OSI KATMAN MODELİNDE 3. KATMAN GÜVENLİK DUVARI UYGULAMASI

ONUR BAŞKAYA

YÜKSEK LİSANS TEZİ

ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2010

ANKARA

Onur BAŞKAYA tarafından hazırlanan OSI KATMAN MODELİNDE 3. KATMAN GÜVENLİK DUVARI UYGULAMASI adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç.Dr.Erkan AFACAN .....
Tez Danışmanı, Elektrik-Elektronik Müh. AD

Bu çalışma, jürimiz tarafından oy birliği ile Elektrik-Elektronik Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Doç.Dr.Atilla YILMAZ .....
Elektrik-Elektronik Müh. AD, Hacettepe Üniversitesi

Doç.Dr.Erkan AFACAN .....
Elektrik-Elektronik Müh. AD, Gazi Üniversitesi

Doç.Dr.Erkan AFACAN .....
Elektrik-Elektronik Müh. AD, Gazi Üniversitesi

Tarih : 18/05/2010

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onamıştır.

Prof.Dr.Bilal TOKLU .....
Fen Bilimleri Enstitüsü Müdürü

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.

Onur BAŞKAYA

OSI KATMAN MODELİNDE 3. KATMAN GÜVENLİK DUVARI UYGULAMASI

(Yüksek Lisans Tezi)

Onur BAŞKAYA

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MAYIS 2010

ÖZET

Bilgisayar ağları günümüzde hemen her yerde yaygın olarak kullanılmaktadır. Bu nedenle ağ üzerinden paylaşılan bilginin güvenliğinin sağlanması büyük önem kazanmıştır. Bilgi hırsızlığı ve kötüye kullanım gün geçtikçe artmaktadır. Bilgi güvenliğinin sağlanması ihtiyacı yeni teknolojilerin ve yeni sektörlerin ortaya çıkmasına yol açmıştır. Bu teknolojilerin en önemli ürünlerinden bir tanesi ağ seviyesinde güvenlik sağlayan güvenlik duvarıdır.

Bu çalışmada C programlama dili ve Linux çekirdeğinin bir parçası olan 'Netfilter' kullanılarak bir güvenlik duvarı uygulaması tasarlanmıştır. Güvenlik duvarı uygulamasında genel fonksiyonlar, içerik filtreleme, paket filtreleme, NAT ve loglama kısımları mevcuttur. ICMP yankı istek bombardımanı ve SYN bombardımanı atakları başarıyla engellenmiştir. Ayrıca NAT yapma işlemi de sınanmış ve başarıya ulaştığı görülmüştür.

Bilim Kodu : 9051.014
Anahtar Kelimeler : Güvenlik Duvarı, IP Tabloları
Sayfa Adedi : 42
Tez Yöneticisi : Doç.Dr. Erkan AFACAN

THIRD LAYER FIREWALL APPLICATION IN OSI LAYER ARCHITECTURE (M.Sc.Thesis)

Onur BAŞKAYA

GAZİ UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY
May 2010

ABSTRACT

Computer networks are widely used almost everywhere in our day. For this reason it has become very important to maintain the security of the shared information over networks. Information theft and abuse have been increasing day by day. The need for the maintenance of the information security has led to new technologies and new sectors. One of the most important products of these new technologies is the firewall which provides network level security.

In this work, a firewall application has been designed by using C programming language and 'Netfilter' which is a part of Linux kernel. In the application developed, general functions, content filtering, packet filtering, NAT and logging are included. ICMP echo request bombardment and SYN bombardment attacks are successfully prevented. Also, NAT operation is tested and it is shown that it has been successful.

Science Code : 9051.014
Key Words : Firewalls, IP Tables
Page Number : 42
Adviser : Assoc. Prof.Dr. Erkan AFACAN

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren Hocam Doç. Dr. Erkan AFACAN' a yine tecrübelerinden faydalandığım arkadaşım Adem BÜYÜKÖZER'e, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli arkadaşlarıma ve aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

ÖZET……. …iv
ABSTRACT…… v
TEŞEKKÜR…… …. ….vi
İÇİNDEKİLER…… vii
ÇİZELGELERİN LİSTESİ… ix
ŞEKİLLERİN LİSTESİ……..... x
SİMGELER VE KISALTMALAR…… xi
1. GİRİŞ 1
2. OSI (OPEN SYSTEM INTERCONNECTION) REFERANS MODELİ.....7
2.1. OSI Referans Modeli Mimarisi Katmanları.....7
2.2. OSI Referans Modeli Mimarisi.....8
2.3. İnternet Ulaşım Katmanı Protokolleri.....12
2.3.1. TCP protokolü.....12
2.3.2. TCP bölütünün yapısı 14
3. BİLGİSAYAR AĞLARINDA GÜVENLİK ZAAFİYETLERİ VE TEDBİRLERİ 16
3.1. Yetki Aşımları 17
3.2. Uygulamaya Yönelik Saldırılar 17
3.3. İşletim Sistemi ya da Uygulama Seviyesinde Kullanılan İstismarlar ...18
3.4. Virüs ve Benzeri Yazılımlar 18
3.5. Ağ Saldırıları.....19
3.5.1. Port tarama teknikleri.....19
3.5.2. TCP protokolü.....22
3.5.3. DoS saldırı çeşitleri.....25
3.6. DoS Saldırılarına Karşı Alınabilecek Önlemler 34
4. GÜVENLİK DUVARLARI 35
4.1. Güvenlik Duvarı Tipleri 36
4.1.1. Yazılım tabanlı güvenlik duvarları.....37
4.1.2. Donanım tabanlı güvenlik duvarları 38
4.2. Güvenlik Duvarlarının Özellikleri 38
4.2.1.Yazılım tabanlı güvenlik duvarlarının özellikleri 38
4.2.2.Donanım tabanlı güvenlik duvarlarının özellikleri 42

Sayfa

5. IPTABLES GÜVENLİK DUVARI 44
5.1. Birkaç Iptables Örneği 46
5.2. GTK+ Kütüphanesi ve Oluşturulan Güvenlik Duvarı.....47
5.2.1.GTK+ kütüphanesi.....47
*5.2.2.*Oluşturulan güvenlik duvarının anlatımı 47
5.3. Çalışma Testi 50
5.3.1.Deney Düzeneği.....50
5.3.2.Yazılan Güvenlik Duvarının DoS Saldırı Türlerine Verdiği Tepki51
5.3.3.Yazılan Güvenlik Duvarının Sınanması 56
5.4. Değerlendirme.....62
6. SONUÇ 64
KAYNAKLAR 68
EKLER 70
EK-1 Güvenlik Duvarı Yazılımı Kodları…….. 71
ÖZGEÇMİŞ.....83

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 4.1. Noktadan Noktaya Ağ Bağlantısı .....…...41
Çizelge 4.2. Sunucu – İstemci Ağ Bağlantısı ……..41

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 1.1. Noktadan Noktaya Ağ Bağlantısı 5
Şekil 1.2. Sunucu – İstemci Ağ Bağlantısı 6
Şekil 2.1. OSI 7 Katmanlı Başvuru Modeli ve Katmanlar 9
Şekil 2.2. OSI' de Uygulama ve Ağ Ara Bağlaşım Hizmetleri Seviyeleri 10
Şekil 3.1. Şirinleme Saldırısı 27
Şekil 3.2. SYN Bombardıman Saldırısı 32
Şekil 5.1. Oluşturulan Güvenlik Duvarı 48
Şekil 5.2. Deney Düzeneği..... .51
Şekil 5.3. Başarılı Ping Yankısı… 57
Şekil 5.4. Başarısız Ping Yankısı 58
Şekil 5.5. Başarılı SYN Bombardıman Saldırısı.....59
Şekil 5.6. Başarısız SYN Bombardıman Saldırısı.....60
Şekil 5.7. SNAT Öncesi Paketler..... 61
Şekil 5.8. SNAT Sonrası Paketler.....62

SİMGELER VE KISALTMALAR

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

Kısaltmalar	Açıklama
ASCII	American Standard Code for Information Interchange (Kodlar Arası Değişim İçin Amerikan Standardı)
ATM	Asynchronous Transfer Mode (Asenkron Transfer Modu)
DMZ	Demilitarized Zone (Arındırılmış Bölge)
DoS	Denial of Service (Hizmeti Engelleme Saldırısı)
DSL	Digital Subscriber Line (Sayısal Abone Hattı)
EBCDIC	Extended Binary Coded Decimal Interchange Code (Genişletilmiş İkilik Kod Onluk Kod Değişimi)
FDDI	Fiber Distributed Data Interface (Fiber Dağıtık Veri Arayüzü)
FSF	Free Software Foundation (Ücretsiz Yazılım Kurumu)
GLIB	Graphic Library (Grafik Kütüphanesi)
GPL	General Public Licence (Genel Kamusal Lisans)
GTK+	GNU Image Manipulation Program Toolkit (Çok Platformlu Grafiksel Kullanıcı Arayüzü Geliştirme Aracı)
HTML	Hyper Text Markup Language (Zengin Metin İşaret Dili)
ICMP	Internet Control Message Protocol (İnternet Kontrol Mesaj Protokolü)
IP	Internet Protocol (İnternet Protokolü)

Kısaltmalar	Açıklama
ISDN	Integrated Services Digital Network (Bütünleştirilmiş Sayısal Ağ Hizmetleri)
LAN	Local Area Network (Yerel Alan Ağı)
MAN	Metropolitan Area Network (Kampüs Alan Ağı)
MTU	Maximum Transmission Unit (Maksimum İletim Birimi)
NAT	Network Address Translation (Ağ Adres Aktarımı)
OSI	Open System İnterconnection (Açık Sistemler Bağlantısı)
OWASP	Open Web Application Security Project (Açık Ağ Uygulama Güvenlik Projesi)
PRI	Primary Rate Interface (Birincil Tarife Arayüzü)
QoS	Quality of Service (Bağlantı Servis Kalitesi)
SQL	Structured Query Language (Yapısal Sorgulama Dili)
TCP	Transport Control Protocol (İletim Kontrol Protokolü)
UDP	User Datagram Protocol (Kullanıcı Veri Bloğu Protokolü)
URL	Uniform Resource Locator (Tekdüzen Kaynak Bulucu)
VPN	Virtual Private Network (Özel Sanal Ağ)
WAN	Wide Area Network (Geniş Alan Ağı)
WWW	World Wide Web (Dünya Çapında Ağ)

1. GİRİŞ

Günümüzde bilgisayarlar tek başına bir sistem olmak yerine sistemin bir parçası olarak hizmet vermektedir. Böylece çalışma ortamlarında daha az maliyetle daha fazla performans ihtiyacı karşılanmış olur. Bilgisayar ağlarının oluşturulmasının temelinde maliyeti yüksek cihazların ortak kullanımı, çağımızın en büyük gereksinimi olan bilgiye hızlı erişim ve paylaşımı gösterilebilir. Bu paylaşıma örnek olarak, küçük bir ofiste ortak bir projede aynı doküman üzerinde çalışan bir ekip olabileceği gibi internet ortamında sanal bir ticarethanenin işletmecisinin ihtiyacı da gösterilebilir.

Bir bilgisayar ağının genel olarak ölçeği LAN (Yerel Alan Ağı), MAN (Kampüs Alan Ağı), WAN (Geniş Alan Ağı) ve Uzak Bağlantılar olmak üzere dörde ayrılabilir. Her birinin kendisine özgü teknolojileri, standartları vardır ve oluşturulmak istenen ağa göre bu standartlar ve teknolojiler göz önüne alınarak bir çözüm oluşturulur.

LAN: Bu ağın temel özelliği, sistemlerin aynı ortamda veya birbirine yakın mesafede olmalarıdır. Bu nedenle sistemler arasında kullanılacak kabloların seçiminde büyük esneklik vardır ve kablolama alt yapısı bir kez kurulduktan sonra maliyetsiz bir iletim ortamı sağlar. LAN uygulamalarında yüksek hızlara çıkılabilir. Ethernet (Fast veya Gigabit Ethernet), Jetonlu Halka (Token Ring) ve FDDI (Fiber Dağıtık Veri Arayüzü) uygulamaya bağlı olarak seçilebilecek LAN teknolojileridir. Bir ağda ihtiyaca göre birden fazla teknoloji kullanılabilir.

KAMPÜS AĞI*:* LAN ile benzer özelliklere sahiptir, ancak mesafe daha uzaktır. Dolayısıyla kablo seçiminde LAN uygulamasındaki gibi esneklik yoktur. Burada LAN da kullanılan Ethernet, Jetonlu Halka, FDDI ve ATM (Asenkron Transfer Modu) teknolojilerinin yanında WAN'larda kullanılan E1, PRI (Birincil Tarife Arayüzü) gibi sayısal iletişim hizmetleri kullanılır.

WAN: Birbirine çok uzakta olan kampüs ağları ve LAN'ları birbirine bağlar. Temel özelliği mesafenin çok uzak olması ve buna bağlı olarak altyapı ihtiyacının başka bir firma tarafından karşılanmasıdır. Burada iletişim ortamının bant genişliğinin sınırlı olması ve bant genişliğine göre ücret ödenmesi kullanılacak teknolojinin iyi optimize edilmesini gerekli kılar.

UZAK BAĞLANTI: Tek bir bilgisayarın veya küçük bir ofiste bulunan bilgisayar grubunun merkezi bir yere bağlanmasıdır. WAN'nın bir parçası olarak düşünülebilir. Temel özelliği, birkaç kullanıcının olması ve iletim ortamı olarak büyük bant genişliği gerektirmemesidir. Ancak sistemlerde bağlantı servis kalitesi (QoS) istenebilir. Burada kullanılan teknolojiler, Analog Modem, Frame Relay, X.25, ISDN, xDSL. gibi teknolojilerdir.

Hangi ağ türü olursa olsun bilgisayarların birbiriyle haberleşebilmesi için aynı dilden konuşabiliyor olması ve sadece kendini tanımlayan bir kimliğe ihtiyacı vardır. Anlaşmada ortak bir protokolün kullanımı ve o bilgisayara özel kimlik IP (internet protokol) adresi ile sağlanır. IP adresleri o ülkede sorumlu IP dağıtıcısı tarafından, ilgili servis sağlayıcı ya da firmalara ücret karşılığı tedarik edilir. Fakat bilgisayar sayısı halihazırdaki IP sayısı ile karşılanamayacak duruma gelmektedir. Dolayısıyla alternatif yollara başvurulmaktadır.

Bu bağlamda, Network Address Translation (Ağ adresi çeviricisi) özel ağları genel ağlardan ayırmak için özel ağın IP adresini genel ağın IP adresine çevirmek yoluyla kullanılan ortak metottur. Genellikle özel ağın içindeki birçok kullanıcı için bir tek genel ağ IP adresi mevcuttur. Bu durumda tranfer katmanı port numarası değişir ve bu metot ağ adresi ve port numarası çevirme olarak adlandırılır [1]. Böylece IP adresleri port numaralarına aktarılarak sanal IP adresleri oluşturulur. Ağ adresi çevirme işlemi özel ağların çıkış noktalarındaki ağ geçitlerinde yapılır. Genellikle ağ geçidi olarak da güvenlik duvarları kullanılır.

Güvenlik duvarları genel ağ ile özel ağ arasında IP ve port kısıtlamaları getirerek erişim denetimi yapan cihazlardır. Ticari yazılım ve donanım olabildiği gibi açık kaynak kodla yazılmış güvenlik duvarları da mevcuttur. Bu iki ürün ailesi devamlı rekabet halindedir ve birbirlerine göre avantaj ve dezavantajları mevcuttur.

Bilgisayar Ağlarının Tarihsel Gelişimi

Başlangıçta, işletmelerde sunucu görevini ana bilgisayar (mainframe) adı verilen, o zamanın şartlarına göre yüksek performanslı ama bir o kadar da büyük bilgisayarlar yapıyordu. Bu bilgisayarlar soğutulan ve birçok güvenlik elemanınca kontrol edilen odalarda tutulur, sadece sınırlı sayıda kullanıcının kullanmasına izin verilirdi. Büyük boy bilgisayarlar oldukça pahalı ve kullanışsız olmalarının yanında soğutma ve bakım giderleri oldukça yüksekti. Bu sistemlerin kullanılması için bilgisayar üreticileri, kendi başlarına çalışamayan aptal (dump) terminaller ürettiler. Bu terminaller kendi başlarına çalışmayan ve yalnızca büyük boy bilgisayarlara bağlandıktan sonra, ondan aldığı verilerle çalışabilen cihazlardı. Bu çözüm de her işi sunucuya yüklüyor ve performans düşüklüğüne ve yüksek maliyete neden oluyordu.

İnternetin kökleri 1962'ye, J.C.R. Licklider'in ABD'nin en büyük üniversitelerinden biri olan Massachusetts Institute of Technology'de (MIT) tartışmaya açtığı Galaktik Ağ kavramına kadar uzanır. Licklider bu kavramla, küresel olarak bağlanmış bir bilgisayar ağında, isteyen herkesin herhangi bir yerden veri ve programlara erişebilmesini ifade etmiştir. MIT'de araştırmacı olarak çalışan Lawrance Roberts ile Thomas Merrill, 1965'te bilgisayarların ilk kez birbirleriyle konuşmasını gerçekleştirmiştir. Lawrence G. Roberts 1966'da DARPA'da çalışmaya başlamış ve 1967'de ARPANET isimli projeyi önermiştir. ARPANET çerçevesinde ilk bağlantı 1969'da dört merkezle yapılmış ve ana bilgisayarlar arası bağlantılar olarak internetin ilk şekli ortaya

çıkmıştır. ARPANET' i oluşturan ilk dört merkez Los Angeles' taki California Üniversitesi, Stanford Research Institute, Utah Üniversitesi ve SantaBarbara' daki California Üniversitesi'dir.

Network Control Protocol (NCP), ARPANET' teki ilk standart ağ protokolü olarak kullanılmaya başlanmıştır. Ekim 1971' de ARPANET' teki her bilgisayar bir diğerine NCP ile bağlanabiliyordu. Kısa süre içinde merkezdeki birçok bilgisayar ARPANET ağına bağlanmıştır. 1972'de e-posta adres formatı ile telnet protokolünün dokümanı yayınlanmış ve e-posta ilk defa ARPANET içinde kullanılmaya başlanmıştır. NCP'den daha yeni olanaklar getiren Transmission Control Protocol / Internet Protocol (TCP/IP) adındaki bu yeni protokol, 1 Ocak 1983'te ARPANET içinde kullanılmaya başlanmıştır. TCP/IP bugün var olan internet ağının ana halkası olarak yerini almıştır. İlk internet omurga ağı, 1986'da National Science Foundation (NSFNet) tarafından oluşturulmuştur.

1986'da internet erişimi, teknik bilgisi olmayan kişiler tarafından da kolay kullanılır hale dönüştürülmüştür. İnternet üzerindeki bilgilere, dosyalara ve arşivlere kolay ve hızlı erişimin sağlanabilmesi amacıyla 1989'da European Laboratory for Particle Physics' de (CERN) bir başka çalışma başlatılmıştır. Bu çalışma 1991'de World Wide Web (www) protokolü adı altında kullanılmaya başlanmıştır [2]. Böylece internete erişen herkes sitelerde yayınlanan bilgilere erişebilip istediği kaynaktan yararlanabilmektedir.

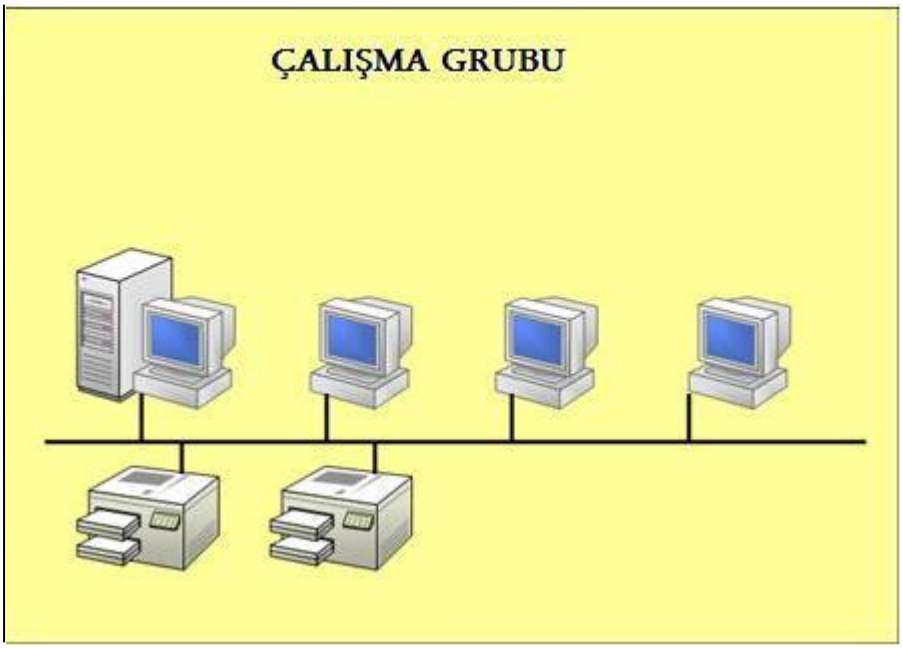
Bilgisayar ağı üzerindeki bilgi iletimi ve paylaşımı bazı kurallar dahilinde yapılmaktadır. Bu kurallara kısaca "İnternet Protokolleri", ya da TCP/IP protokoller ailesi denir. TCP/IP (Transmission Control Protocol / Internet Protocol), bilgisayarlar ile veri iletme / alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır. Bir başka deyişle, TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını koyar.

Ağ Türleri

Bilgisayar ağları, ağ üzerinde bilgisayarların nasıl yapılandırıldığına ve bilgilere nasıl erişildiğine göre ikiye ayrılır:

- Noktadan noktaya ağ
- Sunucu-istemci ağ

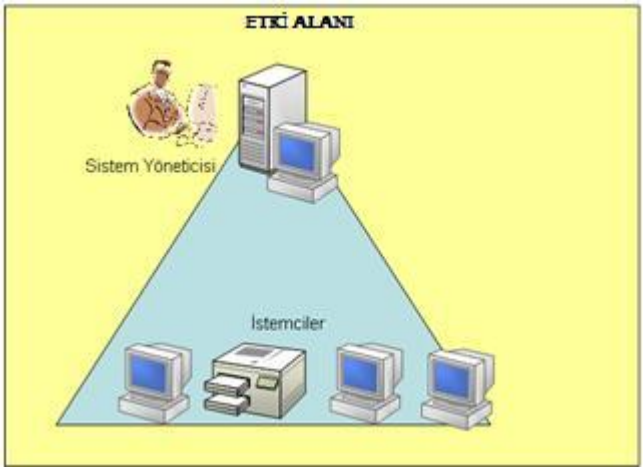
Noktadan noktaya ağlarda, genellikle sınırlı sayıda PC birbirine bağlıdır (Şekil 1.1.). Bu bilgisayarlar düzey olarak aynıdır. Yani içlerinden birinin ana bilgisayar olarak kullanılması söz konusu değildir. Bir bağlantı aracılığıyla isteyen kullanıcılar birbirleriyle iletişim kurar ya da dosya alışverişi yapabilirler.



Şekil 1.1 Noktadan Noktaya Ağ Bağlantısı

Sunucu-istemci ağlarda, bir ana bilgisayar vardır (Şekil 1.2.). Ana makine üzerinde ağ yönetimi yapılır. Ayrıca ağa girecek (login) ya da bağlanacak herkes, bu ana makine üzerinde yer alan kullanıcı hesaplarına göre kontrol edilerek bağlantı gerçekleştirilir. Böylece kullanıcı ve dosya temelinde

güvenlik sağlanmış olur. Bunun dışında kullanıcı girişlerinde, kimlik bilgilerinin kontrolü işlemi yapılmış olur.



Şekil 1.2 Sunucu-İstemci Ağ Bağlantısı

2. OSI (OPEN SYSTEM INTERCONNECTION) REFERANS MODELİ

Veri paketleri bir ağ üzerinde kaynaktan hedefe doğru ilerlerken ağ üzerindeki tüm cihazların aynı dili ya da protokolü konuşması çok önemlidir. Kısaca protokol, ağ üzerindeki iletişimi daha etkin kılmayı sağlayan bir kurallar kümesidir. Bunu sürücülerin uyması gereken trafik kuralları ya da pilotların uçak kullanırken diğer pilotlarla ve kontrol kulesi ile görüşürken uyduğu özel kurallara benzetmek mümkündür.

Teknik bir tanım yapmak gerekirse protokol; verinin biçimini ve iletişim şeklini belirleyen bir kurallar kümesi veya bir anlaşmadır. Bir bilgisayardaki n katmanı diğer bilgisayardaki n katmanıyla konuşur. Bu iletişimde kullanılan tüm kuralların tamamına n katmanı protokolü adı verilir.

Ağ modelleri, fonksiyonları sadeleştirmek ve anlaşılır kılmak amacıyla katmanlar kullanır. OSI referans modeli ağ iletişimi için en temel modeldir. Başka bir deyişle OSI referans modeli bilginin ağ üzerinde nasıl taşındığını anlamamızı sağlayacak bir iskelettir.

OSI'nin genel yapısı, katmanları ve katmanların fonksiyonları aşağıdaki başlıklar altında ele alınmıştır:

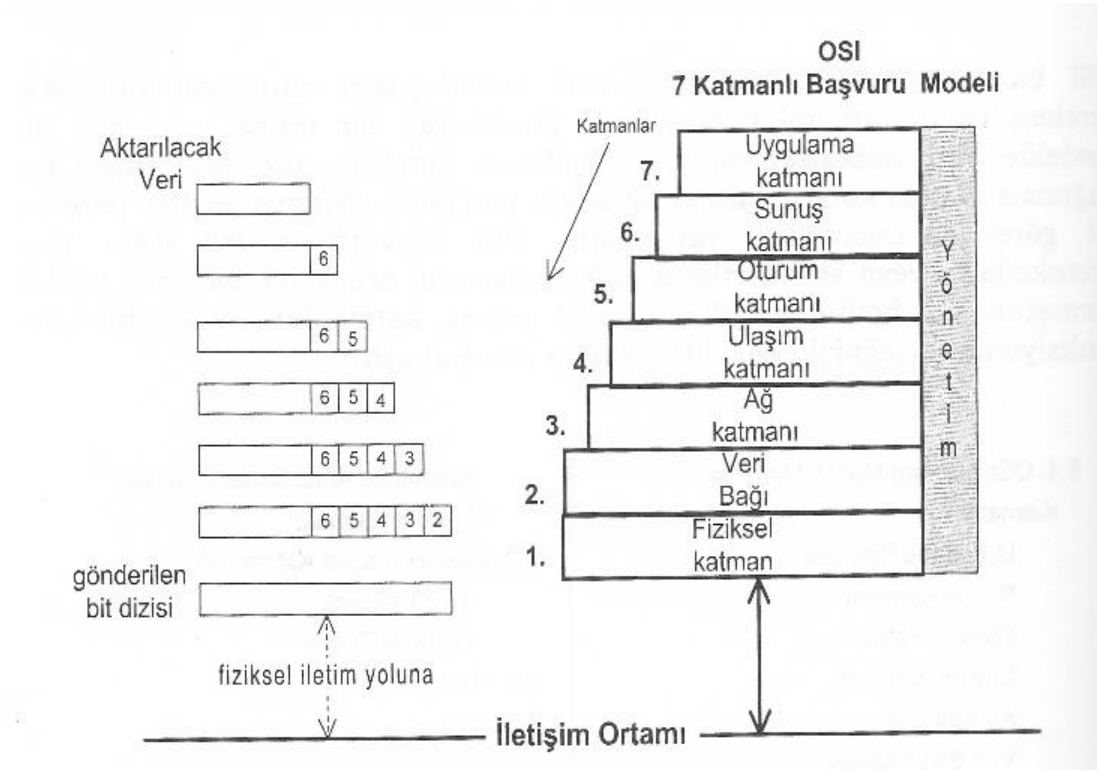
2.1. OSI Referans Modeli Mimarisi Katmanları

- Uygulama Katmanı
- Sunuş Katmanı
- Oturum Katmanı
- Ulaşım Katmanı
- Ağ Katmanı
- Veri Bağ Katmanı
- Fiziksel Katman

OSI standardı ISO tarafından 1979 yılında yayınlandı. Genel yapısı bir düğümün iletişim sürecini çok katmanlı bir yapı şeklinde tanımlamaktır. OSI Modelinde bir uç düğümünde, her biri farklı işleve sahip 7 katman tanımlıdır. Uç bilgisayarlarda 7 katmanın tamamı bulunurken, bilgisayar ağında yer alan ara düğüm cihazlarda daha az sayıda katman bulunabilmektedir. Örneğin ağ içerisinde kullanılan ara cihazlardan tekrarlayıcı (repeater) yalnızca 1. katmana, köprü (bridge) ve anahtar (switch) cihazları 1. ve 2. katmanlara ve yönlendirici (router) cihazı ise, ilk üç katmana ait işlevlere sahiptirler. Sanki, ağ üzerinde bir uç bilgisayar gibi tüm 7 katmanı da içeren geçit yolu (gateway) veya protokol dönüştürücü (protocol converter) de bir ağ cihazıdır.

2.2. OSI Referans Modeli Mimarisi

OSI referans modelinde tam bir hiyerarşik yapı vardır. Hiyerarşinin en üstünde kullanıcıların koşturduğu uygulama programları ve en altta ise verinin bit düzeyinde aktarılması vardır. Ara katmanlar bu iki katman arasında gerekli uyarlamaları içerir. Her katman bir üst katmana hizmet sunarken, bir alt katmandan kendisi için hizmet ister. Aşağıda Şekil - 2.1’ de katmanların sıralanması ve aktarılacak verinin yukarıdan aşağıya ilerlerken genişlemesi görülmektedir.



Şekil 2.1 OSI 7 Katmanlı Başvuru Modeli ve Katmanlar

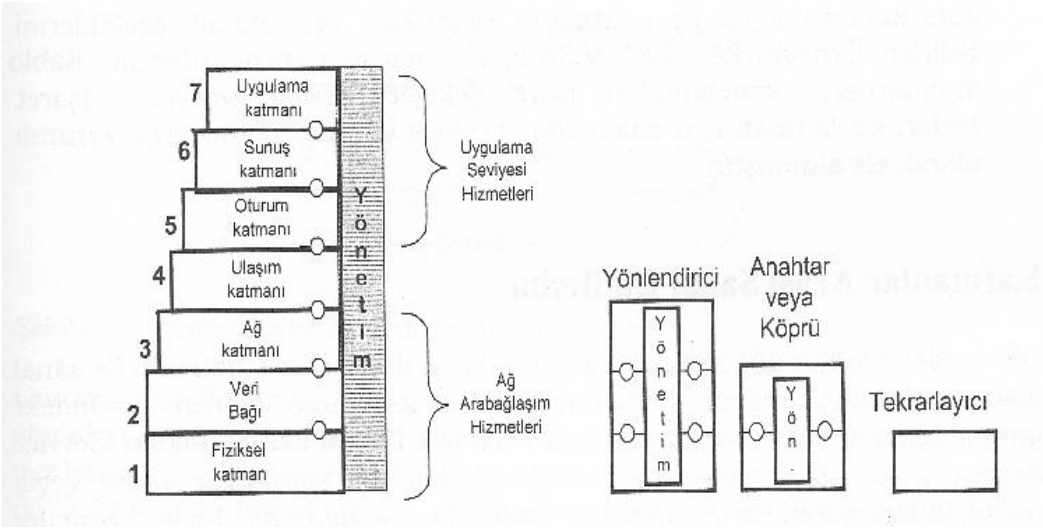
7. Uygulama Katmanı (Application Layer) **:** Uygulama programlarının ağa erişimi için gerekli işlevleri kapsar; kullanıcının etkileşimde bulunduğu uygulama programları doğrudan bu katmanla iletişim içindedir. Bu katman için dosya aktarımı, elektronik mektuplaşma, uzaktan dosya erişimi, ağ yönetimi, terminal protokolleri gibi standartlar geliştirilmiştir.

6. Sunuş Katmanı (Presentation Layer) ***:*** Bilginin iletimde kullanılacak biçiminin düzenlenmesini sağlar: Sıkıştırma/ açma, şifreleme/ şifre çözme, EBCDIC-ASCII dönüşümü ve ters dönüşümü gibi işlevlerin yerine getirilmesini kapsar.

5. Oturum Katmanı (Session Layer) ***:*** Uç düğümler arasında gerekli oturumun kurulması, yönetilmesi ve sonlandırılması işlerini kapsar. İletişimin mantıksal sürekliliğinin sağlanması için, iletişimin kopması durumunda bir senkronizasyon noktasından başlayarak iletimin kaldığı yerden devam

etmesini sağlar. Gönderilecek bilgi “senkronizasyon noktaları” ile sınırları belirlenmiş bloklara ayrılır. Karşı ucun oturum katmanı bir bloğun tamamını doğru olarak elde edip üst katmanına teslim ettikten sonra blokla ilgili işi tamamlamış olduğunu, veriyi gönderen tarafa bildirir. Gönderen taraf ise bloğu belleğinden silebilir. İletişim koparsa son senkronizasyon noktasından başlayarak bilgi gönderilir.

4. Ulaşım Katmanı (Transport Layer) **:** Bilginin son alıcıda her türlü hatadan arındırılmış olarak elde edilebilmesini sağlar. Ulaşım katmanının oluşturduğu bilgi bloklarına bölüm (bölüt) denir. Bunlar son alıcıya sırası bozulmuş olarak gelirse, düzgün olarak sıralanmalıdır. Bunun için bölümler numaralanır.



Şekil 2.2 OSI’de Uygulama ve Ağ Ara Bağlaşım Hizmetleri Seviyeleri

OSI referans modelinin ilk üç katmanı ve 4 katmanın bir kısım özellikleri ağ ara bağlaşım cihazlarında kullanılan işleri yerine getirirler (Şekil – 2.2.). Yukarıdan üç katman ise uygulama programları düzeyinde hizmetleri sunan işlevlere sahiptirler.

3. Ağ Katmanı (Network Layer) **:** Veri paketlerinin bir uçtan diğer uca ağdaki çeşitli düğümler (yönlendirici, geçit yolu vs.) üzerinden geçirilip yönlendirilerek alıcısına ulaşmasını sağlayan işlevlere sahiptir. Veri paketinin alıcısına giderken ağ koşullarına, önceliklere ve diğer parametrelere göre hangi yolun uygun olacağı bu katmanda değerlendirilir. Bu amaçla düğümlere ağ adresi denilen numaralar verilir. Ağ adresi taşıyan bilgi bloklarına paket adı verilir. İnternet' in temel protokol kümesi olan TCP/IP'nin IP protokolü bu katmanda yürütülen bir protokoldür.

2. Veri Katmanı (Data Link Layer) **:** Gönderilecek bilginin hatalara bağışık bir yapıda mantıksal işaretlere dönüştürülmesi, alıcıda hataların sezilmesi, düzeltilemiyorsa doğrusunun elde edilmesi için göndericinin uyarılması gibi işlevleri vardır. Gönderilen / alınan mantıksal işaret bloklarına çerçeve (frame) denir. Çerçevelerin içerdiği bit sayısının alt ve üst sınırları standartlarla belirlenmiştir ve genellikle değişken uzunluktadırlar (HDLC, SDLC...).

1. Fiziksel Katman (Physical Layer) **:** Verinin fiziksel olarak hat üzerinden aktarılması için gerekli işlevleri kapsar. Veri, bu katman için sıradan bit dizisi olarak algılanır; bitlerin taşıdığı anlam bu katmanda yorumlanmaz. Bu katman için tanımlanan standartlar taşıyıcı işaretin şekli, verici ve alıcı konumdaki uç noktaların elektriksel ve mekanik özelliklerini belirler. Örneğin RS-232C, V.35 fiziksel katman standartlarıdır. Kablo standartları, tanımlamaları, işaret şekilleri, gerilim seviyeleri, işaret hızları bu katman için anlamlıdır [3].

OSI referans modelinde, veri paketleri en alttan başlayarak uygulama katmanına kadar çıkar. Veri iletişiminde bulunan iki taraf arasında her katman kendi arasında eşleşir ve paket içeriğinin algılanması ve değerlendirilmesi bu şekilde olur. İletişimin güvenilirliği ulaşım katmanının sorumluluğundadır.

Ulaşım katmanı uç sistemler arasında güvenilir bir iletişim kanalı kurulmasını sağlar. Bu katmanda iki adet protokol mevcuttur. İlki TCP (Transport Control Protocol) diğeri ise UDP (User Datagram Protocol)' dir. TCP ile UDP arasındaki en önemli fark TCP ile yollanan paketlerin gidip gitmediğinin kontrol edilmesi ve veri alışverişinde bulunan cihazlar arasında bir bağlantının oluşturulmasıdır. UDP protokolünün kullanımında ise bir bağlantı oluşturulmaz ve paketlerin gidip gitmediği kontrol edilmez. Bu protokol genelde verinin hızlı iletilmesinin verinin kaybına göre daha önemli durum arz etmesi gereken durumlarda tercih edilir.

2.3. İnternet Ulaşım Katmanı Protokolleri

2.3.1. TCP protokolü

TCP bağlantılı (connection-oriented) ve güvenilir (reliable) bir protokoldür. Bağlantılı bir protokol olduğundan iki bilgisayar hemen iletişime geçmez. Önce aralarında bir oturum açarlar, birbirlerine bu oturum için kendi parametrelerini gönderirler (hand shaking). Eğer şartlar uygunsa iletişime başlarlar. Tıpkı telefon görüşmesinde "alo" demeden konuşmaya başlamamamız gibi.

Güvenilir olduğu için de gönderilen verinin akıbetinden endişe etmeye gerek yoktur. Çünkü TCP bir takım hata sezme ve düzeltme mekanizmalarıyla verinin kaybolmasına izin vermez.

TCP bir üst katmandan gelen veriyi transfere uygun hale gelebilmesi için belli uzunlukta bölütlere böler. Bu bölütlerin alıcı tarafta doğru sırayla alınması için her bölüte bir sıra numarası verir. Böylece veri transferi sırasında kaybolan, yerine ulaşmayan ya da yanlış sırayla alınan paketler sorun oluşturmaz. Ayrıca karşı taraftaki alıcı bilgisayar, aldığı paketler için "tamam, veriyi tam olarak aldım" anlamında "acknowledged" (ACK) paketi göndermek

zorundadır. Verinin gönderici bilgisayardakiyle aynı olup olmadığı, bir tür algoritmayla hesaplanır. Algoritma sonuçları her iki tarafta da aynıysa veri bozulmadan gönderilmiş demektir. Paketi gönderen bilgisayar, ACK paketini belli bir süre içinde almazsa, ilgili paketi yeniden gönderir.

Veri akışının kontrolü “kayan pencereler” (sliding windows) denilen bir mekanizmayla sağlanır. Veriyi gönderen bilgisayar, gönderdiği her bölüt için karşı taraftan bir ACK biti beklemez. Belli sayıda bölütü topluca göndererek, gönderdiği bu sayı için bir onay bekler. Belli sayıdaki bu bölüt topluluğuna pencere (window) denir. Alıcı taraftaki bilgisayarın TCP katmanı, gönderici bilgisayarın TCP katmanına “benim pencere büyüklüğüm bu kadar, fazlasını gönderme” anlamında bir bilgi gönderir. Pencere büyüklüğü, bilgisayarın bir defa da alabileceği veri miktarını gösterir. Gönderici bilgisayar bu veri miktarı kadar veri göndermek zorundadır, fazla gönderirse alıcı tarafta dikkate alınmaz. İletişim sırasında pencere boyutu karşılıklı anlaşmayla değişebildiğinden, bu olaya “kayan pencereler” adı verilir.

Bir bilgisayarın TCP üzerinden aynı anda birden fazla işlemi kullanabilmesi portlar yardımıyla sağlanır. Hem TCP, hem de UDP portları kullanır. Port numaraları 0 ile 65,536 arasında değişir. Mesela ftp 21. portu kullanırken, telnet 23 nolu portu kullanır. 0 ile 1024 arasındaki portlar bilinen portlar (well-known ports) olarak bilinir. Bu portların listesi RFC 1700’ de verilmiştir. Port numarasıyla birlikte IP adresine “soket numarası” denilir. TCP bağlantılar bu soketler üzerinden sağlanır. Bir uygulama kendi başına bir soket oluşturarak, karşı taraftaki bir uygulamanın soketine bağlanabilir. Windows NT/2000 ya da UNIX işletim sistemlerinin hangi portları kullandığını “netstat” komutuyla görebiliriz. Komut promptunda “netstat – na” yazarak veri gönderen ya da dinleme durumunda olan portlarımızı görebiliriz. Burada –a parametresi tüm (all) portları gösterirken, -n parametresi nümerik (numerical) formatta gösterir.

2.3.2. TCP bölütünün yapısı

TCP üzerinden gerçekleştirilen saldırıların nasıl yapıldığının anlaşılması için, TCP bölütünün yapısı iyi bilinmelidir. Çünkü bilgisayar korsanlarının (hacker) kullandığı tekniklerin ve programların pek çoğu, TCP bölütünün yapısına ve bunlardaki güvenlik açıklarına dayanarak yapılmıştır.

TCP daha önce de belirtilen görevleri yerine getirebilmek için, ulaşım katmanında parçalara ayırdığı verinin önüne başlık bilgisini ekler. Başlık bilgisiyle birlikte veriye "TCP bölütü" denir.

TCP bölütünün genel yapısı şöyledir:

Gönderen Port (Source Port): Veriyi gönderen bilgisayarın kullandığı TCP portudur.

Alıcı Port (Destination Port): Alıcı bilgisayarın TCP portudur.

Sıra Numarası (Sequence Number): TCP'nin böldüğü veri parçacıkları olan bölütlere verdiği sıra numarasıdır.

Onay Numarası (Acknowledgement Number): Bir sonraki seferde alınması umulan TCP paketinin bir sonraki 8 bitlik alanı.

Başlık Uzunluğu (Header Length): TCP başlığının uzunluğunu gösterir.

Rezerve Edilmiş (Reserved): İleride kullanılmak üzere saklı tutulmuştur.

Kod Bitleri ya da Bayraklar (Code Bits or Flags): Bölütle ilgili kontrol bilgilerini taşır. Toplam 8 bayrak vardır ama bunların 6 tanesi yoğun olarak kullanılır. SYN bayrağı TCP bağlantısı kurulurken karşı tarafa ben hazırım bilgisini

yollayan veridir. ACK bayrağı yollanan her verinin alındığı teyidini karşı tarafa bildiren veridir. URG bayrağı verinin içeriğinde acil bilgi olduğunu gösterir. RST bayrağı pakette sorun olduğunu veya bağlantının koparılacağını gösterir. FIN bayrağı, bağlantının veri yollayan tarafının daha fazla verisinin olmadığını, bağlantıyı koparabileceğini belirtir. PSH bayrağı verinin TCP katmanı tarafından hemen yollanmasını tetikler [4].

Pencere (Window): Akış denetimi için kullanılır.

Hata Sınama Bitleri (Checksum): Bölütün hatalı ulaşıp ulaşmadığını kontrol etmek için kullanılır.

Acil İşaretçisi (Urgent Pointer): Acil olarak bir verinin iletilmek istendiği durumlarda kullanılır.

Opsiyon (Option): Şu an bir tane tanımlanmıştır: Maksimum TCP bölüt boyutu.

Veri (Data): Üst katman protokollerinin verisi [5].

3. BİLGİSAYAR AĞLARINDA GÜVENLİK ZAAFİYETLERİ VE TEDBİRLERİ

1990'lı yıllarda yaşanan hızlı teknolojik gelişmelerin sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Hayatımızın birçok alanında bilgisayar ve bilgisayar ağı teknolojileri "olmazsa olmaz" bir şekilde yer almaktadır. İletişim, para transferleri, kamu hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan sadece birkaçıdır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir. Bilgisayarların her alanda kullanılır hale gelmesi bilgisayar ağları ve yazılım konusunda uzmanların ve bu özelliklerini kötüye kullanan insanların artışına da sebep olmuştur.

Bu güvenlik ihlalleri kendi içinde yetki aşımları, uygulamaya yönelik saldırılar çapraz taraflı betik (Cross Site Scripting), yapısal sorgulama dili enjeksiyonu (SQL injection), işletim sistemi ya da uygulama seviyesinde kullanılan istismarlar (exploit), virüs ve benzeri yazılımlar, ağ saldırıları şeklinde sınıflandırılabilir.

Bu güvenlik açıklarından ağ katmanı seviyesinde en çok kullanılan atak türlerinden biri DDoS (Distributed Denial of Service) ataklarıdır. Arbor Network firması günlük 1000 ölçülebilir DDoS atağı gözlemlenmiştir. Bu atakların büyük bölümü göze çarpmayan küçük web siteleri ve ev kullanıcılarını hedef almaktadır [6].

3.1. Yetki Aşımları

Bu saldırı türünde amaç erişim izni olmayan uygulamalara erişim izni oluşturacak açıkların kullanılmasıdır. Genellikle dışarıdan saldırılar içerideki sistemlere bir kullanıcı arayüzü ile erişilmesini sağlayan internet sayfaları üzerinden yapılır. Seçilecek web sayfasında şifrelendirilmemiş URL (Tekdüzen Kaynak Bulucu)'lar kullanılarak admin hakkı ile erişim sağlanmaya çalışılır. Bir başka metot da internet, intranet ortamından yada elde edilmiş şifreli bir dosyayı eksiksiz arama (brute force)/sözlük metotları ile şifre kırma operasyonları gerçekleştirilerek sisteme yetki dışı erişim sağlanmasıdır. Eksiksiz arama ataklarında bilgisayar korsanı şifrelenmiş dokümanın bir kısmını muhtemel şifresiz halini tahmin ederek kullanılan şifreleme anahtarını olası ihtimaller için dener. Anahtar uzayı çok geniş olduğu için her bir anahtar ihtimalini denemek mümkün değildir [7]. Parola ile erişilen sistemlerde, parolalarda ek karakter kullanılmadığı durumlarda eksiksiz arama kullanılmaktadır. Olabilecek bir, iki karakterli yada karakterlerle birlikte numaralı olasıklar denenerek parola çözülmeye çalışılır. Bu atak türlerine direnebilmek için şifreleme sisteminin yerel politika ve prosedürlerle kolay hatırlanır, uzun, karışık karakterli ve değiştirilen parolanın eskisi ile aynı olmamasını teşvik etmek eksiksiz arama ataklarının hızını düşürecektir [8].

3.2. Uygulamaya Yönelik Saldırılar

Uygulamaya yönelik saldırılarda amaç bir web sunucusu üzerinden ya da bir veritabanı sunucusu üzerinden değerli bilgiyi çekmektir. Yetki aşımı kullanılabileceği gibi, çapraz taraflı betik ataklarıyla sayfa yönlendirmeleri yapılarak kullanıcı bilgilerini çalma/kötüye kullanma şeklinde de güvenlik ihlalleri mevcuttur. Bu atakta bilgisayar korsanı saldırıya açık siteye erişen kullanıcının web tarayıcı bilgilerini kendine yönlendirir. Yansıtmalı çapraz taraflı betik ataklarında istismar programları bu siteye ulaşan kullanıcı formları gibi bilgileri bilgisayar korsanına iletir. Yansıtmalı olmayan çapraz

taraflı betik ataklarda ise genel kullanımlı bir web içeriğinin içine kötü niyetli kod gömülür ve mağdur bu programı istismara uğramış web sayfasından kendi çalıştırır. Bu kodlar genelde kötü niyetli sitelere yönlendirmek yada kullanıcı bilgilerini çalmak için kullanılır [9].

Yine yapısal sorgulama dili enjeksiyonu gibi metotlarla yazılım esnasında farkına varılmayan SQL sorgularında oluşan güvenlik açıkları değerlendirilerek veritabanı üzerinden bilgi çekmek de mümkündür. Bu saldırı türündeki tehditlere maruz kalmamak için portal ve veritabanı yazılımı geliştirenlerin OWASP (Open Web Application Security Project/Açık Ağ Uygulama Güvenlik Projesi) standartlarına uygun yazılım geliştirmesi gerekmektedir. Ayrıca ilgili araçlar kullanılarak bu yazılımlar periyodik olarak güvenlik taramalarından geçirilmelidir.

3.3. İşletim Sistemi ya da Uygulama Seviyesinde Kullanılan İstismarlar

İstismarlar işletim sistemi ve işletim sistemlerinin kullandıkları uygulamaların güvenlik açıklarını değerlendirip uzaktan erişim sağlayan, ya da açığın türüne bağlı olarak içerde bir fonksiyonu çağırabilen kötü amaçlı yazılmış yazılımlardır. Bu yazılımlar bir dosyaya eklenmiş olarak gelip açılabileceği gibi, bir web sayfası hatta gerekli koşullar sağlanırsa uzaktan IP numarası ile de etkinleştirilebilir. Bu ataklardan korunmak için güvenlik yamalarının devamlı izlenmesi ve özellikle kritik öneme sahip olanlarının zaman kaybedilmeden yüklenmesi gerekir.

3.4. Virüs ve Benzeri Yazılımlar

Virüsler, yazılımların sonuna kendini ekleyerek çalıştırılan program ile aktive olabilen ufak yazılımlardır. Solucanlar (worm) ise aynı şekilde aktive olan fakat kendini ağdaki diğer bilgisayarlara da atabilen daha tehlikeli yazılımlardır. Truva atları (Trojan) ise tarihteki Truva atı modellemesi ile

oluşturulmuş, sisteme yerleştiklerinde dışarıya bir port veya servis açan, böylece dışarıdan erişimi sağlayan ufak yazılımlardır.

Günümüzün en önde gelen tehditlerini içeren bu zararlı kodlar her gün üretilmekte ve firmalara ciddi anlamda maliyet yüklemektedir. Bu gibi yazılımlardan korunmanın yolu ise kaynağı belli olmayan uygulama dosyalarının çalıştırılmaması ve anti-virüs yazılımları ile sistemlerin korunmasının sağlanmasıdır.

3.5. Ağ Saldırıları

Ağ seviyesindeki saldırılar genelde OSI katmanında veri katmanı veya ağ katmanı seviyesinde gerçekleşir. Bu saldırılar varyasyon olarak en fazla çeşitliliğe sahip olan ataklardır. Ağ dinleme, servislerin kötüye kullanımı, açık portların kötüye kullanımı, DoS atakları bunlardan sadece birkaçıdır. Ağ saldırılarının ilk adımında port taraması yapılarak karşı sistemin hangi portlarının açık olduğu bilgisi edinilir.

3.5.1. Port tarama teknikleri

Port tarama işleminde amaç, TCP paketinin başlık kısmındaki bazı bayraklarından ya da TCP/UDP protokollerinin işleyişinden yararlanarak erişilmek istenen sistemin dinlemede olan portlarını keşfetmektir. Port tarama metotlarında en çok kullanılan metotlardan 8 tanesi, TCP SYN taraması, TCP connection (bağlantı) taraması, UDP taraması, TCP boşluk (null) taraması, TCP FIN taraması, TCP ACK taraması, TCP window (pencere) taraması, TCP Xmas taramasıdır.

TCP SYN taraması

TCP, güvenilir bir protokol olduğundan bağlantı kurmak için üç yollu el sıkışmanın gerçekleşmesi gerekir. Hedef sistemle bağlantı kurmak isteyen makine bu amaçla hedefe SYN paketi gönderir, eğer karşı makine SYN ve ACK paketleriyle cevap verirse, bu makinenin aktif olduğu anlaşılır. TCP SYN taraması bu teknikten hareketle üç yollu el sıkışma için gerekli olan paket yerine, RESET paketi gönderir. Bu şekilde asla bağlantı kurulmasına izin verilmez. Üç yollu el sıkışmanın olmaması ve dolayısıyla bağlantının kurulmamasından dolayı bu yöntem “yarı-açık tarama” olarak da bilinir.

Bu tekniğin TCP bağlantı taramasına göre iki avantajı vardır. Birincisi tam bir TCP bağlantısı olmadığından hedef sistemde bu tarama görünmeyebilir. İkinci avantajı ise, üç yollu el sıkışma gerçekleşmediğinden daha hızlıdır.

TCP bağlantı taraması

En basit port tarama yöntemidir. Hedef sistemdeki portların her biriyle üç yollu el sıkışma tamamlayabilmek için bağlantı kurulmaya çalışılır. Bu amaçla bilgisayar korsanı, saldıracağı sistemdeki makineye SYN paketi gönderir ve cevap olarak SYN/ACK cevap paketini bekler. RESET paketi gelir yada cevap gelmezse o portlarda kapalı demektir.

TCP FIN taraması

FIN paketi, gönderici bilgisayar veri göndermeyi kestiği ve bağlantıyı bitirmek istediği durumda kullanır. Bu teknikte hedef sistemdeki portlara FIN paketleri gönderilir. Eğer kapalı bir port, ortada hiç bağlantı yokken beklemediği bir FIN paketi alırsa RST paketiyle cevap vermek zorundadır. Bu durumda FIN paketi yollayan kişi, karşıdaki portun kapalı olduğunu anlar. Eğer cevap gelmezse, bu olay portun açık olabileceğini gösterir.

TCP XMAS taraması

Hedef porta FIN, URG ve PUSH paketleri gönderilir. RST paketleri gelirse portların kapalı olduğu, gelmezse açık olduğu varsayılır.

TCP Null taraması

Bu yöntemde bayraklar kapalı konuma getirilir. Yollanan paketlere karşılık RST paketleri gelmezse, portların dinleme durumunda olduğu yani açık olduğu anlaşılır.

TCP ACK taraması

Bu teknik hedef sistemde kullanılan güvenlik duvarlarının ya da yönlendiricinin tipini ve kurallarını öğrenmek için kullanılır. Bu sayede güvenlik duvarının basit filtreleme yöntemiyle mi çalıştığı anlaşılabilir.

Bu teknikte, eğer dışarıdan bir ACK paketi gelmişse, güvenlik duvarı ya da yönlendirici, daha önceden kendi iç ağından bir makinanın SYN paketiyle bağlantı kurmak istediğini ve ACK paketinin buna karşılık olarak geldiğini varsayar. Eğer karşıdan RST gelirse bu durumda hedef port un “filtresiz” olduğu, yani paket filtreleme özelliğine sahip cihazın iç ağdaki hedef porta izin verdiği anlaşılır. RST paketi yerine “ICMP port unreachable” (ICMP paketi porta erişemiyor) mesajı gelirse ya da hiç cevap gelmezse, o portun “filtrelenmiş” olduğu, yani sistemdeki bir paket filtreleme gibi bir mekanizmanın portun cevap vermesini engellediği düşünülür.

TCP windows taraması

TCP ACK taramasına çok benzer. IBM-AIX, HP-UX, BeOS, SunOS 4.x, Ultrix, IRIX ya da FreeBSD gibi bazı Unix tabanlı sistemlerde TCP Window

Size'dan kaynaklanan anormallikten yararlanarak açık ya da fitreli/filtresiz portları bulmak için kullanılır.

UDP taraması

UDP, TCP'den bir çok yönüyle farklıdır. Mesela, UDP'de bağlantı kurmak için üç yollu el sıkışma olayı yoktur, sıra numaraları ve kod bitleri de yoktur. Paketler gelişigüzel gönderilir ve kaybolan paketlerin yenisi gönderilmez. Bu nedenle bu yöntemle yapılan taramalara pek güvenilmez.

Bu teknikte hedef sisteme UDP paketleri gönderilir. Eğer sistem "ICMP port unreachable" mesajı verirse, ilgili portun kapalı olduğu anlaşılır. Bu mesajı vermezse açık olduğu kabul edilir. UDP connectionless (bağlantısız) bir protokol olduğundan bu tekniğin doğruluğu ağın bant genişliği ya da sistem kaynakları gibi bir takım faktörlere bağlıdır [10].

3.5.2. TCP protokolü

Bu saldırı türünde amaç ağ üzerinde gereksiz trafik oluşturarak ya da hizmet veren sunucunun üzerinde aşırı yük oluşturarak hizmetin aksamasını sağlamaktır. DoS saldırıları sunucuların sağladıkları hizmetlerde yavaşlamalara, hatta servislerin tamamen hizmet dışı kalmasına yol açabilir, sistemlerin çökmesine neden olabilirler. TCP / IP protokolü mimarisini hedef alan bu saldırılar sistemlere genellikle zarar vermeseler de zaman ve para kayıplarına neden olurlar. DoS saldırılarının amacı değişik yöntemler kullanarak servisleri hizmet dışı bırakmak ve bilgisayar ağı üzerine binen yükü artırmaktır. Bu saldırıların amaçları şöyle sıralanabilir:

- Bilgisayar ağı üzerinde gereksiz yük yaratarak ağın performansını düşürmek.

- İki bilgisayar arasında yaratılan bağlantıları hedef alarak servislerin çalışmasını engellemek.
- Ağ içerisinde belirli servisleri hizmet dışı bırakmak.
- Sadece belirli bir kişi veya bilgisayarı hedef alarak hizmet almalarını engellemek.

Değişik yöntemler kullanılarak gerçekleştirilen (virüs vb.) hizmetlere yönelik saldırılar da DoS saldırıları olarak adlandırılabilir. DoS saldırıları bilgisayar ağının işlevlerini tamamen ortadan kaldırabilir. Saldırılar zayıf makinelerden daha gelişmiş makinelere olabileceği gibi yavaş makinelerden daha hızlı bilgisayarlara da yöneltilebilir. Aralarında ağ bant genişliği, işlemci hızı gibi sebeplerden dolayı farklar olan iki sistem arasında meydana gelen saldırılar "asimetrik saldırılar" olarak adlandırılır.

DoS saldırıları hedefleri itibari ile üç grup içerisinde incelenebilir:

- Kaynakları Hedef Alan Saldırılar: Değerli, kısıtlı kaynakların tükenmesini amaçlayan saldırılardır.
- Yapısal Ayarları Hedef Alan Saldırılar: Bilgisayar ve ağların yapılandırılmasını etkisiz kılmayı, sekteye uğratmayı amaçlayan saldırılardır.
- Fiziksel Saldırılar: Ağ birimlerinin çalışmasını engellemeyi amaçlayan saldırılardır.

<u>Kaynakları hedef alan saldırılar</u>

Bilgisayar ve ağ sistemlerinin çalışma performansını etkileyen çok sayıda etken vardır. Bellek, CPU, ağ bant genişliği gibi değerlerin akıllıca kullanılması gerekir. Bunlar son derece değerli, tekrarlanamayan, değeri o anki kullanım performansı ile ölçülen kaynaklardır.

Bilgisayar Ağ Bağlantısını Hedef Alan Saldırılar: DoS saldırıları çoğunlukla ağ bağlantılarını hedef alır. Ağ bağlantılarını hedef alan DoS saldırılarının amacı

bilgisayarların veya ağların birbirleri ile haberleşmesini engellemektir. DoS saldırılarında genellikle network seviyesindeki işleyişi sağlayan paketler kullanılır. Bunlardan biri de SYN paketidir. SYN paketleri ağ ortamında iki cihazın ilk bağlantı kurulumu esnasında tarafların hazır olduğunun karşılıklı teyidini sağlar. “SYN Bombardımanı” saldırısı bu tür saldırılara örnek olarak gösterilebilir. “SYN Bombardımanı” saldırısı ağ bant genişliğini hedef almaz. Çok sayıda bağlantı isteği göndererek sunucuların baş edemeyeceği miktarda yarı açık bağlantı isteği yaratmayı amaçlar. Bu sayede çekirdek kaynakları kısıtlanarak sunucu hizmet veremeyecek duruma düşürülebilir.

Sistem Kaynaklarının Saldırı Amaçları İçin Kullanılması: Saldırganlar sistemlerin hizmet sunmak amacı ile yarattığı kaynakları saldırı amacı ile kullanabilirler. “Yankı”, “zaman” ve DNS servislerine yöneltilen UDP saldırıları örnek olarak gösterilebilir. Bu servislere yöneltilen çok fazla sayıda UDP paketleri yüksek miktarlarda ağ ve çekirdek kaynağı kullanılmasına neden olur.

Ağ Bant Genişliği Tüketimi: Saldırganlar çok fazla sayıda paket yaratarak veya yarattırarak bilgisayar ağının taşıdığı yükü en üst düzeye çıkartabilirler. Bu tür saldırılara “ICMP yankı saldırıları” örnek olarak gösterilebilir. Bu saldırılar genellikle birden fazla bilgisayar tarafından koordineli olarak gerçekleştirilir.

Diğer Kaynakların Tüketilmesi: Saldırganlar sistemlere ait olan başka kaynakları da gereksiz kullanım yolu ile suiistimal edebilirler. İşletim sistemleri belirli sayıda uygulamanın yaratılmasına izin verirler. Basit bir program ile çok fazla sayıda işlem yaratılarak işletim sistemlerinde gereksiz bellek kullanımına neden olunabilir. Saldırganlar ayrıca isteyerek hata mesajlarının (log) oluşmasına neden olabilirler. Bu bilgiler kayıt miktarının artmasına neden olurlar ve sistemler için ek yük getirirler. Bu tür saldırılara “email bombardımanı” saldırıları da örnek olarak gösterilebilir. Kullanıcılara

ait şifrelerin bilerek yanlış girilmesi ve hesapların kilitlenmesi de problemlere ve işlevselliğin azalmasına neden olur.

Yapısal ayarları hedef alan saldırılar

Doğru olarak yapılandırılmamış bilgisayarlar doğru ve verimli hizmet veremezler. Saldırganlar bilgisayar ve ağ birimleri üzerinde yer alan yapılandırma ayarları üzerinde değişiklik yapılmasına neden olan saldırılar düzenleyerek sistemlerin çalışmasını sekteye uğratabilirler. Hatta tamamen hizmet dışı kalmalarına neden olabilirler. Bu saldırılara "ARP Saldırıları" örnek olarak gösterilebilir.

Fiziki saldırılar

Bu tür saldırılar bilgisayarlara ve diğer bilgisayar ağına yapılan fiziki müdahalelerdir. Bilgisayar sistemlerinin yer aldığı odalara erişim kısıtlanmalıdır. Sadece yetkili personelin bu sistem odalarına girişlerine izin verilmelidir. Fiziki güvenlik saldırılarının meydana gelmesini önlemek en başta gelen tedbirlerden biridir.

3.5.3. DoS saldırı çeşitleri

Hizmet etkisizleştirme (Denial of service) saldırıları

Saldırılar gün geçtikçe değişik metotlar ile gerçekleştirilmektedir. Saldırılar saldırganların yaratıcılıkları ölçüsünde tehlikeler yaratır. DoS saldırılarını tek çatı altında toplamak, kaynaklarını ve hedeflerini kesin olarak belirtmek son derece zordur. Sistemlerin çalışmasını hedef alan her türlü saldırı bu kapsam içerisinde değerlendirilebilir. Saldırılar doğrudan saldırgan tarafından gerçekleştirilmeyebilir. Virüs saldırıları bunlara örnek olarak gösterilebilir. En

çok bilinen ve etkinliğini günümüzde de gösteren saldırılar aşağıda özetlenmiştir.

Toplu yayın adresli (Broadcast) paket yayımı

DoS saldırılarının çoğu amaçlarına ulaşabilmek için bilgisayar ağı üzerinde bulunan tüm noktalara paketlerin taşınmasını sağlayan toplu yayın adresleri kullanır. RFC 919 toplu yayınlanan mesajların yayımı ile ilgili bazı standart ve kısıtlamalar öngörmektedir. Buna göre 255.255.255.255 toplu yayın mesajları yönlendiriciler tarafından bilgisayar ağı dışına taşınamaz. 255.255.255.255 adresi aynı ağ üzerinde bulunan tüm adresler tarafından algılanır. Bu nedenle bu adresi hedef alan paketlerin yönlendiriciler tarafından ağ sınırları dışına taşınmaması gerekir.

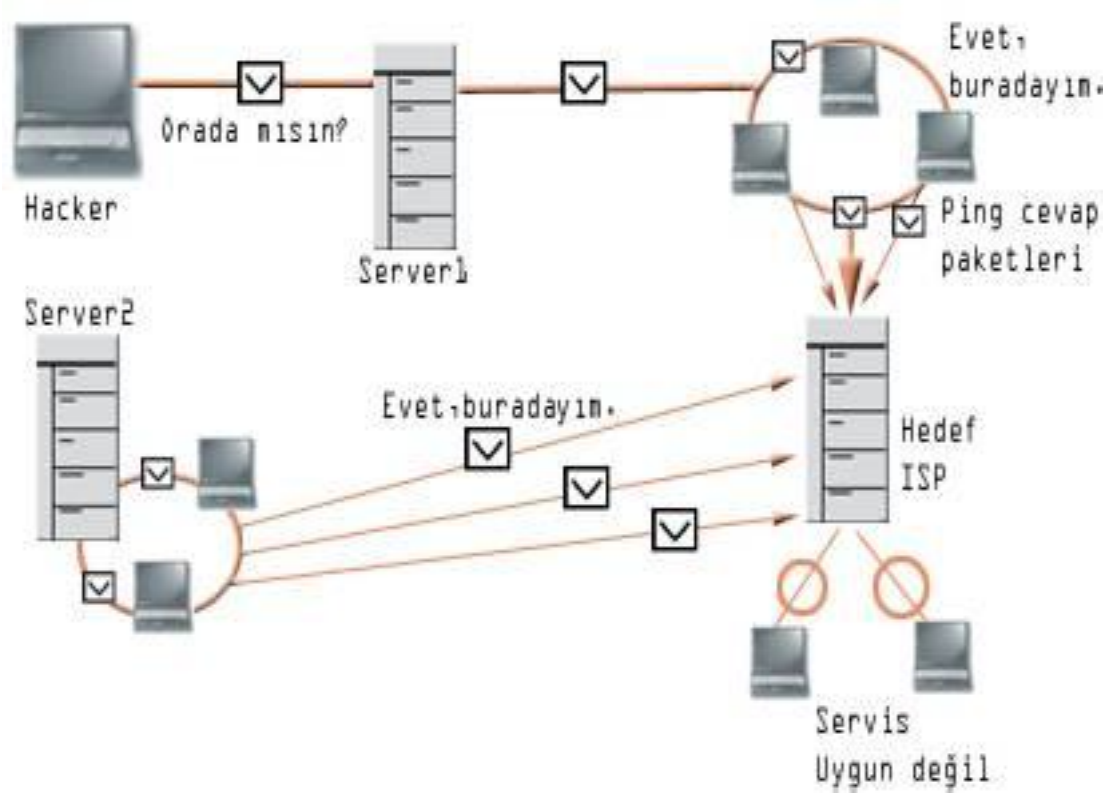
- 255.255.255.255 adresini hedef alan paketler ağ üzerinde bulunan tüm noktalara iletilir.
- 10.255.255.255 adresini hedef alan paketler 10'lu bilgisayar ağı üzerinde bulunan tüm noktalara iletilir.

Yukarıda verilen örnek alt ağ kullanılmadığı sürece aynı anlamı taşır. Verilen iki örnek için de istisnalar mevcuttur. Eğer bilgisayar ağları ayrılmış ise yukarıda tanımlanan sistem kullanılamaz. Alt ağlar için tanımlanmış olan toplu yayın adresleri kullanılır.

Şirinleme (Smurf) saldırısı

Şirinleme saldırısı ICMP protokolüne ait özellikleri kötüye kullanan, bant genişliğini hedef alan saldırı türüdür. İsmini saldırının yapıldığı programdan alır. Ağlarda bulunan bilgisayarlara karşı sıklıkla kullanılan saldırı türüdür.

Ping, bilgisayarların bilgisayar ağı üzerinde aktif olarak bulunup bulunmadığını belirlemek için kullanılan bir uygulamadır. Ping programı ICMP yankı istek mesajları üreterek hedef bilgisayara gönderir. Eğer hedef bilgisayar aktif ise aldığı bu mesaja karşılık olarak ICMP yankı yanıt (reply) mesajı yayınlayarak istekte bulunan bilgisayara gönderir. Şirin saldırısı sırasında saldırgan çok fazla sayıda ICMP yankı istek (request) mesajı yayımlar. Bu mesajlar kaynak IP adresi olarak, hedef alınan bilgisayarın IP adresini; hedef IP adresi olarak ise toplu yayın adresini alır. Hedef adres olarak toplu yayın adresleri içeren paketler ağ üzerinde bulunan tüm noktalar tarafından alınır. Alınan bu pakete karşılık aktif olan bilgisayarlar ICMP yankı yanıt mesajları yayınlayarak saldırgan tarafından belirlenen “hedef” bilgisayara iletir. Ağ üzerinde bulunan tüm bilgisayarlar tarafından gönderilen bu mesajlar bilgisayar ağ yükünde bir artışa ve hedef bilgisayarın verdiği hizmetlerde verimsizliğe yol açar (Şekil 3.1.).



Şekil 3.1. Şirinleme Saldırısı

Aktif olan 100 bilgisayardan oluşan bilgisayar ağı üzerinde 300 Kb/s ile şirinleme saldırısı yapıldığı düşünülürse ağa binecek yük 3 Mb/s olarak hesaplanabilir.

Aşağıda verilen şirinleme saldırısı 255.255.255.254 alt ağ maskesine sahip olan bilgisayar ağı üzerinde gerçekleştirilmiştir. Ağ için toplu yayın adresi 198.208.197.31' dir. Saldırgan 198.208.197.15 bilgisayarına ait ICMP yankı istek mesajlarını toplu yayın olarak yaratmıştır. Bilgisayar ağı üzerinde aktif olarak bulunan bilgisayarlardan bazılarının bu isteğe ICMP yankı yanıt paketleri göndererek karşılık vermişlerdir.

198.208.197.15 198.208.197.31 ICMP Yankı (ping) istek
ICMP
Tür: 8 (Yankı (ping) istek)
Kod: 0
Kontrol Toplam (checksum) : 0xd85b (geçerli)
Belirteç: 0x0200
Dizi Numarası: 0x7300
Data: (32 Oktet)

198.208.197.7 198.208.197.15 ICMP Yankı (ping) yanıt
ICMP
Tür: 0 (Yankı (ping) yanıt)
Kod: 0
Kontrol Toplam (checksum) : 0xe05b (geçerli)
Belirteç: 0x0200
Dizi Numarası: 0x7300
Data: (32 Oktet)

198.208.197.21 198.208.197.15 ICMP Yankı (ping) yanıt

ICMP

Tür: 0 (Yankı (ping) yanıt)

Kod: 0

Kontrol Toplam (checksum) : 0xe05b (geçerli)

Belirteç: 0x0200

Dizi Numarası: 0x7300

Data: (32 Oktet)

198.208.197.9 198.208.197.15 ICMP Yankı (ping) yanıt

ICMP

Tür: 0 (Yankı (ping) yanıt)

Kod: 0

Kontrol Toplam (checksum) : 0xe05b (geçerli)

Belirteç: 0x0200

Dizi Numarası: 0x7300

Data: (32 Oktet)

198.208.197.10 198.208.197.15 ICMP Yankı (ping) yanıt

ICMP

Tür: 0 (Yankı (ping) yanıt)

Kod: 0

Kontrol Toplam (checksum) : 0xe05b (geçerli)

Belirteç: 0x0200

Dizi Numarası: 0x7300

Data: (32 Oktet)

198.208.197.6 198.208.197.15 ICMP Yankı (ping) yanıt

ICMP

Tür: 0 (Yankı (ping) yanıt)

Kod: 0

Kontrol Toplam (checksum) : 0xe05b (geçerli)
Belirteç: 0x0200
Dizi Numarası: 0x7300
Data: (32 Oktet)

Normal olarak 255.255.255.255 hedef IP adresine yönelik paketler ağ içerisinde gözlemlenmez. Bu paketler eğer komşu bilgisayar ağları tarafından iletiliyorsa bu tür paketlerin yönlendirilmemesi için gerekli işlemlerin yürütülmesi gerekir.

Toplu yayın mesajları daha önceden belirtildiği üzere ağ üzerinde bulunan tüm birimler tarafından alınır. Tanımlanamayan kullanışsız toplu yayın mesajları DoS saldırılarının işaretçisi olarak tanımlanabilir. Hedef IP adresi olarak toplu yayın adresleri tanımlayan paketlerin ağ içerisinde sürekli izlenmesi gerekir.

ICMP (Internet Kontrol Mesaj Protokolü) yankı istek bombardımanı

Ping bombardıman saldırılarının amacı sistemlerin ağ imkanları ile başa çıkamayacakları miktarlarda ICMP yankı istek paketleri yollayarak bant genişliği harcayıp kaynaklarının kullanılmasını engellemektir. Alınan her ICMP yankı istek paketine karşılık ICMP yankı yanıt mesajı yayınlanır. Bant genişliği yüksek olan bilgisayar ağlarından, nispeten daha küçük bant genişliği olan bilgisayar ağlarına yapılan saldırılar ağ bağlantılarının tamamen kopmasına neden olabilir. Bu saldırılar genellikle koordineli olarak tek bir hedefe yönelik gerçekleştirilir.

SYN bombardıman saldırıları

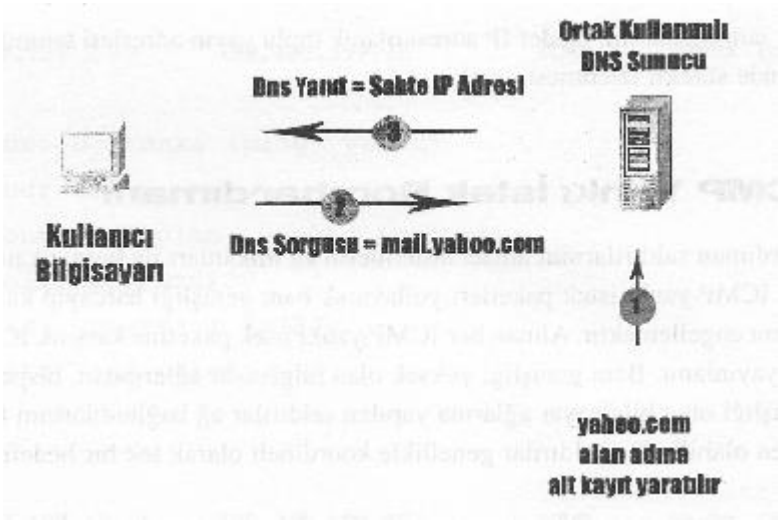
Sıklıkla görülen DoS saldırılarından birisi de sunucularla çok fazla sayıda yarı açık bağlantılar yaratmaktır. Bu tür saldırılar genellikle internete bağlı

bilgisayarlara karşı gerçekleştirilir. Amacı sadece sunucuyu işlevsiz kılmaktan öte düşünceler de içerebilir.

İnternete bağlı TCP tabanlı hizmet veren tüm sunucular bu tür saldırıların hedefidir. Bu tür saldırılarda saldırının kaynağının kesin olarak belirlenmesi oldukça zordur. Saldırganlar kendi IP adreslerini içeren Syn paketleri yerine sahte IP adresleri kullanırlar.

İstemci ve sunucular TCP tabanlı bağlantı kuracakları zaman birbirlerini takip eden mesaj değişimi gerçekleştirirler. Telnet, http, ftp vb. tüm servisler TCP protokolünü kullanırlar. Bağlantının gerçekleşmesi TCP protokolüne ait bir özellik olan “üç adımlı bağlantı kurulumu” (Three way Handshaking) işlemi sonucunda gerçekleşir. İstemci sunucuya SYN mesajı gönderir; sunucu bu isteğe SYN-ACK mesajı ile yanıt verir. En son olarak istemci ACK paketi gönderir ve TCP bağlantısı kurulmuş olur. İyi niyetle tasarlanmış olan TCP protokolünün bu özelliği saldırganlar için önemli bir tasarım açığı olarak görülebilir.

TCP bağlantı kurulum adımları saldırganlar için DoS saldırılarında kullanılır. Saldırganlar yanıltıcı IP adresleri kullanarak SYN bombardımanı yaparlar (Şekil 3.2.). Bunun sonucunda sunucular bu istek paketlerine SYN-ACK mesajları ile yanıt verirler. Böylece yarı açık bağlantılar yaratılmış olur. Saldırganların amacı bağlantı kurmak değil, sadece istek yaratmaktır. Sunucular TCP bağlantı bilgilerini data yapıları içerisinde saklarlar. Her bağlantı için sunucu belleğinde yer ayırır. Bu alan içerisinde TCP protokolü ve IP protokolüne ait olan veriler tutulur. Bağlantı için tutulan sayaç içerisinde belirtilen zaman aşımı süresi dolana kadar bilgiler bellek içerisinde saklanır. Çok fazla yarı açık bağlantı büyük miktarlarda bellek kullanımı gerektirir. Bellek tamamen dolduğunda ise sunucu yeni bağlantı isteklerine karşılık veremeyecek duruma gelir.



Şekil 3.2. SYN Bombardıman Saldırısı

Bu saldırılar sırasında alınan SYN paketlerinin kaynakları kesin olarak belirlenemez. Saldırı sırasında aktif olan kaynaklara ait olan IP adresleri kullanılır. Aktif olmayan bilgisayarlara ait IP adreslerinin kullanımı ICMP "hedef bilgisayar erişilemez" mesajının yaratılmasına sebep olur. Bu da sunucunun bağlantı için ayırdığı belleği silmesine neden olur. Saldırıların birden fazla kaynak tarafından eşgüdüm içerisinde yapılması saldırının başarı olasılığını artırır.

Bu tür saldırılardan korunmanın yolu, kaynak ve hedef IP adreslerinin birlikte doğruluğunun sınanarak IP datagramların yönlendirilmesinin sağlanmasıdır.

Aşağıda Syn bombardımanı sonucunda meydana gelen data akış izlerini içeren örnek verilmiştir. http (80) üzerinde çalışan servise yönelik saldırıda değişik IP adreslerinden SYN paketleri gönderilmiş ve yarı açık bağlantılar yaratılmıştır.

174.184.77.50 62.214.253.23 TCP 45706>http [SYN]
135.125.99.38 62.214.253.23 TCP 28992>http [SYN]
29.244.192.63 62.214.253.23 TCP 36617>http [SYN]

158.10.149.170 62.214.253.23 TCP 15507>http [SYN]

Gözyaşı (Teardrop) saldırısı

DoS saldırılarından bazıları işletim sistemlerinin, modüllerin veya programların tasarım hatalarından kaynaklanan özelliklerini saldırı amacı ile kullanır. Bu saldırı türlerine “teardrop” saldırısı örnek olarak gösterilebilir.

Bilgisayar ağları yapısal özelliklerine göre değişik büyüklüklerde paketlerin taşınmasına olanak sağlarlar. Ağlar üzerinde taşınabilecek en büyük değer MTU (Maksimum İletim Birimi) olarak ifade edilir. Ağ ortamında iletilen paketlerin büyüklüğü bu değere göre işlem görür. Taşınabilecek paket büyüklükleri arasında farklar olan ağlar arasında veri iletimi sırasında parçalama (fragmentation) işlemi yürütülür. MTU değeri büyük olan ağdan MTU değeri küçük olan bilgisayar ağına paketlerin iletimi bu sayede gerçekleşir. Parçalanan paket üzerinde yer alan dataların yerleri offset adı verilen değer ile işaretlenir. Bu sayede parçalanan paketlerin paketleri alan bilgisayar tarafından yeniden birleştirilmesi sağlanır.

Gözyaşı saldırısı paketlerin parçalanması ve birleştirilmesi işlemini saldırı amacı ile kullanır. Offset değerleri çakışma gösteren paketler yaratılarak saldırının yapılacağı hedeflere gönderilir. Paketleri alan bilgisayarlar parçaları birleştirmekte çok büyük güçlük yaşar. Hatta işletim sistemleri tamamen işlevsiz kalabilir.

135.245.151.23 62.214.253.23 UDP (frag: 286 : 3600)
135.245.151.23 62.214.253.23 UDP (frag: 286 : 3825)

Yukarıda gözyaşı saldırısına ait olan izler verilmiştir. Birinci paket 286 – 3600 arasını tanımlarken, diğer paket 286 – 3825 arasındaki verileri tanımlamaktadır. Bu da aynı paket için çakışma yaratmaktadır.

DoS saldırıları saldırganların hayal gücü ile sınırlıdır. Hizmetleri ve ağ altyapılarını hedef alan çok değişik saldırı türleri geliştirilebilir. Saldırıların oluşmasını engellemek genellikle imkansızdır; ancak etkilerini azaltmak mümkündür.

3.6. DoS Saldırılarına Karşı Alınabilecek Önlemler

DoS saldırılarını tamamı ile durdurabilecek kesin bir yol yoktur. Ancak saldırıların bilgisayar ağı ve hizmetleri açısından etkisi azaltılabilir. Ağ içerisinde yer alan herhangi bir hizmet DoS saldırılarının hiç beklenmeyen ve daha önceden belirlenemeyecek bir yol kullanılarak hedefi olabilir. Genel olarak ağ içerisinde güvenliğin sağlanması bir bütündür. Güvenlik için ağ içerisinde belirli kuralların konması, risklerin ve ağ içerisinde değerlerin belirlenmesi gerekir. Oluşabilecek problemlere karşı savunma ve problemlerin ortadan kaldırılması ve zararların telafi edilmesi amacı ile yapılandırmaların ve kuralların konması gerekir [10].

4. GÜVENLİK DUVARLARI

Güvenlik duvarları özel ağ ile internet gibi herkese açık ağların arasında trafiği sınırlandıran bir yazılım veya cihazdır. Örneğin, belirlenen bir servisin özel ağdan internete çıkışını engellemede kullanılabilir. Güvenlik duvarı yapılandırılmasında genellikle 3 ara yüz oluşturulur. Bunlardan biri dış ağ (internet gibi), biri intranet yani özel ağ ve diğeri de sunucuların barındırıldığı DMZ (demilitarized zone) alanıdır. DMZ'tin oluşturulmasının temel nedeni sunucuların kullandığı bazı servislerin özel ağ yapısı için tehlike arz etmesidir. Böylece iç ağ korunmuş olur. Güvenlik duvarlarının küçük ağlarda konfigürasyonu ve yönetimi kolaydır. Fakat ağ yapısı büyüdükçe çalışan dış ağa bağımlı uygulamaların ihtiyaçları da artar ve güvenlik duvarı yönetimi de zorlaşır. Uygulamada genelde her şey bloklanır ve ihtiyaç doğrultusunda açılır. Ayrıca güvenlik duvarına erişim sadece sorumluluğu üstlenen sistem yöneticilerine verilir, geri kalan IP'lere ve kullanıcılara kapatılır.

Güvenlik duvarlarında kurallar oluşturulurken ve yönetilirken her şeyin kolay anlaşılabilir bir ara yüz ile yapılabilmesi önemlidir. Bu ara yüzden güvenlik duvarı üzerinden geçen trafik de izlenmeli ve analiz imkânı olmalıdır. Bu ara yüzden trafik devamlı izlenmeli ve şüpheli durumlar rapor edilmelidir.

Güvenlik duvarlarının ağ katmanında çalıştığını unutmamak gerekir, zira uygulama katmanında çalışan atakları algılayamaz. IP ve port seviyesindeki kısıtlar geçilirse güvenlik duvarı atıl kalmış olur. Uygulama seviyesinde ise uygulama imzalarını baz alan IPS (Intrution Prevention System), kötücül yazılımları etkisizleştirir. Bundan dolayı güvenli bir ağ için bu iki sistem arka arkaya kullanılır. Güvenliğin sağlanması sadece bu cihazların konfigürasyonuna bağlı değildir. Sistem yöneticilerinin ve kullanıcıların eğitilmesi, spam filtreleme sistemleri, antivirüs ve gerektiği takdirde veritabanı güvenlik duvarları da kullanılmalıdır.

Güvenlik duvarı bir ağ geçidi olması dolayısıyla iç ağdaki bilgisayarlara da IP dağıtabilir. Günümüzde IPv4 sayısı gittikçe azaldığı da düşünülürse legal IP'lerin sanallaştırılması gerekliliği rahatlıkla söylenebilir. Güvenlik duvarı bu işi NAT (Network Address Translation) işlemi ile yapar. Dış ağa tek bir IP ile erişim sağlanırken iç ağa da sanal IP'ler verir. Bu özellik aynı zamanda iç ağdaki bir bilgisayarın IP'sini de dış ağa karşı saklamış olur.

Günümüzdeki güvenlik duvarları bir başka teknoloji olan VPN (Virtual Private Network) ihtiyacını da karşılamaktadır. VPN teknolojisinde uzak bağlantılarda ister iki güvenlik duvarı arasında (site to site VPN) ister bir kullanıcının kullanacağı sertifika ile tek bir bilgisayardan (client to site VPN) sisteme erişimi kripto ile tünellenmiş şekilde iç ağa erişebilir [11].

4.1. Güvenlik Duvarı Tipleri

Güvenlik duvarları yazılım tabanlı ve donanım tabanlı olarak ikiye ayrılabilir. Ancak unutulmamalıdır ki yazılım ve donanım bir bütündür. Her yazılımın çalışması için gerekli bir donanım ve her donanımın işleyişini sağlayan bir yazılım vardır.

Yazılım ve donanım tabanlı olarak ayrılmasının nedeni, yazılım tabanlı güvenlik duvarlarının herhangi bir sunucu üzerinde çalışabilmesidir. Donanım tabanlı güvenlik duvarları ise üreticisi tarafından gerekli donanım ve bu donanımın işlevini sağlayacak ve kullanıcı arabirimini sağlayacak yazılım ile birlikte üretilir ve bu şekilde kullanıcı kişi ya da kuruluşa sunulur.

Aşağıda bu iki güvenlik duvarı türünün genel avantajları ve dezavantajları anlatılmaktadır.

4.1.1. Yazılım tabanlı güvenlik duvarları

Bu tip güvenlik duvarları, genellikle kişisel ve sunucu bilgisayarları üzerine kurulabilen ve işletim sistemi ile bütünleşik olarak çalışan yazılımlardır. Genellikle yazılım şeklinde satılırlar ve hepsinin çalışabildiği belirli işletim sistemleri vardır. Bu yüzden bu tür güvenlik duvarları işletim sistemine bağımlıdır. Bir işletim sisteminde çalışan bir güvenlik duvarı diğerinde çalışmayacaktır. Bu tip güvenlik duvarlarına örnek olarak birçok kişisel ve kurumsal güvenlik duvarı verilebilir. Kişisel ve ev kullanıcısı için güvenlik duvarı örnekleri olarak Symantec Norton Personal Firewall, Conseal PC Firewall, ZoneLabs Zone Alarm, Sygate Personal Firewall verilebilir.

Bu tür güvenlik duvarları açık kaynak kodlu veya kapalı kaynak kodlu olabilir. Açık kaynak kodlu olanlar tamamen ücretsiz olup GPL (General Public License) lisansıyla dağıtılırlar. Kısaca, GPL, FSF tarafından geliştirilen ve kamunun kullanımına sunulan bir bilgisayar lisansıdır. GPL pek çok özgür yazılım tarafından kullanılmaktadır. GPL'in en fazla kullanıldığı platformlardan birisi Linux işletim sistemidir.

GPL altında yayınlanan bir yazılımla her istediğinizi yapamazsınız. Örneğin o yazılımı, beraberinde kaynak kodları olmaksızın dağıtamazsınız. Başka birisinin dağıtım haklarını kısıtlayamazsınız.

Kapalı kaynak kodlu ürünlerin tüm telif hakkı ise üretici firmaya ait olmakla beraber kullanmak isteyen kişi ve kuruluşun ilgili firmadan belirli bir ücret karşılığında ürünün lisansını alması gerekir. Alınan ürün hiçbir şekilde başka bir kişiye verilemez, üzerinde değişiklik yapılamaz ve sadece lisans sözleşmesinde yazan şekilde kullanılabilir. Her iki özellikteki güvenlik duvarlarının da kendine ait avantaj ve dezavantajları bulunmaktadır.

4.1.2. Donanım tabanlı güvenlik duvarları

Bu tip güvenlik duvarları donanım şeklinde tasarlanmış ve üzerine bazı işlemleri gerçekleştirebilecek, kullanıcı arabirimi sunacak çeşitli yazılımlarla donatılmıştır. Genellikle hepsinde kendine özel bir işletim sistemi bulunmaktadır. Arka planda çalışan servisler sadece güvenlik duvarı için kullanılacak olanlardır. Genel olarak tüm işlemler çeşitli donanımlar tarafından yapılmaktadır. Bu tür güvenlik duvarlarına genellikle bir konsol portu üzerinden veya http protokolü üzerinden bağlanılarak gerekli konfigürasyonlar yapılmaktadır. Bu tür güvenlik duvarları yönetim konsolları sayesinde işletim sistemlerinden bağımsız olarak kullanılabilirler. Bu sebepten dolayı genellikle tercih edilirler. Bu tür donanım üreten firmalara örnek olarak Checkpoint, Junipe, Cisco Systems, 3Com, Lucent gibi firmalar verilebilir. Yine bu tür güvenlik duvarlarına örnek olarak da Cisco firmasının üretimi olan Pixve Watchguard, Lucent firmasının üretimi olan Brick ve 3Com VPN firewallar verilebilir.

4.2. Güvenlik Duvarlarının Özellikleri

4.2.1. Yazılım tabanlı güvenlik duvarlarının özellikleri

Genel avantajları

- Bu tür güvenlik duvarları genellikle işletim sistemleriyle bütünleşik olarak çalıştıklarından çok daha ayrıntılı bir şekilde raporlama alınabilir.

- Uygulama yazılımları oldukları için gerekli donanım sağlandığı sürece rahatlıkla bir yerden başka bir yere aktarılabilirler.

Genel dezavantajları

- İşletim sistemine bağımlıdırlar, her yazılım her işletim sisteminde çalışmayabilir.

- İşletim sistemi üzerinde çalıştıkları için işletim sistemlerinin de bakımı söz konusudur.

- İşletim sistemlerinde bulunan hatalardan etkilenirler ve bu nedenle performansları düşebilir.

- Donanım uyuşmazlığından kötü etkilenebilirler.

- Kurulum süreleri donanımsal güvenlik duvarlarına oranla çok daha uzun sürmektedir.

Bu tür güvenlik duvarları açık veya kapalı kaynak kodlu olabilirler. Bunlarında kendi içlerinde avantajları ve dezavantajları mevcuttur.

Açık kaynak kodlu güvenlik duvarlarının avantajları

- Kaynak kodları açık olduğundan lisans ücreti yoktur.

- Kaynak koduna gerektiğinde eklentiler yapılabilir, hataları kolaylıkla bulunup arındırılabilir.

- Kullanılacak ortama göre istenildiği gibi değişiklik yapılarak maksimum performans elde edilmesi sağlanabilir ve gereksiz eklentilerden kurtulabilinir.

Açık kaynak kodlu güvenlik duvarlarının dezavantajları

Genellikle bir firma desteği olmayan bireysel çabalar ile oluşturuldukları için satış sonrası bakım ve destek yeterli olmaz.

Kapalı kaynak kodlu güvenlik duvarlarının avantajları

- Genellikle üretici firmaya belirli bir lisans ücreti ödendiği için çeşitli anlaşmalar yapılarak üretici firma tarafından kurulum ve destek hizmeti garantisi vardır.

- Belirli bir firma tarafından geliştirildiği için uzun zaman geçtikten sonra bile geliştirilmesine devam edilir ve hataları giderilebilir.

Kapalı kaynak kodlu güvenlik duvarlarının dezavantajları

- Kapalı kodlu oldukları için geliştirilmesi, hataların giderilmesi ve eklemelerin yapılması sadece üretici firma tarafından yapılabilir. Herhangi bir gereksinimde üretici firmanın beklenmesi gerekecektir.

- Kullanıcının karşılaşacağı herhangi bir sorunun sebebini tespit etmek çok daha zordur [12].

Açık kaynak kodlu güvenlik duvarlarının geliştirilmesine ayrılan bütçelerin kapalı kaynak kodlu güvenlik duvarlarına göre daha kısıtlı olmasına karşın geliştirilmeye müsait olması bir avantajdır. İki alanda yapılan karşılaştırma çalışmasında;

İlk güvenlik duvarı www, ftp, telnet ve smtp trafiği gibi protokollerin denetimi mevcut açık kaynak kodlu bir üründür. Üzerindeki HTTP-Gopher vekil sunucu ile web sitelerini, java, javascript ve aktif-x uygulamalarını her kullanıcının

web tarayıcısının güvenlik seviyesi ile filtreleyebilmektedir. Ayrıca TIS (Trusted Information Systems) güvenlik duvarı üzerindeki araçlar ile mail güvenliğini, sendmail için vekil sunucu görevi alarak genel ağdan özel ağa yapılan atakları kesmek yoluyla yapabilmektedir.

İkinci güvenlik duvarı olan Cisco IOS, güvenli bağlatıyı sağlayan çeşitli uygulama seviyesindeki vasıflara entegre durumdadır. Bunlardan biri erişim listeleri yazarak web trafiğinden gelen Java uygulamalarını kesebilmektedir. Cisco IOS'un bu yönüyle Linux uygulaması olan TIS'e göre dezavantajı vardır çünkü TIS güvenli sitelerin listesine gerek duymadan kullanıcıların web tarayıcısının listelerini kullanmaktadır. Ayrıca Cisco IOS aktif-x uygulamalarını henüz kesememektedir.

(Performans ölçümü için iki güvenlik duvarı karşılaştırıldığında, Cisco 2621 50 Mhz RISC cihaz 50 mb hafıza ile LINUX güvenlik duvarı ise 350 MHz Pentium cihaz 96 mb hafıza ile test edilmiştir.)

Çizelge 4.1 Paket büyüklüğü 1 byte olan trafiğin analizi

Kural Sayısı	0	50	100	150	200
FIREWALL					
Cisco (paket sayısı)	2541	1604	1434	1312	1216
Linux (paket sayısı)	5277	4293	4377	4033	3574

Çizelge 4.2 Paket büyüklüğü 128 byte olan trafiğin analizi

Kural Sayısı	0	50	100	150	200
FIREWALL					
Cisco (paket sayısı)	571	120	119	118	116
Linux (paket sayısı)	724	718	705	694	670

Çizelge 4.1. ve Çizelge 4.2. de görüldüğü gibi hem paket büyüklüğünün 1 byte olduğu hem de 128 byte olduğu, 0 dan 200 kurala göre iki güvenlik duvarının testinde Linux'un analiz edebildiği paket sayısı daha fazladır [13].

4.2.2. Donanım tabanlı güvenlik duvarlarının özellikleri

Genel avantajları

- En büyük avantajları uygulama için özel geliştirilmiş entegre devreler (ASIC) kullanılmış olmasıdır. Bu sayede daha yüksek performans sağlayabilirler.

- Genellikle en kötü saldırılarda bile cihaz kapatılıp tekrar açıldığında çalışmaya devam ederler.

- Donanımın yedekli çalışması durumlarında iyi performans verirler.

- Minimum seviyede yazılım kullanıldığından ve bu yazılımların tam olarak ne oldukları bilinmediğinden yazılım açıklarından son derece az etkilenirler.

- Hizmet dışı kalma süreleri oldukça azdır.

- Şirket desteği olduğundan güncellemeleri otomatik ve hızlıdır.

Genel dezavantajları

- Yazılabilecek kurallar ve yapılabilecek işlemler cihazın kapasitesi (işlemci gücü, hafıza miktarı vs.) ile sınırlıdır.

- Özellikle küçük yapıda olanları donanımsal olarak genişletilebilme şansı düşüktür. Genellikle bir üst sürümlerinin alınması gerekir. Diğer tiptekilerde ise performans artırımı için gerekli güncellemeler hem pahalı hem de zordur.

- Raporlama işlemleri genellikle sınırlıdır.

- Değişik saldırılara karşı güncellenmeleri kolay değildir ve uzun bir zaman ister.

- Yazılımlarındaki sürüm güncellemeleri genellikle kapanıp tekrar açılma gerektirir.

- Özelleştirilmiş bir donanım yapısında olmalarından dolayı diğer sistemlere oranla pahalı sistemlerdir [12].

5. IPTABLES GÜVENLİK DUVARI

Iptables, profesyonel Linux çekirdeği olan 2.4 serisi çekirdekler içerisinde gelen ve Netfilter kodunu yapılandırmak için kullanılan bir güvenlik duvarı aracıdır. Iptables, paket filtrelemeli bir güvenlik duvarının kurulumu için idealdir. Linux bu işlemleri çekirdek seviyesinde gerçekleştirebilmektedir. Çekirdek içindeki Netfilter modülü de bu iş için geliştirilmiştir.

İlk nesil paket filtreleme kodu olan ipfw basit filtreleme desteği verebiliyordu. Esnek ve karışık konfigurasyonlarda yetersiz kaldığından şu an nadiren kullanılmaktadır. IP filtrelemenin ikinci nesili IP Chain (zinciri) olarak adlandırılmıştır. Son nesil olan paket filtreleme kodu olan Netfilter'da sadece Linux'un 2.4 ve sonrası çekirdek versiyonlarında kullanılan iptables komutu entegredir.

Netfilterdeki en önemli içerik, zincir yapısında sisteme giren sistemden çıkan ve yönlendirilen paketler için kurallar olmasıdır. Varsayılan ayarlarda üç zincir yapısı vardır fakat yeni zincirler oluşturulup öntanımlı olarak ilişkilendirilebilir. INPUT zinciri yerel sisteme giriş yapan paketler için, OUTPUT yerel sistemden farklı sistemlere yollanan paketler için, FORWARD ise paketin farklı bir ağa yönlendirilmesi için kullanılır [14].

Linux çekirdeği tüm bu kategoriler için kuralların listesini tutar. Kural listeleri iptables komutlarıyla muhafaza edilir. Kullanıcı tanımlı zincir oluşturmak, silmek kural eklemek, zincire kural eklemek, zincirden kural çıkarmak ve zincirdeki kuralları değiştirmek için kullanılan parametreler aşağıda verilmiştir.

-A: Zincire yeni bir kural ekler.

-D: Zincir içerisinde bir kuralı siler.

-E: Zincirin adını değiştirir.

-F: Zincir içindeki kuralları siler.

-I: Zincir içerisinde herhangi bir yere kural ekler.

-L: Zincir içindeki kuralları listeler.

-N: Kullanıcı tanımlı kurallar ile yeni bir zincir oluşturur.

-P: Zincirin uygulayacağı öntanımlı kuralı tanımlar.

-R: Küme içerisinde bir kuralı değiştirir.

-X: Boş bir zinciri siler.

-Z: Zincirin tutmakta olduğu paket ve bayt sayaçlarını sıfırlar.

Güvenlik duvarı kurallarında paket filtrelemede hangi paketlerin hangi aksiyonlarla filtreleneceği bilgisi eşleştirilebilir. Aksiyon varsayılan güvenlik politikaları ile belirlenebileceği gibi kullanıcı tanımlı ek aksiyonlar da kural setinde kullanılabilir. Varsayılan politikalardaki aksiyonlar;

ACCEPT: Paketin güvenlik duvarından geçmesini sağlar.

DROP: Paketin güvenlik duvarı tarafından elenmesini sağlar.

QUEUE: İşlem görene kadar kuyukta saklar.

RETURN: Kullanıcı tanımlı kural setinin işlenmesi esnasında varsayılan kural setine dönmesini sağlar.

Kuralların yönetimi için parametreler:

-p: Kuralın tanımlı olduğu protokolün tanımlanmasında kullanılır (TCP, UDP, ICMP)

-s: Kuralın uygulandığı paketin kaynak adresini tanımlar. Adres tek bir kullanıcı adı olabileceği gibi, bir ağ adı ya da bir IP adresi olabilir.

--sport: Kuralın uygulanacağı paketin hangi kaynak porttan geleceğini belirler.

-d: Kuralın uygulandığı paketin hedef adresini tanımlar. Adres tek bir kullanıcı adı olabileceği gibi, bir ağ adı ya da bir IP adresi olabilir.

--dport: Kuralın uygulanacağı paketin hangi hedef porta gideceğini belirler.

--icmp-type: Kuralın uygulanacağı icmp tipini seçer.

-i: Kuralın uygulandığı giriş arabirimini tanımlar.

-o: Kuralın uygulandığı çıkış arabirimini tanımlar [15].

5.1. Birkaç Iptables Örneği

- # iptables –F

Tüm kuralları siler.

- # iptables –A INPUT –p tcp –dport 50 –j ACCEPT

50. port açılıyor.

- # iptables –A OUTPUT –p tcp –dport telnet –j REJECT

Giden Telnet bağlantıları yasaklanır.

- # iptables –F

iptales –A INPUT –j REJECT

iptables –A OUTPUT –j REJECT

iptables –A FORWARD –j REJECT

Tüm ağ trafiği engellendi.

- # iptables -A INPUT -p tcp --dport xxx -j REJECT

xxx ile belirtilen port numarasını, dışarıdan içeriye gelen isteği reddetmek için kapatır.

5.2. GTK+ Kütüphanesi ve Oluşturulan Güvenlik Duvarı

5.2.1. GTK+ kütüphanesi

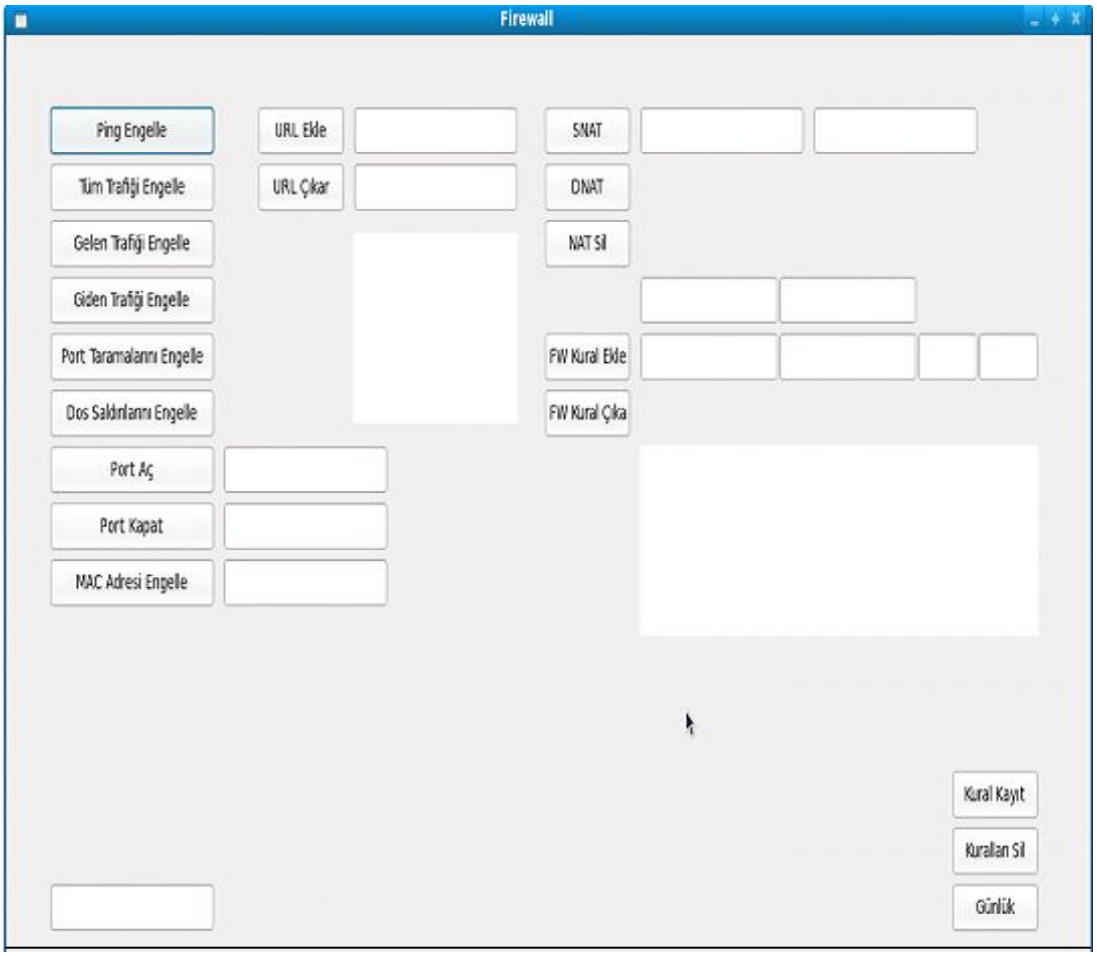
Linux dünyasında geliştirilen uygulamaların büyük bir çoğunluğu iki farklı grafik kütüphanesi kullanılarak yazılmaktadır. Bunlardan GTK+ kütüphanesi C için görsel öğelerin oluşturulabilmesi için kullanılır. GTK+ kütüphanesi GLIB kütüphanesi ile etkileşimli çalışır ve çalışma öncesinde GLIB kütüphanesinin de kurulu olması gerekir. Çoğunlukla görsel uygulama yazacak C geliştiricileri tarafından rağbet görmektedir [16].

5.2.2. Oluşturulan güvenlik duvarının anlatımı

Şekil 5-1 de oluşturulan güvenlik duvarı uygulaması, sadece bir forum üzerinde, kullanıcının rahat kullanabilmesi amacıyla çok sade bir biçimde yapılmıştır. Oluşturulan bu güvenlik duvarı ile bir sistem için gerekli olan başlıca modüller ele alınmıştır. Bu modüller, GTK+ kütüphanesinde, C kullanılarak ve Linux'un güçlü Güvenlik duvarı yazılımı Iptables ile oluşturulmuştur. Oluşturulan güvenlik duvarında kullanıcı tek tek kuralları belirler, bu arada güvenlik duvarı uygulamasında oluşan kurallar bir dosyada tutulur. Buradaki amaç, kullanılan komutların tutulması ve sonradan görme olanağının sağlanmasıdır.

Oluşturulan güvenlik duvarında kullanıcının kara listeye aldığı IP numaraları ya da URL'ler farklı bir dosyada tutuluyor. Buradaki amaç ise, kullanıcı tüm kurallarını silip tekrar kural oluştururursa, daha önceden kara listeye aldığı IP numaralarının engellenmeye devam etmesidir. Kullanıcı kara listeye aldığı IP'leri elle silmediği sürece bu IP'ler sistemde engelli bir şekilde kalır.

Günlük tutma modülünde ise oluşan günlükler /var/log/message.log dosyasında tutulması için ayarlanmıştır.



Şekil 5.1 Oluşturulan Güvenlik Duvarı

Burada butonların tek tek ne işe yaradığı anlatılacaktır.

Ping Engelle: Bu kural sayesinde sisteme gelen ICMP paketleri engellenecektir.

Tüm Trafiği Engelle: Burada sisteme gelen ve giden bağlantı engellenir. Bu kuralla ne kullanıcı dışarıya bağlanabilir ne de dışarıdan bir bağlantı gelebilir.

Gelen Trafiği engelle: Bu kuralla sisteme gelen tüm bağlantılar engellenir fakat sistem dışarıya hala veri gönderebilir.

Giden Trafiği engelle: Bu kuralla giden tüm bağlantılar engellenir fakat sisteme gelen bağlantılar açıktır.

Port Taramalarını Engelle: Bu kuralla SYN, ACK, FIN, RST eşleştirmeleri 1 sn olarak ayarlanır. Belirli periyotlarla tarama yapılmasını engellemeyi sağlamaktadır.

URL filtreleme: Bu kural ile kullanıcı kendisine bir kara liste hazırlayabilir. Bu kara liste diğer kurallardan farklı olarak başka bir dosyada tutulur. Bu sayede kurallar silinse bile bu kara listede bulunan IP'ler engellenmeye devam edilecektir. Kural ekleme ve çıkartma iki ayrı butonla kontrol edilir.

SNAT (Source NAT): Bu kuralla, ilk edit kutusuna kaynak ağ adresi yazılır (192.168.1.0/24 gibi). İkinci edit kutusuna ise sistemin yönlendirilmek istendiği IP adresi (hedef IP) girilir (193.162.40.5 gibi). Böylece paketin kaynağı olan özel ağ IP bloğu, hedef IP ile gizlenerek paket 193.162.40.5 IP'si ile gönderilir.

DNAT (Destination NAT): Bu kuralla, ilk edit kutusuna kaynak ağ adresi yazılır (192.168.1.2 gibi). İkinci edit kutusuna ise güvenlik duvarının iç ağda olan yönlendirilecek IP adresi yazılır (193.162.40.5 gibi). Ayrıca iç ağdaki hedef IP'ye hangi port ile erişileceği de belirtilerek güvenlik duvarının kaynak tarafındaki arayüzü hedeflenerek iç ağdaki IP' ye erişilebilir.

NAT Sil: Nat kurallarını siler.

Port Aç: Bu kuralla istenilen herhangi bir port açılacaktır.

Port Kapat: Bu kuralla istenilen herhangi bir port kapatılacaktır.

Mac Adresine Göre Host Engelle: Bu kuralda ise verilen MAC adresine göre engelleme yapılmaktadır.

FW Kural Ekle/Çıkar: Kaynak IP, Hedef IP, port numarası, IP'lere ait arayüzler ve alınacak aksiyon belirtilerek istenilen kısıtlamalar yapılabilir.

Kural Kayıt: Bu buton tanımlanan tüm kuralların kayıt edilmesini sağlar.

Tüm Kuralları Sil: Bu butonla tanımlanmış olan tüm kurallar silinir. Yalnızca daha önceden oluşturulmuş olan kara listedeki IP'ler engelli kalır.

Günlük: Son olarak bu buton sayesinde günlük tutulur. Sistemde gelen ve giden paketlerle ilgili tüm bilgiler tutulur.

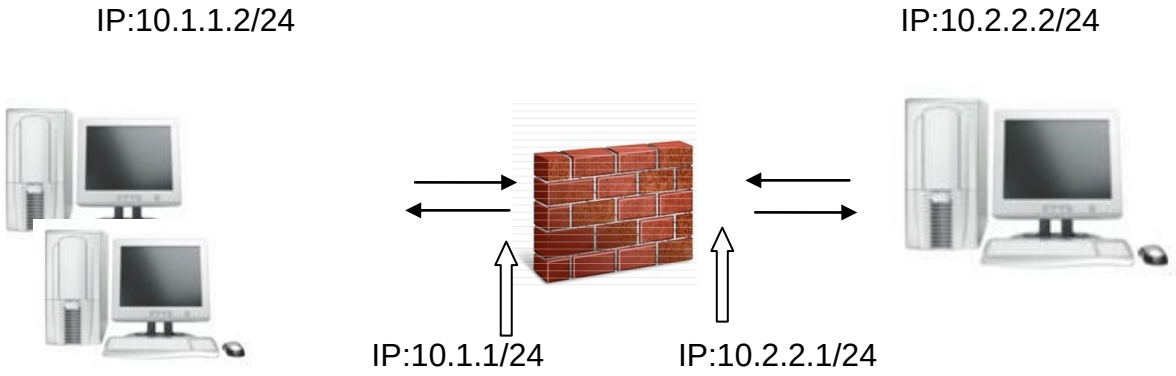
Yukarıda anlatılan kurallar için C'nin dosya işlemleri kullanılmıştır. Bu sayede tüm kurallar kaydedilmiş ve çalıştırılmıştır.

5.3. Çalışma Testi

Tez kapsamında yapılmış olan sınamalar bu bölümde sunulmuştur.

5.3.1. Deney düzeneği

Tez çalışmasının bir parçası olarak, atak engelleme ve güvenlik duvarı fonksiyonlarının testi için deneysel düzenek hazırlanmıştır (Şekil 5.2). Düzenekte iki adet bilgisayar, bir adet sanal bilgisayar ve bir adet güvenlik duvarı kullanılmaktadır. Güvenlik duvarı iki ağı kendi üzerindeki ağ kartları ile ayırmış ve ağlar arasında yönlendirme ve paket filtreleme yapabilir durumdadır. Zira iki farklı ağ arasında yönlendirme yapılmadan haberleşme sağlanması mümkün değildir. Yönlendirme işlemi OSI referans modelinin üçüncü katmanı olan ağ katmanında gerçekleşir.



Şekil 5.2. Deney Düzeneği

Bilgisayarlardan biri ve sanal bilgisayar 10.1.1.0/24 ağında yer almakta ve IP adresleri sıra ile 10.1.1.2 ve 10.1.1.3 olarak verilmektedir. Güvenlik duvarının 10.1.1.0/24 ağını gören bacağının IP adresi 10.1.1.2'dir. İkinci ağ olan 10.2.2.0/24 ağ adresine bakan bacağı ise 10.2.2.1'dir. 10.2.2.0/24 ağındaki bilgisayarın IP adresi 10.2.2.2'dir.

5.3.2. Yazılan güvenlik duvarının DoS saldırı türlerine verdiği tepki

Bu bölümde yazılmış olan güvenlik duvarının DoS saldırı türlerine verdiği tepkiler incelenmiştir.

Hizmet etkisizleştirme saldırıları

Hizmet etkisizleştirme saldırıları genelde uygulama seviyesinde virüs ya da worm (solucan) türü yazılımlarla gerçekleştirilir. Bu kötücül yazılımların amacı bulunduğu bilgisayara ya da bulunduğu ağa zarar vermektir. Solucanlar virüslerden farklı olarak, kendilerini bulunduğu bilgisayardan farklı

bilgisayarlara kopyalamak isterler. Bu nedenden ötürü ağ üzerinde de fazla sayıda bağlantı açarlar.

Solucan ya da virüs türü yazılımlar ağda iyi algılanıp ayırt edilemeyebilirler. Bu konudaki güvenlik önlemi ağ geçidi önündeki ve kullanıcı bilgisayarları üzerindeki anti-virüs yazılımları ile gerçekleştirilmektedir. Anti-virüs yazılımlarının virüs ve solucan imzalarını tanıyıp engelleyebilmeleri için bu imzaları içeren büyük veritabanları vardır. Bu veritabanları hergün geliştirilen virüs ve solucan türlerinin imzalarıyla zenginleştirilir.

Bu teze konu olan güvenlik duvarı, içerik filtreleme özelliği dışındaki atakları ancak ağ seviyesinde engelleyebildiği için bu tür saldırıların önüne geçememektedir.

Toplu yayın adresli saldırılar

Veri paketlerini aynı anda tüm ağa anons yapmak gerekirse o ağda toplu yayın yapılır. Böylece o ağdaki tüm bilgisayarlar gönderilen paketi alacaklardır. Bu yayın metodu her ne kadar gerekli olsa da bilgisayar korsanları tarafından kullanılabilir bir saldırı yöntemine dönüştürülebilmektedir. Bu atak türünde yoğun şekilde trafik oluşturulup iletilmesi gereken verilerin de yerine ulaşamaması ya da iletişimin yavaşlaması hedeflenir.

Bu saldırı türünde yapılması gereken, ağları kendi içinde bir anahtar ya da ağ geçidi ile ağ katmanında ayrı bölütlere ayırmaktır. Böylece toplu yayın paketlerinin kısıtlanması sağlanmış olur.

Bu teze konu olan güvenlik duvarının hali hazırda iki arayüzü vardır. Ayrılan ağlarda toplu yayın yapabilme alanı ikiye bölünmüştür, böylece bu atağın etkisi azaltılmıştır.

Şirinleme saldırısı

Şirinleme saldırılarında, tek bir noktadan, farklı IP adreslerden gönderiliyormuş gibi seçilen hedefe doğru ICMP paketlerinden olan ping paketleri gönderilir. Farklı IP adreslerinden geldiği düşünülen ping paketlerine hedefteki sunucu tarafından yankı paketleri gönderilmeye çalışılır, fakat bir süre sonra sunucu yankı paketlerine cevap veremez hale gelir. Gelen isteklere tepki veremeyen sunucu asli işini de yapamaz duruma düşer.

Şirinleme ataklarından korunmanın en iyi yolu ICMP paketlerinin güvenlik duvarında engellenmesi ve iç ağa erişiminin durdurulmasıdır. Teze konu olan güvenlik duvarı uygulamasında “Ping Engelle” butonu, Linux altındaki GLIB ve GTK+ kütüphaneleri kullanılarak, GTK Widget’ların bir göstergece atanması ile GTK Frame üzerindeki GTK Window’ a konumlandırılmış GTK buton nesnesi ile elde edilmiştir. Butona basıldığında ping paketlerinin güvenlik duvarına ve arkasındaki ağa erişimi engellenmiş olur, böylece şirinleme saldırısından etkilenilmez. Güvenlik duvarının etkilenmemesi için kural zincirindeki “INPUT”, arkadaki ağı koruyabilmek için ise “FORWARD” kuralları kullanılır. “Ping Engelle” butonuna basıldığında C ‘deki system fonksiyonu ile Netfilter kodundaki iptables komutunun ICMP paketlerindeki yankıyı belirten “—icmp type echo-request” parametresi çağırılıp “DROP” aksiyonu verilir. Böylece gelen ping isteklerine yankı dönüşü olmaz. Eğer komutun çalışmasında bir sorun yaşanırsa system fonksiyonunda çağırılan komut “-1” değerini alacaktır, bu durumda hata mesajı kutusunda “tekrar dene” diye bir uyarı mesajı gelecektir. Programda yer alan “Ping Engelle” butonunun kodu Ek-1’de yer alan güvenlik duvarı yazılım kodlarının içinde verilmiştir.

ICMP yankı istek bombardımanı

ICMP yankı istek bombardımanı saldırısı da şirinleme saldırısı gibi çok sayıda ping paketinin hedef bilgisayara yollanması prensibine dayanır. Fakat burada kullanılan kaynak tek IP adresi ve tek bilgisayardır. Bu tür atakların engellenmesi farklı noktalardan gelen saldırılara göre daha kolaydır.

Teze konu olan güvenlik duvarı “Ping Engelle” butonu ile bu tür atakları engellemektedir. Geliştirilmiş olan uygulamada “Ping Engelle” butonu, Linux altındaki GLIB ve GTK+ kütüphaneleri kullanılarak, GTK Widget’ların bir göstergece atanması ile GTK Frame üzerindeki GTK Window’ a konumlandırılmış GTK buton nesnesi ile elde edilmiştir. Butona basıldığında ping paketlerinin güvenlik duvarına ve arkasındaki ağa erişimi engellenmiş olur, böylece şirinleme saldırısından etkilenilmez. Güvenlik duvarının etkilenmemesi için kural zincirindeki “INPUT”, arkadaki ağı koruyabilmek için ise “FORWARD” kuralları kullanılır. “Ping Engelle” butonuna basıldığında C ‘deki system fonksiyonu ile Netfilter kodundaki iptables komutunun ICMP paketlerindeki yankıyı belirten “—icmp type echo-request ” parametresi çağırılıp “DROP” aksiyonu verilir. Böylece gelen ping isteklerine yankı dönüşü olmaz. Eğer komutun çalışmasında bir sorun yaşanırsa system fonksiyonunda çağırılan komut “-1” değerini alacaktır, bu durumda hata mesajı kutusunda “tekrar dene” diye bir uyarı mesajı gelecektir. Programda yer alan “Ping Engelle” butonunun kodu Ek-‘1de yer alan güvenlik duvarı yazılım kodlarının içinde verilmiştir.

SYN bombardıman saldırısı

SYN bombardıman saldırısında amaçlanan hedef bilgisayara sürekli olarak SYN bayrağı “1” olarak ayarlanmış paketler yollayarak, atak yapılacak bilgisayarın TCP bağlantısı oluşturmak üzere üçlü el sıkışma (hand shaking) pozisyonunda kalmasını sağlamaktır. Bu atakta çok fazla sayıda bağlantı

yarıda bırakılır ve hedef bilgisayarın bu bağlantıları beklemesi sağlanır. Açılan yarı bağlantılar sistemi yorar ve iş göremez hale getirir.

Bu tür ataklarda yapılması gereken SYN bayrağı “1” olarak ayarlanmış paketler için, belirli bir zaman diliminde paket sayısında eşik değeri belirlemektir. Bu eşik değeri geçildiğinde paketler reddedilmelidir.

Teze konu olan güvenlik duvarı uygulamasında “DoS Saldırılarını Engelle” butonu, Linux altındaki GLIB ve GTK+ kütüphaneleri kullanılarak, GTK Widget’ların bir göstergece atanması ile GTK Frame üzerindeki GTK Window’ a konumlandırılmış GTK buton nesnesi ile elde edilmiştir. Butona basıldığında SYN bombardıman atakları sonlandırılabilmektedir. Butona basılması ile birlikte C programlama dilindeki system fonksiyonu çağırılır ve güvenlik duvarının bu atağı engelleyen Netfilter kodunun iptables komutundaki “tcp --syn -m limit --limit 1/s --limit-burst 3” parametresi koşturulur. Bu komut, SYN bayrakları “1” olarak ayarlanmış paketlerin saniyede 3 adetten fazla olup olmadığını kontrol etmektedir. Eğer komutun çalışmasında bir sorun yaşanırsa system fonksiyonunda çağırılan komut “-1” değerini alacaktır, bu durumda hata mesajı kutusunda “tekrar dene” diye bir uyarı mesajı gelecektir. Programda yer alan “Ping Engelle” butonunun kodu Ek-1’de yer alan güvenlik duvarı yazılım kodlarının içinde verilmiştir.

Gözyaşı (Teardrop) saldırısı

Gözyaşı saldırılarında maksimum iletim biriminden kaynaklanan parçalanmış veri paketleri kullanılır. Bu paketlerin anlamlı hale gelebilmesi için paketlerin sıra numaralarına sadık kalınarak alıcı tarafta birleştirilmesi gerekmektedir. Bu atak türünde paketelerin sıra numaraları başka paketlerinki ile karıştırılarak hedef bilgisayar iş yapamaz hale getirilir.

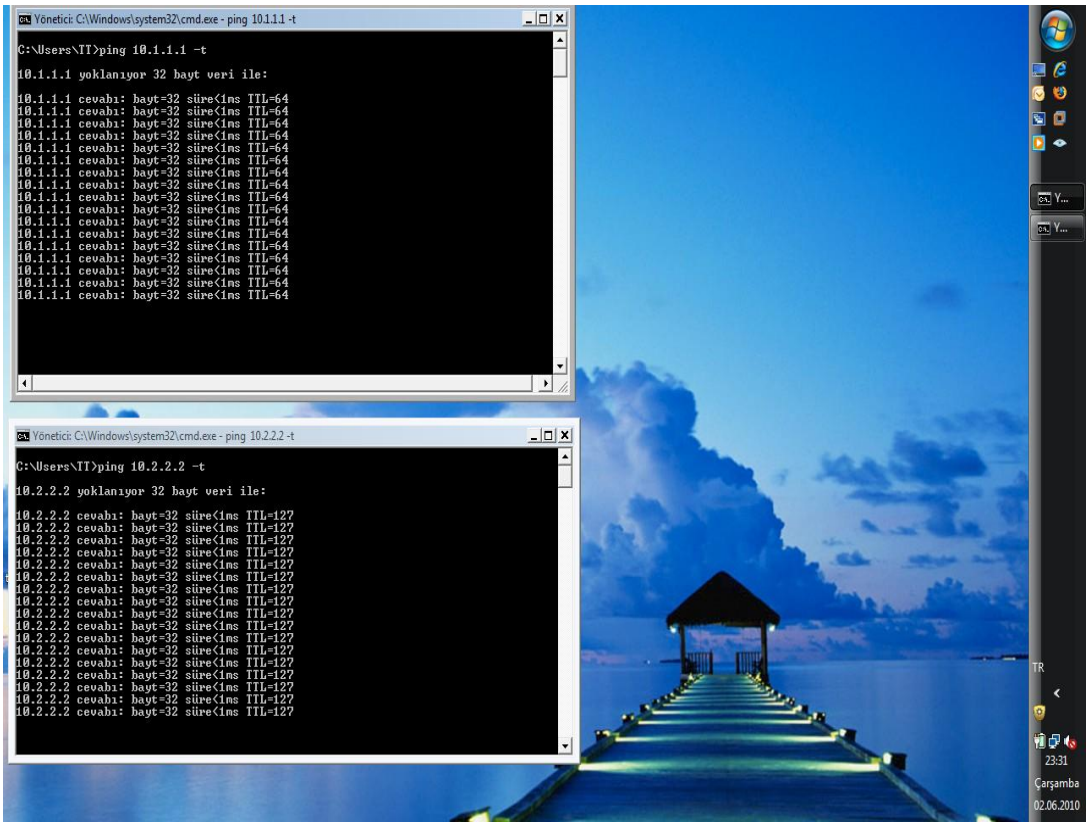
Bu paketlerin engellenmesi için parçalanmış paketlerin güvenlik duvarı tarafından algılanması gerekmektedir. Tez konusu olan güvenlik duvarı bu atağı engelleyememektedir.

5.3.3. Yazılan güvenlik duvarının sınanması

Ölümcül Ping saldırısı sınaması

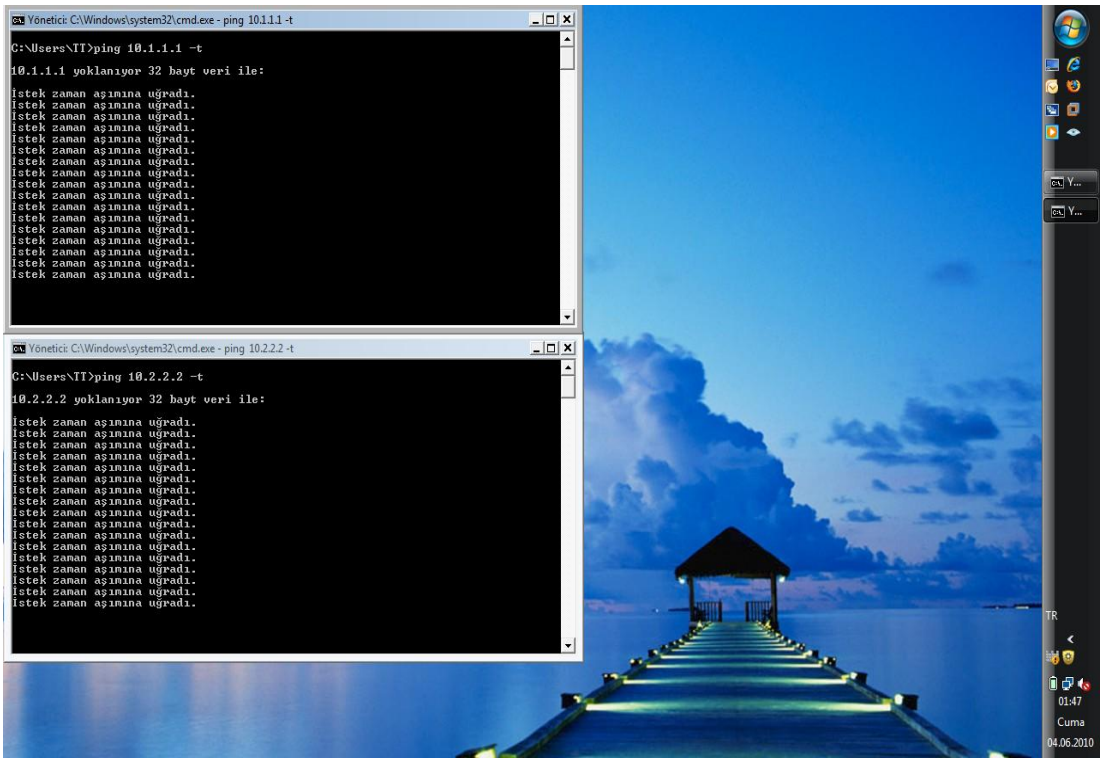
Bu sınamada amaçlanan, deney düzeneğinde (Şekil 5.2.) bulunan 10.1.1.2 IP adresli bilgisayarın DoS ataklarından olan ölümcül ping atağı ile 10.2.2.2 IP adresli bilgisayara saldırmasını, aradaki güvenlik duvarı ile sonlandırmaktır.

İlk adımda 10.1.1.2 IP adresli bilgisayardan güvenlik duvarının 10.1.1.1 IP adresli bacağına ve diğer ağda olan 10.2.2.2 IP adresli diğer bilgisayara ping paketi gönderilmektedir. Herbir arayüze gönderilen 17 adet ping paketinden kayıpsız olarak yankı alınabildiği görülmüştür (Şekil 5.3.). 10.2.2.2 IP adresli bilgisayara 10.1.1.2 IP adresli bilgisayardan ping atılabilmesi, arada bir yönlendirme işlemi olduğunu göstermektedir. Yönlendirme işlemi, üzerinde iki adet ağ kartı olan güvenlik duvarı tarafından yapılmaktadır.



Şekil 5.3. Başarılı Ping Yankısı

İkinci adımda güvenlik duvarı arayüzündeki (Şekil 5.1.) “Ping Engelle” butonuna basılmıştır. Beklenen etki 10.1.1.2 IP adresli bilgisayarın 10.1.1.1 IP adresli güvenlik duvarı bacağından ve 10.2.2.2 IP adresli bilgisayardan ping paket yankılarının dönmemesidir.



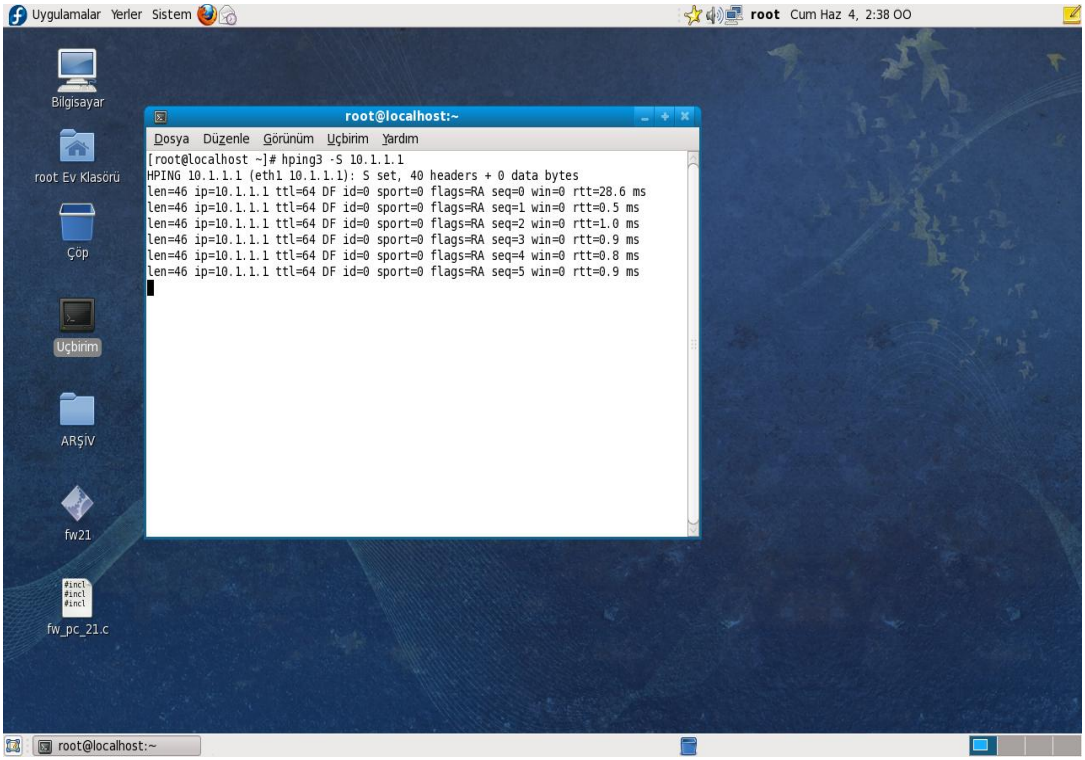
Şekil 5.4. Başarısız Ping Yankısı

Üçüncü adımda 10.1.1.2 IP adresli bilgisayardan güvenlik duvarının 10.1.1.1 IP adresli bacağına ve diğer ağda olan 10.2.2.2 IP adresli diğer bilgisayara ping paketi gönderilmektedir. Herbir arayüze gönderilen 17 adet ping paketinden hiçbirinden yankı alınamadığı görülmüştür (Şekil 5.4.). Bu durum güvenlik duvarının ping paketlerini kestiğini göstermektedir. Böylece ping ile yapılacak bir atak da engellenmiş olmaktadır.

SYN bombardıman saldırısı sınaması

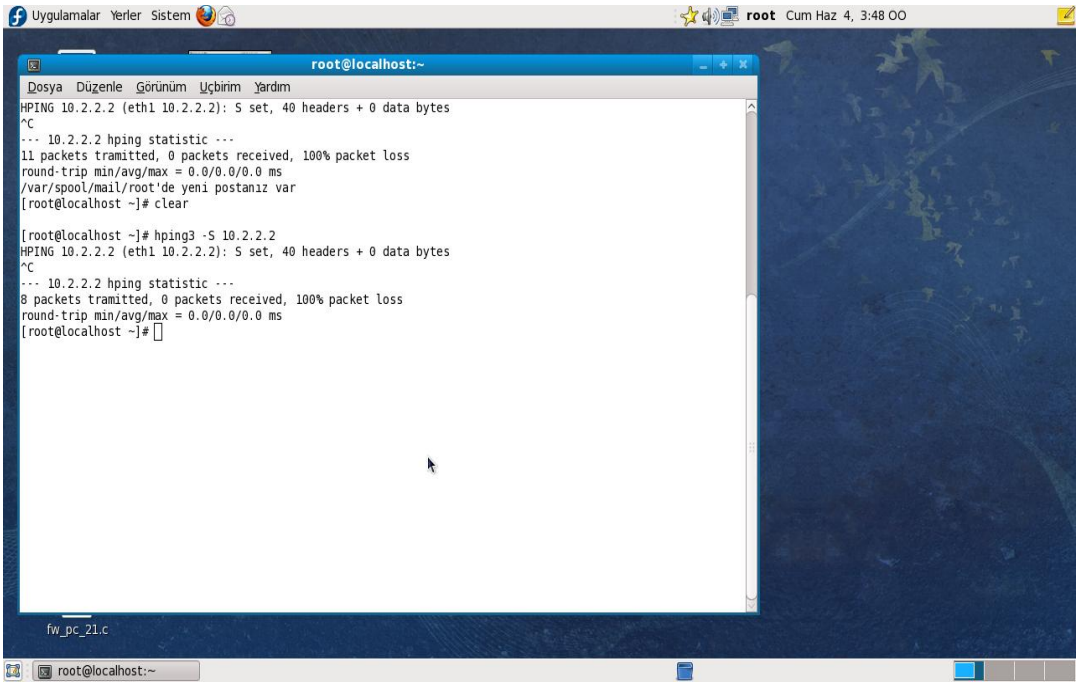
Bu sınamada SYN bombardıman saldırısını simüle etmek için DoS saldırı testlerinde kullanılan hping3 aracı kullanılmaktadır. Bu araç TCP paketleri üzerinde istediğimiz bayrakları değiştirme olanağı sunan bir araçtır. “-S” parametresi ile SYN paketleri üretilebilmektedir.

Hping3 aracı Linux üzerinde çalıştığı için ilk adımda daha önce sanal bilgisayar olarak kurulan 10.1.1.3 IP adresine sahip bilgisayar üzerinden 10.2.2.2 IP adresli bilgisayara hping3 aracının "–S" parametresi ile SYN paketleri oluşturup saldırıda bulunulmaktadır. Toplamda 6 adet SYN paketi gönderilmiş ve tüm paketler karşı tarafa başarı ile ulaşmıştır (Şekil 5.5).



Şekil 5.5. Başarılı SYN Bombardıman Saldırısı

İkinci adımda güvenlik duvarı arayüzündeki (Şekil 5.1.) "DoS Saldırıları Engelle" butonuna basılmıştır. Beklenen etki 10.1.1.3 IP adresli bilgisayarın 10.2.2.2 IP adresli bilgisayara gönderdiği SYN paketlerinin kesilmesidir.

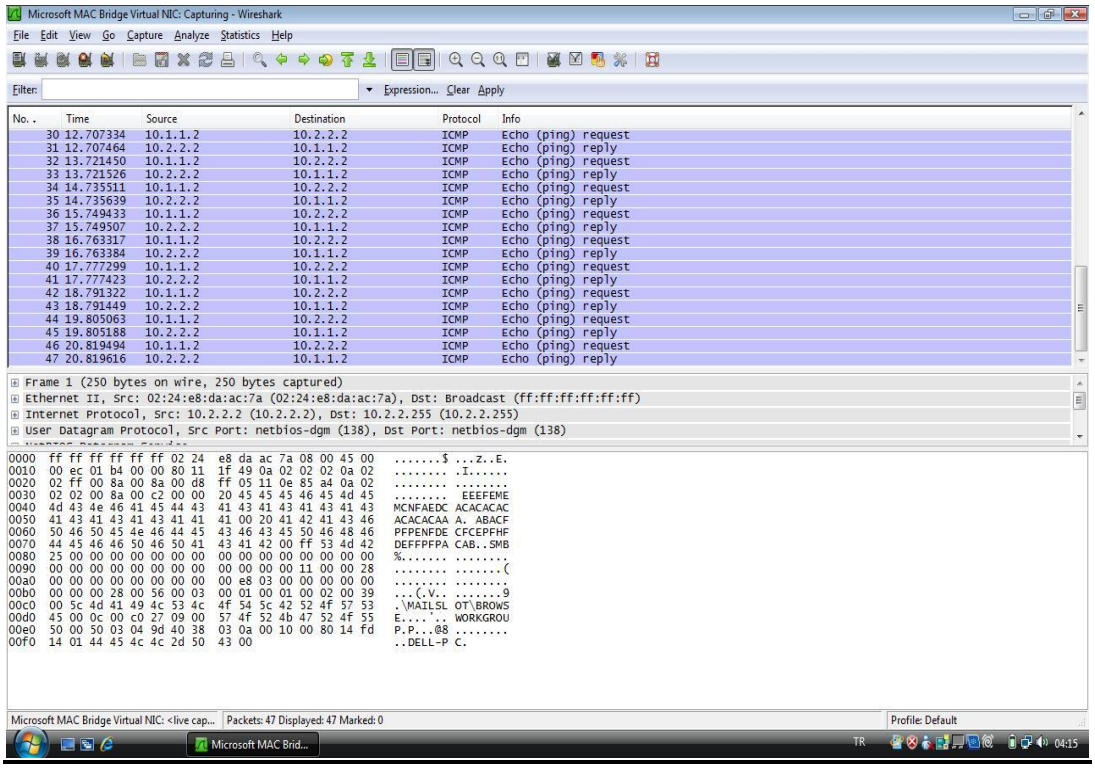


Şekil 5.6. Başarısız SYN Bombardıman Saldırısı

Üçüncü adımda 10.1.1.3 IP adresli bilgisayardan diğer ağda olan 10.2.2.2 IP adresli bilgisayara SYN bayrağı “1” olan paketler gönderilmektedir. Toplamda 8 adet SYN paketinden hiçbirinin karşı tarafa ulaşmadığı görülmüştür (Şekil 5.6.). Bu durum güvenlik duvarının SYN paketlerini kestiğini göstermektedir. Böylece SYN paketleri ile yapılacak bir atak da engellenmiş olmaktadır.

SNAT sınaması

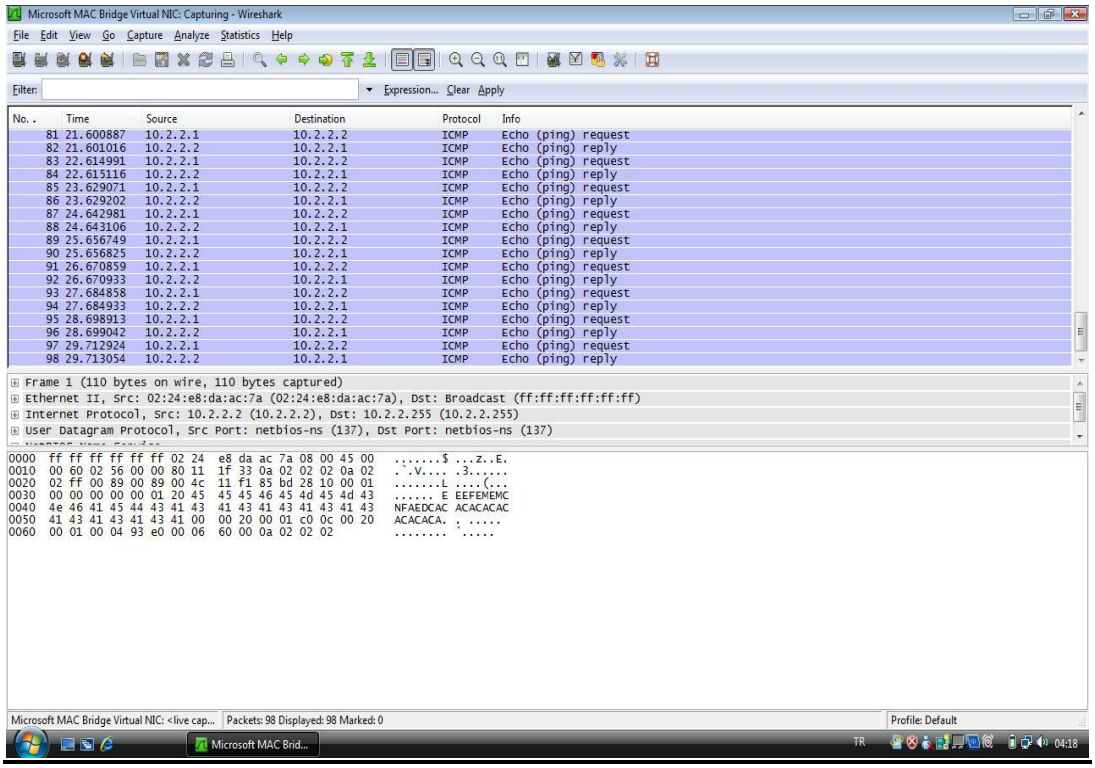
İlk adımda 10.1.1.2 IP adresli bilgisayardan 10.2.2.2 IP adresli diğer bilgisayara ping paketi gönderilmektedir. Gönderilen ping paketleri 10.2.2.2 bilgisayarı üzerinden ağ trafiği analiz aracı olan Wireshark ile analiz edilmiştir. Kaynak IP adresine bakılmış ve 10.1.1.2 olduğu görülmüştür (Şekil 5.7).



Şekil 5.7. SNAT Öncesi Paketler

İkinci adımda güvenlik duvarı arayüzü üzerinde (Şekil 5.1.) SNAT ile ilgili girişlerin yapıldığı kutuların ilkine ping paketlerinin gönderildiği kaynağa ait ağ adresi olan 10.1.1.0/24 IP adres bloğu girilmektedir. İkinci alana da ping paketlerinin kaynak IP adresinin görünmesi istenilen IP adresi girilmektedir. Bu IP adresi de güvenlik duvarının hedefe yakın olan 10.2.2.1 IP adresidir. Bu girişler yapıldıktan sonra SNAT butonuna basılır (Şekil 5.2.).

Üçüncü adımda 10.2.2.2 bilgisayarı üzerinden Wireshark ağ trafiği izleme aracıyla SNAT yapılmış paketlerin kaynak IP adresine bakılmış ve daha önceden kaynak adres olarak ayarlanmış olan 10.2.2.1 olduğu görülmüştür. Halbuki ping paketleri 10.1.1.2 IP adresi üzerinden gönderilmektedir. Böylece bir ağa ait bilgisayardan gönderilen veri paketlerinin o ağa ait güvenlik duvarının dış IP adresi ile anons edilebildiği görülmüştür (Şekil 5.8.).



Şekil 5.8. SNAT Sonrası Paketler

5.4. Değerlendirme

Günümüzdeki güvenlik ihtiyaçları doğrultusunda bir ağ geçidi güvenlik duvarı yazılımı geliştirilmiştir. Geliştirilen güvenlik duvarında hedeflenen, ayrı ağ ortamlarından gelen trafiği farklı arayüzlerinde birleştiren ve geçiş esnasında belirlenen kurallar doğrultusunda filtreleyen bir yapının oluşturulmasıdır. Böylece ihtiyaç doğrultusunda OSI refererans modelinde 3. Katman olan ağ katmanı seviyesinde IP ve port denetimi sağlanmaktadır.

Oluşan kurallar, kural ekle/çıkar butonları ve metin kutuları vasıtasıyla ayarlanabilmektedir. Yazılan güvenlik duvarı uygulamasında ağ geçidi denetimi dışında, en çok gereksinim duyulan fonksiyonlar modellenmiş ve program arayüzünde kullanılması sağlanmıştır. Bu fonksiyonlar sayesinde

güvenlik duvarı olarak kullanılan bilgisayar üzerinden de oluşturulan trafik denetlenebilir hale getirilmiştir.

Bu projede hedeflenen ağ seviyesinde trafik denetimi olmasına karşın, uygulama seviyesinde girilen internet sayfalarının da kısıtlaması mümkün kılınmıştır. Böylece oluşturulan bir kara liste dahilinde belirlenen sayfalara erişim engellenebilmektedir. Bu özellik pratik hayatta içerik filtreleme ürünleri ile sağlanmaktadır. Özellikle firmaların imajlarının zedelenmesini ve hukuki açıdan sıkıntıya girmesini engelleyen bu ürün ailesi açık kod ve kapalı kod olarak piyasada satılmaktadır.

Açık kaynak kodla oluşturulan teze konu olan güvenlik duvarı uygulamasında DoS ataklarından SYN bombardımanı saldırısı hping3 aracı ile denenmiş ve atak durdurulmuştur. Denenen bir diğer atak olan ICMP paket saldırısında ping paketleri kullanılmış ve başarılı bir şekilde atak engellenmiştir. Ayrıca ataklar dışında SNAT hizmetinin de ağ analiz cihazlarıyla gözlemlenmesi gerçekleştirilmiş ve başarılı sonuç alınmıştır. Günümüzdeki ticari ürünlerin yeteneklerinin bir kısmını gerçekleyen bu çözüm açık kaynak kod ile yazılan güvenlik duvarlarının da uygun maliyetli bir alternatif olabileceğini bir kez daha kanıtlamıştır.

6. SONUÇ

Günümüzde, performans artırma ve çalışmalarda paylaşım sağlamak amacıyla bilgisayar sistemlerinin kendi aralarında senkron bir şekilde çalışması elzem hale gelmiştir. Bilgisayar sistemlerinin bir arada çalışmasını sağlayan bilgisayar ağları günümüz bilgi teknolojilerinde ayrı bir branş halini almıştır. Bilgisayar ağlarının her alanda kullanılması, bilgi güvenliğini de önemli bir konu haline getirmiştir. Zira günümüzdeki en değerli kavram bilgidir.

Bilgi, savunma sanayinde kullanılan kritik bir plan olabileceği gibi, bir bankadaki hesap bilgileri ya da bir güvenlik sisteminin kayıtları da olabilir. Bilginin güvenliğini sağlayabilmek için OSI katman modelindeki 3. Katman olan ağ katmanı önem arz etmektedir. Bilginin çalınması ya da sistemlerin hizmet veremez hale getirilmesinde genellikle bu katman teknolojilerinin kullanılması göze çarpmaktadır. Sadece ağ katmanında alınan tedbirler bir sistem için yeterli olmayacağı gibi bu katmanın güvenli hale getirilmemesi durumunda sistemlerde çok büyük bir zafiyet meydana gelecektir. Bu katmanda kullanılan güvenlik cihazları güvenlik duvarlarıdır.

Güvenlik duvarlarının görevi, sistemde oluşturulmuş ağlar arasında gerek IP bazında, gerekse port bazında kısıtlar oluşturarak ağların birbirine erişimini kontrol altına almaktır. Böylece erişim yetkileri IP ve port bazında gerektiği kadar verilebilecektir.

Bu çalışmada, açık kod bir güvenlik duvarı uygulamasının yeteneklerinin bir kısmı incelenmiş ve test edilmiştir. Teze konu olan güvenlik duvarı Fedora 11 Linux ortamında geliştirilmiştir. Kodlamada C ve grafik arayüzü için GTK+ kütüphanesi kullanılmıştır. Güvenlik duvarının fonksiyonlarında Netfilter'dan yararlanılmıştır.

Yazılan güvenlik duvarı uygulamasında hedeflenen beş ayrı içerik mevcuttur. İlk olarak, ağ geçidi rolü alan güvenlik duvarının hali hazırda kullanılan DoS ataklarından olan ICMP yankı istek bombardımanı ve SYN bombardımanı ataklarına karşı ağı koruması hedeflenmiş ve başarıya ulaştığı gözlenmiştir. SYN bombardıman ve ICMP yankı isteği bombardırmanı atakları sınamalarına tezde yer verilmiş ve tam olarak başarı sağlanmıştır. Genel güvenlik duvarı fonksiyonlarının kaynak kodları Ek-1 Güvenlik Duvarı Yazılım Kodlarında mevcuttur.

İkinci içerik ise içerik filtreleme olarak görev alan kısımdır. Her ne kadar uygulama katmanında çalışan ayrı bir cihaz olarak günümüzde kullanılsa da güvenliğin önemli bir katmanıdır ve projede yer verilmiştir. Güvenlik duvarının içerik filtreleme kısmında "URL Ekle", "URL Çıkar" butonlarının yanındaki kutulara istenmeyen URL yazılıp, butona basarak dosyaya aktarılması ile filtrelenecek adresler hafızaya alınmaktadır. Böylece güvenlik duvarı uygulaması açılıp kapandığında istenmeyen URL listesi tutulmaya devam edecektir. Daha sonra bu dosyadan okunan adreslere erişim IPTABLES komutu ile engellenmektedir. Ticari ürünlerde sakıncalı içerik barındıran URL'ler ürüne ait veritabanlarında tutulmakta ve her gün çevrimiçi olarak listeleri yenilenmektedir. İçerik filtrelemenin kaynak kodları Ek-1 Güvenlik Duvarı Yazılım Kodlarında mevcuttur.

Üçüncü kısımda NAT işlemi ele alınmıştır. NAT kendi içinde SNAT ve DNAT olarak ikiye ayrılmaktadır. SNAT bir ağın tek bir legal IP ile genel ağa çıkarılması için gereken IP çevrim yöntemidir. Böylece hem daha az legal IP ile birçok bilgisayarın genel ağa erişimi sağlanmaktadır, hem de özel ağdaki bilgisayarların IP adresleri gizlenmiş olmaktadır. DNAT ise genel ağdan özel ağa gelen paketler için kullanılır. Gelen paketin hedef IP adresi belli olmadığı durumlarda bir port açılır ve o porta içerideki bilgisayarın IP adresi eşleştirilir. Böylece gelen paketler içeriye yönlendirilebilir hale gelir. Güvenlik duvarı uygulamasında SNAT özelliğinin kullanılabilmesi için SNAT butonu yanında

bulunan ilk kutuya özel ağın ağ adresi (örn: 10.1.1.0/24), ikinci kutuya ise hangi IP adresi ile saklanmak istediği yazılıp butona basmak gerekmektedir. Tez içinde bu işlemin sınaması yer almaktadır. Yapılan sınamada paketlerin kaynak IP adres değişikliği ağ trafik analiz araçları ile tespit edilmiştir. Eğer DNAT yapılmak istenirse güvenlik duvarındaki SNAT butonu yanında bulunan ilk kutuya port adresi (örn: 80), ikinci kutuya ise hangi IP adresine erişilmek istendiği yazılıp butona basılması yeterlidir. NAT işlemi için Netfilter'da PREROUTE ve POSTROUTE kural zincirleri kullanılmaktadır. NAT fonksiyonları kaynak kodları Ek-1 Güvenlik Duvarı Yazılım Kodlarında mevcuttur.

Dördüncü kısımda ise, güvenlik duvarının IP ve port filtreleme işlemi ele alınmıştır. Ağ geçidi olarak kullanılan güvenlik duvarının ağlar arasındaki paket filtrelemesini yapması için trafiğin hangi porttan aktığının bilinmesi gerekmektedir. Her ne kadar değiştirilebilir olsa da, varsayılan ayarlarda TCP'de ilk 1024 port bilinen portlardır (örn: Telnet portu 23'tür vs.). Güvenlik duvarının arayüzünde kaynak IP, hedef IP, port numarası ve alınacak aksiyon (örn: DROP, ACCEPT vs.) belirtilerek filtreleme işlemi yapılır. Paket filtrelemenin kaynak kodları Ek-1 Güvenlik Duvarı Yazılım Kodlarında mevcuttur.

Beşinci ve son kısımda ise güvenlik duvarının kayıt tutma özelliği ele alınmıştır ("Günlük butonu"). Bu butona basarak oluşan trafiğin kayıtları /var/log/message.log dosyasına alınmaya başlanır. Kayıt tutmanın kaynak kodları Ek-1 Güvenlik Duvarı Yazılım Kodlarında mevcuttur.

Güvenlik duvarları genel olarak ticari ürünler ve açık kaynak kod ürünler olarak ayrılabilir. Ticari güvenlik duvarları geçmişte güvenlik ve ağ mühendislerine büyük kurumlarda fonksiyonel olarak, yüksek performans, kararlı paket filtreleme, yönetim kolaylığı, otomatik yedeklilik ve yüksek güvenli operasyon sağlamışlardır. Büyük kurumlarda ürünlerin fiyatları bu

vasıflar karşısında göz önüne alınmamaktadır. Yine de verilen para ihtiyaç duyulan basit özelliklere göre daha yüksek olabilir [17]. Ucuz olması da açık kod güvenlik duvarlarının en büyük avantajıdır.

KAYNAKLAR

1. Tuxen, M., Rungeler, I., Stewart, R., Rathgeb, E., "Network Address Translation for the Stream Control Transmission Protocol", ***Network, IEEE***, 22 (5):26-32, (2008).

2. Tekin, F., "İnternet ve İleri Erişim Teknolojileri", Yüksek Lisans Tezi, ***Sakarya Üniversitesi Fen Bilimleri Enstitüsü***, Sakarya, 1-2, (2006).

3. Çölkesen, R., Örencik, B., "Bilgisayar Haberleşmesi ve Ağ Teknolojileri", ***Papatya Yayınları,*** İstanbul, 51-54, (1999).

4. Feit, S., "TCP/IP Architecture, Protocols, and Implementation with Ipv6 and Ip Security", ***McGraw-hill***, 307, (1999).

5. Stallings, W., "Data and Computer Communications", ***Prentice – Hall International, INC.,*** United States of America, 510-514, (1997).

6. Nazario, J., "DDoS Attack Evaluation", ***Network Security***, 2008 (7):7-10, (2008).

7. Nalini, N., Rao, G.R., "Attacks of Simple Blok Ciphers via Efficient Heuristics", ***Information Sciences***, 177 (12): 2553-2569 (2007).

8. Yapp, P., "Passwords: Use and Abuse", ***Computer Fraud & Security***, 2001 (9): 14-16, (2001).

9. Watson, D., "Web Application Attacks", ***Network Security,*** (10):10-14, (2007).

10. Yılmaz, D., "HACKING – Bilişim Korsanlığı ve Korunma Yöntemleri", ***Hayat Yayıncılık,*** İstanbul, 41-45, (2005).

11. Dirican, C. O., "Teori ve Uygulamalar ile TCP / IP ve Ağ Güvenliği", ***Açık Akademi Yayınları,*** İstanbul, 397-411, (2007).

12. Karabatak, G., “Açık Sistemdeki Güvenlik Duvarını Kullanarak Ağdaki Paketlerin Kontrolü”, Yüksek Lisans Tezi, ***Fırat Üniversitesi Fen Bilimleri Enstitüsü,*** Elazığ, 14-16, (2006).

13. Patton, S., Doss, D., Yurcik, W., “Open Source Versus Commercial Firewalls: Functional Comparison”, Proceedings 25th Conference on Local Computer Networks, **IEEE, Computer Society**, Tampa, Florida, (2000).

14. Lockhart, A., “Network Security Hacks”, ***O’Reilly***, United States of America, 117-118, (2006).

15. Hunt, C., “TCP/IP Network Administration, 3rd Edition”, ***O’Reilly***, United States of America, 427-430, (2002).

16. Vardar, M. A., “Linux Altında Programlama”, ***Papatya Yayınları***, İstanbul, 33-35, (2002).

17. Potter, B., “Open Source Firewall Alternatives”, ***Network Security*****,** (1): 16-17, (2006).

EKLER

EK-1. Güvenlik Duvarı Yazılımı Kodları

```
#include <gtk/gtk.h> //GTK Kütüphanesi#include <stdio.h>#include <string.h>

int main( int argc,char *argv[] ) //Main Fonksiyonu{GtkWidget*window,*frame,*ping_buton,*url_filtreleme_buton_ekle,*trafik_engelle_buton,*gelen_trafik_engelle_buton,*portGtkWidget *giden_trafik_engelle_buton,*port_taramasini_engelle_buton,*dos_saldirilarini_engelle_buton,*url_filtreleme_bGtkWidget *mac_eng_buton,*gunluk_buton,*snat_buton,*dnat_buton,*natsil_buton,*fw_buton_ekle,*fw_buton_cikar,*kural_kayi

Pencere,çerçeve, buton tanımlaması

GtkWidget *url_filtreleme_edit_ekle,*url_filtreleme_edit_cikar,*hata_mesaji_edit,*port_ac_edit,*port_kapat_edit,*mac_en

Editbox tanımlamaları

GtkWidget *yonlendir_kaynak_edit_ekle,*yonlendir_hedef_edit_ekle,*fw_kaynak_edit,*fw_hedef_edit,*fw_aks_edit,*fw_port_e

GtkWidget *url_filtreleme_listbox,*list,*firewall_kural_listbox; //Listbox tanımlamaları

gtk_init (&argc, &argv );

window = gtk_window_new (GTK_WINDOW_TOPLEVEL ); //Pencere Oluşturuyorgtk_window_set_position(GTK_WINDOW(window), GTK_WIN_POS_CENTER); //Pencereyi ekranın ortasına alıyorgtk_window_set_default_size(GTK_WINDOW(window), 1250, 1180); //Pencerenin boyutunu ayarlıyorgtk_window_set_title(GTK_WINDOW(window), "GUVENLIK DUVARI"); //Pencereye isim veriyor

frame = gtk_fixed_new(); //Çerçeve oluşturuluyorgtk_container_add(GTK_CONTAINER(window), frame); //Çerçeveyi, Pencerenin üzerine alıyor
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
hata_mesaji_edit=gtk_entry_new();          //Editbox          özellik
girişigtk_widget_set_size_request(hata_mesaji_edit,          190,
35);gtk_fixed_put(GTK_FIXED(frame), hata_mesaji_edit, 50, 600);

port_ac_edit=gtk_entry_new();gtk_widget_set_size_request(port_ac_edit,
190, 35);gtk_fixed_put(GTK_FIXED(frame), port_ac_edit, 250, 290);

port_kapat_edit=gtk_entry_new();gtk_widget_set_size_request(port_kapat
_edit, 190, 35);gtk_fixed_put(GTK_FIXED(frame), port_kapat_edit, 250,
330);

mac_eng_edit=gtk_entry_new();gtk_widget_set_size_request(mac_eng_edi
t, 190, 35);gtk_fixed_put(GTK_FIXED(frame), mac_eng_edit, 250, 370);

url_filtreleme_edit_ekle=gtk_entry_new();gtk_widget_set_size_request(url
_filtreleme_edit_ekle,      190,      35);gtk_fixed_put(GTK_FIXED(frame),
url_filtreleme_edit_ekle, 400, 50);

url_filtreleme_edit_cikar=gtk_entry_new();gtk_widget_set_size_request(ur
l_filtreleme_edit_cikar,      190,      35);gtk_fixed_put(GTK_FIXED(frame),
url_filtreleme_edit_cikar, 400, 90);

yonlendir_kaynak_edit_ekle=gtk_entry_new();gtk_widget_set_size_reques
t(yonlendir_kaynak_edit_ekle,          190,
35);gtk_fixed_put(GTK_FIXED(frame), yonlendir_kaynak_edit_ekle, 730,
50);

yonlendir_hedef_edit_ekle=gtk_entry_new();gtk_widget_set_size_request(
yonlendir_hedef_edit_ekle,  190,  35);gtk_fixed_put(GTK_FIXED(frame),
yonlendir_hedef_edit_ekle, 930, 50);

fw_kaynak_edit=gtk_entry_new();gtk_widget_set_size_request(fw_kaynak
_edit, 160, 35);gtk_fixed_put(GTK_FIXED(frame), fw_kaynak_edit, 730,
210);

fw_hedef_edit=gtk_entry_new();gtk_widget_set_size_request(fw_hedef_ed
it, 160, 35);gtk_fixed_put(GTK_FIXED(frame), fw_hedef_edit, 890, 210);
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
fw_aks_edit=gtk_entry_new();gtk_widget_set_size_request(fw_aks_edit,
70, 35);gtk_fixed_put(GTK_FIXED(frame), fw_aks_edit, 1120, 210);

fw_port_edit=gtk_entry_new();gtk_widget_set_size_request(fw_port_edit,
70, 35);gtk_fixed_put(GTK_FIXED(frame), fw_port_edit, 1050, 210);

list=gtk_list_new();                    //Listbox                    özellik
girişigtk_list_set_selection_mode(GTK_LIST(list),
GTK_SELECTION_SINGLE);gtk_container_add(GTK_CONTAINER(wi
ndow),                list);gtk_widget_set_size_request(list,                190,
135);gtk_fixed_put(GTK_FIXED(frame), list, 400, 140);gtk_widget_show
(list);

firewall_kural_listbox=gtk_list_new();gtk_list_set_selection_mode(GTK_
LIST(firewall_kural_listbox),
GTK_SELECTION_SINGLE);gtk_container_add(GTK_CONTAINER(wi
ndow),
firewall_kural_listbox);gtk_widget_set_size_request(firewall_kural_listbox
, 460, 135);gtk_fixed_put(GTK_FIXED(frame), firewall_kural_listbox,
730, 290);gtk_widget_show (firewall_kural_listbox);

/*FILE *dg;char satir[20];char *c;dg=fopen("/tmp/url.txt","r");GtkWidget
*list_item;do{

c=fgets(satir,20,dg);
if(c!=NULL)

{
list_item=gtk_list_item_new_with_label(c);gtk_container_add(GTK_CON
TAINER(list), list_item); gtk_widget_show(list_item);

}

}while(c!=NULL); fclose(dg);*/

void Ping_engelle() //Ping engelle fonksiyonu

BU FONKSİYON İLE PING ENGELLENMEKTEDİR
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
void Trafik_engelle() //Trafik engelle fonksiyonu

BU FONKSİYON İLE GELEN GİDEN TRAFİK ENGELLENMEKTEDİR

void Gelen_trafik_eng() //Gelen Trafik engelle fonksiyonu

BU FONKSİYON İLE GELEN TRAFİK ENGELLENMEKTEDİR

void Giden_trafik_eng() //Giden Trafik engelle fonksiyonu

BU FONKSİYON İLE GİDEN TRAFİK ENGELLENMEKTEDİR

void Dos_eng() //DoS ataklarını engelle fonksiyonu

BU FONKSİYON İLE SYN BOMBARDIMAN ATAĞI ENGELLENMEKTEDİR

void Port_eng() //Port taramalarına karşı engelleme fonksiyonu
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

BU FONKSİYON İLE PORT TARAMA (XMAS VE NULL YÖNTEMLERİ İÇİN) ENGELLENMEKTEDİR

```
void Port_ac() //Port açma fonksiyonu
```

BU FONKSİYON İLE PORT AÇILMAKTADIR

```
void Port_kapat() //Port kapatma fonksiyonu
```

BU FONKSİYON İLE PORT KAPATILMAKTADIR

```
void Mac_eng() //MAC engelle fonksiyonu
```

BU FONKSİYON İLE MAC ADRESİNE GÖRE TRAFİK ENGELLENMEKTEDİR

```
void Gunluk() //LOG tutma fonksiyonu
```

BU FONKSİYON İLE TRAFİK KAYITLARI TUTULMAKTADIR

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
void url_ekle() //URL engelleme için blacklist'e url ekleme fonksiyonu

BU FONKSİYON İLE URL ENGELLENMEKTEDİR

void url_cikar() //URL çıkartma için blacklistten url çıkarma fonksiyonu

BU FONKSİYON İLE ENGELLENEN URL'YE İZİN VERİLMEKTEDİR

void Snat() //Source NAT fonksiyonu

BU FONKSİYON İLE SNAT UYGULANMAKTADIR

void Dnat() //Destination NAT fonksiyonu

BU FONKSİYON İLE DNAT UYGULANMAKTADIR

void Natsil() //Oluşturulan NAT ları silme fonksiyonu

BU FONKSİYON İLE UYGULANAN NAT'LAR SİLİNMEKTEDİR
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
void kural_kayit() //Kuralların kaydedilmesi fonksiyonu

BU FONKSİYON İLE UYGULANAN KURALLAR KAYDEDİLMEKTEDİR

void kural_sil() //Kural sil fonksiyonu

BU FONKSİYON İLE UYGULANAN KURALLAR SİLİNMEKTEDİR

void Fw_ekle() //Fw kural ekleme fonksiyonu

BU FONKSİYON İLE GÜVENLİK DUVARINA KURAL EKLENMEKTEDİR

void Fw_cikar() //Fw kural çıkarma fonksiyonu

BU FONKSİYON İLE GÜVENLİK DUVARINDAN KURAL ÇIKARILMAKTADIR

 ping_buton=gtk_button_new_with_label("Ping Engelle"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(ping_buton, 190, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), ping_buton, 50, 50); //Butonun çerçeve üzerindeki yeri belirleniyor
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
g_signal_connect(ping_buton,
"clicked",G_CALLBACK(Ping_engelle),""); //Ping_Engelle fonksiyonu
çağrılıyor

trafik_engelle_buton=gtk_button_new_with_label("Tüm Trafiği Engelle");
//Yeni buton oluşturulup isim
veriliyorgtk_widget_set_size_request(trafik_engelle_buton, 190, 35);
//Butonun size'ı belirleniyor
gtk_fixed_put(GTK_FIXED(frame),trafik_engelle_buton, 50, 90);
//Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(trafik_engelle_buton,
"clicked",G_CALLBACK(Trafik_engelle),""); //Trafik engelle fonksiyonu
çağrılıyor

gelen_trafik_engelle_buton=gtk_button_new_with_label("Gelen Trafiği
Engelle"); //Yeni buton oluşturulup isim
veriliyorgtk_widget_set_size_request(gelen_trafik_engelle_buton, 190, 35);
//Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame),
gelen_trafik_engelle_buton, 50, 130); //Butonun çerçeve üzerindeki yeri
belirleniyor

g_signal_connect(gelen_trafik_engelle_buton,
"clicked",G_CALLBACK(Gelen_trafik_eng),""); //Gelen trafik engelle
fonksiyonu çağrılıyor

giden_trafik_engelle_buton=gtk_button_new_with_label("Giden Trafiği
Engelle"); //Yeni butonoluşturulup isim veriliyor
gtk_widget_set_size_request(giden_trafik_engelle_buton, 190, 35);
//Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame),
giden_trafik_engelle_buton, 50, 170); //Butonun çerçeve üzerindeki yeri
belirleniyor

g_signal_connect(giden_trafik_engelle_buton,
"clicked",G_CALLBACK(Giden_trafik_eng),""); //Gidentrafik engelle
fonksiyonu çağrılıyor
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
port_taramasini_engelle_buton=gtk_button_new_with_label("Port Taramalarını Engelle"); //Yeni butonoluşturulup isim veriliyorgtk_widget_set_size_request(port_taramasini_engelle_buton, 190, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame),

port_taramasini_engelle_buton, 50, 210); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(port_taramasini_engelle_buton, "clicked",G_CALLBACK(Port_eng),""); //günlük tut

dos_saldirilarini_engelle_buton=gtk_button_new_with_label("Dos Saldırılarını Engelle"); //Yeni buton oluşturulup isim veriliyorgtk_widget_set_size_request(dos_saldirilarini_engelle_buton, 190, 35);

//Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), dos_saldirilarini_engelle_buton, 50, 250); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(dos_saldirilarini_engelle_buton, "clicked",G_CALLBACK(Dos_eng),"");

port_ac_buton=gtk_button_new_with_label("Port Aç"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(port_ac_buton, 190, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), port_ac_buton, 50, 290); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(port_ac_buton, "clicked",G_CALLBACK(Port_ac),"");

port_kapat_buton=gtk_button_new_with_label("Port Kapat"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(port_kapat_buton, 190, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), port_kapat_buton, 50, 330); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(port_kapat_buton, "clicked",G_CALLBACK(Port_kapat),"");
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
mac_eng_buton=gtk_button_new_with_label("MAC Adresi Engelle"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(mac_eng_buton, 190, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), mac_eng_buton, 50, 370); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(mac_eng_buton, "clicked",G_CALLBACK(Mac_eng),"");

url_filtreleme_buton_ekle=gtk_button_new_with_label("URL Ekle"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(url_filtreleme_buton_ekle, 100, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), url_filtreleme_buton_ekle, 290, 50); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(url_filtreleme_buton_ekle, "clicked",G_CALLBACK(url_ekle),"");

url_filtreleme_buton_cikar=gtk_button_new_with_label("URL Çıkar"); //Yeni buton oluşturulup isim veriliyor

gtk_widget_set_size_request(url_filtreleme_buton_cikar, 100, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), url_filtreleme_buton_cikar, 290, 90); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(url_filtreleme_buton_cikar, "clicked",G_CALLBACK(url_cikar),"");

gunluk_buton=gtk_button_new_with_label("Günlük"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(gunluk_buton, 100, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), gunluk_buton, 1090, 600); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(gunluk_buton, "clicked",G_CALLBACK(Gunluk),"");

natsil_buton=gtk_button_new_with_label("NAT Sil"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(natsil_buton, 100,
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), natsil_buton, 620, 130); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(natsil_buton, "clicked",G_CALLBACK(Natsil),"");

snat_buton=gtk_button_new_with_label("SNAT"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(snat_buton, 100, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), snat_buton, 620, 50); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(snat_buton, "clicked",G_CALLBACK(Snat),"");

dnat_buton=gtk_button_new_with_label("DNAT"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(dnat_buton, 100, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), dnat_buton, 620, 90); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(dnat_buton, "clicked",G_CALLBACK(Dnat),"");

fw_buton_ekle=gtk_button_new_with_label("FW Kural Ekle"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(fw_buton_ekle, 100, 35);

//Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), fw_buton_ekle, 620, 210); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(fw_buton_ekle, "clicked",G_CALLBACK(Fw_ekle),"");

fw_buton_cikar=gtk_button_new_with_label("FW Kural Çıkar"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(fw_buton_cikar, 100, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), fw_buton_cikar, 620, 250); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(fw_buton_cikar,
"clicked",G_CALLBACK(Fw_cikar),"");

kural_kayit_buton=gtk_button_new_with_label("Kural Kayıt"); //Yeni buton oluşturulup isim veriliyor
```

EK-1. (Devam) Güvenlik Duvarı Yazılımı Kodları

```
gtk_widget_set_size_request(kural_kayit_buton, 100, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), kural_kayit_buton, 1090, 520); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(kural_kayit_buton,
"clicked",G_CALLBACK(kural_kayit),"");

kural_sil_buton=gtk_button_new_with_label("Kuralları Sil"); //Yeni buton oluşturulup isim veriliyor gtk_widget_set_size_request(kural_sil_buton, 100, 35); //Butonun size'ı belirleniyor gtk_fixed_put(GTK_FIXED(frame), kural_sil_buton, 1090, 560); //Butonun çerçeve üzerindeki yeri belirleniyor

g_signal_connect(kural_sil_buton,
"clicked",G_CALLBACK(kural_sil),"");

gtk_widget_show_all(window); //Pencere üzerindeki bileşenler gösteriliyor
gtk_main ( ); return0; }
```

ÖZGEÇMİŞ

Soyadı, Adı	: BAŞKAYA Onur
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 26.04.1978
Medeni hali	: Evli
Telefon	: 0 (312) 313 80 25
e-mail	: baskayaonur@gmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	İstanbul Ünv. / Elektrik-Elektronik Müh.	2002
Lise	Ankara Atatürk Anadolu Lisesi	1996

İş Deneyimi

Yıl	**Yer**	**Görev**
2003-2004	Probil A.Ş.	Uzman
2004-2006	Erdemir A.Ş.	Mühendis
2006-2008	T.C. Dışişleri Bakanlığı	Haberleşme Mühendisi
2008-	Türk Telekom A.Ş.	Uzman

Yabancı Dil

İngilizce

Hobiler

Satranç, Spor, Bilgisayar Teknolojileri