ISSN:1306-3111
e-Journal of New World Sciences Academy
2010, Volume: 5, Number: 2, Article Number: 1A0072

ENGINEERING SCIENCES
Received: March 2009
Accepted: March 2010
Series : 1A
ISSN : 1308-7231

Elmas Yıldız
Nursal Arıcı
Gazi University
nursal@gazi.edu.tr
Ankara-Turkey

GERÇEK ZAMANLI BİR SALDIRI TESPİT SİSTEMİ TASARIMI VE GERÇEKLEŞTİRİMİ

ÖZET

Bu çalışmada, gerçek zamanlı bir saldırı tespit sistemi olarak tasarladığımız ve gerçekleştirdiğimiz yazılım tanıtılmıştır. Bu sistem, DoS ataklarından biri olan Brute Force tipi bir saldırının tespit edilip engellenebilmesi için tasarlanmış, Visual Studio.NET 2005 C# programlama dili ve Microsoft Office 2007 Access kullanılarak gerçekleştirilmiştir. Uygulamada geliştirilen saldırı tespit sistemi saldırıyı IP tabanlı tespit etmesi ve gerçek zamanlı bir saldırı tespit sistemi olmasından dolayı önemlidir.

Anahtar Kelimeler: Saldırı Tespit Sistemleri, DoS Saldırıları, Brute Force atakları, Veri Madenciliği, Yapay Sinir Ağları

DESIGN AND IMPLEMENTATION OF A REAL TIME INTRUSION DETECTION SYSTEM

ABSTRACT

In this study, a developed software as a real time intrusion detection system has been introduced. This software has been designed and developed in order to detect and blocked the Brute Force Type attack which is one of DoS attacks. Proposed application has been developed by using the programming language C# on Microsoft Visual Studio .NET 2005 and Microsoft Office 2007 Access. The developed system as a real time detection system can make a IP based detection.

Keywords: Intrusion Detection Systems, DoS Attacks, Brute Force Attacks, Data Mining, Artificial Neural Networks

1. GİRİŞ (INTRODUCTION)

Saldırı, bilginin mahremiyetini, bütünlüğünü ve erişilebilirliğini tehlikeye atabilecek girişimlerin kümesi olarak tanımlanmaktadır [1]. Saldırı tespiti ise, bir bilgisayar sisteminde veya ağda meydana gelen olayları izleyerek, bilginin mahremiyetini, bütünlüğünü ve erişilebilirliğini bozmak ya da sistemin güvenlik mekanizmalarını aşmak için yapılan hareketler olarak tanımlanan saldırı işaretlerini analiz etme işlemidir [2].

Saldırı Tespiti Sistemleri (Intrusion Detection System), bilgisayar sistemlerine ve ağ kaynaklarına olan saldırıları tespit etmek, sistemi izleyip anormal olan durumları saptamak ve bunlara karşı gerekli önlemleri almayı amaçlayan güvenlik sistemleridir.

Veri madenciliği, büyük miktarlardaki verinin içinden geleceğin tahmin edilmesinde yardımcı olacak anlamlı ve yararlı bağlantı ve kuralların bilgisayar programları aracılığıyla aranması ve analizidir. Veri Madenciliği teknikleri ile büyük veri kümelerinden oluşan veritabanı sistemleri içerisinde gizli kalmış bilgilerin çekilmesi sağlanır. Bu işlem, istatistik, matematik disiplinleri, modelleme teknikleri, veritabanı teknolojisi ve çeşitli bilgisayar programları kullanılarak yapılır [3].

DoS (Denial Of Servise) saldırıları ağın veya cihazların hizmet dışı kalmasını sağlayan bir atak tekniğidir. DoS ataklarından biri olan Brute Force saldırısı ise sistemin kullanıcı hesabını ve şifresini kırmak için tahminlere dayalı deneme yanılma yöntemini kullanarak saldırı yapar.

Bu çalışma kapsamında veri madenciliği tekniğini kullanarak DoS ataklarından Brute Force tipi saldırıları IP tabanlı tespit eden gerçek zamanlı bir saldırı tespit sistemi yazılımı geliştirilmiştir. Amaç, tespit edilen IP adreslerinin sisteme girişini engellemek ve e-posta ile sistem yöneticisini bildirmektir. Bu amaç doğrultusunda geliştirilen saldırı tespit sistemi yazılımı kullanıcı adı, IP adresi, tarih ve saat gibi bilgileri sistem yöneticisine sunmaktadır.

2. ÇALIŞMANIN ÖNEMİ (RESEARCH SIGNIFICANCE)

Saldırı Tespit Sistemleri(STS) geliştikçe, yapılan saldırıların ve saldırı türlerinin de arttığı görülmüştür. STS'ler için geliştirilen literatürdeki uygulamalar incelendiğinde, araştırmacıların uygulamalarında statik bir veritabanı kullandıkları ve uygulama içinde bu veritabanının yeni saldırı türleri eklemeye uygun olmadığı tespit edilmiştir. Güncel bir veri kümesi olmayışı veya oluşturulamayışı STS'lerin başarısını engelleyen bir etken olarak karşımıza çıkmaktadır.

Gerçek zamanlı STS çalışmalarının pek çoğunda önceden hazırlanmış veri kümelerinin kullanılmış olduğu belirlenmiştir. Yapılan bu çalışma ile gerçek zamanlı bir STS tasarımının nasıl yapılabileceği, STS tasarımını yaparken kullanılabilecek güncel bir veri kümesinin nasıl oluşturulabileceği ile ilgili yaklaşımlar ortaya konulmaya çalışılmıştır. Uygulamada geliştirilen saldırı tespit sistemi saldırıyı IP tabanlı tespit etmesi ve gerçek zamanlı bir saldırı tespit sistemi olmasından dolayı önemlidir.

3. SALDIRI VE SALDIRI TİPLERİ (INTRUSION AND INTRUSION TYPES)

3.1. Saldırı Tanımı (Description of Intrusion)

Var olan bilgi ve bilgisayar güvenliği sistemini aşmak veya atlatmak, zafiyete uğratmak, kişileri doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemlerin işleyişini aksattırmak,

durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler, saldırı veya atak olarak adlandırılmaktadır [4].

Çalışmada ağ üzerinden yapılan saldırılardan biri olan Brute force tipi bir DoS saldırısı tespit edilmesi amaçlanmıştır. Bu atak türünün seçilmesinin nedeni, çok basit ve ilkel bir yöntem olmasına rağmen hala güncel bir saldırı tekniği olmasıdır. Bu özelliği en acemi korsanların bile DoS atakları düzenleyerek sistemleri kolayca kullanılmaz hale getirmelerine yol açmaktadır. DoS atakları arasından Brute Force tipi saldırının seçilmesinin nedeni ise veri madenciliği tekniği ile saldırı tespitinin rahatlıkla uygulanabilmesidir.

3.2. Saldırı Tipleri (Intrusion Types)

Ağ üzerinde yapılan saldırılar bilgi tarama, yönetici hesabı ile yerel oturum açma, Kullanıcı hesabının yönetici hesabına yükseltilmesi ve hizmet engelleme saldırıları olmak üzere dört kategoriye ayrılır.

Denial of Service (DoS) atakları Internet'e bağlı olan ağları ve cihazları hedef alır. Bu tip atakların amacı bilgiyi çalmak değil ağı veya cihazları iş göremez hale getirmektir [5].

DoS ataklarından biri olan ve çalışmamızda adı geçen Brute Force saldırıları sistemlerde kullanıcı hesaplarını ve şifreleri kırmak için tahminlere dayalı deneme yanılma yöntemiyle yapılan bir saldırı çeşididir. Burada amaç kullanıcının şifresini ele geçirmek ve sisteme o kullanıcı üzerinden sızmaktır. Sözlük saldırılarına çok benzer. Bir dosyadan tahmini şifreleri alır ve tek tek dener. Uygulamalarda bu tip saldırıları algılayan ve önlem alan bir sistem yoksa korsan, hesaba ait şifreyi bulana kadar saldırıya devam edebilir [6].

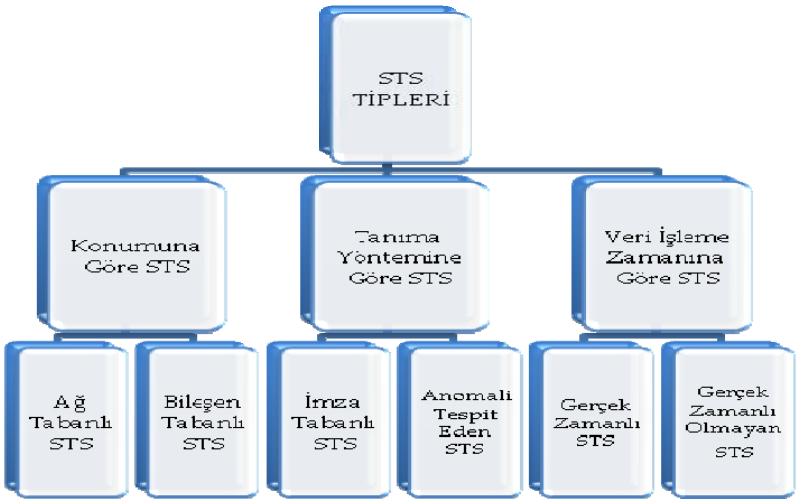
4. SALDIRI TESPİT SİSTEMLERİ (INSTRUSION DETECTION SYSTEMS)

4.1. Saldırı Tespit Sistemlerinin Tanımı (Description of Instrusion Detection Systems)

Saldırı Tespiti Sistemi(STS), bir sisteme karşı yapılan saldırıları tespit etme amaçlı kullanılan sistemlerdir. Burada asıl amaç, bir saldırı olduğunda bilgilendirme amaçlı uyarılar vermektir. Bu şekilde sistem yöneticileri potansiyel zayıf noktalardan ve sisteme karşı yapılan saldırılardan haberdar olabilir, buna uygun şekilde önlemler alabilirler. Kısaca STS, amacı uyarmak olan bir savunma sistemidir. Bu amaçla, bütün ağ trafiği STS tarafından dinlenebilir veya önemli bileşenler, bileşen bazında dinlenerek STS'ne yönlendirilebilirler (Şekil 1)[7].

4.2. STS'lerin Sınıflandırılması (Classification of Instrusion Detection Systems-IDS)

Saldırı tespit sistemleri; Şekil 1'de görüldüğü gibi konumuna, tanımına ve veri işleme zamanına göre sınıflandırılır. Çalışmada geliştirilen STS gerçek zamanlı bir saldırı tespit sistemidir. Saldırıyı tespit edip sistem yöneticisine e-posta yolu ile bildirimde bulunmaktadır.



Şekil 1. Saldırı Tespit Sistemleri Tipleri
(Figure 1. Types of Intrusion Detection Systems)

4.3. Saldırı Tespit Sistem Yazılımı Özellikleri (Properties of IDS Software)

- Bilgisayar sistemleri ve ağlar arasındaki trafiği dikkat çekmeden analiz edebilmelidir. Gizli (stealth) modunu desteklemelidir.
- Sisteme yapılan saldırılara karşı koyabilmeli ve ağ yöneticisine bildirebilmelidir.
- Gerçek zamanlı saldırı tespiti yapabilmelidir.
- Saldırı tespitlerini ağ ve işletim sistemlerini inceleyerek yapabilmelidir.
- Ağda dolaşan paketleri görüntüleyebilmeli ve saldırı içerikli olup olmadığını tespit edebilmelidir.
- Kullanıcı grafik ara yüzü ile kolayca yönetilebilmelidir.
- Saldırı durumunda konsola alarm gönderebilmeli (SNMP), e-posta atabilmeli, aktif oturumu görüntüleyebilmeli, raporlama yapabilmeli, saldırı tehdidi içeren bağlantıları kesebilmeli, durdurabilmelidir [8].

5. SALDIRI TESPİT SİSTEMİNDE KULLANILAN TEKNİKLER (TECHNIQUES APPLIED ON IDS)

STS'lerde, anormallik ve kötüye kullanım (imza) tabanlı yaklaşımları modellemek için günümüze kadar birçok teknik kullanılmıştır. Bu teknikler, elde edilen verilerin modellenmesi, sınıflandırılması veya kural tablolarının oluşturulması için geliştirilmiştir [9].

STS'lerinde kullanılan teknikler;

- Veri Madenciliği,
- Kural Tabanlı Sistemler,
- Tanımlayıcı İstatistikler,
- Eşik Değeri Tespiti,
- Durum Geçiş Analizi,
- Uzman Sistemler,
- Örüntü Eşleme.

5.1. Veri Madenciliğinde Kullanılan Modeller (Models Applied on Data Mining)

Veri madenciliği modelleri gördükleri işlevlere göre 3 ana başlık altında toplanabilir. Bunlar;

- Sınıflama ve Regresyon,
- Kümeleme,
- Birliktelik Kuralları ve Ardışık Zamanlı Örüntüler

Saldırı tespit sistemi çalışmamızda veri madenciliğinde kullanılan modellerden biri olan sınıflama modeli kullanılmıştır. Bu model içinde kullanılan yöntem ise yapay sinir ağlarıdır.

5.2. Yapay Sinir Ağları (Artifical Neural Network)

Yapay sinir ağı(YSA), dışarıdan gelen girdilere dinamik olarak yanıt oluşturma yoluyla bilgi işleyen, birbiriyle bağlantılı basit elemanlardan oluşan bilgi işlem sistemidir [10].

YSA'ların STS'lerde kullanımı, YSA'nın normal sistem davranış izleriyle eğitilmesi ile başlar. Normal veya anormal olarak sınıflandırılan olay akışları yapay sinir ağına verilir. Toplanan veriler ile sistemin davranışına bağlı olarak öğrenme değişimi yapılabilir. Yani eğitim, izin veriliyorsa sürekli hale getirilebilir. Buradaki yaklaşım, kullanıcının "n" adet hareket veya komutundan sonraki hareket veya komutunun tahminen eğitilmesidir. Bu tahminin yapılması için öncelikle eğitim veri seti oluşturulmalı, daha sonra da eğitim tamamlanmalıdır [9].

6. VERİ MADENCİLİĞİ İLE SALDIRI TESPİT YAZILIMI (APPLICATION SOFTWARE OF INTRUSION DETECTION USING DATA MINING)

Ağ güvenliğinin devamlı olarak sağlanmasının yolu, yetkisiz erişimleri gerçek zamanlı olarak tespit etmektir. Etkili bir saldırı tespit sistemi, atak ve şüpheli ağ erişimlerini etkin bir şekilde tespit ederek ağ güvenliğinin bir bacağını oluşturur. Ama bu istenmeyen trafiğin sadece saptanması yeterli değildir. Kullanılan saldırı tespit uygulamasından beklenen bir diğer özellik, belirlenecek bu tür istenmeyen bağlantılara anında yanıt verebilmeli ve ağ kaynaklarına yetkisiz erişimi engellemelidir.

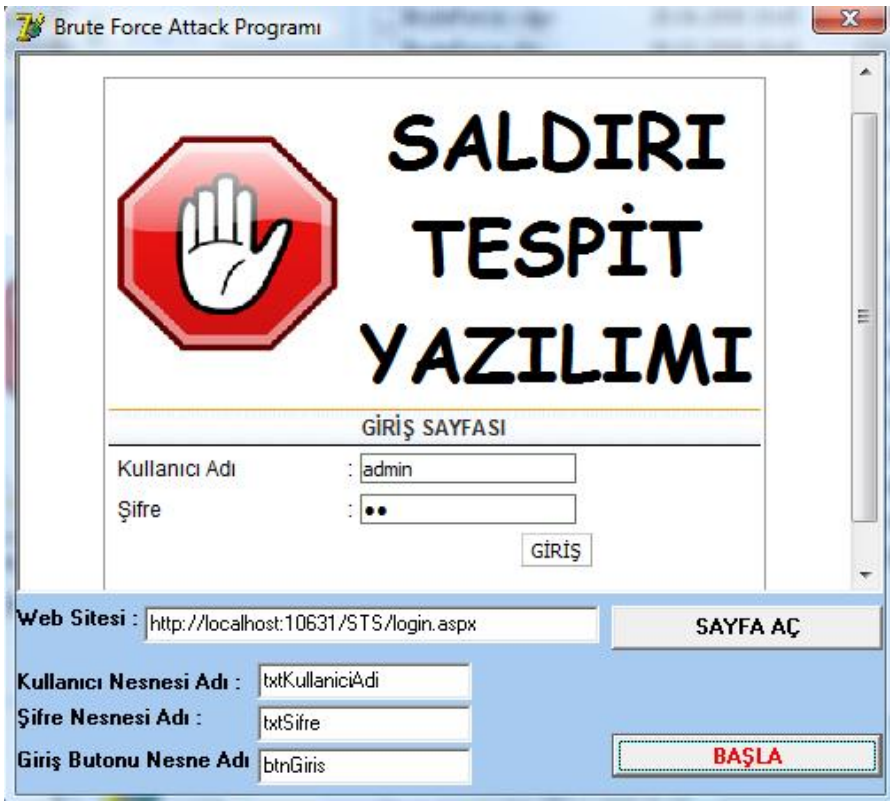
Bu makalede açıklanan saldırı tespit sistemi, gerçek zamanlı bir saldırı tespit sistemi olup Brute Force tipi saldırıları IP tabanlı tespit eder. Tespit edilen IP adreslerinin sisteme girişi engellenir ve e-posta ile sistem yöneticisine bildirilir. Ayrıca saldırı tespit sistemi uygulaması, sisteme yapılan her türlü erişimin kullanıcı adı, IP adresi, tarihi ve saati bilgilerini de yöneticiye sunmaktadır.

Saldırı tespiti için geliştirilen yazılımda kullanılan model sınıflamadır. Kullanılan yöntem ise YSA'dır. Bu yöntem aracılığı ile sisteme giriş yapmaya çalışan kullanıcıların saldırı yapıp yapmadıkları tespit edilmeye çalışılmıştır.

Uygulama için iki ayrı yazılım geliştirilmiştir. Bunlar; Brute Force saldırı yazılımı ve web tabanlı saldırı tespit yazılımlarıdır.

6.1. Brute Force Saldırı Yazılımı (Brute Force Attack Software)

Yazılım, Borland Delphi 7.0 programlama dili kullanılarak yazılmıştır. Kullanıcı girişli web sitelerine Brute Force saldırı yapmaktadır. Yazılımın ekran görüntüsü Resim 1'de gösterilmiştir.



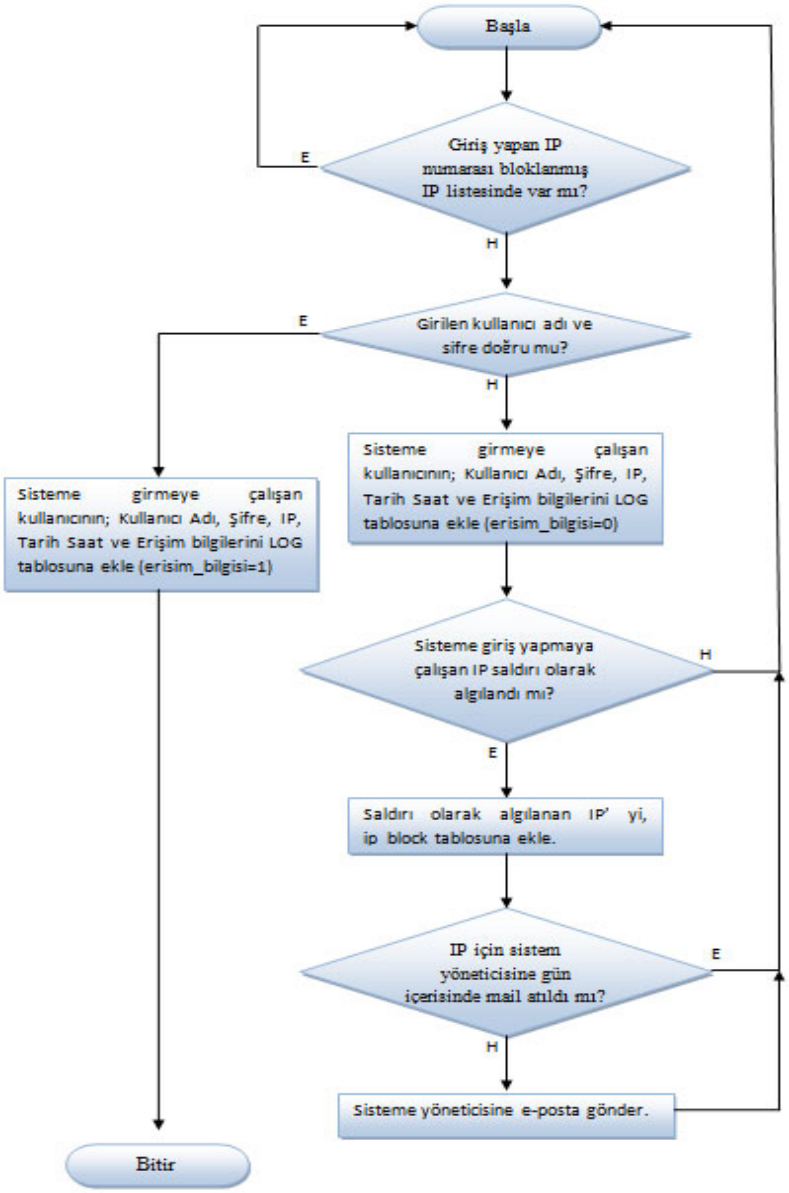
Resim 1. Brute Force saldırı yazılımı ekran görüntüsü
(Picture 1. Screenshot of the Brute Force attack software)

Yazılımda web sitesi adresi, kullanıcı adının yazılacağı nesne adı, şifrenin yazıldığı nesne adı ve sisteme giriş için tıklanacak butonun nesne adı parametre olarak girilir. Parametreler girildikten sonra "SAYFA AÇ" butonuna tıklanarak, adresi girilen web sayfası açılır. Parametre olarak kullanılan nesne adlarını tespit edebilmek için saldırı yapılacak web sitesi herhangi bir web tarayıcıda açılır. Açılan web sitesi üzerinde sağ tıklanıp "Kaynağı görüntüle" seçilerek web sayfasının kaynak kodlarına erişilir. Buradan kullanıcı adı, şifre ve giriş butonunun nesne adları alınarak yazılıma parametre olarak girilir.

"BAŞLA" butonuna basıldığı anda yazılım içerisinde açılan web sitesine Brute Force saldırı başlar. Bu saldırıyı yaparken kullanıcı adı sabit bir değer olarak girilir (Örnek kullanıcı adları: admin, administrator, yonetici, root vb.). Yazılım tarafından şifre alanı bir haneden altı haneye kadar denenmeye başlanır. Bu şekilde doğru kullanıcı adı ve şifre yakalanarak sisteme giriş yapılması amaçlanmaktadır.

6.2. Saldırı Tespit Sistemi Yazılımı (Intrusion Detection System Software)

Bu yazılım, Visual Studio.NET 2005 programlama ortamında hazırlanmış web yazılımı ve Microsoft Office 2007 Access programı kullanılarak hazırlanmış veritabanı dosyalarından oluşmaktadır. Yazılım Şekil 2'de gösterilen algoritmaya göre tasarlanmıştır.

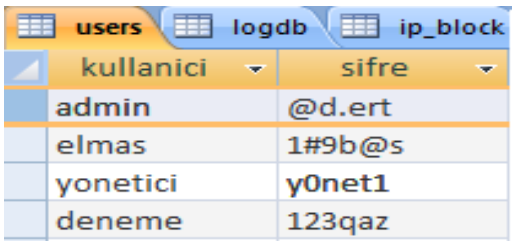


Şekil 2. Saldırı tespit yazılımı akış diyagramı
(Figure 2. Flow chart of ıntrusion detection software)

Veritabanında beş adet tablo vardır. Bunlar:

- Users tablosu,
- Logdb tablosu,
- Ip_block,
- Egitim,
- Mail tablosudur.

Users tablosu "kullanici" ve "sifre" olmak üzere iki alandan oluşmaktadır. Sisteme giriş için tanımlı olan kullanıcıların, kullanıcı adları ve şifreleri bu tabloda tutulur. Örnek bir users tablosu Resim 2'de gösterilmiştir.



users | logdb | ip_block

kullanici	sifre
admin	@d.ert
elmas	1#9b@s
yonetici	y0net1
deneme	123qaz

Resim 2. Users tablosu
(Picture 2. Users table)

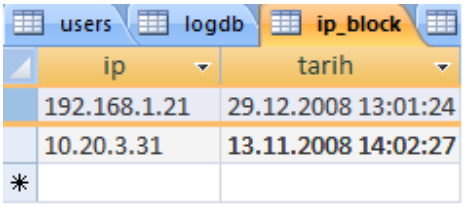
Logdb tablosu "kullanici", "ip", "tarih" ve "erisim_basarili_mi" alanlarından oluşmaktadır. Sisteme giriş yapmaya çalışan kullanıcıların hangi kullanıcı adı, IP ve tarihte sisteme giriş yaptıkları veya yapmaya çalıştıklarının kayıt bilgisini tutar. Bu tablodaki "erisim_basarili_mi" alanı değer olarak "E" veya "H" tutar. Sisteme başarılı bir şekilde giriş yapan kullanıcılar için "E", sisteme giriş yapamayan kullanıcılar için "H" bilgisini tutar. Böylelikle sisteme giriş yapabilen ve yapamayan kullanıcılar ayırt edilir. Örnek bir logdb tablosu Resim 3'te gösterilmiştir.

logdb

kullanici	ip	tarih	erisim_basarili_mi	sifre
admin	78.180.12.74	09.12.2009 13:52:17	H	******
admin	78.180.12.74	09.12.2009 13:52:17	H	******
admin	78.180.12.74	09.12.2009 13:52:17	H	******
admin	78.180.12.74	09.12.2009 13:52:17	H	******
admin	78.180.12.74	09.12.2009 13:52:17	H	******
admin	78.180.12.74	09.12.2009 13:52:18	H	******
admin	78.180.12.74	09.12.2009 13:52:08	H	******
admin	78.180.12.74	09.12.2009 13:52:08	H	******
admin	78.180.12.74	09.12.2009 13:52:18	H	******
admin	78.180.12.74	09.12.2009 13:52:18	H	******
admin	78.180.12.74	09.12.2009 13:52:19	H	******
admin	78.180.12.74	09.12.2009 13:52:19	H	******
admin	78.180.12.74	09.12.2009 13:52:19	H	******
admin	78.180.12.74	09.12.2009 13:52:19	H	******
admin	78.180.12.74	09.12.2009 13:52:18	H	******
admin	78.180.12.74	09.12.2009 13:52:18	H	******
admin	78.180.12.74	09.12.2009 15:42:15	E	******
admin	78.180.12.74	09.12.2009 16:07:53	E	******
admin	78.180.12.74	09.12.2009 16:06:49	E	******
admin	78.180.12.74	09.12.2009 15:42:58	E	******
admin	78.180.12.74	09.12.2009 15:32:14	E	******
admin	78.180.12.74	09.12.2009 15:30:04	E	******
admin	78.180.12.74	09.12.2009 15:24:00	E	******
admin	78.180.12.74	09.12.2009 15:46:44	E	******

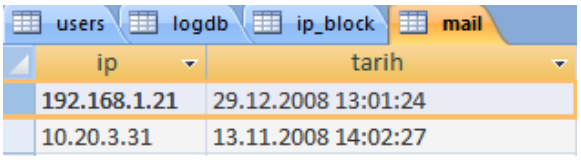
Resim 3. Logdb tablosu
(Picrure 3. Logdb table)

Ip_block tablosu "ip" ve "tarih" olmak üzere iki alandan oluşmaktadır. Saldırı yapıldığı tespit edilen veya yetkili sistem kullanıcısının, sisteme girişe izin vermediği IP'lerin tutulduğu tablodur. Örnek bir ip_block tablosu Resim 4'te gösterilmiştir.



Resim 4. Ip_block tablosu
(Picrure 4. Ip_block table)

Mail tablosu "ip" ve "tarih" olmak üzere iki alandan oluşmaktadır. Saldırı yapıldığı tespit edilen IP'ler önceden belirlenmiş olan e-posta veya e-posta adreslerine otomatik olarak bildirilir. Hangi IP'ler için hangi tarih ve saatte e-posta atıldığı bu tabloda tutulur. Örnek bir mail tablosu Resim 5'de gösterilmiştir.



Resim 5. Mail tablosu
(Picture 5. Mail table)

Egitim tablosu, "basarili", "basarisiz" ve "atak" olmak üzere üç alandan oluşmaktadır. Sisteme giriş yapmaya çalışan kullanıcı IP'lerinin log bilgilerine bakılarak; bunun saldırı olup olmadığına karar verilmesi için kullanılan tablodur. Bu tablo YSA' nı eğitmek için kullanılır. Bu tablodaki kayıtlar yetkili sistem kullanıcı tarafından oluşturulur. Tablo içerisinde saldırı olarak kabul edilecek ve saldırı olarak kabul edilemeyecek durumların kaydı bulunur. Örnek bir egitim tablosu Resim 6'da gösterilmiştir.

Uygulamada amaç; hazırlanan web yazılımına bağlanmaya çalışan kullanıcıların hangi IP'lerden bağlandıklarını tespit edip, hazırlanan eğitim tablosunu kullanarak eğitilen YSA'nın bu girişlerin bir saldırı olup olmadığına otomatik olarak karar vermesini sağlamaktır.

Hazırlanan saldırı tespit yazılımı kullanıcı giriş ekranı Resim 7'de gösterilmiştir.

egitim

sira_no	basarili	basarisiz	atak
34	0	10	E
35	1	10	E
36	2	10	E
37	3	10	E
38	4	10	E
39	5	10	E
40	6	10	H
41	7	10	H
42	8	10	H
43	9	10	H
44	10	10	H
45	5	15	E
46	20	0	H
47	30	0	H
48	40	0	H
49	0	30	E
50	0	40	E
51	0	20	E

Resim 6. Egitim tablosu
(Picture 6. Egitim table)

Resim 7. Giriş ekranı
(Picture 7. Login screen)

Kullanıcıların sisteme girebilmeleri için kullanıcı adı ve şifrelerini girmeleri gerekmektedir. Kullanıcı adı ve şifre boş geçilemez.

Sisteme giriş yapmaya çalışan kullanıcının kullanıcı adı ve şifresi, veritabanında kayıtlı olan geçerli bir kullanıcıya ait değil ise; Resim 8'deki ekranla karşılaşılmaktadır. Burada sisteme giriş yapmaya çalışan kullanıcının kayıt (log) bilgileri veritabanında "logdb" tablosuna kaydedilmektedir. Veritabanına kaydedilen bilgiler; kullanıcı adı, şifre, kullanıcı ip, sistem tarih saati ve sisteme erişim bilgisidir.

Resim 8. Uyarı mesajı
(Picture 8. Warning message)

Veri toplama işlemi bu aşamada gerçekleşmektedir. Bu işlem basamağı sırasında toplanan veriler daha sonra saldırı tespitinde kullanılmak üzere ilgili tabloya kayıt edilir.

Kullanıcı, giriş sayfasında kullanıcı adı ve şifreyi doğru girerek sisteme girebilmektedir. Sisteme giriş yapan kullanıcı Resim 9'daki gösterilen menü ekranı ile karşılaşacaktır.

Resim 9. Menü ekranı
(Picture 9. Menu screen)

Menü ekranı üzerinden "Log Bilgileri Ekranı"nı tıklayan kullanıcının karşısına Resim 10'da gösterilen log bilgileri ekranı gelecektir.

Resim 10. Log bilgileri ekranı
(Picture 10. Log information screen)

Bu ekranda; sisteme giriş yapmaya çalışan kullanıcıların log bilgileri ve sisteme girişine izin verilmeyen (bloklanan) IP'ler liste olarak alınabilmektedir.

Sistem tarafından saldırı yaptığı kabul edilerek bloklanan IP'leri listelemek için "Bloklanan IP'ler" seçeneği seçilip "Listele" butonuna tıklanır.

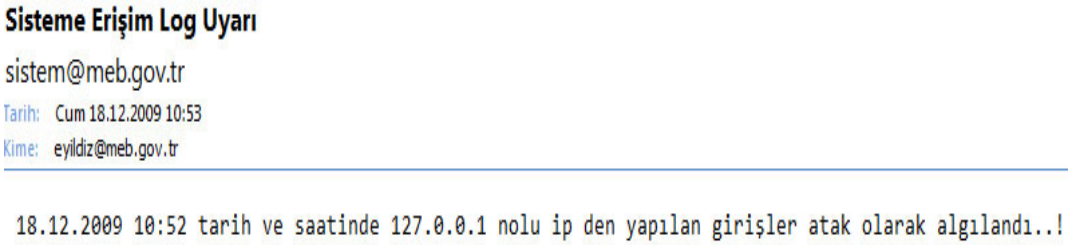
Bloklanmış bir IP'yi blok listesinden çıkarmak için; IP'nin solundaki "Blok Kaldır" butonuna tıklanarak, seçilen IP blok listesinden çıkarılır (Resim 11).

Resim 11. IP' yi blok listesinden çıkarmak
(Picture 11. Removing IP from block list)

Blok listesine alınan IP'den bir daha sisteme giriş yapılmasına müsaade edilmez. Bloklanan IP' den sisteme girilmeye çalışıldığında Resim 12'deki ekranla karşılaşılır.

Resim 12. Uyarı mesajı (bloklanan IP'nin sisteme girişine izin verilmez)
(Picture 12. Warning message (login of the blocked IP to the system is denied)

Yazılımda kurgulanan modele göre sistem; saldırı olarak kabul edilen bir durumla karşılaştığında, önceden belirlenmiş e-posta veya e-posta adreslerine otomatik uyarı e-postası atar (Resim 13). Böylece yetkili kişinin durumdan haberdar olması sağlanmaktadır.



Resim 13. Yönetici bilgilendirme mail
(Picture 13. Administrator information mail)

Yazılımın menü ekranından "Eğitim Tablosu Ekranı" seçildiğinde Resim 14'deki ekran gelmektedir.

Resim 14. Eğitim tablosu ekranı
(Picture 14. Training table screen)

Bu ekran üzerinde YSA ağını eğitmek için kullandığımız eğitim tablosu ile ilgili işlemler yapılmaktadır. Eğitim tablosuna yeni kayıtlar ekleme veya eğitim tablosunda var olan kayıtları silme işlemi bu ekran üzerinde yapılmaktadır. Ekran üzerinde yapılan işlemler Resim 5'de gösterilen egitim tablosunda tutulmaktadır.

Yazılımın menü ekranından "YSA Eğitim Ekranı" seçildiğinde Resim 15'deki ekran ile karşılaşılmaktadır.

Resim 15. YSA eğitim ve test ekranı
(Picture 15. ANN training and test screen)

Ekranda eğitim tablosu kullanarak eğitilmiş YSA, değerler girilerek test edilebilmektedir. Örnek bir test sonucu ekran görüntüsü Resim 16'da gösterilmiştir.

Resim 16. YSA örnek test sonucu ekranı
(Picture 16. Sample ANN test result screen)

Ekran üzerinde önceden hazırlanmış egitim tablosu kayıtları kullanılarak YSA eğitimi yapılmaktadır. "YSA Eğit" butonuna basılarak bu işlem gerçekleştirilmektedir. Bu işlemi yapabilmek için Visual Studio 2005 programı içerisinde YSA için hazırlanmış olan "NeuronDotNet.Core" sınıfı kullanılmıştır.

Bu çalışmada, ileri beslemeli ağ yapılarından olan MLP(Multi-Layered Perceptron) kullanılmıştır. MLP tercih edilmesinin nedeni, bilinen en eski YSA modellerinden olması ve sınıflandırma problemlerinde başarılı sonuçlar üretmesidir. Bunların yanında, farklı öğrenme algoritmaları ile kullanıma uygun olması MLP'nin sağladığı diğer bir avantajdır [6].

MLP'de giriş ve çıkış sayıları, uygulanacak olan probleme göre belirlenirken, ara katman sayısı ile ara katman nöron sayıları "deneme yanılma" yolu ile bulunur [11].

Çalışmada YSA modelini eğitmek için LM(Levenberg-Marquardt) öğrenme algoritması kullanılmıştır. Bu algoritma, Gauss-Newton ve En Dik İniş (Steepest Descent) algoritmalarının en iyi özelliklerinden oluşur ve bu

iki metodun kısıtlamalarını ortadan kaldırır. Genel olarak bu metot yavaş yakınsama probleminden etkilenmez [11].

YSA'nı eğitirken girilen parametre değerleri; giriş nöron sayısı 2 (başarılı ve başarısız giriş sayısı), gizli katman sayısı 1, gizli katmandaki nöron sayısı 3 ve çıkış nöron sayısı 2 (saldırı ve saldırı değil oranları)'dir. YSA eğitimi 5000 adımda yapılacak şekilde belirlenmiştir.

6.3. STS Yazılımının Veri Madenciliği Süreçleri Açısından Değerlendirilmesi (Evaluation from point of Data Mining Process)

- Problemin Tanımlanması: Geliştirilen STS çalışmasında tanımlanan problem; sistemlerde kullanıcı hesaplarını ve şifreleri kırmak için tahminlere dayalı deneme yanılma yöntemini kullanan bir DoS saldırısı türüdür. Amaç; kullanıcının şifresini ele geçirmek ve sisteme o kullanıcı üzerinden sızmak olan brute force saldırılarını gerçek zamanlı olarak engelleyip sistem yöneticisine haber veren bir STS tasarlamaktır.
- Verilerin Toplanması: Geliştirilen STS yazılım projesinde kullanılan YSA modelini eğitmek için gerekli verilerin toplanması sistem yöneticisi tarafından yapılmıştır. Sistem yöneticisi saldırı olarak kabul edilen veya saldırı olarak kabul edilmeyen durumları gösteren bir eğitim tablosu hazırlar ve bu şekilde gerekli verileri toplamış olur.
- Modelin Kurulması: STS' de kullanılan YSA' nın tasarlanmasında ileri beslemeli ağ yapılarından olan MLP kullanılmıştır. Öğrenme algoritması olarak LM algoritması kullanılmıştır. Ağın topolojisi 1 giriş, 1 ara katman ve 1 çıkış katmanından oluşmaktadır. Giriş katmanında başarılı giriş sayısı ve başarısız giriş sayısı olarak iki giriş değeri vardır. Ara katmanda 3 nöron vardır. Çıkış katmanında saldırı ve saldırı değil olarak iki çıkış değeri vardır. YSA ağı hazırlanmış eğitim tablosu kullanılarak eğitilir. YSA' nı eğitmek için Visual Studio 2005 programlama ortamındaki hazır sınıflardan olan "NeuronDotNet.Core" kullanılmıştır.
- Modelin Değerlendirilmesi: Eğitilen YSA, yazılım projesi içinde hazırlanan test ekranı kullanılarak test edilmiştir. Bu şekilde model değerlendirilmiş olmaktadır.
- Modelin Kullanılması: Eğitilmiş olan YSA, saldırı tespit işlemini yapabilmesi için yazılıma entegre edilmiştir. Saldırı tespiti yapıp yapmadığını test edebilmek için geliştirilen brute force yazılımı ile geliştirilen STS yazılımına saldırı düzenlenmiştir. Yapılan saldırı işlemi sonucunda geliştirilen STS' nin brute force saldırıyı algılayıp, saldırı yapılan IP adresini engellemiş ve yetkili kullanıcıya e-posta yolu ile bildirimde bulunmuştur.
- Modelin İzlenmesi: Tasarlanan YSA, saldırı tespit sistemi içinde izlenerek zaman içerisinde oluşabilecek durumlara göre yeniden eğitilebilir.

7. SONUÇLAR VE DEĞERLENDİRME (CONCLUSIONS AND EVALUATION)

Bilgi çağında, bilginin kendisi kadar güvenliği de önemli bir konu haline gelmiştir. Çünkü artık saldırılar hem çeşitli sebeplerle bilinçli kişi ve kişilerce yapılırken, hem de bilinçsiz kullanıcılar tarafından istenmeden yapılmakta ve sistemlere zarar vermektedir. Üstelik bilinçli kullanıcılara karşı önlem almak mümkün iken, kurum ve kuruluşların içerisinde yer alan bilinçsiz kullanıcılar için çoğu zaman daha zor olmaktadır.

Veri tabanlarında önemli veriler bulunduran kurum ve kuruluşlar ağlarını çok katmanlı güvenlik yöntemleriyle korumaya çalışmaktadırlar. Bunlardan biri olan saldırı tespit sistemleri büyük ağlara sahip kurum ve kuruluşlar için oldukça önemlidir. Ancak Saldırı Tespit Sistemlerini doğru yapılandırmaları ve takip etmeleri gerekmektedir.

Bu çalışmada, DoS ataklarından biri olan Brute Force tipi saldırıları IP tabanlı tespit eden gerçek zamanlı bir saldırı tespit sistemi uygulaması geliştirilmiştir. Tespit edilen IP adreslerinin sisteme girişi engellenir ve e-posta ile sistem yöneticisine bildirilir. Ayrıca saldırı tespit sistemi uygulaması, kullanıcı adı, IP adresi, tarih ve saat gibi bilgileri sistem yöneticisine sunmaktadır.

Geliştirilen saldırı tespit sistemi yazılımı doğru kullanıcı adı ve şifre ile girildiğinde, sistem yöneticisine seçilen tarihe ait hatalı girişleri, saldırı yaptığı kabul edilerek engellenen IP listesini, YSA eğitimi ekranını ve eğitilen YSA test ekranını gösterir.

Aynı IP'den bir dakika içerisinde yapılan başarılı ve başarısız girişlerin sayısı tespit edilerek, sistem yöneticisi tarafından eğitilmiş olan YSA' ya parametre olarak gönderilir. YSA'dan dönen saldırı ve saldırı değil değerleri karşılaştırılarak (saldırı>saldırı değil), yapılan bağlantının saldırı olup olmadığına karar verilir. Saldırı yapıldığına karar verilen IP, blok tablosuna eklenir ve belirlenen e-posta adreslerine yazılım tarafından yapılan işlemle ilgili olarak e-posta gönderilir. Blok tablosuna eklenen IP'den yapılan bağlantılar artık geçersiz kabul edilir ve sisteme girişine izin verilmez.

Bu çalışmada açıklanan STS çalışmasında göz önüne alınması gereken noktalar şu şekilde sıralanabilir:

- Her sistem yapısına göre farklılıklar içerebilir (Kullanıcı sayısı, ağ trafiği, uygulama sunucularının ve veritabanlarının cevap süresi gibi.). Burada STS tasarımında bulunacak kişinin bu ve benzeri ölçütleri göz önünde bulundurması gerekir.
- YSA eğitimi için gerekli olan verilerin toplanması zaman almaktadır.
- YSA yapısının kurulması ve test edilmesi deneme yanılma yöntemi ile olduğundan zaman almaktadır. Sistemin istenilen doğruluk oranına ulaşıncaya kadar işlemlerin tekrar edilmesi gerekmektedir.

Kurum ve kuruluşların kişisel bilgisayar kullanıcılarının Saldırı Tespit Sistemi kurması ve bunu düzenli olarak takip etmesi gerekmektedir. Bunun bir ihtiyaç ve güvenlik duvarı kadar önemli bir uygulama olduğunu tüm sistem yöneticileri tarafından dikkate alınması gerekmektedir. Gerçekleştirilen bu çalışma ile sistem yöneticilerinin STS'leri, ihtiyaçlarına göre nasıl yapılandırabilecekleri hususunda fikir vermesi beklenmektedir.

KAYNAKLAR (REFERENCES)

1. Pei, J., Upadhyaya, S.J., Farooq, F., and Govindaraju, V., (2004). "Data mining for intrusion detection: techniques, applications and systems," 20th International Conference on Data Engineering (ICDE'04), 1063-6382.
2. Lunt, T.F., (1988). "Automated audit trail analysis and intrusion detection: A survey", 11th National Computer Security Conference, Baltimore, 65-73.
3. Akpınar, H., (2007). "Veri tabanlarında bilgi keşfi ve veri madenciliği", İstanbul Üniversitesi İşletme Fakültesi Dergisi, 29 : 1 (2000).
4. Canbek, G. ve Sağıroğlu, Ş., "Bilgisayar sistemlerinde yapılan saldırılar ve türleri: bir inceleme", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23 (1-2): 1-12.
5. Hussain, A., Heidemann, J., and Papadopoulos, C., (2004). "Distingushing between singel and multisource atttacks using signal processing", Computer Networks, 46.
6. Balkanay, A., (2007). "Örün (WEB) Güvenliği", Ağ Güvenliği Dersi Eğitim Notları, İstanbul Teknik Üniversitesi Bilişim Enstitüsü Bilgisayar Bilimleri Yüksek Lisans Programı, İstanbul, 10
7. Şahin, O., (2008). "Sınır Güvenliği", Tübitak-UEKAE Ağ Güvenliği Grubu Eğitim Raporu, Ankara, 261-344.
8. İnternet : "Saldırı tespit sistemi alınırken dikkat edilecek hususlar"http://www.olympos.org:81/article/articleview/275/1/2/saldiri_tespit_sistemi_ids_alirkendikkat_edilecek_hususlar (2008).
9. Güven, E.N., (2007). "Zeki saldiri tespit sistemlerinin incelenmesi, tasarimi ve gerçekleştirilmesi", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2-20.
10. Öztemel, E., (2003). "Yapay Sinir Ağları", Papatya Yayınları, İstanbul, 25-27
11. Sağıroğlu, Ş., Beşdok, E. ve Erler, M., (2003). "Mühendislikte Yapay Zeka Uygulamaları-I Yapay Sinir Ağları", Ufuk Kitabevi, Kayseri, 10-100.