İSTANBUL ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

BİTİRME PROJESİ 1

SIFIR GÜN SALDIRISI VE DOS

Hazırlayanlar : Anıl Ertürk 1358130030

Danışman : Yrd.Doç.Dr. M.Ali AYDIN

HAZİRAN - 2018

ÖNSÖZ

İnternet hayatın her alanında kullanılmaktadır. Gittikçe daha da çok kullanılmaktadır. İnternet %100 güvenli olması için inşa edilemez çünkü bilgi paylaşımının bu kadar kolay ve hızlı olması ve aynı anda internetin güvenlik gibi diğer özelliklerininde mükemmel olması imkansızdır. tavizler verilmek zorundadır ve sonuç günümüz internetidir. Tabiki kurulmuş internet sistemini/protokolünü bilen ve zayıf noktalara saldıran insanlar her zaman olacaktır.

Yazılım sistemleri ilk kuruldukları zaman en zayıf oldukları zamandır. Çünkü zaman geçtikçe hatalar ve eksikler düzeltilecektir. İlk hali yazılımın çeşitli saldırılara en açık olduğu hallerden birisidir.

Anıl Ertürk 1358130030

İÇİNDEKİLER

ÖNSÖZ ..... **II**

İÇINDEKILER ..... **III**

ŞEKIL LISTESI ..... **IV**

TABLO LİSTESİ ..... **V**

KISALTMA LİSTESİ ..... **V**

ÖZET ..... **VIII**

SUMMARY ..... **VIIII**

1. GİRİŞ **1**

2. GENEL KISIMLAR……..…**3**

2.1. İNTERNET ALTYAPISI……..3

3. KULLANILAN ARAÇ VE YÖNTEM **2**

3.1.1. Kullanılan Programlama Dilleri ve Platformlar 2

4. TARTIŞMA VE SONUÇ……...**6**

KAYNAKLAR……**9**

ŞEKİL LİSTESİ

Şekil 2.1 : Internet Layers……1
Şekil 2.1 : Server……..5
Şekil 2.1 : Client1……6
Şekil 2.1 : Client2……7

TABLO LİSTESİ

Tablo 3.1 : Projedeki paketler ve onların içlerindeki sınıflar…….5
Table 3.2 : Projedeki paketler ve onlarin içlerindeki sınıflar…….5

KISALTMA LİSTESİ

DOS	**:**	Denial Of Service
IP	**:**	Internet Protocol
HTTP	**:**	HyperText Transfer Protocol
GUI	**:**	Graphics User Interface
TCP	**:**	Transmission Control Protocol
IDE	**:**	Integrated Development Environment

ÖZET

SIFIR GÜN SALDIRISI VE DOS

İnternet çok kısa bir süre içerisinde çok geniş bir kitleye yayıldı ve hiçbiryere gitmiyor. İnternetin popülerliğiyle beraber artan istismar, güvenlik sorunları ve bunlarla başa çıkan güvenlik mekanizmalarında birçok gelişmeye neden olmuştur.

Sifir gün saldirisi bilgisayar sektöründeki genel bir terimdir. Sistemlerin güven zafiyetleri ve özellikle yeni sistemlerin güvenlik zafiyetlerini konu alir. Yazilim sektörü doğasi gereği başta en saldiriya açik haldedir ve zaman geçtikçe açiklar kapatilir. Diğer mühendislik dallarindan farklidir.

Günümüzde bilgisayar ağ sistemleri client-server bazlı ve multithreadded'dır. Yani istemciler sunucularla konuşur. Sunucular birden fazla istemciyle, istemciler birden fazla sunucu ile aynı anda iletişim kurabilir.

DOS saldırısı eğer önlem alınmadıysa sıfır gün saldırısı olabilir ve bu multithreaded internet sistemlerini çeşitli yollarla yavaşlatmayı veya durdurmayı amaçlar.

SUMMARY

ZERO DAY ATTACK AND DOS

Internet spread too a very large userbase in a very short time and it is going nowhere. With the popularity came the exploitation, security problems and mechanizms to deal with these problems.

Zero day attack is a general term in computer business. It’s about security vulnerabilities of computer systems and especially new computer systems. Software business is the most vulnerable to attacks when its first setup because of its nature. One of the differences of software business compared to other engineering areas.

In todays world the internet is mostly client-server based and multithreaded. Client talks to server. Server talks to multiple clients. Of course clients can talk to more than one server if they want to.

DOS attack can be a zero day attack if not prevented and it aims to slow down or stop these multithreaded internet systems.

1. GİRİŞ

1.1 Neden internet mükemmel güvenliğe sahip değil?

Eskiden bilgisayarlar büyük, pahalı ve nadirdi. Sadece birkaç üniversitede, akademisyenler tarafından iletişim amaçlı kullanılıyordu. Dolayısı ile bilgisayar ağları hiçbir zaman bugünkü koşullar düşünerek hazırlanmadığı için, doğasında birçok güvenlik zafiyeti vardır. Hem mükemmel güvenliğe sahip hemde günümüzdeki gibi kolay ve hızlı veri iletişimine sahip olmak mümkün değildir. Dolayısı ile taviz verilmek zorundadır. Nasıl bisikletimizi basit bir kilitle kitliyorsak, evimize çelik kapı koyuyorsak ve banka parayı silahla koruyorsa, bilgisayar sektöründede her kişi ve kurum gerektiği kadar güvenlik kullanır. Mümkün olduğunca verimli sistemler ekleyerek bu bilgisayar ağları ayakta tutulmaya devam ediliyor. Buna iyi bir örnek şifrelemesi kolay ama anahtarı bilmeden deşifrelemesi zor olan kriptolojilerdir.

1.2 Sıfır gün saldırısı(Zero day attack) ve yazılım sistemlerinin doğası

Sıfır gün saldırısı bilgisayar sektöründeki genel bir terimdir. Sistemlerin güven zafiyetleri ve özellikle yeni sistemlerin güvenlik zafiyetlerini konu alır. Yazılım sektörü doğası gereği başta en saldırıya açık haldedir ve zaman geçtikçe açıklar kapatılır. Diğer mühendislik dallarından farklıdır. Diğer mühendislik dallarında sistemle ilgili herşey ilk başta tasarlanır ve bir kerede inşa edilir. Yazılım sektöründede non structural, non functional bir kod düşünürseniz bu kodda daha sonra değiştirmeye pek açık olmayan, herşeyin birbiriyle direk olarak iç içe olduğu bir sistemdir. Ama bu kadar eski stil, verimsiz, yazılımcılar tarafından kaçınılan/kötülenen bir yazılım stili bile üzerinde çalışması zor olsada yeni dosyayı eski dosya ile değiştirmek kolaydır. Ki dediğimiz gibi bu tarz kötü yazılım stilleri kullanılmaz. Üzerinde çalışması kolay modüler, yapısal, nesneye yönelik yazılım stilleri kullanılır. Dolayısı ile yazılım sektörü çalışan parçaları teker teker yapıp eklemeye, parçaları değiştirmeye çok ama çok yatkın bir sektördür. Bir köprü inşa etmekle çok farklıdır. Ayrıca sistemler diğer mühendislik sektörlerine göre daha karmaşıktır, içerdiği her parçanın herşeyle her türlü etkileşimini bilmek imkansız olduğu için hatalar sıktır. Milyonlarca satır koda sahip sistemler vardır. Bu bilindiği için yazılım yazılırken modüler bir şekilde, her modüle kullandığı veri tipini verecek şekilde yazılım dizayn edilir. Ayrıca testler yapılır.

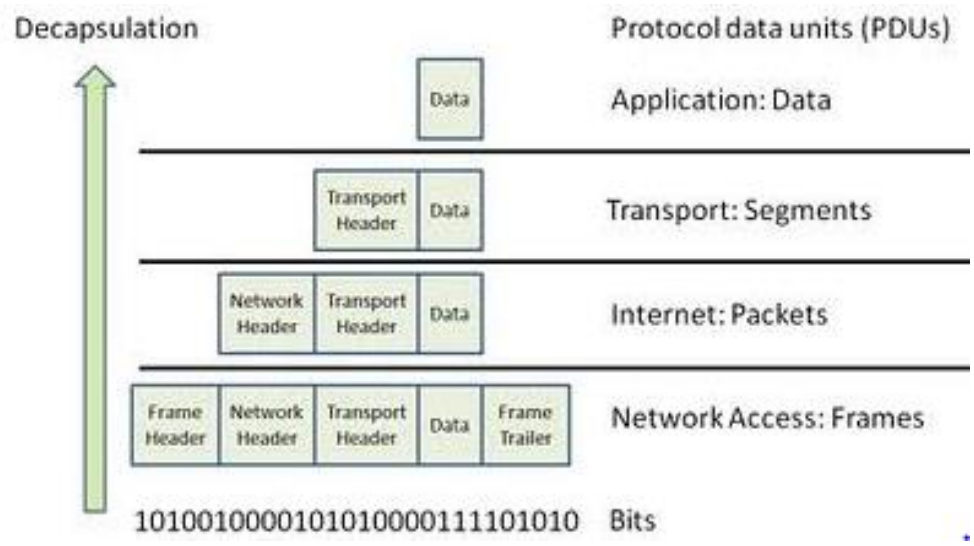
Günümüzde bilgisayar ağ sistemleri client-server bazlı ve multithreadded'dır. Yani istemciler sunucularla konuşur. Sunucular birden fazla istemciyle, istemciler birden fazla sunucu ile aynı anda iletişim kurabilir. Dolayısı ile ben projemde client-server şeklinde çalışan multithreadded serverlara bilgisayar ağlarının ve bilgisayar ağlarını kullanan sistemlerin zayıf noktalarını kullanarak saldırı yöntemlerini göstereceğim ve aynı anda bu saldırı yöntemlerinin firewall mantığı ile nasıl durdurulabileceğini göstereceğim.

Network yapısını nasıl güvenlik amaçlı kullanıp ve kurduğumuz sistemlerin nasıl mümkün olduğunca güvenli olmasını sağladığımızı gösterebilriz. Transport seviyesinde portların zayıf noktalarını gösterebiliriz. Bir client'in yaptığı işlemleri analiz edip zararlı olduğuna karar verirsek server'ı meşgul etmesini önleyebiliriz.

Port ve IP, yani soket kullanarak farklı soketler farklı clientlara hizmet veriyor. Client sayısı arttıkça thread sayısı artıyor. Bilgisayar ağlarının sıkıntılarından birisi sınırlı kaynak(port, server donanımı, vs.). Bilgisayar ağlarından saldırı yapılırkende saldırının yapıldığı sistemin naıl işlediği bilindiği için bu istismar edilerek saldırılıyor. Ve çoğu zaman sistem yapılan işlemleri sıradan işlemler sanıyor. Bunların özellikle tesbit edilmesi içinde firewall gibi sistemler kullanılıyor.

2. GENEL KISIMLAR

2.1. İNTERNET ALTYAPISI



Şekil 2.1 : Internet Layers

İnternette kaynak sınırlıdır. Dolayısı ile HTTP connection, port sayısı sınırlıdır. Ayrıca server'ın işlemci kapasitesi ve internet bant genişliği sınırlıdır. Dolayısı ile biz bu sistemlerin altında yatan zayıflıkları kullanarak saldırı yapabiliriz.

3. KULLANILAN ARAÇ VE YÖNTEM

3.1. SİMÜLASYON

3.1.1. Kullanılan Programlama Dilleri ve Platformlar

Hem geliştirme hem test için Netbeans IDE'sini kullandık. Glassfish open-source full application server kullandık internet ortamını simüle etmek için.

Programlamada, Sun firmasına ait Java platformunun, Java2 SDK 1.8.172 Standart Edition ürünü kullanılmıştır. Java'nın tercih edilmesinin sebebi, çalışma grubunun diğer programlama dillerine göre daha yatkın olması ve nesne yönelimli olması gösterilebilir. Özellikle, proje kodları yazılırken, nesne yönelimli programlamanın sunduğu daha standardize kod yazabilme olanağı ve bunun getirdiği daha rahat çözümler üretebilme kod yazımını kolaylaştırmıştır. Ayrıca, Java'nın tercih edilmesinin bir başka sebebi de, Java'nın içerdiği geniş paket kitaplığıdır. Kodların bazı kısımları, C gibi orta seviyeli programlama dilleri ile daha zor yazılabilecekken, Java ile bu kısımlar daha rahat gerçeklenmiştir.

Tablo 3.1 : Projedeki paketler ve onların içlerindeki sınıflar

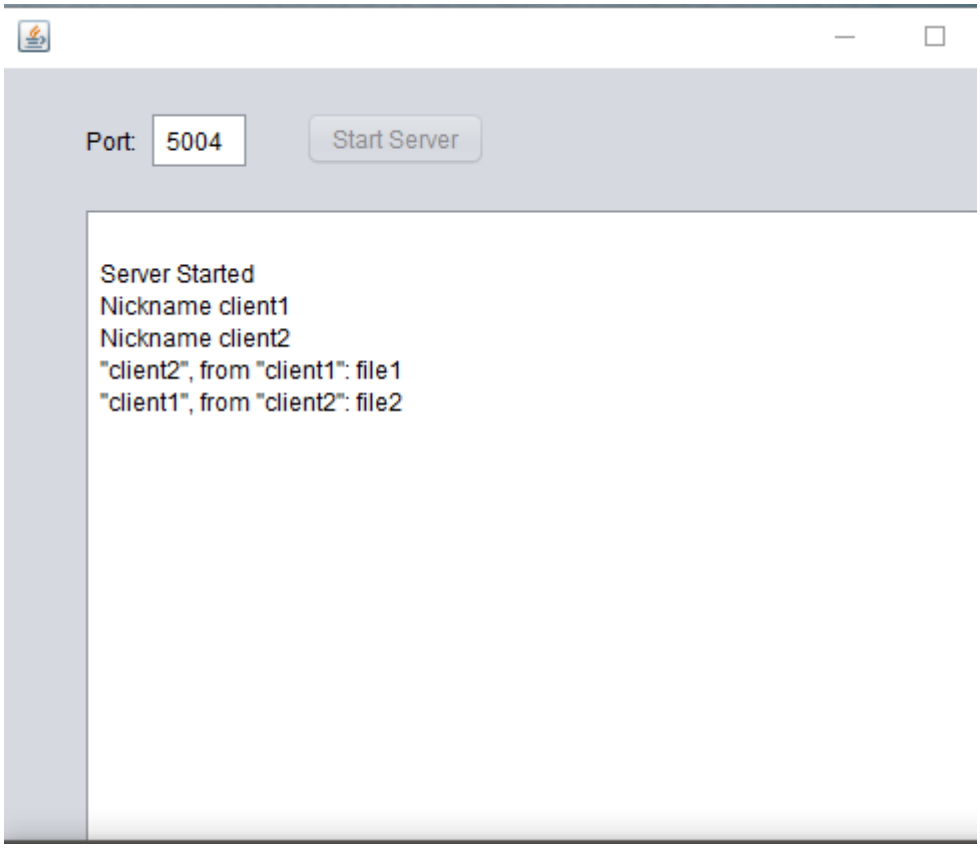
java.net	**java.util.concurrent**	**java.io**
Socket	ArrayBlockingQueue	IOException
InetAddress		
ServerSocket		

Tablo 3.2 : Projedeki paketler ve onların içlerindeki sınıflar

java.util.logging	**java.util**	**java.io**
Level	Scanner	PrintWriter
Logger	ArrayList	
	HashMap	

4. TARTIŞMA VE SONUÇ

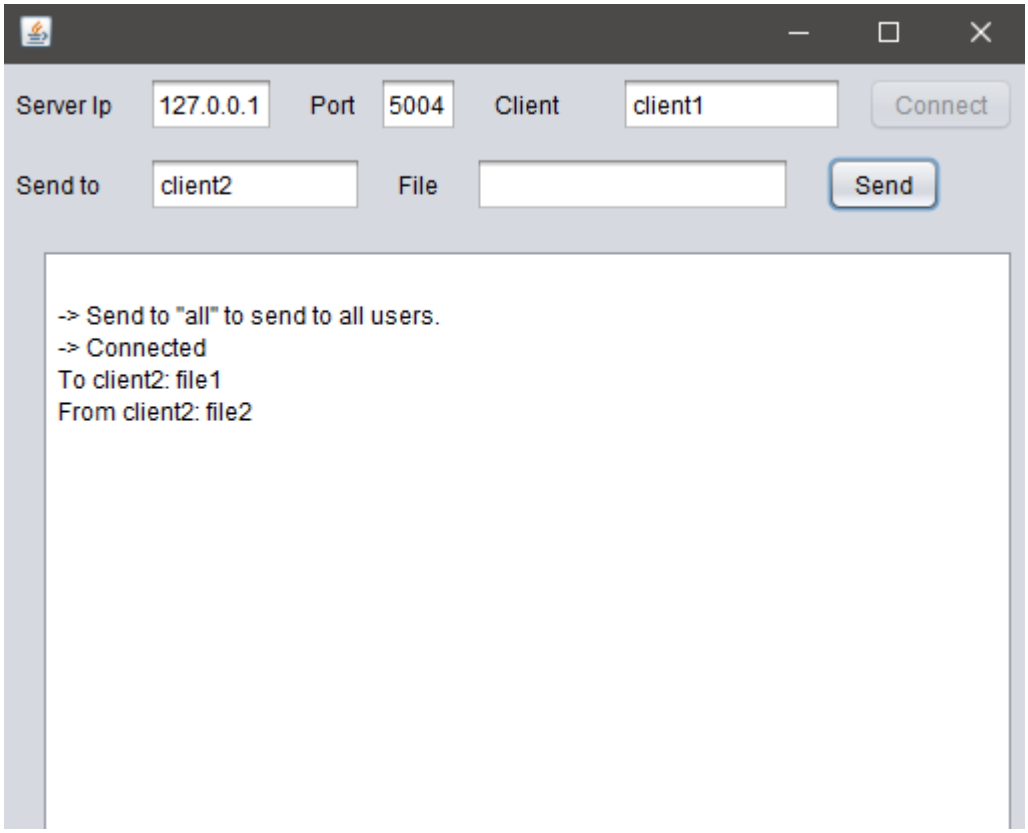
Swing GUI kullanarak arayüzümüzü oluşturduk. Input, output ve kontrolümüzü bu şekilde yapıyoruz.



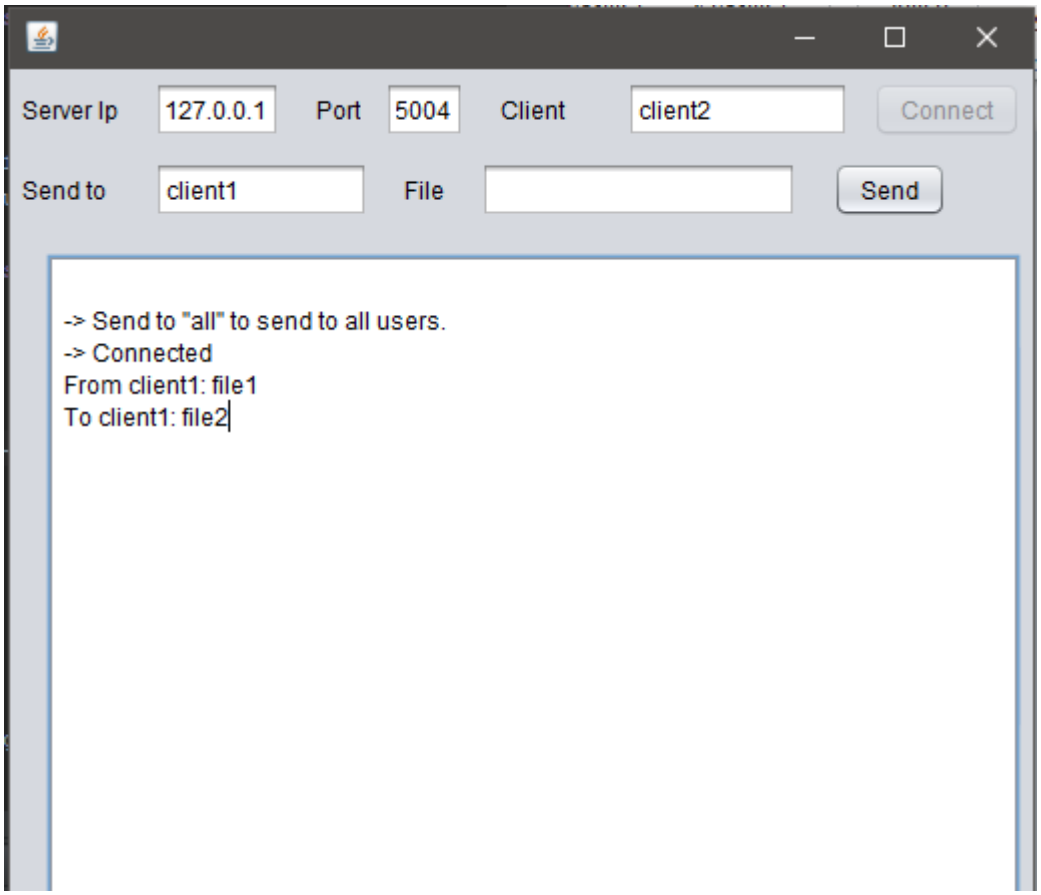
Şekil 2.2 Server

Programımız client-server mantığıyla çalışır. Transport seviyesinde kodlanmıştır. Dolayısı ile protokolde kodlanmıştır. Client ve server bilir birbirine bilgi göndereceğini ve bu bilgiyi okuyacağını çünkü iki tarafta programı kurmalıdır.

Program dosya aktarımı yapmaktadır TCP kullanarak. Server multi-threaded olduğu için birden çok client'a aynı anda servis verebilir.



Şekil 2.3 Client1



Şekil 2.4 Client2

Clientlar birbirine dosya gönderebilmek için birbirlerinin isimlerini kullanır. Client'lar aslında server ile konuşur, server'a gönderir dosyayı, server kendi içinde işlem yapar ve dosyayı gönderilecek adrese gönderir. Server ana ekranındada trafiği görebiliriz.

Sonuç olarak tek bir kaynaktan DOS saldırısı yapılınca server'ın tesbit edip bağlantıyı kesmesi kolaydır. Fakat birçok kaynaktan saldırı yaparsak bunun engellenmesi çok daha zordur. Server'ın kaynaklarını meşgul etmek server'ın gerçek client lar ile yaptığı bant genişliğini düşürür.

KAYNAKLAR

DEITEL, Paul, DEITEL, Harvey, 2015, Java How to Program, Pearson, USA, One Lake Street, Upper Saddle River New Jersey 07458, 0-13-380780-0