**BİLGİSAYAR AĞLARINA YAPILAN SALDIRILARIN SINIFLANDIRILMASI**

**1.GİRİŞ**

Günümüzde bilişim alanındaki en büyük sorunlardan biri ağ güvenliğidir.Büyük şirketler kurmuş oldukları ağ sistemlerinin saldırılara karşı korunması için yaşamsal bir savaş vermektedirler.Bundan dolayı çok büyük yatırımlar yapmakta ve büyük paralar harcanmaktadır.Ticari anlamda firmalar büyük zarar görmektedirler.Diğer taraftan bu tür sistemleri üreten ve yazılım geliştiren firmalar büyük bir para kazanmaktadırlar.Saldırı çeşitleri arttığı sürece her gün yeni bir ağ güvenliği programı ve sistemi ortaya çıkmaktadır.Tabii olarak bu gelişme yüzünden büyük bir pazar oluşmaktadır.

Burada sadece büyük firmalar değil kişisel bazdaki kullanıcılarda bilgi saklama ve korunması için çeşitli programlar ve sistemler almaktadır.Dünya çapında büyük bir pazar haline gelen bu güvenlik sistemleri dünya ülkelerinde olduğu gibi ülkemiz ekonomisine büyük zararlar vermektedir.

Yapılan araştırmalar dünya genelinde şirkete yapılan atakların % 70 ila % 90 arasında şirket çalışanları tarafından yapıldığını ortaya koymaktadır. Bu bilgi hırsızlığından tutun bilerek yada bilmeyerek sistemlere verilen zararları kapsamaktadır. Genelde işinden kötü şekilde ayrılan şirket çalışanları sistemlere ait bilgilerini başkalarına verebilmekte yada özellikle sistemleri sabote edebilmektedirler. Kendi bilgisayarlarına kurdukları “sniffer”(paket dinleyici) lar sayesinde başka kişilerin maillerini yada gizli bilgilerini elde edebilmektedirler. Yada her türlü önleminizi dışarıdan gelebilecek saldırılara karşı almışken içeriden birisi kolaylıkla önemli sistemlere erişebilir kritik bilgileri silip değiştirebilir yada rakip bir firmaya verebilir. Yada meraklı bir kullanıcı yeni öğrendiği hacker araçlarını sizin firmanız üzerinden başka firmalara girmek için kullanabilirler.

Güvenlik için yapılan her yatırıma karşı bu saldırılar sürmektedir.Hatta Amerika’da dünyanın en iyi korunan , girilmesi imkansız olan Savunma Bakanlığı bilgisayarlarına girilmiş ve bilgilere ulaşılmıştır. Amerika’da bu tür saldırılara ağır cezalar uygulanırken Türkiye’de bir yasal boşluktan dolayı yakalananlar elini kolunu sallayarak hapisten çıkmaktadır.

**2.AĞ GÜVENLİĞİ SAĞLAMA YÖNTEMLERİ**

Ağ güvenliği sağlanırken sadece güvenlik duvarı (firewall) tek başına düşünülmemelidir. Güvenlikte esas olan süreklilik,kullanılan cihazların ve yazılımların bir bütün halinde kurulması ve işletilmesidir.Ağ ortamındaki tüm elemanların bu sistem içine alınması gerekir.Fiziksel koruma yapılırken merkezi birim olduğu yer bir kontrol noktası haline getirilmelidir.Bu kontrol noktası ayrı bir odada olmalı ve sadece belli kişilerin girmesi sağlanmalıdır.Sistem içinde bir kabinet var ise bu kabinet her zaman kilit altında tutulmalıdır.Şu unutulmamalıdır ağ üzerinde saldırılar sadece dışardan değil en fazla içerdeki personelden gelmektedir.

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

dolayısıyla ağ trafiğinin güvenliği için çok gereklidir. Cihazlarda kurulum sırasında oluşan varsayılan (default) ayarların, kullanıcı tarafından aktif edilen bazı ayarların iptal edilmesi veya düzgün olarak tekrar ayarlanması gerekebilmektedir.

Ağ güvenliği tam olarak aşağıdaki güvenlik kavramlarını bir bütün olarak ele alınmasıyla sağlanabilir.

* İnternet bağlantı güvenliği
* Saldırı ve Saldırı tespit sistemleri
* Veri güvenliği
* Virüslerden koruma
* Şifreleme
* Log analizi
* VPN Güvenliği

**2.1.Internet Bağlantı Güvenliği**

İnternet’in genişlemesi ile beraber ağ uygulaması da beklenmedik şekilde genişlemiştir.Bu gelişmeyle birlikte ağ kurulup işletmeye alındıktan sonra ağ yönetimi ve ağ güvenliği büyük önem kazanmıştır.Çünkü internete bağlı ağ sistemleri arasında dolaşan hiçbir veri gerekli önlemler alınmadığı takdirde güvenli değildir. Ağın güvenilir biçimde çalıştırılması anahtar sözcük konumuna gelmiştir. Çünkü ağın günümüz teknolojisi ile kurulup çalıştırılmasıyla iş bitmemekte esas iş ağ performansının ve güvenilirliğinin sağlanmasında bitmektedir.

Firmanın bilgisayar sistemini kullanan personel genelde kişisel bilgilerini bilgisayarlarında depolarlar. Bu kişiler bilgisayarları Internet`e bağlandığında kişisel bilgilerinin ekstra koruma gerektirdiğini bilmeliler.Ağlar bilgisayarlar ve veritabanları gibi değerli kaynakları birbirine bağlar ve firma için gerekli olan servisleri sağlarlar. Bir sunucunun sağladığı özellikler çoğaldıkça güvenlik açıkları içerme riski de o oranda artar. Bunun sebebi Internet protokol ve standartlarının dizayn edilirken güvenliğin düşünülmemesidir.

Kullanıcıların genelde işlerini yeterlilikle yapabilmeleri ağ servislerine bağlıdır. Eğer kullanıcıların bu servislere erişimi engellenirse daha az üretken olurlar ve bu da firma için mali kayıp demektir.

2003 yılında birçok kereler rastladığımız yaygın kullanılan işletim sistemi ve uygulamalarda bulunan açıkları kullanarak dağılan solucanlara (örn: Sql slammer, nachi bv.) karşı yine tedbirli olmak gerektiğini belirten uzmanlar, yeterli güvenlik önlemi alınmadan 24 saat Internet'e açık bırakılan sistemlerin hacker'lar tarafından kötü amaçlı olarak servis kesintisi atakları için kullanılabileceğini söylüyorlar. Spam konusunda da her yıl artış olacağını söyleyen uzmanlar bunun için kurumların ek güvenlik çözümlerine gereksinimi olacağını belirtiyorlar.

Uzmanlar kurumsal Internet güvenliği için şirket içi eğitimlerin olması gerektiğini, çalışanlara Internet bağlantısında dikkat etmeleri gerekli noktaların, e-posta alışverişinde göz önüne alınması gereken hususların ve her bir çalışanın kendi masaüstü koruma yazılımı ile sistemini periyodik olarak virüslere karşı taramasını öneriyorlar.

Servis kullanımı engelleme (DoS) Internet`teki istemci ve sunucular için en ciddi tehditlerden biridir. Aynı zamanda engellenmesi en zor güvenlik tehdididir. Bir servis kullanımı engelleme saldırısı kurbanın normalde erişebildiği bir servise erişebilmesini engelleyen kötü amaçlı bir saldırıdır. Bir saldırganın bunu gerçekleştirebilmesi için pek çok farklı yol vardır.

Bunun için özel ağ ile İnternet arasına bir Firewall konulması gerekmektedir.Bu sistem ile ağ güvenliği tam olarak sağlanır ve erişim hakları düzenlenir.

Bu sistem kurulurken şu noktalara dikkat edilmelidir.dikkat edilmelidir.Kurulmadan önce ne tür bilgilerin koruncağı, ne derecede bir güvenlik uygulanacağı ve kullanılacak güvenlik algoritmaları önceden belirlenmelidir.Firewall’ın sistem üzerinde etkili kullanılması için ağ ortamı ile internet arasındaki tüm trafiğin Firewall üzerinden geçilirmelidir.

**SALDIRI TÜRLERİ:**

Birkaç tip saldırı türü vardır. Bunları DoS (nuke), Remote Exploits ve Trojanlar olarak ayırabiliriz.

**NUKE:** Nuke, sisteminizi kilitleyen, göçerten, Internet erişimini kesen ve bu gibi zararlar veren saldırılara Nuke (nükleer bombanın kısaltması gibi) adı verilir.

Nuke siz internete bağlıyken ISS nizce size verilen bir ip numarası yardımı ile bir başka kişinin özel programlar yardımı ile bilgisayarınıza paketler gönderilmesi ve bu paketlerin bilgisayarınıza zarar vermesidir.

**OOB Nuke:** (Out of band Nuke ) Sadece Windows NT ve 95’de bir bug olan OOB nuke, işletim sistemi Windows olan bir makinanın 139. portuna (Netbios session port) MSG\_OOB tipi bir bağlantı (connection) yapılmasıyla gerçekleşir. Eğer 95 kullanıyorsanız sisteminizin mavi ekran vererek Internet bağlantısının kopmasına, NT kullanıyorsanız sistemin durmasına yol açar.

**Land:** Bilgisayarı kendi kendine senkronize ettirerek, arka planda Internet meselelerini yürüten Winsock adlı programın sonsuz döngüye girmesini sağlar. Böylece farenizi bile hareket ettiremezsiniz. Kaynak IP (Source), Kaynak Port ve Hedef IP (Destination IP) IP, Hedef Port’un aynı olduğu bir IP paketi, Land saldırısının gerçekleşmesini sağlar.

**Teardrop, Boink, Nestea:** Internet üzerinde gelen giden veri, parçalar halinde taşınır, daha sonra işletim sistemi tarafından birleştirilen paket parçacıkları veriyi oluşturur (fragmentation). Çoğu sistemin duyarlı olduğu bu saldırı tipleri, bilgisayarınızın bozuk olarak bölünmüş 2 paketi birleştirmeye çalışması ile gerçekleşir. Boink, teardrop saldırısının ters olarak çalışan halidir. Nestea, teardrop saldırısının küçük değişimlere uğramış halidir ve teardrop ve boink saldırılarına karşı patch edilmiş Linux sistemlerinde etkilidir.

**Brkill:** Eğer Windows yüklü bir bilgisayara, bağlantının sonlanması ile oluşan PSH ACK tipi bir TCP paketi gönderirseniz Windows size o anki son bağlantı seri numarasını gönderir. Buradan yola çıkarak hedef makinedeki herhangi bir bağlantıyı zorla kesmeniz mümkün olur.

**ICMP Nuke:** Bilgisayarlar çoğu zaman aralarındaki bağlantının sağlamlığını birbirlerine ICMP paketleri göndererek anlarlar. Bu saldırı varolan bir bağlantının arasına sanki hata varmış gibi ICMP\_UNREACH paketi göndererek oluşur.

**Jolt/SSPing:** Windows 95 ve NT’nin yüksek boyuttaki bölünmüş ICMP paketlerini tekrar birleştirememesinden kaynaklanan bir saldırı tipidir. 65535+5 byte’lık bir ICMP paketi göndermek bu saldırıyı gerçekleştirir.

**SMURF:** Networkler’de “broadcast address” olarak tanımlanan ve kendine gelen mesajları bütün network’e yönlendiren makineler vardır. Eğer birisi başka biri adına o makineye ping çekerse, ağ üzerindeki bütün çalışan makineler hedef olarak belirlenen makineye ping çeker. Smurf, bu işlemi yüzlerce broadcast makineye tek bir kaynak IP adresinden ping çekerek saldırı haline çevirir.

Bir anda bilgisayarlarınıza on binlerce bilgisayarın ping çektiğini düşünürsek değil sizin şirketinizin bağlantısı, maalesef Turnet (Türkiye Internet omurgası) çıkış gücü bile buna cevap vermeye yetmez ve bağlantılarınız kopar.

**Suffer:** Suffer saldırısı bilgisayarınıza sanki binlerce farklı bilgisayardan bağlantı isteği geliyormuş gibi SYN paketleri gönderir. Bu saldırının sonunda Windows yeni bağlantılar için yeterli hafıza ayıramaz ve kalan hafızayı da bitirir. Bazı firewall türleri de böyle bir durum karşısında binlerce soru kutucuğu açarak makinenin kilitlenmesine sebep olur.

**Exploit’ler:** Exploit’in kelime anlamı “kötüye kullanma, sömürme” demek. Yani sisteminizin normal bir özelliğinin bir açığını yakalayarak, bunu kötüye kullanabilir, sisteminizdeki, bilgilere ulaşabilirler. Exploitler genelde sistem tabanlı olarak çalışırlar yani Unix’e ait bir exploit Windows için çalışmaz. Bu güne kadar bulunan yaklaşık olarak 1000’in üzerinde exploit vardır.Aşağıda çok popüler olan bir kaç tanesinden bahsedilecektir.

**Windows Null Session Exploit:** Windows işletim sistemi, dışarıdaki kullanıcılara network üzerinde hiç bir hakka sahip olmadan oturum, kullanıcı ve paylaşım bilgilerini (session, user ve share) verir. Ve ne kadar ilginçtir ki, bu exploit, Windows Network API’sinde belgelenmiş ve feature (özellik) olarak gösterilmiştir. Kötü niyetli birisi bu exploit’i kullanarak sistem hakkında çok kritik bilgiler sahibi olabilir.

**PHF Exploit:** Bu exploit oldukça eski olmasına rağmen halen karşılaşabileceğiniz bir güvenlik açığıdır. Phf cgi yardımı ile sistemdeki dosyalara admin olarak erişebilirsiniz.

Yukarıdaki örnek Unix işletim sistemi ya da türevini kullanan bir makineden kullanıcı bilgilerinin ve şifrelerinin bulunduğu passwd dosyasını görmenizi sağlar.

**ASP Exploit:** Active server page (ASP) özelliği kullanan Web sunucularda URL’nin sonuna bir nokta (.) yada ::şDATA yazarak ASP’nin içeriğini (source code) görebilirsiniz. Eğer ASP’nin içerisinde her hangi bir şifre varsa bu exploit çok tehlikeli olabilir.

http://www.aspkullananserver.com/

default.asp. ya da

http://www.aspkullananserver.com/

default.asp::şDATA

**Sendmail Exploit:** Eski “send mail” sürümlerinde bir kaç basit hile ile sistemin şifrelerinin tutulduğu dosyayı çekmeniz mümkün. Ayrıca sistem kullanıcıları hakkında bilgi almak (EXPN) ya da bir kullanıcı isminin o sunucuda olup olmadığını da öğrenmek mümkün (VRFY).

telnet mail.server.com:25

**ICQ Tabanlı Exploitler:** Son derece zayıf bir mimariye sahip olan ICQ sistemi, kolayca taklit edilebilen hatta gerçek “spoofing” bile yapmanıza gerek kalmayan bir sistemdir. ICQ kullanıcıları kolayca mesaj bombasına tutulabilir, şifreleri değiştirilebilir, onaya gerek kalmadan listenize alabilir, IP’si kullanıcı istemese bile görülebilir ya da ICQ chat yaparken mesaj taşması (flooding) yapılabilir.

**Yerel Ağ Saldırıları**

 Çoğunlukla switch, hub ve yönlendiricilerin hedef alındığı

Saldırılardır.

 Hatalı switch yapılandırması, hub kullanımı ve yönlendiricilerdeki hatalı yapılandırmalardan kaynaklanır

 Paket Yakalama

 ARP/MAC Sahteciliği

 Ortadaki Adam Saldırısı

 Oturuma Müdahale Etme

 Ağ İletişiminin Aksatılması

 Kriptolanmış Oturumlara Müdahale

**Kablosuz Ağ Saldırıları**

 Kablosuz Ağlara Yönelik Saldırılar

 Kablosuz Ağların ve İstemcilerinin Saptanması

 Kimlik Doğrulama Yöntemlerinin Analizi

 MAC Adresi Sahteciliği

 Kriptolamaya Yönelik Saldırılar

 Kriptosuz Ağların Saptanması

 WEP Kriptolamanın Kırılması

 WPA Kriptolamanın Kırılması

 Kablosuz İstemcilere Saldırılar

 Sahte Erişim Noktası Oluşturma ve Erişimleri Kaydetme

 Erişilebilir İstemciye Yönelik Saldırılar Düzenleme

Ağa bağla bilgisayar sistemlerindeki çeşitleri tehditleri genel anlamda incelersek;

Fiziksel tehditler:

Bu durum ,bilgisayar donanım / yazılımın hırsızlık, sel, vandalizm, yangın, savaş, doğal afet, deprem vb) bir sonucu olarak kayıp veya hasar görmüş olduğu bir durumdur .

   Kasıtsız ve yanlışlıkla yapılan hata:

Bu durum kullanıcı ,operatör yada programcı kaynaklı hatalar sonucu oluşun veri bozulmalarını içerir.

   Yetkisiz erişim Bazı yetkisiz kişiler, programlar veya sistem, ağa ulaşma iznini elde edebilirler. Bu sonuç, bilgi sızmasının sisteme verdiği hasarı gösterir.. Tipik örnekler ,kaçak olarak dosyaların kopyalaması ve veri yakalamak için ağın dinlenmesi.

  Kötü amaçlı programlar:

Bu tarz yazılım programları,hedef bilgisayarların kaynaklarını kullanmak yada yok etmek için tasarlanmıştır.Çeşitli tiplerde ortaya çıkabilirler:

 Virüsler,

Veriler üzerinde değişiklik yapabilme veya onları yok etme veya başka programlara eklenebilme özelliklerine sahip ,kötü amaçlı yazılımlardır.

 Solucanlar,

Kendi kopyalarını üreten bağımsız programlardır.

Virüsler gibi mağdur programa yapışmazlar

Genellikle bilgisayarları tıkarlar.

Ağlar aracılığıyla çoğalır.

  Truva Atları,

Yararlı işlevlerinin yanı sıra zararlarıda vardır.

Program,Oturum açma ekranı gibi görünür ancak kimlik ve şifreleri toplar.

Bilgisayar ve ağ güvenliği tehditlerini tartışırken,Wiliam,Stalling(2005) Bilgi sağlayıcı gibi bilgisayar sisteminin fonksiyonları görüşünden onları karakterize edip tanımladı.Kaynaktan gelen o bilgi akışı,dosya yada ana bellek bölgesi,konumu yada başka bir dosya yada kullanıcı adıdır.Yukarıdaki ana fikir 3 gruba ayrılmış tehditler kategorisi ile desteklenir.

      **Interruption(Kesilme)**

Bir Varlık olarak sistem yok edilmiş yada Kullanılamaz hale geliyor.Bu kullanılabilirlik saldırısıdır..Örnekler bir donanım parçası yıkmını(harddisk gibi),iletişim hattının kesilmesi yada dosya yönetim sisteminin devre dışı bırakılmasını içerir.

   **Interception(Dinleme)**

Yetkisiz bir parti,bir varlığa erişmeye hak kazanır.Bu birgizlilik saldırısıdır.Yetkisiz parti bir kişi,bir program yada bir bilgisayar olabilir.Örnekler ,verileri yakalamak için yasadışı dinleme ve dosya ve programların yasadışı kopyalanmasını içerir.

      **Modification(Değiştirme)**

Yetkisiz bir parti sadece varlığa erişme izni değil,aynı zamanda varlığın değişrilerek bozulmasına yol açar.Bu bütünlük üzerine bir saldırıdır.Örnekler,bir veri dosyasındaki değişen değerleri,program değiştirme içerir yani farklı şekillerde çalışan,mesaj içeriğini değiştirerek bir ağ içide iletilir**.**

      **Fabrication(Fabrikasyon)**

Yetkisiz bir parti sisteme sahte nesneleri ekleyebilir.Bu özgünlük saldırısıdır.Örnekler,sahte mesajların bir ağa ,bir kayda yada dosyaya yazılmasını içerir.

Bütün bilgisayar ve ağ güvenliği tehditleri,hemen hemen aynı sonuçları gösterir. Bunlar, gizlilik , özgünlük ve bütünlük durumunu etkilerler. Bu nedenle, kusursuz bilgisayar ve ağ güvenliği tehditleri / saldırılar için önleyici tedbirlere ,acil ve sürekli ihtiyaç vardır.

Bilgisayar sistemlerinde en genel anlamda sızma ya da saldırı makine başından yapılacak

izinsiz erişimlerden başlar ve çok geniş bir spektruma yayılır. Bilgisayar ağları söz konusu

olduğunda ise saldırılar sadece bu tip kullanıcı ve erişim temelli saldırılar ile sınırlı kalmaz.

Ağ üzerinden yapılan saldırılar günümüzde en sık karşılaşılan problemlerdir. Bu çalışma ağ

üzerinden yapılan saldırıları ve onlara karşı geliştirilen saldırı tespit mekanizmalarını

incelemeyi hedeflemektedir. Bu tip saldırılar 4 temel kategoride incelenebilirler.

**1) Bilgi Tarama (Probe ya da scan):** Bu saldırılar bir sunucunun ya da herhangi

makinanın, geçerli ip adreslerini, aktif portlarını veya işletim sistemini öğrenmek için

yapılan saldırılardır. Bilinen saldırılardan bunlara örnek olarak:

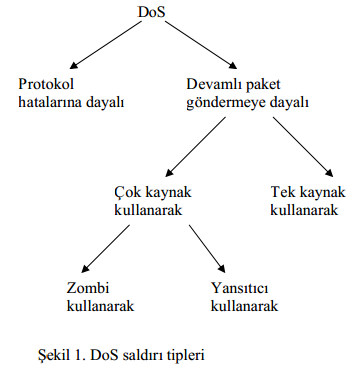
a. ipsweep: belirli bir protu sürekli tarama saldırısı.

b. Portsweep: bir sunucu üzerindeki hizmetleri bulmak için tüm portları tarar.

**2) Hizmet Engelleme (Denial of Service - DoS):** Bu saldırılar genelde TCP/IP protokol

yapısındaki açıklardan faydalanarak veya bir sunucuya çok sayıda istek yönelterek

onu tıkamaya sebep olan saldırılardır. DoS saldırıları kendi içinde gruplara ayrılır.



Protokol hatalarına dayalı saldırılara örnek olarak ping-of-death (ölümüne ping) saldırısı

yani bir tek büyük boyutlu ICMP eko mesajı gönderilmesi saldırısı vardır. Başka bir

saldırı, TCP SYN paketinin içersine kaynak ve varış adresi aynı makine olan bir paket

gönderilmesiyle olur. Bunlar tek paketle ya da az paketle gerçekleştirilen, protokollerin

açıklarını kullanan saldırılardır. Diğer gruptaki saldırılar devamlı istekte bulunulmasına

dayanır. Hem sunucu makine hem de ağ meşgul edilir. Örneğin bu, bir sunucuya devamlı

bağlantı isteği yapmak olabilir. Saldırı tek bir makine kaynaklı olabileceği gibi ağ

üzerinden ele geçirilen birçok makine ile de yapılabilir. Bu tip makinelere zombi denir.

Eğer zombi kullanılmıyorsa yansıtıcı da kullanılabilir. Yansıtıcı herhangi bir sunucu

olabilir. Saldırgan kurbanın adresi ile sorgu yapar ve dolayısıyla sunucu farkında olmadan

kurbanın adresine cevaplar gönderir. Özel olarak kullanılan saldırlardan bazıları:

a. Smurf: ICMP mesajlarının broadcast ile tüm ağa dağıtılmasıyla oluşur.

b. Selfping: kullanıcının makinayı sürekli pinglemesiyle gerçekleşir.

c. tcpreset: saldırgan kurbanın kurmaya çalıştığı bağlantılar için kurban adına

reset göndererek bağlantısını engeller.

d. mailbomb:saldırgan sunucuya sürekli mail gönderir.

**3) Yönetici Hesabı ile Yerel Oturum Açma (Remote to Local - R2L):** Kullanıcı

haklarına sahip olunmadığı durumda misafir ya da başka bir kullanıcı olarak izinsiz

erişim yapılmasıdır.

Bunlara örnek:

a. Sshtrojan: unix üzerinde çalşına bir trojan saldırısıdır.

b. guest: tahmini kolay şifreleri bularak sisteme girilmesidir.

**4)** **Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi (User to root - U2R):** Bu tip

saldırılarda sisteme girme izni olan fakat yönetici olmayan bir kullanıcının yönetici

izni gerektirecek işler yapmaya çalışmasıdır. Örnekleri:

a. Eject: Solaris üzerinde eject programı ile tampon taşmasına yol açıp, yönetici

haklarına sahip olunmasıdır.

b. Sqlattack: sql veritabanı kurulu Linux makinalarda sunucuya bağlanan

kullanıcının belirli komutlarla yönetici hakları ile komut satırı elde etmesidir.

Bu çalışma çerçevesinde tüm bu saldırıları yakalamaya odaklanan saldırı tespit

sistemlerinin yapıları, kullandıkları tespit yöntemleri genel olarak tanıtılacaktır. Fakat özelde

odaklanılacak konu bir kullanıcının hakkı olmadan sisteme giriş yapmak istemesi veya

sisteme girmeye hakkı olup da bazı işlemlere izni olmayan kullanıcının bu izinleri aşmaya

çalışması gibi saldırılar olmayacaktır. Genel tanımlar verildikten sonra daha çok ağ üzerinden

yapılan saldırı tespitine yönelik çalışmalara odaklanacağız.

Ağ trafiğini esas alarak, burada oluşan anormallikleri gözlemleyerek, saldıryı

belirlemek mümkündür. Bu tip modellere ağ aktivitesi modelleri (Network activity models)

adı verilir ve ağdaki trafik yoğunluğu üzerinden saldırı tespitine odaklanırlar. Bu durumda

tespit edilebilecek saldırılar yukarda sıralanan saldırılardan 3. ve 4. maddelere giren ve en

yaygın saldırılardan olan DoS ve tarama (probe) saldırıları olacaktır. Bu tipteki saldırıların ne

kadar önemli olduğu 2002 yılında yapılan bir çalışmada gösterilmiştir. Burada internet

üzerindeki 1600 ağdan toplanmış verilerin analizi yapılmıştır [1]. İnternet üzerinde hergün

25000 civarında saldırı gerçekleştiği saptanmıştır. Bu çalışmadan alınan aşağıdaki grafikte

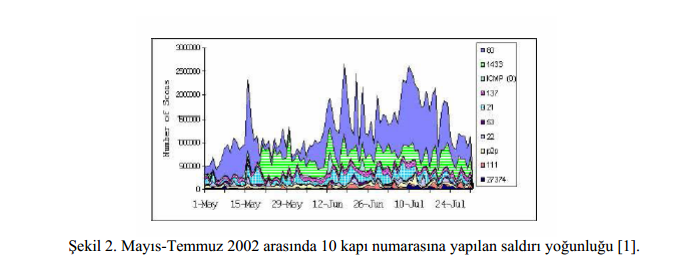
sadece yoklama (probe/scan) saldırısı göz önüne alındığında Mayıs-Temmuz ayları arasındaki

kapı numaralarına karşı düşen saldırı yoğunluğu verilmiştir. Tek bir saldırı tipi için verilen

Şekil 2, durumun ne kadar ciddi boyutlarda olduğunu göstermektedir. Bundan başka sadece

1999 yıllında NASA, NATO, Beyaz saray, Pentagon gibi merkezlere yapılan ve başarı

sağlanan saldırıların sayısı 10’u geçmektedir.



1980’lerde sadece bilgisayar sistemleri uzmanları tarafından yapılan saldırılar artık

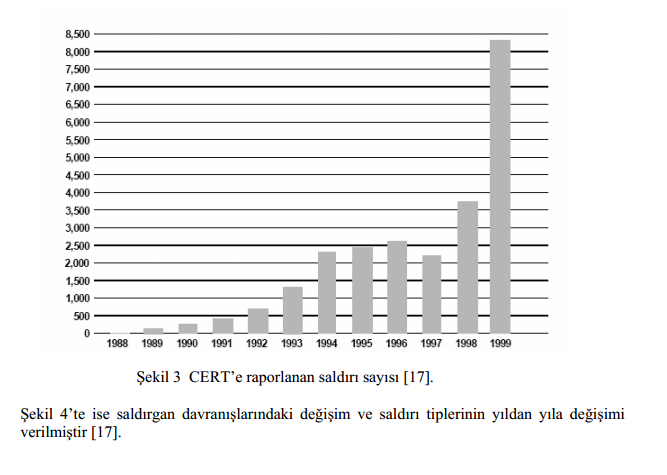
otomatikleşmiş saldırı araçları ile çok daha hızlı sürede yapılmaktadır. CERT (Computer

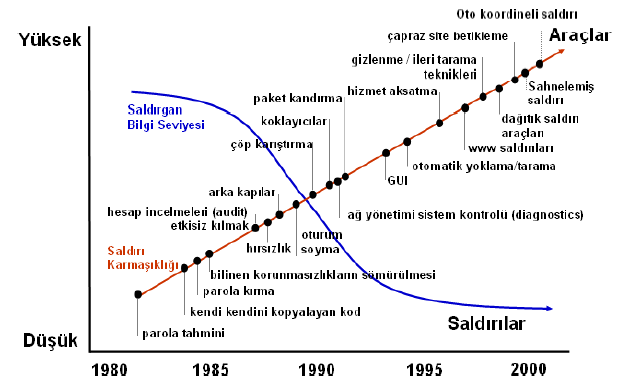
Emergency Readiness Team) tarafından 2000 yılında yayınlanan bir rapordan alınan değerler

Şekil 3’te gösterilmiştir. Saldırı sayılarındaki artışın boyutları daha o senelerden çok ciddi

boyutlara ulaşmış ve giderek elektronik ticaret uygulmalarının da artmasıyla fazlaca maddi

kayıba yol açmaya başlamıştır.



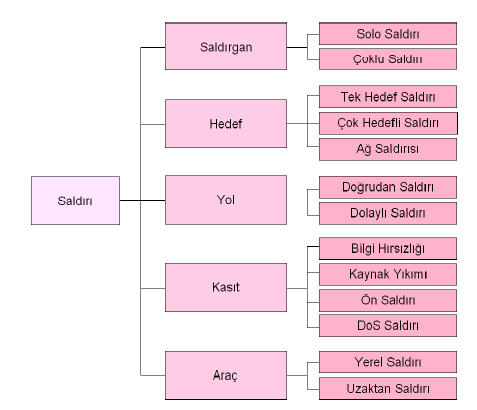


Saldırganların sahip olduğu veya olması gereken teknik bilgi seviyesi ve yaptıkları saldırıların

boyutları da zamanla değişim göstermektedir. Şekil 4’de gösterildiği gibi, saldırılar zamanla ve gelişen teknoloji ile oldukça farklılıklar göstermektedir.

Parola tahmin etme ya da işyerlerinde kağıt notların atıldığı çöpleri karıştırma gibi basit saldırılar, günümüzde artık yerini daha kapsamlı olan çapraz site betikleme (cross site scripting) , oto koordineli (auto coordinated), dağıtık (distributed) ve sahnelenmiş (staged) saldırılara bırakmıştır. Saldırılar veya saldırılarda kullanılan araçlar teknik açıdan gittikçe karmaşıklaşırken, saldırıları yürütecek saldırganın ihtiyaç duyduğu bilginin seviyesi de gittikçe azalmaktadır. Bu durum saldırı ve saldırgan sayısını, saldırılar sonucunda oluşacak zararları artırırken, saldırıyı önlemek için yapılması gerekenleri de zorlaştırmaktadır.

Saldırılar çeşitli şekillerde sınıflandırılarak incelenebilir. Saldırgan sayısına, hedef türüne, kullanılan yola, kasıt ve araçlara göre saldırılar, Şekil 5’te gösterildiği gibi sınıflanmaktadır.



**Şekil 5.** Saldırıların sınıflandırılması.

Tek bir saldırgan tarafından yürütülen solo saldırı, en genel türde saldırıların başında gelir ve saptanması daha kolaydır. Sistem korunmasızlık saldırıları ve yetkisiz erişim, solo saldırı türündedir. Birden fazla saldırganın karıştığı saldırılar, çoklu saldırı olarak adlandırılır. IP kandırma (spoofing) , e-posta bombardımanı ve ağ taşkını (flooding) bu tür saldırılardır. “Back Orifice” ve Winnuke saldırıları gibi saldırılar, tek hedefe yönelik saldırılardır. Anormal paket yayınlama saldırısı, tarama saldırısı ve anonim FTP saldırısı çok hedefli saldırılardır.

DNS kandırma (DNS Spoofing) , yönlendirici (router) saldırısı ve ağ DoS (Denial of Service, hizmet aksattırma) saldırısı, ağ saldırı türüdür. Doğrudan saldırılar arasında arabellek taşması, ölümüne ping (ping of death) saldırılarını saymak mümkündür. Yerel saldırılar sisteme giriş (login) yapıldıktan sonra Gerçekleştirilmektedir.

**SALDIRI TÜRLERİ**

Başlıca saldırı türleri arasında, kaynak kod istismarı (code exploit), gizli dinleme (eavesdropping), Gizli dinleme, Hizmet Aksattırma Saldırıları (DoS, Denial of Service) Deneme Yanılma,Casus YazılımlarDağıtılmış Hizmet Reddi ((Distributed Denial of Service–DDoS) , dolaylı saldırılar, arka kapılar (backdoor), doğrudan erişim saldırıları, sosyal veya toplum mühendisliği ve kriptografik saldırıları saymak mümkündür. Bu saldırılar aşağıda sırasıyla açıklanmaktadır.

**Kaynak Kod İstismarı (Code Exploit)**

Sistemde kullanılan (işletim sistemi için hazırlanan sistem programları dahil) tüm yazılımlarda var olabilecek arabellek taşması (buffer overflow), CGI betikleme (scripting) hataları ve şifreleme hataları gibi yazılım kusurları, bir bilgisayar sisteminin kontrolünün ele geçirilmesine veya o bilgisayarın beklenmedik bir şekilde çalışmasına neden olabilir.

Bu, son yıllara kadar gözden kaçırılan bir konu olarak, bir çok saldırıya açık kapı bırakmış bir korunmasızlıktır.

Bazı yazılım firmalarının rekabet, karlılık gibi sebeplerle geliştirdikleri yazılım paketlerinde

saptadıkları kimi hatalar için hata ayıklaması ve düzeltmesi yapmadan ürünü bir an önce piyasaya çıkarttığı bile belirtilmektedir . Özellikle işletim sistemi yazılımları tasarlanırken, geliştirilirken ve test edilirken, güvenliği hiç

bir şekilde göz ardı etmeyecek çalışmalara ihtiyaç vardır. En çok kullanılan işletim sistemi olarak belirtilen

Microsoft Windows işletim sisteminde, bu tür kaynak kod kusurları, hazırlanan güvenlik bültenleri ile kullanıcılara

duyurulmakta, çok önemli düzeltmeler (“hot-fix”) ve belirli aralıklarda çıkan hizmet paketleri, kullanıcılara gerek

çevrimiçi gerekse CD gibi ortamlarda sunulmaktadır. Bu düzeltmelerin çokluğu, işletim sistemi geliştirilmesi

sırasında öngörülmeyen veya dikkat edilmeyen yazılım kusurlarının çokluğuna işaret etmektedir. Bu konuda

Microsoft firması, piyasaya çıkardığı işletim sistemi yazılımları için güvenliği merkeze alan çalışmalara hız

vermiştir. “Güvenlik Geliştirme Yaşam Döngüsü” (SDL, Security Development Lifecycle) yaklaşımı ile geliştirilen

Windows Server 2003’ün, Windows 2000’e göre çok daha az güvenlik bülteni ile piyasaya sürüldüğü

belirtilmektedir . Microsoft, güvenliğin önemini algılamış ve bu konudaki yatırımlarını ve çalışmalarını artırmaya başlamıştır.

**Gizli Dinleme**

Bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınmasıdır. Bu saldırı tipinde, hatta kaynaktan hedefe giden verinin arada elde edilip, değiştirilerek hedefe gönderilmesi bile mümkündür.

İngilizce “eavesdropping” (saçak damlası) olarak adlandırılan bu saldırının, sanıldığının aksine çok farklı uygulama alanı bulunmaktadır.

Hiç bir bilgisayarla etkileşimi olmayan tek başına çalışan bir bilgisayar bile,

mikroçip, ekran veya yazıcı gibi elektronik parçalarından yayılan elektrik veya elektromanyetik yayılım takip edilerek gizlice dinlenebilir.

Bu cihazların bu tür dinlemelere olanak vermemesi için, Amerikan hükümeti 1950’li yılların ortasından başlayarak TEMPEST adında bir standart geliştirmiştir.

**Hizmet Aksattırma Saldırıları (DoS, Denial of Service)**

Hizmet aksattırma saldırıları, yetkisiz erişim veya sistem kontrolünü ele geçirmeye yarayan saldırılardan farklı bir amaç için gerçekleştirilen saldırılardır.

Bu saldırının tek amacı, bir bilgisayar, sunucu veya ağın kaldırabileceğinden

daha fazla yük bindirilmesi sağlanarak; sistemin kullanılmaz hale getirilmesidir. Bu tip saldırılar genelde bant genişliği, boş disk alanı veya CPU zamanı gibi bilgi işlem kaynaklarının tüketilmesi; yönlendirme (routing) bilgileri gibi yapılandırma bilgilerinin bozulması ve fiziksel ağ bileşenlerinin bozulması şeklinde yapılmaktadır.

Ağ üzerinde kilit önem taşıyan bir sunucuya yapılan bu tip bir saldırı, tüm ağın işlemez hale gelmesine yol açabilir. Bu saldırıları önlemek için tüm ağın analizi gerektiğinden, saldırıların önüne geçilmesi çok zordur. Dağıtık hizmet aksattırma saldırıları (DDoS, Distributed Denial of Service), tek bir kaynaktan değil de birden fazla ele geçirilmiş konak bilgisayardan, tek bir hedefe doğru yapılan hizmet aksattırma saldırısıdır. Yeterli sayıda saldırgan bilgisayar kullanarak, çok büyük ve iyi ağ bağlantılı web sitelerinin hizmetleri bile aksattırılabilir.

Hizmet reddi (Denial of service-DoS) hizmet aksatma amaçlı bir saldırı çeşitidir. Bir sisteme yapılan düzenli saldırılar sonucunda sistem çalışamaz ve hizmet veremez hâle gelebilir. Ayrıca DoS saldırılarıyla hedef sisteme ait kaynakların tüketilmesi de amaçlanır. Bir kişinin bir sisteme düzenli veya arka arkaya yaptığı saldırılar sonucunda hedef sistemin kimseye hizmet veremez hâle gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlanır. Bu saldırı önemli sunucuların servis vermeyi durdurması gibi büyük sorunlara yol açabilir.

Bir DoS saldırısının yaptıkları;

Nework’ü trafik ile doldurmak böylece normal network trafiğini engellemek,

İki makine arasındaki iletişimi bozar, bu sayede bir servise erişimi engeller,

Özel birinin bir servise erişimini engeller,

Servisin belirli bir sistem veya kişi ile iletişimini bozar.

Günümüzde en çok karşılaşılan yaygın DoS saldırısı şunlardır:

**SYN (eşzamanlı) taşması: S**unucuya gönderilen ve istemci bağlantısı isteyen paket taĢmasıdır. Paketlerde kaynak IP adresleri geçersizdir. Sunucu bu sahte isteklere yanıt vermekle uğraşırken geçerli isteklere yanıt veremez.

**Ping of death (Ölüm pingi):** Bir cihaza, IP tarafından izin verilen maksimum boyuttan (65,535 bayt) büyük bir paket gönderilir. Bu tür saldırılar artık bilgisayar sistemleri üzerinde etkili değildir.

**Deneme Yanılma**

Ağ kesintilerine yol açan saldırıların tümü özel olarak DoS saldırıları değildir. Hizmet reddine yol açabilen başka bir saldırı türü de deneme-yanılma saldırısıdır. Deneme yanılma saldırılarında hızlı bir bilgisayar, parolaları tahmin etmeye veya bir şifreleme kodunun şifresini çözmeye çalışmak için kullanılır. Saldırgan, koda erişim kazanmak veya kodu çözmek için art arda hızlı şekilde çok sayıda olasılığı dener. Deneme yanılma saldırıları, belirli bir kaynakta aşırı trafik oluşması nedeniyle veya kullanıcı hesaplarının kilitlenmesiyle hizmet reddine yol açabilir.

**Casus Yazılımlar**

Casus yazılım (spyware) kişisel bilgi toplama veya kullanıcının onayı alınmadan bilgisayarın yapılandırmasını değiitirme gibi belirli davranışları gerçekleştiren programlardır.

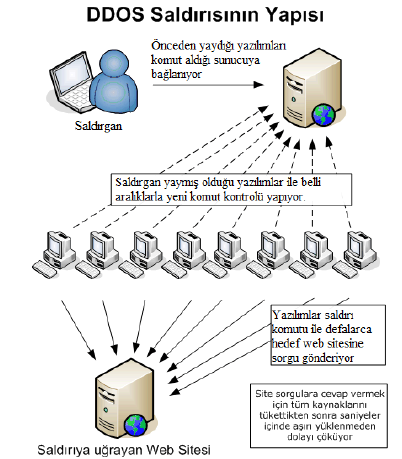
Casus yazılımlar genellikle kullanıcının onayı alınmadan bilgisayara kurulur. Kurulduktan sonra kullanıcının internette gezinti bilgileri toplanabilir. Bu bilgiler reklam veren kişi ya da kuruluşlara veya *İnternet*teki diğer kişilere gönderilir ve parola, hesap numarası gibi bilgileri de içerebilir.

Casus yazılım genellikle bir dosya indirilirken, başka bir program yüklenirken veya bir açılır pencereye tıklandığında bilmeden yüklenir. Bilgisayarı yavaşlatabilir ve dâhili ayarları değiştirerek diğer tehditler için daha fazla zayıflık oluşturabilir. Ayrıca casus yazılımı bilgisayardan kaldırmak çok zor olabilir.

**Dağıtılmış Hizmet Reddi ((Distributed Denial of Service–DDoS)**

Dağıtılmış hizmet reddi (DDoS) saldırıları DoS saldırılarının farklı kaynaklardan yapılması ile gerçekleşir. Saldırganlar bazı yazılımlar tasarlayarak (Truva atı, solucan vb.) bu yazılımları *İnternet* kullanıcılarına e-mail ya da çeşitli yollarla yükleyerek geniş kitlelere yayar. Bu şekilde yetki elde ettikleri çok sayıdaki internet kullanıcılarının bilgisayarlarını istedikleri zaman istedikleri siteye binlerce sorgu göndermek için kullanır. Saldırganın kontrolü altındaki onlarca bilgisayardan tek bir sunucuya binlerce sorgu göndermekte; bu da hedef makinenin band tüketmesine ya da tıkanmasına neden olmaktadır

.



**Dolaylı Saldırılar**

Bu tür saldırılar, uzaktan erişilerek devralınmış üçüncü parti bir bilgisayardan başlatılan değişik türde saldırıları

kapsamaktadır. Hayalet bilgisayar (zombie computer) olarak adı geçen başka bir bilgisayarın saldırıda kullanılması, saldırıyı gerçekleştiren asıl kaynağın belirlenmesini güçleştirir.

**Arka kapılar**

Bilgisayar üzerinde sıradan incelemeler ile bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlatan veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler, arka kapı olarak adlandırılmaktadır. Arka kapı, kurulu bir program şeklinde (örneğin Back Orifice) olabileceği gibi; var olan meşru bir programın bizzat kendisinde, o programı yazan kişi tarafından belgelendirilmemiş bir biçimde, kasten bırakılmış olabilir. Bu tür saldırılarda özellikle Truva atı (Trojan horse) programları yoğun bir şekilde kullanılmaktadır.

**Doğrudan Erişim Saldırıları**

Bir bilgisayar sistemine doğrudan fiziksel erişime sahip olan bir kişinin yaptığı saldırılar bu grupta toplanmaktadır.

Bilgisayara fiziksel erişim sağlayan kişi, işletim sistemlerinde kendisi için bir kullanıcı belirlemek gibi ileride

kullanılabilecek çeşitli değişiklikler yapabilir; yazılım solucanları, klavye dinleme sistemleri ve gizli dinleme cihazlarını sisteme kurabilir.

Doğrudan erişime sahip olan saldırgan ayrıca, CD-ROM, DVD-ROM, disket gibi yedekleme ünitelerini, bellek kartları, sayısal kameralar, sayısal ses sistemleri, cep telefonu ve kablosuz/kızılötesi bağlantılı cihazları kullanarak, büyük miktarda bilgiyi kendi tarafına kopyalayabilir. Bu açıdan, bir bilgisayar sistemi üçüncü şahısların kullanımına kısa süreliğine bile olsa bırakılmamalıdır.

**Sosyal veya Toplum Mühendisliği**

İnsan faktörü, her işte olduğu gibi bilgisayar sistemleri güvenliğinde de, en önemli etken olarak karşımıza

çıkmaktadır. Albert Einstein “Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı, aslında evrenin

sonsuzluğundan da o kadar emin değilim.” sözü, sosyal mühendisliğin her zaman gündemde olacağını belirtmiştir.

Bilgisayar sistemlerinde karşılaşılan güvenlik ile ilgili bir çok olay, insan faktörünün kasten veya bilerek devreyegirmesiyle meydana gelmektedir. Bilgisayar güvenliğinde sosyal mühendislik, bir bilgisayar korsanının, ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar kullanarak,

sisteme erişmek için gerekli bilgiyi elde etme tekniklerine verilen genel addır. Özellikle telefon ile kullanıcı ve şifre bilgilerini elde etme, buna en tipik örnektir. Korsan sıradan bir şirket kullanıcısı gibi sistem yöneticilerinden bu tür bilgileri edinebilir.

Bu konuda bir çok taktik düşünülebilir ve tüm bu taktiklerden yara almadan çıkmak için

yapılması gereken en önemli şey; kullanıcıların düzenli olarak eğitilmesi ve sistem yöneticileri dahil tüm

kullanıcıların istisnasız güvenlik politikalarını uygulamasıdır.

Bilgisayar sistemlerinde gerçekleşen bir çok hasar insan hatasından kaynaklanmaktadır. Kurum içi kullanıcıların aslında bizzat kendileri, kullandıkları sisteme en çok hasar

veren kişilerdir.

Bir diğer dikkat edilmesi gereken husus, bir şirketten ayrılan veya çıkartılan kişinin, daha sonradan çalışmış olduğu bu şirkete zarar vermesi veya saldırması olasılığıdır. Bunun için şirketten ayrılan kişiler için çeşitli güvenlik politikaları oluşturulmalıdır.

**Kriptografik Saldırılar**

Şifrelenmiş bilgilerin şifresini kırmak veya çözmek için yapılan saldırılardır. Bu saldırılar, kriptoanaliz yöntemleri ile gerçekleştirilmektedir. Bunlar arasında kaba kuvvet saldırısı

(brute force attack), sözlük saldırısı (dictionary attack), ortadaki adam saldırısı (man in the middle attack), sadece şifreli metin (chipertext only), bilinen düz metin (known plaintext), seçilen düz metin veya şifreli metin (chosen plaintext, chipertext), uyarlanır seçili düz metin(adaptive chosen plaintext) ve ilişkili anahtar (related key attack) saldırılarını saymak mümkündür.



**T.C**

**TRAKYA ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

**BİLGİSAYAR AĞLARINA YAPILAN SALDIRILARIN SINIFLANDIRILMASI**

**HAZIRLAYAN: 2110203371 RANA ANIL SARIKAYA**

**DANIŞMAN:DOÇ.DR.M.TOLGA SAKALLI**

**2014**

**KAYNAKLAR**

1.CERT/CC Statistics 1988-2005, Mellon Software Engineering Institute, CERT Coordination Center,

http://www.cert.org/stats/cert\_stats.html.

2. Shamir, A., Turing Lecture on Cryptology: A Status Report, ACM, 2002 A.M. Turing Award Winners, 8,

2002.ss

3. Guttman, E., Leong, L., Malkin, G., Request for Comments: 2504, Users' Security Handbook, ISOC, RFC James Cannady, “Artificial neural networks

for misuse detection,” Proceedings of the 1998

National Information Systems Security Conference

(NISSC’98), Arlington, VA, 1998.

Bace, R., 2000. Intrusion Detection, Macmillan

Technical Publishing, Indianapolis USA.

4. Bace, R. and Mell, P., 2001. Intrusion

Detection Systems, NIST Special Publication

on Intrusion Detection Systems, SP 800-31,

Gaithersburg.

5.McHugh J., Christie A., and Allen J., 2000.

Defending Yourself: The Role of Intrusion

Detection Systems, *IEEE Software*, 17(5),

6.DİRİCAN Okan Can, TCP/IP ve Ağ Güvenliği, Açık Akademi Yayınları, İstanbul, 2005. 7.ÖZBİLEN Alper, Bilgisayar Ağları ve Güvenliği**,** Pusula Yayıncılık, Ankara, 2005.

8.Wei Jiang,“Survey of network and computer attack taxonomy”, in

proceedings of 2012 IEEE Symposium on Robotics and

Applications(ISRA), 2012, pp.294-297

9. C. E. Landwehr, A. R. Bull, J. P. McDermott, W. S. Choi, “A

Taxonomy of Computer Program Security Flaws, with Examples”,

ACM Computing Surveys26( 3), 1994, pp.211-254

10.Dr.Çölkesen,R. , Prof.Dr.Örencik,B. , “Bilgisayar Haberleşmesi ve Ağ Teknolojileri” ,ISBN:975-6797-00-2 , 2002

11.S.M. Bellovin. *Security Problems in the TCP/IP Protocol Suite*. Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989.