# VERİ VE AĞ GÜVENLİĞİNE GİRİŞ(INTRODUCTION TO DATA AND NETWORK SECURITY)

Bilgisayarlaşmanın artmasıyla birlikte, dosyaları ve bilgisayarda saklanan diğer bilgileri korumak gerektiği açıktır. Özellikle, zaman-paylaşımlı ve halka açık iletişim sistemleri gibi paylaşılmış sistemlerde veri güvenliği daha da önemlidir. Veriyi korumak ve saldırganları engellemek için tasarlanmış olan sistem ve araçların genel adı Bilgisayar Güvenlik Sistemidir.

İkinci ana konu, dağıtık sistemler ve son kullanıcının terminali ile bilgisayar arasındaki veri taşıyan haberleşme olanaklarının güvenliğe etkileridir. Ağ güvenliği tedbirleri verinin iletimi sırasında onun korunmasını esas alır. Gerçekte ağ güvenliği kavramı, bütün iş yerleri, devlet ve akademik kuruluşlar veri işleme birimlerini birbirlerine iletişimi ağ ile bağladıkları için ortak bir ağ ortaya çıkar ki bunda birbirine bağlı ağlar adı verilir. Bu durumda koruma, ağ’daki bütün birimleri kapsar.

#### Bazı Güvenlik Tecavüzleri

* Kullanıcı A , Kullanıcı B’ ye bir dosyayı transfer eder. Dosya, bozulmadan korumayı gerektiren hassas bilgileri(Ödeme bordrosu gibi) içermektedir. Dosyayı okumaya yetkili olmayan kullanıcı C, iletimi gözleyebilir ve iletim sırasında, dosyanın bir kopyasını alabilir.
* Bir ağ yöneticisi olan D, kendi yönetimindeki bilgisayar E’ ye bir mesaj gönderir.Gönderilen mesaj, E’ de bir grup kullanıcının bilgisayar erişim yetkilerinin güncellemesini içerir. Kullanıcı F, mesajı alıp,içeriğini değiştirerek, D’den geliyormuş gibi E’ ye gönderir. E’ de bu şekliyle kullanıcıların yetkilendirilmelerini günceller.
* Kullanıcı F, aldığı bir mesajı değiştirmek yerine kendi mesajını hazırlayarak sanki D’den geliyormuş gibi E’ ye gönderir. E aldığı bu mesaja göre yetkilendirme dosyasını günceller.
* Farklı işlemler için ,müşteriden geliyormuş gibi borsa aracısına gönderilen bir mesaj ile para kaybı’na neden olunur ve müşterinin mesaj göndermesi engellenebilir.

#### Saldırılar servisler ve Mekanizmalar.

1. **Güvenlik saldırısı:** Bir kuruluşun bilgi güvenliği saygınlığını azaltır. Engelleme, Dinleme, Değiştirme ve yeniden oluşturma olarak 4 sınıf saldırı vardır.
2. **Güvenlik Mekanizması:** Bir güvenlik atağının anlaşılması, korunma veya onarımdır.
3. **Güvenlik Servisi:** Veri işleme sistemi ve kuruluşun bilgi iletim sisteminin güvenliğini artırma servisidir. Servis güvenlik saldırılarını engeller ve servis sağlamak için çeşitli güvenlik mekanizması kullanır.

**Güvenlik Servis özellikleri aşağıda açıklanmıştır.**

* **Gizlilik:** İletilen verinin pasif saldırılardan korunması. Diğer bir konu trafik akışının analiz edilmekten korunması. Bir saldırganın kaynak ve hedef arasında trafiği izlemesi önlenir.
* **Yetkilendirme**: Bu servis, haberleşmenin yetkili kişilerce yapılmasını sağlar. İkaz veya alarm gibi tek bir mesaj durumunda, yetkilendirme servisininin fonksiyonu, alıcıya mesajın kaynağı konusunda güven vermektir.
* **Bütünlük:** Mesajın bütünlüğünü sağlar. Mesajın tamamının değişmemesini temin eder.
* **İnkar edilememe**: Gönderici veya alıcının iletilen bir mesajı inkar etmemesini sağlar.
* **Erişim Denetimi:** Erişim denetimi ağ güvenliğinde, host sistemlere ve uygulamalara haberleşme bağlantıları ile erişimi sınırlandırır. Bu denetimi sağlamak için, her bir kişiye erişim hakkı verilmelidir.
* **Kullanıma hazırlık:** Saldırıların bir kısmı kullanılabilirliğin azalması veya kaybolmasına neden olabilir. Saldırıların bir kısamı iyi niyetli olabilir, oysa bir kısmı sistemin kullanılabilirliğini engeller. Bu servis kullanılabilirliğin sürekli olmasını sağlamaya yöneliktir.

### Güvenlik mekanizmaları

Bilgi ve ağ güvenliğini sağlamak için birçok mekanizma mevcuttur. Bunlar kriptografik teknikler,

şifreleme benzeri transformasyonlar sıkça kullanılan tekniklerdir.

### Saldırılar

Bilgi sistemini saldırılardan korumak için saldırıları tanımak gerekir. Bu kapsamda tehdit(threat) ve saldırı(attack) termilerini kısaca açıklamak gerekir. **Tehdit**, belirli durum, yetenek, veya olay olduğu anlarda güvenlik foksiyonunun yerine getirilmesini engelleyen potansiyel bir güvenlik bozucusu olduğu halde; **saldırı**, sistemin güvenlik servislerini etkisiz hale getirmeyi amaçlayan akıllı bir tehditten üretilen ani bir hücumdur.

Bazı örnek saldırılar aşağıda verilmiştir.

Bilgilere yetkisiz erişimin elde edilmesi

Başka bir kullanıcının yetkilerini alarak onun yerine geçme Saldırganın yasal lisansını genişletme

Saldırganın kendisini haberleşme yapan kullanıcıların arasına yerleştirmesi Haberleşme hattının dinlenilmesi

Haberleşmenin engellenmesi

Saldırgan tarafından oluşturulan diğer bir kullanıcıya ait bilgilerin alındığını açıklamak

İletilen bilgilerin içeriğinin değiştirilmesi.

### OSI Güvenlik Mimarisi

Bilgi güvenliğinde sistematik bir yaklaşım olarak X.800 OSI güvenlik mimarisi, yöneticilerin güvenlik oraganizasyonlarını düzenlemeleri için önemli bir yaklaşımdır. OSI yaklaşımı güvenlik servisleri, mekanizmalar ve saldırılara yoğunlaşmıştır.

### Güvenlik Servisleri

Kimlik Doğrulama(Authentication) Erişim Denetimi(Access Control) Veri Gizliliği(Data Confideality) Veri Bütünlüğü(Data Integrity) İnkar edememe(Nonrepudation)

### Güvenlik Mekanizmaları

X.800 OSI güvenlik mimarisinde mekanizmalar iki grupta toplanmıştır., Kendine özgü güvenlik mekanizmaları

Şifreleme, Sayısal imzalar, Erişim dentimi, Veri bütünlüğü, Kimlik doğrulama, Trafik analizini önleme, Yönlendirme denetimi ve noter makamı kullanılması

Kendine özgü olmayan güvenlik mekanizmaları

Güvenli fonksiyonellik, Güvenlik etiketi, Olay ortaya çıkartma, Güvenlik denetleme izleme, Güvenlik geri kazanımı

### Güvenlik saldırıları

X.800 mimarisinde güvenlik saldırıları pasif ve aktif saldırılar olmak üzere iki türlüdür.

Pasif saldırılar, mesaj içeriğinin ifşa edilmesi ve trafik analizidir. Veri içeriği değiştirilmediği için pasif saldırıları ortaya çkartmak çok güçtür. Bu saldırılardan korunmak , anlamaktan daha uygun çözümlerdir.

Aktif Saldırılar, saldırganın kimliğini gizlemesi(masquarade), geri gönderme(replay), Mesajın değiştirilmesi(modification of message) ve servis durdurma(denial of service) dir.

Aktif saldırılar pasiflere göre zıt özelliktedirler. Aktif saldırılar tespit edilebilirler ve karşı önlem alınabilirler. Buna karşı aktif saldırıları tamamen önlemek çok zordur.

### Ağ Güvenliği için bir model

Ağ güvenliğinde genel bir model şekil 1.1’de gösterilmiştir. Gönderici ve alıcı mesajları gizli olarak iletirken ,güvenli bir üçüncü şahıs gizli bilgilerin dağıtıcısı olarak hizmet vermekte, her iki taraf arasında noter görevi de görmektedir.

Bu genel güvenlik mimarisi, güvenlki servislerinin tasarımında dört temel işi gösterir.

1. Güvenlik ilişkili dönüşümler için bir algoritma tasarımı
2. Algoritma ile kullanılacak gizli bilginin üretimi
3. Gizli bilginin dağıtımı ve paylaşımı için yöntem geliştirme
4. Güvenlik algoritmasını ve güvenlik servisini sağlayacak gizli bilginin kullanımını sağlayacak bir protokol belirleme.

Güvenli üçüncü şahıs (,hakem,gizli bilgi dağıtıcısı)

Yönetici Yönetici

Mesaj

Gizli Bilgi

Bilgi Kanalı

Mesaj

Gizli Bilgi

Güvenlikle ilgili dönüşüm

Gizli Bilgi

Güvenlikle ilgili dönüşüm

Şekil-1.1. Ağ Güvenliği için Model

# GÜVENLİK GEREKLERİ VE KORUNACAK VARLIKLAR (Why Secure Your Network)

#### Giriş

Bilgisayar ağları, insanların bilgiye kolay ulaşımı, dolayısıyla çalışmalarındaki verimin artmasını sağlayan büyük bilgi ağlarıdır. Bilgiye kolay ulaşım için sunulan hizmetler (servisler, http, ftp, vs) aynı zamanda zarar verilebilme riski de taşımaktadır. Bilgisayar ağlarının sunduğu imkanlardan faydalanmak, fakat gelebilecek zararları en aza indirmek gerekir. Fakat bu tedbir birtakım şeylerden ödün vermemizi gerektirir. Güvenliği ön plana almak, hızı da aynı oranda azaltmak anlamına gelmektedir.

Alınabilecek güvenlik önlemlerini tartışmadan önce güvenlik konusunun neden gerekli olduğunun, nelerin korunması gerektiğinin anlaşılması daha faydalı olacaktır.

#### Korunacak varlıklar

Bir ağda güvenlik ile ilgili bir çalışma yapılmaya başlandığında ilk karar verilmesi gereken nelerin korunması gerektiğidir. Korunması gereken varlıklar üç ayrı ana başlıkta toplanabilir.

1. Veriler
2. Kaynaklar
3. Saygınlık

Bu varlıklar ayrı ayrı incelenecektir.

#### Veriler

Veriler, güvenlikle ilgili olarak üç özelliğe sahip olmalıdır;

* + - * Gizlilik: Verilerin , başkaları tarafından öğrenilmesi istenmeyebilir.
      * Bütünlük : Sahip olunan verilerin başkaları tarafından değiştirilmesi istenmeyebilir
      * Kullanıma hazırlık: Verilerin istendiği zaman ulaşılabilir olup kullanıma hazır olması istenir.

Daha çok gizlilikle ilgili güvenlik üzerinde durulur. Gerçekten de bu konuda risk çoktur. Bir çok kişi ya da kuruluş için gizli bilgiler bilgisayar üzerinde tutulur. Bu bilgisayarların güvenliği de internet bağlantısı kopartılarak sağlanmaktadır. Bu şekilde bilginin gizliliği sağlanmış olabilir ama kolay ulaşılabilirlik ortadan kalkmış olur. Yani bir şekilde ağa bağlanılmalıdır. Bu durumda güvenlik politikaları belirlenerek, bilgilerin güvenliğinin sağlanması gerekmektedir.

#### Kaynaklar

Halka açık olan ağlara(İnternet’e) bağlanmakla riske atılacak ikinci şey, bilgisayar kaynaklarıdır. Başka insanların bir kuruluşa ait bilgisayardaki sabit diskte yer alan boş alanları kendi amacı için kullanmak istemesi her ne kadar mevcut verilere zarar vermeyecek bir şey olsa da istenecek bir durum değildir. Bunun gibi diğer kaynakların da (işlemci,bellek, ...) başkaları tarafından kullanılması, kabul edilebilir bir şey olamaz

#### Saygınlık

Her kişi ya da kurumun saygınlığının ağ üzerinde de korunması önemlidir. Meydana gelebilecek güvenlik problemleri kişi ve kurumların doğrudan aleyhine olup kötü reklamdır. ağ üzerinde

işlemler yapan bir kişinin, başka bir kişinin adını kullandığı düşünülürse, zarar verme durumunda doğrudan muhatap alınacak kişi saygınlığını kaybetme durumuyla karşı karşıya kalacaktır.

Genelde başka birinin hesabından girip sahte elektronik postalar atarak zarar verilir. Bunun sahte olduğunun kanıtlanması neredeyse imkansızdır. Böyle durumlarda, sahteciliği yapan kişinin kullandığı hesaba sahip kişi kadar kurum da zarar görür.

Halka açık ağlara(örn.internet) açılmayı düşünen kurumların eğitim ya da güvenlik politikası içinde, saygınlığın korunması için kişilere düşen güvenlik tedbirlerinin anlatılması gerekir. Ayrıca periyodik olarak takibinin yapılması şarttır.

#### Bilgisayar Ağına Saldırı

* + 1. ***Giriş***

Internet’in doğuşu ve gelişimi arasında aslında çok kısa bir zaman aralığı vardır. Bu kadar hızlı bir büyümenin olabileceği Internet’in doğuş yıllarında beklenmiyordu. Özellikle 1985 yılından sonra büyük yatırımlar yapıldı ve hızla yaygınlaştı. Ama bu hızlı gelişim birtakım konuların standartlarının tam olarak oluşturulmadan kullanıma geçirilmesinden dolayı bazı sorunları beraberinde getirdi. Özellikle de güvenlik sorunlarını ortaya çıkardı.

Güvenlik hemen her bilgisayar ağında öncelikli olarak düşünülmesi gereken bir konudur. Halka açık ağ(Internet) ortamında ise çok daha önemlidir. Birçok ticari firma ya da başka kuruluşlar ürünlerini ve hizmetlerini Internet ortamına aktarmak istemektedirler. Ancak bu birtakım risklerin de alınması gerektiği anlamına da gelir. Değişik güvenlik mekanizmalarının bir arada kullanılmasıyla bu riski azaltmak mümkündür.

#### Saldırganlar

Saldırgan (Hacker), ağ üzerindeki genelde bazı servisler veren makinalara hiçbir hakkı olmadan erişip zarar veren kişidir. Bilgi hırsızı olarak da tarif edilebilir. Fakat ev ya da banka soyguncularından çok farklıdırlar. İyi görünümlü, sistemler hakkında çok bilgisi olan insanlardır. Genellikle sistemin bilinen açıklıklarından ve sistem yöneticisinin bilgisizliğinden faydalanırlar.

İstatistiki raporlara göre saldırıların çoğunun firma içerisinden yapıldığı tespit edilmiştir. İçeriden gelen saldırı, sistem sadece dışarıya karşı korunmalı durumda ise çok zarar verebilir.

Saldırganların büyük firmaların ağına girdikleri ve büyük ölçekte sitemlere zarar verdikleri bilinmektedir. Bunu genellikle eğlence, kendini göstermek ya da sisteme zarar vermek için yaparlar.

Saldırganlar iki genel türde toplanabilir:

* + - 1. Kötü niyetli saldırganlar
      2. Kötü niyetli olmayan saldırganlar
      3. **Kötü niyetli saldırganlar (Malicious hacker)**

Sisteme gerçekten zarar vermek amacıyla girerler. Açığını buldukları sistemlere verebilecekleri en büyük zararı vermeyi amaçlarlar. Bu tür saldırganlar genelde ekip halinde çalışırlar. Kredi kartları kullanan sitelerden kart numaralarını ve parolalarını alıp kişi ve şirketlere büyük zararlar verebilirler.

Tablo2-1’de belirtilen bilgisayar korsanları, casuslar,teröristler ve profesyonel suçlular bu gruba girmektedir.

### Kötü niyetli olmayan saldırganlar

Sistemlere genellikle eğlenmek için saldırıda bulunurlar. Çok fazla zararlı olmayan tiplerdir. Hatta sistem yöneticisi eksikliklerini ve sistemin zayıf noktalarını bu sayede görebilir. Bu tür saldırganlar, bir saldırgan grubuna üye değildir. Genellikle yaptıkları, kendilerine daha sonra kullanmak için hesap açmak ve sistemin zayıf gördüğü yerleri belirten notlar koymaktır. Bu işi zevk için yapan insanları bu kategoriye sokabiliriz. Bu gruba girenler aşağıdaki tabloda meraklılar olarak belirtilmiştir.

Saldırgan, kullandığı araçlar, sisteme erişim yolları ve amaçlarının ne olabilecekleri tablo 2-1’de özetlenmiştir.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Saldırganlar | Araçlar | Erişim | Sonuç | Amaç |
| Bilgisayar  korsanları | Kullanıcı  komutları | Gerçekleme  zayıflıkları | Bilgi bozma | Finansal kazanç |
| Casuslar | Komut dosyası  veya Program | Tasarım  zayıflıkları | Bilgi çalma ya da açığa  bilgi çıkartma | Politik kazanç |
| Teröristler | Araç takımı | Yapılandırma  zayıflıkları | Hizmet çalma | Sosyal statüye  meydan okuma |
| Meraklılar | Dağıtık araçlar | İzinsiz erişim | Hizmet önleme | Zevk için |
| Profesyonel  suçlular | Veri dinleyici  sistemler |  |  |  |

Tablo 2-1 Saldırganlar ve amaçları

#### Saldırı Türleri

Bu bölümde son yıllarda internette kullanılan saldırı yöntemlerine değinilecek ve sınıflandırılmaya çalışılacaktır. Saldırıların tanımları yapılacak ve sisteme verebileceği zararlar üzerinde durulacaktır. Saldırıya karşı alınabilecek önlemler güvenlik duvarı olmaksızın anlatılacak ve güvenlik duvarı düzeyinde yapılabilecekler açıklanacaktır.

Saldırganlar sisteme ağ üzerinden ulaşabilecekleri için, ağa bağlı cihazlar her zaman saldırıya açık durumdadır. Burada yapacakları, hedef makinaya ulaşmak, yazılım ve donanıma zarar vermek şeklinde olabilir. Şirkete ait veritabanına ulaşıp verilere erişebilir, değiştirebilir ya da silebilirler. Burada asıl olan, saldırganın ne yapmak istediğidir. İşine yarayan kayıtları, dosyaları alabilir ve sisteme (yazılım, donanım) zarar verebilir. Verilen hizmetleri servis dışı bırakabilir. Sadece Internet bağlantısına zarar verebilir. Truva atı türünde programları bir şekilde hedef makinaya yükleyerek kullanıcıyı takip edebilir.

### Saldırıların Sınıflandırılması

Bilgisayar ve ağ saldırıları için değişik sınıflandırmalar yapılmıştır. Aşağıda süreçsel ve işlemsel sınıflandırmalar anlatılacaktır.

* + - * 1. **Süreçsel Sınıflandırma**

Internet’te gerçekleştirilen veri transferiyle ilgili güvenlik sorunları dört kategoriye sokulabilir.

**Engelleme:** Sistemin bir kaynağı yok edilir veya kullanılamaz hale getirilir. Donanımın bir kısmının bozulması iletişim hattının kesilmesi, veya dosya yönetim sisteminin kapatılması gibi.

**Dinleme:** İzin verilmemiş bir taraf bir kaynağa erişim elde eder. Yetkisiz taraf, bir şahıs, bir program veya bir bilgisayar olabilir.Ağdaki veriyi veya dosyaların kopyasını alabilir

**Değiştirme:** İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklik de yapar. Bir veri dosyasının değiştirilmesi, farklı işlem yapmak üzere bir programın değiştirilmesi ve ağ üzerinde iletilen bir mesaj içeriğinin değiştirilmesi gibi.

**Oluşturma:** İzin verilmemiş bir taraf, sisteme yeni nesneler ekler. Ağ üzerine sahte mesaj yollanması veya bir dosyaya ilave kayıtlar eklenmesi.

Burada dinleme pasif bir saldırı türüdür. Engelleme, değiştirme ve oluşturma ise etkin bir saldırı türü olarak görülmektedir.

Normal Akış

Bilgi Hedefi

Bilgi Kaynağı

(3) Değiştirme

Bilgi Hedefi

Bilgi Kaynağı

(1) Engelleme

Bilgi Hedefi

Bilgi Kaynağı

(4) Oluşturma

Bilgi Hedefi

Bilgi Kaynağı

(2) Dinleme

Bilgi Hedefi

Bilgi Kaynağı

Şekil 2-1 Süreçsel Sınıflandırma

#### İşlemsel Sınıflandırma

Genel anlamda bir saldırı yöntemler, kullanılan yollar ve sonuçları açısından düşünülebilir. Bilgisayar ya da bilgisayar ağına saldıran kişi, istediği sonuçlara çeşitli adımlardan geçerek ulaşmak zorundadır. Bu adımlar aşağıdaki şekil 2-2 den de görüldüğü gibi araçlar,erişim ve sonuçlar şeklindedir.

Saldırganlar

Araçlar

Erişim

Sonuçlar

Amaçlar

Şekil 2-2 İşlemsel Sınıflandırma

#### Saldırıların Gruplandırılması

Saldırıları değişik açılardan değerlendirerek, değişik gruplamalar yapmak mümkündür. Saldırıda kullanılan yöntem, saldırının kullandığı yöntem, saldırının amaçladığı uygulamalar ve saldırı sonucunda oluşan zararlar gruplama için kullanılabilecek yöntemlerdir.

### CERT Gruplandırması

(Computer Emergency Responce Team) tarafından yapılmış olan saldırı türleri ve açıklamaları tablo2-2’de listelenmiştir.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Probe,Scan,Scam | Bir sistemdeki açık ve kullanılan portların taranması ve bu portlardan  hizmetlere yönelik saldırıları türüdür. | | | | | | | | |
| Prank | Kullanıcı hesaplarının yanlış oluşturulması sonucu oluşan açıklardan  yapılan saldırı türleridir. | | | | | | | | |
| Email spoofing | Başka bir kullanıcı adına e-posta gönderilmesi... | | | | | | | | |
| Email  bombardment | Bir e-posta  gönderilmesi | adresine | | genelde | farklı | adresten | çok | sayıda | e-posta |
| Sendmail attack | Smtp portuna yönelik saldırılardır... | | | | | | | | |
| Break-in | Verilen hizmetlerin devre dışı bırakılmasına yönelik saldırı türüdür. | | | | | | | | |
| Intruder gained root  access | Saldırganın normal kullanıcı olarak girdiği sistemde süper kullanıcı  yetkisini kazanması. | | | | | | | | |
| Intruder installed trojan horse  program | Saldırganın girdiği sisteme genelde daha sonra tekrar rahat girebilmesi ya da uzaktan yönetim için ajan program yerleştirimesi. | | | | | | | | |
| Intruder installed packed sniffer | Saldırgan tarafından hedef makinaya yönelik paket dinleyici yerleştirilerek yapılan saldırı türüdür. Bu şekilde bir yerel ağ korumasız  bir konak üzerinden saldırılara açık hale gelebilir. | | | | | | | | |
| NIS attack | Ağ kullanıcı yönetim sistemine yönelik saldırı türüdür. | | | | | | | | |
| NFS attack | Ağ dosya yapısına yönelik saldırı türüdür. Genellikle ağ erişimini devre  dışı bırakmada kullanılır. | | | | | | | | |
| Telnet attack | Uzaktan erişim protokolünün açıklarından faydalanılarak yapılan saldırı  türüdür. | | | | | | | | |
| Rlogin or rsh attack | Uzaktan erişimde kullanılan servislerin açıklarına yönelik yapılan saldırı  türüdür. | | | | | | | | |
| Cracked password | Kolay tahmin edilebilir parolaların tahmini ya da şifreli hallerine göre  sözlük saldırısı yapma türüdür. | | | | | | | | |
| Anoymous FTP  abuse | Anonim erişim  saldırılardır. | | izni | verilen | dosya | aktarım | sunucularına | | yönelik |
| IP spoofing | IP adres yanıltmasıyla yapılan saldırı türüdür. | | | | | | | | |
| Configuration error | Çok kullanılan programdaki kullanıcılardan kaynaklanan konfigürasyon  hatalarından doğan açıklıklardır. | | | | | | | | |
| Misuse of hosts  resources | Konak kaynaklarının yanlış kullanımı sonucu ortaya çıkan açıklıklar. | | | | | | | | |
| Worm,Virus | Konaklarda kullanıcılardan habersiz çalışan zararlı programlar. | | | | | | | | |

Tablo 2-2: Saldırı türleri

Yukarıda da belirtildiği gibi değişik gruplamalara gitmek mümkündür. Bazı saldırıları sadece bir gruba koymak mümkün değildir.

[www.cert.org](http://www.cert.org/) adresinde bu gruplandırılmış saldırıların ne kadar süredir var olduğu, ne tür zararlara yol açtığı ve yaygınlığı gibi bilgiler bulunmaktadır.

### İletişim Protokollerini Kullanan Saldırılar

IP sahteciliği (IP spoofing)

TCP dizi numarası saldırısı (TCP sequence number attack) ICMP atakları

Ölümcül ping

TCP SYN seli atağı (TCP SYN Flood Attack) IP parçalama saldırısı (IP Fragmentation Attack)

Internet yönlendirme saldırısı (Internet Routing Attacks) UDP sahteciliği ve Dinleme (UDP Spoofing and Sniffing)

UDP portunu servis dışı bırakma saldırısı (UDP Port Denial-of-Service Attack) Rasgele port taraması (Random port scanning)

ARP saldırıları (ARP Attacks) Ortadaki adam saldırıları

### IP saldırıları

IPV4’te bulunan güvenlik eksikliklerinden faydalanılarak yapılan atak türleridir. Bazı örnekleri şunlardır: Out of Band Nuke, Land, Teardrop, Boink, Nestea, Brkill, ICMP Nuke, Jolt/Ssping, Smurf, Suffer3

Bu saldırılardan bir kısmı detaylı olarak anlatılacaktır.

### İşletim sistemine özel saldırılar

Exploit olarak isimlendirilen bu saldırılar, sistem tabanlı olarak çalışırlar. Yani Unix için yapılan bir exploit MS Windows için çalışmaz.

Windows Null Session Exploit PHF Exploit

ASP Exploit Sendmail Exploit

### Uygulama Katmanı Saldırıları

DNS,SMTP,MIME,NFS,NTP saldırıları

Uzaktan giriş ile saldırılar (Hacking and Remote Login) Bilgi sızdıran saldırılar

URL sahteciliği (URL Spoofing) CGI saldırıları

X-Windows sistem saldırıları

Kötü niyetli java ve AktiveX uygulamacıkları Sistem log seli

Program ve ağ üstündeki virüsler

Sistem log seli güvenlik duvarına çok sayıda giriş yapılarak log dosyasının dolmasına ve sonuç olarak sistemin kapanmasına neden olan saldırı türüdür.

#### Bazı Saldırı Yöntemleri

Artık klasik hale gelmiş ve genelde iletişim protokollerinin deliklerinden yararlanılarak yapılan saldırılar anlatılacaktır.

### IP Aldatması (IP Spoofing)

Aldatma saldırısının genelde yapılan türü IP aldatmasıdır. Sahtecilik olarak çevirmek mümkündür. IP paketlerinin kaynak IP' sini değiştirmekle sağlanmaktadır. Böylece paketi alan hostun, paketin geldiği kaynak adresini bilmesini engellenmiş olur. Host gelen paketin saldırgandan değil de kullanıcıdan geldiğini sanır.

IP adreslerine göre çalışan servisler üzerinde oldukça etkilidir. Sahte paketler üretme (fabrication) bu şekilde yapılabilmektedir.

Internet’e bağlanan bilgisayarlar birbirleriyle IP adreslerini kullanarak haberleşmektedir. IP paketleri üretildiği bilgisayardan hedef bilgisayara IP adreslerini kullanarak giderler. İletişimde bulunulan bilgisayarın IP numarasının bilinmesi güvenlik açısından oldukça önemlidir. İnternet’te servis veren bazı bilgisayarlar sadece belirli IP adreslerine hizmet verirler. Güvenlik duvarlarının kullandığı paket filtreleme mekanizması genelde bu adresler üzerinde yapılır. Paket filtreleme örneğinde de anlatıldığı gibi bazı IP adreslerine ait paketlerinin geçişine izin verilir ya da reddedilir.

Ayrıca güvenlik duvarı kullanılarak, bazı IP adreslerine verilecek hizmetlerin sınırlandırması da sağlanabilir. Gelen isteğin kaynak IP adresine bakılarak böyle bir işlem yapılır. Bunun anlamı kullanıcıya IP adresine göre yetki vermektir. IP adresine bakılarak yetki verilmesi çalışmaları rahatlatacaktır; fakat güvenlik açısından bazı riskler taşımaktadır.

Kaynak IP adresine göre yüksek yetki verilen bir kullanıcıya ait adres bilinmesi durumunda risk ortaya çıkmış olur. Saldırgan kaynak IP adresini değiştirmek suretiyle hakkı olmayan bir yetkiyle sisteme girebilir.

Saldırganın sahte IP paketleri kullanarak sisteme girmesi durumunda verebileceği zarar, IP adresine verilen yetkiyle orantılıdır. Bu şekilde yetkili kullanıcı olarak sisteme girebilen bir saldırgan sisteme çok kolay ve oldukça fazla zarar verebilir.

Böyle bir saldırıya karşı alınabilecek önlem yoktur. Ancak Kaynak IP yanında Hedef IP ve MAC adresine de bakılarak saldırı olduğuna karar verilebilir. Bunu iç ağın Internet’e açıldığı noktaya güvenlik duvarı kurmakla sağlamak mümkündür.

### TCP SYN paketi akışı saldırıları

IP adresi kullanılarak gerçekleştirilen bir saldırı türüdür. Genelde TCP/IP servislerinin devre dışı bırakmak için kullanılır.

TCP bağlantı temelli bir protokoldür. Birbiriyle iletişim kuran iki bilgisayar, paketlerini kurulu bir hat üzerinden aktarırlar. Bunun için de iletişim başlangıç aşamasında bu hattın kurulması gerekir. Bu da bazı el sıkışma kurallarıyla mümkün olmaktadır. TCP protokolünün el sıkışma sistemi üç yollu el sıkışma (three way handshake) mekanizmasıdır. Üç yol denmesi, bu işlemin üç aşamada gerçekleşmesinden dolayıdır.

İlk olarak, bir sunucu bilgisayardan servis isteyecek diğer bilgisayar (istemci), bağlantı kurmak istediğini göstermek için SYN bayrağı kalkık(set) paketini, sunucu bilgisayara gönderir. Bu paketi alan sunucu SYN paketi aldığını ve bağlantı isteğini onayladığını yine SYN bayrağı kaldırılmış(set) paketi (SYN-ACK paketi) istemci bilgisayara gönderir. Üçüncü aşamada ise sunucu bilgisayarın gönderdiği SYN-ACK paketini alan istemci bilgisayar sunucuya bu paketi aldığını bildiren bir paket gönderir(ACK).

Bağlantı

isteği

SYN (SN\_A)

Cevap



SYN(SN\_B),

ACK(SN\_A+1)

istemci

ACK(SN\_B+1)

### A

~~veriler~~

Şekil 2-3 TCP el sıkışma mekanizması

sunucu

### B

Bu mekanizmada saldırıya açık nokta, bir bilgisayarın istemci olarak bir bilgisayara el sıkışma mekanizmasını başlatacak SYN paketini göndermesi, buna karşılık sunucu bilgisayardan SYN- ACK paketini aldıktan sonra son paketi (ACK) göndermemesi ile oluşur. Böyle bir durumda sunucu tarafında açılmış fakat tamamlanmamış bir bağlantı isteği oluşacaktır. Bu bağlantı isteği uzun bir süre dolumuna kadar açık tutulacaktır. Bu tür bağlantılara yarı açık bağlantılar denir. Bu mekanizmanın kötüye kullanılabilecek noktası, arka arkaya belirtilen bu işlemlerin yapılmasıyla ortaya çıkar. Böyle bir durumda yarı açık birçok bağlantı oluşacaktır.

Herhangi bir hizmet bir port üzerinden verilmektedir. Buraya gelen istekler bir kuyruğa alınır ve istemciden üç yollu bağlantıdaki son paket gelene kadar kuyrukta tutulur. Dolayısıyla kuyruktaki tamamlanmayan bağlantı isteklerinin artması kuyruğun dolmasına sebep olacaktır. Kuyruk dolduğunda ise yeni gelen bağlantı isteklerine cevap veremeyecektir. Dolayısıyla servis kilitlenecektir. Bazı sistemlerde bellek taşmasına sebep olacağından bu durum sunucu bilgisayarı devre dışı da bırakabilir.

Bu saldırıyı önlemek için TCP protokolü üzerinde açıklıklarını kapatacak değişiklikler yapılmaktadır. Bu değişiklikler paket filtreleme düzeyinin üstünde TCP protokolü düzeyinde yapılmaktadır.

### TCP sıra numarası tahmini yoluyla gerçekleştirilen saldırılar

Daha önce IP adresi yoluyla yanıltma yöntemi anlatılırken, IP adresine göre yetkilendirme yapan servislere karşı bu yöntemin kullanılması durumunda sistemin saldırıya karşı olduğundan bahsedilmişti. IP adresi yoluyla yanıltma tekniğinin birlikte kullanıldığı yöntemlerden biri TCP sıra numarası tahmini yoluyla yapılan saldırıdır. Bu TCP/IP protokolünün açıklıklarından olarak kabul edilir. IP adresine göre yetkilendirme yapan programlara saldırılarda bu yöntem kullanılır.

Bu saldırıyı anlamak için TCP protokolündeki üç yollu el sıkışma mekanizmasını detaylı incelemek gerekmektedir. TCP protokolü daha öncede bahsedildiği gibi bağlantı temelli bir protokoldür. Bunun anlamı bir oturuma ilişkin IP paketlerinin aktarılması sırasında verilen güvendir. Hedef uca uygun sırada ulaşmamaları durumunda, düzenlenmesi ve aradan paketlerin gelmemesi durumunda da tekrar o paketin istenmesi TCP katmanında yapılmaktadır. Bunları gerçekleştirmek için bazı mekanizmalar kullanılır. TCP sıra numarası (TCP sequence number ), gönderilen paketlerin oturum içindeki sırasını gösterir. Bu değer kullanılarak doğru sırada alınmamış paketlerin sıraya konulması ve en son alınan pakete ilişkin bilgilendirme karşı tarafa yapılmaktadır. Bu sayede paketin hedefe ulaştığından emin olunması sağlanmış olur; aksi durumda paketin tekrar gönderilmesi işlemi yapılır.

Saldırıya açık kısmı ise, TCP üç yollu bağlantı şekli üzerinden açıklayalım. İstemci bilgisayar sunucu bilgisayara istekte bulunacağını bir SYN paketi göndererek ifade etmektedir. Bu pakette J

ile gösterilen, istemci bilgisayarın gönderdiği bilgilere verdiği sıra numarası bilgisidir. Bu paketi alan sunucu bilgisayar cevap olarak SYN-ACK paketi göndermektedir. Bu pakette de, K ile gösterilen,sunucu bilgisayarın gönderdiği pakete verdiği sıra numarası vardır. SYN(K) ile gösterebileceğimiz bu bilgiyle birlikte, haberleşmenin senkronize bir şekilde devam etmesini sağlamak üzere istemci tarafından gönderilen ve J sıra numarasını taşıyan paketin alındığına ilişkin bilgilendirmenin de yapılması gerekir. Bu amaçla da ACK(J+1) ile gösterebileceğimiz ve en son alınmış olan pakete ilişkin sıra numarası bilgisi de ACK olarak istemci bilgisayara gönderilir. Bu paketi alan istemci bilgisayar da, sunucunun göndermiş olduğu son paketi aldığını göstermek üzere ACK(K+1) paketini sunucuya göndererek, bağlantının kurulması işlemini tamamlar. Bağlantının kurulabilmesi ve daha sonra da devam edebilmesi için bu bilgilendirme ACK paketlerinin karşılıklı olarak aktarılması şarttır.

Saldırı yöntemi aşağıdaki örnekle açıklanmıştır

A,B ve C bilgisayarlarından oluşan bir sistem olsun. A bilgisayarının IP adresi yoluyla aldatma yöntemini kullanmak suretiyle kendisini C bilgisayarındaymış gibi göstererek, sunucu olan B bilgisayarına bağlanmaya çalıştığını düşünelim ve üç yollu el sıkışma mekanizmasında gerçekleşecekleri inceleyelim;

A bilgisayarı ilk SYN paketini gönderme konusunda bir zorluk yaşamayacaktır. Bu pakete kendi sıra numarasını (SN\_A) ekleyerek ve C bilgisayarından geliyormuş gibi göstermek üzere ‘kaynak adres’ kısmını değiştirerek B bilgisayarına gönderecektir. Bu paketi alan B sunucu bilgisayarı, SYN(SN\_B ) ACK (SN\_A+1) bilgilerini taşıyan paketi, kendisiyle haberleşmek istediğini düşündüğü C bilgisayarına gönderecektir. Üç yollu el sıkışma mekanizmasının tamamlanabilmesi için son paket olan ACK(SN\_B+1) paketinin B bilgisayarına gönderilmesi gerekir. Oysa SN\_B paket numarası bilgisini içeren paket, üç yollu el sıkışma mekanizmasını başlatan ve kendisini C bilgisayarı gibi gösteren A bilgisayarına değil de C bilgisayarına gönderilmiştir. Dolayısıyla A bilgisayarının kendisi kendisini C bilgisayarı gibi gösteren B sunucusuna bağlantıyı tamamlayabilmesi için, SN\_B değerini belirlemesi ve ACK (SN\_B+1) paketini yine C bilgisayarından geliyormuş gibi göstererek B bilgisayarına göndermesi gerekmektedir. Bunu başarabildiği anda üç yollu el sıkışma mekanizması tamamlanacak ve B sunucu bilgisayarı C bilgisayarı ile haberleştiğini düşünecektir.

Eğer bu saldırı, IP adresi ile yetkilendirme yapan bir servise yapılıyorsa, B sunucusunun C’ ye güvendiği ve ona verdiği yetki oranında, A bilgisayarı B üzerinde işlemler yapacaktır.

A bilgisayarının B sunucusuna C bilgisayarıymış gibi bağlanma senaryosu tablo2-3’de özetlenmiştir;

|  |  |  |  |
| --- | --- | --- | --- |
| Paket  Üretici | Kaynak  Adres | Hedef  Adres | Paket |
| A | C | B | SYN(SN\_A) |
| B | B | C | SYN(SN\_B), ACK(SN\_A+1) |
| A | C | B | ACK(SN\_B+1) |

Tablo 2-3 TCP el sıkışma mekanizması Bundan sonra karşılıklı bilgi akışı başlar.

Görüldüğü gibi saldırının en kritik noktası, A bilgisayarının SN\_B’ yi belirlemesidir. Eğer A bu değeri doğru olarak belirleyebilirse, saldırıya başlangıç için büyük oranda başarılı olmuş demektir. Sıra numarası bilgisinin ne şekilde verildiğini incelememiz, bu konuya da açıklık getirecektir. Bir bağlantıda kullanılacak sıra numarası bilgisi için bir başlangıç değeri belirlenir; daha sonradan da her veri aktarımında bu değer, aktarılan veri miktarı kadar arttırılır. Başlangıç değeri belirlenirken de, bu işlem için kullanılan, 32 bitlik sayıcıdaki değer kullanılır. Bu değer belli aralıklar ve durumlarda arttırılarak düzenli bir çalışmanın yapılması garanti edilmeye çalışılır. Her saniye için belli bir sayı ve her gerçekleşen bağlantı içinde bir başka sayı sayıcıya eklenir.

Acaba böyle düzenlenen bir sayıcıdaki değerin, dolayısıyla gerçekleşecek yeni bir bağlantıya verilecek sıra numarasının (senaryoda SN\_B idi), başka bilgisayarlarca (örnekte A) belirlenebilmesi, sayıcının düzenlenmesindeki algoritmanın ne kadar iyi olduğuna bağlıdır. Bu algoritmayla sıra numarasının tahmini kolaylaşmaktadır. Bunu yapacak saldırgan, hedef bilgisayara önce normal bir bağlantı gerçekleştirecek, hedef bilgisayardaki sıra numarası sayıcısının o andaki değerini belirleyecektir. Sonrasında da, sayıcının artış algoritmasını, hedef bilgisayarla aradaki mesafeyi ve diğer bazı unsurları göz önüne alarak, bir süre sonra kullanılacak sıra numarasını tahmin edebilecektir.

Bu tahminler yapılabildiği takdirde saldırı için gerekli zemin hazırlanmış demektir. Hedef bilgisayara güvenilir bir bilgisayar gibi ulaşılmış demektir.

Burada dikkat edilmesi gereken bir nokta daha vardır. Bağlantı kurulumu aşamasında B sunucu bilgisayarının, C bilgisayarına SYN (SN\_B) ACK(SN\_A+1) paketlerini göndermesi durumunda nelerin olacağının da göz önüne alınması gerekir. Böyle bir durumda, paketi C bilgisayarı algılarsa bağlantı isteğinde bulunmadığını gösteren RST paketini B bilgisayarına gönderecektir. Bu durumda B sunucu bilgisayarı üç yollu bağlantı işlemini kesecektir. Bu nedenle A bilgisayarındaki saldırgan ya C bilgisayarının devrede olmadığı bir anı gözleyecek ya da B bilgisayarının göndermiş olduğu paketin, C bilgisayarı üzerinden gideceği servise ilişkin portun SYN kuyruğunu doldurarak, bu paketin C bilgisayarı tarafından alınamamasını sağlayacaktır. Dolayısıyla C bilgisayarı cevap vermeyecektir.

Saldırıya ilişkin en kritik nokta, sıra numarasının tahmin edilebilir olmasıdır. Bu sayının tahmin edilemez hale getirilmesi durumunda saldırılar önlenecektir. Bunun için de sıra numarasını belirleyen sayıcının algoritmanın güçlendirilmesi gerekir.

### IP Servis Durdurma Saldırısı (smurf)

Yanlış kaynak adresi bilgisiyle oluşturulmuş ICMP ‘echo request” paketleri kullanılarak gerçekleştirilen, çoğu durumda hedef bilgisayarın kilitlenmesine sebep olan, ayrıca saldırıda hedef olarak kullanılan ağlarda önemli derecede performans sorunları yaratabilen bir saldırıdır. “smurf” adının verilmiş olması, saldırganların bu işlevleri yapan programlardan birisinin smurf olmasından dolayıdır.

Saldırı iki işlemden oluşmaktadır. Hedef alınan bilgisayarın IP adresinin “kaynak adres” olarak kullandığı sahte ICMP “echo request” paketlerinin hazırlanması ve bu paketlerin herkese yayınlanacak (broadcast) şekilde tüm bilgisayarlara yönlendirmesinin sağlanmasıdır.

ICMP (Internet Control Mesaj Protocol), ağ üzerindeki hataların belirlenmesi, bazı kontrol bilgilerinin karşılıklı değiştirilmesi, ağın belli açılardan gözetlenmesi imkanlarını sağlayan hizmetler verir. Bunlardan biri de, bir cihazın o anda açık olup olmadığını, belli fonksiyonları yerine getirip getirmediğini belirlemekte kullanılan hizmettir. ICMP bu işlemi gerçekleştirmek

için, denetlenmek istenen cihaza “echo request” paketi gönderir. Bunu alan cihaz ise, “echo reply” paketi ile, ağ üzerinde faal bir şekilde bulunduğunu bildirir. Bu sayede cihazların ulaşılabilir olup olmadığını, bu yolla da eğer bir sorun yaşanıyorsa sorunun nereden kaynaklandığını belirlemek mümkün olabilmektedir. Bu mekanizma çoğu işletim sistemi tarafından, genellikle de “ping” adı altında gerçeklenmektedir.

Saldırının ikinci unsurunu ICMP paketlerinin, bir ağın herkese yayın (broadcast) IP adresine yönlendirilmesi sonucu oluşturur. Bilindiği gibi çoğu durumda hazırlanan IP paketlerin “hedef adres” kısmında, paketin ulaşması gereken bilgisayarın IP adresi bulunur. Eğer hedef IP adres kısmında herkese yayın adresi varsa, bu paket tüm bilgisayarlara yöneltilecek demektir. Herkese yayın adresleri, IP adresinin konak kısımlarına ilişkin bitlerin tamamının ‘1’ olduğu adrestir. Örneğin C sınıfı bir IP adresi ağı için ağ IP adresi : 193.140.76.0 ise herkese yayın adresi : 193.140.76.255 olacaktır.

Saldırgan kendisine hedef olarak seçtiği cihazın IP adresini ‘kaynak adres’ kısmına yerleştirdiği ICMP ‘echo request’ paketlerini, yine ara hedef olarak seçtiği ve saldırısında basamak olarak kullanacağı ağın herkese yayın adresine gönderir. Böyle bir saldırıda saldırgan, ara hedef ve hedef olmak üzere üç nokta vardır. Şimdi belirtilen özellikteki paketlerin saldırgan tarafından üretilerek gönderilmesi durumunda olabilecek sonuçları inceleyelim.

Bilindiği üzere bu paketlerin ‘hedef adres’ kısmında, ara hedef ağın herkese yayın adresi bulunmaktadır. Dolayısıyla, eğer yol üzerinde veya ara hedef ağın internete açılan yüzünde bulunan yönlendiricide bu paketlerin filtrelenmesi yönünde bir çalışma yapılmamışsa, saldırgan tarafından üretilen paket, ara hedef olan ağa ulaşacaktır. Paket herkese yayın adresini taşıdığından, ağ üzerinde yer alan ve açık olan bütün bilgisayarlar tarafından alınacaktır. ICMP ‘echo request’ paketi olduğundan, paketin kaynak adres kısmında yer alan bilgisayara (hedef bilgisayar) ara hedef ağ üzerinde yer alan her bilgisayar ICMP ‘echo reply’ paketi gönderecektir. Bu paketler de ara hedef ağ trafiği üzerinde etkili olacak, performansı kötüleştirecektir. Saldırganın kullandığı paket boyu, gönderilme süresi ve ağda bulunan aktif bilgisayar sayısı arttıkça performans düşüşü daha fazla olacaktır.

Aslında asıl amaç ağa değil de hedef bilgisayara zarar vermektir. Bu da ağda yer alan bütün bilgisayarların ICMP ‘echo reply’ paketlerini hedef bilgisayara yöneltmekle gerçekleşmiş olur. Yoğun paket bombardımanına tutulan bilgisayar kilitlenir hatta yerel ağda da problemler çıkar. Saldırganlar bu yüzden birden fazla ara ağ kullanmaya çalışırlar.

Bu saldırı biçimi herkese yayın IP trafiğinin filtrelenmesi ve bilgisayarların herkese yayın IP kaynak adresli ICMP paketlerine cevap vermesinin engellenmesi yöntemleriyle engellenebilir.

### UDP Portlarından Saldırı

Smurf saldırılarının benzeri olan, ICMP paketleri yerine UDP paketlerinin kullanıldığı saldırı türüdür. Bir bilgisayar üzerinde veya birkaç bilgisayar arasında, gerçek UDP portlarına yöneltilecek yoğun paket akışıyla gerçekleştirilen bu saldırılar, tek bir bilgisayar üzerinde gerçekleştiriliyorken bu bilgisayarın performansının düşmesine, birden fazla bilgisayar arasında gerçekleştiriliyorken ise,ağın performansının düşmesine sebep olacaktır.

Birbiriyle haberleşmekte olan iki UDP servisinden birisi veya her ikisi, üreteceği yoğun paket akışıyla,karşısındaki bilgisayarın servisini kilitlemeyi, bilgisayarın performansını kötüleştirmeyi başarabilir. UDP servisleri bağlantı temelli olmadıklarından, herhangi bir el sıkışma mekanizması ya da bazı kontrol bilgilerinin karşılıklı değiştirilmesi gerekmediğinden, bu tür saldırılara açıktır.

Örnekle açıklayalım;

7 numaralı portu kullanan UDP echo servisi, karşısındaki bilgisayardan (istemci) aldığı bilgileri olduğu gibi geri gönderir. 19 numaralı port üzerinden servis veren UDP 'chargen' servisi ise, istemci bilgisayardan her paket alışında, rasgele sayıdaki verilerden oluşan paketi geri gönderir. Bu iki servise ilişkin UDP portlarının aynı bilgisayar üzerinde veya değişik bilgisayarlar arasında birbirine bağlanması, sonsuz bir trafiğin oluşmasına sebep olacaktır. Bu hem servisi veren bilgisayarı hem de trafiğin aktığı ağı etkileyecektir.

Böyle bir saldırı sonucunda doğabilecek sonuçları şunlardır:

Saldırının yöneltildiği servisler kilitlenebilir. Bu servisleri veren bilgisayarların performansı düşebilir ve servisleri veren bilgisayarların bulunduğu ağın trafiğini arttırır.

Bu saldırı tipinden korunmak için alınabilecek önlemlerin başında saldırıda kullanılan servislerin bilgisayarların üzerinden kaldırmak gelir. Bu servislere ilişkin paketlerin güvenlik duvarı üzerinden filtrelenmesini sağlamaktır. Tabii bu yaklaşım kullanılıyorken, iptal edilecek servislerin ne kadar gerekli olduğu da önemlidir. Bazı servislerden vazgeçilmesi zordur (Örneğin UDP kullan DNS servisleri). Böyle bir durumda iyi hazırlanmış paket filtreleme kuralları ile, sadece belli bilgisayarların bu servislerden yararlanması sağlanıp diğerlerinin ulaşmaları reddedilebilir. Bu tür saldırılarda en çok kullanılan UDP servisleri chargen ve echo servisleridir. Bu servisler aslında neredeyse hiç kullanılmazlar. Dolayısıyla bu servislerin iptal edilmesi ya da güvenlik duvarı üzerinden filtrelenmesi, normal çalışmayı etkilemeyecektir.

Bir bilgisayar üzerinde çalışan UDP echo ve chargen servislerini iptal etmek için yapılacaklar her sistem için farklıdır. Unix sistemler için yapılması gereken, inetd.conf dosyası içerisinde, bu servislere ilişkin tanımlamaların yapıldığı satırların başına '#' koymak ve o satırın dikkate alınmaması sağlanır. Aktif olması için sistemin tekrar başlatılması gerekir. Aynı işlemler diğer UDP servisleri içinde uygulanabilir. Böylece bu servislerden gelebilecek saldırılar önlenmiş olacaktır.

Saldırıların daha çok hangi servislere yapıldığının tespiti için ağa saldırıları kontrol edip raporlayan (intrusion detection) programların kullanılması faydalı olacaktır.

### NFS'e yönelik saldırılar

NFS (Network File System), ağ üzerindeki bilgisayarların dosyalarını birbirleriyle paylaşmalarını sağlayan bir protokoldür. Ancak bu protokolün açıklarının kullanılmasıyla, sistemi büyük zararlar verilebilecek bir saldırıya açmış olursunuz.

NFS uzun zamandır üzerinde çalışılan bir protokoldür ve saldırı programları internette yaygın olarak bulunmaktadır.

NFS'e yönelik saldırılar değişik sonuçlar doğurabilir. Saldırgan hedef bilgisayar üzerinde süper kullanıcı yetkisiyle işlemler yapabilecek duruma gelebilir.

Alınabilecek önlemeler;

Güvenlik duvarından NFS servislerine ait paketlerinin geçişi engellenebilir. Aynı şeklide internet üzerinden bu servislere ulaşım yasaklanabilir. Bu önlemeler NFS'e dışardan gelebilecek saldırılar içindir. İç ağdan gelebilecek saldırılara hala açıktır.

Güvenlik duvarı üzerinden alınabilecek önlemelerin yanı sıra /etc/exports dosyası üzerinde yapılacak bazı düzenlemelerle alınabilecek önlemlerde vardır. NFS ile ilgili yamaların takip edilip programa eklenmesi de saldırıların etkisini azaltacaktır.