BİLGİSAYAR VE AĞ GÜVENLİĞİ DERSİNİN FARKINDALIĞININ OLUŞTURULMASI VE DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

Akıb ÇETİN

Danışman
Dr. Öğr. Üyesi Levent ÇELİK

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ
ANABİLİM DALI
Haziran 2018

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BİLGİSAYAR VE AĞ GÜVENLİĞİ DERSİNİN FARKINDALIĞININ OLUŞTURULMASI VE DEĞERLENDİRİLMESİ

Akıb ÇETİN

Danışman
Dr. Öğr. Üyesi Levent ÇELİK

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ ANABİLİM DALI

Haziran 2018

TEZ ONAY SAYFASI

Akıb ÇETİN tarafından hazırlanan "Bilgisayar ve Ağ Güvenliği Dersinin Farkındalığının Oluşturulması ve Değerlendirilmesi" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 19/06/2018 tarihinde aşağıdaki jüri tarafından **oy birliği** ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Dr. Öğr. Üyesi Levent ÇELİK

İmza

Başkan : Dr. Öğr. Üyesi Hüseyin ÇAKIR
Gazi Üniversitesi Gazi Eğitim Fakültesi ……

Üye : Dr. Öğr. Üyesi Ertuğrul ERGÜN
Afyon Kocatepe Üniversitesi Uz. Eğ. MYO ……

Üye : Dr. Öğr. Üyesi Levent ÇELİK
Afyon Kocatepe Üniversitesi Eğitim Fak. ……

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

.....
Prof. Dr. İbrahim EROL
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu Tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

19/06/2018

Akıb ÇETİN

ÖZET

Yüksek Lisans Tezi

BİLGİSAYAR VE AĞ GÜVENLİĞİ DERSİNİN FARKINDALIĞININ OLUŞTURULMASI VE DEĞERLENDİRİLMESİ

Akıb ÇETİN

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü

İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Levent ÇELİK

Çeyrek asır önce bilgisayar ve bilgisayar bileşenlerini kullanan kişi hatta kuruluş sayısı en gelişmiş ülkelerde dahi onlarla ifade edilirken bu oran günümüzde milyarlarca kullanıcı ile ifade edilmektedir. Bilgisayar ve bileşenlerinin günden güne gelişmesi ve bu hızlı gelişime paralel olarak da başta kurumlar olmak üzere kişisel kullanıcılar tarafından hızla kullanımın yaygınlaşması sonucunda kaçınılmaz sonuç olarak bilgisayarlar ve bileşenlerinin güvenliği konusu göz ardı edilemez bir hal almıştır.

Bu nedenlerden dolayı başta üniversite öğrencileri olmak üzere bilgisayar kullanıcılarının bilgisayarların ve bilgisayar ağlarının güvenliklerine dair ilgilerini ve farkındalıklarını artırmak amacıyla üniversite öğrencilerine yönelik Bilgisayar ve ağ güvenliği dersinin konularını kapsayan bu çalışmada, temel bilgisayar ve ağ güvenliği içeriklerine yer verilerek çalışmanın yardımcı kaynak olması amaçlanmıştır. Bu çalışmanın sonunda; uygulama öncesi farkındalıkları ve uygulama sonrası farkındalıklarının değişimlerini ölçmek amacıyla yapılan testler ve değerlendirmeler ile öğrencilerin farkındalık seviyeleri ölçülmüş ve bu çalışmanın etkililiği gözlemlenerek öğrencilerin bilgisayar ve ağ güvenliği konusundaki eksik ve yanlış bilgilere sahip oldukları gözlemlenmiştir.

2018, xii +117 sayfa

Anahtar kelimeler: Bilgisayar ve Ağ Güvenliği Dersi, Eğitim Programı, Farkındalık

ABSTRACT

M.Sc. Thesis

FORMATION AND EVALUATION OF COMPUTER AND NETWORK SECURITY COURSE

Akıb ÇETİN

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technologies Management

Supervisor: Asst. Prof. Levent ÇELİK

While the number of the people and even the instutitions using computer and computer components were expressed with tens even in the most developed countries quarter-century ago, this rate is expressed by billions of users today. The inevitable result is that the security of computers and its components has become unignorable as a result of development of computer and its compenent day by day and its widespread usage by initially institutes and personal users in paralel with this fast development.

For these reasons, this study, which includes the topics of computer and network security course in order to increase the awareness of the security of computer users and computer networks and especially the security of university students, is aimed to be a supplementary resources by providing basic computer and network security contents and at the end of the study, students awareness levels were measured by the tests and the evaluations which were used to understand the changes between the students pre-implementation awareness level and post-implementation awareness level. Consequently, it was concluded that students have incomplete and incorrect knowledge about the computer and network security.

2018, xii +117 pages

Keywords: Computer and Network Security Course, Curriculum, Awareness

TEŞEKKÜR

Tez yazım sürecinde başta düşünce, fikir ve görüşlerini esirgemeyen saygıdeğer hocam Dr. Öğr. Üyesi Levent ÇELİK'e teşekkürlerimi sunarım.

Tez yazım aşamasında değerli katkılarından dolayı Sayın Öğr. Grv. Burak OLUR'a teşekkür ederim.

Tez yazım süresince beni yalnız bırakmayan ve manevi desteklerini esirgemeyen aile bireylerimin tüm fertlerine teşekkürlerimi sunarım.

Bu çalışmanın yazım aşamasının her anında yanımda olan ve destekleri ile teşvik eden Sayın Ayşe DENİZ'e teşekkür ederim.

Akıb ÇETİN

AFYONKARAHİSAR, 2018

İÇİNDEKİLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

Kısaltmalar	
AV	Antivirüs
AIX	Advanced Interactive eXecutive
ARP	Address Resolution Protocol
CARP	Common Address Redundancy Protocol
CCPD	Hücresel Dijital Paket Verisi
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
HTTP	Hypertext Transfer Protocol
IPS	Intrusion Prevention System
IR	Infrared – Kızıl Ötesi
ISP	Internet Service Provider - İnternet Servis Sağlayıcısı
ISS	İnternet Servis Sağlayıcı
L3	Layer 3 (OSI 3. Katman)
L7	Layer 7 (OSI 7. Katman)
LAN	Local Area Network – Yerel Alan Ağı
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MAN	Kentsel Alan Ağları
NAT	Network Address Table
OSI	Open Systems Interconnection
PEAP	Protected Extensible Authentication Protocol
RAS	Remote Access Server
RF	Radyo Frekansı
TCP/IP	Transmission Control Protocol / Internet Protocol
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator.
UTM	Unified Threat Management
VLAN	Virtual Private Network – Sanal Özel Ağ
VPN	Sanal Özel Ağ
WAN	Geniş Alan Ağları
WWAN	Kablosuz Geniş Alan Ağları
WPAN	Kablosuz Kişisel Alan Ağları

RESİMLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Bilgisayarların hayatımıza girdiği 20.yüzyılın ortalarından bugüne kadar geçen 70 yıllık sürede asıl gelişimini, değişimini ve insanlar tarafından kullanımının hızla yaygınlaşmasının sürecini, son çeyrek asır olarak değerlendirebiliriz. Çeyrek asırdır bilgisayar kullanımının arttığını ve insanların bilgisayarlara gösterdikleri ilginin yaygınlaştığını düşünsek de bilgisayarların insanoğlunun hayatına dolaylı olarak girdiği yıllar çok daha öncesidir diyebiliriz.

1980'li yıllarda kişisel bilgisayarların çoğalması bilgisayar ve iletişim teknolojilerindeki gelişmeler, bilgisayar ve ağlarının daha yararlı olmasını sağlanmıştır. Bunun üzerine ağ kavramı gelişmiş ve ihtiyaçlara göre ağ bileşenleri ile uygulamaları geliştirilmiştir. Büyüklüklerine göre ağ kavramları ortaya çıkmış ve daha sonra uygulamalarına geçilmiştir. İlk olarak Yerel Alan Ağları (Local Area Networks- LAN) ortaya çıkmış, daha sonra daha geniş coğrafyadaki bilgisayarların birbirleriyle haberleşme ihtiyaçları geniş alan ağları (Wide Area Networks- WAN) kavramının ve uygulamasının doğmasına neden olmuştur.

Bilgisayarların yaygınlaşmasının asıl nedeni teknolojik gelişmeyle birlikte ergonomik bir hâl almasınındı etkisi yadsınamaz bir gerçektir. Ancak bilgisayarların son çeyrek yüzyılın başlarında kullanıcı sayıları 10 binler ile ifade edilirken tahmin edilemez ve öngörülemez bir hızda yaygınlaşması ve gelişime uğraması sonucu kullanıcı sayıları milyarlar ile ifade edilmeye başlanmıştır.

60'lı yılların başlarında askeri ve istihbari amaç için kullanılan kapalı devre bilgisayar ağı sisteminin(intranet) 80'li yılların başlarına gelindiğinde kapalı devre olmaktan çıkarak belirli protokoller kurallar ile binlerce bilgisayarın bir ağa bağlanması sağlayan sistemlerin yaygınlaşması sonucu kaçınılmaz olmuştur. Giderek hızlı bir şekilde yaygınlaşan internetin hızla yaygınlaşması tabii ki herkesi kabulü olduğu ve olacağı üzere bilgisayar kullanımının bu denli hızlı bir şekilde yaygınlaşmasının baş etkeni olarak interneti kabul edebiliriz.

İnternet ile birlikte yeni bir çağ ortaya çıkmış ve bu ortaya çıkan çağ milenyum çağ olarak adlandırılmıştır. Bu adlandırma öylesine ortaya çıkmamıştır zira adlandırmanın asıl nedeni bilgisayarların ve teknolojinin tahmin edilemez gelişimi ve değişimidir ve kaçınılmaz olarak internet ile birlikte bilgisayar kullanımın hızla yaygınlaşması sonucu ortaya çıkan siber güvenlik hassasiyeti tabii ki her geçen gün artmaya devam ederek artık üzerinde profesyonel manada uzmanlar tarafından durulması gereken bir sonuç olmuştur.

Bilgisayar ve bilgisayarların bağlı oldukları ağların güvenliğinin sağlanması için alınması gereken önlemler için sistematik bir şekilde güvenlik politikası oluşturulmaya başlanarak bilgisayar ve ağ güvenliğinin sağlanması uzmanlar tarafından amaçlanmıştır. Bu çalışmanın hazırlanmasındaki amaç bilgisayar ve ağ güvenliği konusundan kişisel kullanıcıların gerekli bilgi ve dokümanlar ile uygulamalı örneklemeler anlatılarak kullanıcıların temel düzeyde sade ve gerekli bilgiler ile farkındalıklarını artırarak siber güvenlik konusunda bilinçlenmelerini sağlamaktır.

Kablolu ve kablosuz ağlar beraberinde güvenlik sorunlarını da getirmişlerdir. Bilindiği üzere ağlarda iletim ortamı olarak hava kullanılmaktadır. Bu, sinyalin havanın götürebildiği yere kadar gidebilmesi anlamına gelmektedir. Bunun dışında, kablosuz ağların teknolojileri de kablolu ağlara benzer güvenlik özelliklerine sahiptir.

Kullanıcının bulunduğu iş türüne, büyüklüğüne ve taşıdıkları verilerin niteliği ile kullanıcı sayılarına göre farklı güvenlik parametreleri uygulanabilir. Sahip olduğu avantajlarından dolayı, günümüzde ağların kullanımı önemli hale gelmiştir. Bu çalışma; giderek kullanımı ve buna bağlı olarak önemi artan bu teknolojiyi tanıtması, altyapısını, güvenlik yöntemlerini bir arada incelemesi ve örnek bir uygulamayı sunması bakımından, bu konuda araştırma yapmak isteyenlerin başvurabileceği bir kaynak niteliğinde olacaktır.

1.1 Amaç

Bu çalışmanın hazırlanmasındaki amaç başta üniversite öğrencileri olmak üzere Bilgisayar ve Ağ Güvenliği dersi alan tüm diğer öğrencilerin kaynak olarak istifade edebilecekleri çalışma olması amaçlanmıştır. Ve mevcut olan Bilgisayar ve Ağ Güvenliği konularını kapsayan diğer kaynaklara nazaran içerik olarak daha efektif ve doğrudan istedikleri bilgileri içeren ve bu şekilde öğrencilerin derse olan farkındalıkları ile ilgilerin artırmaya yönelik kaynak bir çalışma olmasını sağlamaktır.

2. LİTERATÜR BİLGİLERİ

2.1 Bilgisayar ve Ağ Güvenliği

Bilgisayar ve bilgisayarların bağlı olduğu oldukları ağların dışarından gelebilecek tüm saldırılara karşılık koyabilmesi için sistem yönetiminde kesinlikle güvenlik önlemlerine dair politikalar belirlenmeli ve bu politikaların uygulanabilmesi sağlanmalıdır. Sağlanacak ve alınacak güvenlik önlemlerinin tüm evresinde kullanılan sistematik parametreler ve protokoller vardır bu nedenle alınmış ve alınacak olan önlemlerin genel olarak bilgisayar ve ağ güvenliği protokolleri denilmektedir.

Bilgisayar ağlarında güvenlik kavramı; günümüz de bilgisayar ağları büyüdükçe ağlardaki güvenlik önlemleri de bizim açımızdan önem kazanmıştır. Güvenlik önlemleri başlangıçta uygulanabilir ve yönetilebilir gözükürken kullanıcı sayısı ve ağ fiziksel yapısının değişmesi ile birlikte önlemlerin sürdürülebilirliği ve yönetilebilirliği azalmaktadır. Kurmuş olduğumuz sistem, sistemdeki en zayıf halka kadar güvenlidir. Çünkü en zayıf halka da oluşacak bir açık tüm sistemin ele geçirilmesine sebep olabilir.

Ağlarda güvenlik sağlamak için ağımızdaki cihazların özelliklerini iyi bilmemiz gerekmektedir. Sistemlerin bir bütün olarak değerlendirerek güvenlik önlemlerini almamız gerekmektedir. En zayıf halkadan başlayarak güvenlik önlemlerini almalıyız. Yerel ağlarımızda kullanıcıların kimlik kontrollü bağlanması, adresleyebilmesi için bir yöntem belirlenmelidir. Bir kullanıcının ağa hangi kullanıcı ile girdiği, hangi port'ta olduğu, IP adresi ve Mac adresi kayıt altında olmalıdır. Tabi ki bunları takip etmek zordur fakat devamlı takip ve güncellemeler ile bu işlem yapılabilir (Çiçek 2016).

Ağ protokolleri; verilerin nasıl paketleneceğini, kullanılacağını ve ağdan iletileceğini belirten anlaşmalardır. Satıcılar ve endüstriyel komiteler, bu anlaşmaları geliştirirler ve firmalar bunlara uygun yazılımlar üretmeye çalışırlar. Bu tip yazılımların ilk denemelerinde bazı firmalar daha başarılıdır, fakat birkaç ay içerisinde deneme yanılma yöntemiyle yazılımlar doğru Resimlerini alırlar (Derfler 2000).

Bilgisayar ağları, adından da anlaşılacağı üzere birden fazla bilgisayarın birbirleri ile haberleşmesini sağlamak üzere ortaya çıkan iletim ağıdır. İhtiyaçlar çerçevesinde binlerce bilgisayarın haberleşmesini sağlamak amacıyla gereksinim duyulan iletim yollarını kapsayan ağa WAN (Geniş alan ağı) denir (Hosgör 2014).

Ağ protokolleri; bilgisayarlar ve internet ağları birbirleri arasındaki tüm iletişimi katmanlardan oluşan protokoller üzerinden sağlar. Bu nedenle internet ve bilgisayar ağları katmanlı yapılardan oluşmaktadır, protokol sisteminin en başındaki haberleşmeyi sağlayan uygulama katmanını saymazsak ağ protokolleri dört ana katmandan oluşur. Her bir katmanın yapacağı görevler protokoller tarafından paylaştırılır (Yavaş 2017).

Bilgisayarlar arasındaki bağlantılar bakır teller üzerinde de olabildiği gibi değişik özellikteki kablolar ile de sağlanabilir bunlar gününüzde en çok kullanılan fiber optik kablolardır, buna ilave olarak radyo link sistemleri, uydular ve kısa mesafeler için kızılötesi iletişim sistemleridir. Bilgisayarları ağları fiziksel boyutlarına göre aşağıdaki gibi türlere ayrılmıştır (Öner 2010).

Her birey bilgi sistemleri üzerinden hizmet alırken veya hizmet sunarken kurumsal bilgi varlıklarını kullanmaktadır. Bu hizmetler kurumsal anlamda bir hizmet alımı olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemler de olabilir. Burada kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir (Vural 2007).

2.1.1 Bilgisayar Ağlarının Tarihçesi

Bilgisayar ağlarının tarihi karmaşıktır. İcadı ve ticarileşme süreci de oldukça karmaşıktır, ama temel gelişim süreçlerine bakmak yararlı olacaktır: 1940'larda bilgisayarlar, hata yapmaya eğilimli geniş araçlardı. 1947'de yarı iletkenlerin bulunuşu, daha küçük, daha güvenilir bilgisayarların yapımını mümkün hale getirdi. 1950'lerin sonunda küçük bir parça yarı iletkenin üzerinde, birçok birleşik transistörden oluşan entegre devreler geliştirildi. 1960'larda terminallerle ve entegre devrelerle birlikte, büyük bilgisayarlar yaygın bir şekilde kullanılmaya başlandı.

1960'ların sonlarında ve 1970'lerde minibilgisayarlar olarak adlandırılan daha küçük bilgisayarlar üretildi. Ancak, bu minibilgisayarlar modern standartlara göre hala oldukça büyüktü. 1977'de Apple Bilgisayar Şirketi, Mac olarak da bilinen mikro bilgisayarı üretti. 1981'de IBM (International Business Machines), ilk PC'ni (Personel Computer) sundu. 1980'lerin ortasında kullanıcılar, dosyalarını diğer bilgisayarlarla paylaşmak için modemleri kullanmaya başladılar.

Bu bilgisayarlar, bülten panoları (bulletin boards) olarak adlandırılıyordu. Kullanıcılar bülten panolarına bağlanıp, dosya yüklemek gibi mesaj bırakıp alabilirlerdi. Bu tip bir sistemin eksikliği, doğrudan iletişimin çok az olmasıydı. Diğer bir kısıtlaması, bülten panolu bilgisayarın her bağlantı için bir modeme ihtiyaç duymasıydı. Eğer beş insan aynı anda ağa bağlanmak isterse, bunun için beş modem bes ayrı telefon hattına bağlanırdı.

1960'lardan 1990'lara U.S. Department of Defense (DoD), askeri ve bilimsel araştırmalar için, güvenilir geniş alan ağlarını (Wide Area Network-WAN) gelistirdi. Bu teknoloji, bülten panolarında kullanılan noktadan noktaya iletişimden farklıydı. Çoklu bilgisayarların, birçok farklı yol boyunca bağlı olmasına izin vermekteydi. Ağ, kendi kendine bilginin bir bilgisayardan diğerine nasıl hareket edeceğine karar verebilirdi. Bir bağlantı, aynı zamanda birçok bilgisayar tarafından kullanılabilirdi. DoD tarafından geliştirilen WAN, en sonunda internet haline geldi.

2.1.2 Ağ Kavramına Giriş

Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan çalışma biçimine, bilgisayar ağı (computer network) denir. Bir bilgisayar ağında çok sayıda bilgisayar yer alır. Bu bilgisayarlar; yan yana duran iki bilgisayar olabileceği gibi, tüm dünyaya yayılmış binlerce bilgisayar da olabilir. Ağ içindeki bilgisayarlar belli bir biçimde dizilirler. Bilgisayarlar arasında genellikle kablo ile bağlantı sağlanır. Kablo bağlantısının mümkün olmadığı durumlarda, mikro dalgalar ve uydular aracılığıyla ağ içindeki iletişim kurulur. Bilgisayar ağlarının ilk uygulamaları 1960'lı yılların sonlarında başlamıştır.

Ancak yerel bilgisayar ağlarının yaygınlaşması 1980'li yıllarda başlamış ve gelişmiştir. 1980'li yıllarda, kişisel bilgisayarların çoğalması, bilgisayar teknolojisindeki ve iletişim teknolojilerindeki gelişmeler, bilgisayar ağlarının daha yararlı olmasını sağlamıştır.

Bilgisayar ağlarının kullanım amacı, kaynakların ve bilginin (veri, ses, görüntü ya da video) paylaşılması ve kişiler arasında iletişimin sağlanmasıdır. Bu paylaşım ve iletişimi sağlamak, birbirinden bağımsız ya da işlevsel olabilmek için; birbirine gereksinim duyan bilgisayarlar, çeşitli yöntemlerle bağlanarak bilgisayar ağını oluşturur (Baykal 2001).

Bilgisayar ağları, kaynakların etkin paylaşımını sağlayarak ve bilgi akısını hızlandırarak verimli bir iletişim ortamı sunar. Böylece farklı bilgisayarlardaki dokümanlar ortaklaşa kullanılabilir. Bilgisayar ağları yazıcı gibi donanımların da ortaklaşa kullanılabilmesini sağlar. Bilgisayar ağına bağlı olan bir bilgisayar, diğer bilgisayarlarla bağlantı içindedir. Diğer bilgisayarlarla iletişim kurar, onların sabit diskinde yer alan verilere erişir, programlarından yararlanır. En basit biçimi ile ag, genellikle modemlerle birbirine seri bağlantılı olan iki makinedir. Daha karışık ağ yapılarında ise, TCP/IP (Transmissions Control Protocol/Internet Protocol), protokolü kullanılmaktadır. Bu; yüz binlerce bilgisayarın birbirine bağlı olduğu internet üzerinde, diğer bilgisayarlar ile bağlantı kurmamızı sağlayan protokol ailesidir.

3. METOT ve YÖNTEM

3.1 Uygulamanın Amacı ve Yöntemi

Bu çalışmanın amacı Bilgisayar ve Ağ Güvenliği dersi kapsamında kullanılabilecek bir eğitim içeriği geliştirmek ve sonrasında öğrencilerden geri dönüşler almaktır. Öğrencilerden gelen geri dönüşlere göre bir içerik hazırlayarak ve uygulama yaparak öğrencilerin Bilgisayar ve Ağ Güvenliği dersine karşı farkındalıklarını oluşturmak ve kişisel güvenlik önlemlerini alabilmeleri sağlamaktır.

Hazırlanan bu çalışma öncesi yapılan değerlendirme süreçlerinden edinilen verilere göre daha sade ve daha az teknik bilgi ve dokümanlara yer vererek bu şekilde hazırlanmış olan bu çalışmanın amacına yönelik olarak Bilgisayar ve Ağ Güvenliği dersinin konularını kapsayan içeriklere yer verilmiş ve öğrencilerin derse karşı olan ilgilerinin artırılması amaçlanmıştır.

Bilgisayar ve ağ güvenliği dersinin işlendiği dönem süresince hazırlanan program öğrencilere kaynak olarak sunulmuştur. Programın hazırlanma aşamasında konusunda uzman kişiler tarafından görüş alınmış ve uzmanların görüşleri doğrultusunda içeriklere yer verilmiştir.

3.2 Ağ Güvenliğine Giriş

Ağ güvenliği, günümüz teknolojik altyapısı ile internet kullanımında en önemli ve üzerinde durulması gereken olaydır. Ağ güvenliği OSI'nin tüm uygulamalarında olmalıdır. Ağ güvenliğini sadece güvenlik duvarları(firewall) ile sağlanacağını düşünmek birçok güvenlik sorunlarını görmezden gelmek demektir ki bu sistem üzerinde oluşabilecek açıkların ağ üzerindeki etkisi sanılandan daha yıkıcı ve telafisi mümkün olmayan zararlara yol açabilir. Sistem üzerindeki ağ güvenliği elemanlarının bütünü üzerinde sürekli olarak güvenlik önlemleri ele alınmalı ve bu süreç kesintisiz olarak devam etmektedir. Güvenli iletişimde olması gereken birkaç özellik aşağıda belirtilmiştir:

- **Gizlilik:** Ağ üzerinde gönderilen ve alınan veri paketlerinin içeriğini sadece gönderici ve alıcı görmeli gönderilen verilerin içeriğini sadece tarafların anlayabilmesi gerekmektedir. Gönderilen mesajın içeriğini yetkisiz kişilerin anlayamaması için mesaj bozuk ve gitmesi gereken yere şifreli olarak gitmelidir.
- **Mesajın doğruluğu:** Mesajı gönderenler birbirlerinin kimliğini yapsalar dahi mesaj iletim halindeyken değiştirilmediğinden emin olmaları gerekmektedir.
- **Uç nokta kimlik denetimi**: Gönderici ve alıcı birbirlerinin kimlik denetimlerini yaparak kimliklerini doğrulamaları gerekmektedir.
- **İşlevsel güvenlik:** Sızma tespit sistemlerin ve güvenlik duvarlarına saldırı sırasında ortaya konan organizasyona karşı koymak için kullanılmalıdır (Karanfil 2009).

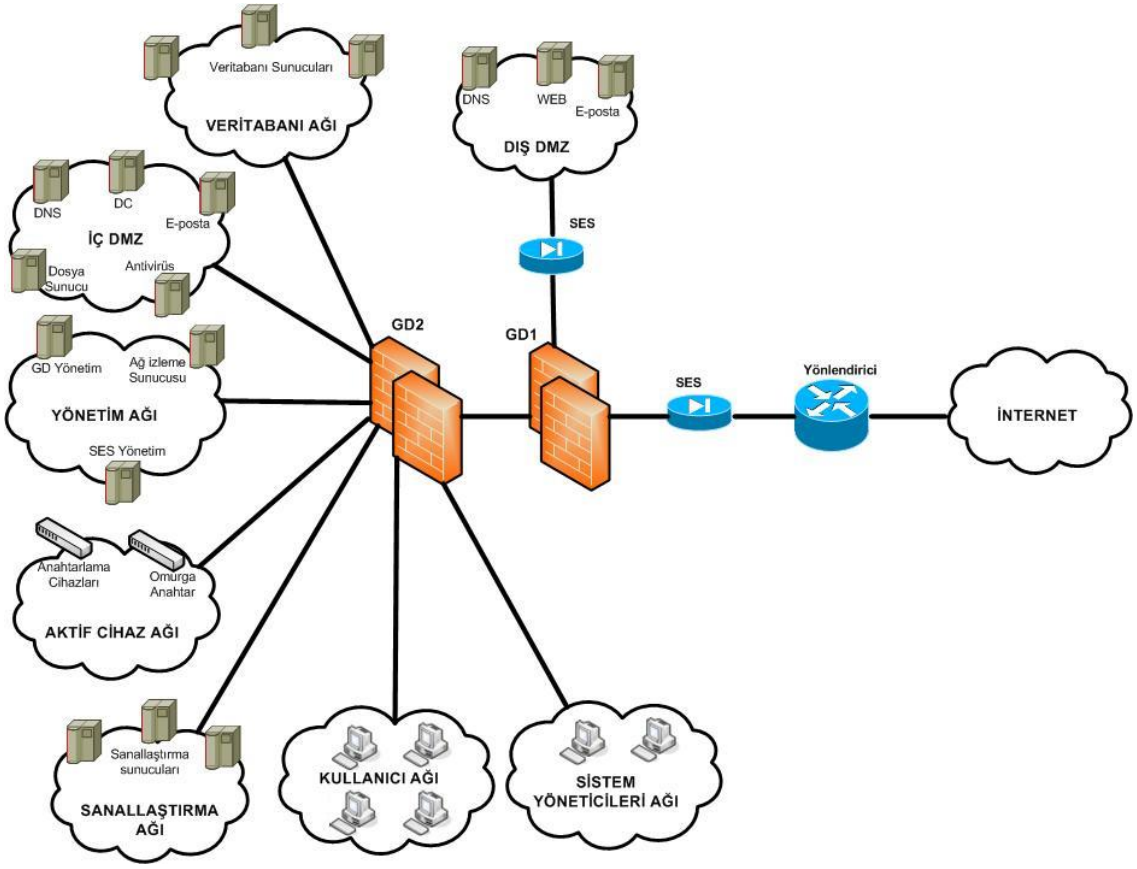
Bilgisayar ve bilgisayar ağlarının yaygınlaşması ağ güvenliğini daha da önemli kılmaya başlamıştır. Önemi artan bilgisayar ve ağlarının güvenliğine dair önlemler almak ve uygulamak günümüze göre daha kolay ve olmazsa olmaz değildi ancak günümüz teknoloji ve internet çağı olmasından da kaynaklı olarak kullandığımız tüm ağların ister kişisel ister kurumsal güvenlik önlemini almak hayati derecede önem arz etmektedir.

Kurmuş olunan sistem, sistemdeki en zayıf halka kadar güvenlidir. En zayıf halkadan kaynaklı bir açık ve sızma sistemin bütününe zarar verecek ve sistemi tamamen bizim kontrolümüzden çıkartabilecektir, bu nedenle ağ güvenliğimizi en zayıf halkadan almalıyız. Yerel ağlarda kullanıcıların kimlik kontrolü ile bağlanması, adreslenebilmesi için bir yöntem belirlenmelidir. Bu yöntem IP ve Mac temelli olmalıdır kesinlikle bunları takip etmek zordur ama devamlı olarak takip etmek ve sistem güvenliğini güncellemek işimizi kolaylaştıracaktır (Çiçek 2016).

Kurum ve kuruluşlar ihtiyaç duydukları ağ güvenliğini büyüklüklerine ve maddi imkanlarına göre dizayn etmeli ve seçenekleri en iyi şekilde değerlendirip güvenlik konusunda maksimum düzeyde tedbirlerini almalılardır. Kullanıcılarını periyodik olarak eğitimlere almalı ve giriş seviyesinde de olsa tüm kullanıcılara ağ güvenliği konusunda gerekli önlemlerin almalarını sağlayacak değişik yazılımlar sağlanmalıdır (Çakar 2005).

Metro Ethernet olarak bildiğimiz ve kampüs ağları gibi yerel ağların internet sağlayan network sisteminin başlangıç noktasını oluşturan teknoloji VLAN yapısı üzerine kurulmuş bir teknolojidir.

VLAN aynı fiziksel yollardan aynı ortamı paylaşan aynı kablolar üzerinde iletişim sağlayan yerel ağ kullanıcılarını sanki farklı noktalardaymış gibi yapılandıran yönteme yola verilen isimdir. VLAN sayesinde kullanıcılar farklı ağlarda çalışıyormuş gibi yapılandırma yapabilirler LAN ağının üzerinde farklı bir ağ gibi çalışan VLAN'lar oluşturmak sistemimiz için tek başına asla yeterli bir önlem olmamakla birlikte switch cihazları üzerinde yapılabilen güvenliğin bir parçası olan yazılımlardır ve bu sayede daha esnek daha kullanışlı bir yapı oluşturabiliriz (Dennis 2004). Güvenli ağ topolojisine Resim 3.1'de yer verilmiştir.



Resim 3.1 Güvenli ağ topolojisi (İnt. Kyn. 1)

3.3 Bilgisayar Ağları

Bilindiği üzere birden fazla bilgisayarın Ethernet kartları aracılığı ile haberleşmesi olayına ağ diyoruz. Bilgisayarların kendi aralarında oluşturdukları ağ üzerinden haberleşmelerini sağlayan ağ yapıları mevcuttur bu yapılardan herhangi birinin mutlaka bir bilgisayarda olması gerekmekte olup bu yapıları, ağ türleri adı altında üç başlıkta inceleyebiliriz.

- Yerel alan ağı (LAN)
- Geniş alan ağı (WAN)
- Şehir alan ağı (MAN)

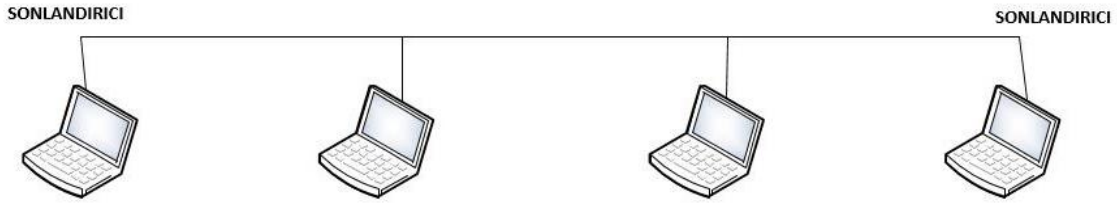
3.3.1 Yerel Alan Ağı (Lan)

Ofis, bina, yerleşke gibi fiziksel alan içerisinde ve bölgesel olarak sınırlı alanlarda kullanılan ağa türüdür ve fiziksel yerleşimlere göre 3 çeşittir.

- Doğrusal yerleşim (Bus topolojisi)
- Halka yerleşim (Ring topolojisi)
- Yıldız yerleşkesi (Star topolojisi)

- **Doğrusal Yerleşim (Bus topolojisi)**

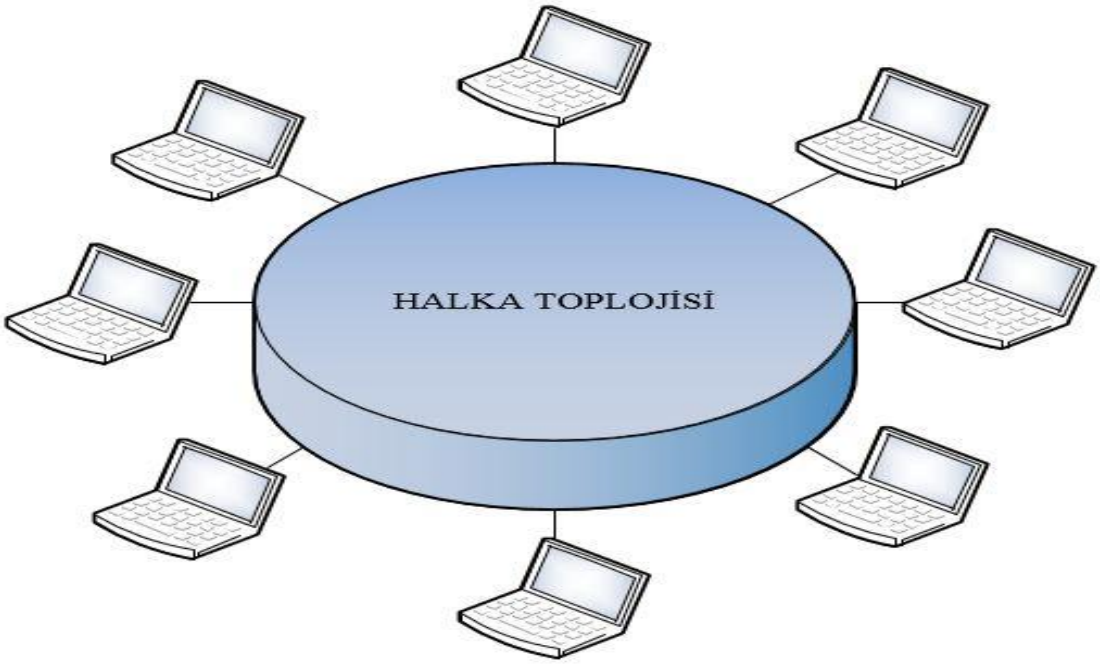
Doğrusal yerleşim ağ topolojisinde bilgisayarlar birbirleri arasında kablo bağlantısı ile iletişime geçerek veri iletimi yapabilirler. Bu kablolar boyunca veri iletişimi sağlayan ağ içerisindeki ortak olarak kullanılan veri kanallarına terminaller eklenebilir. Bu yerleşim ağ türü diğer topolojilere göre daha az maliyetli ve daha basittir. Bilgisayarlar arasındaki bağlantıyı sağlayan kablo uçları bir sonlandırıcı ile sonlandırılır ve bu şekilde iletişim sağlanan ağ çeşitlerinin herhangi bir noktasında oluşan arıza tüm ağ iletimini etkiler ve veri iletimi sonlanabilir. Resim 3.2'de Bus Topolojisi örnek çizimi paylaşılmıştır.



Resim 3.2 Bus topolojisi visio çizimi.

- **Halka Yerleşim (Ring topolojisi)**

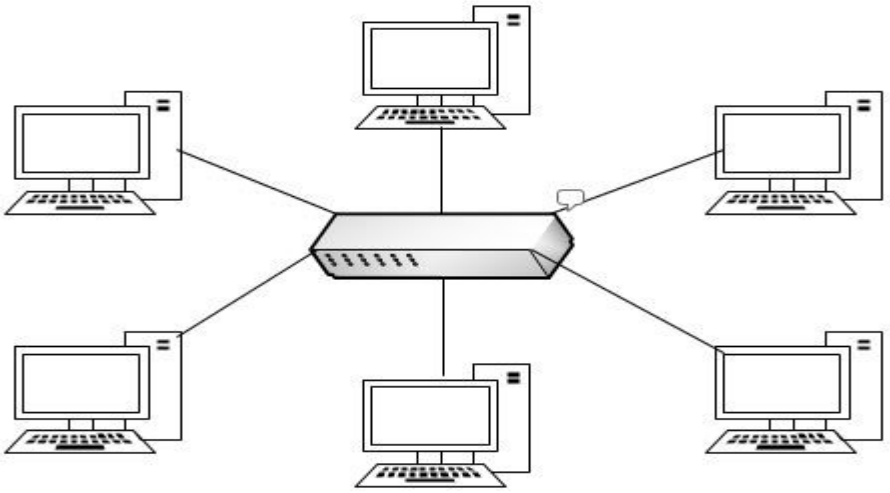
Bu topoloji adından da anlaşılacağı üzere bilgisayarlar arasındaki bağlantıyı ve veri iletimini halka biçimindeki bağlantı şeklinde yapan ağ türüdür. Halka şeklindeki kablolu bağlantılarda, ağ üzerindeki veriler tek yönlü hareket ederler ve sürekli olarak halka üzerinde daireler çizerler. Bu tür yerleşim topolojisi ile oluşturulan ağ yapıları diğer topolojilere nazaran biraz daha maliyeti yüksek ve verim iletim hızı kullanılan kablolama sistemine bağlı olan ağ türüdür. Halka topolojisine örnek olan çizim resim 3.3'de gösterilmiştir.



Resim 3.3 Halka topolojisi visio çizim.

- **Yıldız Yerleşim (Star topolojisi)**

Yıldız yerleşim topolojileri genellikle kampüs network sistemlerinde de kullanılan bir ağ türüdür. Yıldız topoloji türünde ağ sisteminde bulunan tüm bilgisayarlar direkt olarak hub ya da switchlere bağlı olarak sisteme dâhil edilirler. Kullanılan kablo uzunluğu diğer topolojilere oranla daha fazla olduğundan maliyeti en yüksek ağ topolojisi olup bu tür bağlantı çeşitlerinde meydana gelebilecek arızaları bulmak ve çözüm üretmek daha kolaydır zira arıza sadece bulunduğu kabloyu o kabloya bağlı olan cihazları etkilemektedir. Yıldız topolojisi örnek olarak sunulan çizim resim 3.4'de paylaşılmıştır.



Resim 3.4 Yıldız topolojisi visio çizimi.

3.3.2 Geniş Alan Ağı (WAN, Wide area network)

Ülkerler arası bilgisayar iletişim ağını sağlayan geniş alan ağıdır. Bir nevi uluslara arası ağ türüdür, örneğin; herhangi bir kurumsal şirketin, firmanın yerelde bulunan bilgisayar ağını dış dünyaya açan ve diğer ülkeler ile bağlantısını sağlayan ağ çeşididir.

3.3.3 Şehir Alan Ağı (MAN, Metropolitan area network)

Yerel alan ağı yani Lan'ın(Yerel alan ağ) kapsadığı alandan daha geniş ama Wan(Geniş alan ağ) yani geniş alan ağına nazaran daha dar kapsamlı alan ağıdır, geniş alan ağları dünya ile bağlantıyı sağlarken şehir alan ağları sadece bulunduğu şehir içerisindeki bilgisayarları birbirine bağlayan alan ağıdır.

3.4 Bilgisayar Ağ Protokolleri

Bilgisayarların, kurumsal ve kişisel kullanımlarının artması sonucu bilgisayarlar arasındaki haberleşmeleri ile veri iletişimi sağlayan ağ alt yapıları ve teknolojileri yetersiz kaldığından birçok teknoloji firması ağ çeşitleri üzerinden çalışmalar yapmış ve bu çalışmalar sonucunda kendilerine özgü çözümler üretmeye başlamışlardır. Ancak teknoloji firmalarının kendi gereksinimlerine özgün ortaya çıkarttıkları ağ çeşitlerine bir standart getirilmesi kaçınılmaz olmuş ve bunun sonucu olarak İSO tarafından açık sistemler ara bağlantısı olan OSI modeli geliştirilmiş ve tüm üreticilerin bu standarda göre çalışmalar yapması sağlanmıştır. OSI modelini temel alarak yapılan çalışmalar ve üretilen çözümler neticesinde birçok sorun çözüme ulaşmıştır. OSI modeli yedi katmandan oluşturulmuş olsa da temel katmanı saymaz isek dört ana katman üzerine kurulmuş ve tüm işlemler bu dört katman üzerinden yürütülmektedir. Ağlar arası iletişimi yapacak olan görevler bu katmalar üzerinden yürütülen protokoller tarafından paylaşılmıştır. Katmanlar arasında kullanılan en yaygın protokoller TCP/IP protokolüdür ancak bu protokoller farklı katmalarda bulunan, farklı özellikteki protokollerdir. Her ne kadar TCP/IP protokolleri farklı katmanlarda bulunan ve farklı özellikleri olan protokoller olsa da TCP/IP olarak kullanıldıklarında, bu katmanlarda bulunan diğer tüm protokollerin başlama noktası olarak ifade edilir. TCP/IP protokolü bir nevi diğer protokollerin başlangıç kümesidir.

3.4.1 OSI Modeli

Ağ protokollerinin çıkış noktası olarak kabul ettiğimiz, teknolojik yetersizlik sonucu firmaların yapmış oldukları çalışmalar neticesinde ortaya birçok ağ çeşitleri geliştirilmiştir. Firmaların kendileri için geliştirdikleri ağ çeşitlerinin birbirleri arasındaki senkronizasyon sorunlarından doğan arızaların sonucu olarak ortaya çıkan ara bağlantı sorunlarının çözüme kavuşturulmasının, ancak temel nokta olarak kabul edilecek bir çalışma modelinin geliştirilmesi ile mümkün olabileceğini gören Uluslararası Standartlar Teşkilatı(ISO) öncülüğünde geliştirilen ara bağlantı modeline OSI modeli denilmiş ve bu modelinin geliştirilmesinden sonra teknoloji firmalarının

OSI modeline uygun olarak yapmış oldukları çalışmalar ile ara bağlantı sorunu çözümlenmiştir.

OSI (Open Systems Interconnetion) modelini ISO (International Organization for Standardization) geliştirilmiştir. Bu şekilde amaç birden fazla bilgisayarın kendi araların haberleşmesini sağlamaktır. OSI modeli ilk defa 1974 yılında kullanılmaya başlamış ancak ilk zamanlar sadece belli firmaların kendi donanımları için kullandıkları bu model 1984 yılında yeniden düzenlenerek günümüzdeki 7 katmanlı modelini almıştır.1984 yılından sonraki düzenlemenin en iyi fonksiyonlarından biri tamamen farklı kullanıcı makineleri ve donanımları arasındaki veri transferine yardımcı olmasıdır. Örneğin bir Unix Hot'u bir Pc ya da Mac arasında veri transferi yapabilmektedir (Çiçek,2016).

3.4.1.1 OSI Katmanları

OSI modeli, ağ üzerindeki haberleşmenin, veri iletiminin yapılmasını sağlayan ağlar arasındaki katmanlardan oluşmaktadır. OSI modeli, uygulama katmanı, sunum katmanı, oturum katmanı, ulaştırma katmanı, ağ katmanı, veri bağlantı katmanı ve fiziksel katman olmak üzere yedi katmandan oluşmaktadır. OSI modelindeki birbirinden bağımsız yedi katmanın arasında kesinlikle bağlantı vardır ve aradaki bağlantıda süreklilik esastır bu nedenle herhangi bir katmanda çalışan fonksiyonlar diğer katmanlardan bağımsız olarak çalışıyor gözükse de ancak birbirlerinin bilgisi dahilinde çalışabilmektedir. OSI modeli, yedi katmanın temel aldığı ve tcp/ip protokollerinin de kullandığı dört ana katman üzerine oluşmuştur. Bilgisayar Ağlarının çalışma prensibi olan OSI çalıma modelinin uygulanma yöntemini gösterir şablona aşağıda yer verilmiştir. Tcp/Ip protokollerine ait örnek şablon tablosuna resim 3.5'de yer verilmiştir.

SEVİYE	Katman Adı	VERİ	ÖRNEKLER
Katman 1	Fiziksel (donanım) katman	Bit Katarı	Kablo, voltaj değeri, sinyal zamanlama
Katman 2	Veri bağlantısı katmanı	Çerçeve	Akış kontrolü, hata kontrolü, fiziksel adresleme
Katman 3	Ağ katmanı	Paket	Router, Quality of Service, IPv4, IPv6, ARP
Katman 4	Ulaşım - erişim katmanı	Segment	TCP, UDP
Katman 5	Oturum (session) katmanı	Veri	Uzaktan Bağlantı
Katman 6	Sunum katmanı	Veri	Kodlama, MIME
Katman 7	Uygulama katmanı	Veri	HTTP,FTP,CMIP

Resim 3.5 OSI Katmanları ((İnt. Kyn. 5).

- Uygulama katmanı
- Sunum katmanı
- Oturum katmanı
- Ulaştırma katmanı
- Ağ katmanı
- Veri bağı katmanı
- Fiziksel katman

- **Uygulama katmanı (Aplication layer)**

Bu katman, modelin en üst katmanı olup kullanıcıya en yakın olandır. Kullanıcıların bilgisayarlarında çalıştıracakları programlar ile ağ sistemi üzerinde aracı görevi görür ve programların ağ sistemi üzerinde çalışmasını sağlar. Bu katmanı kullanan uygulamalardan bazıları e-mail uygulaması veri tabanı uygulamaları ve basit dosya aktarım uygulamalarıdır örneğin; FTP iletim protokolü ve basit ağ yönetim protokolü olan SNMP uygulamaları gibi. Ağ sistemi üzerinden iletim sağlayan uygulamaların osi modeli üzerinden incelenerek işleme alındığı uygulama katmanıdır.

- **Sunum Katmanı (Presentation layer)**

OSI modelinin ilk geliştirildiği yıllarda bu katmanın görevi verileri derleyerek sadece bilgisayarların okuyabileceği formata çevirmesini yaparak ilgili katmana sunmasıydı ancak gelişen teknoloji ile hayatımıza laptop tablet ve akıllı telefonlar gibi değişik yapıda cihazlar girdi ve bu yeni teknolojik cihazların farklı formatlarda olması sunum katmanının önemini daha da artırdı. Kısacası sunum katmanı; bilgisayar ağlarına bağlı olan değişik formattaki tüm cihazlara gönderilen verilerin, işlenerek derlenerek cihazların okuya bileceği şekilde formatlama görevini yerine getirerek ilgili katmana ileten katmadır.

- **Oturum Katmanı (Session layer)**

Bu katmanın görevi adından da anlaşılacağı üzere cihazların aynı ağ üzerinde aynı anda farklı oturumlar ile ağ üzerinde işlemler yapabilmesine olanak sağlayan katmadır. Bir nevi sunum katmanı ile taşıma katmanı arasında iletişimi sorunsuz olarak sağlayan katmandır. Örneğin bir A kullanıcısı paylaşılmış bir klasörün içindeki bir dosyayı ağdaki paylaşımlı yazıcıya gönderebilirken diğer B kullanıcısı aynı dosya üzerinde farklı işlemler yapabilmektedir. Bu katmanın ayrıca kullanıcılar için en önemli görevlerinden biride ağ sistemi üzerinden çalışan uygulamaların birbirleri ile karışmasını önlenmesi ve haberleşmelerinin sağlanmasıdır.

- **Ulaştırma Katmanı (Transport layer)**

Diğer adı taşıma katmanı olan bu katmanın görevi, ağ üzerinde gelen verileri parçalara ayırır ve gelen bilgilerin doğruluğunu kontrol ederek gönderilmesi gereken yere güvenli bir şekilde iletilmesini sağlar. Bu katmanın, üzerinde veri akışı sağlanırken verilerin hatasız şekilde ayıklama ve düzeltme görevi de vardır.

- **Ağ Katman (Network layer)**

Ağ katmanı gelen verilerin farklı ağlara gönderilmesi gerektiğinde yönlendiricilerinde kullanacağı bilgileri ekleyen katmandır. Bu katman araçlığı ile iletilen veriler paketler halinde taşınırlar. Farklı ağlar üzerinden veri iletiminin sağlandığı en ekonomik yoldur.

- **Veri Bağlantı Katmanı (Data link layer)**

Bu katman fiziksel ağ ile olan iletim sırasında verilerin fiziksel katmana ulaşmasını sağlayan kuralları uygular ve bu kuralları kullanır. Katmanlar arası gönderilecek verilerin nasıl taşınacağını ve fiziksel adresleme ile ağ topolojisini belirler. Veri bağlantı katmanında veriler ağ katmanında olduğu gibi paketler halinde ve belirli çerçevede taşınır, çerçevelerin görevi paketlerin doğruluğunu kontrol ederek gönderilmesini sağlamaktır.

Bu katman içerisindeki haberleşmenin büyük bir bölümü ağ üzerinde bulunan ethernet kartı ile token ring olarak adlandırılan erişim yöntemleri kullanılarak yapılır. Veri bağlantı katmanı ağ üzerindeki bilgisayarların kullanıcılarının belirlenmesi ile hatasız olarak kontrol görevini yerine getirir. Bu katman ayrıca network anahtarlama cihazlarından olan Switch'lerin Mac adresi tabanlı olarak çalıştığı katmandır.

- **Fiziksel Katman (Physical layer)**

Adından da anlaşılacağı üzere bu katmanda gerçekleşen veri iletimleri sinyaller üzerinden fiziksel kablolar (Kablo, fiber optik, radyo sinyalleri) aracılığı ile yapılır. Fiziksel katmanda veriler kablolar üzerinden bit olarak iletirler ve bu katmadan bir ve sıfır olarak gönderilen sinyaller yine alıcı tarafta olan fiziksel katmanda okunan bu sinyaller tekrar bir ve sıfır hale dönüştürülür.

Veri iletiminin sağlıklı şekilde yapılabilmesi için her iki tarafta da aynı kuralların tanımlamış olması gerekmektedir. Hub bu katmadan çalışan bir cihazdır. Bu cihazlar gelen veriyi sinyallere çevirerek ve çoğaltarak ilgili portlara kablolar aracılığı ile iletirler.

3.4.2 TCP/IP Modelleri

Etki Alanı Adı Hizmeti Protokolü (DNS): İnternet adlarını IP adresleri olarak çözümlemek için kullanılır.

Dosya Transfer Protokolü (FTP): Sistemler arasında etkileşimli dosya transferi için kullanılır.

Önemsiz(Trivial) Dosya Transfer Protokolü (TFTP): Bağlantısız etkin dosya transferi için kullanılır.

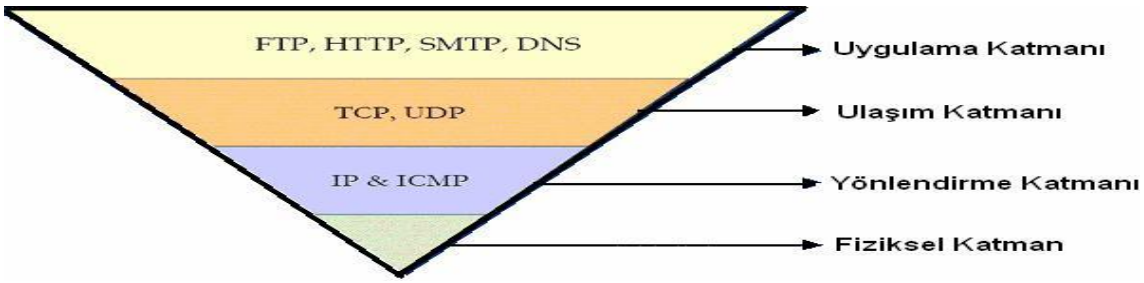
Simple Mail Transfer Protocol (SMTP): Posta mesajlarının ve eklerinin transferi için kullanılır.

Postane Protokolü (POP): E-posta istemcileri tarafından uzak sunucudan e-posta almak için kullanılır.

İnternet Mesaj Erişim Protokolü (IMAP): E-posta alımı için kullanılan başka bir protokolü.

Hypertext Transfer Protocol (HTTP): World Wide Web'in web sayfalarını oluşturan dosyaları aktarmak için kullanılır.

Telnet: Sunuculara ve ağ cihazlarına uzaktan erişim sağlamak için kullanılan terminal emülasyon protokolüdür. Tcp/İp modelinin çalışma prensibi resim 3.6'daki görsel ile ifade edilmiştir.



Resim 3.6 TCP/IP modeli ((İnt.Kyn.6).

3.5 Kablosuz Ağlar

Kablosuz teknoloji; en basit anlamıyla, bir veya daha fazla cihazın fiziksel bağlantı olmaksızın haberleşmesi demektir. Kablosuz ağlar; kablolu iletişime alternatif olarak uygulanan, RF (Radyo Frekansı) teknolojisini kullanarak havadan bilgi alış verisi yapan esnek bir iletişim sistemidir. Kablosuz ağlar, aletler arasında ve geleneksel kablolu ağlar arasında taşıyıcı mekanizma olarak hizmet verirler.

3.5.1 Kablosuz Ağların Çalışma Prensipleri

Kablosuz ağ bağlantı merkezleri veya cihazları aslına bakarsak router modemlerin çalışma prensibine benzer şekilde radyo frekansları üzerinden küçük sinyaller üreterek

çalışırlar. Kablosuz yani Wifi(Kablosuz ağ) cihazlarının belirli standartlar ile çalışma prensipleri vardır bunlardan en bilineni ve kullanılanı 802.11b standardıdır ve bu standartlar kendi aralarında da çeşit ve özelliklerine göre ayrılmışlardır. Wifi(Kablosuz ağ) standartları ilk olarak uluslararası sivil toplum örgütü olan Elektik Elektronik Mühendisleri Enstitüsü tarafından geliştirilmiş ve bu nedenle de çoğumuzun bildiği ve aşina olduğu IEEE kısaltması, enstitünün İngilizcesinden alınmıştır. Günümüz teknolojik gelişmelerin neticesinde mobil cihazların ve dizüstü bilgisayarların tamamında üzerlerine entegre edilmiş Wifi(kablosuz ağ) alıcıları bulundururlar, bulundurmayanlarda ise PCMCIA kartlar ile kablosuz alıcı özelliğini sorunsuz olarak kullanabilirler.

Kablosuz ağ sistemleri radyo frekansları ile çalışmaktadır. Radyo frekansları ile haberleşme üç çeşit olabilmektedir. Bunlar alıcı(receiver) verici(transmitter) ve alıcı-verici(trans-receiver) olarak adlandırılmaktadır.

Alıcılar; adından anlaşılacağı üzere sadece radyo sinyallerini alabilen ancak gönderme özelliği olmayan aygıtlar üzerinden yapılmakta olup bu sisteme en basit örnek FM radyoları ve televizyonları gösterebiliriz.

Vericiler; Bunlar sadece radyo sinyalleri gönderebilen ama sinyal alma özelliği olmayan elektronik devrelerdir. Bunlara örnek olarak televizyon ve radyo vericilerini gösterebiliriz.

Alıcı-Vericiler; Adından anlaşılacağı üzere aynı anda sinyal alma ve gönderme özelliğine sahip olan aygıtlara denir ve bu aygıtlara örnek olarak telsiz röleleri ile cep telefonlarını verebiliriz.

Günümüz kablosuz ağ teknolojilerinde en yaygın olarak kullanılan kablosuz iletişim ağ modeli çift yönlü ve eş zamanlı iletişim modelidir. Şehirlerin birçok farklı noktalarında kurulu bulunan kablosuz ağ noktaları arasında mükemmel bir uyum içerisinde çalışan ağ oluştururlar. Bu kusursuz çalışmanın sonucu olarak da trende otobüslerde parklarda

bahçelerde bilumum halka açık bölgelerde belirli aralıklarla yerleştirilmiş bağlantı noktaları üzerinde özgürce ve kesintisiz olarak bağlantı kurulabilmektedir.

Son olarak kablosuz ağ teknolojilerinde yeni yeni adından bahsedilen ağ teknolojisi WiMAX'tir. Wimax teknolojisinin temelde çalışma prensibi standart kablosuz ağ sistemleri ile aynıdır fakat çok güçlü mikrodalga iletimiyle sinyalleri daha uzak mesafeleri yayarak iletim ağını daha uzaklara taşıyabilmek mümkün olacaktır (Bilgiustam).

3.5.1.1 Kablosuz Ağların Çalışma Modları

Kablosuz cihazlar adaptörlerinin kullandıkları sürücülere ve yapacakları işe göre dört farklı modda çalışabilme özelliğine sahiptirler;
Bunlar:

- Managed Mod
- Mater(hostap) Mod
- Ad-hoc Mod
- Monitör Mod

Master Mod: Etrafta bulunan kablosuz cihazlara erişimin sağlandığı tüm kablosuz ağ adaptörleri bu modda çalışır.

Managed Mod: Herhangi bir erişim noktasına bağlanan ve hizmet alan istemcilerin çalıştığı mod.

Ad-Hoc Mod: Arada AP (Access point) olmadan tüm kablosuz istemcilerin kendi aralarında çalıştıkları mod.

Monitör Mod: Herhangi bir ağ bağlamadan tüm trafiğin izlenmesine olanak sağlayan ve kablosuz ağların güvenliğinde kullanılan bir mod'dur.

3.5.2 Kablosuz Ağlarda Güvenlik

Kablosuz ağlarda güvenliğin sağlanabilmesi için kullanıcılara direkt olarak konan engeller vardır, bu engelleri aşacak kullanıcı bilgilerine sahip olmayanlar ağa giriş yapamazlar ancak kablolu ağlarda uygulanan fiziki engellerin, veri iletimini sadece binalar arasında sınırlı kalmayıp kızılötesi sinyaller ve frekanslar aracılığı ile yapan kablosuz ağlarda uygulamak mümkün değildir. Bir güvenlik mekanizması, kullanıcıların ağ giriş yapmasından bir önceki adımda mutlaka konulmalıdır.

Kablosuz ağlardaki güvenlik IEEE standartlarından olan 802.11 standardı ile sağlanır. 802.11 protokolünün esas güvenlik mekanizması WEP (Wired Equivalent Privacy)'dir. Ancak 802.11 Protokolü'nün esas güvenlik mekanizması olan WEP eski cihazların desteklediği ve önerilmeyen ağ güvenliği yöntemidir. WEP protokolünün yerine kişisel ev kullanıcıları için daha güvenli olan WPA-Kişisel ve WPA2-Kişisel protokol önerilir.

3.5.3 Kablosuz Ağlarda Güvenlik Amaçlı Temel Önlemler

Kablosuz ağ teknolojisi günümüz internet alt yapısının vazgeçilmezi olmuştur. Kablosuz ağlar ev kullanıcılarının ve kurumsal firmaların en çok tercih ettiği bağlantı yoludur. Kablosuz ağların hızla yaygınlaşması beraberinde güvenlik zafiyetlerini de getirmiştir zira kablosuz ağların güvenlik zafiyetleri kablolu ağlara nazaran daha fazladır. Kablosuz ağlarda güvenlik önlemlerini almak için anti virüs yazılımları, güvenlik duvarları(firewall) saldırı tespit sitemleri, şifreleme ve parola politikaları gibi bilinçli kullanıcılar ile değişik teknolojiler önemli rol almaktadır.

3.5.4 Erişim Noktası Ayarlarının Değiştirilmesi

Kablosuz ağların en çok karşılaştığı saldırılar başkasının internetini izinsiz olarak kullanmak ve erişim sağlamak isteyen meraklı kullanıcılardır. Bu şekilde kablosuz ağlara yapılacak saldırıları engellemenin değişik yolları vardır. En sık rastlanılan güvenlik açığı internet erişimi sağlamak için kullanılan modem ara yüzlerinin varsayılan şifrelerini değiştirmemeleridir.

Hacker olarak tanımladığımız bilgisayar korsanlarının daha önceleri denenmemiş yollardan ve her yönden yapacakları yoğun saldırılara karşı koyabilecek, engelleyecek ve internet kullanıcılarını her düzeyde koruyabilecek savunma sistemi ile yazılımdan söz etmek mümkün değildir. Kullanıcılara ağ ve bilgi güvenliğinin önemine dair farkındalık yaratacak bilgilendirmelerin ve eğitimlerin farklı platformlarda sürekli olarak yapılmasını sağlanmak günümüzde zorunlu bir hal almıştır.

3.5.4.1 Erişim Kontrolü

Kablosuz ağlarda en sık karşılaşılan problemlerdendir zira ağ giriş anahtarını bilen herkes ağa giriş yapabilir. Kullanıcılardan birinin WEP şifresini bir başkasına söyleme ya da çaldırma durumunda WEP protokolünü kullanarak ağımızın güven altında olduğunu düşünmemizin geçerliliği kalmayacaktır. Dolayısı ile bu tip durumlarla karşılaşmamak için 802.1x protokolünü kullanmak tüm kullanıcıların yararına olacaktır.

3.5.4.2 802.1x Protokolü

802.1x başlarda kablolu yerel ağlarda kullanılmak üzere tasarlanmış ancak son zamanlarda kablosuz yerel ağların daha çok kullanılmasıyla popülerlik kazanmıştır. Bu durumda yani hem kablolu hem kablosuz yerel ağlarda kullanılıyor olması fazladan birçok gereksinim doğurmuştur.

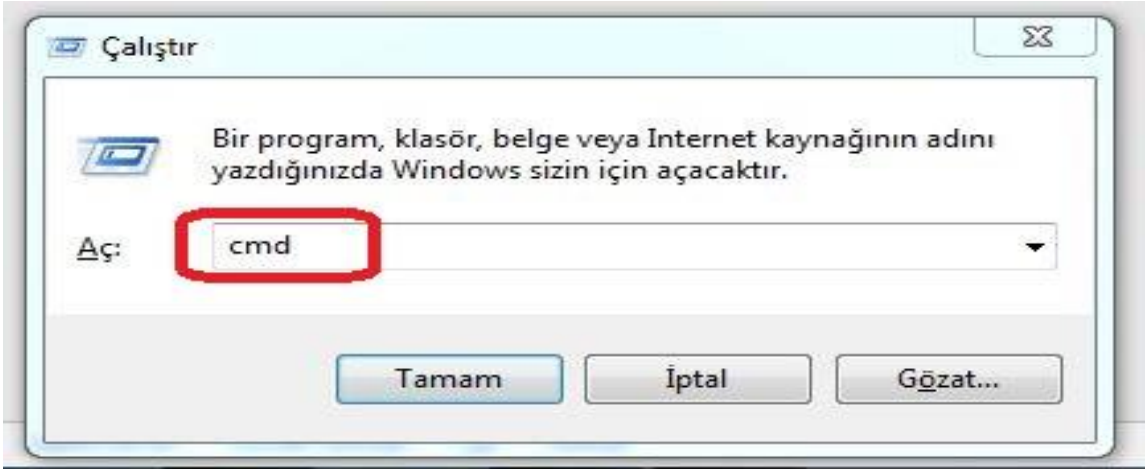
802.1x protokolü genellikle LAN (Local Area Network-Yerel Alan Ağ) bağlatısına sahip topolojilerde iç ağa üzerinden kullanıcıların internete erişim sağlamaları sağlamak amacıyla port tabanlı erişim kontrolü yapan bir protokoldür. Ağ tabanlı port tabanlı kullanıcı doğrulaması yağabilmek için herhangi bir kullanıcıya ya da gruba yönelik ağa erişim politikası uygulaması imkânı da tanır.

Genel olarak 802.1x protokolü üzerinden ağa erişim politikası uygulayan birimlerin kurumların başında gelen ve en yaygın olarak kullanan kurumlar üniversitelerdir. Bu protokolün kullanıldığı en bilinen uygulama eğitim kurumlarında kullanılan eduraom(üniversiteler arası kablosuz ağ) uygulamasıdır.

3.5.4.3 Mac Tabanlı Erişim Kontrolü

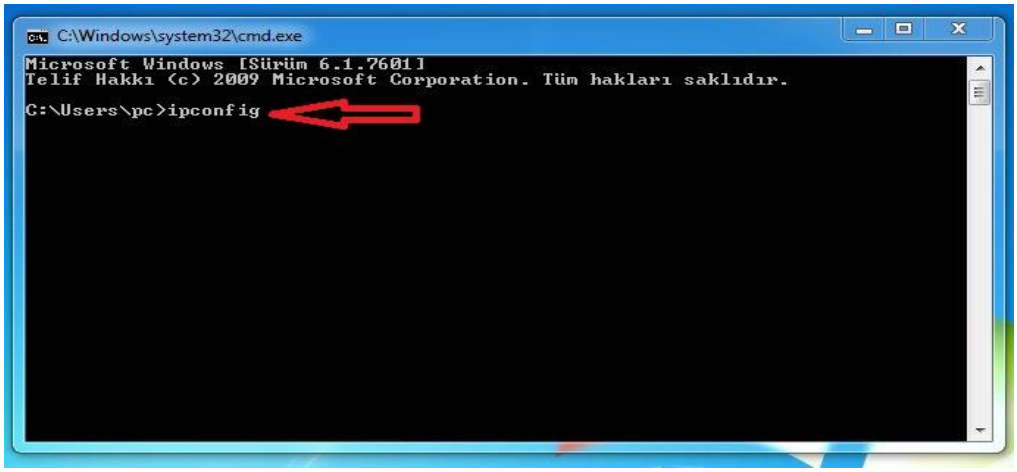
Yaygın olarak kullanılan erişim noktası(AP) cihazlarının genelinde güvenlik amaçlı konulmuş olan özelliklerden bir tanesi de Mac Tabanlı Erişimdir. Bu erişim modelinde kablosuz ağ cihazına bağlanmak isteyen kullanıcıların cihazlarına ait Mac adres bilgilerinin cihaz üzerinde tanımlanması gerekmektedir böylelikle erişim noktası üzerinde tanımlanmamış cihazların kablosuz ağımıza bağlanması engellenmiş olacaktır.

Ancak bu yönteminde zayıf yönleri vardır, her ne kadar ağımız şifreli olsa da uzmanlaşmış hackerlerin erişim noktasına tanımlanmış olan cihazlara ait Mac adres bilgilerine ulaşması zor olmayacaktır. Mac adres bilgilerine ait yapılacak değişiklikler işletim sistemleri üzerinden yapılsa da zor değildir kaldı ki Mac adres bilgilerini değiştiren Mac-Changer yazılımları oldukça yaygın olarak kullanılmaktadır.



Resim 3.7 Açılan pencere 1.

CMD'ye klavye üzerinde **windows + r** tuşlarına basarak ya da başlat menüsü arama kısmına çalıştır yazarak "Windows Çalıştır" uygulamasını açarız.



Resim 3.8 Cmd komut penceresi 2.

Ve burada komut ekranına **ipconfig** yazarak kendi bilgisayarınıza ve modeminize ait bilgileri görebiliriz.

Default Gateway bizim modeminizin IP adresidir. Bu IP adresini herhangi bir tarayıcıda (İE, Edge, Mozilla, Chrome vb.) adres çubuğuna yazmanız halinde modeminizin ara yüzüne ulaşabilirsiniz.

Resim 3.9 Cmd penceresi 3.

Resim 3.10 Tp-Link modem ara yüz ekranı.

3.5.5 Kablosuz Ağlarda Şifreleme Yöntemleri

Kablosuz ağ erişim yollarını başkalarının izlemesine giriş yapmasına ve ağ trafiğini izlemesini engelleyen sistemlerden biride şifreleme yapmaktır. Kablosuz ağlarda yapılan şifrelemeler daha öncede belirttiğim gibi farklı protokoller aracılığı ile yapılmaktadır bunlarda ilki WEP (Wired Equivalent Privacy) diğeri WPA (Wi-Fi Protecdet Access)'dir. Ancak her iki protokolde tek başlarına ağımızı korumak için yeterli güvenlik sağlamaya bilir çünkü; internette yapılacak kısa bir aramadan sonra Linux tabanlı işletim sistemleri üzerinden bir kablosuz ağ adaptörü ile kablosuz ağımıza sızma yapılması içten bile değildir.

Bugüne kadar WEP protokolünü kullanan kullanıcılara WPA protokolünü kullanmaları önerilirdi zira WEP protokolünün açıklarını WPA ile kapatıldığı düşünülürken, WPA'nında güvenilir olmadığı 2008 senesinde bir üniversite öğrencisi tarafından 15 dakika gibi kısa bir süre içinde kırılarak ispatlanmıştır. Aslında WPA protokolündeki açık TKIP (Emporal Key Integrity Protocol) bileşeninden kaynaklanmaktaydı.

3.5.5.1 Kablosuz Ağlara Saldırı ve Savunma

Kablosuz ağlar uzun zamandır hayatımızda olmasına rağmen ülkemizde kullanıma başlaması daha yenidir diyebiliriz zira 11 12 yıllık bir geçmişi ancak var. Türkiye'de kablosuz ağların yaygınlaşmaya başlaması 2005 yılı itibari ile başlamış ve ön koşulsuz olarak kontrolsüz bir şekilde hızla yaygınlaşmıştır.

Kablosuz ağ standartları ilk yıllarda güvenlik yönünden oldukça zayıftı bu nedenle de olası güvenlik açıkları ve riskleri ciddi tehlikeler oluşturuyordu bir nevi kurumlar ve şirketler networklarında bulunan switch'lerin router'ların birer slotu'nu halka açmış gibi bir durumla karşı karşıya idiler. Kablosuz ağların yabancılar tarafından izinsiz olarak tespit edilmesi güncel yasalar ile suç teşkil etmemektedir.

Kablosuz ağlara yapılan saldırılar hakkında edinilen bilgilerin kullanıcılara sağladığı faydalara iki açıdan baktığımız zaman bir kurum ya da kablosuz ağ sahipleri için hasar ne olabilir? Saldırganlar veya meraklıları içinse kazanç ne olabilir.

- Hasar;
    - Firmamızın veya kişisel ağımıza sızılması
        - Bilgilerin çalınması
        - E-maillerin okunması
        - Daha ciddi saldırıların ve tehditlerin ilk adımı
        - ……. vb
    - İnternet ağımızın (kullanım kotası) sömürülmesi (kişisel kullanıcılar için)
    - Kurumsal ağın kullanılamaz hale gelmesi

- Kazanç;
    - Erişim kısıtlaması olmaksızın internet erişimi
    - Ticari bilgileri geçirerek rakipleri saf dışı bırakma
    - Kişisel bilgilere erişilerek bankacılık işlemleri yapabilme
    - Kurumlara ya da kişilere duyulan husumetin bu şekilde intikamını alabilme
    - Ve kişinin kendini tatmin etmesi bundan zevk alması gibi

Kullanıcıların genelinde bulunan ve internet ağlarına dair güvenlik önlemlerini alma konusunda pasif ve ilgisiz davrananların hem fikir oldukları "Beni/bizi neden hacklesinler" anlayışı bilgilendikten sonra birazcık da olsa kırılabilir.

3.5.5.2 Kablosuz Ağlarda Güvenlik Sorunu Nerede Başlıyor

Sniffing, Arp Poisoning tarzı kullanılan siber saldırı atakları genellikle iç network ağına bağlı olarak en sık yapılan atak türleridir. Bu tür atakların açtığı tahribatlar ilk başlarda önemsiz ataklar ve tahribatlar olarak kabul edilmişlerdir. Bu saldırılar için saldırganın muhakkak iç ağa ulaşması gerekmektedir ancak bu durum kablosuz ağlar için o kadar

masum değildir zira kablosuz ağlar da yaşanılan güvenlik açıkları sayesinde içeriye ulaşmak daha kolay ve daha çok zarar verecek nitelikte olabilmektedir.

3.5.5.3 Kablosuz Ağlarda Güvenlik Parametreleri

Kablosuz ağlara dair alınacak önlemlerin evreleri ve bu evrelerin kendi içerisinde ayrıştığı alanları oluşturan parametreleri şu aşağıdaki gibi açıklayabiliriz.

- Wep
- Wpa
- Rsn
- Radius/Wpa-Radius
- Wireless Gateway
- Kurumsal özel çözümler

- **Open Security;** Bu tür bağlantılarda Open Security olarak bilinen güvenlik modeline şifre gerektirmeyen bağlantı demektir. Yani isteyen kullanıcı bu tür ağlara şifresiz olarak hiçbir güvenlik parametresine takılmadan ağa kolayca bağlanabilirler.
- **Wep;** Open Security ve Wep en çok kullanılan modeldir. Dediğimiz gibi Open Security hiçbir güvenlik sağlamamaktadır ancak Wep güvenlik adımı olarak ortaya çıkmıştır ancak wep protokolü kablosuz ağlar için geliştirilen bir güvenlik protokolü olsa da ciddi anlamda tam bir fiyasko ve hatalar içermektedir.
- **Wpa;** Wep protokolüne alternatif olarak geliştirilmiş olan ve çok daha güçlü bir parametredir.
- **Radius;** Daha çok kurumların ve çok sayıda kullanıcısı olan sistem yöneticilerinin tercih ettiği bir güvenlik modelidir kullanıcı ile istemci arasındaki iletişimi sağlar ve kullanıcılara güvenli bir kablosuz ağ olanağı sağlar ancak bu modeli kişisel kullanıcıların teknik olarak kullanması mümkün olsa da pratikte tekli kablosuz ağlar için elverişli değildir.
- **Rsn;** Henüz çok yeni bir model olmasından kaynaklı tam olarak oturmamıştır. Wpa bu modelin temelinde yer almakla birlikte henüz piyasada kullanılan kablosuz ağ erişim

cihazları (AP) bu modeli desteklememektedir. Kısacası sistem yöneticilerinin kullanıma alanlarına girmemiş bir modeldir.

- **Wireless Gateway;** Halka açık yerlerde kullanıma sunulan internet sağlayıcılarının kurduğu bir sistemdir. Bağlanmak isteyen kullanıcılar bir defaya mahsus ağ ile kablosuz cihazlar arasında bağlantı oluşturduktan sonra aldıkları onay ile internete çıkabilmektedir. Ülkemizde bu modeli yaygın olarak kullanan firmaların başında Türk Telekom (TT Net) gelmektedir ve Amerika başta olmak üzere dünyada birçok firma bu modeli kullanmaktadır. Ancak bu sistem tahmin edileceği üzere kendi içerisinde birçok açık barındırmaktadır
- **Kurumlara Özel Çözümler;** İlk zamanlar güvenli bir model olarak kullanıma sunulan Wep modeli sanılanın aksine telafi edilemeyen güvenlik açıkları barındırmasından dolayı firmalar kendi önlemleri farklı opsiyonlar ile almaya çalıştılar ve Cisco gibi uluslararası firmalar kendilerine özgü güvenlik önlemleri içeren Access Point'ler ürettiler. Bu tür önlemler geniş çaplı kullanıcılar tarafından kullanılarak tecrübe edilemediği ve olası yaşanacak sorunların tespit edilmesi için bir zaman sorunu olmasından kaynaklı olarak tamamen güvenilir diyemeyiz. Ancak geliştirilen birçok sistem mantık hataları içerirken henüz kullanıma sunulanlarında güvenlik gereksinimi olarak ciddi bakılamaz.

3.5.5.4 Kablosuz Ağlara Sızmaları Önleyici Tedbirler

- Parola politikalarını analiz ederek ağ üzerindeki güvenlik duvarı tarafında gerekli önlemleri alabilecek çalışmayı yapmak.
- Ağ üzerinde güvenlik testleri yapılarak sniffing işlemlerinin tespitinin yapılması için dinleme araçları kullanılmalıdır.
- Sistem yöneticilerinin, erişim hakları ve protokolleri güvenliği ve şifrelerin güvenliğinin sağlanması amacıyla gereksiz servislerin kapatılması gibi ayarları yapması
- WEP şifrelemede en az 128 bit şifreleme tercih edilmelidir
- İşletim sistemleri ile kullanılan programlara ait güvenlik ve sistem güncelleştirmelerinin düzenli olarak kontrol edilmesi bunların en son sürüm olmasına dikkat edilmesi.
- Kullanılmadığı zamanlarda kablosuz erişim noktalarının yayınlarının kapatılması.

- Son kullanıcıların periyodik aralıklar ile modem şifrelerinin güncelleştirilmesi huşunda gerekli bilgilendirmelerin yapılması.
- Web ortamında tam güvenliğin hiçbir zaman sağlanamayacağı kesinlikle unutulmamalıdır.
- Her türlü hacking saldırılarının hukuki bir yaptırımı olacağı konusunda kullanıcıların bilinçlendirilmesi.

Kablosuz ağlara karşın yapılacak saldırıların önlenmesine dair paylaşılan temel önlemlerin uygulamaya konulması durumunda kablosuz ağ erişimlerine yapılan saldırıların çok büyük oranda önüne geçileceği ve bununla birlikte yerel ağların korunması önemli ölçüde sağlanmış olacaktır.

3.6 İşletim Sistemi Güvenliği

Windows işletim sistemleri genel olarak tüm dünyada bilgisayar olarak adlandırılan akıllı makinelerin üzerinde yüklü olarak insanların kullanımına sunulmuş bir işletim sistemi olmasından kaynaklı olarak da sistemin güvenliğinin sağlayıcı önlemler alınması kullanıcıların kişisel ve kurumsal amaçlı kullanımlarında hayati derecede önem arz etmektedir.

Bu nedenledir ki işletim sistemimiz için alınması ve hatta almamız gereken önlemler vardır be bu önlerin her geçen gün önemin daha da artması neticesinde daha çok ve daha sorunsuz güvenlik önleyici adımlar atmamız gerektedir. İşletim sistemimiz için aldığımız alacağımız güvenlik önlemlerinin daha fazla ne kadar artırabilir olduğunu bu bölümde anlamaya çalışabiliriz.

3.6.1 Windows'un Temel Güvenlik Önlemleri

Bilgisayarların ve işletim sistemlerinin güvenliğinden söz ederken yönetici konumunda olan kişiler olası güvenlik açıklarını fark etmekte ve bunlara karşın önlemler almaktadırlar. Ancak alınan önlemlere rağmen gerçek hayatta çok daha tehlikeli saldırılar ile karşılaşılabilmektedir.

Temel güvenlik önlemi olarak kullandığımız işletim sistemlerimiz için alacağımız önlemlerin öncesinde bilgisayar ve benzer cihazlarımızı daha çok internete bağlanmak için kullandığımızı baz alarak evvela internet güvenliğimizi sağlamakla başlamalıyız ve önlemlerimizi bu temelde almalıyız zira güvenlik önlemi almadan internete bağlantı yaptığımız her an bilgisayarımızın dolayısı ile işletim sistemlerimizin zararlı yazılımlar ve programlardan zarar görmesi kaçınılmazdır.

Kişisel güvenlik açığı ve tehditlerinin başında internete girmek için kullandığımız modemler gelmektedir. Bu cihazlar biz kişisel kullanıcıların dış dünyaya açılmamızı sağlayan kapımızdır bu nedenle modem güveliği konusunda hassas davranmalı ve modemimizin fabrikasyon güvenlik tedbirlerinin dışında kişisel bilgimiz ile alabileceğimiz tüm önlemleri almalı ve dışarından bizim iznimiz olmadan modemimiz üzerinde herhangi bir değişikliğe imkân vermeden gerekli tedbirleri almalıyız.

Bir diğer önemli güvenlik tedbiri de kullandığımız işletim sistemlerinin orijinal olmasıdır. Biz kişisel kullanıcılar genellikle bilgisayar ve benzeri bir cihaz aldığımızda maliyeti düşürmesi için en başta vazgeçtiğimiz sistemin ana parçası olan işletim sistemleridir ve birçoğumuz maalesef işletim sistemleri olmayan (Freedos ya da toplama) bilgisayarlar alıyoruz.

Ancak işletim sistemleri orijinal olmayan bilgisayarlar sizi hem yasal açıdan çok zor bir duruma sokar hem de içinde bulunan bir malware (zararlı yazılım) sayesinde tüm bilgilerinizi bilmediğiniz insanların eline verebilirsiniz. Bu nedenle bilgisayar alırken işletim sistemi de satın almanız en güvenli yoldur

- Tehdit örnekleri
- Çeşitli Bilgi Güvenliği Riskleri
- Pareto Prensibi

- **Tehdit Örnekleri**

- Bilgisayar veya bilgisayar özelliği olan cihazların donanım bileşenlerinin açık ve tozlu ortamlarda bulunması (nem güneş ışığı ve ortamın aşırı sıcaklığı).

- Kullanılan yazılımlardaki güvenlik açıklarının giderilmemesi.
- Verilerin bulunduğu dosyaların ele geçirilmesi.

3.6.1.1 Çeşitli Bilgi Güvenliği Riskleri

Çizelge 3.1 Güvenlik riskleri (İnt. Kyn. 7).

TEHDİT	BİLGİ VARLIĞI/AÇIKLIK	RİSK
Servis dışı bırakma saldırıları	Kurumun web sitesi	Web servisinin işlevsiz hale gelmesi iş gücü ve maddi kayıp
Beşerî iş gücü zayıflıkları	USB belleklerin kullanımına ilişkin kural belirlenmemesi/taşıma kolaylığı	Kurum envanterinde kayıtlı olan kopyalama aygıtlarının kaybolması
Sistem odasının fiziki koşullarının ve havalandırma sistemlerinin arızalanması	Sunuculara ait hafıza bileşenleri/sınırlı kullanım ömrü	Sunucu arızalanması/Sunucu bileşenlerinin kurum dışına çıkarılması
Sistem yöneticilerinin yoğun çalışması	Güvenlik duvarı(firewall)/Kural listesi	Kullanıcı hataları/Kontrolsüz açık erişim

3.6.2 Fiziksel Güvenlik

Bilgisayara, kullanım hakkı olan kullanıcılar dışında hiç kimsenin fiziksel olarak erişememesi ve kullanıcıların da fiziksel olarak bir zarar vermesinin engellenmesi, alınması gerek önlemlerin başında gelmektedir. Bu önlemlerin düzeyi kurumun ve kişisel kullanıcıların stratejik konumuna bağlı olarak belirlenmelidir. Kullanıcıları rahatsız etmeyecek düzeyde ama bilgisayarın depoladığı bilgi ve verdiği servislerin önemine bağlı olarak ayarlanmalıdır.

Gerekli güvenlik önlemleri farklı yollardan ve farklı araçlardan da sağlanabilmektedir. Örneğin, kritik çalışmalar yapan birçok kamu kurumu ve özel şirket sistem odalarının kapılarında biometrik cihazlar kullanmakta ve kameralarla içeriyi izlemektedir. Kurumsal güvenlik önlemleri kurum ve kurum çalışanlarının bilgisayar ve sistem güvenliği için önemli olduğu kadar kişisel kullanıcı olarak ev ve işyerlerinde kendi özel hayatlarının bir parçası olarak kullandıkları bilgisayarların güvenliği de en az

kurumların bilgisayar güvenliği kadar hayati öneme haizdir. Bu nedenlerden dolayıdır ki alınması gereken önlemlere dair birkaç yol aşağıda sırlanmıştır.

➢ **Bilgisayar açılış işlemi kesinlikle sabit diskten olmalı;** Bilgisayarların güvenliğini tehdit eden virüs ve benzeri birçok tehdit fiziksel yollarla bulaşmaktadır. Bu nedenledir ki dış müdahalelere maruz kalabilir olması öngörülerek bilgisayarların açılış işlemleri mutlaka sabit disk(Hdd) üzerinden gerçekleşmelidir.

Dış müdahalelere maruz kalabilen ve yabancı kişilerin kullanılabileceği ortamlarda bulunan bilgisayarların açılış işlemleri Cd-Rom ya da Flash Bellek(Usb) üzerinden gerçekleşmesi durumunda işletim sisteminin üzerine yeni bir işletim sistemi yüklenebilecektir. Günümüz bilgisayar teknolojilerinde artık kullanılmayan ama halen bilgisayar kasalarının üzerinde sürücüsü bulunan ve sabit disk olarak bilinen flopy disk(disket) ile açılış disketi aracılığıyla bilgisayar içerisindeki bilgiler zamanla hasar görebilmektedir.

➢ **Disk yapılandırması NTFS olmalı;** Disk yapılandırması Windows işletim sistemlerinde FAT32 ya da NTFS olarak ayrılmaktadır. FAT32 disk yapılandırmalarını Windows 9x sürümleri kullanmaktadır. Windows 2000/XP her ikisini de kullanabilmekte, Windows NT ise sadece NTFS kullanmaktadır. NTFS yapılandırılmış sabit disklerde kullanıcı düzeyinde dosya ve dizinlere erişim hakkı verilebiliyor olması kullanıcıların bilinçsizce ya da bilinçli olarak sistem dosyalarına ya da kişisel dosyalara verecekleri zararları engelleme şansı vermektedir.

➢ **Fat32 ve Nfts arasındaki Farklar**

- FAT32 sadece 32GB alanları destekler. Bu nedenle 32GB tan büyük disklerde ise diski 32'lik parçalara bölmek gerekir. Ancak NTFS Terabayt a varan büyük disk boyutlarını destekler**.**
- NTFS te dosya sıkıştırması ve dosya şifreleme bulunur. Birde NTFS dosya sistemi erişim listesi ile çalışır(axesslist). Ancak FAT32 de bu özellikler yoktur.
- Bu özellikler NTFS i network ortamında çok güvenli hale getirir. Yani bir kullanıcı bir dosya ya erişmek istediğinde ilk baş erişim listesine kullanıcının hakkı olup

olmadığına bakılır. Eğer gerekli izni varsa dosya ya erişir. Birde veri şifreleme ile dosyalar şifrelenir ve başka kullanıcılar tarafından okunamaz hale getirilebilir. Bu özellikler NTFS i network ortamında güvenli kılan özelliklerdir.

Son olarak bilgisayar ve benzeri cihazların fiziksel güvenliklerinin mutlaka sağlanmasına dair yukarıda da yaptığım açıklamaların devamı olarak birkaç başlık altında alınacak önlemlerden bilgiler aşağıda paylaşılmıştır.

- Kilitli Sistem odası ve Kilitli sunucu dolapları

✓ Sistem odasının ve sunucu kabinlerinin anahtarları kimde?
✓ Sistem odası güvenlik kameraları ile izleniyor mu?
✓ Sistem bileşenlerine doğrudan usb bellek, taşınabilir hdd ve cd-room takılabiliyor mu?

- Akıllı Kart ve Biyometrik sistemler

✓ Erişim yetkisi olanların listesi?
✓ Kim ya da kimler tarafından yetkilendiriliyor?
✓ Kayıtları kimler inceliyor?

- Sistem Yedekleri

✓ Yedekleme üniteleri güvenlikli ortamda mı?
✓ Alınmış olan yedekler kullanılabilir durumda mı?

- Hata Riski Toleransı

✓ Oluşabilecek olası arızalara karşın diskler optimum kullanıma göre ayarlanmış mı?
✓ Sunucu ve sunucu bileşenleri yedeklenmiş olarak yapılandırışmış mı?
✓ Doğal afetlere karşın önlemler alınmış mı?

3.6.2.1 Fiziksel Güvenlik Önlemi Alınmayan Ortamlardaki Riskler

- Yönetici şifresinin değiştirilmesi
- Yönetici şifrelerinin çalınması
- Önemli işletim sistemleri dosyalarının değiştirilmesi
- Kritik bilgileri çalınması
- Servis dışı bırakma
- SID sahteciliği (SID Spoofing)

3.7 Topoloji Güvenliği

Bilgisayarlarımızın bağlı bulunduğu ağların genel olarak son kullanıcıya ulaşan kısımların sistemsel olarak anlatımına topoloji diyoruz. Topoloji dediğimiz an aklımıza ilk gelen kesinlikle network ağımızın alt yapısındaki tüm donanımsal ve fiziksel çalışmanın aşamaları gelmelidir. Salt olarak sadece interneti birkaç kablo aracılığı ile son kullanıcılara ulaşıldığı düşünülmemeli ve ağ topolojisi dendiği zaman bir nevi internetin mutfağı olarak nitelendirilmelidir.

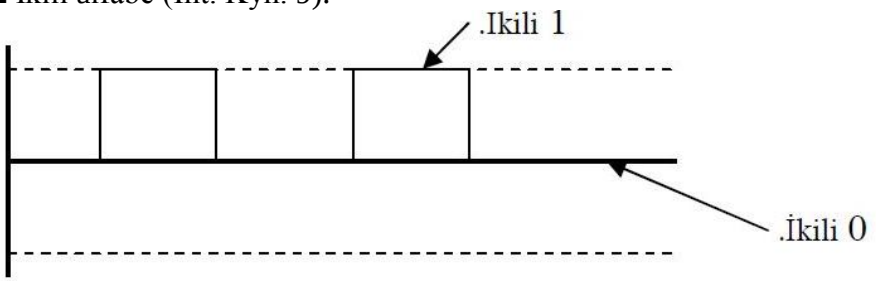
Sonuç olarak her sistemin bir çalışma evresi ve bu çalışma evrelerinin de birer kendi içerisinde güvenlik zafiyetleri olabileceği göz önünde bulundurarak topolojimizi oluşturan tüm evrelerim güvenliği üzerinde de hassasiyetle durmalıyız. Bu nedenler tüm network alt yapısı ile son kullanıcılara kadar ulaşan sistemin evreleri için alacağımızın ve dahi alınan tüm önlemlere totalde topoloji güvenliği denmektedir.

3.7.1 Ağ İletimin Anlaşılması

- **Sayısal iletişim;** aracı olarak ilk kullanılan telgrafa ait iletişim dili olan mors alfabesine benzer olan bir kodlamadır. Birbirinden farklı karakterleri temsil eden dizinlerin temsil eden farklı darbe izleri kullanır.

Analog sistemlerde göre bu sistemde kullanılan darbeli alfaben gürültü ortamlardan etkilenmesine rağmen analog iletişime göre daha verimlidir ve ikili alfabeye örnek çizim çizelge 3.2'de gösterilmiştir.

Çizelge 3.2 İkili alfabe (İnt. Kyn. 9).



- **Elektromanyetik parazit;** Elektromanyetik gürültüyü değişken akım taşıyan iletişim devreleri taşır. Eğer bu manyetik alan herhangi bir iletken tarafından kesilirse, bu iletken geçen alanın da etkisi ile iletken alanın gücü ile orantılı elektriksel işaret indüklenir. Bu şekilde yapılan kablolama sistemlerinde yapılacak olan herhangi bir mandallama durumundan ağ üzerinde geçen trafiğin dinlenmesi olasıdır. Genel olarak ağ topolojilerinde kullanılan kablolamalarda fiyatının ucuz olmasından da dolayı UTP (unshided twisted pair) tipi kablo kullanılır.

- **Fiber Optik Kablo:** Fiber optik kabloma teknolojisinde bilgi ışığa çevrilerek iletilir. Fiber optik kablolama, kampüs network'leri benzeri yapılarda sistem odaları içerisinde kurulan ve internet alt yapısının dağıtım merkezi olan omurga olarak adlandırılan anahtarlamalara, ISS'lerin(internet servis sağlayıcısı) sağlandığı bağlantılarda kullanılır zira kenar nokta olarak tabir edilen merkeze uzak birimlere de kullanılması son zamanlarda artarak devam etmektedir. Bu kablolama türünü pahalı olması ve dış etkenlere maruz kalması daha olası olacağı için ve bu müdahaleler sonucu oluşan hasarın onarımının zaman ve parasal olarak karşılanması ek külfetler getirdiğinden dolayı halen internet taşıma işlemleri utp tipi kablolar kullanılarak internet erişimi sağlanmaktadır.

3.7.2 Topoloji Güvenliği

Topoloji ağ ortamlarında kullanılan fiziksel bağlantıların ve araçların iletişim kuralları için kullanmakla birlikte ağı sistemin birbirinden farklı iletişim kuralları vardır bu sistemi oluşturan ağ cihazlarının da kendi aralarında yaptığı haberleşme trafiğine ait kuralları ifade etmek içinde kullanılan topolojinin kendine ait güvenlik gereksinimleri ve kuralları vardır.

Topolojisi yani ağ iletim hattı güvenli olmayan hiçbir ağ alt yapısının ve dahi kullanıcıların internet ve bilgisayar güvenliğinden söz edemeyiz. Bu nedenle topolojimizi oluşturan ağ yapımızın içerisindeki tüm parçaların güvenliğini sağlayacak önlemler almalıyız. Alınacak önlemlerin başında ağ sistematiğini oluşturan alt yapının ve donanım parçalarının güvenliğidir.

Unutulmamalıdır ki ağ topolojimizde oluşacak herhangi bir güvenlik açığı tüm ağ iletim hattını etkilemekle birlikte tüm kullanıcılarında ağ ve bilgisayar güvenliğini etkiyecektir. Bu nedenlerdir ki topolojimizin güvenliği kurumsal olarak hayati önem arz etmekle birlikte kişisel kullanıcılar içinde bilgisayar güvenlikleri açısından önem arz etmektedir. Topolojimiz için alacağımız önlemlerden bazıları aşağıda anlatılmaya çalışılmıştır.

3.7.2.1 Ethernet İletişim

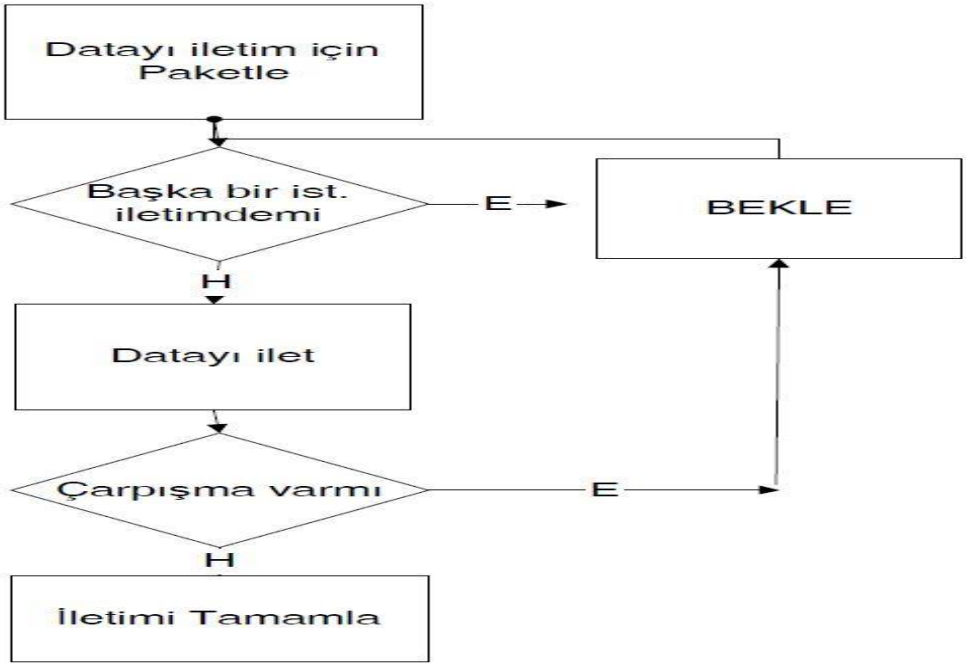
Ethernet en popüler yerel ağ topolojisidir. Değişik türdeki neredeyse tüm kablo çeşitleri ile çalışabilmesi, tak çalıştır özelliği ve daha da önemlisi çok düşük maliyeti ile en çok tercih edilen iletişim topolojisidir. Haberleşme protokolü CSMA/CD (Carrier Sense Multiple Access/ Collision Deteckt)'dir.

- **Taşıyıcı Anlama (Carrier Sense):** Ethernet'in kendine ait bir çalışma prensibi vardır bu prensibe göre Ethernet her bir istasyon üzerinde iletim olup olmadığını anlamak için hattı dinler. Bunun anlamı her bir istasyon hattını gözleyebilmektedir ve nedeni de hattın boş olduğu bir anda veri göndermeye başlamasıdır.

➢ **Çoklu Erişim (Multiple Access):** Birden fazla istasyonun aynı ağa bağlanmasıdır. Bu yapıdaki ağlar, istasyonlar tarafından paylaşılarak veri iletiminde kullanılabilirler. Ayrıca herhangi bir yeni ağ eklenmesi durumundan kolaylıklar farklı ağlar eklenebilir.

➢ **Çarpışma Bulma (Collision Detection):** Farklı ağların aynı anda veri gönderip göndermediklerini kontrol ederek olası çarpışmaların önüne geçmeye çalışan anlaşmalardır. Farklı ağların, istasyonların aynı anda birbirlerine doğru veri göndermeleri sonucunda çarpışma olacak ve çarpışma neticesinde istasyonlar üzerindeki verilerde kayıplar olacaktır. Ethernet CSMA/CD protokolünün çalışma algoritmasına örnek çizim, çizelge 3.3'de gösterilmiştir.

Çizelge 3.3 Ethernet CSMA/CD protokolünün çalışma algoritması (İnt. Kyn. 10).



3.7.3 Temel Ağ Donanımı

Ağ oluşturan donanımların güvenlik açıklarını, güvenlik ihlallerini bilmek ve buna göre önlemler alabilmek için ağ üzerindeki donanımların çalışma prensiplerinin bilinmesi gerekmektedir. Ağ oluşturan donanımların başta gelenleri Tekrarlayıcılar (repeaters), hublar, switchs(anahtarlar), köprüler(bridges) ve yönlendiriciler (routerlar)'dir.

3.7.3.1 Anahtarlama (Switching)

OSI başvuru modelinin 2. Katmanında mac tabanlı olarak çalışan topoloji aygıtlarıdır. Bu cihazlar kampüs ve daha büyük network alt yapısına sahip olan topolojilerin olmazsa olmazlarıdır. Çalışma mantığı tüm anahtarlama cihazları ile aynı olarak görülse de switchler, topolojinin ve ağın güvenliğinin sağlanmasında en etken donanım parçasıdır. Genellikle kampüs ağları olarak adlandırdığımız yapılarda kenar nokta cihazları olarak kullanılan ve merkez omurga üzerindeki dağıtımın en uç noktalara değişik kurallar çerçevesinde aktarılması görevini gören switchleri, hub gibi internet dağıtıcı cihazlarından ayıran en önemli özellik kendi üzerindeki interneti belirlenen kurallar çerçevesinde kullanıcılara iletilmesi görevini de görmeleridir.

ACL (Acess list) cihaz üzerine gelen verileri iletmek, yönlendirmek ve silmek için kullanılan ara yüz yazılımıdır. Switchlerin genel olarak çalıştığı osi katmanı, layer-2 olarak kabul edilse de günümüzde maliyeti açısından tercih edilmesi oldukça zor olan layer-3 seviye olarak ip tabanlı çalışan switchlerinde kullanımı yaygınlaşmaya başlamıştır. Layer-3 switchler kaynak ve hedefin IP adresi olduğu üst katman portlarından oluşur. Layer-3 switchlerde ACL oluştururken her bir port'a satır şeklide kurallar yazılır ve listeye tanımlanır. Portlar üzerinde ki tanımlanan kurallar gelen verileri iletir ya da geri çevirirler (permit, deny).

Resim 3.11 Anahtarlama cihazı (İnt. Kyn. 11).

Ağ Anahtarı (Switch):

Switchler yani ağ anahtarları network topolojilerinin vazgeçilmez ve önemli donanım parçalarıdır. Herhangi bir topoloji oluşumunda önemli olan merkez noktada bulunan dağıtım noktalarından çıkan internetin en uç noktalara aynı kalitede, hızda ve güvenli bir şekilde iletilmesidir. Kampüs ağları gibi dağınık yerleşkelere sahip topolojilerde switchlerin tercih edilmesinin nedenlerinin başında switchlerin, OSI referans modeli içerisindeki katmanlara uyumlu olmasıdır.

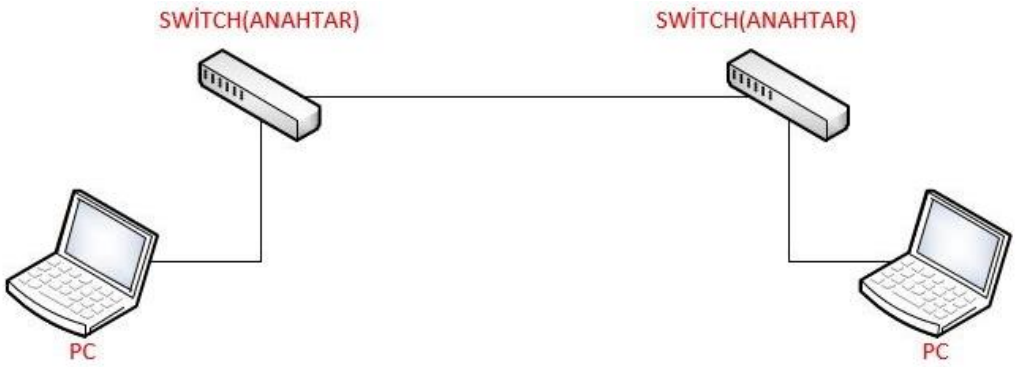
Aynı zamanda *Layer 2* ve *Layer 3* uygunluğuna sahip switchler yönetibilir switchlerdir ve buda tercih nedenlerindendir. Ayrıca kullanım amacı aynı fakat birbirinden tamamen farklı olan hub'ların yerine de tercih edilmelerinin birden fazla nedenleri vardır bunların başında ağ üzerinde dağıtılması gereken verinin hub'larda aynı anda farklı noktalara dağıtılmasının mümkün olmaması ama bu dağıtımın swicthlerde kesintisiz ve aynı hızla gerçekleşebiliyor olmasıdır.

Örnekleyecek olursak Hub'ları 4 taraflı bir kavşak olarak düşünürsek ve bu kavşaktan aynı anda farklı yönlere giden araçların hareket etmesi sonucu bir kaza yaşanması kaçınılmazdır ancak bu durum switchlerde böyle değildir kavşakta bulunan tüm araçlar aynı anda farklı yönlere hızlarını kesmeden ve kazaya uğramadan gidebileceklerdir.

Örnekleyecek olursak; 10 Gbps sahip bant genişliğini 8 port'lu bir hum her bir portuna paylaşım yaparak dağıtırken, 24 portlu bir switch tüm bant genişliğini her bir portuna 10 Gbps olacak şekilde dağıtabilmektedir.

Switch tercih edilmesinden nedenlerinden birkaçını aşağıdaki gibi sıralayabiliriz.

- Anahtarla birbirine bağlı iki bilgisayarlık ağ oluşturma
- Anahtar için ad ayarlama
- Cihaz yapılandırmasına erişimi sınırlama
- Büyük başlık mesajlarını yapılandırma
- Yapılandırmayı kaydetme

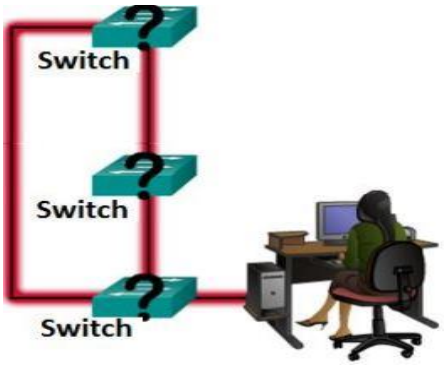


Resim 3.12 Anahtarlama visio çizimi.

Ağ Anahtarlarının Adları:

Adlar için bazı adlandırma kuralları şunlardır;

- Harf ile başlamalı
- Boşluk içermemeli
- Harf veya sayı ile bitmeli
- Sadece harf, sayı ve tireler kullanılmalı
- Uzunluğu 64 karakterden az olmalı



Resim 3.13 Anahtarlama (İnt. Kyn. 13)

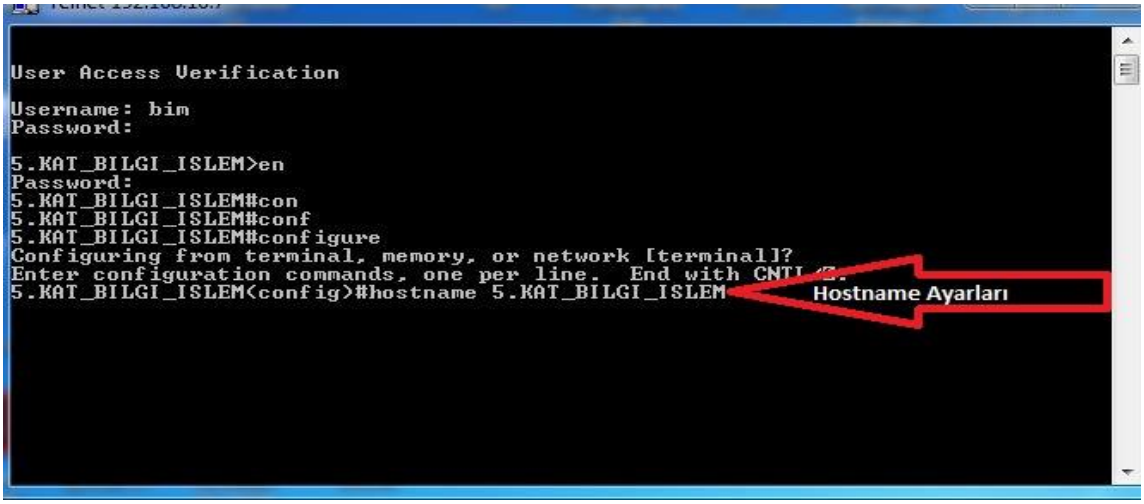
Ağ Anahtarlarının Adları ve Yapılandırılması:

Anahtarlama cihazlarının yapılandırılması yapılırken mutlaka cihazlara ait isimlendirme yapılmalıdır (Hostname). Yapılacak isimlendirme, cihazın bulunduğu binada ya da kabinette başka bir cihaz olmayacaksa bulunduğu binanın, yerleşkenin ismi de

verilebilir ya da sadece kenar nokta cihazı olarak kullanılan birimlerinde isimleri verilebilir.

Resim 3.14 Switch giriş ekranı 1.

Hostname: Host adları cihazların ağ veya internet üzerinden ağ yöneticileri tarafından tanımlanmasına olanak sağlar.

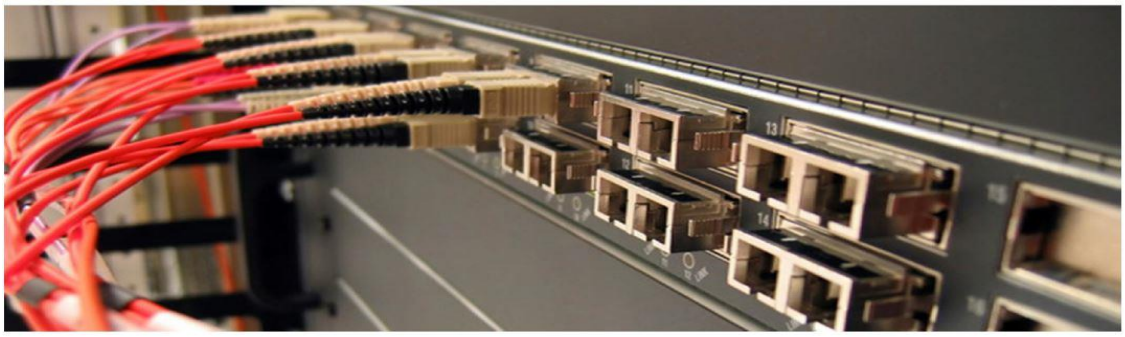


Resim 3.15 Switch configrasyon ekranı.

3.7.3.2 Omurga Anahtarlama (Backbone)

Yönlendirme cihazların OSI başvuru modelinin 3.katmanı olan network ağ cihazlarıdır. Yönlendiriciler kendi işletim sistemlerine sahiptirler dolayısıyla programlanabilir ve gerekli yapılandırma işlemleri gerçekleştirilebilir.

Yönlendirici *(router)* olarak da bilinen LAN-WAN, WAN-LAN bağlantılarda veya VLAN'lar arası bağlantılarda kullanılır. Üzerlerinden genel olarak LAN ve WAN bağlantıları için kullanılan, en az birer adet LAN ve WAN bağlantı portlar bulunur. Yönlendiricilerde çalışan ROS (router operating system) önemlidir zira cihazın üzerindeki yönlendirici işletim sistemi (Ros) hem kendi görevini yerine getirebilmeli hem de ağ üzerinde tanımlanmış olan protokol kümesini destekliyor olması gerekir. Bu nedenle TCP/IP protokolü kullanılacak ağlarda yönlendirici üzerinde IP protokolü yüklü olmalıdır.



Resim 3.16 Anahtarlama cihazı (İnt. Kyn. 13).

3.7.4 Ağ Cihazlarında Güvenlik

Bir ağın(network) güvenliği dikkat edilmesi gereken önemli bir konudur. Ağ güvenliği için çoğu zaman güvenlik duvarları(firewall) yetersiz kalmaktadır. Güvenli bir ağda çalışmak tüm cihazlar ve kullanıcılar açısından gerekli önlemler alınmalıdır. Ayrıca güvenliğin sürekli ve kesintisiz olması önemli bir husustur.

Ağ cihazlarının ayarlanması, yönetimi ve kontrolü aşağıdaki bağlantı yolları ile sağlanabilmektedir. Son olarak default(varsayılan) ip adresini herhangi bir browser' a (tarayıcı) yazdıktan sonra açılan modem ara yüz giriş ekranından, modemimize ait giriş bilgileri ile giriş yapıyoruz ve aşağıdaki örnekte görüldüğü gibi ilgili menülerden mac filtreleme işlemini yapıyoruz.

- HTTP protokolü ile
- Telnet veya SSH ile

- SNMP protokolü ile
- TFTP veya FTP ile
- Konsol portuyla

Ağ cihazlarına erişim güvenliğinde bağlantı yollarından biri olan konsol portu aracılığı ile yapılan bağlantılar fiziksel bağlantı olduğu için diğer bağlantı yollarına göre daha güvenlidir diyebiliriz. Diğer bağlantı yolları TCP/IP protokolleri ile olduğundan ve bu protokollerin kendi içlerinde barındırdığı zafiyetlerden doğacak olan güvenlik açıkları olacağından önlem alınması cihazın ve ağın güvenliği açısından önelidir.

3.7.4.1 Ağ da Fiziksel Güvenlik

Ağ cihazlarına kolaylıkla erişebilen saldırganların aynı zamanda cihazlara fiziksek olarak erişebilecekleri ve konsol port'u üzerinden cihazlara erişim kurabilecekleri göz ardı edilmemelidir.

Cihazlara fiziksel olarak erişebilen saldırgan data kablolarını tab (özel ekipmanla kablo erişimi) ederek hattı dinleyebilir ve hat üzerinde ağa trafik gönderebilir. Kabul edilmelidir ki bir ağ, en güçlü güvenlik duvarları ve güvenliği sağlayıcı yazılımların son sürümleri ile korunuyor olsa ve yönetilse de fiziksel olarak güvenlik önlemleri alınmayan topolojilerin güvenli olduğundan söz edilmesi yüzde yüz mümkün değildir. Alınacak bazı fiziksel güvenlik önlemlerine aşağıda yer verilmiştir.

- Cihazlar sadece ağ yöneticisinin veya onun yardımcısının açabileceği kilitli odalarda tutulmalıdır. Oda ayırmanın mümkün olmadığı yerlerde özel kilitli dolaplar (kabinetler) içine konmalıdır.
- Cihazlara fiziksel olarak kimin ve ne zaman eriştiğini belirten erişim listeleri tutulmalı (*access auditing*) ve bu listeler sık sık güncellenmelidir.
- Kablolar tek tek etiketlenmeli ve kayıtları tutulmalıdır. Kullanılmayan kablolar devre dışı bırakılmalıdır.
- Cihazların yakınına güvenlik bilgileri (şifre, IP adresi) gibi bilgiler yapıştırılmamalı ve gizli tutulmalıdır.

- Aktif cihazların elektriği aldığı güç kaynaklarının yeri belirlenmeli ve saldırganın bu güç kaynaklarını kesmesi engellenmelidir. Devamlı güç kaynaklarına (ups) yatırım yapılmalıdır.
- Aktif cihazların fiziksel erişime açık olduğu yerlerde saldırganın güç kablosunu çıkartmasını engellemek için cihazın üstünde çeşitli aparatlar kullanmalı, güç kablosunu gözden ırak tutmalı, mümkünse uzakta ve fiziksel güvenliği sağlanan bir prize bağlanmalıdır.
- Her ne kadar aktif cihazların çalınması pek olası olmasa da bu tür olayları engellemek için mümkünse çeşitli kilit ve alarm mekanizmaları kullanılmalıdır.

3.8 Güvenlik Duvarı (Fırewall)

Güvenlik duvarları özel ağ alanlarını internet gibi herkese açık olan ağların gelen ve giden trafiğini sınırlandıran özel bir yazılım ve cihaz uygulamasıdır. Özel ağ üzerinden erişimi güvenlik zafiyeti doğuracak servislerin diretk olarak özel ağ alanına erişmesini ve internete çıkış yapmasını kurallar(policy) çerçevesinde sınırlandırmada ve engellemede kullanılabilir. Güvenlik duvarları genel olarak 3 ana başlıktan ve ara yüzlerden oluşur.

Bunlardan biri dışa açık olan internet biri iç ağ olarak sadece iç ağ üzerinden erişilebilen alan olan intranet diğeri de sistem içerisindeki sunucuların özel alana giriş yapmasını sağlayan DMZ (Arındırılmış bölge) alanıdır.

Sunucuların DMZ(özel alan) üzerinden dışarıya açılmasını sağlamaktaki asıl amaç sunucuların kullandıkları bazı servislerin özel ağ yapısına tehdit arz eden uygulamalardan ve servislerden oluşmasıdır. Ağ yapısı büyük giderek büyüyen yapılar ile ağ üzerinde bulunan kullanıcı sayılarının binlerle (kampüs ağları gibi) ifade edilen ağlarda dışa bağımlı uygulamaların ve ihtiyaçların artmasından dolayı güvenlik duvarlarının yönetimi zorlaşacaktır. Güvenlik duvarlarının yönetimi ve takibi sadece ağ yöneticileri tarafından yürütülür ve diğer ip'lere dolayısıyla kullanıcılara bu alan kesinlikle kapatılır.

Güvenlik duvarları yazılımları her ne kadar karmaşık ve karışık görünse de ağ yöneticileri tarafından oluşturulan kurallar olabildiğince basitleştirilerek kolay ve anlaşılır bir ara yüz ile yapılması tavsiye edilir. Güvenlik duvarı aracılığı ile belirli periyotlarla ağ üzerinden geçen trafiğin izlenmesi ve analiz edilerek gerekli politika güncellemeleri yapılarak raporlaştırılması gerçekleştirilmelidir.

Güvenlik duvarları ağ katmanında çalışmakta olduğundan unutulmamalıdır ki, uygulama katmanında çalışan ve gelen atakları tespit edip engelleyemez. IP ve port seviyesindeki kuralları engelleri aşıp gelen saldırıların geçilmesi güvenlik duvarının tamamen devrenden çıkartarak işlevsiz hale getirecektir.

Uygulama seviyesinden gelen zararlı yazılımları IPS (Intrution Prevention System) etkisiz hale getirerek saldırıyı bertaraf edebilir. Bundan dolayı güvenli bir ağ için bu iki sistem arka arkaya kullanılır. Güvenliğin sağlanması sadece bu cihazların konfigürasyonuna bağlı değildir. Sistem yöneticilerinin ve kullanıcıların eğitilmesi, spam filtreleme sistemleri, anti virüs ve gerektiği takdirde veri tabanı güvenlik duvarları da kullanılmalıdır.

Güvenlik duvarlarının bir diğer işlevide her geçen gün giderek azalan IPV4 adreslerini bir nevi ağ geçidi görevi de gördüğü için legal yollardan iç ağ üzerinden sanallaştırarak kullanıcılara sanal Ip'ler dağıtabilir. Güvenlik duvarı bu işi NAT (Network Address Translation-Ip Adresi Yönlendirme) işlemi ile gerçekleştirmektedir. Dış dünyaya tek bir gerçek ip ile çıkılırken içerde sanal Ip'ler dağıtır. Bu şekilde hem IPV4 adreslerinden tasarruf edilmiş hem de iç ağdaki sanal ip kullanıcıları dışa karşı korunmuş olacaktır.

Günümüzdeki güvenlik duvarları bir başka teknoloji olan VPN (Virtual Private Network) ihtiyacını da karşılamaktadır. VPN teknolojisinde uzak bağlantılarda ister iki güvenlik duvarı arasında (site to site VPN) ister bir kullanıcının kullanacağı sertifika ile tek bir bilgisayardan (client to site VPN) sisteme erişimi kripto ile tünellenmiş şekilde iç ağa erişebilir.

3.8.1 Güvenlik Duvarı Türleri

Güvenlik duvarları yazılım ve donanım tabanlı olarak ayrıştırılabilir. Ancak donanımı olmayan yazılım ve yazılımı olmayan donanım olamayacağı için böyle bir ayrıştırmaya girmek aslında çokta mantıklı değildir.

Yazılım ve donanım tabanlı olarak ayrıştırılmasının nedeni genellikle freebsd(Pfsense) olan ve herhangi bir donanıma ihtiyaç duymadan gerçek veya sanal bir sunucu üzerinden de çalışabilen yazılımların olmasından dolayıdır. Donanım tabanlı olan güvenlik duvarları ise yine üretici firmaları tarafından cihaz ile birlikte donanımı tamamlayıcı işlevi olan yazılımları ile birlikte kullanıcılara sunulan uygulamalardır.
Kendi içinde ayrıştırılan güvenlik duvarları aşağıda anlatılmaktadır.

3.8.1.1 Yazılım Tabanlı Güvenlik Duvarları

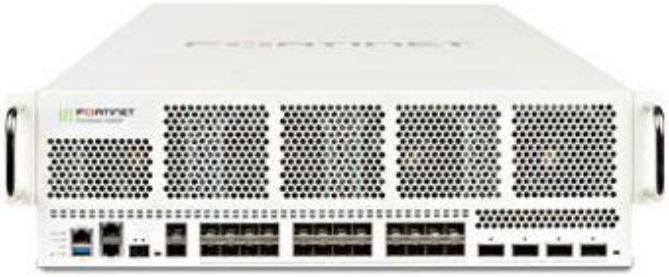
Yazılım tabanlı güvenlik duvarları genellikle açık kaynak kodlu yazılımlardır. Yazılım tabanlı güvenlik duvarları işletim sistemi tabanlı olarak çalıştıklarından dolayı her işletim sistemine uyumlu olmaya bilir.

Örneğin Windows tabanlı güvenlik duvarları Linux tabanlı işletim sistemlerine uyumlu olmadığı için çalışmayacaktır. Açık kaynak kodlu güvenlik duvarları genel olarak yine açık kaynak kodlu bir işletim sistemi olan Linux ile uyumludurlar. Açık kaynak kodlu olan güvenlik duvarları tamamen ücretsiz olup GPL (General Public License) lisansıyla dağıtırlar. GPL, FSF (Özgür Yazılım Vakfı) tarafından desteklenen ve geliştirilen kamunun kullanımına sunulan bilgisayar lisansıdır. GPL özgür ve açık kaynak kodlu pek çok yazılım tarafından kullanılmakta olup en fazla kullanılan işletim sistemi Linux'tur.

Resim 3.17 Yazılım tabanlı norton firewall örneği (İnt. Kyn. 14).

3.8.2 Donanım Tabanlı Güvenlik Duvarları

Adından da anlaşılacağı üzere donanım temelli olan güvenlik duvarlarıdır. Bu tür güvenlik duvarları yine kendisine uygun olarak geliştirilen ve içerisinde kullanıma sunulan yazılımlar ile birlikte kendilerine özgü işletim sistemleri ve ara yüz ile kullanıcılarına sunulmaktadır. İçerisinde çalışan kendisine öz kullanıcı ve ara yüz birimi yazılımlar ile desteklenen güvenlik duvarlarının arka planında çalışan tüm servisler sadece güvenlik duvarı için kullanılacak olanlardır. Donanım tabanlı güvenlik duvarlarına iki yoldan bağlantı kurulabilir bunlardan en sık kullanılanı http protokolü kullanılarak browser üzerinden sağlanan bağlantı olup bir diğeri fiziksel olarak consol portu üzerinden consol kablosu ile yapılan bağlantılardır.



Resim 3.18 Donanım tabanlı fortinet firewall örneği (İnt. Kyn.15).

3.8.2.1 Güvenlik Duvarlarının Özellikleri

Güvenlik duvarları bilgisayarlarımızı ve bilgisayarlarımızın bağlı olduğu ağları korumak için konulmuş önlemlerin ve kişisel güvenlik ayarlarımızın uygulandığı yazılımdır. Windows gibi ücretsiz ve açık kaynak olmayan işletim sistemlerinin üzerinde üretici firmaların temel düzeyde işletim sistemlerinin içerisinde olan güvenlik uygulamaları mevcuttur.

Ancak güvenlik duvarları profesyonel manada çoklu kullanıcısı olan yapılarda muhakkak kullanılmalı ve kullanılmaktadır da. Bilakis sistem yöneticileri tarafından hassasiyetle üzerinde durulan günlük ve an anlık güvenlik politikaları geliştirecek şekilde kullanıma elverişli sistemlerdir. Güvenlik duvarları aracılığı ile; bilgisayarları ve bilgisayar ağlarının güvenlik seviyeleri istenilen zaman da istenilen şekilde düzenlenebilir.

Kablosuz ağlar üzerinden ağımıza girmeye çalışan yabancılara karşı koruma kalkanı ile davetsiz misafirleri engelleyebilir. İnternet erişimi sağladığımızın cihazlar üzerinden hangi sayfalara portallara girileceğini denetleye bilir ve zararlı yazımları indirilmesini kullanılmasını engelleye bilir. Kullanıcıların belirli zaman dilimlerimde internet erişimleri kısıtlanabilir veya network ağ için bant genişliğini yoracak programların ve milyarlarca kişinin kullandığı sosyal portallara mesai saatleri içerisinde girilmesine kısmi engeller konabilir.

Kısacası güvenlik duvarı sistemleri olmayan kullanıcılar ve ağ yapıları silahsız olarak nöbet tutan askerler gibi tehlikelere karşı her an hedef olmaktan kurtulamazlar.

- **Yazılım tabanlı güvenlik duvarlarının özellikleri**

Avatanjları;

- İşletim sistemleri temelli çalıştıklarından dolayı detaylı bir şekilde raporlama işlemi yapmak oldukça kolaydır.

- Uygulama yazılımları oldukları için gerekli donanımsal destekler sağlandıktan sonra bir yerden bir yere taşıma işlemi oldukça kolaydır.

Dezavantajları;

- İşletim sistemli temelli olarak çalıştıklarından dolayı uyumlu olmadıkları işletim sistemlerinde çalışmazlar.
- İşletim sistemi üzerinde çalıştıkları için belirli periyotlar ile işletim sisteminin bakımının yapılması gerekmektedir.
- İşletim sistemleri üzerinden oluşan her türlü hatalara etkilenirler ve bu sebeple performanslarında yavaşlama olabilir.
- Her donanım uyumlu olmayabilirler.
- Kurulum süreler donanımsal güvenlik duvarlarına göre daha uzun sürmektedir.

Bu tür güvenlik duvarları kendi içlerinden açık ve kapalı kaynak kodlu yazılımlara sahip olabileceklerinden dolayı kendi aralarındaki avantaj ve dezavantaj da vardır.

- **Açık kaynak kodlu güvenlik duvarlarının avantajları;**

- Lisansları ücretsiz olduğu için herhangi bir maliyeti söz konusu değildir.
- Kaynak koduna gerekli eklentiler yapılarak, hatalar kolaylıkla tespit edilip ayıklanabilir.
- Kullanılacak ortama göre istenildiği gibi değişiklik yapılarak maksimum performans elde edilmesi sağlanabilir ve gereksiz eklentilerden kurtulabilinir.

- **Açık kaynak kodlu güvenlik duvarlarının dezavantajları;**

- Genel olarak kullanıcıları tarafından kurulu yapıldığından herhangi bir teknik destek söz konusu değildir.

➢ **Kapalı kaynak kodlu güvenlik duvarlarının avantajları;**

- Lisansı için ücret ödenip kullanıldığı için herhangi bir sorunda teknik destek alma hizmeti ve garantisi vardır.
- Belirli bir firma tarafından geliştirildiği için geliştiricileri tarafından güncellenecek olması ve güncellenen sürümün kullanma imkânına sahip olunması.

➢ **Kapalı kaynak kodlu güvenlik duvarlarının dezavantajları;**

- Kapalı kaynak kodlu yazılımların geliştirilmesini güncellemesini hatalarının giderilmesini yine üretici firma tarafından yapılacağı için üretici firmanın bu tür gereksinimleri karşılaması beklenmelidir.

- Kullanıcılar karşılaştıkları sorunlarda üretici firmadan başka hiçbir kişi ya da kuruluşlarda yardım alamaz.

➢ **Donanım tabanlı güvenlik duvarlarının özellikleri**

Avantajları;

- En bariz avantajları sadece kendileri için geliştirilmiş olan ASIC entegre devreler kullanılmış olması ve bu sayede yüksek performas gösterebilmeleri.
- Herhangi bir anlık arızada veya hatada resEtlendiğinde cihazın tekrardan kendini toplayabilmesi.
- Yedekleme sistemi olan yapılarda sorusunsuz çalışabilmesi.
- En az seviyede yazılım gereksinim duymalarından dolayı yazılımsal hataların minimum olması ve kolay çözümlenebilmesi.
- Hizmet dışı kalma durumları yazılımsallara göre yok denecek kadar azdır.
- Üretici desteği olacağı için daha çabuk ve daha kolay update edilebilir.

Dezavantajları;

- Donanımsal yeterlilikleri zamanla kaybolacaktır.
- Donanımsal yetersizliklerden dolayı fiziki olarak yeni bir cihaz alma gereksinimin doğması.
- Raporlama işlemi genel olarak daha dar kapsamlıdır.
- Spesifik saldırılara karşı korumasız olabilirler.
- Herhangi bir güncelleme durumundan cihazın resetlenmesi gerekmektedir.
- Donanımsal yenilikler ile revize edilmesinin maliyetli olması.

3.9 IP Adresi

IP (İnternet Protokolü) adresi, bir bilgisayar ağında iletişim için internet teknolojisini kullanan bir aygıtın belirleyici numarasıdır. IP adresi, o cihazın hangi servis sağlayıcısı veya ağı kullandığını ve internete hangi lokasyondan bağlandığını belirler. İnternet Servis Sağlayıcısı, internete bağlanan her cihaza benzersiz bir IP adresi tanımlar. IP adresi aynı zamanda, bir dijital aygıtın bir başka dijital aygıtla da internet aracılığıyla iletişime geçmesini sağlar.

IP adresi olan iki cihaz, internete bağlı oldukları sürece, aynı ağa bağlı olmaksızın da birbiriyle etkileşim kurabilir. Ayrıca bir internet sitesine, alan adı yerine sadece IP adresi yazılarak da erişim sağlanabilir.

3.9.1 Statik IP ile Dinamik IP ve Aralarındaki Fark

IP adresleri kendi içinde, statik ve dinamik olmak üzere ikiye ayrılır. Statik IP adresi; hiçbir zaman değişmeyen, kalıcı bir Ip adresidir. Dinamik IP adresi ise bir cihaza, internete her bağlanışında yeniden tanımlanan yani geçici bir IP adresidir. Statik IP adresleri bilgisayara, bir admin(yönetici) tarafından manuel(elle) olarak atanır.

Dinamik IP adresleri ise bilgisayar ara yüzü ya da sunucu yazılımı tarafından, otomatik olarak atanır. IP adresleri, servis sağlayıcı tarafından, statik olacak şekilde de tanımlanabilir.

Bilgisayarlarını uzak erişim ile kontrol etmek isteyen veya kamera sistemine giriş yapmak isteyen kullanıcıların yaşayacağı sorunlarının çözümü, internet servis sağlayıcıları tarafından yıllık cüzi bir ücret karşılığında Statik yani değişmeyen sabit Ip adresi almaları ile mümkündür. Sabit IP adresi almak istemeyen kullanıcılar aşağıdaki başlıklar altında da değineceğim üzere Ddns olarak açıklanan sistemi kullanan web servisler aracılığı ile kullanmış oldukları dinamik IP adreslerini hostname(alan adı) adresi edinerek sabitleyebilir ve sorunlarına çözüm üretebilirler.

Her ne kadar Ddns üzerinden dinamik IP adresleri sabitlenebiliyor olsa da kullanıcıların statik IP adresi edinmelerini daha sağlıklı olacaktır.

Statik yani sabit IP adresleri adından anlaşılacağı üzere değişken olmayan kişiye özel olarak internet servis sağlayıcıları tarafından kişilere, kurumlara ve özel kullanıcılara tahsis edilen IP adresleridir. Statik IP adresi sahibi olan kullanıcılar internet güvenliği olarak da dinamik IP adresi kullanıcılarına göre daha güvenlikli internete sahip olmakla birlikte bilgisayarları ile yapacakları birçok işlemde dinamik IP adresi ile internete bağlanan milyonlarca kullanıcının yaşadığı birçok sorun ile karşılaşmayacaklardır.

3.9.2 IP Adresleri Güvenliği

Bir önceki başlık içerisinde de değindiğim gibi internete bağlanmamızı sağlayan tüm cihazların Ip adresleri yani internete giriş sağlayabilmesi için bir kimlik numarası olmak zorundadır. Ancak son yıllarda kişi başı sahip olunan ve internete bağlanabilen cihaz sayısı neredeyse minimum 3 hatta 5 adet (telefon, tablet, ipad, laptop ve masaüstü pc) olması olağan bir hal almaya başladı, hal böyle olunca ve sahip olunan cihaz sayıları her geçen gün artmaya devam ettikçe bu cihazların internete bağlantı yapabilmesini sağlayan ip adresleri giderek yetmemeye başladığı için ISP yani internet servis

sağlayıcıları ellerindeki sınırlı sayıdaki IP adreslerini nat'layarak yani port bazlı çoğaltmalar yaparak bu sorunun önüne geçmeyi denediler ancak başarılı olamadılar.

Nat yaparak IP sorununun önüne geçemeyen servis sağlayıcıları çözümü aboneleri için hiçte güvenli olmayan yollarda aramaya başladılar.

3.9.3 Nat

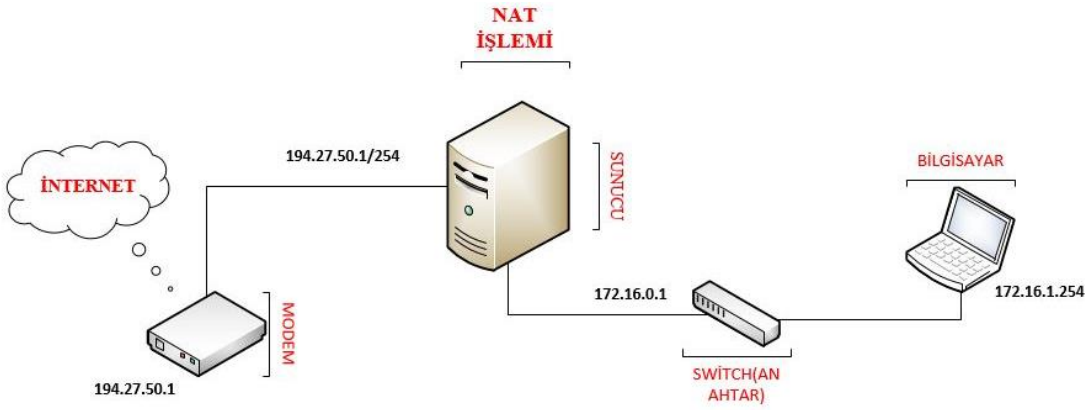
Nat (Network Address Translation) Ağ Adresi Çeviricisi; bir ağda bulunan bilgisayarın, kendi ağı dışında başka bir ağa veya İnternete çıkarken farklı bir Ip adresi kullanabilmesi için geliştirilmiş bir İnternet protokolüdür. Yani Nat bilgisayarın sahip olduğu IP adresini istenilen başka bir adrese dönüştürür.

Kampüs ağları gibi anlık binlerce kullanıcıları olan ağ modellerinde kullanılır genellikle. Çok kullanıcılı ağlarda Nat işlemi yapılması zorunluluk arz etmektedir zira aynı anda binlerce kişinin internete bağlanmasını sağlayacak kadar Ipv4 adresine sahip olmak mümkün değildir.

Örneğin kampüs ağlarında genel olarak özel ip adreslerinden olan 172.16 …. 'lı IP bloğu kullanılır bu tür özel IP adresleri Nat işlemi yapılarak kullanılabilmektedir ancak. Dünya üzerinde birçok şirket ve kurum yerel ağlarında yukarıda verilen özel Ip'leri kullanmakta, dış bağlantılarını ise Nat yapabilen uygun yönlendiriciler (router) kullanarak, IP adreslerini genel adreslere (public address) çevirerek sağlamaktadırlar.

Genellikle Nat işlemini en sık yapan ve kullan kurumların başında üniversiteler gelmektedir. Üniversitelere, ulusal olarak en büyük internet servis sağlayıcısı olan Türk Telekom üzerinden Ulaknet aracılığı ile sınırlı sayıda Ipv4 adresleri verilmektedir. Bu verilen IP adresleri asla bir üniversitenin ihtiyacını görecek sayıda değildir bu nedenledir ki üniversiteler havuzlarında bulunan IP adreslerini titizlikle ve azami ölçüde ihtiyaç olan yerlerde kullanmaktadırlar. (Sunucular vb.)

Üniversiteler genel olarak kişisel kullanıcılarına sanallaştırılmış özel IP adreslerini tahsis ederler ve o şekilde internete bağlanmalarını sağlayabilirler aksi halde her kullanıcıya gerçek IP adresleri vererek internete çıkmalarını sağlamak teknik olarak asla mümkün değildir. Klasik Nat işleminin çalışma prensine örnek çizim 3.19'de gösterilmiştir.



Resim 3.19 Nat işlemi visio çizimi

Resim 3.20' de gösterilen işlemden sonra tabi ki sınırlı sayıdaki gerçek IP adresleri bu işlemden sonra onlarca sanal IP adresine dönüşmüyor IP adresleri sanallaşmış olabilir ancak örnek vermek gerekirse; Nat işleminden sonra 10 adet gerçek IP adresini 100 adet sanal Ip adresine dönüştüğünü söylemek teknik olarak mümkün değildir.

Nat işleminden sonra sanallaştırılan IP adreslerinin binlerce kullanıcıya hizmet edecek şekilde çoğaltmak için sistem üzerinde yapılması gereken işlemler vardır. Sistem üzerinde yapılan bu işlemleri kısaca özetlemek gerekirse sistemde kurulu olan Dhcp Server aracılığı ile sanallaştırılan IP adresleri bloklanarak aynı ve farklı Vlan blogları ile kullanıcıların ihtiyacından daha fazla sayıda çoğaltılabilinir.

3.9.3.1 Nat Ddns

Dinamik DNS olarak da bilinmektedir. ISP'lerin (İnternet Servis Sağlayıcıları) sabit yani statik Ip desteği vermediği durumlarda kullanıcıların yardımına koşan bir sistemdir. Ddns sisteminin gerekliliği artıran nedenler (Dvr ve Ipcam ile ev ve işyeri bilgisayarlarımıza uzak erişim gibi) neredeyse tüm internet kullanıcılarını

ilgilendirmeye başladıkça eskiye nazaran önemi her geçen gün artmaktadır. Özellikle günümüzde ev ve iş yeri güvenliğimizin vazgeçilmez parçası olan kapalı devre güvenlik kamera sistemlerini kullanan kullanıcıların genellikle dinamik yani değişken Ip kullanmalarından kaynaklı erişim sorunlarının çözümü ancak ddns sistemi ile mümkün olabilmektedir.

3.10 Switch(Anahtar) Şifreleme Yöntemleri

Cihazların ayarları menüler aracılığıyla, komut (*command*) yazarak veya grafik ara yüzlerle yapılabilmektedir. Cihazlarda kurulum sırasında oluşan varsayılan (default) ayarların, kullanıcı tarafından aktif edilen bazı ayarların iptal edilmesi veya düzgün olarak tekrar ayarlanması gerekebilmektedir.

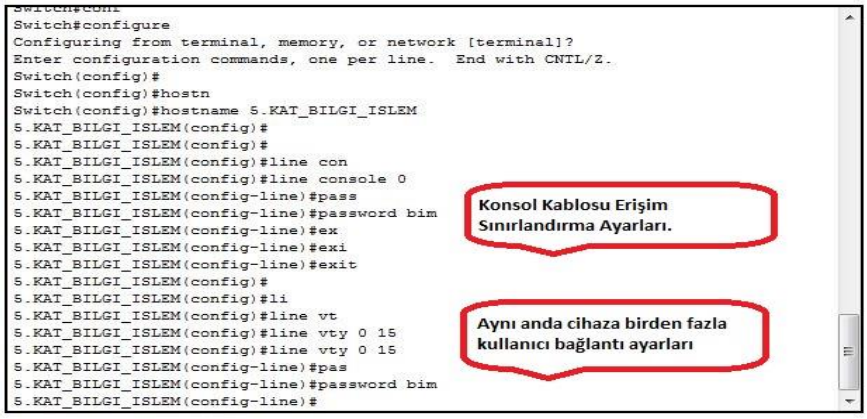
Şifre yönetmenin en iyi yolu LDAP, TACACS+ veya RADIUS doğrulama (authentication) sunucuları aracılığıyla onay mekanizmasını kullanmaktır. Bu sistem kullanılsa bile yetkili (privileged) haklar için o cihaza yerel (local) tanımlı bir şifre, konfigürasyon dosyasında bulunmalıdır. Birçok yönetilebilir cihaz, kullanıcı (user) modu ve yetkili (enable) mod gibi iki ayrı login mekanizmasına sahiptir. Kullanıcı modunda sadece ara yüzler (interface) incelenebilirken yetkili modda ek olarak cihaz konfigürasyonu da yapılabilmektedir. Cisco cihazlarında girilen kullanıcı ve parolaların konfigürasyon dosyasında gözükmemesi için "service password-encryption" komutu girilmiş olmalıdır. Zayıf şifreleme algoritması kullanan "enable password" komutu yerine MD5-tabanlı algoritmayla şifreyi koruyan "enable secret" komutu kullanılmalıdır. "no enable password" komutu kullanılarak enable password'ler silinmeli yerine "enable secret yeni_şifreniz " ile yeniden şifreler girilmelidir.

Burada tanıtılan parolalar:

- **Enable password**- Ayrıcalıklı EXEC moduna erişimi Sınırlandırır.
- **Enable secret**- Şifrelenmiştir ve ayrıcalıklı EXEC moduna erişimi sınırlandırılır.
- **Console password-** Konsol bağlantısı kullanılarak cihaza erişimi sınırlandırır.
- **VTY password-** Telnet üzerinden cihaza erişimi sınırlandırır.

Ayrıcalıklı **exec** erişimini daha güvenli kılmak için anahtarlama cihazların daha eski komotu olan enable komutu değil enable secret komutu kullanılabilir. Enable secret komutu cihaza verilen şifreyi şifreli hale dönüştürmektedir.
Kullanıcı bazlı **exec** erişimini güvenli kılmak;

- Konsol portu güvenli kılınmalıdır yetkisiz personelin fiziksel olarak kablo bağlayarak cihaza erişmesini sınırlar.
- Vty hatları telnet üzerinden cihaza erişim sağlar. Destekleyen vty hattı sayısı cihaz ve cihazın yazılımına sürümüne göre farklılık gösterebilir.



Resim 3.20 Switch parola ekranı.

3.10.1 Anahtar Cihazı Şifreleme Ekranını Şifreleme

Anahtar cihazının ara yüzünde tanımlama yaparken cihazınız destekliyorsa eğer aşağıdaki komutları cihazın üzerinde uygulandığı zaman cihaza verdiğimiz password ara yüz ekranında kriptolanmış şekilde görünecektir. Bu tür bir tanımlamaya ait ekran görüntülerine aşağıda yer verilmiştir.

Bu tür bir kriptolama işlemi için anahtar(switch) cihazın içerisinde şifreleme tanımlamalarını yaptıktan sonra

Resim 3.21 Switch parola kriptolama ekranı.

Service password-encryption; parola şifreleme konfigürasyonu yapılır.

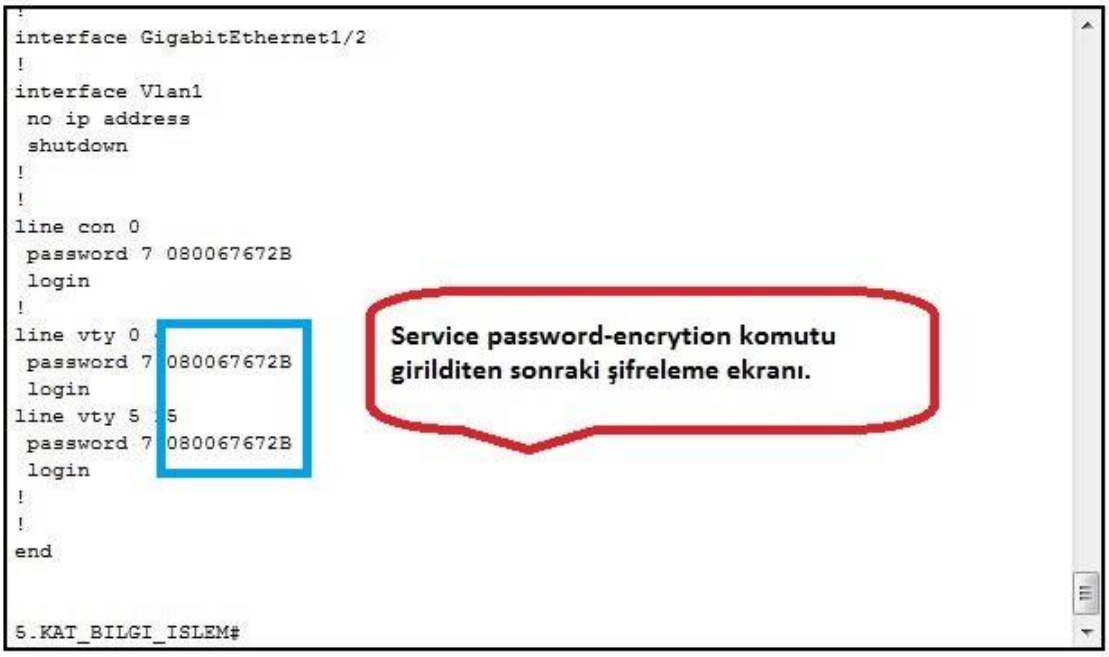
- Yapılandırmayı görüntülerken şifrelerin düz metin olarak görünmesini engeller.
- Bu komutun amacı yetkisiz kişilerin yapılandırma dosyasındaki şifreleri görüntülemesini önlemektir.

- Uygulandıktan sonra, şifreleme hizmetini kaldırmak şifrelemeyi tersine çevirmez.

Service password-encryption; parola şifreleme konfigürasyonu girilmeden önceki cihaza ait ekran görüntüsünde cihaza tanımlanan parola *"AKIB"* olarak görünmektedir.

Resim 3.22 Switch parolasını kriptolama işleminden önce.

Service password-encryption; parola şifreleme konfigürasyonu girildikten sonraki cihaza ait ekran görüntüsünde, parola ekranındaki şifreler kriptolanmış şekilde görülmektedir.

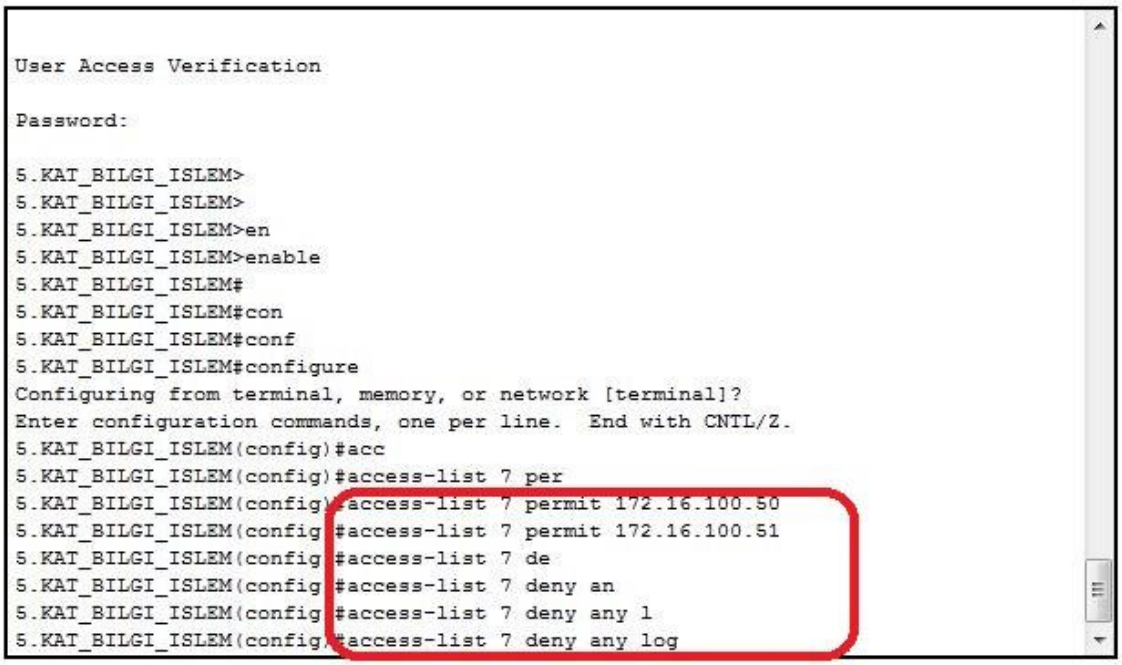


Resim 3.23 Switch parolasını kriptolama işlemi.

3.10.2 Cihaz Erişim Protokol Ayarları

Ağ cihazlarının ayarlanması, yönetimi ve kontrolünde kullanılan HTTP, Telnet, SSH, SNMP, TFTP ve FTP; TCP/IP protokolünün alt elemanları olduklarından, bu protokolün zayıflıklarına karşı önlem alınması gerekmektedir. Bu türden erişimlerde denetim, bu cihazların ve dolayısıyla ağ trafiğinin güvenliği için çok gereklidir.

Ağ cihazlarına, ağ yöneticilerinin dışında uzaktan erişim yapmak isteyenleride engelleyebilmek için belirli ip adresine göre sınırlandırma yapılabilir. Örneğin Cisco cihazların üzerinde IOS'de sadece *172.16.100.50 ve 172.16.100.51* IP'lerin erişimine izin verilmesi ve diğer Ip'lerin engellenmesi aşağıdaki access-list ile sağlanmaktadır.



Resim 3.24 Switch parolasını kriptolama işlemi.

Örnekte verilen 7 numaralı access-list belirtilen IP'lere izin vermekte (permit), diğer IP'leri kabul etmemektedir (deny). Bu access-list'in devreye girmesi için herhangi bir ara yüzde etkin hale getirilmesi gerekmektedir.

3.10.2.1 TFTP-FTP İle Erişim

Cihazlara yeni işletim sistemleri veya konfigürasyonları TFTP veya FTP gibi protokollerle yüklenebilmekte veya Ağ Yönetim İstasyonu'na yedek amaçlı alınabilmektedir. Özellikle TFTP protokolü, UDP kullanması ve kullanıcı-cihaz doğrulama sistemleri kullanmamasından dolayı bilinen bazı güvenlik açıklarına sahiptir.

Bu yüzden bu protokoller cihazlarda access-list ile kontrol altına alınmalı ve dosya transferi belirli IP'lerle sınırlandırılmalıdır. TFTP sunucu olarak kullanılan Ağ Yönetim İstasyonu'nda da bu protokolü kullanırken uygulayacağı ek güvenlik ayarları yapılmalı, mümkünse bu servis bu makinede sadece kullanılacağı zaman açılmalıdır. Cihaz FTP'yi destekliyorsa bu protokolün kullanılması tercih edilmelidir.

HTTP Erişimi:

HTTP protokolü ile web ara yüzünden erişim, cihaza interaktif bağlantı demektir. Yönetilebilir cihazlarının birçoğunun üzerinde web sunucusu çalışır. Bu da 80. portta bir web sunucunun kurulu beklediğini gösterir. Daha önceden de belirtildiği gibi HTTP servisi verilecekse bu ağ yönetimini sağlayan belirli IP'lere kısıtlı olarak verilmelidir. Cihaz güvenliği nedeniyle mümkün olduğunca bu tür web üzerinden yönetimin kullanılmaması gerektiği önerilmektedir. Ama web üzerinden yönetim gerekiyorsa web sunucusu sadece sistem yöneticisinin bileceği başka bir port üzerinden, örneğin 500 nolu port'ta çalıştırılabilecek şekilde ayarlanmalıdır.

HTTP protokolünde doğrulama mekanizması ağda şifrenin düz metin şeklinde gönderimi ile sağlandığı için efektif değildir ama farklı üreticilerin değişik çözümleri bulunmaktadır. Doğrulama mekanizması, onay sunucuları (Tacacs+, Radius …vb) kullanılarak yapılabilir. Cisco IOS'de doğrulama mekanizması "*ip http authentication*" komutuyla sağlanmaktadır.

Telnet ve Secure Shell (SSH) Erişimi:

Telnet ile erişimlerde saldırganın ağ üzerinden dinlenme (sniff) yoluyla iletilen bilgiyi elde etmesi mümkün olduğundan, iletilen veriyi şifreleyen SSH protokolü mümkün olduğunca kullanılmalıdır. SSH şu anda bütün cihazlar ve cihazların üzerinden işletim sistemleri tarafından desteklenmemektedir. Bu konuda üretici firmanın cihaz dokümantasyonu incelenmelidir. Cihazlara yapılan uzak erişimlerde ssh protokolü tercih edilmelidir zira ssh telnet ile yapılan erişimlere göre daha güvenilir bir yoldur.

SNMP Erişimi:

Simple Network Management Protokol (SNMP), cihaz ve ağ yönetimi için vazgeçilmez bir protokoldür. Trafik istatistiklerinden bellek ve CPU kullanımına kadar bir cihaz hakkında çok detaylı bilgiler edinilebilmektedir. Bir veya daha fazla Ağ Yönetim İstasyonu, üzerlerinde çalışan yazılımlarla belirli aralıklarla ağ cihazları ve

sunuculardan (server) bu istatistikleri toparlayacak (poll) şekilde ayarlanmalıdır. Cihazda gözlenen CPU, bellek veya hat kullanımının fazla olması bir saldırı tespiti olabilmektedir. Toplanan verileri grafiksel olarak görüntüleyen Multi Router Traffic Grapher (MRTG) ve (Cacti) gibi programlar bulunmaktadır.

SNMP protokolünün, özellikle SNMP Version 1'in birçok uygulamasında zayıflık (vulnerability) olduğu CERT 'in raporlarında belirtilmiştir. Birçok cihaz üretecisi bu konuda yama (patch) çıkartmış ve önerilerde bulunmuştur. SNMP Version 1, düz metin (clear text) doğrulama dizileri (string) kullandığından bu doğrulama dizilerinin spoof edilmesi söz konusu olabilmektedir. Bu yüzden MD5'a dayanan öz(digest) doğrulama şeması kullanan ve çeşitli yönetim verilerine kısıtlı erişim sağlayan SNMP Version 2'nin kullanılması gerekmektedir. Mümkünse her cihaz için ayrı bir MD5 gizli (secret) değeri kullanılmalıdır. Daha detaylı bilgi için incelenebilir.

Öneriler:

- Sadece Oku (*Read only*) ve Oku-Yaz (*Read-Write*) erişimleri için kullanılan varsayılan SNMP şifre (*community*) adları değiştirilmeli ve bu iki parametre birbirinden farklı olmalıdır.
- SNMP şifrelerine kritik bir UNIX makinasındaki root şifresi gibi davranılmalıdır.
- Ağ Yönetim İstasyonu tarafından SNMP erişimi yapılırken "Sadece Oku" parametresi kullanılmalıdır. Mümkünse cihazlarda "Oku-Yaz" parametresi iptal edilmelidir.
- Ağ Yönetimi için ayrı bir subnet, mümkünse VLAN yaratılmalıdır. Access-list ve Ateş Duvarı (*firewall*) kullanılarak bu ağa dış ağlardan gelen trafik kısıtlanmalıdır.

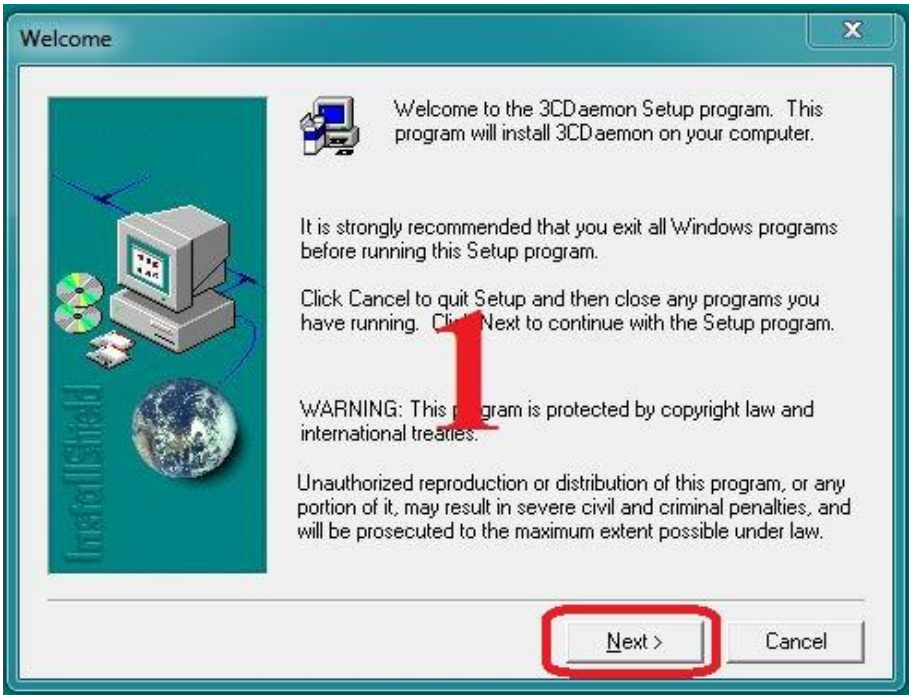
Ağ Yönetim İstasyonları, ağdaki cihazlara ait SNMP şifre dizileri gibi doğrulama bilgileri bulundurdukları için doğal bir saldırı hedefi durumuna gelmektedir. Bu yüzden bu marinaların fiziksel, yazılımsal ve ağ güvenlikleri sağlanmalıdır.

3.10.3 Switch Network Kayıtlama (Loggıng) Ayarları

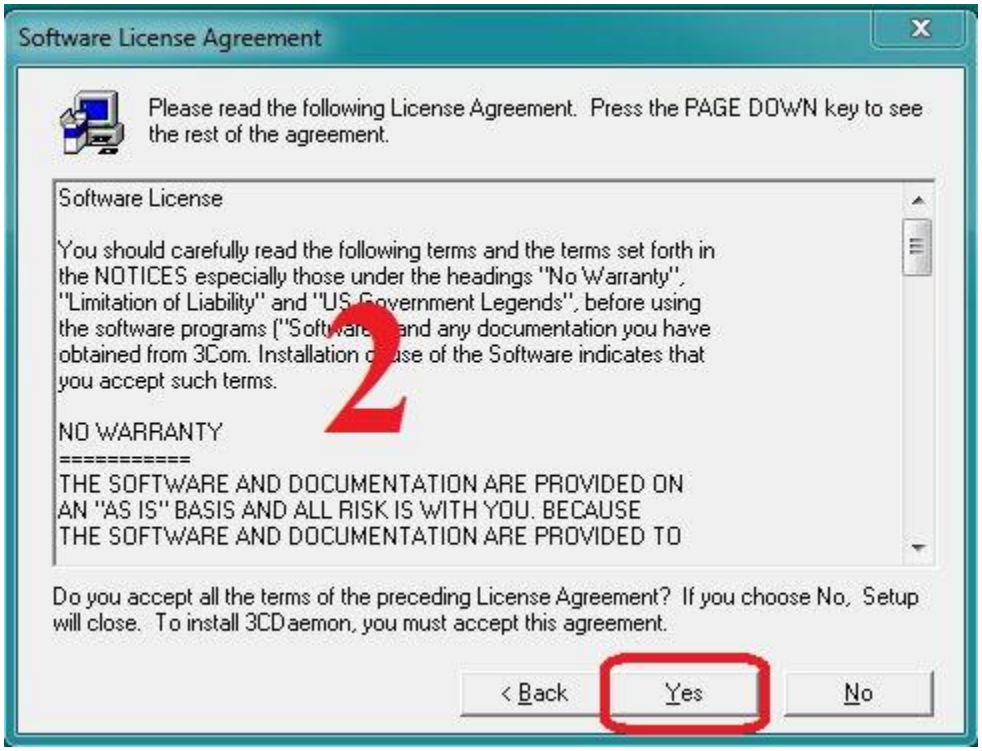
Ağ cihazları çeşitli hadiseler (event) hakkında kayıtlama özelliğine sahiptir. Bu kayıtlar, güvenlik hadiselerinin belirlenmesinden ve önlem alınmasında kritik önem taşıyabilmektedir. Ara yüzlerin durum değişikliği, sistem konfigürasyon değişikliği, access-list'lere takılan (match) bağlantılar gibi güvenlik açısından önemli olan bilgilerin kaydı tutulabilmektedir.

Kayıtlar düzenli olarak takip edilmeli ve sistemin düzgün çalışıp çalışmadığı kontrol edilmeldir. Farklı cihazlardan Ağ Yönetim İstasyonu'na gönderilen mesajların zamana göre senkronize olması için cihazlarda Network Time Protokol (NTP) çalıştırılmalıdır.
Bu işlem için kullanabileceğimiz ücretsiz programlar olduğu gibi anlık network ağımızı durumunu gösteren analiz eden ve trafiği inceleyen aynı zamanda log tutan profesyonel yazılımlarda mevcuttur. Bunlardan bazıları IMC (Network Traffic Analyzer) Cacti gibi yazılımlardır.

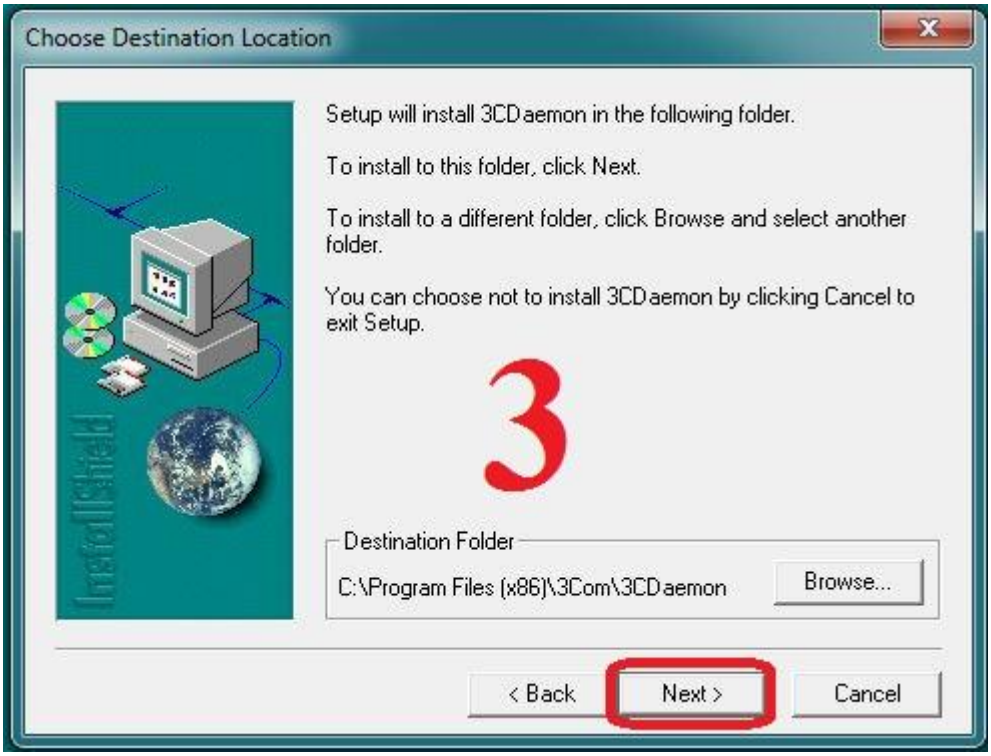
Bu yazılımlardan biri olan 3CDaemon kurulumunu inceleye biliriz.



Resim 3.25 3Cdaemon kurulum ekranı 1.



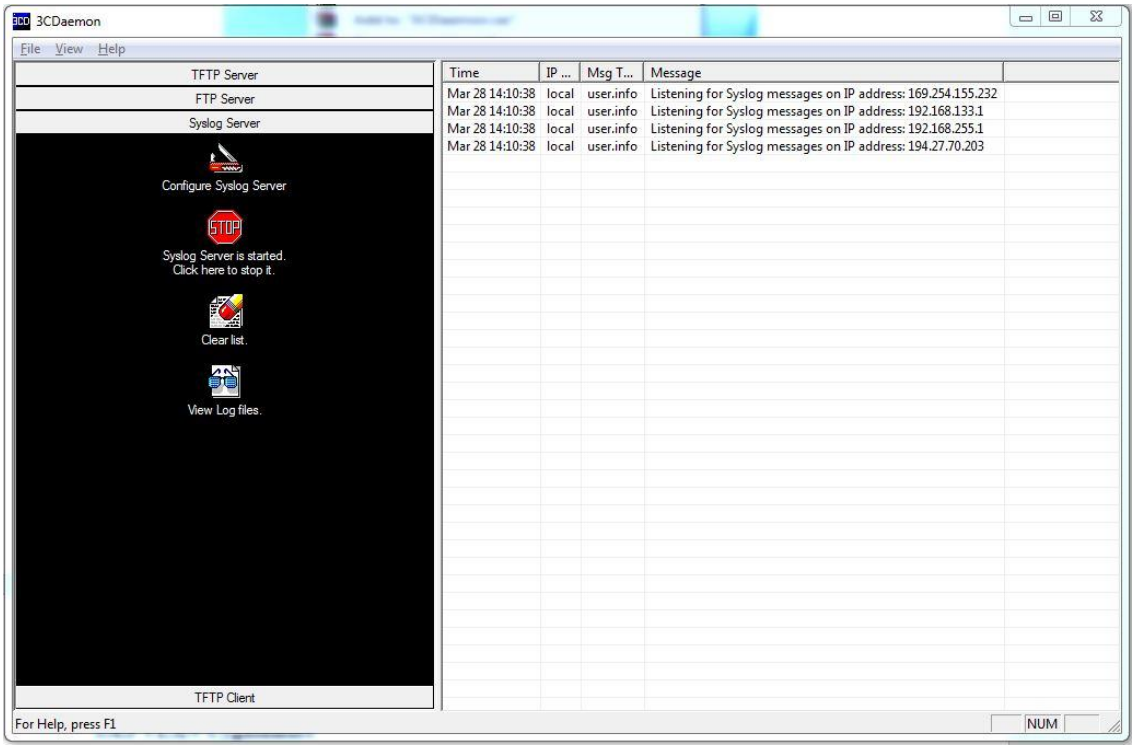
Resim 3.26 3Cdaemon kurulum ekranı 2.



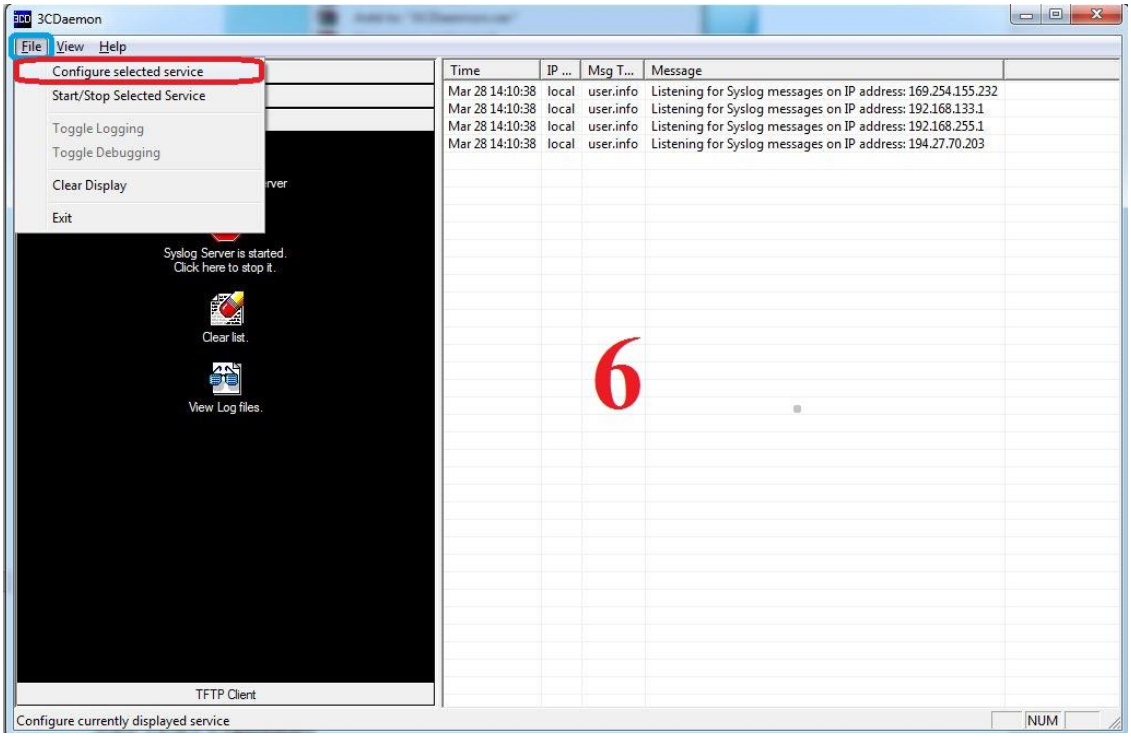
Resim 3.27 3Cdaemon kurulum ekranı 3.

Resim 3.28 3Cdaemon kurulum ekranı 4.

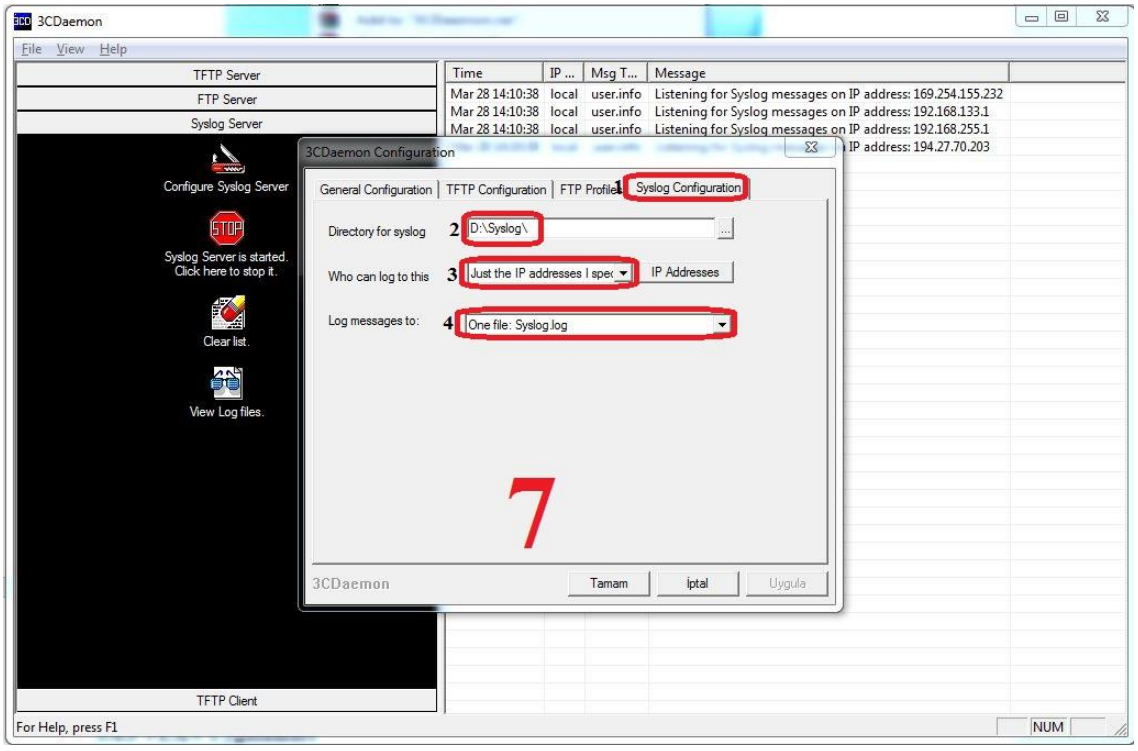
Resim 3.29 3Cdaemon kurulum ayarı



Resim 3.30 3Cdaemon arayüz 1.



Resim 3.31 3Cdaemon arayüz 2.



Resim 3.32 3Cdaemon arayüz 3.

1 ile numaralandırmış konfigrasyon ekranında yazılıma ait syslog ayarları yapılmaktadır.

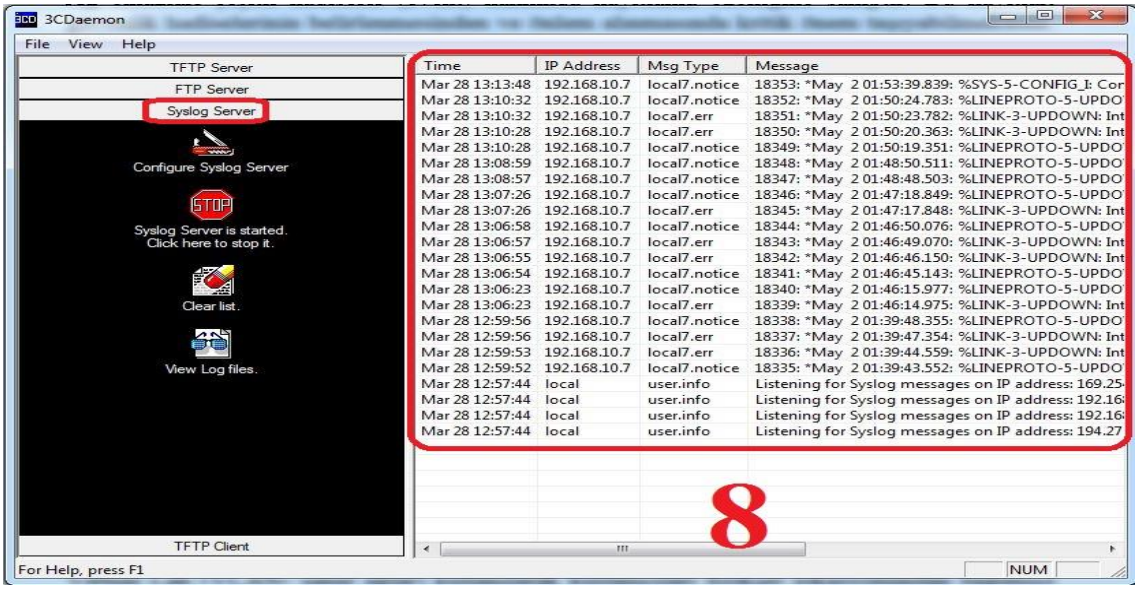
2 ile numaralandırılmış sekmede Logları kaydedeceği lokasyonu seçiyoruz.

3 ile numaralandırılmış sekme ise tutulacak olan log kayıtlarının aynı ağ üzerinde bulunan tüm cihazlarımı yoksa sadece bizim belirleyeceğimiz Ip adresine sahip cihazlara veya sadece local'de tutulacağının seçileceği sekmedir.

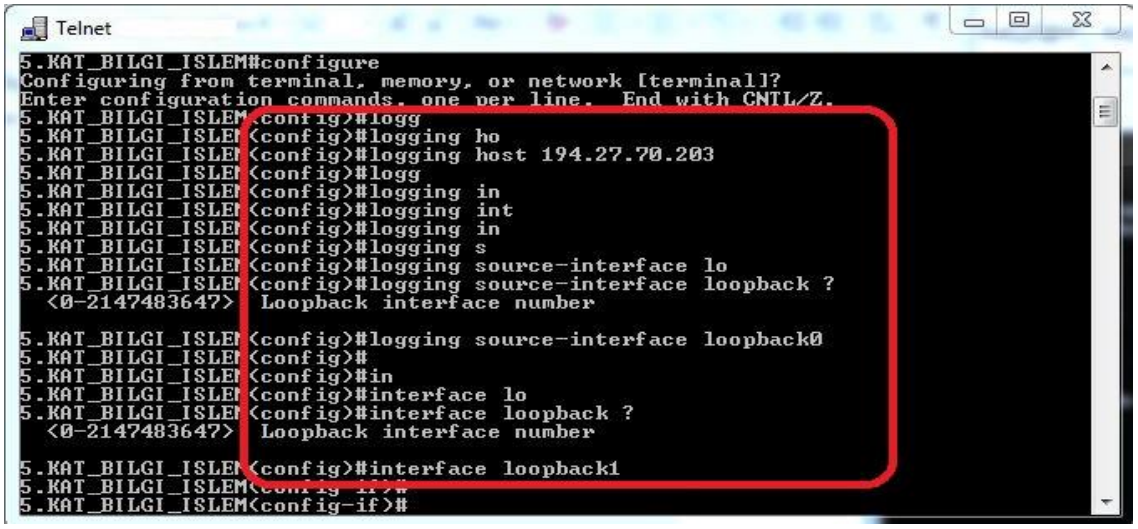
4 ile numaralandırılmış sekmede Log messages to kısmından tüm logları Syslog.log dosyasınamı kaydetsin yoksa info, debug, warning gibi türlerine göre ayırmak istiyor isek Log by priority seçeneğini seçiyoruz.

Kayıt tutma yani loglama işlemini bir program üzerinden anlatım yapmaya çalıştım zira aynı işlevi gören birden fazla lisanslı ve ücretsiz olarak kullanıcıların hizmetine sunulmuş birden fazla program mevcuttur ben bu başlık altında free yani lisanslama

işlemi gerektirmeyen anlık loglama yapabilen basit bir programın kullanımına dair yapılacak işlemleri anlattım.



Resim 3.33 3Cdaemon arayüz 4.



Resim 3.34 Cisco Switch CLI Ekranı

3.11 VLAN Uygulamaları

Virtual Lan (VLAN- sanal ağlar) kullanılarak kullanıcıları fiziksel lokasyonundan bağımsız olarak gruplamak, farklı subnetlerde toplamak mümkündür. VLAN'a almak tek başına bir güvenlik önlemi sayılmamakla beraber bir güvenlik artışı olmaktadır. Ağ Yönetimi için ayrı bir VLAN yaratılmalıdır. Bölgeler VLAN trafiklerine göre prunning

yapılarak ayrılmalı, sadece o bölgede kullanılan VLAN'lar iletilmelidir. VLAN bilgilerini ve bütün ağ trafiğini aktif cihazlar arasında taşımak için kullanılan cihaz port'ları "trunk" olarak tanımlanmaktadır. Trunk olmayacak port'ların trunk olarak tanımlanması o port'a bağlı cihazın bütün ağ trafiğini almasını sağlayacağından bu tür yanlış tanımlamalar mutlaka düzeltilmelidir.

Cihazların kullanılmayan portlarını L3 (OSI 3.katman) bağlantısı verilmemiş bir Vlan'a atamalı veya portlar "disable" edilmelidir. Böylece saldırganın cihazın boş portuna girip ağa ulaşması engellenmiş olmaktadır.

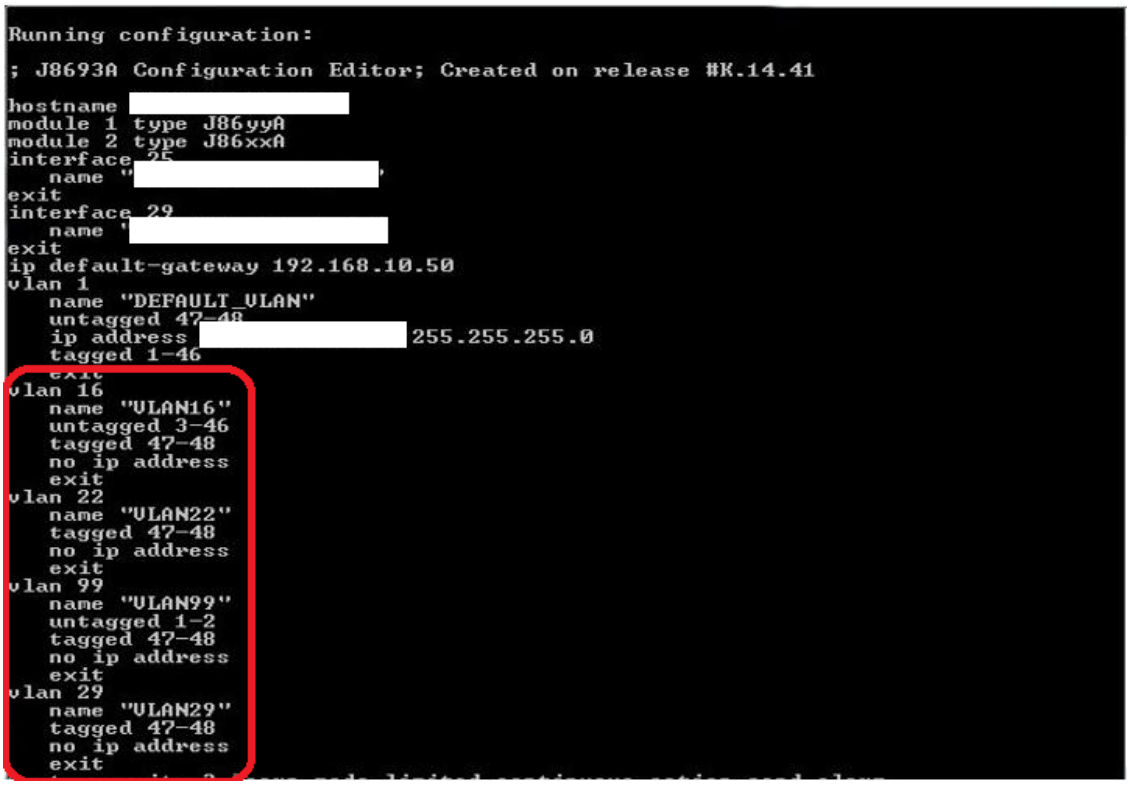
Switch'in port numarasına, cihazın MAC adresine veya kullanılan protokole göre dinamik Vlan ataması uygulanarak cihazların VLAN ve IP bilgileri tek noktadan kontrol edilebilmekte ve daha güvenilir ağ yapısı oluşturulmaktadır. Böylelikle sadece kayıtlı MAC adreslerine sahip cihazlar izin verilen ağlara ulaşabilmektedir.

3.11.1 VLAN Yapılandırmaları

VLAN, bir Lan network üzerinden ki ağ kullanıcılarının ve kaynakların sistemsel olarak gruplara ayrılmasına ve kenar anahtar cihazlarının(switch) üzerinde portlara atanmasıyla yapılır. Vlan yapılandırmasını yapmaktaki asıl amaç tüm ağ üzerinden geçen broadcast trafiğini azaltarak gruplar halinde ilgili port ve Vlan'lara yönlendirilmesiyle bant genişliğinin daha en uygunu kullanmasını sağlamaktır. Daha basit anlatımla ağ üzerindeki trafiği ayrı ayrı yollara ayırarak trafiği bölümlere paylaştırdığı için ağ daha az yorulmaktadır.

VLAN yapılandırması yapmaktaki amaç her ne kadar ağ üzerindeki trafiği rahatlatmak ve bant genişliğini daha optimal kullanmak olsa da bir diğer önemli neden de ağ güvenliğidir. Güvenlik amacıyla alınan önlemlerin en sık kullanılanlarından biride ağımız üzerinden internete bağlanmak isteyen misafir kullanıcılar için sadece onların bağlanacağı bir Vlan bölümü oluşturup misafir kullanıcıları o Vlan üzerinden internete bağlanmalarını sağlamaktır. Bunun önlemlere örnek olarak captive portal'ıda örnek verebiliriz.

Network üzerinde Vlan'lar oluşturarak segmentlere bölmek olası networksel arızaları daha kolay tespit edip daha çabuk çözüme kavuşturabilmesine olanak sağlayacaktır.



Resim 3.35 Hp 3500 L3 Switch VLAN örneği.

3.11.2 VLAN Yapılandırması Kullanma Sebepleri

Güvenlik: Hassas bilgileri içeren sistemleri birbirinden ayırarak bunlara yapılabilecek sızma olasılıklarını azaltır.

Projeler/Özel Uygulamalar: Vlan kullanılarak proje yönetimi ve özel uygulamalar daha da basitleştirilir. Vlan'da bütün gerekli düğümler birarada kullanılmaktadır.

Performans/Bant Genişliği: Ağ trafiği daha dikkatli bir şekilde izlenebilir.

Yayın/Trafik Akışı: Vlan' ın temel prensiplerinden birisi trafik akışının Vlan üyesi olmayan diğere düğümlere geçmemesidir. Böylece yapılan yayın miktarını otomatik olarak azaltır.

Departmanlar/Özel İş Türleri: Bir şirket içinde farklı departmanlar için farklı Vlan' lar kurularak ağı fazlasıyla kullanan departmanlar ayrılabilir. Birçok switch'e Telnet ile girilip isim, domain, portlar gibi Vlan parametreleri girilerek Vlan oluşturulabilir. Vlan oluşturulduktan sonra bir network segmenti ilgili porta bağlanarak Vlan' ın bir parçası haline getirilebilir. Vlan lar arasındaki haberleşme routerlar aracılığıyla olur. Vlan' lar birden fazla switche dallanabilir ve aynı şekilde bir switchte birden fazla Vlan olabilir.

3.11.3 VLAN Trunking Protokolü

VLAN trunking protokolü (VTP) Vlan konfigürasyonu üzerindeki switchlerin birbiriyle haberleşmesini sağlayan bir protokoldür. Bu protokol kullanılam ağ cihazlarına göre değişiklik göstermektedir.

Vlan trunking protokolü: Çok sayıda kenar nokta anahtarları(switch) barındıran ağ yapılarında bulunan Vlan'ları adından anlaşıldığı üzere Trunk (bağlantı noktası) sayesinde diğer kenar nokta switchlere taşımayı sağlayan protokoldür. Vlan oluşturulmasının ve Vlan'ların ağ cihazları içerisinde yapılandırması işleminin en önemli gerekçelerinden biriside ağ güvenliği ve dolayısı ile kullanıcıların bilgisayar güvenliği içindir.

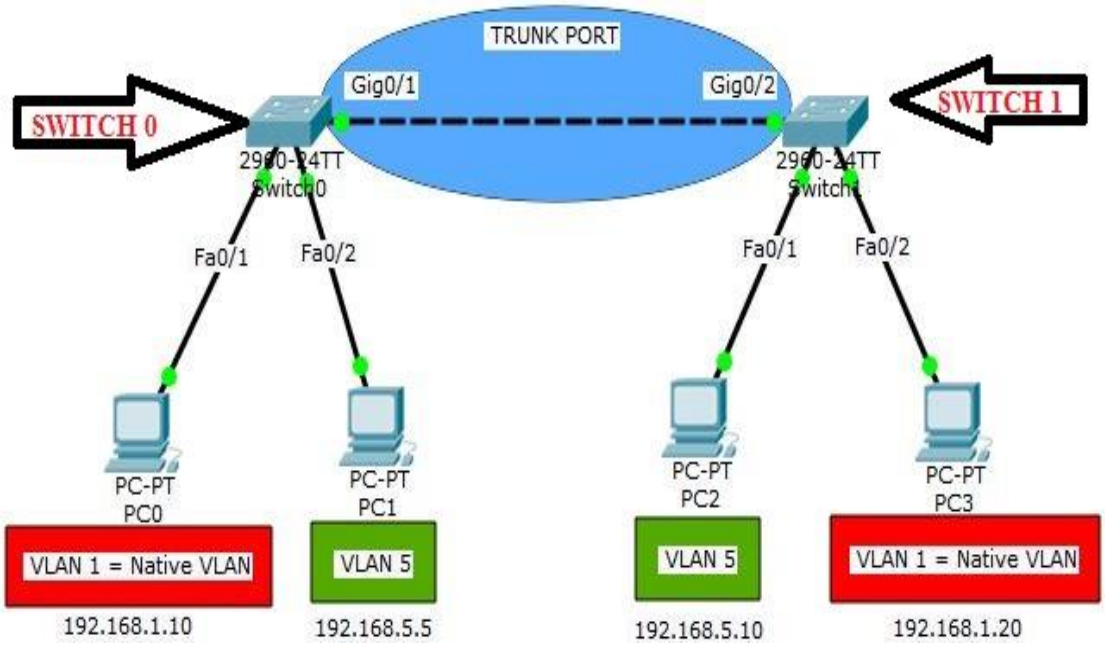
Vlan yapılandırmaları kullanılan cihazların yazılımlarına göre farklı parametreler ve configrasyonlar kullanılarak yapılır. Ancak Vlan yapılandırması yapmak ağın büyüklüğüne göre zaman alabilir zira tek bir noktadaki ağ cihazı üzerinde yapmakla tüm ağ omurgasına ulaşmasını sağlamak mümkün değildir.

Omurga dediğimiz dağıtıcı(router) cihazın üzerinde yapılan işlemler mutlaka route edilerek diğer kenar noktadaki Layer 2 destekli ağ anahtarına ulaştırılması gerekmektedir. Bu işlemleri, dağınık lokasyonlar da bulunan ve ağ topolojisini oluşturan cihazlarının fiziken bulundukları noktalarda yapmak gerekebilmektedir

Vlan trunk protokolünün ve Vlan yapılandırmasının ağ güvenliği için önemini anlatmakla birlikte neden kullanılması gerektiğinide kısmen anlatmaya çalıştım çok

uzun bir süreç olan bu işlemlerin yapıldıktan sonraki kenar nokta cihazlarında nasıl kullanıldıklarını aşağıdaki görseller ile kısmen de olsa paylaşmaya çalıştım. Vlan oluşturmak ve oluşturulan Vlanları client portlarına taşıma configrasyonları değişik marka ve model deki network cihazlarına göre farklılık gösterebilmektedir.

Trunk işleminin nasıl yapıldığını cisco packet tracer smilasyon programı aracılığı ile görebiliriz.



Resim 3.36 Cisco Packet Tracer 1 (VTP Ayarları).

Cisco Switch1 üzerinde gerekli ayarları yapıyoruz.

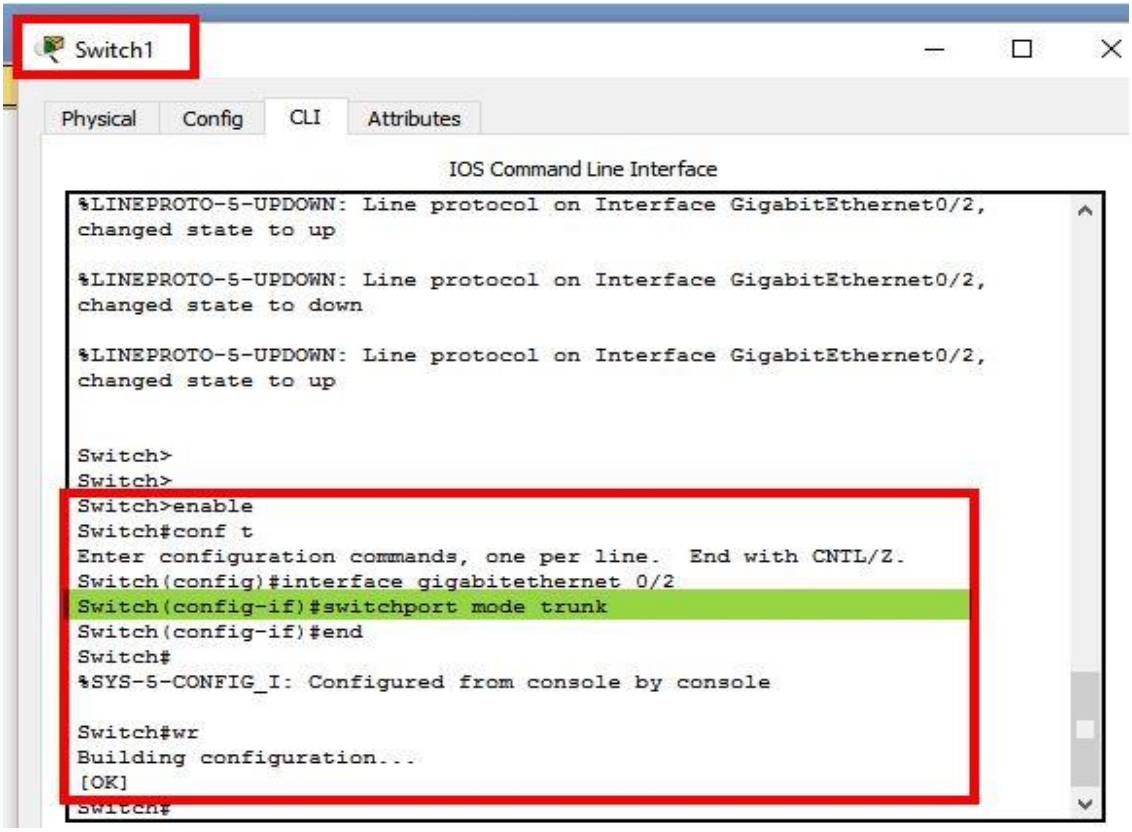
Switch#conf t

Switch(config)#interface gigabitethernet 0/2

Switch(config-if)# switch port trunk

Switch(config-if)#end

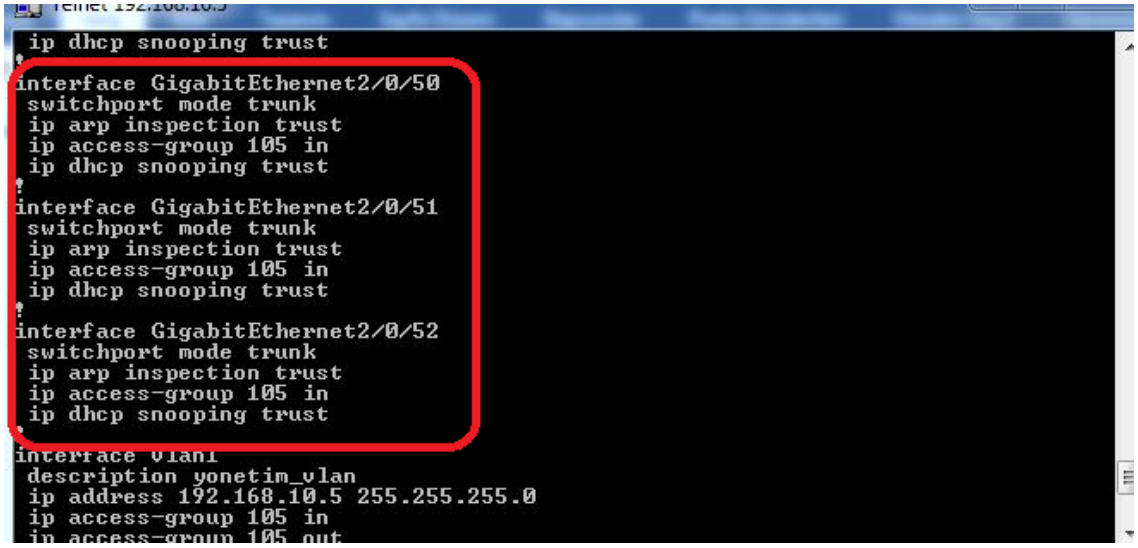
Switch(config-if)# write memory



Resim 3.37 Cisco packet tracer 2 (VTP Ayarları).

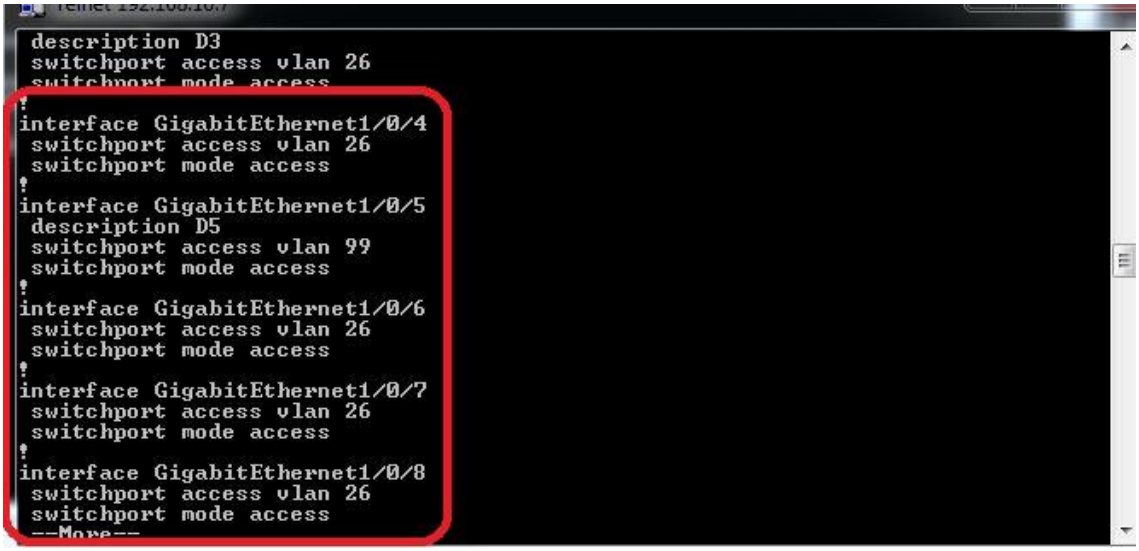
Resim 3.38 Cisco packet tracer 3 (VTP Ayarları).

Yukarıdaki işlemin aynısını diğer Switch üzerinde yaptıktan sonra *switch interfaces switchport komutu* ile port 0/2 ninde trunk olduğunu görebiliriz.



Resim 3.39 Cisco 2960 Sw. Vtp ayarları.

Kenar nokta anahtarı üzerinde yapılan Trunk olayının çalışabilir olması için atanmış Vlan'ların ilgili portlara access edilmesi gerekmektedir.



Resim 3.40 Cisco 2960 Sw. Port Trunk işlemi.

Resim 3.21 'de yapılan işlem anahtar üzerinde daha önceden trunk yapılan yanı dağıtılmış olan Vlan'ların portlara atanma işleminin son halidir. Resim 'de görüleceği üzere farklı Vlan'lar farklı portlara atanmıştır ve bu atanan portlar kullanıcı portları ile ağ üzerinde olan access point vb. cihazlarıdır. Birbirinden farklı Vlan'lar ile ağa bağlanmaları sağlanarak ağın ve kullanıcıların güvenliği için önlem alınmıştır.

3.12 Ağ Cihazlarında Port Güvenliği

Kampüs gibi yerelde geniş bir ağ altyapısına ve aynı anda binlerce kullanıcıya hizmet veren topolojiye sahip ağ(network) yapılandırmalarında switchler üzerinden portların, dolayısıyla ağın güvenliğini sağlamak açısından alınan önlemler vardır. Bu ve benzeri güvenlik önlemlerindeki asıl amaç, kenar noktada bulunan switchlerin üzerinden internete bağlanan kullanıcıların switchlere yapılacak herhangi bir fiziksel tap'lama saldırılarından etkilenmemesi ve portlar üzerinden ağa gelecek olası saldırıları derhal kesintiye uğratmak için portları ***shut down*** konuma getirmektir.

Bu amaçla kenar noktalarda kullanılan switchlerin ara yüzlerinde yapılan tanımlamaların içerisinde port güvenliğini sağlamak için yapılan ayarlamalar vardır. Bu ayarlamalara ***port-security*** (port güvenliği) denilmektedir.

3.12.1 Port-Security Nedir?

Birden fazla bilgisayar bulunan ağlarda güvenliği en üst seviyelere çıkarabiliriz. Normal şartlarda herhangi switch portuna bağlı olan bilgisayar her ağ ortamına rahatlıklar girebilir ve bu yöntem ağ yöneticilerinin tercih ve tavsiye ettiği bir yöntem değildir. OSI başvuru modelinin 2.katmanı (layer-2) ağ trafiğinin mac tabanlı olarak izlenmesine ve kontrol edilmesine olanak sağlayan bir özelliktedir. Yönetilebilir switchler üzerinden Mac adresi bazlı kısıtlaması yapabiliriz. Ve bu kısıtlamayı yapabilmemize olanak sağlayan özelliğe **Port-Security** özelliği denilmektedir.

Port-Security özelliğini yönetilebilir switchler üzerinden aktif hale getirerek tek bir porttan birden fazla bilgisayarın ağa giriş yapmasını engelleyebiliriz. Bu özellik, genellikle odalarda bulunan internet duvar uçlarına kullanıcılar tarafından modem veya hub gibi çoğaltıcı özelliği olan cihazlar takılarak birden fazla bilgisayarın ağa giriş yapmasına imkân sağlanan durumlarda ağ güvenliği açısından oldukça etken bir yöntem olarak kullanılmaktadır.

3.12.2 Port-Security Ayarları

Cisco Packet Tracer smilasyon programı ve kenar nokta switch'i üzerinden port-security yapılandırma ayarlarına aşağıda yer verilmiştir.

Switch'lerde cihazlarınızı mac adresine göre tanımlayarak port güvenliği oluşturabilirsiniz. Switch'ler mac adreslerini öğrenerek, kaydeder. Bir portta kaç adet mac adresinin tanımlı olacağını ve belirtilen kurallar dışında portun nasıl bir tepki vereceğini belirleyebiliriz. Bu sayede dışardan Switch'imize takılacak herhangi bir network cihazında sistem güvenliğini sağlayabiliriz.

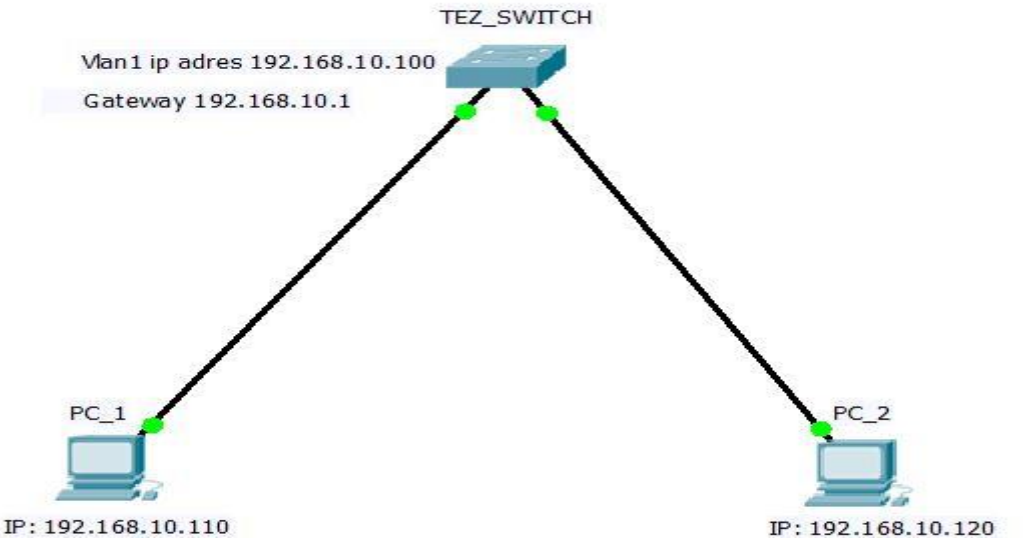
Switch (config)# interface fastethernet 0/1: Komutu ile güvenliği aktif edeceğimiz portu belirleriz.

Switch (config-if) # switchport port-security: İlgili porta güvenlik oluşturulur**.**

Switch (config-if) # switchport port-security violation: Shutdown Kurallar dışına çıkıldığında uygulanacak işlem belirlenir. Shutdown seçeneği ile trafiği tamamen kapatabilirsiniz. Shutdown Seçersek farklı bir mac adresi ile porta bağlanıldığında o portu kapatılacaktır ve geri açılması için ağ yöneticisinin switche erişerek o portu tekrar Noshutdown yapması gerekecektir. Restrict 'i seçersek farklı bir mac adresi ile ağa bağlanıldığında o mac adresindeki bilgisayarın ağ üzerinde hiçbir işlem yapamamasını sağlarız. Tekrar mac adresi tanımlanmış olan bilgisayarı ağa eklersek sorunsuz şekilde iletişime geçecektir.

Switch (config-if) # switchport port-security mac-address sticky: Bu kural ile porta bağlanan cihazların mac adreslerine göre porta kaydı tutulacak ve bu kuraldan sonra ilgili portun altında bağlı bulunan cihazın mac-adresi tanımlanmış olacaktır.

Switch (config-if) # switchport port-security maximum: Kuralı ile ilgili porta farklı mac adreslerine sahip olan en fazla kaç cihazın bağlanabileceğini tanımlayabiliriz.



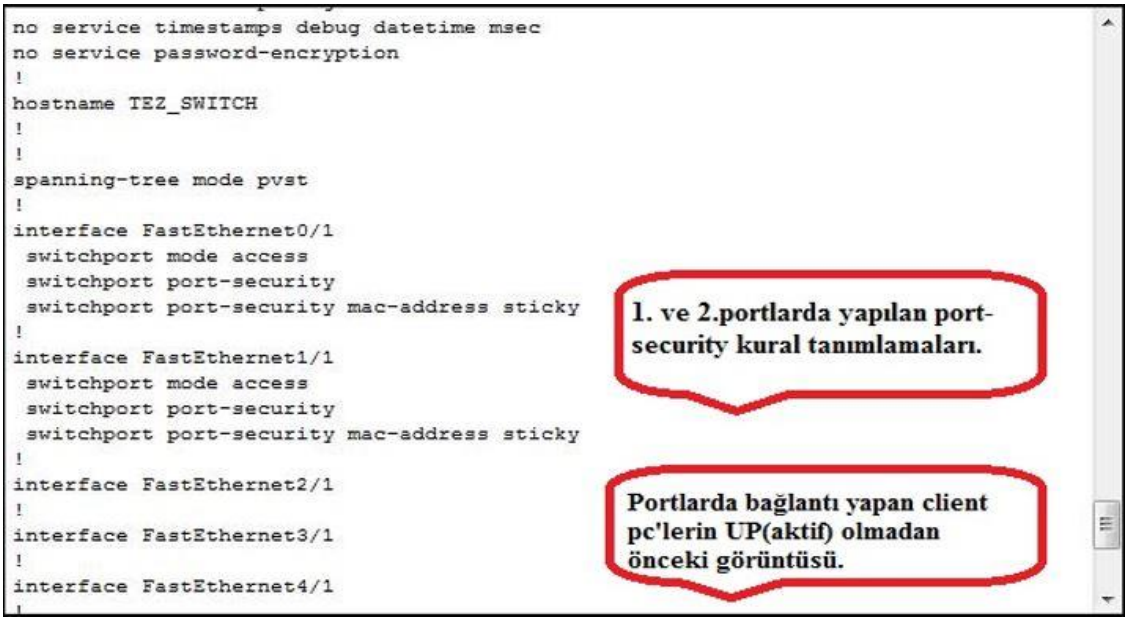
Resim 3.41 Cisco Packet Tracer 4.

Cisco packet tracer programı ile Resim 3.22'de smule edilmiş olarak gösterilen ve default modda hiçbir kural tanımlanması yapılmadan çalışan topolojiye küçük bir örnektir.

```
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname TEZ_SWITCH
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet1/1
!
interface FastEthernet2/1
!
interface FastEthernet3/1
!
interface FastEthernet4/1
!
interface FastEthernet5/1
!
interface Vlan1
 ip address 192.168.10.100 255.255.255.0
!
ip default-gateway 192.168.10.1
!
```

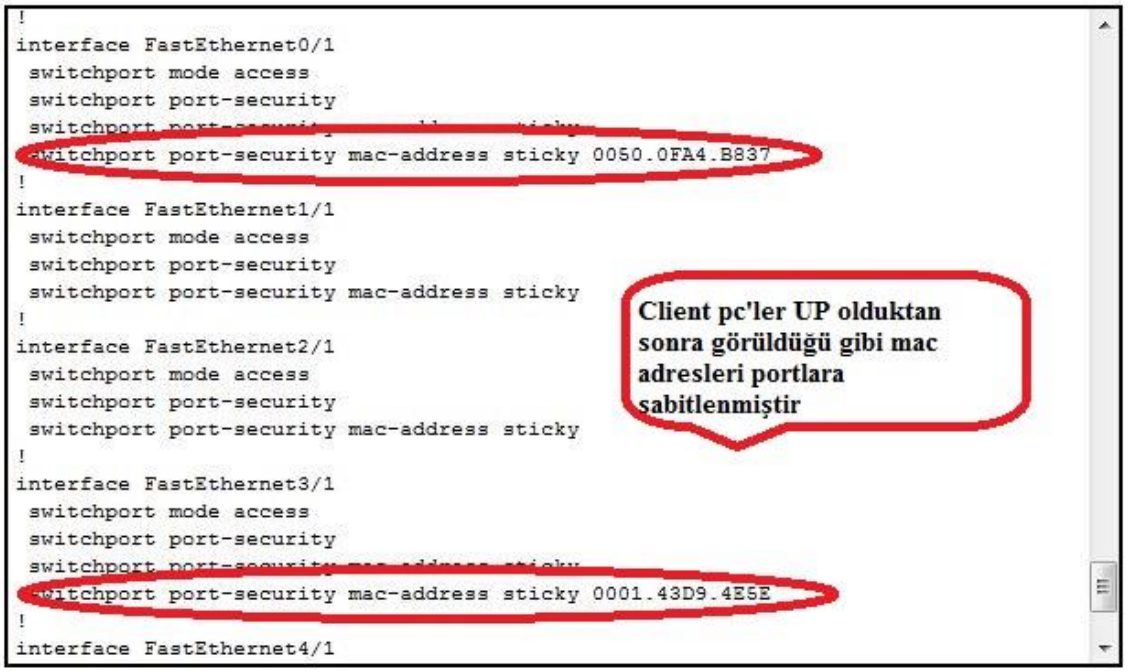
Switch üzerinde bulunan portların kural tanımlanmamış default modu

Resim 3.42 Cisco Packet Tracer 5 (Port Security Ayarları).



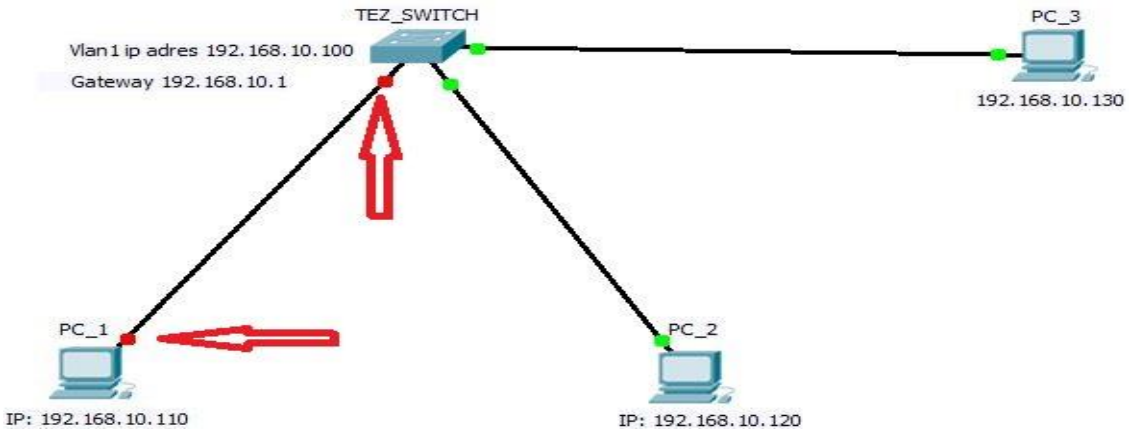
Resim 3.43 Cisco Packet Tracer 6 (Port Security Ayarları).

Aşağıda da görüldüğü gibi ***port-security*** kuralı tanımlanan portlara bağlı olan client pc'lerin mac adresleri, *mac-address stiky* kuralı gereği bağlı oldukları portlara sabitlenmiştir. Bu şekilde kural tanımlanan portlara ilk bağlanan PC'lerin ya da mac adresine sahip cihazların dışından bir başka cihaz bağlanamamaktadır.



Resim 3.44 Cisco Packet Tracer 7 (Port Security Ayarları).

Smule edilen topolojimizdeki client PC'lerin bağlı olduğu ve altında ***port-security*** kurallarının tanımlandığı portlardan birine bir başka client pc'yi eklediğimizde Resim 3.47'de görüleceği üzere port tanımlanmış kural gereği yabancı bir mac-adresine sahip PC'nin kendisine bağlanmasına izin vermeyip ***shutdown*** yaparak kapalı konuma geçmiştir.



Resim 3.45 Cisco Packet Tracer 8 (Port Security Ayarları).

Resim 3.48' de gösterildiği gibi *port-security* kuralı tanımlanan portlara bir başka client pc eklenmeye çalışıldığında port, switc üzerinden de görüldüğü gibi kendisini *shutdown* moduna çekerek yabancı mac-adresine ait PC'yi ağa dahil etmemektedir.

```
TEZ_SWITCH>en,
Translating "en,"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

TEZ_SWITCH>en
TEZ_SWITCH>enable
TEZ_SWITCH#
TEZ_SWITCH#sh
TEZ_SWITCH#show po
TEZ_SWITCH#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        1           1                0        Shutdown
        Fa1/1        1           0                0        Shutdown
        Fa2/1        1           0                0        Shutdown
        Fa3/1        1           1                1        Shutdown
---------------------------------------------------------------------
TEZ_SWITCH#
```

Resim 3.46 Cisco Packet Tracer 9 (Port Security Ayarları).

3.13 Kullanıcı Bazlı Güvenlik

Günümüzde “bilgi güvenliği” farkında lığı sadece büyük ağların ihtiyacı değil 3-5 kullanıcılı ağlarda bile gerekli önlemlerin alınması, doğru konfigürasyonun yapılması, güvenliğin sağlanmasında en önemli faktörlerdendir. Kullanıcı kimliğinin doğrulanması, orta büyüklükteki ve büyük ağlarda bir dizin yapısı kullanılarak yapılır.

MAC address kısıtlamalı Kimlik Doğrulamalı Internet Erişimi konfigürasyonunun ve Mac adres kısıtlaması bize, her kullanıcının ağ kablosunu takıp veya kablosuz yayına bağlanıp internet te dolaşmasını engellemek ve bu erişim kontrolünün tamamen bizim kontrolümüzde olmasını sağlayacaktır.

User Authentication ise, kullanıcı mac adresi tanımlandıktan sonra internet erişimini sağlarken, logların daha anlaşılabilir bir şekilde tutulması için faydalı olacaktır. Bunu yapmayıp direkt internet izni de verebilirdik. Fakat bu bizim için ve log kayıtlarını anlamakta zorlanmamıza neden olacaktır.

3.13.1 Kimlik Doğrulama Sunucusu (Radius)

Radius (Remote Authentication Dial-In User Service) uzak kimlik doğrulama protokolüdür. Genellikle radius sunusu AAA görevlerini gerçekleştirmek için kullanılır. Radius sunucular genel olarak çok kullanıcılı kurumlarda kampüslerde ve işletmelerde ağa üzerinden internete giriş yapabilmeleri için kimlik bilgilerinin sorgulanarak kontrol edilmesini sağlayan yapılardır.

Daha çok internet servis sağlayıcılar(IIS) tarafından kullanılsa da kendi kullanıcılarına hesap açma yetkilendirme ve yapabilmek için merkezi bir kontrol birimi olarak kullanmak isteyen tüm ağ yöneticileri tarafından da kullanılabilir.

Bu işlem için radius sunucuların görevlerini yerine getirmelerini sağlayan AAA 3 ana görevlendirme evreleri vardır.

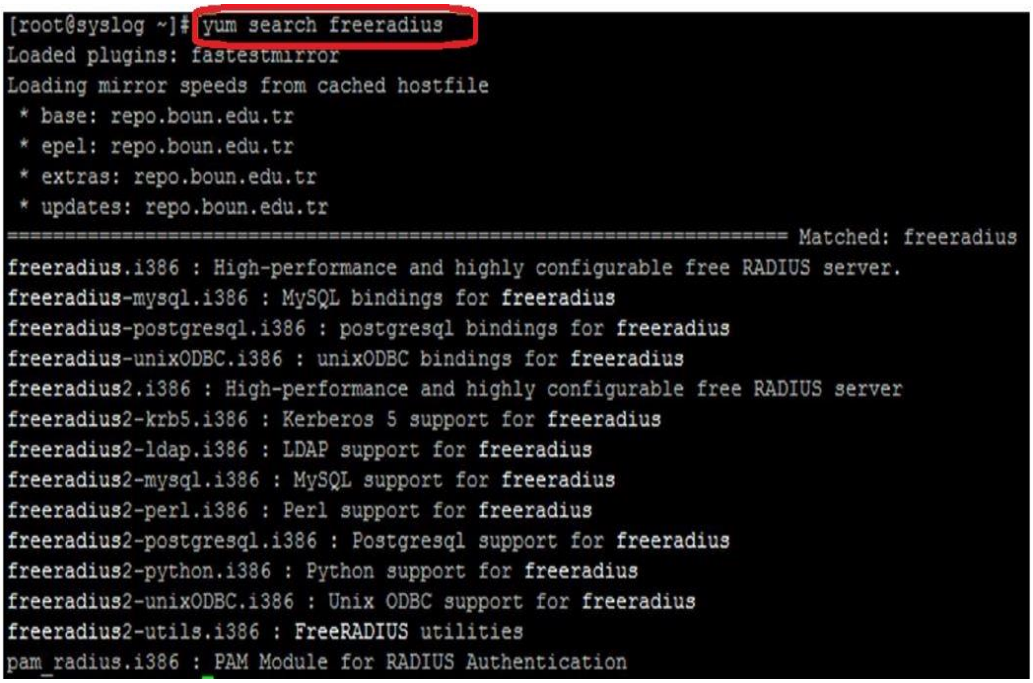
Kimlik doğrulama evresi: Bir kullanıcı adı ve parolasını sistem üzerinde bulunan veri tabanında doğrulara ve kimlik bilgileri doğrulandıktan sonra yetkilendirme işlemi başlar.

Yetkilendirme evresi: Kullanıcıların istekte bulunması sonucu kaynağa erişmesine izin alabilmesi için süzgeçten geçerek lokalden IP adresi atanır.

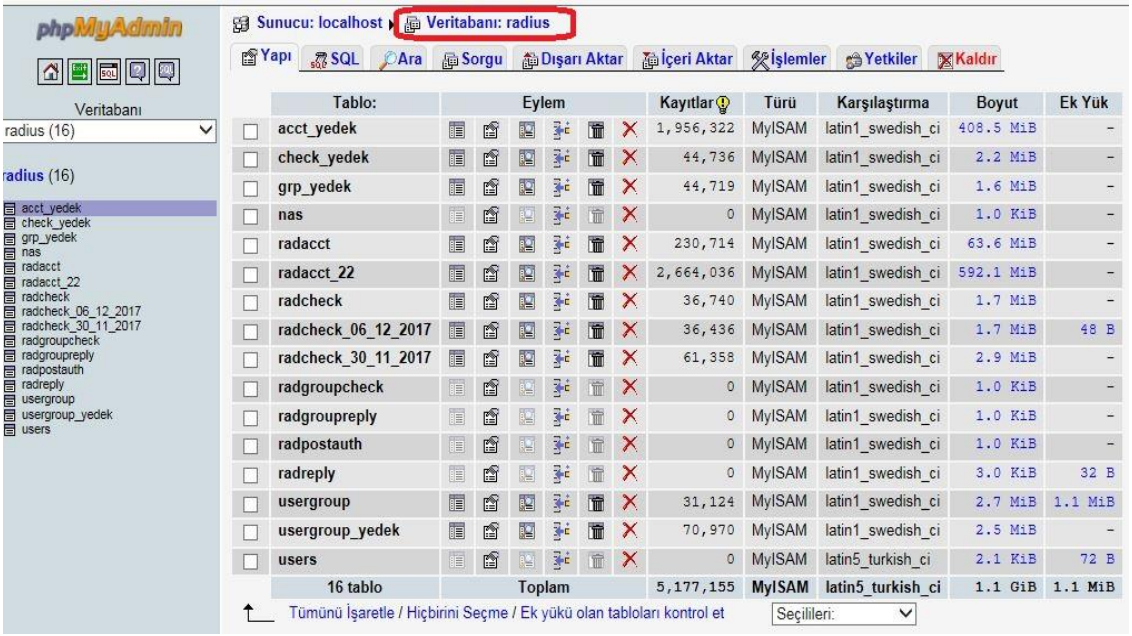
Hesap yönetimi evresi: Kaynak kullanımına ilişkin olarak bilgileri toplar ve eğilim analizlerine göre raporlama işleminde kullanılır.

Radius için geliştirilen yazılımlardan biride FreeRadius'tur. Bu yazılım ile yapılabileceklerin başlıcaları şunlardır.

- Kişi bazında yetkilendirme yapılabilir.
- Gruplar tanımlanıp, farklı erişim hakları verilebilir.
- Yapılan girişlerin kaydı tutulabilir.
- Sisteme o an bağlı kullanıcı listesini gösterebilir.
- Tek kullanıcının aynı anda iki bağlantı yapması engellenebilir.
- Proxy kullanımını destekler



Resim 3.47 Free radius ekranı.



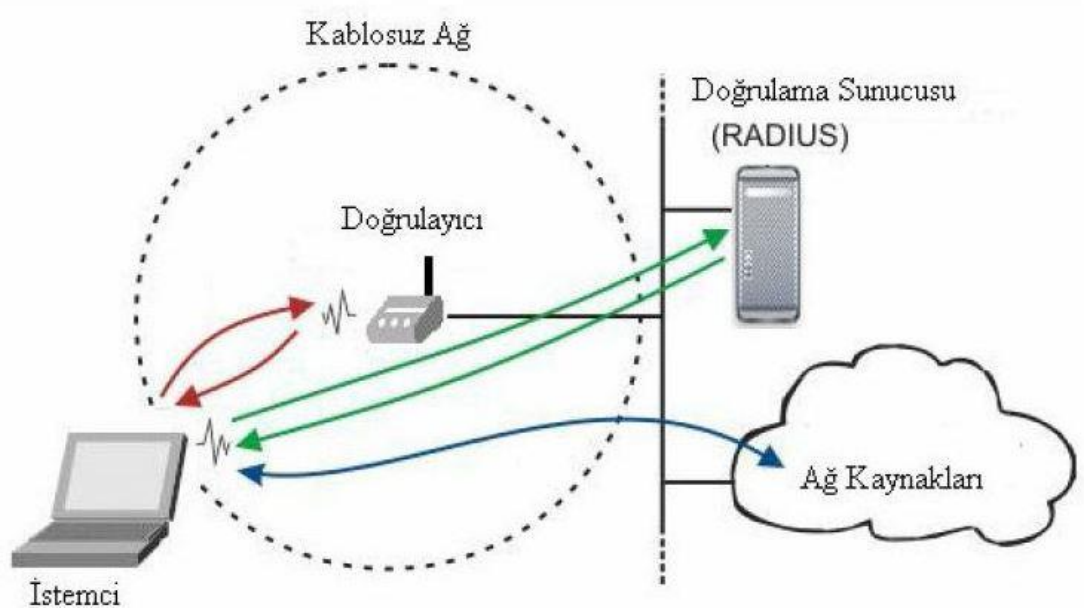
Resim 3.48 Radius veritabanı.

3.13.2 Kimlik Denetimi (802.1X)

Kullanıcı bazlı kimlik denetimlerinden biride güvenlik protokolleri ile yapılan denetimlerdir. 802.1x protokolü bunlardan biridir. 802.1x protokolünü kullanacak radius server üzerinden kimlik doğrulaması yapılabilmesi için omurga ve kenar nokta anahtarlama(switching) cihazlarında güvenlik ayarları tanımlanması gerekmektedir.

Makine, istemci aygıtı olarak bir 802.1X ağına bağlanabilir. Tipik bir 802.1X ağı, bir RADIUS sunucusundan (kimlik doğrulama sunucusu), LAN anahtarından (kimlik doğrulayıcı) ve kimlik doğrulama yazılımı içeren istemci aygıtlarından (doğrulama isteyenler) oluşur. Bir aygıt, 802.1X ağına bağlanmayı denerse, aygıt bağlantının yetkisiz bir kullanıcı tarafından yapıldığını kanıtlamak için kullanıcı kimlik doğrulamasından geçmelidir.

Kimlik doğrulama bilgileri bir RADIUS sunucusuna gönderilir ve RADIUS sunucusu tarafından kontrol edilir; bu sunucu, kimlik doğrulama sunucusuna bağlı olarak ağa iletişime izin verir veya reddeder. Kimlik doğrulaması başarısız olursa, LAN anahtarı (veya erişim noktası), ağın dışından erişimi engeller.



Resim 3.49 IEEE 802.1x Yapılandırması (İnt.Kynk.18).

3.13.3 Kimlik Denetimi (Mac Authentication)

Mac adresi bazlı kimlik denetimlerinde kullanıcıların mac adresleri, radius sunucularında olduğu gibi sistem üzerinde bulunan veri tabanında işlenmiş olması gerekmektedir. Bu şekilde mac adresleri ile yapılan kimlik denetimlerinin yapılabilmesi için anahtarlama cihazlarının üzerinde mac authentication protokolü kullanılmaktadır.

```
domain default enable system
#
mac-authentication
mac-authentication user-name-format mac-address with-hyphen uppercase
#
radius scheme
 server-type extended
 primary authentication 10.2.0.4
 primary accounting 10.2.0.4
 key authentication secret
 key accounting secret
 user-name-format without-domain
#
#
domain       .edu.tr
 authentication default radius-scheme
 authorization default radius-scheme
 accounting default radius-scheme
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
mac-authentication
#
```

Resim 3.50 Mac kimlik doğrulama ekranı

3.14 Ağ Güvenliği Paketleri

Ağ güveliği paketleri genel olarak sistem ve ağ güvenliğinin test edilmesi anlık trafiğin izlenmesi ve olası güvenlik açıklarının tespit edilmesini sağlayan programlara yazılımlara genel olarak ağ güvenliği paketleri denilmektedir.

Ağ güvenliği paketleri içerisinde kullanılan yazılım ve programların birçoğu açık kaynak kodlu işletim sistemi olan Linux ile uyumlu olarak tasarlanmakla beraber paket içerisindeki birçok yazılımın sağlıklı olarak sonuç vermesi Linux tabanlı sistemlerde kullanılması ile daha mümkündür.

Kullanılan ve kullandığımız teknolojinin her geçen gün kendini yenilemesi ve yeniledikçe evrimleşmesi sonucu bir yerden sonra verilerimizin güvenliğini sağlamak kurumsal ve dahi kişisel kullanıcılar bakımından zaruret halini almıştır. Bu durum ise bilgisayar ağlarının öneminin artmasına ve bu öneme paralel olarak da bilgisayar ağlarının güvenliğinin performansının gerçek zamanlı olarak sağlanması ihtiyacı gündeme gelmiştir.

İşte bu doğrultuda; kablolu ya da kablosuz bir ağdan ya da iletişim kablosundan geçen paketlerin kaybolmadan, sorunsuz, hızlı ve güvenli bir şekilde geçip geçmediğinin analizinin yapılması çok büyük önem taşımaktadır.

3.14.1 Ağ Güvenliği Paketleri ve Paket Analizleri

Ağ paketi dinleme ve yakalama yazılımları arasında en çok bilinen ve kullanılanları wireshark vimax ve cain&abel gibi yazılımlardır. Bu kısımda Wireshark paket analiz yazılımının kurulumuna yer vererek ağ trafiğini inceleyeceğiz

3.14.2 Wireshark

Wireshark, 1998 yılında Ethereal adıyla sadece ağ üzerindeki sorunları dinlemeye anlamaya analiz etmeye ve tespit edilen sorunlara çözüm üretmek için geliştirilen farklı bileşenler ile çalışan bir projedir.

Wireshark adıyla yazılan bu yazılım bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkân tanımaktadır. Kısacası bilgisayara bağlı olan her türlü ağ kartlarındaki tüm Tcp/Ip paketlerini dinleyen analiz eden ve mesajlar ile raporlayan programdır.

WireShark her ne kadar casus bir yazılım olarak görülse de günümüzde farklı ve yararlı amaçlar için kullanıldığı yerler vardır. Bunlardan bazıları şunlardır;

- Şebeke problemlerinde sorun çözme
- Güvenlik problemlerini sınamak
- Uygulamaya konan protokollerde oluşan hataları onarmak veya arındırmak
- Ağ problemlerinin içindeki bilgileri öğrenebilmek amacıyla kullanılmaktadır
- Ağ uzman ve yöneticileri tarafından ağ trafiğinin incelenmesi, sorunlarının irdelenmesi/çözümlenmesi
- Ağ/bilgi güvenliği mühendisleri tarafından güvenlik problemlerinin incelenmesi

3.14.2.1 WireShark Kurulum

Windows: https://www.wireshark.org/download.html adresinden indirilebilir ve standart kurulum adımları uygulanarak kurulum işlemi gerçekleştirilebilir.

Linux: apt-get komut satırı aracında sudo apt-get install wireshark komutu ile gerekli paketlerin edinilmesi ve yükleme işlemi gerçekleştirilebilir.
Linux ortamında apt-get komut satırı aracında sudo apt-get install wireshark komutu ile gerekli paketlerin edinilmesi ve yükleme işlemi gerçekleştirilebilir. Yüklemem işleminden sonra Wireshark ile paket yapabilmek için aşağıdaki komutların gerekli sistem izinleri için koşulması gerekmektedir.

Resim 3.51 WireShark Linux kurulum.

3.14.2.2 Wireshark Özellikleri

- Windows, Unix, OSX, Solaris, FreeBSD, NetBSD ve birçok işletim sistemleri için uygundur.
- Yerel ağ ara yüzünden paketleri tutar, ayrıntılı bir şekilde protokol bilgileriyle görüntüler.
- Tutulan bilgileri kaydetme özelliği vardır.
- Çeşitli kriterler de paket arar ve filtreler.
- Çeşitli istatistikleri yapılan ayarlar doğrultusunda kullanıcıya sunar.
- Birçok protokol için şifre çözme desteği sunar. (IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP ve WPA/WPA2'yi içerir).

3.14.2.3 Wireshark İle Paket Dinleme

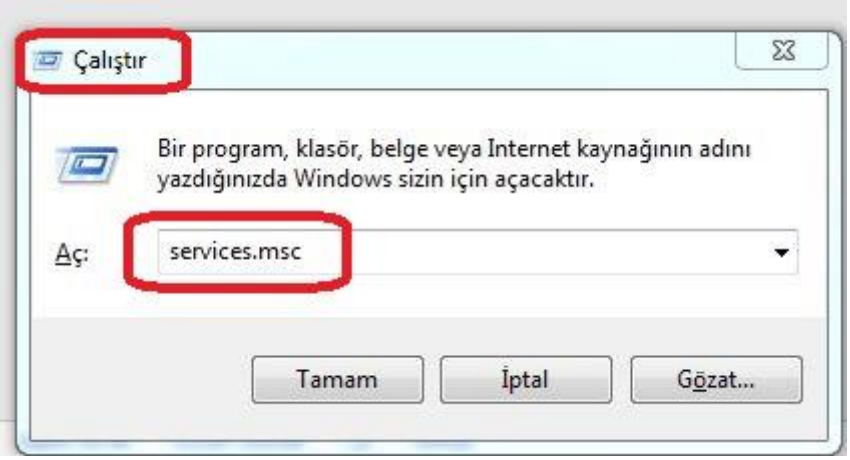
Öncelikle WireShark programı ile yapacağımız paket yakalama ve dinleme işlemlerinden önce WireShark kuracağımız bilgisayarın üzerinde yapmamız gereken ayarlamalar olacaktır.

Wireshark ile yerel ağdaki bir bilgisayarın network trafiğini dinlemek için yapılması gereken adımlar;

Network trafiği dinlenecek olan bilgisayarda olması gerekenler;

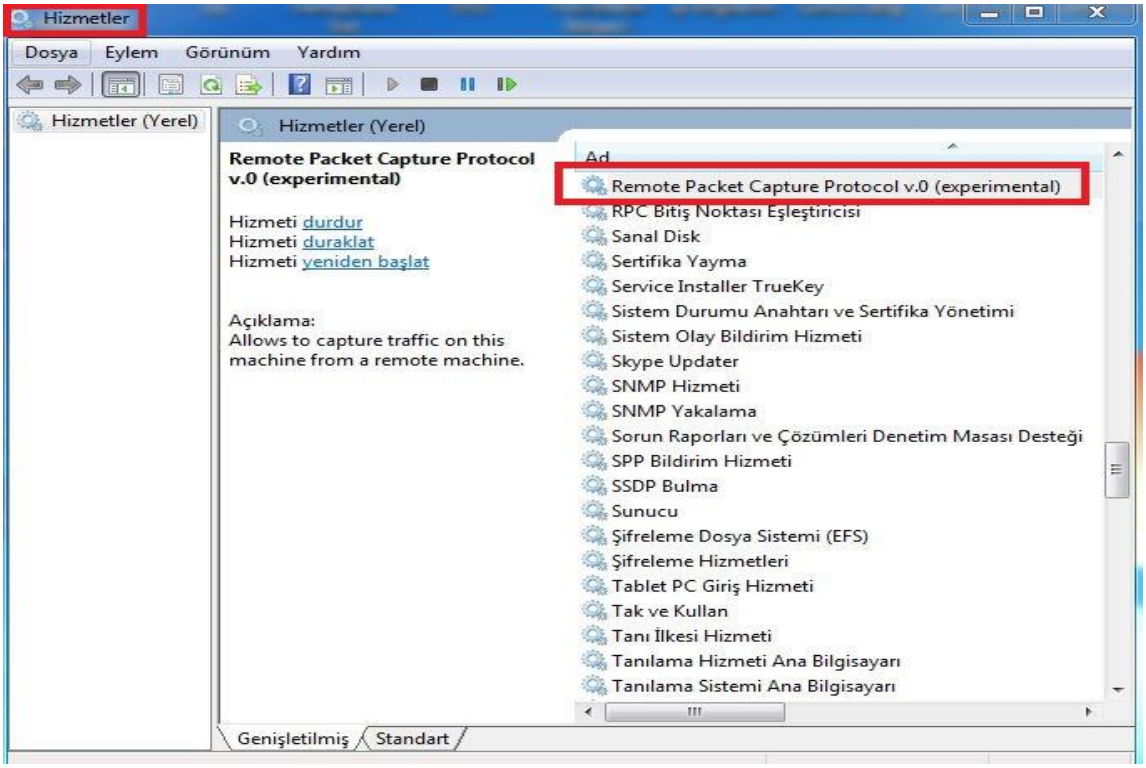
- **Administrator** yetkili kullanıcı adı ve şifresi.
- **Remote Packet Capture Protocol** değeri **enable** ve yukarıdaki kullanıcıya izinli olması.
- Uzak makinanın **windows** olması gerekiyor.

Bilgirayarımızın ***çalıştır*** *(ctrl+run)* servisine ***services.msc*** komutunu yazıp enter'a bastıktan sonra karşımıza gelen hizmetler menüsünden Uzak Paket Yakalama Protokolünü (Remote Packet Capture Protocol) aktif hale getiriyoruz.



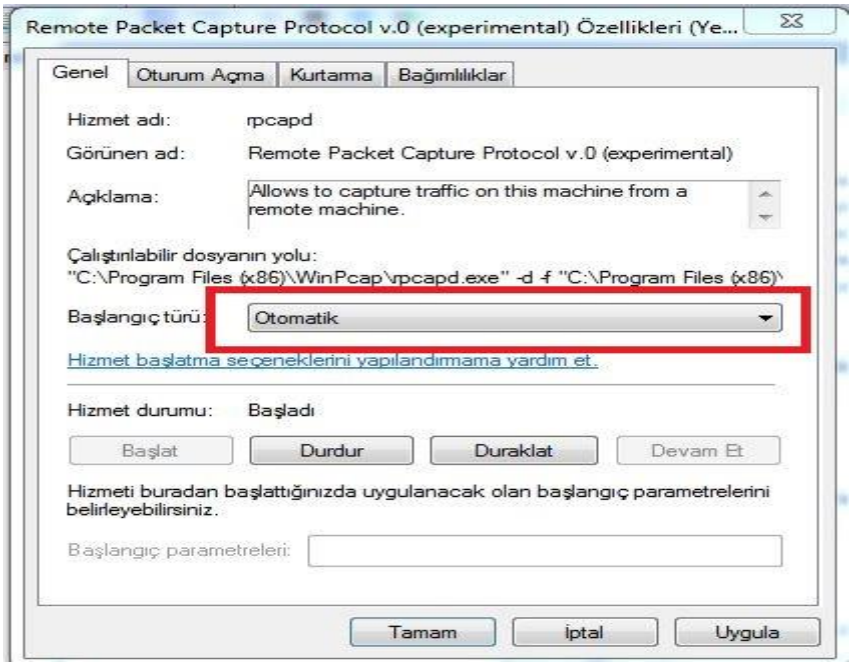
Resim 3.52 Çalıştır ekranı.

Hizmetler menüsünü açarak *Remote Packet Capture Protocol* sekmesini buluyoruz.



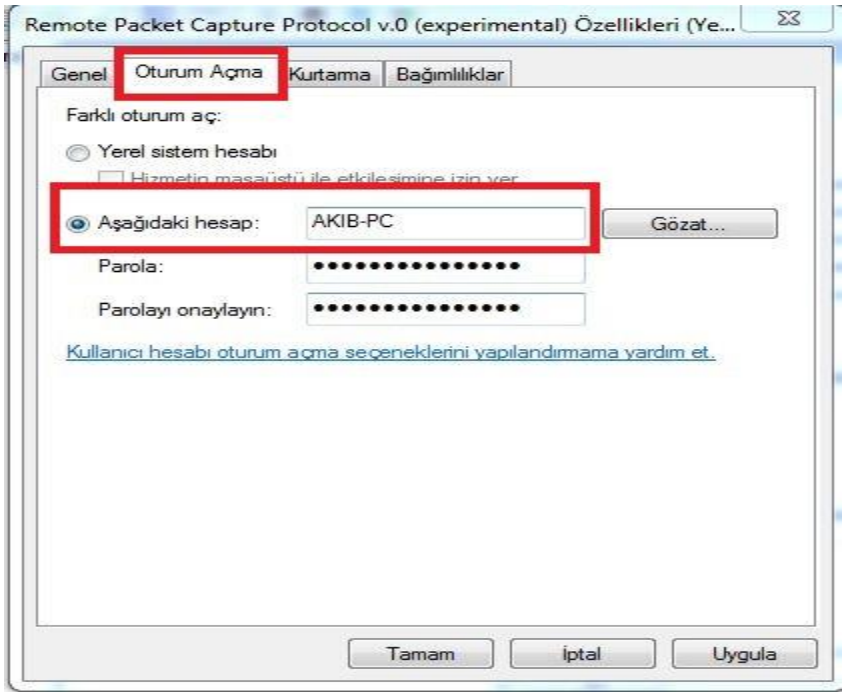
Resim 3.53 Wireshark sistem ayarları 1.

Remote Packet Capture Protocol sekmesi üzerindeki iken çift tıklayarak açılan pencerede sekme *devre dışı* ise *otomatik* hale getiriyoruz;



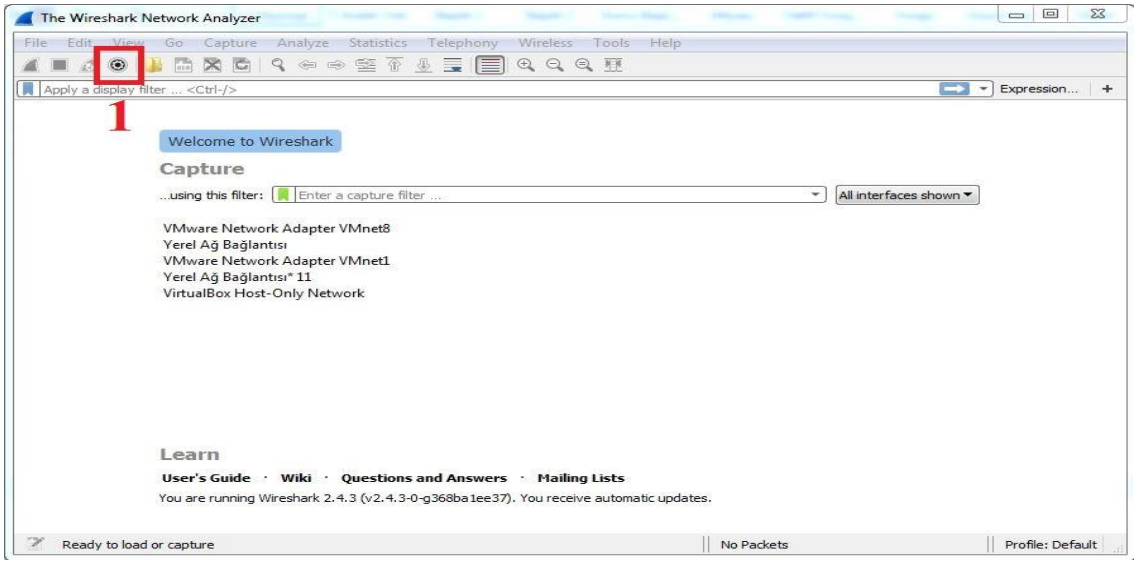
Resim 3.54 Wireshark sistem ayarları 2.

Son olarak açılan pencereden çıkmadan önce oturum aç sekmesinden izleme ve dinleme yapacağımız karşı bilgisayara ait kullanıcı bilgilerini giriyoruz.



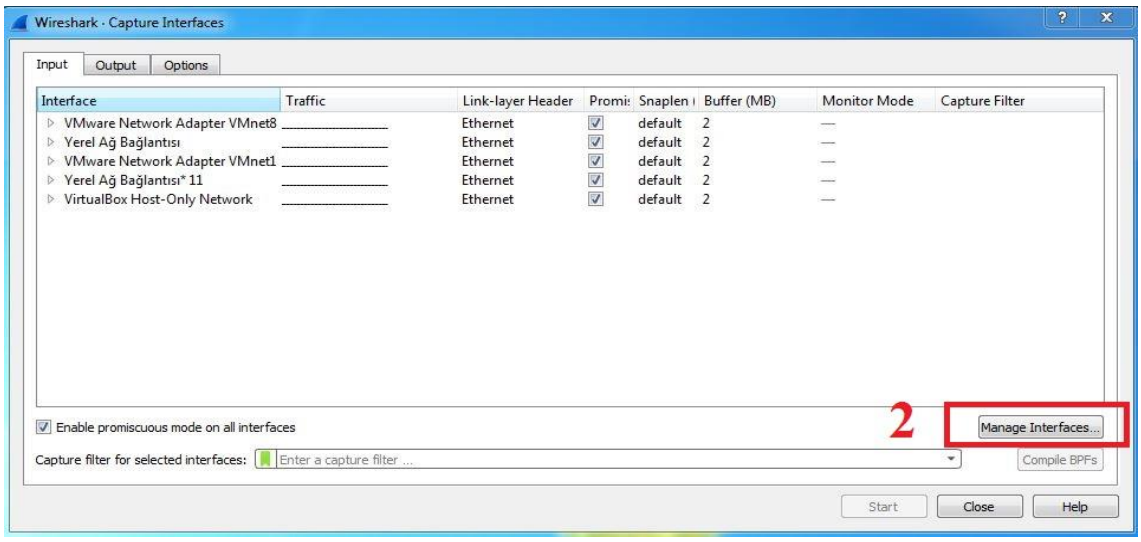
Resim 3.55 Wireshark sistem ayarları 3.

Bu işlemlerden sonra WireShark programını başlatıyoruz ve aşağıdaki resimlerde de görüldüğü gibi karşı bilgisayarı programa ekliyoruz.

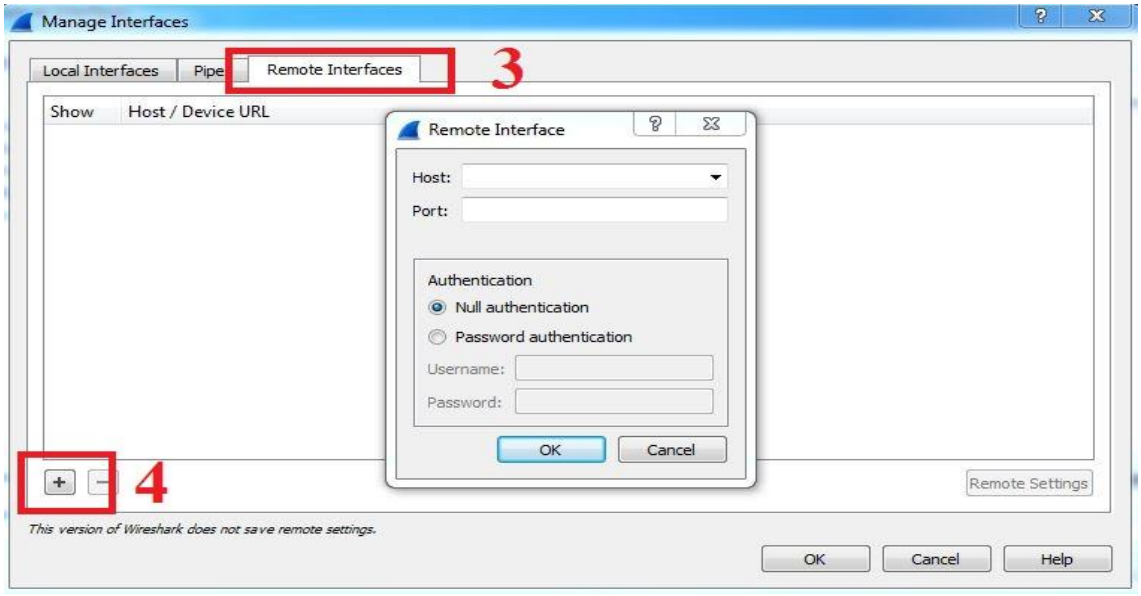


Resim 3.56 Wireshark sistem ayarları 3.

1 numara ile işaretlenen sekme *capture options* sekmesi oluyor ve bu sekmeyi seçtiğimizde aşağıdaki pencere açılıyor; 2 numara ile işaretlediğimiz *Manage Interfaces* sekmesini tıkladıktan sonra;

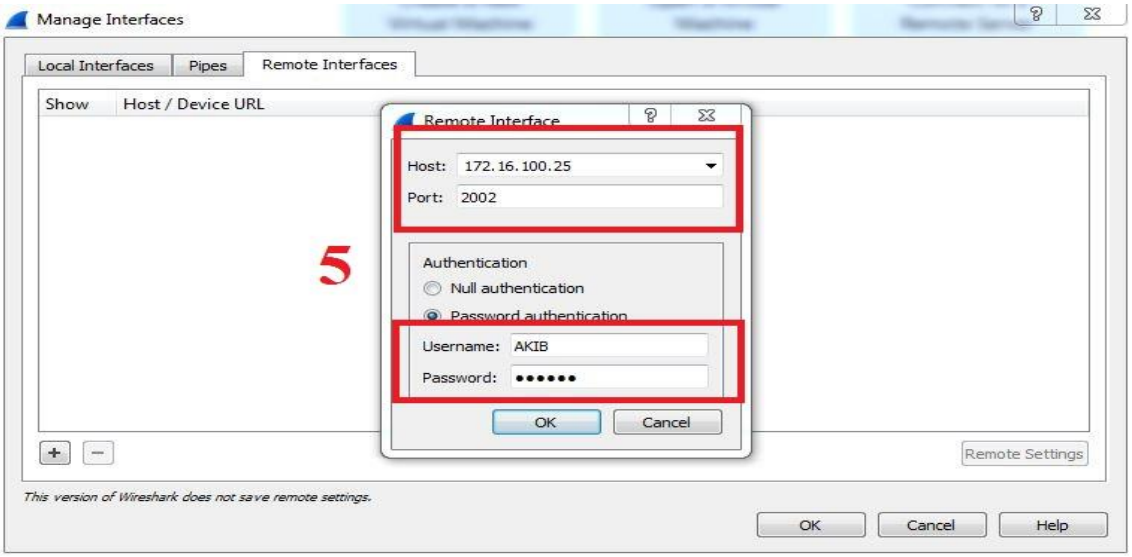


Resim 3.57 Wireshark sistem ayarları 4.



Resim 3.58 Wireshark sistem ayarları 5.

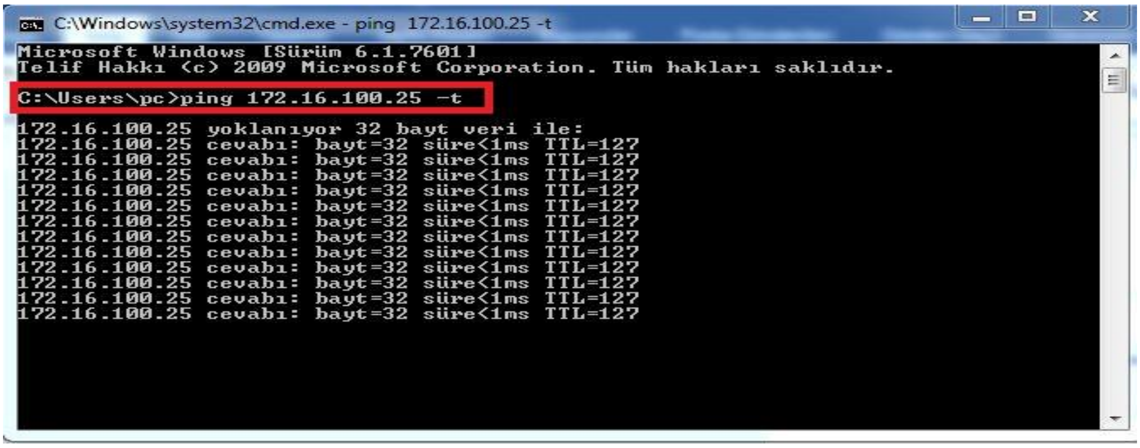
3. numara ile işaretlenen sekme olan *Remote Interfaces* sekmesini tıklayarak 4 numara ile işaretlediğimiz *add* sekmesinden programa dinleme ve izleme yapılacak karşı bilgisayarın *IP*, *Port*, *Username*, *Password* bilgilerini giriyor ve tamam diyerek karşı bilgisayarı eklemiş oluyoruz.



Resim 3.59 Wireshark sistem ayarları 6.

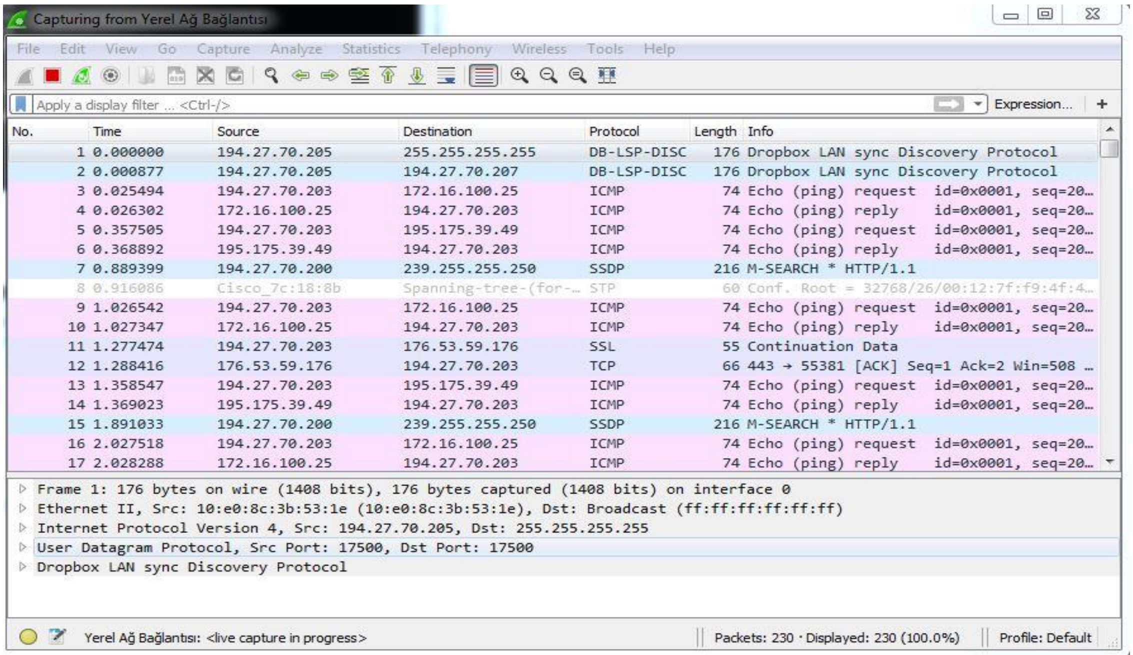
Bu adımları gerçekleştirdikten sonra Host alanında uzak makinanın network kartları görünecektir. Bu kartlardan birini seçerek trafiği dinleyebilirsiniz. Bu işlemdeki örnek penetrasyon(Pentest) testlerinin temeli oluşturan küçük bir başlangıç ayarlarıdır.

Örnekleyecek olursak WireShark programına eklediğimiz bilgisayarın Ip adresine bilgisayarımız üzerinden ping işlemi başlatıyoruz

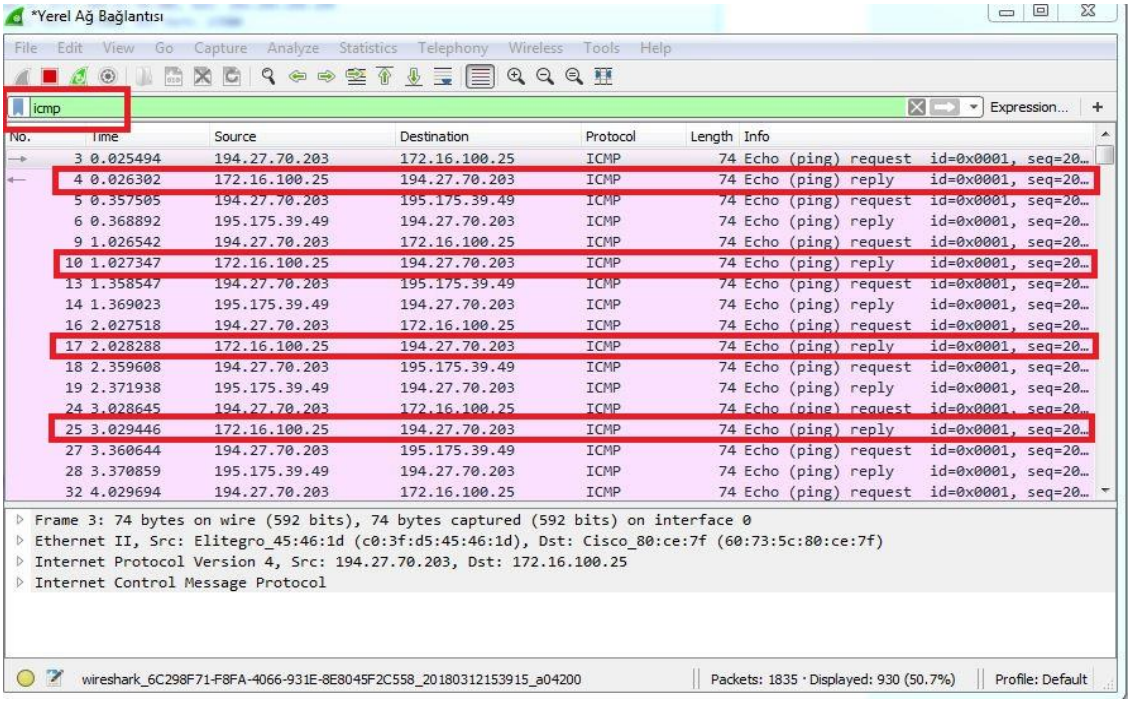


Resim 3.60 Cmd Ping penceresi.

Ping işleminden önceki filtrelenmemiş ve aynı ağ üzerinde bulunan diğer bilgisayarlardan gelen ağ trafiğinin akış görünümü;



Resim 3.61 Wireshark arayüz 1.



Resim 3.62 Wireshark arayüz 2.

Gözüktüğü gibi bu paket; Border Gateway Protocol (BGP) oturumunda, *172.16.100.25* ve *194.24.70.203* adresleri arasında yakalanmıştır. Bu paket seçilerek, açılan "Protocol Tree Window" ve "Data View Window" bölümlerinden daha da ayrıntılı incelenebilir. ***194.27.70.203** nolu Ip adresi WireShark programının kullanıldığı bilgisayara ait gerçek Ip adresidir.

Son olarak program ara yüzünde bulunan ve programı kullanırken veya başka bir bilgisayar ekleme işlemi yaparken kullandığımız ***Capture*** sekmesinde bulunan menüleri açıklayalım.

- **Capture**

- **İntarfaces:** Wiresharkın kullanacağı ağ arabirimi ve özellikleri ayarlanır.
- **Options:** Uygulama sırasında kullanılacak ağ arabirimi seçimi adres çözümleme özellikleri, görünüm özellikleri uygulama durdurmak için ayarlanacak özellikler gibi birçok ayarlanabilir bölüm içermektedir.
- **IP adress:** Seçilen ağ arabirimin sahip olduğu ip adresidir.

• **Manage Interfaces:** Karşı bilgisayarı eklemek için gerekli olan bilgilerin girildiği arayüz.

• **Capture Filter:** Paket yakalama sırasında filtreleme özelliği sunar. İstenmeyen paketlerin yakalanmasını engelleyerek hem analiz işlemini kolaylaştırır hem de programın çalışması sırasında daha az paket ile sistem kaynaklarını idareli kullanır.

3.15 TCP/IP Portları

En çok kullanılan portlar, internet üzerinden iletişim için kullanılan TCP/IP portlarıdır. Çok çeşitli başka portlar da vardır. Fakat bu yazıda genel ve sık kullanılan tcp ve udp portları açıklanacaktır.

Protokol, kendisine uyulması gereken bir talimatlar setine verilen isimdir. Bunun gibi internet üzerinden iletişimde takip edilen çeşitli talimatlar vardır. Temelde, internet üzerinde iki tip protokol vardır. Bunlar TCP ve UDP' dir. TCP aktarım kontrolü, UDP ise kullanıcı veri paketleri protokolü için vardır.

Peki neden bu protokoller internet üzerindeki basit bir iletişim için kullanılmak zorundadır. Çünkü, iletişimin güvenli ve hızlı olması gerekir. TCP'de veri transferi bir pc' den diğerine direkt olarak yapılır. İki cihaz da veri transferi için birbiriyle bağlı olması gerekir. Bu iki pc veya cihaz transfer boyunca bağlı kalır ve veri aktarımı bittikten sonra bağlantı kesilir. Diğer taraftan UDP' de veri, paketler haline getirilir ve internet üzerinden gönderilir. Burada iki pc veya cihaz arasında direkt bağlantı yoktur. Fakat UDP aktarımı güvenli bir veri aktarımı garantilemez. İletişim hızı TCP'ye kıyasla UDP'de daha yavaştır.

3.15.1 Port Güvenliği

Gün geçtikçe bilgisayar ve bilgisayar teknolojileri hayatımızın her alanında varlığını hissettirerek ve artırarak devam ettiriyor. Öyle ki herkes artık birden fazla bilgisayar ve benzeri bilgi iletişim cihazlarına sahipler. Kişisel ve iş hayatımızın her anının vazgeçilmezi olan bilgisayarları güvenli kullanmakta bilgi güvenliğimiz açısından

oldukça önemli bir hal almıştır. Günümüzde çok sayıda başkalarının bilgilerini ele geçirerek kendilerine çıkar elde etmek isteyen ve genel olarak hacker denilen saldırganlar vardır ve bu saldırganların saldırıları bilgisayar kullanımı ile doğru orantılı olarak artmaktadır.

Bu nedenle kişisel ve kurumsal olarak kullandığımız bilgisayarların dolayısı ile kişisel bilgilerimizin güvenliğini kendi kendimize sağlaya bileceğimiz basit yollarda vardır. Alınacak önlemlerin başında port güvenliği gelmektedir.

3.15.1.1 Port Güvenliği

İşletim sistemimiz üzerinde çalışan ve işletim sistemimizin üzerinden bilgisayarımıza erişim sağlamak isteyen yazılımların programların geçiş ya da giriş yaptığı kapılar vardır ve bu kapıların bilgisayar dilindeki ismi port'tur. Portlar üzerinden geçiş yapan program ve benzeri yazılımlar her zaman güvenli değildir ve bu nedenle güvenlik açığı oluşturmaktadır.

Portlar üzerinde yapılan veya alınan güvenlik önlemlerinin en başında zararlı yazılımların giriş yaptığı yapacağı portların işletim sistemimiz üzerinden kapatılmasıdır. Casus yazılım ve programların kullandığı kullanabileceği portların kısaca nasıl kapatılacağı aşağıdaki görseller ile basit şekilde gösterilmiştir.

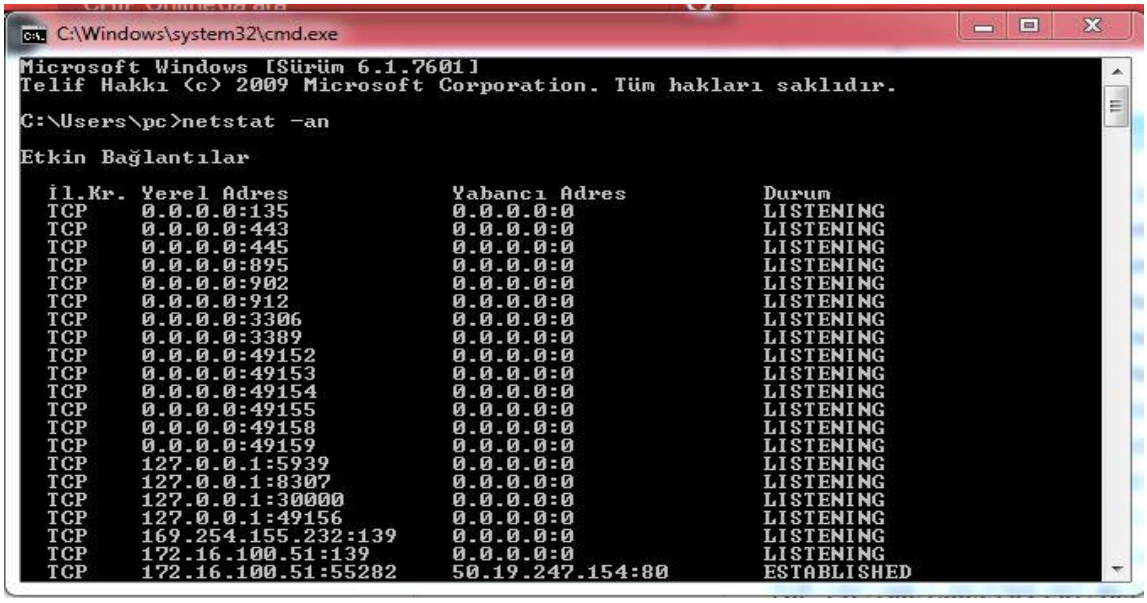
Öncelikle bilgisayarımızda açık olan portları belirlemeliyiz ve bu işlemi için aşağıdaki yolu izleyerek yapabiliriz.

3.15.1.2 Port Kullanımı

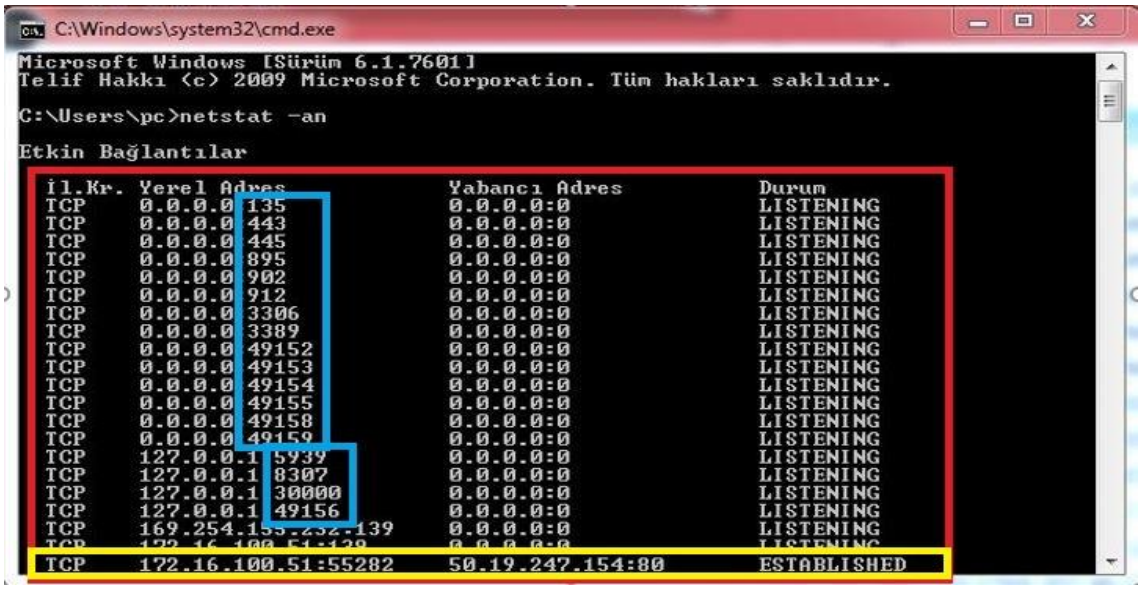
Portlarin mantığını kavrayan birisi bağlantı noktalarının ne denli önem taşıdığına vakıftır. Listening durumda olan bir port, o port'a bağlanmak için yazılmış bir tojan için güzel bir kapıdır. Sistemdeki açık ve etkin olan portları aşağıdaki işlemi yaparak bulabiliriz.

Başlat\Çalıştır cmd yazın enterlayın. Komut satırına netstat –an yazın ve PC'mizdeki açık portalar bakalım (C:\netstat -an).

Resim 3.65 'de ki cmd ekranında sistemimizde çalışan ev açık olan portlar listelenmiştir.



Resim 3.63 Cmd Port ekranı 1.



Resim 3.64 Cmd Port ekranı 2.

Resim 3.66'da kırmızı renk ile çerçevelenmiş alan sistemde bulunan tüm ip adreslerini ve ip adreslerinin üzerinden giriş yapmak isteyen ve çalışan yazılım ile programların

giriş yaptıkları yapmak istedikleri portları listelemekte iken mavi renk ile çerçevelenmiş kısımlar sistem üzerinde çalışan port'ları göstermektedir.

Portların Kapatılması:

Yukarıdaki Resimlerde de gösterilen cmd ekranındaki port listelerinde bulunan ve "Listening" = 1 nolu satırda sistemimize ait 135 no'lu port dinleme durumunda, yabancı adresten gelecek bağlantı isteğini kabul edecek ve bağlantı kurulacaktır.

"Established" = Kurulu olan mevcut bağlantılarımızdır. Örnek olarak 3.67 no'lu resimde sarı renk ile çerçevelenen alana bakabilirsiniz.

Resim 3.65 Cmd Port ekranı 3.

Sistemime ait olan 172.16.100.51 ip adresim 55282 no'lu portumu kullanarak yabancı adres olan 50.19.247.154 [CW] ile ona ait 80 no'lu portla iletişim kurmuş.

En çok kullanılan portların başında gelen ***sys_sent*** durumu vardır. Bu bizim veya uzak pc'nin bağlantı kurma isteği gönderdiği anlamındadır.

Genel olarak kurum ağlarının sistem tarafında firewall (güvenlik duvarı) kurulu olacağından firewall'un ilk kurulum aşamasında varsayılan olarak bazı portları kapalıdır. Bu kapanan portlar kullanıcıların yaptıkları işlerle ilgili olarak kullandıkları yazılım ve portların gereksinim duyacağı portlar sistem yöneticileri tarafından kullanıcı bazlı olarak açılır. Bunun dışında kişisel kullanıcılarda yaptıkları ve kullandıkları yazılım ve programlara göre kendi isteklerine cevap verecek şekilde politika belirleyebilirler. Tüm kişisel ve kurumsal bilgisayar sistemlerinde genel olarak kullanılan ve varsayılan olarak açık olan portlar vardır bunlardan bazıları şunlardır;

135.137.138.139.443.445 vb. gibi port numaraları tüm bilgisayarlarda açık olarak çalışırlar. Ancak aynı zamanda dışarıdan gelen siber saldırıların büyük bir çoğunluğu bu

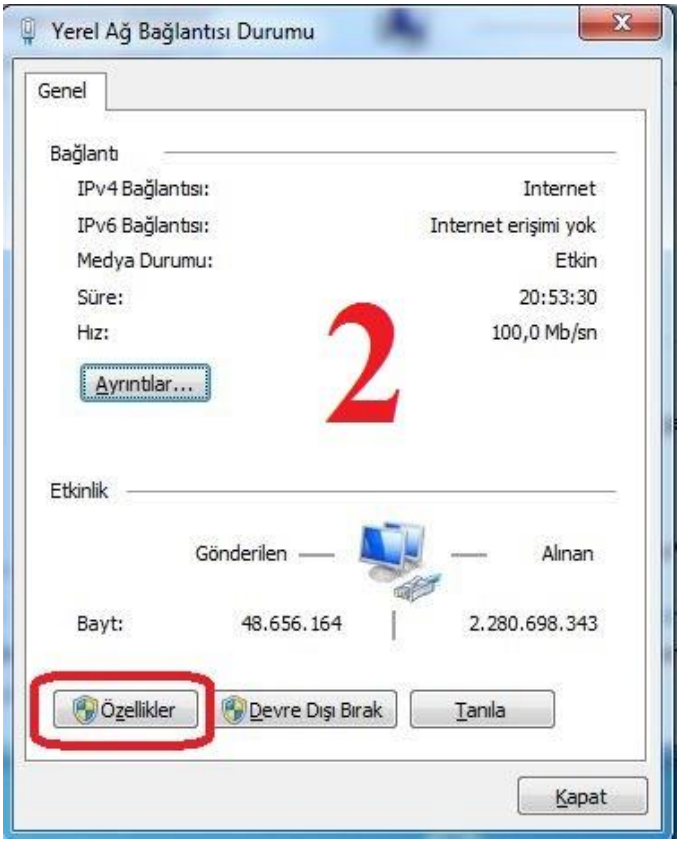
portlar üzerinden gelmekte olup bu portlar en çok saldırıya uğrayan ilk 10 port arasındadır. Sistem üzerinde varsayılan olarak açık olan bu portlar genellikle Listening durumunda oldukları için gelen tüm bağlantı isteklerini ***(syn_ent)*** yani kabul ederler.

Sistemimiz 'de net stat -an sonucu açık olarak listelenen portların bilgisayarımız üzerinden nasıl kapatılacağını görelim. Birçoğumuz dns ayarlarımızı değiştirmek için kullandığı ağ bağdaştırıcı ayarları menüsünde port kapatma işlemini paylaşılan görsellerde görebiliriz.

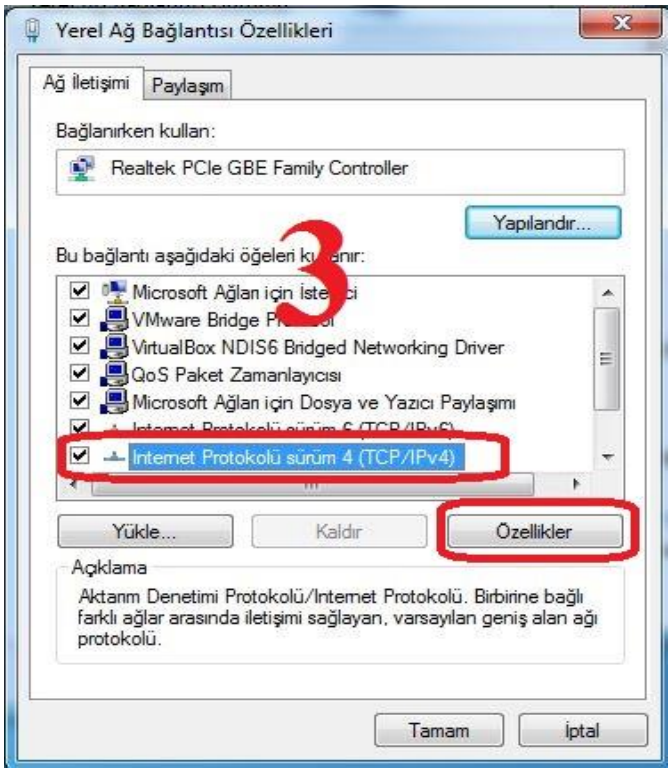
Sırasıyla portları kapatmak için sırasıyla; Yerel Ağ Bağlantısı\\Özellikler\\İnternet İletişim Kuralları(TCP/IP) çift tıklıyoruz ardından gelişmiş tuşuna tıklıyoruz ve WINS sekmesine geçip en altta TCP/IP üzerinden NetBoıs'u devre dışı bırak işaretleyip tamam dedikten sonra modemimizi kapatıp tekrar açıyoruz ve bu işlemden sonra 137,138 ve 139 portlarını kapatmış oluyoruz. Portların kapatıldığını yine cmd ekranında netstat -an işlemini yaparak kontrol edebiliriz. Ancak bu işlem kişisel bilgisayarlarımızda etkili olabilir dhcp sunucu üzerinden alınan sanal bir ip ile internet erişimi sağlanan kurumsal yapılarda firewall olacağından bu işlemin yapılması fayda sağlamayacaktır.

Kısacası birçoğumuzun kişisel bilgisayarlarında DNS ayarlarını değiştirmek için kullandığı menülerden yapıyoruz port kapatma işlemini.

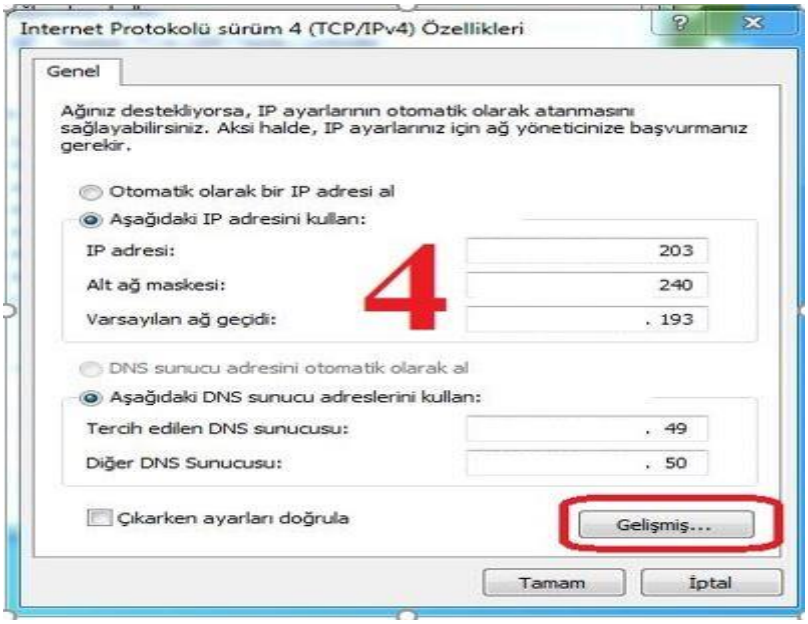
Resim 3.66 Yerel ağ bağlantısı.



Resim 3.67 Yerel ağ bağlantısı durumu.



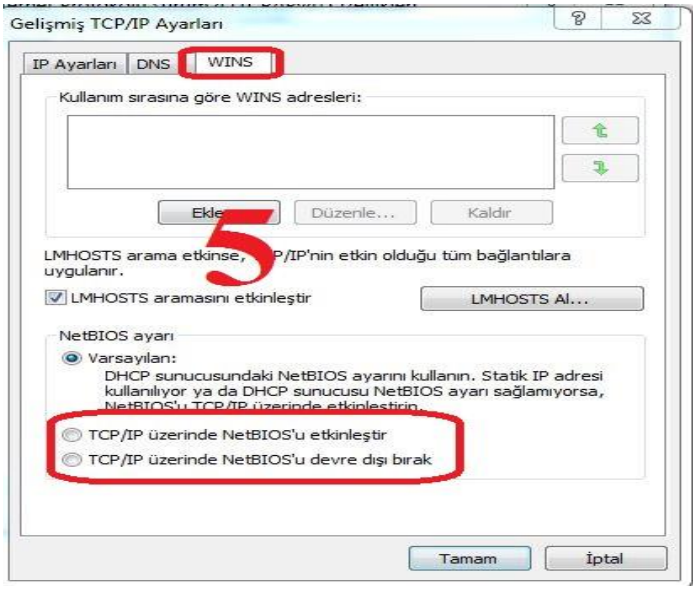
Resim 3.68 Yerel ağ bağlantısı özellikleri.



Resim 3.69 IPS ayarları.

Son olarak TCP/IP üzerinde NetBIOS etkinleştir seçeneğini tıkladıktan sonra modemimizi kapatıp tekrar başlatıyoruz.

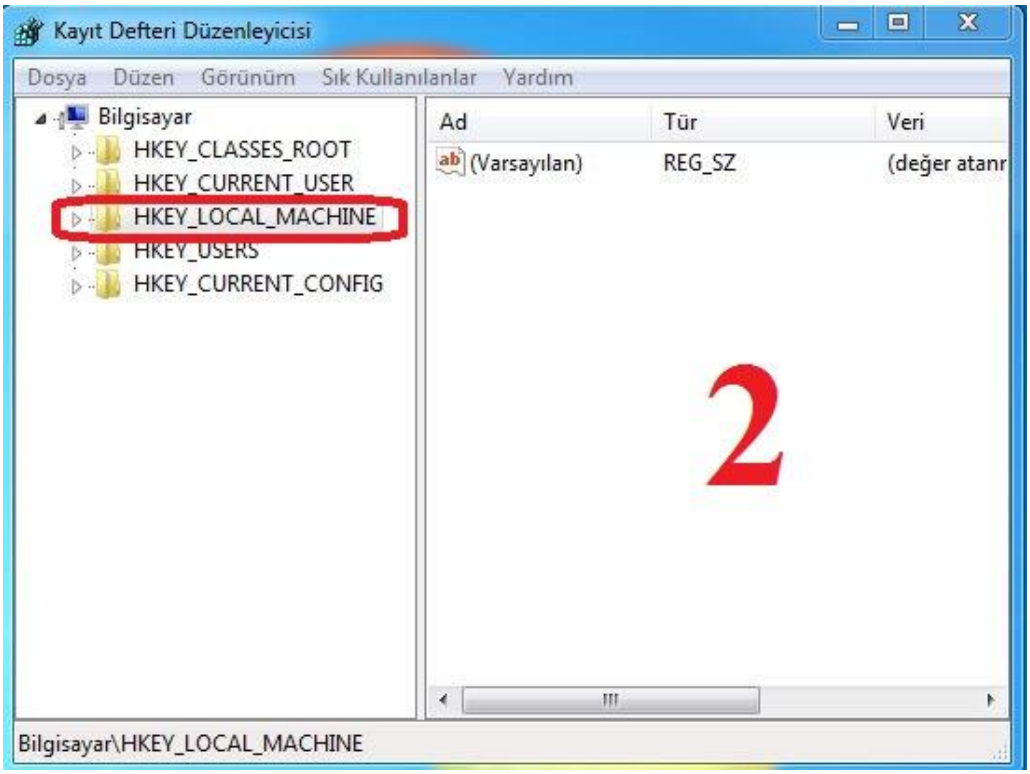
• Yapılan işlemde dikkat ettiğiniz üzere statik ip kullanıldığı için bu işlemin sonuçlarını görmememiz mümkün olamayacağından işlem sonunda "NetBIOS etkinleştir" seçeneği seçilmeyip varsayılan olarak bırakılmıştır.



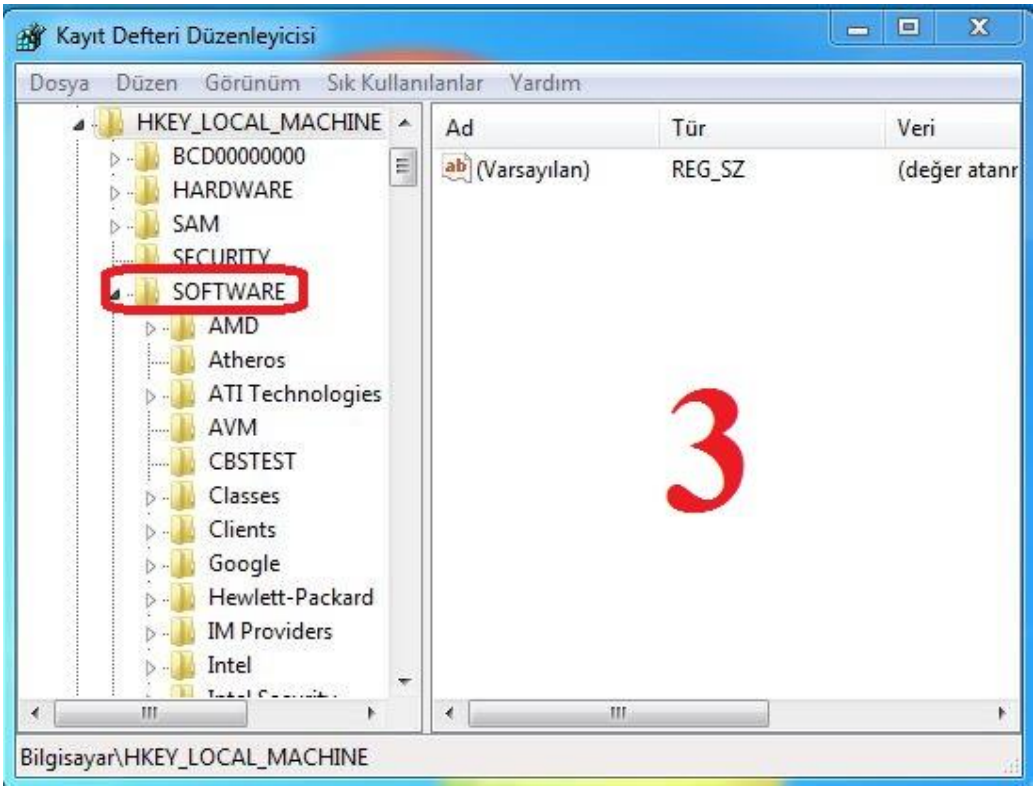
Resim 3.70 Gelişmiş Ips ayarları.

Son olarak port kapatma işleminde 135. Portun nasıl kapatılacağını görelim. Bu işlem bilgisayarımızın kayıt defteri olan sistem dosyalarının bulunduğu menülerden yapıyoruz.

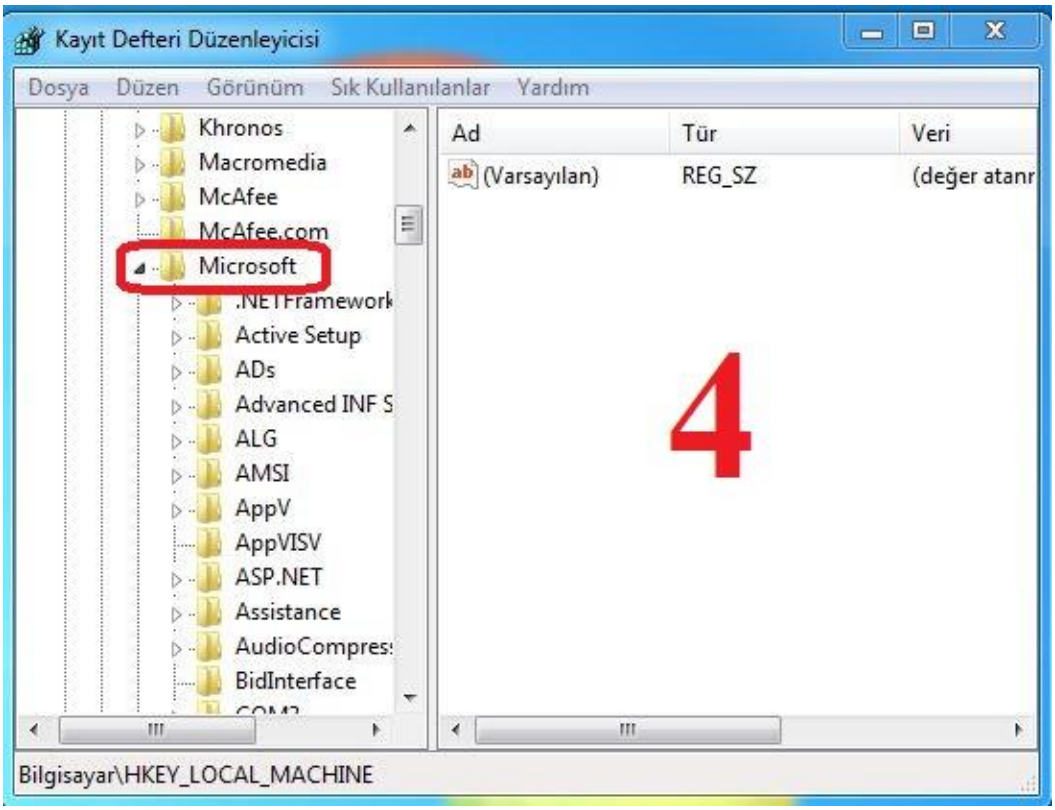
Resim 3.71 Çalıştır ekranı.



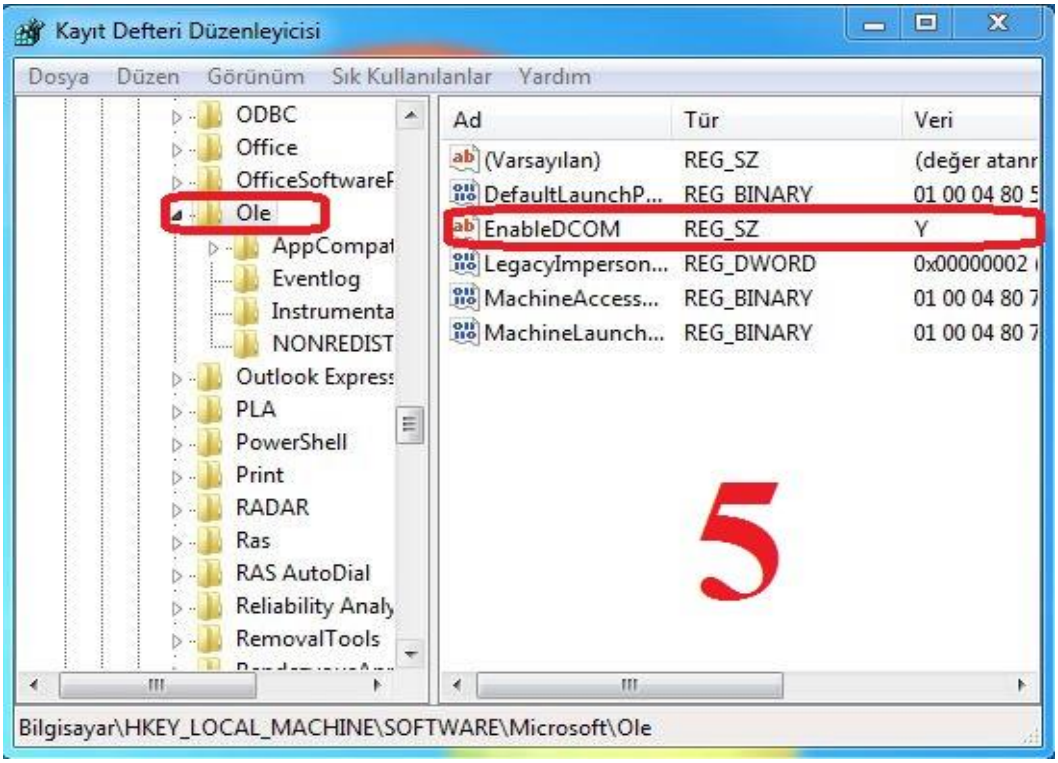
Resim 3.72 Kayıt defteri port ayarları 1.



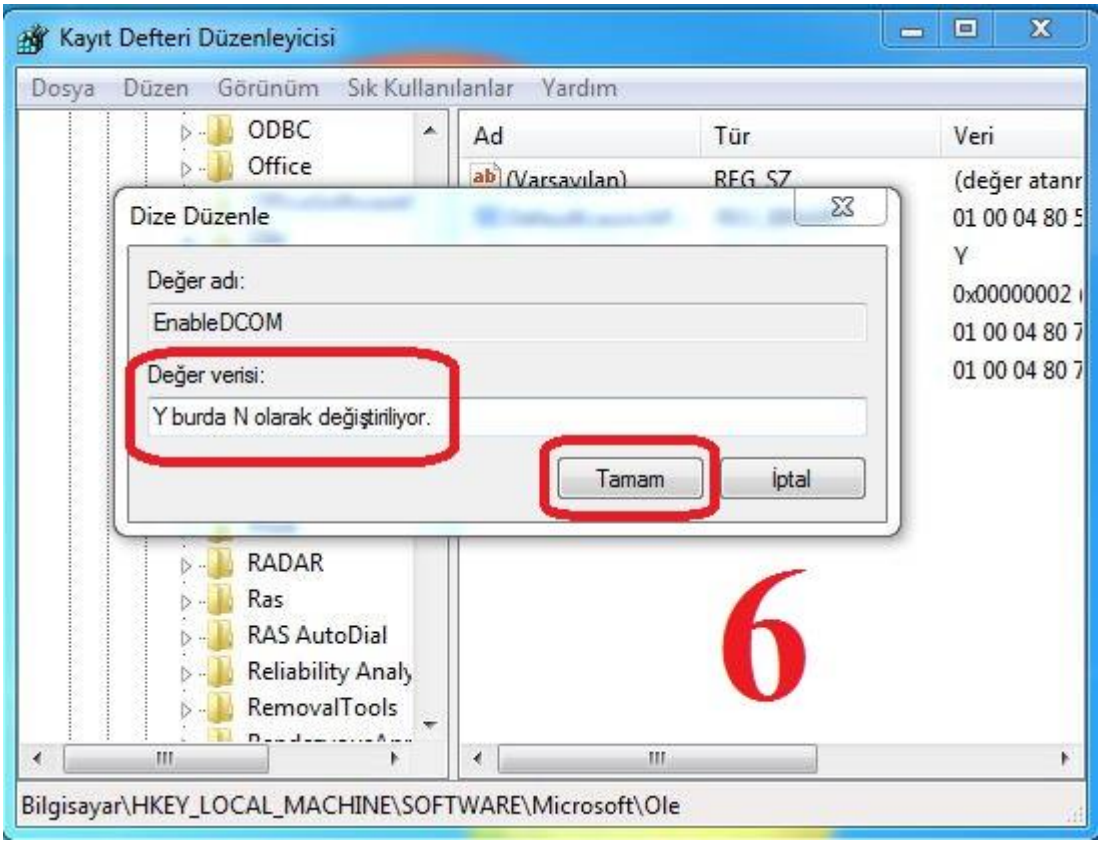
Resim 3.73 Kayıt defteri port ayarları 2.



Resim 3.74 Kayıt defteri port ayarları 3.



Resim 3.75 Kayıt defteri port ayarları 4.



Resim 3.76 Kayıt defteri port ayarları 5.

Ve yine son olarak regedit menüsü içerisinde iken bir üst basamakta RPC yi açarak (HKLM\Software\Microsoft\RPC) sağ tarafta DCOM Protocols girdisini çift tıklayarak ve ncacn_ip_tcp adlı veriyi silip diğerlerine dokunmadan tamam dedikten sonra regedit menüsünden çıkıyoruz.

• Unutmayın ki kayıt defterinde bilinçsizce yapacağınız herhangi bir işlem sisteminizin sağlıksız ve sorunlu çalışmasına sebebiyet verecektir, kayıt defteri menüsünde iken azami dikkat göstermeniz yararınıza olacaktır.

443. port Https SSL sertifikasına sahip olan kurumsal firma ve kuruluşların ile daha çok bankaların web adreslerinde kullandıkları port'tur.

Örneğin;

Resim 3.77 SSL Sertifikalı Web adresi.

3.15.1.3 Başlıca Kullanılan TCP/IP Portları

msp	TCP, UDP	18	Message Send Protocol
ftp	TCP, UDP	21	File transfer protocol
ssh	TCP, UDP	22	Remote login protocol
telnet	TCP, UDP	23	Telnet
smtp	TCP, UDP	25	Simple Mail Transfer Protocol
domian	TCP, UDP	53	Domain Name Sever
www	TCP, UDP	80	World Wide Web veya HTTP
rtelnet	TCP, UDP	107	Remote Telnet Services
pop 2	TCP, UDP	109	Post Office Protocol 2
pop 3	TCP, UDP	110	Post Office Protocol 3
sftp	TCP, UDP	115	Simple File Transfer Protocol
snmp	TCP, UDP	161	Simple Network Management Prot.
bgp	TCP, UDP	179	Border Gateway Protocol

Veri iletişiminde kullanılan port numaraları cihaz kimliğini tayin edemez fakat tayin edilen servisi uygulamak için kullanılırlar. Örneğin HTTP, web servisleri için, FTP ise dosya transferi için kullanılır. Bu portların ismi sağlanacak servisi ifade eder.

4. BULGULAR

Bu çalışmanın değerlendirilmesinde nitel araştırma yöntemlerinden istifade edilmiştir. Nitel araştırma "gözlem, görüşme ve doküman analizi gibi nitel veri toplama tekniklerinin kullanıldığı, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konmasına yönelik nitel bir sürecin izlendiği araştırma" olarak tanımlanmaktadır (Yıldırım ve Şimşek 2016).

4.1 Çalışmanın değerlendirilmesi

Bu çalışma Afyon Kocatepe Üniversitesi Bilgisayar ve Eğitim Teknolojileri Öğretmenliği bölümü 3.ve 4. Sınıf öğrencilerinden 40 öğrenciye kaynak olarak sunulmuştur. Hazırlanmış olan çalışmanın değerlendirilmesinde 10 öğrenci seçilerek, seçilen bu 10 öğrenciye çalışmanın yararlılığı ve öğrenciler üzerindeki etkisi ile çalışmanın kaynak olarak sunulmasından önce ve sonraki Bilgisayar ve Ağ Güvenliği dersine karşı olan farkındalık ve ilgi seviyelerini ölçmek ve değerlendirmek amacıyla 10 adet değerlendirme sorusu sorulmuştur.

4.2 Çalışmayı Değerlendirmeleri İstenen Öğrenci Grubu

Çizelge 4.1 Değerlendirme yapan öğrenci grubu.

NO	KOD	CİNSİYET	BÖLÜM	SINIF
1	P1	ERKEK	BÖTE	3
2	P2	ERKEK	BÖTE	4
3	P3	KADIN	BÖTE	4
4	P4	ERKEK	BÖTE	3
5	P5	KADIN	BÖTE	4
6	P6	KADIN	BÖTE	3
7	P7	ERKEK	BÖTE	4
8	P8	KADIN	BÖTE	3
9	P9	KADIN	BÖTE	3
10	P10	ERKEK	BÖTE	4

Amaçlı örneklem yöntemlerinde olan maksimum çeşitlilik örneklem yöntemi "Maksimum çeşitlilik örneklemi; evrende incelenen problemle ilgili olarak kendi içinde benzeşik farklı durumların belirlenerek çalışmanın bu durumlar üzerinde yapılmasıdır. Burada araştırmacı araştırdığı sorunların türleri ve yoğunluğunda değişme olabileceğine inandığı farklı durumları örneklemine alabilecektir. Bu tür bir örneklemede genelleme kaygısı olmamakla birlikte, problemle ilgili farklı durumların örnekleme alınması nedeniyle, evren değerleri hakkında önemli ipuçları verebileceği söylenebilir" (Uysal, 2010).

4.3 Değerlendirme Sorularının Hazırlanması

Bu çalışmanın hazırlanma aşamasında Bilgisayar ve Ağ Güvenliği dersi kapsamında hazırlanmış olan diğer kaynaklar incelenmiş olup diğer tüm kaynakların değerlendirme sürecinde kullanıldıkları yöntemler araştırılmıştır. Ve ayrıca konusunda uzman kişilerin görüşleri de alınarak öğrencilerin farkındalıklarının artırılmasına yönelik tüm değerlendirme sorularından istifade edilerek sonuçlarda en maksimum seviyede verilerin elde edilmesinin sağlayıcı olmasına özen gösterilmiş ve çalışmanın öğrenciler üzerindeki etkisini ölçe bilecek değerlendirme soruları hazırlanmıştır.

Hazırlanan değerlendirme sorularının Bilgisayar ve Ağ Güvenliği dersi alan tüm öğrencilerin kaynak olarak kullanmak isteyecekleri ve öğrencilerin farkındalık düzeylerinin artırılmasına etki edecek verilerin elde edilmesi için benimsenen bu yöntemin tercih edilme sebebi öğrencilerin dersin kapsadığı konularda yaşadıkları sorunların etraflıca ortaya konulması hedeflenmiştir. (Yıldırım ve Şimşek 2016)

4.4 Değerlendirme Verilerinin Toplanması

Hazırlanan bu çalışmayı değerlendirmeleri istenen ve Tablo 4.1'de sunulan öğrencilerin seçilmelerinin en önemli sebebi derse katılımlarının gözetilerek seçilmeleri olmuştur. Hazırlanan değerlendirme soruları öğrencilere eğitim sonunda elektronik ortamda gönderilmiş olup öğrencilerden sorulara belirli bir zaman diliminde yanıtlamalarını

istemek yerine esnek bir zaman dilimi sunarak öğrencilerden gelen geri dönüşlerin daha gerçekçi olması ve daha faydalı sonuçlara ulaşılması amaçlanmıştır.

4.5 Bilgisayar ve Ağ Güvenliği Dersi Uygulama Değerlendirme Soruları

1. Uygulama öncesi bilgisayarınızın güvenlik önlemlerini alıyor muydunuz?

2. Uygulama öncesi bilgisayar güvenliği hakkında kendinizin yeterli bilgiye sahip olduğunuzu düşünüyor muydunuz?

3. Uygulamada kullanılan yöntemden ve anlatımdan memnun kaldınız mı?

4. Uygulama kapsamını içerik olarak yeterli buldunuz mu?

5. Uygulama içeriğinin güncel konuları kapsadığını düşünüyor musunuz?

6. Uygulamada anlatılan yazılım ve programlar hakkında daha önce bilginiz var mıydı?

7. Uygulama içeriğini teknik olarak yeterli buldunuz mu?

8. Uygulama sonrası edindiğiniz bilgilere göre ağ güvenliği konusunda kendinizi yeterli buluyor musunuz?

9. Uygulama sonrası bilgisayar ve ağ güvenliği konusundaki farkındalığınız arttı mı?

10. Edindiğiniz bilgiler ile ortak kullanım alanlarında kendi ağ güvenliğinizi sağlayacak yeterli bilgiye sahip olduğunuzu düşünüyor musunuz?

4.6 Verilerin Analizi, Bulgular ve Değerlendirme

Hazırlanan çalışmayı değerlendirmesi istenen öğrenciler, Bilgisayar ve Ağ Güvenliği dersine katılımı ve diğer öğrencilere nazaran derse karşı ilgileri daha fazla olanlar

arasından seçilmişlerdir. Elde edilen verilerin bulguların analiz edilmesinde betimsel analiz yöntemi kullanılmıştır. “Betimsel analiz, çeşitli veri toplama teknikleri ile elde edilmiş verilerin daha önceden belirlenmiş temalara göre özetlenmesi ve yorumlanmasını içeren bir nitel veri analiz türüdür. Bu analiz türünde araştırmacı görüştüğü ya da gözlemiş olduğu bireylerin görüşlerini çarpıcı bir biçimde yansıtabilmek amacıyla doğrudan alıntılara sık sık yer verebilmektedir. Bu analiz türünde temel amaç elde edilmiş olan bulguların okuyucuya özetlenmiş ve yorumlanmış bir biçimde sunulmasıdır” (Özdemir 2011).

“Betimsel analiz dört aşamada gerçekleşmektedir. Birinci aşamada araştırmacı araştırma sorularından, araştırmanın kavramsal çerçevesinden ya da görüşme ve gözlemlerde yer alan boyutlardan hareket ederek veri analizi için bir çerçeve oluşturur. Böylece verilerin hangi temalar altında düzenleneceği ve sunulacağı belirlenmiş olur. Ardından, araştırmacı daha önce oluşturmuş olduğu çerçeveye dayalı olarak verileri okur ve düzenler. Bu süreçte verilerin anlamlı ve mantıklı bir biçimde bir araya getirilmesi önem taşımaktadır. Bu aşamadan sonra araştırmacı düzenlemiş olduğu verileri tanımlar. Bunun için gerekli yerlerde doğrudan alıntılara da başvurmak zorunda kalabilir. Bu sürecin sonunda araştırmacı tanımlamış olduğu bulguları açıklar, ilişkilendirir ve anlamlandırır. Araştırmacı bu aşamada ayrıca yapmış olduğu yorumları daha da güçlendirmek için bulgular arasındaki neden sonuç ilişkilerini açıklar ve ihtiyaç duyulması durumunda farklı olgular arasında karşılaştırma yapar” (Özdemir 2011).

Değerlendirme sonunda elde edilen verilere dayanılarak öğrencilerin ilgili ders kapsamındaki konulardaki eksiklikleri ve çalışmaya yön vermesi açısından da veriler ışığında çıkarımlar elde edilerek çalışmanın en optimal şekilde öğrenciler tarafından istifade edebilmeleri ve uygulanabilir olmasına özen gösterilmiştir.

4.6.1 Uygulamanın Sonuçlarının Değerlendirilmesi

Yazılı olarak hazırlanan çalışmayı değerlendirmesi istenen öğrencilerden gelen geri dönüşlere göre çalışmanın genel anlamda yararlı olduğu ancak Bilgisayar ve Ağ Güvenliği dersini kapsayan konuların içerik olarak daha fazla örneklemeler ile

desteklenmesi gerektiğini ifade etmişlerdir. Ve kaynak olarak daha faydalı şekilde istifade edebilmeleri için kaynağa ayrılan zamanın daha geniş ve devamlılığı olması konusunda görüş birliğine varmış oldukları değerlendirilmiştir. Örneğin, P1 öğrencisi ***"Anlatımdan memnun kaldım ama farklı yöntemler de kullanılabilirdi"*** demiştir. P3 öğrencisi ise ***"İçerik geliştirilebilir"*** diyerek çalışmanın kapsamındaki konuların içeriklerinin daha fazla olması gerektiğini ifade etmiştir.

Değerlendirme sonunda genel olarak öğrencilerin bilgisayar ve ağ güvenlikleri hakkında çok fazla bilgiye sahip olmadıkları ama çalışma sonrası farkındalıklarının ve bilgi seviyelerinin arttığı anlaşılmıştır. Örneğin P2 öğrencisi: ***"Kısmen yeterli buluyorum öncesinden bilgim az olduğu için şu an yeterli miktarda bilgi sahibiyim"*** demiştir. Diğer taraftan öğrencilerin bilgisayar ve ağ güvenlikleri konusunda kendi güvenlik önlemleri almaları konusunda farkındalıklarını ve şekilde bilgi sahibi olmadıkları değerlendirilmiştir. Öğrencilerin geneli (P1, P2, P3, P4, P5, P6, P7, P8, P94, P10) **"Uygulama öncesi bilgisayar güvenliği hakkında kendinizin yeterli bilgiye sahip olduğunuzu düşünüyor muydunuz?"** sorusuna ***"Hayır düşünmüyordum"*** cevabı vermiştir.

Uygulamanın değerlendirilme sorularının arasında olan **"Uygulama öncesi bilgisayar güvenliği hakkında kendinizin yeterli bilgiye sahip olduğunuzu düşünüyor muydunuz?"** Sorusuna öğrencilerin geneli ***"çok az bilgim vardı"*** ya da ***"hiçbir bilgim yoktu"*** diyerek yanıtlamışlardır. Bir diğer **"Uygulama öncesi bilgisayarınızın güvenlik önlemlerini alıyor muydunuz?"** değerlendirme sorusuna yine öğrencilerin tamamı (P1, P2, P3, P4, P5, P6, P7, P8, P9, P10) ***"Hayır almıyorum"*** olarak yanıtlamışlardır.

Çalışmanın hazırlanma aşamasından benzer kaynaklara göre daha sade ve daha anlaşılır olmasına dikkat edilmiştir. **"Uygulama içeriğinin güncel konuları kapsadığını düşünüyor musunuz?"** sorusuna da yer verilmiş olup öğrencilerin (P1, P2, P4, P5, P6, P7, P8, P10) çoğunluğu ***"Evet içeriğinin güncel olduğunu düşünüyorum"*** derken. P3 ve P9 öğrencileri çalışmanın içerik olarak güncel konulara fazla yer verildiğini düşünmediklerini ifade etmişlerdir.

Öğrencilere sorulan değerlendirme sorularının arasında bulunan **"Uygulama içeriğini teknik olarak yeterli buldunuz mu?"** sorusuna öğrencilerin tamamına yakını ***"Evet teknik olarak içeriği yeterli buldum"*** demişlerdir.

Çalışmanın asıl amacı olan Bilgisayar ve Ağ Güvenliği dersine karşı olan farkındalığı ve ilgiyi artırmak olmasından da kaynaklı olarak öğrencilere sorulan sorular arasında verilerin değerlendirme kısmının da en önemli donesi ve geri dönüşü olan **"Uygulama sonrası bilgisayar ve ağ güvenliği konusundaki farkındalığınız arttı mı?"** sorusuna öğrencilerin tamamına yakını (P1, P2, P3, P4, P5, P6, P7, P8, P94, P10) ***"Tam olarak değilse de bilgi çalışma sonrası bilgi sahibi oldum ve farkındalığım arttı"*** olarak yanıt vermişlerdir.

Sonuç olarak çalışmanın değerlendirilmesi için belirlenen kriterler çerçevesinde seçilen öğrencilere sorulan sorulara gelen geri dönüşler değerlendirildiğinde, değerlendirmeye katılan öğrencileriler çoğunluğu (P1, P2, P4, P5, P6, P7, P8, P10) çalışmayı faydalık bulduklarını ve kendileri üzerinde Bilgisayar ve Ağ Güvenliği konusunda farkındalıklarının arttığını ifade ederken diğer öğrencilerden P3 kişisi çalışmaya ayrılan sürenin ve çalışmanın kapsadığı konuları yetersiz bulduğunu ifade ederken P9 öğrencisi çalışmayı içerik olarak faydalı bulduğunu ancak yer verilen uygulama kısımlarının yetersiz kaldığını ifade etmiştir.

5. TARTIŞMA ve SONUÇ

Bilgisayar ve Ağ Güvenliği ders müfredatını kapsayan konularda tekdüze ve alışalı gelmiş anlatımdan ziyade çalışmanın içeriğinde daha yenilikçi ve uygulanabilir örneklemelere yer verilerek öğrencilerin derse karşı olan ilgilerini artırmaya yönelik güncel konulara da değinilmiş ve bu şekilde öğrencilerin derste öğrendiklerinin daha kalıcı olmasının sağlanması amaçlanmıştır.

Öğrencilerin Bilgisayar ve Ağ Güvenliği konusunda sanılanın aksine bilgi seviyelerinin ve farkındalık düzeylerinin olması gerekenin çok altında olduğu saptanmış ve derse konu olan içeriklerin öğrencilerin bilgi düzeylerine göre hazırlanmasına dikkat edilerek öğrencilerden gelen geri dönüşlerde dikkate alınarak dersin konularını oluşturan içerikler birkaç kez revize edilerek güncellenmiştir.

Çalışmanın asıl amacı öğrencilerin bilgi seviyeleri artırmaktan ziyade derse olan farkındalıklarının artmasını sağlamaktır. Bilgisayar ve Ağ Güvenliği dersine ve ders içeriğini oluşturan konulara dair farkındalıkları artırılan öğrencilerin derse olan ilgilerinin ve öğrenme arzularının arttığı gözlemlemiştir.

Hazırlanan bu çalışmanın konusunu oluşturan Bilgisayar ve Ağ Güveliği dersini kapsayan konuların içeriklerinin hazırlanma aşamasında çok fazla teknik bilgi ve dokümana yer vermeden öğrencilerin veya bu çalışmayı kaynak olarak kullanacak olan kişisel bilgisayar kullanıcılarının da rahatlıkla anlayabilecekleri temel seviye bilgilerini artırabilecekleri içeriklere yer verilmiştir.

Çalışmanın, Afyon Kocatepe Üniversitesi Bilgisayar ve Öğretin Teknolojileri Bölümü öğrencilerine bir dönem boyunca kaynak olarak sunulması ve uygulanmasından sonra yapılan değerlendirme verilerine göre öğrencilerin geneli çalışmayı içerik olarak yeterli bulduğunu ifade etmiştir. Uygulamayı değerlendiren öğrencilerden gelen geri dönüşleri çalışmanın içerik olarak yeterli düzeyde olduğunu gösterirken öğrencilerin genel olarak kişisel bilgisayar güvenlik önlemlerini almak konusunda ihmalkâr davrandıkları görülmüştür. Öğrencilere uygulamayı değerlendirmeleri için sorulan sorulara verdikleri

cevaplar bilgi güvenliği konusuna önem vermedikleri gibi bu hususta endişe duymuyor olmadıklarını da göstermiştir.

Çalışmanın öğrenciler nezdinde diğer kaynaklara göre yapılan değerlendirmesinde, içerik olarak sade, anlaşılır ve uygulamaları ile birlikte istifade etmek isteyecekleri bir kaynak olabileceği öğrencilerin çoğunluğu tarafından ifade edilerek desteklenmiştir. Ve bu anlamda öğrencilerde gelen geri dönüşlere göre olumlu veya olumsuz yanıtlarının net olarak kestirimini yapabilmek için, nicel araştırma yöntemlerine nitel çalışmalar da geliştirilip daha net sonuçların gerekçeleriyle alınabileceği düşünülmüştür.

6. KAYNAKLAR

Aysal, H. (2007). Güvenlik ve İnternet Erişim Politikaları Oluşturulması: İstanbul Üniversitesi'nde Uygulama Süreci. Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Baykal, N. (2001). Bilgisayar Ağlarına Giriş, Bölüm 12. Bilgisayar Agları.1.Baskı.SAS Bilişim, Ankara. **499.**

Çakar, H. (2005). Bilgisayar ağ güvenliği ve güvenlik duvarları. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elâzığ.

Çiçek, İ. (2016). İnternet Omurgasının Altyapısı NETWORK TCP/IP UNIX. İstanbul.

Dennis, M., Keith, R., ve Louis, D. (2007). Security and interconnection of medical USA: Department of Veterans Affairs, Veterans Health Administration.

Dertler, F. (2000). Network Sistemleri. Sistem Yayıncılık, İstanbul.

Hoşgör, E. (2014). Bilgisayar Ağı ve Çeşitleri Nedir? İstanbul

Ido, D. (2007). How to Cheat at Securing Your Network. Topologies and IDS,**281-315.**

Karanfil, M. (2009) Bilgisayar ve Ağ Güvenliği Yöneticiliği. İstanbul

Karatabak, G. (2006). Açık Sistemdeki Güvenlik Duvarı Kullanarak Ağdaki Paketlerin Kontrolü. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elâzığ.

Kınay, M. (2005) Kablosuz Ağlar (Wıreless Networks) Ve Kablosuz Ağlarda Güvenlik, Yüksek Lisans Tezi Yüzüncü Yıl Üniversitesi, Fen Bilimleri Enstitüsü.

Lehr, W. Chapin, J. (2010). “On The Convergence of Wired and Wireless Access Network Architectures”, Information Economics and Policy, 22(1), **33-41**. (Lehr, Chapin).

Mahler, K. (1999). Cisco Certified Network Associate. Cisco Press, **507**.

Öner, D. (2010). Bilgisayar Ağları. Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Özdemir, M. (2011). Nitel veri analizi: sosyal bilimlerde yöntembilim sorunsalı üzerinde bir çalışma. Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi, 1(1), **325-336**.

Vural, Y. (2007). Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri, Gazi Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans, **297** Ankara.

Yıldırım, A., ve Şimşek, H. (2008). Sosyal bilimlerde nitel araştırma yöntemleri (6. Baskı). Ankara: Seçkin Yayıncılık.

İNTERNET KAYNAKLARI

1. http://www.banadersanlat.com/guevenli-ag-mimarisi-tasar-m-1
Erişim Tarihi: 11.12.2017

2. http://www.turkcenet.org/temel-aclgileri-mainmenu-5/temel-bilgiler-mainmenu-9/8
Erişim Tarihi: 13.12.2017

3. https://b120606056.wordpress.com/konu-anlatimi
Erişim Tarihi: 15.12.2017

4. http://gulferdi.blogspot.com.tr/2014/04/network-topolojisi.html
Erişim Tarihi: 28.12.2017

5. https://www.kunfeyekun.org/kf/osi-katmanli-yapisi-ve-isleyisi.36566/
Erişim Tarihi: 05.01.2018

6. https://sudo.ubuntu-tr.net/ag-protokolleri
Erişim Tarihi: 08.01.2018

7. http://www.tech-worm.com/microsoftun-tarihcesi-ve-gelisimi/
Erişim Tarihi: 22.01.2018

8. http://www.alosgk.com/2017/08/butce-ve-issizlik-verilerine-pareto.html
Erişim Tarihi: 24.01.2018

9. http://diyot.net/hexadecimal-sayi-sistemi/
Erişim Tarihi: 02.02.2018

10. https://www.muhendisbeyinler.net/ethernet-nedir-ne-ise-yarar/
Erişim Tarihi: 04.02.2018

11. http://www.azurinfo.fr/reseau/
Erişim Tarihi: 08.03.2018

12. https://www.emaze.com
Erişim Tarihi: 11.03.2018

13.http://ciscoswitchrouters.blogspot.com.tr/2014/03/uso-del-comando-hostname.html
Erişim Tarihi: 01.04.2018

14.http://www.techniquenet.co.uk/technique-network-services/fibre-optic-network
Erişim Tarihi: 10.04.2018

15. http://help.incredimail.com/incredimail/help_center/
Erişim Tarihi: 15.04.2018
16. https://www.fortinet.com/products/next-generation-firewall.html
Erişim Tarihi: 18.03.2018
17. https://rizasahan.wordpress.com/
Erişim Tarihi: 22.032018
18. http://www.neutr10.com/cgn-ip-nedir/
Erişim Tarihi: 23.03.2018
19. http://agciyiz.net/kablolu-baglantilar-icin-802-1x-dogrulama-1/
Erişim Tarihi: 15.01.2018
20. http://web.firat.edu.tr/mbaykara/agguvenligi.pdf
Erişim Tarihi: 02.04.2018
21. http://www.furkanozbay.com/2014/08/wireshark-ile-ag-dinleme.html
Erişim Tarihi: 05.04.2018
22. http://www.btmakaleleri.info/2016/04/sik-kullanilan-bilgisayar-ag-portlari.html
Erişim Tarihi: 12.04.2018

ÖZGEÇMİŞ

Adı Soyadı	: Akıb ÇETİN
Doğum Yeri ve Tarihi	: Kırıkkale – 1981
Yabancı Dili	: İngilizce
İletişim	: akibcetin@kku.edu.tr

Eğitim Durumu(Kurum ve Yıl):

Lise	: Kırıkkale Kurtuluş Lisesi
Lisans	: Anadolu Üniversitesi

Çalıştığı Kurum/Kurumlar ve Yıl:

TÜİK Kocaeli Bölge Müdürlüğü	: 2006-2007
Amasya Milli Eğitim Müdürlüğü	: 2007-2012
Afyon Kocatepe Üniversitesi	: 2012-2017
Kırıkkale Üniversitesi	: 2017 -