AĞDAKİ AKTİF CİHAZ SAVUNMASIZLIKLARI İÇİN GÜVENLİK POLİTİKASI GELİŞTİRME SİSTEMİ

Özgür TONKAL

YÜKSEK LİSANS TEZİ
BİLGİSAYAR BİLİMLERİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Haziran 2013
ANKARA

Özgür TONKAL tarafından hazırlanan AĞDAKİ AKTİF CİHAZ SAVUNMASIZLIKLARI İÇİN GÜVENLİK POLİTİKASI GELİŞTİRME SİSTEMİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Prof. Dr. O. Ayhan ERDEM
Tez Yöneticisi

Bu çalışmada, jürimiz tarafından oy birliği ile Bilgisayar Bilimleri Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Başkan : Prof. Dr. M. Ali AKCAYOL

Üye : Prof. Dr. O. Ayhan ERDEM

Üye : Yrd. Doç. Dr. Hüseyin POLAT

Üye :

Üye :

Tarih : 12/06/2013

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Özgür TONKAL

AĞDAKİ AKTİF CİHAZ SAVUNMASIZLIKLARI İÇİN GÜVENLİK POLİTİKASI GELİŞTİRME SİSTEMİ

(Yüksek Lisans Tezi)

Özgür TONKAL

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2013

ÖZET

Bu tezde, kurumsal ağlarda kullanılan anahtarlar üzerindeki güvenlik konfigürasyonu eksikliklerinden dolayı oluşacak güvenlik açıklıklarını gidermeyi sağlayan bir yazılım geliştirilmiştir. Kurumsal ağlarda en çok rastlanan saldırı türleri belirlenmiştir. Bu saldırılar için yapılandırılması gereken konfigürasyonlar geliştirilen yazılım ile çok daha kolay ve kısa sürede yapılabilmektedir. Geliştirilen yazılım web tabanlı olarak çalışmaktadır. Sunulan web arayüz ile yönetim kolaylaştırılmıştır. Sunulan yazılım linux tabanlıdır. Herhangi bir linux bilgisayar üzerine bağdaştırılılarak merkezi olarak onlarca kurumun anahtarları uzaktan kontrol edilebilmektedir ve konfigürasyon yapılabilmektedir. SSL VPN teknolojisini kullanarak uzak bağlantı güvenli şekilde sağlanmaktadır. Geliştirilen yazılım ile Procurve marka tüm anahtarlar üzerinde başarılı sonuçlar elde edilmiştir.

Bilim Kodu : **702.01.014**
Anahtar Kelimeler : **Ağ güvenliği, SSL VPN, yerel ağ saldırıları, anahtar güvenliği**
Sayfa Adeti : **70**
Tez Yöneticisi : **Prof. Dr. O. Ayhan ERDEM**

SECURITY POLICY DEVELOPMENT SYSTEM FOR ACTIVE DEVICE VULNERABILITIES ON NETWORK

(M.Sc. Thesis)

Özgür TONKAL

GAZİ UNIVERSITY

INFORMATION INSTITUTE

June 2013

ABSTRACT

In this thesis, software has been developed to correct security weaknesses due to the lack of security configuration on the switches used with institutional networks. The most common types of attacks on institutional networks have been determined. The configurations needed to be configurated for these attacks can be performed much more easier and in a short time through the developed software. The developed software works as web based. The management has been facilitated with the presented web interface. The presented software is linux based. Associated on any computer with a Linux operating system, the switches of many institutions can be controlled and configured centrally and remotely. The remote connection is provided safely with the use of SSL VPN technology. By the help of the developed software, successful results have been obtained on all the switches marked as Procurye.

Science code : **702.01.014**
Key Words : **Network security, SSL VPN, LAN attack, switch security**
Page Number : **70**
Adviser : **Prof. Dr. O. Ayhan ERDEM**

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren Danışman Hocam Sayın Prof. Dr. O. Ayhan ERDEM'e, çalışmam sırasında desteklerini esirgemeyen arkadaşım Ramazan KOCAOĞLU'na, ayrıca maddi ve manevi her türlü destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli aileme teşekkür ederim.

İÇİNDEKİLER Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
BPDU	Bridge Protocol Data Unit (Köprü Protokolü Veri Birimi)
C.E.R.T	Computer Emergency Response Team (Bilgisayar Acil Durum Ekibi)
CDP	Cisco Discovery Protocol (Cisco Keşif Protokolü)
DHCP	Dynamic Host Configuration Protocol (Dinamik Host Yapılandırma Protokolü)
FTP	File Transfer Protocol (Dosya Aktarım Protokolü)
HTTP	Hypertext Transfer Protocol (Hiper Metin Transferi Protokolü)
LAN	Local Area Network (Yerel Alan Ağı)
MAC	Media Access Control (Ortam Erisim Denetimi)
NAT	Network Address Translation (Ağ Adres Çevirimi)

Kısaltmalar	Açıklama
OSI	Open Systems Interconnection (Açık sistem bağlantı modeli)
PHP	Hypertext Preprocessor (Hipermetin Ön İşlemci Betik Dili)
SMTP	Simple Mail Transfer Protocol (Basit Posta Gönderme Protokolü)
SSL	Secure Socket Layer (Güvenli Soket Katmanı)
STS	Saldırı Tespit Sistemleri
TCP	Transmission Control Protocol (İletim Kontrol Protokolü)
UDP	User Datagram Protocol (Kullanıcı Veri Birimi Protokolü)
VLAN	Virtual Local Area Network (Sanal Yerel Alan Ağı)
VPN	Virtual Private Network (Sanal Özel Ağ)

1. GİRİŞ

İnsanlığın gelişim süreçlerinde en önemli yeri alan "bilgi", tarih boyunca insanoğlunun düşüncesini, yaşayışını, davranışını belirleyen faktörlerin basında gelen büyük bir güç olarak yerini korumuştur. Bilgiye mekândan bağımsız olarak erişme isteğinin sonucu olarak bilişim teknolojilerinde baş döndürücü gelişmeler meydana gelmiştir. Yaşamın her alanında kullanılma başlanan bilişim teknolojileri ile birlikte paylaşılan bilgilerin güvenliğinin sağlanması sorunu ortaya çıkmıştır. En gereksiz görünen bilginin bile bir başkası için çok büyük öneme sahip olabileceği gerçeği bilgi sistemlerini saldırganların hedefi haline getirmiştir. Bu yüzden bilginin gizliği ve bütünlüğünün sağlanması, yararlı bilgilerin başkalarının veya saldırganların ellerine geçmemesi için bilgi sistemlerine gelecek olası saldırılar hakkında bilgi sahibi olmak ve gerekli önlemleri almak oldukça önemlidir.

Bilgi sistemlerine yapılan saldırıları organize ve organize olmayan saldırılar ile dışardan yapılan ve içerden yapılan saldırılar olmak üzere dört gruba ayrılabilir [1].

İçerden saldırı yapan kişiler, çalışmakta olan veya daha önce çalışmış işçiler, müteahhitler, iş ortakları olabilir. Bunların yerel ağ kaynaklarına hâlihazırda veya geçmişte ulaşma hakkı olmuş olabilir. Bu kişilerin şirket içi politikalar, süreçler ve uygulamalar hakkında bilgisi vardır ve bu bilgilerini, bazen de şirket dışındaki kötü niyetli kişilerle ortaklık yaparak saldırılar düzenlemek için kullanırlar [2].

Günümüzde yaygın şekilde kullanılan bilgi güvenliği sistemleri; kriptolama, ateş duvarları, sızma tespit ve önleme sistemleri aslında bir yerel alan ağını dışardan gelen saldırıları karşı önemli oranda korumaktadır. Bunun farkında olan saldırganlar saldırıyı içeriye sızarak içerden gerçekleştirmektedirler veya daha önce belirttiğimiz yerel alan ağı üzerindeki kaynaklara erişim hakkı olanlar saldırıyı gerçekleştirmektedir. 1997'de ABD Savunma Bakanlığı'na yapılan saldırıların %87'si içerden yapılan saldırılardır. 2004 yılından 2006 yılına kadar yapılan çalışmalarda içerden yapılan saldırıların %31'den %27'ye düşmüş olduğu görülse de parasal açıdan daha büyük zarar vermişlerdir [3].

Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü CERT (Computer Emergency Responce Team) programı, CSO (chief security officer) dergisi, ABD Gizli Servisi ve Deloitte firması işbilirliği ile 2011 yılında yapılan siber güvenlik araştırma sonuçlarına göre katılımcıların; %58'i bilgi sistemlerine yapılan saldırıların dışarıdan (ağ sistemleri ve veri erişim yetkisi olmayanlar tarafından) yapıldığını , %21'i saldırıların içeriden (yetkili erişeme sahip çalışanlar tarafından) yapıldığını , %21'i saldırıların kaynağının belli olmadığı belirtmişlerdir. 607 katılımcının %46'sına göre içeriden gerçekleştirilen saldırıların verdiği zarar, dışarıdan gerçekleştirilen zarardan daha fazla olmuştur [4].

Bilgi güvenliğini sağlamadaki kişi ve kurumların bilgi ve tecrübe eksikliklerinin yanında saldırganların saldırı yapabilmeleri için ihtiyaç duydukları yazılımlara internet üzerinden kolaylıkla erişebilmeleri, fazla bilgi birikimine ihtiyaç duyulmaması ve en önemlisi ise kişisel ve kurumsal bilgi varlıklarına yapılan saldırılardaki artışlar, gerek kişisel gerekse kurumsal bilgi güvenliğine daha fazla önem verilmesine yeni yaklaşımların ve standartların kurumlar bünyesinde uygulanması zorunluluğunu ortaya çıkarmıştır.

Kurumsal ağlar oluşturulurken ağdaki aktif cihazların(switch-router-firewall-access point vb) güvenlikle ilgili olan konfigürasyonları ikinci plana atılır ve genelde bu ayarlar ağ cihazlarında varsayılan konfigürasyonlarda bırakılır. Bu varsayılan güvenlik konfigürasyonlarından dolayı ağda kritik güvenlik açıkları oluşmaktadır. Bu açıkların neler olduğunu bilen saldırgan ağı kullanılamaz hale getirebilir ya da fark edilmeden ağı dinleyebilir. Etkin ve genel kullanılan saldırı türlerine örnek olarak, parola saldırıları, MAC adresi kandırmaca, ARP zehirlenmesi, IP adresi kandırmaca, sahte trafik oluşturma, DNS kandırmaca, HTTP trafiğinde araya girme ve DoS saldırıları sıralanabilir [5].

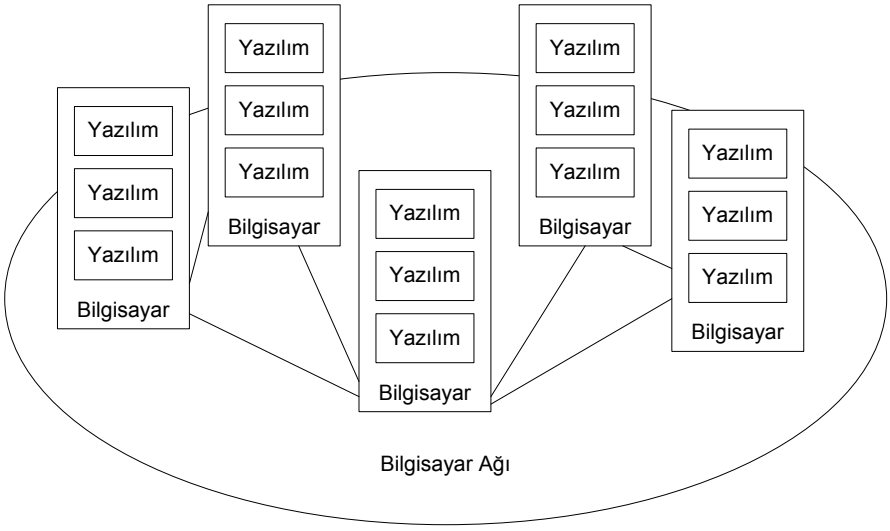
Son yıllarda en temel ağ bileşenlerine ve standartlarına yapılan başarılı saldırılar bu nedenden dolayı ağ güvenliği konusunda teknik analizlerin ve detaylı akademik çalışmaların gerekliliğini ortaya koymaktadır.

Bu nedenle bu çalışma içerisinde, aktif cihaz konfigürasyon eksiklerinden kaynaklanan ağ savunmasızlıklarını ortaya koyacak bir ağ topolojisi tasarlanmıştır. Geliştirilen uygulama ile merkezi olarak aktif cihaz konfigürasyonu test edilmiş ve ağ savunmasızlıkları giderilmiştir. Bu çalışma esnasında tamamen açık kaynak kod yazılımlar tercih edilmiş ve kullanılmıştır. İlgili topolojinin oluşturulmasında, işletim sistemleri üzerinde geliştirilen uygulamalarda, uygulamanın geliştirilme süreci içerisinde açık kaynak kod yazılımlar tercih edilmiştir. Özellikle açık kaynak kod yazılımların ücretsiz olarak temin edilebilmesi ve uygulama kodlarının incelenebilmesi tercihin birincil sebepleri olmuşlardır.

Tez, Giriş bölümü birinci bölüm olmak üzere beş bölümden oluşmaktadır. İkinci bölümde ağ ve bilgi güvenliği kavramları ile birlikte ağ ve bilgi güvenliğini sağlamak için kullanılan teknolojilerden, üçüncü bölümde ağ güvenliğini tehdit eden saldırı türlerinden ve yerel ağ saldırılarına karşı alınacak tedbirlerden, dördüncü bölümde yazılım geliştirme ve sunum ortamıyla ilgi bilgiler verilmiştir. Yine bu bölümde tez uygulaması çalıştırılarak, uygulamaya ait detaylardan bahsedilmiştir. Tezin son bölümü olan beşinci bölümünde ise yapılan çalışmaya ait sonuçlar ve öneriler bulunmaktadır.

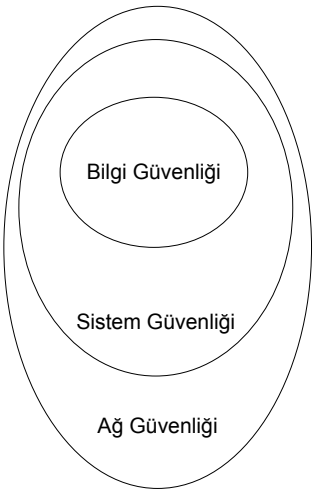
2. AĞ VE BİLGİ GÜVENLİĞİ

Ağ (network), paylaşım amacıyla iki ya da daha fazla bilgisayarın belirli bir ortam (media) aracılığıyla (bakır, fiber, vb.) haberleşme, bilgiye erişim, kaynak paylaşımı (veri, yazıcı, uygulamalar ve internet), yedekleme, gibi amaçlar için oluşturduğu yapıdır [6]. Bilgisayar kullanımı geniş kitlelere açılıp, internetin yaygınlaşması ve ticari anlamda önem kazanması ile birlikte bilgisayar ağlarının güvenliğini sağlamak; iletilen ve kullanılan bilginin güvenliğini sağlamak gerektiği için büyük önem kazanmıştır. Bilgi güvenliği bilgiyi ve bilgi istemlerini izinsiz erişim ve kullanımdan, bozulmalardan, değişimden veya tahribattan koruma anlamına gelir. Oluşturulan her bilgisayar ağı içerisinde çeşitli sayılarda bilgisayarlardan ve bu bilgisayarların üzerinde çalışan farklı yazılımlardan meydana gelir. Şekil 2.1' de örnek bir bilgisayar ağının iç yapısı görülmektedir.



Şekil 2.1. Bilgisayar ağ yapısı [7]

Şekil 2.1'de görüldüğü gibi her bilgisayar ağı kendi içerisinde bir sistem barındırır ve bu sistemler aracılığıyla bilgi işlenir, bilgi alışverişi yapılır. Ağ güvenliğinin, sistem güvenliği ve bilgi güvenliği bileşenlerinden oluştuğu Şekil 2.2'de görülmektedir. Dolayısıyla bilgi güvenliğini sağlamak öncelikle sistem güvenliğini ve ağ güvenliğini sağlamak ile mümkün olacaktır.



Şekil 2.2. Ağ güvenlik bileşenleri [7]

Ağ ortamlarının temelinde yatan paylaşım ve uzaktan erişim imkânlarının kullanılması sonucunda yeni güvenlik açıkları meydana gelmiştir. Bu açıklar, kötü niyetli veya meraklı kişiler tarafından kullanıldığında; bilgilere yetkisiz erişim, sistemler ve servislerin kullanılamaz olması, bilgilerin değiştirilmesi veya ifşa edilmesi vb. güvenlik ihlâlleri oluşmaktadır. Bilgisayar ağlarının yaygınlaşmasıyla güvenlik ihlâlleri artmış, bilgi güvenliği için alınması gereken önlemler fazlalaşmıştır.

Güvenli Bilgisayar Sistemi Değerlendirme Kriterleri (TCSEC-DoD Trusted Computer System Evaluation Criteria) ağ sistemlerinin güvenliği için geliştirilmediğinden 1987 yılında TCSEC'in güvenilir ağ yorumlaması (Trusted Network Interpretation) adını verdiği Kırmızı Kitap (Red Book) yayımlanmıştır [8]. Kırmızı Kitap, Turuncu Kitaba ek olarak bilgisayar ağları ve bileşenlerinin güvenliğiyle ilgili konuları da içermektedir. Ancak işlevsellik açısından pek kullanışlı olmadığından çok fazla kullanım alanı olmamıştır.

Bir yerel alan ağını oluşturan sunucu ve istemciler kablolu ya da kablosuz olarak birbirleriyle iletişim kurabilirler. Bir ağ ortamında kullanılan sistemlerin ve bu sistemler üzerinde saklanan her türlü verinin korunması ancak etkin bir ağ güvenliği denetimi ile yapılabilir. Bu kapsamda öncelikle bir ağın güvenilirliği ile ilgili olarak

"Güvenilir Sistem" teriminin açıklanması gerekebilir. Güvenilir Sistem, hem ağ içi haberleşmede hem de ağın dış dünya ile haberleşmesinde ağ trafik yoğunluğunun artması, içerden/dışarıdan yetkisiz erişim veya önemli bir verinin saklanması gibi durumlarda hiç bir zafiyet oluşturmadan ağ güvenliğini sağlayabilen güçlü sistemdir. Bu sistem hem kullanılan ağ cihazlarının ve hem de bu cihazlar üzerinde çalışan uygulama programlarının iyi bir konfigürasyonla seçilmesi ve çalışmasının devamı ile mümkündür.

Çizelge 2.1. Ağda alınabilecek önlemler [9]

AĞDA ALINABİLECEK ÖNLEMLER	Birinci Katman	Ikinci Katman	Üçüncü Katman
	Bulaşmasını Engelleme	*Bulaşmış Sistemi Saptama*	*Kurtarma ve Etkileri Azaltma*
4.1. L2 Cihazlar ile Alınabilecek Önlemler			
4.1.1. MAC Adresi Bazında Güvenlik		X	X
4.1.2. 802.1x Tabanlı Kimlik Tanımlama	X	X	
4.1.3. Broadcast/Multicast Sınırlandırması		X	X
4.2. L3 Cihazlar ile Alınabilecek Önlemler			
4.2.1. VLAN Bazlı Güvenlik Çözümleri	X		X
4.2.2. Erisim Listeleri Alınabilecek Çözümler	X	X	X
4.2.3. QoS ile Bandgenişliği Sınırlaması			X
4.2.4. Yeni Nesil Güvenlik Çözümleri		X	X
4.3. Güvenlik Cihazları ile Alınabilecek Önlemler			
4.3.1. Firewall (Güvenlik Duvarları)	X	X	X
4.3.2. Antivirüs Geçitleri	X	X	X
4.3.3. IDS/IPS Sistemleri	X	X	X
4.4. Diğer Sistemler ile Alınabilecek Önlemler			
4.4.1. Saldırgan Tuzağı Ağları (Honeynet)		X	
4.4.2. Merkezi Log Kontrolü		X	
4.4.3. Trafik Analizi		X	
4.4.4. DNS Sunucu			X
4.4.5. Arp Saldırılarını Tespit Edebilen Uygulamalar		X	

Ağ ortamında sahip olunan verilerin güvenliğinin sağlanmasında Çizelge 2.1'de gösterildiği gibi farklı kademelerde güvenlik seviyeleri uygulanır bu kademeler;

- Ağa erişimi sorgulama/koruma
- Ağ kaynaklarını hizmet türleri açısından koruma
- Bilgisayarlara bağlantıyı sorgulama
- Uygulama programları seviyesinde sorgulama/koruma
- Veri kaydı düzeyinde koruma
- Kayıt alanı düzeyinde koruma

Bu seviyeler sırasıyla, ağa erişimi veya ağ üzerinde ki hizmetlere erişimi denetleyen Güvenlik Duvarları (Firewall) seviyelerinden bilgisayar veya uygulama programının içine girmeyi ve en son seviyelerde de iyi bir şifreleme ve anahtarlama algoritmasının çalışmasını içeren sistemlere adım adım yaklaşmayı açıklar.

Ağ güvenliğini sağlayabilmek için Güvenlik Duvarları (Firewall), Saldırı Tespit Sistemleri (IDS) ve Rol Tabanlı Erişim Kontrolleri (RBAC) kullanılabilir. Bu kapsamda ağ güvenliğini sağlamaya yönelik çözümler aşağıdaki gibi özetlenebilir.

2.1. VPN (Virtual Private Network - Sanal Özel Ağ)

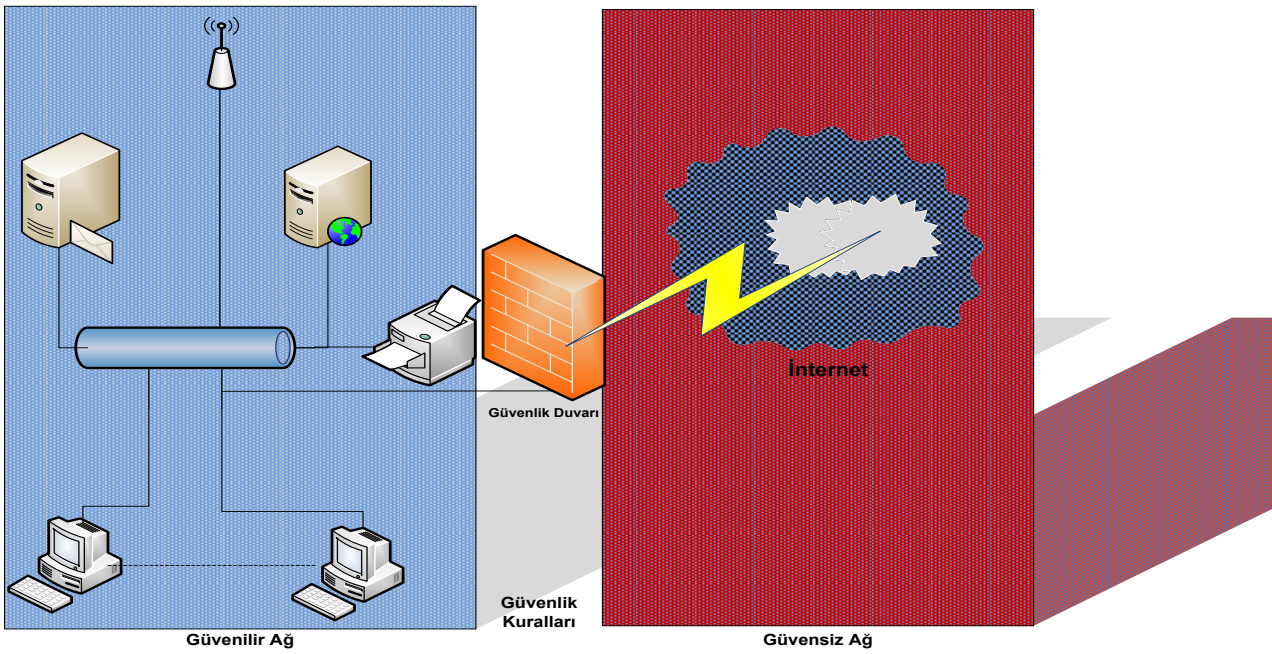
Daha çok kişi veya kurumların bilgiye ulaşmak veya bilgilerini paylaşmak için belirlenmiş bir adrese internet ortamından erişimlerini sağlayan özel bir yoldur. Ve bu yol kullanılacak bir Firewall ile iki uç arasında bir kanal oluşturmak ve bu kanala girecek verilerin şifrelenmiş paketler halinde seyahatini sağlayarak yetkisiz kişilerin kullanımına engel olma mantığı üzerine bina edilmiştir.

2.2. Güvenlik Duvarları (Firewall)

Güvenilir ağların (kurumsal ağlar) sınır kısmında denetleme noktaları oluşturarak, bu denetleme noktalarından güvensiz ağlara (internet) doğru giden veya güvensiz ağlardan gelen ağ trafiğini, kurumsal güvenlik politikalarında belirlenen kurallar veya filtrelere göre denetleyerek hangi isteklerin kabul veya red edileceğine karar veren yazılım veya donanım çözümleridir [10].

Güvenlik duvarları, tek noktadan erişim denetimi ile ağ üzerindeki bilgisayarlara dış dünyadan erisen kullanıcıların kullanımına kurallar koyarak olası saldırıların en aza indirilmesinde kullanılmaktadır. Bilgisayar güvenliğinin sağlanmasında gizlilik, erişilebilirlik, bütünlük ve kimlik denetimi gibi temel bilgi güvenliği unsurlarını tehdit eden saldırılara karsı bazı önlemler güvenlik duvarları tarafından alınmakta ancak bu önlemler bilgisayar güvenliğinin sağlanmasında tek basına yeterli değildir.

Kurumsal bilgisayar ağlarında ağ güvenliğinin sağlanmasında kullanılan güvenlik duvarına bir örnek, Şekil 2.3'te verilmiştir.



Şekil 2.3. Güvenlik duvarı yapılandırmasına bir örnek [14]

Güvenlik duvarları, dış ağlardan (güvensiz ağ) gelecek tehditlere karsı kendi üzerinden geçen ağ trafiğini koruma altına alırken ağ içerisinden gelecek tehditlere, izin verilen servislerden gelen saldırılara, arka kapılara ve virüslere, sazan avlamalara ve casus yazılımlara karsı koruma sağlayamazlar. Farklı yapılandırma şekilleri olsa da güvenlik duvarları saldırıları engellemede ve güvenliği sağlamada daha önceki paragrafta vurgulandığı gibi tek basına yeterli değildir ancak ağ güvenliğinin sağlanmasında önemli bileşenlerden birisidir.

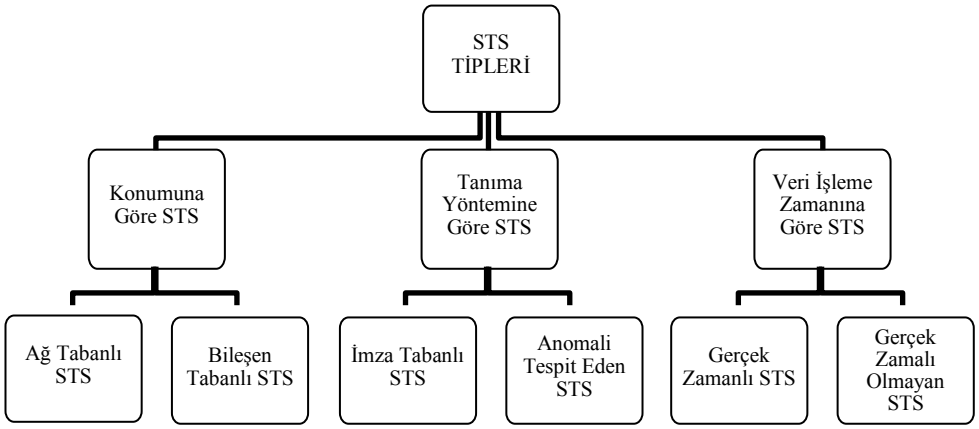
2.3. Saldırı Tespit Sistemi (Intrusion Detection system-IDS)

"Saldırı tespiti, bir sisteme yapılan izinsiz müdahalelerin mümkünse önceden, olay anında veya daha sonra; sistem günlüklerinden veya bilgisayar ağı trafiğinden alınan verilerden yola çıkılarak çeşitli metotların yardımı ile analizidir" [11].

Saldırı tespitinin amacı; bu müdahaleleri mümkünse önlemek ve saldırıları kayıt altına alarak e-posta, kısa mesaj, konsol uyarı mesajı vb. gibi yollardan yetkili kişileri bilgilendirmektir [11].

Saldırı tespit sistemleri bilgilerin; gizlilik, bütünlük ve erişilebilirliğini tehdit eden, yetkisiz olarak bilgiye erişebilmek için bilgisayar ağlarına veya bilgisayarlara karsı yapılan saldırıların tespit edilmesinde kullanılan uyarı veya alarm sistemleri olup güvenlik duvarının yetersiz kaldığı durumlarda ek koruma sağlamaktadır [12]. Saldırıyı önceden tespit ederek engellemek, saldırı sonucu çalışmayan bir sistemi yeniden çalışır hale getirmekten daha ekonomik bir çözümdür.

Saldırı tespit sistemleri; Şekil 2.4'de görüldüğü gibi konumuna göre, saldırıyı tanıma yöntemlerine göre ve veri işleme zamanına göre sınıflandırılır [13].



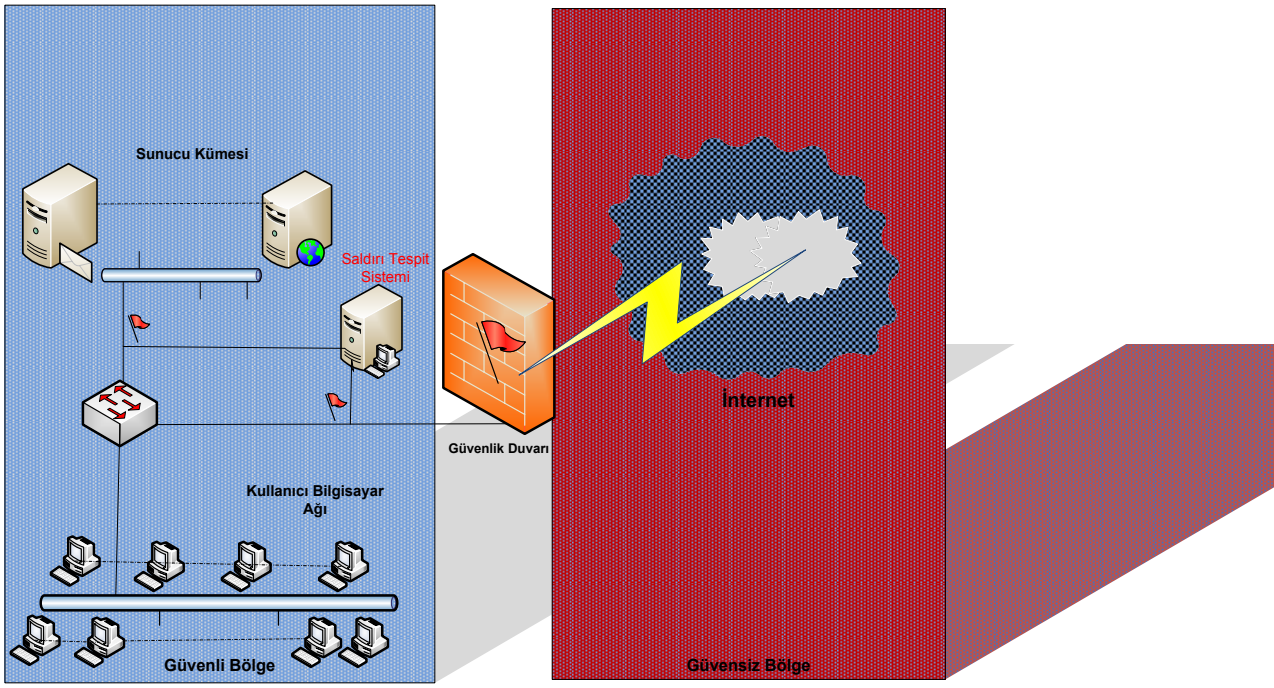
Şekil 2.4. Saldırı tespit sistemleri tipleri

Saldırı tespit sistemleri, içerik olarak iki farklı mimaride çalışmaktadırlar [14]. İlk yapıda çeşitli imzalar (veri tabanına kayıtlı saldırılar) ile paketleri incelemek ve saldırıları tespit etmek amaçlanmaktadır. İkinci yapıda ise bilgisayarların ve ağın normal isleyişi belirlenerek, olabilecek herhangi bir normal dışı hareketin saldırı olarak algılanması sağlanmaktadır. İmza tabanlı saldırı tespit sistemleri günümüzde yaygın olarak kullanılmaktadır. Antivirüs sistemleri gibi ağ üzerinde yakalanan paketleri inceleme seklinde çalıştıkları için saldırının imza tanımının önceden

tanımlanmış olması gereklidir. Bu yöntemin can alıcı noktası, saldırı imza listelerinin güncellenmesinin sağlanmasıdır aksi takdirde güncel saldırılara karsı koruma sağlanamayacaktır.

İkinci yapıdaki saldırı tespit sistemlerinde ise, ağda veya çeşitli sunucularda düzenli olarak yapılmakta olan işlemler takip edilerek sistemin normal isleyişinin zeki yaklaşımlarla (yapay sinir ağları, bulanık mantık, uzman sistemler, vb.) öğrenilmesi esasına dayanır. Bu yapıda çalışan saldırı tespit sistemleri, anormal hareketler gördüklerinde bu hareketleri saldırı olarak rapor ederler. Örnek vermek gerekirse, isim çözme sunucusuna (DNS) normal isleyişinde TCP/UDP 53 nolu porttan istek gelmesi gerekirken, TCP/23 (telnet) portundan istek gelmesi saldırı olarak algılanabilir. Öğrenme temelli saldırı tespit sistemlerinin gerçek hayattaki çalışması örnekte anlatıldığı kadar da başarılı değildir. Çünkü bu tür sistemlerin normal olarak nitelendirilebilecek davranışları öğrenmeleri oldukça fazla zaman almaktadır. Ayrıca bu davranışların zaman içerisinde değerbilirliği, kurulduğu sistemlerin yeniden yapılandırılması veya yeni sistemlerle birlikte yeni davranışların eklenmesi öğrenme isini zorlaştırmaktadır.

Kurumsal bilgisayar ağlarında yer alan saldırı tespit sistemine bir örnek Şekil 2.5’de verilmiştir.



Şekil 2.5. Saldırı tespit sistemine bir örnek [14]

Saldırı tespit sistemlerinin kullanımında en fazla karşılaşılan problemlerden birisi saldırı tespit sistemlerinin sistemdeki normal bir davranışı saldırı olarak tespit etmesidir (False Positive). Bu hatadan dolayı saldırı tespit sistemlerinden beklenen başarı elde edilememiştir [14].

2.4. Rol Tabanlı Erişim Sistemi (RBAC)

RBAC (Role-based access control), bilgi ve iletişim sistemlerine erişim haklarının yönetilmesi için 1980'lerin sonlarına doğru geliştirilen bir güvenlik sistemidir. Bu güvenlik sistemi, çok büyük ağ uygulamaları için daha düşük maliyette ve daha az karmaşık güvenlik yönetimi oluşturur. RBAC, kullanıcıların rollerini ve yetkilerini tanımlayarak güvenlik yönetimini kolaylaştırır. Rol, kullanıcıların gruplanması anlamında kullanılmaktadır.
RBAC'ın yararları aşağıdaki gibi sıralanabilir:

- Ayrı ayrı kişiler değil, roller kontrol altına alınır.

- Yönetim tek bir noktadandır.

- Rol tanımları kurumun iş tanımlarına uygun olacak şekilde esnekleştirilebilir.

- Rollerin erişim hakları çok kısa süreler içinde kolaylıkla kapatılabilir veya kaldırılabilir.

2.5. Kablosuz Ağ Güvenliği

Kablosuz ağlar, son zamanlarda oldukça ilgi gören ve kullanımı gittikçe yaygınlaşan bir ağ türüdür. Kullanıcılara sunduğu hareketlilik (mobility) imkânı, kablolama maliyetinin olmayışı, kullanım kolaylığı ve buna benzer üstünlüklerinden dolayı günümüzde giderek daha fazla tercih edilmeye başlanmıştır. Kablosuz ağların, iletim ortamı olarak havayı kullanmasından kaynaklanan güvenlik problemlerinden dolayı, kablolu ortamlara göre güvenliğinin sağlanması daha zordur.

WEP (Wired Equivalent Privacy - Kabloya Eşdeğer Mahremiyet (KEM)), WPA (Wi-Fi Protected Access - Wi-Fi korumalı Erişim) ve EAP (Extensible Authentication Protocol - Genişletilebilir Kimlik Doğrulama Protokolü) kablosuz ağlar için geliştirilen güvenlik protokolleridir [15]. Kimlik doğrulama mekanizması olmayan WEP algoritması, kablosuz ağ güvenliğini sağlamada (bütünlük, gizlilik) sonradan yapılan iyileştirmelere rağmen başarısız olmuştur. WPA, WEP protokolünün eksikliklerini gidermesi için Wi-Fi Alliance ve IEEE tarafından geçici olarak oluşturulmuş bir protokoldür. WPA, WEP'e göre daha güçlü bir şifreleme yöntemi olan TKIP (Temporal Key Integrity Protocol)'i desteklemektedir. EAP protokolü ise uçtan uca iletişim için kimlik doğrulaması sağlar [16]. Kablosuz ağların güvenliğinin sağlanması için IEEE tarafından kablosuz ağlardaki güvenlik problemlerine detaylı çözümler üretmesi amacı ile 802.11x standardı geliştirilmiştir. Bu standartla güvenilir bir şifreleme, kimlik doğrulama ve veri bütünlüğünün sağlanması amaçlanmaktadır [17].

2.6. Sunucu Güvenliği

Sunucular bir bilgi işlem merkezini oluşturan en önemli parçalardandır. Her bilgi işlem merkezinde çok çeşitli sunucular vasıtasıyla İnternet erişim hizmeti, e-posta hizmeti gibi hizmetler verilir. Aynı zamanda verilerin önemli bir bölümü merkezi olarak sunucularda tutulur. Bu nedenle sunucu güvenliği en önemli hususlardan birisi, hatta önde gelenidir. Kurum ağını dışarıdan gelen saldırılara karşı güvenli hale getirmek için iyi tasarlanmış bir çevre ağının varlığı önemli bir etmendir. Böyle bir ağ aynı zamanda iç ağın diğer ağlara karşı saldırılarda kullanılmasını önlemeye de yarar. En yaygın kullanılan çevre ağ öğesi güvenlik duvarıdır.

Çevre ağda DMZ (demilitarized zone) yapısı kullanılarak iç ağ ve internet arasında korumalı bir dolaylı erişim mimarisi kullanılabilir. Bu yapıda ilk önemli karar DMZ içine hangi sunucuların konacağıdır. Genel bir yaklaşım, kurum dışından erişilebilen tüm hizmetleri DMZ içine koymaktır. DMZ erişimi de bir veya daha fazla firewall kullanarak güvenli hale getirilmelidir. Yüksek güvenlik gerektiren kurum yapılarında DMZ içindeki her host kendine ait bir firewall ile trafik kontrolü yapabilir. Birden fazla firewall kullanılması, saldırıya yenik düşmüş bir atağın kurumun diğer yapılara vereceği zararı önlemek için tercih edilmesi gereken bir yapıdır. Ticari firewall uygulamaları geniş bir fiyat-özellik yelpazesi oluştururlar. Bunun yanında yaygın bir açık kaynak firewall seçeneği iptables uygulamasıdır.

Kurum ağının sunucuları çoğu zaman fiziksel olarak farklı yerlerde bulunduğundan sistem yöneticisi tarafından uzaktan erişimle konfigüre edilirler. Uzaktan erişim işlemi de güvenlik açısından zayıf bir noktadır ve güçlendirilmelidir. Bunun için, telnet, rlogin, rsh uygulamalı yerine, açık anahtar yapısı ile yüksek güvenlik sağlayan Secure Shell (ssh) uygulamaları tercih edilmelidir. En temel ve gerekli internet hizmetlerinden birisi DNS (domain name server)'tir. Aynı zamanda çeşitli analizlerde görülen de DNS'in internetin en başta gelen güvenlik zayıflığı olduğudur. En popüler DNS sunucusu BIND'dir. Kurum ağının DNS saldırılarına karşı korunması için, DNS sunucusu en yeni güvenlik yamaları ile güncellenmeli ve

konfigürasyon parametreleri dış ağa gerekli minimum hizmeti sağlayacak şekilde seçilmelidir.

Kurumdaki kullanıcıların çeşitli hizmetlere erişmek için kullandıkları kimlik ve parola bilgilerini merkezi bir yerde tutmak hep aynı kimlik doğrulama mekanizmasını kullanmak, hem kullanım kolaylığı hem de takip açısından tercih edilmesi gereken bir seçenektir. Diğer yandan, merkezi bir yapı, saldırıları tek bir noktaya odaklayacağından bu sunucunun yüksek güvenlikli olmasını gerektirir. Erişimlerin merkezi kontrolü için tercih edilebilecek bir uygulama LDAP (Lightweight Directory Access Protocol)'dur. Açık kaynak sürümleri de yaygın olarak kullanılan LDAP aynı zamanda kullanıcı bilgilerinin kurum içinde kolayca paylaşımı için de kullanılır.

Veri tabanlarına yönelik tehditler, sunucunun ele geçirilmesi, veri hırsızlığı, verilerin değiştirilmesi ve DoS olarak özetlenebilir. Veri tabanına yönelik saldırılar kurum dışından olabileceği gibi, verilerin bir kısmına erişme hakkı bulunan kurum içi kullanıcıların erişim hakkına sahip olmadıkları veriye ulaşmaları şeklinde de olabilir. Böyle bir yapı veritabanı sunucusunun kullanıcı profillerine ve rollerine göre konfigüre edilmesini gerektirir.

DNS gibi, e-posta kullanımının yaygınlığı da bu hizmete yönelik saldırı ve kötü kullanımların yaygınlığını beraberinde getirir. E-posta hizmetlerine yönelik tehditler arasında e-postanın yolda okunması (eavesdropping), posta kutularının e-posta bombardımanına tutulması, sahte e-postaların oluşturulup gerçek alıcılara gönderilmesi, spam, virüslerin yayılması, e-posta sunucusunun ele geçirilip başka saldırılar için kullanılmasını sayabiliriz. E-postaların sunucular arasında transferi MTA (Mail Transfer Agent) uygulamaları tarafından sağlanır. Yaygın kullanılan bir MTA postfix uygulamasıdır. MTA'lar birbirleri ile SMTP ile iletişim kurup e-postaları transfer ederler. MTA'lar güvenlik gereksinimlerine göre yapılandırılmalıdır. Bunun yanında MTA arkasında virüs ve spam gibi içerik filtrelemesi yapan uygulamalar kullanılmalıdır. Yaygın kullanılan MTA'ların hepsi böyle bir filtreleme desteğine uyumludurlar.

Her ne kadar firewall gibi önlemlerle kurum ağı dışarıya karşı korunsa da, tüm bu duvarlar kurumun web sunucusuna ait trafiğe geçiş vermek zorundadırlar. Çoğu zaman web sunucusu kurumun diğer hizmetlerine entegre olarak çalıştığından, web sunucusunun zayıflığı doğrudan kurum sistem yapısının zayıflığı olarak ortaya çıkar. Web sunucusu saldırıları, sunucuyu çökertmekten, şifrelerin ele geçirilmesine kadar geniş bir alanı kapsar. Güvenli bir web hizmeti için güvenli yazılım esaslarına göre tasarlanmış ve kodlanmış bir web sunucusuna gereksinim vardır. Apache açık kaynak sunucusu en yaygın kullanılan web sunucusudur. Bunun yanında dinamik içerikli web hizmetlerinin kurum içi hizmetlerle birleştirmesi güvenlik gerekleri göz önünde bulundurularak yapılmalı, ancak gerekli minimum hizmet web servisine entegre edilmelidir. Son olarak da sunucunun savunma mekanizmaları otomatik zayıflık test eden uygulamalarla test edilmelidir. Dosya paylaşımı için kullanılan dosya sunucularına erişim de güvenli yollarla yapılmalı, şifrelerin açık gönderildiği FTP gibi protokoller yerine güvenli sftp, scp protokolleri tercih edilmelidir.

2.7. İnternet Güvenliği

Günümüz teknolojisinde kurumlarda verimliliği arttırmak, yeniliklerden haberdar olmak yolunda en önemli unsur elektronik haberleşmeden geçmektedir. Diğer bir değişle İnternet bağlantısı iş ortamında vazgeçilmez bir unsur haline gelmiştir. Kurumlar, çalışanlarına araştırma, kendilerini geliştirme ve yeniliklerden haberdar olma amacıyla İnternet'e çıkma olanağı tanımaktadır. İnternet, bilgiye erişmenin ve araştırma yapmanın en hızlı, en kolay ve en güncel yoludur. Fakat korunmasız bir ağ olduğu için her türlü saldırılara açıktır ve mutlaka güvenliğinin sağlaması gerekmektedir.

Web sitelerinin kullanımının yaygınlaşmasından dolayı bu sitelere yapılan saldırılar en yaygın saldırılardan birisidir. Özellikle Web sitesini kıran saldırganlar bu siteye bağlanan kişileri kolaylıkla kendilerine yönlendirebilir ve kişilerin bilgilerini ele geçirebilirler. Web sitesinin gerçekte bağlanılan Web sitesi olduğundan emin olunması gerekmektedir. Dolayısıyla, Web sitelerinin ve bu sitelere bağlanan

kişilerin kimliklerini ispat edebilmeleri ve güvenli olarak birbirleriyle iletişim kurabilmeleri için elektronik kimlik belgelerine ihtiyaçları vardır. Elektronik kimlik (E-kimlik) belgeleri, kişilerin, kurumların ve Web sunucularının İnternet üzerinde kimliklerini ispatlamak için kullandıkları elektronik dosyalardır. Temeli çift anahtarlı kriptografi teknolojisine dayanan bu belgeler, sahiplerine ait kimlik bilgilerinin yanı sıra sahiplerinin elektronik açık anahtar bilgisini de içermekte ve bu açık anahtar bilgisinin belirtilen kişi, kurum ya da Web sunucusuna ait olduğunu garanti etmektedirler.

E-posta gönderme ve alma işlemi, İnternet üzerinden yapıldığı için birçok güvenlik sorununu da beraberinde getirmektedir. E-postaların başkaları tarafından yakalansa bile anlaşılmaması, gönderen kişinin kimliğinden ve gönderilen mesajın değişmediğinden emin olunması için sayısal şifreleme ve sayısal imza teknolojileri kullanılmaktadır. Kurumsal ortamlarda bilgisayar sisteminin düzgün çalışabilmesi, potansiyel sorunlara karşı korunması, meydana gelebilecek olaylarda en kısa zamanda ve en az kayıpla ayağa kalkılabilmesi için alınması gereken önlemleri, virüslere karşı alınacak önlemler ile birlikte düşünmek gerekmektedir.

Virüslere karşı en genel koruma yöntemi anti-virüs programlarının kullanılmasıdır. Anti-virüsler, virüslere karşı korunmada oldukça etkilidirler ama hiçbir zaman %100 koruma sağlayamazlar. Virüsün özellikleri, anti-virüs programının özellikleri, güncelleme sıklığı, düzenli ve gerektiğinde virüs taramasının yapılması gibi birçok faktör korunmanın etkisini etkiler. Yani, virüslere karşı korunmada hiçbir zaman sadece anti-virüs ile korunma yeterlidir diye düşünülmemelidir. İnternet, kişi ve kurumlara ürettikleri ya da sahip oldukları bilgilerin paylaşımı konusunda altyapı oluşturmakta ve bilgiye daha etkin ve hızlı bir şekilde erişilmesini sağlayacak servisler sunmaktadır. İnternet üzerinden paylaşılmış veri ağlarına erişebilmek, o bölgedeki yerel İnternet Servis Sağlayıcısının aranması söz konusu olduğundan uzak bağlantılarda ödenen ücretler büyük ölçüde düşmektedir. VPN, kullanıcıların pahalı telekom tarifeleri yerine interneti kullanarak güvenli ve şifreli bir şekilde iletişimini sağlayan özel bir sanal ağ alt yapısıdır. Aynı zamanda şifreleme, doğrulama ve yetkilendirme uygulamaları ile güvenliği sağlamak üzere geliştirilmiş bir ağ modeli

olarak ta tanımlanabilir. Dolayısıyla İnternet, uzaktan erişim için klasik bağlantıların yerini almakta ve birçok kurum kendi geniş alan yapısını kurmaktansa bilgi paylaşımı için VPN' i tercih etmektedir.

VPN'de veriyi gönderenin ve alanın onaylanması yani kimlik doğrulama özelliğinden dolayı taraflar birbirlerinin kimliğinden emin olmaktadır. En temel kimlik doğrulama protokolleri Karşılıklı Kimlik Doğrulama Protokolü (CHAP-Challenge Handshake Authentication Protocol) ve Şifre Doğrulama Protokolü (PAP-Password Authentication Protocol)' dür.

Verinin şifreli olarak iletilmesi verinin sadece iki taraf için anlaşılır olması anlamına gelmektedir. İnternet Protokolü Güvenliği (IPSec-Internet Protocol Security) ve Noktadan Noktaya Tünel Protokolü (PPTP-Point to Point Tunneling Protocol) gibi protokoller güvenli bir tünel oluşturarak iletişimin yani trafiğin şifrelenmesini sağlarlar. IPSec, PPTP' den daha güçlü bir şifreleme ve doğrulama sağlar. Daha güvenli bir iletişim için VPN'lerin kendi içindeki güvenlik uygulamalarının dışında AAA sistemleri gibi harici onaylama sistemlerinin de kullanılması önerilmektedir.

Bilgi İşlem Merkezleri için veri ve sistemlerinin güvenliğini sağlamak kadar yedekleme sistemlerini kurmakta çok büyük önem taşımaktadır. Temel olarak bilgi kayıplarının dört ana sebebi vardır. Bunlar donanım arızaları, yazılım hataları, insandan kaynaklanan olaylar (sabotaj, saldırı) ve doğal afetler (deprem, sel)'dir. Bu sebeplerden dolayı oluşabilecek bilgi kayıplarını en alt düzeye indirmenin ve sistemin devamını sağlamanın yolu yedekleme sistemleri kurmaktır. Bilgilerin kopyalarının çeşitli ortamlarda tutulması sistemin ya da herhangi bir kopyanın bozulması durumunda geri dönüş için çok önemlidir. Düzenli olarak yedek almak ve yedeklerin çalıştığından emin olmak iyi bir yedekleme için mutlaka olmak zorundadır. Yedekleme Sistemlerindeki en önemli kararlardan bir tanesi de güvenilir, hızlı, kullanılabilir ve güncel bir sistemin kurulmasıdır. Dolayısıyla yedeklenmiş bir bilgi herhangi bir bozulma olmadan yıllarca saklanabilmelidir. Yapılan işi aksatacak bir olayla her zaman karşılaşılabilir ve her an bir yedeğe ihtiyaç duyulabilir. Bu nedenle karşılaşılabilecek herhangi bir soruna önceden hazırlıklı olmak ve önlemini

almak gerekmektedir. Bunun için İş Devamlılığı Planlaması (BCP-Business Continuity Planning) ve/veya Felaket Kurtarma Planlaması (DRP-Disaster Recovery Planning) yapılabilir.

2.8. Kişisel Bilgisayar (PC) Güvenliği

Bilgisayar güvenliğinin sağlanması için akıllı kart ve akıllı anahtar gibi karmaşık ve pahalı çözümler kullanılabilir. Bu çözümlerin yanı sıra her kullanıcının rahatlıkla uygulayabileceği çözümler de mevcuttur. Örneğin, bilgisayarlara açılış şifresi koymak ve bu şifreyi gerekli durumların dışında başkaları ile paylaşmamak alınması gereken önlemlerden birisidir. Aynı zamanda şifreli ekran koruyucuları kullanılmalı ve bu ekran koruyucularının devreye giriş süreleri uygun bir şekilde ayarlanmalıdır.

2.9. Diğer Sistemler ile Alınabilecek Önlemler

Alınabilecek önlemler aşağıdaki gibidir:

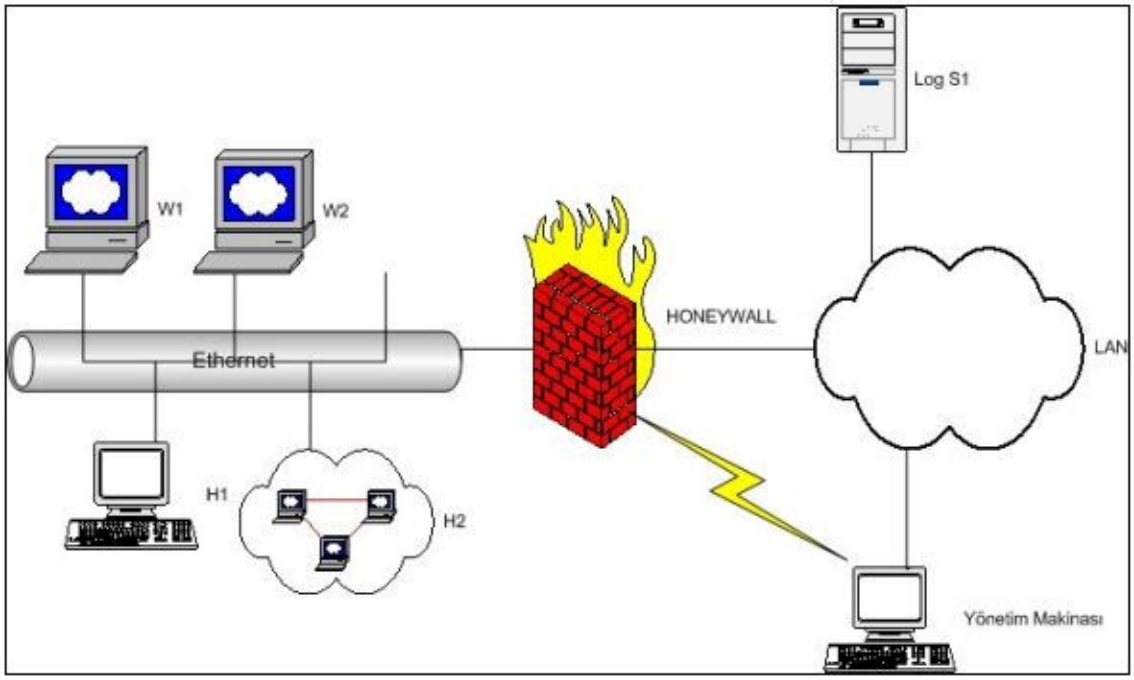
• Saldırgan Tuzağı Ağları (Honeynet)
• Merkezi Log Sunucu Sistemi
• Trafik Akış Analizi Sunucuları
• DNS Sunucu

2.9.1 Saldırgan tuzağı ağları (Honeynet)

Zararlı yazılım ve saldırganların saldırılarını saptamak için tuzak sistemleri (honeypot) kullanılabilir. Tuzak ağı (honeynet), tuzak sistemlerinden oluşan bir ağdır. Açık kaynak kodlu yazılımlarla bu tür sistemler kurmak ve yenilerini geliştirmek mümkündür. Saldırgan tuzağı ağı (honeynet), kurum tarafından kullanılmayan bir alt ağı kullanacak şekilde ayarlanmalıdır. Güvenlik duvarından, bu ağa gelen bütün trafiğe izin verilmelidir. Bu ağ, normalde dışarı hiç trafik oluşturmadığı için, bu ağa gelen bütün trafik incelenilmesi gereken ağ trafiğidir. Bu

trafik, saldırı trafiği olmaktadır [18]. Çeşitli bilinen zayıflıkları simüle eden, virüs ve worm etkinliğini yakalama amaçlı kurulan sistemlere örnek olarak "Nepenthes" ve "Amun" yazılımları verilebilir [19].

Bunun yanı sıra, "Honeyd" yazılımı ile bir makine üzerinde farklı işletim sistemlerini simüle eden sanal makineler, sanal yönlendiriciler ve sanal ağlar oluşturulabilir. Burada amaçlanan, bu makinelere saldırganların veya zararlı yazılımların erişimlerini takip etmektir. Ayrıca transparan olarak çalışan "Honeywall" yazılımı çalışan sistem, üzerinden geçen trafiği analiz etmekte, düzgün ayarlanması durumunda alt ağdaki tuzak sistem makinelerinin ele geçirilmesini ve buradan dışarı saldırı yapılmasını engelleyebilmektedir. ULAK-CSIRT Honeynet çalışma grubu bu konuda çalışmalarına devam etmektedir [20]. Ege Üniversitesi'nde kurulan tuzak ağının mantıksal mimarisi Şekil 3'de verilmiştir. Honeywall'in arkasında çeşitli honeypot sistemleri kurulmuştur [18].



Şekil 2.6. Ege Üniversitesi saldırgan tuzağı ağı mimarisi [18]

2.9.2 Merkezi log sunucu sistemi

Sistem loglarının düzenli takip edilmesi gerekmektedir. Birden fazla ve farklı sistemlerin loglarını; hepsine tek tek girip bakmaktansa, merkezi bir log sunucusuna atmak en etkin çözüm olmaktadır. Büyük miktardaki log'u analiz etmek ve içlerinden kritik mesajları çıkarmak için çeşitli yazılımlara ve betiklere(script) ihtiyaç duyulmaktadır. Sistem yöneticilerinin kullanabileceği log analizi ile bilgiler Ranum'un log analizi notlarında ayrıntılı olarak anlatılmıştır [21].

Ağ cihazlarından gelecek logları sürekli ve kesintisiz tutacak bir log sunucusu mutlaka bulundurulmalıdır. Bu sunucudaki kayıtlar incelenerek, kötü bir yazılım bulaşmış bilgisayarın yeri tespit edilebilir. Sistem yöneticilerinin kullanabileceği "syslog", "syslog-ng" gibi birçok açık kaynak kodlu yazılım log analizi için kullanılabilir.

2.9.3 Trafik akış analizi sunucuları

Bilinmeyen ve saldırı saptama sistemleri tarafından saptanamayan saldırılar için trafik çözümleme süreçleri kullanılmaktadır. Kurum ağı trafiği ve özellikle saldırgan tuzağı ağına gelen trafik, trafik akış analizi sunucuları tarafından ayrıntılı olarak incelenebilmektedir.

Trafik akış ile bahsedilen, iki makine arasındaki iletişimin özetlenmesidir. İletişime ilişkin yön, adres, ağ kapısı ve trafik büyüklüğü gibi bilgilerin çözümlenme için elde edilmesidir. Ağ trafiği çözümlenerek ağın normal davranışını modellemek mümkündür. Haftanın herhangi bir günü için, çeşitli zaman aralıklarında trafiğin özelliğini belirtecek veriler elde edilebilir. Trafik bilgisinde, incelenmesi ve saptanması gerekenlere örnek olarak aşağıdakilerden söz edilebilir [18]:

- O an çalışmayan makinelere/alt IP ağlarına giden trafik
- Yüksek ağ kapılarına giden/gelen servis isteği trafiği
- Yüksek bağlantı oranları

• Yüksek paket oranları
• İzlenmeyi engellemek için veriyi başka veri akışlarında saklayarak yapılan saldırılar (Covert channels)

Elde edilen ortalama değerlerden yaşanan sapmalar, kurum ağında farklı bir etkinliğin gerçekleştiği konusunda ipucu verecektir. Özellikle servis aksatma saldırıları, güvenlik açığı tarama girişimleri veya saldırı sonrasında sunucuların farklı amaçlar için kullanılması gibi saldırılar bu şekilde saptanabilir. Bunun yanı sıra, saldırının boyutu, saldırganın başka hangi sunucu ve servislere erişim kurduğu/kurmaya çalıştığı da incelenebilecektir [18].

2.9.4 DNS sunucu

Zararlı yazılımların bir kısmı IRC kanalları ile yönetilmektedirler [22]. Yazılım önceden belirlenmiş domain adı ile belirli bir IRC sunucusuna bağlanmakta ve istenen komutları almaktadır. İletişimi sağlayan IRC sunucusuna dinamik DNS adreslemesi ile ulaşmalar engellenerek, özellikle botnet türündeki kötü yazılımların etkinlikleri engellenmektedir. DNS sunucularını, zararlı yazılımlardan dolayı üzerlerine gelebilecek gereksiz trafik yükünü azaltmak için kaynağı olmayan adresler bollanmalıdır.

Ayrıca DNS sunucularına saldırı gibi gelebilecek istekleri gözlemleye bilmek için "dnstop" gibi açık kaynak kodlu yazılımlar kullanılabilir.

2.9.5 ARP saldırılarını tespit edebilen uygulamalar

Arp zehirlemesi tekniği, kötü amaçlı yazılımlar tarafından sıklıkla kullanılan bir teknik haline gelmiştir. Bu teknik ile aradaki adam saldırısı ile (man in the middle attack) hedef bilgisayarın bütün veri akışı dinlenebilmektedir. Arp tabanlı bu türden saldırılar için Arpwatch gibi uygulamalar sistem yöneticilerine yardımcı olabilecek açık kaynak kodlu yazılımlardır. Arpwatch ile ağdaki ARP aktiviteleri izlenerek loglanabilir [23].

3. AĞ SALDIRILARI

Ağ saldırıları denince öncelikle OSI'nin üçüncü (Ağ Katmanı) ve daha yukarı katmanlarıyla ilgili ataklar akla gelmektedir. Fakat ikinci katman atakları da en az üst katmanlara yönelik yapılan ataklar kadar etkili olabilmektedir. İkinci katman atakları yerel alan ağlarının içinden (LAN) yapıldığı için güvenlik duvarı ya da saldırı engelleme / tespit etme sistemleri tarafından engellenememektedir / tespit edilememektedir. Çünkü bu sistemler genellikle üçüncü ve daha üst katmanların güvenliği için tasarlanmıştır.

Ayrıca saldırı tespit veya engelleme sistemleri genellikle dış ağdan iç ağa gelebilecek saldırıları tespit ya da engellemek için kullanılmaktadır. Bu sistemler iç ağda yer alan bir saldırganı, yine iç ağda yer alan switchlere yapılacak saldırıları tespit edebilme / engelleme yetenekleri bulunmamaktadır.

Ağ güvenliği tüm OSI katmanlarının güvenliğinin ele alınmasıyla asıl amacına ulaşacaktır. Üst katmanların güvenliğinin alınıp, ikinci katman güvenliğinin ele alınmaması ağ güvenliğinin tam anlamıyla anlaşılamadığını gösterir. Bilgi sistemlerindeki güvenliğin sistemdeki en zayıf halka kadar olduğunun bilinmesi çok önemlidir.

Veri paketleri network cihazları aracılığı ile ağ üzerinden aktarılırken, kötü amaçlı kişiler bu cihazları ve bilgisayarları paket koklama (sniffing) ya da aldatma (spoofing) işlemleri yaparak bilgileri ele geçirebilirler.

Saldırganlar bu cihazların IP/MAC tablolarının tutulduğu ARP(Adres Çözümleme Protokolü) belleklerini zehirleyerek (kandırarak), paketlerin kendilerine ulaşmasını sağlayabilirler [24]. Saldırgan ele geçirdiği paket üzerinde değişimler yaparak bunu gerçek alıcısına gönderebilir. Yapılan bu işlemlerden ne göndericinin ne de alıcının haberi olmayacaktır. Tüm iletim boyunca kendi aralarında haberleştiklerini sanacaklar ve saldırgan kendini aradan çekip bilgisayarların ARP belleklerini eski haline getirmesiyle aldatma işlemi son bulacaktır.

3.1. Paket Koklama

Ağ üzerinde iletilen verilerin çalınması işlemine paket koklama denir. Bir paket koklayıcı ağ üzerindeki tüm trafiği kontrol etmek için bilgisayar içerisine yerleşir ve kendi kendine çalışır. Bunlar yazılımsal ya da donanımsal olabilir. Birçok koklayıcı, ayrımsız tür olarak adlandırılan "promiscuous mode" özelliğine sahip ethernet kart modülü vasıtasıyla kendileri haricinde diğer kullanıcılara iletilen paketleri de izinsizce ele geçirip, işleyebilirler. Bazı UNIX bilgisayarlarda tek bir komut satırı yazarak bilgisayarın ayrımsız tür ile çalışması sağlanabilir.

3.1.1. Paket koklayıcıların çalışma ortamı

İki farklı çalışma ortamı bulunmaktadır [25,26].

Paylaşımlı Ortam (Shared Ethernet):

Bu ortamda tüm kullanıcılar hub sayesinde paket alımı ve gönderiminde ortak bir ağ yapısı kullanarak haberleşirler ve bant genişliği için rekabet ederler. Bu yapıda ayrımsız tür özelliğine sahip ethernet kartları kullanılarak veriye gizlice ulaşılabilir. Yapılanlardan ne alıcının ne de göndericinin haberi olmaz.

Anahtarlamalı Ortam (Switched Ethernet):

Bu ortamda ise tüm bilgisayarlar hub yerine switch vasıtasıyla haberleşirler. Switch her bir bilgisayarın MAC (Ortam Erişim Kontrolü) adresini yani fiziksel ethernet adresini bir tabloda saklar. Switchler tüm ağda broadcast yayın yapmazlar, ellerindeki CAM'e (İçerik Adresleme Tablosu) tablolarına bakarak iletimlerini gerçekleştirirler ve her bir porta belirli bir MAC adresi tahsis edildiğinden bu yapı sayesinde iletimlerini gerçekleştirirler. Bu ortamda da switche çok fazla istek gönderip onun gelen isteklere cevap veremeyip, hub modunda çalışmaya başlamasına ve paketleri tüm kullanıcılara broadcast olarak aktarmasına neden olunabilir.

3.1.2. Koklama Türleri

IP Tabanlı Koklama:

Hub ortamında ya da bus topolojili bir ortamda herhangi bir bilgisayara ayrımsız tür özelliğini içeren bir kart takılarak koklama işlemi gerçekleşir. Saldırgan ele geçirdiği paketin hedef adreslerinde filtrelemeler yaparak, koklama işlemini gerçekleştirir. Bu işlem sadece switchsiz ortamlarda yapılabilir.

MAC Tabanlı Koklama:

Bu ortamda da yine ayrımsız tür özellikli Ethernet kartına sahip bilgisayar, mevcut yazılım vasıtasıyla elde ettiği paketi değişime uğratabilir. Paketler üzerinde ilgili alıcıların MAC adresleri filtrelenerek tüm paketler koklanabilir. Bu işlemler IP tabanlı koklamada olduğu gibi switchsiz ortamlarda gerçekleştirilebilir.

ARP Tabanlı Koklama:

Bu metot diğerlerine oranla biraz farklı işlem görür. Burada koklama yapacak bilgisayar switchli ortamda çalıştığından, ayrımsız tür özelliğinde olan bir Ethernet kartına sahip olmasına gerek yoktur. Burada yapılan işlem; switchler üzerindeki IP/MAC tablolarının saldırganlar tarafından yanlış ARP cevapları ile doldurulması ya da çok fazla istek alan switchin hub modunda çalışması sağlanarak koklama yapılır. ARP (Address Resolution Protocol) protokolü, IP'nin hizmetlerini kullanmaz o nedenle IP başlığı içermez [24]. ARP paketi, sadece yerel ağ üzerinde hazırlanıp gönderilir. Uzak ağlardaki (yönlendiricilere bağlı ağlar) kullanıcıların fiziksel adresini bilmek bir anlam ifade etmez. Çünkü yönlendiriciler fiziksel adreslere göre değil ağ katmanı mantıksal adresine göre (IP adresi) yönlendirme yapar. Bu yüzden routerlar üzerinde ARP kandırması yapılamaz.

Bir paket koklayıcı ağ üzerinde herhangi bir açık olup olmadığını anlamak ve verileri ele geçirip işlem yapabilmek için, Hata Analizi Cihazı, Veri Yakalama Cihazı,

Tampon Bellek, Performans Analizci, Kod Çözücü, Paket Düzenlemesi ve Aktarılması gibi çeşitli cihazlar kullanmaktadır [27].

Yine internet üzerinden erişilebilecek açık kaynak kodlu paket koklayıcılar; "Tcpdump" ve "Wireshark" yazılımları da paketlerin yakalanarak içeriğinin incelenmesi için kullanılmaktadırlar [27].

3.1.3. Paket koklayıcılarının kullanım amacı

Yöneticilere yardımcı koklayıcılar:

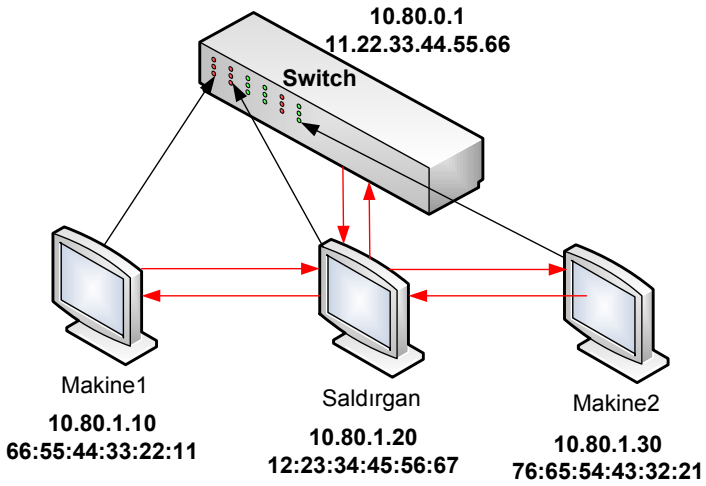
Paket koklayıcının bir ağda kullanılması LAN/WAN yöneticilerine ağ trafik analizi ve ağda bir problem olmuşsa bunun nerede olduğunun tanımlanmasını sağlar. Birçok koklayıcı kullanılıp sistem kontrol altına alınabilir. Bu şekilde bir paket koklayıcı hata ve performans analizi yapabilir. Hata analizinde ağdaki problemler bulunur, performans analizinde ise ağ tıkanıklıkları bulunabilir. Ayrıca paket koklayıcı, ağa zorla girmek isteyen kişileri ağ yöneticilerine bildirir.

Saldırganlara yardımcı koklayıcılar:

Saldırgan gibi kötü amaçlı kişilerin sistem üzerinde zarar vermek amacıyla kullandıkları programlardır. Bu şekilde ağda iletilen paketler ele geçirilip sistemlere büyük zararlar verilebilir.

3.2. Aldatma

Ağ üzerinde iletilen bilgiyi çalmak için bilgisayarlar ve ağ cihazları üzerinde çeşitli işlemler yapılıp, paketler yanlış hedeflere gönderilebilir.



Şekil 3.1. Switchli ağlardaki aldatma işlemi

Şekil 3.1'de, ARP belleğinde IP/MAC adresleri eşlemesini yanıltarak ARP aldatmacası gerçekleştirilmektedir [28]. Veriler ilgili portlara gönderilirken, aradaki saldırgan switchin ARP belleğini zehirleyerek her bir bilgisayara iletilen bilgilerin kendi üzerinden gitmesini sağlayabilir. Kırmızı bağlantılarla gösterildiği gibi iletim saldırgan bilgisayar üzerinden gerçekleşir.

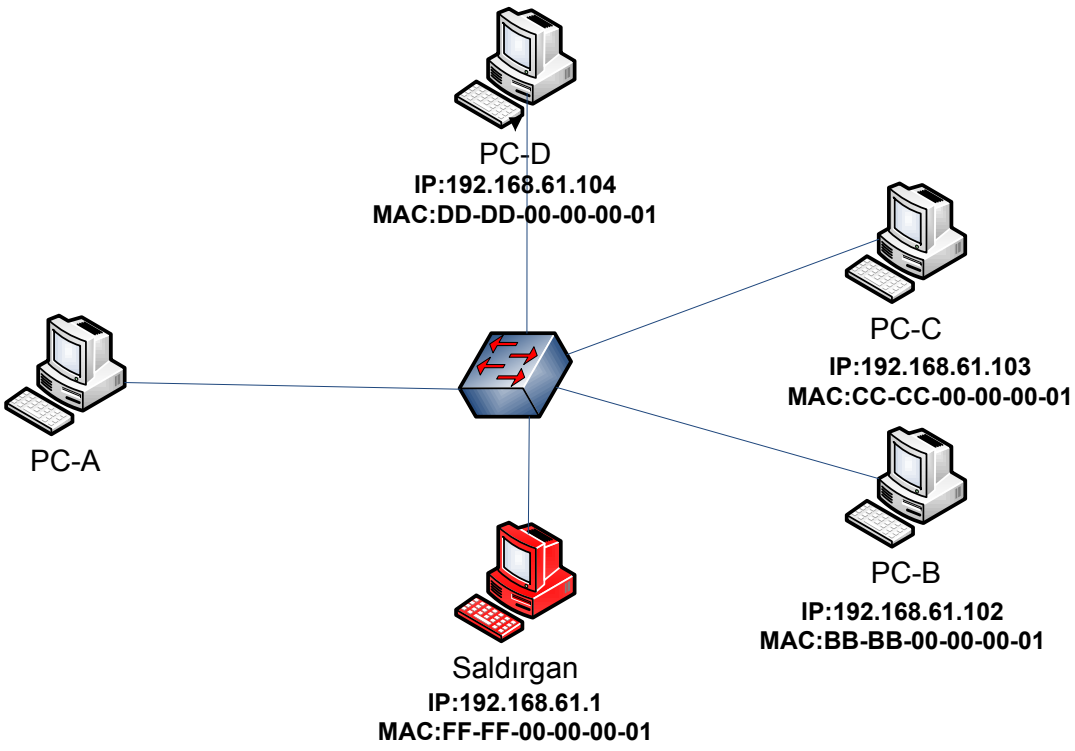
3.2.1. ARP Aldatmacası

ARP sahtekarlığı (ARP spoofing, ARP flooding, ARP poisoning) saldırısı lokal ağlarda gerçekleştirilebilen bir saldırıdır. Bu saldırı, üç şekilde gerçekleştirilmektedir:

- Birincisi; hedef bilgisayarın ARP tablosunun yanlış bilgilerle dolmasını sağlayarak, hedef bilgisayarın göndereceği paketlerin saldırganın istediği adreslere gitmesini sağlamak.

- İkincisi; hedef bilgisayarın göndereceği tüm paketlerin, saldırganın bilgisayarı üzerinden geçmesini sağlamak (Man in the Middle).

- Üçüncüsü de; hedef bilgisayarın, paketlerini bir başka bilgisayara göndermesini sağlayarak bu bilgisayara servis dışı bırakma (Denial of Service) saldırısı yapmak şeklindedir.



Şekil 3.2. Örnek ağ topolojisi [29]

Birinci saldırı

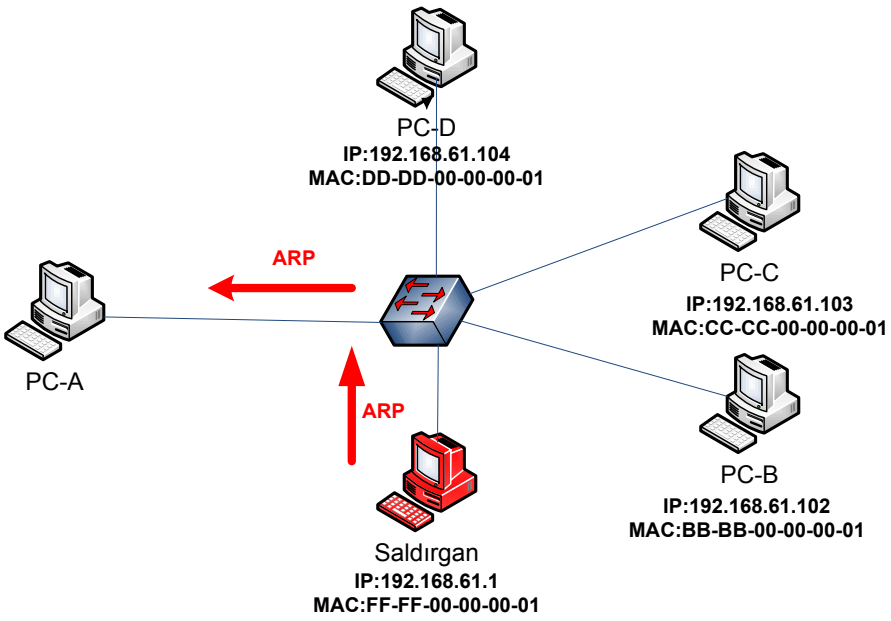
Ağda yer alan bilgisayarların birbirleriyle haberleşme yaptıkları durumda, A bilgisayarının ARP tablosu Çizelge 3.1'deki gibi olacaktır:

Çizelge 3.1 A bilgisayarının ARP tablosu

IP Adresi	MAC Adresi
192.168.61.1	FF-FF-00-00-00-01

…	
192.168.61.102	**BB-BB-00-00-00-01**
192.168.61.103	**CC-CC-00-00-00-01**
192.168.61.104	**DD-DD-00-00-00-01**
…	

Normal durumda A bilgisayarı, C bilgisayarına bir çerçeve göndereceği zaman çerçevenin hedef MAC adresi kısmına koyacağı adres CC-CC-00-00-00-01 olacaktır. İlk saldırıda saldırgan A bilgisayarının göndereceği tüm çerçevelerin ED-12-33-88-AA-B0 MAC adresli bir bilgisayara gönderilmesini sağlayacaktır. Bunun için saldırgan, A bilgisayarına sürekli olarak sahte ARP (spoofed ARP) çerçeveleri yollayacaktır. A bilgisayarı da ARP tablosunu gelen bu sahte ARP mesajlarına göre güncelleyecektir. ARP mesajları, herhangi bir durum tablosu tutmadıkları (stateless) ve ARP'ta herhangi bir kimlik doğrulama mekanizması olmadığı için de A bilgisayarı gelen ARP mesajlarının doğru bilgisayardan gelip-gelmediği kontrolünü yapamayacaktır. Tüm bilgisayarlar gibi A bilgisayarı da kendisine gelen ARP mesajlarıyla ARP tablosunu herhangi bir kontrole tabi tutmadan güncellemek durumundadır.



Şekil 3.3. Arp mesaj dağılımı [29]

Saldırgan; A bilgisayarına lokal ağda yer alan tüm IP adresleri için tek bir adet MAC adresini içeren (ED-12-33-88-AA-B0) ARP mesajları gönderecektir. Bu durumda A bilgisayarının ARP tablosu Çizelge 3.2'de gösterilen duruma dönecektir:

Çizelge 3.2. A Bilgisayarının ARP tablosu

IP Adresi	MAC Adresi
192.168.61.1	ED-12-33-88-AA-B0
192.168.61.2	ED-12-33-88-AA-B0
192.168.61.3	ED-12-33-88-AA-B0
…	ED-12-33-88-AA-B0
192.168.61.102	ED-12-33-88-AA-B0
192.168.61.103	ED-12-33-88-AA-B0
192.168.61.104	ED-12-33-88-AA-B0
…	ED-12-33-88-AA-B0
192.168.61.201	ED-12-33-88-AA-B0
192.168.61.202	ED-12-33-88-AA-B0
…	
192.168.61.253	ED-12-33-88-AA-B0
192.168.61.254	ED-12-33-88-AA-B0

A bilgisayarı ağdaki herhangi bir bilgisayara paket göndermek istediği zaman paketlerin hepsi ED-12-33-88-AA-B0 MAC adresine sahip olan bilgisayara gönderilecektir. Bu saldırıda saldırgan; A bilgisayarına göndereceği sahte ARP çerçevelerindeki MAC adresini değiştirmek suretiyle, A bilgisayarının göndereceği tüm paketleri istediği bilgisayara göndermeyi başarabilecektir. Bu şekilde saldırgan, A bilgisayarından çıkan tüm paketleri istediği bir bilgisayardan dinleyebilecektir.

İkinci saldırı

Bu saldırı, birinci saldırıda bahsedilen yöntemle gerçekleştirilmektedir. Bu saldırıda saldırgan, sahte ARP (spoofed ARP) çerçevelerinin içerisine kendi bilgisayarının MAC adresini yazmak suretiyle hedef bilgisayardan çıkan tüm paketlerin kendi bilgisayarı üzerinden geçmesini sağlar. Bu saldırı, "man-in-the-middle (MiM)" saldırısı olarak da bilinmektedir. Saldırgan, tüm ağa yolladığı ARP mesajlarının içerisine varsayılan ağ geçidinin (default gateway) MAC adresi yerine kendi MAC adresini yazarsa da kendisi varsayılan ağ geçidi olmuş olacaktır. Böylece ağdan dışarıya çıkacak olan tüm trafik saldırganın bilgisayarına gelebilecektir.

Üçüncü saldırı

Bu saldırı da yine birinci saldırıda bahsedilen yöntemle gerçekleştirilmektedir. Bu saldırı türünde saldırganın amacı, hedef bilgisayardan dışarı çıkacak olan paketleri dinlemek değil, hedef bilgisayara servis dışı bırakma (DoS) saldırısı yapmaktır. Bunun için saldırgan tüm ağda yer alan bilgisayarlara sahte ARP mesajları yollar. Bu mesajların içerisine de hedef bilgisayarın MAC adresini yazar. Böylece ağda yer alan tüm bilgisayarlar paketlerini hedef bilgisayara yollar. Bu da hedef bilgisayarın ethernet bağlantısının limitinin dolmasına sebep olur. Ayrıca hedef bilgisayarın işlemci gücünün de %100 oranında kullanılmasına sebep olarak, hem hedef bilgisayarın işlem yapmasını engellemiş olur, hem de ağda yer alan diğer bilgisayarların bağlantılarını engellemiş olur. Saldırgan tüm ağı etkileyip, bu saldırıyı çok fazla dikkat çekmeden yapmak isterse de, sahte ARP mesajlarını tüm ağa değil de, dönüşümlü olarak ağda yer alan bazı bilgisayarlara göndererek ağdaki

bilgisayarların erişim sorununu gizlemiş olur. Ağdaki bilgisayarlardaki erişim problemi dönüşümlü olarak gözlendiğinden, bunun bir atak olduğunun anlaşılması oldukça zor olacaktır.

Çözüm

Oldukça eski bir protokol olan ARP'ın çalışma yapısından kaynaklanan bu sorunların protokol bazında bir çözümü bulunmamaktadır. ARP'ın bu eksikliğini, switch cihazları üzerinde alınacak önlemlerle kapatmak mümkündür.
Switch cihazları da IP adresi – MAC adresi eşleşmelerini (ARP tablosu) port bazında tutmaktadır. Switch cihazları üzerinde port bazında bir IP adresi – MAC adresi eşleştirmesi yapıldığı takdirde ilgili porttan farklı bir MAC adresinin gelmesi mümkün olmayacaktır. Böylece saldırgan bağlı olduğu switch cihazının portundan farklı IP adresi – MAC adresi eşleşmelerine sahip olan ARP mesajları gönderemeyecektir. Switch cihazının bir portu için sadece bir IP adresi ve bir MAC adresi tanımlanabilecektir.

Bu önleme; "Dynamic ARP Inspection" ya da "Dynamic ARP Protection" denmektedir. "Dynamic ARP Inspection" / "Dynamic ARP Protection" yapılandırması yapılmış olan switch cihazları, aynı zamanda 0.0.0.0 ya da 255.255.255.255 gibi geçerli olmayan IP adreslerinden gelen ARP isteklerini de engelleyecektir.

DHCP sunucusunun bulunduğu bir sistemde Cisco marka switch cihazlarında bu özellik Çizelge 3.3'de gösterilen ayarlamalarla aktif hale getirilir:

Çizelge 3.3. Cisco switchleri için yapılandırma komutları

```
Cisco(config)#ip dhcp snooping vlan 53, 61
Cisco(config)#ip arp inspection vlan 53,61
Cisco(config)#interface GigabitEthernet 5/48
Cisco(config-if)#ip dhcp snooping trust
Cisco(config-if)#ip arp inspection trust
```

Çizelge 3.3'de, IP adreslerinin otomatik olarak dağıtıldığı (bir DHCP sunucusunun bulunduğu) bir sistemde 53 ve 61 numaralı VLAN'ler için "Dynamic ARP Inspection" özelliği aktif hale getirilmiştir. Switch cihazı 53 ve 61 numaralı VLAN'lere bağlı olan portlar için kendi üzerinde tuttuğu IP adresi – MAC adresi tablosuna bakarak ARP çerçevelerine izin verecek ya da bu çerçeveleri düşürecektir. Çizelge 3.4'de HP ProCurve marka switch cihazlarında DHCP sunucusunun bulunduğu bir ortamda "Dynamic ARP Protection" özelliğini aktif hale getirecek kodlar gösterilmiştir.

Çizelge 3.4. HP ProCurve Switch cihazları için yapılandırma komutları

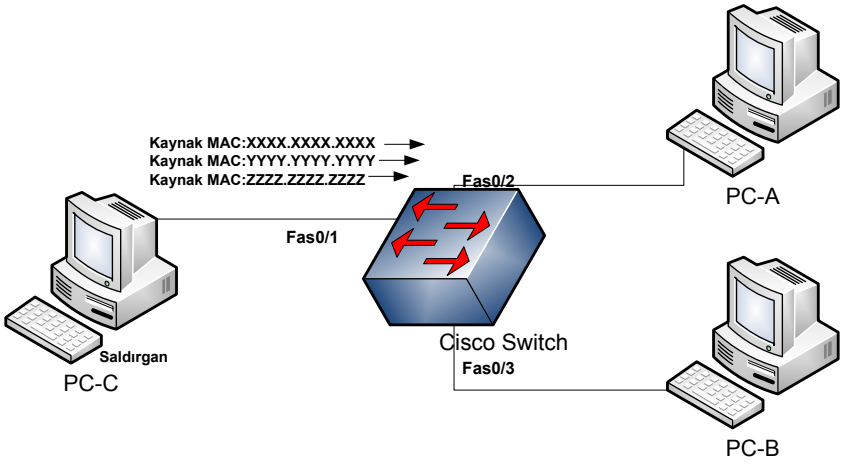
```
ProCurve(config)# arp-protect vlan 53,61
ProCurve(config)# arp-protect trust c1-c12, e3
```

Bu konfigürasyonlarda dikkat edilmesi gereken husus, anahtarlama cihazlarının birbirlerine bağlandıkları portların güvenilir (trusted) olarak tanımlanmasıdır. Güvenilir olarak tanımlanmayan portlardan gelen ARP istekleri kontrol edilemeyecek, güvenilir olmayan (untrusted) portlardan gelen ARP mesajları da kontrol edilecektir.

3.2.2. MAC taşması (MAC Flooding) atağı

Her bir switchin üzerinde, switche bağlı ağ cihazlarının MAC adresleriyle switchin portlarının eşleştirildiği bir tablo bulunmaktadır. Switch, portları arasındaki veri iletişimini bu tablodaki bilgilere bakarak yapmaktadır. Bu tabloya MAC adres tablosu denebildiği gibi CAM (Content Address Memory) tablosu da denilmektedir. MAC adres tablosunda; port numarası, porta bağlı olan bilgisayarların MAC adresleri ve ilgili portun hangi VLAN'e ait olduğu gibi bilgiler yer almaktadır. Switch, portlarına gelen bir çerçevenin önce hedef MAC adres kısmına bakmaktadır. Daha sonra çerçevenin içinde yer alan bu hedef MAC adresinin kendi MAC adres tablosunda olup, olmadığına bakmaktadır. MAC adresini tabloda bulursa çerçeveyi ilgili porta göndermektedir. Yapılan bu işleme anahtarlama (switching) denilmektedir. Tüm ikinci katman switchleri bu prensibe göre çalışmaktadır. Switch cihazlarının önemli bir zafiyeti, switchlerin MAC adres tablosunun dolması durumunda ortaya çıkmaktadır. Switchlerin MAC adres tablolarının bir sınırı vardır. Bu kapasite, cihazın marka, model ve donanımına bağlı olarak değişiklik göstermektedir.

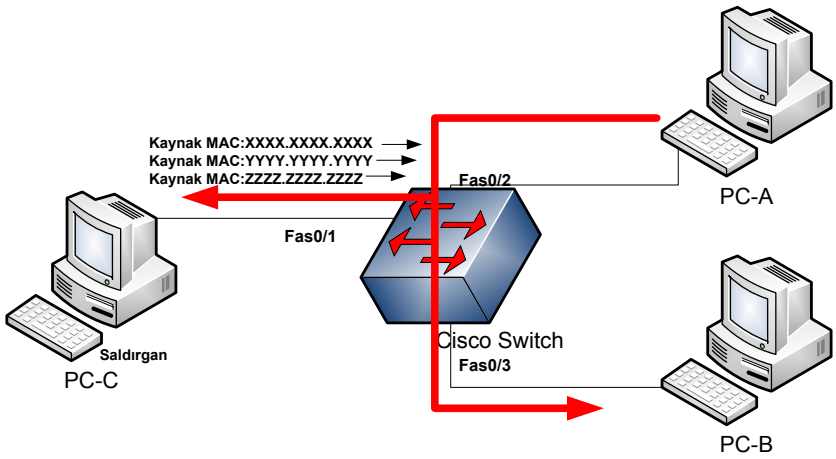
Gelen çerçevenin hedef MAC adresi switchin MAC adres tablosunda bulunduğu takdirde switch bu çerçeveyi ilgili porta göndermektedir. Fakat switche gelen çerçevenin hedef MAC adresi, switchin MAC adres tablosunda bulunmadığı durumlarda, switch çerçeveyi tüm portlarına yollamaktadır.



Şekil 3.4. Sahte MAC adresi gönderimi [29]

Switchin MAC adres tablosunun tamamen dolu olduğu düşünülürse ve switchin, beşinci portuna bağlı C bilgisayarından gönderilen çerçevenin hedef MAC adresinin, switchin MAC adres tablosunda bulunmadığı varsayılırsa switch bu durumda, beşinci portundan gelen çerçeveyi diğer tüm portlarına yollayacaktır. Bu da ilgili beşinci porttan çıkan tüm bilginin diğer portlara da gönderilmesi sonucunu doğuracaktır. Bu da saldırganın, switch üzerinde herhangi bir port yönlendirmesi yapmadan, sadece switchin MAC adres tablosunu sahte MAC adresleriyle doldurmak suretiyle, switch üzerindeki tüm trafiği dinleyebilmesine yol açacaktır. Bu durum ayrıca switchin performansına da olumsuz etki edecektir.

Şekil 3.4 ve Şekil 3.5'de Mac Flooding Atağı' nın oluşumu adım adım gösterilmiştir.



Şekil 3.5. Tüm portlara bilginin gönderilmesi [29]

Çözüm:

Switch cihazların portlarına MAC adresi kilitlemesi uygulanırsa olası saldırıya karşı önlem alınabilir. Cisco cihazlar için Çizelge 3.5'de, HP switchler çin Çizelge 3.6'da MAC adresi kilitlemesi örnek konfigürasyon satırları bulunmaktadır.

Çizelge 3.5. CISCO Konfigürasyonu

Anahtar(config)#interface range GigabitEthernet 3/2 – 48 Anahtar(config-range)# switchport mode access Anahtar(config-range)# switchport port-security Anahtar(config-range)# switchport port-security maximum 3 Anahtar(config-range)# switchport port-security violation restrict Anahtar(config-range)#switchport port-security mac-address sticky

Çizelge 3.6. HP ProCurve konfigürasyonu

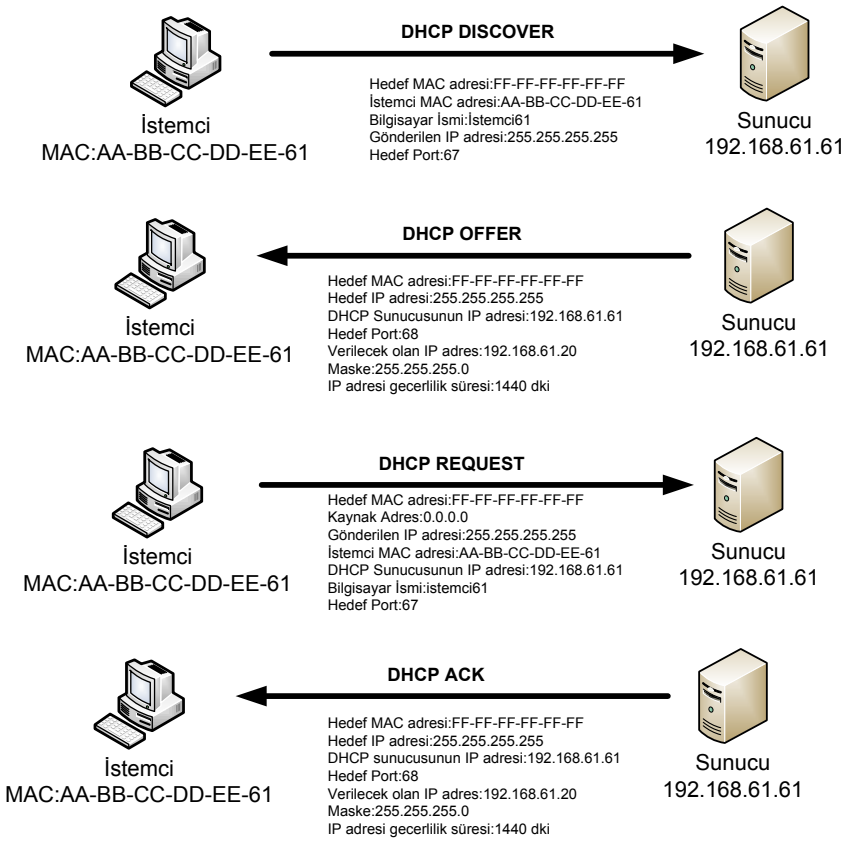
Anahtar(config)#port-security ethernet 1-10 address-limit 3 learn-mode static action send-disable

3.2.3. DHCP Snooping Atakları

DHCP sömürü (DHCP Starvation) ve sahte DHCP (Rogue DHCP) saldırıları ikinci katmanda gerçekleştirilebilecek olan önemli saldırılardan iki tanesidir.

DHCP Çalışma mantığı

Otomatik olarak IP adresi alma ayarıyla ağa bağlanmış olan bir bilgisayar, IP adresi almak için 255.255.255.255 adresine UDP 67 numaralı hedef portundan bir istek mesajı gönderir. Bu mesaja DHCP DISCOVER mesajı denir.



Şekil 3.6. DHCP Çalışma mantığı [29]

DHCP DISCOVER mesajını alan DHCP sunucusu bu mesaja UDP 68 numaralı hedef portu üzerinden DHCP OFFER mesajıyla karşılık verir. DHCP sunucusu tarafından gönderilen bu DHCP OFFER mesajında; istemcinin MAC adresi, istemciye verilecek olan IP adresi, ağ maskesi bilgisi, verilecek olan IP adresinin geçerlilik süresi ve IP dağıtan DHCP sunucusunun IP adresi yer alır.

Bir istemci aynı anda sadece bir DHCP sunucusundan gelen DHCP OFFER mesajını değerlendirebilir. İstemci kendisine en önce ulaşan DHCP OFFER mesajını hesaba katar. Bir DHCP sunucusundan gelen DHCP OFFER mesajını alan istemci bu mesaja DHCP REQUEST mesajıyla karşılık verir. DHCP REQUEST mesajı da 255.255.255.255 adresine yollanmak durumundadır. Çünkü IP adresi alma sürecinin bu aşamasında istemcinin henüz bir IP adresi bulunmamaktadır.

DHCP REQUEST mesajını alan DHCP sunucusu bu mesaja DHCPACK mesajıyla karşılık vererek istemcinin IP adresi isteğini onaylamış olur. Böylece istemci, IP adresini ve diğer ağ parametrelerini DHCP sunucusundan almış olur. Şekil 3.6'da DHCP' nin çalışma mantığı gösterilmiştir.

DHCP'nin yapısında bir kimlik doğrulama mekanizması bulunmadığından DHCP sunucular kendilerine DHCP OFFER mesajlarıyla yapılan her isteğe cevap vermek durumundadırlar. Bu durum DHCP protokolünün zayıf noktalarından birisidir.

DHCP sömürü saldırısı şu şekilde gerçekleşmektedir:

Saldırgan, bilgisayarının MAC adresini periyodik olarak değiştirir ve her MAC adresi değiştirdiğinde de lokal ağda yer alan DHCP sunucusundan DHCP OFFER mesajıyla IP adresi talep eder. Saldırgan, DHCP sunucusundan yaptığı her IP isteğinde bilgisayarının MAC adresini değiştirmek zorundadır. Çünkü gönderilen DHCP OFFER mesajıyla beraber DHCP sunucusuna istemcinin MAC adresi de gönderilmektedir. DHCP sunucusundan yapılan bu IP adresi talepleri belirli bir süre sonra DHCP sunucusunun dağıttığı adres uzayının tükenmesine yol açacaktır. Bu şekilde saldırgan, DHCP sunucusunun dağıttığı tüm IP adreslerini alarak normal kullanıcıların IP adresi alamamasına neden olacaktır. Bu saldırıya DHCP sömürme saldırısı denmektedir. Bu saldırı aynı zamanda servis dışı bırakma (denial of service) saldırısının bir türüdür.

Bir başka tür DHCP saldırısı ise lokal ağa sahte bir DHCP sunucusu konumlandırılarak gerçekleştirilmektedir. Bir ağda birden fazla DHCP sunucusunun yer alması durumunda istemci bilgisayar, DHCP DISCOVER mesajına ilk cevap veren DHCP sunucusunun IP ayarlarını alır. DHCP DISCOVER mesajlarına lokal ağda yer alan hangi DHCP sunucusunun cevap vereceği ise tamamen belirsiz bir durumdur. Saldırgan, IP adresi isteğinde bulunan istemcilere istediği IP adresi ayarlarını verebilecektir. Saldırgan, IP ayarlarında yer alan "default gateway (varsayılan ağ geçidi)" adresini yine lokal ağda kontrolü kendisinde olan bir bilgisayarın IP adresi olarak belirlerse bu durumda da sahte DHCP sunucusunun IP

dağıtmış olduğu tüm istemcilere ait olan trafik, belirlemiş olduğu bu bilgisayar üzerinden akacaktır. Böylece saldırgan IP dağıtmış olduğu tüm bilgisayarların ağ trafiğini gözetleme imkânına da sahip olacaktır. Bu saldırıya sahte DHCP saldırısı denmektedir ve bu saldırı araya girme (man-in-the-middle) saldırısı türlerinin biridir. DHCP'nin yapısı gereği bu tür saldırılara karşı bir önlemi bulunmamaktadır. Bu saldırılara karşı önlemler ancak lokal ağlarda yer alan switch cihazları üzerinde alınabilmektedir. Lokal ağlarda yer alan switch cihazlarının bu saldırılara karşı önlem alabilme özellikleri bulunmalıdır.

DHCP sömürüsü saldırısına karşı önlem almak oldukça kolaydır. Switch cihazlarının portlarına MAC adres kilitlemesi uygulayarak bu saldırıdan kurtulmak mümkündür. Cisco cihazlar için Çizelge 3.7'de, HP Procurve cihazlar için Çizelge 3.8'de saldırıyı önlemek için yapılması gereken konfigürasyonlar gösterilmiştir.

Çizelge 3.7. Cisco DHCP Snoop konfigrusyon kodları

```
Cisco(config)#ip dhcp snooping vlan 20-61
Cisco(config)#interface GigabitEthernet 6/17 (DHCP sunucusunun bağlı olduğu port)
Cisco(config-if)#ip dhcp snooping trust
```

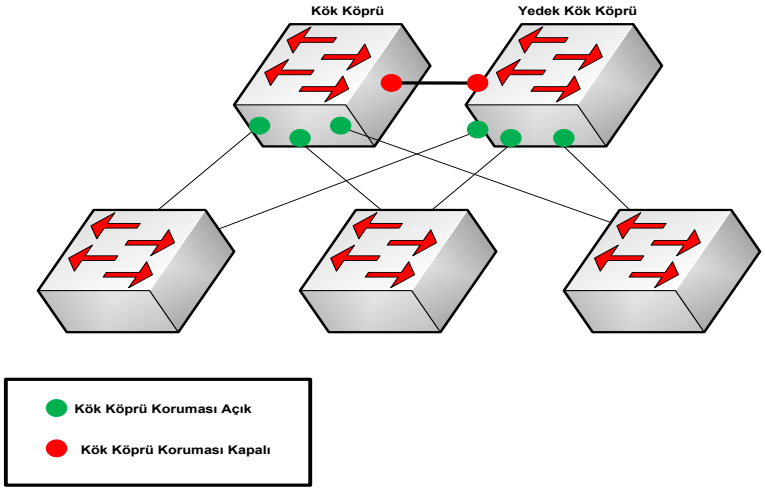
Çizelge 3.8. HP ProCurve DHCP Snoop konfigrusyon kodları

```
ProCurve(config)#dhcp-snooping
ProCurve(config)#dhcp-snooping authorized-server 10.1.1.10
ProCurve(config)#dhcp-snooping trust a1-a20
ProCurve(config)#dhcp-snooping vlan 1-3
```

3.2.4. Spanning-Tree protokolü (STP) atakları

Spanning-Tree protokolü bir ağda anahtarlama döngülerini (switching loops) engellemek için kullanılan bir protokoldür. Spanning-Tree protokolünün aktif olduğu switchler kendi aralarında bir kök anahtar (root switch) seçerler.
Spanning-Tree protokolüne dâhil olan her switchin bir "bridge ID" değeri vardır. Bu değer "bridge prirotity" ve MAC adresi değerlerinden oluşur. "bridge prirority" nin varsayılan değeri 32768'dir. "bridge prirority" değeri en düşük olan switch kök switch olarak seçilir. Bu seçim, BPDU çerçeveleri aracılığıyla yapılır. Ağa BPDU çerçevesi üreten bir bilgisayar bağlanıp, bağlanan bilgisayarın ürettiği BPDU çerçevelerinin içindeki "birdge prirority" değeri de 0 yapılmak suretiyle ağa bağladığımız bilgisayarın kök switchin yerini alması sağlanabilir. Böylece tüm ağ trafiği bağlanan bu sahte kök switch bilgisayarı üzerinden geçer. Ayrıca kök switchin yerine geçen bu bilgisayarın ağ kablosunu sürekli, söküp takmak suretiyle kök switch seçimini tekrar başlatarak ağda bağlantı kesintilerine ve performans problemlerine de yol açmak mümkündür. Ağa, kendisini bir switchmiş gibi gösteren bir bilgisayar yerine normal bir switch de bağlanabilir. Bağlanan switchin "bridge priority" değeri "0" yapılarak bu switch de "root bridge" olarak seçtirilebilir.

Şekil 3.7'de çizilen topoloji üzerinde root bridge (kök köprü) durumu gösterilmiştir.



Şekil 3.7. STP Guard Ağ topolojisi [29]

Ağ üzerindeki saldırılara karşı önlem almak için switchlere; Cisco cihazlar için Çizelge 3.9'daki, HP ProCurve Cihazlar için Çizelge 3.10'daki komutlar girilmelidir.

Çizelge 3.9. Cisco marka switchler için STP Guard

```
ANAHTAR_CISCO(config)#interface range fastethernet 7/2 - 46
ANAHTAR_CISCO(config-if-range)#spanning-tree rootguard
```

Çizelge 3.10. HP ProCurve marka switchler için STP Guard

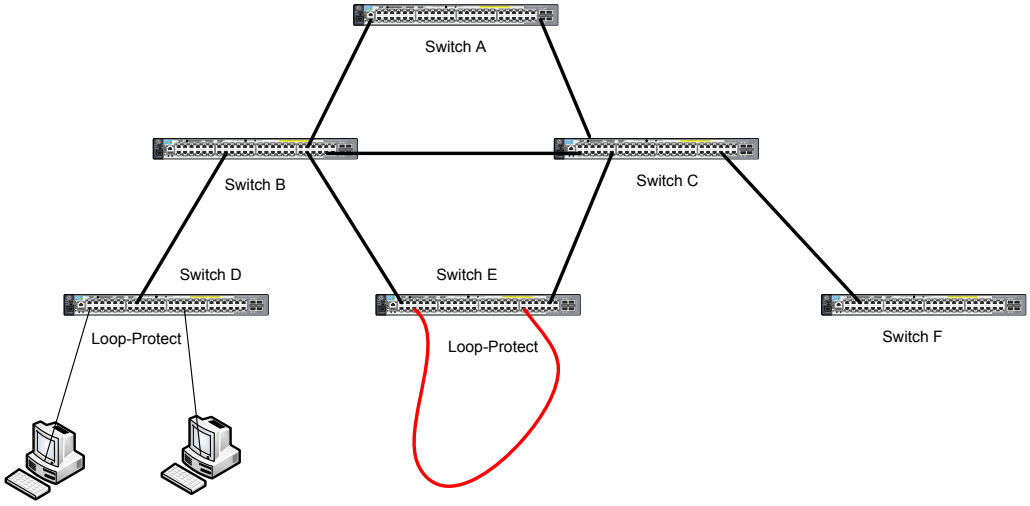
```
ANAHTAR_HP(config)#spanning-tree A1 - A20 root-guard
```

3.2.5 Loop Protect

Cihazın fiziksel portlarını ve sistemin genelini korumaya yöneliktir. Kullanıcıların en sık yaptığı aynı kablonun iki ucunun da aynı switche ya da birbirlerine bağlı bir switch gurubuna takılması sonucu sistemin çalışmaz hale getirilmesinin önüne geçmek için tasarlanmıştır. Bu sayede bilerek ya da bilmeyerek sisteme bu şekilde zarar verebilecek tüm sorunlar başlamadan bertaraf edilir. Loop protect özelliği Spanning Tree Protocol'ünün farklı bir çeşidi olarak düşünülebilir. Amaç, yanlışlıkla ya da bilerek ağ içerisinde switchlerin ikinci katman paketlerini kendi kendilerine düşürebilecek bir mekanizmaya sahip olmamasının ortaya çıkaracağı sorunları engellemektir. Bu sorunlar, ağ içerisinde network performansında ciddi kayıplar yaşanmasına ya da ağın tamamen saldırı boyunca kullanılamaz hale gelmesine neden olabilir.

Şekil 3.8'de örnek bir ağ topolojisi oluşturularak "Loop Protect " özelliği açıklanmaya çalışılmıştır. Switch E üzerinde bir porttan çıkan kablo yine aynı

switchin farklı bir portuna takılmıştır. Böyle bir durumda oluşan Loop (döngü)'larla cihaz zamanla kullanılamayacak duruma gelecektir.



Şekil 3.8. Loop Protect Örnek ağ topolojisi

Çözüm

Loop hatasını önlemek için "Loop Detect " yöntemi kullanılmaktadır. Switchin konfigürasyon komutlarının yer aldığı kısma Çizelge 3.11'de gösterilen komutların girilmesi gerekmektedir. Girilen komutlar ile cihazın portlarında "Loop" algılaması aktif hale getirilir.

Çizelge 3.11. Cisco ve Procurve cihazlar için Loop Protect

Cisco(config))#Spanning-tree loopguard default	Cisco Cihazlar
ProCurve(config)#dhcp-snooping	HP ProCurve Cihazlar

Ağ üzerinde tüm güvenlik önlemleri alınmış olsa dahi, ağ üzerinde bulunan sunucular ve diğer cihazlar bir kesintisiz güç kaynağı ya da bir jeneratöre bağlanmamışsa alınmış olunan ikinci katman ve daha yukarı katman güvenlik

önlemleri bir elektrik kesintisi durumunda hiçbir anlam ifade etmeyecektir. Ya da ağ ortamının bulunduğu binada elektrik şalteri herkesin ulaşabileceği bir yerdeyse ve bulunduğu yerde yeterli güvenlik önlemleri de alınmamışsa üst katmanlar için alınmış olunan güvenlik önlemleri yine bir işe yaramayacaktır. Çünkü elektrik kesilirse sistem haliyle çalışamayacaktır.

4. GELİŞTİRME VE SUNUM ORTAMI

Bu bölümde; uygulamanın geliştirilmesinde kullanılan araçlardan bahsedilerek geliştirilen uygulama ayrıntılı olarak anlatılmıştır. Uygulamada kullanılan araçlara ilişkin detaylar aşağıda başlıklar halinde belirtilmiştir.

4.1. VMware Workstation

VMware sanallaştırma dünyasında en çok rağbet edilen yazılım olarak göze çarpmaktadır. Hem ücretli hem de ücretsiz kullanım için bulunan yazılımları ile farklı amaçlar için farklı hizmetler sunmaktadır. Özellikle son zamanlarda sanallaştırma ile bakım, devamlılık, yedekleme gibi işlemlerin ucuz ve zahmetsizce gerçekleştirilebilmesinden ötürü, sanallaştırma yazılımlarına olan rağbet gün geçtikçe artmaktadır. VMware gibi XEN, VirtualBox, QEMU gibi yazılımlar açık kaynak kod dünyasında yerlerini almaktadırlar. Burada VMware Workstation uygulamasının tercih edilmesindeki en büyük sebep ağ uygulamaları için oldukça esnek şartlar sağlamasıdır [30].

VMware Workstation (Gelişmiş Sanal Makine Yaratma Aracı) işletim sistemleri ve ağ alt yapılarını sanallaştırma için kullanılan ve bu konuda farklı çözümleri olan bir masaüstü kullanım için öngörülen VMware uygulamasıdır. Unix ve Linux türevleri başta olmak üzere hemen hemen bütün işletim sistemleri için desteği bulunmaktadır. Bütün bunların yanında özelleştirilmiş ağlarda oluşturmak mümkündür.

VMware aynı bilgisayarda disk bölümlendirmeye gerek kalmadan birden fazla işletim sistemine sahip olmak için kullanabilen bir sanal makine yazılımıdır. Ağ, cihaz kontrolü, dosya paylaşımı, kopyala yapıştır özellikleri, geri alma/ileri alma gibi özellikleri bu sanal makine yazılımı üzerinden çalıştırdıkları işletim sisteminde de kullanılabilir ve güvenli bir şekilde işletim sistemi kullanılabilir [31].

VMware farklı sürümleri mevcut olup (VMware 8.0, 7.0, 6.5, 6.0, 5.5, 5.0, 4.5) en son sürümü Windows işletim sistemi için VMware Workstation 9.0.2 (2013-03-07) sürümüdür [32].

VMware Workstation, bu çalışma içerisinde ilgili yazılımın geliştirilmesi sırasında Windows işletim sistemine sahip bir bilgisayar üzerinde ikinci bir işletim sistemi kurmak için kullanılmıştır.

4.2. Bash Script

Bash GNU işletim sistemi için bir kabuk ya da başka bir deyişle komut dili yorumlayıcısıdır. Bourne-Again SHell sözcüklerinde türetilmiş bir kısaltmadır. Bell Araştırma Laboratuarının Unix'inin yedinci sürümündeki, şu anki Unix kabuğu sh'ın atasının yazarı Stephen Bourne'a atfen bu isim verilmiştir [33].

Bash, sh'ın hemen hemen tüm özelliklerini ve Korn kabuğu olan ksh ile C kabuğu olarak bilinen csh'ın kullanışlı özelliklerini bir araya getirir. IEEE POSIX belirtiminin IEEE POSIX Kabuk ve Araçları bölümüne (IEEE Standardı 1003.1) uygun bir ürün olması amaçlanmıştır. sh'ın hem etkileşimli hem de programlama için kullanımını işlevsel olarak arttıran geliştirmeler içerir [33].

GNU işletim sistemi, csh'ın bir sürümü de dahil olmak üzere başka kabuklarla da teçhiz edilmişse de Bash öntanımlı kabuktur. Diğer GNU yazılımları gibi Bash'de bir çok işletim sistemine uyarlanabilir - MS-DOS, OS/2 ve Windows platformları için bağımsız olarak desteklenen sürümleri vardır [33].

Bash Script dilinin kullanıcıya zaman kazandıran birçok özelliği vardır.

<u>Bash Script Dili Özellikleri</u>

- Bash Script dilinin en önemli özelliklerinden birisi dosya isimlerini tamamlamasıdır. Komut satırında tamamlanmamış bir komut veya dosya ismi yazıldıktan sonra "TAB" tuşuna basılırsa satır tamamlanacaktır. Komut

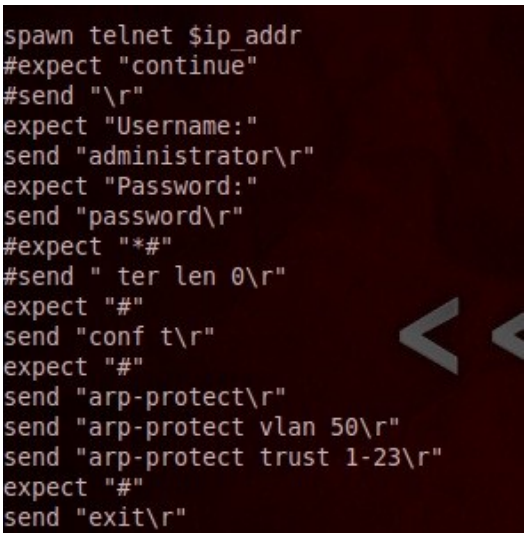
satırındaki karakter kümesiyle başlayan birden fazla komut varsa bir sinyal sesi duyulacak ve kullanıcıdan yeteri kadar karakteri yazılması beklenecektir. Çizelge 4.1'de Bash Script dilinin kullanımına örnek oluşturacak komutlar gösterilmiştir.

Çizelge 4.1. Bash Script komutları

$ ls
 	
postgres mandel.doc lilo-howto
 	
$ vi post <TAB>
 	
$ vi postgres

- Bash Script diliyle daha önceden yazılmış komutlar yön tuşları kullanılarak bulunup tekrar kullanılabilmektedir.

Şekil 4.1'de program içerisinde kullanılan Bash Script komutlarının bir bölümünün görüntüsüne yer verilmiştir.



Şekil 4.1. Bash Script yapılandırma komutları

Bash Script dili; Linux işletim sistemi çekirdeği üzerinde PHP dili ile uyumu ve kullanım kolaylığı gibi özelliklerinden dolayı geliştirilen yazılımda tercih edilmiştir.

4.3. PHP Dili

PHP (Hypertext Preprocessor - Üstünyazı Önişlemcisi); genel ağ için yaratılmış, sunucu taraflı, çok geniş kullanımlı, genel amaçlı, HTML içerisine gömülebilen betik ve programlama dilidir. PHP, ilk kez Rasmus Lerdorf tarafından 1995 yılında, web üzerinden sayfasına ziyaret edenleri izlemek amacıyla bir dizi Perl betiği kullanılarak geliştirilmiştir [34].

PHP 2013 yılı istatistiklerine göre, 200 milyondan fazla web sitesinde yüklü olarak bulunmaktadır ve gün geçtikçe kullanımı yaygınlaşmaktadır [35]. Kolay öğrenilmesi ve hızlı performansı tercih edilmesinde ana etkenleri oluşturmuştur.

Geliştirilen yazılımda, web ara yüzünün tasarımında kullanılmıştır. Linux işletim sistemi altında Bash Script dili ile uyumlu olacak şekilde kullanılmıştır.

Şekil 4.2'de geliştirilen uygulamanın tasarımında kullanılan PHP kodlarının bir bölümü gösterilmektedir.

```php
<?php
session_start();

$name = $_POST['user'];
//$email = $_GET['email'];
$passw = $_POST['passw'];
$submit = $_POST['submit'];

        //$sorgu = "SELECT * FROM user where username='$name' and password='$passw'";
        //$say = mysql_num_rows($result);
//echo $row['username'];
//echo $row['password'];
if(isset($submit)){
        if($name == "admin" and $passw == "123456")
        {
        $_SESSION['giris'] = "true";
        $_SESSION['user'] = $user;
        $_SESSION['passw'] = $passw;
        header('Location:netwdevcontrol.php');
        //echo "Dogru.";
        }
        else
        {
        echo "Yanlis girdiniz...";
        }
}
?>
```

Şekil 4.2. PHP tasarım kodlarının bir bölümü

4.4. VPN (Sanal Özel İletişim Ağı)

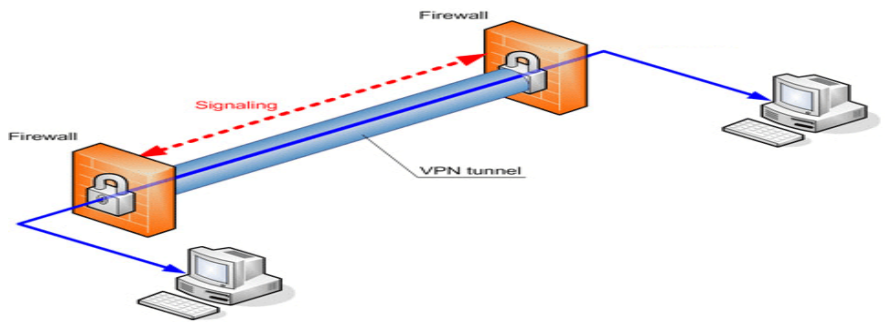
VPN, Virtual Private Network'ün (Sanal Özel Ağ) kısaltması olup, ağlara güvenli bir şekilde uzaktan erişimde kullanılan bir teknolojidir. Sanal bir ağ uzantısı yarattığından uzaktan bağlanan makine konuk gibi değil, ağa fiziksel olarak bağlıymış gibi görünür.

Ortak kullanıma açık veri ağları üzerinden kurum ağına bağlantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi esas olarak alınmaktadır. Dağınık yapıdaki özel iletişim ağlarının üzerinde bulunan bilgilerin, kamu iletişim ağı altyapısını kullanarak paylaşılması sırasında, kamu iletişim ağı üzerinden geçen bilgilerin üçüncü kişiler tarafından deşifre edilmesinin engellenmesi gerekmektedir. VPN bu sorunu ortadan kaldırmak için geliştirilmiş bir sistemdir.

VPN sayesinde, özel iletişim ağına ait uzaktaki kullanıcıların, güvenilir olmayan kamu iletişim ağları üzerinden, kendi iletişim ağları ile serbestçe ve güvenilir bir şekilde haberleşmesi sağlanabilmektedir [36].

VPN sistemleri kendi özel bilgilerinizi taşıyan haberleşme paketlerinin korunmasını, kendi aralarında yarattıkları sanal tünellerin sayesinde yapabilmektedir. VPN sistemlerinde dört seviyeye kadar güvenlik sağlanabilmektedir. Bu seviyeler, “Sertifikasyon, Şifreleme, Tanımlama-Sorgulama ve Tünelleme” olarak sayılmaktadır [36].

Şekil 4.3’de örnek bir VPN uygulaması gösterilmiştir.



Şekil 4.3. VPN uygulaması

SSLVPN

İnternetin gelişimiyle kurum ağlarına uzaktan erişerek bilgi paylaşımı yapmak hem ekonomiklik hem de verimlilik artışı sağlamıştır. Uzaktan erişim ihtiyacı beraberinde sorunsuz bağlantı ve güvenlik kaygılarını da beraberinde getirmiştir. Güvenli uzaktan erişim yolu olan IPSec (Internet Protokol Security) VPN, kullanıcı bazlı sorunları ve yüksek toplam sahip olma maliyeti nedeni ile yerini daha kolay yönetilebilir ve ekonomik olan SSL VPN teknolojisine bırakmaktadır.

SSL VPN teknolojisi basit olarak, kullanıcı tarafında herhangi bir VPN yazılımına veya donanımına gerek kalmadan, işletim sistemlerinde standart olarak gelen internet tarayıcıları vasıtası ile kurum ağına güvenli erişim sağlama şeklidir. Çok fazla mobil kullanıcı olan kurumlara her kullanıcıdaki VPN yazılımının sağlıklı çalışmasını sağlamak oldukça zordur. SSLVPN, kolay kurulumu ve yönetimi sayesinde güvenli ve esnek bir bağlantı sağlamaktadır.

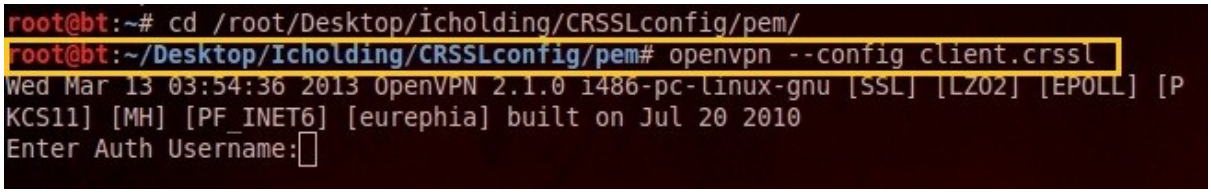
OpenVPN

OpenVPN, endüstri standardı SSL/TLS protokolünü kullanarak 2. veya 3. katmanda VPN oluşturabilen, sertifika, smart card, kullanıcı adı/şifre gibi çeşitli kimlik denetimi metodlarını destekleyen, kullanıcı veya grup bazlı erişim kontrol kuralları uygulayabilen açık kaynak kodlu bir SSL VPN çözümüdür.

OpenVPN kurulum ve yönetiminin kolay olması ve güvenli alt yapı oluşturması yaygın olarak tercih olarak edilmesi sonucunu doğurmuştur. OpenVPN;

- Linux, Windows 2000/XP ve üzeri, OpenBSD, FreeBSD, NetBSD, Mac OS X ve Solaris işletim sistemlerinde çalıştırılabilir.
- OpenSSL kütüphanesinin sunduğu encryption, authentication, ve certification özelliklerini kullanabilir.
- Nat üzerinden sorunsuz tünelleme imkanı
- İsteğe bağlı olarak GUI ile yönetim.
- Kablosuz ağlar için güvenli erişim imkânı sağlanmaktadır.

Şekil 4.4'de BackTrack yazılımı üzerinden OpenVpn kurulumu yapmak için girilmesi gereken komutlar gösterilmiştir.



Şekil 4.4. OpenVpn kurulum komutları

4.5. BackTrack5 İşletim Sistemi

BackTrack, program değildir. Offensive Security Grubu tarafından geliştirilen tamamen özgür olan bir işletim sistemidir. Hacking denilince akla gelen ilk Linux yazılımıdır. Aslında güvenlik uzmanları tarafından ağ ve sistem güvenliğini sağlamak amacıyla kullanılmaktadır.

BackTrack, içinde birçok gelişmiş araç barındıran, sistem ve ağlarda bulunan güvenlik açıklarını test etmek için, diğer bir ifade ile penetrasyon (sızma); hedef sistem ve ağdaki zayıflıkları kullanarak sisteme sızmaya çalışma simülasyonudur [37]. Bu şekilde sistemdeki zayıflıkları raporlanarak tedbir alınması sağlanır. Testlerinde kullanılmak üzere oluşturulmuş, Debian / Ubuntu tabanlı bir Linux dağıtımıdır. Uzmanlarının sıklıkla kullandıkları bir denetim platformudur.

Şekil 4.5. BackTrack arayüzü

Hackerların kullandıkları teknikler kullanılarak hedef sistem ve ağdaki güvenlik zaafiyetleri açığa çıkararak raporlama yapılıp tedbir alınması sağlanır. Dijital dünyadaki gerçek saldırıların aynısını simüle edilerek, bir hackerin yapabileceği tüm saldırı senaryoları uygulanabilir [37].

BackTrack'te bulunan araçların her biri pratik kullanım şekil ve saldırı tekniklerinin uygulanmasındaki başarılarıyla ön plana çıkmaktadır. Zaten üstün özellikleri bulunan bu linux dağıtımının amacı da budur.

BackTrack, literatürde "hack machine" diye geçen içinde bir pentesterin (sistem mühendisinin) ihtiyaç duyabileceği neredeyse bütün yazılımların olduğu bir sistemdir. Bu yazılımların hepsini kullanmak mümkün değildir. Bu uygulamalar temel olarak iki kategoride incelenir.

1-Tarama amaçlı (scan)
2-Saldırı amaçlı (attack)

Bu zamana kadar tüm BackTrack versiyonları milyonlarca kullanıcı tarafından indirilmiştir. Çok da eski olmayan tarihsel sürece baktığımızda, ilk BackTrack dağıtımının 26 Mayıs 2006 tarihinde , BackTrack 1.0 Beta adıyla yayınlandığını görürüz. Daha sonra 6 Mart 2007 (BackTrack 2 Final), 19 Haziran 2008 (BackTrack 3 Final), 9 Ocak 2010 (BackTrack 4), 8 Mayıs 2010 (BackTrack 4 R1), 22 Kasım 2010 (BackTrack 4 R2), 10 Mayıs 2010 (BackTrack 5), 20 Ağustos 2011 (BackTrack 5 R1) ve 1 Mart 2012 (BackTrack 5 R2) şeklinde bir tarihsel süreçle şu anki son haline gelmiştir ve geliştirilmesine devam edilmektedir [37].

4.5.1. BackTrack test metodojisi

Backtrack 5, bünyesinde barındırdığı yüzlerce pentest aracı ile güvenlik profesyonelleri için çok önemli bir platformdur. Bu araçları kullanmak için de bir metot belirlenmeli ve bu metota göre düzenli bir çalışma sağlanmaktadır. Şimdide bu metotları inceleyelim.

1. Hedef Belirleme: İlk olarak bir hedefin olması gerekir. Bilgisayar korsanları da işe ilk olarak hedef belirleyerek başlarlar.

2. Bilgi Toplama: Hedef sistem hakkında bilgi toplanmalıdır. Güvenlik uzmanı, kamuya açık kaynaklardan hedef hakkında genel bilgiler toplar. Bu kaynaklar; internet kaynakları, forumlar, sosyal paylaşım siteleri şeklinde sıralanabilir. BackTrack5'te tüm bu kaynaklardan bilgi toplamak için araçlar bulunmaktadır.

3. Keşif: Hedef sistem hakkında toplanan bilgilerden yararlanarak keşif yapılır. Hedef sistemin ağ yapısı, kullanılan güncel teknolojiler, aktif sistemler ve kullanılan işletim sistemleri gibi bilgiler elde edilir.

4. Hedef Hakkında Elde Edilen Bilgilerin Kategorilenmesi: Bu aşamaya kadar elde edilen bilgileri kullanılarak sistemli bir gruplama işlemi yapılır.

5. Zayıflıkların Haritalanması: Bu aşamada hedef sistemde bulunan açıklık ve zayıflıklar tespit edilerek bir şablon oluşturulur.

6. Sosyal Mühendislik: Sosyal mühendislik, insanların güven duygusunu sömürerek istenilen bilgilere ulaşma metodudur. Sistemlerde bulunan en önemli zayıflık, insan psikolojisinin yönlendirilmesiyle oluşur. BackTrak5 işletim sisteminde sosyal mühendislik saldırılarında kullanılan birçok araç bulunmaktadır.

7. Hedefin Exploit Edilmesi: Keşfettiğimiz açıkları analiz ettikten sonra, bu açıkları kullanarak sisteme yetkisiz erişim sağlamaya çalışabiliriz. Bu aşama saldırının en tehlikeli aşamasıdır. BackTrack5'te gelişmiş exploit araçları bulunmaktadır.

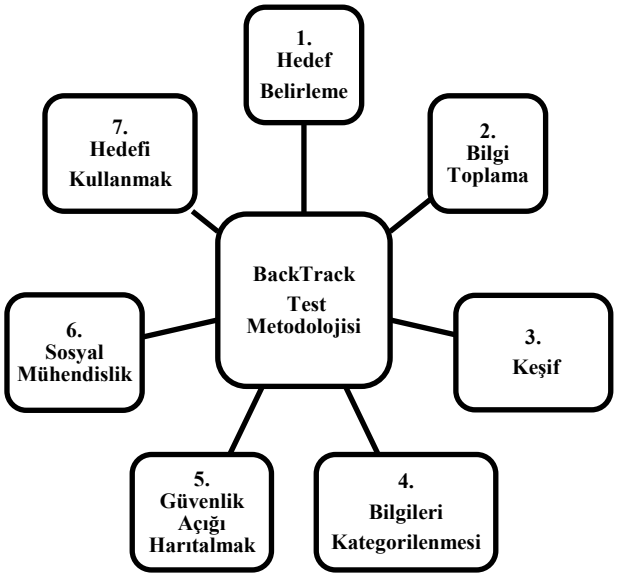
8. Yetki Yükseltme: Sisteme erişimi sağladık fakat normal kullanıcı (user) haklarına sahibiz. Ama biz yönetici haklarına sahip olup sistemde tam anlamıyla etkin olmak ve istediğimiz değişiklikleri yapmak istiyoruz.

Windows sistemlerde Administrator, Linux sistemlerde ise Root en yetkili kullanıcıdır. BackTrack5'te bunun için çeşitli metotlar bulunmaktadır.

9. Erişimi Devam Ettirme: Bu aşamada yapılması gereken şey sisteme istediğimiz zaman girip çıkabileceğimiz ve uzun süre kendimizi ele vermeden kullanabileceğimiz bir yol bulmak.

10. İzleri Temizleme: Sistemde güvenliğe yardımcı olması ve yanlış kullanımların raporlanabilmesi için loglama (kayıt altına alma) mekanizması çalışmaktadır. Bir hacker sisteme kaçak giriş yaptığı zaman sistemde yaptığı eylemler loglanmaktadır. Hacker, yasal suçlamalara maruz kalmamak ve sisteme erişimini uzun süre devam ettirebilmek için bu log dosyalarını silmeye çalışacaktır.

11. Dokümantasyon ve Raporlama: Güvenlik testlerini yaptığınız sistem / kurumdaki idari ve teknik ekip, penetrasyon yöntemi ve bulunan zayıflık ve açıklıkları incelemek isteyecektir. Çünkü güvenlik boşluklarını görüp buna uygun tedbirler alacaktır. Bunun için de test süreci ve sistem zayıflıkları, güvenlik zafiyetleri ayrıntılı olarak belgelendirilmeli ve raporlanmalıdır.



Şekil 4.6. BackTrack test metodolojileri

4.6. Geliştirilen Yazılım

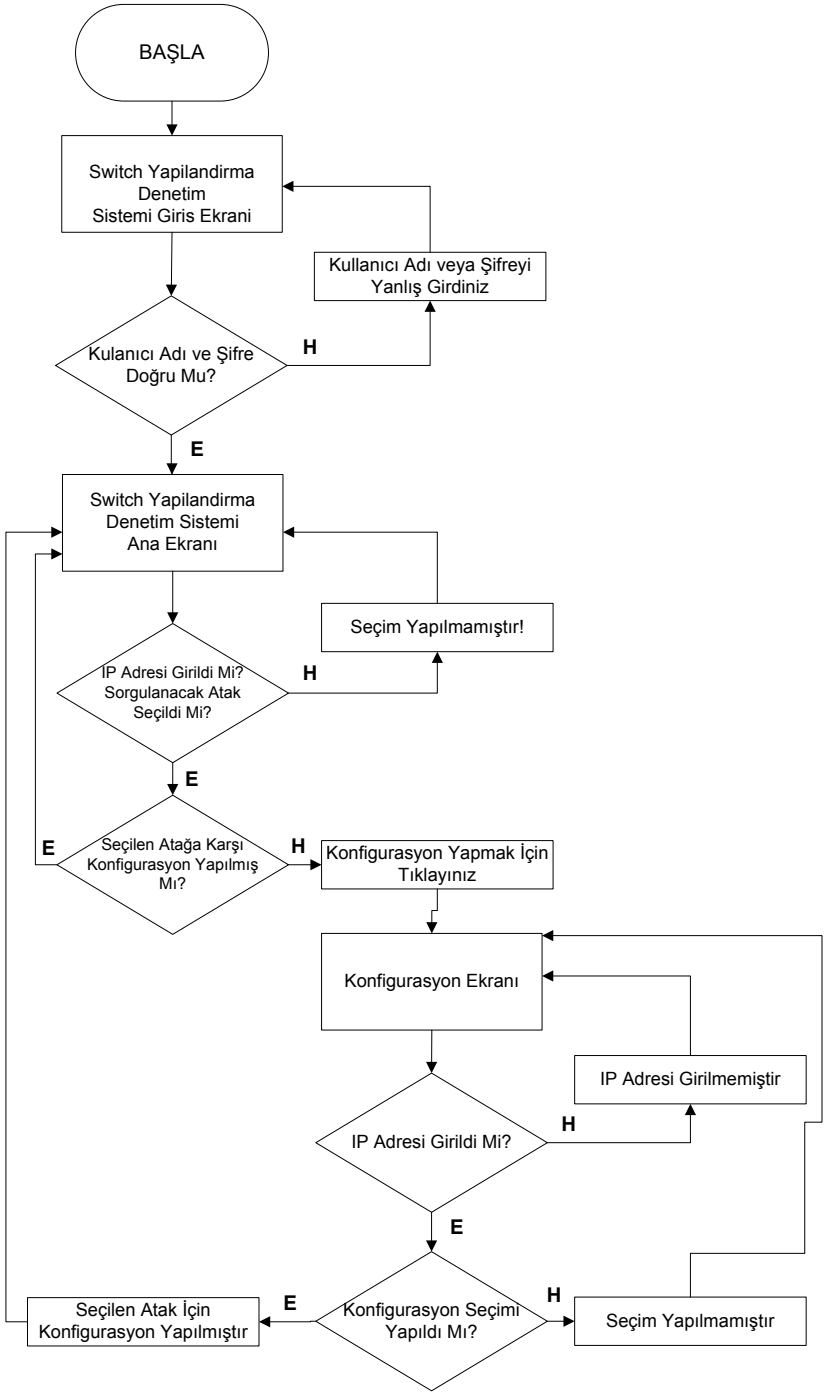
Ağ güvenliğinin sağlanabilmesinin en etkili yolu ağ ortamına dışarıdan veya içerinden gelebilecek saldırıları bilmek ve olası saldırılara maruz kalmadan gerekli önlemleri almaktan geçmektedir. Ağ güvenliğinin öneminin farkında olan birçok kurum; fiziksel güvenlik cihazlarının yanında saldırı tespit sistemleri veya engelleme sistemlerini de kullanmaya başlamıştır.

Ağ saldırıları denince öncelikle dışarıdan yapılan saldırılar akla gelmektedir. Ancak içeriden (yerel ağ ortamından) gerçekleştirilen saldırılar da dışarıdan yapılan saldırılar kadar etkili olabilmektedir. Yerel alan ağı (LAN) saldırıları ağ içerisinden yapıldığı için güvenlik duvarı ya da saldırı engelleme/tespit etme sistemleri tarafından engellenememektedir.

Bu tezde, kurumsal ağlarda kullanılan kenar switchler üzerindeki konfigürasyonların eksikliklerini bulmayı amaçlayan bir yazılım geliştirilmiştir. Geliştirilen yazılım HP Procurve marka tüm switch modelleri için kullanılabilir. Yerel alan ağlarında kullanılan switchler üzerinde bir takım yapılandırmalar mevcuttur. Bu yapılandırmalar sayesinde kurumda planlanan ağ mimarisi gerçekleştirilebilir. Yerel alan ağların kendi içerisinden gelen saldırıların önlenebilmesi switchler üzerinde yapılacak olan konfigürasyonlar ile sağlanabilir. Fakat bu konfigürasyonlar genelde yapılandırılmamaktadır. Çünkü bu konfigürasyonların yapılması oldukça karmaşık, zaman alıcı ve hata yapma olasılığının yüksek olduğu bir iştir. Bu konfigürasyonların teknik bilgisi olmayan kişiler tarafından bile yapılmasını mümkün kılabilmek için bir yazılım geliştirilmiştir. Geliştirilen yazılım ile tek bir bilgisayar ile onlarca kurumsal ağın switchleri üzerindeki güvenlik yapılandırmaları kontrol edilebilir. Eğer konfigürasyon eksiği var ise uzaktan birkaç adımda gerekli konfigürasyonlar yapılandırılabilir.

4.6.1. Switch Yapılandırma Denetim Sistemi Yazılımı

Yazılım, PHP ve Bash Script dilleri kullanarak geliştirilmiştir. Sunulan yazılım web üzerinden görsel olarak yönetilmektedir. Yazılımda kullanılan akış şeması Şekil 4.6.1'de gösterilmiştir.



Şekil 4.6.1. Switch Yapılandırma Denetim Sistemi Akış Şeması

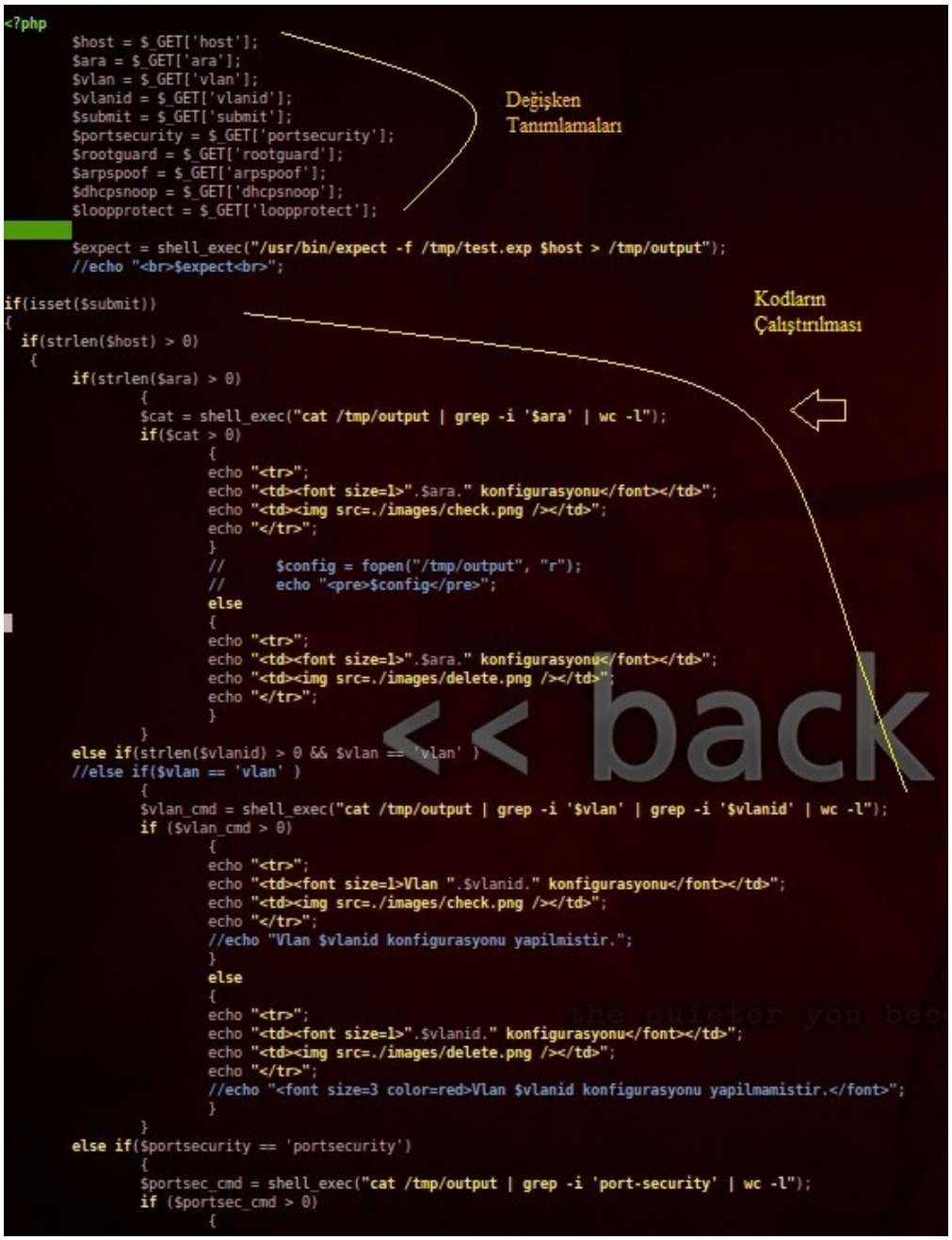
Şekil 4.6.1'de geliştirilen yazılımın güvenli şekilde kullanabilmesini sağlayan bağlantı sayfası gösterilmiştir. Kullanıcı ilgili alanları doldurarak yazılım ana ekranına yönlendirilir.

Şekil 4.6.2. Kullanıcı adı ve şifresi giriş ekranı

Yazılıma giriş yapıldıktan sonra, kontrol edilecek güvenlik yapılandırmalarının bulunduğu ana sayfa ekranı gözükecektir. Şekil 4.6.3'de yazılımın ana ekranı gösterilmiştir.

Şekil 4.6.3. Yazılımın ana ekranı

IP Adresi kısmına güvenlik konfigürasyonu incelenecek olan switchin ip adresi yazılmalıdır. Daha sonra, kontrol edilmek istenen yerel alan ağı güvenlik yapılandırmalarından istenilenler işaretlenecektir. Bu çalışmada yerel alan ağı içerisinde en çok gerçekleşen 5 atak türüne karşı yapılandırma ayarlarının kontrolüne yer verilmiştir. (Şekil 4.6.5)



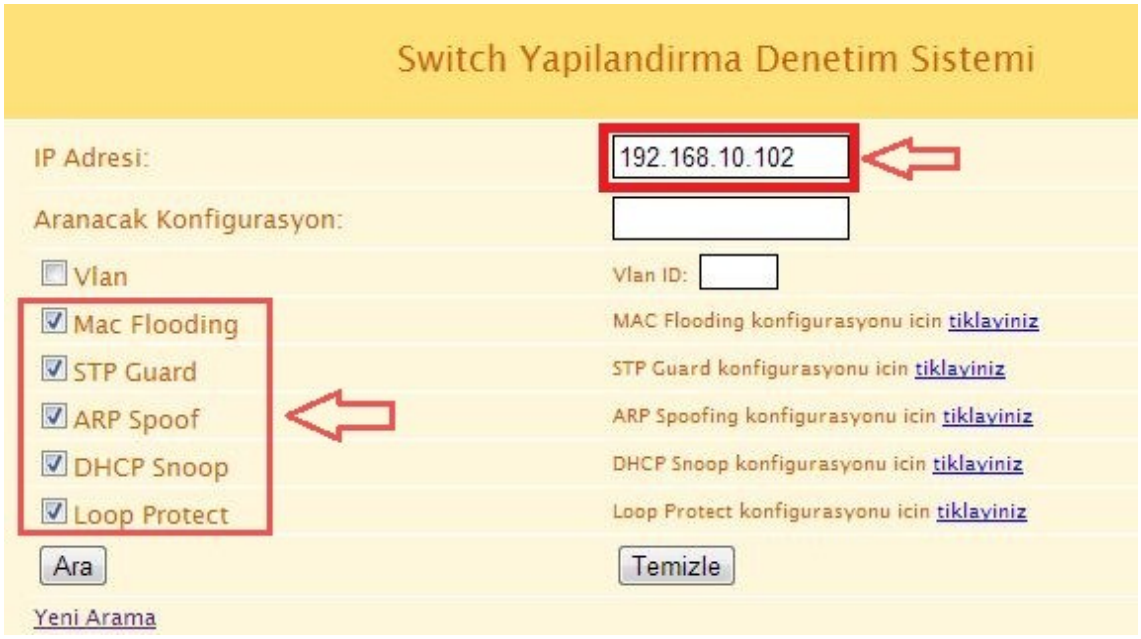

```php
<?php
        $host = $_GET['host'];
        $ara = $_GET['ara'];
        $vlan = $_GET['vlan'];
        $vlanid = $_GET['vlanid'];
        $submit = $_GET['submit'];
        $portsecurity = $_GET['portsecurity'];
        $rootguard = $_GET['rootguard'];
        $arpspoof = $_GET['arpspoof'];
        $dhcpsnoop = $_GET['dhcpsnoop'];
        $loopprotect = $_GET['loopprotect'];

        $expect = shell_exec("/usr/bin/expect -f /tmp/test.exp $host > /tmp/output");
        //echo "<br>$expect<br>";

if(isset($submit))
{
  if(strlen($host) > 0)
   {
        if(strlen($ara) > 0)
                {
                $cat = shell_exec("cat /tmp/output | grep -i '$ara' | wc -l");
                if($cat > 0)
                        {
                        echo "<tr>";
                        echo "<td><font size=1>".$ara." konfigurasyonu</font></td>";
                        echo "<td><img src=./images/check.png /></td>";
                        echo "</tr>";
                        }
                        //      $config = fopen("/tmp/output", "r");
                        //      echo "<pre>$config</pre>";
                        else
                        {
                        echo "<tr>";
                        echo "<td><font size=1>".$ara." konfigurasyonu</font></td>";
                        echo "<td><img src=./images/delete.png /></td>";
                        echo "</tr>";
                        }
                }
        else if(strlen($vlanid) > 0 && $vlan == 'vlan' )
        //else if($vlan == 'vlan' )
                {
                $vlan_cmd = shell_exec("cat /tmp/output | grep -i '$vlan' | grep -i '$vlanid' | wc -l");
                if ($vlan_cmd > 0)
                        {
                        echo "<tr>";
                        echo "<td><font size=1>Vlan ".$vlanid." konfigurasyonu</font></td>";
                        echo "<td><img src=./images/check.png /></td>";
                        echo "</tr>";
                        //echo "Vlan $vlanid konfigurasyonu yapilmistir.";
                        }
                        else
                        {
                        echo "<tr>";
                        echo "<td><font size=1>".$vlanid." konfigurasyonu</font></td>";
                        echo "<td><img src=./images/delete.png /></td>";
                        echo "</tr>";
                        //echo "<font size=3 color=red>Vlan $vlanid konfigurasyonu yapilmamistir.</font>";
                        }
                }
        else if($portsecurity == 'portsecurity')
                {
                $portsec_cmd = shell_exec("cat /tmp/output | grep -i 'port-security' | wc -l");
                if ($portsec_cmd > 0)
                        {
```

Şekil 4.6.4. Yazılım Ana Ekran Kaynak Kodları

Şekil 4.6.5'de ana ekranın girdileri yapılmış hali gözükmektedir.



Şekil 4.6.5. Ana ekran üzerindeki girdilerin belirlenmesi

Ana ekran üzerindeki ilgili alanlar eksiksiz bir şekilde girildikten sonra "Ara" butonuna tıklanarak program çalışmasına başlanır.

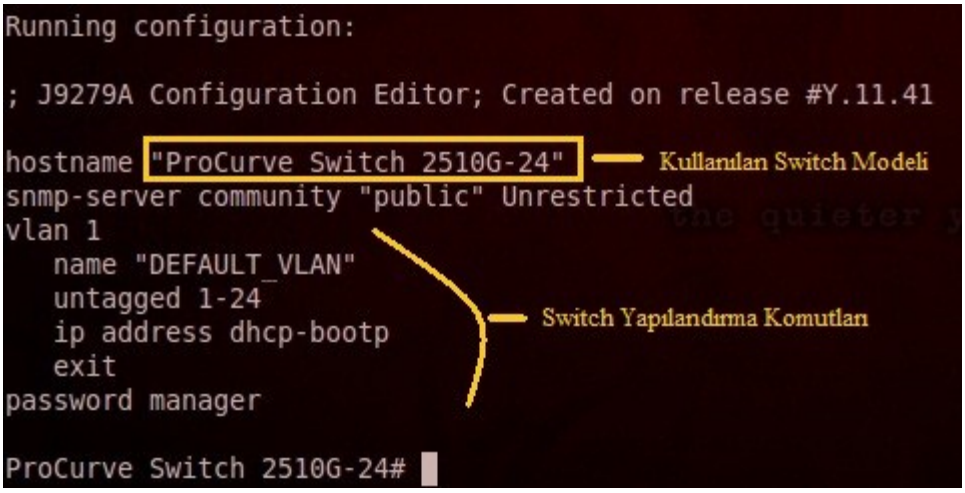
Aşağıdaki linux betik kodlarında switchlere bağlanma işlemini sağlayan kod parçası verilmiştir.

```
#!/usr/bin/expect
#set timeout 20
# set passw [lrange $argv 0 0 ]
set ip_addr [lrange $argv 0 0]
# set scriptname [lrange $argv 2 2]
# set arg1 [lrange $argv 3 3]
# set timeout -1
#log_user 0
# set env(TERM) vt100
spawn telnet $ip_addr
expect "continue"
```

```
send "\r"
expect "Username:"
send "**********\r"
expect "Password:"
send "**********\r"
#expect "*#"
#send " ter len 0\r"
expect "#"
send "show run\r"
#sleep 5
#expect "*#"
#send "ex\r"
#expect "1>"
# sleep 5
#send "ex\r"
#expect "*\?"
#send "*y\r"
#sleep 5
#send "\033"
expect eof
#interact
#exit
```

Switch üzerindeki konfigürasyon yazılım tarafından incelendikten sonra, Mac Flooding konfigürasyonunun yapılandırılmadığı ya da eksik yapılandırılması sonucu çalışmadığı tespit edilmiştir.

Şekil 4.6.6'da switch yapılandırma komutları gösterilmiştir. Yapılandırma komutlarından da anlaşılacağı gibi komutlar arasında Mac Flooding atağına yönelik herhangi bir düzenleme yoktur.



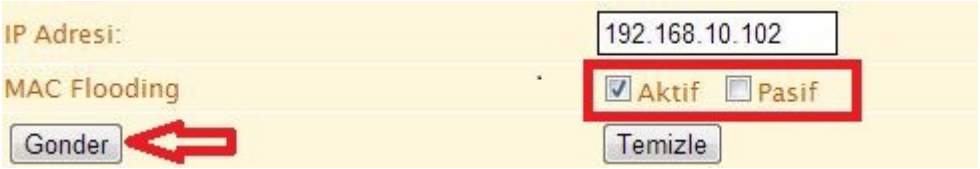
Şekil 4.6.6. ProCurve switch yapılandırma komutları

Bunu bir uyarı şeklinde ekrana getirmiştir.(Şekil 4.6.7) Eğer istenirse konfigürasyon yapmak için tıklanılması istenilen yere tıklanarak gerekli olan tüm düzenlemelerin sunulan yazılım ile yapılması sağlanabilir. Şekil 4.4.7'de kontrol sonrası güvenlik yapılandırma eksiklerinin bulunması gösterilmiştir.

Şekil 4.6.7. Kontrol sonrası güvenlik yapılandırma eksiklerinin bulunması

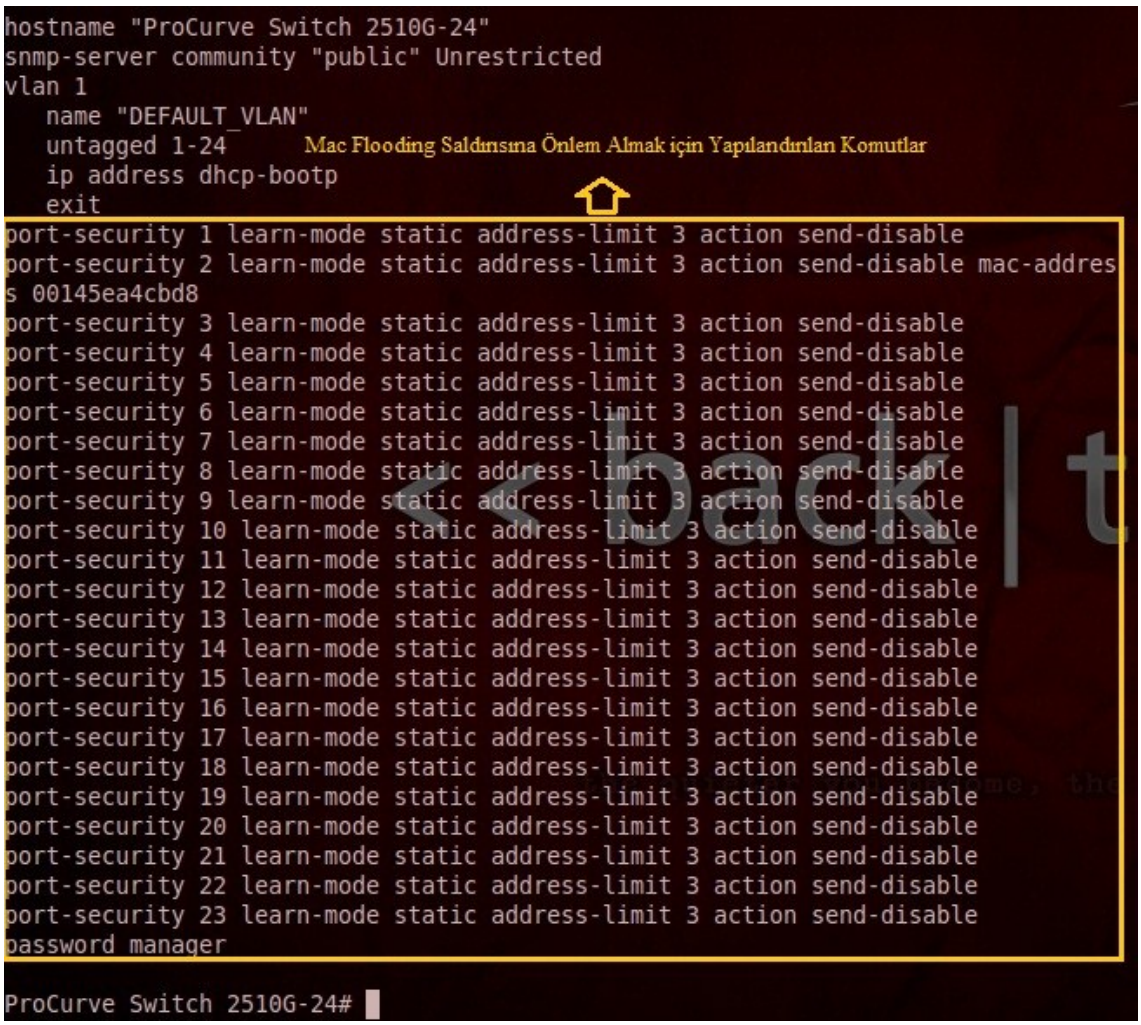
Konfigürasyon yaptırmak için tıklandıktan sonra, gelen ekrana tekrar yapılandırılması istenilen switchin ip adresi girilerek ve "Aktif" kutusu işaretlenerek

gerekli olan konfigürasyonun yapılması sağlanır. Şekil 5.8'de bu durumun yapılmasını sağlayan arayüz gösterilmiştir.



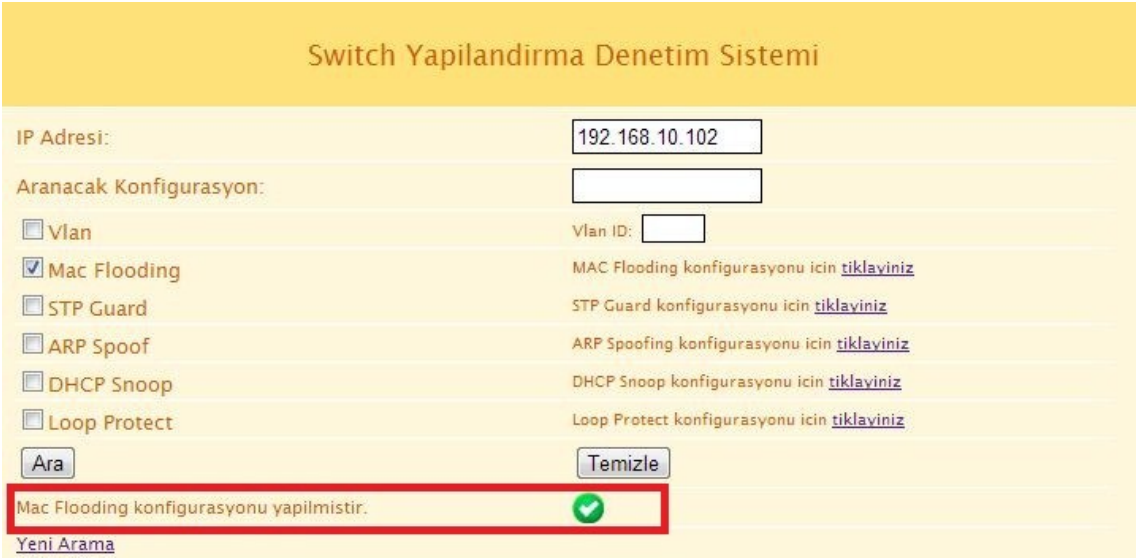
Şekil 4.6.8. Konfigürasyonun yapılmasını sağlayan arayüz

"Gonder" butonuna tıklandıktan sonra yazılım aracılığı ile "Mac Flooding" atağına önlem almak için gerekli kodlar Şekil 4.6.9'da gösterildiği gibi switch yapılandırma komutları arasına eklenmiştir.



Şekil 4.6.9. Mac Flooding yapılandırılması yapılmış switch yapılandırma komutları

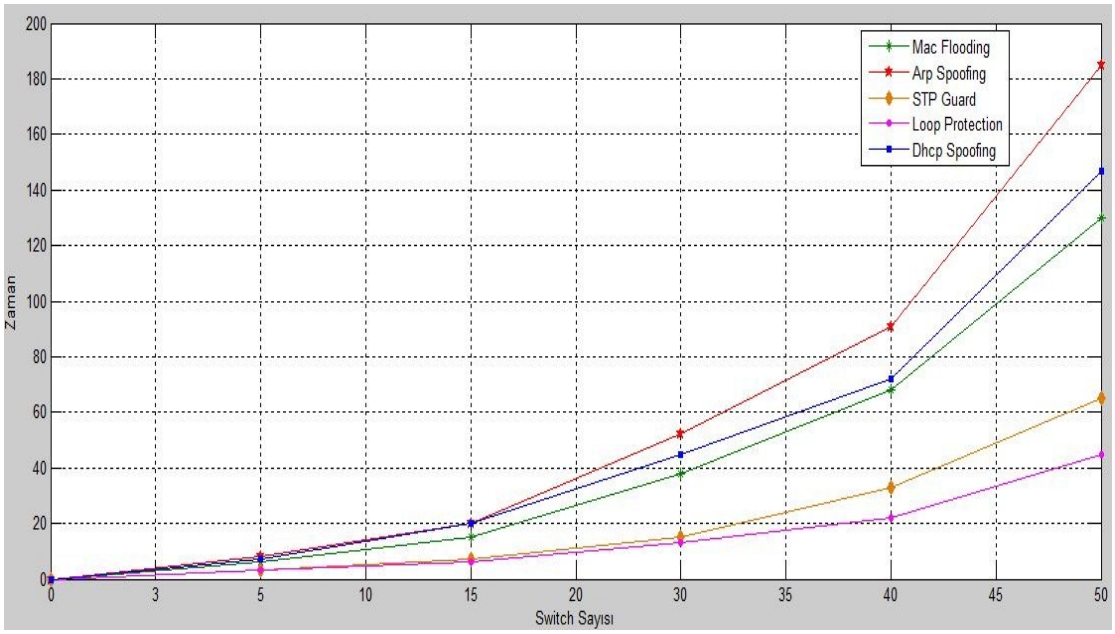
Bu sayede, yapılandırılması zor, zaman alıcı ve teknik bilgi gerektiren işlemler, çok daha kolay, kısa sürede ve teknik bilgi birikimi olmadan yapılması mümkün hale gelmiştir. Şekil 4.6.10'da gerekli konfigürasyonun yazılım tarafından yapılması sonrası, tekrar "Mac Flooding" konfigürasyon eksiğinin ve çalışır olma durumunun tespiti için kontrol ettirilmesi sonucu elde edilen ekran görüntüsü verilmiştir.



Şekil 4.6.10. Konfigürasyon sonrası tekrar kontrol edilme işlemi

Geliştirilen yazılım aracılığı ile farklı büyüklükteki ağ ortamlarına kullanılan HP ProCurve marka kenar switchler üzerinde yapılandırma ayarları yapılmıştır. Uygulama 3, 5 ve 10 switch kullanımının olduğu ağlara uygulanarak, farklı switch sayıları için tahmini hesaplamalar yapılarak oluşturulmuştur. Uygulamada kullanılan bütün switchler aynı özelliklere sahip olup varsayılan konfigürasyon ayarlarına sahiptirler.

5 farklı yerel ağ saldırısına (Mac Flooding, STP Guard, ARP Spoof, DHCP Snoop, Loop Protect) karşı yapılan yapılandırma ayarları sonucunda Şekil 4.6.11'deki grafik elde edilmiştir.



Şekil 4.6.11. Gerçekleştirilen yerel ağ saldırılarının switchlere bulaşma sürelerinin karşılaştırılması

Şekil 4.6.11'de gösterilen grafikte X ekseni, ağ ortamında kullanılan switch sayısını ifade ederken Y ekseni yapılandırma ayarları sonucunda geçen süreyi dakika cinsinden ifade etmektedir.

Şekil 4.6.11'de gösterilen grafikten alınan bilgilere göre;

- Ağda kullanılan switch sayısı arttıkça 5 yerel ağ saldırısı için de switch yapılandırma süresi artmaktadır.

- Her atağın yapılandırma süresi farklı olmakla birlikte; en uzun yapılandırma süresine "Arp Spoofing" atağı sahip olduğu görülürken, en kısa yapılandırma süresine "Loop Protect" atağının sahip olduğu görülmüştür. Bu farklılığın en büyük nedeninin atakların konfigürasyon komutlarından kaynaklanmakta olduğu tahmini yapılabilir.

Yapılan uygulama ile yerel ağlarda kullanılan HP ProCurve marka kenar switchler üzerinde yapılandırma ayarlarının kontrolü yapılmıştır. Bu kontroller sayesinde, kenar switchler, belirlenen 5 saldırıya (Mac Flooding, STP Guard, ARP Snoof, DHCP Snoop, Loop Protect) karşı denenmiştir. Yapılmayan güvenlik yapılandırma ayarlamalarından kaynaklanan ağ savunmasızlıkları ortaya konulmuştur. Tespit edilen ağ savunmasızlıkları kısa sürede giderilerek güvenli bir yerel ağ ortamı sağlanmıştır.

5. SONUÇ VE ÖNERİLER

İnternetin hayatın her alanına girmesiyle birlikte elektronik ortamlarda verilen hizmetlerin (e-ticaret, e- kurum, e-devlet, e-ödeme, e-öğrenme, vb) sayısı da her geçen gün artmakta, bu ortamların kullanımı ise yaygınlaşmaktadır. Elektronik ortamda verilen hizmetlerin sayısının artmasıyla birlikte, saldırganlar için bu hizmetin verildiği sistemler cazibe merkezi haline gelmektedir. İçerisinde önemli bilgiler (kurumsal ve kişisel) barındıran bilgi sistemlerinin güvenliğinin sağlanması ve yönetimi önem kazanmıştır.

Kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Bundan dolayı kurumlar ağ ve bilgi güvenliğini sağlamak için; ateş duvarları, anti-virüs yazılımları, saldırı tespit ve önleme sistemleri gibi çözümler üretmişlerdir. Ancak kullanılan çözümlerin birçoğu dışardan gelecek saldırılara yönelik olmuştur. Yerel ağ içerisinden gelen saldırılar göz ardı edilmiştir.

Yerel ağ içerisinden gerçekleştirilen saldırılar son yıllarda artış göstermiştir. Bunun en önemli nedeni, geliştirilen yazılımlarla bilgi düzeyi ne olursa olsun artık herkesin saldırı yapabilecek konuma gelmiş olmasıdır. Yapılan araştırmalar sonucu içerden yapılan saldırıların verdiği zararın boyutunun, dışardan gerçekleştiren saldırılardan daha çok olduğu ortaya çıkmıştır.

Veriler bir ortamdan diğer ortama aktarılırken her an çalınma, değişime uğrama ya da yok edilme tehlikesi ile karşı karşıyadır. Veri paketleri network cihazları vasıtasıyla ağ üzerinden aktarılırken, kötü amaçlı kişiler bu cihazları ve bilgisayarları paket koklama ya da aldatma işlemleri yaparak bilgileri ele geçirmektedirler.

Bu çalışmada yerel ağ saldırıları konusunda ayrıntılı bir inceleme yapılmıştır. Yerel ağlarda en fazla kullanılan 5 saldırı türü (Mac Flooding, STP Guard, ARP Spoof, DHCP Snoop, Loop Protect) belirlenmiştir. Bu saldırılara karşı önlem alabilecek bir yazılım geliştirilmiştir.

Geliştirilen yazılım ile HP ProCurve kenar switchler üzerinde, belirlenen 5 saldırı türüne karşı yapılandırma sorgusu yapılabilmektedir. Bu saldırılara karşı switch yapılandırma ayarları gerçekleştirilerek ağ savunmasızlıkları ortadan kaldırılmaktadır.

Switch Yapılandırma Denetim Sistemi ile;

Uzak bilgisayar ağlarındaki switch ataklara karşı localhostta çalıştırılan uygulama ile korunur. Merkezi olarak switch konfigürasyonu denetlenir, açık varsa anında giderilebilir. Teknik bilgisi olmayan birisi bile kolayca konfigürasyon kontrolü yapabilir. Güvenli bağlantı ortamı kullanılarak (SSL VPN) ağ savunmasızlıkları giderilir.

Ağ saldırıları gün geçtikçe artmakta, yapılan saldırılarda buna paralel olarak çeşitlenmektedir. Geliştirilen yazılım ile 5 saldırı türüne karşı savunmasızlık testi yapılmaktadır. Çeşitlenen saldırılarla birlikte saldırı türleri değişecektir. Bu yüzden yazılımın yeni saldırı türlerine göre güncellenmesi gerekecektir. Uygulama, ağ ortamında yaygın olarak kullanılan HP ProCurve marka switchler üzerinde çalışmaktadır. Farklı ağ ortamlarında, farklı switchler için bu uygulamanın geliştirilerek kullanılması gerekmektedir.

Bruce Schneier'in de belirttiği gibi "Güvenlik bir ürün değil, bir süreçtir." Ağ ve bilgi güvenliğinin sağlanması için bütün güvenlik çözümlerinin bir arada kullanılması gerekmektedir.

Yerel alan ağlarını saldırılardan korumak için geliştirilen ateş duvarları, anti-virüs yazılımları, saldırı tespit ve önleme sistemleri dışardan gelecek saldırılar içindir, iç tehditler için sağladıkları önlemler sınırlıdır. Sistem yöneticileri ve ağ güvenlik sorumluları da iç tehditleri yeteri kadar bilmemekte ve önem vermemektedir. Dış tehditlere verilen önem kadar içten gelecek saldırılar için de sistemler ve yazılımlar geliştirilmeli, bu konuya daha fazla önem verilmelidir.

KAYNAKLAR

1. Deal, Richard A. Cisco router firewall security. Cisco Systems, 2004.
2. Cappelli, Dawn, et al. "Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition–Version 3,1." CERT, January (2009).
3. Frank L. Greitzer, Andrew P. Moore and Down M. Cappelli, Dee H. Andrews, Lynn A. Carroll, Thomas D. Hull, Comabating the Internal Cyberthreat, IEEE, Security and Privacy 2008, January/Ferbuary
4. İnternet: ” 2011 CyberSecurity Watch Survey” http://www.sei.cmu.edu/newsitems/cybersecurity_watch_survey_2011.cfm (07.03.2013)
5. Maple, Carsten, Helen Jacobs, and Matthew Reeve. "Choosing the right wireless LAN security protocol for the home and business user." Availability, Reliability and Security, 2006. ARES 2006. ***The First International Conference on. IEEE***, 2006.
6. Groth, D., Toby, S., “Network+ Study Guide, Fourth Edition”, ***Neil Edde & Sybex, Inc.***, Alameda, 4, (2005).
7. Clancy, T. C., & Goergen, N. (2008, May). Security in cognitive radio networks: Threats and mitigation. In ***Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*** (pp. 1-8). IEEE.
8. Lehtinen, R., “Computer Security Basics, 2nd Edition” , ***O'Reilly***, Sebastopol, 302, (2006).
9. Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Klavuzu, **Sürüm 0.1, ULAKCSIRT**-2008-01

10. Strebe, M., Perkins, C., "Firewalls 24Seven, Second Edition" ***Neil Edde & Sybex Inc.***, Alameda, 7, (2002).

11. Can, E., "Gerçek zamanlı veriler yardımı ile karar veren bir bilgisayar ağı saldırı tespit sisteminin tasarlanması ve gerçeklenmesi", Yüksek Lisans Tezi, ***Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 4-5 (2007).

12. Abraham, A., Grosan, C., "Evolving Intrusion Detection Systems", Genetic Systems Programming Theory and Experiences, ***Springer***, Netherlands, 59, (2006).

13. Yıldız, E., "Veri Madenciliği Teknikleriyle Saldırı Tespiti ve Bir Uygulama", Yüksek Lisans Tezi, ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, 15-16 (2007).

14. Vural, Y., "Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri", Yüksek Lisans Tezi, ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, 36-37 (2007).

15. Gürkas, G. Z., Durukan, S., Zaim, A. H., Demir, A., Aydın, M. A., "802.11b Kablosuz Ağlarda Güvenligin Ag Trafigi Üzerindeki Etkilerinin Analizi", ***II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi***, İstanbul, 10-11, (2005).

16. Wi-Fi Alliance, "Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise", ***Wi-Fi Alliance March 2005***, Austin, 7-8, (2005).

17. Edney, J., Arbaugh, W. A., "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", ***Addison Wesley***, Boston, 12-13, (2003).

18. Karaarslan E., "Web Saldırı Sistemlerinin Etkinleştirilmesi için Sistem Farkındalığı ve Çok Katmanlı Güvenlik Önlemlerinin Gerçekleştirilmesi", Doktora Tezi, ***Ege Üniversitesi Fen Bilimleri Enstitüsü***, İzmir,120-121 (2008).

19. Karaarslan, E., Akın, G., & Demir, H.," Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Yöntemleri", ***Akademik Bilişim 2008***, Çanakkale, 232-237, (2008).

20. Soysal M. , Bektaş O., HoneyWall Kurulumu, http://csirt.ulakbim.gov.tr/dokumanlar/HoneyWall.pdf, (07.02.2013)

21. Ranum M., System Logging and Log Analysis, http://www.ranum.com/security/computer_security/archives/logging-notes.pdf, (12.01.2013)

22. Akın G. , Güneş A., "Bir Wormun Anatomisi, ***Akademik Bilişim 2007***, 681-685, (2007)

23. İnternet: "ArpWatch", http://blog.csirt.ulakbim.gov.tr/?p=54 (2013).

24. Wagner R., "Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks", ***SANS Institute***, August 2001

25. Danielle L.," Sniffing", ***SANS Security Essentials (GSEC),*** June 1, 2001

26. Velasco V., "Introduction to IP Spoofing", ***SANS Institute 2000-2002***, 2003

27. Sağıroğlu Ş., Bektaş O., Soysal M., "Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması", ***3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı***, Ankara, 132-138, (2008).

28. Siles R., "Real World ARP Spoofing", August 2003.

29. İnternet: " İkinci Katman Saldırıları", http://www.bilgiguvenligi.gov.tr/aktif-cihaz-guvenligi/ikinci-katman-saldirilari-1-3.html (07.03.2013)

30. İnternet: Wikipedia "VmWare" , http://en.wikipedia.org/wiki/Vmware (2013).

31. Alkan G., "Sanallaştırılmış Ağ Topolojisi Üzerinde Güvenlik Duvarı ve Tehdit Gözetleme Sistemlerinin Otomatize Test Edilmesi", Yüksek Lisans Tezi, ***Sakarya Üniversitesi Fen bilimleri Enstitüsü***, Sakarya, 2009.

32. İnternet: "WMware Sürümleri", http://www.vmware.com (2013).

33. İnternet: Wikipedia, "Bash (Unix shell)", http://en.wikipedia.org/wiki/Bash_(Unix_shell), (2013).

34. Lerdorf, R., Tatroe, K., & MacIntyre, P. ,2nd ed.,"*Programming Php",* ***O'Reilly Media***, Incorporated, 2006.

35. İnternet: Netcraft's Web Server Survey, "PHP just grows & grows" http://news.netcraft.com/archives/2013/01/31/php-just-grows-grows.html 2013.

36. Yüksel Z., "Ağ Güvenliği ve Güvenlik Duvarında VPN ve NAT Uygulamaları", Yüksek Lisans Tezi, ***Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü***, İstanbul, 2007.

37. Ali, S.,. Heriyanto,T., "BackTrack 4: Assuring Security by Penetration Testing", ***Packt Publishing Ltd***, Birmingham, 9-15, 2011

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: TONKAL, Özgür
Uyruğu	: Türkiye
Doğum tarihi ve yeri	: 05.04.1985 ANKARA
Medeni hali	: Evli
Telefon	: 0(505) 501 06 52
e-mail	: ozgrcglr@hotmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Lisans	Gazi Üniversitesi / Bilgisayar Sistemleri Öğretmenliği	2008
Lise	Yılmaz Kayalar Anadolu Lisesi	2004

İş Deneyimi

Yıl	Yer	Görev
2008-2010	Taşova Ş.P.A.Y Mesleki ve Teknik Eğitim Merkezi	Teknik Öğretmen
2010..	Ankara Ulus Teknik ve EML	Teknik Öğretmen

Yabancı Dil

İngilizce

Hobiler

Satranç, Bilgisayar teknolojolileri, Futbol