkisi olmayan veya sistem açıklarından faydalanmak isteyen kişilere karşı bilgi

güvenliğini artıracaktır. Bu yapılandırmaların en önemlilerinden birisi, sistem üzerinde mutlaka kimlik denetleme sertifikasının bulunmasıdır. Tasarlanan Uzaktan Eğitim Sistemi için SSL sertifikası satın alınmış ve sisteme entegre edilmiştir. Bu işlem tamamen IIS üzerinde yapılmıştır. Resim 3.9 üzerinde WELANIMAL Uzaktan Eğitim Sistemi için yapılan IIS ayarları görüntülenmektedir.



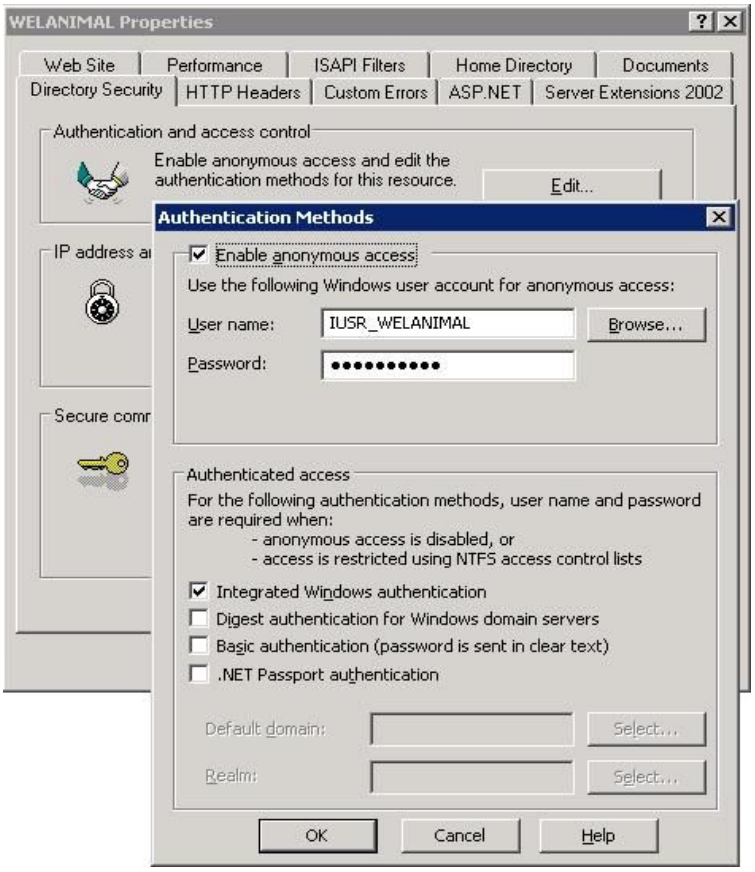
Resim 3.9 WELANIMAL projesi için gerçekleştirilen IIS ayarları.

Resim 3.10 ise satın alınan SSL sertifikası hakkında bilgiler içermektedir. Satın alınan SSL sertifikası belirli zaman aralığında geçerlidir. Anlaşma süresinin dolması durumunda tekrar satın alınması söz konusudur. Bundan dolayı anlaşma uzun tutulmalı veya anlaşma süresinin takibi mutlaka yapılmalıdır.



Resim 3.10 WELANIMAL projesi için satın alınan SSL sertifika bilgileri

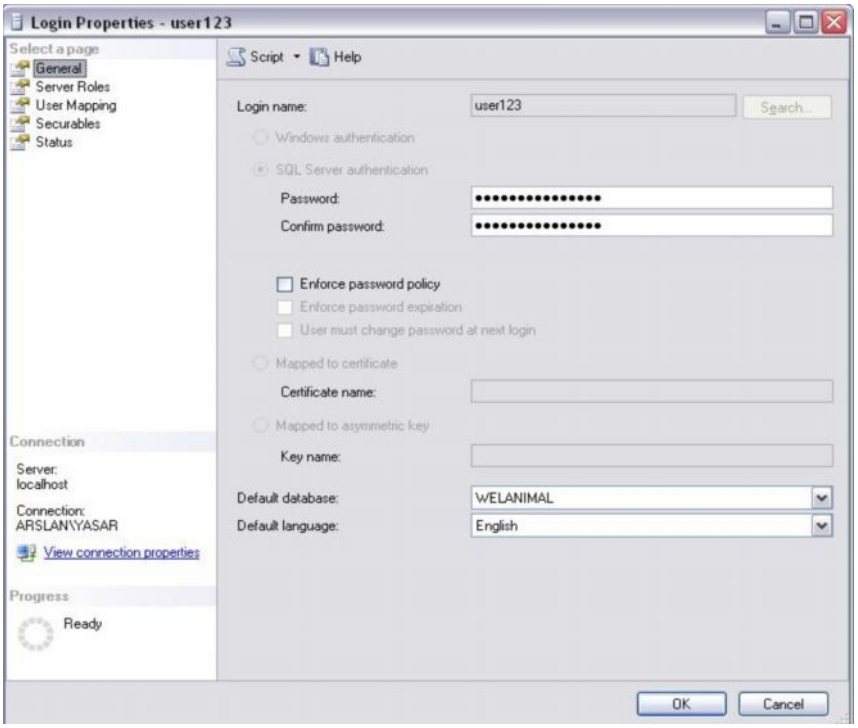
Resim 3.11 üzerinde, misafir kullanıcıların sisteme bağlanmalarını sağlanıyor. Enable Anonymous Access (Dışardan bağlanan kullanıcıya izin ver işlemi) seçeneğinin işaretli olması ile diğer kullanıcıların herhangi bir işlem yapmadan web sayfasını görüntüleyebilmeleri sağlanmaktadır. Integrated Windows Authentication (Yerel sunucu bilgisayar üzerinde kimlik denetimi) seçeneği ise, proje yerel sistemde çalıştırırken herhangi bir denetlemeye gerek kalmadan çalıştırılabilmesine olanak sağlar.



Resim 3.11 Web Sayfası Yetki Yapılandırması

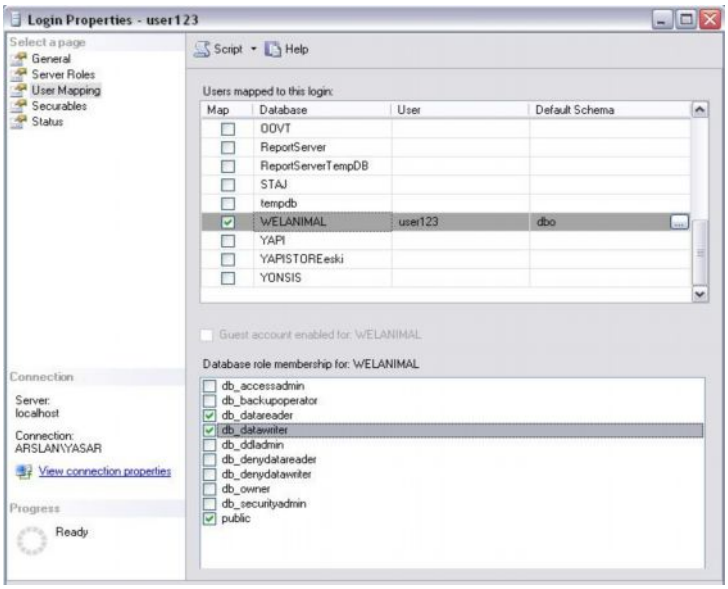
3.3.3. Veritabanı Sunucusu (MSSQL Server 2005) Yapılandırması

- Tasarlanan WTUES için veritabanı sisteminde WELANIMAL adlı veritabanı oluşturulmuş ve güvenlik çalışmaları yapılmıştır. Bunun için MSSQL Server üzerinde farklı kullanıcı adları ve şifreler tanımlanarak her kullanıcı için ayrı hesap oturumları oluşturulur. Resim 3.12 üzerinde user123 adlı kullanıcı için Karma Güvenlik kipinde yeni bir oturum hesabı oluşturuluyor.



Resim 3.12 Karma Güvenlik kipinde yeni bir kullanıcı tanımının yapılması

Resim 3.13 üzerinde proje yazılımının bağlantı kurup işlem yapacağı kullanıcı yetkileri tanımlanıyor. Sadece WELANIMAL veritabanına erişim ve bu veritabanı için okuma ve yazma hakları veriliyor. Bunun dışında farklı bir işlem yapılması engelleniyor.



Resim 3.13 Kullanıcı yetki tanımlamaları

3.4. Yazılım Güvenliği

Tasarlanan Web Tabanlı Uzaktan Eğitim Sistemi yazılım güvenliğinde, gerekli görülen bilgi güvenliği çalışmaları yapılmıştır. Bu çalışmalar yazılımın analizi, kodlanması ve test edilmesi esnasında defalarca yenilenmiştir.

3.4.1. Yazılım Analizi

WTUES üzerinde yapılan bilgi güvenliği analiz işlemleri şu şekilde bölümlendirilmiştir.

Kullanıcı Kayıt İşlemi: Sisteme dışarıdan üye olmak isteyenler için elektronik posta hesabına şifrenin gönderilmesi uygulamasıdır. Sistem bu arayüz vasıtası ile kullanıcı adı, e-posta hesabı ve birtakım bilgileri kullanıcıdan ister, bu bilgiler girildikten sonra onay tuşunun tıklanmasıyla işlem başlatılır. Bu kısımda bazı bilgilerin girilmesi zorunlu tutulmuştur, bu bilgiler olmadan herhangi bir işlem gerçekleştirilmez. Sistem, kullanıcı e-posta hesabına kullanıcı adı ve en az 6 karakterden oluşan rastgele üretilmiş bir giriş şifresini otomatik olarak gönderir. Kullanıcı kendisine gelen kullanıcı adı ve şifresi ile sisteme giriş yapar. Eğer daha önce var olan bir kullanıcı adı alınmak istenirse, sistem aynı isimden bir kullanıcı adı daha alınmasına izin vermez. Eğer sistem tarafından o anda herhangi bir aksaklıktan dolayı işlem yarıda kalmış ve kullanıcıya bu bilgi e-postası gönderilememiş ise, kullanıcı adı sistem tarafından alınmış kabul edilmez ve silinir. Kullanıcı kayıt işlemine devam eder ve yine aynı kullanıcı adı ile tekrar üye olabilir. Kullanıcı e-posta hesabına e-posta gönderilmesinin yanında, bilgi amaçlı olarak, yöneticinin de e-posta hesabına bu kayıt bilgileri gönderilir.
Bu kısımdaki en önemli noktalardan biriside, kullanıcı tipinin belirlenmesidir. Sistemde yönetici, eğitmen ve öğrenci olmak üzere 3 tip vardır. Bu 3 tip kullanıcı tek noktadan sisteme giriş yapmaktadır. Yeni kayıt olan kullanıcı, varsayılan olarak öğrenci tipindedir. Ancak eğitmen olarak işlem yapması gereken kullanıcıların tipleri, yönetici tarafından değiştirilirler.

Kullanıcı Giriş İşlemi: Kullanıcı ana sayfa üzerinde bulunan giriş kutularına kullanıcı adı ve şifresini yazarak sisteme giriş yapar. Tek noktadan girişi olan sistemde kullanıcı adı ve şifresi kontrol edilir. Eğer kullanıcı bilgileri doğru ise, kullanıcı tipi sisteme bildirilir. Bu tipe göre erişim hakkı bulunan sayfa ve formlara yönlendirilir ve sistemde güvenli bir şekilde oturum açmış olur. Kullanıcı giriş yapsın veya yapamasın her türlü giriş denemesinde bilgiler sistem

tarafından kayıt altına alınır. Hangi tarih ve saatte, hangi noktadan (bağlantı IP numarası) bağlandığı ve ne tür kullanıcı adı ile giriş yapmayı denediği log şeklinde veritabanına kaydedilir. Eğer arka arkaya 3 kez hatalı giriş yaparsa, bu kullanıcı bilgisi farklı bir tabloda saklanır ve yöneticiye mesaj veya e-posta yöntemi ile ulaştırılır. Bazı bilgisayar korsanları sisteme sızmak için kullanıcı giriş arayüzünü kullanırlar ve birtakım bilgileri buraya girerek sistemi yanıltmaya çalışırlar. Yâda bir başkasına ait kullanıcı adını kullanarak şifre denemesi yaparlar ve onun hesabına girmeye, bilgilerine ulaşmaya çalışırlar. Bu konu hakkındaki detaylı bilgi, çok kullanıcılı sistem güvenliği kısmında ele alınacaktır.

Şifre Hatırlatma: Kullanıcı eğer, kullanıcı adı veya şifresini unutursa ilgili linke tıklayarak arayüze ulaşır. Bu arayüz üzerinde kullanıcı adı ve e-posta hesabı bilgilerini almak üzere tasarlanmış, iki giriş noktası mevcuttur. İster kullanıcı adı, isterse e-posta adresini girerek şifresinin e-posta hesabına gelmesi sağlanır. Sistem burada, kullanıcının e-posta adresine tekrar rastgele karakterlerden oluşmuş yeni bir şifre gönderir. Çünkü kullanıcı şifreleri veritabanında MD5 formatında şifrelenmiş şekilde kayıt edilmektedir ve şifrelenmiş bilginin gerçekte hangi değeri ifade ettiği kesinlikle bilinmemektedir. Bu yüzden kullanıcıya eski şifresinin ne olduğuna ilişkin bir bilgi gönderilmez. Yeni şifresi gönderilerek tekrar giriş yapması ve şifresini değiştirmesi sağlanmaktadır.

Sisteme Girişin Engellenmesi: Ana sayfada sistemde kullanılmak üzere birtakım linkler verilmiştir. Ancak bu linkler yetki dâhilindedir. Eğer kullanıcı henüz sisteme giriş yapmamış ise bu kısımlardan faydalanamayacak ve karşısına giriş ekranı veya üye ol uyarısı gelecektir. Karşısına gelen formlarda, biraz önce anlatılan kısımlar gibi çalışacaktır.

Kullanıcıya göre işlemler: Sistemin 3 tipte kullanıcısı olduğunu belirtmiştik. Her kullanıcının erişebileceği linkler ve formlar onun yetkileri dâhilindedir. Kullanıcı sisteme giriş yaptıktan sonra, tüm sisteme yetkileri dâhilinde işlem yapabilecektir. Örneğin sadece kendisine gelen mesajları görüntüleyebilecek, kendisi ile ilgili derslerde işlem yapabilecek ve ayrıca yaptığı her işlem sistem tarafından kayıt altına alınacaktır. Diğer yandan, yönetici derslerin yönetimini yaparak yetkili olduğu kişileri belirlerken, bu yetkili kişiler dersleri düzenleyebilecek, öğrenci ise bu dersi takip ederek yetkisinin dışında farklı dersleri inceleme ve düzenleme gibi bir yetkisi bulunmayacaktır.

Kullanıcı Yetkilerinin Düzenlenmesi: Kullanıcı işlemleri sadece yöneticinin kontrolü altındadır. Yönetici olarak sisteme giren kişi bu arayüzü görebilmektedir. Yönetici bu kısımda isterse kayıtlı kullanıcıların sisteme girişini kısa bir süreliğine engelleyebilir veya tamamen silebilir. Yetki vereceği kişileri seçerek yetkilerini düzenleyebilir.

Form İşlemleri: Her form yetkiye göre hareket etmektedir. Duyurular, etkinlikler gibi birtakım formları sadece yönetici tarafından yetkisi belirlenmiş kişiler düzenleyebilir. Aynı şekilde ders konuları, ders içerikleri gibi düzenleme formları, yetkiye göre değişiklik göstermektedir.

İçerikler ve dosyalar: Bilgi bakımından çok önem arz eden formlar özellikler ders içeriği, sınavlar, anketler, dosya alışverişi, soru bankaları gibi yapılardır. Bu yapılar veri bakımından diğer yapılara göre daha yoğun işleme tabi tutulmaktadır. Sadece text tabanlı değil, görsel sesli ve görüntülü iletişim söz konusudur. Bilgi güvenliği ve erişimi bakımından yetkili kişilerin dışında bu bilgilere erişim kesinlikle engellenmiş olmalıdır. Sistemde bazı dosyalar kodlanmış şekilde veritabanında saklı tutulmaktadır. Özellikle mesajlaşma ve dosya transferleri konusunda bu mantık kullanılmaktadır. Ders içeriği gibi öğrenciye sunulması gereken dosyalar ise yetkiye göre herkesin kendi klasöründe tutulmaktadır.

3.4.2. Kullanıcı Yetkilerinin Kontrolü

Afyon Kocatepe Üniversitesi WELANIMAL projesi rol tabanlı bir sistem yapısı üzerine inşa edilmiştir. Uygulama içerisinde 4 farklı tür kullanıcı ve bu kullanıcılara ait rol yetkileri belirlenmiştir. Bunlar; yönetici, eğitmen, koordinatör ve öğrenci şeklindedir. Tüm bu davranışlar sistem içerisinde tek bir noktadan yönetilecek ve girişler tek bir giriş sayfasından yapılacaktır. Bunun yapılabilmesi için önce genel uygulamamız üzerindeki web.config dosyası üzerinde şu şekilde bir eklenti yapmak gerekiyor.

```
<authentication mode="Forms">
<forms name=".ASPXROLEBASED" loginUrl="Login.aspx" protection="All"
path="/"/>
</authentication>
```

Bu kısımda ASPXROLEBASED özelliği rol tabanlı bir uygulama olduğu ve loginUrl parametresi ile de kullanıcının, yetkisi dışında bir sayfaya erişmek istediğinde karşısına çıkacak giriş sayfasının ismi belirtiliyor. Kullanıcının karşısına giriş ekranı gelir ve giriş yapılır. Kullanının giriş yapması esnasında gerçekleşen hareketler ve algoritma şu şekildedir.

- Veritabanı üzerine bağlantı kurularak bu kullanıcının şifresi ile birlikte böyle bir tanımın var olup olmadığı belirlenir. Buradaki bir diğer ayrıntı da sorgulamalarda direk SQL komutları yerine güvenlik amacıyla MSSQL Server üzerinde Stored Procedure betikleri hazırlanarak kod içerisinden çağrılmaları sağlanmıştır. Eğer veritabanında kullanıcı tablosunda böyle bir kullanıcı ve şifresi tanımlı ise hazırlanan bu betik geriye kullanıcının ne tür bir role sahip olduğunu döndürür. Zira kullanıcı tablosunda kullanıcılar tanımlanırken, rol alanı oluşturularak rolü tanımlanmıştır.
- Kullanıcıya ait rol tanımının döndürülmesi ile birlikte bu kullanıcının erişim yetkisi olan sayfalara yetkisi sağlanmalı ve yetkisi dışındakiler yasaklanmalıdır. Bunun en kolay çözümü proje içerisinde her bir rol için birer klasör açmak ve yine her bir klasör içersine web.config dosyaları oluşturarak ilgili klasöre yetkilendirme yapılacak şekilde yapılandırılması gerekmektedir. Uygulamanın bulunduğu klasöre admin, egitmen, koordinator ve ogrenci seklinde klasörler oluşturulmuştur. Örnek olarak admin klasörünün içerisine bir web.config oluşturuluyor ve şu şekilde yapılandırılması sağlanıyor.

```
<authorization>
      <allow roles="admin"/>
      <deny users="*"/>
</authorization>
```

  Buradaki ayrıntı kısaca; sadece admin rolü olarak sisteme bağlananlar bu klasörün içerisindeki sayfalara erişebilsin (allow parametresi) ve başka rollerden gelen kullanıcılar buradaki sayfalara erişmesin (deny parametresi).
- Daha sonraki adım ise admin rolü için hangi sayfaların buradaki klasör içersine atılacağının tespit edilmesi ve bu rollere göre sayfaların düzenlenmesi işlemidir. Her bir role göre sayfalar düzenlenir ve ilgili klasörler içersine atılır.
- Kullanıcı girişi kod bloğu: Aşağıda kullanıcı girişi için yapılandırılmış kod bloğu listelenmektedir. Veritabanı bağlantıları ile birlikte sorgulama betiği çalıştırılır ve eğer sistemde böyle bir kayıt varsa kullanıcı rolü geriye döndürülerek ilgili klasörüne

yönlendirilir. Aksi durumda ise uyarılar vererek sisteme yetki vermez, girişi sağlanmaz.

```
SqlConnection Connection = new
SqlConnection(ConfigurationManager.AppSettings["Connection"].ToString());
SqlCommand Command = new SqlCommand();
Command.CommandText = "UserCheck";
Command.Connection = Connection;
Command.CommandType = CommandType.StoredProcedure;
      //Parametre tanımlamaları yapılıyor.
Command.Parameters.AddWithValue("@ComingUserID", txtUserID.Text);
Command.Parameters.AddWithValue("@Pass", Pasword);
try
{   Connection.Open();
    SqlDataReader Reader = Command.ExecuteReader();
    Reader.Read();
    if (Reader["Result"].ToString() == "0")
    {   //Başarısız giriş sonucunda kullanıcıya mesaj veriliyor
        Reader.Close();
        Connection.Close();
        lblStatus.Text = "Unknown User or Password";
    }
    else
    {   //Kimlik doğrulaması ile birlikte Session tanımlamaları yapılarak
        //ilgili klasöre giriş sağlanıyor.
        Session.Timeout = 20;
        Session["UserID"] = txtUserID.Text;
        Session["IDUSER"] = Reader["IDUSER"].ToString();
        Session["UserType"] = Reader["UserType"].ToString();
        UserLoginType = Reader["UserType"].ToString();
        Reader.Close();
        Connection.Close();
        if (UserLoginType == "ADMIN")
            SystemLogin("admin");
        else if (UserLoginType == "TEACHER")
            SystemLogin("teacher");
        else if (UserLoginType == "STUDENT")
            SystemLogin("student");
} }
catch (Exception ex)
```

```
 {    //Hata oluşması durumunda kullanıcıya mesaj gönderiliyor.
     lblStatus.Text = "Error Occured";
}
```

Yukarda belirlenen kod bloğu, sisteme giriş penceresinde bulunan sisteme giriş düğmesi ile ilişkilendirilmektedir. Çalışan kod eğer kimlik doğrulaması doğru ise kullanıcıyı, yetki sahibi olduğu bölgeye yönlendirir. Yönlendirme kod bloğu ise aşağıda belirtilmektedir.

```
void SystemLogin(string klasor)
{
      FormsAuthenticationTicket ticket = new FormsAuthenticationTicket(1,
      txtUserID.Text, DateTime.Now, DateTime.Now.AddMinutes(30), false,
      klasor, FormsAuthentication.FormsCookiePath);
      string encTicket = FormsAuthentication.Encrypt(ticket);
      HttpCookie cookie = new
      HttpCookie(FormsAuthentication.FormsCookieName, encTicket);
      if (ticket.IsPersistent) cookie.Expires = ticket.Expiration;
      Response.Cookies.Add(cookie);
      string returnUrl =  klasor + "/Default.aspx";
      if (returnUrl == null) returnUrl = "Default.aspx";
      Response.Redirect(returnUrl);
}
```

3.4.3. Kullanıcı Kişiselleştirme

Web Tabanlı Uzaktan Eğitim Sistemi'ne farklı kullanıcı tiplerinde giriş yapıldığında; derslerim, sınavlarım, notlarım gibi kişiye özel bilgiler her formun açılışında o kişinin bilgi ve yetkilerine göre göre şekillenmesi gerekir. Bunun için formlar arası kullanıcı bilgilerinin bellekte saklanması ve uygulama kapatılıncaya kadar devam etmesi için tasarlaran WTUES'inde Session metodu kullanılmıştır.Session bilgileri kullanıcı oturumunu kapatana kadar sistem belleğinde saklanmaktadır. Aşağıda gösterilen kod bloğunda kullanıcı bilgileri çağrılarak session tanımlamaları yapılmıştır.

```
Session.Timeout = 20;
Session["IDUSER"] = Reader["IDUSER"].ToString();
Session["UserType"] = Reader["UserType"].ToString();
```

```
UserLoginType = Reader["UserType"].ToString();
```

Bazı durumlarda kullanıcı uzun süre sistem üzerinde işlem yapmadığı zaman timeout işlemi gerçekleştirilir ve kullanıcının session tanımlamaları yok edilir. Fakat kullanıcı bu durumun farkına varmaz ve işlem yapmak ister. Bu durumda hem güvenliği güçlendirmek hem de oluşabilecek hataların önüne geçmek üzere, formların açılış kısımlarına aşağıdaki kod bloğu uygulanmıştır.

```
try
{
      If(Session[“IDUSER”].ToString().Length > 0)
            IDUSER = Session[“IDUSER”].ToString();
      Else
            Response.Redirect(“~/Default.aspx”);
}
catch
{  Response.Redirect(“~/Default.aspx”); }
```

3.4.4. Kimlik Denetiminde Şifreleme

Tasarlanan WTUES üzerinde MD5 algoritması kullanılarak şifrelenme yapılmıştır. Kullanıcı şifreleri MD5 formatına dönüştürülerek veritabanındaki alanında saklanmaktadır. Şifrelenmiş bilgi geriye döndürülememekte ve sistem yöneticisi tarafından dahi bilinememektedir. Bundan dolayı kullanıcının sisteme girişi esnasında, kullanıcı şifresinin gerçek olup olmadığı kontrol edilirken, girmiş olduğu şifre MD5 formatına çevrilerek, veritabanında saklanan bilgi ile kontrol edilmektedir. Eğer eşleşiyorsa girilen şifre doğru bir şifre olarak kabul edilmektedir. Aşağıda belirtilen kod bloğu üzerinde MD5 kullanıcı şifre bilgisinin MD5 formatına dönüştürülmesi gösterilmektedir. Dönüştürülen veri bir değişkene aktarılarak, kullanıcı adı ile birlikte ilgili veritabanı sistemine sorgulanmak üzere, parametre şeklinde gönderilir.

```
byte[] Veri = Encoding.UTF8.GetBytes(txtPassword.Text);
MD5 MD5Nesne = new MD5CryptoServiceProvider();
byte[] MD5Sonuc = MD5Nesne.ComputeHash(Veri);
string PassCode = Convert.ToBase64String(MD5Sonuc);
```

Veritabanı üzerinde kullanıcı tablosu üzerinde veri sorgulayarak kullanıcı bilgilerini kontrol eden Stored Procedure kod bloğu aşağıda gösterilmektedir. Bu işlemde kullanıcı tablosu sorgulanıyor, eğer bilgiler doğru ise 1 değeri, yanlış ise 0 değeri geriye döndürülmektedir.

```
CREATE Procedure [dbo].[UserCheck]
      @KullaniciID nvarchar(50),
      @Password nvarchar(50)
AS
BEGIN
      Declare @IDUSER bigint
      Select @IDUSER=IDUSER from KULLANICILAR
      Where KullaniciID = @ KullaniciID AND Password = @Password
      If @@rowcount > 0
            Select '1' as Result,@IDUSER as IDUSER
      Else
            Select '0' AS Result
END
```

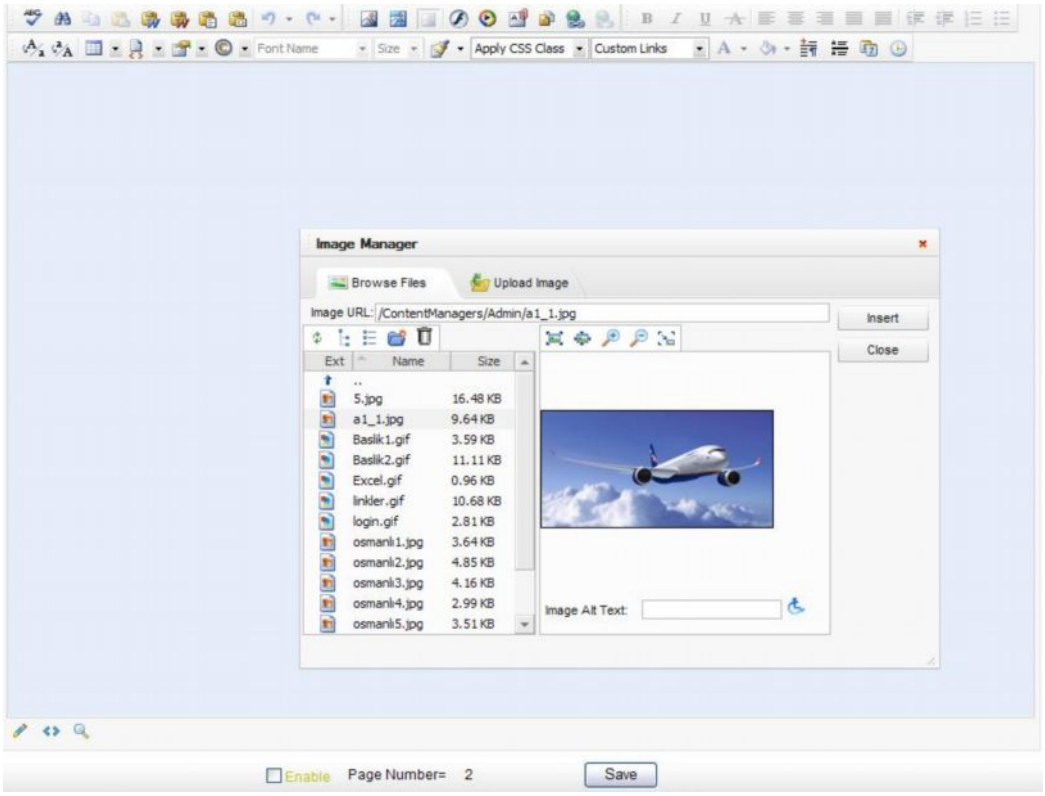
3.4.5. İçeriklerin Saklanması ve Gösterimi

WTUES üzerinde üzerinde içerik hazırlanmasına yardımcı olacak bir araç tasarlanmıştır. Bu aracın amacı; eğitmenlerin tek bir noktadan ortak formatta içeriklerini kendileri hazırlayarak, belirli kontrollerden sonra yayınlayabilmesidir. İçeriklerin kontrolü, derslerden sorumlu koordinatörler tarafından yapılmakta ve incelemenin ardından içeriğin yayınlanmasını sağlamaktadırlar. İçeriğin kontrolünde görülen herhangi bir aksaklıkta, içerik tekrar eğitmene yönlendirilerek düzenleme yapması sağlanmaktadır. Kontrolden başarıyla geçen içerikler, ilgili dersi seçen öğrenciler tarafından görüntülenebilmektedir.

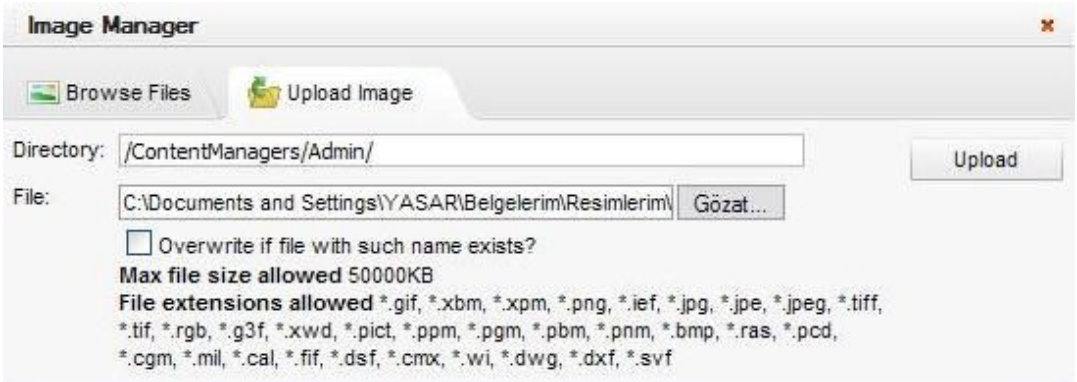
Resim 3.14 üzerinde basit içerik hazırlama editörü görüntülenmektedir. İçerik hazırlama aracında bilgi güvenliği en üst seviyede tutulmaya çalışılmıştır. Bu amaçla yapılan çalışmalar şu şekildedir:

- İçerik hazırlarken her bir eğitmen için, kendi yardımcı dosyalarını saklayabilecekleri klasörler oluşturulmuştur. Bu dosyalar kullanılarak, görsel ve işitsel bakımdan içerikler zenginleştirilebilmektedir. Bu dosyalara sadece uygulama ulaşabilmekte ve klasörün sahibi eğitmen tarafından üzerinde değişiklikler yapılabilmektedir.

- Dosya upload işleminde, sadece belirli formatlardan dosyalar kabul edilmektedir. Bunların dışındaki dosyaların aktarılması mümkün değildir. Ayrıca her bir dosya için maksimum dosya boyutu sabit tutulmuştur. Bu değerin üzerindeki dosyaların aktarımı yine mümkün değildir. Bunun yanında eğitmenin aktaracağı dosya adedinde herhangi bir kısıtlama getirilmemiştir. Resim 3.15 üzerinde, eğitmen tarafından dosya upload işlemi gerçekleştiriliyor.

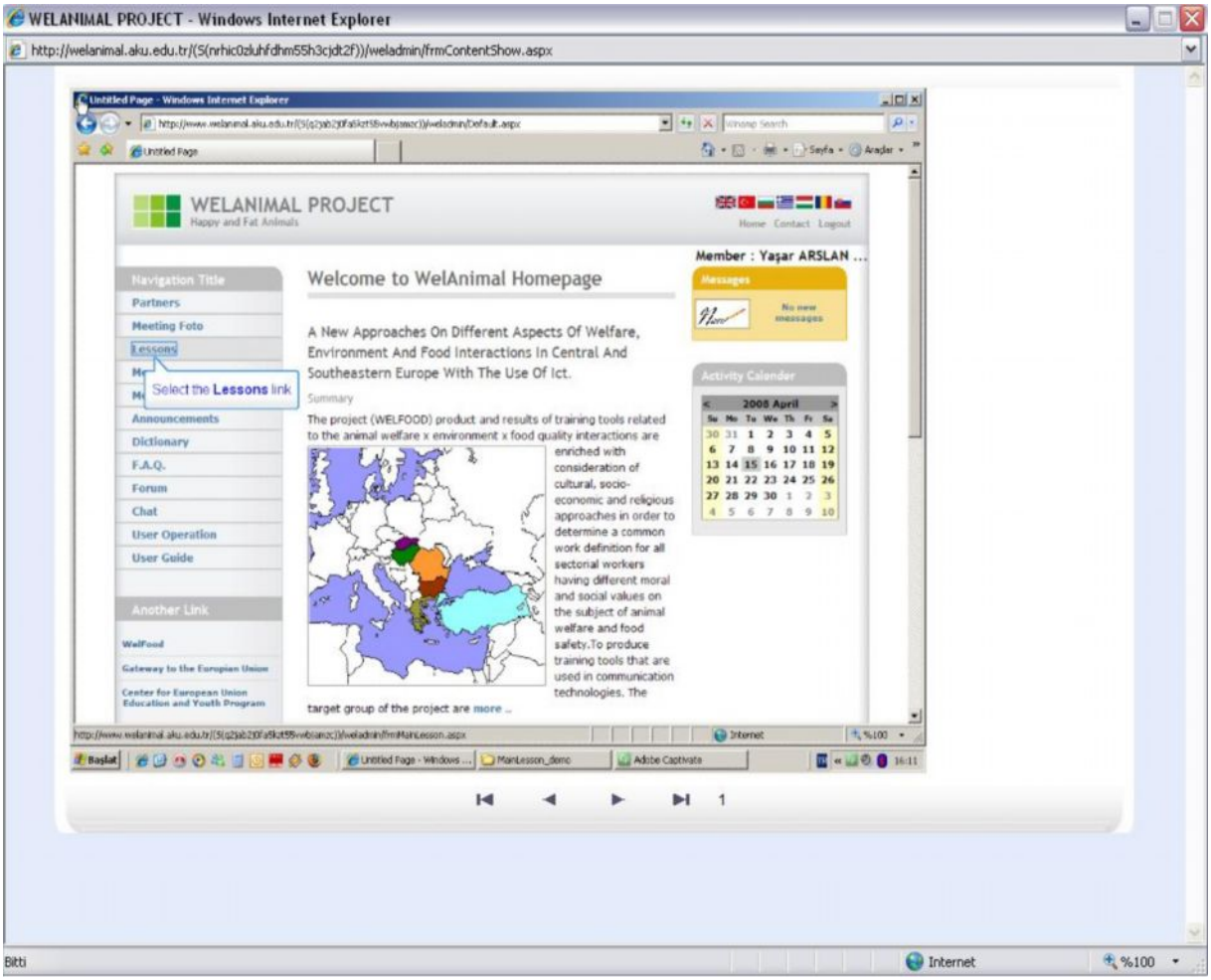


Resim 3.14 İçerik hazırlama editörü (RAD Web Editor)



Resim 3.15 Dosya upload işlemi ve kısıtlamaları (RAD Web Editor)

- İçerik hazırlama esnasında editör aracılığı ile resim, ses, video gibi yardımcı dosyalar istenildiği gibi tasarlanabilir. Buradaki önemli husus, tüm tasarım şekli, arka planda bir html kodunu barındırmaktadır. Html kodunun olmasındaki amaç ise öğrenci bu içeriği incelerken, eğitmenin hazırlamış olduğu tasarımın aynısının öğrencide de bulunmasıdır. Öğrencin içeriği inceleme esnasında üzerinde herhangi bir değişiklik yapmasına yetkisi yoktur. Öğrenci sadece içeriği görüntüler. İçeriğin tam anlamıyla bozulmadan öğrenciye gösterilmesini alt kısımda çalışan html kodları sağlamaktadır ve html kodları içeriğin hazırlanması esnasında veritabanında güvenli bir şekilde saklanır. Dikkat edilmesi gereken nokta: İçerik html kodlarının veritabanında, fakat yardımcı içerik dosyalarının eğitmenlerin klasörlerinde saklanıyor olmasıdır. Böylelikle öğrenciler içerikleri tamamen elde edemezler, ancak web tarayıcısının izin verdiği ölçülerde veya kullanacakları özel birtakım programlarla sadece tarayıcıya yansıyan resim, video gibi bazı dosyaları kendi bilgisayarlarına indirebilirler. Özel hazırlanmış animasyonlara yine erişimleri mümkün değildir, sadece sistem vasıtasıyla izleyebilirler. Burada yapılan çalışma ile, hazırlanmış içeriklerin izinsizce başka kimselere dağıtılması engellenmiştir. Çünkü ders içeriklerinin hazırlanması özenli bir çalışma gerektirir ve hazırlanan ders içeriklerinin izinsiz olarak başkaları tarafından ele geçirilmesinin önüne geçilmelidir. İçeriklerin korunmasından, uzaktan eğitim sistemi sorumludur. Resim 3.16 üzerinde, tasarlanan Uzaktan Eğitim Sistemi web uygulamasının çalışma yapısını anlatan bir içeriğin, öğrenci tarafından takibi görülmektedir.



Resim 3.16 Öğrenci içerik takibi bölümü

3.4.6. Sistem Hata Denetimleri

Gerek yazılım kodlarında gerekse veritabanı Stored Procedure yapıları içerisinde oluşabilecek hatalar için çok sayıda hata denetimleri kullanılmıştır. Hem yazılım hemde veritabanı üzerinde hata denetimleri try-catch metodu ile sağlanmaktadır. Böyle bir yapıda programcı hata oluşması durumuna göre kodlamada try-catch bloklarını kullanır. Aşağıdaki kod, bir güncelleme işleminde yapılan hata denetiminin Stored, Procedure yapısı içerisinde kullanılmasını göstermektedir. Oluşan durum program tarafından değerlendirilir ve kullanıcıya yansıtılır.

```
BEGIN TRY
      Update tblDonemKapatma Set Durum=0 Where Optk=@Optk AND Durum=1
```

```
      Set @IslemSonuc=1
END TRY
BEGIN CATCH
      Set @IslemSonuc=0
END TRY
--Sonuç Döndürülüyor
Select @IslemSonuc
```

Veritabanı hata denetimlerinde diğer bir önemli husus ise işlemlerin yarıda kalması durumudur. Özellikle geri dönüşümü olmayan kritik işlemlerde kullanılması sistem içerisindeki veri bütünlüğünü korumaktadır. Bu özellik transaction işlemidir. Bu özellik sayesinde eğer işlem esnasında bir hata ile karşılaşılmışsa yapılan işlemler geriye alınarak veriler eski haline getirilir. Geri alma işlemine ise rollback adı verilir. Aşağıdaki kod bloğu üzerinde, tasarlanan WELANIMAL projesi üzerinde kullanımı gösterilmektedir.

```
BEGIN TRANSACTION
   DELETE FROM tblDersListesi Where Yil=@YeniYil AND BolumKodu=@BolumKodu
   Exec [BolumDersAktar]
   IF (@@error<>0)
   BEGIN
      ROLLBACK  --Hata varsa işlemi geri al
      Set @IslemSonuc=0
   END
   ELSE
      Set @IslemSonuc=0
COMMIT
SELECT @IslemSonuc
```

3.4.7. Güvenlik için Ek Modüllerin Oluşturulması

Bir web uygulamasında bilgi güvenliğini sağlamanın gerekli görüldüğü noktalardan birisi de, uygulama içerisine kontrol mekanizmalarının oluşturulmasıdır. Tasarlanan Uzaktan Eğitim Sistemi üzerinde bu amaçla birçok kontrol mekanizması geliştirilmiş ve uygulama içerisinde kullanılmaya başlanmıştır. Bu mekanizmalardan bazıları ve görevleri şu şekildedir:

Kullanıcı giriş kayıtlarının tutulması: Sisteme üye olan veya olmayan her bireyin giriş yapması esnasında alınan kayıtlardır. Kullanıcının giriş ekranından her seferinde yaptığı işlem, birtakım bilgileri ile birlikte kayıt altına alınır. Bu kayıtlar; işlem zamanı, girdiği kullanıcı adı, hangi IP numarasıyla bağlandığı ve giriş işleminin başarılı olup olmadığı durumlardır. Eğer kullanıcı 3 defa sisteme girmeyi denemiş ve başarılı olamamışsa bu işlem farklı bir alanda tutularak sistem yöneticisini uyarma amaçlı kullanılır. Buradaki amaç, sisteme izinsiz girişlerin tespit edilmesi ve gerektiğinde IP adresinin güvenlik duvarından engellenmesidir. Resim 3.17 üzerinde sistem giriş kayıtlarının tutulması ve sisteme girmek için rastgele kullanıcı adları ile giriş yapmaya çalışan bir IP numarasının tespit edilmesi görülmektedir.

Yeni üye kayıtlarının tutulması: Sisteme yeni üye kullanıcıların takibi için geliştirilmiş bir mekanizmadır. Sisteme yeni kayıt yaptıran üyenin şifresi e-posta adresine gönderilmektedir. Ancak sistemin güvenliğini tehlikeye atmak için sürekli farklı kullanıcı adları ile kayıt yaptırmak isteyenler olabilir. Bu durumun ortaya çıkarılması amacıyla yeni kayıt üyelerinin düzenli kayıtları ve sisteme girişleri kontrol edilir. Ayrıca her bir yeni kayıtta sistem yöneticisine, yeni kayıtlı üyenin bilgilerini içeren bir e-posta gönderilmektedir.

Önemli yapıların kayıtlarının tutulması: Sistem içerisinde dönem kapatma, dönem güncelleme, yeni kayıt aktarımları gibi bazı özel yapılar bulunmaktadır. Bu yapıları yapabilme yetkileri sistem yöneticisinden ayrı olarak koordinatörlere verilmiştir. Bu işlemlerin hangi koordinatör tarafından ne zaman yapıldığı ve hangi işlemleri içerdiği kayıt altına alınması sistem yöneticisinin işini kolaylaştıran bir yapıdır. Hazırlanan bu mekanizma ile bu işlemlerin kontrolü, kolayca takip edilebilir hale gelmiştir.

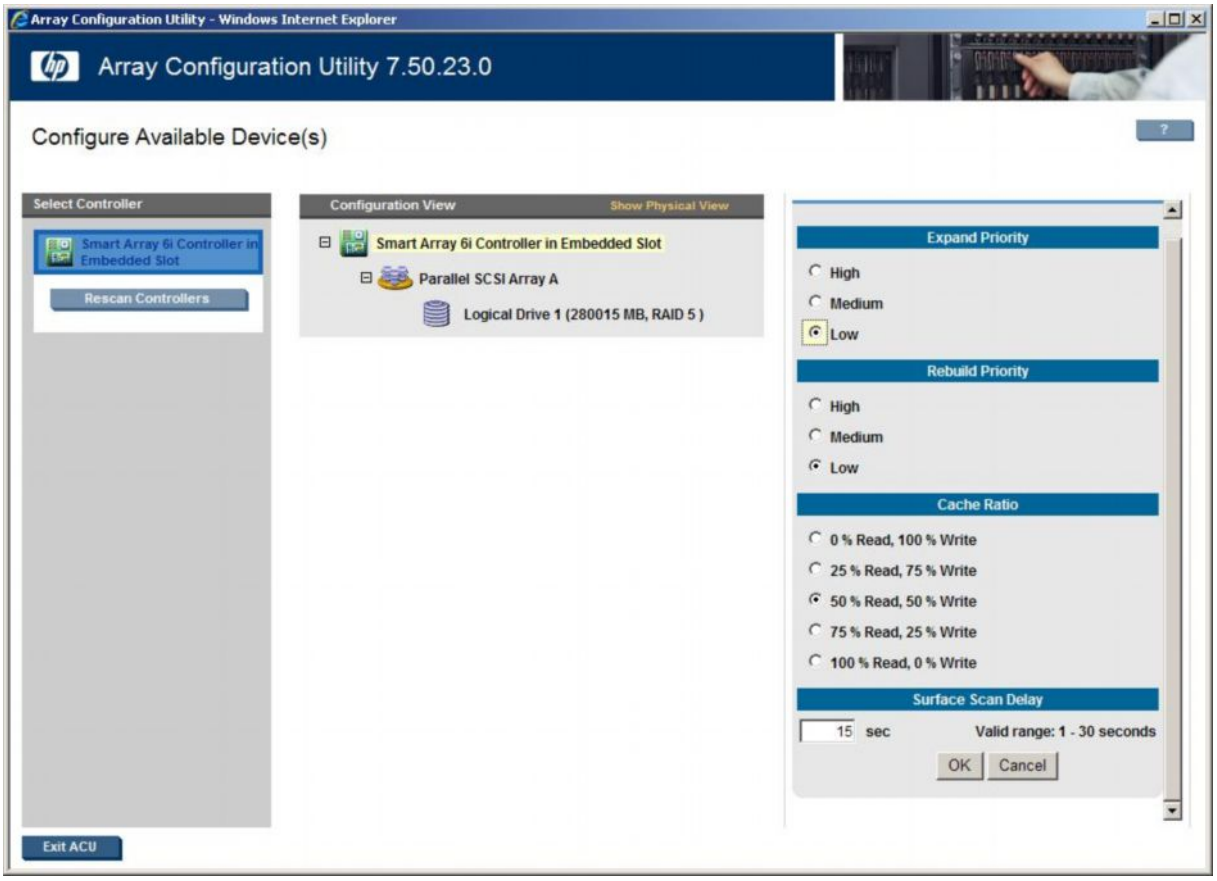
Resim 3.17 Sistem giriş kayıtlarını inceleme arayüzü

3.5. Bilginin Saklanması

3.5.1. Bilgi Yedekleme ve Geri Dönüşüm

WELANIMAL projesinde kullanılmak üzere harici ve dâhili yedekleme üniteleri devreye alınmıştır. Anlık tüm değişiklikler, dâhili disk depolama birimine, daha uzun sürekli periyodik yedekler ise harici teyp depolama birimine aktarılmaktadır. Anlık verilerin yedeklemeleri aralıksız olarak disk depolama birimi olarak kullanılan HP Storage Works ünitesine yapılmaktadır. Günlük, haftalık ve aylık periyodik yedekler ise teyp depolama ünitesi olarak kullanılan HP Ultrium Autoloader teyp depolama ünitesine yapılmaktadır.

Resim 3.18 üzerinde HP StorageWorks disk depolama ünitesini yöneten yazılımın arayüzü görülmektedir. Burada yeni bir disk alanı oluşturularak sunuculardan birisi için kullanıma açılacaktır.



Resim 3.18 HP StorageWorks disk depolama ünitesi yazılım arayüzü

4. WTUES'nin TEST EDİLMESİ

4.1. Performans Testi

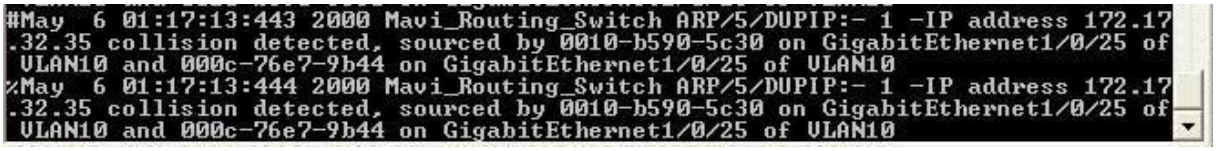
Tasarlanan WTUES'nin sistem ve yazılım performans testi yapılarak test sırasında tespit edilen yavaşlıklar giderilmiştir. Performans testi; Afyon Kocatepe Üniversitesi ana merkez yerleşkesi, ilçe yerleşkeleri, üniversite dışı noktalar ve hatta ülke dışından kullanıcılar tarafından talimatlar verilerek yapılmıştır. Merkez yerleşke içerisinde 60 kişilik bilgisayar laboratuarında öğrencilerin sisteme aynı anda giriş yapmaları ve kendi hesapları üzerinde sürekli dolaşarak içerik takibi yapmaları istenmiştir. Aynı işlem diğer bir yerleşke üzerinde de denenmiştir. Sisteme giriş yapıldıktan sonra açılan bazı sayfalarda yavaşlıklar tespit edilmiş ve bu yavaşlıklar yazılım tarafından düzenlenerek giderilmiştir.

Diğer yandan Afyon Kocatepe Üniversitesi dışarısından bağlantı yapmak isteyen kullanıcıların bazı sayfaları görememeleri tespit edilmiş ve bunun sebebinin de IPS cihazı tarafından bazı sayfalara güvenlikten dolayı engelleme yapıldığı saptanmıştır. Bu engellemenin sebebi, bazı sayfaların farklı teknolojiler ile tasarlandığından ve güvenlik açıkları içerebileceğinden dolayı IPS tarafından düşük seviyeli güvenlik açığı olarak tespit edilmesidir. Engellenen bu sayfalar yeniden düzenlenmiş ve sorun giderilmiştir.

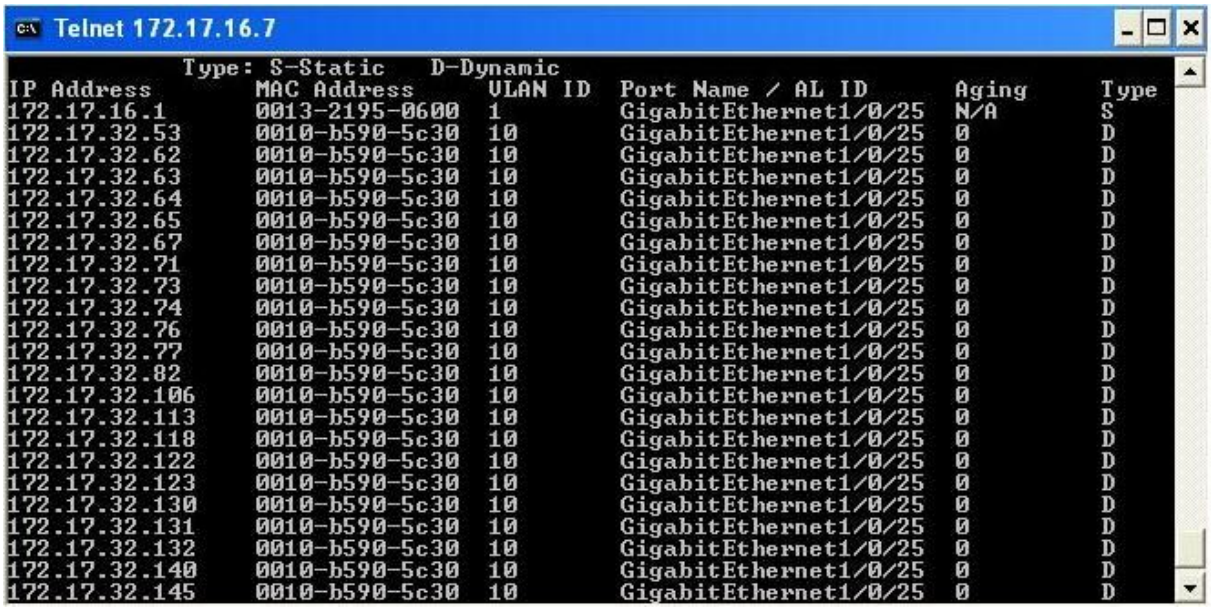
4.2. Ağ ve Güvenlik Taramaları

Ağ trafiği, omurga switch ve diğer uç noktalardaki ağ donanımları üzerinde yapılan çalışmalarla test edilmiştir. Ağ donanım cihazları haberleşme işlemlerini TCP/IP protokolünün fiziksel katmanında devam ettirmektedirler. Bu fiziksel katman, ağa bağlı cihazların fiziksel adreslerine göre çalışmaktadır. Fiziksel adres donanımların ağ kartlarında bulunmakta ve MAC adresi olarak adlandırılmaktadırlar. Ağ donanımı üzerinde testler, fiziksel katman değerlendirilerek yapılmıştır. Testler sırasında laboratuar içerisinde bazı bilgisayarların sistemin işleyişini büyük oranda kestiği görülmüştür, bunun en büyük nedeni ise anti virüs yazılımını güncellemeyen bir bilgisayarın ağ üzerinde yaptığı virüs ataklarıdır. Bu virüs bilgisayara ait ağ geçidi cihazının MAC adresini kendine kopyalamakta ve böylece tüm trafiğin kesilmesine neden olmaktadır. Hatta ağ üzerindeki bilgisayarların MAC

adreslerini de kendine tanımlamaktadır. Böylece ağ üzerindeki paket trafiğini tamamen durdurmaktadır. Resim 4.1 üzerinde omurga switch üzerinde ağ trafiği incelenirken ortaya çıkan uyarılar görülmektedir. Resim 4.2 üzerinde ise omurga üzerinde sisteme bağlanmış IP ve bunlara ait MAC adresleri listelenmektedir. Virüslü bilgisayar diğer donanımlara ait MAC adresini kendi bağlantısına kopyalamış ve ağ trafiğini bozmuştur. Böylece ağ donanım cihazları MAC adreslerine göre çalıştıklarından dolayı, bu adresler sistem içerisindeki ağ trafiğini şaşırtmıştır.



Resim 4.1 Switch üzerinde 0010-b590-5c30 numaralı MAC adresi birden fazla cihaz üzerinde göründüğünden dolayı, sistem sürekli uyarılar vermektedir.



Resim 4.2 Switch üzerinde 0010-b590-5c30 numaralı MAC adresi birden fazla cihaz üzerinde görülmektedir.

Ağ üzerinde test işlemi olarak yapılması gereken bir diğer nokta ise ağ paketlerinin dinlenmesidir. Buna sniffer adı verilir. Ağ trafiğindeki tüm paketlerin dinlenmesi donanımsal olarak hub adı verilen küçük cihazlarla mümkündür, çünkü bu cihaz, üzerindeki bir porta gelen tüm veriyi diğer portlara da göndermektedir. Uygun geçiş noktalarına bu cihaz konarak

dinleme yapılabilir ancak bu eski bir metottur. Bunun yerine switch üzerinde port-mirroring adı verilen bir metot kullanılır. Bu metot ile ağ üzerinde, ağ geçidi olarak ayarlanmış bir port, cihaz üzerindeki boş bir porta eş zamanlı olarak yönlendirilmiş olur. Böylelikle aynı veriler aynı anda iki porta da aktarılmış olur. Boş olan porta bir bilgisayar takılarak ağ trafiği dinlemeye alınabilir. Bu amaçla omurga switch üzerinde port-mirroring ayarı şu şekilde yapılmıştır.

- `Mirroring-group 1 inbound GigabitEthernet6/0/6 mirrored-to GigabitEthernet6/0/12`
- `Mirroring-group 1 outbound GigabitEthernet6/0/6 mirrored-to GigabitEthernet6/0/12`

Ağ geçidi olarak tanımlanmış 6/0/6 portundaki tüm veriler giriş ve çıkış olarak bu iki komutla 6/0/12 portuna eş zamanlı olarak yönlendirilmiştir.

Firewall sunucusu üzerinden geçen tüm ağ paketleri log olarak tutulmakta ve belirli bir sure saklanmaktadır. Sistem test aşamasında ağ üzerinde çok sayıda bilgisayar ile işlem yapılmış ve deneme amaçlı virüslü bilgisayarlar sisteme bağlanmıştır. Firewall sunucusunu zorlamak amaçlı yapılan bu test sonucunda, firewall log dosyaları dolarak diskler üzerinde yer kalmamıştır. Sistem kısa bir sure tıkanarak cevap veremez hale gelmiştir. Bu sorunu aşmak için, firewall sunucusu üzerindeki disk kapasiteleri artırılarak log dosyalarının disk depolama ünitesine yazılması sağlanmıştır. Bu ayarlardan sonra, log dosyalarının dolması durumunda sistem tıkanmamıştır.

Veritabanı sunucusu üzerine, çok sayıda SQL sorguları yoğun bir şekilde gönderilmiştir. Veritabanı sisteminin testi için yapılan bu çalışmada, bazı durumlarda yavaşlıklar hissedilmiş ve sunucu hafızası artırılarak bu sorun çözülmüştür. Benzer şekilde web sunucusu üzerindeki sistem hafızası da artırılmıştır.

Yapılan düzenlemelerden sonra sistem log dosyaları ve sistem performansı günlük olarak incelenmiş ve herhangi bir soruna rastlanmamıştır.

5.TARTIŞMA ve SONUÇ

Eğitim ve öğretim alanında önemli bir noktaya gelen WTUES, teknolojinin gelişmesi ile büyük değişimlerden geçmektedir. Web tabanlı yazılım mimarisi üzerine kurulan sistem, farklı web araçlarını ve detaylı form arayüzlerini içerisinde barındırmaktadır. Ayrıca WTUES'nin çalışacağı donanım ve ağ altyapısı, sistemin tüm özelliklerini kullanabilecek, gelişmiş bir yapıda tasarlanmakta ve yapılandırılmaktadır. Ancak hazırlanan bu sistemle birlikte dikkat edilmesi gereken husus, sistemin bilgi güvenliğinin sağlanmasıdır. WTUES'nde bilgi güvenliği, ağ, sunucu ve yazılım aşamalarında dikkatle ele alınarak, gelebilecek saldırı veya güvenlik tehditlerine karşı, sistemin sağlıklı bir yapıya kavuşturulması sağlanmalıdır.

Bu tez çalışması ile birlikte, yeni tasarlanan WTUES üzerinde tüm güvenlik çalışmaları farklı metodlar kullanılarak denenmiş ve başarılı metotlar sistem üzerine entegre edilmiştir. Ağ, sistem ve yazılım olmak üzere 3 farklı boyutta ele alınan bu çalışmalar titizlikle yapılmış, güvenlik metotları uygulanırken çok sayıda sistem yeniden kurulup yapılandırılmıştır.

WELANIMAL projesinin analiz aşamasında, tüm güvenlik önlemleri düşünülmüş ve yazılıma başlanmadan once güvenlik çalışmalarına başlanmıştır. Böylelikle sistem altyapısının ihtiyacı olan donanımsal cihazların da alımına başlanmıştır. Sunucu, ağ ve yedekleme cihazlarının alınması ile birlikte, ağ üzerinde iyileştirme çalışmalarına başlanmıştır. WELANIMAL projesi ile internet hızı artırımı gerekli görülmüş ve Metro Ethernet teknolojisi ile gerekli hıza ulaşılmıştır.

Tasarlanan WTUES üzerinde güvenlik çalışmaları test edilmiş, problem yaşanan bölümler tekrar gözden geçirilerek, uygulama bugünkü haline getirilmiştir. Mayıs 2008 tarihi itibari ile yayın hayatına başlayan WELANIMAL WTUES, Kasım 2008 tarihine kadar çeşitli güncellemelerden geçmiştir. Güncellemelerin büyük bir kısmı yazılım ve sistem yapısında tespit edilen güvenlik eksikliklerin giderilmesi şeklinde olmuştur. Dünya üzerinde farklı bölgelere hizmet verebilecek şekilde tasarlanan sistem http://www.welanimal.com adresinden farklı dillerde kullanılabilir hale getirilmiştir.

Sistemin kullanıma açılması ile birlikte hergün yeni kullanıcıların sisteme üye oldukları ve etkileşimli eğitim bölümlerini kullandıkları tespit edilmiştir. Kullanıcı ile ilgili bilgiler düzenli olarak sistem tarafından sistem yöneticisine elektronik posta ile bildirilmektedir. Sistemin yayına başlamasından itibaren yaklaşık 8 aylık bir sureçte ciddi güvenlik sorunu yaşanmamış ancak sistem tasarımcıları tarafından tespit edilen bazı güvenlik önlemleri eklenmiştir.

Tasarlanan WTUES üzerinde etkileşimli eğitim kullanımında bazı sıkıntılar olmuştur. Bu sıkıntılar mesai saatlerinin yoğun olduğu zamanlarda internet hatlarında yaşanan yavaşlıktan kaynaklanmaktadır. Hat üzerinde oluşan yoğun ağ trafiği WTUES'nin erişim hızını etkilemektedir. Bunun için yapılması gereken, üniversite internet hattının dışında ayrı bir hat kiralanarak Uzaktan Eğitim hizmetinin bu hat aracılığı ile uygulanmasıdır.

6.KAYNAKLAR

Alkan, Cevat., 1981, "Açık üniversite uzaktan eğitim sistemlerinin karşılaştırmalı olarak incelenmesi", Ankara Üniversitesi, Ankara.

Aslantürk, O., 2002, "Bir Web tabanlı uzaktan eğitim sisteminin tasarlanması ve Gerçekleştirilmesi", Hacettepe Üniversitesi, Ankara.

Bates, A.W., 1995, "Technology, Open Learning and Distance Education", Routledge, London,

2000, "Managing Technological Change", Jossey-Boss Inc, San Francisco.

Bonk, Curtis J., 2000, "Online training in an online world".

Carswell, A.D. ve Venkatesh, V., 2002, "Learner outcomes in an asynchronous distance education environment", International Journal of Human-Computer Studies, 56(5), 475-494.

Daniel, J.S., 1996, "Mega Universities and Knowledge Media", Kogan Page Ltd., London.

Dennis M.S, Keith R.M, Louis D, 2007, "Security and interconnection of medical devices to healthcare networks", Department of Veterans Affairs, Veterans Health Administration, USA.

Guillaume J., Emmanuel L., Patrick S., 2007, "Design, implementation and evaluation of a QoS-aware transport protocol", CNRS/LAAS – ENSICA, France.

Ido D, 2007, "Topologies and IDS", How to Cheat at Securing Your Network, Pages 281-315.

McLendon, E. 1999, "Rethinking Academic Management Practices: A Case Meeting New Challenges in Delivery", Journal of Distance Learning Administrations 2, 1-12.

Minh H., Prasant M., 2007, "Metropolitan Ethernet Network: A move from LAN to MAN", Computer Science Department, University of California at Davis, CA, United States.

Mitchell, E.F., 1977, "Cooperative Vocational Education", Allyn and Bacon , Inc., Boston.

Neville, A.M., 1977, "Properties of Concrete", Pitman Publishing, London.

Özen, Ü. ve Kahraman, S., 2001, "Web tabanlı uzaktan eğitimde sistem tasarımı", Akdeniz İ.İ.B.F. Dergisi, 2, 81-102.

Yiğit, Y., Özden, M. Y., 2007, "Web Tabanlı Eğitim Materyali İçersisinde İnternet Üzerinden Görüntü Aktarımı".

İnternet Kaynakları **Erişim Tarihi**

1- http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf 12.09.2008

2- http://www.tippingpoint.com/products_ips.html 17.09.2008

3- http://belgeler.org/howto/iptables-usage_concepts.html 03.10.2008

4- http:// www.msakademik.net/makaleler_detay.aspx?id=525 11.10.2008

5- http://www.msakademik.net/makaleler.aspx?grup=GUV 12.10.2008

6- http://www.signum.com.tr/ortakatman/testperformans.html 01.11.2008

7- http://aemc.jpl.nasa.gov/activities/bio_regen.cfm 18.11.2008

8- http://www.scribd.com/doc/330129/VPN-Routing-and-Forwarding 25.11.2008

ÖZGEÇMİŞ

Adı Soyadı	Yaşar ARSLAN
Doğum Yeri	Afyon
Doğum Tarihi	01/03/1977
Medeni Hali	Evli
Yabancı Dili	İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise	Afyon Lisesi Lisesi 1995
Lisans	Doğu Akdeniz Üniversitesi 2002

Çalıştığı Kurum/Kurumlar ve Yıl aralığı

Afyon Kocatepe Ünv.	2002 – 2009

Yayınları

Y. Arslan, Y. Boy, M. Doğan, "E-Öğrenme Sisteminin Hizmet İçi Eğitimde Kullanılması ve E-Öğrenme Sitelerinin Kullanım Kolaylığı Açısından İncelenmesi", Akademik Bilişim 2007 Dumlupınar Üniversitesi, 31 Ocak - 2 Şubat 2007, Kütahya / Türkiye